DRAFT

Australian Government
Civil Aviation Safety Authority

ADVISORY CIRCULAR
AC 21-57 v1.0

Airworthiness cybersecurity of remotely piloted aircraft systems (RPAS)

File ref: D25/184494

November 2025

DRAFT

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.

Advisory circulars are intended to provide advice and guidance to illustrate a means, but not necessarily the only means, of complying with the Regulations, or to explain certain regulatory requirements by providing informative, interpretative and explanatory material.

Advisory circulars should always be read in conjunction with the relevant regulations.

Audience

This advisory circular (AC) applies to:

- designers and manufacturers (OEMs) of remote piloted aircraft systems (RPAS)
- designers and manufacturers (OEMs) of RPAS subsystems
- remotely piloted aircraft (RPA) operator's certificate (ReOC) holders and applicants
- remote pilots (RePL) and other remote crew members
- safety assurance professionals involved in RPAS operations
- other support personnel involved in RPAS operations.

Purpose

This AC provides advice on the airworthiness cybersecurity of RPA including the assurance and protection of aviation information systems from cyber threats. A robust and systematic approach to the assurance of airworthiness cybersecurity ensures that the potential for intentional unauthorised electronic interactions that may result in adverse effects upon the safety of an aircraft has been adequately addressed during the design of the RPA.

For further information

For further information or to provide feedback on this AC, visit CASA's contact us page.

Status

This version of the AC is approved by the National Manager, Airworthiness and Engineering Branch.

Table 1: Status

Version	Date	Details
1.0	November 2025	Initial draft version for consultation.

Unless specified otherwise, all subregulations, regulations, Divisions, Subparts and Parts referenced in this AC are references to the *Civil Aviation Safety Regulations 1998 (CASR)*.

Contents

1 Reference material

1.1 Acronyms

The acronyms and abbreviations used in this AC are listed in the table below.

Table 2: Acronyms

Acronym	Description
AC	advisory circular
ADAHRS	air data, attitude and heading reference system
ADS-B	Automatic Dependent Surveillance–Broadcast
AHRS	attitude and heading reference system
ATC	air traffic control
ATS	air traffic service
BLOB	binary large object
BMS	battery management system
C2	command and control
C3	command, control and communication
CAN	controller area network
CAR	Civil Aviation Regulations 1988
CASA	Civil Aviation Safety Authority
CASR	Civil Aviation Safety Regulations 1998
CEH	complex electronic hardware
CVE	common vulnerabilities and exposures
DSSS	direct sequence spread spectrum
ESC	electronic speed controller
FCS	flight control system
FHSS	frequency hopping spread spectrum
FLS	field loadable software
FPGA	field programmable gate array
FTS	flight termination system
GCS	ground control station
GNSS	global navigation and satellite system
GPS	Global Positioning System

Acronym	Description
HIRF	high intensity radiated field
I2C	inter-integrated circuit
IMA	integrated modular avionics
IUEI	intentional unauthorised electronic interaction
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
JTAG	Joint Test Action Group
NAA	national aviation authority
OEM	original equipment manufacturer
PRS	parachute recovery system
RF	radio frequency
RPA	remote piloted aircraft
RPAS	remote piloted aircraft system
RPS	remote pilot station
RTCA	Radio Technical Commission for Aeronautics
RX	receive
SBOM	software bill of materials
SORA	Specific Operations Risk Assessment
SPI	serial peripheral interface
SW	software
TX	transmit
UAS	uncrewed aircraft system
UART	universal asynchronous receive/transmit
VHF	very high frequency
ZTA	zero trust architecture

1.2 Definitions

Terms that have specific meaning within this AC are defined in the table below. Where definitions from the civil aviation legislation have been reproduced for ease of reference, these are identified by 'grey shading'. Should there be a discrepancy between a definition given in this AC and the civil aviation legislation, the definition in the legislation prevails.

Table 3: Definitions

Term	Definition
defence in depth	an architectural strategy in which more than one security measure is used, such that a successful attack would require vulnerabilities in multiple security measures. (Source: RTCA DO-355A)
digital signature	a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. (Source: IETF RFC 2828)
failure condition (FC)	a condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events. (Source: SAE ARP 4754B)
failure condition classification (FCC)	a discrete scale allowing categorisation of the severity of the effects of a failure condition. Classification levels are defined in the applicable regulation and advisory material. For example, AC 25.1309 ARSENAL (revised) and AMC 25.1309 define the following classifications: Catastrophic, Hazardous, Major, Minor and No Safety Effect. (Source: SAE ARP 4754B)
function	intended behaviour of an aircraft, system, equipment, or item regardless of implementation. (Source: SAE ARP 4754B)
integrity	a qualitative or quantitative attribute of a system, equipment, or an item indicating that it can be relied upon to work as intended. (Source: SAE ARP 4754B)
intentional unauthorised electronic interaction (IUEI)	a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorised access, use, disclosure, denial, disruption, modification or destruction of information and/or aircraft system interfaces. (Source: RTCA DO-356A)
isolation	physical or logical boundaries between security measures or functions intended to ensure that compromise or failure of one security measure or function (or of a shared resource) does not affect another security measure or function. (Source: RTCA DO-356A)
remotely piloted aircraft system	a set of configurable elements consisting of a remotely piloted aircraft, its associated remote pilot station (or stations), the required command and control links and any other system elements as may be required at any point during the operation of the aircraft.
partitioning	the use of physical or logical boundaries to separate portions of a system or an item such that the portions may be considered independent. (Source: SAE ARP 4754B)
validation	the determination that the requirements for the product are correct and complete. (Source: SAE ARP 4754B)
verification	the evaluation of an implementation of requirements to determine that they have been met. (Source: SAE ARP 4754B)

Term	Definition
vulnerability	a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. (Source: RTCA DO-326A)

1.3 References

Legislation

Legislation is available on the Federal Register of Legislation website https://www.legislation.gov.au/

Table 4: Legislation references

Document	Title
Civil Aviation Act 1988	
Part 21 of CASR	Certification and airworthiness requirements for aircraft and parts
Part 101 of CASR	Unmanned aircraft and rockets
Part 101 Manual of Standards	Unmanned aircraft and rockets

International Civil Aviation Organization documents

International Civil Aviation Organization (ICAO) documents are available for purchase from http://store1.icao.int/

Many ICAO documents are also available for reading, but not purchase or downloading, from the ICAO eLibrary (https://elibrary.icao.int/home).

