UK Civil Aviation Authority

Guidance on Cyber Safety Objectives for Specific Category Operations

CAP 3098

Published by the Civil Aviation Authority, 2025

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

First published April 2025

Enquiries regarding the content of this publication should be addressed to: **Cyber@caa.co.uk**

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP3098

Contents

Introduction

As part of the of the Specific Operation Risk Assessment framework for Remote Piloted Air Systems (RPAS) operations in the specific category, we have considered the Cyber Safety Extension which was published as part of JARUS SORA 2.5 and produced this guidance for operators.

Cyber Security is a fundamental part of ensuring safe RPAS operations, primarily due to the technology involved in both the RPAS itself as well as the ground station and Command & Control (C2) links. In most cases, RPAS face similar threats to those faced by manned aviation, this is why the basic regulation sets out to achieve an equivalent level of safety. This equivalency of safety is met by SORA which uses a holistic safety risk management process to evaluate the risks related to a given operation and then provide proportionate requirements that an operation should meet to ensure a Target Level of Safety is met.

As RPAS are unmanned, they lack the human presence in the aircraft which typically is an important factor in manned aviation system resilience and decision making. This results in an increased reliance on technology and requires that a significant proportion of the resilience, usually assumed by a human, is derived from the system itself. This requires the RPAS to be designed, developed, and operated using secure by design principles to ensure each element/subsystem has basic cyber resilience to achieve the required level of safety. This is important as all technical subsystems consist of hardware and/or software, and each has the potential to introduce cybersecurity vulnerabilities with cyber safety implications.

This CAP defines basic cybersecurity concepts and threats to identify their impact on an operator. The objective of this document is to ensure that reasonable and proportionate cyber safety considerations are applied in the context of the SORA method. Whether a specific OSO must meet a Low, Medium, or High level of robustness is defined by the level of robustness required of the SAIL in the JARUS SORA, section 2.5.2 Step #9 - Identification of Operational Safety Objectives (OSO). The levels of robustness specified for cyber requirements in this extension represent the levels identified in SORA Step #9. The SORA process with the steps can be found in Appendix F.

This includes a minimal level of cyber safety requirements for the:

- proposed operations
- equipment OEMs
- equipment maintainers
- service providers.

These requirements have been allocated to the relevant OSOs with associated levels of assurance.

Acronyms

AES: Advanced Encryption Standard

AMC: Acceptable Means of Compliance

C2: Command and Control

C3 link: Command and control link + additional safety communication link

CAA: Civil Aviation Authority

CISA: Cybersecurity & Infrastructure Security Agency

CISSP: Certified Information Systems Security Professional

CONOPs: Concept of Operations

GCS: Ground Control System

GM: Guidance Material

GNSS: Global Navigation Satellite Systems

ICAO: International Civil Aviation Organisation

IOT: Internet of Things

NCSC: National Cyber Security Centre

NPSA: National Protective Security Authority

OEM: Original Equipment Manufacturer

OSO: Operational Safety Objective

PEDs: Personal Electronic Devices

PKI: Public Key Infrastructure

RMP: Risk Management Program

RPAS: Remote Piloted Air System

SAIL: Specific Assurance and Integrity Level

SLA: Service-Level Agreement

SSL: Secure Sockets Layer

TLS: Transport Layer Security

URL: Uniform Resource Locator

WPA/2/3: Wi-Fi Protected Access / 2 / 3

Applicable Regulation

Article 11 to UK Regulation (EU) 2019/947 – Rules for conducting an operational risk assessment.

Under Article 11, the UK SORA will be used as an acceptable means of compliance (AMC) and this Cyber Extension CAP is part of the AMC for UK SORA.

Article 12 to UK Regulation (EU) 2019/947 - Authorising operations in the 'specific' category

Under Article 12 of the RPAS Regulation, the CAA shall evaluate the risk assessment and the robustness of the mitigating measures that the RPAS operator proposes to keep the RPAS operation safe in all phases of flight. This risk assessment and any corresponding mitigations will need to consider technical measures for the safety and security of the proposed operation.

Annex to UK Regulation (EU) 2019/947 – UAS.SPEC.050

The RPAS Regulation details the requirements for those intending to conduct RPAS activity in the Open or Specific categories within the UK. Part B of the Regulations covers the specific category, with UAS.SPEC.050 describing the responsibilities of the RPAS operator.

Under UAS.SPEC.050 (1) (a) (iii), the RPAS operator shall establish measures to protect against unlawful interference and unauthorised access.

This is one of the regulatory drivers behind providing guidance material to operators in the form of Operation Safety Objectives (OSOs) that are specific to cyber security, as cyber vulnerabilities or weaknesses can pose a significant risk to air safety.

The Cyber OSOs are designed to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain the safety of the RPAS and other airspace users. Not all the objectives are designed to be technical controls to be implemented by the operator, many of them are simple documented processes or procedures that can be put in place to provide a basic level of cyber hygiene.

Definitions and Key Terms

There are several definitions and key terms relating to cyber security:

Cyber Threat

Anything capable of compromising the security of, or causing harm to, information systems and internet connected devices including hardware, software and associated infrastructure, the data on them and the services they provide.

Cyber Safety

Aviation Cyber Safety is seen as the union of cyber security and aviation safety and refers to the protection of aviation operational technologies (such as systems in the Aircraft Control Domain and Ground Control Systems Domain) to prevent cyber related events from affecting Aviation Safety. Operational technologies may rely on corporate IT resources, therefore the dependencies and the assumptions on the security provided by corporate IT shall also be considered.

Jamming

A deliberate blocking or interference with a wireless communication system by transmission of radio signals that disrupt information flow in wireless data networks by decreasing the signal to noise ratio.

OSO Operational Safety Objectives

Operational Safety Objectives are the specific risk mitigation activities used to substantiate the level of integrity and assurance that constitute SORA Robustness. These are detailed in Annex A. This annex provides guidance material (GM) and references industry standards and practices where applicable.

Personal Electronic Devices

Personal Electronic Devices are portable electronic devices such as smartphones, tablets and laptops.

SORA Robustness

To properly understand the SORA process, it is important to understand the key concept of robustness. Robustness is the term used to describe the combination of two key characteristics of a risk mitigation or operational safety objective: the level of integrity (i.e., how good the mitigation/objective is at reducing risk), and the level of assurance (i.e., the degree of certainty with which the level of integrity is ensured).

Spoofing

A technique used to gain unauthorised access to computers whereby an intruder sends messages to a computer indicating that the message is coming from a trusted source.

Unauthorised Access

in connection with the security of systems relating to RPAS operations includes hacking, jamming, or spoofing of services; also includes physical access to systems such as the GCS or RPAS.

Unlawful Interference

These are acts or attempted acts such as to jeopardize the safety of civil aviation, including but not limited to: unlawful seizure of aircraft, destruction of an aircraft in service, use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment.

Prior to Application

Cyber Security Culture

Following the publication of JARUS SORA 2.5 Cyber Safety Extension and the subsequent UK SORA project, it is of vital importance that organisations consider cyber security as part of their safety processes. Many of the enabling systems for RPAS operations rely on technology, which means they can be vulnerable to malicious activity and something that isn't secure may pose an air safety risk.

The effective culture of Cyber Safety relies heavily on the buy-in from the highest levels within an organisation; therefore, affirming a business level commitment to fully understand and address cyber-safety is essential and serves as the catalyst towards establishing an organisational commitment to cyber safety.

