Annex E (Cyber)

Table of Contents

INTRODUCTION

The need for effective and risk-proportional cybersecurity is paramount given that aviation is reliant on interconnectivity between large numbers of systems controlled and operated by many stakeholders. The aviation sector may be an attractive target for a cyber-attack, for various threat actors, with a wide range of motivational reasons, capabilities, and sophistication to achieve their objective to successfully exploit vulnerabilities in the aviation ecosystem. These vulnerabilities exist in humans, equipment, and processes/procedures alike and exploitation can either target one of these elements in an isolated manner or scale up to complex multi-vector attacks affecting the whole system. Lack of effective and risk-proportionate cybersecurity can have a negative impact on aviation safety, as well as on an operator's business operations from dispatch reliability, data collection, information privacy and service uptime.

Note: The scope of Annex E is limited to those areas which affect flight safety and protection of the public. In addition, we address mainly operators with the information provided in this annex rather than OEMs, etc.

As an outline, it is worth introducing the following notions and definitions:

1. *Cybersecurity:* Refers to the protection of information systems and data from cyber-related events that may disrupt organisation's business and activities.
2. *Aviation Safety:* Is the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level.
3. *Aviation Cyber Safety:* As the figure 1 illustrates, Aviation Cyber Safety is seen as the union of the two previous domains 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.

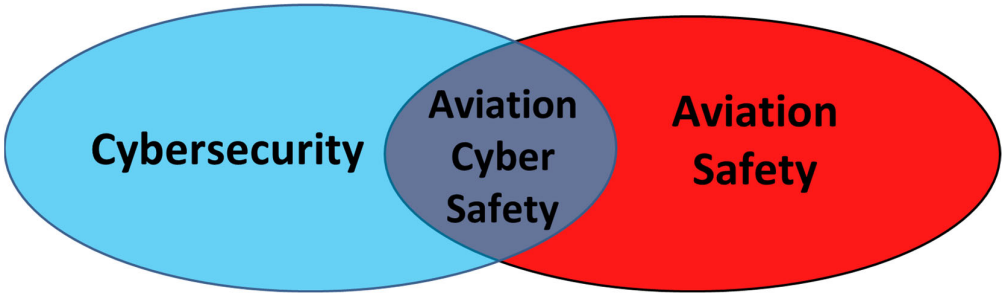

Figure 1 – Cybersecurity and Safety Interactions in Aviation

Cybersecurity in aviation requires cybersecurity threats to be considered as part of the risk management process. Cybersecurity threats in aviation are understood as intentional unauthorized electronic interactions impacting aviation safety.

These threats exist across the global aviation ecosystem and can impact the entire aircraft and operations lifecycle, i.e., design, build, operate, maintain and disposal. The scope of this document involves the orange highlighted area as illustrated in Figure 2. The operator must determine if a cyber risk has been mitigated to reach an acceptable level in support of their proposed operations including the consideration of the support for this objective provided by an operator's supply chain.

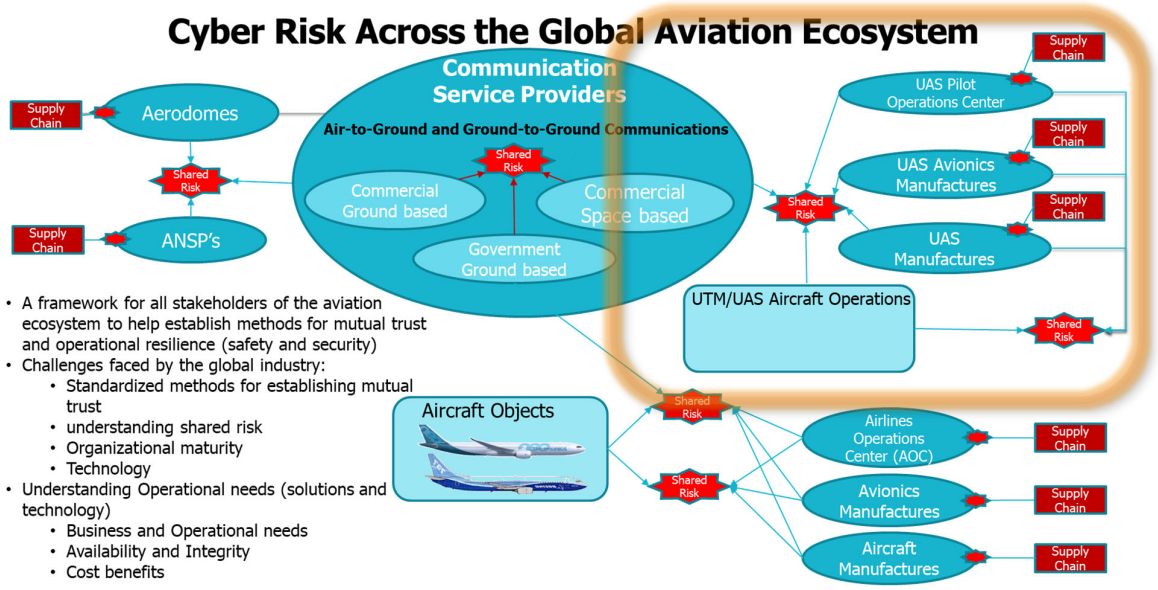

Figure 2 – Cyber Risk across the Global Aviation Ecosystem

This annex 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 Specific Operations Risk Assessment (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 #8 - Identification of Operational Safety Objectives (OSO). The levels of robustness specified for cyber requirements in this Annex represents the levels identified in SORA Step #8.

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.

