

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

October 2026

DRAFT

Contents

1	Introduction	5
2	OSO #02 – RPAS manufactured by competent or proven entity	6
2.1	General	6
2.2	Level of robustness	6
2.3	Level of integrity	6
2.4	Level of assurance	7
2.5	Means of compliance	7
2.6	Additional guidance	8
3	OSO #03 – RPAS maintained by competent or proven entity	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	Responsibilities of RPAS designers	15
3.6	Guidance for RPAS designers	16
4	OSO #04 – RPAS components essential to safe operations are designed to an airworthiness design standard	20
4.1	General	20
4.2	Level of robustness	20
4.3	Level of integrity	20
4.4	Level of assurance	21
4.5	Means of compliance	21
4.6	Additional guidance	22
5	OSO #05 – RPAS is designed considering system safety and reliability	28
5.1	General	28
5.2	Level of robustness	28
5.3	Level of integrity	28
5.4	Level of assurance	29
5.5	Means of compliance	30
5.6	Additional guidance	30
6	OSO #06 – C3 link characteristics are appropriate for the operation	38
6.1	General	38
6.2	Level of robustness	38
6.3	Level of integrity	38
6.4	Level of assurance	39
6.5	Means of compliance	39
6.6	Additional guidance	40
7	OSO #07 – Conformity check of the RPAS to ensure consistency to the ConOps	43
7.1	General	43

7.2	Guidance for RPAS designers and manufacturers	43
8	OSO #18 – Automatic protection of the flight envelope from human error	45
8.1	General	45
8.2	Level of robustness	45
8.3	Level of integrity	45
8.4	Level of assurance	46
8.5	Means of compliance	46
8.6	Additional guidance	47
9	OSO #19 – Safe recovery from human error	49
9.1	General	49
9.2	Level of robustness	49
9.3	Level of integrity	49
9.4	Level of assurance	49
9.5	Means of compliance	50
9.6	Additional guidance	51
10	OSO #20 – A Human Factors evaluation has been performed and the human-machine interface (HMI) found appropriate for the mission	53
10.1	General	53
10.2	Level of robustness	53
10.3	Level of integrity	53
10.4	Level of assurance	54
10.5	Means of compliance	54
10.6	Additional guidance	55
11	OSO #24 – RPAS designed and qualified for adverse environmental conditions	58
11.1	General	58
11.2	Level of robustness	58
11.3	Level of integrity	58
11.4	Level of assurance	58
11.5	Means of compliance	59
11.6	Additional guidance	59
Appendix A	OSO #02 – Compliance	63
Appendix B	OSO #05 – Compliance	66
Appendix C	OSO #24 – Compliance	76



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 AusSORA is a risk assessment process for drone operators to assess and mitigate risks for complex remotely piloted aircraft systems (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. CASA recognises that manufacturers may not share detailed intellectual property; in such cases, substantiation may be provided directly by the designer/manufacturer to CASA, where appropriate.
- 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.
- 1.6 In addition to the criteria, 'means of compliance' and 'additional guidance' sections in each OSO aim to define:
- methods, processes, or evidence used to demonstrate that a requirement or objective has been satisfied
 - what is acceptable and expected evidence for different levels of robustness.
- 1.7 The annex presents performance-based approach with flexible methods proportionate to risk and SAIL level. Applicants can bring their proposed means of compliance to meet the performance-based requirements.
- 1.8 As the SAIL increases, airworthiness expectations increase in a manner proportionate to the level of risk. However, these expectations are not intended to replicate the rigour of type certification, particularly at SAIL IV and below.
- 1.9 Accepted evidence may be reused across multiple applications for the same product configuration, provided the manufacturer maintains robust configuration management that ensure the evidence remains valid for the configuration being assessed.
- 1.10 This annex does not introduce functional test-based approaches as a means of compliance as in JARUS SORA.
- 1.11 However, compliance with certain requirements may be demonstrated through satisfactory operational experience. Applicants should present such operational experience in a systematic and structured manner, supported by evidence acceptable to CASA.

2 OSO #02 – RPAS manufactured by competent or proven entity

2.1 General

- 2.1.1 The OSO #02 is intended to demonstrate that the RPAS manufacturer is competent in manufacturing the RPAS with a controlled and standardised quality.
- 2.1.2 OSO #02 ensures that risks arising from manufacturing-related issues are managed.

2.2 Level of robustness

- 2.2.1 The required level of robustness for OSO #02 is specified in Table 1 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 1: OSO #02 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	H	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 #02.

Table 2: OSO #02 Level of integrity

Level of integrity	Criterion
Low	As a minimum, manufacturing procedures cover: • specification of materials • suitability and durability of materials used • processes necessary to allow for repeatability in manufacturing and conformity within acceptable tolerances • configuration control.
Medium	As a minimum, manufacturing procedures cover: • specification of materials • suitability and durability of materials used • processes necessary to allow for repeatability in manufacturing and conformity within acceptable tolerances • configuration control • verification of incoming products, parts, materials, and equipment • identification and traceability • in-process and final inspections and testing • control and calibration of tools • handling and storage • non-conforming item control.
High	As a minimum, manufacturing procedures cover:

Level of integrity	Criterion
	• specification of materials • suitability and durability of materials used • processes necessary to allow for repeatability in manufacturing and conformity within acceptable tolerances • configuration control • verification of incoming products, parts, materials, and equipment • identification and traceability • in-process and final inspections and testing • control and calibration of tools • handling and storage • non-conforming item control • personnel competence and qualification • supplier control.

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 #02.

Table 3: OSO #02 Level of assurance

Level of assurance	Criterion
Low	The declared manufacturing procedures are developed in accordance with a means of compliance acceptable to CASA.
Medium	The declared manufacturing procedures are developed in accordance with a means of compliance acceptable to CASA. The evidence is available that each RPAS has been manufactured in conformance to its design.
High	The declared manufacturing procedures are developed in accordance with a means of compliance acceptable to CASA. The evidence is available that each RPAS has been manufactured in conformance to its design. Manufacturing procedures and conformity of the RPAS to its design and specification are recurrently verified through process or product audit by a competent third party.

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 #02.

Table 4: OSO #02 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	a. The RPAS manufacturer should maintain an effective quality management system, or an equivalent program, based on documented manufacturing procedures that, at a minimum, address the criteria applicable to a low level of integrity. b. The manufacturing procedures should be developed in accordance with a means of compliance acceptable to CASA. c. 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	a. The RPAS manufacturer should maintain an effective quality management system, or an equivalent program, based on documented manufacturing procedures that, at a minimum, address the criteria applicable to a medium level of integrity. b. The manufacturing procedures are developed in accordance with a means of compliance acceptable to CASA. c. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.
High	a. The RPAS manufacturer should maintain an effective quality management system, or an equivalent program, based on documented manufacturing procedures that, at a minimum, address the criteria applicable to a high level of integrity. b. The manufacturing procedures are developed in accordance with a means of compliance acceptable to CASA. c. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. 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 Key Considerations

- 2.6.1.1 **Specification of materials:** Materials should be clearly specified to ensure they meet functional, quality, safety and regulatory (if required) requirements. Specifications should define material type, grade, dimensions, tolerances, applicable standards, and revision status where relevant. Changes to specifications should be reviewed and controlled.
- 2.6.1.2 **Suitability and durability of materials used:** Materials should be suitable for their intended application and capable of maintaining required performance throughout expected operating and environmental conditions. Consideration should be given to reliability, wear, corrosion, fatigue, environmental exposure, and potential safety impacts associated with material failure.
- 2.6.1.3 **Processes necessary for repeatability in manufacturing and conformity within acceptable tolerances:** Manufacturing processes should be planned and controlled to achieve repeatable outcomes and maintain conformity within specified tolerances. Controls may include documented procedures, work instructions, process monitoring, operator training, and defined acceptance criteria. Critical process steps and operational risks should be identified and managed appropriately to minimise variation and prevent defects.

- 2.6.1.4 **Configuration control:** Drawings, specifications, software versions, bills of materials, and process documents should be controlled to ensure only current approved revisions are used. Changes should be reviewed, approved, documented, traceable, and communicated to relevant personnel prior to implementation.
- 2.6.1.5 **Verification of incoming products, parts, materials, and equipment:** Incoming materials, components, products, and equipment should be verified against specified requirements prior to use. Verification methods may include inspection, testing, sampling, review of supplier documentation, or validation checks. The level of verification should reflect supplier performance, product criticality, and operational risk. For Commercial Off-the-Shelf (COTS) parts, additional verification may be required in accordance with a COTS Parts Management Plan (CPMP) as discussed in section 2.6.3.
- 2.6.1.6 **Identification and traceability:** Products, materials, and components should be identified throughout manufacturing, storage, and delivery as necessary to maintain conformity and support traceability. Traceability methods may include serial numbers, batch numbers, work orders, labels, or controlled digital records. Appropriate records should be maintained to support investigation of quality, conformity, reliability, or safety issues.
- 2.6.1.7 **In-process and final inspection and testing:** Inspection and testing activities should verify that products and processes conform to defined requirements before release. This should include appropriate in-process inspections, final inspections, and functional or performance testing where required. Increased attention should be given to critical characteristics, defect prevention, conformity and verification of safety related requirements.
- 2.6.1.8 **Control and calibration of tools:** Monitoring, measuring, and test equipment should be maintained, protected, and calibrated at planned intervals to ensure accurate and reliable results. Calibration status should be identifiable, records maintained, and actions taken where equipment is found to be out of tolerance or potentially affecting product conformity.
- 2.6.1.9 **Handling and storage:** Products and materials should be handled, packaged, stored, preserved, and transported in ways that prevent damage, deterioration, contamination, mix-ups, or loss of identification. Storage conditions and handling methods should be appropriate for the product type, operational environment and applicable safety or conformity requirements.
- 2.6.1.10 **Non-conforming item control:** Non-conforming products or materials should be identified and controlled to prevent unintended use or delivery. Nonconformities should be documented, evaluated, and dispositioned by authorised personnel. Corrective actions should address root causes, prevent recurrence, and consider potential impacts on product conformity, reliability, and safety.
- 2.6.1.11 **Personnel competence and qualification:** Personnel performing work affecting quality should be competent based on appropriate education, training, skills, experience, and demonstrated ability. The personnel should understand their responsibilities, the importance of conformity objectives, product safety considerations, and the impact of human factors on safety outcomes.
- 2.6.1.12 **Supplier control:** Suppliers should be evaluated, selected, monitored, and periodically reviewed to ensure they consistently meet specified quality, delivery, traceability, and conformity requirements. Supplier controls may include approved supplier lists, performance monitoring, audits, corrective actions, and communication of applicable technical and quality requirements. The extent of supplier oversight should reflect supplier performance, product criticality, and operational risk.
- 2.6.1.13 Appendix A provides a checklist for manufacturers to document and address each topic.

2.6.2 Quality management system and relevant standards

- 2.6.2.1 Manufacturers should have a quality management system (QMS) or equivalent program to ensure that appropriate manufacturing procedures are effectively used in the manufacturing of the RPAS. Proper manufacturing procedures confirm that the final products are manufactured with adequate quality standards.

- 2.6.2.2 While the rest of the document refers to a QMS, any program that has the same intention and provides the same measures to assure the quality of the product can be considered a QMS by CASA.
- 2.6.2.3 An efficient and effective QMS demonstrates that the manufacturer has the ability to manage all manufacturing activities to provide products meeting certain standards and repeatability in manufacturing processes by robust practices.
- 2.6.2.4 ISO 9001:2015 can be used by manufacturers to demonstrate a QMS. Its requirements define how to establish, implement, maintain, and continually improve a QMS. While this standard has not been developed for aviation, it provides the best practices for various industries. The related sections that align with the manufacturing procedures given in the level of integrity criteria should be addressed in the manufacturer's quality management system.
- 2.6.2.5 AS9100D which was developed based on ISO9001 is specific for the aerospace industry. Besides tailored specifications for the aerospace industry, AS9100D provides additional requirements for quality management and product safety.
- 2.6.2.6 While QMS based on ISO9100:2015 or AS9100D is good to have as a practice, CASA does not expect full compliance with these standards for SAIL III and SAIL IV operations.
- 2.6.2.7 The QMS should address all activities related to the target level of integrity.
- 2.6.2.8 While the criteria do not include internal auditing activities, such activities should be in place for an adequate QMS.
- 2.6.2.9 Manufacturers should have documented manufacturing and quality control procedures for an effective and efficient QMS.