It is important to the regulator that organisations seek the highest-level executive sponsorship within their business and utilise this to address cyber-safety within their proposed operations.

Threat Analysis and Risk Assessment

This activity requires an applicant to undertake a risk assessment which has been informed by threat analysis, some useful publications to inform this assessment have been published by the NPSA[1] and MITRE[2]. Both the assessment and mitigations should have a focus on the applicant's cyber security policies and plans, as well as the physical security of the operational environment.

Further Information

The CAA website[3] has more information on cyber security certification, as well as information published by ICAO[4] and CISA[5] on addressing RPAS threats and actions to take.

[1] National Protective Security Authority

[2] Mitre Engenuity

[3] CAA Cyber Security

[4] ICAO RPAS

[5] CISA Air Aware

Operational Safety Objectives

Operational Safety Objectives 01 – Ensure the Operator is competent and/or proven.

Cyber Criterion #1 – Organisation Culture

Low - SAIL (II)

Integrity

The applicant shall have sponsorship for cyber safety that includes the followings:

a. Highest-level executive sponsorship for Cyber safety.
b. A Cyber safety policy letter that identifies organisational stakeholder roles and responsibilities.
c. A Cyber safety awareness and training course such that stakeholders within organizations clearly understand their role in cyber safety.

Assurance

a. The applicant declares that an effective cyber safety organisational culture is in place.

Medium - SAIL (III)

Integrity

Same as Low, in addition:

a. The applicant shall maintain:
    i. A recurring training program on new and evolving cyber safety threats.
    ii. Training program procedures that identify staff who require such training and frequency of their refresher training.
b. The applicant shall also establish and follow a framework to address cyber safety.
c. The role of cyber safety manager shall equally be designated**.** i.e., the responsible person is identified, and exercises duties according to the demand.

Assurance

a. The applicant has supporting evidence that policies addressing cyber safety exist and that all required training is being conducted and is effective.

Guidance Material

a. Staff should get refresher training annually.

High - SAIL (IV, V, VI)

Integrity

Same as Medium, in addition:

a. The role of cyber safety manager shall be dedicated to an identified person exercising responsibility for implementing and maintaining an effective cyber safety program within their organisation.

Assurance

Same as Medium, in addition:

a. The Policies are validated, and the training is verified by a competent third party.
b. The applicant possesses an industry recognized cybersecurity accreditation that recognise compliance with the relevant standards by CMMI Institute, NIST or ISO in compliance with applicable legislation.

Cyber Criterion #2 - IT and Data Security

Low - SAIL (II)

Integrity

a. The applicant shall have a corporate policy that addresses IT and data security, including physical access to electronics, lab equipment, and data.
b. The policy shall include Role-based authentication for safety-critical data access.
c. Terms of Service and privacy policies for safety critical equipment and services shall be readily available.

Assurance

a. The applicant declares that IT and Data Security policies are in place.

Medium - SAIL (III)

Integrity

Same as Low, in addition:

a. The applicant shall ensure that computers and PEDs used for business-related activities are physically secured when not in use. Hard drives shall be encrypted.
b. The applicant's corporate policy shall support multiple authentications as per CISSP Common Body of Knowledge:
    - Type 1 (Something you know).
    - Type 2 (Something you have); and
    - Type 3 (Something you are) authentication factors.
c. The applicant's IT systems shall support logging of anomalies or malicious activities based on configured polices and rules.

Assurance

a. The applicant has evidence that IT and Data Security policies are in place and are being followed.

Guidance Material

a. Logging functionality is widely available in various commercial security suites and could be a valuable input for further analysis in industry groups.
b. Physically secured does not necessarily mean locked in a vault. It could be just that operator's place of business is secured when no one is there.

High - SAIL (IV, V, VI)

Integrity

Same as Medium, in addition:

a. The applicant shall develop a policy for monitoring and updating corporate IT and data security policies and practices as required for evolving threats.
b. Operational Safety Critical Data at rest shall be encrypted.

Assurance

a. Corporate policies are validated by a competent third party.

Guidance Material

a. A geofence definition would be one example of safety critical data at rest.

Cyber Criterion #3 – Industry Group Participation

Low - SAIL (II)

Integrity

a. The applicant shall subscribe to and/or regularly consults the website officially supported/recommended by the RPAS supplier/manufacturer to keep aware of any necessary software/hardware updates linked to potential security breaches.

Assurance

a. The applicant declares appropriate awareness is being maintained.

Medium - SAIL (III)

Integrity

Same as Low, in addition:

a. The applicant shall subscribe to broader notifications regarding active threats and appropriate supplier/manufacturer update channels to maintain awareness of needed enterprise software/hardware updates.

Assurance

a. The applicant has evidence that appropriate awareness is maintained, active threat notifications are received, and flight logs (criterion #6) are being analysed for anomalies.

High - SAIL (IV, V, VI)

Integrity

Same as Medium, in addition:

a. The applicant's dedicated cybersecurity manager shall be a member of an industry group deemed appropriate by the CAA.

b. The applicant shall capture, track and address shortfalls in security processes and shall verify fixes are effective.

Assurance

Same as Medium.

Cyber Criterion #4 – Risk Management Program

Low - SAIL (II)

Integrity

a. The applicant's RMP shall include both safety and security risk analyses.

Assurance

Not Applicable.

Medium - SAIL (III)

Integrity

a. Same as Low SAIL requirement.

Assurance

a. Documentation is provided that includes an audit of the organization's RMP is in place and effective.

High - SAIL (IV, V, VI)

Integrity

Same as Medium, in addition:

a. RMP has been validated and verified.

b. The organisation follows a life-cycle management approach for continuous evolution and improvement.

Assurance

a. Documentation is provided that the organization's RMP has been independently verified and shows that the implemented RMP has an effective life-cycle management.

Cyber Criterion #5 – Audit Program for Cyber-Safety Issues

Low - SAIL (II)

Integrity

a. The applicant has a self-inspection process.

Assurance

a. The applicant declares audits are being conducted.

Medium - SAIL (III)

Integrity

a. The applicant has a basic internal audit program.

Assurance

a. The audit program is documented.

Guidance Material

a. A basic internal audit programme ensures each OSO with cyber implications has been at least broadly addressed.

High - SAIL (IV, V, VI)

Integrity

a. The applicant has a robust audit program.

Assurance

a. Audits are conducted by an external, independent, qualified entity.

Guidance Material

a. A robust internal audit program ensures each topic within the OSOs with cyber implications has been specifically addressed.

Cyber Criterion #6 – Flight Logs

Low - SAIL (II)

Integrity

a. Since some cyber-attacks can be intermittent and difficult to track, it is important that the applicant implements a method by which RPAS activities are logged for subsequent analysis.
b. Besides the main attribute from the system, the log must record any security events which can later be used to detect anomalies and/or suspicious activities. This maybe a written log or electronic.

Assurance

a. The applicant can declare that they perform this activity.

Guidance Material

a. The log may be in written or electronic format.

Medium - SAIL (III)

Integrity

Same as Low, in addition:

a. The log file should be stored electronically and have basic integrity protection.

Assurance

a. The applicant must document this activity, the analysis results of log data is in an auditable format and used to find anomalies.

Guidance Material

a. Basic integrity protections are to ensure log files cannot be changed without knowledge - Log files are to be kept in two distinct forms; an original log file and an auditable log file kept separately to ensure no accidental or malicious changes affect the logs.

