

ED-334

GUIDANCE FOR COMMON MODE ANALYSIS FOR LIFT - THRUST SYSTEM FOR VTOL ENHANCED CATEGORY

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

FEBRUARY 2025

FOREWORD

1. This document was developed by EUROCAE Working Group 112 “VTOL”, SG-2 “Lift-Thrust” and was approved by the EUROCAE Director General on 16 January 2025.
2. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.

following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
4. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
5. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
6. Copies of this document may be obtained from:

EUROCAE

9 – 23 rue Paul Lafargue

93200 Saint-Denis

France

Telephone: +33 1 49 46 19 65

Email: eurocae@eurocae.net

Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	i
TABLE OF CONTENTS	i
TABLE OF FIGURES.....	i
TABLE OF TABLES.....	ii
CHAPTER 1 INTRODUCTION	1
1.1 PURPOSE AND SCOPE.....	1
1.2.1 Background.....	1
1.2.2 Discussion.....	2
1.3 COMMON MODE ANALYSIS BACKGROUND	3
1.4 DEFINITIONS AND ABBREVIATIONS DEFINITIONS AND ABBREVIATIONS.....	4
1.4.1 Abbreviations	4
1.4.2 Definitions	4
1.5 REFERENCES	4
CHAPTER 2 DISCUSSION.....	5
2.1 DEFINITION OF "SINGLE FAILURE"	5
2.2 GENERAL CONSIDERATIONS	5
CHAPTER 3 PROPOSED WAY AHEAD FOR CMA DISCUSSION.....	6
CHAPTER 4 CMA DISCUSSION.....	7
4.1 CMA DISCUSSION ON PROPELLER	7
CHAPTER 5 CMA DISCUSSION ON BATTERIES	18
5.1 DEFINITIONS/DESCRIPTION	18
5.2 GENERIC FUNCTIONAL BREAKDOWN	20
5.3 FUNCTION SEVERITY/CMA	20
5.4 EXAMPLES OF COMMON MODES	20
5.5 A TO PROVIDE ELECTRICAL ENERGY/POWER.....	20
5.6 B TO PROTECT BATTERY / VEHICLE CONSIDERING OVERHEAT CONDITION	21
5.6.1 B.1 to Protect Battery from Vehicle Abuse Condition	21
5.6.2 B.2 to Protect Vehicle from Battery Internal Failure	21
5.7 ERRORS CHECK LIST/MITIGATIONS	21
WG-112 SG-2 MEMBERSHIP	53
IMPROVEMENT SUGGESTION FORM	60

TABLE OF FIGURES

Figure 5-1: CMA discussion on batteries description	19
---	----

TABLE OF TABLES

Table 4-1: Propeller CMA Check list	8
Table 5-1: Functional Breakdown.....	20
Table 5-2: Batteries CMA Check list	22

CHAPTER 1

INTRODUCTION

1.1 PURPOSE AND SCOPE

This document contains the results of discussions and considerations regarding Common Mode Analysis (CMA) application for Lift Thrust System for eVTOL in the frame of SG2 DP002 task sheet.

The objective is to give guidance for the application of SC VTOL and proposed MOC SC VTOL considering the enhanced category.

The SC VTOL and MOC 4 SC VTOL respectively require the no single failure criteria paying particular attention to common cause failures, including common mode errors and cascading failures in MOC VTOL.2510.7b when independence cannot be shown.

In addition, MOC 4 VTOL.2300 gives a special focus on Fly by Wire, highlighting the need for high integrity and availability.

1.2 DESCRIPTION OF LIFT THRUST SYSTEM FOR EVTOL

1.2.1 Background

The two following examples provide a description of lift and thrust principles for conventional aircraft. Flight control is also described, in order to make the link with VTOL specificities described later.

1.2.1.1 Aeroplane example

The thrust is directly produced by the engines, by reaction or using a propeller,

The lift is provided by wings as a function of aircraft speed. Sufficient lift can be maintained for landing by gliding (depending on flight phase),

Flight control: flight control surfaces provide the control of the aeroplane independent of thrust generation.