COMMON CYBERSECURITY ATTRIBUTES, CONCEPTS AND THREATS

Although cybersecurity in aviation (or what we are calling Cyber Safety) focuses on the potential effects on safety; the attributes of the information that shall be protected, as well as the basic concepts and the threats, are common to the broader notion of cybersecurity. In the following paragraphs an introduction to the above-mentioned concepts is provided.

1.1 ATTRIBUTES

C – I – A: Confidentiality, Integrity and Availability are the key security attributes, requiring appropriate protection and which underpin cybersecurity.

1.1.1 Confidentiality

Confidentiality is the attribute that information is not made available or disclosed to unauthorized individuals, entities, or processes. Confidentiality must not be interchanged with privacy, but rather considered as a component of privacy to protect data from unauthorized disclosure.

1.1.2 Integrity

Integrity focuses on maintaining and assuring the accuracy and completeness of data over its entire lifecycle but preventing unauthorized or undetected modification.

1.1.3 Availability

For an information system to serve its purpose it is necessary that information is available when it is needed. This includes all system components required to store and process information, security controls to protect information and communication channels and interfaces to access and distribute the information.

1.1.4 Authenticity

The attribute of Authenticity ensures that an entity/identity is genuine and/or not corrupted from the original. In an aviation context authenticity could be relevant to ensure only authentic components of an aircraft can exchange data with each other.

A – A – A: Authentication, Authorisation, and Accounting represent an identity and access management model and is used to manage access to assets and maintain system security.

1.1.5 Authentication

Authentication describes an act, process, or method to ensure a device, software, application, system, entity, person, or identity is true or genuine. In information technology authentication is often used when the identity of a device, software, application, system, entity, person requires confirmation in the process of logging on to a system.

1.1.6 Authorisation

Authorization is the function of specifying access rights and/or privileges to resources in the context of Access Control in the field of Information and Computer Security. Appropriate authorization ensures that a successfully authenticated entity can access only the authorized information, for example, specific records on a network resource, and nothing more.

1.1.7 Accounting / Non-Repudiation

“Non-Repudiation, in addition to “Authenticity” is sometimes used as an extension to the C-I-A concept. “Non-Repudiation” can also be seen as alternative for “Accounting. It describes the process of ensuring that a subject of an activity, or event, cannot deny that the event occurred. It can also be seen as assurance that an electronic transaction had happened. This is particularly important when attempting to deter insider threats and during post-attack investigations because it allows to review the activities/transactions a subject/system has conducted.

1.2 CONCEPTS

1.2.1 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.

1.2.2 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.

1.2.3 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.

1.2.4 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.

1.2.5 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.

1.2.6 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.

1.3 THREATS

1.3.1 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.

1.3.2 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 the 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 cryptographically protected like GNSS and ADS-B.

1.3.3 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.

1.3.4 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 disable 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.

1.4 ATTACKER PROFILE

Attacker profile can vary from basic user, insider, hacktivist, terrorist to nation-state. Depending on the profile of the attacker considered, the probability of the threats may vary. Also, motivations are often linked to financial gains but may cover making a social or political point, espionage or in intellectual challenge. For example, in regard to the difficulty of an attack, man-in-the-middle attacks on a secured network are rather difficult; if combined with a low motivation, such an attack may be given a lower priority for mitigation.

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.

2.1 BASE SYSTEM

The "Base System"[1] can be understood as the "operating system" or "motherboard" of the UAS which allows, manages, and controls the communication between the various subsystems.

2.1.1 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.

2.1.2 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"

2.2 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.

2.2.1 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 "Man-in-the-middle" 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.

2.2.2 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.

[1] https://www.researchgate.net/publication/261449270_The_vulnerability_of_UAVs_to_cyber_attacks_-_An_approach_to_the_risk_assessment

2.3 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.

2.3.1 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.

2.3.2 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 in regard to GNSS sensors.

2.4 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.

2.4.1 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.

2.4.2 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.

2.5 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.

2.5.1 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.

2.5.2 Mitigations

Similar to the possible mitigation measures mentioned in section 2.2.2 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 the use in guidance systems.

2.6 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.

2.6.1 Threats and consequences

Threats can emerge from inappropriately trained algorithms due to a 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.

2.6.2 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.

2.7 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.

2.7.1 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.

2.7.2 Mitigations

Due to the many subsystems involved in a sophisticated FTS a 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 chapter 2.6.2 apply.

OPERATIONAL SAFETY OBJECTIVES CYBER SAFETY CONSIDERATIONS

2.1 INTRODUCTION

The following tables describe the implementation of cyber safety at various levels for each Operational Safety Objective (OSO). This annex defines basic cyber safety concepts, threats, and identifies operator impacts. 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 #8 - Identification of Operational Safety Objectives. The levels of robustness specified for Cyber requirements in this Annex parallel the levels identified in SORA Step #8.

2.2 OSO#01 – ENSURE THE OPERATOR IS COMPETENT AND/OR PROVEN

- Organizational Culture - Leadership Commitment is essential to managing the threat of cyber incidents in aerospace systems and supporting infrastructure. Aviation industry organisations should take the responsibility to instil a culture of cyber safety by establishing overall awareness, capability, and readiness to protect unmanned aviation systems, operations and all applicable supporting infrastructure and services.

- Enacting an effective culture of cyber safety relies heavily on the buy-in and sponsorship from the highest level within an organisation. Affirming a business level commitment to fully understand and address cyber safety is essential and serves as the catalyst towards establishing an organizational commitment to cyber safety. Organizations should obtain the highest-level executive sponsorship within their business and establish a framework to address cyber safety.

- Organizational commitment begins with a cyber safety governance policy that identifies stakeholder roles/responsibilities.

- Cyber safety awareness and training are fundamental to ensuring that industry stakeholders within organizations clearly understand their role.