2.6.3 Commercial Off-the-Shelf parts

- 2.6.3.1 Commercial off-the-shelf (COTS) parts are ready-made products sourced from the open market. COTS parts are intended for use in multiple general applications and may not have been developed to the same level of integrity and assurance required for RPAS applications. An understanding of the COTS part design, capabilities and potential safety effects is needed along with proper configuration control. In some cases, additional screening and testing of the COTS parts may be required to ensure acceptable performance. The level of screening and testing required will depend on the COTS part intended use and potential safety impacts.
- 2.6.3.2 To ensure good configuration control, an applicant should develop a COTS parts management plan (CPMP). At a minimum, the CPMP should include the information shown in Table 5.

Table 5: OSO #02 COTS parts management plan (CPMP)

SAIL	I	II	III	IV	V	VI
COTS parts list	O	O	✓	✓	✓	✓
COTS part classification	O	O	✓	✓	✓	✓
Design assessment	O	O	✓	✓	✓	✓
Conformity inspection plan	O	O	O	✓	✓	✓

- 2.6.3.3 The COTS parts list should provide an accurate description of the COTS parts used, and include all the details necessary to establish the exact parts and their configuration, such as:

- manufacturer
- part number
- serial numbers
- specification number
- part description (i.e. physical dimensions, physical characteristics, software version).

2.6.3.4 Each COTS part should be classified in the CMCP into one of the following categories based on their worst-case failure mode in accordance with OSO #05 hazard severity definitions:

- Non-critical: COTS part whose failure would have no greater than a Minor effect on the aircraft and/or crew.
- Major: COTS part whose failure would have no greater than a Major effect on the aircraft and/or crew.
- Critical: COTS part whose failure could have a Hazardous or Catastrophic effect on the aircraft and/or crew.

2.6.3.5 A COTS design assessment should be conducted to confirm the COTS parts classification and determine if additional acceptance testing may be required to ensure the COTS part performs as intended and demonstrates repeatability. The necessary scope and detail of this assessment is dependent on the COTS part classification as shown in Table 6.

2.6.3.6 A COTS conformity inspection plan is used to screen COTS parts prior to installation. The intent of a conformity is to verify key features prior to installation and to ensure COTS part integrity and configuration consistency. The scope and detail of the conformity inspection is dependent on the COTS part classification as shown in Table 6.

Table 6: OSO #02 COTS evaluation criteria

COTS categories	COTS design assessment	COTS conformity inspection plan
Non-critical	Design assessment should confirm that the severity effect of any potential COTS failure condition is less than Minor and has been accounted for in the OSO #05 safety assessment.	The conformity inspection plan should: • show that the part is built as specified and to the correct configuration • show that there is no evidence of any defects or damage.
Major	Design assessment should confirm that the severity effect of any potential COTS failure condition is less than Major and has been accounted for in the OSO #05 safety assessment.	The conformity inspection plan should address the criticality of the COTS part. At a minimum, procedures: • show that the part is built as specified and to the correct configuration • show that there is no evidence of any defects or damage • verify safety critical dimensions, materials, and functional checks as needed.
Critical	Design assessment should confirm that any COTS failure condition with a potential Hazardous or Catastrophic severity effect has been accounted for in the OSO #05 safety assessment.	The conformity inspection plan should be sufficient to comply with the integrity requirements of the assigned SAIL as given in Table 2.

COTS categories	COTS design assessment	COTS conformity inspection plan
	In addition, the design assessment should determine if additional COTS acceptance testing is required to support applicable SAIL robustness criteria. If additional acceptance testing is required, then the test procedures and pass/fail criteria should be documented.	

2.6.3.7 In addition to configuration control, it is important that the risk of obsolescence be considered when selecting COTS parts. This includes gathering information on:

- existing configurations and versions of the COTS parts that are currently available
- future design and manufacturing changes that may be made by the manufacturer of the COTS parts.

2.6.3.8 Some options to minimise the risks of obsolescence and lack of configuration control may include:

- formal contract or arrangement with the manufacturer of the COTS parts
- procurement of COTS parts directly from the original manufacturer
- procurement of additional parts from the same manufacturing batch for future use.

3 OSO #03 – RPAS maintained by competent or proven entity

3.1 General

- 3.1.1 The objective of OSO #03 is to ensure the RPAS is kept in a condition for safe operation throughout its operational life through the execution of maintenance requirements and maintenance management processes by competent maintenance personnel and documented via the organizational and maintenance records.
- 3.1.2 The operator is responsible for demonstrating compliance with OSO #03. To support this, the RPAS designer should provide maintenance requirements, instructions and other technical data necessary for the operator to establish and maintain compliance.
- 3.1.3 This guidance material predominantly focuses on the information that should be provided by RPAS designers to support operators in demonstrating compliance with OSO #03. Further guidance specific to the operator is provided in [AC 101-01 Remotely piloted aircraft systems - licensing and operations](#), [AC 101-05 Functions and duties of RPAS maintenance controllers](#) and in other sections of [AC 101-06 - AusSORA – Assessment requirements and criteria](#).

3.2 Level of robustness

- 3.2.1 The required level of robustness for OSO #03 is specified in Table 7 and categorised as low (L), medium (M), or high (H), with corresponding SAIL.

Table 7: OSO #03 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	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 8 provides the criteria for different integrity levels for OSO #03.

Table 8: OSO #03 Level of integrity

Level of integrity	Criterion
Low	The RPAS Operator maintenance instructions and requirements are defined, cover (when applicable) the RPAS designer instructions and requirements, and are adhered to. The maintenance staff is competent and has received an authorisation to carry out RPAS maintenance.
Medium	The RPAS Operator maintenance instructions and requirements are defined, cover (when applicable) the RPAS designer instructions and requirements, and are adhered to. The maintenance staff is competent and has received an authorisation to carry out RPAS maintenance.

Level of integrity	Criterion
	Preventive/Scheduled maintenance/inspection of each RPAS is organized and in accordance with the RPAS Operator maintenance program on the basis of the RPAS designer scheduled maintenance requirements and adapted to the specificities of RPAS operations. Upon completion, the maintenance log system is used to record all maintenance conducted on the RPAS including releases. A release to service can only be accomplished by a staff member who has received an authorisation to release to service for that particular RPAS model/family.
High	The RPAS Operator maintenance instructions and requirements are defined, cover (when applicable) the RPAS designer instructions and requirements, and are adhered to. The maintenance staff is competent and has received an authorisation to carry out RPAS maintenance. Preventive/Scheduled maintenance/inspection of each RPAS is organized and in accordance with the RPAS Operator maintenance program on the basis of the RPAS designer scheduled maintenance requirements and adapted to the specificities of RPAS operations. Upon completion, the maintenance log system is used to record all maintenance conducted on the RPAS including releases. A release to service can only be accomplished by a staff member who has received an authorisation to release to service for that particular RPAS model/family. The maintenance staff works in accordance with a maintenance procedure manual that provides information and procedures relevant to the Operator maintenance facility, records, maintenance instructions, release, tools, material, components, defect deferral.

3.4 Level of assurance

3.4.1 The level of assurance must not be less than the required level of robustness. Table 9 presents the criteria for the different assurance levels for OSO #03.

Table 9: OSO #03 Level of assurance

Level of assurance	Criterion
Low	The RPAS Operator maintenance instructions are documented. The maintenance conducted on the RPAS is recorded in an RPAS technical log. A list of maintenance staff authorised to carry out maintenance is established and kept up to date.
Medium	The RPAS Operator maintenance instructions are documented. The maintenance conducted on the RPAS is recorded in an RPAS technical log.

Level of assurance	Criterion
	The RPAS Operator maintenance program layout is in accordance with standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA. A list of maintenance staff authorised to carry out maintenance is established and kept up to date. A list of maintenance staff with authorisation to release to service is established and kept up to date.
High	The RPAS Operator maintenance instructions are documented. The maintenance conducted on the RPAS is recorded in an RPAS technical log. The RPAS Operator maintenance program layout is in accordance with standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA. The Operator Maintenance Program and the maintenance procedures manual are validated by CASA. A list of maintenance staff authorised to carry out maintenance is established and kept up to date. A list of maintenance staff with authorisation to release to service is established and kept up to date.

3.5 Responsibilities of RPAS designers

3.5.1 Table 10 outlines the designer's responsibilities with varying levels of robustness for OSO #03.

Table 10: OSO #03 Responsibilities of RPAS designers

Level of robustness	Responsibilities
Low	The RPAS designer should make available technical data to enable the operator to establish the operator maintenance requirements and instructions demonstrating low level robustness.
Medium	The RPAS designer should make available technical data to enable the operator to establish the operator maintenance requirements and instructions demonstrating medium level robustness.
High	The RPAS designer should make available technical data to enable the operator to establish the operator maintenance requirements and instructions demonstrating high level robustness.

3.6 Guidance for RPAS designers

3.6.1 For the purposes of this guidance:

- Maintenance requirements are the maintenance tasks, intervals, life limits and applicability conditions that are necessary to maintain and service the RPAS to ensure continued safe operations throughout its defined operational life.
- Maintenance instructions are the technical information, procedures, and supporting data required to enable maintenance personnel to correctly perform the maintenance requirements.
- Maintenance program is developed by the operator as a structured system for planning, scheduling, controlling, recording, and reviewing the maintenance requirements for the RPAS.

3.6.2 The RPAS designer should make available maintenance requirements and maintenance instructions that enable operators to establish and maintain the evidence needed to demonstrate compliance with OSO #03.

3.6.3 These requirements and instructions should ensure the continued safe operation of the RPAS throughout its operational life.

3.6.4 The maintenance requirements and maintenance instructions provided by the RPAS designer are commonly referred to as instructions for continuing airworthiness (ICA).

3.6.5 Table 11 describes the expected data and related processes for each robustness level. It also identifies the evidence expected to be established by the operator, which relies on maintenance information provided by the RPAS designer.

Table 11: Maintenance content for different robustness levels

Concept	Low Robustness	Medium Robustness	High Robustness
Maintenance requirements	The maintenance requirements should include basic servicing and maintenance for safety-critical systems and components.	The operator maintenance requirements should include basic and preventive servicing and maintenance along with intervals for accomplishment. The maintenance requirements should identify those tasks that address safety-critical systems and components.	The operator maintenance requirements should include basic and preventive servicing and maintenance along with intervals for accomplishment. The maintenance requirements should identify those tasks that address safety-critical systems and components. The technical data should be developed using a documented engineering methodology, such as that described in OSO #05, appropriate to the complexity of the design.
Maintenance instructions	The instructions should be in English, unambiguous, and of a level of detail sufficient for maintenance	The instructions should be in English, unambiguous, and of a level of detail sufficient for maintenance	The instructions should be in English, unambiguous, and of a level of detail sufficient for maintenance

Concept	Low Robustness	Medium Robustness	High Robustness
	personnel to accomplish the maintenance requirements.	personnel to accomplish the maintenance requirements. The maintenance instructions should provide information to support maintenance personnel, such as a basic systems description, schematics, troubleshooting procedures, and configuration control. The level of detail should be appropriate for the complexity of the RPAS and the maintenance requirements.	personnel to accomplish the maintenance requirements. The maintenance instructions should provide information to support maintenance personnel, such as a basic systems description, schematics, troubleshooting procedures, and configuration control. The level of detail should be appropriate for the complexity of the RPAS and the maintenance requirements.
Maintenance programme	The operator maintenance program provides a planning and control mechanism to ensure the operator maintenance requirements are complied with. The operator may track the next due maintenance requirements via one or more log cards or other equivalent process. The operator's maintenance program may be less restrictive than the data from the RPAS designer suggests, provided that a justification has been documented by the operator.	The operator maintenance program provides a planning and control mechanism to ensure the operator maintenance requirements are complied with. The operator may need to supplement the use of log cards by introducing processes to ensure robust planning and control, configuration management, and defect management. The operator's maintenance program may be less restrictive than the data from the RPAS designer suggests, provided that a technical assessment has been done and documented by the operator that the deviation is unlikely to reduce safety margins.	The operator maintenance program provides a planning and control mechanism to ensure the operator maintenance requirements are complied with. The operator may need to supplement the use of log cards by introducing processes to ensure robust planning and control, configuration management, and defect management. The operator's maintenance program may be less restrictive than the data from the RPAS designer suggests, provided that a technical assessment has been done and documented by the operator that the deviation is unlikely to reduce safety margins, with agreement from the RPAS designer. The operator should review the maintenance program periodically to ensure that it is effective in ensuring safety of flight and make corrective changes where appropriate.