High - SAIL (IV, V, VI)

Integrity

Same as Medium, in addition:

a. The log file should be stored tamper proof.

Assurance

Same as Medium, in addition:

a. The applicant conducts regular/recurring log (not event triggered) analysis, and the procedures are validated by a competent third party.

Operational Safety Objective 03 – RPAS maintained by competent and/or proven entity.

Cyber Criterion #1 – Malware Protection

Low - SAIL (I, II)

Integrity

a. The applicant has maintenance procedures aiming at verifying the authenticity of firmware/software sources.

Assurance

a. The applicant declares that maintenance procedures exist with the objective to reduce the risk of introducing malware during maintenance activities.

Acceptable Means of Compliance

a. For the integrity requirement the applicant may include checking the correct website/URL and verification of valid and authentic SSL certificates for https connections before downloading software updates to the RPAS and supporting equipment.

Medium - SAIL (III, IV)

Integrity

Same as Low, in addition:

a. Procedures to verify the authenticity and integrity of the software, and

b. Procedures to regularly scan maintenance related computers and removable media for malware.

Assurance

a. The applicant has supporting documentation that maintenance procedures exist to address with the objective to reduce the risk of introducing malware during maintenance activities.

Acceptable Means of Compliance

a. For the integrity requirement the applicant may include a process such as verifying check sums and digital signatures (e.g., PKI), as well as scanning the software for malware prior to installation. This does not require new procedures to be developed if the applicant employs appropriate security software that performs the same task.

High - SAIL (V, VI)

Integrity

Same as Medium, in addition:

a. Employment of advanced malware protection.

Assurance

Same as Medium, in addition:

a. The procedures are validated by a competent third party.

Acceptable Means of Compliance

a. To provide advanced malware protection methods, organisations may employ separate testing environments that allow:
   - continuous monitoring of systems,
   - retrospective alerting and remediation, and
   - the implementation of protection mechanisms for multiple attack vectors/entry points (firewall, network, endpoint, email),
   - for a malware to be examined in a secure environment and analyse the intent of a given malicious software (it is acknowledged that this is an advanced capability).

Cyber Criterion #2 – Supply Chain Management

Low - SAIL (I, II)

Integrity

a. Computer systems and associated hardware/software and support services used in the maintenance of RPAS are sourced from reputable suppliers.

Assurance

a. The applicant declares that reasonable and appropriate supply chain security measures have been taken.

Guidance Material

a. Systems used for maintenance include but are not limited to:
   - RPAS spare parts,
   - Maintenance computers,
   - Diagnostic equipment,
   - GCS software,
   - RPS software,
   - Diagnostic software.

Medium - SAIL (III, IV)

Integrity

Same as Low SAIL requirement.

Assurance

a. The applicant has supporting documentation that reasonable and appropriate supply chain security measures have been taken.

High - SAIL (V, VI)

Integrity

Same as medium, in addition:

a. Computer systems and associated software used in the maintenance of RPAS are sourced from trusted suppliers. For example, components may have a Hash and digital signature associated with them to verify authenticity.

Assurance

Same as Medium, in addition:

a. The measures are validated by a competent third party.

Cyber Criterion #3 – Physical Security

Low - SAIL (I, II)

Integrity

a. The applicant applies basic physical security principles against unauthorised access or theft.

Assurance

a. The applicant declares they have adequate physical security provisions.

Acceptable Means of Compliance

a. For the integrity requirement this may include a time-out policy for systems such as mobile phones and computers.

Medium - SAIL (III, IV)

Integrity

Same as Low, in addition:

a. Computers used for the maintenance of the RPAS are physically secured when not in use.

Assurance

a. The applicant has documentation that they have adequate physical security provisions.

Acceptable Means of Compliance

a. Physical security could include locking maintenance computers in a secure cabinet or locking the maintenance facility when not in use.

High - SAIL (V, VI)

Integrity

Same as Medium, in addition:

a. Physical access to the RPAS is controlled.

Assurance

Same as Medium, in addition:

a. The physical security provisions are validated by a competent third party.

Cyber Criterion #4 – Controlled Access

Low - SAIL (I, II)

Integrity

a. The applicant ensures that access to computers, computer networks and information systems used for RPAS maintenance have basic access controls.

Assurance

a. The applicant declares that they employ basic access controls.

Guidance Material

a. As a minimum, the applicant should implement username and a password following NCSC guidance.

Medium - SAIL (III, IV)

Integrity

Same as Low, in addition:

a. access is restricted to only authorized maintenance personnel requiring access.

b. Data access controls with tracking and record or data management practices.

Assurance

a. The applicant has documentation that access controls are employed.

Guidance Material

a. Access in this context refers to computer user accounts used to log into maintenance computers, networks, and information systems. Action should include restricting individual user accounts to a level appropriate to the role undertaken by the person.

High - SAIL (V, VI)

Integrity

Same as Medium, in addition:

a. Individual user accounts are set to a level appropriate to the role undertaken by each maintainer, and

b. Access employs two-factor authentication.

c. Data encryption in transit and at rest.

Assurance

Same as Medium, in addition:

a. Access controls are validated by a competent third party.

Cyber Criterion #5 – Wireless Access Protected

Low - SAIL (I, II)

Integrity

a. Wireless networks used in the maintenance of the RPAS has basic encryption of the network traffic enabled.

Assurance

a. The applicant declares that all wireless networks used in the maintenance of the RPAS have basic network traffic encryption enabled.

Acceptable Means of Compliance

Some basic encryption examples that the applicant can use:

1. AES,
2. WPA2 Enterprise,
3. WPA3,

Guidance material

a. As a minimum, the applicant should change any default credentials that the system was shipped with and implement a username and a password following NCSC guidance to access the wireless network.

Medium - SAIL (III, IV)

Integrity

Same as low, in addition:

a. Advanced/stronger encryption of the network traffic is enabled.

Assurance

a. The applicant has documentation that all wireless networks used in the maintenance of the RPAS utilize advanced/stronger encryption for the network traffic.

Guidance Material

a. The applicant should use an algorithm of strength like WPA2 Enterprise or greater.

High - SAIL (V, VI)

Integrity

Same as Medium, in addition:

a. Strong network encryption and access control/user or device authentication is employed.

Assurance

Same as Medium, in addition:

a. The security and encryption measures are validated by a competent third party.

Guidance Material

a. Applicant should have a system with similar strength of 802.1X authentication.

Cyber Criterion #6 – Software/Firmware Updates

Low - SAIL (I, II)

Integrity

a. The applicant has update management procedures to check for, verify authenticity, and apply original equipment manufacturer (OEM) updates.

Assurance

a. The applicant declares that maintenance procedures exist to review OEM security updates for applicability and are installed where appropriate.

Guidance Material

a. This should include updates to all supporting infrastructure.

Medium - SAIL (III, IV)

Integrity

Same as Low, in addition:

a. Maintenance procedures to check other computer systems used in the maintenance of the RPAS.

Assurance

a. The applicant has supporting documentation showing maintenance procedures exist to review OEM security updates for applicability and are installed where appropriate.

High - SAIL (V, VI)

Integrity

Same as Medium, in addition:

a. Maintenance procedures review OEM security updates to all computer systems used in the maintenance of the RPAS for applicability and installed where appropriate.

b. The organisation implements change management policies to test updates before installation, which reduces risks of detrimental operational impacts of installed updates.

