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 UK Specific Operation Risk Assessment (UK SORA) methodology for Unmanned Aircraft System (UAS) 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 UAS operations, primarily due to the technology involved in both the UAS itself as well as the ground station and Command & Control (C2) links. In most cases, UAS face similar threats to those faced by crewed aviation, this is why Assimilated Regulation (EU) 2018/1139 (the UK Basic Regulation) sets out to achieve an equivalent level of safety. This equivalency of safety can be achieved by applying by the UK SORA methodology, which uses a holistic safety risk management process to evaluate the risks related to a given operation and then identify proportionate mitigations that a UAS operator may consider applying to enable their operation to achieve a Target Level of Safety.

UAS lack the human presence in the aircraft which typically is an important factor in crewed 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 UAS 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 cyber security vulnerabilities with cyber safety implications.

This document defines basic cyber security concepts and threats to identify their impact on an operator. This document defines basic cyber security concepts and threats to identify their impact on a UAS operation. It aims to support the UAS operator to consider reasonable and proportionate cyber safety mitigations within the context of the UK SORA methodology. Whether a specific OSO should meet a Low, Medium, or High level of robustness is determined by the level of robustness required of the Specific Assurance and Integrity Level (SAIL) in the UK SORA, Step #9 – Final SAIL decision.

This includes guidance on a minimal level of cyber safety measures relevant to the:

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

These considerations have been allocated to the relevant OSOs with associated levels of assurance. This document presents the UK Civil Aviation Authority’s (CAA) current guidance on assessing cyber safety risks when applying for a UK SORA-based operational authorisation.

As UK SORA matures, and as JARUS continues its work in relation to cyber risk assessment and mitigation, our collective understanding will grow which will inform the CAA's plans to update the UK SORA methodology as it relates to cyber safety. In the meantime, the CAA has developed this interim guidance to help stakeholders mitigate cyber risks in line with the CAA's thinking.

The CAA will continuously review this policy concept to consider technological developments, new evidence from Operators and test sites, and any associated research. This will inform safety monitoring processes and may affect our views and this policy.

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: Portable Electronic Devices

PKI: Public Key Infrastructure

RMP: Risk Management Program

SAIL: Specific Assurance and Integrity Level

SLA: Service-Level Agreement

SSL: Secure Sockets Layer

TLS: Transport Layer Security

UAS: Unmanned Aircraft System

URL: Uniform Resource Locator

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

Applicable Regulations

Articles 5(2) and 11 of UK Regulation (EU) 2019/947 – 'Specific' category of UAS operations and Rules for conducting an operational risk assessment.

Article 5(2) of Assimilated Regulation (EU) 2019/947 (the UAS Regulation) requires a UAS operator applying for an operational authorisation to submit a risk assessment that complies with the rules in Article 11 of that Regulation. The risk assessment must identify mitigating measures, including technical measures, that will enable the proposed operation to be conducted safely. UK SORA has been adopted as an acceptable means of complying with the rules in Article 11. This Cyber Extension CAP provides additional guidance to support the application of UK SORA and should be considered accordingly.

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

Under Article 12 of the UAS Regulation, the CAA must evaluate the risk assessment and the robustness of the mitigating measures that the UAS operator proposes to keep the UAS operation safe in all phases of flight.

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

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

UAS.SPEC.050(1)(a)(iii) requires the UAS operator to 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 risk mitigations specific to cyber security that a UAS operator may wish to consider in relation to relevant Operational Safety Objectives (OSOs), as cyber vulnerabilities or weaknesses can pose a significant risk to air safety.

The cyber considerations are designed to identify and mitigate against inadvertent or malicious introduction of such cyber vulnerabilities, to maintain the safety of the UAS and other airspace users. Not all cyber considerations are designed to be technical controls that the operator is advised to consider implementing. Many suggest simple documented processes or procedures that may help promote 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 should 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 referred to in the context of UK SORA.

Portable Electronic Devices (PEDs)

Portable electronic devices such as smartphones, tablets and laptops.

UK SORA robustness

To properly understand the UK SORA methodology, 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 UAS operations, this includes hacking, jamming, or spoofing of services; it also includes physical access to systems such as the Ground Control System (GCS) or UAS.

Unlawful interference

These are acts or attempted acts such as to jeopardise the safety of civil aviation, including but not limited to: unlawful seizure of aircraft, destruction of an aircraft in service, and 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 UAS operations rely on technology, which means they can be vulnerable to malicious activity. Something that isn't secure may pose an air safety risk.