Table 5: ICAO references

Document	Title
Chicago Convention	Annex 8, Airworthiness of Aircraft

Advisory material

CASA's advisory materials are available at https://www.casa.gov.au/publications-and-resources/guidance-materials

Table 6: Advisory material references

Document	Title
AC 21-10	Experimental certificates
AC 21-13	Type certification of Australian-designed aircraft
AC 21-43	Experimental certificates for uncrewed aircraft
AC 101-01	Remotely piloted aircraft systems - licencing and operations

Other references

CASA's advisory materials are available at https://www.casa.gov.au/publications-and-resources/guidance-materials

Table 7: Other references

Document	Title
ASTM F3532-23	Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions
JARUS SORA 2.5	JARUS Guidelines on SORA - Main Body
JARUS SORA 2.5 Annex E	Jarus Guidelines on SORA - Annex E - Integrity and Assurance Levels for the Operational Safety Objectives (OSO)
JARUS SORA 2.5 Cyber Safety Extension	JARUS Guidelines on SORA - Cyber Safety Extension
ISO 27005	Information Security Risk Management
IETF RFC 2828	Internet Security Glossary
RTCA DO-326B	Airworthiness Security Process Specification
RTCA DO-355A	Information Security Analysis for Continuing Airworthiness
RTCA DO-356A	Airworthiness Security Methods and Considerations
SAE ARP 4754B	Guidelines for Development of Civil Aircraft and Systems

2 Introduction

2.1 Airworthiness cybersecurity

2.1.1 Airworthiness cybersecurity is the assurance and protection of aviation information systems from cyber threats; most importantly, that of intentional unauthorised electronic interactions that may result in adverse effects upon the safety of an aircraft.

2.1.2 An intentional unauthorised electronic interaction (IUEI) is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorised access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces[1].

2.1.3 Modern aircraft systems are increasingly interconnected, which potentially renders them increasingly vulnerable to cybersecurity threats.

2.1.4 For remote piloted aircraft systems (RPAS), cybersecurity threats represent unique and potentially heightened potential risks to aviation safety, due to the high levels of reliance placed on both airborne and ground-based software and electronic hardware for the safe conduct of RPA operations, and to the absence of a human pilot on the aircraft able to intervene directly in the event of interference or failure.

2.2 Scope

2.2.1 Airworthiness cybersecurity considerations are highly specialised and are scoped to mean the specific cybersecurity considerations that fall within an identified "aircraft-level" system boundary.

2.2.2 For a RPAS, this 'aircraft-level' boundary contains the airborne sub-systems that are installed within the Remote Piloted Aircraft (RPA), as well as the ground-based sub-systems that directly support an RPA flight operation, such as the Remote Pilot Station (RPS), the command and control (C2) links between the RPS and RPA, and any other supporting infrastructure[2] that is relied upon to safely control the RPA in-flight.

2.2.3 The focus of this guidance material is on airworthiness cybersecurity considerations that potentially affect the most important and safety-critical RPAS subsystems, such as flight controllers, sensors and actuators, surveillance and navigation equipment, command and control (C2) links, and mission systems.

2.2.4 This guidance[3] is not intended to extend to, nor address, broader cybersecurity considerations such as organisational or enterprise-wide cybersecurity. For more general information on cybersecurity principles and approaches, readers may wish to consult suitable references such as the Australian Signals Directorate (ASD) Information Security Manual or the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.

2.2.5 Airworthiness standards and practices for the cybersecurity assurance of certified aircraft (including RPAS) have been developed and published by aerospace consensus standards organisations (CSO's) such as the RTCA, EUROCAE and the ASTM. These standards and practices outline detailed methodologies and activities to be performed to assure the

[1] This definition appears in RTCA DO-356A.

[2] Examples of other supporting infrastructure may include a real-time kinematics (RTK) base station used to enhance the accuracy of GNSS positioning during RPA operations, or a mission planning tool (external to the RPS) used to support the flight operation.

[3] Nothing in this guidance is intended to create any inconsistency with the, or form interpretation of, primary cybersecurity legislation, including (but not limited to) the Cyber Security Act 2024 (Cth) and the Security of Critical Infrastructure Act 2019 (Cth).

cybersecurity of type certified aircraft and aeronautical products. These standards have been referenced in this document where appropriate.

2.3 RPA risk assessment and operational approval

2.3.1 Operations of UAS (RPA) currently take place under Part 101 of CASR. Regulation 101.030 of CASR sets out the broad requirements that relate to the approval of an area of operation for an uncrewed aircraft (UAS). In considering whether to approve an area for the proposed operation, under subregulation 101.030 (3), CASA is required to take into account the likely effect on the safety of air navigation of the operation of a UAS.

2.3.2 For a UAS (RPA) operating above 400 ft, regulation 101.250 of CASR allows a person to operate a very small RPA, small RPA, or medium RPA outside an approved area (as defined under regulation 101.030) provided the operator has CASA's approval to do so and the RPA stays clear of populous areas.

