

DRAFT



Australian Government
Civil Aviation Safety Authority

ANNEX A TO AC 101-06 V1.0

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

April 2026

DRAFT

Contents

1	Introduction	4
2	OSO #04 – UAS components essential to safe operations are designed to an airworthiness design standard (ADS)	5
2.1	General	5
2.2	Level of robustness	5
2.3	Level of integrity	5
2.4	Level of assurance	6
2.5	Means of compliance	6
2.6	Additional guidance	7
3	OSO #05 – RPAS is designed considering system safety and reliability	13
3.1	General	13
3.2	Level of robustness	13
3.3	Level of integrity	13
3.4	Level of assurance	14
3.5	Means of compliance	15
3.6	Additional guidance	15
4	OSO #24 – UAS designed and qualified for adverse environmental conditions	23
4.1	General	23
4.2	Level of robustness	23
4.3	Level of integrity	23
4.4	Level of assurance	24
4.5	Means of compliance	24
4.6	Additional guidance	24
Appendix A	OSO #05 – Compliance	29
Appendix B	OSO #24 – Compliance	37



Acknowledgement of Country

The Civil Aviation Safety Authority (CASA) respectfully acknowledges the Traditional Custodians of the lands on which our offices are located and their continuing connection to land, water and community, and pays respect to Elders past, present and emerging.

Artwork: James Baban.

1 Introduction

- 1.1 This Annex to AC 101-06 v1.0 - Australian Specific Operational Risk Assessment (AusSORA) provides guidance on the means of compliance with the airworthiness-criteria for manufacturers and designers.
- 1.2 Australian specific operation risk assessment (AusSORA) is a risk assessment process for drone operators to assess and mitigate risks for complex RPAS operations. It is tailored from JARUS SORA 2.5 according to Australian operational and regulatory context.
- 1.3 As part of the AusSORA approval process, operators must comply with the operational safety objectives (OSO) for their intended specific assurance and integrity level (SAIL) of the operation.
- 1.4 Some of these requirements are related to the airworthiness aspects of the RPAS and should be supported by manufacturers and designers.
- 1.5 In the following sections, criteria for each OSO corresponding to different SAIL are explained as follows:
- **Level of robustness** is the combined measure of a risk mitigation or operational safety objective's effectiveness and reliability. It helps determine the minimum requirements for integrity and assurance levels.
 - **Level of integrity** describes the effectiveness of a risk mitigation or safety objective in achieving its intended risk reduction or control outcome.
 - **Level of assurance** is the degree of confidence that the specified level of integrity is achieved and maintained.
 - **Means of compliance** are the methods, processes, or evidence used to demonstrate that a requirement, standard, or objective has been satisfied.
 - Further guidance on the criteria and the means of compliance.

2 OSO #04 – UAS components essential to safe operations are designed to an airworthiness design standard (ADS)

2.1 General

- 2.1.1 The intent of OSO #4 is to ensure that RPAS and its components have been designed to contribute to the required target level of safety (TLOS) through compliance with appropriate airworthiness design standards (ADS).
- 2.1.2 OSO #4 ensures that the RPAS has been designed to meet the requirements of appropriate ADS, with a particular emphasis on the structural integrity, flight characteristics, system functionality and operational factors.

2.2 Level of robustness

- 2.2.1 The required level of robustness for OSO #04 is specified in Table 1 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 1: OSO #04 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	O	O	O	L	M	H

2.3 Level of integrity

- 2.3.1 The level of integrity must not be less than the required level of robustness. Table 2 provides the criteria for different integrity levels for OSO #04.

Table 2: OSO #04 Level of integrity

Level of integrity	Criterion
Low	The UAS components essential to safe operations are designed to an ADS considered adequate by CASA and in accordance with a means of compliance acceptable to CASA to contribute to the overall safety objective of 10^{-4} per flight hours (FH) for the loss of control of the operation.
Medium	The UAS components essential to safe operations are designed to an ADS considered adequate by CASA and in accordance with a means of compliance acceptable to CASA to contribute to the overall safety objective of 10^{-5} /FH for the loss of control of the operation.
High	The UAS components essential to safe operations are designed to an ADS considered adequate by CASA and in accordance with a means of compliance acceptable to CASA to contribute to the overall safety objective of 10^{-6} /FH for the loss of control of the operation.

2.4 Level of assurance

2.4.1 The level of assurance must not be less than the required level of robustness. Table 3 presents the criteria for the different assurance levels for OSO #04.

Table 3: OSO #04 Level of assurance

Level of assurance	Criterion
Low	The applicant declares that the required level of integrity has been achieved.
Medium	The applicant has supporting evidence that the required level of integrity is achieved. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience.
High	CASA validates the claimed level of integrity.

2.5 Means of compliance

2.5.1 Table 4 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #04.

Table 4: OSO #04 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	<ol style="list-style-type: none"> The RPAS has been designed and developed in accordance with a CASA - accepted compliance basis derived from an ADS identified by CASA and tailored to the specific operational conditions. The applicant submits the established compliance summary along with a declaration of compliance demonstrating low-level robustness. The applicant must demonstrate that the design is appropriate for a TLOS of 10^{-4}/FH for a SAIL IV operation. The applicant must conduct function and reliability flight tests according to a CASA-agreed test plan. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA. CASA may request the applicant to provide supporting evidence for assessment.
Medium	<ol style="list-style-type: none"> The RPAS has been designed and developed in accordance with a d CASA accepted compliance basis derived from and ADS identified by CASA and tailored to the specific operation conditions. The applicant submits the established compliance summary along with a declaration of compliance demonstrating medium-level robustness. The design is appropriate for a TLOS of 10^{-5}/FH for a SAIL V operation. The applicant must conduct function and reliability flight tests according to a CASA-agreed test plan. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA. CASA conducts an assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

Level of robustness	Evidence requirement and assessment process
High	<ul style="list-style-type: none"> a. The RPAS has been designed and developed in accordance with a CASA - accepted compliance basis derived from the ADS identified by CASA and tailored to the specific operational conditions. b. The applicant submits the established compliance summary along with a declaration of compliance demonstrating high-level robustness. c. The design is appropriate for a TLOS of 10⁻⁶/FH for a SAIL VI operation. d. The applicant must conduct function and reliability flight tests according to a CASA-agreed test plan. e. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA. CASA conducts a comprehensive assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

2.6 Additional guidance

2.6.1 Airworthiness design standards

- 2.6.1.1 Airworthiness design standards are a set of regulatory and technical requirements that define the minimum safety and design criteria that an aircraft, or a critical component of an aircraft, must meet to be considered safe for the intended flight operation.
- 2.6.1.2 Within the SORA framework, starting at SAIL IV, it is recognised that the safety objectives associated with an operation cannot be achieved unless the components of the aircraft that are essential to safe operations are designed in accordance with an ADS.
- 2.6.1.3 An adequate ADS must comprehensively define the technical requirements to ensure the safety and required performance of the intended operation. This includes, but is not limited to:
- **Structural integrity:** Requirements for the design and durability of the RPAS airframe and payload structures to withstand all expected operational loads.
 - **Flight characteristics and performance:** Standards ensuring the RPAS remains stable, predictable, and controllable during all flight phases, whether manually controlled or automated.
 - **Propulsion systems:** Requirements for the reliability, efficiency, and safety of the propulsion system(s), including tolerance to adverse environmental factors.
 - **System functionality:** Requirements to ensure that all airborne and ground-based systems operate reliably, securely, and predictably to support safe RPAS operation under all anticipated conditions. These systems must be designed to maintain control of the aircraft and prevent hazardous situations in the event of a failure or a degradation in performance.
 - **Safety and emergency provisions:** Requirements for risk mitigation features to protect people, property, and other airspace users in the event of abnormal or failure conditions. Examples of these features are the integration of geofencing systems, parachute recovery systems (PRS), or flight termination systems (FTS).
- 2.6.1.4 Examples of ADS that have been identified by CASA as being potentially suitable for establishing a compliance basis include the following:
- EASA Special Condition Light-UAS (EASA SC-LUAS)
 - ASTM F2910-22 Standard Specification for Design and Construction of a Small Unmanned Aircraft System (sUAS)

- ASTM F3298-24 Standard Specification for Design, Construction, and Verification of Lightweight Unmanned Aircraft Systems
- ASTM F3563-22 Standard Specification for Design and Construction of Large Fixed Wing Unmanned Aircraft Systems
- JARUS Certification Specification for Light Unmanned Aeroplane Systems (JARUS CS-LUAS)
- JARUS Certification Specification for Light Unmanned Rotorcraft Systems (JARUS CS-LURS)
- NATO STANAG 4671 - Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR)
- NATO STANAG 4703 - Light Unmanned Aircraft Systems Airworthiness Requirements.