Assurance

Same as Medium, in addition:

a. The procedures are validated by a competent third party.

Operational Safety Objective 05 – RPAS is designed considering system safety and reliability.

Cyber Criterion #1 – Cyber Safety Risk Assessment

Low - SAIL (I, II)

Integrity

a. The applicant reviews the CONOPs for cyber threats like those discussed in Appendix E and Appendix C of this CAP and selects a RPAS that employs Concepts from Appendix E and the Mitigations in Appendix D.

Assurance

a. The applicant declares that a basic security assessment and threat mitigations have been undertaken.

Acceptable Means of Compliance

a. For the integrity requirement, the applicant may provide a high-level documentation that outlines their process for selection of the RPAS and how they believe the system has the appropriate mitigations against the threats presented in Appendix C and Annex B for how to do a basic security assessment.

Medium - SAIL (III, IV)

Integrity

Same as Low, in addition:

a. The applicant performs a cyber safety risk assessment using a standard acceptable to the CAA.

Assurance

a. The applicant has supporting documentation that a security risk assessment and threat mitigations have been undertaken.

Acceptable Means of Compliance

a. For the integrity requirement, the applicant may use
   i. ISO27005 risk assessment methodology,
   ii. NIST 800-53 risk assessment (Cyber Security Framework),
   iii. Cyber Security Risk Foundation (CRF) – CRF GRM,
   iv. the method presented in Annex B.

High - SAIL (V, VI)

Integrity

Same as Medium SAIL requirement.

Assurance

Same as Medium, In addition:

a. The assessment is validated by a competent third party.

Cyber Criterion #2 – GNSS Equipment, if used

Low - SAIL (I, II)

Integrity

a. The applicant employs basic threat mitigations.

Assurance

a. The applicant declares that basic threat mitigations are employed.

Medium - SAIL (III, IV)

Integrity

Same as low, in addition:

a. The applicant implements health monitoring and reporting of received signal strength, number of satellites, including identification and time comparisons.

b. The applicant implements GNSS jamming detection.

c. The GNSS equipment makes use of multi-constellation GNSS.

Assurance

a. The applicant has supporting documentation that has evidence for threat mitigations are employed.

High - SAIL (V, VI)

Integrity

Same as Medium SAIL requirement.

Assurance

Same as medium, In addition:

a. The threat mitigations are validated by a competent third party.

Cyber Criterion #3 – Resilience in the Face of a Cyber Attack

Low - SAIL (I, II)

Integrity

a. The applicant reviews the CONOPs for cyber threats like those discussed in Appendix E and Appendix C of this Extension and selects a RPAS that employs Concepts from Appendix B and the Mitigations in Appendix C such that probable cyber threats should not result in the RPAS departing the operational volume.

Assurance

a. The applicant declares that the evaluation has been undertaken.

Medium - SAIL (III, IV)

Integrity

Same as low, in addition:

a. The review is performed using an acceptable industry standard.

Assurance

a. The applicant has supporting documentation that the evaluation has been undertaken.

Acceptable Means of Compliance

a. The applicant may use the NCSC Cyber Incident Response process.

High - SAIL (V, VI)

Integrity

Same as medium

Assurance

Same as Medium, in addition:

a. The evaluation is validated by a competent third party.

Cyber Criterion #4 – Life Cycle Security Appraisal

Low - SAIL (I, II)

Integrity

a. The applicant has procedures to re-accomplish the review called out in Criterion #1, whenever new or recently uncovered cyber threats are identified.

Assurance

a. The applicant declares that procedures exist to update the Security Risk Assessment.

Guidance Material

a. The applicant should establish the verification period for each threat identified in the Security Risk Assessment and when there is an event which reveals a change in the scenario/assumptions used for the assessment.

Medium – (III, IV)

Integrity

Same as Low

Assurance

a. The applicant has supporting documentation that procedures exist to update the Security Risk Assessment.

High – (V, VI)

Integrity

Same as Medium

Assurance

Same as medium, in addition:

a. The procedures are validated by a competent third party.

Cyber Criterion #5 – Test and Security Validation

Low - SAIL (I, II)

Integrity

Not Applicable

Assurance

Not Applicable

Medium - SAIL (III, IV)

Integrity

a. The applicant evaluates the effectiveness of threat mitigations identified as part of adherence to this guidance using an acceptable industry standard.

Assurance

a. The applicant has supporting documentation that the evaluation of mitigation effectiveness has been undertaken.

High - SAIL (V, VI)

Integrity

Same as medium. In addition:

a. Evaluation is performed using a recognized aeronautical standard.

Assurance

Same as medium, in addition:

a. The evaluation of mitigation effectiveness is validated by a competent third party.

Operational Safety Objective 06 – C3 Link Characteristics (E.G. Performance, Spectrum use) Are Appropriate for the Operation

Cyber Criterion #1 – Datalink Encryption

Low - SAIL (II, III)

Integrity

Not applicable

Assurance

Not applicable

Medium - SAIL (IV)

Integrity

a. The C3 link employs encryption.

Assurance

a. The applicant has documentation showing that link is properly encrypted.

High - SAIL (V, VI)

Integrity

a. The C3 link meets the minimum operational performance standards defined in RTCA DO-377B or similar.

Assurance

Same as Medium, in addition:

a. The datalink encryption is validated by a competent third party.

Cyber Criterion #2 – Authentication

Low - SAIL (II, III)

Integrity

a. The datalink employs basic mutual peer entity authentication between the GCS and RPAS.

Assurance

a. Applicant declares that data link employs basic authentication.

Acceptable Means of Compliance

a. The applicant may use TLS 1.3 and beyond in addition to passwords for basic authentication.

Medium - SAIL (IV)

Integrity

a. The datalink employs advanced mutual peer entity authentication between the GCS and RPS.

Assurance

a. Applicant has documentation showing that link employs advanced authentication methods.

Acceptable Means of Compliance

a. The applicant may use an industry standard IOT cyber security best practice for authentication to meet the intent of advanced authentication.

High - SAIL (V, VI)

Integrity

a. The datalink employs aviation standard authentication methods or equivalent. In addition, human to machine interfaces employ multifactor authentication.

Assurance

Same as Medium, in addition:

a. The authentication methods are validated by a competent third party.

Acceptable Means of Compliance

a. The applicant may use the PKI certificates as described in ATA specification No 42 to meet the intent of aviation standard authentication.

Cyber Criterion #3 – Access Control

Low - SAIL (II, III)

Integrity

a. The control station is paired with the GCS using as a minimum a password. Default passwords are changed and meet security best practices for length, complexity, expiration, history as best as configuration settings allows.

Assurance

a. The applicant declares that data link employs basic access control.

Medium - SAIL (IV)

Integrity

Same as low, in addition:

a. The system implements the concept of least privileged access.

Assurance

a. The applicant has documentation showing that link employs advanced access control functions.

High - SAIL (V, VI)

Integrity

Same as medium, in addition:

a. Human to machine interfaces utilise multifactor access control, and machine to machine interfaces utilise aviation standard access control methods according to the CAA/competent authorities' requirements.

Assurance

Same as Medium, in addition:

a. The access control functions validated by a competent third party.

Guidance Material

a. Access control in this respect is the ability to restrict utilisation of the datalink. In the absence of an authentication-based access system, a physical security plan acceptable to CAA should be employed.