1.2.1.2 Helicopter example

The thrust is given by the engines and the cyclic pitch setting of the rotor.

The lift is provided by the rotor and its collective pitch angle. Lift is reduced in case of engine loss, but autorotation with vertical speed control for flare and landing remains possible.

Flight control: helicopter control is maintained as long as sufficient rotor speed is available.

For these two examples, the flight controls are independent from lift and thrust generation. Aircraft control is maintained after engine power loss.

1.2.1.3 VTOL

Currently, various VTOL configurations are being developed, with significantly diverse architectural and technical choices.

Among them, we can cite:

1. Vehicle architectures:

- Tilting wings,
- Tilting propellers (possibly including thrust vectoring),
- Many small propellers or fewer larger propellers,
- Variable speed at propeller level to control VTOL lift and attitude,
- Variable pitch (possibly in combination with variable speed) at propeller level to control VTOL lift and attitude,
- Ducted fans / propellers.

2. Power source types:

- Conventional engine and fuel such as gas turbine or reciprocating piston engine,
- Electric motor(s),
- Li-Ion batteries,
- Hybrid propulsion,
- Hydrogen fuel cell,
- Etc.

This list is far from being exhaustive, and combinations between these characteristics can be observed.

1.2.2

Discussion

is the case for conventional aircraft (helicopter or aeroplane).

As a consequence, most of the VTOL vehicle architectures currently being developed:

- Have limited or no gliding or autorotation capability: the vertical speed control is lost in case of total or significant power loss,
- Control the vehicle by controlling the thrust vector: vehicle control is lost in case of total or significant power loss, or loss/malfunction of thrust setting control.

Effective and acceptable mitigation means may be different when addressing failure conditions affecting the lift/thrust function or the flight control function of conventional aircraft. This is due to various reasons:

- Experience,
- Complexity,
- Severity conditioned by flight phase ("full time, part time"),
- Severity driven by availability and integrity, or just integrity,
- Etc.

Therefore, from aircraft function level, safety constraints allocated to Flight Control will be inherited by the Lift and Thrust system to a certain extent, as Lift and Thrust directly contributes to Flight Control.

This extent may vary depending on the level of Lift and Thrust contribution to the Flight Control.

Of course, these considerations regarding distributed lift and thrust contributing to vehicle control can be different, or vary dependent on the flight phases.

Presence of wings, or tilted surfaces, presence of independent control surfaces on wings can lead to different conclusions. Such a vehicle may be able to maintain a controlled trajectory after power loss. Considering the vertical take-off / landing capabilities, this controllability may not be possible 100% of the time, but the power loss would not be "full time" critical.

As an example, variable speed propellers which ensure the lift and thrust, but also the full controllability of the A/C should have the same safety objectives as Flight Control.

Lift and thrust provided by propellers having a capability to rotate upon motor loss and having an independent controllable pitch could be submitted to less severe constraints, provided that auto-rotation capability can be demonstrated.

This is a possible mitigation for which credit can be claimed, but which will not be debated in this document.

General opinion is that the new VTOL enhanced category aircraft, which fly mainly over congested areas will require to have at least the same level of safety as conventional CS-25 aircraft or CS-29 helicopters (refer to MOC VTOL.2510 for safety level).

It is considered in this document that the Flight Control function encompasses the Flight Control system and the Lift/Thrust System. This covers the architecture with the highest level of integration, as described above. Of course and as explained, mitigation at vehicle architecture level may exist and credit could be taken from this during the CMA. Unfortunately, considering the multitude of possible architectures, it is not possible to analyze all solutions in this document. If an applicant's design is not of the highest level of integration, it will have to identify with the authority which mitigations can be claimed.

1.3

COMMON MODE ANALYSIS BACKGROUND

Starting from regulation, the need for CMA is cascaded through 2x.1309 (or MoC SC VTOL 2510 and 2300), and the associated AMCs which refer to ED-79B/ARP4754B and ED-135/ARP4761A as guidance documents.

ED-79B/ARP4754B and ED-135/ARP4761A are the two main documents which currently describe how to conduct a CMA, covering the notion of single failure, common mode error, and cascading failures.

