BRAZILIAN NATIONAL CIVIL AVIATION AGENCY (ANAC)

DEPARTMENT OF AIRWORTHINESS

SAFETY OBJECTIVES FOR POWERED-LIFT CERTIFICATION LEVEL 2

PROPOSED POLICY AND JUSTIFICATIONS

1 INTRODUCTION

Through this document, the Brazilian National Civil Aviation Agency (ANAC) makes available its proposed safety objectives for Powered-Lift Certification Level 2 aircraft and justifications.

2 BACKGROUND

2.1 Certification Levels

The concept of safety continuum provides a balanced approach between the risk and safety benefits for certification of civil aircraft depending on size, mission, capability, and other aspects. For powered-lift aircraft, ANAC proposes the Powered-Lift Certification Levels according to **Table 1**.

Table 1 - Powered-Lift Certification Levels

Maximum Passenger Seating Configuration and Maximum Gross Weight	**Powered-Lift Certification Level**
0-1 Passengers & ≤ 5,670 kg (12,500 lbs.)	1
2-6 Passengers & ≤ 5,670 kg (12,500 lbs.)	2
7-9 Passengers & ≤ 5,670 kg (12,500 lbs.)	3

These proposed certification levels are based on the airplane certification levels defined in requirement §23.2005 of RBAC 23 amdt. 64 (equivalent to FAA 14CFR §23.2005 amdt. 64, and EASA CS-23 amdt. 5), with the exception that ANAC is currently limiting the certification levels for powered-lift to a maximum gross weight of 5,670kg (12,500 lbs.) or less, which is compatible with the definition of small aircraft in accordance with RBAC 01. Significantly heavier powered-lift aircraft will require the evaluation of additional and specific characteristics than those currently taken into consideration by ANAC for existing powered-lift designs.

2.2 Safety Objectives

In carrying out a system safety assessment as required for the certification of civil aircraft, the applicant must show that there is a logical and acceptable inverse relationship between the average

probability and the severity of failure conditions. Safety objectives are then established at means of compliance level as part of the pass/fail criteria for successful compliance determination. In particular, the safety objectives provide the relationship between the aircraft certification level, the severity of its failure conditions, and the minimum required average probabilities and Functional Development Assurance Levels (FDALs).

Safety objectives for conventional aircraft such as airplanes and helicopters are defined in well-established and harmonized means of compliance that are issued (or recognized) by each certification authority. Powered-lift aircraft, on the other hand, are heavier-than-air aircraft capable of vertical takeoff, vertical landing, and low speed flight that depends principally on engine-driven lift devices or engine thrust for lift during these flight regimes and on nonrotating airfoil(s) for lift during horizontal flight.[1] An electric propulsion, vertical take-off and landing aircraft (eVTOL) is one type of powered-lift aircraft that typically integrates distributed electric propulsion and flight controls.

The design novelties and intended operation of these vehicles require a specific assessment for the establishment of applicable safety objectives. The safety objectives defined for conventional aircraft may not be directly appropriate for powered-lift designs. In this context, safety objectives for powered-lift aircraft have been defined by EASA[2] and proposed by the FAA[3], which are not fully harmonized.

2.3 Baseline Case: eVTOL Powered-Lift Certification Level 2

The ANAC has performed its assessment of safety objectives for powered-lift aircraft leveraging from existing guidance material related to the concept of safety continuum, dialogue with the industry and certification authorities, and considering key characteristics of these new designs and intended operation. These aspects were evaluated for a baseline case of an eVTOL with maximum seating configuration of 2-6 passengers (i.e. Powered-Lift Certification Level 2) operated for compensation or hire for urban air mobility. This baseline case includes most powered-lift aircraft currently under development, including the ones that ANAC received applications for certification and international validation.

3 TECHNICAL DISCUSSION

3.1 Introduction

The safety objectives are part of the means of compliance for system safety requirements identified in the certification basis of the design, in particular RBAC §23.2510 and its equivalent for powered-lift aircraft. They define quantitative and qualitative targets that are accepted as aids to engineering judgment in a system safety assessment.