Cyber Criterion #4 – Data Integrity and Anti-Replay Protections

Low - SAIL (II-III)

Integrity

Not Applicable

Assurance

Not Applicable

Medium - SAIL (IV)

Integrity

a. The datalink employs industry standard IOT cybersecurity best practices.

Assurance

a. The applicant has documentation showing that the data link employs advanced data integrity and anti-replay protection.

High - SAIL (V, VI)

Integrity

a. The datalink employs aviation standard data integrity and anti-replay protection methods or equivalent.

Assurance

Same as Medium, in addition:

a. The data integrity and anti-replay protection functions are validated by a competent third party.

Operational Safety Objectives 13 – External Services Supporting RPAS Operations Are Adequate to the Operation

Low - SAIL (I, II)

Integrity

a. The level of Cybersecurity for any externally provided service necessary for the safety of the flight is adequate for the intended operation. If the externally provided service requires communication between the operator and service provider, effective communication to support the service provisions is in place. Roles and responsibilities between the applicant and the external service provider are defined.

Assurance

a. The applicant declares that the requested level of cybersecurity for any externally provided service necessary for the safety of the flight is achieved (without evidence being necessarily available).

Medium – SAIL (III, IV)

Integrity

Same as Low.

Assurance

a. The applicant has supporting evidence that the required level of cybersecurity for any externally provided service required for safety of the flight can be achieved for the full duration of the mission. This may take the form of a Service-Level Agreement (SLA) or any official commitment that prevails between a service provider and the applicant on relevant aspects of the service (including quality, availability, responsibilities).
b. The applicant has a means to monitor externally provided services which affect flight critical systems and take appropriate actions if lapses in cyber safety could lead to the loss of control of the operation.

High – SAIL (V, VI)

Integrity

Same as Medium.

Assurance

Same as Medium, in addition:

i. The evidence of the externally provided service cybersecurity is achieved through demonstrations.
ii. A competent third party validates the claimed level of integrity.

Appendix A: Operational Safety Objectives Tables

OSO #01- Ensure the Operator is competent and/or proven.

		SAIL Level					
		SAIL I	**SAIL II**	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**
OSO #01 Ensure the Operator is competent and/or proven	Cyber Criterion #1 Organisation Culture	None	Low	Medium	High	High	High
	Cyber Criterion #2 IT and Data Security	None	Low	Medium	High	High	High
	Cyber Criterion #3 Industry Group Participation	None	Low	Medium	High	High	High
	Cyber Criterion #4 Risk Management Program	None	Low	Medium	High	High	High
	Cyber Criterion #5 Audit Program for Cyber Safety issues	None	Low	Medium	High	High	High
	Cyber Criterion #6 Flight Logs	None	Low	Medium	High	High	High

OSO #3 - RPAS Maintained by competent and/or proven entity.

		SAIL Levels					
		SAIL I	**SAIL II**	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**
OSO #3 RPAS Maintained by competent and/or proven entity	Cyber Criterion #1 Malware Protection	Low	Low	Medium	Medium	High	High
	Cyber Criterion #2 Supply Chain Management	Low	Low	Medium	Medium	High	High
	Cyber Criterion #3 Physical Security	Low	Low	Medium	Medium	High	High
	Cyber Criterion #4 Controlled Access	Low	Low	Medium	Medium	High	High
	Cyber Criterion #5 Wireless Access Protected	Low	Low	Medium	Medium	High	High
	Cyber Criterion #6 Software/Firmware Updates	Low	Low	Medium	Medium	High	High

OSO #5- RPAS is designed considering system safety and reliability.

		SAIL Levels					
		SAIL I	**SAIL II**	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**
OSO #5 RPAS is designed considering system safety and reliability	Cyber Criterion #1 Cyber Safety Risk Assessment	Low	Low	Medium	Medium	High	High
	Cyber Criterion #2 GNSS Equipment, if used	Low	Low	Medium	Medium	High	High
	Cyber Criterion #3 Resilience in the Face of a Cyber Attack	Low	Low	Medium	Medium	High	High
	Cyber Criterion #4 Life Cycle Security Appraisal	Low	Low	Medium	Medium	High	High
	Cyber Criterion #5 Test and Security Validation	Low	Low	Medium	Medium	High	High

OSO #6 - C3 link characteristics (e.g. performance, spectrum use) are appropriate for the operation.

		SAIL Levels					
		SAIL I	**SAIL II**	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**
OSO #6 C3 link characteristics (e.g. performance, spectrum use) are appropriate for the operation	Cyber Criterion #1 Datalink Encryption	None	Low	Low	Medium	High	High
	Cyber Criterion #2 Authentication	None	Low	Low	Medium	High	High
	Cyber Criterion #3 Access Control	None	Low	Low	Medium	High	High
	Cyber Criterion #4 Data Integrity and Anti-Replay Protections	None	Low	Low	Medium	High	High

OSO #13 - External Services Supporting RPAS Operations are adequate to the operation

		SAIL Levels					
		SAIL I	**SAIL II**	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**
OSO #13 External Services Supporting RPAS Operations are adequate to the operation	Cyber Criterion #1	Low	Low	Medium	Medium	High	High

Appendix B: Threat Analysis and Risk Assessment

i. System Scoping and Asset Identification

System scoping or critical system scoping is an activity that is intended to assist in the identification and documentation of cyber related mission critical processes, and the associated assets and services which support these processes that would impact safety. This activity will aid in applying comprehensive, appropriate, and proportionate cyber security measures. Appropriate personnel should be included in the scoping activity to ensure complete coverage of your systems and processes, for example, Subject Matter Experts within Safety, Security, and Engineering.

When identifying the scope of system critical processes, the CAA recommends you make an informed and competent consideration of reasonable and expected impacts. The CAA recommends that you ignore implausible scenarios or highly complex chains of events or failures — a reasonable worst-case scenario should be used.

To ensure that the scope is accurate and includes mission critical processes that would reasonably be considered in scope, it is advised that you use a logical method and include all stakeholders deemed relevant by the organisation (e.g., workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc).

Appendix D provides an overview of the systems that should be considered as a minimum as part of your system scoping exercise.

You are ultimately responsible for your own risks and the identification and validation of your mission critical process scope. Whereby if you are utilising third party systems in your product, then we encourage you to have assurance from your third-party vendors regarding their cyber security via some form of written record by a responsible person in the third-party organisation.

ii. Threat Analysis

The threat landscape constantly evolves, with the number of new threats growing exponentially. It is therefore imperative that you have an approach to evaluate the threat at appropriate intervals or as an ongoing task. You may wish to use external organisations to perform threat analysis if you do not possess the knowledge to perform this internally.

The NCSC provide weekly threat reports as well as sector specific threat reports. We encourage you to engage with the NCSC to better understand the threat and to receive any other cyber security support. The latest threat reports can be found on the NCSC's website and you can sign-up to the NCSC Early Warning system.

You can do an annual threat analysis of your corporate enterprise system as well as the system you are developing to understand system vulnerability. Threat analysis activities can be made through systematic and evidencable approaches such as STRIDE, TVRA, MITRE ATT&CK etc.

The threat analysis above, alongside asset identification will provide the fundamental information a developer will require to undertake a thorough cyber risk assessment.

Appendix C provides a general overview of the threats that you may encounter as a RPAS operator.

iii. Risk Assessment

The risk assessment can classify the risk in likelihood and severity or impact levels and should have a named individual assigned as an owner to each individual risk.