- 2.6.1.5 CASA recognises that not all ADS are intended to achieve the same level of rigour. Consequently, an ADS that may be appropriate for an RPAS at a lower robustness may not be appropriate for the same RPAS at higher robustness. The applicant should determine the most appropriate ADS for their intended level of robustness. Applicants may also seek to tailor the applicable requirements contained in the ADS for the relevant systems fitted to the RPAS and for its intended operations.
- 2.6.1.6 Established ADS for conventional type-certificated aircraft, such as Part 23 and Part 27 of CASR¹, may be applied when developing a compliance basis for an RPAS, provided that the requirements are appropriately tailored and augmented to address RPAS-specific considerations. Similarly, for related RPAS components such as engines or propellers, established ADS such as Part 33 and Part 35 of CASR, or other ADS such as special conditions published by national aviation authorities (NAAs) such as EASA or FAA, may be applied when developing a compliance basis. In some cases, the development of compliance basis elements for unique or unusual aspects of an RPAS design may occur without reference to published ADS.
- 2.6.1.7 CASA may accept an ADS proposed by an applicant other than listed in Paragraph 2.6.1.4 of this Annex. Applicants wishing to propose an alternate ADS for their compliance basis should contact CASA to discuss the appropriateness of the proposed ADS.
- 2.6.1.8 In all cases, and particularly for operations at higher SAIL, CASA recommends early engagement by the applicant to determine the acceptability of the proposed ADS for the specific RPAS and intended operation if proposing a design standard which is not already identified by CASA as being acceptable for the required level of assurance.

2.6.2 Applicability and relationship to other OSO

- 2.6.2.1 OSO #04 is not intended to duplicate requirements that are already addressed by other OSOs, including the following:
- OSO #05 (system safety and reliability)
 - OSO #06 (C3 link characteristics)
 - OSO #18 (flight envelope protection)
 - OSO #19 (safe recovery from human error)
 - OSO #20 (HMI)
 - OSO #24 (environmental factors).

¹ Part 23 of CASR incorporates by reference EASA CS-VLA, EASA CS-23 and FAA 14 CFR Part 23; Part 27 of CASR incorporates by reference EASA CS-27 and FAA 14 CFR Part 27.

- 2.6.2.2 When another OSO covers any aspect of the ADS, the requirement of that OSO takes precedence over the ADS requirement.
- 2.6.2.3 The requirements defined in the ADS may support compliance with these OSOs. In such cases, the applicant may cross-reference the related requirements between OSOs and provide evidence demonstrating how the RPAS design meets these requirements and shows compliance with the relevant OSOs.
- 2.6.2.4 Applicability of requirements in an ADS would, generally, be determined by the design configuration and the operational use. For example, stall speed measurement requirements would only be applicable to a fixed wing aircraft and continuous icing requirements would only be applicable if flight into known icing was permitted. Appropriateness of requirements in the ADS can be based on the SAIL of the operation. For example, the quantitative requirements in an ADS that addresses system safety analysis may not be appropriate at lower SAILS. Where an aircraft designer has determined that a requirement in the ADS is not applicable, this should be clearly documented and justified by an appropriate technical rationale.

2.6.3 Compliance basis

- 2.6.3.1 A compliance basis is the set of airworthiness requirements that apply to a specific RPAS design, ensuring it is designed and built to achieve the required TLOS for the intended operation.
- 2.6.3.2 Compliance basis can be the same as one of the potentially identified ADS, or it can be tailored from one or more identified ADS, for specific operational conditions and safety objectives.
- 2.6.3.3 The compliance basis must cover components essential to safe operations whose failure would significantly impair the capability of the operator to meet the requested target level of safety in terms of loss of control of the operation.
- 2.6.3.4 Any tailoring to an ADS should be clearly documented and justified by an appropriate technical rationale and be accepted by CASA.

2.6.4 Compliance summary

- 2.6.4.1 Applicants should prepare a compliance summary that declares whether the RPAS satisfies each requirement of the compliance basis and that identifies the verification methods that have been employed to substantiate this compliance.
- 2.6.4.2 [AC 21-13 - Australian designed aircraft – type certification](#) provides guidance on the preparation of a compliance summary. Based on this guidance, a suitable structure for a compliance summary would contain the following information for each requirement of the compliance basis:
- a. Column 1 – Requirement
 - b. Column 2 – Compliance declaration:
 - i. C – Complies
 - ii. N/C – Does not comply
 - iii. N/A – Not applicable (as agreed with CASA)
 - iv. O – Open issue
 - c. Column 3 – Method of compliance e.g. calculations/analysis; lab/rig test; ground test; flight test; design drawing etc. A suggested code is:
 - i. A – Analysis
 - ii. T – Test
 - iii. I – Inspection
 - iv. D – inherent in the Design

- v. E/S – Equivalent Safety
 - vi. O/E – based on satisfactory Operational Experience (e.g. for a class of material or a technique)
 - vii. S – Simulation
- d. Column 4 – References (to supporting information, by document identifier and title)
- e. Column 5 – Remarks
- 2.6.4.3 If the compliance statement for an item is a 'N/C' or 'O', the remarks column should include a statement on the action being taken. For example, development of an Issue Paper, preparation of an equivalent safety submission, preparation of modifications. The final issue of the Compliance Summary² should contain no 'open' items.
- 2.6.4.4 At SAIL IV, low level of robustness, applicants typically are not required to populate Column 4 or provide supporting documents, unless specifically requested by CASA.
- 2.6.4.5 Column 3 provides a range of verification methods that are acceptable when declaring compliance to ADS requirements. If the wording of a specific requirement does not identify a particular verification method, such as by test or inspection, a designer is free to decide which verification method to use when demonstrating compliance with the requirement.
- 2.6.4.6 Column 5 provides for the designer to provide appropriate remarks, such as the technical rationale or justification, to support the declaration of compliance in Column 2.
- 2.6.4.7 Table 5 provides guidance on the methods of compliance that can be used.

Table 5: Methods of compliance

Method	Explanation	Examples
Analysis	<p>It involves the use of qualitative analysis, engineering calculations, computer models, and mathematical techniques to predict how a component, system, or structure will behave under operational and worst-case conditions.</p> <p>It is used in the design phase to predict structural, aerodynamic, or system performance without requiring physical prototypes.</p>	<ul style="list-style-type: none"> • Finite Element Analysis (FEA) to verify the airframe can withstand operational loads. • Flight path modelling for BVLOS (Beyond Visual Line of Sight) operations. • Electrical load analysis (ELA) Thermal analysis for lithium-ion battery safety.
Test	<p>It is a physical evaluation of a product, system, or component under controlled conditions to verify it meets performance requirements.</p> <p>It is used to prove compliance conclusively by showing that the real-world behaviour matches the expectation.</p>	<ul style="list-style-type: none"> • Flight tests to verify stability and control. • Battery endurance and environmental testing. • Fail-safe testing for GPS loss or communication link dropouts. • Iron-bird testing of flight control system and actuators.
Inspection	<p>Inspection is the visual, dimensional, or non-destructive examination of aircraft parts and assemblies.</p>	<ul style="list-style-type: none"> • Verifying the correct assembly of electrical wiring. • Visual inspection of rotor blades for cracks or delamination.

² The Compliance Summary is a 'living' document, continuously amended throughout the duration of the program, and serves as the master reference for all activities aimed toward compliance.