- The implementation of both safety and security requires organizations to have an effective Risk Management Program (RMP) that not only includes the criticality analysis and impact of the various risks to an organization's business and operations but also looks at risk holistically and its analyses that includes both safety and security.
    - The RMP includes appropriately identifying and scoping the boundaries of resources and assets based upon the criticality of risk and identifies the appropriate control objectives for each operating environment.

- The objective is to ensure an organisation effectively manages and mitigates risks, not only meet the needs of an organisation, but to also satisfy those requirements expected by the community and environment in which they operate.
- The organisation must have an RMP in place that identifies the criticality of resources and incorporates within its analyses both safety and security.
- The RMP implemented should be audited to ensure that it not only meets the needs of the organisation but is also effective in ensuring appropriate management of safety and security risks.
- The RMP implementation should be validated and verified to ensure that proven processes are in place enabling it to evolve and improve over time as threats and risks change both internally and externally.

TECHNICAL ISSUE WITH THE UAS		**LEVEL of INTEGRITY**		
		Low	**Medium**	**High**
OSO #1 Ensure the operator is competent and/or proven	Criterion #1 (Organisational Culture)	1) Highest-level executive sponsorship identified for Cyber safety 2) Cyber safety policy letter identifies organisational stakeholder roles and responsibilities 3) Cyber safety awareness and training are conducted so that stakeholders within organizations clearly understand their role in cyber safety	Same as Low, in addition: 1) A recurring training program on new and evolving cyber safety threats exist and is maintained 2) Training program procedures identify employees who require such training and frequency of refresher training Note: It is recommended that employee get refresher training annually. 3) A framework to address cyber safety established and followed 4) The role of cyber safety manager is **designated**, i.e., the responsible person is identified, and exercises duties according to the demand	Same as Medium, in addition: 1) The role of cyber safety manager is **dedicated** to an identified person exercising responsibility for implementing and maintaining an effective cyber safety program within their organization

	Comments			
	Criterion #2 (IT and Data Security)	1) Corporate policy addresses IT and data security, including physical access to electronics, lab equipment, and data 2) Role-based authentication (e.g. username/password) required for safety-critical data access 3) Terms of Service and privacy policies for safety critical equipment and services are readily available.	Same as Low, in addition: 1) Computers used for the business-related activities are physically secured when not in use[1]. Hard drives should be encrypted. 2) Policy supports multiple authentication: Type 1 (Something you know); Type 2 (Something you have); and Type 3 (Something you are) authentication factors, as per CISSP Book of Knowledge 3) Applicant's IT systems support logging of anomalies or malicious activities based on configured polices and rules (this logging functionality is widely available in various commercial security suites and could be a valuable input for further analysis in industry groups)	Same as Medium, in addition: 1) A policy for monitoring and updating corporate IT and data security policies and practices as required for evolving threats. 2) Safety Critical Data at rest[2] are encrypted
	Comments	[1] Physically secured does not necessarily mean locked in a vault. It could be just that the Operator's place of business is secured when no one is there. [2] A geofence definition would be one example of safety critical data at rest.		
	Criterion #3 (Industry Group Participation)	The applicant subscribes to and/or regularly consults the website officially supported/recommended by the UAS supplier/manufacturer to keep aware of any necessary software/hardware updates linked to potential security breaches. [1].	Same as Low, in addition: The organisation subscribes to broader notifications regarding active threats and appropriate supplier/manufacturer update channels to maintain awareness of needed enterprise software/hardware	Same as Medium, in addition: 1) The dedicated cybersecurity manager is a member of an industry group deemed appropriate by the Regulator, e.g. A-ISAC, ECCSA.

			updates	2) Captured and tracked shortfalls in security processes are addressed and fixes have been verified as effective
	Comments	*[1] Such as a customer support portal, mandatory updates, etc.*		
	Criterion #4 (Risk Management Program)		The organization's RMP includes both safety and security risk analyses	Same as Medium, in addition: RMP has been validated and verified The organisation follows a life-cycle management approach for continuous evolution and improvement
	Comments	2nd edition of ISO 21384-3		
	Criterion #5 (Audit Program for Cyber Safety issues)	The applicant has a self-inspection process.	The applicant has a basic internal audit program[1]	The applicant has a robust audit program[2]
	Comments	*[1] A basic internal audit programme ensures each OSO with cyber implications has been at least broadly addressed. [2] A robust internal audit program ensures each topic within the OSOs with cyber implications has been specifically addressed.*		
	Criterion #6 (Flight Log)	Since some cyber-attacks can be intermittent and difficult to track, it is important that the Operator implements a method by which UAS activities are logged for subsequent analysis. Besides the main attributes	Same as Low, in addition: The log file should be stored electronically and have basic integrity protection [1]	Same as Medium, in addition: The log file should be stored tamper-proof.

		from UA, the log must record any security events which can later on be used to detect anomalies and/or suspicious activities. This may be a written log or electronic.		
	Comments	*[1] To ensure log files cannot be modified without knowledge. Refer to ARINC 852*		

TECHNICAL ISSUE WITH THE UAS		**LEVEL of ASSURANCE**		
		Low	**Medium**	**High**
OSO #1 Ensure the operator is competent and/or proven	Criterion #1 (Organisational Culture)	The applicant declares that an effective cyber safety organisational culture is in place	The applicant has supporting evidence that policies addressing cyber safety exist and that all required training is being conducted and is effective.	Same as Medium, in addition: 1) The Policies are validated, and the training is verified by a competent third party 2) The applicant possesses an industry recognized cybersecurity accreditation like those that recognise compliance with the relevant standards by CMMI Institute, NIST or ISO in compliance with applicable legislation.
	Comments			