It's highly likely that there will be crossovers between safety risks and security risks. It is important that the developer clearly documents the relationships between these risks. Where these risks are already identified in a safety risk assessment, the link to the cyber event should be clearly identified in the safety risk assessment and noted in the cyber security risk assessment documentation.

Risks can be calculated to understand historic, current, and residual risks. Developers can also consider the controls that are in place for each risk, and these should be documented in the risk assessment. Where there is a control, a residual risk column can be included to indicate how the implemented control reduces the risk scores.

Where a developer is considering using third-party technologies, software, or services, consideration around the security impact and associated risks of such suppliers ought to be considered and documented within the risk assessment. Further guidance around supply chain security is available from NCSC.

iv. Risk Response

Based on your risk assessment, each risk should have 1 of 4 risk responses:

- Treat
- Tolerate
- Transfer
- Terminate

Risk responses of Treat, Tolerate, Transfer or Terminate are widely accepted terminologies when assessing what the appropriate response for a particular risk statement is. We recommend that you consider the 'why' behind your reasoning as part of the risk assessment documentation. Should you deem a risk is transferable, it is advisable you detail who the risk is being transferred to and why, alongside any formal agreements that will detail the risk transfer and a piece of evidence that confirms the risk has been transferred to the transferee. Where treat is used as a response, the appropriate evidence would need to be documented in the control's column of the risk assessment documentation.

v. Example Risk Assessment Temple

This section provides example titles that organisations can use to present the cyber security risk assessment.

Titles	Descriptions
Risk ID	It is a good practise to have an internal Risk ID for the identified cyber risks which can be linked to an Haz Log, if the cyber risk contributes to safety hazard.
Department	The internal department that owns the responsibility of the asset. E.G. If it is an internally developed or externally bought RPAS component/sub-system then it will be the engineering or if it is the company IT, then it's the IT.
Asset	What is the asset? Computer, laptop, network card, C2 module (RF Card), camera, LIDAR etc. Should include system name (model no)
Supplier	Supplier of the system or the end user of the system
Threat	Threat types mentioned in Appendix C.
Vulnerability	Vulnerability, either ones you have acquired via the NCSC channel or the ones you have identified from publicly available CVEs or ones you have identified through internal vulnerability testing of the system.
Probability	The probability of the vulnerability being exploited, be realistic with your numerical/qualitative analysis. These are pre-mitigation values
Impact	If the vulnerability is exploited, the impact on the operation, whether that be drone operation or business operation, be realistic like the above-mentioned exercise. These are pre-mitigation values.
Risk Rating	The combined value of the probability (p) and impact (i); usually p.x.i
Risk Owner	Named senior responsible owner (that can be the post the individual holds within the organisation)
New Probability	This is post-mitigation value of the probability of a vulnerability being exploited.
Implemented Controls/Mitigation	Controls that have been implemented to mitigate the vulnerability or will be implemented to mitigate the vulnerability
New Impact	This is post-mitigation value of the impact of a vulnerability being exploited
Residual Risk Rating	The new combined value of the probability and impact: p.x.i

Appendix C: Cyber Threats

i. Denial of Service/Distributed Denial of Service (DoS/DDoS)

A Denial of Service/Distributed Denial of Service (DoS/DDoS) is an attack on an Information and Computer Technology (ICT) system where the attacker's objective is to either disrupt the service provided by an ICT resource to make it temporarily or indefinitely unavailable. The attacker typically floods the target system with superfluous requests to overload it and prevent it from processing legitimate requests. A DDoS is an amplified version of a DoS which is characterised by flooding the target system from multiple, distributed systems at the same time, which makes it difficult or impossible to stop by blocking individual attack sources.

In addition, electromagnetic jamming can also be understood as a form of DoS/DDoS because it saturates the electromagnetic spectrum to such a degree that signals between e.g., an Unmanned Aircraft System (UAS) and the operator (ground control station) cannot be transmitted reliably anymore.

ii. Hijacking

Hijacking is a type of network security attack whereby the attacker takes control of a communication link between two entities and masquerades as one of them.

iii. Malware

Malware is malicious software designed to compromise the confidentiality, integrity and/or availability of information, data, and/or communications technology system or network. Examples of malware include software that disables virus protection software, trojans, ransomware, and other types of malicious code which could allow an attacker to take over operational control of the UAS. To provide advanced malware protection methods, organizations may employ separate testing environments that allow:

- continuous monitoring of systems,
- retrospective alerting and remediation, and
- the implementation of protection mechanisms for multiple attack vectors/entry points (firewall, network, endpoint, email),
- for a malware to be examined in a secure environment and analyse the intent of a given malicious software (it is acknowledged that this is an advanced capability),

Malware is often used in cyber-crime activities and can be designed to execute targeted attacks such as causing damage to safety-relevant systems. In aviation, a malware infection could result in catastrophic outcomes in both ground and airborne systems. Thus, appropriate protection mechanisms must be an integral part in the Design, Development, Deployment and Operations of system elements, and is a recurring activity throughout the system's lifecycle.

iv. On-path attack

This is a type of attack where a hacker positions themselves between two systems in a communication channel to steal sensitive information. This attack involves either eavesdropping or impersonating one of the systems. This attack can take the form of intercepting traffic; where an attacker will install a software on a system, listen in on the local network or redirect data to pass through a node they control, using malicious apps; attacker can inject code into an application or use malicious apps to intercept data, or spoofing; attacker can impersonate the system and generate believable system messages (text, voice on a call or an entire communication system).

v. Open-Source Software Supply Chain Attack

Software library attack is a type of cyber-attack that occurs when malicious code is inserted into a third-party library that is used by developers to create software. This attack works by identifying libraries or software dependencies which have weak security (e.g. Code checks or authentications) and then injecting malicious code into the codebase. The developers then use infected library or dependency in their software, making it vulnerable. The attacker now has access to the software and the system it runs on.

vi. Spoofing

Spoofing is an attack whereby an attacker disguises a fake information source to make it appear legitimate. A common method of overloading a system with spoofed information is known as spamming. Spoofing is one of the most common forms of cyber-crime. Typically, the attacker creates spoof spam with the intention of illegitimately gathering information from the user but can also include more direct effects such as providing false navigation/position information. Spoofing can also happen in the RF domain when the signals are not adequately cryptographically protected.

Appendix D: Basic UAS security impacted areas of cyber safety

In general, UAS face very similar threats to those faced by manned aviation. However, as UAS are unmanned, they lack the human presence in the aircraft which typically is an important factor in manned aviation system resilience. This results in an increased reliance on the technology in use and requires that a significant fraction of the resilience, usually assumed by a human, is derived from the system itself. This requires the UAS to be designed and developed using security by design principles to ensure each element/subsystem has basic cyber resilience to achieve the required level of safety. This is important as all technical subsystems consist of hardware and/or software, and each has the potential to introduce cybersecurity vulnerabilities (e.g. weaknesses in processes, products and people that can be exploited) with cyber safety implications.

Vulnerabilities in hardware can either be exploited through physical access or through exploiting existing or intentionally placed weaknesses within the system architecture or lifecycle management processes (e.g., through the supply chain). In contrast to software that runs on top of or makes use of hardware, it is important to note that firmware is considered part of hardware when programmed in a read only memory (ROM) as it controls the hardware's basic behaviour and acts as its "operating system", especially in the context of field-programmable gate arrays (FPGAs).