Concept	Low Robustness	Medium Robustness	High Robustness
Maintenance personnel competency	The operator should be satisfied that maintenance personnel are sufficiently competent to carry out the maintenance instructions. Competency should be based on adequate technical knowledge of the RPAS and applicable maintenance tasks and may further be based on appropriate training.	The operator should ensure that maintenance personnel are sufficiently competent to carry out the maintenance instructions. Competency should be based on adequate technical knowledge of the RPAS and applicable maintenance tasks, supported by appropriate training or experience. The maintenance personnel authorised to release the RPAS to service should have sufficient knowledge and understanding of the operator's maintenance program.	The operator should ensure that maintenance personnel are sufficiently competent to carry out the maintenance instructions. Competency should be based on adequate technical knowledge of the RPAS and applicable maintenance tasks, supported by demonstrated and appropriate training or experience. The maintenance personnel authorised to release the RPAS to service should have sufficient knowledge and understanding of the operator's maintenance program.

3.6.6 Maintenance requirements

- 3.6.6.1 The RPAS designer should establish and document the maintenance requirements necessary to support the continued safe operation of the RPAS throughout its operational life.
- 3.6.6.2 The maintenance requirements should identify, as applicable, matters including, but not limited to:
- scheduled maintenance tasks and intervals
 - scheduled servicing tasks and intervals
 - inspection requirements and intervals;
 - functional checks and testing requirements;
 - component life limitations
 - overhaul, restoration or replacement requirements and intervals
 - maintenance-critical items and tasks
 - software and firmware configuration requirements;
 - calibration and rigging requirements;
 - conditional inspections following abnormal events (such as. hard landing, impact or lightning strike)
 - any other maintenance requirements necessary to support the continued safe operation of the RPAS.
- 3.6.6.3 The designer should identify any maintenance requirements that are mandatory because failure to accomplish them could adversely affect the continued safe operation or approved configuration of the RPAS.

- 3.6.6.4 Mandatory maintenance requirements should be clearly distinguished from recommended maintenance activities to ensure operators can readily identify those requirements necessary to preserve the approved configuration and continued safe operation of the RPAS.

3.6.7 Maintenance instructions

- 3.6.7.1 The RPAS designer should provide maintenance instructions containing the procedures, technical data and supporting information necessary for maintenance personnel to correctly perform the maintenance tasks.
- 3.6.7.2 As applicable, the maintenance instructions should include:
- maintenance procedures
 - inspection methods and acceptance criteria
 - servicing procedures
 - repair instructions and limitations
 - troubleshooting procedures
 - testing and functional check procedures
 - required tools, equipment and consumables
 - system descriptions, functions and schematics
 - configuration management procedures
 - software and firmware installation procedures
 - maintenance release procedures.
- 3.6.7.3 The designer should validate the maintenance requirements and instructions to ensure they adequately support the reliability and safe operation of the RPAS.

4 OSO #04 – RPAS components essential to safe operations are designed to an airworthiness design standard

4.1 General

- 4.1.1 The intent of OSO #4 is to ensure that RPAS and its components have been designed to contribute to the required overall safety objective through compliance with appropriate airworthiness design standards (ADS).
- 4.1.2 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.

4.2 Level of robustness

- 4.2.1 The required level of robustness for OSO #04 is specified in Table 12 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 12: OSO #04 Level of robustness

SAIL	I	II	III	IV	V	VI
Robustness	O	O	O	L	M	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 #04.

Table 13: OSO #04 Level of integrity

Level of integrity	Criterion
Low	The RPAS 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 RPAS 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 RPAS 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.

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 #04.

Table 14: 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.

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 #04.

Table 15: OSO #04 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	a. 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. b. The applicant submits the established compliance summary along with a declaration of compliance demonstrating low-level robustness. c. The applicant demonstrates that the design is appropriate for an overall safety objective of 10^{-4}/FH for a SAIL IV operation. d. The applicant conducts function and reliability flight tests in a manner acceptable to CASA. e. 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	a. 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 operation conditions. b. The applicant submits the established compliance summary along with a declaration of compliance demonstrating medium-level robustness. c. The applicant demonstrates that the design is appropriate for an overall safety objective of 10^{-5}/FH for a SAIL V operation. d. The applicant conducts 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 and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. 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	- 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. - The applicant submits the established compliance summary along with a declaration of compliance demonstrating high-level robustness. - The applicant demonstrates that the design is appropriate for an overall safety objective of 10^{-6}/FH for a SAIL VI operation. - The applicant conducts 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 and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. 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 Airworthiness design standards

- 4.6.1.1 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, should meet to be considered safe for the intended flight operation.
- 4.6.1.2 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.
- 4.6.1.3 An adequate ADS should 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).
 - **Aircraft flight manual:** Requirements for the development of an aircraft flight manual that provides clear operating limitations, procedures, performance information, and instructions necessary to ensure the safe operation of the RPAS throughout its intended operational envelope.

- **Maintenance manual:** Requirements for the development of a maintenance manual that provides instructions for inspection, servicing, repair, testing, and continued airworthiness activities necessary to ensure the RPAS remains in a safe and serviceable condition throughout its operational life.

4.6.1.4 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.

4.6.1.5 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.

4.6.1.6 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.

4.6.1.7 CASA may accept an ADS proposed by an applicant other than listed in Paragraph 4.6.1.4 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.

4.6.1.8 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.

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.

4.6.2 Applicability and relationship to other OSO

- 4.6.2.1 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).
- 4.6.2.2 When another OSO covers any aspect of the ADS, the requirement of that OSO takes precedence over the ADS requirement.
- 4.6.2.3 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.
- 4.6.2.4 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.

4.6.3 Compliance basis

- 4.6.3.1 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 overall safety objective for the intended operation.
- 4.6.3.2 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.
- 4.6.3.3 The compliance basis should 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.
- 4.6.3.4 Any tailoring to an ADS should be clearly documented and justified by an appropriate technical rationale and be accepted by CASA.

4.6.4 Compliance summary

- 4.6.4.1 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.
- 4.6.4.2 [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, (such as 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 (such as 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
- 4.6.4.3 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.
- 4.6.4.4 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.
- 4.6.4.5 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.
- 4.6.4.6 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.
- 4.6.4.7 Table 16 provides guidance on the methods of compliance that can be used.

Table 16: Methods of compliance

Method	Explanation	Examples
Analysis	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. It is used in the design phase to predict structural, aerodynamic, or system performance without requiring physical prototypes.	- 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.

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
Test	It is a physical evaluation of a product, system, or component under controlled conditions to verify it meets performance requirements. It is used to prove compliance conclusively by showing that the real-world behaviour matches the expectation.	• 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	Inspection is the visual, dimensional, or non-destructive examination of aircraft parts and assemblies.	• Verifying the correct assembly of electrical wiring. • Visual inspection of rotor blades for cracks or delamination. • 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.	• 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.	• 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 for systems where single failures do not result in catastrophic consequences.	• 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	Used to validate operational suitability in safe, simulated environments. 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 should be validated.	• Virtual testing of detect-and-avoid algorithms using digital twins. • Demonstrating swarm coordination in a simulator before real flight testing.

4.6.5 Experimental flight tests

4.6.5.1 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.

- 4.6.5.2 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.
- 4.6.5.3 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.
- 4.6.5.4 CASA [AC 21-47 - Flight test safety](#) covers topics such as test planning principles, hazard analysis and risk management.

4.6.6 Function and reliability flight test program

- 4.6.6.1 CASA requires RPAS manufacturers to demonstrate function and reliability for the intended purposes through an appropriate program of flight testing.
- 4.6.6.2 For the purposes of this guidance, function means that the RPAS, its systems, and equipment perform their intended behaviour without introducing safety hazards. Reliability means that the RPAS, its systems, and equipment continue to perform those functions consistently in service.
- 4.6.6.3 Function and reliability flight tests should be conducted for the number of hours agreed with CASA under a flight test plan to specific RPAS make, model and configuration.
- 4.6.6.4 The flight test plan should 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.
- 4.6.6.5 Testing should be completed without experiencing any failure that could result in loss of flight, loss of control, or an unplanned landing.
- 4.6.6.6 Prior to the function and reliability testing, designers should perform experimental flight tests to show compliance with the requirements if it is stated as a method of compliance in the compliance summary.

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

5.1 General

- 5.1.1 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.
- 5.1.2 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.

5.2 Level of robustness

- 5.2.1 The required level of robustness for OSO #05 is specified in Table 17 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 17: OSO #05 Level of robustness

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

5.3 Level of integrity

- 5.3.1 The level of integrity must not be less than the required level of robustness. Table 18 provides the criteria for different integrity levels for OSO #05.

Table 18: 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	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. 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. No single failure can lead to a catastrophic failure condition.

5.4 Level of assurance

5.4.1 The level of assurance must not be less than the required level of robustness. Table 19 presents the criteria for the different assurance levels for OSO #05.

Table 19: 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	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. System safety assessments are conducted in accordance with means of compliance acceptable to CASA. Appropriate development assurance activities are performed for critical functions implemented by SW or CEH to ensure safety objectives are met.
High	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. System safety assessments are conducted in accordance with means of compliance acceptable to CASA. Appropriate development assurance activities are performed for critical functions implemented by SW or CEH to ensure safety objectives are met. Supporting safety assessment and development assurance activities are validated by CASA.

5.5 Means of compliance

5.5.1 Table 20 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #05.

Table 20: OSO #05 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	a. FHA and DIA are available for review. b. The applicant follows an appropriate system safety assessment methodology acceptable to CASA, such as - 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	a. FHA, DIAs, and supporting safety analyses are available for review. b. The applicant follows an appropriate system safety assessment methodology acceptable to CASA, such as - 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	a. FHA, DIAs, and supporting safety 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.

5.6 Additional guidance

5.6.1 Applicability and relationship to other OSOs

5.6.1.1 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.

- 5.6.1.2 The safety and reliability considerations of OSO #05 also 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.
- 5.6.1.3 For SAIL III, designers should evaluate the basic aircraft-level structural integrity and flight performance and handling aspects of the aircraft as part of OSO #05 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 DIA.
- 5.6.1.4 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.
- 5.6.1.5 Where an aircraft is fitted with payloads or similar internal or external systems, OSO #05 is also applicable to these systems and their installations.
- 5.6.1.6 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.
- 5.6.1.7 Compliance with OSO#05 safety objectives may be considered in conjunction with the containment safety requirements and ground risk mitigation requirements, if applicable.
- 5.6.1.8 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](#).

5.6.2 Functional hazard assessment (FHA)

- 5.6.2.1 An FHA is defined as a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity³.
- 5.6.2.2 The FHA serves as a key 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 and ensure that the safety objectives are achieved. Since safety assessment is an iterative process, the design is continually reassessed and refined until the required level of safety is achieved.
- 5.6.2.3 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.
- 5.6.2.4 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.
- 5.6.2.5 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.
- 5.6.2.6 Designers should minimise each identified hazard to an acceptable level based on the severity of the failure condition.

³ Definition from SAE ARP4761A.

- 5.6.2.7 Section B.2 of Appendix B contains an FHA template acceptable to CASA and provides an example FHA for reference.

5.6.3 Failure conditions and severity classifications

- 5.6.3.1 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)
 - loss of indication
 - uncommanded or unintended behaviour.
- 5.6.3.2 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.
- 5.6.3.3 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 21 identifies the severity class associated with different aircraft and crew effects.

Table 21: 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.

- 5.6.3.4 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.
- 5.6.3.5 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.
- 5.6.3.6 Two critical design principles incorporated into safety assessment process as mitigations are redundancy and fail-safe design.
- 5.6.3.7 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.