	Criterion #2 (IT and Data Security)	The applicant declares that IT and Data Security policies are in place	The applicant has evidence that IT and Data Security policies are in place and are being followed	Corporate policies are validated by a competent third party.
	Comments			
	Criterion #3 (Industry Group Participation)	The Applicant declares appropriate awareness is being maintained	The applicant has evidence that appropriate awareness is maintained, active threat notification are being received and flight logs (criterion #6) are being analysed for anomalies	Same as Medium
	Comments			
	Criterion #4 (Risk Management Program)	N/A	Documentation is provided that includes an audit of the organization's RMP is in place and effective	Documentation is provided that the organization's RMP has been independently verified and shows that the implemented RMP has an effective life-cycle management
	Comments			
	Criterion #5 (Audit Program for Cyber Safety issues)	The applicant declares audits are being conducted	The audit program is documented	Audits are conducted by an external, independent, qualified entity.
	Comments			
	Criterion #6 (Flight Log)	The applicant can declare that they perform this activity.	The applicant must document this activity, the analysis results of log data is in an auditable	Same as Medium, in addition: The applicant conducts regular/recurring log (not event

			format and used to find anomalies	triggered) analysis, and the procedures are validated by a competent third party.
	Comments			

2.3 OSO#02 –UAS MANUFACTURED BY COMPETENT AND/OR PROVEN ENTITY

Clearly, the manufacturer of the UAS is an important factor in the overall system's resilience to cyber threats. A well-established cyber risk assessment process resident in a strong Organizational Culture (OSO #1) combined with a safety risk assessment process as already defined in OSO #5, and specifically required in OSO #10/12 (below) with a maintenance cyber hygiene established in OSO #3 (below), should sufficiently cover supply chain cyber threats addressed by this OSO.

2.4 OSO#03 UAS MAINTAINED BY COMPETENT AND/OR PROVEN ENTITY

- There are many aspects of UAS maintenance that have a direct impact on cyber safety. These range from the sourcing of spare parts to the installation of software updates into various UAS systems. The introduction of malicious software, also known as malware, into the UAS is a prime example. Malware is an umbrella term used to characterise any code or content that could have a malicious, undesirable impact on systems. Its introduction into the UAS could either be intentional or unintentional during routine maintenance actions. It is important that UAS maintainers have a good understanding of what malware is and the various ways in which it could be introduced. Some examples of risk-entailing maintenance actions introducing malware include:
    (1) Downloading software updates from unsupported/non-verified and unsafe sources on the internet
    (2) Using infected removable media (e.g., SD cards, thumb drives) on/between maintenance computers
    (3) Connecting, either wired or wireless, infected removable media and Portable Electronic Devices (e.g., maintenance computers, tablets, data loaders) to the UA and RPS
    (4) Connecting, either wired or wireless, infected computer-based test equipment to the UA and RPS
- Malware could also be installed into spare parts and UAS computer systems (laptops, diagnostic equipment etc) within the supply chain. In addition to having robust user education and awareness, the risk of malware can be reduced in many ways, including such things as only sourcing software parts from supported, manufacturer supported and trustworthy/known sources, regularly checking maintenance computers and removable media for malware, sourcing spare parts and computer systems from reputable, trusted and if need be, authorised suppliers.

- Access control is also important, as allowing untrusted persons to access UAS and maintenance computer systems and information systems, either physically or wirelessly, introduces risk. This risk can be reduced by doing such things as locking away computer systems, employing username and passwords on computers, limiting computer user account privileges, as well as securing wireless networks.

TECHNICAL ISSUE WITH THE UAS		**LEVEL of INTEGRITY**		
		Low	**Medium**	**High**
OSO #3 UAS maintained by competent and/or proven entity	Criterion #1 (Malware Protection)	The applicant has maintenance procedures aiming at verifying the authenticity of firmware/software sources[1]	Same as Low, in addition: 1) Procedures to verify the authenticity and integrity of the software[2], and 2) Procedures to regularly scan maintenance related computers and removable media for malware.	Same as Medium, in addition: Employment of advanced malware protection[3]
	Comments	*[1] This includes checking the correct website (correct URL) and verification of valid and authentic SSL certificates for https:// connections before downloading software updates to the UA and RPS.* *[2] This includes such things 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.* *[3] See section 1.3.4*		
	Criterion #2 (Supply Chain Management)	Computer systems and associated hardware/software[1] and support services used in the maintenance of UAS are sourced from reputable suppliers.	Same as Low	Same as medium, in addition: Computer systems and associated software used in the maintenance of UAS are sourced from trusted suppliers. For example,

				components may have a Hash and digital signature associated with them to verify authenticity.
	Comments	*[1] This includes such things as UAS spare parts, maintenance computers, diagnostic equipment, UA software, RPS software, diagnostic software etc.*		
	Criterion #3 (Physical Security)	The applicant applies basic physical security principles against unauthorised access or theft[1].	Same as Low, in addition: Computers used for the maintenance of the UAS are physically secured when not in use[2].	Same as Medium, in addition: Physical access to the RPS is controlled.
	Comments	*[1] This includes such things as having a mobile phone or computer locked when not in use.* *[2] Physical security could include locking maintenance computers in a secure cabinet or locking the maintenance facility when not in use.*		
	Criterion #4 (Controlled Access)	The applicant ensures that access to computers, computer networks and information systems used for UAS maintenance have basic access controls[1].	Same as Low, in addition: 1) access[2] is restricted to only authorized maintenance personnel requiring access. 2) Data access controls with tracking and record or data management practices	Same as Medium, in addition: 1) Individual user accounts are set to a level appropriate to the role undertaken by each maintainer, and 2) Access employs two-factor authentication. 3) Data encryption in transit and at rest.
	Comments	*[1] As a minimum username and strong passwords* *[2] Access in this context refers to computer user accounts used to log into maintenance computers, networks, and information systems. This includes restricting individual user accounts to a level appropriate to the role undertaken by the maintenance*		