The objective of this document is not to supersede those documents, but to specifically highlight within a very limited scope a methodology for lift and thrust systems fitted to VTOL enhanced category.

In particular, this document does not develop how Independence Principles/Requirements related to failures/errors or FDAL/IDAL assignment are established.

The present status quo on conventional multi-engine aeroplanes or helicopters is that there is independence but no dissimilarity between engines. The engines are certified according to CS-E regulation with requirements which provide a level of confidence on engine safety performance compatible with HAZ events at engine level. CS-E regulation is the result of decades of experience. An additional layer handled by the aircraft manufacturer is used to demonstrate the CAT substantiation including the “no single failure” demonstration at aircraft level, taking into account aircraft system architecture.

On the other hand, all FbW systems on conventional aircraft embed strong independence usually done by hardware and software dissimilarity to cover availability purposes. This independence is complete to a greater or lesser extent but as a minimum covers complex items. The integrity is covered by various means such as dissimilarity or different contextual usage.

To summarize the situation for conventional aircraft, the non-dissimilarity is accepted for engines, while some dissimilarity and various other mitigations are systematically implemented for FbW; retained strategies vary from one OEM to another. This is the result of decades of satisfactory experience.

Considering the piloting difficulty of the currently proposed VTOL vehicle architectures, in particular upon rotor failure, it is supposed that these vehicles will have to be equipped with full-authority FbW flight control systems. FbW systems developed for conventional aircraft have demonstrated an acceptable safety level with regard to CMA and therefore the FbW core of a VTOL architecture should consider similar Common Causes mitigation strategies.

Concerning Lift and Thrust, the key differences with respect to conventional aircraft are:

- New technologies (for some VTOLs): HVDC battery, High Voltage electrical networks and associated Electrical Power Management, Electric motors rather reciprocating internal combustion or gas turbine engines,
- Change of scope as Lift and Thrust contributes to the aircraft control.

As a consequence, it is necessary to evaluate carefully the LTS situation versus Common Modes considerations. Being a new technology, field experience cannot be claimed as is the case for conventional engines.

One of the key questions concerns acceptable mitigations to satisfy common modes expectations for a full-time critical function. In particular it should help to answer the MOC VTOL: “*Sources of common mode failures include development, manufacturing, installation, maintenance, shared resource, event outside the system(s) concerned, etc. When identifying mitigation means for specific common modes, the means should be appropriate to the common mode failure/error. It is important to note that even items that are developed to IDAL A may be subject to development error. Such error may simultaneously affect several instances of the same item with potential functional or safety consequences. EASA has experienced cases, where a development error in IDAL A item has even resulted in simultaneous failures of all affected equipment. Therefore, it should not be assumed that IDAL A items are protected from such development errors and consequently they should be included in the scope of the common mode analysis irrespective of the FDAL/IDAL of the system/item.*” (Source:

EASA MOC SC-VTOL, Issue 2 – MOC VTOL.2510 Equipment, systems, and installations - §9(b) Common mode considerations).

1.4

DEFINITIONS AND ABBREVIATIONS

1.4.1

Abbreviations

AC	<i>Alternate Current</i>
BMS	<i>Battery Management System</i>
CAT	<i>Catastrophic</i>
CCA	<i>Common Cause Analysis</i>
CMA	<i>Common Mode Analysis</i>
CSCI	<i>Configuration Software Configuration Item</i>
DC	<i>Direct Current</i>
DAL	<i>Design Assurance Level</i>
ETSO	<i>European Technical Standard Order</i>
EASA	<i>European Aviation Safety Agency</i>
EHPS	<i>Electric / Hybrid Propulsion System</i>
FbW	<i>Flight by Wires</i>
HAZ	<i>Hazardous</i>
LTS	<i>Lift Thrust System</i>
LTU	<i>Lift Thrust Unit</i>
MOC	<i>Mean Of Compliance</i>
MOPS	<i>Minimum Operational Performance Specification</i>
PFMEA	<i>Process Failure Mode and Effects Analysis</i>
PRA	<i>Particular Risk analysis</i>
VTOL	<i>Vertical Take Off and Landing</i>
ZSA	<i>Zonal Safety Analysis</i>

1.4.2

Definitions

Battery: device used for energy storage, consisting of one or more electrically connected cells, having positive and negative terminals. A battery may include inter-cell connectors, protective devices, circuitry, and other components.