- 5.6.3.8 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.
- 5.6.3.9 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.
- 5.6.3.10 Each severity classification is associated with an allowable probability, as discussed in section 5.6.4. 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.

5.6.4 Allowable probabilities and design assurance levels

- 5.6.4.1 The SORA methodology establishes an acceptable target level of safety (TLOS) of $10^{-6}/\text{FH}$ (i.e., 1 fatality per 1,000,000 flight hours) across all levels of SAIL.
- 5.6.4.2 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.
- 5.6.4.3 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 ($L = 10^{-3}/\text{FH}$), whereas a SAIL IV operation requires a stricter rate of one failure per 10,000 flight hours ($L = 10^{-4}/\text{FH}$). Consequently, aircraft systems must be designed to be ten times more reliable to achieve the TLOS for each increase in SAIL.
- 5.6.4.4 Table 22 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 B.1 of Appendix B.

Table 22: 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 $L=10^{-6}$ $P_f=1$	No probability or FDAL requirement	$<10^{-3}$ No FDAL requirement	$<10^{-5}$ FDAL D	$<10^{-6}$ FDAL C	$<10^{-7}$ FDAL B

Failure Condition Classification	No Effect	Minor	Major	Hazardous	Catastrophic
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
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 $Pf \leq 10^{-4}$	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 = $L \cdot Pf = 10^{-6}$ for all SAIL (SAIL I - SAIL VI)

L = Operational failure rate (loss of aircraft)

Pf = Probability of fatality, given operational failure (loss of aircraft)

- 5.6.4.5 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.
- 5.6.4.6 Each specific failure condition must meet the probability target defined in Table 22. If there is a probability requirement, probability of each:
- Minor failure condition must be less than probable.
 - Major failure condition must be less than remote.
 - Hazardous failure condition must be less than extremely remote.
 - Catastrophic failure condition must be extremely improbable.
- 5.6.4.7 As indicated in Table 22, 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.
- 5.6.4.8 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.
- 5.6.4.9 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.
- 5.6.4.10 At SAIL IV, development assurance for SW and CEH is only required for catastrophic failure conditions and is proportionately limited to FDAL D, the level typically applied to minor failure conditions in the type certification of normal category (Part 23) aircraft.
- 5.6.4.11 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.

- 5.6.4.12 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 should allocate those functions to at least two different items (such as, redundancy) and demonstrate the absence of common cause failures.

5.6.5 System safety assessment

- 5.6.5.1 The system safety assessments (SSA) are intended to evaluate proposed architectures, identify safety requirements and verify the implemented design meets safety objectives and requirements.
- 5.6.5.2 System safety assessment methods, including the DIA, should be applied to show hazards are minimised to an acceptable level (and in accordance with the allowable quantitative probability values in Table 22, where applicable) as part of the FHA process. CASA recommended safety assessment methods are discussed further in Appendix B.3.
- 5.6.5.3 The safety assessment process for OSO #5 is outlined in Figure 1.

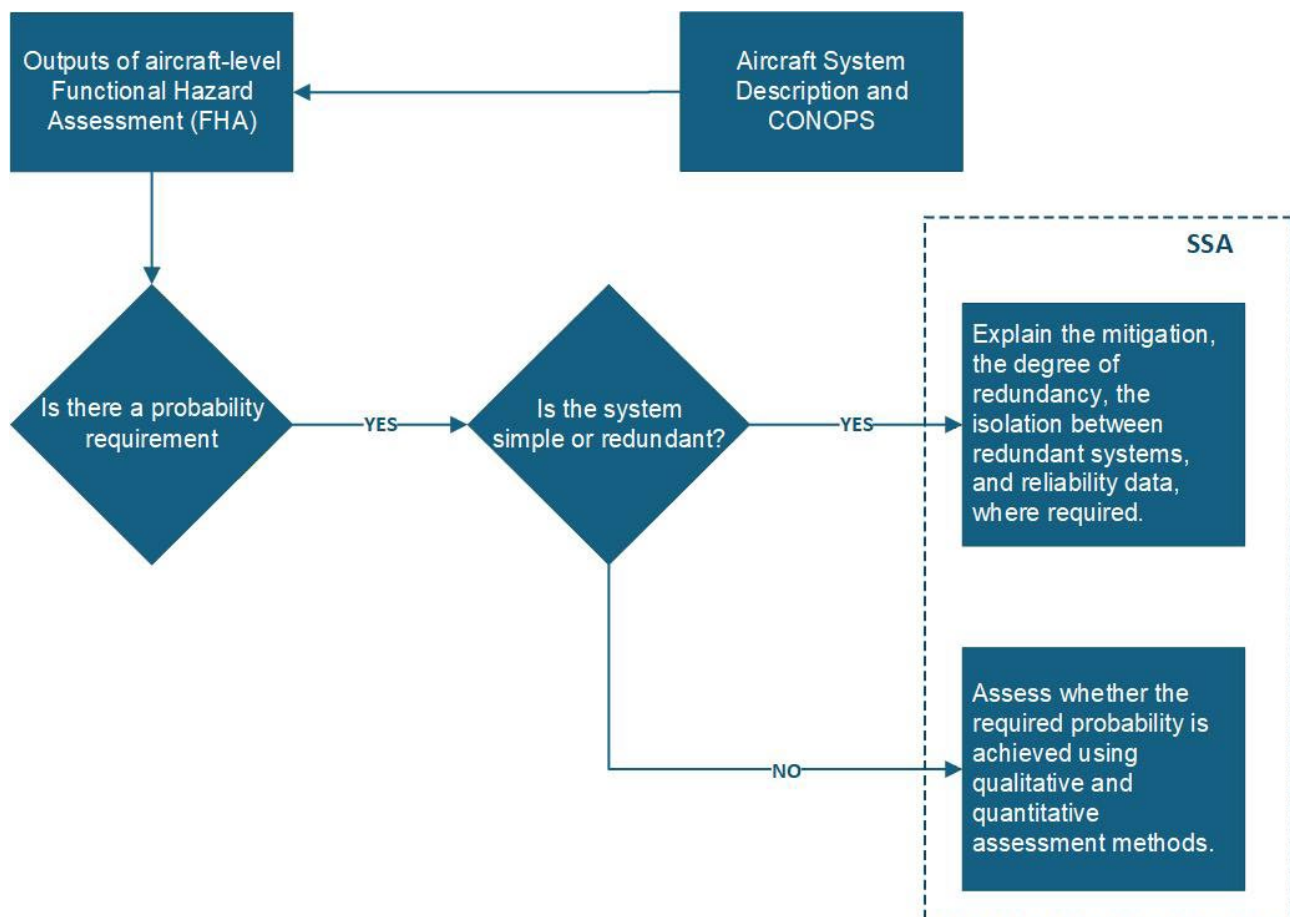


Figure 1: Simplified safety assessment process for OSO #05

- 5.6.5.4 As part of the system safety assessments, designers should 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.

- 5.6.5.5 Even with redundant systems, designers should consider the total loss of a function. In such systems, redundancy may be used to reduce the probability of total loss, but it does not change the inherent severity classification.
- 5.6.5.6 If the RPAS has a PRS, credit can be taken for the existence of a PRS because loss of the aircraft would require the loss of both the PRS and another critical system or function. The probability of both failures occurring; however, would still have to be accounted for in an accompanying qualitative or quantitative assessments.
- 5.6.5.7 A common cause failure (CCF), which occurs when two or more supposedly independent systems fail simultaneously due to a shared cause, should consider the independence requirements.
- 5.6.5.8 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.
- 5.6.5.9 To declare compliance with OSO#05, the designer must confirm that all system safety objectives and independence requirements are satisfied.

5.6.6 Design and installation appraisal

- 5.6.6.1 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.
- 5.6.6.2 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.
- 5.6.6.3 DIA should be used to verify that all requirements coming from the FHA are satisfied.
- 5.6.6.4 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.
- 5.6.6.5 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.
- 5.6.6.6 When forming an appraisal is not possible without additional assessment, qualitative or quantitative 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.

5.6.7 System safety assessment process and methods

- 5.6.7.1 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 objectives can be achieved. 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.
- 5.6.7.2 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.

- 5.6.7.3 Reliability record of the technology, systems developed per standards, and satisfactory service experience on the same or similar systems are examples of the rationale used to support simple system assessment.
- 5.6.7.4 Similar approaches may be used for a complex system with more rigorous analysis and based on experienced engineering judgement.
- 5.6.7.5 For a qualitative FTA, designers should structure the fault tree without assigning numeric rates. They can stop at the logical structure to show that the architecture is acceptable by:
 - identifying single points of failure
 - identifying combinations of failures that lead to the top event
 - demonstrating independence of redundancies.
- 5.6.7.6 Similarly, a qualitative FMEA can be used to show coverage of failure effects and to ensure no overlooked hazards by:
 - identifying all failure modes of each component
 - describing their effects on the system
 - showing whether they lead to hazardous/catastrophic failure conditions.
- 5.6.7.7 For CCA, designers should identify all common causes and list mitigations such as architectural separation, shielding, and system reliability.
- 5.6.7.8 Quantitative safety analyses aim to show that the probability of hazardous and catastrophic events is below the target thresholds provided in Table 22. They provide measurable, numerical evidence of safety compliance to meet safety objective.
- 5.6.7.9 For a quantitative safety analyses, designers should perform a qualitative safety analysis first and have a valid model to analyse, such as an FTA and FMEA. This is followed by providing validated numerical reliability data. For example, designers should assign failure rates to basic events in FTAs and then compute the probability of the top event to show compliance with the target levels.
- 5.6.7.10 Numerical reliability relies on data such as failure rates of hardware, mean time to failures (MTTF) data, and error probabilities. The data should be shown to be applicable and come from a reliable source.
- 5.6.7.11 Further guidance on recommended system safety analyses is provided in Appendix B.3.

5.6.8 Demonstrating system safety and reliability through flight test

- 5.6.8.1 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.
- 5.6.8.2 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.
- 5.6.8.3 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.
- 5.6.8.4 Section 4.6.5 of this Annex provides guidance on conducting experimental flight tests in Australia.

6 OSO #06 – C3 link characteristics are appropriate for the operation

6.1 General

- 6.1.1 The intent of OSO #06 ensures that the selected C3 links, necessary for the safety of flight, are suitable for the intended operation by demonstrating that it provides the required communication performance under the expected operating and environmental conditions.
- 6.1.2 This guidance is intended for RPAS designers. It provides guidance for demonstrating that the selected C3 links are appropriate for the intended operations. The guidance for operators is provided in other sections in AC 101-06.

6.2 Level of robustness

- 6.2.1 The required level of robustness for OSO #06 is specified in Table 23 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 23: OSO #06 Level of robustness

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

6.3 Level of integrity

- 6.3.1 The level of integrity must not be less than the required level of robustness. Table 24 provides the criteria for different integrity levels for OSO #06.

Table 24: OSO #06 Level of integrity

Level of integrity	Criterion
Low	The applicant determines that performance, RF spectrum usage and environmental conditions for C3 links are adequate to safely conduct the intended operation. The RPAS remote pilot has the means to continuously monitor the C3 performance and ensures the performance continues to meet the operational requirements.
Medium	The applicant determines that performance, RF spectrum usage and environmental conditions for C3 links are adequate to safely conduct the intended operation. The RPAS remote pilot has the means to continuously monitor the C3 performance and ensures the performance continues to meet the operational requirements.
High	The applicant determines that performance, RF spectrum usage and environmental conditions for C3 links are adequate to safely conduct the intended operation. The RPAS remote pilot has the means to continuously monitor the C3 performance and ensures the performance continues to meet the operational requirements. The use of licensed frequency bands for C2 Link is required.

6.4 Level of assurance

6.4.1 The level of assurance must not be less than the required level of robustness. Table 25 presents the criteria for the different assurance levels for OSO #06.

Table 25: OSO #06 Level of assurance

Level of assurance	Criterion
Low	The applicant declares that the required level of integrity has been achieved.
Medium	Demonstration of the C3 link performance is in accordance with standards considered adequate by CASA or in accordance with means of compliance acceptable to CASA.
High	Demonstration of the C3 link performance is in accordance with standards considered adequate by CASA or in accordance with means of compliance acceptable to CASA. Evidence is validated by CASA.

