Politecnico di Torino

Corso di Laurea Magistrale
in Ingegneria Aerospaziale LM-20
A. A. 2020/2021
Sessione di Laurea Dicembre 2021

Tesi di Laurea Magistrale

NO HAZARD APPROACH FOR THE CERTIFICATION OF COMMERCIAL PARTS ON EASA AIRCRAFT

Relatori:

Prof. Maggiore Paolo
Ing. Vazzola Matteo

Candidata:

Santaniello Luigia Rachele
Matricola 266091

SUMMARY

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The purpose of this thesis is to analyze the approach of the certification of commercial parts on EASA aircraft, the Airbus A320neo aeroplane and the Eurocopter AS350 Ecureuil (Airbus H125) rotorcraft, which results no safety criticals.

The analysis throws its roots in the study of the ICAO aeronautical regulation hierarchical structure and, in particular, the Certification Specifications CS25 and CS27, respectively related to large aeroplanes and small rotorcrafts. The focus has turned on the parts concerning to on-board systems and equipment, in order to derive the requirements necessary for the certification.

In parallel, the applicable standards ARP-4754A and ARP-4761 have been analyzed as a guideline for the development of this work, in order to give emphasis on safety aspects and demonstrate compliance with the airworthiness regulations.

However, the applicable standards DO-178B, DO-254, DO-160 and MIL-STD-810G are also considered in support of the demonstration the compliance of the products in exam with the regulations.

Firstly, the commercial parts are introduced and divided in two groups: on one side the UPS and a pair of batteries are analyzed, on the other side, the electronical items, Apple iPad Air 4 and Panasonic Thoughtbook 55 are considered as EFBs (Electronic Flight Bag), which must have minimal or negligible impact on safety (Design Assurance Level C and D). Secondly, an overview of the two aircraft features, A320neo and AS 350, is presented.

The derived requirements from the Certification Specifications, respectively CS-25 and CS-27, are compared with the parts features in order to demonstrate their compliance to the airworthiness regulations and the EFB requirements list is matched with the electronical items features. The results of the analysis is to verify the compliance with the requirements and to assess subsequently the possible mitigations actions to be implemented on board, in order to support an increasing employ of commercial parts already developed and known for specialized use, reducing design and testing costs and exploiting already existing resources.

In conclusion, the example of the applicability and the use of commercial parts in the space context is mentioned, referring to Ingenuity, which mounts a commercial and inexpensive Qualcomm® Snapdragon™ 801 processor.

The thesis work is carried out in collaboration with TPS Aerospace Engineering, under the careful supervision of Eng. Matteo Vazzola.

2 SAFETY AND RISK ASSESSMENT

In the past, aeroplane systems were designed to fulfil performance requirements, to the 'single failure' criterion, or to the fail-safe design concept, which define a safe design based on the failures effects and their combinations.

With the passing of the years, the development of the on-board aircraft systems focused particularly on more safety-critical functions and, inevitably, the system complexity enhanced. If on one hand, the systems were increasingly sophisticated and avant-garde, on the other hand the loss of one or more functions, provided by the systems, could have meant a potential hazard occurrence to the aeroplane and its occupants. Moreover, the interaction between systems performing different functions began to be considered in terms of malfunctions.

This experience has led to consider that the probability of a failure is inversely linked to its severity consequences.

In the aeronautical world, safety represents the probability that a system will not be affected by critical or catastrophic failures for a given mission, or more simply, the freedom from an unacceptable risk. In order to achieve safety objectives, therefore, it is necessary to manage tolerable risk, which is the risk accepted in a given context based on values imposed by human society.

Risk is defined as the product of the probability of a failure occurrence and the severity of the failure condition, FC, which is defined in the AMC 25.1309 as "*a condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events*", [1].

Starting from the definition of a certain tolerable risk, iso-risk curves are plotted, as shown in the Figure 1:

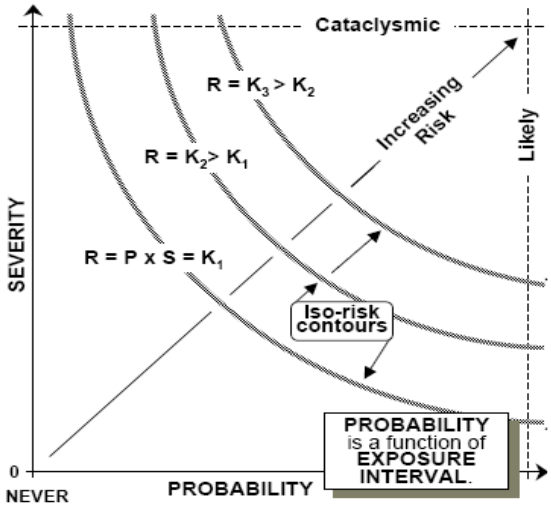

Figure 1: Iso-risk curves in function the severity of the failure consequences, [2]

Along the iso-risk contour, the risk is constant and identifies the event to be analyzed. The analysis will provide a value to compared with the tolerable risk: if it were to be greater, it must be downgraded to a tolerable level through maintenance actions or other interventions.

According to the MIL-STD-882D [3], the failure severity classification is provided in order to offer a qualitative measure of potential worst consequences, as described in the Table 1:

CATEGORY	CONSEQUENCE	DESCRIPTION
I	Catastrophic	Permanent damage or death of people and loss of systems
II	Hazardous	Severe injury to the people, major property damage, or major system damage which will result in mission loss
III	Major	Minor injury to the people, minor property damage, or minor system damage which will results in delay or loss of availability or mission degradation.
IV	Minor or Negligible	Not injury or system damage, but which will result in unscheduled maintenance or repair

Table 1: Failure severity classification according to MIL-STD-882D, [3].

The AMC 25.1309, [1], reports the previous categories and defines:

- **Minor**. FCs that would not affect aeroplane safety and the crew knows the operating procedures and is able to take actions.
- **Major**. FCs that would affect noticeably the safety, for example provoking the reduction of the safety margins and aircraft functionalities, the increase of the crew workload and the discomfort to occupants.
- **Hazardous**. FCs that would affect significantly the safety, determining an amplification of the effects mentioned before: the safety margins and aircraft are significantly reducted, the flight crew is not longer able to perform their tasks, due to the distress or the high workload and different injuries could regard a small number of occupants.
- **Catastrophic**. FCs which would irreversibly affect the safety, compromising it completely and causing deaths and the loss of the aircraft.

The AMC 25.1309 [1] also provide the probability of failure occurrence classification, as illustrated in the Table 2:

LEVEL	CATEGORY	PROBABILITY
A	Frequent	$\geq 10^{-1}$
B	Probable	$10^{-5} \leq P \leq 10^{-1}$
C	Remote	$10^{-7} \leq P \leq 10^{-5}$
D	Extremely Remote	$10^{-9} \leq P \leq 10^{-7}$
E	Extremely Improbable	$\leq 10^{-9}$

Table 2: Failure occurrence probability according to AMC 25.1309, [1].

In summary, failure conditions having more severe effects could be improbable to occur.

The risk matrix, at the basis of the risk assessment, summarizes and brings together the concepts set out above, because it represents the failure severity classification, as declared in the Safety Management System presentation from [4], in function of the probabilities of occurrence of the failure, as illustrated in the figure:

Risk Matrix

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					

Figure 2: ICAO risk matrix, source [4].

The yellow region identifies the acceptability band beyond which the risk is no longer acceptable and a new design must be provided.

In the entire system life cycle, the safety is considered and managed by the safety management system, which is an internal organizational structure to manage the risk associated with safety and ensure the effectiveness of the controls to guarantee it, developed throughout the product life and continuously updated.

Safety requirements are mandatory and are dictated by airworthiness entities such as ICAO and EASA. However, these requirements impose redundancies and/or additions of components that are not useful for the nominal mission, but which appear to be necessary in the event of a critical failure to fill up technological gaps and maintain the defined level of safety. In other words, these redundancies enhance the system complexity and cost, and the logistic reliability falls down.

With the safety requirements met, the design choices will be projected in terms of system effectivness (SE) . It could be defined as the comparison between the performances, the reliability and the mantainability and the LCC (life cycle cost), as defined in the equation (1):

$$SE = \frac{C * R_d * R_m * A(R_b, M)}{LCC} \quad (1)$$

where C is the capability, ability of the system to behave in such a way as to satisfy all requirements, R_d is the dispatch reliability, reliability at the start, R_m is the mission reliability and A is the availability, the ability of a system to perform a certain function

under certain conditions at a certain moment of time, that is function of the R_b, the logistic reliability, defined also as failure rate, and M, the maintanability, that is the ease of maintaining a system.

Consequently, the low logistic reliability, due to the redundancies, can be compensated by enhancing the maintainability of the aircraft and maximizing the availlability, such as going to increase the MTBF (mean time between failures) and decrease the MTTR (mean time to repair), that is the mean time for maintenance checks.

As reported from the AMC 25.1309 [1], historical data provide that the probability of a serious accident due to operational causes was approximately one per million hours of flight (10^{-6}), of which only the 10 % (10^{-1}) were attributed to failure conditions caused by the on-board systems. However, it was assumed, arbitrarily, that there are about one hundred potential failure conditions (10^{-2}) in an aircraft, defined as catastrophic. As a result, the average probability per flight hour for catastrophic failure conditions would be 10^{-9} which quantifies the probability term “extremely improbable”. This value represents the designed safety necessary to guarantee an achieved safety of 10^{-6}, which is two orders of magnitude higher.

The designed safety takes on different values depending on the aircraft category defined from the safety continuum.

According to the FAA [5], the safety continuum is a balanced approach between the safety objectives and the social expectations, which integrates the phases of design, production and operations in the safety and risk management, dictated by the airworthiness bodies, according to the type of aircraft category (type) for each of which there will be requirements to satisfy.

3 AERONAUTICAL REGULATION

The key approach of airworthiness bodies (ICAO, EASA, FAA) is the integration of the concept of safety and risk management in the design and production phases of the system and more generally of the aircraft.

These bodies promote a different approach depending on the category of aircraft (type), for each of which specific requirements will be obtained. This concept is the basis of the *Safety Continuum*. The types, according to the FAA [5] are:

- Part 25
- Part 23 Commuter
- Part 23 Class III
- Part 23 Class II
- Part 23 Class I
- Light Sport
- Experimental

As illustrated in the Figure 3, the social accepted risk decreases more and more while the operations complexity increases as the types of aircraft, considering that the zero risk level coincides to no air transport.

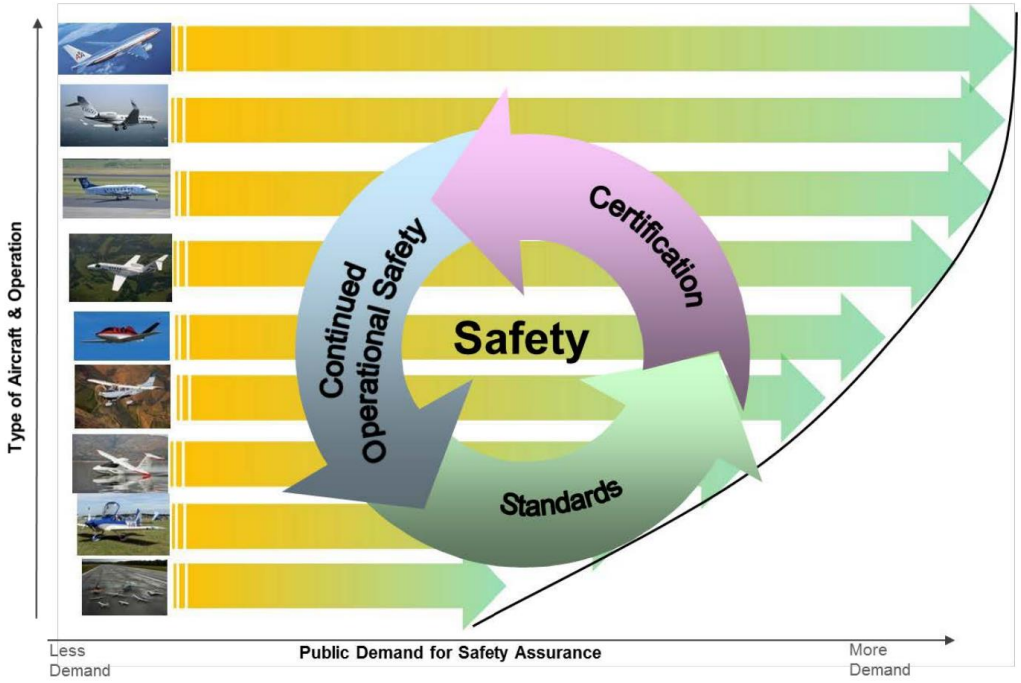

Figure 3: Safety continuum according to FAA, [5].

3.1 AIRWORTHINESS BODIES

The supranational airworthiness body is the ICAO (International Civil Aviation Organization), whose flag is reported in the Figure 4, a specialized agency of the United Nations. It lays the foundation of the modern international air navigation and promotes the planning and development of international air transport in a safe context, considering also the growth.

Figure 4: ICAO flag, [6].

For international civil aviation, the ICAO Council adopts standards and recommended practices concerning air navigation and its infrastructure. Moreover, the ICAO defines the protocols for air accident investigation and the 52 countries, participant to the Chicago Convention on International Civil Aviation in 1944, with their own transport safety authority, will continue the investigation.

The ICAO technical body, the Air Navigation Commission (ANC), is composed of 19 commissioners, who are independent expert with no political intents and provide to develop International Standards And Recommended Practices. Once approved by the commission, standards are sent to the Council, the political body of ICAO, for consultation and coordination with the member states before the final adoption.

The ICAO documentation structure is centred on Convention and Articles, from which descend 19 Annexes, inclusive of standards and recommended practices, to which appendices and attachments refer. The Convention and Articles are supported by the PANs (Procedures for Air Navigation Services) and helped to the obtaining of the Guidance and Circulars in order to be consulted from the applicant, always clarified and supported by policy statements, assembly resolutions and state letters.

3.2 FAA AND EASA

At the continental level, the main reference authorities are the FAA for the United States and the EASA for Europe, whose flags are shown in the Figure 5:

Figure 5: On the left, the FAA flag and on the right the EASA flag.

The FAA (Federal Aviation Administration) is the most important aviation agency of the U.S. government, regulating air traffic management, certificating aircraft, setting standards, training personnel and protecting the U.S. properties during the launch or re-entry of commercial space vehicles, as the organization declares in its statement: "*Our continuing mission is to provide the safest, most efficient aerospace system in the world*", [7]. Moreover, the ICAO delegated to the FAA the authority of supervise the surrounding international waters.

The EASA (European Aviation Safety Agency) is the child of the JAA (Joint Aviation Authorities), that was a voluntary association of the National Airworthiness Agencies of European States, established in 1970 with the aim of establishing common requirements for the aircraft design and construction, flight operations, maintenance and pilot licenses, in order to match the regulations of the Contracting States and ensure a high level of safety in the field of Civil Aviation.

Nowadays, EASA, as new regulatory system, has the fundamental role of promoting the most important common safety and environmental protection standards in the civil aviation in Europe and around the world and ensuring an unique European market in the aviation field.

The EASA main tasks presently include:

- Developing laws on safety and provide technical assistance to the European Commission and the member states in developing the regulations;

- Promoting inspections, training and standardization programs to guarantee uniform implementation of European aviation safety legislation in all member states;
- Providing and approving "Type Certifications" of aircraft and its parts to ensure their safety compliance to the environment and to the airports;
- Releasing certification approvals and guaranteeing supervision of the organizations, operating in the field of aircraft design, production and maintenance in third countries;
- Collecting data, analysis and research for the improvement of aviation safety;
- Issuing of the Airworthiness Directives.

3.2.1 EASA LEGISLATIVE PROCESS

EASA legislation is based on a hierarchical structure, such as the ICAO, that refers to the Chicago Convention of 1944 [8]. The structure can be schematized as illustrated in the Figure 6:

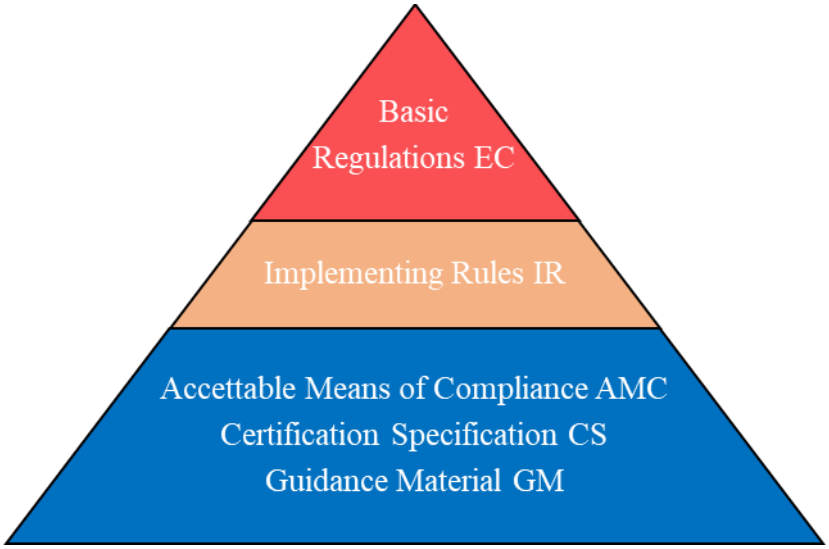

Figure 6: EASA legislative hierarchical structure.

The Basic Regulation and the Implementing Rules represent the so-called Hard Law: the first ones include absolutely mandatory regulations, coming from the European Parliament and the Council, and Essential Requirements ER, while the latter represent operational rules, with Cover Regulation and several annexes, released by the European Commission. At the basis of the pyramid, the Soft Law, released by EASA, includes the Acceptable Means of Compliance, the Certification Specification and the Guidance Material.

According to EASA [9], the Acceptable means of compliance (AMC) represent a set of no-mandatory standards adopted in order to help the applicant to implement the requirements and illustrate means to establish compliance and with the Basic Regulation and its implementing rules. Moreover, as reported in the [10], the Certification Specifications (CS) are technical standards, which include means to show compliance with the Basic Regulation and its implementing rules and represent a list of requirements to achieve by the organisations in order to obtain the certification. In conclusion, the Guidance material (GM) helps to clarify the meaning of a requirement or specification and support the interpretation of the Basic Regulation, its implementing rules and AMC, as mentioned in [9].

The basic regulation 1139/2018[1], [11], has issued two important implementing rules, from the European Commission, concerning:

1. the Initial Airworthiness n. 748/2012[2], [12], which deals with the implementation for the airworthiness and environmental certification for aircraft and related products and parts, and the regulations for the approval of design and production companies.
2. the Continuing Airworthiness n.1321/2014[3], [13], which include rules on the maintenance of the airworthiness of aircrafts and their parts and the approval of the companies and of the personnel capable of carrying out these tasks.

From the Initial Airworthiness descend the Annex Part-21, which aims to organize the design processes in order to track, evaluate and manage errors, which can be projected in terms of failure conditions, while from the Continuing Airworthiness descend the Part-M, the Part-145, the Part-66 and the Part-147, which purposes to organize the processes in order to maintain the airworthiness capability.

The Part 21 is divided in the Certification Specifications CS and the relatives Acceptable Means of Compliance AMC and Guidance Material GM, whose purpose is the compliance with product requirements, pursued by organizing processes, personnel, structures, software and machines.