Battery cell: A single electrochemical unit which exhibits a voltage across its two terminals and is used as a component of a battery module.

Battery Management System (BMS): Any electronic system that manages a rechargeable battery (cell or battery pack), such as by protecting the battery from operating outside its safe operating area, monitoring its state, calculating secondary data, reporting that data, controlling its environment, authenticating it and / or balancing it.

Battery Modules: A battery module is a combination of multiple battery cells.

1.5

REFERENCES

- ARP
- SC-VTOL
- MoC VTOL
- CS P
- ED-12 DO-178
- ED-80 DO-254

CHAPTER 2

DISCUSSION

2.1 DEFINITION OF “SINGLE FAILURE”

The following extracts of MOC SC VTOL 2510 (8)(b) and (9)(b) can be useful to better understand the notion of single failure and error:

Error: An omission or incorrect action by a flight crew member or maintenance personnel, or a mistake in requirements, design, or implementation. Note: Errors may be failures (Source: adapted from AMC

25.1309 in Book 2 of CS-25 Amdt. 24).

“A single failure includes any set of failures which cannot be shown to be independent from each other. Common-cause failures (including common mode failures) and cascading failures should be evaluated as dependent failures from the point of the root cause or the initiator. Errors in development, manufacturing, installation, and maintenance can result in common-cause failures (including common mode failures) and cascading failures.”

“Establish program-specific checklists (for common mode types, sources, and resulting failures/errors). ED-135/ARP4761A paragraph K.3.1 can be followed for this purpose. These checklists should be used to detect elements that may defeat the redundancy or independence principles within the design.”

This is defined in EASA MOC SC-VTOL, Issue 2 – MOC VTOL.2510 Equipment, systems, and installations - §8(b) Single failure and common cause failure considerations.

Failure: An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). (Source: adapted from AMC 25.1309 in Book 2 of CS-25 Amdt. 24).

2.2 GENERAL CONSIDERATIONS

As previously stated, the objective of this document is not to offer a defined list of acceptable mitigations, but rather to define a non-exhaustive list of potential common mode mitigations for a given set of techno bricks.

The objective of the applicant will be to determine the right level of mitigations.

Sometimes:

- a sole mitigation can be enough, if, for example it is considered sufficiently robust
- several layers of mitigation may be necessary.

The exercise focuses on Common Modes, therefore there is no quantitative approach; quantitative objectives will drive, inter alia, the required number of redundancies, but generally no credit can be taken from identical redundancies to avoid common modes. Nevertheless, it is also acknowledged that identical redundancies, used in different contexts (e.g.: usage, stress level, environmental conditions), may bring a certain level of mitigation.

There are also some state-of-the-art rules in aeronautical world, such as quality controls, equipment acceptance tests, etc. These are not designed in the first instance as mitigations against common modes; however, they may be extended so as to serve as mitigations. For example, a dedicated inspection or test which aims to discard equipment with a fault identified through a CMA exercise as potential root cause of a common mode, can be considered as a mitigation.

There is no specificity to the implementation of a CMA for an enhanced category VTOL: there is no need to propose an AMC for CMA implementation on VTOL aircraft, existing material is applicable.

CHAPTER 3

PROPOSED WAY AHEAD FOR CMA DISCUSSION

The question to be answered is how to make LTS (with an FCS contribution) robust to common error/failure in case of multiple or redundant systems.

CMA is described in ED-135/ARP4761A Main body §4.6 and Appendix M. As a reminder, the objective of the CMA is to identify and demonstrate that independence requirements have been defined and are fulfilled.

As an example, it is necessary to demonstrate sufficient independence in case of DAL reduction with system architecture consideration.