2.3.3 In the absence of a regulatory approval under regulations 101.030 or 101.250, an RPA operation is required to be conducted in accordance with the standard RPA operational conditions, as outlined by regulation 101.238 of CASR. Importantly, operations under standard RPA operational conditions are restricted only to those operations that take place at or below 400 ft AGL, by day, and in visual line of sight (VLOS) only. Operations over 400 ft AGL, or beyond visual line of sight (BVLOS), are not permitted.

2.3.4 In determining whether to grant a regulatory approval under regulation 101.030 for the purposes of regulation 101.250 of CASR, an operational risk assessment process is performed. CASA has adopted the Joint Authorities Rulemaking for Unmanned Systems (JARUS) Specific Operational Risk Assessment (SORA) methodology as one means, but not the only means, of performing a risk assessment for a proposed UAS operation.

2.3.5 Annex E of the JARUS SORA outlines the technical and operational assurance activities to be conducted under the SORA risk assessment process to achieve operational approval for differing levels of systems assurance (SAIL level). These operational safety objectives (OSOs) are further augmented by complementary requirements for cybersecurity assurance that detailed in the JARUS SORA Cyber Safety Extension.

2.3.6 The JARUS SORA Cyber Safety Extension outlines cyber assurance activities to be performed, across various operational safety objectives (OSOs). These requirements vary depending on the intended SAIL level of the proposed operation. Most significantly, for OSO #5 (UAS is designed considering system safety and reliability), the Cyber Safety Extension outlines a range of required activities for the review of potential cyber threats (for RPA operations at SAIL levels I-II) or the conduct of a formal cybersecurity risk assessment (for RPA operations at SAIL level III, or above).

2.3.7 In support of this, Chapter 3 of this AC provides further guidance on the categorisation, review and assessment of cyber threats. Chapter 4 of this AC outlines a suitable methodology and activities for the conduct of a cybersecurity risk assessment process that addresses the requirements of SORA.

2.3.8 Additionally, Appendix A of this AC provides an outline of some potential cyber threats, organised by functional area, as a further guide to UAS designers and security researchers seeking to mitigate potential cyber threats in their UAS (RPA) architectures and aircraft designs.

3 Security concepts

3.1 Security attributes

3.1.1 Confidentiality

3.1.1.1 The security attribute of confidentiality refers to the protection of information from unauthorised disclosure and the protection of systems from unauthorised access.

3.1.2 Integrity

3.1.2.1 The security attribute of integrity refers to ensuring that information within a system remains consistent and correct and that the functionalities of systems are correct, complete and work as intended.

3.1.3 Availability

3.1.3.1 The security attribute of availability refers to whether information remains accessible when required and extends to assuring that systems responsible for implementing functionalities remain accessible and operative when needed.

3.1.3.2 Taken together, these attributes form the recognised 'C-I-A' security triad that captures the most fundamental security attributes that are required in any secure information system. These foundational attributes also underpin a range of key security principles that address the design and implementation of reliable, functional and secure systems in practice.

3.2 Security principles

3.2.1 Secure by design

3.2.1.1 The secure by design principle embodies both an architectural and an organisational approach towards building systems that are inherently secure. The secure by design principle recognises the importance of incorporating security-related considerations into the design and development process from the outset: starting with the initial phases of system conceptual design and requirements definition, and moving through to later phases such as implementation, verification and validation of the system.

3.2.1.2 Practitioners of secure by design approaches leverage an in-depth understanding of cybersecurity architectural and implementation best practices, as well as real-world experience of both historical and emerging security threats (typically identified through detailed knowledge and analysis of the many classes of common vulnerabilities and exposures, or CVEs, that have been identified and mitigated across information systems over a period of years, and in some cases, decades), to ensure that the system will fulfil its intended security objectives.

3.2.1.3 Secure by design integrates security thinking into the entire systems development life cycle, rather than allowing security to be approached as a bolt-on or post-facto step; often in the latter case with the aim of simply fulfilling a compliance objective.

3.2.2 Defence in depth

3.2.2.1 Defence in depth is an architectural strategy in which more than one security measure is used, such that a successful attack would require vulnerabilities in multiple security measures[4]. The

[4] This definition appears in RTCA DO-355A.

principle of defence-in-depth is widely deployed in typical and best-practice architectures for modern information systems, particularly organisational and enterprise information systems.

3.2.2.2 For airworthiness cybersecurity applications, such as RPAS, leveraging the principle of defence in depth, while possible, can be more difficult than for conventional information systems. This is due in part to the often-limited isolation (both physical and logical) between disparate aircraft-level functional elements, and to the inherent increase in system complexity that arises whenever a more complex system architecture is adopted.

3.2.2.3 Additional architectural and implementation complexity may add to the potential burdens of assuring the correctness and safety of the system, and more complex architectures may be more difficult to assure. Furthermore, the implementation of additional defences may also give rise to additional latent errors or defects in those implementations, which in turn may increase overall safety risk.

3.2.2.4 Also, in some cases, additional architectural complexity and defensive measures may also contribute to unpredictability of software execution paths for the system, introducing a source of 'non-determinism' that can degrade both the predictability and the performance of certain safety-critical functions.

3.2.2.5 Effectively reconciling and balancing competing system-level considerations, such as correctness, completeness, performance, assurance, and security, for the design of an aircraft-level system, can be a challenging exercise.

3.2.3 Least privilege

3.2.3.1 The principle of least privilege is a defensive design principle intended to limit the effect, and ultimately the impact, of an initially successful cyberattack. Least privilege requires that a user's (or program's) level of access and privileges to any shared or underlying system resources is kept to the minimum that required for the implementation of the intended function.