Method	Explanation	Examples
		<ul style="list-style-type: none"> • Visual inspection of free movement of control surfaces without binding or jamming.
Inherent in Design	Compliance is achieved through fundamental design features, eliminating the need for complex analysis or testing.	<ul style="list-style-type: none"> • Use of nyloc nuts to prevent loosening under vibration • Use of modular redundancy for flight-critical systems • Use of keyed components to prevent errors during assembly
Equivalent Safety	It achieves the same level of safety through an alternative method to the exact prescribed requirement in a standard.	<ul style="list-style-type: none"> • Use of a PRS as an equivalent safety to meet a spin recovery requirement of an ADS.
Operational experience	Leverages real-world data from fielded drones to demonstrate reliability and safety.	<ul style="list-style-type: none"> • Demonstrating safe operation based on sufficient flight hours in operational conditions applicable to the intended operation. • A component has been used on another fleet for sufficient flight hours without failure, so it may not need additional testing.
Simulation	<p>Used to validate operational suitability in safe, simulated environments.</p> <p>Compliance is shown through simulated operation in a controlled environment, usually for human factors or testing of scenarios too risky to perform in real flight. Any simulations used for verification must be validated.</p>	<ul style="list-style-type: none"> • Virtual testing of detect-and-avoid algorithms using digital twins. • Demonstrating swarm coordination in a simulator before real flight testing.

2.6.5 Experimental flight tests

- 2.6.5.1 Experimental flight tests for research and development (R&D) purposes can facilitate initial operations to support the development of the RPA design. These operations, when combined with analysis and simulations, enable manufacturers to incrementally test systems and improve designs.
- 2.6.5.2 R&D flight tests will also allow experimental flight tests for compliance purposes or function and reliability test purposes to be performed. CASA may request these tests to be performed with a conformed test article, suitably calibrated equipment, and potentially witnessed by CASA.
- 2.6.5.3 CASA [AC 21-43 - Experimental Certificates for Unmanned Aircraft](#) and [AC 21-10 - Experimental certificates](#) provide further details on experimental flight tests for aircraft including RPAS.
- 2.6.5.4 CASA [AC 21-47 - Flight test safety](#) covers topics such as test planning principles, hazard analysis and risk management.

2.6.6 Function and reliability flight test program

- 2.6.6.1 CASA requires RPAS manufacturers to demonstrate function and reliability for the intended purposes through an appropriate program of flight testing.

- 2.6.6.2 Function and reliability flight tests must be conducted for the number of hours agreed with CASA under a flight test plan to specific RPAS make, model and configuration.
- 2.6.6.3 The flight test plan must be proportionate to the SAIL level and the intended operational purposes. CASA will agree to a flight test plan only where the proposed test points, conditions, and number of flight-test hours are demonstrably scaled to these factors and are adequate to achieve the required objectives.
- 2.6.6.4 Testing must be completed without experiencing any failure that could result in loss of flight, loss of control, or an unplanned landing.
- 2.6.6.5 Prior to the function and reliability testing, designers must perform experimental flight tests to show compliance with the requirements if it is stated as a method of compliance in the compliance summary.

3 OSO #05 – RPAS is designed considering system safety and reliability

3.1 General

- 3.1.1 The intent of OSO #05 is to ensure that the aircraft and its systems have been designed with potential risks in mind, that adequate mitigations for those risks have been appropriately considered and implemented, and that the aircraft can be reasonably expected to be safe for its intended operation.
- 3.1.2 To declare compliance to OSO #05 at SAIL III and above, applicants should be able to demonstrate that they have:
- assessed the aircraft, its systems and components
 - considered all operational phases and conditions
 - identified all hazards that may arise from probable failures of the RPAS or any external systems that support its operation
 - minimised these hazards to an acceptable level for the intended operation.

3.2 Level of robustness

- 3.2.1 The required level of robustness for OSO #05 is specified in Table 6 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 6: OSO #05 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	H	H

3.3 Level of integrity

- 3.3.1 The level of integrity must not be less than the required level of robustness. Table 7 provides the criteria for different integrity levels for OSO #05.

Table 7: OSO #05 Level of integrity

Level of integrity	Criterion
Low	The equipment, systems, and installations are designed to minimise hazards to an acceptable level in the event of a probable failure of the RPAS or of any external system supporting the operation.
Medium	The equipment, systems, and installations are designed to minimise hazards to an acceptable level in the event of a probable failure of the RPAS or of any external system supporting the operation.

Level of integrity	Criterion
	Software (SW) and Complex Electronic Hardware (CEH) whose development error(s) may cause or contribute to catastrophic failure conditions are developed in accordance with means of compliance acceptable to CASA.
High	<p>The equipment, systems, and installations are designed to minimise hazards to an acceptable level in the event of a probable failure of the RPAS or of any external system supporting the operation.</p> <p>SW and CEH whose development error(s) may cause or contribute to hazardous or catastrophic failure conditions are developed in accordance with means of compliance acceptable to CASA.</p> <p>No single failure can lead to a catastrophic failure condition.</p>

3.4 Level of assurance

3.4.1 The level of assurance must not be less than the required level of robustness. Table 8 presents the criteria for the different assurance levels for OSO #05.

Table 8: OSO #05 Level of assurance

Level of assurance	Criterion
Low	A Functional Hazard Assessment (FHA) and supporting design and installation appraisals (DIA) that show hazards are minimised to an acceptable level are available.
Medium	<p>A Functional Hazard Assessment (FHA), design and installation appraisals (DIA) and supporting system safety assessments (SSA) that show hazards are minimised to an acceptable level are available.</p> <p>System safety assessments are conducted in accordance with means of compliance acceptable to CASA.</p> <p>Appropriate development assurance activities are performed for critical functions implemented by SW or CEH to ensure safety objectives are met.</p>
High	<p>A Functional Hazard Assessment (FHA), design and installation appraisals (DIA) and supporting system safety assessments (SSA) that show hazards are minimised to an acceptable level are available.</p> <p>System safety assessments are conducted in accordance with means of compliance acceptable to CASA.</p> <p>Appropriate development assurance activities are performed for critical functions implemented by SW or CEH to ensure safety objectives are met.</p> <p>Supporting safety assessment and development assurance activities are validated by CASA.</p>

3.5 Means of compliance

3.5.1 Table 9 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #05.

Table 9: OSO #05 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	<ul style="list-style-type: none"> a. FHA and DIA are available for review. b. The applicant follows an appropriate system safety assessment methodology acceptable to CASA, such as <ul style="list-style-type: none"> i SAE ARP 4761 ii EUROCAE ED-280. c. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA on the basis of FHA and design and installation appraisals conducted. CASA may request the applicant to provide supporting evidence for assessment.
Medium	<ul style="list-style-type: none"> a. FHA, DIAs, and supporting analyses are available for review. b. The applicant follows an appropriate system safety assessment methodology acceptable to CASA, such as <ul style="list-style-type: none"> i SAE ARP 4761 ii EUROCAE ED-280. c. Assurance evidence for SW and CEH is available for review. d. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA on the basis of FHA, design and installation appraisals, supporting analyses and assurance evidence for SW and CEH. CASA conducts an assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.
High	<ul style="list-style-type: none"> a. FHA, DIAs, and supporting analyses are available for review. b. The applicant follows an appropriate system safety assessment methodology acceptable to CASA, such as SAE ARP 4761. c. Assurance evidence for SW and CEH is available for review. d. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA on the basis of FHA, design and installation appraisals, supporting analyses and assurance evidence for SW and CEH. CASA conducts a comprehensive assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

3.6 Additional guidance

3.6.1 Applicability and relationship to other OSOs

3.6.1.1 OSO #05 is applicable to all aircraft systems that are required to function correctly to ensure the safe operation of the aircraft, including the flight control system, navigational system, propulsion system, fuel/energy storage and management systems, C2/C3 link systems, the remote pilot

station (RPS) / ground control station (GCS), mission or payload systems, and other supporting systems.

- 3.6.1.2 The safety and reliability considerations of OSO #05 apply to the aircraft's structural integrity and flight performance and handling aspects. For example, the airframe has the function of maintaining structural integrity in the aircraft-level.
- 3.6.1.3 For SAIL III, designers should evaluate the basic aircraft-level structural integrity and flight performance and handling aspects of the aircraft by performing relevant design and test activities, such as analysis, ground testing and flight testing. Compliance data for the structural substantiation and verification of flight characteristics can be included in the design and installation appraisal that complements the FHA.
- 3.6.1.4 At SAIL IV and above, aircraft-level structural and flight aspects are primarily addressed by OSO #04. Designers can declare compliance against OSO #05 for these aspects by referencing the compliance summary evidence generated under OSO #04.
- 3.6.1.5 Where an aircraft is fitted with payloads or similar internal or external systems, OSO #05 is applicable to these systems and their installations.
- 3.6.1.6 In determining compliance to OSO #05, the designer should also consider the response of the aircraft and its systems to the failure of any external system that is relied upon to support the operation of the aircraft.
- 3.6.1.7 Compliance with OSO#05 safety objectives may be considered in conjunction with the containment safety requirements and ground risk mitigation requirements, if applicable.
- 3.6.1.8 The JARUS SORA Cyber Safety Extension lists requirements for cybersecurity for OSO #05. The designers should satisfy the objectives for the relevant SAIL. CASA provides further guidance on airworthiness cybersecurity in [AC 21-57 - Airworthiness Cybersecurity of Remotely Piloted Aircraft Systems](#).