Software is designed and developed to control hardware. Vulnerabilities in software can be introduced/exploited throughout all lifecycle stages, from design, development, deployment and operations. In some cases, also the decommission phase could introduce vulnerabilities, e.g., when they allow for the exfiltration of cryptographic keys if they haven't been appropriately removed or destroyed. Attacks can range from remote code injection, DoS, up to sending unintended aircraft commands.

Below are some examples of the UAS subsystems that should be developed using security by design principles to protect against cyber safety threats. These principles, in many cases may lie within the responsibility of the OEM. Where applicable and possible, we provide examples for threats, consequences, and potential mitigations for each subsystem. The provided threats, consequences and mitigations do not intend to satisfy completeness because this would quickly exceed the scope of this document.

i. Base System

The “Base System” can be understood as the “operating system” or “motherboard” of the UAS which allows, manages, and controls the communication between the various subsystems.

Threats and consequences

The base system is the main interface through which all the other subsystems like sensors, transceivers, etc. are connected and communicate with each other. If not thoroughly designed a compromise by malware could have severe consequences up to loss of control of the UAS or malicious takeover by an attacker. Threats can materialise through poor supply chain management, bad system design where uncontrolled or even unknown connections with the base system are possible but also through vulnerabilities in base system components. An example for latter could be the vulnerability of certain processor families, allowing altering of functions.

Mitigations

Application of the “Security by Design” concept, establishment of a “Supply Chain Security Management” and appropriate “Defence in Depth” principles along with trusted execution, when possible, to create multiple barriers for an attacker.

ii. Communication Links

The communication links represent the links between the unmanned aircraft and the control station, including command, control, and communications, as well as other non-payload and payload links. Communication links typically rely on radio frequency-based technologies.

Threats and consequences

Often, and especially for small UAS, the links are unencrypted and use an already congested and contested radio frequency spectrum. Attackers with a low to medium degree of knowledge and access to equipment can not only intercept communication links but also hijack communications to a degree where an attacker acts as a so called On-Path-Attack who can intercept, receive, manipulate, and forward information between Remote Pilot Station (RPS) and UAS and vice versa. Communication channels are also prone to other forms of attacks such as jamming of the frequency/electromagnetic spectrum, resulting in a DoS situation.

Mitigations

The mitigation of attacks such as jamming is rather difficult for an operator and comparably easy to execute for an attacker. Several technological implementations like frequency hopping can reduce the effects of jamming however, the wide availability and low cost of simple jamming devices can represent a serious challenge. Spoofing requires more effort on the side of the attacker and the potential mitigations are more effective compared to the ones for jamming. The application of cryptographic methods to allow checks for integrity and authenticity can significantly reduce the success of spoofing attacks.

iii. Sensors

UAS typically employ a wide range of sensors essential to the safe operation of the unmanned aircraft. Other examples of systems or sensors of an UAS include ADS-B and camera systems which are often used for “detect and avoid” capability.

Threats and consequences

One example is the GPS sensor (or any other GNSS sensor), where due to the weak GPS signal it is inherently prone to jamming. A more advanced and concerning category of attack is "spoofing" (GPS, ADS-B, TCAS, ACAS) where an attacker uses a local transmitter to act as a valid signal to feed false information to the UAS to either hijack or neutralise it.

Mitigations

Similar to the challenges faced for mitigation of attacks on communication links, an effective mitigation of attacks on GNSS is difficult to achieve due to the inherently weak signals which can easily be jammed or spoofed. It could be useful to employ multi-constellation and multi-frequency concepts regarding GNSS sensors.

iv. Avionics

Avionics are responsible for converting input signals (received through sensors or command and control links) into commands to control the flight of the unmanned aircraft. This includes such things as engine control, flight controls etc.

Threats and consequences

Threats can materialise from malicious software that was loaded onto the platform without appropriate safeguards to ensure integrity, e.g., manufacturer certificates or data loading without appropriate checks for the authenticity of the software being loaded. The possible consequences are manifold and range from bricking the UAS up to UAS takeover by an attacker.

Mitigations

Examples on how certain threats could be avoided could include the use of cryptographic methods for data loading, strictly limiting the possible interfaces to avionics (reduction of attack surface) and well- established procedures for personnel responsible for maintenance, repair, and overhaul. Adequate supply chain management constitutes another important element that could mitigate attacks.

v. Guidance Systems

The guidance system of an UAS is responsible for the determination of the flight path and includes information on waypoints, mission objectives, collision avoidance, etc.

Threats and consequences

Threats can emerge from manipulated databases where terrain and waypoint information are not reliable. These manipulations can have different causes like interception of communication channels, malware which made its way onto the UAS in the process of data loading, etc.

Mitigations

Similar to the possible mitigation measures mentioned in section appendix B.ii the application of cryptographic methods for checks of integrity and authenticity could reduce the threat that unverified data is loaded onto an UAS. This process should also include the systems used on the ground like maintenance devices, database servers, etc. to ensure the integrity and authenticity of available information intended for use in guidance systems.

vi. Autonomous Control

A subsystem for autonomous control allows the UAS to operate without the intervention of a remote pilot. Often these controls are enabled by machine learning and artificial intelligence-based technologies.

Threats and consequences

Threats can emerge from inappropriately trained algorithms due to manipulated, incomplete, falsely tagged, biased, etc. datasets. In addition, and through the dual-use nature of ML/AI based technology it can be used for good or malicious purposes. The field of counter AI is still a developing one but the research activities and the open nature of findings available will ensure quick progress.

Mitigations

The analysis of how to mitigate turning good ML/AI into malicious use is, at the time of writing, still ongoing. Threat vectors and scenarios are widely available on how attackers can and could interfere with such systems resulting in potential serious outcomes. It is therefore premature to provide other suggestions for mitigations than to encourage a thorough assessment of the use of ML/AI based technology and the underlying training methodologies including their available datasets. Such evaluations should be risk- and performance-based, focusing on the level of safety and security achieved and can consider following measures:

- Controlling or auditing the origin of datasets, development of HW/SW and training of ML/AI.
- Using immutable algorithms (those made by the manufacturer that cannot be manipulated by the end user) instead of mutable algorithms (those subject to potential manipulation or change by operators other than the manufacturer); using the same, immutable code (not subject to change by users) on every unmanned aircraft tends to enhance cybersecurity.

vii. Flight Termination System (FTS)

Some UAS are designed with a flight termination system. A flight termination system consists of those components needed to end the unmanned aircraft's flight in a controlled manner during off nominal conditions.

Threats and consequences

A cyber-attack on this system could result in catastrophic consequences like an unmanned aircraft crashing on a densely populated area, potentially resulting in injury or death. The components involved in an FTS are numerous and could include GNSS, camera systems, attitude sensors, engine status sensors, etc. This also increases the potential threat surface where an attacker could attempt to attack the FTS.

Mitigations

Due to the many subsystems involved in a sophisticated FTS mitigation is accordingly complex and requires application of thorough "security by design" principles. If ML/AI enabled technologies are part of a FTS system, then the same challenges as mentioned in appendix B.vi apply.