6.5 Means of compliance

6.5.1 Table 26 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #06.

Table 26: OSO #06 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	a. The applicant should demonstrate that the selected C3 link is suitable for its intended purpose by showing that: - i the performance characteristics support safe operation - ii the link provides an appropriate level of reliability - iii degradation and loss-link conditions have been addressed - iv monitoring capabilities enable timely detection of unsafe conditions - v any limitations and assumptions have been identified. b. 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	a. The applicant should demonstrate that the selected C3 link is suitable for its intended purpose by showing that: - i the performance characteristics support safe operation - ii the link provides an appropriate level of reliability - iii degradation and loss-link conditions have been addressed - iv monitoring capabilities enable timely detection of unsafe conditions - v any limitations and assumptions have been identified. b. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. 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	a. The applicant should demonstrate that the selected C3 link is suitable for its intended purpose by showing that: - i the performance characteristics support safe operation - ii the link provides an appropriate level of reliability - iii degradation and loss-link conditions have been addressed - iv monitoring capabilities enable timely detection of unsafe conditions - v any limitations and assumptions have been identified. b. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

6.6 Additional guidance

6.6.1 For the purpose of this OSO, a C3 link includes the Command and Control (C2) link and any communication link required for the safety of flight.

6.6.2 Relationship to safety analyses

- 6.6.2.1 This OSO works in conjunction with OSO #05 (when required by the SAIL). OSO #05 manages the holistic system safety assessment, assigning development assurance requirements and quantitative reliability requirements based on the severity of events due to system functional failure for the entire aircraft system. This includes both the assurance of function and system performance when operating as intended (i.e. the ability to complete successfully the function assigned), and the ability to manage function and system degradation to an acceptable level.
- 6.6.2.2 OSO #06 refines the potential multitude of methods to achieve functional, safe, and reliable C3 links by providing more detailed requirements related to the development of the C3 links.
- 6.6.2.3 The severity determination is driven from the intended functionality of the C3 link, and the intended SAIL of the operation. It is therefore critical to clearly define the intended function and intended operational environment of any C3 links.
- 6.6.2.4 OSO #05 should drive the severity of a loss of C3 links for SAIL III and higher operations.
- 6.6.2.5 For SAIL II operations, an operational hazard analysis should be undertaken for the C3 links used as part of the operation. This analysis should identify any C3 link whose loss of function could lead to a loss of control of the operation, or, whose failure, if undetected, could result in a latent single point of failure leading to a loss of control of the operation.
- 6.6.2.6 Through the safety analyses in OSO #05, or hazard analysis for SAIL II intended operations, the role of each C3 link and the communication architecture used to support it should be assessed. The assessment should identify the allocation of functions between the aircraft, control station and supporting infrastructure, as well as intended contingency actions or procedures to manage a detected loss of link before or during a transaction. This assessment should result in the allocation of four core safety metrics to each of the C3 links:
- **Maximum transaction time:** the maximum allowable time for the communication transaction to be completed. Once this time expires, alternative or contingency actions should be implemented.
 - **Availability:** The probability that an operational communication transaction can be initiated when needed.

- **Continuity:** The probability that an operational communication transaction can be completed within the maximum transaction time.
- **Integrity:** The probability that one or more undetected errors are transmitted in a communication transaction completed within the maximum transaction time.

6.6.2.7 For each C3 link, the required maximum transaction time should be driven by the timings required by the functionality itself. For example, direct flying of the aircraft needs to occur within a relatively short time period, whereas updates to flight plans due to weather will likely only need much longer times before a contingency is activated.

6.6.3 C3 link design, test and evaluation

- 6.6.3.1 At this stage, the data required to demonstrate that each C3 link can achieve the four-core metrics defined above should be determined. This may include, but is not limited to, the communication technologies used, RF spectrum employed, any environmental or operational factors that may affect link performance, including degraded or lost-link conditions.
- 6.6.3.2 For any claims of availability and continuity, it is necessary that there be methods to monitor the link to detect the inability to start or complete a communication transaction. It is expected that monitoring is included as part of the design regardless of the link reliability.
- 6.6.3.3 The applicant should demonstrate that the selected C3 links provide adequate communication performance for both the data being exchanged and the functions being supported.
- 6.6.3.4 The performance assessment should consider the communication system as a whole, including:
- the communication architecture and technologies used
 - channel coding techniques used
 - the RF spectrum used and any associated spectrum authorisation requirements
 - aircraft and ground installation characteristics, in particular the intended transceiver locations, gain patterns, masking issues, and directionality/pointing requirements
 - expected operating range and coverage
 - environmental conditions and susceptibility to interference
 - foreseeable degradation mechanisms.
- 6.6.3.5 Depending on the required communication performance, operating environment and SAIL, either licensed or unlicensed spectrum may be suitable, provided the applicant demonstrates that the selected communication solution satisfies the established performance requirements.
- 6.6.3.6 In general, but particularly where unlicensed spectrum is used, appropriate interference mitigation measures (such as code division multiple access (CDMA) or frequency diversity techniques) should be implemented where necessary.
- 6.6.3.7 Where direct radio links are used, the assessment should consider communication performance throughout the operational envelope, including:
- link margin
 - antenna characteristics
 - free-space path loss
 - terrain and obstacle effects (including Fresnel zone clearance)
 - weather effects
 - expected interference sources.
- 6.6.3.8 Where cellular, satellite or other network-based communication technologies are used, the assessment should consider:

- network coverage and availability
- dependence on external communication service providers, which may require agreements between the operator and an external service provider
- communication latency
- infrastructure failures
- interference detection and mitigation
- network security.

6.6.3.9 The applicant should demonstrate that the remote pilot is able to determine when communication performance no longer supports safe operation. This may be achieved through:

- received signal-strength indication (RSS)
- link-quality monitoring
- communication status monitoring
- alerts for degraded performance or impending loss of link.

6.6.3.10 For low level of robustness, signal-strength monitoring and warning alerts may be sufficient. Applications requiring more demanding communication performance may require additional monitoring parameters.

6.6.3.11 Performance requirements may be established using recognised standards, engineering analysis, modelling and simulation, flight testing, service history, manufacturer data, or an appropriate combination of these methods.

6.6.3.12 The designer should provide operators with sufficient information in flight manuals to determine whether the C3 link is suitable for the intended operation. This information should describe the supported functions, system architecture, communication technologies, performance characteristics, spectrum requirements, monitoring provisions, operational limitations, environmental constraints and lost-link behaviour together with any associated procedures.

6.6.4 Demonstrating C3 link suitability

6.6.4.1 Because communication solutions vary significantly in technology, architecture and operating environment, prescriptive performance values may not be appropriate in all cases.

6.6.4.2 The applicant should demonstrate that the selected C3 link is suitable for its intended purpose by showing that:

- the performance characteristics support safe operation
- the link provides an appropriate level of reliability
- degradation and loss-link conditions have been addressed
- monitoring capabilities enable timely detection of unsafe conditions
- any limitations and assumptions have been identified.

6.6.4.3 For any demonstration of availability or continuity requirements, this should also demonstrate that the contingency actions, regardless of what they are, are effective at managing the loss of link performance.

7 OSO #07 – Conformity check of the RPAS to ensure consistency to the ConOps

7.1 General

- 7.1.1 The objective of OSO #07 is for the operator to ensure that the configuration of the RPAS intended for the operation conforms to the RPAS design data considered during the SORA approval process. Therefore, the operator is responsible for demonstrating compliance.
- 7.1.2 The integrity criterion is the same for all robustness levels. The operator must have RPAS conformity check procedures that periodically verify that:
- the RPAS intended to be used for the operation is in a condition for safe operation
 - the RPAS configuration conforms to the RPAS design data, including any design limitations (for example, maximum payload weight), considered under the approved concept of operations.
- 7.1.3 While the operator is responsible for demonstrating compliance, the RPAS designer and manufacturer are responsible for providing the information necessary for the operator to establish conformity check procedures.
- 7.1.4 It is important to note that any changes to the design, either via modification or repair, may constitute a change in configuration and should be considered as part of OSO #7 conformity checks.
- 7.1.5 This material focuses on guidance for RPAS designers and manufacturers.

7.2 Guidance for RPAS designers and manufacturers

- 7.2.1 Designers and manufacturers should provide operators with configuration baseline information to identify the configuration considered in the SORA approval process and verify ongoing conformity with that configuration. The configuration baseline should reflect the RPAS design data considered under the approved concept of operations and SORA assessment.
- 7.2.2 This information may include details of identified hardware, software, structural components, equipment, parts, limitations, and any other configuration items necessary to ensure safe operation.
- 7.2.3 The configuration baseline should identify the software and firmware versions, together with any associated configuration settings considered in the SORA approval process necessary to maintain conformity.
- 7.2.4 Designers and manufacturers should establish processes to monitor operational experience, service data, occurrences, defects, failures, malfunctions, and other safety-related information relevant to the RPAS design. This information should be regularly reviewed to determine whether design or configuration changes are necessary to maintain an acceptable level of safety.
- 7.2.5 This approach provides a mechanism for maintaining configuration conformity and addressing safety-related design issues identified after operational approval.
- 7.2.6 Particular attention should be given to parts, systems, software, equipment and functions whose failure, malfunction, or degradation could adversely affect the safe RPAS operation or invalidate assumptions and mitigations relied upon in the approved concept of operations.

- 7.2.7 Where a design deficiency, unsafe condition, or other safety concern is identified, the designer or manufacturer should assess the need for corrective action. Corrective actions may include changes to hardware, software, structural components, equipment, parts, operating limitations, inspections, or maintenance requirements.
- 7.2.8 Classification of repairs and modifications may be used in determining the appropriate level of assessment, implementation and corrective actions.

7.2.9 Classification of repairs and modifications

- 7.2.9.1 Repairs and modifications should be classified according to their potential effect on the safe RPAS operation and the validity of the approved configuration baseline.
- 7.2.9.2 A repair or modification may be considered minor where it has no appreciable effect on safety, system functionality, reliability, performance, operating limitations, or the assumptions and mitigations relied upon for the operational approval.
- 7.2.9.3 A repair or modification should be considered major where it may affect the safe RPAS operation, alter the configuration baseline, affect parts, systems or functions relied upon to support the approved concept of operations, introduce new hazards, or invalidate assumptions, limitations, or mitigations associated with the approved concept of operations.
- 7.2.9.4 A major design change should be considered significant where it alters the overall RPAS configuration, introduces a new system architecture or operational capability that requires substantial reassessment of the safety evidence supporting the approval.
- 7.2.9.5 In determining the classification of a repair or modification, the focus should be on the safety impact and operational consequences of the change rather than the nature of the design activity itself. Consideration should be given to effects on structural integrity, flight characteristics, operating limitations, software, hardware, equipment, system functionality, reliability, and any safety assumptions or mitigations relied upon in the operational approval.
- 7.2.9.6 Further guidance on the classification of design changes is provided in [AC 21-12 Classification of design changes](#).

7.2.10 Communication with CASA and operators after approval

- 7.2.10.1 Where a change is necessary to address a safety concern, the designer or manufacturer should notify affected operators and CASA, as appropriate, and provide sufficient information to enable implementation of the required corrective action.
- 7.2.10.2 Where a change in hardware, firmware or software may change the configuration of an aircraft in operation, for example, a software or firmware update pushed to extant systems used in operation, the designer or manufacturer should inform operators of the change, allowing operators to undertake the conformity inspection to validate the new configuration meets the safety case.
- 7.2.10.3 Even where a design change has not yet been developed or implemented, any significant safety concern should be communicated to CASA and affected operators without undue delay.

8 OSO #18 – Automatic protection of the flight envelope from human error

8.1 General

- 8.1.1 The flight envelope defines the performance boundaries of the RPA to ensure safe operation within the structural limits, controllability, manoeuvrability, and system operating limitations of the RPA.
- 8.1.2 Automatic flight envelope protection is intended to prevent the remote pilot from operating the RPA outside its defined safe operating limits.
- 8.1.3 This OSO is not applicable where the applicant demonstrates that the remote pilot is not directly involved in the flight control loop, such as during highly automated operations, pre-programmed flight operations, or operations where the remote pilot performs only high-level supervisory functions.
- 8.1.4 Where OSO #18 is not applicable, applicants should demonstrate that the remote pilot is not directly involved in the control loop (section 8.5).