3.6.2 Functional hazard assessment (FHA)

- 3.6.2.1 An FHA is defined as a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity³.
- 3.6.2.2 The FHA serves as key a tool in safety assurance by classifying failure conditions and guiding design decisions to enhance system reliability and safety. It enables designers to evaluate aircraft reliability and implement design changes that result in increased reliability, such that the safety objective is achieved. Since safety assessment is an iterative process, the design is continually reassessed and refined until the required level of safety is achieved.
- 3.6.2.3 To conduct an FHA, designers need to identify aircraft functions, the aircraft system architecture, operational conditions, and crew procedures. The sources of data typically can be found in aircraft- or system-level description documents, the CONOPS for the proposed operation, system and sub-system requirements documents, and implementation artefacts.
- 3.6.2.4 As the aircraft-level FHA is the initial step in the safety assessment process, it assists designers to determine the criticality of aircraft systems and to establish appropriate safety objectives for those systems by identifying potential hazards. For systems that are identified as critical, designers should perform a system-level FHA to further analyse and address these system-specific hazards.
- 3.6.2.5 An FHA should identify each aircraft function, describe the associated hazards for each function, specify the flight phase(s) during which the hazard may occur, and assess the severity of the hazard based on its potential effects on the aircraft and flight crew.
- 3.6.2.6 Designers should minimise each identified hazard to an acceptable level based on the severity of the failure condition.

³ Definition from SAE ARP4761A.

3.6.2.7 Section A.2 of Appendix A contains an FHA template acceptable to CASA, and section A.3 of Appendix A provides an example FHA for reference.

3.6.3 Failure conditions and severity classifications

3.6.3.1 All potential failures should be identified for each high-level aircraft function. Designers should identify various modes of failure, including but not limited to the following:

- total loss of function
- partial loss of function
- degraded performance or impaired functionality
- erroneous or inconsistent input or output (data)
- uncommanded or unintended behaviour.

3.6.3.2 Each failure condition defined in an FHA identifies a specific aircraft function affected, the applicable phase of flight, the associated failure mode, and the effects of the failure condition on the aircraft and remote crew.

3.6.3.3 The effects on the aircraft and the remote crew help to determine the severity class of a failure condition (i.e. No Effect, Minor, Major, Hazardous or Catastrophic). Table 10 identifies the severity class associated with different aircraft and crew effects.

Table 10: Qualitative descriptions of severity of failure conditions

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 reductions in functional capabilities or safety margins.	Loss of aircraft with potential for fatalities on the ground.
Effect on flight crew	No effect on flight crew.	Slight increase in workload that involves crew action well within crew capabilities.	Significant increase in workload or in conditions impairing crew efficiency.	Excessive workload impairs ability to perform tasks accurately or completely.	Unable to maintain control of aircraft.

3.6.3.4 Designers should consider the effects of these failure modes in different phases of the flight. For example, for a fixed-wing aircraft, incorrect air data may lead to degraded ability to control airspeed during the cruise phase of flight, which can significantly reduce the aircraft's functional capabilities and safety margins, and lead to increased crew workload. Accordingly, this would likely be classified as a major failure condition.

3.6.3.5 Designers should document all factors considered when determining the severity classification of a failure condition in the FHA table. When assigning a severity class, the focus should be on the consequences of the failure, not on its likelihood.

3.6.3.6 Two critical design principles incorporated into safety assessment process as mitigations are redundancy and fail-safe design.

3.6.3.7 Redundancy involves incorporating multiple independent means to perform the same function. It means that if one means fails, another means can maintain safe operation. Redundancy in C2 links, energy storage systems (for example, batteries), flight control system (FCS), and inertial measurement unit (IMU), may reduce the criticality of a single failure.

- 3.6.3.8 A top-level function that is provided by a modular and redundant system may have different severity classifications depending on the type of failure. A total loss of the function may be catastrophic, whereas a partial loss of one individual element of a redundant system may have little or no immediate impact. These failure modes should be captured and analysed separately within the safety assessment to demonstrate that the design achieves an acceptable level of safety.
- 3.6.3.9 Fail-safe design focuses on minimising the severity of failure conditions by designing systems that default to a safe state upon a fault. For example, return to home (RTH) and hover in place are commonly used fail-safe design elements for RPAS which may reduce the severity classes. The implementation of hierarchical flight control laws that provide graceful degradation in the presence of sensor or actuator failures are another example of fail-safe design.
- 3.6.3.10 Each severity classification is associated with an allowable probability, as discussed in section 3.6.4. Qualitative and qualitative analysis may be used to demonstrate that the acceptable level of probability can be achieved for the severity classification identified within the FHA.

3.6.4 Allowable probabilities and design assurance levels

- 3.6.4.1 The SORA methodology establishes an acceptable TLOS of 10^{-6} /FH (i.e., 1 fatality per 1,000,000 flight hours) across all levels of SAIL.
- 3.6.4.2 The TLOS considers both the aircraft’s technical characteristics (characteristic dimension, likely impact velocity) and population-related characteristics (population density, fraction of people exposed to potential harm). For example, the probability of a fatality in case of loss of control of a SAIL V operation is calculated as 10^{-1} (1 fatality per 10 losses of control). Accordingly, the acceptable operational failure rate (L) for a SAIL V operation is found to be 10^{-5} (1 loss of control per 100,000 flight hours) to achieve the 10^{-6} TLOS target. An operational failure may be caused by aircraft systems, or due to operational aspects such as pilot mishandling. However, the scope of OSO #05 is limited to technical failures only.
- 3.6.4.3 Each one-level increase in SAIL implies a tenfold (one order of magnitude) reduction in the acceptable probability for an operational failure leading to a loss of control (L). For example, a SAIL III operation allows one operational failure per 1,000 flight hours ($L = 10^{-3}$ /FH), whereas a SAIL IV operation requires a stricter rate of one failure per 10,000 flight hours ($L = 10^{-4}$ /FH). Consequently, aircraft systems must be designed to be ten times safer to achieve the TLOS for each increase in SAIL.
- 3.6.4.4 Table 11 provides indicative allowable quantitative probabilities for individual failure conditions at a given severity class for a given level of SAIL. Further information on the rationale for allowable quantitative probabilities is provided in section A.1 of Appendix A.

Table 11: Allowable quantitative probabilities (in per FH) and functional design assurance levels (FDAL) for different severity classes and SAIL

Failure Condition Classification	No Effect	Minor	Major	Hazardous	Catastrophic
Probability Classification	No probability requirement	Probable	Remote	Extremely remote	Extremely improbable
SAIL VI $L=10^{-6}$ Pf=1	No probability or FDAL requirement	$<10^{-3}$ No FDAL requirement	$<10^{-5}$ FDAL D	$<10^{-6}$ FDAL C	$<10^{-7}$ FDAL B
SAIL V $L=10^{-5}$ Pf= 10^{-1} (0.1)	No probability or FDAL requirement	$<10^{-3}$ No FDAL requirement	$<10^{-4}$ No FDAL requirement	$<10^{-5}$ FDAL D	$<10^{-6}$ FDAL C

Failure Condition Classification	No Effect	Minor	Major	Hazardous	Catastrophic
SAIL IV L=10 ⁻⁴ Pf = 10 ⁻² (0.01)	No probability or FDAL requirement	No probability or FDAL requirement	< 10 ⁻³ No FDAL requirement	< 10 ⁻⁴ No FDAL requirement	<10 ⁻⁵ FDAL D
SAIL III L = 10 ⁻³ Pf = 10 ⁻³ (0.001)	No probability or FDAL requirement	No probability or FDAL requirement	No probability or FDAL requirement	< 10 ⁻³ No FDAL requirement	<10 ⁻⁴ No FDAL requirement
SAIL I - II Pf <= 10 ⁻⁴	No probability or FDAL requirement	No probability or FDAL requirement	No probability or FDAL requirement	No probability or FDAL requirement	No probability or FDAL requirement