Appendix E: Concepts

i. Security by Design

Security by design is a paradigm that something, for example software, is built from its foundations with the objective of it being secure. Against the background of increasing cyber threats, this design and development approach is becoming increasingly mainstream and builds on a robust architecture design. Architectural decisions are often based on well-known security tactics and patterns which ensure a system provides the required cyber resilience. In aviation systems, and especially in safety relevant systems, the security by design approach is an integral part in the overall design and development process.

ii. Cyber Hygiene

Most of the exploitation of cyber vulnerabilities arise from those who use the Internet – companies, governments, academic institutions, and individuals alike – but who do not practice what can be referred to as good cyber hygiene. They are not sufficiently sensitive to the need to protect the security of the Internet community of which they are a part. The openness of the Internet is both its blessing and its curse when it comes to security. The term Cyber Hygiene therefore stands as a colloquial term referring to best practices and other activities that computer system administrators and users can undertake to improve their cybersecurity while engaging in common online activities, such as web browsing, emailing, texting, etc.

iii. Supply Chain Security Management

Supply chains are often highly complex and may involve many suppliers in different countries. This can introduce a variety of cybersecurity risks, such as entry points for the introduction of malware, which can negatively impact upstream partners and downstream customers.

iv. Defence in Depth

Defence in depth is an information assurance concept in which multiple layers of security controls or design features such as segmentation or isolation are placed throughout an information technology system. The intent is to provide an improved resilience by several protection layers in the event of a security control failure, or if a vulnerability is exploited. It can cover aspects of personnel, procedural, technical, and physical security for the duration of the system's lifecycle.

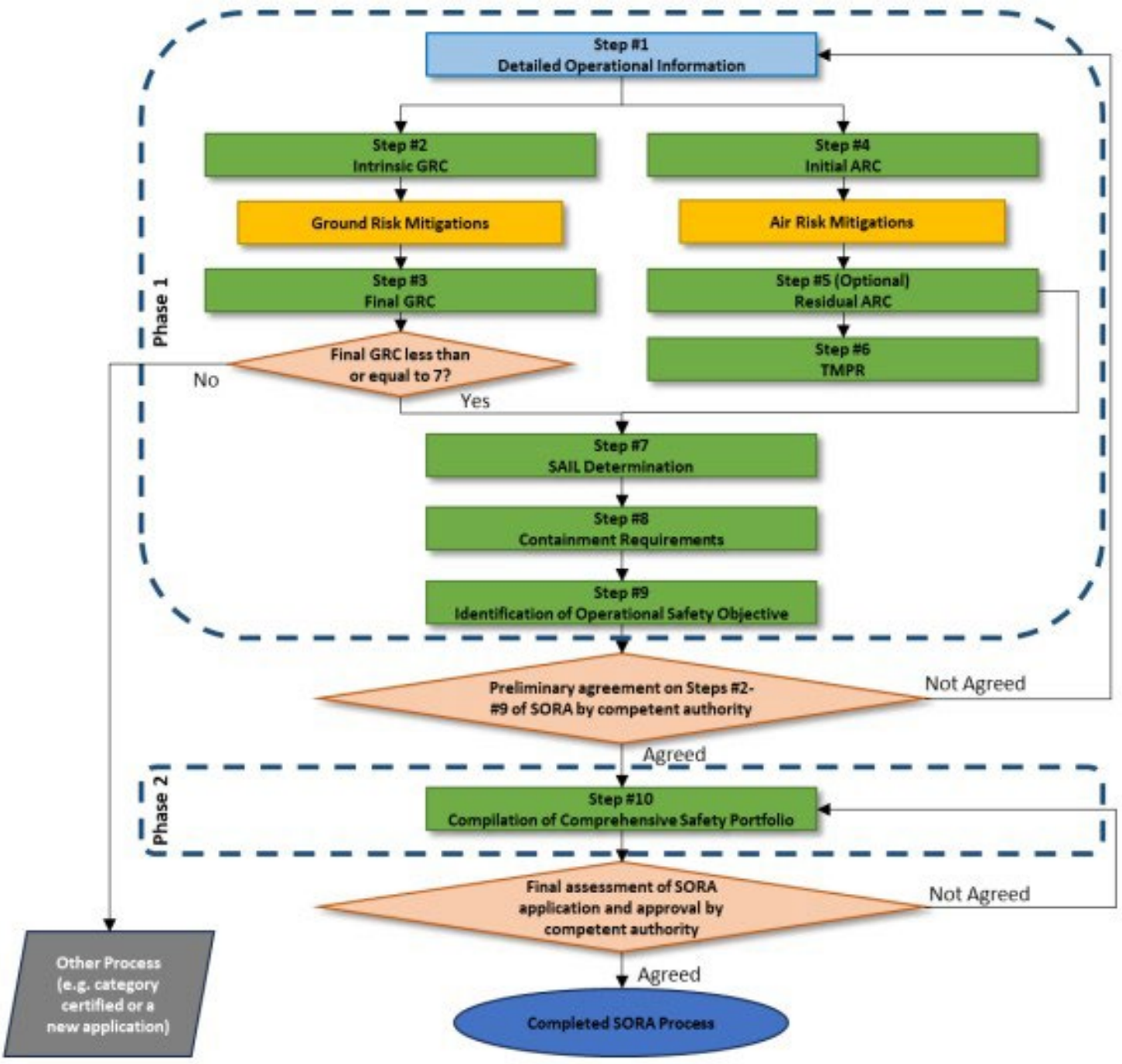
v. Least privilege access.

The least privilege access model is one of the building blocks of layered security and aims to limit access to reduce the scope of a cyber-attack's effect within a system. The goal is that a user or program's access level is kept to the minimum necessary to complete the intended task. In the event of a compromise, the damage is limited to only those elements of the system that the original process had been granted access. In addition to this principle, secure IT systems should follow the principle of minimal service. It states that the system should have everything that is required for the operation - and nothing else.

vi. Secure by Default

Secure by default concept ensures that the default configuration settings of a product are the most secure settings possible. It covers the technical effort to ensure that the right security functionalities are built into software and hardware. This concept has an added benefit of removing the burden of knowledge from the installer or system integrator on how to lock a system down, providing them with an already secure product.

Appendix F: JARUS SORA Process



This flowchart outlines the Specific Operations Risk Assessment (SORA) process, which is used to evaluate and approve drone operations based on safety risk. Here's a summary of the process:

Phase 1: Risk Assessment

- Step #1 – Detailed Operational Information.
  - Begin by describing the operation in detail.

1. **Ground Risk Assessment**
   - Step #2 – Intrinsic GRC (Ground Risk Class)
   - Step #3 – Final GRC (after applying Ground Risk Mitigations)

➢ If Final GRC ≥ 7, the process diverts to another certification route.

2. **Air Risk Assessment**
   - Step #4 – Initial ARC (Air Risk Class)
   - Step #5 – Residual ARC (Optional)
   - Step #6 – TMPR (Tactical Mitigations Performance Requirements)

3. **SAIL and Safety Objectives**
   - Step #7 – SAIL (Specific Assurance and Integrity Level) Determination
   - Step #8 – Containment Requirements
   - Step #9 – Identification of Operational Safety Objectives

4. **Preliminary Agreement**
   - Agreement between the applicant and the competent authority based on Steps #2–#9 to the competent authority.

➢ If Not Agreed, rework and resubmit.

Phase 2: Safety Portfolio & Approval

- Step #10 – Compilation of Comprehensive Safety Portfolio

- Final Assessment & Approval:
  - If approved, the SORA process is completed.
  - If not approved, revise and resubmit.

Outcome

- If GRC is too high or the authority does not approve, the process may shift to another path (e.g., certification route).
- If all steps are successfully completed and approved, the SORA Process is completed, authorising the operation.