According to [10], the list of the CS, contained in the Part-21, includes:

- CS-22 Sailplanes and Powered Sailplanes
- CS-23 Normal, Utility, Aerobatic and Commuter Aeroplanes
- CS-25 Large Aeroplanes
- CS-26 Additional airworthiness specifications for operations
- CS-27 Small Rotorcraft
- CS-29 Large Rotorcraft
- CS-31GB Gas Balloons
- CS-31HB Hot Air Balloons
- CS-31TGB Tethered Gas Balloons
- CS-34 Aircraft Engine Emissions and Fuel Venting
- CS-36 Aircraft Noise

[1] Official Journal Reference OJ L 212, 22.8.2018, p. 1–122;
[2] Official Journal Reference OJ L 224, 21.8.2012, p.1-85;
[3]Official Journal Reference OJ L 362, 17.12.2014, p. 1.

- CS-APU Auxiliary Power Units
- CS-AWO All Weather Operations
- CS-Definitions on Definitions and Abbreviations
- CS-E Engines
- CS-ETSO European Technical Standard Orders
- CS-LSA Light Sport Aeroplanes
- CS-P Propellers
- CS-SIMD Simulator Data
- CS-STAN Standard Changes and Standard Repairs
- CS-VLA Very Light Aeroplanes
- CS-VLR Very Light Rotorcraft
- CS-MMEL Master Minimum Equipment List
- CS-GEN-MMEL Generic Master Minimum Equipment List
- CS-CCD Cabin Crew Data
- CS-FCD Flight Crew Data
- AMC-20 General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances

In accordance with the 748/2012 regulation [12], the design companies must obtain the approval for the demonstration of capability from EASA. It includes the Design Organizations Approvals (DOA), such as the tracking of the applicated standards in the project.

EASA manages all the DOAs, issues the related DOA certificates, provides for their continued surveillance and releases the compliance statements for alternative procedures.

Similarly for the production, there is the POA (Production Organizations Approval), as mentioned in the Subpart G of EC 748/2012 [12].

3.3 AIRWORTHINESS

The "airworthiness" condition of the aircraft and its constituent parts through a process of certification of companies and products assures the safety, that is, in other words, acquire and own all the necessary requirements to fly in safe conditions within certain limits.

The imposition of restrictive airworthiness standards by the authorities guarantees on the one hand a high level of safety, but on the other hand it could make the certification process very long and complicated, due to economic and/or technical reasons. Consequently, it is necessary to find in the airworthiness regulations a proposal that is technically and economically reasonable, but nevertheless appropriate to the type of aircraft.

As mentioned in the previous chapter, ensuring safety involves costs and at a certain point, the additional increase of the level of safety is no longer synonymous with a “practicable” choice, given the raise in weight, cost or operating limitations. For this reason, each class of aircraft (airplanes, rotorcraft, acrobatic, etc.), divided in turn in different categories (depending on weight, number of passengers, etc), owns its airworthiness standard: as the complexity of the aircraft increases, according to the value of certain parameters, the level of complexity of the standard itself grows.

The airworthiness control of aircraft range over different type of activities from the certification of the aircrafts and their parts to the certification of the companies related to the design, production and maintenance, management of continuous airworthiness, to the licensing of the aircraft operators and flight personnel, whose exclusive competence is of the European Commission.

According to the [11] , the areas interested by the airworthiness are mentioned below:

- Approval and Design Organizations
- Production
- Aircraft Register
- Type Certificate
- Continuous airworthiness
- Maintenance
- Airworthiness Certificate
- Airworthiness Prescriptions
- EASA - Safety Information

- EU-USA bilateral agreement
- Remotely Piloted Aircraft Systems (RPAS)

The Basic Regulation 1139/2018 [11] claims that all aircraft, including products, parts and appliances installed, shows compliance with the essential airworthiness requirements, imposed in the Annex I of the Regulation. It is also required that all products, aircraft, engines and propellers have a Certificate of Approval (Type Certificate), released when the product and/or its modifications have been compliant to the requirements of the Certification Base.

Moreover, the regulation [11] explains that each aircraft, conforming to an approved type, is associated with an Airworthiness Certificate which verifies that the aircraft is operated and maintained in accordance with the essential requirements of continuous airworthiness. A "Permit to Fly" can be issued for single aircraft, of a non-approved type, which must be used for limited purposes, such as for example the case of experimental, demonstration, research and development flights.

In each member state, EASA has conferred powers to each Civil Aviation Authority of monitor and release approval of the design and operational organizations.

In Italy, ENAC supervise and helps companies, institutions, research centres and universities that operate in the aviation field, through training, consultancy and research activities, with the main objective of promoting the development of civil aviation.

Type Certificate (or Approval), submitted to EASA, is the document that demonstrates that an aviation product is compliant with the applicable requirements, including the EU Regulation 1139/2018 and the respective implementation rules or Part 21.

As EASA mentioned in the [14], a DOA company sets up the process for obtaining certification of an aircraft in four main steps:

1. *Technical Familiarization and Construction of a Basic Certification*, i.e., a set of requirements to be respected, applicable standards, recommended practices, which support the certification process.
2. *Establishment of a Certification Program*, which represents a set of steps to be followed and activities to be carried out to meet the requirements of the Certification Base and must produce a Compliance Documentation, including a series of reports, specifications, drawings, calculations and analyzes, including the so-called Safety Assessment.

3. *Compliance demonstration*, which represents the means which the applicant demonstrates compliance with the requirements of the regulatory: the structure, engines, control systems, electrical systems and flight performance are analyzed compared to the Certification Basis. This demonstration is supported by analysis during ground tests (such as bird strike) and during flight tests.
4. *Technical closure and issue of approval*, which is the closure of the EASA investigation and the issue of the certificate.

The release of the TC allows the start of series production. An example of the TC document is shown in the Figure 7:

EASA
European Union Aviation Safety Agency

TYPE CERTIFICATE

EASA.A.670

This certificate is issued by the European Aviation Safety Agency (EASA) in accordance with Regulation (EU) 2018/1139, in particular Article 77 (1) (e) thereof and Commission Regulation (EU) No. 748/2012 to

MAGNAGHI AERONAUTICA S.p.A.

VIA GALILEO FERRARIS 76/80
80142 NAPOLI NA
ITALY

and certifies that the product type design listed below complies with the applicable Type Certification Basis and, if applicable, environmental protection requirements when operated within the conditions and limitations specified on the associated Type Certificate Data Sheet Number: **EASA.A.670**

Type Design:	**Sky Arrow 600 Sport**
Model	**Initial Certification Date***
Sky Arrow 600 Sport	02 August 2019

*Note: With regard to a product for which a type certificate was issued before 28 September 2003 by an EASA Member State, the Initial Certification Date refers to the date of issuance of the initial type certificate of this product by the competent authority of that State.

Figure 7: Example of Type Certificate released by EASA, [15].

However, the Airworthiness Certificate, according to the art. 31 of the ICAO Chicago Convention, [8], declares that "*each aircraft performing international navigation must be provided with a Certificate of Airworthiness issued or validated by the Authority of the State in which the aircraft is registered*".

The European community legislation that contains the requirements for the release of the airworthiness certification for each aircraft is included in the Part-21, which concerns “Easy Access Rules for Airworthiness and Environmental Certification” (Regulation (EU) No 748/2012), [12].

Actually, the Annex Part 21 [16] defines the Airworthiness Directives as "*a document, issued or requested by EASA, which prescribes the actions to be carried out by an aircraft in order to restore an adequate level of safety, where the safety level of that aircraft is in danger of being compromised*". In particular, the AD requires the execution of inspections, replacements, modifications and procedures necessary and declared mandatory for the maintenance of the airworthiness of the aircrafts and its parts, in order to avoiding and/or preventing compromised conditions safety. For this purpose, in each AD, the unsafe conditions, the types of aircraft, parts and equipment involved, the corrective actions required and the necessary time must be highlighted.

The unsuccessful application or the failing of the compliance to these directives of an aviation product establishes the ending of the validity of the Airworthiness Certificate.

3.4 SAFETY ASSESSMENT

The issue of the airworthiness certificate occurs through different methodologies or philosophies, including the safety assessment.

In the aircraft design and certification, the safety assessment of equipment, systems, and installation represents an important milestone and it is essential to carry on the assessment in the early project phases in order to obtain unpleasant intervention leading to expensive design changes.

As previously mentioned, an acceptable level of safety inevitably implies an acceptable accident rate and regarding the systems, contrary to the structure, a probabilistic approach is considered.

The safety assessment dictates are contained in paragraph XX.1309 [10] of each CS, which provides indications concerning the safety for equipment, installations and systems and the bases to implement what EASA and in general, the airworthiness entity requires. It is associated with the AMC XX.1309 [1], which contains references to the recommended practices ARP 4754A [17] and ARP 4761 [18] and to the DO-178B [19] and DO-254 [20] standards and, as well as providing definitions of failure, failure condition, their classification, quantitative terms of probability of failure occurrence and the fail-safe design (introducing redundancies and a fault tolerance approach), mentioned above. In particular, the CS25.1309 [21] quotes that for systems:

"Any catastrophic failure condition must (i) be extremely improbable [1 in 10^{-9} *flight hours]; and (ii) must not result from a single failure."*

In the US, the paragraph XX.1309 is found in the FAR corresponding to the aircraft category.

Additionally, as suggests EASA [22], a Safety Program Plan should be created in order to manage adequately the safety assessment process. It specifies the objective and describes the safety activities that are appropriate at the aircraft level and then to the system level. For each level, the Failure Conditions are identified and tracked through the development process to prove that the design implementation is satisfying the safety criteria.

According to [22], the Safety Program Plan should cover these activities:

a. Establishing the requirements at the aircraft level, that must be implemented and analysed in the safety assessments;
b. Identifying applicable safety standards;

c. Recognizing the project safety organization, expressing its responsibilities and its relationship with partners and/or suppliers, being always compliant to the safety process;
d. Illustrating the content of the safety activities and the deliverables;
e. Explaining the key project milestones and the related reports which are needed;
f. Including the concepts of the management, validation of the safety requirements and the verification that the design shows compliance with these requirements;
g. Linking with the other appropriate plans (e.g. certification plan, validation and verification plan, process assurance plan).

The safety assessment process has the crucial role to establish adequate aircraft and systems safety requirements and to demonstrate that the implementation meets these requirements.

The safety assessment activities are described in the following sections of this document.

The guideline for the development of civil aircraft and systems focused on safety and the common modelling techniques to assess the safety of a system are respectively the recommended practices SAE ARP 4754A and SAE ARP 4761.

3.4.1 SAE ARP 4754A

In the early 90's, the FAA demanded SAE (Society of Automotive Engineering) to produce an aerospace recommended practice in order to demonstrate the regulatory compliance for highly-integrated or complex avionics systems and in 1996 the ARP4754A was published.

The ARP4754A, *Guidelines for Development Of Civil Aircraft and Systems*, [17], is a guideline for development of civil aircraft and systems which supports aircraft functions, focused on safety aspects. It represents a recommended no-mandatory practice, therefore it has the role of supporting the certification of Aircraft systems during "*the complete aircraft development cycle, from systems requirements through systems verification*", as mentioned, [17].

These practices help to solve interactions in systems development in a large and highly integrated environment. The ARP4754A includes:

- all necessary information to develop an aircraft system, considering the operating environment and the functions performed by the aircraft;
- the Integral Process, an iterative process that includes eight steps, including the Safety Assessment;
- Compliance with regulations;
- Context of Part 25 or CS 25;
- Guideline documents;
- Background documents (for compatibility).

In particular, according to the [17], the Integral Process consists of several steps:

1. Safety Assessment (compliance with regulations 1309 of the CSs), (System Safety);
2. DAL (development assurance level) assignment, which determines the rigor of complex hardware and software development and verification activities, to avoid human errors in the design phase that can have more or less serious consequences for safety in the denial of one of the functions they perform, (System Safety);
3. Requirements Capture (System Engineering): further detail for existing requirements and new derived requirements are identified at each requirements identification phase and allocation process (i.e., system and item);
4. Requirements Validation (System Engineering);
5. Implementation Verification (System Engineering);
6. Configuration Management (CM);

7. Process Assurance (Systems): it describes the means that ensure the development assurance activities are maintained and followed;
8. Certification and Regulatory Authority Coordination (Project Management PM).

The practice includes validation of requirements and verification of the design implementation for certification and product assurance, but it does not mention the development of the aircraft structure (that adopt a deterministic philosophy), the MMEL (most minimum equipment list), necessary to define the checklist, the CDL (Configuration Deviation List), modifications to the on-board installations in order to operate in different configurations, the Software Development (DO-178B), the Electronic Hardware Development (DO-254), the Guidelines and Methods for Conducting the Safety Assessment (ARP4761) and Safety Assessment of Transport Airplanes in Commercial Service (ARP5150).

The diagram in the Figure 8 highlights the relation between the Safety Assessment process and the System Development process.

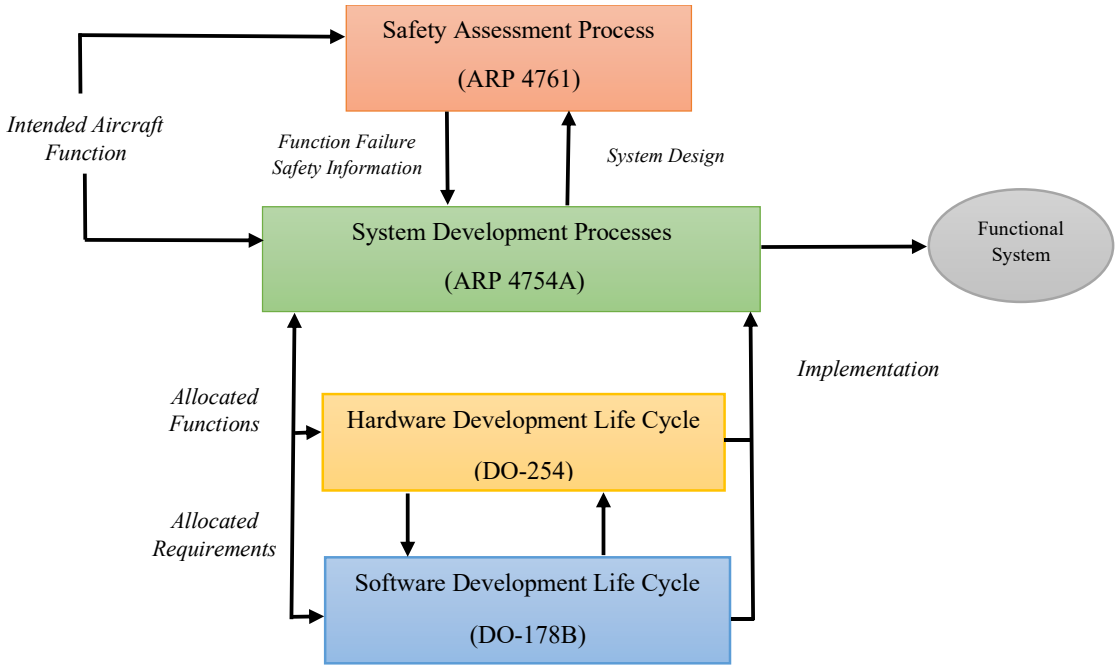

Figure 8: Relation between the Safety Assessment and System Development.

Starting from the initial planning phase, the Integral Process interfaces with the development process, which develops the functions of the aircraft, born in the concept, allocates these functions to each system, develops a system architecture (layering of functions across systems

with a tree structure), allocates the requirements of the systems to the components and proceeds with the implementation of the system.

The SAE ARP 4754A is schematized in the so-called V Diagram, reported below in the Figure 9, [17], which on the left side adopts a top-down approach, because it concerns the development and validation of safety requirements starting from the allocation of the requirements, first at the aircraft level, then at the system level and finally at the item level, then to proceed, on the right side, with the implementation of the design and move on to a bottom-up approach, in which the safety requirements are verified by gradually increasing levels.

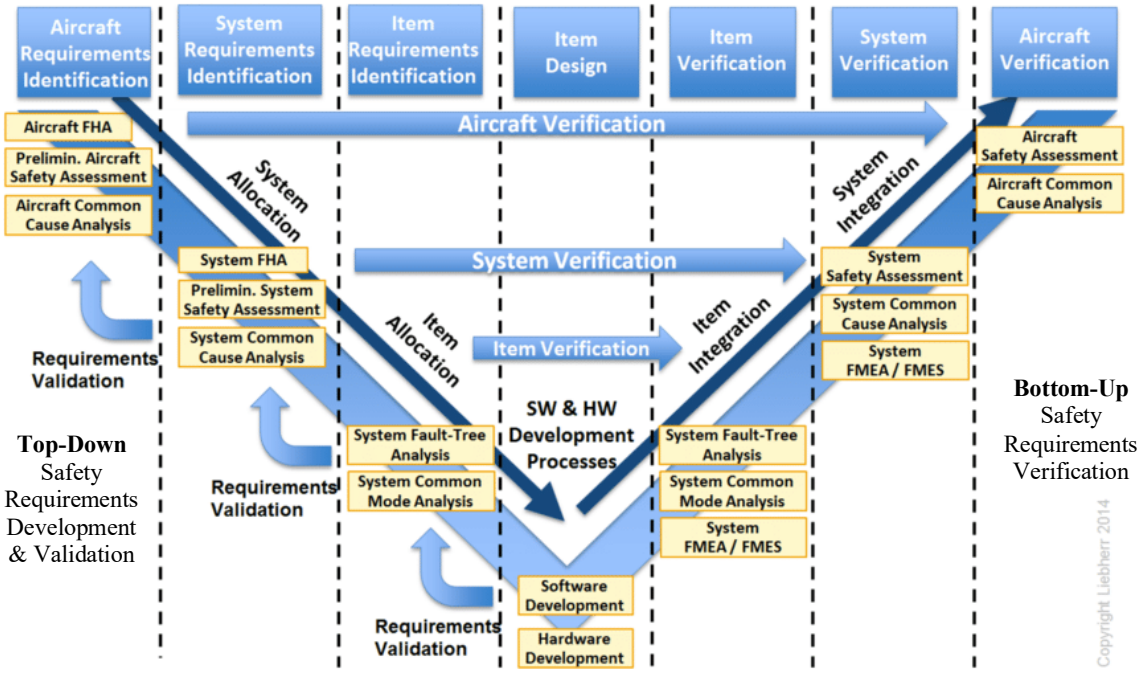

Figure 9: V Diagram of the ARP 4754A [17].

The process that guides the development of systems and their functions, controlling activities and results to obtain a certain level of performance, characteristics, and safety (human and environmental) is called Development Assurance. In other words, it represents all the actions planned and suggested by ARP 4754A, which serve to demonstrate with an adequate level of confidence that the project complies with the requirements defined by the reference CS and that errors in the design and implementation phases are identified and corrected, so that the system meets the applicable Certification Basis.

The purpose of Development Assurance is to develop the aircraft system with all the activities in order to guarantee the achievement of the objectives with a disciplined method, in which an assessment and limitation of the probability that errors made in the activities can impact the

safety of the whole aircraft. Human behaviour is regulated to ensure the constant updating of traceability, identification and correction of the errors.

The DAL (Development Assurance Level) for functions, equipment or software comes from the Safety Assessment and represents the method to prescribe more or less rigorous rules and measures depending on the criticality of the failure condition, in order to avoid errors during the development phases of the functions and systems. The procedures according to the DAL are also included in the DO-178B (for software development) and DO-254 (for the development of electronic hardware) standards.

As mentioned before, DAL allocation is related to the severity of the failure condition, considering that the failure condition can be caused by one or more failures and/or errors and the possible independence between the development processes can limit the consequences of the errors. Moreover, the DAL levels are defined with a letter, as the Table 3 shows:

DAL ASSIGNMENT	FC SEVERITY
A	• Catastrophic • Catastrophic from combination of errors between two or more independently functions or items.
B	• Hazardous • Hazardous from combination of errors between two or more independently functions or items.
C	Major
D	Minor
E	No safety effect

Table 3: DAL assignment criterion depending on FC severity.