3.2.3.2 In the event a vulnerability is identified and exploited by an attacker, least privilege helps to ensure that the effects and impacts of a successful cyberattack on the overall system are minimised.

3.2.4 Zero trust

3.2.4.1 The zero trust principle is a defensive design principle that enforces that no user, device, or architectural element (such as a subsystem) is inherently trusted by default, regardless of the physical or logical location (apparent or actual) of the user, device, or element within the overall system.

3.2.4.2 Traditional information systems have implemented loose security and trust boundaries, in which users and devices that are located (or appear to be located) within certain defined security domains, or zones, are assumed to be legitimate and are trusted by default. This violates the principle.

3.2.4.3 The zero trust principle, when applied at the architectural definitional level of system, leads to the concept of zero trust architecture (ZTA). ZTA architectural elements may be implemented at either the physical or logical levels of a system's realisation, and sometimes at both levels[5].

3.2.4.4 ZTAs reject the inherent assumption of trusted-by-default semantics within the system's trust boundary, and instead enforce appropriate privacy, verification and access control with all elements of the system; typically, by using established cryptographic methods such as encryption, digital certificates, and digital signatures. Implementing ZTAs may also require security-driven architectural changes to enhance the degree of isolation and segregation

[5] An example of this might be the use of hardware-level encryption for system memory (a physical level ZTA mechanism), coupled with software-level encryption of inter-system communications over a shared message bus such as CAN (a logical level ZTA mechanism).

between system elements, thereby ensuring that internal trust boundaries are appropriately granular to enforce and implement the zero trust principle in practice.

3.2.4.5 As for defence in depth (discussed in section 3.2.2), leveraging the principle of zero trust in airworthiness cybersecurity applications, such as RPAS, can be more difficult than for conventional information systems. Airworthiness domains and networks historically implement trusted-by-default semantics, and the use of cryptographic techniques inside the trust boundary of typical aerospace systems is currently rare. As a result, this places extreme dependence upon the effective definition enforcement of the security domain (and its related trust boundary) from external interference to achieve the system security objective.

3.2.4.6 The use of ZTA approaches may enhance security, but also brings new challenges, such as the secure and effective management and distribution of cryptographic elements including digital certificates and encryption keys. The use of ZTAs also may drive additional functional requirements to safely address new failure scenarios, such as the appropriate behaviour of a system if the cryptographic assurances between subsystems that are relied upon during normal operation suddenly fail.

3.2.5 Supply chain security

3.2.5.1 Supply chain security relates to the protection of system elements, including software and hardware, from instances of intentional interference. This may include interference that occurs prior to any initial integration of system elements into the overall system.

3.2.5.2 A cautious approach towards the qualification of suppliers who deliver hardware, software or fully pre-integrated elements is an important control in mitigating the potential for a supply chain attack. The careful sourcing of hardware components, particularly semiconductor components, from established and trusted industry distributors is one important way to assure the authenticity and integrity of these components.

3.2.5.3 Similarly, it is important to recognise that sourcing pre-manufactured subsystems (particularly integrated electronic hardware, or software) from external suppliers places a strong degree of reliance on the supply chain security management practices of those suppliers.

3.2.5.4 Supply chain considerations also extend beyond security, to related issues of reliability and performance that arise from whether a supplied part (or element) is genuine; such that the manufacturer's technical data and quality assurances for performance and reliability can be relied upon.

3.3 Threat categorisation

3.3.1 The identification and categorisation of potential cybersecurity threats is an important initial step in the overall cybersecurity assurance process.

3.3.2 Several popular models for the categorisation of cybersecurity threats currently exist. One widely adopted and industry-accepted model for threat categorisation is the STRIDE model[6].

3.3.3 The STRIDE model provides a common taxonomy for the classification of cybersecurity threats, according to six distinct cyber threat categories:

- Spoofing (S)
- Tampering (T)
- Repudiation (R)
- Information Disclosure (I)

[6] The STRIDE model is outlined in many sources. For example: K. Ley Best et al (RAND Corporation), How to Analyze the Cyber Threat from Drones, published 2020, pg. 6.

- Denial of Service (D)
- Elevation of Privilege (E)

3.3.4 Spoofing (S) refers to the targeting of a system with intentionally falsified messages or data to elicit responses or to inappropriately trigger system behaviours (either expected or unexpected).

3.3.5 Examples of spoofing might include the targeting of an RPA's onboard GNSS (GPS) receiver with synthesised GNSS (GPS) RF signals for the purposes of affecting the receiver's position estimate; or the targeting of the RPA's C2 or C3 link with arbitrary message traffic designed to trigger unexpected RPA functions or behaviours.

3.3.6 Tampering (T) refers to the intentional manipulation of data or executable code that is intended to trigger unexpected behaviours or effects, or to implement unauthorised and altered system behaviours.

3.3.7 Examples of tampering might include a software- or firmware-level 'supply chain' attack that modifies the executable code of a safety-critical RPA control elements such as a flight controller to implant 'malware' containing erroneous, modified, or additional logic; or the targeting of an RPA C2 / C3 link with intentionally falsified or corrupted message traffic to trigger unexpected failure modes that lead to loss of control over the RPA.

3.3.8 Repudiation (R) relates primarily to the non-deniability of historical information exchanges, which may be particularly relevant for messages that relate to agreements or transactions. Whilst repudiation is important property for many information systems, it is typically a less important consideration for the domain of aircraft-level cybersecurity. Non-repudiation properties may however be useful for providing certain kinds of secure and auditable mechanisms, such as event logging.