These objectives are applicable to all the aircraft systems and their combinations. They establish minimum availability and integrity safety constraints that should be achieved at the aircraft, system and item levels. As such, the safety objectives are one of the key aspects for establishing the overall

[1] Ref.: FAA 14CFR §1.1.
[2] Ref.: EASA MOC SC VTOL Issue 2
[3] Ref.: Draft PS-AIR-21.17-03

level of safety of the design, along with other safety-related requirements included in the certification basis.

As explained in section 2, the safety objectives were assessed and are proposed for a baseline configuration of an eVTOL with maximum seating configuration of 2-6 passengers operated for compensation or hire for urban air mobility, considering the principles of the safety continuum. To facilitate reading and understanding, when referring to safety objectives throughout this document, sometimes only the levels required for "Extremely Improbable" / "Catastrophic" failure conditions will be mentioned, and the others are derived.

3.2 Comparative Evaluation

The baseline powered-lift configuration was first evaluated in comparison with published guidance material for aircraft with similar passenger capacity, payload, design weights, and operations. This assessment aimed at comparing existing guidance material for the application of the safety continuum concept to different types of vehicles, including conventional airplanes and helicopters, powered-lift aircraft including eVTOLs, and Remotely Piloted Aircraft System (RPAS). This comparative evaluation is presented in **Table 2**.

Table 2 - Comparable safety objectives for each Catastrophic failure condition

Standard	Type of Aircraft	Minimum Required Probability per FH	Development Assurance Level
FAA AC 23.1309-1E(1)	Conventional airplane	$<10^{-7}$ or $<10^{-8}$	DAL C or DAL B
FAA PS-ASW-27-15(2)	Conventional helicopter	$<10^{-7}$ or $<10^{-8}$	DAL C or DAL B
ASTM F3230-21a, F3061/F3061M-22b(3)	Conventional airplane	$<10^{-7}$	DAL C
Draft FAA PS-AIR-21.17-01(4)	Powered-lift	$<10^{-8}$	DAL B
EASA MOC SC VTOL Issue 2(5)	VTOL	$\leq 10^{-9}$	DAL A
JARUS AMC RPAS.1309(6)	RPAS	$<10^{-8}$ or $< 10^{-9}$	DAL B or DAL A

(1) Depending on MTOW higher or lower than 6,000 pounds.
(2) Depending on MTOW higher or lower than 4,000 pounds, $<10^{-9}$ and FDAL A if twin turbine or higher than 7,000 pounds.
(3) Assuming multi-engines propulsion.
(4) Assuming operation for compensation or hire.
(5) Assuming operation over congested areas.
(6) RPAS-23, depending on MTOW higher or lower than 6,000 pounds, $<10^{-7}$ and DAL B if RPAS-27.

3.3 Relationship between quantitative safety objectives and accident statistics

ANAC sought to make a parallel with the analyses to determine safety objectives presented in FAA AC 25.1309-1B[4] and AC 23.1309-1E[5]. These standards relate the safety objectives associated with each catastrophic failure condition to serious/fatal accident statistics of the aircraft by assuming a contribution of system-related design hazards and a given number of failure conditions in the design. A catastrophic failure condition is a failure condition that would result in multiple fatalities, usually with the loss of the aircraft. Examples are illustrated on the table below.

Table 3 - Relationship between accident rate and quantitative probability for each catastrophic failure condition

Source	Assumed probability of serious/fatal accident	Share of systems-related hazards	Assumed # of catastrophic failure conditions	Quantitative probability for catastrophic failure condition
Part 23 Class I	1×10^{-4} / FH	10%	10	1×10^{-6} / FH
Part 25	1×10^{-6} / FH	10%	100	1×10^{-9} / FH

As discussed in section 2.3 the baseline case concerns a powered-lift Certification Level 2 aircraft employed in passenger transportation for compensation or hire, which aligns with RBAC/Part 135 operations. ANAC evaluated statistical data available for fatal accidents related to RBAC/Part 135 operations in the accident databases of Brazil's CENIPA[6] (Data available from the last 10 years) and USA's NTSB[7] (Data from the last 20 years). When accounting for both airplane and helicopter operations under RBAC/Part 135, the Fatal Accident rate as per these databases is around 2-5 x 10^{-6} per flight hour. This represents average rates for different categories and classes of aircraft, not accounting for the number of fatalities involved in each accident. It is expected that the rate of accidents with multiple fatalities for small aircraft is higher in this range.