If safety is based on FDAL A or IDAL A alone (no DAL decomposition), some authorities may request in addition to the Development Assurance, a CMA to support, for catastrophic scenarios, that remaining residual errors are minimized, and/or that sufficient mitigations exist. Some authorities may also ask that a CMA support the “no single failure criteria” (typically if shown by FDAL A or IDAL A alone).

Lift and thrust contributes to the Flight Control function for which availability and integrity have to be demonstrated.

Rather than developing a full CMA example, which will necessarily re-use already known methods, typically those developed in ED-79B/ARP4754B and ED-135/ARP4761A to identify independence principles/requirements, or to focus on a specific vehicle architecture, it is proposed to focus on a limited exercise.

The idea is to have a discussion about possible CMA approaches to cover availability and integrity for several technological bricks of LTS which are common to most VTOL architectures, and which are not used in the same manner on conventional aircraft:

- electric motors (will be covered in a future issue of this document)
- batteries
- propellers. Propeller is not a system but should be considered as a set of propellers which failure of one propeller may directly or indirectly impact the others.

Indeed, these technological bricks, despite not being entirely novel, will be used for the first time with such a high severity level.

Other technologies, also not entirely novel could be used for the first time, but will not be detailed in this document, despite fully relevant for a CMA. As examples, SSPC, tilting motors, propeller pitch control, etc.

No assumption is made about vehicle or system architecture choices, the idea is simply that for each of the technological bricks the CMA questionnaire (checklist) be established and possible common modes and mitigations discussed.

Knowledge of potential common modes affecting technological bricks is used as an input for upstream architecture studies. This will help to define an appropriate architecture.

The appropriate architecture can be based on different strategies such as contextual usage, dissimilarity, quality, extensive checking, high FDAL/IDAL, etc., and of course a mix of several mitigation means is possible.

The resulting architecture is not a unique choice, several architectures may be possible, each will have advantages and drawbacks.

NOTE: *Common modes are of course a safety risk, but a difference can be made between common modes which affect reliability and may have mid/long term effects, and common modes which are revealed by a trigger. Such a trigger (environment, system state, etc.) can affect all redundancies at the same time or during the same flight. This last category is of course the most critical.*

CHAPTER 4

CMA DISCUSSION

Following the CMA methodology as described in ED-135/ARP4761A Main body §4.6 and Appendix M, checklists will be used for this analysis.

Checklists depend on various inputs.

The first level is based on a subset of categories given by Appendix M (development, Manufacturing, Integration, Maintenance). Next levels are refined subcategories which depend on the systems being analyzed, the technologies, the field experience and any other relevant input.

Considering the risk identified in the most refined “error” category, possible mitigations are discussed.

When necessary, additional information is given by the “comment” column.

The two following paragraphs present a model CMA focused respectively on Propellers, Batteries. A future issue will cover Electric motors.

For each of the three topics, the ED-135/ARP4761A Appendix M checklist is used. Nevertheless, some categories may be considered for one topic and not for another if deemed as not relevant or not considered to simplify the reading of this document.

4.1

CMA DISCUSSION ON PROPELLER

It is proposed to start a first discussion by assuming a propeller (without pitch control) as a first test case without considering the cascading effect in case of burst or blade release. This event will be analyzed in accordance with ED-306.

The discussions start by identification of possible errors during the whole life cycle of the system, then possible mitigation actions are identified.

Only the propellers are concerned in the frame of this CMA discussion. The associated actuators are not in the scope of this CMA.

Assumptions:

- A common failure on a given number of propellers leads to a catastrophic/hazardous failure condition (without consideration of cascading effects).
- The propellers under study are of similar design.

The discussions are summarized in the following table.

The first three columns identify the Errors to be considered according to the product life cycle.

The remaining columns describe possible mitigations with accompanying explanation and comments.