An effective culture of cyber safety relies heavily on 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 CAA 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 UAS threats and actions that may be taken to mitigate them.

[1] National Protective Security Authority

[2] Mitre Engenuity

[3] CAA Cyber Security

[4] ICAO UAS

[5] CISA Air Aware

Operational Safety Objectives

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

Cyber Component #1 – Organisation Culture

Low - SAIL 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Ensure highest-level executive sponsorship for cyber safety.
- Issue a cyber safety policy letter that defines stakeholder roles and responsibilities.
- Provide a cyber safety awareness and training programme so that all stakeholders understand their specific duties.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that an effective cyber safety culture is established and maintained.

Medium - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Maintain a recurring training programme on current and emerging cyber safety threats.
- Define procedures to identify which staff require training and specify the frequency of their refresher courses.
- Adopt and comply with a recognised cyber safety framework.
- Designate a Cyber Safety Manager who is responsible for implementing and overseeing the cyber safety programme.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Retain evidence that cyber safety policies are in place.
- Demonstrate that all required training is delivered and achieves its intended outcomes.

Further Guidance Material

Consider an annual refresher training programme for all staff.

High - SAIL 4, 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Designate the Cyber Safety Manager as a dedicated role responsible for implementing and maintaining an effective cyber safety programme.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Validate policies and secure third-party verification of all training activities.
- Acquire and maintain an industry-recognised cyber security accreditation (e.g. CMMI Institute, NIST or ISO) in compliance with applicable legislation.

Cyber Component #2 - IT and Data Security

Low - SAIL 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Have a corporate policy that addresses IT and data security, including physical access to electronics, lab equipment, and data.
- Include role-based authentication for safety-critical data access within that policy.
- Make Terms of Service and privacy policies for safety-critical equipment and services readily available.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that IT and data security policies are in place.

Medium - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Ensure that computers and PEDs used for business-related activities are physically secured when not in use, and that hard drives are encrypted.
- Implement multi-factor authentication in line with the CISSP Common Body of Knowledge, covering:
  - Type 1 (something you know)
  - Type 2 (something you have)
  - Type 3 (something you are)
- Configure IT systems to log anomalies or malicious activities based on defined policies and rules.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide evidence that IT and data security policies are both in place and actively enforced.

Further Guidance Material

Logging functionality is widely available in various commercial security suites and could be a valuable input for further analysis in industry groups.

'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 4, 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Develop a policy for monitoring and updating corporate IT and data security policies and practices in response to evolving threats.
- Ensure that operational safety-critical data is encrypted at rest.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Have corporate policies validated by a competent third party.

Further Guidance Material

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

Cyber Component #3 – Industry Group Participation

Low - SAIL 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Subscribe to and/or regularly consult the website officially supported or recommended by the UAS supplier/manufacturer to stay aware of any software or hardware updates linked to potential security breaches.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that appropriate awareness of supplier/manufacturer updates is being maintained.

Medium - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Subscribe to broader threat-notification channels and supplier/manufacturer update services to maintain comprehensive awareness of required enterprise software and hardware updates.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide evidence that awareness mechanisms are maintained, active threat notifications are received, and flight logs (criterion #6) are analysed for anomalies.

High - SAIL 4, 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Ensure the dedicated Cyber Security Manager is a member of an industry group deemed appropriate by the CAA.
- Capture, track, and address shortfalls in security processes—and verify that implemented fixes are effective.

Assurance Guidance

Same as Medium.

Cyber Component #4 – Risk Management Program

Low - SAIL 2

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following:

- Include both safety and security risk analyses in the Risk Management Plan (RMP).

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Not applicable at this level.

Medium - SAIL 3

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Maintain an RMP that includes both safety and security risk analyses.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that an audit of the organisation's RMP is in place and effective.

High - SAIL 4, 5, 6

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Validate and verify the RMP through formal review processes.
- Adopt a life-cycle management approach to ensure continuous evolution and improvement of the RMP.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that the RMP has been independently verified and that its life-cycle management processes are effective.

Cyber Component #5 – Audit Program for Cyber Safety Issues

Low - SAIL 2

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following:

- Establish a self-inspection process.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that audits are being conducted.

Medium - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Implement a basic internal audit program.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Document the internal audit program.

Further Guidance Material

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

High - SAIL 4, 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Maintain a robust internal audit program.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Engage an external, independent, qualified entity to conduct audits.