The DAL can also be applied to the functions (FDAL), generated at the end of the Functional Hazard Analysis when the sub-functions are derived from the top level functions, and to the IDAL items, after the allocation and decomposition of the sub-functions into items.

However, the severity of the failure conditions depends on the operativity level of the aircraft and not on the magnitude of the damage that can be produced. Consequently, the DAL of an element can be reduced if the system presents:

1. Functional Redundancies, i.e. multiple implementations of the same function.
2. Partitioning, isolating the effects of a malfunction.
3. Automatic and active control of the element.

Despite the DAL level quantify the severity of the failure condition, it is often necessary to support it with a qualitative evaluation, through the FMEA and the FTA.

3.4.2 SAE ARP 4761

The SAE ARP 4761 "*Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*", [18], is a recommended practice which defines and illustrates the methods to assess systems safety.

As listed in the practice [18], the primary safety assessment processes are:

a. Functional Hazard Assessment (FHA): Identifies aircraft and system functions in order to find the potential functional failures and classifies the hazards associated with specific failure conditions, making the Catastrophic FC extremely remote. The FHA is developed early at the aircraft level, then at system level and at item level and it is updated as new functions or Failure Conditions are identified. Each function has its numbered reference.
b. Preliminary Aircraft Safety Assessment (PASA): defines the aircraft safety requirements and provide a preliminary indication for the architecture, compliant with safety requirements.
c. Preliminary System Safety Assessment (PSSA): a proposed architecture is examined to verify whether it meets the safety requirements at the system level, completing the list of failure conditions, identified by the FHA at the aircraft level, and the list of safety requirements. The PSSA can identify alternative strategies and its outputs are used in the definition of the SSA (System Safety Assessment), just as the PASA is used as an input for the ASA (Aircraft Safety Assessment). The PASA/PSSA are conducted iteratively at multiple stages of system development including aircraft, system, and item design definitions. At the lowest level, the PSSA determines the safety related design requirements of hardware and software.
d. System Safety Assessment (SSA): Collects, analyses, and documents verification that the systems, as implemented, meet the safety requirements established by the PSSA. The process is similar to the PSSA one, but it is more detailed, verify the integrity of the project and allows to close the system development;
e. Aircraft Safety Assessment (ASA): derives a list of the aircraft safety activities from the concept development to the detailed design development and purposes to show the compliance with aircraft level requirements, ensuring the application of the appropriate method (i.e. FTA, fault tree analysis; FMEA, failure modes and effect analysis; FMECA, failure modes and criticality effect analysis). In conclusion, it allows to release the aircraft CDR (Critical Design Review), review of the final project made by a multidisciplinary unit

that freezes the project, after which any modification to the project will be expensive and difficult.

f. Common Cause Analysis (CCA): analyses the common causes of failures, ensures that the functions are adequately independent in terms of repercussion of the failure and verifies that these requirements have been met. The concept of independence is linked to the physical and/or technical separation between the systems or the items, in order to minimize the chaining of events and reduce the probability of common errors. Consequently, it is necessary to confirm that such independence exists, or that the lack of independence is acceptable. The CCA offers the tools to verify this independence or to detect specific dependencies.

The mutual influence of systems and items can have different origins, thus the CCA exploits three methods to achieve the safety assessment:

i) PRA (Particular Risk Analysis): analyses the particular risks, that are the events which originate outside the airplane (or system), over which there is no jurisdiction and which may violate interdependence (i.e. afflict redundancies, concatenations of functions, fires on board, explosions due to high pressure, fluid-fuel leakage).

ii) CMA (Common Mode Analysis): analyses the common modes of failure and studies the manner of chaining events, related to human errors, installations and maintenance.

iii) ZSA (Zonal Safety Analysis): considers the physical interaction of the different failure modes of the components present in the same area of the aircraft and identifies more critical areas where adverse events can occur and then damage the aforementioned zone. The riskiest areas must be provided with independence, separating functions and/or systems.

These analyses may be executed at any stage of the design process. However, the most cost-effective phase is the preliminary design one, due to the potential influence on system architecture and installation. However, confirmation may not always be feasible until implementation is complete.

The Figure 10 summarizes the fundamental relationships between the four specific assessments mentioned before and the system development processes. In reality, there are many feedback loops within and among these relationships, not represented for better clearness.

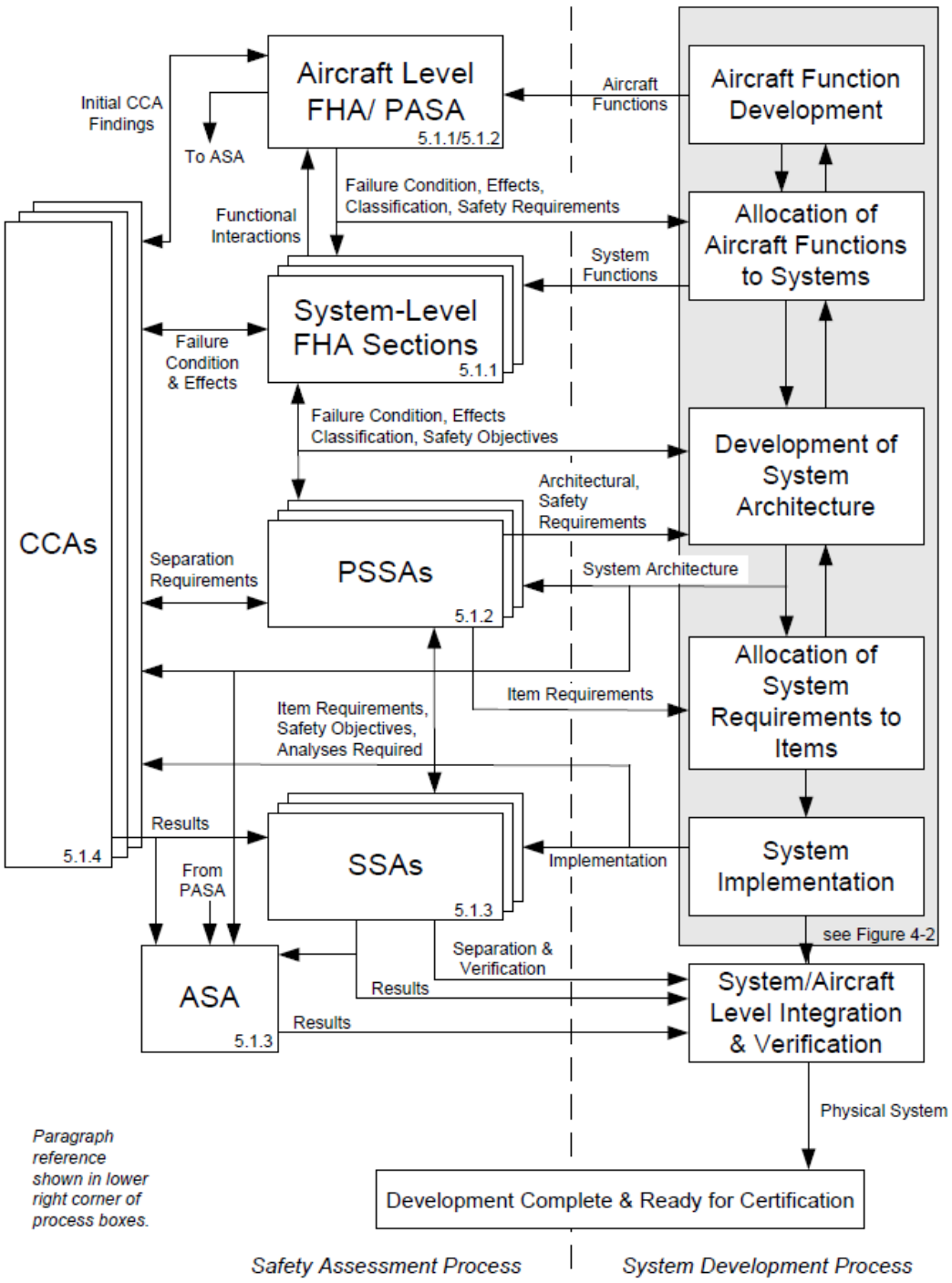

Figure 10: Relation between Safety Assessments at different levels and the System Development processes [18].

Each safety assessment activities provides its level of detail needed, depending on the aircraft-level Failure Condition classification, the degree of integration, and the complexity of the system implementation.

According to [18], the ARP 4761 suggests further analysis methods to identify and minimize the safety risks:

1. FMEA (Failure Modes and Effect Analysis) is a qualitative bottom-up technique used to consider how the basic components of a system can fail to perform their design objective. This could be implemented an equipment level or at a functional level. The technique is based on a detailed system description, contemplates the failure of each component of the system and its effects on the overall system. For each sub-component of the system the technique considers:
   a. All the potential failure modes.
   b. The effects that each of these failures would have on the system.
   c. The possible causes of the failure modes.
   d. All the mitigation actions applicable to the failures within the system or its environment.

   As reported from [18], malfunctions at system level, caused by the sub-component failures, which determines a safety impact, are identified as hazards. The analysis is applied at different system level, defined by the level of detail of the system description used to support the analysis. On one hand, the advantages of this method are surely the systematicity and rigor, the possibility to create a record of the hazards identification process and the ductility of being applied to a wide range of types of system, but, on the other hand, the disadvantages concern the fact that it contemplates hazards coming from a single-point failure modes rather than a combination of failures and the being cost and time expensive.

   A typical FMEA template, proposed by the ECSS-Q-ST-30-02A, [23], is shown in the Figure 11:

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)											
Product: Project/Phase: System/Subsystem/Equipment:					Prepared by: Approved by: Date:			Document reference: Issue: Page of			
Ident. number	Item/ block	Function	Failure mode	Failure cause	Mission phase/ Op. mode	Failure effects a. Local effects b. End effects	Severity	Failure detection method/ observable symptoms	Compensation provisions	Correction actions	Remarks

Figure 11: FMEA template according to ECSS-Q-ST-30-02A, [23].

2. FMECA (Failure Modes and Effect Criticality Analysis) is a quantitative bottom-up technique, similar to the previous one in the steps, but it classifies failure modes based on the criticality of the consequences for each mission phase or operating mode. The criticality is the measure that combines the severity of the failure and the probability of occurrence, identified by a critical number CN. If $CN \geq 6$, an element is critical, but even if the number is less, the element could be critical when it is single-point to failure, thus it has catastrophic consequences.
3. FTA (Fault Tree Analysis) is a top-down technique to solve the causes of an unwanted Top Event through the development of a Fault Tree, starting from a high-level event up to identifying the minimum combination of elementary events (Minimal Cut Sets) which generates that event. It is a detailed logical model from the relationship of the unwanted event to more basic events, developed according to the applicable standard ECSS-Q-ST-30-02A, [23]. The steps followed are:
   a. The causes of a specific failure (Top Event) are identified.
   b. The boundary within the analysis must develop are defined.
   c. The basic events and the human errors are identified.
   d. The probability of a certain failure occurring is quantified and what elements contribute.

   The tree basis consists of elementary events (represented by circles) which are linked together through logic gates, until going back to the starting point, the top event (parallelogram). The intermediate events are represented as rectangle. They can be AND gates, so to have the fault it is necessary that all the channels afferent to the gate are faulty, or the OR gate, in which only one fault is necessary to obtain the fault of the channel.

   To develop an FTA, a detailed knowledge of the system is required and in the case of more sophisticated analyses, you can refer to software, which solve the logic tree, solving the Boolean equation, through which you can find the Minimal Cut Set The great limitation of the FTA is the recognition of faults due only to the negation of functions.

   The Figure 12 shows an example of the FTA implementation, suggested by ICAO [24], which starts from the Top Event (Fire). For occurring fire, there needs to be both fuel, oxygen and an ignition source (Intermediate Event). The use of the AND gate is to underline that all three need to be present at the same time to make the top event

starts. The example shows three possible sources of fuel, three possible sources of ignition and a single source of oxygen, which represent the elementary events (circle). The OR gate means it would only need one of these to be present. This means that the loss can be prevented if just one of these sources is controlled. The numbers shown in the circles represent the probability of the primary failures, thus, through the combinations of these events, it could be calculated the probability of the occurrence of the Top Event.

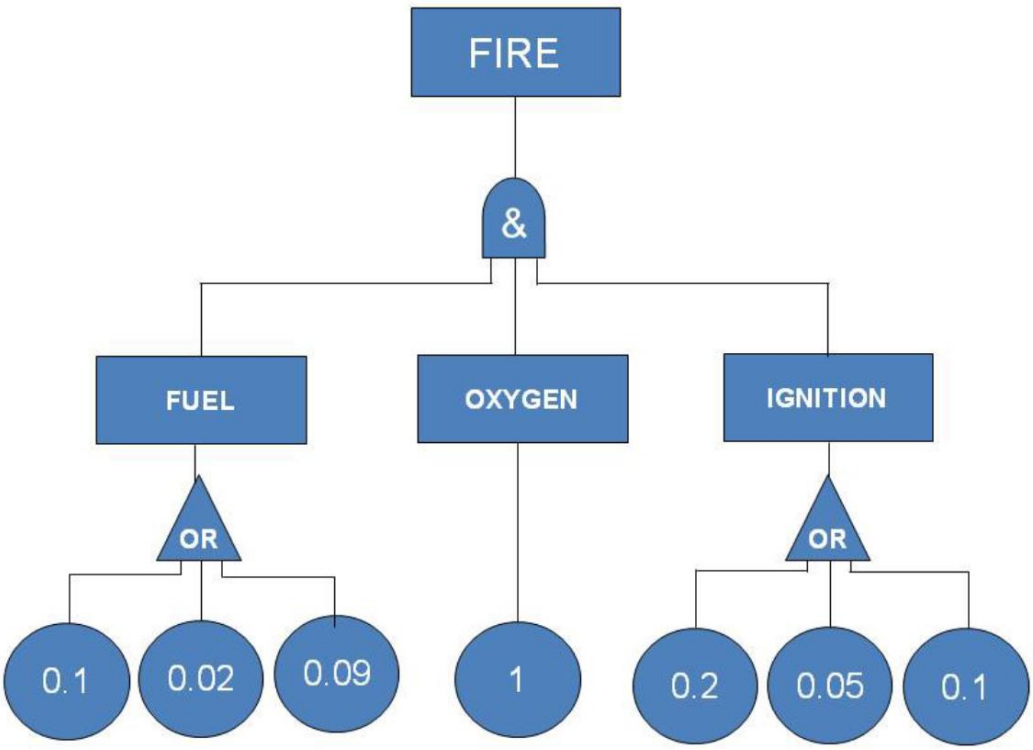

Figure 12: Fault Tree Analysis example from ICAO, [24].

3.4.3 RTCA DO-178B

The ARP 4754A, [17], involves the system development, but the software development is entrusted to the standard RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification,* [19]. It is a guideline concerning the safety development of software used in the airborne systems, developed in the first 90's by the safety-critical working group RTCA SC-167 (Radio Technical Commission for Aeronautics) and WG-12 of the European Organisation for Civil Aviation Equipment (EUROCAE), publishing the document as RTCA/DO-178B for RTCA and ED-12B for EUROCAE, [19].

Although technically a guideline, it is recognized worldwide for regulating safety in the integration and the development of the avionics software in the aircraft systems.

The life process of developing embedded software in aircraft systems is depicted in this document, but the intention of the DO-178B is not to be mandatory.

As mentioned in the previous chapter, the system safety assessments, combined with methods such as SAE ARP 4754A, determine the mitigation DAL and may allow obtaining of the DO-178B software level objectives to be satisfied. For this reason, DO-178B main theme is the design assurance and verification, after the prerequisite safety objectives have been determined.

According to the standard [19], the software level determines the number of objectives to be satisfied. The software that performs safety-critical functions will have assigned a high DAL level.

The independence between the software development team and the verification and validation processes guarantees the separation of responsibilities, clearly documented, and thus the integrity of the activities. In other words, for the objectives that must be satisfied with independence, the person who developed the item must not coincide with the person verifying the item (such as a requirement or source code). However, an automatic verification could be conducted by a qualified tool.

All system requirements be mapped as the Table 4 illustrates:

DAL	FC	OBJECTIVES	WITH INDIPENDENCE	FAILURE RATE
A	Catastrophic	66	25	$10^{-9}/h$
B	Hazardous	65	14	$10^{-7}/h$
C	Major	57	2	$10^{-5}/h$
D	Minor	28	2	$10^{-3}/h$
E	No Effect	0	0	N/A

Table 4: Objectives relating to the FC categories, according to the DO-178B, [19].

The standard does not prescribe the application of a precise development scheme but describes separate processes which regards multiple life cycles and their interactions. The progression of the processes to be implemented depends on the project and its properties.

The DO-178B articulates the life cycle of a software in four main activities, [19]:

1. SW PLANNING PROCESS determines what will be done to produce safe, requirements-based software, compliant to airworthiness requirements. The objectives of this phase are:
   a. Identifying the system requirements and certification levels.
   b. Defining the inter-relationships between processes, sequencing, feedback, and transition criteria.
   c. Establishment of the lifecycle environment, in terms of methods and tools.

   The process plans obtained are the Plan for Software Aspect of Certification (PSAC), Software Development Plan (SDP), Software Verification Plan (SVP), Software Configuration Management Plan (SCMP) and Software Quality Assurance Plan (SAP).
2. SW DEVELOPMENT PROCESS coincides most of the time with V model and concerns:
   a. SW REQUIREMENTS PROCESS analyses the system architecture and requirements to generate the high-level requirements, which are relating to function, performance, interface, and safety. These requirements must be provided to the System Safety Assessment for their validation.
   b. SW DESIGN PROCESS develops the Design Description, where the requirements obtained previously are reduced iteratively in order to extract the low-level requirements and the software architecture, necessary to implement the source code. The derived requirements must be defined and analysed by the System Safety Assessment Process

to ensure that the high-level requirements are not compromised. The Software Design Process is complete when both the associated Integral Processes and its objectives are achieved.

c. SW CODING PROCESS products the source code from the design process and its integration into a real-time environment. The source code must be traceable, verifiable, consistent and must correctly implement the low-level requirements. The object code is also generated and, once again, the process is complete when both the associated Integral Processes and its objectives are achieved.

d. SW INTEGRATION PROCESS develops the finished system (Integrated airborne system or equipment), exploiting the target computer, the Source Code and the Object Code produced by the Software Coding Process.

   The goal of the Integration Process is to load the Executable Object Code into the user equipment for hardware/software integration.

3. SW VERIFICATION PROCESS identifies and reports any errors resulting from the development and ensures that the same verification process is exhaustive. The activity is carried on with reviews, testing, integration and more. Verification cases and procedures, Verification results, analysis and traceability are obtained.
4. SW CONFIGURATION MANAGEMENT PROCESS establishes safe and effective configuration control for all the artifacts and provides the archive and the revision identification of developments environment, integration tool and other documents.
5. SW QUALITY ASSURANCE PROCESS ensures that the software life cycle process is going to produce a quality software and each process is analysed in order to obtain the expected outputs. Any changes are reported, evaluated, and resolved to guarantee process integrity.
6. SW CERTIFICATE LIAISON establishes the communication and the understanding between the applicant and the certification authority, to whom is provided the compliance substantiation.