	Criterion #5 (Wireless Access Protected)	Wireless networks used in the maintenance of the UAS has basic encryption of the network traffic enabled[1].	Same as low, in addition: Advanced/stronger encryption of the network traffic is enabled[2].	Same as Medium, in addition: Strong network encryption and access control/user or device authentication is employed[3]
	Comments	*[1] As a minimum a password/passphrase is required to access the wireless network and it has been changed from the default that the system was shipped with. In addition, passwords should meet security standards for length, complexity, expiration, history, and reuse. Basic encryption example: WPA + AES, WPA2 Enterprise, WPA3.* *[2] As a minimum WPA2 Enterprise* *[3] For example WPA2 + 802.1x authentication, e.g., via RADIUS server*		
	Criterion #6 (Software/Firmware Updates)	The applicant has update management procedures to check for, verify authenticity, and apply OEM updates[1].	Same as Low, in addition: Maintenance procedures to check other computer systems used in the maintenance of the UAS[2].	Same as Medium, in addition: Maintenance procedures review OEM security updates to all computer systems used in the maintenance of the UAS for applicability and installed where appropriate. The organisation implements change management policies to test updates before installation, which reduces risks of detrimental operational impacts of installed updates.
	Comments	*[1] This includes such things as UA and RPS software* *[2] This includes such things maintenance computers, diagnostic equipment etc.*		

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #3 UAS maintained by competent and/or proven entity	Criterion #1 (Malware)	The applicant declares that maintenance procedures exist with the objective to reduce the risk of introducing malware during maintenance activities.	The applicant has supporting documentation that maintenance procedures exist to address with the objective to reduce the risk of introducing malware during maintenance activities.	Same as Medium, in addition: The procedures are validated by a competent third party.
	Comments			
	Criterion #2 (Supply Chain Management of the UAS spare parts, maintenance, computers, diagnostic equipment, software, etc.)	The applicant declares that reasonable and appropriate supply chain security measures have been taken. [1]	The applicant has supporting documentation that reasonable and appropriate supply chain security measures have been taken. [1]	Same as Medium, in addition: The measures are validated by a competent third party. [1]
	Comments	*[1] The applicant incorporates cybersecurity requirements that contribute to the assurance of C-I-A of the information exchange*		
	Criterion #3 (Physical Security)	The applicant declares they have adequate physical security provisions.	The applicant has documentation that they have adequate physical security provisions.	Same as Medium, in addition:

				The physical security provisions are validated by a competent third party.
	Comments			
	Criterion #4 (Controlled Access)	The applicant declares that they employ basic access controls.	The applicant has documentation that access controls are employed.	Same as Medium, in addition: Access controls are validated by a competent third party.
	Comments			
	Criterion #5 (Wireless Access Protected)	The applicant declares that all wireless networks used in the maintenance of the UAS have basic network traffic encryption enabled.	The applicant has documentation that all wireless networks used in the maintenance of the UAS utilize advanced/stronger encryption for the network traffic.	Same as Medium, in addition: The security and encryption measures are validated by a competent third party.
	Comments			
	Criterion #6 (Software/Firmware Updates)	The applicant declares that maintenance procedures exist to review OEM security updates for applicability and are installed where appropriate.	The applicant has supporting documentation showing maintenance procedures exist to review OEM security updates for applicability and are installed where appropriate.	Same as Medium, in addition: The procedures are validated by a competent third party.
	Comments			

2.5 OSO#04 –UAS DEVELOPED TO AUTHORITY RECOGNISED DESIGN STANDARDS

The standard to which a UAS is designed is also an important factor in the overall system's resilience to cyber threats. A well-established cyber risk assessment process resident in a strong Organizational Culture (OSO #1) combined with a safety risk assessment process as already defined in OSO #5, and specifically required in OSO #10/12 (below) with a maintenance cyber hygiene established in OSO #3 (above), should sufficiently cover threats addressed by this OSO.

2.6 OSO#05 –UAS IS DESIGNED CONSIDERING SYSTEM SAFETY AND RELIABILITY

It is often difficult to analyse the apparent failures induced by cyber-safety shortfalls. For example, a GPS spoofing incident could appear as a malfunction of GPS equipment, inducing a fly-away event. Likewise, a C2 link jamming cyber-attack would likely manifest itself as a loss of link. Therefore, a system cyber-safety analysis considering cyber-safety events as potential causes of functional failures shall be used and coordinated with the system safety analysis. The equipment, systems, and installations minimize hazards in the event of malfunctions or failure of the UAS caused by Intentional unauthorized electronic interactions. A well-established cyber risk management process resident in a strong Organizational Culture (OSO #1) combined with a safety risk assessment required in OSO #10/12 (below) should sufficiently cover threats addressed by this OSO.

2.7 OSO#06 C3 LINK CHARACTERISTICS (E.G. PERFORMANCE, SPECTRUM USE) ARE APPROPRIATE FOR THE OPERATION

- (a) For the purpose of the SORA and this specific OSO, the term "C3 link" encompasses:
    - the Command and Control (C2) link, and
    - any communication link required for the safety of the flight.
- Therefore, this OSO addresses the cyber safety requirements in any C2 link to ensure continuity and reliability of the link between the Remote Pilot Station (RPS) and the UA or other service necessary for safety of flight. The C2 link comprises the telecommand or telecontrol datalink required to safely operate the UA. It does not include the transfer of payload data, such as video imagery, unless the video is used for safety of flight. Operational, or payload, data links should be assessed as well to determine risk of lateral movement within the network.