Further Guidance Material

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

Cyber Component #6 – Flight Logs

Low - SAIL 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Implement a method to log UAS activities for subsequent analysis, recognising that some cyber attacks can be intermittent and difficult to track.
- Ensure that, beyond the system’s main attributes, the log captures any security events that could later be used to detect anomalies or suspicious activities; this may be in written or electronic form.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that UAS activity logging and subsequent analysis are being performed.

Further Guidance Material

The log may be in written or electronic format.

Medium - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Store the log file electronically and implement basic integrity protections to guard against unauthorised modification.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Document the logging process and ensure that the analysis results of log data are maintained in an auditable format and actively used to identify anomalies.

Further Guidance Material

- 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 4, 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Store the log file in a tamper-proof medium or system to provide strong guarantees of immutability.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Conduct regular, recurring analyses of log data (beyond event-triggered reviews) and have those procedures validated by a competent third party.

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

Cyber Component #1 – Malware Protection

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Establish maintenance procedures that verify the authenticity of firmware and software sources.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that maintenance procedures are in place aimed at reducing the risk of introducing malware during maintenance activities.

Further Guidance Material

For the integrity consideration the applicant may include checking the correct website/URL and verification of valid and authentic Secure Sockets Layer (SSL) certificates for https connections before downloading software updates to the UAS and supporting equipment.

Medium - SAIL 3, 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Implement procedures to verify both the authenticity and integrity of software (e.g., checksum or digital-signature validation).
- Regularly scan maintenance-related computers and removable media for malware.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that these maintenance procedures exist and are designed to reduce the risk of introducing malware during maintenance.

Further Guidance Material

For the integrity consideration the applicant may include a process such as verifying check sums and digital signatures, 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 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Employ advanced malware protection solutions across maintenance environments.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have these procedures validated by a competent third party.

Further Guidance Material

To provide advanced malware protection methods, organisations may employ separate testing environments that allow:

- continuous monitoring of systems,
- retrospective alerting and remediation,
- the implementation of protection mechanisms for multiple attack vectors/entry points (firewall, network, endpoint, email), and
- 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 Component #2 – Supply Chain Management

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Source computer systems and all associated hardware, software, and support services used in UAS maintenance from reputable suppliers.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that reasonable and appropriate supply chain security measures have been taken.

Further Guidance Material

Systems used for maintenance include but are not limited to:

- UAS spare parts,

- Maintenance computers,
- Diagnostic equipment,
- GCS software,
- RPS software,
- Diagnostic software.

Medium - SAIL 3, 4

Integrity Guidance

Same as Low SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that reasonable and appropriate supply chain security measures have been implemented.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Source computer systems and software from trusted suppliers, incorporating cryptographic verification (e.g., component hashes and digital signatures) to confirm authenticity.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have supply chain security measures and sourcing practices validated by a competent third party.

Cyber Component #3 – Physical Security

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Apply basic physical security principles to guard against unauthorised access or theft.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that adequate physical security provisions are in place.

Further Guidance Material

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

Medium - SAIL 3, 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Ensure that computers used for UAS maintenance are physically secured when not in use.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that adequate physical security provisions are maintained.

Further Guidance Material

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

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Control physical access to the UAS itself.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have the physical security provisions validated by a competent third party.

Cyber Component #4 – Controlled Access

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Ensure that access to computers, networks, and information systems used for UAS maintenance employ basic access controls.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that basic access controls are in place.

Further Guidance Material

As a minimum, the applicant should implement username and a password following National Cyber Security Centre (NCSC) guidance.

Medium - SAIL 3, 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Restrict access strictly to authorised maintenance personnel.
- Implement data access controls with tracking and record-management practices.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that these access controls are employed.

Further Guidance Material

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 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Configure individual user accounts with permissions strictly aligned to each maintainer’s role.
- Employ two-factor authentication for all access.
- Ensure data encryption both in transit and at rest.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have access controls and their implementation validated by a competent third party.

Cyber Component #5 – Wireless Access Protected

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Enable basic encryption on all wireless networks used for UAS maintenance.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that all maintenance-related wireless networks have basic traffic encryption enabled.

Further Guidance Material

Some basic encryption examples that the applicant can use:

- Advanced Encryption Standard (AES),
- Wi-Fi Protected Access 2 (WPA2) Enterprise,
- Wi-Fi Protected Access 3 (WPA3),

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 3, 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Enable stronger/advanced encryption on the network traffic.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that all maintenance-related wireless networks utilise advanced encryption for network traffic.