SORA TLOS = L*Pf = 10⁻⁶ for all SAIL (SAIL I - SAIL VI)
 L = Operational failure rate (loss of aircraft)
 Pf = Probability of fatality, given operational failure (loss of aircraft)

- 3.6.4.5 Designers are able to determine the required level of assurance for aircraft functions by identifying the severity class for each failure condition associated with the function at the intended SAIL of the operation.
- 3.6.4.6 Each specific failure condition must meet the probability target defined in Table 11. If there is a probability requirement, probability of:
 - each Minor failure condition must be less than probable
 - each Major failure condition must be less than remote
 - each Hazardous failure condition must be less than extremely remote
 - each Catastrophic failure condition must be extremely improbable.
- 3.6.4.7 As indicated in Table 11, the quantitative probability targets associated with each severity class vary with the SAIL. Therefore, the qualitative probability classes should be interpreted according to the assigned SAIL.
- 3.6.4.8 The table indicates the varying levels of design rigour required for different SAILs. For instance, a low level of robustness requirement for SAIL III means designers need only focus on minimising hazards with hazardous or catastrophic severity to meet the criteria, and the reliability targets for the systems providing these functions are lower than those for higher SAIL operations.
- 3.6.4.9 The table also provides FDAL requirements, which focus on the functional aspects of a system and its potential impact on safety in a structured way.
- 3.6.4.10 The level of required design assurance depends on the associated FDAL. Depending on SAIL, CASA may accept RTCA DO-254, RTCA DO-178C, or ASTM F3201-24 as appropriate standards for hardware and software development assurance. Designers may propose alternative methodologies for hardware and software assurance by agreement with CASA.
- 3.6.4.11 To achieve OSO #05 at a high level of robustness for SAIL V and VI, no single failure can lead to a catastrophic failure condition. Therefore, designers must allocate those functions to at least two different items (e.g. redundancy) and demonstrate the absence of common cause failures.

3.6.5 System safety assessment

- 3.6.5.1 The SSA is a process to evaluate proposed architectures, identify safety requirements and verify the implemented design meets safety objectives and requirements.
- 3.6.5.2 System safety assessment methods, including a DIA, and supporting safety analyses, should be applied to show hazards are minimised to an acceptable level (and in accordance with the allowable quantitative probability values in Table 11, where applicable) as part of the FHA process.
- 3.6.5.3 The safety assessment process for OSO #5 is outlined in Figure 1.

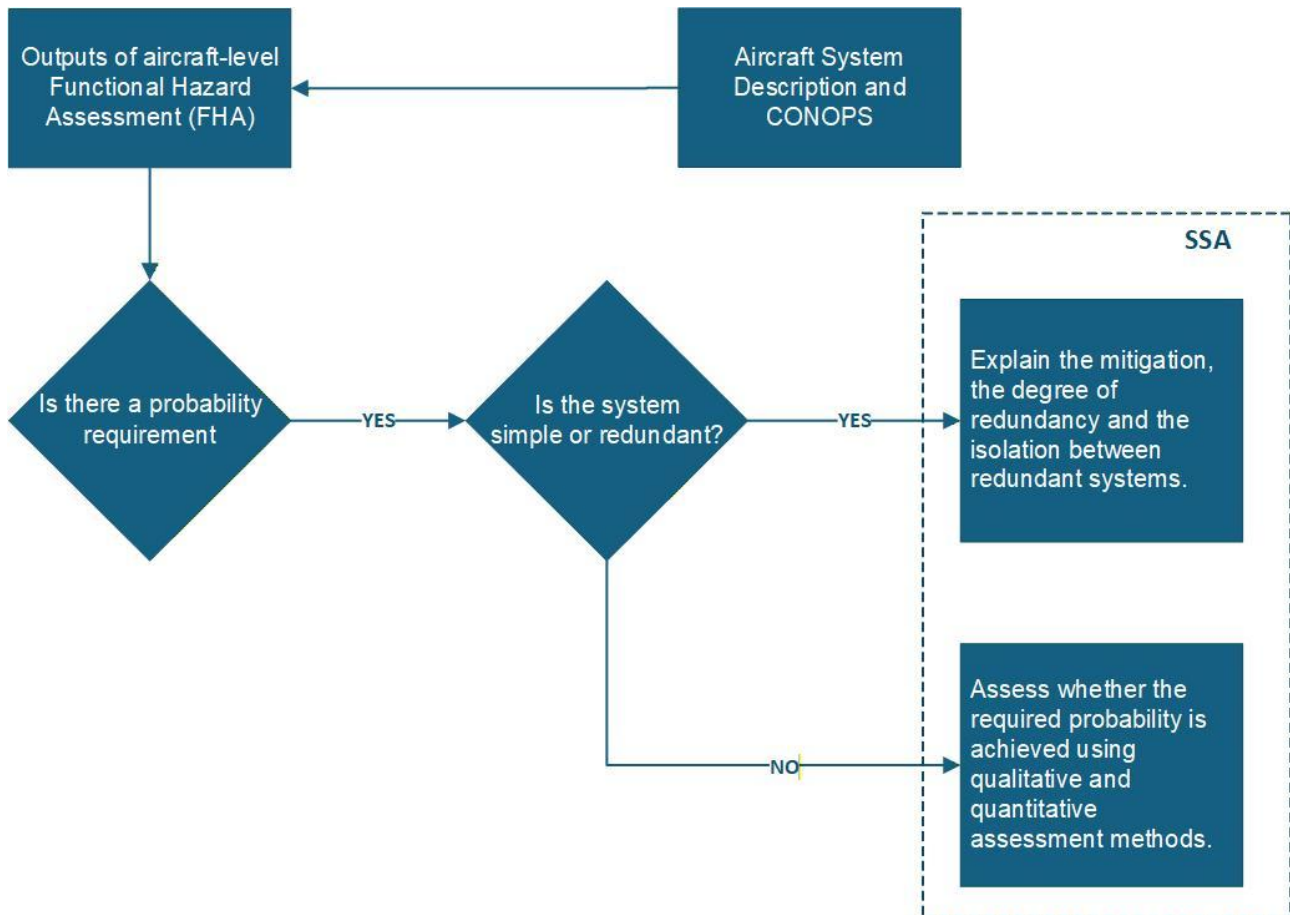


Figure 1: Simplified safety assessment process for OSO #05

- 3.6.5.4 As part of the system safety assessment, designers must show that any design principles, such as redundancy, fault detection, fail-safe design, and system segregation, that have been used as mitigations are effective and independent.
- 3.6.5.5 Redundancy has already considered in the severity classification during conducting FHA and has reduced the requirement for some conditions. However, designers should minimise the hazard associated with total loss of a function. In such systems, redundancy is used to reduce the probability of total loss and thereby minimise the associated hazard, but it does not change the inherent severity classification.
- 3.6.5.6 Similarly, a credit for the existence of a PRS can be taken as a means to minimise a hazard to an acceptable level.
- 3.6.5.7 A common cause failure (CCF), which occurs when two or more supposedly independent systems fail simultaneously due to a shared cause, must consider the independence requirements.

- 3.6.5.8 Catastrophic failure can occur despite multiple redundancies if CCF are not appropriately considered under the FHA. As an example, redundant flight control systems that are reliant upon shared power distribution or signal conditioning elements may be at risk of common cause failures in the event of failures in those elements.
- 3.6.5.9 To declare compliance with OSO#05, the designer must confirm that all system safety requirements and independence requirements are satisfied.