TECHNICAL ISSUE WITH THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #6 C3 link characteristics (e.g., performance, spectrum use) are appropriate for the operation	Criterion #1 (Datalink Encryption)	N/A	The C2 link employs encryption	The C2 link meets the minimum operational performance standards defined in RTCA/DO-377A or similar [1]
	Comments	*Derived from Spanish CAA, Operational Scenarios and Security Measures. Annex to "DOC. 1.3_02_SECURITY REQUIREMENTS_BASIC RPAS COMMUNICATIONS EQUIPMENT". REV 3, 21 November 20181 https://www.seguridadaerea.gob.es/sites/default/files/Doc.1.3_02_Rev%205_Requisitos_Security_Equipo_basico_comunicaciones_RPAS_5617_ESP_REV.pdf* *[1] The C2 link security function provides confidentiality of any sensitive data transferred through it; for this purpose local connections supporting the C2 link traffic meets the criteria of RTCA DO-377A Table 3-22 and section 4.3 or similar.*		
	Criterion #2 (Authentication)	The datalink employs basic mutual peer entity authentication between the UA and RPS[1]	The datalink employs advanced mutual peer entity authentication between the UA and RPS[2]	The datalink employs aviation standard authentication methods or equivalent[3]. In addition, human to machine interfaces employ multifactor authentication.
	Comments	*[1] TLS (Transport Layer Security)/SSL and passwords meet the intent of basic authentication.* *[2] The use of industry standard IOT cybersecurity best practices for authentication meet the intent of advanced authentication.* *[3] PKI certificates, as per ATA Specification No 42, meets the intent of aviation standard authentication*		
	Criterion #3 (Access Control)	The control station is paired with the UA using as a minimum a password. Default passwords are changed and meet security best practices for length, complexity,	Same as low, in addition: The system implements the concept of least privileged access. [1]	Same as medium, in addition: human to machine interfaces utilise multifactor access control, and machine to machine interfaces utilise aviation standard access control methods according to the NAA/competent authorities' requirements [2]

		expiration, history as best as configuration settings allows.		
	Comments	*Note the principle of 'least privilege' means a process, a user, or a program is able to access only the information and resources that are necessary for its legitimate purpose. The principle of 'access control' is a security technique that regulates who or what can view or use resources in a computing environment.* *[1] Refer to section 1.2.5* *[2] Access control in this respect is the ability to restrict utilization of the datalink.* *In the absence of an authentication-based access system, a physical security plan acceptable to the competent authority is employed.*		
	Criterion #4 (Data Integrity and Anti-replay Protection)	N/A	The datalink employs industry standard IOT cybersecurity best practices.[1]	The datalink employs aviation standard data integrity and anti-replay protection methods or equivalent.
	Comments	*The UAS C2 Link System security function provides data integrity and anti-replay protection for command and control communications between the UA and RPS.* [1] As an example consult: The Consumer Technology Association (CTA) is actively working on a standard for IoT cybersecurity as well as an appendix of that work specifically dedicated to UAS (CTA-2088), "**Baseline Cybersecurity for Small Unmanned Aerial Systems" -** https://standards.cta.tech/apps/group_public/project/details.php?project_id=594		

TECHNICAL ISSUE WITH THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #6 C3 link characteristics (e.g., performance, spectrum use) are appropriate for the operation	Criterion #1 (Datalink Encryption)	N/A	The applicant has documentation showing that link is properly encrypted	Same as Medium, in addition: the datalink encryption is validated by a competent third party.
	Comments			
	Criterion #2 (Authentication)	Applicant declares that data link employs basic authentication.	Applicant has documentation showing that link employs advanced authentication methods.	Same as Medium, in addition: the authentication methods are validated by a competent third party.
	Comments			
	Criterion #3 (Access Control)	The applicant declares that data link employs basic Access Control	The applicant has documentation showing that link employs advanced Access Control functions	Same as Medium, in addition: the access control functions validated by a competent third party.
	Comments			
	Criterion #4 (Data Integrity and Anti-replay Protection)	N/A	The applicant has documentation showing that the data link employs advanced data integrity and anti-replay protection.	Same as Medium, in addition: the data integrity and anti-replay protection functions are validated by a competent third party.
	Comments			

2.8 OSO#07 –INSPECTION THAT THE UAS IS CONSISTENT WITH THE CONOPS

Not applicable. The physical Inspection of the UAS to ensure consistency to the ConOps is not a cyber issue.

2.9 OSO#08/11/14/21 –OSOs Related to Operational Procedures

Appropriate cyber hygiene shall be added to all Operational Procedures and is an Operator responsibility. The guidance in OSO #1 for Operator Competence and OSO #3 for Maintenance shall be incorporated into the appropriate Operational Procedures.

2.10OSO#09/15/22 – OSOs Related to Remote Crew Training

Proper training of personnel is an Operator's responsibility. The guidance in OSO #1 for Operator Competence and OSO #3 for Maintenance shall be added to the appropriate training requirements – both initial and recurring.

2.11 OSO#10/12 OSOs Related to Safe Design and Safe Operation

Like modern aircraft, UAS consist of different systems, such as communications, navigation, and flight control, many of which rely on external services for their functioning. These systems must be designed to an appropriate level of safety so that cyber safety threats do not unreasonably compromise the UA's ability to maintain controlled flight and stay within the operational volume. The scope of this OSO includes those external systems, for example GNSS, which support the UAS operation and are not already part of the UAS.