Further Guidance Material

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

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Employ strong network encryption combined with user- or device-level authentication (e.g., 802.1X).

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have the security and encryption measures validated by a competent third party.

Further Guidance Material

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

Cyber Component #6 – Software/Firmware Updates

Low - SAIL 1, 2

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following:

- Establish update management procedures to check for, verify the authenticity of, and apply original equipment manufacturer (OEM) updates.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Declare that maintenance procedures exist to review OEM security updates for applicability and install them where appropriate.

Further Guidance Material

This should include updates to all supporting infrastructure.

Medium – SAIL 3, 4

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Include maintenance procedures to check other computer systems used in UAS maintenance.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that these procedures are in place to review and install OEM security updates as appropriate.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Ensure maintenance procedures review OEM security updates for all computer systems used in UAS maintenance and install them where appropriate.
- Implement change management policies to test updates before installation, reducing the risk of detrimental operational impacts.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Have these update and change management procedures validated by a competent third party.

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

Cyber Component #1 – Cyber Safety Risk Assessment

Low - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Review the Concept of Operations (CONOPs) for cyber threats (as outlined in Appendices C and B of this CAP) and select a UAS that implements the concepts from Appendix D and the mitigations in Appendix C.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that a basic security assessment and threat mitigations have been undertaken.

Further Guidance Material

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

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Perform a cyber safety risk assessment using a CAA-acceptable standard.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Supply documentation demonstrating that a security risk assessment and corresponding threat mitigations have been completed.

Further Guidance Material

For the integrity consideration, the applicant may use

- ISO27005 risk assessment methodology,
- NIST 800-53 risk assessment (Cyber Security Framework),
- Cyber Security Risk Foundation (CRF) – CRF GRM,
- the method presented in Appendix A in combination with the controls presented in the above standards.

High - SAIL 5, 6

Integrity Guidance

Same as Medium SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have the security assessment validated by a competent third party.

Cyber Component #2 – GNSS Equipment, if used

Low - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Employ basic threat mitigations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that basic threat mitigations are in place.

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following in addition to Low-level considerations:

- Implement health monitoring and reporting of Global Navigation Satellite System (GNSS) parameters, including received signal strength, number of satellites, satellite identification, and time comparisons.
- Deploy GNSS jamming detection capabilities.
- Use multi-constellation GNSS equipment.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation evidencing that threat mitigations have been implemented.

High - SAIL 5, 6

Integrity Guidance

Same as Medium SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have the threat mitigation measures validated by a competent third party.

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

Low - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Review the CONOPs for cyber threats (as outlined in Appendices C and B of this Extension) and select a UAS that implements the concepts from Appendix D and the mitigations in Appendix C so that probable cyber threats cannot cause the UAS to depart its intended operational volume.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that the evaluation has been undertaken.

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Perform the CONOP review using an industry-accepted standard.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that the CONOP evaluation has been completed.

Further Guidance Material

The applicant may use the NCSC Cyber Incident Response process.

High - SAIL 5, 6

Integrity Guidance

Same as Medium SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have the evaluation validated by a competent third party.

Cyber Component #4 – Life Cycle Security Appraisal

Low - SAIL 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Establish procedures to re-accomplish the review called out in Criterion #1 whenever new or recently uncovered cyber threats are identified.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that procedures exist to update the Security Risk Assessment.

Further Guidance Material

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 – 4

Integrity Guidance

Same as Low SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that procedures exist to update the Security Risk Assessment.

High – 5, 6

Integrity Guidance

Same as Medium SAIL considerations.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have those update-procedure processes validated by a competent third party.

Cyber Component #5 – Test and Security Validation

Low - SAIL 3

Integrity Guidance

Not Applicable

Assurance Guidance

Not Applicable

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Evaluate the effectiveness of threat mitigations identified in this guidance using an acceptable industry standard.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that the evaluation of mitigation effectiveness has been undertaken.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Perform mitigation-effectiveness evaluations using a recognised aeronautical standard.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have those evaluations validated by a competent third party.

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

Cyber Component #1 – Datalink Encryption

Low - SAIL 2, 3

Integrity Guidance

Not applicable

Assurance Guidance

Not applicable

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Employ encryption on the C3 link.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation demonstrating that the C3 link is properly encrypted.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Ensure the C3 link meets the minimum operational performance standards defined in RTCA DO-377B or an equivalent specification.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Have the datalink encryption validated by a competent third party.