8.2 Level of robustness

- 8.2.1 The required level of robustness for OSO #18 is specified in Table 27 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 27: OSO #18 Level of robustness

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

8.3 Level of integrity

- 8.3.1 The level of integrity must not be less than the required level of robustness. Table 28 provides the criteria for different integrity levels for OSO #18.

Table 28: OSO #18 Level of integrity

Level of integrity	Criterion
Low	The RPAS incorporates automatic protection of the flight envelope to prevent the remote pilot from making any single input under normal operating conditions that would cause the RPA to exceed its flight envelope or prevent it from recovering in a timely fashion.
Medium	The RPAS incorporates automatic protection of the flight envelope to ensure the RPA remains within the flight envelope or ensures a timely recovery to the designed operational flight envelope, following foreseeable single or multiple remote pilot errors under normal, abnormal, and emergency operating conditions.
High	The RPAS incorporates automatic protection of the flight envelope to ensure the RPA remains within the flight envelope or ensures a timely recovery to the

Level of integrity	Criterion
	designed operational flight envelope, following foreseeable single or multiple remote pilot errors under normal, abnormal, and emergency operating conditions.

8.4 Level of assurance

8.4.1 The level of assurance must not be less than the required level of robustness. Table 29 presents the criteria for the different assurance levels for OSO #18.

Table 29: OSO #18 Level of assurance

Level of assurance	Criterion
Low	The automatic protection of the flight envelope has been developed in-house or out of the box (such as, using Commercial Off the Shelf elements), using engineering best practices.
Medium	The automatic protection of the flight envelope has been developed to standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA.
High	The automatic protection of the flight envelope has been developed to standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA. Evidence is validated by CASA.

8.5 Means of compliance

8.5.1 Table 30 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #18.

Table 30: OSO #18 Means of compliance

Level of robustness	Evidence requirement and assessment process
Not Applicable	The applicant declares, in a form and manner acceptable to CASA, that the RPAS incorporates a flight control architecture in which the remote pilot is not directly involved in the control loop during operation. CASA may request supporting evidence to substantiate the applicability claim.
Low	- The RPAS incorporates automatic flight envelope protection functions intended to prevent unsafe exceedance of safety-critical flight parameters resulting from foreseeable single remote pilot input errors during a normal operation. - The flight envelope protection functions may be implemented using commercially available or in-house systems without formal development assurance standards. - Compliance is demonstrated through functional analysis, simulation, and representative flight testing showing that foreseeable pilot input errors do not result in unsafe flight conditions or loss of control. - 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

Level of robustness	Evidence requirement and assessment process
	supporting evidence for assessment.
Medium	a. The RPAS incorporates automatic flight envelope protection functions that ensure the medium level of integrity criteria is achieved. b. The automatic flight envelope protection functions are developed, integrated, and verified by standards, methods and processes acceptable to CASA. c. Compliance is demonstrated through documented analysis, simulation, ground testing, and representative flight testing covering foreseeable pilot-error scenarios and abnormal operational conditions. d. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.
High	a. The RPAS incorporates automatic flight envelope protection functions that ensure the high level of integrity criteria is achieved. b. The automatic flight envelope protection functions are developed, integrated, and verified by standards, methods and processes acceptable to CASA. c. Compliance is demonstrated through comprehensive analysis, simulation, hardware/software integration testing, and representative flight testing across the operational envelope, including degraded and worst-case operational scenarios. d. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

8.6 Additional guidance

- 8.6.1 The flight envelope limits are derived from substantiated aerodynamic, structural, propulsion, or controllability constraints. The related parameters may include speed, altitude, angle of attack, bank angle, structural load limits, angular rates (yaw, pitch, and roll), descent rates, and propulsion limits.
- 8.6.2 Exceedance of the approved flight envelope may result in loss of control, structural damage, or degradation of critical system performance.
- 8.6.3 Where the remote pilot is not in the loop during the operation, the remote pilot has no means of directly changing these parameters.
- 8.6.4 Compared to conventional aircraft, many RPAS operate with reduced situational awareness, communication latency, simplified control interfaces, and may be flown by relatively inexperienced operators. In addition, many operations are conducted BVLOS, further reducing the remote pilot's ability to directly assess the aircraft's condition. As a result, the RPA itself should incorporate safeguards that prevent unsafe operation resulting from foreseeable human error.
- 8.6.5 Flight envelope protection functions typically operate by limiting, modifying, filtering, or overriding unsafe remote pilot commands that could otherwise cause the RPAS to exceed approved operational limits. The applicant should identify hazardous flight conditions that could result from remote pilot error and define the associated protection functions or recovery mechanisms implemented to mitigate those conditions.

- 8.6.6 Examples of flight envelope protection functions include attitude limiters, stall protection systems, fly-by-wire command limiting, load-factor limiting, control authority limiting, angular-rate limiting, and energy-state protection functions. Protection functions may operate continuously, conditionally, or only during specific phases of flight. The applicant should describe the activation conditions, control authority, and operational limitations associated with the protection functions.
- 8.6.7 In order to design flight envelope protection functions, the applicant should clearly define the RPA's flight control functions used to achieve a change in the parameters listed in section 8.6.1, as well as the means in which the remote pilot can influence and change these parameters. The combination of the RPA's flight control functions, and how the remote pilot can influence them will determine how the flight envelope protection function works to prevent a flight envelope exceedance. The applicant should clearly define how the flight envelope prevention function works to prevent the erroneous human input from progressing through the flight control loop to an unsafe state.
- 8.6.8 Compliance may be achieved through software-based protections, inherent aerodynamic stability characteristics, mechanical control limitations, or a combination thereof. Examples include stall-resistant aircraft characteristics, control surface travel limits, thrust or power limitations, and restricted control authority. Evidence should demonstrate that these characteristics effectively prevent unsafe exceedances or support timely recovery to a safe operating condition.
- 8.6.9 Evidence supporting compliance should demonstrate that foreseeable remote pilot errors do not result in loss of control, unsafe flight conditions, or unrecoverable exceedance of the approved flight envelope. Such evidence may include simulation results, flight test reports, pilot-error scenario testing, control-input limit demonstrations, recovery demonstrations following incorrect pilot commands, and operational evaluations of the flight envelope protection functions.
- 8.6.10 Compliance should be appropriate to the complexity and robustness level required.
- 8.6.11 Demonstrations should include representative pilot-error scenarios under representative operational conditions. The pilot-error scenarios include conditions such as:
- incorrect pilot inputs
 - inappropriate mode selections
 - delayed pilot responses
 - excessive control commands
 - recovery from foreseeable operator mistakes.
- 8.6.12 OSO #05 addresses failures, development errors, implementation assurance, and verification activities associated with automatic flight envelope protection systems. OSO #18 addresses the existence and effectiveness of the automatic flight envelope protection function itself. For example, OSO #18 ensures that a stall protection function exists and performs its intended protective function, while OSO #05 addresses whether the stall protection function was designed, implemented, and verified to an appropriate level of robustness.
- 8.6.13 For a low level of robustness, the protection function may rely on commercially available, or autopilot systems developed without formal aviation design assurance processes, including COTS components, without formal development assurance evidence.
- 8.6.14 For medium and high levels of robustness, while CASA may not prescribe specific standards, applicants should use relevant sections of the applicable airworthiness design standards (ADS), together with the compliance basis addressed under OSO #04 and the development assurance levels and safety objectives established under OSO #05 during the development of the flight envelope protection functions.

9 OSO #19 – Safe recovery from human error

9.1 General

- 9.1.1 Human error may lead to hazardous conditions through incorrect actions, omissions, delayed actions, or misinterpretation of system information. OSO #19 addresses the ability of the RPAS to detect, manage, and recover from reasonably foreseeable human errors before they result in hazardous conditions.

Note: The flight envelope protection is excluded from this OSO since it is specifically covered by OSO #18.

9.2 Level of robustness

- 9.2.1 The required level of robustness for OSO #19 is specified in Table 31 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 31: OSO #19 Level of robustness

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

9.3 Level of integrity

- 9.3.1 The level of integrity must not be less than the required level of robustness. Table 32 provides the criteria for different integrity levels for OSO #19.

Table 32: OSO #19 Level of integrity

Level of integrity	Criterion
Low	Systems detecting and recovering from human errors are developed to industry best practices.
Medium	Systems detecting and recovering from human errors are developed to standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA.
High	Systems detecting and recovering from human errors are developed to standards considered adequate by CASA or in accordance with a means of compliance acceptable to CASA.

9.4 Level of assurance

- 9.4.1 The level of assurance must not be less than the required level of robustness. Table 33 presents the criteria for the different assurance levels for OSO #19.

Table 33: OSO #19 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.

9.5 Means of compliance

9.5.1 Table 34 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #19.

Table 34: OSO #19 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	a. 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. b. Evidence may include qualitative identification of foreseeable human errors and demonstration that appropriate detection, alerting, or recovery functions are implemented in the system design. This may be supported by analysis, inspection, or representative testing showing that unsafe conditions resulting from human error are mitigated.
Medium	a. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met. b. Evidence includes design documentation for functions that include human interaction and any protection functionality implemented, structured identification of human error scenarios and supporting demonstration that detection and recovery mechanisms are effective. This may include analysis, simulation, testing, or operational evidence showing that errors are identified in a timely manner and do not lead to hazardous conditions.
High	a. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met. b. Evidence includes design documentation for functions that include human interaction and any protection functionality implemented, comprehensive identification of human error scenarios and detailed demonstration that recovery remains achievable under representative and worst-case conditions. This includes validation of detection, alerting, and recovery functions through analysis, simulation, testing, and/or operational evaluation.

9.6 Additional guidance

- 9.6.1 OSO #19 complements OSOs #08, #09 and #20. While these OSOs aim to reduce the likelihood of human error through operational procedures, training and human-machine interface (HMI) design, residual errors may still occur. OSO #19 addresses these residual errors by requiring system features that detect unsafe conditions arising from human error, mitigate their consequences, and support safe recovery.
- 9.6.2 The errors may include incorrect system configuration, selection of an incorrect operating mode, improper deployment of equipment, activation of inappropriate automation functions, mismanagement of mission systems, incorrect contingency procedure activation, or failure to respond appropriately to system failures or abnormal conditions.
- 9.6.3 Compliance with OSO #19 should be achieved through system functions that detect human error, prevent escalation of unsafe conditions, and support recovery actions appropriate to the intended operation.
- 9.6.4 The applicant should identify reasonably foreseeable human errors associated with the intended operation and evaluate their potential safety consequences. This assessment should consider all personnel whose actions may affect the safety of the operation, including remote pilots, payload operators, and supporting crew, and may be aligned with the system safety assessment processes used for OSO #05.
- 9.6.5 Functions implemented to detect, prevent or recover from human errors should be defined and documented as part of design development, explaining their relationship between the human errors identified, when they occur, how they occur, and how the functions resolve the error.
- 9.6.6 The depth of analysis, implementation and validation should be commensurate with the required level of robustness:
- For low robustness, qualitative identification of foreseeable human errors and application of industry best practices may be sufficient.
 - For medium robustness, the applicant should provide systematic evidence that error detection and recovery functions are suitable and effective for the intended operation.
 - For high robustness, the applicant should provide comprehensive evidence that recovery remains achievable in representative normal, abnormal and degraded operating conditions.
- 9.6.7 The RPAS should incorporate means to detect and alert the remote crew to abnormal or unsafe conditions resulting from human error or automatically initiate protective actions where appropriate. Detection and warning functions may include system state monitoring, configuration checks, geofencing, and other sensing or diagnostic capabilities supporting the detection and correction of human error.
- 9.6.8 In addition to detection, the RPAS should support safe recovery from human error by providing means to prevent escalation of the condition and enable corrective action. Recovery provisions may include recovery guidance, command validation, configuration rollback, automatic reconfiguration, protective automation, fail-safe modes, or other measures appropriate to the RPAS design.
- 9.6.9 Where recovery relies on operator intervention, the system should ensure that:
- the error condition is detectable by the remote crew
 - the system provides sufficient information to identify the error condition and execute the recovery action
 - recovery actions are available and accessible
 - sufficient time and capability exist to take effective corrective action before a hazardous condition develops.
- 9.6.10 The RPAS should provide clear feedback following safety-critical actions. This may include confirmation that a command has been accepted, rejected, is in progress, or has resulted in a

system mode change. The feedback supports timely detection and recovery from incorrect or unintended actions.