The FAA, [25], illustrates all the process in the scheme shown in the Figure 13, where the recursive aspect is highlighted:

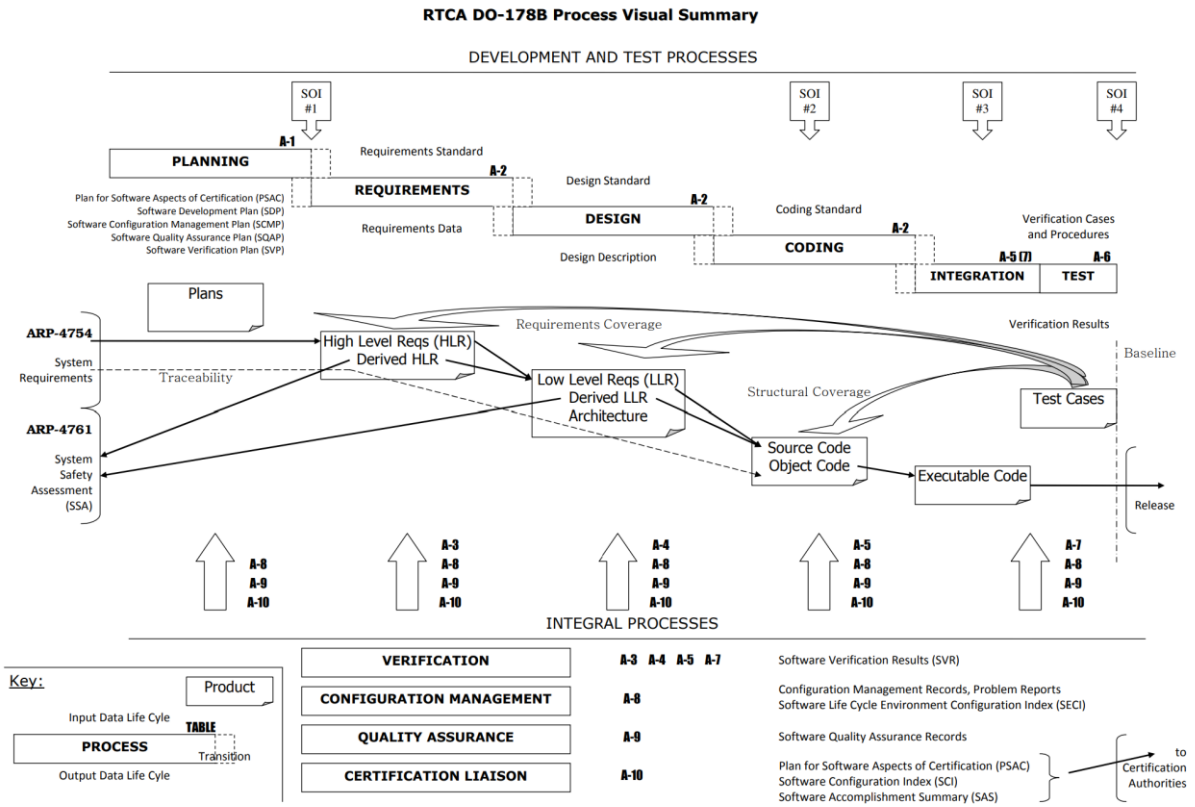

Figure 13: RTCA DO-178B Process visual summary, according to the FAA, [25] .

Nowadays, the RTCA DO-178C/EUROCAE ED-12C replaced the DO-178B/ED-12B standard, with an upgrade which interested the "core" guidance and produced four significant new documents, [26]: Software Tool Qualification Considerations (RTCA DO-330/EUROCAE ED-215), Model-Based Development and Verification (RTCA DO-331/EUROCAE ED-218), Object-Oriented Technology and Related Techniques (RTCA DO-332/ EUROCAE ED-217) and Formal Methods (RTCA DO-333/EUROCAE ED-216).

The resulting standard, published in December 2011, preserve the original DO-178B purpose of providing an objectives-based approach in order to obtain safety confident level that complies with airworthiness requirements, and extend the guidance to account for major technological improvements.

3.4.4 RTCA DO-254

With the increasing complexity of the electronic hardware employed in aircraft safety critical functions, new safety and certification considerations must be adopted. The formal safety standard applied to complex aircraft hardware is the DO-254/ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* [20].

The document provides design guidance assurance for the development of airborne electronic hardware, so that it safely performs its intended function in its defined environment.

It also classifies electronic hardware items into simple or complex categories: according to the standard, the simple item as "*if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour*", [20]. On the contrary, a complex item assurance must be achieved by additional means, i.e., commonly supposed to be complex custom micro-coded components, as field programmable gate arrays (FPGA), programmable logic devices (PLD), and application-specific integrated circuits (ASIC), including any associated macro functions.

Moreover, the DO-254 establishes objectives and activities for the systematic design assurance of the electronic hardware, and, similarly to the DO-178B, requires that all system requirements be mapped to:

DAL	FC	OBJECTIVES	FAILURE RATE
A	Catastrophic	40	$10^{-9}/h$
B	Hazardous	39	$10^{-7}/h$
C	Major	37	$10^{-5}/h$
D	Minor	31	$10^{-3}/h$
E	No Effect	0	N/A

Table 5: Objectives relating to the FC categories, according to the DO-254, [20].

The DO-254/ED-80 standard is the counterpart to the deep-rooted software standard RTCA DO-178C/EUROCAE ED-12C. With DO-254/ED-80, the certification authorities have highlighted that hardware and software in the avionic equipment are critical to safe operation of aircraft.

The document describes five DALs, A through E, which depend on the consequences effect of a failure on the aircraft. A highly critical system will receive a higher DAL, with DAL A reserved for the most critical systems. For DO-254, the difference between meeting DAL A and DAL B is minimal. Level A is the most severe, defined as "catastrophic" effect (e.g., deaths and/or loss of the aircraft), while a failure of Level E hardware will not affect the safety of the aircraft. Being compliant with level A requires a much higher level of verification and validation than the other levels compliance.

The DO-254 is also a process-oriented standard, as the Figure 14 from [27] illustrates:

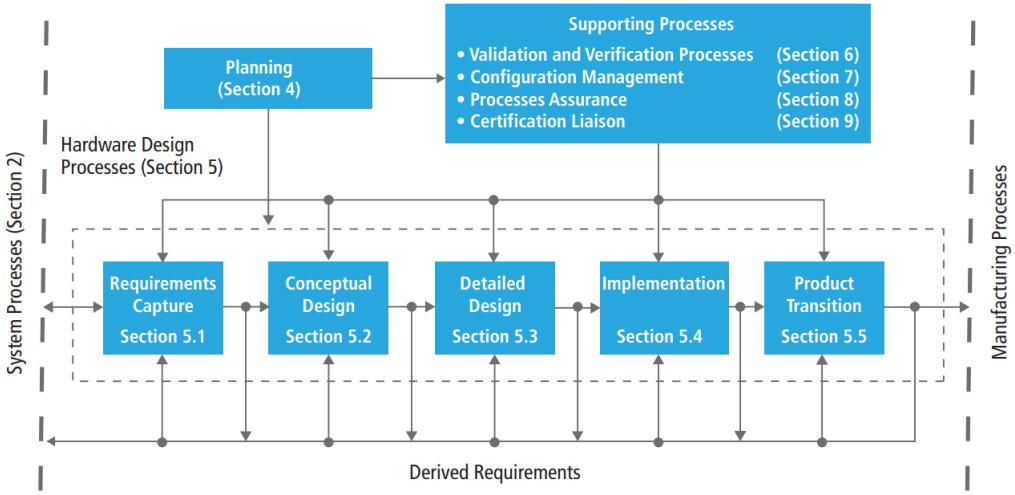

Figure 14: DO-254 process, [27].

In the Hardware life cycle process, the hardware design and hardware verification need to be done independently.

As described in the standard [20], the content includes:

1. HW PLANNING PROCESS defines the means by which the functional and airworthiness requirements are converted into the hardware item with acceptable level of confidence of assurance that the item will safely perform its intended function. Moreover, the standards are selected, the hardware development and verification environments are established, and the means of compliance are defined.

   The planning process is the first step where the design company announces its approach towards the certification. First, the company submits to the authorities (i.e., EASA, FAA) its approach to the standard and how it is implemented, through the PHAC (Plan for Hardware Aspects of Certification).
2. HW DESIGN PROCESS is divided in different steps:

a. REQUIREMENTS CAPTURE AND VALIDATION, that identifies and records all types of hardware item requirements in an iterative process.
b. CONCEPTUAL DESIGN, that produces a high-level design concept, gradually broken down into smaller, more manageable components.
c. DETAILED DESIGN, that obtains detailed design data using the high-level requirements and data of the previous step. For each component described in the conceptual design, the hardware design should implement requirement for that component. Each high-level requirement should be traced to the top-level module implementing that requirement.
d. IMPLEMENTATION exploits the detailed design data to generate the hardware item.
e. PRODUCTION TRANSITION PROCESS, where the manufacturing data, test facilities and general resources must be examined to ensure availability and suitability for production.

3. HW VERIFICATION & VALIDATION PROCESS
   a. VALIDATION PROCESS ensures that the derived requirements are correct and complete with respects to the system requirements allocated to the hardware item, throughout the design life cycle.
   b. VERIFICATION PROCESS provides assurance that the hardware item implementation being compliant with the requirements, through reviews, tests analyses and assessment of the results.
4. CONFIGURATION MANAGEMENT PROCESS provides the ability to consistently replicate the configuration item CI, regenerates the information and modify the CI if necessary. It also allows the collection of the documents, the tracking, and the identification of the data.
5. PROCESSES ASSURANCE ensures that the life cycle process objectives are met, and the activities are completed as outlined in the plans. The process assurance activities should be achieved with independence, in order to avoid subjective assessments.
6. CERTIFICATION LIAISON establishes a communication between the applicant and the certification authority.

The standard also dedicates a section to the Tool Assessment and Qualification process, that represent another important aspect of the DO-254 process. Tools used during verification and design could introduce new sources of errors and therefore must be tested to an acceptable level

of confidence. In fact, if a tool fails to detect an error in the hardware test, the entire DO-254 process is compromised. The tool is identified, classified as a design tool, or verification tool and evaluated on a level of A to E depending on the effect consequences of the failure.

3.4.5 RTCA DO-160

Important aircraft navigation and communications systems must be robust enough to withstand the different environmental conditions faced during all the flight envelope. For this reason, near to the DO-254 and DO-178B, it is concurrently contemplated the RTCA DO-160, *Environmental Conditions and Test Procedures for Airborne Equipment,* [28] in order to standardize the production and testing of these sensitive components.

The standard represents a set of procedures and environmental test practices for testing airborne equipment for all aircraft categories from light general aviation aircraft and helicopters to the military aircraft.

In particular, the document outlines a set of minimal standard environmental test conditions and corresponding test procedures for airborne equipment.

The aim of these tests is to provide a controlled method in order to assure the invariance of the performance characteristics of airborne equipment in environmental conditions similar to those possibly faced in the aircraft operations.

According to the standard [28], the description of the standard conditions and then all the environmental test conditions and test procedures are presented in the following order:

1. TEMPERATURE AND ALTITUDE, that check the effects (in terms of performance) of temperature and altitude, including loss of cabin pressure, on the equipment.
2. TEMPERATURE VARIATION, that exercises the items capability of surviving extreme temperature changes and the effects of varying coefficients of thermal expansion.
3. HUMIDITY, that checks the effects of high concentrations of humidity and the item ability to face the moisture effects.
4. OPERATIONAL SHOCK AND CRASH SAFETY, that checks the effects of mechanical shock.
5. VIBRATION, that checks the effects of vibration and the equipment's capability to operate during all vibration scenarios.
6. EXPLOSION PROOFNESS, that submits the item to an environment under vacuum, with a gaseous mixture of combustibles.
7. WATERPROOFNESS, that submits the item to dripping water or pooled water scenarios in order to check the unit will completely perform its functions.
8. FLUIDS SUSCEPTIBILITY, including different fluids, from the beverage to cleaners.

9. SAND AND DUST, that submits the item to an environment of blowing sand and dust of specific particle sizes, where the item must operate at the end of exposures.
10. FUNGUS RESISTANCE, that determines which material is negatively affected by fungi.
11. SALT & FOG, that proves that the test item survives the multiple exposures of salt fog and the accelerated corrosion.
12. MAGNETIC EFFECT, that ensures the lack of magnetic interferences on board.
13. POWER INPUT, that replicates the conditions of aircraft power from before engine start to after landing.
14. VOLTAGE SPIKE, that establishes if an equipment can resist the effects of voltage spikes when it touches its power leads, either AC or DC.
15. AUDIO FREQUENCY CONDUCTED SUSCEPTIBILITY - POWER INPUTS, that decides if the equipment will accept frequency of the components.
16. INDUCED SIGNAL SUSCEPTIBILITY, that establishes the acceptance of a level of induced voltages caused by the installation environment from the equipment.
17. RADIO FREQUENCY SUSCEPTIBILITY (Radiated and Conducted), that concerns the radiated susceptibility.
18. EMISSION OF RADIO FREQUENCY ENERGY, that is relating to the radiated emissions (HIRF, High-intensity radiated field).
19. LIGHTNING INDUCED TRANSIENT SUSCEPTIBILITY, that matters the lightning susceptibility and
20. LIGHTNING DIRECT EFFECTS, that concerns the lightning direct effects.
21. ICING, that defines the performance characteristics variation under conditions of rapid changes in temperature, altitude, and humidity.
22. ELECTROSTATIC DISCHARGE, that checks for resilience against the ESD during operation.
23. FIRE, FLAMMABILITY, that ensures the item does not represent a source to fire.

These procedures can be used in conjunction with applicable equipment performance standards (minimum specification under environmental conditions), in order to ensure a satisfactory degree of confidence in performance.

3.4.6 MIL-STD-810

The DO-160 standard has a military-grade equivalent proposed by the FAA which is MIL-STD-810, *Environmental Engineering Considerations and Laboratory Tests,* [29].

The standard [29] includes environmental management, engineering processes, military acquisition program planning and engineering direction, necessary to assess the impact of the environmental conditions on the equipment during all its entire service life.

The purpose of this standard is to define environmental stress features, develop test conditions customized to the equipment and its environmental life cycle, assess equipment performance when exposed to these strong conditions, identify defects in features, processes and methods regarding the equipment and demonstrate compliance with regulatory requirements.

According to the MIL-STD-810G [29], it is divided in three parts:

1. Part One describes management, engineering and technical roles in the environmental design and test process.
2. Part Two covers the environmental laboratory test methods to be applied exploiting the Part One guideline.
3. Part Three contains a collection of climatic data and guidance, coming from numerous military sources.

In conclusion, as evidenced in the standard [29], there are limitations relating to the laboratory testing that impose to use proper engineering judgment to evaluate the laboratory results. In fact, in many situations, test laboratories are not able to replicate real-world environmental stresses (singularly or in combination), therefore the laboratory and verification testing approval may not coincide.

4 DERIVATION OF THE REQUIREMENTS FROM THE CERTIFICATION SPECIFICATIONS

According to EASA [10], the Certification Specifications (CS) are no-mandatory technical standards adopted in order to meet the fundamental requirements of the Basic Regulation. Moreover, the CSs are exploited in the establishment of the certification basis (CB).

In this work, CS-25 and CS-27, respectively relating to Large Aeroplanes and Small Rotorcraft, are considered.

The CS-25 is dedicated to turbine powered Large Aeroplanes. The standard [21] is divided in nine subparts and sixteen appendices, supported by the relative AMC-25 that provides guidelines necessary to implement the requirements, showing the means to establish compliance and with the Basic Regulation.

Similarly, the CS-27 is associated to the Small Rotorcraft, with maximum weights of 3175 kg and nine or less passenger seats. The document [30] consists of seven subparts and four appendices, supported by its AMC-27.

The subparts considered in this work are tailored to those equipment that do not affect the safety.

Consequently, all the requirements regarding to the engine, the powerplant, the primary avionics equipment, the navigation and communication instruments and the structure are excluded from the analysis.

The items involved in this assessment fall into the category corresponding to a low DAL (D or E), which means that the impact on the safety of the failures, caused by these items, is minor or negligible.

4.1 CERTIFICATION SPECIFICATION 25

The CS-25 parts examined are:

- Subpart C (Structure)
- Subpart D (Design and Construction)
- Subpart F (Equipment)
- Subpart G (Operating Limitations and Information)

For each subpart, the CS-25 obtained requirements are verbatim stated, as the regulation reports [21], in the following tables. The texts are not fully reported from the EASA standard, because the aim is to focus on the dictates of interest of the work.

1. SUBPART C

REQUIREMENTS	TOPIC	DESCRIPTION
CS 25.365	PRESSURIZED COMPARTMENT LOADS	*"Any structure, component or part, inside or outside a pressurised compartment, the failure of which could interfere with continued safe flight and landing, must be designed to withstand the effects of a sudden release of pressure through an opening in any compartment at any operating altitude".*
CS 25.561	EMERGENCY LANDING CONDITIONS	*"For equipment, cargo in the passenger compartments and any other large masses, the following apply:* *(1) These items must be positioned so that if they break loose, they will be unlikely to:* *(i) Cause direct injury to occupants;* *(ii) Penetrate fuel tanks or lines or cause fire or explosion hazard by damage to adjacent systems;* *(iii) Nullify any of the escape facilities provided for use after an emergency landing.* *(2) When such positioning is not practical (e.g. fuselage mounted engines or auxiliary power units) each such item of mass must be restrained under all loads up to those specified in sub-paragraph (b)(3) of this paragraph. The local attachments for these items should be designed to withstand 1·33 times the specified loads if these items are subject to severe wear and tear through frequent removal (e.g. quick change interior items).* *(d) Seats and items of mass (and their supporting structure) must not deform under any loads up to those specified in*

		subparagraph (b)(3) of this paragraph in any manner that would impede subsequent rapid evacuation of occupants".
CS 25.581	LIGHTINING PROTECTION	*"(a) The aeroplane must be protected against catastrophic effects from lightning.* *(b) For metallic components, compliance with sub-paragraph (a) of this paragraph may be shown by:* *(1) Bonding the components properly to the airframe; or* *(2) Designing the components so that a strike will not endanger the aeroplane.* *(c) For non-metallic components, compliance with sub-paragraph (a) of this paragraph may be shown by:* *(1) Designing the components to minimise the effect of a strike;* *(2) Incorporating acceptable means of diverting the resulting electrical current so as not to endanger the aeroplane".*

Table 6: CS-25 Subpart C requirements, [21].