3.3.9 Information Disclosure (I) relates to the unauthorised release of sensitive or confidential data during exchanges of data or messages between the RPA's system elements. This applies most obviously for the communication exchanged between the RPA and the RPS for the purposes of real-time command and control.

3.3.10 An example of information disclosure might be the inadvertent or unintentional sharing of important RPA operational parameters such as internal telemetry, RPA state (e.g., position, velocity, or intent such as flight plan), or video transmissions (which may additionally incorporate 'on-screen display' telemetry data), particularly when transmitted insecurely over C2 or other broadcast or data links.

3.3.11 It is important to note that an intentional broadcasts of RPA operational information, such as position reports made using ADS-B or similar ATC surveillance technologies, do not inherently represent a cybersecurity threat in this threat category.

3.3.12 Denial of Service (D) refers to the intentional 'jamming' or 'flooding' of either RPA C2 communication links (either analog or digital), or of RPA on-board data buses or internal interfaces, with arbitrary transmissions or traffic intended to degrade or inhibit the functional performance of the RPA or its sub-systems.

3.3.13 Examples of Denial of Service (also known as 'DoS') attacks might include instances of externally-transmitted RF interference ('jamming') of GNSS (GPS) satellite signals, leading to a loss of GNSS (GPS) position estimate by the RPA's on-board GNSS (GPS) receiver; or the intentional 'jamming' or 'flooding' of an RPA C2 or C3 link with the intent of degrading the ability for the RPA to be safely controlled from the RPS.

3.3.14 Elevation (or escalation) of Privilege (E) typically relates to the manipulation of operating system or hardware-level functionalities to obtain additional privileges relating to file or memory access permissions, or to process ownership and control. Elevation of privilege is an important consideration for real-time operating system (RTOS) or 'embedded system' elements deployed within an RPA.

3.3.15 Elevation (or escalation) attacks are particularly relevant for more complex or highly integrated RPA, where disparate software elements, such as flight control, communications, surveillance, and payload or mission systems, are deployed to shared operating system environments that

utilise shared hardware resources. In such cases, a vulnerability in one software functional element may be able to be exploited to enable an attacker to move 'laterally' to attack other logically separate functional elements that are executed upon the same underlying logical and physical resources.

4 Security risk assessment

4.1 Overview

4.1.1 Figure 1 contains a depiction of a 'V-model' process as applied to security risk assessment. The process is aligned to a conventional systems engineering 'V-model' approach, with the analysis-related activities of functional definition, threat identification and threat assessment appearing on the left-side of the 'V', and with the corresponding verification-related activities of threat mitigation, security validation and security evidence appearing on the right-side of the 'V'.

4.1.2 The security risk assessment process outlined in this chapter is aligned to the processes outlined in published consensus standards for airworthiness cybersecurity assurance, such as RTCA DO-326A and ASTM F3532-23. The description of some activities has been streamlined and simplified with the intent of being more proportionate to the level of assurance appropriate for a low- to medium- risk RPAS operation (up to a SAIL IV operation under the JARUS SORA operational risk assessment model, or an equivalent operation).

4.1.3 Prospective applicants for airworthiness-related approval of higher-risk RPAS operations, such as SAIL V or SAIL VI operations, or certified RPAS operations, should anticipate an increased level of assurance for airworthiness security risk assessment is likely to be required.

4.1.4 Type certificate applicants (certified RPAS) should expect to follow the guidance and objectives outlined within the established consensus standards, including RTCA DO-326A and its related standards, or other standards acceptable to CASA, as a means of compliance during the type certification process.

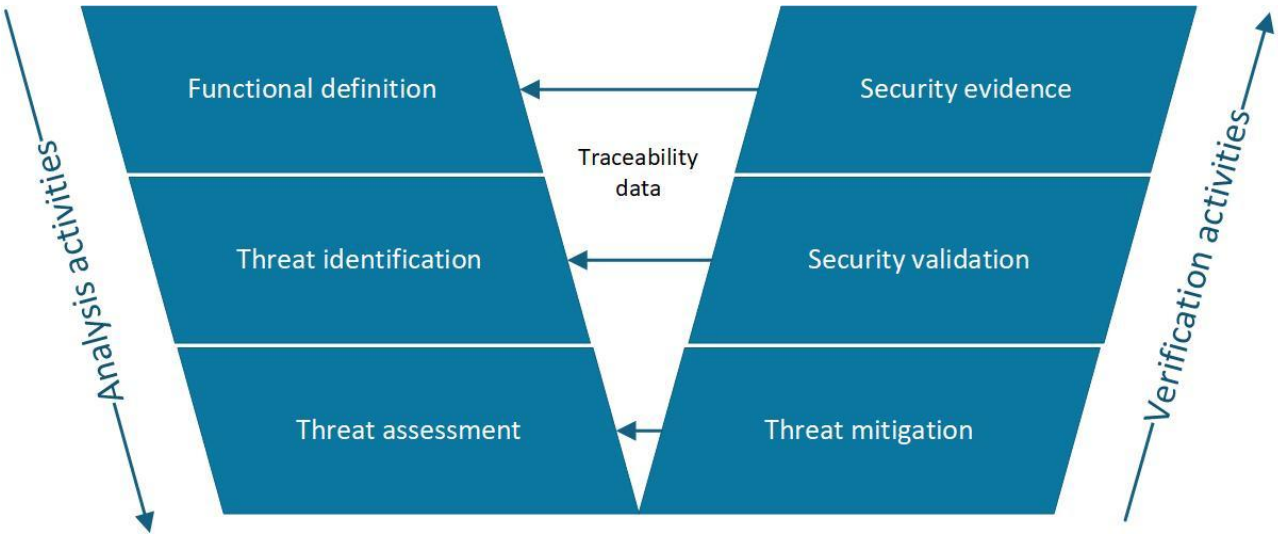

Figure 1: V model process

4.2 Process

4.2.1 Functional definition

4.2.1.1 The starting point in the security assessment process is the identification and definition of all significant aircraft-level functions that may be potentially vulnerable to cybersecurity attack. These aircraft-level functions often 'map' closely to their associated functional elements or subsystems; however, certain functions may be implemented across more than one subsystem (either physically, logically, or both), or conversely, a single subsystem may implement and provide more than one aircraft-level function.