- 9.6.11 The RPAS should incorporate protections, where practicable, against commands or action sequences that could result in hazardous conditions. These may include confirmation of safety-critical commands, interlocks, configuration checks, command filtering, or constraints that prevent violation of defined safety limits.
- 9.6.12 Recovery provisions should remain available and effective during degraded modes, failures, or abnormal operating conditions. Where complete recovery is not possible, the RPAS should degrade in a predictable and controlled manner that maintains an acceptable level of safety and supports safe continuation or safe termination of the flight.

10 OSO #20 – A Human Factors evaluation has been performed and the human-machine interface (HMI) found appropriate for the mission

10.1 General

- 10.1.1 OSO #20 intends to evaluate whether human factors (HF) have been considered in the HMI design and whether it is appropriate for the intended operation.
- 10.1.2 While the operator evaluates the suitability of the HMI for the intended operation, the designer shall consider human factors in the system design to minimise the likelihood of human error and to support safe and effective operation.
- 10.1.3 This guidance focuses on designer responsibilities.

10.2 Level of robustness

- 10.2.1 The required level of robustness for OSO #20 must be determined in accordance with Table 35 and categorised as optional (O), low (L), medium (M), or high (H), with corresponding SAIL.

Table 35: OSO #20 Level of robustness

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

10.3 Level of integrity

- 10.3.1 The level of integrity must not be less than the required level of robustness. The criteria associated with each level of integrity are provided in Table 36.

Table 36: OSO #20 Level of integrity

Level of integrity	Criterion
Low	The RPAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation.
Medium	The RPAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation.
High	The RPAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation. Human Factors evaluation is expected to cover: an appraisal to check that the remote crew workload remains acceptable in

Level of integrity	Criterion
	both normal and emergency situations; - an appraisal of the efficiency of the emergency procedures (efficacy of the actions, expected potential latencies); - analyses to check if prioritization of alarms and emergency procedures should be put in place to organize emergency procedures in such a way that they remain adapted to the criticality of the situation.

10.4 Level of assurance

10.4.1 The level of assurance must not be less than the required level of robustness. Table 37 lists the criteria for the different assurance levels for OSO #20.

Table 37: OSO #20 Level of assurance

Level of assurance	Criterion
Low	The applicant conducts a human factors evaluation of the RPAS to determine if the HMI is appropriate for the mission. The HMI evaluation is based on inspection or analyses. The adequacy of the result of the HMI evaluation is declared.
Medium	The applicant conducts a human factors evaluation of the RPAS to determine if the HMI is appropriate for the mission. The HMI evaluation is based on demonstrations or simulations. The adequacy of the result of the HMI evaluation is declared.
High	The applicant conducts a human factors evaluation of the RPAS to determine if the HMI is appropriate for the mission. The HMI evaluation is based on demonstrations or simulations. CASA witnesses the HMI evaluation.

10.5 Means of compliance

10.5.1 Table 38 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #20.

Table 38: OSO #20 Means of compliance

Level of robustness	Evidence requirement and assessment process
Low	- The RPAS designer provides relevant system information to the operator to support HMI evaluation for the intended operation. - The applicant demonstrates that the HMI presents system information clearly, supports situational awareness, enables required actions to be performed correctly and within the required time, and does not introduce unnecessary workload. - 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	The applicant provides evidence that human factors have been systematically considered in the HMI design.

Level of robustness	Evidence requirement and assessment process
	b. The applicant demonstrates that the HMI presents system information clearly, supports situational awareness, enables required actions to be performed correctly and within the required time, and does not introduce unnecessary workload. c. The evaluation covers representative tasks and operational scenarios appropriate for the intended operations, including displays, controls, alerts, system modes, and overall usability. d. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.
High	a. The applicant provides evidence that human factors have been systematically considered in the HMI design. b. The applicant demonstrates that the HMI presents system information clearly, supports situational awareness, enables required actions to be performed correctly and within the required time, and does not introduce unnecessary workload. c. The evaluation covers representative normal, abnormal and emergency scenarios including degraded modes and multiple concurrent events where applicable. d. Demonstrations are witnessed by CASA, as required. e. The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

10.6 Additional guidance

- 10.6.1 OSO #20 focuses on the design of the HMI to minimise the likelihood of human error by supporting correct situational awareness and understanding of external environmental states, system states and mode to facilitate appropriate decision-making and effective task execution.
- 10.6.2 Compliance with OSO #20 should reduce the frequency and severity of human error through appropriate design of the interface between human and machine.
- 10.6.3 For low levels of robustness, compliance may be based on inspection and analysis. In such cases, designer involvement may be limited where sufficient operational assessment is provided.
- 10.6.4 For low levels of robustness, designers should provide system information to support operational approval and safe use. This may be delivered by:
- defining intended use
 - defining system functions including expected interactions, system limitations and flight modes
 - identifying required crew tasks to operate the system correctly
 - providing flight manual information
 - validating usability for intended operational conditions
 - identifying residual procedural or training needs.
- 10.6.5 For medium level of robustness, the designer should demonstrate, through a structured human factors engineering approach, that the remote pilot and crew can correctly interpret external

environment states, interpret system states and modes, maintain situational awareness, and perform required tasks under expected operating conditions.

10.6.6 Evaluation of abnormal and emergency conditions is expected at high level of robustness.

10.6.7 The HMI and work environment should allow the remote crew to perform their duties without excessive concentration, skill, alertness, or fatigue, and its design should consider human factors principles.

10.6.8 All system controls, equipment, and displays are parts of the HMI and should be included in the HMI evaluation.

10.6.9 The evaluation should cover representative tasks and scenarios within the operational limitations defined by the designer. It should consider factors such as:

- number and roles of crew members
- number of RPAs managed
- automation levels
- duration and tempo of operations
- operational environment (including airspace and proximity to hazards)
- communication and coordination demand.

10.6.10 The evaluation should include the following aspects for specific tasks and scenarios:

- **Display and control usability:** ability to identify system states, perform actions, and manage responsibilities.
- **Information quality:** resolution, latency, and accuracy are adequate for the operation.
- **Situational awareness:** ability to detect and understand safety-critical conditions.
- **Crew workload:** perceived cognitive effort associated with task performance.

10.6.11 Designers should ensure that the HMI presents safety-critical information necessary for the remote crew to monitor the RPAS. As appropriate for the intended operation, this information may include:

- flight parameters representing the current state of the RPA
- deviations between actual and allowable operating limits
- predicted remaining endurance and operational range
- applicable airspace and air traffic constraints
- geofence status and conformance
- meteorological limitations affecting the operation
- obstacle and terrain information
- failures or degradation of safety-critical systems, including system health status
- historical trends or predictive information where these assist situational awareness and decision-making.

10.6.12 Designers should provide normal indications, cautions and warnings that enable the remote crew to recognise abnormal conditions, understand their significance, and take appropriate action in a timely manner. Alerts should be prioritised according to their operational significance and presented consistently with other HMI information.

10.6.13 Designers should consider the following activities to support compliance:

- Human factors engineering process:
 - define human factors requirements

- trace requirements to system design features
- trace design features to verification activities
- maintain configuration control
- Task analysis:
 - decompose operator tasks
 - identify error-prone and time-critical steps
 - identify information and system dependencies
- Human error analysis (Detection and recovery aspects are addressed under OSO #19.):
 - identify and analyse potential human errors
 - identify contributing conditions and system influences
- HMI verification:
 - Demonstrate that:
 - » alerts are understandable and appropriately prioritised
 - » displays are readable and interpretable
 - » controls are unambiguous and consistent
 - » system modes are clear and support correct awareness
 - » HMI design does not introduce unnecessary workload and supports completion of required tasks within acceptable workload limits
- Representative user evaluation:
 - Where appropriate, the evaluation should include:
 - » representative users
 - » realistic operational scenarios
 - » multi-tasking conditions
 - » degraded and abnormal modes.

10.6.14 When simulation is used, the validity of the targeted environment used in the simulation needs to be justified.

10.6.15 Designers may refer to established human factors guidance and industry practices for avionics and control interfaces as supporting reference material. While these references were developed primarily for manned aviation, many of the underlying human factors principles are applicable to RPAS, particularly for ground control stations and remote crew interfaces. Recommendations include:

- CS 27.1302 and associated AMC
- GAMA Publication 10 – Cockpit / flight deck design
- GAMA Publication 12 – Integrated cockpit design
- RTCA DO 372
- FAA HF display/control guidance (DOT/FAA/TC 16/56).

11 OSO #24 – RPAS designed and qualified for adverse environmental conditions

11.1 General

- 11.1.1 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.
- 11.1.2 It also aims the RPAS has enough qualifications for environmental operating conditions which may be seen during an operation.

11.2 Level of robustness

- 11.2.1 The required level of robustness for OSO #24 is specified in Table 39 and categorised as optional (O), medium (M), or high (H), with corresponding SAIL.

Table 39: OSO #24 Level of robustness

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

11.3 Level of integrity

- 11.3.1 The level of integrity must not be less than the required level of robustness. Table 40 provides the criteria for different integrity levels for OSO #24.

Table 40: 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.

11.4 Level of assurance

- 11.4.1 The level of assurance must not be less than the required level of robustness. Table 41 presents the criteria for the different assurance levels for OSO #24.

Table 41: 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.

Level of assurance	Criterion
High	CASA validates the claimed level of integrity.

11.5 Means of compliance

- 11.5.1 Table 42 outlines the evidence required from applicants and CASA's assessment process to demonstrate compliance with varying levels of robustness for OSO #24.

Table 42: OSO #24 Means of compliance

Level of robustness	Evidence requirement and assessment process
Medium	- The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct an assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met. - Partial qualification may be acceptable (for medium robustness only).
High	The applicant is required to make a declaration of compliance in a form and manner acceptable to CASA and provide sufficient evidence for CASA to conduct a comprehensive assessment of the declared compliance. If deficiencies are identified during the assessment, resubmission may be required to ensure the intent of the OSO is met.

11.6 Additional guidance

11.6.1 Environmental qualification

- 11.6.1.1 To assure safe operation, RPAS components, equipment, and systems that are critical to the safety of flight should be appropriately tested and qualified for both anticipated (nominal) environmental conditions, as well as certain applicable adverse environmental conditions.
- 11.6.1.2 The RPAS manufacturer should identify the intended operational conditions that the RPAS, and its systems, are designed to meet within the flight manual, or an equivalent document.
- 11.6.1.3 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.
- 11.6.1.4 The RPAS manufacturer should assess the likely risk of encountering adverse environmental conditions in the intended operational environment using an appropriate assessment methodology.
- 11.6.1.5 RPAS components, equipment and systems that may cause loss of control of the operation upon failure should have adequate qualification to substantiate their reliability and safety when operated within the intended operational conditions.
- 11.6.1.6 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 43.
- 11.6.1.7 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.

- 11.6.1.8 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.
- 11.6.1.9 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.
- 11.6.1.10 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.
- 11.6.1.11 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 C.

Table 43: 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 Simulation		Typically required at SAIL III and above. Partial compliance may be acceptable for 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.

Condition	Limitations	Compliance Method	Evidence Documents	Remarks
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.		
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.

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

Appendix A

OSO #02 – Compliance

A.1 Checklist

A.1.1 Applicant should demonstrate compliance to items identified in Table 44 to declare compliance.