OSOs RELATED TO SAFE DESIGN		**LEVEL of INTEGRITY**		
		Low	**Medium**	**High**
OSO #10 & OSO #12	Criterion #1 (Cyber Safety Risk Assessment)	The applicant reviews the CONOPs for cyber threats like those discussed in Section 1.3 and Section 2 of this Annex and selects a UAS that employs Concepts from section 1.2 and the Mitigations in Section 2.	Same as Low, but the applicant performs a cyber safety risk assessment using an acceptable industry standard considered adequate by the competent authority and / or in accordance with means of compliance acceptable to that authority[1].	Same as Medium
	Comments	*[1]Acceptable standards could include, for example, RTCA DO-326A/EUROCAE ED-202A, etc.*		

	Criterion #2 (GNSS Equipment, if used)	The applicant employs basic threat[1] mitigations.	Same as low, in addition: 1) The applicant implements health monitoring and reporting of received signal strength, number of satellites, including identification and time comparisons. 2) The applicant implements GNSS jamming detection. 3) The GNSS equipment makes use of multi-constellation GNSS.	Same as medium.
	Comments	*[1] Threats can be mitigated using, for instance; packet filtering, encryption, intrusion detection systems or other means of mitigation.*		
	Criterion #3 (Resilience in the Face of a Cyber Attack)	The applicant reviews the CONOPs for cyber threats like those discussed in Section 1.3 and Section 2 of this Annex and selects a UAS that employs Concepts from section 1.2 and the Mitigations in Section 2 such that probable cyber threats should not result in the UAS departing the operational volume.	Same as low, in addition: the review is performed using an acceptable industry standard[1].	Same as medium, in addition: the review is performed using a recognized aeronautical standard[2].
	Comments	*[1] Acceptable industry standards could include, for example, NIST SP 800 series, ISO 27000 series, etc.* *[2] Acceptable aeronautical standards could include, for example, RTCA DO-326A/EUROCAE ED-202A etc.*		
	Criterion #4 (Life Cycle Security Appraisal)	The applicant has procedures to re-accomplish the review called out in Criterion #1, whenever new or recently uncovered cyber threats are identified.		

	Comments	*[1] 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 (e.g. a new vulnerability is discovered).*		
	Criterion #5 (Test and Security Validation)	N/A	The applicant evaluates the effectiveness of threat mitigations identified as part of adherence to this guidance using an acceptable industry standard[1]	Same as medium. In addition, evaluation is performed using a recognized aeronautical standard[2].
	Comments	*[1] Acceptable industry standards could include, for example, CTIA Test Plan Level 2 or 3.* *[2] Acceptable aeronautical standards could include, for example, RTCA DO-326A/EUROCAE ED-202A etc.*		

OSOs RELATED TO SAFE DESIGN		**LEVEL of ASSURANCE**		
		Low	**Medium**	**High**
OSO #10 & OSO #12	Criterion #1 (Security Risk Assessment)	The applicant declares that a basic security assessment and threat mitigations have been undertaken.	The applicant has supporting documentation that a security risk assessment and threat mitigations have been undertaken.	Same as Medium. In addition, the assessment is validated by a competent third party.
	Comments			
	Criterion #2 (GNSS Equipment)	The applicant declares that basic threat mitigations are employed.	The applicant has supporting documentation that threat mitigations are employed.	Same as medium. In addition, the threat mitigations are validated by a competent third party.
	Comments			

	Criterion #3 (Resilience in the Face of a Cyber Attack)	The applicant declares that the evaluation has been undertaken.	The applicant has supporting documentation that the evaluation has been undertaken.	Same as medium. In addition, the evaluation is validated by a competent third party.
	Comments			
	Criterion #4 (Life Cycle Security Appraisal)	The applicant declares that procedures exist to update the Security Risk Assessment.	The applicant has supporting documentation that procedures exist to update the Security Risk Assessment.	Same as medium. In addition, the procedures are validated by a competent third party.
	Comments			
	Criterion #5 (Test and Security Validation)	N/A	The applicant has supporting documentation that the evaluation of mitigation effectiveness has been undertaken.	Same as medium. In addition, the evaluation of mitigation effectiveness is validated by a competent third party.
	Comments			

2.12 OSO#13 External services supporting UAS operations are adequate to the operation

External services supporting UAS operations are adequate to the operation. For the purpose of the SORA and this specific OSO, the term "External services supporting UAS operations" encompasses any service provider necessary for the safety of flight (e.g., Communication Service Provider (CSP), UTM service provider, etc.). It is assumed that the service providers covered in this OSO are essentially Information Services, for which very adequate cybersecurity standards already exist (e.g., NIST 800 framework, ISO 27000 series, etc.). A good example of this is the FAA requirement for system cybersecurity when becoming an approved UTM Services provider. The difference in Robustness comes from the level of Assurance, which is generally in line with other OSOs.

DETERIORATION OF EXTERNAL SYSTEMS SUPPORTING UAS OPERATION BEYOND THE CONTROL OF THE UAS		LEVEL of INTEGRITY		
		Low	**Medium**	**High**
OSO #13 External services supporting UAS operations are adequate to the operation	Criteria	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.		
	Comments	*For example, ISO 23629-12 contains security requirements for the UTM Service Providers.*		

DETERIORATION OF EXTERNAL SYSTEMS SUPPORTING UAS OPERATION BEYOND THE CONTROL OF THE UAS		LEVEL of ASSURANCE		
		Low	**Medium**	**High**
OSO #13 External services supporting UAS operations are adequate to the operation	Criteria	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).	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,	Same as Medium, in addition: - The evidence of the externally provided service cybersecurity is achieved through demonstrations. - A competent third party validates the claimed level of integrity.

			responsibilities). 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.	
	Comments			

2.13 OSO#16/17/18/19/20 OSOs Related Human Error

For OSO #16, Multi crew coordination, the security technical controls for authentication and authorization that are called for in the OSOs #1/6 requirements should be sufficient. The OSO regarding the Remote crew being fit to operate (OSO #17) is not impacted by cyber issues since it is primarily focused on each human's physical and mental fitness to perform duties and discharge responsibilities safely. OSO #18, Automatic protection of the flight envelope from human errors, should be adequately covered in OSOs #5, 10/12 as should OSO #19, Safe recovery from Human Error, when combined with the cyber hygiene defined in OSO #3. For OSO #20, A Human Factors evaluation has been performed and the Human-Machine Interface (HMI) found appropriate for the mission, misleading information presented to the remote pilot and Operations crew is the issue and should be adequately addressed in OSOs #10/12 (above).