In assessing the causes and contributors, these data also validate the assumption in the existing guidance material that a relatively small portion of serious/fatal accidents are directly related to system-related failures as main contributors. This is valid for aircraft of different classes, capabilities and technologies, so the same assumption of 10% share of systems-related hazards in existing guidance material is used in this assessment. Since eVTOLs are more complex than similar capacity conventional airplanes and helicopters (see section 3.4.2), it is evaluated that powered-lift designs will certainly have more than 10 catastrophic failure conditions, but having likely less than 100 catastrophic failure conditions that are assumed for transport category airplanes in published guidance material.

Considering the above, assuming a fatal accident rate for a 2-6 maximum passenger aircraft on the order of 1 x 10^{-5} per flight hour, a 10% share of system-related contribution, and 100 catastrophic failure conditions for the vehicle, the acceptable quantitative probability per flight hour of each

[4] Ref.: FAA AC 25.1309-1B Appendix A

[5] Ref.: FAA AC 23.1309-1E Section 15

[6] CENIPA – Painel SIPAER, available at https://painelsipaer.cenipa.fab.mil.br/extensions/Sipaer/Sipaer.html

[7] NTSB – Statistical Reviews, available at https://www.ntsb.gov/safety/Pages/research.aspx

catastrophic failure condition for a Powered-Lift Certification Level 2 aircraft should be on the order of 1 x 10^{-8} per flight hour or less. The specific characteristics of an eVTOL type of powered-lift aircraft were evaluated against this proposed safety objective and is presented in the section 3.4.

3.4 Assessment of Specific eVTOL Characteristics

The following specific characteristics of eVTOL aircraft were considered and reviewed by ANAC for their potential impact on the proposed quantitative safety objective:

- Intended operation
- Integrated full fly-by-wire flight controls and distributed electric propulsion systems
- Indirect piloting and envelope protections
- Weight and dimensions
- Other specific design characteristics

3.4.1 Intended Operation

The baseline case considered in this assessment is of an eVTOL aircraft designed to perform urban air mobility operations for compensation or hire. ANAC evaluated the particulars of this type of operation, as well as consistency and level playing field with existing similar operation of conventional aircraft.

EASA established a differentiated category for VTOL that are operated as commercial passenger transport or over "congested areas". These Category “Enhanced” VTOL have more stringent safety objectives aligned with Transport Category airplanes and helicopters. This seems consistent with European regulations that limit commercial air transport operation of helicopters over congested hostile environments (such as urban areas) to multi-engine rotorcraft certificated as Category A[8] under CS-27 Class IV or CS-29, with few exceptions. Similar operational restrictions are not adopted in Brazil and in the United States, both having intense operations of single engine helicopters over urban environments with acceptable level of safety.

The FAA, on the other hand, proposed through Draft Policy PS-AIR-21.17-01[9] a reduction in the safety objectives for the case of private operations (no compensation or hire). ANAC’s assessment was performed for a baseline case involving RBAC/Part 135 operations, which are the main intended operation for eVTOL aircraft currently under development. Although the safety objectives could be adjusted for private operations, the ANAC has no data at this moment to validate a reduction by one order of magnitude. In addition, since safety objectives are safety constraints that drive the design at the aircraft level, such a distinction would only have practical applicability for powered-lift designs that are specific or customized to private operations.

Finally, considering the baseline scenario of operations over congested (densely populated) areas, there is a potential concern for increased threat to people on the ground. This aspect is evaluated in more detail in section 3.4.4.