3.6.6 Design and installation appraisal

- 3.6.6.1 Design and installation appraisal (DIA) should identify a safety assurance approach with adequate mitigations and features/architectures to minimise the probability and severity of failure in the system, such as redundancy, fault tolerance, isolation, partitioning, proven reliability and similarity. It should be given as a reference in the FHA in the 'Remarks' column.
- 3.6.6.2 DIA is a qualitative appraisal of the integrity and safety of the system design and its installation. ASTM F3309-21 section 4.4 provides further guidance for how to conduct the DIA.
- 3.6.6.3 DIA should be used to verify that all requirements coming from the FHA are satisfied.
- 3.6.6.4 As a part of the DIA process, the designer should document, but is not limited to,
- system definition
 - implemented architecture description
 - design features supporting safety
 - evaluation of relevant requirements.
- 3.6.6.5 If the applicant can provide a rationale behind the decision on how the hazard is minimised to an acceptable level within the 'Remarks' column of the FHA, a separate DIA is not required if additional information containing the system definition and architectural analysis that supports the decision is provided.
- 3.6.6.6 When forming an appraisal is not possible without additional assessment, qualitative or quantitative system safety assessment methods can be used to support the DIA. The results of safety assessments are inputs to the DIA and help to justify the appraisal.

3.6.7 System safety assessment process and methods

- 3.6.7.1 Safety assessment methods, such as fault tree analysis (FTA), common cause analysis (CCA), and failure modes and effects analysis (FMEA), may be used as analysis techniques to assure system safety. Depending on the severity classification and acceptable probability these analysis methods may be either quantitative or qualitative (as shown in Figure 1). ARP4761A provides further guidance on the use of these analysis techniques.
- 3.6.7.2 Such assessment methods help the designer to identify and evaluate system requirements. For a simple system, the rationale used in the assessment should be straightforward and apparent for an experienced engineering judgment. It uses logical reasoning, failure mode analysis, and independence arguments.
- 3.6.7.3 Reliability record of the technology, satisfactory service experience on similar systems and systems developed per standards are examples of the rationale used in some assessments.
- 3.6.7.4 Similar approaches may be used for a complex system with more rigorous analysis and based on experienced engineering judgement.
- 3.6.7.5 For a qualitative FTA, designers structure the fault tree without assigning numeric rates. They can stop at the logical structure to show whether the architecture is acceptable and only:
- identify single points of failure
 - identify combinations of failures that lead to the top event

- demonstrate independence of redundancies.

3.6.7.6 Similarly, a qualitative FMEA is used to show coverage of failure effects and to ensure no overlooked hazards. Designers must:

- identify all failure modes of each component
- describe their effects on the system
- show whether they lead to hazardous/catastrophic failure conditions.

3.6.7.7 For CCA, designers must identify all common causes and list mitigations such as architectural separation, shielding, and system reliability.

3.6.7.8 Quantitative SSA aims to show that the probability of hazardous and catastrophic events is below the target thresholds provided in Table 11. It provides measurable, numerical evidence of safety compliance to meet safety objective.

3.6.7.9 For a quantitative SSA, designers must perform qualitative SSA first and have a valid model to analyse, as in FTA and FMEA. This is followed by providing numerical reliability data. For example, designers must assign failure rates to basic events in FTA and then compute the probability of the top event to show compliance with the target levels.

3.6.7.10 Numerical reliability relies on data such as failure rates of hardware, mean time between failures (MTBF) data, and error probabilities.

3.6.8 Demonstrating system safety and reliability through flight test

3.6.8.1 CASA expects designers to have demonstrated aircraft functions for each flight phase and evaluate/demonstrate safety for likely failure conditions by adequate means such as flight testing, ground testing, component testing, in-service experience, analysis and simulation. These methods can be used as evaluation methods for claims made under the appraisal process.

3.6.8.2 Evidence of compliance with OSO#05 may be collected during flight operations conducted under a Part 101 approval where OSO #05 is optional, during excluded category RPA operations or during flight tests conducted under an experimental certificate.

3.6.8.3 Experimental flight tests for R&D purposes allow designers to perform testing without the requirement to firstly show compliance to objectives of OSO#05. With an incremental approach to risk, designers can test their systems, gain evidence, and ultimately demonstrate compliance with requirements.

3.6.8.4 Section 2.6.5 of this Annex provides guidance on conducting experimental flight tests in Australia.

4 OSO #24 – UAS designed and qualified for adverse environmental conditions

4.1 General

- 4.1.1 The intent of OSO #24 is to ensure that RPAS has been designed by taking measures in the design phase to prevent failures that may occur due to adverse environmental conditions during an operation.
- 4.1.2 It also aims the RPAS has enough qualifications for environmental operating conditions which may be seen during an operation.

4.2 Level of robustness

- 4.2.1 The required level of robustness for OSO #24 is specified in Table 12 and categorised as optional (O), medium (M), or high (H), with corresponding SAIL.

Table 12: OSO #24 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	O	O	M	M	H	H

4.3 Level of integrity

- 4.3.1 The level of integrity must not be less than the required level of robustness. Table 13 provides the criteria for different integrity levels for OSO #24.

Table 13: OSO #24 Level of integrity

Level of integrity	Criterion
Medium	The RPAS is designed to perform as intended in the environmental conditions defined and reflected in the flight manual or equivalent document.
High	The RPAS is designed using environmental standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA.

4.4 Level of assurance

4.4.1 The level of assurance must not be less than the required level of robustness. Table 14 presents the criteria for the different assurance levels for OSO #24.

Table 14: OSO #24 Level of assurance

Level of assurance	Criterion
Medium	The applicant has supporting evidence that the required level of integrity is achieved. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience.
High	CASA validates the claimed level of integrity.

4.5 Means of compliance

4.5.1 Table 15 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #24.

Table 15: OSO #24 Means of compliance

Level of robustness	Evidence requirement and assessment process
Medium	<ul style="list-style-type: none"> a. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA. CASA conducts an assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met. b. Partial qualification may be acceptable (for medium robustness only).
High	<ul style="list-style-type: none"> a. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA. CASA conducts a comprehensive assessment of the declared compliance based on the supporting evidence. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

4.6 Additional guidance

4.6.1 Environmental qualification

4.6.1.1 To assure safe operation, RPAS components, equipment, and systems that are critical to the safety of flight must be appropriately tested and qualified for both anticipated (nominal) environmental conditions, as well as certain applicable adverse environmental conditions.

4.6.1.2 The RPAS manufacturer must identify the intended operational conditions that the RPAS, and its systems, are designed to meet within the flight manual, or an equivalent document.

4.6.1.3 Operators must ensure that the RPAS is only operated within the operational conditions and in accordance with any associated operational limitations identified in the flight manual.

4.6.1.4 The RPAS manufacturer must assess the likely risk of encountering adverse environmental conditions in the intended operational environment using an appropriate assessment methodology.

4.6.1.5 RPAS components, equipment and systems that may cause hazardous failure conditions must have adequate qualification to substantiate their reliability and safety when operated within the intended operational conditions.

- 4.6.1.6 Environmental conditions that may relate to potential operational limitations include temperature range, intended altitude, wind speeds, humidity conditions, sand/dust conditions, precipitation conditions, presence of icing, and proximity to lightning sources or high intensity radiated fields (HIRF). A list of potentially applicable conditions for environmental qualification is provided in Table 16.
- 4.6.1.7 Maximum and minimum operating temperature ranges, altitude limits (service ceiling), maximum wind speeds (including gusts) and the operational humidity range should be identified in the flight manual, or equivalent document. The need for further operational limitations relating to other conditions depend upon the likelihood of encountering those conditions and whether appropriate environmental qualification, such as test, has been conducted.
- 4.6.1.8 Test is the principal method of demonstrating compliance to many environmental qualification requirements. Environmental qualification of RPAS components, equipment and systems to key conditions relating to temperature and altitude, temperature variation, and humidity may be shown by test, or by analysis or simulation. Particularly at high robustness (SAIL V - SAIL VI), it is unlikely that simulation or analysis, in the absence of supporting test evidence, would provide an adequate substantiation.
- 4.6.1.9 If a proposed operation exposes the RPAS to HIRF or lightning environments, the manufacturer should provide supporting evidence for qualification and establish appropriate operational limitations for such conditions. Examples of potential sources of HIRF include radar systems, mobile phone telecommunication towers, high voltage transmission lines, and radio and television transmitters.
- 4.6.1.10 RTCA DO-160G is one standard acceptable to CASA for environmental qualification. This standard defines environmental test conditions and test procedures for airborne equipment. The test procedures per RTCA DO-160G are primarily intended for environmental equalisation for type-certified aircraft. Therefore, CASA does not mandate strict or exhaustive testing in conformity to RTCA DO-160G for equipment qualification at medium robustness (SAIL III - SAIL IV). An applicant may adapt test conditions and procedures outlined in RTCA DO-160G, or other similar standards, when demonstrating compliance with the requirements of OSO #24. Applicants are encouraged to seek early guidance from CASA on appropriate environmental qualification.
- 4.6.1.11 The RPAS manufacturer is required to declare compliance and provide supporting evidence to CASA. An example environmental qualification statement for OSO #24 is provided in Appendix B.1.

