Czech Technical University in Prague
Faculty of Transportation Sciences
Department of Air Transport

Magazine of Aviation Development
6(3):12-16, 2018, ISSN: 1805-7578
DOI: 10.14311/MAD.2018.03.02

Unmanned Aircraft as a Subject of Safety and Security

Michaela Mlezivová[1]*

[1]Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University in Prague, Prague, Czech Republic

***Corresponding author**: Czech Technical University in Prague, Faculty of Transportation Sciences, Department of Air Transport, Horská 3, 128 03 Prague, Czech Republic, Email: mlezimic@fd.cvut.cz

Abstract

Currently increasing UAV operation significantly changes the view of conventional aviation. Unmanned aerial vehicles have become part of air traffic and therefore, its operation should be adequately controlled through related legislative framework and law enforcement procedures. Considering the fact, that single unmanned aircrafts will be soon replaced by swarms, it is necessary to get prepared for all possible UAs applications and define all rules including also emergency and law enforcement procedures in case that public safety is endangered.

This paper summarizes recent regulatory framework for UAVs in EU and US and points out a concealed weakness of legislative requirements. The legislative scope addressed in this paper is limited primarily to civil aviation. The second part stresses the security threat created by an uncontrolled or violently-controlled UA. Aerial vehicles detection and disposal methods are described in the last part of paper.

Keywords

Unmanned Aircraft; UAV; Safety; Security; Legislation; Anti-drone

1. Introduction

The blooming UAV market increases the pressure on safety and security improvements. Among other things, it requires creation of high-quality legislation which should clearly define more requirements on safety integrity and architecture of control systems. Even though, law enforcement units and military forces do not have to care about new regulatory framework applicable to the civil aviation, they must keep track of UA's increasing popularity. From their perspective, UAVs represent two major roles – a tool for law enforcement purposes and a security threat.

Effective regulation of UAVs' operation is fundamental for sustainability of:

- Safety, by preventing any collision with surrounding air traffic (especially near airports) and by keeping UAVs away from persons and property on the ground and to the environment;
- Security, by keeping UAVs at an appropriate distance from areas with special restrictions;
- Privacy protection, by rules providing a proper separation from residential areas.

This paper summarizes recent regulatory framework for UAVs in EU and US and points out a concealed weakness of legislative requirements. The legislative scope addressed in this paper is limited primarily to civil aviation. The second part stresses the security threat and deals with ways how to prevent or reduce its consequences. Detection and disposal methods are described in the last part of paper.

2. Brief overview of regulatory framework for UAS

In comparison to European environment, FAA is significantly advanced with the legislative restrictions on unmanned aerial vehicles operation. Basically, a pilot of a small UAV can choose from two options, each with different requirements depending on how a pilot wants to fly an UAV. Either way, a pilot must obtain a remote pilot certificate and register a UAV under either Part 107 (Small UAS Rule) or Section 336 (Special Rule for Model Aircraft). [1]

The training course for pilots aims to raise safety awareness through providing important knowledge of applicable regulations. The scope contains small unmanned aircraft system rating privileges, limitations, and flight operation, effects of weather on UA performance, UA loading and performance, emergency procedures, maintenance and preflight inspection procedures. [1]

In the European context of UA operation, EASA has no direct competence to regulate unmanned aircrafts lighter than 150 kg since this right is still under national aviation authorities (AA). The current regulatory framework for UAS differs across all EU member states. Registration of UAS depends both on the type of UAS and on the purpose of usage (e.g. registration might be only required for professional use). Furthermore, some AAs require registration for an operator only, while others for a UAS as well. For example, registration for an operator is required in the Czech Republic, Denmark, Finland or the Netherlands. But, for instance in Spain, registration is only required for a UAS with MTOW of more than 25 kg. The fragmented regulatory framework across the EU has been no longer acceptable for EASA and therefore, the national regulations will be progressively replaced in 2019 and 2020 by new European legislations. [2]

All member states of European Union are subjected to adopt EU policies concerning regulatory and certification process of EASA. With the new Basic Regulation for unmanned aircrafts, EASA will set the new rules particularly for the approval of design, production and maintenance organisations, air operator certificates, operations of UA and licenses of personnel. The adopted regulatory framework will work for three categories of UA's operations - open, specific and certified. Drones shall comply with different requirements of each category (see Fig. 1). [2]

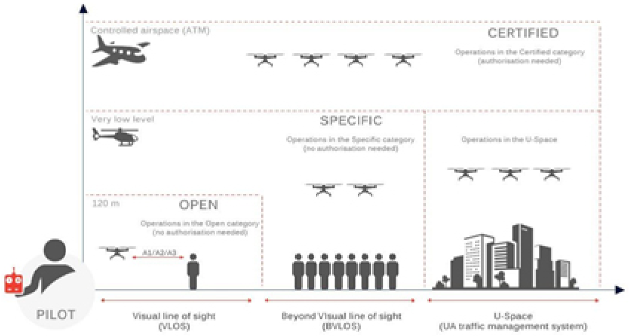
Controlled airspace (ATM)
CERTIFIED
Operations in the Certified category
(authorisation needed)
Very low level
SPECIFIC
Operations in the Specific category
(no authorisation needed)
Operations in the U-Space
120 m
OPEN
Operations in the Open category
(no authorisation needed)
A1/A2/A3
PILOT
Visual line of sight
(VLOS)
Beyond Visual line of sight
(BVLOS)
U-Space
(UA traffic management system)

Figure 1. Graphical representation of new UAS categories.[3]

2.1 Lack of Requirements on UA's Control Software

Regulatory framework for unmanned aircrafts operation should ensure the highest common level of safety protection. The new legislation should take into account also the fact, that since there is no pilot onboard, the control software of UA takes the responsibility for maintaining UA's safety and security. It is surprising, that there is no mandated standard in place defining the requirements on functional safety of UA's control system. Considering the risks involved, it is certainly needed the UAS to be developed to meet an acceptable level.