TABLE 4-1: PROPELLER CMA CHECK LIST

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
Development	Specification	Missing/mismatch requirements	Define General Requirement Specification for UAM Equipment, to be used as a reference and driving all the specifications dedicated to the subsystems	
		Bad identification of spectrum, constraints (loads, speeds, torque, mission profile, unbalance, induce vibration)	For each detailed design model, make a validation with several methods (analysis, experience, pair review, etc.) to make sure influencing parameters are appropriately captured with possible range, for example: - nominal - maximal (e.g.: in normal conditions, in adverse conditions, in failure conditions, etc.) - transient - cyclic values - etc. Define the appropriate factors of safety (for loads, materials) to be considered for analysis and tests (both static & fatigue). Specification of sufficient design margins to cover all possible conditions/events (ageing, fatigue, operational/environmental conditions/events). Identification, validation and verification of design assumptions by test (flight, test rig, endurance, etc.). Characterization of the propeller by test (incl. Identification of the operational and critical limits of the propeller, relevant measurements during robustness/stress tests). Specification of additional protection mean to reduce the effects if adverse condition or failure occur: - active protection: Overspeed/overtorque limitation	Validation of the specification is not detailed here, but is a key topic to prevent errors.

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
			- preventive protection: Usage Monitoring System to check in real life consistency between usage and design assumptions (cycles counting, spectrum, loads recording, etc.) - specific inspections (during turn around, maintenance inspection, balancing check, etc.). Sufficient in-service experience with similar specification, for example on an in-service aircraft with a similar mission profile and environmental operating conditions.	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
	Environmental constraints (vibration, temperature, humidity, PRA's topics, etc.)		Identify relevant environment for normal use, exceptional use and failure cases. For each environment and relevant usage case: - make sure maximum levels are identified - spectrum is known. Examples of environment are: - temperature, temperature cycles - lightning - hail - icing - bird(s) - volcano ashes, sand and dust - FOD aggression in flight and on ground - etc. These environments have to be considered alone, but can also be cumulated. As an example, hail combined with lightning strike is a likely situation. For some material, several environments can have a significant impact. As an example for composite materials: the degradation factors can be induced by moisture, temperature and contaminants (acid rain, pollution, sand/dust) Mitigation can be: - stronger protective layers like additional painting, instrumental inspections - design margin - endurance and robustness tests - etc. The resulting stresses of normal usage (start /stop phases, accelerations, etc.) should also be combined with environments.	The key idea is to be able to demonstrate with confidence that all the failure modes of one or several propellers, or malfunction due to external threats (resulting from failure(s), external event, adverse conditions), have been fully identified, tested and their worst impacts assessed.