2. SUBPART D

REQUIREMENTS	TOPIC	DESCRIPTION
CS 25.611	ACCESSIBILITY PROVISIONS	*"(a) Means must be provided to allow inspection (including inspection of principal structural elements and control systems), replacement of parts normally requiring replacement, adjustment, and lubrication as necessary for continued airworthiness. The inspection means for each item must be practicable for the inspection interval for the item. Non-destructive inspection aids may be used to inspect structural elements where it is impracticable to provide means for direct visual inspection if it is shown that the inspection is effective and the inspection procedures are specified in the maintenance manual required by CS 25.1529".*
CS 25.683	OPERATION TESTS	*"(c) It must be shown that under vibration loads in the normal flight and ground operating conditions, no hazard can result from interference or contact with adjacent elements".*
CS 25.771	PILOT COMPARTMENT	*"(e) Vibration and noise characteristics of cockpit equipment may not interfere with safe operation of the aeroplane".*

CS 25.789	RETENTION OF ITEMS OF MASS IN PASSENGER AND CREW COMPARTMENTS AND GALLEYS	*"(a) Means must be provided to prevent each item of mass (that is part of the aeroplane type design) in a passenger or crew compartment or galley from becoming a hazard by shifting under the appropriate maximum load factors corresponding to the specified flight and ground load conditions, and to the emergency landing conditions of CS 25.561(b).* *(b) Each interphone restraint system must be designed so that when subjected to the load factors specified in CS 25.561 (b)(3), the interphone will remain in its stowed position".*
CS 25.831	VENTILATION	*"(c) There must be provisions made to ensure that the conditions prescribed in subparagraph (b - Crew and passenger compartment air must be free from harmful or hazardous concentrations of gases or vapours) of this paragraph are met after reasonably probable failures or malfunctioning of the ventilating, heating, pressurisation or other systems and equipment".*
CS 25.863	FLAMMABLE FLUID FIRE PROTECTION	*"(a) In each area where flammable fluids or vapours might escape by leakage of a fluid system, there must be means to minimise the probability of ignition of the fluids and vapours, and the resultant hazards if ignition does occur".*
CS 25.869	FIRE PROTECTION: SYSTEMS	*"(1) Components of the electrical system must meet the applicable fire and smoke protection requirements of CS 25.831(c) and CS 25.863".*
CS 25.899	ELECTRICAL BONDING AND PROTECTION AGAINST STATIC ELECTRICITY	*"(a) Electrical bonding and protection against static electricity must be designed to minimise accumulation of electrostatic charge, which would cause:* *(1) Human injury from electrical shock,* *(2) Ignition of flammable vapours, or* *(3) Interference with installed electrical / electronic equipment.* *(b) Compliance with sub-paragraph (a) of this paragraph may be shown by* *(1) Bonding the components properly to the airframe or* *(2) Incorporating other acceptable means to dissipate the static charge so as not to endanger the aeroplane, personnel or operation of the installed electrical/electronic systems".*

Table 7: CS-25 Subpart D requirements, [21].

3. SUBPART F

REQUIREMENTS	TOPIC	DESCRIPTION
CS 25.1301	FUNCTION AND INSTALLATION	*"(a) Each item of installed equipment must* *(1) Be of a kind and design appropriate to its intended function;* *(2) Be labelled as to its identification, function, or operating limitations, or any applicable combination of these factors. (See AMC 25.1301(a)(2))* *(3) Be installed according to limitations specified for that equipment.* *(b) Electrical wiring interconnection systems must meet the requirements of subpart H of this CS-25".*
CS 25.1309	EQUIPMENT, SYSTEMS AND INSTALLATIONS	*"(a) The aeroplane equipment and systems must be designed and installed so that:* *(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(1) of this paragraph.* *(e) Certification Maintenance Requirements must be established to prevent the development of the failure conditions described in CS 25.1309(b) and must be included in the Airworthiness Limitations Section of the Instructions for Continued Airworthiness required by CS 25.1529".*
CS 25.1316	ELECTRICAL AND ELECTRONIC SYSTEM LIGHTINING PROTECTION	*"(b) Each electrical and electronic system that performs a function whose failure would reduce the capability of the aeroplane or the ability of the flight crew to respond to an adverse operating condition must be designed and installed so that the function recovers normal operation in a timely manner after the aeroplane is exposed to lightning".*
CS 25.1317	HIRF PROTECTION	*"(c) Each electrical and electronic system that performs a function whose failure would reduce the capability of the aeroplane or the ability of the flight crew to respond to an adverse operating condition must be designed and installed so that the system is not adversely affected when the equipment providing the function is exposed to equipment HIRF test level 3, as described in Appendix R".*

CS 25.1319	EQUIPMENT, SYSTEMS AND NETWORK INFORMATION PROTECTION	*"(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.* *(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained".*
CS 25.1321	ARRANGEMENT AND VISIBILITY	*"(a) Each flight, navigation, and powerplant instrument for use by any pilot must be plainly visible to him from his station with the minimum practicable deviation from his normal position and line of vision when he is looking forward along the flight path".*
CS 25.1353	ELECTRICAL EQUIPMENT AND INSTALLATIONS	*"(a) Electrical equipment and controls must be installed so that operation of any one unit or system of units will not adversely affect the simultaneous operation of any other electrical unit or system essential to the safe operation. Any electrical interference likely to be present in the aeroplane must not result in hazardous effects upon the aeroplane or its systems except under extremely remote conditions.* *(c) Storage batteries must be designed and installed as follows:* *(1) Safe cell temperatures and pressures must be maintained during any probable charging or discharging condition. No uncontrolled increase in cell temperature may result when the battery is recharged (after previous complete discharge):* *(i) At maximum regulated voltage or power.* *(ii) During a flight of maximum duration; and* *(iii) Under the most adverse cooling condition likely to occur in service.* *(2) Compliance with sub-paragraph (1) of this paragraph must be shown by test unless experience with similar batteries and installations has shown that maintaining safe cell temperatures and pressures presents no problem.*

		(3) No explosive or toxic gases emitted by any battery in normal operation, or as the result of any probable malfunction in the charging system or battery installation, may accumulate in hazardous quantities within the aeroplane. *(4) No corrosive fluids or gases that may escape from the battery may damage surrounding aeroplane structures or adjacent essential equipment.* *(d)Reserved.* *(e) Electrical bonding must provide an adequate electrical return path under both normal and fault conditions, on aeroplanes having earthed electrical systems (see CS 25.899)".*

Table 8: CS-25 Subpart F requirements, [21].

4. SUBPART G

REQUIREMENTS	TOPIC	DESCRIPTION
CS 25.1529	INSTRUCTIONS FOR CONTINUED AIRWORTHINESS	*"Instructions for Continued Airworthiness in accordance with Appendix H must be prepared".*
CS 25.1581	AEROPLANE FLIGHT MANUAL	*"(a) Furnishing information. An aeroplane Flight Manual must be furnished with each aeroplane, and it must contain the following:* *(1) Information required by CS 25.1583 to 25.1587 .* *(2) Other information that is necessary for safe operation because of design, operating, or handling characteristics.* *(3) Any limitation, procedure, or other information established as a condition of compliance with the applicable noise standards.* *(b) Approved information. Each part of the manual listed in CS 25.1583 to 25.1587 that is appropriate to the aeroplane, must be furnished, verified, and approved, and must be segregated, identified, and clearly distinguished from each unapproved part of that manual.* *(d) Each aeroplane Flight Manual must include a table of contents if the complexity of the manual indicates a need for it".*

Table 9: CS-25 Subpart G requirements, [21].

Some of the requirements mentioned above are supported by the related AMCs, that explain and clarify the means to satisfy the requirements. In particular, as explained in the standard [21]:

- AMC 25.365 does not contemplate the risk of impact between the structures due to decompression.
- AMC 25.581 underlines that it is referred to external metal and non-metal parts, giving extensive explanations and provides the Industrial standard of reference.
- AMC 25.831 provides clarifications regarding the recirculation of air and its conveyance in the relative ducts.
- AMC 25.863 explains that the ventilation required by some electrical or electronic equipment or by areas subject to flammable liquids or vapours must be guaranteed without causing hazards.
- AMC 25.869 expresses that the electrical equipment in case of failure must not release harmful quantities to the crew or passengers and, moreover, it must not be subject to explosion under normal or fail conditions. This can be assured by being compliant with the Explosion Proofness Standards of RTCA DO-160/EUROCAE ED-14.
- AMC 25.899 concerns all the information, procedures and related standards about the Protection against Lightning Discharges, Characteristics of Lightning Discharges, Protection against the Accumulation of Static Charges, Primary and Secondary Bonding Paths and Resistance and Continuity Measurements.
- AMC 25.1309 provides the procedures about the System Design and Analysis, focusing on the safety aspect. In particular, as regards the purpose of this work, the failure conditions may be classified as reported [21]:

  (1) No Safety Effect: Failure conditions that have negligible or no effect for the safety; for example, these Failure Conditions do not have impact on the aircraft capability or crew workload.

  (2) Minor: Failure conditions that would not affect aeroplane safety and the crew knows the operating procedures and is able to take actions.

  Moreover, the requirements highlights that the equipment, systems, and installations covered by CS 25.1309(a)(2) (no-safety critical) are typically those linked with comforts for passengers such as passenger entertainment systems, whose failure in fact, should not affect the safety of the aeroplane.

Operational and environmental qualification requirements for those equipment are limited to the tests that are necessary to show that their normal or irregular functioning does not adversely affect the safety.

- AMC 25.1319 clarifies that the term 'adverse effects on the safety of the aeroplane' refers to security breaches.
- AMC 25.1353 describes the possible sources of interference, including conducted and radiated interference, malfunctions of electrically-powered devices, parasitic currents and voltages in the electrical distribution systems.
- AMC 25.1581 identifies the information that must be provided in the AFM (Aircraft Flight Manal) under the airworthiness regulations and provides guidelines about the form and content of the approved section of an AFM.

In the final section of the standard, the appendices provide further information, with graphs, tables, illustrations, and data. In particular, the appendices F, H and R are analysed in order to clarify the means and the range of applicability of the requirements.

The appendix F provides "*Test Criteria and Procedures for Showing Compliance with CS 25.853, 25.855 or 25.869*", [21], also about the electrical system components. In particular, the material test criteria and test procedures are shown and detailed.

Furthermore, the appendix H identifies the requirements for the formulation of Instructions for Continued Airworthiness as mentioned by CS 25.1529. Specifically, the Instructions for Continued Airworthiness must include, [21]:

a. Aeroplane maintenance manual or section
b. Maintenance Instructions
c. Diagrams of structural access sheets and information needed to obtain the access for inspections when access plates are not provided.
d. Details for the application of special inspection techniques
e. Information necessary to apply protective treatments to the structure after inspection.
f. All structural data such as identification, discard recommendations, and torque values.
g. A list of special tools required.

Finally, the appendix R identifies the HIRF (High-Intensity Radiated Field) environments and equipment HIRF test levels for electrical and electronic systems under CS 25.1317. The field intensity values for the HIRF environments and the three equipment HIRF test levels are evaluated during the peak of the modulation cycle.

4.2 CERTIFICATION SPECIFICATION 27

Concerning the CS-27, the parts considered are:

1. Subpart B (Flight)
2. Subpart C (Strength)
3. Subpart D (Design and Construction)
4. Subpart F (Equipment)
5. Subpart G (Operating Limitations and Information)

Comparably to the CS-25, the following tables present the derived requirements, as they are verbatim expressed in the standard, [30]. The requirements are not fully reported from the EASA standard, because the aim is to focus on the dictates of interest of the work.

1. SUBPART B

REQUIREMENTS	TOPIC	DESCRIPTION
CS 27.251	VIBRATION	*"Each part of the rotorcraft must be free from excessive vibration under each appropriate speed and power condition".*

Table 10: CS-27 Subpart B requirements, [30].

2. SUBPART C

REQUIREMENTS	TOPIC	DESCRIPTION
CS 27.561	EMERGENCY LANDING CONDITIONS	*"(c) The supporting structure must be designed to restrain under any ultimate inertial load factor up to those specified in this paragraph, any item of mass above and/or behind the crew and passenger compartment that could injure an occupant if it came loose in an emergency landing. Items of mass to be considered include, but are not limited to, rotors, transmission and engines. The items of mass must be restrained for the following ultimate inertial load factors:* *(1) Upward – 1.5 g* *(2) Forward – 12 g* *(3) Sideward – 6 g* *(4) Downward – 12 g* *(5) Rearward – 1.5 g".*

Table 11:CS-27 Subpart C requirements, [30].

3. SUBPART D

REQUIREMENTS	TOPIC	DESCRIPTION
CS 27.610	LIGHTINING AND STATIC ELECTRICITY PROTECTION	*"(b) For metallic components, compliance with sub-paragraph (a) may be shown by:* *(1) Electrically bonding the components properly to the airframe; or* *(2) Designing the components so that a strike will not endanger the rotorcraft.* *(c) For non-metallic components, compliance with sub-paragraph (a) may be shown by:* *(1) Designing the components to minimise the effect of a strike; or* *(2) Incorporating acceptable means of diverting the resulting electrical current to not endanger the rotorcraft.* *(d) The electrical bonding and protection against lightning and static electricity must:* *(1) Minimise the accumulation of electrostatic charge;* *(2) Minimise the risk of electrical shock to crew, passengers, and servicing and maintenance personnel using normal precautions.* *(3) Provide an electrical return path, under both normal and fault conditions, on rotorcraft having grounded electrical systems; and* *(4) Reduce to an acceptable level the effects of static electricity on the functioning of essential electrical and electronic equipment".*
CS 27.663	GROUND RESONANCE PREVENTION MEANS	*"(a) The reliability of the means for preventing ground resonance must be shown either by analysis and tests, or reliable service experience, or by showing through analysis or tests that malfunction or failure of a single means will not cause ground resonance".*
CS 27.771	PILOT COMPARTMENT	*"For each pilot compartment:* *(a) The compartment and its equipment must allow each pilot to perform his duties without unreasonable concentration or fatigue.* *(b) If there is provision for a second pilot, the rotorcraft must be controllable with equal safety from either pilot seat.* *(c) The vibration and noise characteristics of cockpit appurtenances may not interfere with safe operation".*

CS 27.831	VENTILATION	*"(a) The ventilating system for the pilot and passenger compartments must be designed to prevent the presence of excessive quantities of fuel fumes and carbon monoxide.* *(b) The concentration of carbon monoxide may not exceed one part in 20 000 parts of air during forward flight or hovering in still air. If the concentration exceeds this value under other conditions, there must be suitable operating restrictions".*
CS 27.863	FLAMMABLE FLUID FIRE PROTECTION	*"(a) In each area where flammable fluids or vapours might escape by leakage of a fluid system, there must be means to minimise the probability of ignition of the fluids and vapours, and the resultant hazards if ignition does occur.* *(b) Compliance with sub-paragraph (a) must be shown by analysis or tests.* *(d)Each area where flammable fluids or vapours might escape by leakage of a fluid system must be identified and defined".*

Table 12: CS-27 Subpart D requirements, [30].

4. SUBPART F

REQUIREMENTS	TOPIC	DESCRIPTION
CS 27.1301	FUNCTION AND INSTALLATION	*"Each item of installed equipment must:* *(a) Be of a kind and design appropriate to its intended function.* *(b) Be labelled as to its identification, function, or operating limitations, or any applicable combination of these factors;* *(c) Be installed according to limitations specified for that equipment; and* *(d) Function properly when installed.* *It refers to the height-speed envelope CS 29.87 and the operating limitations CS 29.1583 of the rotorcraft".*
CS 27.1309	EQUIPMENT, SYSTEMS AND INSTALLATIONS	*"(a) The equipment, systems, and installations whose functioning is required by this CS–27 must be designed and installed to ensure that they perform their intended functions under any foreseeable operating condition.* *(b) The equipment, systems, and installations of a multi-engine rotorcraft must be designed to prevent hazards to the rotorcraft in the event of a probable malfunction or failure.* *(c) The equipment, systems, and installations of single-engine rotorcraft must be designed to minimise hazards to*

		the rotorcraft in the event of a probable malfunction or failure".
CS 27.1316	ELECTRICAL AND ELECTRONIC SYSTEM LIGHTINING PROTECTION	*"(a) Each electrical and electronic system that performs a function whose failure would prevent the continued safe flight and landing of the rotorcraft, must be designed, and installed in a way that:* *(1) the function is not adversely affected during and after the time the rotorcraft's exposure to lightning; and* *(2) the system automatically recovers normal operation of that function, in a timely manner, after the rotorcraft's exposure to lightning, unless the system's recovery conflicts with other operational or functional requirements of the system that would prevent continued safe flight and landing of the rotorcraft.* *(b) For rotorcraft approved for instrument flight rules operation, each electrical and electronic system that performs a function whose failure would reduce the capability of the rotorcraft or the ability of the flight crew to respond to an adverse operating condition, must be designed and installed in a way that the function recovers normal operation in a timely manner after the rotorcraft's exposure to lightning".*
CS 27.1317	HIRF PROTECTION	*"(a) Each electrical and electronic system that performs a function whose failure would prevent the continued safe flight and landing of the rotorcraft must be designed and installed in a way that:* *(1) the function is not adversely affected during and after the rotorcraft's exposure to HIRF environment I as described in Appendix D.* *(2) the system automatically recovers normal operation of that function in a timely manner after the rotorcraft's exposure to HIRF environment I as described in Appendix D unless the system's recovery conflicts with other operational or functional requirements of the system that would prevent continued safe flight and landing of the rotorcraft.*

		(3) the system is not adversely affected during and after the rotorcraft's exposure to HIRF environment II as described in Appendix D. *(4) each function required during operation under visual flight rules is not adversely affected during and after the rotorcraft's exposure to HIRF environment III as described in Appendix D.* *(b) Each electrical and electronic system that performs a function whose failure would significantly reduce the capability of the rotorcraft or the ability of the flight crew to respond to an adverse operating condition must be designed and installed in a way that the system is not adversely affected when the equipment providing the function is exposed to equipment HIRF test level 1 or 2 as described in Appendix D.* *(c) Each electrical and electronic system that performs a function whose failure would reduce the capability of the rotorcraft or the ability of the flight crew to respond to an adverse operating condition must be designed and installed in a way that the system is not adversely affected when the equipment providing the function is exposed to equipment HIRF test level 3 as described in Appendix D".*
CS 27.1321	ARRANGEMENT AND VISIBILITY	*"(a) Each flight, navigation, and powerplant instrument for use by any pilot must be easily visible to him.* *(b) For each multi-engine rotorcraft, identical powerplant instruments must be located so as to prevent confusion as to which engine each instrument relates.* *(c) Instrument panel vibration may not damage, or impair the readability or accuracy of, any instrument.* *(d) If a visual indicator is provided to indicate malfunction of an instrument, it must be effective under all probable cockpit lighting conditions".*
CS 27.1351	ELECTRICAL SYSTEMS AND EQUIPMENT GENERAL	*"(b) Function. For each electrical system the following apply:* *(1) Each system, when installed, must be:* *(i) Free from hazards in itself, in its method of operation, and in its effects on other parts of the rotorcraft; and* *(ii) Protected from fuel, oil, water, other detrimental substances, and mechanical damage.*

		(3) No failure or malfunction of any source may impair the ability of any remaining source to supply load circuits essential for safe operation".
CS 27.1353	STORAGE BATTERY DESIGN AND INSTALLATION	*"(a) Each storage battery must be designed and installed as prescribed in this paragraph.* *(b) Safe cell temperatures and pressures must be maintained during any probable charging and discharging condition. No uncontrolled increase in cell temperature may result when the battery is recharged (after previous complete discharge):* *(1) At maximum regulated voltage or power.* *(2) During a flight of maximum duration; and* *(3) Under the most adverse cooling condition likely to occur in service.* *(c) Compliance with sub-paragraph (b) must be shown by test unless experience with similar batteries and installations has shown that maintaining safe cell temperatures and pressures presents no problem.* *(d) No explosive or toxic gases emitted by any battery in normal operation, or as the result of any probable malfunction in the charging system or battery installation, may accumulate in hazardous quantities within the rotorcraft.* *(e) No corrosive fluids or gases that may escape from the battery may damage surrounding structures or adjacent essential equipment.* *(f) Each nickel cadmium battery installation capable of being used to start an engine or auxiliary power unit must have provisions to prevent any hazardous effect on structure or essential systems that may be caused by the maximum amount of heat the battery can generate during a short circuit of the battery or of its individual cells.* *(g) Nickel cadmium battery installations capable of being used to start an engine or auxiliary power unit must have:* *(1) A system to control the charging rate of the battery automatically so as to prevent battery overheating;* *(2) A battery temperature sensing and over-temperature warning system with a means for disconnecting the battery from its charging source in the event of an over-temperature condition; or*

		(3) A battery failure sensing and warning system with a means for disconnecting the battery from its charging source in the event of battery failure".

Table 13:CS-27 Subpart F requirements, [30].