4.2.1.2 Aircraft-level functions that make use of any means of external connectivity, such as RF links or third-party data-link communications, and particularly for bi-directional transmit/receive (TX/RX) or unidirectional receive-only (RX) communications, should undergo detailed technical assessment. Aircraft-level functions that perform transmit-only (TX) communications, such as certain surveillance systems, are less likely to be vulnerable but still should be assessed at a high-level.

4.2.1.3 Aircraft-level functions that make use of internal connectivity to achieve their functional requirements, particularly those functions that connect to significant numbers of other functions (i.e., high 'fan-out' functional elements) or that connect to important or safety-critical functions (i.e., critical functional elements), should be strongly considered for more detailed assessment.

4.2.1.4 In some RPAS (particularly smaller RPAS), multiple aircraft-level functions may be defined and implemented within shared (common) logical elements (such as a real-time operating system, or RTOS), which are typically deployed and executed by shared (common) physical elements (such as a microprocessor-based controller board). In such cases, it is possible that an initially successful cyberattack against one aircraft-level function may enable an attacker to target other unrelated functions deployed to the same shared elements. Detailed technical assessment of all coupled and therefore potentially impacted functions should be considered.

4.2.1.5 Appendix A of this Draft AC provides a high-level identification of some of the most common RPAS functional elements that are typically contained with the aircraft-level boundary of an RPAS.

4.2.2 Threat identification

4.2.2.1 With reference to information that may already be captured by other required engineering design artifacts, such as an aircraft-level functional hazard assessment (AFHA), identify the criticality (failure condition) of each identified aircraft-level function and the corresponding severity (failure condition classification) associated with the loss of the function.

4.2.2.2 For a lower-risk RPAS, where design artifacts such as AFHA may not be readily available, consider at a minimum the potential effects upon the most safety-critical aircraft-level functions such as flight control, control surface actuation, C2/C3 link, GNSS (GPS) positioning, and any RPA technical mitigations such as parachute recovery (PRS) or flight termination (FTS) that are intended to be relied upon and credited as part of an operational approval.

4.2.2.3 With reference to an appropriate threat taxonomy, such as the STRIDE model outlined in section 3.3 of this document, and with appropriate consideration of the criticality of each aircraft level function, systematically identify potential threats (sometimes termed 'threat conditions' and 'threat scenarios') that may arise from instances of interference, such as of spoofing, tampering, or other categories across those aircraft-level functions.

4.2.2.4 As part of the analysis, ensure all flows of data that make use of any external connectivity means, as described in section 4.2.1.2 of this document, are specifically identified, placing additional and particular emphasis on any data flows that involve elements external to the defined aircraft-level boundary for the RPAS.

4.2.2.5 Similarly, ensure the capture of all flows of data between identified aircraft-level functions within the aircraft-level boundary, including both the logical data flows between functions as well as the physical data flows arising from the implementation of these logical flows at a physical architectural (hardware) level.

4.2.2.6 For aircraft-level functions with identified threats and for which the criticality of loss of the function has been categorised as hazardous or catastrophic, conduct a detailed threat assessment and mitigation analysis for each threat in accordance with the guidance outlined in section 4.2.3 of this document.

4.2.2.7 For aircraft-level functions with identified threats and for which the criticality of the loss of the function has been categorised to be less than hazardous or catastrophic, ensure the analysis and any supporting assumptions are appropriately recorded.

4.2.2.8 Appendix A of this document provides a high-level list of some important potential threats (and their associated threat categories) that may be relevant and applicable to RPAS aircraft-level functions.

4.2.3 Threat assessment and mitigation

4.2.3.1 For identified threats to aircraft functions that have been categorised as critical, in accordance with the guidance in section 4.2.2.6, prospective mitigations that would either remove the security risk entirely, or that would reduce the security risk to an acceptable level, should be identified and considered for adoption.

4.2.3.2 For each identified threat, an initial risk level as well as an intended final risk level should be determined, based on the adoption of the mitigation strategy proposed. It may be appropriate to also adopt quantitative risk level measurement tools such as risk scoring to assist in the robust determination of these risk levels.

4.2.3.3 Mitigations can be applied at both the physical and logical levels and may involve the definition and implementation of additional functions or logic, changes to the logical design or physical architecture of the system, the introduction of additional system-wide security measures within shared infrastructure elements, or the adoption of organisational or procedural changes to ensure that a threat is mitigated.

4.2.3.4 Physical-level approaches to mitigation may include design changes to the configuration of hardware elements, including microprocessor general purpose IO (GPIO) interfaces and hardware interrupts, or changes to the physical routing of data buses and peripheral interconnects such as CAN, I2C, SPI, serial UART and JTAG interfaces.

4.2.3.5 Specific physical-level mitigations may be considered, such as the use of discrete signal connections (analog or digital) routed directly to GPIO interfaces, the use of read-only buses to ensure unidirectional data flows (with TX pins physically disconnected, or 'jumpered'), the appropriate partitioning of communications across multiple independent buses, and the comparison of signals obtained from different physical and logical paths to detect erroneous information.