Table 44: OSO #02 Compliance checklist

Topic	Verification	Related evidence
Specification of materials	1. Material type, grade, dimensions, and tolerances are documented. 2. Customer, regulatory, or industry standards are referenced. 3. Service conditions and durability expectations are documented. 4. Revisions/version changes are tracked and approved. 5. Material related risks are evaluated. 6. There is a formal approval and communication process for specification changes.	For example, drawings, specifications, BOMs, design records, engineering requirements, risk assessments, design reviews, change records
Suitability and durability of materials used	1. Materials are evaluated for suitability to their intended application. 2. Wear, corrosion, fatigue, and environmental exposure are considered where applicable. 3. Long term reliability expectations are defined where required. 4. Potential failure modes associated with materials are assessed. 5. Safety or operational impacts of material failure are evaluated.	For example, material selection records, engineering analysis, safety assessments, reliability studies
Processes necessary for repeatability in manufacturing and conformity within acceptable tolerances	1. Manufacturing and service processes are documented and controlled. 2. Acceptance criteria and tolerances are defined. 3. Processes are monitored and controlled for repeatability and conformity. 4. Operators are trained and qualified for assigned tasks. 5. Critical process steps are identified and controlled. 6. Human-factor influences affecting process consistency are considered.	For example, standard operating procedures, work instructions, inspection plans, process metrics, training records, process flowcharts, corrective actions
Configuration control	1. Current approved revisions of drawings and specifications are controlled and available at points of use. 2. Changes to drawings, specifications, software, or process documents are reviewed and approved. 3. Revision history and change records are maintained. 4. Relevant personnel are notified of changes. 5. Configuration changes are traceable and controlled. 6. Configuration discrepancies are identified and corrected.	For example, revision logs, change records, change approvals, change management systems

Topic	Verification	Related evidence
Verification of incoming products, parts, materials, and equipment	1. Incoming materials and components are verified prior to use. 2. Receiving inspections are performed where required. 3. Supplier documentations are reviewed. 4. Verification activities are based on supplier performance and product criticality. 5. Traceability records for critical materials are maintained where required. 6. Acceptance or rejection decisions are documented. 7. COTS Parts Management Plan prepared and implemented.	For example, receiving inspection records, inspection plans, supplier control and traceability reports, batch/serial records, CPMP
Identification and traceability	1. Products and materials are identified throughout production and delivery. 2. Batch numbers, serial numbers, or equivalent traceability methods are used where required. 3. Traceability requirements are defined based on product complexity or risk. 4. Inspection and test records are linked to the relevant product or batch. 5. Production history records are retained. 6. Traceability records support investigation of quality or safety issues.	For example, labels, job travellers, ERP records, retention policy
In-process and final inspections and testing	1. In-process inspections are performed at defined stages of production. 2. Final inspections are completed before product release. 3. Functional or performance testing is conducted where required. 4. Inspection and testing criteria are documented. 5. Inspection plans are done based on risk. 6. Inspection results are recorded and retained. 7. Product release authority is defined and documented. 8. The product release is documented for each aircraft manufactured.	For example, inspection plans, final acceptance records, inspection reports
Control and calibration of tools	1. Tools and measuring devices are suitable for intended use. 2. Monitoring and measuring equipment are calibrated at defined intervals. 3. Calibration records are maintained and traceable. 4. Calibration status is clearly identified on equipment. 5. Maintenance activities are performed where required to preserve accuracy. 6. Tools and measuring equipment are stored and maintained properly.	For example, calibration system, tool control procedures, calibration labels
Handling and storage	1. Materials and products are protected from damage during handling and storage. 2. Storage conditions are suitable and controlled for the products or materials involved. 3. Product identification and conformity are maintained during	For example, storage procedures and logs, FOD

Topic	Verification	Related evidence
	storage and transport. 4. Foreign object debris (FOD) prevention measures are implemented where applicable.	inspections, labelling controls
Non-conforming item control	1. Nonconforming products or materials are identified, documented and controlled. 2. Nonconforming items are segregated where appropriate. 3. Disposition decisions are authorised by designated personnel. 4. Root causes of significant nonconformities are investigated, and corrective actions are implemented to prevent recurrence. 5. Potential impacts on quality, safety, or reliability are evaluated and escalated where required.	For example, non-conformance reports, corrective and preventive action plans
Personnel competence and qualification	1. Competency requirements are documented. 2. Personnel are trained and qualified for assigned responsibilities. 3. Competency evaluations are performed where required. 4. Training records and qualification records are maintained. 5. Personnel understand applicable safety and conformity requirements and their responsibilities. 6. Personnel are authorised for specific activities where required.	For example, training records, evaluations, competency matrix
Supplier control	1. Suppliers are evaluated prior to approval for use. 2. Supplier quality and delivery performance are monitored and evaluated where necessary. 3. Corrective actions are requested and monitored for supplier issues. 4. Traceability or technical requirements are communicated to suppliers where applicable. 5. Supplier oversight is based on product criticality and operational risk.	For example, approved supplier lists, supplier risk assessment, audit reports

Appendix B

OSO #05 – Compliance

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

Reference: Table 22.

- B.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.
- B.1.2 In determining the indicative quantitative probabilities for the different failure condition classifications identified in Table 22, 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).
- B.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.
- B.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.
- B.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.
- B.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 22.
- B.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.
- B.1.8 In confirming whether the probabilities established within Table 22 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.

- B.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.
- B.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.
- B.1.11 In 2024, the European Union Aviation Safety Agency (EASA) published MOC Light UAS.2510-01 (applicable to SAIL 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.

B.2 Aircraft functional hazard assessment template and example

- B.2.1 The template given in Table 45 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.
- B.2.2 An example of an FHA for selected failure conditions is provided in Table 45 for reference.

Table 45: 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.

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
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 Crew: Slight increase in workload to maintain control.	Minor	Probable		
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.

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	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.
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.	Major	Remote	Qualitative Analysis- DIA	Remote pilot initiates emergency procedures and start glide landing approach

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
					Crew: Significant increase in workload.				
	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.
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.	Minor	Probable		Crew initiates C2 link recovery procedures.

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
					Crew: Slight increase in workload.				

B.3 Safety assessment detailed requirements

- B.3.1 There are many types of safety analyses that can be used to conduct an RPAS safety assessment as discussed in Chapter 5. As the risks associated with the loss of an RPAS increase, more detailed analyses are needed to identify potential failure modes and demonstrate that the risks of these failures have been minimized.
- B.3.2 CASA recommends the safety assessment methods and artefacts identified in Table 46 for each SAIL. Short descriptions of these methods and artefacts are provided in the following paragraphs additional to the existing guidance in Chapter 5.

Table 46: Safety analyses methods and artefacts for different SAILS

Analysis	SAIL III (Low Robustness)	SAIL IV (Medium Robustness)	SAIL V (High Robustness)	SAIL VI (High Robustness)
System Description	✓	✓	✓	✓
Aircraft Function Decomposition Table	O	✓	✓	✓
Interdependence Analysis Matrix	O	✓	✓	✓
Functional Hazard Assessment (FHA)	Qualitative analysis is sufficient to demonstrate that safety objectives have been met.	Qualitative or quantitative analysis can be provided to demonstrate that allowable probabilities have been met.	Qualitative and quantitative analysis shall be provided to demonstrate that allowable probabilities have been met.	Qualitative and quantitative analysis shall be provided to demonstrate that allowable probabilities have been met.
Fault Tree Analysis (FTA)	O	Qualitative or quantitative FTAs should be provided for all failure modes with an allowable probability of <1E-5.	Quantitative FTAs should be provided for all failure modes with allowable probabilities of <1E-5 and <1E-6.	Quantitative FTAs should be provided for all failure modes with allowable probabilities of <1E-5, <1E-6, and <1E-7.
Failure Mode and Effects Analysis (FMEA)	O	As needed.	As needed.	As needed.
Common Mode Analysis (CMA)	O	✓	✓	✓

- B.3.2.1 **System description:** The system description can form a part of the DIA document and include at a minimum:
- a description of the RPAS aircraft and its operational support equipment
 - a breakdown of the major RPAS systems and their functions
 - a discussion of basic RPAS operations, crew interfaces, crew alerts and crew responses.

- B.3.2.2 Aircraft function decomposition table:** The purpose of an Aircraft Function Decomposition table is to decompose aircraft functions into sub-functions from which failure conditions can be derived for subsequent safety analyses. An example of an Aircraft Function Decomposition table is provided ARP 4761A Table A2.
- B.3.2.3 Interdependence analysis matrix:** Interdependence analysis provides visibility of the interactions between aircraft functions and systems during normal operation or system malfunction and helps identify the need for functional independence and separation. An example of an Interdependence Analysis matrix is provided in ARP 4761A Table B1.
- B.3.2.4 Functional hazard assessment (FHA):** An FHA is a systematic, comprehensive evaluation of system functions intended to identify and classify failure conditions of those functions according to their severity and provide a basis for system-level safety objectives. An example FHA table is provided in Appendix B. For each failure mode with a safety objective of $< 1E-5$, $< 1E-6$, or $< 1E-7$, a separate narrative should be provided to demonstrate that system-level safety objectives have been met. The narrative should include a discussion of the failure mode, its effect on continued RPAS operation, contributing system failures, preventative design features, crew awareness features, mitigating crew actions, and significant latent failures. Both qualitative and quantitative analyses may be required to demonstrate these safety objectives as discussed in Table 47.

Table 47: Demonstration of safety objectives (adapted from ASTM F3309-20)

Safety Objective: $< 1E-5$	Safety Objective: $< 1E-6$ or $< 1E-7$
Qualitative analysis should be provided to demonstrate this safety objective. For 'loss of function' failure conditions, safety objectives can be demonstrated by: - Showing that there is redundancy in the equipment providing that function. An analysis of a redundant system in the airplane is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel or - In the case where single failures can cause the failure condition, by showing the system is simple, uses conventional architecture, is appropriately qualified for the installed environment and the individual failure rates of its components are below the objective of $1E-5$. For 'malfunction' failure conditions, safety objectives can be demonstrated by: - Showing that the failure condition requires at least two independent failures; or - In the case where a single component can cause the event, showing that only specific component failure modes or a subset of a unit's internal components can result in the failure condition.	Both qualitative and quantitative analyses should be provided to demonstrate these safety objectives. Qualitative analysis can be used to substantiate that each scenario that can cause the failure condition can only result from two or more independent failures. If the second failure in each combination is latent for more than one flight, the function of the component must be verified at a regular interval to minimize the exposure period. This can be accomplished by requiring a preflight check or mandated inspection/maintenance task. Common modes that could invalidate the independence between these failures should also be considered. Any failure conditions with these safety objectives cannot occur as the result of a single failure. Quantitative analysis should be used to numerically substantiate these safety objectives. This can be in the form of a quantitative Fault Tree Analysis.

Safety Objective: <1E-5	Safety Objective: <1E-6 or <1E-7
Justification must be provided for the failure rate apportionment and how that would result in a failure rate on the order of 1E-5.	

- B.3.2.5 **Fault tree analysis:** A fault tree analysis(FTA) is a top-down analysis which focuses on a top-level event and provides a method for determining causes of this event. FTAs can be used to identify single failures and failure combinations which can lead to the top-level event. See ARP 4761A for FTA examples.
- B.3.2.6 Potential latent failures may also be considered in FTA and additional preflight checks, or maintenance requirements may be required to minimize latent failure exposure periods and support RPAS allowable probability criteria.
- B.3.2.7 **Failure mode and effects analysis:** A failure mode and effects analysis (FMEA) is a bottom-up method of identifying the failure modes of a system, function, or item and determining the effects on the next higher level. FMEAs can be used to identify failure effects resulting from single failures. See ARP 4761A for FMEA examples.
- B.3.2.8 **Common mode analysis:** When credit is taken for the independence between failures, a common mode analysis (CMA) should be performed to ensure that there are no common mode failures that would invalidate the assumed independence. The analysis must substantiate that the two failures are indeed independent when considering their design, installations, wiring, and potential common dependencies such as electrical power. Where this independence is not easily justifiable, additional analysis may be required.
- B.3.2.9 Consideration should also be given to physical events which may violate independence, or compromise aircraft safety and survivability. These risks may be internal or external to the aircraft (i.e. uncontained rotor failures or bird strike).
- B.3.2.10 The CMA can be presented in the form of a discussion in the RPAS safety assessment, with references to applicable FTAs and FHAs.

Appendix C

OSO #24 – Compliance

C.1 Example environmental qualification statement

- C.1.1 The format at Table 48 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.
- C.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 48: 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.
Induced Signal Susceptibility	DO-160G, Sec. 19	Not tested. Category X.

Conditions	Standard / Reference	Description
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.