5. SUBPART G

REQUIREMENTS	TOPIC	DESCRIPTION
CS 27.1529	INSTRUCTIONS FOR CONTINUED AIRWORTHINESS	*"Instructions for Continued Airworthiness in accordance with Appendix A must be prepared".*
CS 29.1581	AEROPLANE FLIGHT MANUAL	*"(a) Furnishing information. A rotorcraft flight manual must be furnished with each rotorcraft, and it must contain the following:* *(1) Information required by CS 27.1583 to 27.1589.* *(2) Other information that is necessary for safe operation because of design, operating, or handling characteristics.* *(b) Approved information. Each part of the manual listed in CS 27.1583 to 27.1589, that is appropriate to the rotorcraft, must be furnished, verified, and approved, and must be segregated, identified, and clearly distinguished from each unapproved part of that manual.* *(c) (Reserved).* *(d) Table of contents. Each rotorcraft flight manual must include a table of contents if the complexity of the manual indicates a need for it".*

Table 14: CS-27 Subpart G requirements, [30].

As the final part of the CS-27, the appendices A and D are examined in order to explain and help in the applicability of the requirements.

The appendix A suggests the preparation of the Instructions for Continued Airworthiness. In particular, the content includes [30]:

a. Rotorcraft maintenance manual or section.
b. Maintenance Instructions.
c. Diagrams of structural access plates and information needed to obtain the access for inspections when access plates are not possible.
d. Details for the application of special inspection techniques.
e. Information necessary to apply protective treatments to the structure after inspection.
f. All structural fasteners data.

g. A list of special tools required.

Moreover, the appendix explains the form of the manuals, the necessary quantity of data and the adequate practical arrangement and requires the insertion of the continuing airworthiness practices.

On the other hand, the appendix D identifies the HIRF (High-Intensity Radiated Field) environments and equipment HIRF test levels for electrical and electronic systems under CS 27.1317, always distinguishing three equipment HIRF test levels, assessed during the peak of the modulation cycle.

5 COMMERCIAL PARTS APPLIED TO EASA AIRCRAFT

The certification process of a part for aeronautical or space use is certainly a very long and expensive process and is aimed at the production of parts that perform the functions assigned under specific conditions in a certain operating environment with very high reliability and quality.

Building a product or system from scratch would lead to a higher cost for design, implementation, and testing, as it is a non-existent product, and it has potentially a greater number of failure modes than a single existing component.

Similarly, adopting a fault avoidance philosophy, which aims to minimize failures, would lead to higher costs. It basically involves the adoption of very wide safety margins, as in the spatial case, the use of selected and high-quality parts[4], the constant employ of inspecting systems under production, 100% acceptance test, the lot control and the serializing, the collection and recording of the document compliance, as reported in the MIL-STD-1543, [31].

The achievement of the qualification for aeronautical or spatial use (respectively Aeronautical-qualified and Space-qualified) is very stringent and requires that, for example, a space-qualified component must be designed, manufactured, and tested in order to meet the restrictive electrical, mechanical, or environmental requirements for use in the launch and deployment of satellites or high-altitude flight systems.

It involves a large number of tests, the use of increasingly performing and refined materials, a deeper and longer research and development work, therefore in general, a greater investment of economic resources and human.

The purpose of this work is to certify commercial parts for no-hazard aeronautical use, in particular the application of common use devices aboard the EASA aircraft are considered.

[4] Failure rates of Class S (space) components are about 1/4 those of the highest-quality level parts procured to general military specifications and 1/10 those of high-grade commercial parts, [33].

5.1 COMMERCIAL PARTS

The commercial parts involved in this work are substantially divided in two main categories: on one side the UPS and a pair of batteries are examined and on the other side, the devices belonging to the so-called EFB (Electronic Flight Bag), Panasonic Toughbook 55 and Apple iPad Air 4 are inspected.

5.1.1 UPS

Firstly, the UPS (*Uninterruptible Power Supply*) is taken in exam. It is an electrical equipment employed in case of sudden anomalies in the normal supply of electricity (such as voltage drops). Moreover, it has the capability to provide constantly a perfectly sinusoidal waveform, without accidental alterations and to limit the lack of current to the equipment connected to its output to few milliseconds. UPSs can supply electricity for a short period of time (5-10 minutes at full load), but when the electricity required exceeds this time, the UPS is combined with an auxiliary electric generator, which starts up as soon as the problem occurs and reaches operation optimal in times less, [32].

The UPS examined is the SITOP UPS1600, produced by Siemens, [33], as shown in the Figure 15:

Figure 15: Siemens Sitop UPS 1600 20 A, picture from [33].

As reported in the Siemens Device Data Sheet [33], this UPS has the physical features reported in the Table 15:

DIMENSIONS	
Length	125 mm
Width	50 mm
Height	125 mm
Weight	0.45 kg

Table 15: Siemens SITOP UPS1600 physical features, [33].

According to the Data Sheet [33], it has a supply voltage for DC rated value equal to 24 V and the input voltage range goes from 22 to 29 V DC. The type of energy storage is with batteries and charging current is 0.1 A or 4 A. As output, it allows to obtain the voltage DC rated values in both normal operation and buffering mode equal to 24 V, with a 20 A output current Rated value. Moreover, it presents a short-circuit protection which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I rated for 5 sec/min and the typical active power supplied is of 480 W.

For what concerns the safety, it owns different certificates of suitability, as the CE marking, the UL[5] approval, as approval for USA (cULus-Listed (UL 508, CSA C22.2 No. 107.1), File E197259), C-Tick[6] and CB-certificate[7], while for emitted interference and interference immunity respectively is compliant to EN 55022[8] Class B and to EN 61000-6-2[9]. Furthermore, the UPS is provided of IP20[10] Protection Class, which guarantees the protection of solid bodies

[5] The UL (Underwrites Laboratories) is a global safety certification company instituted to perform safety testing by the U.S. federal agency.

[6] C-Tick is an identification mark registered with the Australian Communications Media Authority (ACMA), that shows the compliance of an electronic device to the applicable electromagnetic compatibility (EMC) requirements.

[7] The IECEE CB releases certificates concerning the safety of electrical and electronic products and components.
The IEC CB is a multilateral accordance between participating countries and certification organizations, based on the use of international standards (IEC).

[8] The standard EN 55022 is about the "*Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement"* and prescribes the radio interference specified for the frequency range 9 kHz to 400 GHz for both class A and class B equipment.

[9] The standard EN61000-6-2 concerns immunity requirements in the 0 Hz to 400 GHz frequency band.

[10]The IP (Degree of Protection) Certification is based on CEI EN 60529/1997 (before CEI 70-1), which classifies the degrees of protection of enclosures for electrical equipment.

larger than 12mm, but not against the penetration of liquids by drops, vapours, or splashes in any direction, [33].

The device could be mounted on snaps onto DIN rail EN 60715 35x7.5/15 as illustrated in the Figure 16:

Figure 16: UPS mounted on the DIN rail EN 60715, [34] .

Finally, the document reports the operating temperature range during the different phases, summarized in the Table 16:

PHASE	TEMPERATURE RANGE
Operation	-25 °C to +70 °C
Transport	-40 °C to +85°C
Storage	-40 °C to +85°C

Table 16: Temperature range of the UPS depending on the phase, [33].

The UPS could be exploited in the applications whose electrical demand is constant in order to avoid serious repercussions, therefore the UPS helps to maintain the equipment active and adequately powered when there is a failure in the normal electrical supply.

5.1.2 BATTERIES

Secondly, a pair of Powersonic PS-1230 Battery, shown in the Figure 17, is analysed:

Figure 17: Powersonic PS-1230 Battery, [35].

According to the Powersonic PS-1230 Data Sheet, [35], the single unit is a 12 Volt / 3.40 Amp hour sealed rechargeable lead acid battery. The battery is made of Absorbent Glass Mat (AGM) in order to obtain superior performance. Thanks to the efficient power to volume ratio, a high value of energy density is achieved, and the design life is assured to be about 5 years.

The document [35] reports that the external case of the battery is made of nonconductive ABS plastic to UL94-HB, that confers high impact resistance to shock, vibration, chemicals, and heat, and the case also owns the flame retardant (FR) feature. This is the so-called "Rugged Construction", which is found in the MIL-STD-810G.

The battery life is guaranteed between 200 and 1000 charge/ discharge cycles depending on the average depth of discharge, under normal operating conditions. Furthermore, the ability to recover from excessively deep discharge is increased through a balanced electrolyte system, special separators, and sophisticated plate structure.

The fully charged batteries can be stored for long periods of time before they need to be recharged, thanks to the low self-discharge rate. The shelf-related ability is enhanced by lower storage temperatures.

In fact, as temperature rises charging voltage should be lowered to avoid overcharge and, vice-versa, increased as temperature drops to avoid undercharge.

The Table 17 represents the temperature range of the battery during the discharge and charge phases:

PHASE	TEMPERATURE RANGE
Discharge	-20 °C to +60 °C
Charge	-15 °C to +50 °C

Table 17: Battery temperature range during the discharge and charge phases, [35] .

The dimensions and weight of a single battery are shown in the Table 18:

DIMENSIONS	
Length	13.28 mm
Width	6.71 mm
Height	6.00 mm
Weight	1.32 kg

Table 18: Powersonic PS-1230 physical features, [35].

According to the document [35], the design flexibility of the batteries allows to adopt series and/or parallel configuration depending on the voltage and capacity required and to be used in either cyclic or standby applications.

Safe operations are guaranteed in any position thanks to the spill-proof construction and the maintenance is little required. In fact, it is not necessary the addition of electrolyte, because gases generated during overcharge are reused in a unique "oxygen cycle", through a defined gas recombination technology.

This type of construction is implemented through the valve regulated design, in which series of one-way low-pressure valves are employed. These valves are self-sealing and allow the expelling of any excess gasses that may be produced in the battery in case of serious overcharging. Robust lead calcium plates confer an extra margin of performance and life.

The Powersonic battery is subjected to stringent quality controls during each step of the manufacturing process in order to guarantee consistency and reliability. It is UL recognized and also compliant to the ISO 9001[11].

[11] The ISO 9001, *Quality management systems*, is the reference standard for the improvement and monitoring both operational and support processes, for designing and implementing the quality management system. It is applied in order to enhance the production, minimize the costs and be more competitive.

5.2 ELECTRONIC FLIGHT BAG

In the past, many aircraft performance calculations are realized using paper material and then on-board the aircraft. With passing of the years, an always increasing amount of information became available in electronic format and proved to be more convenient for flight operators.

The information regarding the flight manuals, communications, aviation data and other notions required on board are stored in the so-called EFBs (Electronic Flight Bag), which have taken on the ability to store and show aviation data, but above all to perform a series of calculations, enter databases (e.g., digital navigation data) and show real-time data from avionics.

According to the AMC 20-25[12], [36], an "*Electronic Flight Bag is an information system for flight deck crew members which allows storing, updating, delivering, displaying, and/or computing digital data to support flight operations or duties*". In fact, it includes any portable electronic display device or combination of devices intended for flight deck or cabin use.

The assessment of an EFB may have both an airworthiness and an operational characteristic depending on the category/type of EFB and its application.

The EFB systems hardware hosts the platform used to operate the EFB software suite.

The aforementioned AMC 20-25 [36] defines two types of EFB systems hardware: portable or installed. The first one, defined as PED, portable electronic device, is not part of the certified aircraft configuration, while the latter is included in the aircraft parts and needs the aircraft airworthiness certification.

A portable EFB can be used inside and outside the aircraft, hosts type A and/or type B EFB or non-EFB software applications. Its mass, dimensions, shape, and position should not affect flight safety.

If mounted, the portable EFB is easily removable from its mounting device or attached to it, without the need of maintenance action or the use of tools by the flight crew. The application of its transmitting capability is recognized in the approved Aircraft Flight Manual (AFM), and in its absence, the EFB transmitting capability may be allowed during only non-critical phases of the flight.

As the standard reports [36], depending on the impact on safety, the applications included in the EFB hardware are of type A or B. The first type of EFB applications could cause

[12] Specifically, this is included in the Annex IX to ED Decision 2019/008/R AMC 20-25A, [36].

malfunctions that are negligible for the safety, so they do not require any airworthiness approval, while the latter type malfunctions could cause minor failure condition, but they do not cover any system or functionality required by airworthiness regulations.

In this work, the EFB systems hardware portable type A are considered.

The AMC 20-25 [36] also provides an operational assessment to the type A portable EFB.

This includes the Electromagnetic Interference (EMI) demonstrations, in which the operation of a PED must not interfere in any way with the operation of aircraft equipment while turned one (or in standby mode) during critical phases of the flight and Environmental testing, in particular for rapid depressurisation and rapid variation of atmospheric conditions.

Moreover, the assessment [36] concerns the use of rechargeable lithium batteries in portable EFBs located in the aircraft cockpit need to be compliant with the requirements mentioned, because of their potential hazard effects to the flight crew and to aircraft safe operations. Portable EFB system design must take into account the source of electrical power and the potential need for an independent battery source. Furthermore, it must be always considered the addition of a possible redundancy of portable EFBs to reduce the risk of exhausted batteries and the availability of alternative battery packs on board.

For what concerns the safe stowage, the use of the EFB under any expected cockpit environmental conditions and the considerations on the position of the display in the flight deck should be documented in the operational assessment and in the EFB policy, where it is assured that the stowage characteristics remain within acceptable limits for the proposed operations. Finally, EFB system routine maintenance actions and procedures, including the periodical check and replacement of the batteries, should be defined in order to ensure the integrity of the EFB system, [36].

5.2.1 PANASONIC TOUGHBOOK

Starting from the EFBs, firstly the Panasonic Toughbook 55 is taken in exam. The device is a 14” display notebook, as shown in the Figure 18:

Figure 18: Panasonic Toughbook 55, [37].

According to the Panasonic Toughbook 55 Data Sheet [37], the model is “rugged”, that is able to handle shock, vibration, extreme temperatures, and pressures, according to the MIL-STD-810G, [29]. It is provided of Windows 10 Pro, but still remains versatile and with universal housing.

The so-mentioned magnesium external case and the "honeycomb" design guarantee great robustness and resistance. The physical features of the device are reported in the Table 19:

DIMENSIONS	
Length	345 mm
Width	32.8 mm
Height	272 mm
Weight	2.08 kg

Table 19: Panasonic Toughbook 55 physical features, [37].

Moreover, its flexibility allows to obtain a wide range of configuration options.

From the data sheet [37], the processor is an Intel® Core ™ i5-8365U vPro ™, with 8 GB of RAM and 256 GB SSD as standard. It is provided with Lithium-ion, 10.8V, 6500mAh (typ.), 6300mAh (min.) battery, that allows high performance and long duration.

The equipment disposes of front camera, voice recognition, audio system, numerous data and audio interfaces, LAN connection, mobile broadband connection, Bluetooth™ and global positioning, which supports GPS, GLONASS, Galileo.

Moreover, the operating temperature range goes from - 29 ° C to +60 ° C and it results compliant also to the MIL-STD-416F, regarding the EMI and EMC tests, [38].

In conclusion, as reported in the data sheet [37], the standard tests passed by the Panasonic Toughbook 55 include:

- IP53 penetration protection (IP5x dust resistance and IPx3 water resistance),
- Resistance to falls from a height of 91 cm,
- Protection from shock, vibration for vehicle docking.

The last two features are also tested by an independent lab after MIL-STD 810G approval.

This “rugged” computer stands optimal for aeronautical and military applications, but, in this work, Panasonic Toughbook 55 is thought for non-avionic applications, such as passenger entertainment.

5.2.2 APPLE IPAD AIR 4

As second EFB, Apple iPad Air 4 is considered. The device belonging to the category of tablets is shown in the Figure 19:

Figure 19: Apple iPad Air by Apple, [39].

As evinced in Apple website [39], iPad Air 4 is designed and produced by Apple, with the intent to adapt its applicability to each type of use, thanks to the operating system iPadOS 15.

It is provided of 10.9" liquid retina LED Backlit Multi - Touch, with fingerprint-proof oleophobic and anti-reflective coatings. The battery that feeds the equipment is built-in rechargeable lithium polymer of 28.6-watt hour, with an autonomy of up to 10 hours of Wi - Fi browsing or video playback.

Moreover, Apple iPad Air 4 shell is made of 100% recycled aluminium and 100% recycled tin for logic board soldering in order to give an adequate resistance and efficiency.

The device offers high performing external and internal cameras, video registration, voice recognition, audio system (speakers and microphones), mobile LTE connection, Bluetooth™ and geolocation with digital compass, Wi-Fi, IBeacon microlocation and integrated GPS / GNSS. Moreover, it is equipped of some sensors, such as touch ID, 3-axis gyroscope, accelerometer, barometer, and ambient light sensor.

The environmental requirements are summarized in the Table 20:

	REQUIREMENTS
Operating Temperature	0 °C to +35 °C
Not Operating Temperature	-20 °C to +45 °C
Relative Humidity	from 5% to 95% in the absence of condensation
Operating Altitude	tested up to 3000m

Table 20: Environmental requirements for Apple iPad Air 4, [39].

In conclusion, Apple iPad Air 4 owns the CE marking approval, in particular it is compliant to the following product specifications:

- EN 55022:2006, Class B (EMC),
- EN 60950-1:2006[13] (Safety),
- EN 62311:2008[14] (Health).

[13]EN 60950-1:2006, I*nformation technology equipment - Safety -- Part 1: General requirements*, is a standard applicable to mains-powered or battery-powered information technology equipment, including electrical business equipment and associated equipment, with a RATED VOLTAGE not exceeding 600 V.

[14]EN 62311:2008 is a standard linked to the assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz).

5.3 EASA AIRCRAFT

The two EASA aircraft presented in this work are the Airbus A320neo aeroplane and the Eurocopter AS350 Ecureuil (Airbus H125) rotorcraft, in order to apply the aforementioned parts.

5.3.1 AIRBUS A320neo

The Airbus A320neo is a narrow-body aircraft designed and produced by Airbus, a successful and versatile jetliner, [40]. The aircraft, shown in the Figure 20, is the longest-range single-aisle aircraft, opening to airlines and passengers to new travel opportunities throughout the world:

Figure 20: Airbus A320neo, [40].

The A320neo dimensional characteristics are shown in the Table 21:

DIMENSIONS	
Overall Length	37.57 m
Fuselage Width	3.95 m
Height	11.76 m
Wingspan (geometric)	35.80 m
Capacity (pax)	From 150 to 194 (maximum)

Table 21: Airbus A320neo dimensional features, [40].

The top, lateral and frontal views are illustrated in the Figure 21:

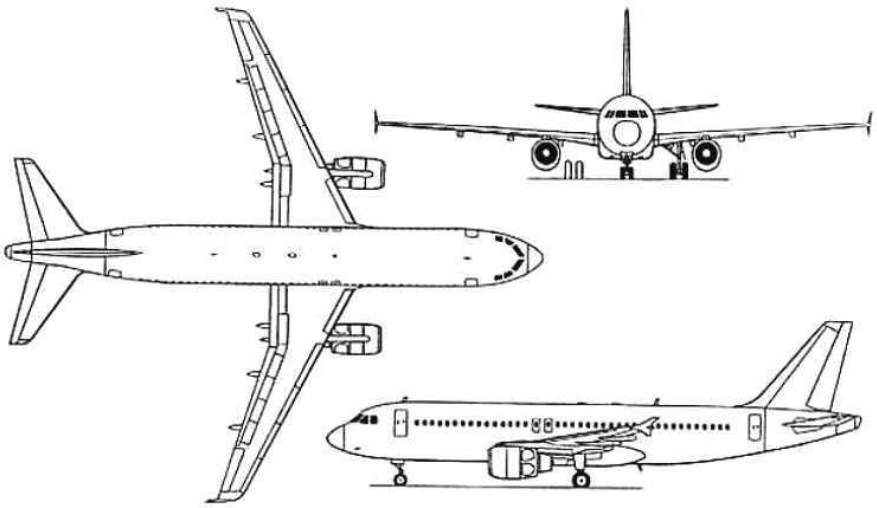

Figure 21: Airbus A320neo top, lateral and frontal views, [41].