Table 16: Potentially applicable conditions for environmental qualification

Condition	Limitations	Compliance Method	Evidence Documents	Remarks
(General)		Test Analysis, Simulation, etc.	Reference to test reports, analysis documents, simulation results, etc.	Applied standard (if applicable), deviations or modifications to test methods, proposed mitigations or operational limitations, etc.
Temperature and Altitude	Appropriate operational temperature range and service ceiling (altitude) limitations.	Test e.g., DO-160G Sec. 4. Analysis		Typically required at SAIL III and above. Partial compliance may be acceptable for

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

Condition	Limitations	Compliance Method	Evidence Documents	Remarks
		Simulation		medium level of robustness.
Temperature Variation	Appropriate operational temperature range limitations.	Test e.g., DO-160G Sec. 5. Analysis Simulation		Typically required at SAIL III and above. Partial compliance may be acceptable for Medium level of robustness.
Humidity	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 6.		Typically required at SAIL IV and above.
Operational Shock / Crash Safety	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 7. Analysis Simulation		Typically required at SAIL IV and above. Analysis and simulation may support in-service data.
Vibration		Test e.g., DO-160G Sec. 8. Analysis Simulation		Typically required at SAIL III and above. Analysis and simulation may support in-service data.
Explosive Atmosphere	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 9.		
Waterproofness	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 10.		Typically required SAIL III and above; or operational limitation.
Fluids Susceptibility	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 11.		
Sand and Dust	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 12.		
Fungus Resistance	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 13.		
Salt Fog	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 14.		

Condition	Limitations	Compliance Method	Evidence Documents	Remarks
Magnetic Effect	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 15.		
Power Input		Test e.g., DO-160G Sec. 16.		Typically required at SAIL III and above.
Voltage Spike		Test e.g., DO-160G Sec. 17.		Typically required at SAIL III and above.
Audio Frequency Conducted Susceptibility	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 18.		
Induced Signal Susceptibility	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 19.		
Radio Frequency Susceptibility	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 20. Analysis Simulation		Typically required at SAIL III and above; or operational limitation.
Emission of Radio Frequency Energy	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 21. Analysis Simulation		
Lightning Induced Transient Susceptibility	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 22. Analysis Simulation		Typically required at SAIL III and above; or operational limitation.
Lightning Direct Effects	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 23.		Typically required at SAIL III and above; or operational limitation.
Icing	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 24.		
Electrostatic Discharge (ESD)	Limitation may control, no need to test.	Test e.g., DO-160G Sec. 25.		

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

Condition	Limitations	Compliance Method	Evidence Documents	Remarks
		Analysis Simulation		
Fire and Flammability		Test e.g., DO-160G Sec. 26.		

Appendix A

OSO #05 – Compliance

A.1 Rationale for allowable quantitative probabilities established under OSO #05

Reference: Table 11.

- A.1.1 To assess the acceptability of a system design under SORA, it is necessary to firstly establish a series of rational and congruent probability values for the acceptable rates of failure of differing failure conditions, across differing SAIL levels.
- A.1.2 In determining the indicative quantitative probabilities for the different failure condition classifications identified in Table 11, CASA has sought to align its approach to the already established 'safety continuum' that is applicable to other similar categories of aircraft, including smaller conventional ('Part 23') type-certificated aircraft as well as non- type-certificated aircraft, such as light sport aircraft (LSA).
- A.1.3 Under SORA, for a SAIL VI operation, an acceptable operational failure rate (loss of aircraft) objective of 10^{-6} per flight hour (FH) is required to be met. This is because, at SAIL VI, the SORA target level of safety (TLOS) requirement of 10^{-6} is achieved solely based on aircraft reliability (i.e., driven only by the operational failure rate), with the associated probability of fatality (given an operational failure) assumed to be 1 (i.e., 10^{-0}) in the event of such a failure during a SAIL VI operation.
- A.1.4 For a SAIL VI operation, to achieve the operational failure rate (loss of aircraft) of 10^{-6} per FH, and based upon the assumption of there being in the order of ten (10^1) individual catastrophic failure conditions that could result in operational failure, an indicative allowable quantitative probability for an individual catastrophic failure condition of 10^{-7} per FH is established.
- A.1.5 Similarly, for each lower SAIL (SAIL V and below) under SORA, where the acceptable operational failure rate (loss of aircraft) to achieve the same SORA TLOS is reduced by 10^{-1} (i.e., a one order of magnitude reduction, per SAIL level), corresponding values for indicative allowable quantitative probabilities have been established. For example, for a SAIL V operation, the indicative allowable quantitative probability for an individual catastrophic failure condition is 10^{-6} per FH, this being one order of magnitude less than the equivalent for a SAIL VI operation.
- A.1.6 For SAIL V and SAIL VI, indicative quantitative probabilities have been established for failure condition classifications other than catastrophic failures, such as hazardous, major and minor failures. For hazardous failures, it is customary to assign a quantitative probability that is one order of magnitude lesser than that of catastrophic failures, with major and other failures similarly assigned to lesser (yet appropriate and rational) values. These values have been reflected in Table 11.
- A.1.7 For SAIL III and IV, indicative quantitative probabilities have been established for certain failure conditions only. Whilst quantitative system safety assessment methods are not mandatory under OSO #05 for operational approval at SAIL III or SAIL IV, the inclusion of these indicative probability values is intended to assist applicants in performing rational and evidence-based system safety assessment.
- A.1.8 In confirming whether the probabilities established within Table 11 for various SAIL levels are congruent to equivalent probabilities established by regulatory authorities for other categories of aircraft operating within the same 'safety continuum', it is helpful to review the already-published guidance for those categories of aircraft.

- A.1.9 Historically, in FAA AC 23.1309-1E ('System Safety Analysis and Assessment for Part 23 Airplanes'), the FAA has defined four classes of aeroplanes; including Class I - typically a single reciprocating-engine aircraft of 6,000 lbs (approx. 2,722 kg) maximum take-off weight (MTOW), and Class II - typically a single turbine-engine (or multiple reciprocating-engine) aeroplane of equivalent MTOW. These two aeroplane classes align most closely to a SAIL VI aircraft. In those cases, FAA AC 23.1309-1E establishes an indicative allowable probability for an individual catastrophic failure of 10^{-6} per FH for a Class I aeroplane, and of 10^{-7} per FH for a Class II aeroplane.
- A.1.10 In 2025, FAA published FAA AC 21.17-4 ('Type Certification-Powered Lift') and an associated policy statement FAA PS-AIR-21.17-01 ('Safety Continuum for Powered-lift'). Together, these publications establish the certification criteria and associated safety continuum for type-certificated powered-lift aircraft, such as cargo- and passenger-carrying electric vertical take-off and landing (eVTOL) aircraft. The policy statement establishes four certification levels (1-4), which are then further sub-classified to a total of 8 levels (from '1A' to '4B') based on operational use. For a certification level '1A' powered-lift aircraft, which likely aligns most closely to a SAIL VI aircraft, the policy statement establishes an indicative allowable probability for an individual catastrophic failure of 10^{-7} per FH.
- A.1.11 In 2024, the European Union Aviation Safety Agency (EASA) published MOC Light UAS.2510-01 (applicable to SAIL III-IV operations) and, in 2025, published MOC Light-UAS High Risk.2510-01 (applicable to SAIL V-VI operations). The EASA means of compliance (MOC) establishes an indicative allowable probability for an individual catastrophic failure of 10^{-8} per FH for a SAIL VI operation and similarly reducing, as expected, by one order of magnitude for each lower SAIL level. This is consistent with the methodology adopted by CASA, although the probability requirement established by EASA is more conservative (by one order of magnitude) than the corresponding CASA requirement.