---

[8] Ref.: COMMISSION REGULATION (EU) No 965/2012 of 5 October 2012, CAT.POL.H.100 and CAT.POL.H.200 regulations.

[9] At the time of this evaluation, the FAA did not publish the final version of Policy PS-AIR-21.17-01 so these considerations are subject to change.

Since the proposed minimum probability objectives for powered-lift Certification Level 2 are consistent with, or exceeds, those applicable to conventional aircraft that perform similar operations in the Brazilian and US operational environment, the proposed safety objectives are consistent with the intended scenario of operation with passengers for compensation or hire over urban areas.

3.4.2 Integrated full fly-by-wire flight controls and distributed electric propulsion systems

The use of full fly-by-wire flight controls integrated with propulsion system increases the complexity of the design. Increase in complexity must be evaluated for the definition of safety objectives. Existing (published) safety continuums are primarily intended for small conventional aircraft with simple systems, based on historical data of accidents pertinent to these aircraft. A new type of aircraft that fully integrates flight controls and distributed electric propulsion within a full authority fly-by-wire control system was not envisioned in these guidance materials. For example:

> *"Generally, the classes deal with airplanes of historical equivalent levels of system complexity, type of use, system reliability, and historical divisions of airplanes according to these characteristics. However, these classes could change because of new technologies. […] For example, airplanes with considerably more than 10 catastrophic failure conditions, that have greater performance characteristics and incorporate many complex systems and advanced technologies may have lower probability values and higher DALs."* [FAA AC 23.1309-1E, §15.e-f]

As far as probability is concerned, the higher system complexity would lead to potentially higher number of failure conditions and their combinations. This effect was already considered in the initial definition of the quantitative safety objects presented in section 3.3 by conservatively assuming the presence of 100 potential catastrophic failure conditions. As a result, the proposed safety objective of 1×10^{-8} per flight hour for powered-lift Certification Level 2 aircraft is one order of magnitude lower (i.e. more restrictive) than 1×10^{-7} per flight hour that would be required for conventional aircraft of similar passenger capacity. The effects of such complexity increase in the Development Assurance Level (DAL) aspects of the safety objectives are detailed in section 3.5.

3.4.3 Indirect piloting and envelope protections

Intrinsically related to the use of fly-by-wire technology, several eVTOL designs use the "indirect piloting" concept, while also providing different levels of flight envelope protections. Indirect piloting in this context means that the pilot no longer acts directly on the control surfaces as in a conventional airplane, but aircraft systems convert pilot intention into direct action at the controls, including thrust changes, flight control surfaces, and flight mode transitions. This puts greater reliance on the availability and integrity of aircraft systems, while aiming at improving the safety of flight by the reduction of pilot workload and providing additional safety features such as flight envelope protections.

These design features were evaluated as such:

- In normal operating conditions, it is considered that automatism and flight envelope protections will lead to benefits to safety.
- In case of system failures, the automations and flight envelope protections are expected to minimize transients, accommodate failures automatically, and reduce pilot workload, thus also improving safety.

- In some extreme cases, the absence of direct commands may limit pilot authority to control the aircraft in such situations. These rare cases would likely require the use of exceptional pilot skills, and the limitations thereof are accounted for in the safety assessment process (usually by assuming such failure conditions as Catastrophic).

The use of indirect piloting and flight envelope protections is then expected to lead to a positive net safety benefit for the fleet operation. Statistical data on accidents corroborate this conclusion, since as outlined in section 3.3, accidents related to human factors such as piloting errors and judgment, as well as operational and environmental issues, predominate over the contribution related to system failures. Through increased flight envelope protections and reduction of pilot workload, these safety enhancing features should be most beneficial for minimizing these main accident contributors. Thus, this characteristic should not require additional changes in the proposed quantitative safety objectives. This evaluation depends on these safety enhancing features being properly developed (requirements, design, and implementation). This aspect is connected to the Development Assurance Level aspects of safety objectives, which are further detailed in section 3.5.