2.14 OSO#23/24 OSOs Related to Environmental Conditions

The main concern is related to obtaining proper weather information from trusted sources so the Operator can meet OSO #23. Data integrity and authenticity of service suppliers addressed in OSO #13 should sufficiently address this issue. For OSO #24, UAS designed and qualified for adverse environmental conditions, there are no known cyber concerns.

2.15 M1 - Strategic Mitigations for Ground Risk

a) Generic criteria: for Criterion #2 (Evaluation of people at risk) Medium Integrity and above, the "authoritative density data" (e.g., data from UTM data service provider) must meet appropriate requirements for authenticity. See OSO #13 for more discussion.
b) Not Applicable to tether.

2.16 M2 - Effects of Ground Impact are Reduced

While it is possible that the system used for compliance with M2 may have cyber vulnerabilities, it is most likely that these susceptibilities are better thought of in terms of M2 system (e.g., the parachute recovery system) reliability. See OSO #4, OSO #5, OSO #10/12.

2.17 M3 - An Emergency Response Plan is in place, operator validated and effective

The Emergency Response Plan (ERP) should include mention of cyber instances and should identify the Operator point of contact, the reporting/escalation process and invoke the appropriate logging and reporting mechanisms. The ERP cyber response should include log analysis, incident evaluation, incident escalation process, and security process development and planning. Training identified for the Medium and High levels of Assurance must also include training on cyber instances for how to respond and recover.

APPENDIX 1: THREAT INFORMATION SHARING

Aviation is reliant on interconnectivity between a large number of systems being controlled by a large number of diverse stakeholders. An improved level of cyber resilience an only be achieved when the relevant stakeholders work together by sharing experiences. Information sharing therefore is key and must be the norm.

Information that should be shared could include details (as far as required confidentiality allows) of systems in use, already known and potential vulnerabilities of systems, applied mitigations, processes, procedures, and best practices used to improve cybersecurity. Due to its global reach, information sharing in aviation also is a difficult endeavour and satisfying each stakeholder's requirements (e.g., confidentiality) is a complex task. Therefore, several specialised organisations have taken this responsibility on board to act as a forum and platform for interested stakeholders to share cybersecurity-relevant information across the aviation sector.

ISAC – INFORMATION SHARING AND ANALYSIS CENTRE

An ISAC represents an entity which due to its connections with numerous stakeholders is ideally positioned to gather, analyse, and disseminate relevant information on cybersecurity risks. This information can include but is not limited to IOC (Indicators of Compromise), hardware and software product vulnerabilities, threat actors, threat vectors, etc.

An ISAC analysis should gather information that will produce meaningful reports for its customers. Based upon this information, customers can react, mitigate, or prevent information security occurrences. ISACs are often created to serve customers of a specific sector, e.g., aviation, energy.

A-ISAC

The Aviation ISAC (A-ISAC) is a specific ISAC serving the aviation sector and its stakeholders. The mission statement of the A-ISAC aims at facilitating collaboration across the global aviation industry to enhance the ability to prepare for and respond to vulnerabilities, incidents, and threats, to disseminate timely and actionable information amongst members and to serve as the primary communications channel for the sector with respect to this information.

ECCSA

The European Centre for Cybersecurity in Aviation (ECCSA) is a voluntary, cooperative partnership within the aviation community whose goal is to better understand the emerging cybersecurity risk in aviation and to provide collective support in dealing with cybersecurity incidents, weaknesses and unauthorised interactions that could potentially affect the sector's resiliency and safety.

ECCSA membership and participation is voluntary, and stakeholders interested and holding a role in safety and security of European Civil Aviation may apply for ECCSA membership after passing applicable security selection criteria.

ATM CERT / CSIRT

To mitigate any confusion with terminology this section will explain the difference between CERT and CSIRT which are sometimes used interchangeably.

CSIRT – Computer Security and Incident Response Team

A CSIRT, according to a 2007 Carnegie Mellon document "Defining Computer Security Incident Response Reams." is defined as: "A computer security incident response team (CSIRT) is a concrete organisational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident."

CERT – Computer Emergency Response Team

The term "CERT" is a registered trademark of the Carnegie Mellon University since 1997 and organisations can apply for authorization to use the "CERT" term. According to Carnegie Mellon, the CERT has a particular focus and niche it occupies, operating as a "… partner with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks …". A "CERT" studies "… problems that have widespread cybersecurity implications and develops advanced methods and tools."

CSIRTs/CERTs thus, have usually a sector or organisation specific scope and focus on the response activities in case of computer security incidents. A practical example for an aviation related CSIRT/CERT is the EATM – CERT, EUROCONTROL: European Air Traffic Management – CERT that supports EUROCONTROL services and products, as well as ATM stakeholders, in protecting themselves against cyber threats that would impact the confidentiality, integrity and availability of their operational IT assets and data.