A.2 Aircraft functional hazard assessment template

A.2.1 The template given in Table 17 may be used for FHA by the applicants. The table should be completed with the relevant details for each column, including the system under consideration, the specific function being assessed, the associated failure mode and its description, the applicable flight phase, the resulting effect of the failure on the aircraft and crew, the assigned final severity classification, the corresponding target probability, the verification artifact used to substantiate the assessment, and any additional remarks or assumptions supporting the determination of the final severity classification and any relevant mitigations to meet the target probability.

Table 17: Aircraft functional hazard assessment template

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks

A.3 Aircraft functional hazard assessment example

A.3.1 An example of an FHA for selected failure conditions is provided in Table 18 for reference.

Table 18: Aircraft functional hazard assessment example

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks
1	VTOL Propulsion	VTOL lift generation during take-off and landing	Total loss of upward lift capability (Simultaneous VTOL motor failure)	Take off, Landing, Transition	Aircraft: Loss of aircraft with potential for fatalities on the ground Crew: Unable to maintain control of aircraft	Catastrophic	Extremely improbable	Qualitative Analysis- DIA	The total loss of the function is extremely improbable because of redundancy. There are 8 different motors to provide this function, and it reduces the likelihood of this failure.
2	VTOL Propulsion	VTOL lift generation during take-off and landing	Total loss of upward lift capability (VTOL motor failure)	Cruise	Aircraft: Loss of vertical landing capability of the aircraft. Aircraft will perform glide landing with possible hard landing. Crew: Significant increase in workload.	Major	Remote	Qualitative Analysis- DIA	The total loss of the function is extremely improbable because of redundancy. There are 8 different motors to provide this function, and it reduces the likelihood of this failure.
3	VTOL Propulsion	VTOL lift generation during take-off and landing	Partial loss of upward lift capability. (One VTOL motor fail)	Take off, Landing, Transition	Aircraft: Is controllable with the remaining VTOL motors	Minor	Probable		

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks
					Crew: Slight increase in workload to maintain control				
4	VTOL Propulsion	VTOL lift generation during take-off and landing	Partial loss of upward lift capability. (Asymmetric VTOL loss caused by 2 or 3 VTOL motors failure)	Take off, Landing, Transition	Aircraft: Uncontrolled descent, possible loss of aircraft in a controlled environment. Crew: Unable to maintain control	Catastrophic	Extremely improbable	Qualitative FTA Analysis-DIA	No single point of failure has identified. Likelihood of this event is extremely remote based on the safety assessment given in the DIA.
xx	Pusher Engine	Providing forward thrust for horizontal flight	Loss of forward thrust capability because of engine failure	Transition, Cruise	Aircraft: Slight reduction in horizontal flight capability and aircraft is controllable with the remaining VTOL motors Crew: Significant increase in workload to maintain control	Major	Remote	Qualitative Analysis- DIA	FCS can maintain horizontal flight using the VTOL motors.
xx	Airframe	Providing structural integrity	Structural failure in flight	All	Aircraft: Potential loss of control and aircraft.	Catastrophic	Extremely improbable	Structural analysis and test activities Report XXX	The flight critical structural components are designed to maintain structural integrity without any failure for the

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks
					Crew: Unable to maintain control of aircraft				loads that can be seen in the flight envelope. Ground testing has been executed for the wing to verify the analysis results. Structural test for the wing was successfully executed at 1.5 times the limit loads to demonstrate the integrity of the structure. Additionally, flight tests have been performed for the boundaries of the flight envelope without any structural failure.
xx	Flight Control System	Maintaining commanded flight	Software failure to command correct value for thrust, pitch, roll, yaw	All	Aircraft: FCS reversionary behaviour triggered. RTH procedure navigates the aircraft to a safe location for forced landing. Crew: Significant increase in workload.	Major	Extremely Remote	Qualitative FTA	Backup FCS takes over and initiates RTH procedure when the total loss of primary FCS function is detected.

DRAFT

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks
xx	Electrical System	Providing power to VTOL motors	Total loss of electrical power to rotors	Take-off, Landing, Transition	Aircraft: Loss of aircraft with potential for fatalities on the ground Crew: Unable to maintain control of aircraft	Major	Remote	Qualitative Analysis- DIA	The total loss of the function is extremely improbable because of redundancy. Backup system is activated and remote pilot initiates emergency procedures.
xx	Electrical System	Providing power to VTOL motors	Loss of electrical power to rotors	Cruise	Aircraft: Loss of vertical landing capability of the aircraft. Aircraft will perform glide landing with possible hard landing. Crew: Significant increase in workload.	Major	Remote	Qualitative Analysis- DIA	Remote pilot initiates emergency procedures and start glide landing approach
	Electrical System	Providing power to avionics	Loss of electrical power to FCS and aircraft sensors	All	Aircraft: Loss of aircraft with potential for fatalities on the ground Crew: Unable to maintain control of aircraft	Catastrophic	Extremely improbable	Qualitative Analysis, DIA	The total loss of the function is extremely improbable because of redundancy. Backup system is activated and remote pilot initiates emergency procedures.

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

#	System	Function	Failure Mode and Description	Flight Phase	Effect	Severity Class	Target Probability	Verification Artifact	Remarks
xx	C2 Link	Providing communication between remote pilot and RPAS	Loss of all C2 links	All	Aircraft: FCS reversionary behaviour triggered. RTH procedure navigates the aircraft to a safe location for forced landing. Crew: Significant increase in workload.	Major	Remote		FCS maintains control and initiates RTH procedure to navigate and land at a safe location, which decreases the severity of this failure condition.
xx	C2 Link	Providing communication between remote pilot and RPAS	Loss of single C2 link	All	Aircraft: Control maintained using remaining C2 link. Crew: Slight increase in workload	Minor	Probable		Crew initiates C2 link recovery procedures.

Appendix B

OSO #24 – Compliance

B.1 Example environmental qualification statement

- B.1.1 The following table format may be used to summarise environmental qualification testing and compliance to the applicable environmental qualification standard, such as RTCA DO-160 or another acceptable standard.
- B.1.2 This table should form part of an environmental qualification report that outlines the qualification testing that has been performed and appropriately substantiates the claim of compliance that has been made for each test condition category identified in the table.

Table 19: Example environmental qualification statement

Conditions	Standard / Reference	Description
Temperature and Altitude	DO-160G, Sec. 4	Tested, based on modified criteria (Category A1, modified).
Temperature Variation	DO-160G, Sec. 5	Tested, based on modified criteria (Category B, modified).
Humidity	DO-160G, Sec. 6	Not tested. Category X.
Operational Shock / Crash Safety	DO-160G, Sec. 7	Not tested. Category X.
Vibration	DO-160G, Sec. 8	Not tested. Category X.
Explosive Atmosphere	DO-160G, Sec. 9	Not tested. Category X.
Waterproofness	DO-160G, Sec. 10	Not tested. Category X.
Fluids Susceptibility	DO-160G, Sec. 11	Not tested. Category X.
Sand and Dust	DO-160G, Sec. 12	Not tested. Category X.
Fungus Resistance	DO-160G, Sec. 13	Not tested. Category X.
Salt Fog	DO-160G, Sec. 14	Not tested. Category X.
Magnetic Effect	DO-160G, Sec. 15	Not tested. Category X.
Power Input	DO-160G, Sec. 16	Tested, based on modified criteria (Category Bxx, modified).
Voltage Spike	DO-160G, Sec. 17	Tested, based on modified criteria (Category A, modified).
Audio Frequency Conducted Susceptibility	DO-160G, Sec. 18	Not tested. Category X.

DRAFT

Guidance for compliance with airworthiness operational safety objectives for Australian specific operational risk assessment

Conditions	Standard / Reference	Description
Induced Signal Susceptibility	DO-160G, Sec. 19	Not tested. Category X.
Radio Frequency Susceptibility	DO-160G, Sec. 20	Not tested. Category X.
Emission of Radio Frequency Energy	DO-160G, Sec. 21	Not tested. Category X.
Lightning Induced Transient Susceptibility	DO-160G, Sec. 22	Not tested. Category X.
Lightning Direct Effects	DO-160G, Sec. 23	Not tested. Category X.
Icing	DO-160G, Sec. 24	Not tested. Category X.
Electrostatic Discharge (ESD)	DO-160G, Sec. 25	Not tested. Category X.
Fire and Flammability	DO-160G, Sec. 26	Not tested. Category X.