3.4.4 Weight and dimensions

Powered-lift aircraft, and eVTOLs in particular, are significantly heavier and larger than conventional helicopters and airplanes with similar passenger and payload capacity. These characteristics were then assessed for their potential impact on the proposed safety objectives.

Weight has been historically used to characterize a certain size or class of aircraft to determine applicable requirements. In this context, weight could be seen as a "proxy" for a set of characteristics – such as performance and complexity – that is attributed to different aircraft and for which a corresponding level of safety is required. However, the aim of this topic is to evaluate the direct effects of significantly heavier design weights that are typical of an eVTOL aircraft.

Specific requirements such as flight performance and crashworthiness ensure the safety of the aircraft and its occupants, already considering the design weights. Therefore, an adverse effect on safety is not expected for people onboard. On the other hand, a significantly heavier aircraft may have an adverse effect on the safety of people on the ground, as the protection offered by shelters such as buildings and residences would be more susceptible to damage by heavier aircraft. During takeoff and landing, the eVTOL impact energy is expected to be lower than that of a conventional airplane (due to lower operating speeds), but higher than that of a conventional helicopter (due to higher mass).

eVTOLs are also up to 50% larger than conventional airplanes (by wingspan) and helicopters (by main rotor diameter) of similar passenger and payload capacity. Aircraft size is an important parameter for assessing the ground risk as a threat for people external to the aircraft[10], as it increases the probability of impacting people on the ground.

Accident data statistics outlined in section 3.3 show that the number of fatalities on the ground for accidents involving conventional aircraft, considering general aviation and RBAC/Part 135 operations in the last 20 years, represents a small fraction (approximately 2%) of the total number of

[10] E.g. JARUS SORA 2.5 RPAS methodology

fatalities relative to those on board. This includes occurrences over different population densities and involving aircraft of different sizes and capacities, many of them larger and heavier than a powered-lift Certification Level 2 aircraft.

One of the factors that can contribute to the reduced number of casualties on the ground is the pilot's ability to direct the aircraft to a more favorable area (e.g. by gliding or autorotation). This capability is more limited on a powered-lift aircraft; however, specific requirements and demonstrations for controlled emergency landing and continued safe flight and landing applicable to powered-lift aircraft ensure an equivalent level of safety.

As a result of this evaluation, ANAC considers that, although there may be an increased ground risk due to the heavier weight and larger dimensions of eVTOL aircraft, considering data available for ground risk relative to onboard fatalities and the compensating factors that are specific to powered-lift aircraft, this factor alone would not justify an increase of one order of magnitude in the proposed safety objectives.

3.4.5 Other specific design characteristics

The safety objectives are applied in addition to other requirements in the certification basis and associated means of compliance, which together comprise the overall level of safety of the aircraft (see section 3.1). The specific design characteristics of eVTOLs listed below were also assessed by ANAC as having additional potential for affecting the definition of safety targets:

- Flight dynamics related to distributed electric propulsion and control.
- Combination of thrust-borne, wing-borne, and semi-thrust-borne sources of lift and flight transitions.
- Large high-capacity and energy-dense batteries as the main source of energy, including potential for thermal runaway.

These characteristics were considered either covered by the previous evaluations, or covered by specific requirements in the certification basis, including the need for specific analysis, laboratory, ground, and flight test demonstrations. Therefore, no change in the proposed safety objectives was deemed necessary for these characteristics.

3.5 Development Assurance Considerations

As discussed in section 3.4.2, eVTOLs are new and complex technology. The possibility of development errors exists either due to increasing complexity or due to the novelty aspects of the technology, its operation and environment. Increased reliance on digital systems for safety-critical functions that were once performed by conventional and fully analyzable components on comparable conventional aircraft would mean that such development errors could have more significant effects on safety if they cause failures in service. In addition, the safety enhancing features discussed in section 3.4.3 are valid only if they are properly developed (requirements, design, and implementation).

Development assurance provides a level of confidence that the system and items development have been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact safety. Development assurance is therefore required for powered-lift at aircraft,

system and item levels. SAE ARP4754B is one example of standard for aircraft and system level development assurance, while RTCA DO-178C and DO-254 provide standards for development assurance at item level for Software and Airborne Electronic Hardware (AEH) respectively.