4.2.3.6 Logical-level approaches to mitigation may include making changes to aircraft-level system architectures or configurations; making changes to the 'top-level' allocation of aircraft-level functions to software or complex electronic hardware (CEH) such as FPGAs; the use of architectural redundancy and diversity approaches such as modular redundancy architectures with voting; or the use of dissimilar version (N-version) programming approaches for robust software implementation.

4.2.3.7 Specific logical-level mitigations may be considered, such as the appropriate use of cryptographic methods to verify the authenticity of information flows (both across and within the system boundary); or the appropriate use of physical and logical partitioning mechanisms including separation kernels, low-level hypervisors, or established aerospace-standard isolation primitives[7] provided by some specialised real-time operating systems (RTOS).

4.2.3.8 Proposed physical and logical mitigations are likely to impact and drive changes to high-level and low-level system architectural designs, high-level and low-level requirements for aircraft functions allocated to software (SW) and complex electronic hardware (CEH), and possibly also to organisational procedures and internal controls. Changes arising from outputs of the security assessment process should be managed by the organisation in an integrated manner using the engineering change processes already established for developing aircraft-level functions and for managing existing system integration activities. Security mitigations should be developed in accordance with the existing processes for achieving the level of design assurance that has been identified as required for the aircraft-level function, including the development of the associated design assurance artifacts, where required.

[7] For example, ARINC 653 is an aerospace standard for space- and time- partitioning of safety-critical real-time operating systems (RTOS) for integrated modular architectures intended to support mixed criticality systems.

4.2.3.9 Appendix A of this draft AC provides a high-level list of useful mitigations that may be relevant and applicable to mitigating potential threats to RPAS aircraft-level functions.

4.2.4 Security verification

4.2.4.1 For each threat, and based on the implementation of mitigations that have been identified in accordance with the guidance in section 4.2.3.1, verify that the mitigation has been successfully accomplished and that it achieves its intended effect of reducing the final security risk to the targeted and acceptable risk level.

4.2.4.2 Once all threat-level security verification activities have been completed, a final risk assessment should be performed. The purpose of the final risk assessment is to verify and validate that all aircraft-level functions have been identified and appropriately categorised for criticality, and that all identified threats have been appropriately mitigated.

4.2.4.3 Threats that have been identified for one aircraft-level function should be considered for their applicability to other functions. Mitigations should be also reviewed to ensure they have not introduced new threats which have not been identified and appropriately analysed.

4.2.4.4 The final risk assessment process should validate that threats have been identified, and mitigations applied consistently, across aircraft-level functions of the same criticality that share a common potential threat. Where multiple threats are intended to be addressed by a shared mitigation (typically when implemented at subsystem or infrastructure level), a common mode analysis should be considered to evaluate whether the overall mitigations are appropriately independent and isolated to ensure that security risks will be controlled in practice.

4.2.4.5 Security verification is both a point-in-time and an ongoing exercise. The security verification process may need to be revisited if new threats are discovered, if new potential mitigations become available, or if significant changes are proposed to aircraft-level functions, or to the designation of the aircraft-level system boundary. These changes typically occur when existing functions are proposed to be integrated onto different platforms or variants, when the design or manufacture of a subsystem is changed, or when new payloads or mission equipment are proposed to be integrated. They can also occur when operational aspects (such as proposed operating locations or airspace) are varied, and particularly where this changes the level of safety assurance (and the related safety objectives) required to be met.

4.2.5 Security evidence

4.2.5.1 Maintaining appropriate artifacts that adequately document the overall outcome of the security risk assessment process is essential for demonstrating that the security risk assessment has been performed appropriately.

4.2.5.2 Maintaining appropriate artifacts also ensures the appropriate capture of information related to the key steps of the analysis, including underlying assumptions and recorded findings, which enables the security risk assessment to be readily and efficiently updated or expanded in response to any proposed change to either the aircraft-level configuration or the intended operations.

Appendix A
RPAS cybersecurity functional elements

A.1 Functional elements

A.1.1 A representative series of 'aircraft-level' functional elements for a typical RPAS configuration are provided in the table below. The purpose of each functional element is described and a top-level mapping from each element to its corresponding threats and mitigations is provided.

Table 7: Relationship for RPA airworthiness cybersecurity assurance, functional elements, threats and mitigations

Functional Element	Purpose	Threats (Category)	Mitigations
Actuation (control surfaces, etc.)	Provides mechanical actuation of control surfaces and related systems on command from FCS to maintain safe and controlled flight.	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering) Uncommanded activation of actuators. (Spoofing)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses, For example, serial UART, I2C, SPI, or CAN.
Attitude and Heading Reference System (AHRS)	Provides FCS with state estimate of aircraft attitude and heading derived from accelerometer, rate gyroscope, and (optionally) magnetometer data.	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources

Functional Element	Purpose	Threats (Category)	Mitigations
			from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses. For example, serial UART, I2C, SPI, or CAN.
Air Data, Attitude and Heading Reference System (ADAHRS)	As for AHRS and additionally provides state estimate of indicated airspeed derived from measurement of static and dynamic pressure.	As above.	As above.
Battery Management Systems (BMS)	Provide management over battery state of charge (SoC), cycles, thermal parameters, charging / discharging including balancing, overall performance monitoring and fault isolation (at cell, pack, or module level).	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses. For example, serial UART, I2C, SPI, or CAN.
Command and Control (C2) Link	Provides bi-directional communication between RPS and RPA.	Unauthorised Information disclosure of aircraft telemetry and mission data. (Information disclosure) Injection of arbitrary commands into RPA	Appropriate use of C2 link encryption protocols and secure authentication of RPS to RPA. RPAS is robust to injection of non-authenticated message traffic over C2 links.