Cyber Component #2 – Authentication

Low - SAIL 2, 3

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Employ basic mutual peer-entity authentication on the data link between the GCS and UAS.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that basic data-link authentication is in place.

Further Guidance Material

The applicant may use Transport Layer Security (TLS) 1.3 and beyond in addition to passwords for basic authentication.

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Employ advanced mutual peer-entity authentication on the data link between the GCS and RPS.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that advanced authentication methods are implemented.

Further Guidance Material

The applicant may use an industry standard Internet of Things (IoT) cyber security best practice for authentication to meet the intent of advanced authentication.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Use aviation-standard authentication methods (or equivalent) for the data link and implement multifactor authentication at human-machine interfaces.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations*:*

- Have authentication methods validated by a competent third party.

Further Guidance Material

The applicant may use the Public Key Infrastructure (PKI) certificates as described in ATA specification No 42 to meet the intent of aviation standard authentication.

Cyber Component #3 – Access Control

Low - SAIL 2, 3

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following:

- Pair the control station with the GCS using, at minimum, a password; change all default passwords and configure length, complexity, expiration, and history settings according to security best practices and system capabilities.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Declare that basic access controls on the data link are in place.

Medium - SAIL 4

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following additional measure that builds on the Low-level considerations:

- Enforce the principle of least privilege in access control.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that advanced access control functions are implemented.

High - SAIL 5, 6

Integrity Guidance
To support the integrity objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Require multifactor access control for human-to-machine interfaces and apply aviation-standard access control methods for machine-to-machine interfaces as specified by the CAA or other competent authority.

Assurance Guidance
To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have the access control functions validated by a competent third party.

Further Guidance Material
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 may be employed.

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

Low - SAIL 2, 3

Integrity Guidance

Not Applicable

Assurance Guidance

Not Applicable

Medium - SAIL 4

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Employ industry-standard IoT cyber security best practices on the data link.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Provide documentation showing that the data link employs advanced data integrity and anti-replay protection.

High - SAIL 5, 6

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- Use aviation-standard data integrity and anti-replay protection methods (or equivalent) on the data link.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following additional measure that builds on the Medium-level considerations:

- Have the data integrity and anti-replay protection functions validated by a competent third party.

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

Low - SAIL 1, 2

Integrity Guidance

To support the integrity objectives, an applicant may wish to consider the following:

- The level of Cyber security 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 Guidance

To support the assurance objectives, an applicant may wish to consider the following:

- Declare that the requisite level of cyber security for externally provided services is met (even if detailed evidence is not provided).

Medium – SAIL 3

Integrity Guidance

Same as Low SAIL guidance.

Assurance

To support the assurance objectives, an applicant may wish to consider the following:

- Supply supporting evidence (e.g., a Service-Level Agreement or formal commitment) demonstrating that the required cyber security level for any externally provided service will be maintained throughout the full duration of the mission.
- Implement monitoring of those external services that affect flight-critical systems and define actions to take if cyber safety lapses could lead to the loss of control of the operation.

High – SAIL 4, 5, 6

Integrity Guidance

Same as Medium SAIL guidance.

Assurance Guidance

To support the assurance objectives, an applicant may wish to consider the following in addition to Medium-level considerations:

- Demonstrate the achieved cyber security level of externally provided services through demonstrations.

- Have a competent third party validate the claimed level of integrity for those services.

Appendix A: Threat Analysis and Risk Assessment

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 C 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.

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 B provides a general overview of the threats that you may encounter as a UAS operator.

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.

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 should be documented in the control's column of the risk assessment documentation.

Example Risk Assessment Template

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

Titles	Descriptions
Risk ID	It is a good practice 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 UAS 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 B.
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 B: Cyber Threats

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.

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.

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, 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),

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 should be an integral part in the Design, Development, Deployment and Operations of system elements, and is a recurring activity throughout the system's lifecycle.

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).

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.

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 C: Basic UAS security impacted areas of cyber safety

In general, UAS face very similar threats to those faced by crewed aviation. However, UAS lack the human presence in the aircraft which typically is an important factor in crewed 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 cyber security 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.

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.

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.

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.

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.

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 Communication Links 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.

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 cyber security.

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 C Autonomous Control apply.

Appendix D: Concepts

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.

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 cyber security while engaging in common online activities, such as web browsing, emailing, texting, etc.

Supply Chain Security Management

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

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.

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.

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.