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
			Possibly, identification of environments and compliance to the objectives can be made in a PRA. Sometimes, mission profile depends on weather conditions and forecast (reduced or aborted in case of adverse conditions, such as hail, storms, strong wind, icing conditions). If systems are used to control the level of the aggression, for example an icing detection to avoid/limit exposure to icing, or ground facilities for weather forecast, the common cause failures/modes of these devices should also be considered. Identification of maximum level of vibration upon failure/external aggression To illustrate the notions of normal use, exceptional use and failure cases, vibrations is used. There are: - normal vibration level - exceptional vibration level (e.g.: of adverse conditions, icing conditions) - failure case, example of blade separation. These vibration levels can be evaluated by tests, analyses, etc.: - unbalance testing and endurance of one or several propellers - blade separation testing - propeller separation testing - propellers susceptibility testing to external vibration generator in failed condition (unbalance rotating parts, flutter, etc.).	
	Sizing	Bad model	The propeller sizing should cover several aspects: - performance - mechanical dimensioning (static, fatigue) - aero elastic behavior	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
			- noise - etc. This could be covered by different models. Models can be empirical (e.g.: noise measurement at various regimes) or based on a physical approach (e.g.: finite elements for mechanical dimensioning). A great care should be taken to the limits of the models. Tests can be used to correlate the models predictions with real measurements. As a result, models could be: - invalidated by the tests (root cause of the error must be investigated) - confirmed by the tests - considered “valid” but with need to re-adjustments Tests should also confirm that the models limits, if any, are confirmed. Model validation and verification by several means: - test: - Physical Mockup can mitigate mistakes related to dimension of the parts and their accessibility - theoretical model based on wind tunnel tests - ground testing - flight testing. - experience, etc. Models can be based on assumptions. Therefore, tracking assumptions during V&V process ensures errors done during and post modeling will be minimized.	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Development/design process				
		Damage tolerance (What kind of damage must be taken into account)	Define sources of possible damages: - external aggression (FOD, gravels, garbage, etc.) - inadvertent damage during servicing - inadvertent damage during manufacturing/assembly (shocks, etc.). NOTE: <i>birds, leisure drones etc., are covered by dedicated process</i> Characterize induced damages (Analysis based on validated models, tests). Define criteria for damage detection (Visual check before flight, scheduled inspection, etc.). Identify and select worst cases damage scenarios combining importance of the damage and time up to detection. Demonstrate, based on the design, that the damage remains acceptable until next possible detection. This should be verified by analysis and/or test. Tests can be performed with artificial damages (debonding, composite warpage, resin poor areas, impacts) that cover above characterized damages. Success criteria can be: - verification of the residual strength on the tested part - fatigue residual life evaluation.	
	Material choice	Inappropriate use of service experience	The minimum required material properties need to be identified for most adverse conditions. Material should be qualified against foreseen environmental and most adverse conditions in single and combined stress.	
		Insufficient margins Incorrect identification of needed material properties	This can be done by experience, sizing and tests (e.g.: at coupon level). If substantiation relies on in service experience, it must be checked that experience is relevant for the new application.	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Manufacturing				
Manufacturing	Process definition	Inadequate process (which degrades material expected properties) Inappropriate surface treatment Incorrect polymerization process	Identification of key characteristics (e.g.: define the surface and heat treatment, surface finishing quality to reach expected key characteristics, etc.) Repeatability of a stable process by manufacturer, mitigation can involve quality in development of FAI (First Article Inspection) and TAI (Test Article Inspection). Control of the process changes. Identification of tests to be done before delivery, able to precipitate undetected flaws. Check/testing of correct material properties (refer to material choice) should be made with parts coming from a process representative of serial process. PFMEA.	
	Material supply	Raw material affected by defaults, leading to corrosion, poor stress/fatigue behavior, etc. Error in the raw material reference Incorrect storage	Use raw materials with Certificate of Conformity. Incoming material quality control with regards to required minimum material properties. Tests on batch samples.	
	Process implementation	Wrong process implementation Supplier variability out of expected range	Quality control of manufacturing process. Set the procedures, acceptance criteria regulating the manufacturing. Define and verify the FAI plan. First article inspection (dimensional inspection, treatments, processes, etc.). Individual/batch testing. PFMEA.	

	Calibration	Incorrect calibration	Calibration plan, test. Cross calibration checks.	
	Verification	Inadequate manufacturing control Inadequate inspection Inadequate testing	Acceptance tests (define the proper plan for ATP, stress screening, etc.). Identification of key characteristics with dedicated controls. PFMEA.	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Integration				
Integration	Fool proofing	Incorrect definition Incorrect implementation	- Parts shall be designed to avoid an incorrect assembly and installation. - Different P/Ns shall be not interchangeable. - Define & apply procedures to assemble/disassemble. - Define key characteristics of assemblies, and hence perform double inspections.	See Vibration line above
	Balancing	Incorrect balancing	Blades will be subjected to static and dynamic balance. Dynamic balancing could be avoided due to the high number of rotor.	

Errors check list			Possible Mitigations	Comments
Error Type	Error Sub Type	Detailed examples		
Maintenance				
Maintenance	Maintenance manual	Inappropriate interpretation of maintenance manual	Check through reviews, that the maintenance manual is non-ambiguous and complete. Check through test the maintenance procedure/criteria, etc., are feasible. Set the conditions for repairability or discard and replace with a new part (the latter seems more appropriate for propellers blade).	
	Skills	Poor qualification/lack of experience of maintainer	Qualification of the maintainer Training, organization of repair shop. - Design measures to avoid/minimize possible maintenance errors, - Verification of the maintenance operation by independent mean/staff. Minimize by design the degree of freedom for the maintainer.	
	Simultaneous repair of a complete set for one UAV		- Set discard time, not repair but replacement	