Based on the concerns of development errors and their potential effects on safety, ANAC performed an assessment to define the Development Assurance Level (DAL) to be required for each Catastrophic failure condition of the baseline configuration (Powered-lift Certification Level 2). A comparison of different assurance objectives is summarized below:

- Aircraft and System Level (SAE ARP4754B):
    - The difference between FDAL A and FDAL B is on the need of employing process independence for FDAL A when performing verification.
- Item Level – Software (RTCA DO-178C):
    - IDAL A requires MC/DC (modified condition/decision coverage) structural coverage analysis, and Object Code traceability in addition to IDAL B.
    - IDAL A requires more verification objectives with independence than IDAL B does.
    - There are additional differences in objectives related to tool qualification, if used.
- Item Level – AEH (RTCA DO-254):
    - There is essentially no difference in assurance objectives between IDAL A and B.

MC/DC increases confidence that the functional requirements have been correctly implemented and that unintended functions have been reduced to an acceptable level, while Object Code traceability confirms that no unverified compiler-generated code is used. Employing independence at multiple levels is a fundamental aspect in existing guidance material for minimizing development errors. In fact, the use of independent checks is a common practice in aviation for catching potential mistakes, not only limited to development errors. Greater independence enhances error detection.

FDAL/IDAL A thus provides considerable safety benefits for minimizing the likelihood of development errors compared with FDAL/IDAL B, especially in the context of a completely new product with increased level of integration and novelty. However, in applying the safety continuum concept, the safety benefits must be balanced with the associated risk. One aspect of such evaluation is balancing effort and cost associated with compliance so that they do not inhibit the introduction of safety enhancing technologies in lower risk aircraft.

Increased use of independence may lead to additional effort and cost to the applicant. While true to some extent, ANAC considers that this occurs in the context of the development of a highly complex vehicle which, by its own complex nature, already requires substantial manpower and knowledge to develop. In this context, and considering the existing guidance material for process independence, this is expected to be accomplished within an existing team that is already commensurate with the level of effort required for developing such a complex vehicle. Costs associated with “DAL A compliance” have been estimated to be around 5 to 10% higher when compared with DAL B. In addition, the most significant increase in effort (and therefore costs) occurs when stepping up compliance to DAL B from DAL C.

The ANAC considers that the safety objective of FDAL/IDAL A for each Catastrophic failure condition provides justifiable safety benefits when compared to the potential increase in effort and cost, given the complexity of the product and its development.

4 CONCLUSION: PROPOSED SAFETY OBJECTIVES FOR POWERED-LIFT CERTIFICATION LEVEL 2

The **Table 4** provides proposed quantitative probabilities and FDALs as safety objectives for each failure condition classification for a powered-lift Certification Level 2 aircraft.

Table 4 - Relationship among severity of failure conditions, probabilities, and development assurance levels for powered-lift Certification Level 2 aircraft

Failure Condition Classification	**No Effect**	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Effect on aircraft	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Loss of aircraft
Effect on flight crew	No effect on flight crew	Slight increase in workload that involves crew actions well within crew capabilities such as routine flight plan changes	Physical discomfort or a significant increase in workload or in conditions impairing crew efficiency	Physical distress or excessive workload impairs ability to perform tasks accurately or completely	Fatalities or incapacitation
Effect on occupants excluding flight crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious injuries or a fatal injury to a single passenger or cabin crew member	Multiple Fatalities
Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Powered-Lift Certification Level 2	No probability or FDAL requirement	$<10^{-3}$ FDAL D	$<10^{-5}$ FDAL C	$<10^{-7}$ FDAL B	$<10^{-8}$ FDAL A

Note: Numerical values indicate an order of probability per flight hour of failure range and are provided here as a reference. FDAL and IDAL assignment methodology should follow a consistent top-down approach methodology (e.g. ARP4754B, §5.2). A qualitative analysis is acceptable to justify minor failure conditions.