IATA	**IATA Information Bulletin**	Bulletin No.: UAS1/2018 Date: 11 June 2018

Subject: Key considerations when protecting manned aviation from drones.

Background:

The use of Unmanned Aircraft Systems (UAS), often referred to as drones, is expanding rapidly and key aviation stakeholders (e.g. airports, aviation authorities) are considering how to mitigate the risk. One solution is to employ suitable technology with appropriate measures.

Anti-Unmanned Aircraft System (Anti-UAS) measures are a set of technological and operational tools that were developed, and are being used, to monitor, detect, identify and record inappropriate or dangerous UAS activities. These activities include the infringement of restrictive or sensitive airspace, or UAS operating dangerously close to manned aviation. These measures may include some countermeasures aimed to neutralize, or limit, potential risks posed by uncooperative UASs. These measures and associated technologies can be both beneficial and harmful to aircraft and ATM operations. Therefore, anti-UAS measures should only be implemented following an appropriate safety assessment taking into account potential impacts to all aviation stakeholders.

Anti-UAS Operational Measures:

Some States, airports and aviation agencies are considering the use of anti-UAS measures to manage safety and security risks posed by uncooperative UASs. Below are some examples of these anti-UAS measures and associated technologies.

Detection of UAS

One available technology is the use of a radio-frequency (RF) signal analyzer. This system is able to detect, monitor, and analyze all relevant radio frequencies and supporting techniques (i.e. frequency hopping) which are used to operate the UAS. The RF signal analyzer can be used in combination with a direction finder to locate the UAS operator. This technique is particularly applicable to FHSS (Frequency-Hopping Spread-Spectrum) UASs operating at 2.4GHz frequency band.

For some UASs that are flying autonomously and may not have simultaneous radio-control links, there are systems such as uncooperative RADAR[1], optical tracking (e.g. video and thermal tracking cameras) or acoustic technologies may be capable to detect these UASs.

Countering UAS

Some existing UAS countermeasures include:

1. Selectively jamming of the RF signal being used to operate the UAS.

2. Interrupting the Wireless Local Area Network (WLAN) signal being used by some UASs or broadcasting a set of radio-communication (RC)/computer commands to “take control” of the UAS are possible. This technology should however be appropriately controlled to avoid instances of possible illegal sabotage or UAS hijack.

3. Use of UAS interceptors. Interceptors may include UAS nets and trained predatory birds. These measures should however be used with proper due regard to the possible additional safety risk to manned aircraft.

[1] Uncooperative RADAR technologies include but not limited to Primary Surveillance RADAR, holographic RADAR and multi-illuminators passive RADAR.

It is very important to note that in general, any UAS countermeasures which infringe on local laws and regulations, or create higher risks and may cause danger to other aviation stakeholders, should be avoided. These high risk solutions may include the use of bullets or laser guns.

Considerations and Suggestions

Anti-UAS measures should generally only be implemented within locations or airspace where there is a recognized safety and security risk to justify any infrastructure and operational costs for anti-UAS measures. The areas of interest include the critical safety-sensitive areas around airports such as final approach, missed approach and departure corridors.

The use of anti-UAS measures should not cause unintended safety or operational hazards to aircraft or aviation infrastructures. For example, the jamming or spoofing[2] of GPS signals needs to be avoided as it may harmfully impact aircraft navigation systems as well as air traffic management systems - both of which heavily rely on functional, uninterrupted GPS signals. Implementation of anti-UAS measures must also be subject to a safety assessment and risk mitigation process in order to manage unintended risks.

In deciding in the deployment of anti-UAS measures, States, airports and aviation agencies are recommended to consider anti-UAS measures that are able to:

1. Support continuous monitoring of UAS activities;

2. Detect, identify and record UAS activities in a timely manner and, where capable, geo-locate the operator of the UAS.

3. Perform effective countermeasures that can be safely and legally activated in time to prevent a UAS from entering an area of interest.

<u>Concurrently, anti-UAS measures should NOT:</u>

1. Create unintended safety hazards and unmitigated risks to other aircraft and aviation infrastructures;

2. Infringe with local laws and regulations

3. Interfere with radio frequencies being used by aircraft, air traffic management (ATM) systems and other legally authorized applications, for example;

    a. GPS/GNSS jammers and spoofing should not be used as anti-UAS measures as they can concurrently interfere with the operations of other aircraft. Moreover, technologies for protecting UASs against GPS/GNSS jamming and spoofing are being tested and expected to soon be commercially available.

    b. RADAR technologies used for anti-UAS purposes, frequency usages by the Anti-UAS system and other RADAR-based systems used for ATM, such as primary surveillance RADARs for approach control and airport surface movements, need to be appropriately coordinated and empirically validated such that there will be no adverse impact to ATM system.

4. Result in UAS maneuvering unpredictably;

    a. Technologies used to disrupt the command/control link between a UAS and its operator, must mitigate the safety risks associated with a UAS not being under anyone's positive control, in particular during a "lost link" stage.

    b. During a "lost link" stage, some UASs are pre-programmed to perform specific maneuverings, such as "stay still", "return to base" and "land now". However, such pre-programming cannot always be guaranteed.

[2] Transmitting signals that imitate GPS signals with the intention to falsely navigate the recipient.