Functional Element	Purpose	Threats (Category)	Mitigations
		control stream. (Tampering) Intentional modification to firmware that degrades or inhibits function or performance. (Tampering) Intentional interference (“jamming”) of C2 Link (Denial of Service)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate use of wideband RF modulation schemes, such as, ‘spread spectrum’, to reduce deniability, particularly where denial may be expected to occur or where denial may lead to an RPA loss of control (LOC) event. Appropriate consideration of redundancy in C2 links, including antenna and frequency range diversity. Appropriate pre-flight configuration of C2 ‘link loss’ behaviour.
Command, Control and Communication (C3) Link	As above, and; Provides a means of transmitting and receiving voice communications on aeronautical radiocommunication frequencies.	Inadvertent disclosure of RPA operational intent and information to non-aviation participants (Information Disclosure) Intentional interference (“jamming”) of communication channel (C3) (Denial of Service)	As above, and; Consider use of encryption for voice communication relayed between RPS and RPA, even where intended to be broadcast by the RPA on aeronautical radio communication frequencies. Appropriate consideration of redundancy in C3 link, including antenna and frequency range diversity. Appropriate consideration of procedures for coordination with ATS facility in the event of a failure or unavailability of the communications link.

Functional Element	Purpose	Threats (Category)	Mitigations
Electronic Speed Controller (ESC)	Maintains real-time sensing and control over electric motor parameters including voltage, current, RPM and temperature, as commanded by the FCS.	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository.
Flight Control System (FCS)	Maintains positive and stabilised control of aircraft attitude and trajectory by setting thrust and actuating control surfaces, preventing loss of control (LOC) in-flight or on ground.	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained directly from OEM and verified for authenticity (using digital signatures or cryptographic hashes as appropriate) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses. For example, serial UART, I2C, SPI, or CAN. Appropriate consideration of system-wide logging of message bus, such as, CAN, traffic.
Flight Termination System (FTS)	Inhibits critical RPA systems (such as propulsion) on command from RPS, providing controlled termination of flight.	Uncommanded activation of FTS. (Spoofing) Intentional modification to firmware that degrades or inhibits	FTS is robust to inadvertent or uncommanded actuation, such as, external sources of electromagnetic or RF interference. Firmware updates obtained from OEMs or open-source

Functional Element	Purpose	Threats (Category)	Mitigations
		function or performance. (Tampering)	repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository.
Ground Control Station (GCS)	See "Remote Pilot Station (RPS)"		
GNSS Receiver	Provides FCS with a state estimate of RPA position derived from space-based navigational sources such as GPS, augmented by SBAS[8] corrections (where available).	Intentional interference ('jamming") of GNSS radio frequency signals. (Denial of service) Intentional interference via transmission of false GNSS radio frequency signals affecting the position estimate. (Spoofing)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. State estimate is robust[9] to rapid or unexpected changes in GNSS position and reported GNSS satellite constellation. Internal systems that are dependent on time synchronisation for their correct operation are robust to any unexpected changes to, or loss of, GNSS-derived timing information.

[8] Geosciences Australia, *Southern Positioning Augmentation Network (SouthPAN)*, available online at: https://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-australia/about-the-program/southpan

[9] This is typically achieved through the application of optimal linear estimator (Kalman filter) approaches that make use of additional sensor inputs such as on-board MEMS accelerometers, with monitoring of filter covariance to detect significant changes in uncertainty of the position estimate.

Functional Element	Purpose	Threats (Category)	Mitigations
Parachute Recovery System (PRS)	Deploys aircraft parachute system on command from RPS to initiate controlled descent and landing of RPA.	Uncommanded activation of PRS. (Spoofing) Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository.
Payload subsystems	Achieves mission objectives and fulfils intended operational requirements.	Uncommanded interference with critical RPA subsystems via communication buses or interfaces. (Spoofing) Intentional modification to firmware that degrades or inhibits function or performance. (Tampering) Injection of arbitrary data or executable code into critical RPA subsystems via communication buses or interfaces. (Tampering) Injection of arbitrary data or messages into critical RPA subsystems via communication buses or interfaces. (Denial of Service)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses. For example, serial UART, I2C, SPI, or CAN.
Power Distribution and Management	Provides electrical power system monitoring, power conditioning and regulation, and power system redundancy, failover and electrical load-shedding (as	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or

Functional Element	Purpose	Threats (Category)	Mitigations
	appropriate) between the RPA's on-board batteries and its electrically powered sub-systems.		dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository. Appropriate consideration of system-wide architectures for the physical separation of communications between sub-systems across independent interfaces and message buses. For example, serial UART, I2C, SPI, or CAN.
Remote Pilot Station (RPS)	Provides command of the RPA (via C2/C3 link) and displays real-time display of RPA state, intent, and status to the remote pilot.	Intentional modification to RPS software that degrades or inhibits function or performance. (Tampering)	Routine software updates are appropriately managed to ensure potential vulnerabilities are addressed. RPS command and control element is connected only to known and secure networks (or, alternatively, is 'air-gapped').
Surveillance	Provides ATS facilities and other airspace users with real-time RPA state information (such as position, velocity and pressure altitude) using aeronautical radio communication frequencies and protocols assigned for this purpose (e.g., ADS-B).	Intentional modification to firmware that degrades or inhibits function or performance. (Tampering)	Firmware updates obtained from OEMs or open-source repositories are verified for authenticity (using digital signatures or cryptographic hashes) and potential vulnerabilities (using SBOM or dependency lists) prior to installation. Firmware updates built from source code are audited (at source code level) for differences against sources from an authoritative repository.