As reported [40], the cabin space is optimized, increasing the seating capacity and the exit limits, which allows the aircraft to bring on board maximum 194 passengers, between 150-180 passengers in typical seating 2-class.

The A320neo, more made of composite materials, represents the optimal combination between an unbeatable fuel efficiency and high performance.

It differs from the previous A320 model due to the new engine option (neo) that assures the delivering per seat fuel enhance of 20% by 2020, as well as the additional range of up to 900 km or 2 tonnes of extra payload, without forgetting a lower operating costs, as reported in the Table 22:

PERFORMANCE	
Range	6300 km
Mach	0.82
MTOW (max take-off weight)	79000 tones
Max fuel capacity	26730 litres
Maximum Flight Altitude	11900 m

Table 22: Airbus A320neo performance features, [40].

Moreover, the use of digital fly-by-wire and side-stick flight controls distinguish the A320neo from the previous versions.

Another fundamental benefit, mentioned in the data sheet of this aircraft [40], is being environmentally friendly: a nearly 50% reduction in engine noise and NOx emissions 50% per cent below the current industry standard.

The A320neo falls into the category of large aircraft, so for the requirements compliance of the on-board installation and use of the commercial parts, the CS-25 will be considered.

5.3.2 EUROCOPTER AS350 ÉCUREUIL (or AIRBUS H125)

The Eurocopter AS350 Écureuil (or Squirrel) is a rotorcraft originally designed and produced by the French Aérospatiale, now become Airbus as Helicopters H125, shown in the Figure 22:

Figure 22: Eurocopter AS350 Ecureuil (Airbus H1250), [42].

As mentioned in the Airbus website [42], the rotorcraft provides a single engine, that makes it a light, versatile and high-performance rotorcraft. The AS350 is suitable for aerial work, firefighting, police surveillance, passenger transport, hoist operations, EMS (Emergency Medical Service) in hot/high ambient conditions and rescue.

It also requires low maintenance and acquisition costs, but offers optimal manoeuvrability, excellent visibility, and low vibration levels in the cabin. The safety is enhanced, and the workload reduced thanks to the glass touchscreen cockpit instrument panel installed on-board.

The dimensional features of the AS350 are shown in the Table 23:

DIMENSIONS	
Rotor Diameter	10.69 m
Cabin Internal volume	3.00 m^3
Capacity (pax)	1 or 2 pilots + up to 6 passengers

Table 23: Dimensional features of Eurocopter AS350 (Airbus H125), [42].

The top, lateral and frontal views are illustrated in the Figure 23:

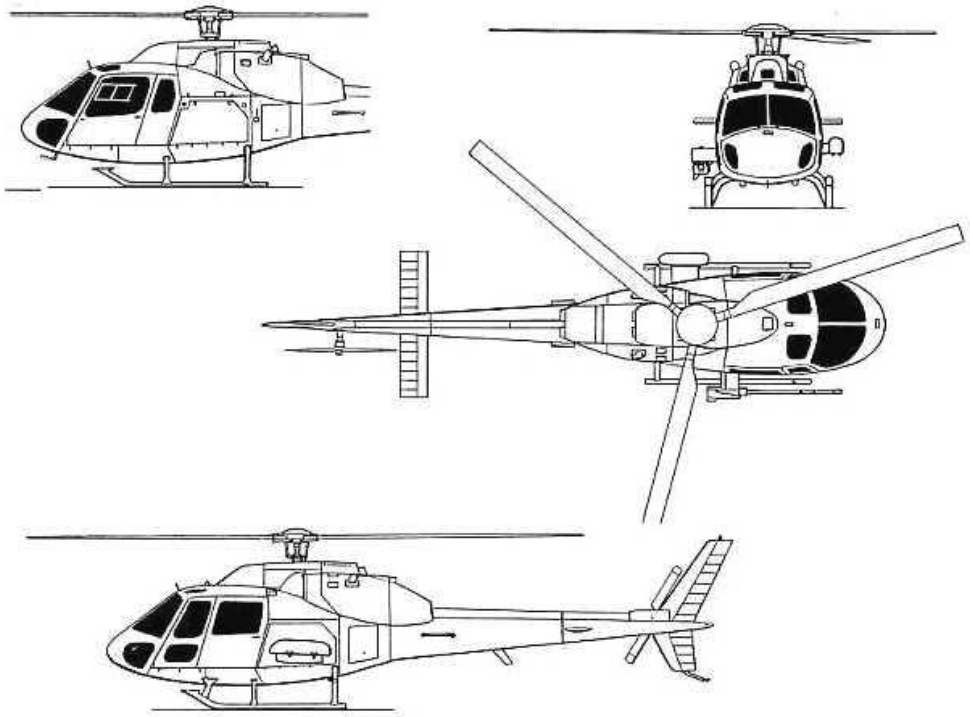

Figure 23: Eurocopter AS350 (Airbus H125) top, lateral and frontal view, [43].

Furthermore, the AS350 is equipped with a turboshaft engine with a dual-channel full authority digital engine control (FADEC) unit, plus a third independent and automatic back-up channel and an automatic start-up.

The performance data era summarized in the Table 24:

PERFORMANCE	
Max Range with standard fuel tanks at SL	630 km
Max Endurance with standard fuel tanks at SL	4 hr. 30 min.
Fast cruise speed	260 km/h
Max flight altitude	7010 m
Hover ceiling OGE	3840 m
MTOW (max take-off weight)	2250 kg
Standard fuel tank capacity	426 kg
Take-off power	710 kW

Table 24: Performance features of Eurocopter AS350 (Airbus H125), [43].

The configuration could vary from four to six passengers, depending on the mission assigned (business aviation, commercial transport operations or tourism and sightseeing operators). In conclusion, the overall flight envelope provides temperatures between - 40°C to +35°C, limited to 50°C, as reported by Airbus H125 data sheet, [43].

For the AS350, the CS-27 requirements will be applied for the on-board installation and use of the commercial parts, because it belongs to the small rotorcraft category.

5.4 REQUIREMENTS APPLICATION AND MITIGATING ACTIONS

The commercial parts described in the previous chapter are subjected to a preliminary and qualitative analysis to verify the compatibility of their characteristics with the requirements for the application on board the Airbus A320neo and Eurocopter AS350 Ecureuil aircraft.

Firstly, the CS-25 obtained requirements are applied to the UPS and battery and then to the EFBs, corresponding to the use on board of the A320neo, as well as the CS-27 requirements are implemented for the Eurocopter AS350 Ecureuil.

Secondly, Panasonic Toughbook 55 and Apple iPad Air 4 features are compared with an EFB compliance checklist from ENAC, [44], in order to obtain a further confirmation of their harmlessness on board.

In conclusion, for the parts characteristics unable to show compliance with the requirements of the CSs, tailored corrective actions are implemented.

5.4.1 CS-25 REQUIREMENTS APPLICATION

For this section, the CS-25 obtained requirements are considered, therefore reference is made to the application on board the Airbus A320neo aircraft, as a Large Aircraft.

However, the EFBs are to be considered non-installable on board, therefore they cannot be recharged on board or at least connected to the on-board electrical system and, as well as the UPS and batteries, the DAL is low (D or E), in order to does not significantly impact on the safety.

This decision was made to obviate the need to size and show the compatibility of electrical cables, the insertion of circuit protective devices and switches, so that essential loads and flight safety are not affected. Supporting this choice was also the objective of the work itself which aims at the certification of commercial parts with a no hazard approach.

5.4.1.1 CS-25 REQUIREMENTS APPLIED TO UPS AND BATTERIES

The CS-25 requirements are compared to the UPS and Batteries features in the Table 25:

CS	UPS SITOP1600 Siemens	Powersonic Battery Ps-1230
25.365	Mounted in pressurized areas.	Mounted in pressurized areas
25.561	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to impede the emergency egress and not to injure the occupants.	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to impede the emergency egress and not to injure the occupants.

25.581	Provided with a short-circuit protection, which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I, rated for 5 sec/min.	Provided of self-sealing low-pressure valves.
25.611	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to obstruct accessibility routes (impeding the inspections or other maintenance actions).	Linked to the UPS or to the devices they power.
25.683	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to interference with the close objects, under normal flight and ground conditions.	Linked to the UPS or to the devices they power.
25.771	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen).	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen).
25.789	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to injure the occupants.	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to injure the occupants.
25.831	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that ensures the protection of the passengers and crew health from toxic and noxious gases.	The batteries incorporate a series of one-way low-pressure valves. These self-sealing valves allow the venting of any excess gasses that may be produced in the battery due to severe overcharging.
25.863	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that ensures the protection of the passengers and crew health from fire and flammability liquids.	The battery presents flame retardant (FR).
25.869	Provided with a short-circuit protection, which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I, rated for 5 sec/min.	The battery life is guaranteed between 200 and 1000 charge/ discharge cycles depending on the average depth of discharge, under normal operating conditions. Furthermore, the ability to recover from excessively deep discharge is increased through a balanced electrolyte system, special separators, and sophisticated plate structure.
25.899	The UPS is compliant to the following standards: for emitted interference EN	Not required.

	55022 Class B and for interference immunity EN 61000-6-2.	
25.1301	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)
25.1309	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that ensures the device is not a source of danger.	Compliant to ISO 9001.
25.1316	Provided with a short-circuit protection, which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I, rated for 5 sec/min.	The battery life is guaranteed between 200 and 1000 charge/ discharge cycles depending on the average depth of discharge, under normal operating conditions. Furthermore, the ability to recover from excessively deep discharge is increased through a balanced electrolyte system, special separators, and sophisticated plate structure.
25.1317	The UPS is compliant to the following standards: for emitted interference EN 55022 Class B and for interference immunity EN 61000-6-2.	Not required.
25.1321	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)
25.1353	Linked to the battery's life.	The battery life is guaranteed between 200 and 1000 charge/ discharge cycles depending on the average depth of discharge, under normal operating conditions. Furthermore, the ability to recover from excessively deep discharge is increased through a balanced electrolyte system, special separators, and sophisticated plate structure.
25.1431	The UPS is compliant to the following standards: for emitted interference EN 55022 Class B and for interference immunity EN 61000-6-2.	Not required.
25.1529	Insertion of the maintenance actions, intervals and tools for the device applicability.	it is not necessary the addition of electrolyte, because gases generated during overcharge are reused in a unique "oxygen cycle", through a defined gas recombination technology.

25.1581	Insertion of all information, table of contents and data regarding the device applicability in the A320neo Flight Manual.	Insertion of all information, table of contents and data regarding the device applicability in the A320neo Flight Manual.

Table 25: CS-25 requirements applied to UPS and batteries.

5.4.1.2 CS-25 REQUIREMENTS APPLIED TO PANASONIC TOUGHBOOK 55 AND APPLE IPAD AIR 4

The application of the CS-25 requirements to the Panasonic Toughbook 55 and Apple iPad Air 4 features is shown in the Table 26 :

CS	Panasonic Toughbook 55	Apple iPad Air 4
25.365	The pressure variation tolerance is ensured as fully rugged laptops are capable of operating adequately at an altitude of 4,572m, which is the highest possible value specified by the MIL-STD-810G test.	Apple iPad Air 4 could not be exposed to high pressure variation.
25.561	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to impede the emergency egress and not to injure the occupants.	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to impede the emergency egress and not to injure the occupants.
25.581	It must be considered in the bonding of the aircraft (Input: 100 V - 240 V CA, 50 Hz/60 Hz; Output: 15,6 V CC, 7,05 A).	Apple iPad Air 4 must be considered in the bonding of the aircraft, considering 10 W Power Adapter.
25.611	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to obstruct accessibility routes (impeding the inspections or other maintenance actions).	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to obstruct accessibility routes (impeding the inspections or other maintenance actions).
25.683	Positioned, mounted (on a dedicated device) and stored in such a way as not to create interference or contact with the other adjacent elements. Compliant with MIL-STD-810G test.	Positioned, mounted (on a dedicated device) and stored in such a way as not to create interference or contact with the other adjacent elements.
25.771	It must not create acoustic and/or vibrational interference with the cockpit instruments and pilot headset.	It must not create acoustic and/or vibrational interference with the cockpit instruments and pilot headset. Its non-reflective and oleophobic coating do not create distractions for the pilot.

25.789	Positioned, mounted (on a dedicated stable mounting device) and stored in a definite place not subject to displacements.	Positioned, mounted (on a dedicated stable mounting device) and stored in a definite place not subject to displacements.
25.831	No emissions of gases or vapours during operations.	No emissions of gases or vapours during operations.
25.863	No escaping of flammable fluids or vapours.	No escaping of flammable fluids or vapours.
25.869	It must be kept away from heat sources. Compliant with fire and smoke protection requirements defined in the MIL-STD-810G test.	It must be kept away from heat sources.
25.899	The Toughbook 55 must be considered in the bonding of the aircraft (Input: 100 V - 240 V CA, 50 Hz/60 Hz; Output: 15,6 V CC, 7,05A).	Apple iPad Air 4 must be considered in the bonding of the aircraft, considering 10 W Power Adapter.
25.1301	Operating temperature from -29 ° C to 60 °C Compliant to the MIL-STD 810G tests (pression, temperature, humidity).	Operating ambient temperature: 0° to 35° C Nonoperating temperature: −20° to 45° C Relative humidity: 5% to 95% noncondensing Operating altitude: tested up to 3000 m.
25.1309	Compliant to MIL-STD 810G.	Compliant to CE marking
25.1316	The Toughbook 55 must be considered in the bonding of the aircraft (Input: 100 V - 240 V CA, 50 Hz/60 Hz; Output: 15,6 V CC, 7,05 A).	Apple iPad Air 4 must be considered in the bonding of the aircraft, considering 10 W Power Adapter.
25.1317	Compliant to MIL-STD-416F (EMI and EMC).	Apple iPad Air 4 has been designed, tested, and manufactured in compliance with radio frequency emissions regulations (EU standards), but such emissions could alter the operation of other electronic devices.
25.1321	It must not distract visually and/or acoustically the pilot. (Away from LCD screen).	It must not distract visually and/or acoustically the pilot. (Away from LCD screen).
25.1353	Lithium-ion, 10.8V, 6500mAh (typ.), 6300mAh (min.). Lithium-ion batteries can rupture, catch fire, or explode when exposed to high temperatures or direct sunlight. Shorting a lithium battery can cause fire and explosion.	Lithium polymer 28.6 watt hour. The battery can explode if short-circuited, due to the very low internal resistance and the consequent tremendous impulse current flowing through the cell. Furthermore, a Li-Poly cell can easily ignite if punctured.

25.1431	Compliant to MIL-STD-416F (EMI and EMC).	Apple iPad Air 4 has been designed, tested, and manufactured in compliance with radio frequency emissions regulations (EU standards), but such emissions could alter the operation of other electronic devices.
25.1529	If mounted, it is easily removable from its mounting device or attached to it, without the need of maintenance action or the use of tools by the flight crew.	If mounted, it is easily removable from its mounting device or attached to it, without the need of maintenance action or the use of tools by the flight crew.
25.1581	Insertion of all information, table of contents and data regarding the device applicability in the A320neo Flight Manual. The application of its transmitting capability is recognized in the approved Aircraft Flight Manual (AFM), and in its absence, the EFB transmitting capability may be allowed during only non-critical phases of the flight.	Insertion of all information, table of contents and data regarding the device applicability in the A320neo Flight Manual. The application of its transmitting capability is recognized in the approved Aircraft Flight Manual (AFM), and in its absence, the EFB transmitting capability may be allowed during only non-critical phases of the flight.

Table 26: CS-25 requirements applied to the Panasonic Toughbook 55 and Apple iPad Air 4.

5.4.2 CS-27 REQUIREMENTS APPLICATION

In this second section, the CS-27 obtained requirements are considered, therefore reference is made to the application on board the Eurocopter AS 350 Ecureuil (Airbus H125), as a Small Rotorcraft.

As for the previous section, the EFBs are to be considered non-installable on board, therefore they cannot be recharged on board or at least connected to the on-board electrical system and, as well as the UPS and batteries, the DAL is low (D or E), in order to does not significantly impact on the safety.

5.4.2.1 CS-27 REQUIREMENTS APPLIED TO UPS AND BATTERIES

The CS-27 requirements are matched to the UPS and Batteries features in the Table 27:

CS	UPS SITOP 1600 Siemens	Powersonic Battery PS-1230
27.251	Mounted in areas away from main rotor, tail rotor, engine and transmission system (high vibration stressed areas).	Mounted in areas away from main rotor, tail rotor, engine and transmission system (high vibration stressed areas). The "Rugged Construction" is a good vibration resistant thanks to nonconductive ABS plastic.
27.561	Positioned, mounted (on a dedicated mounting device) and stored in such a way as not to impede the emergency egress and not to injure the occupants.	Safe operations are guaranteed in any position thanks to the spill-proof construction and the maintenance is little required.
27.610	Provided with a short-circuit protection, which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I, rated for 5 sec/min.	Not required.
27.663	Mounted in areas away from main rotor, tail rotor, engine and transmission system (high vibration stressed areas).	The "Rugged Construction" is good vibration resistant thanks to nonconductive ABS plastic
27.771	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen)
27.831	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that ensures the protection of the passengers and crew health from toxic and noxious gases.	The batteries incorporate a series of one-way low-pressure valves. These self-sealing valves allow the venting of any excess gasses that may be produced in the battery due to severe overcharging.
27.863	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that ensures the protection of the passengers and crew health from fire and flammability liquids.	The battery presents flame retardant (FR).
27.1301	The ambient temperature faced are: ● during operation -25°C to +70 °C ● during transport -40°C to +85 °C ● during storage -40°C to +85 °C	The batteries may be discharged over a temperature range of -40°C to +60°C and charged at temperatures ranging from -40°C to +50°C.

27.1309	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that concerns the achievement of safety operations.	Compliant to ISO 9001.
27.1316	Provided with a short-circuit protection, which has limitation to 3 x I rated for 30 ms; through-conductivity for 1.5 x I, rated for 5 sec/min.	The battery life is guaranteed between 200 and 1000 charge/ discharge cycles depending on the average depth of discharge, under normal operating conditions. Furthermore, the ability to recover from excessively deep discharge is increased through a balanced electrolyte system, special separators, and sophisticated plate structure.
27.1317	The UPS is compliant to the following standards: for emitted interference EN 55022 Class B and for interference immunity EN 61000-6-2.	Not required.
27.1321	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen).	If mounted in the cabin, it must not distract visually and/or acoustically the pilot. (Away from LCD screen).
27.1351	The UPS owns the CE marking, UL approval, as for USA, CB-certificate, C-Tick, that concerns the achievement of safety operations.	Safe operations are guaranteed in any position thanks to the spill-proof construction and the maintenance is little required.
27.1353	It is linked to the feed batteries.	The batteries incorporate a series of one-way low-pressure valves. These self-sealing valves allow the venting of any excess gasses that may be produced in the battery due to severe overcharging.
27.1529	It is linked to the feed batteries life.	Safe operations are guaranteed in any position thanks to the spill-proof construction and the maintenance is little required. In fact, it is not necessary the addition of electrolyte, because gases generated during overcharge are reused in a unique "oxygen cycle", through a defined gas recombination technology.

27.1581	All information, table of contents and data of the item must be inserted in the Rotorcraft Flight Manual.	All information, table of contents and data of the item must be inserted in the Rotorcraft Flight Manual.

Table 27: CS-27 requirements applied to the UPS and Batteries.

5.4.2.2 CS-27 REQUIREMENTS APPLIED TO PANASONIC TOUGHBOOK 55 AND APPLE IPAD AIR 4

The application of the CS-27 requirements to the Panasonic Toughbook 55 and Apple iPad Air 4 features is presented in the Table 28:

CS	Panasonic Toughbook 55	Apple iPad Air 4
27.251	Protected from shocks and vibrations for vehicle docking due to rugged configuration. MIL-STD-810G.	It could be affected by high vibrations during operations.
27.561	Positioned and stored in such a way as not to impede the emergency egress and not to injure the occupants.	Positioned and stored in such a way as not to impede the emergency egress and not to injure the occupants.
27.610	The Toughbook 55 must be considered in the bonding of the rotorcraft (Input: 100 V - 240 V CA, 50 Hz/60 Hz; Output: 15,6 V CC, 7,05A).	Apple iPad Air 4 must be considered in the bonding of the rotorcraft, considering 10 W Power Adapter.
27.663	Compliant to the MIL-STD-810G.	Apple iPad Air 4 could be affected by ground resonance during operation.
27.771	It must not distract visually and/or acoustically the pilot. (Away from LCD screen).	It must not distract visually and/or acoustically the pilot (away from LCD screen) and its non-reflective and oleophobic coating do not create distractions for the pilot.
27.831	No emissions of gases or vapours during operations	No emissions of gases or vapours during operations.
27.863	No escaping of flammable fluids or vapours.	No escaping of flammable fluids or vapours.
27.1301	The operating temperature goes from -29 ° C to 60 ° C and the device is compliant to the MIL-STD-810G tests (pression, temperature, humidity).	The operating temperature goes from 0° to 35° C, while the nonoperating temperature are between −20° and 45° C.
27.1309	Compliant to the MIL-STD-810G.	Apple iPad Air 4 owns the CE marking.

27.1316	The Toughbook 55 must be considered in the bonding of the rotorcraft (Input: 100 V - 240 V CA, 50 Hz/60 Hz; Output: 15 ,6 V CC, 7,05 A).	Apple iPad Air 4 must be considered in the bonding of the rotorcraft, considering 10 W Power Adapter.
27.1317	Compliant to the MIL-STD-416F (EMI and EMC).	Apple iPad Air 4 has been designed, tested and manufactured in compliance with radio frequency emissions regulations (EU standards), but such emissions could alter the operation of other electronic devices.
27.1321	It must not distract visually and/or acoustically the pilot. (Away from LCD screen).	It must not distract visually and/or acoustically the pilot. (Away from LCD screen).
27.1351	Lithium-ion, 10.8V, 6500mAh (typ.), 6300mAh (min.). Lithium-ion batteries can rupture, catch fire, or explode when exposed to high temperatures or direct sunlight. Shorting a lithium battery can cause fire and explosion.	Lithium polymer 28.6 watt hour. The battery can explode if short-circuited, due to the very low internal resistance and the consequent tremendous impulse current flowing through the cell. Furthermore, a Li-Poly cell can easily ignite if punctured.
27.1353	Possible use of breakers and/or switchers in order to minimise the electrical distress and avoid serious malfunctions.	Apple iPad Air 4 has been designed, tested and manufactured in compliance with radio frequency emissions regulations (EU standards), but such emissions could alter the operation of other electronic devices.
27.1529	If mounted, it is easily removable from its mounting device or attached to it, without the need of maintenance action or the use of tools by the flight crew.	If mounted, it is easily removable from its mounting device or attached to it, without the need of maintenance action or the use of tools by the flight crew.
27.1581	All information, table of contents and data of the item must be inserted in the Rotorcraft Flight Manual. The application of its transmitting capability is recognized in the approved Aircraft Flight Manual (AFM), and in its absence, the EFB transmitting capability may be allowed during only non-critical phases of the flight.	All information, table of contents and data of the item must be inserted in the Rotorcraft Flight Manual. The application of its transmitting capability is recognized in the approved Aircraft Flight Manual (AFM), and in its absence, the EFB transmitting capability may be allowed during only non-critical phases of the flight.

Table 28: CS-27 requirements applied to the Panasonic Toughbook 55 and Apple iPad Air 4.

5.4.3 APPLICATION OF ENAC EFB COMPLIANT CHECKLIST

After qualitatively comparing the requirements of the CSs and the characteristics of the commercial parts, a further verification is provided by a compliance checklist of EFBs, provided by ENAC , [44], for Panasonic Toughbook 55 and Apple iPad Air 4.

This checklist is not meant to replace the approval for additional electronic devices on-board from the Certification Authorities, but it helps to verify that no further hazards will occur.

Both in the first use and in the later significant modifications of the EFB, such as updates or insertion of software or hardware, the checklist must be elaborated and inserted in the EFB manual.

The Table 29 shows the original structure and questions of the ENAC compliance checklist, [44]:

Requirement	***Reference***	***Panasonic Toughbook 55***	***Apple iPad Air 4***
Has an EMI assessment of the EFB been undertaken, and using which method?	*AMC1 CAT.GEN.MPA.140*	✓ *(MIL-STD-416F)*	✓ *(EU standards)*
Is the EFB hardware Installed or Portable?	*AMC1 CAT.GEN.MPA.141(a)*	*Portable*	*Portable*
Is the EFB able to be easily removed from its mount or stowage?		✓	✓
Does the EFB have a suitable Mount or Viewable Stowage? If not have procedures been developed to ensure that it is stowed during critical phases of flight?		✓	✓
The placement of the EFB is such that to avoid any impairment to the crew's external view, the access to instruments and it does not impede emergency egress?		✓	✓
Is the display within 90 degrees of the crew member's line of sight, and would glare or reflection interfere with the pilot?		✓	✓

If rotorcraft power is used, are the characteristics compatible with the EFB?		✓	✓
Does the EFB have data connectivity to the rotorcraft; if so, how is transfer of data controlled?		*X*	*X*
Are all connecting cables/power adaptors approved by the EFB manufacturer and placed so as not to cause obstruction?		✓	✓
If a viewable stowage (support) is used has its location been documented as part of the EFB policy?		✓	✓
The viewable stowage and associated mechanisms are such that it does not impede the flight crew members in the performance of any task (open window, switches, levels…)?		✓	✓
Is the viewable stowage easily locked in position?		✓	✓
Does the viewable stowage's range of movement accommodate the expected range of anthropometric constraints?		✓	✓
Will the viewable stowage be able to withstand all foreseeable conditions such as turbulence or hard landings?		✓	✓
With the viewable stowage fitted is there any interference with aircraft controls or equipment?		*X*	*X*
Can the viewable stowage be removed from the aircraft without the use of tools?		✓	✓
Have procedures been put in place to ensure that the means of securing the viewable stowage remain within acceptable limits, and who will be responsible for conducting these serviceability checks?		✓	✓
If the viewable stowage uses a suction cup type attachment, how was it demonstrated		✓	✓

that they would function following a rapid decompression?			
How has it been demonstrated that following detachment of a viewable stowage it will not jam the flight controls, injure the crew or cause damage?		✓	✓

Table 29: EFB compliance checklist, provided from ENAC, [44].

The first requirement concerns the EMI assessment and which methodology was applied to obtain compatibility: in the case of the Toughbook 55, it was compliant with MIL-STD-416F, while Apple iPad Air complies with EU standards.

However, the EFBs are not expected to have a data connection in the analysis performed, therefore they cannot transfer data and the involved boxes are marked with an X.

Furthermore, the application and use of the EFBs is of the no-hazard type, therefore any potential feature or functionality of the EFBs that may cause interference with the aircraft equipment is disabled.

In conclusion, the last requirement regards the emergency landing conditions, extensively discussed in CS xx.561 requirements.

5.5 MITIGATING ACTIONS

All the interventions necessary to ensure that the characteristics of a part match the reference legislation, respecting its content, are included in the mitigation actions.

When a feature or functionality of a part does not fully comply or is totally opposed to the dictates of the legislation, mitigation actions must be developed and implemented to always maintain and ensure a no-hazard result.

By order, all the mitigation actions to be assessed for each device will be mentioned.

Firstly, for the UPS, it is recommended to position and mount it in a fixed position in the cabin, away from parts subjected to vibrations, intense loads and/or thermal and pressure stress. Furthermore, the position and installation must neither create visual or acoustic distractions for the pilot, nor be an obstacle to the escape route or a mass item that could fall and injure people.

From a technical point of view, the UPS must be contained in a case in order to maintain the operational temperature range and must not be exposed to the external areas.

In a subsequent post-installation phase, the UPS must be considered in the bonding of the helicopter or airplane and undergo the environmental tests dictated by the DO-160 standard.

Secondly, the batteries provide low power so there is no need to consider safety mitigation actions. Furthermore, all functional and technical characteristics are fully included in the requirements of the CSs.

For what concerns the EFB, Panasonic Toughbook 55 owns different military standard certifications. In fact, according to this work aim, it is only recommended, in subsequent phases, to carry out environmental tests provided by DO-160, regarding Audio Frequency Conducted Susceptibility - Power Inputs.

However, it must be positioned away from the line sight of view of the pilot, not creating distractions and, in case of mount Toughbook, the mounting device must be controlled and verified that is in the correct position and it is not subjects to movements or falls.

Its lithium-Ion batteries provide low power, but it must be avoided the direct exposure to sunlight or heat sources. In case of installation on board a rotorcraft, it is necessary that the Toughbook is not exposed to external areas in order to remain within the operating temperature range. However, the device must be not also exposed to vibrational and pressure stress and/or external intense loads, therefore the installation must take place away from the transmission areas, from the rotors or from the engine.

Finally, Apple iPad Air 4 represents the most delicate and fragile device of the four, as various mitigation actions must be taken to remedy the lack of compliance with the requirements. It must not be exposed to the areas more interested by vibrations or other intense loads, due to the rotorcraft ground resonance, because it has very low resistance ranges to thermal, structural shocks or falls. Consequently, it must be mounted on a solid and fixed device to dock it in order to prevent injuries to the persons and preserved from external sources.

Moreover, the operative temperature range must be maintained stowing or using the device in the internal areas, avoiding the long and continuous exposure to the sunlight or heat sources, as well as for the batteries. They are covered with a plastic casing that prevents the punctures, but it is not thermally insulated.

As for the Toughbook, Apple iPad Air 4 must be positioned away from the line of sight of the pilot and mounted on a device to easily docks and seamlessly integrates it.

In subsequent phases, it is recommended to carry out environmental tests provided by DO-160, regarding Audio Frequency Conducted Susceptibility - Power Inputs, Fire and Flammability, and technical tests provided by the DO-178B and DO-254 standards.

6 CONCLUSIONS

In this section, an example of space application will be provided concerning the use of commercial parts, from which the conclusions common to all the work will be deduced.

The application and use of commercial parts, tested, verified and then certified, also impacted the space context. For instance, the small drone-helicopter, named Ingenuity, designed and built by NASA to support the Perseverance rover in its mission to Mars, is equipped with a processor that is even less powerful than a common latest generation smartphone, [45]. The Figure 24 shows NASA Ingenuity:

Figure 24: NASA Ingenuity representation, [45]

According to NASA [45], Ingenuity mission is a technology demonstration devoted to test a first autonomous and monitored flight on the Martian field. The helicopter was released by the rover Perseverance to the surface where it realized a series of three successful flights. The mission difficulty was very high due to the different atmosphere condition of Mars, the mission objectives regarding the distance covered and the altitude reached, and to the only remote control from the Earth.

For these reasons, the primary requirements of this application are certainly great reliability, slight precision, and strong resistance to the different and difficult environmental conditions they will have to face.

NASA has declared [45] that Ingenuity drone consists of a Qualcomm® Snapdragon™ 801 processor, shown in the Figure 25:

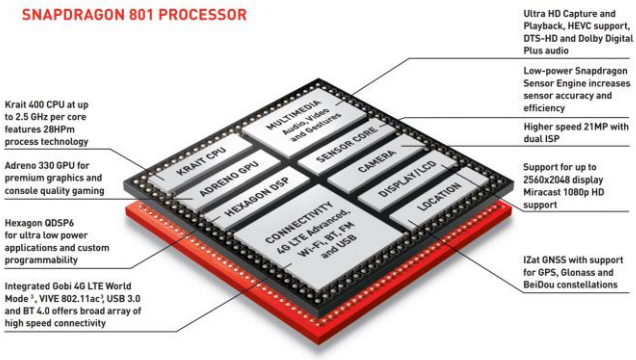

Figure 25: Qualcomm® Snapdragon™ 801 processor, [46]

According to what provided by the manufacturer [46], the processor is a quad-core up to 2.5 GHz, with Adreno 330 GPU, has the ability to produce video in 4K and provide the position via satellite systems (GLONASS, GPS, Beidou), among many characteristics that distinguish it. It represents an excellent compromise between power efficiency and reliability and high performance. Moreover, the costs are very low compared to those incurred to design, build and implement a space-qualified product, as the market cost of *Snapdragon 801* is a few hundred dollars, making it very inexpensive and at an excellent quality/price ratio.

In other words, a valid, at the same time reliable and cost-effective, alternative can be implemented and exploited even in a very sophisticated and complex field such as space, where human intervention during operations is almost impossible. In this way, not only the design, development, production and implementation times of any new qualified product are reduced, but also the costs are greatly amortized.

Consequently, the certification of commercial parts for no-hazard aeronautical use, as well as for the space context, becomes fundamental, in order from one side to support an increasing employ of commercial parts already developed and known for specialized use, reducing design, and testing costs and exploiting already existing resources, without forgetting the advantages for the environmental impact, due to the, albeit minimal, reduction of industrial processes, and on the other side to optimize the long certification process according to certain qualification classes (i.e. Space-qualified), while maintaining high standards of quality, reliability for the component and the mission as a whole, and above all for safety.

The ambition is to lay the foundations for an aeronautical and above all space market that could become more economically permissive and attractive, as well as environmentally sustainable.

7 REFERENCES

[1] EASA, *AMC 25.1309,* 2020.

[2] M. Forte e Salvador, «Risk assessment: workers operating in loading/unloading (shipping/receiving) areas,» 2013.

[3] FAA, *MIL-STD-882D,* 2000.

[4] ICAO, *Safety Management System,* 2018.

[5] FAA, *The Safety Continuum – A Doctrine for Application,* 2015.

[6] ICAO, «ICAO,» [Online]. Available: https://www.icao.int/Pages/default.aspx.

[7] FAA, «FAA,» [Online]. Available: https://www.faa.gov/.

[8] ICAO, «Convention On International Civil Aviation,» 1944.

[9] EASA, «AMC,» [Online]. Available: https://www.easa.europa.eu/document-library/acceptable-means-compliance-amcs-and-alternative-means-compliance-altmocs.

[10] EASA, «CS,» [Online]. Available: https://www.easa.europa.eu/document-library/certification-specifications.

[11] European Parliament, «Regulation (EU) 2018/1139,» 2018.

[12] European Parliament, «Commission Regulation (EU) No 748/2012,» 2012.

[13] European Parliament, «Official Journal of the European Union, L 362,» 2014.

[14] EASA, «Aircraft Certification,» [Online]. Available: https://www.easa.europa.eu/domains/aircraft-products/aircraft-certification.

[15] Sky Arrow, «Sky Arrow Type Certification EASA CS-LSA,» [Online]. Available: http://www.skyarrow.it/2019/10/the-sky-arrow-type-certification-easa-cs-lsa/.

[16] EASA, «Part 21- Airworthiness and Environmental Certification».

[17] SAE, ARP 4754A - Guidelines for Development of Civil Aircraft and Systems, 2010.

[18] SAE, ARP 4761 - Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment, 1996.

[19] RTCA, DO-178B - Software Considerations In Airborne Systems And Equipment Certification, 1992.

[20] RTCA, DO-254 - Design Assurance Guidance for Airborne Electronic Hardware, 2000.

[21] EASA, CS-25 Amendment 26, 2020.

[22] EASA, «Annual Programmes & Reports,» [Online]. Available: https://www.easa.europa.eu/annual-programmes-reports.

[23] ECSS, European Cooperation for Space Standardization, «ECSS-Q-ST-30-02A,» 2001.

[24] ICAO - NEBOSH National Diploma - Unit A | Managing Health and Safety, «Fault Tree Analysis (FTA) and Event Tree Analysis (ETA),» 2014. [Online]. Available: https://www.icao.int/sam/documents/2014-adsafass/fault%20tree%20analysis%20and%20event%20tree%20analysis.pdf.

[25] FAA, «Job Aid - Conducting Airborne Electronic Hardware Reviews,» 2008.

[26] RTCA, DO-178C, 2011.

[27] Cadence, «DO-254 Explained,» 2019.

[28] RTCA, DO-160 Environmental Conditions and Test Procedures for Airborne Equipment, 2010.

[29] FAA, MIL-STD-810G Environmental Engineering Considerations and Laboratory Tests.

[30] EASA, CS-27 Small Rotorcraft Amendment 8, 2021.

[31] FAA, MIL-STD-1543 Reliability Program Requirements For Space And Launch Vehicles, 1988.

[32] Wikipedia, «Uninterruptible power supply,» [Online]. Available: https://en.wikipedia.org/wiki/Uninterruptible_power_supply.

[33] Siemens, *SITOP UPS1600 Data Sheet 6EP4136-3AB00-2AY0,* 2015.

[34] Wikipedia, «DIN rail,» [Online]. Available: https://en.wikipedia.org/wiki/DIN_rail.

[35] POWERSONIC, «Powersonic PS-1230 Battery Technical Specifications,» 2018.

[36] EASA, AMC 20-25 Airworthiness and operational consideration for Electronic Flight Bags (EFBs), 2014.

[37] Panasonic, «Panasonic Toughbook 55 Data Sheet,» 2019.

[38] FAA, MIL-STD-461F Electromagnetic Interference Characteristics Of Equipment, 2015.

[39] Apple Inc., «iPad Air,» [Online]. Available: https://www.apple.com/lae/ipad-air/.

[40] Airbus, «Airbus A320 family,» [Online]. Available: www.airbus.com/aircraft/passenger-aircraft/a320-family/a320neo.html.

[41] Skybrary, «Airbus A320,» [Online]. Available: https://www.skybrary.aero/index.php/File:A320_3D.jpg..

[42] Skybrary, «Eurocopter AS 350 Ecureuil,» [Online]. Available: https://www.skybrary.aero/index.php/AS50..

[43] Airbus, «Airbus H125,» [Online]. Available: https://www.airbus.com/helicopters/civil-helicopters/intermediate-single/h125.html.

[44] ENAC , «EFB compliance checklist,» [Online]. Available: https://www.enac.gov.it/documenti/electronic-flight-bag-efb-compliance-checklist.

[45] NASA, «6 Things to know about NASA's Ingenuity Mars Helicopter,» 2020. [Online]. Available: https://www.nasa.gov/feature/jpl/6-things-to-know-about-nasas-ingenuity-mars-helicopter/.

[46] Qualcomm Snapdragon, «Qualcomm Snapdragon 801 Processor Data Sheet,» [Online]. Available: https://www.qualcomm.com/media/documents/files/snapdragon-801-processor-product-brief.pdf.

[47] ECSS, European Cooperation for Space Standardization, *ECSS-Q-ST-30C,* 2017.

[48] NASA, «EEE Parts Risk Assessment Matrix for Space Flight Applications /7, /8».