The high rate of human-error related accidents in manned aviation will no longer represent such a problem for unmanned aviation since all UAVs are increasingly becoming operator-independent. The control systems can work autonomously using various algorithms and already launched a new era of vision and collision avoidance. Therefore, it is more necessary than ever to pay attention to the control systems of UAs. If we take in account the defensive barriers from Reason model, which is a widely accepted tool used in risk analysis and risk management in manned aviation, they are represented by Regulations, Training and Technology layers. It is apparent, that the new European legislation for UA's operation is still more oriented on reducing of human factor errors than on increasing a safety integrity level of used technology.

There are few standards in place which could be taken as a reference for creating safe computing systems:

1. IEC 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)" is an international standard which defines the requirements and guidelines for its application. It ensures that systems are designed, implemented, operated and maintained to meet the required safety integrity level (SIL), no matter field where the system is intended to be put in operation. This standard is already commonly used in aviation industry. [4]

2. The standard DO-178C "Software Considerations in Airborne Systems and Equipment Certification" defines requirements on software development in the avionics industry and provides detailed guidelines for the production of all software for airborne systems and equipment. DO-178 recognizes that software safety must be considered throughout the lifecycle - i.e. phase of planning, development (requirements / design / implementation), testing, verification and certification. [5]

The system's errors can be caused by either a random event (a failure or a design or manufacturing error) or by an intentional activity of an intruder. Therefore, besides the safety aspects it is certainly critical to ensure the system to be resistant against external attacks. UAV can only be considered safe when no one else besides appointed operators can take over control.

Especially in military applications, it is unacceptable that any non-encrypted information would be received by a third party and thus data encryption represents a must-have feature of data link systems leading the current market. The primary communication paths are:

1. duplex channel between an aircraft and a ground control station; and
2. one-way path between an aircraft and GNSS satellites

The first mentioned path, the communication between an aircraft and a GCS is more than desired to be safe, secure and reliable. The most common encryption used in the current market of data link systems is the Advanced Encryption Standard (AES) with block and key sizes with a minimum of 128 and a maximum of 256 bits.

3. Unmanned Aircraft as a Security Threat

The uncontrolled operation of unmanned aircrafts poses a major threat not only to the surrounding air traffic. The current (or in EU being prepared) legislation regulates the operation of unmanned aircrafts in order to minimize risks and enhance the safety. However, legislation does not actively help with countering an UA attack.

There are many civilian and military areas or events which should be protected against hostile acts coming from airside. Unfortunately, the ways how to deal with such air threats are limited and closely depend on many factors. Moreover, the consequences when a drone returns to the ground must be taken into account as well. The more sophisticated UAS is, the bigger security threat it represents, and it gets even worse in case of swarms.

The basic concept of security strategy consists of both proactive and defensive approach.

3.1 Proactive Approach

A proactive approach is generally aimed to identify and apprehend any hostile action before it comes to a strike. Security information service and intelligence services are responsible for collecting and evaluating information concerning terrorist threats. It works well in case of organized crime, however they cannot effectively fight with random acts of individuals.

3.2 Defensive Approach

Defensive approach basically means both the measures taken to minimize consequences of attack and the measures aimed directly to destroy or reduce the effectiveness of a threat. The first step which must be done is to detect/identify the threat.

3.2.1 Detection methods

The UA detection methods are closely related with both the environment and the target's characteristics. Radars are likely the most used systems for UA detection. More precisely, two radar configurations:

- active radar (mainly PSR) transmits a signal which is then reflected back to the receiver,
- passive radar detects any RF emission (therefore this does not work for autonomous UAs).

The advantage of an active radar is, that only one PSR can provide, besides the basic detection, also further information about the object, such as its size, shape or speed and the direction of its movement. On the other hand, a passive radar detects an object regardless its reflective surface size and moreover, since the radar does not transmit any signal, it cannot be localized and jammed. Further sensors, such as acoustic, optical or IR sensors, are also used as parts of detection systems.

As mention above, all detection methods closely depend on many other factors. Therefore, technical solutions, that integrate multiple detection methods into one device, provide the most reliable outputs. At the same time, a combination of several sensor types contributes to more accurate identification of targets.

Anyway, it is necessary to detect the approaching object as soon as possible for further evaluation and decision-making. Once the flying object is detected, a competent operator shall receive evaluated data – i.e. as much information as possible to describe UA's actual status (such as speed, coordinates, altitude, predicted trajectory or at least predicted direction, dimensions, etc.). Of course, it is not easy to gather all these information in a short time, however even approx. info about the target's speed might help a lot.

3.2.2 Disposal methods

There are many ways how to directly minimize a hostile air threat, however in certain cases taking drones down safely is almost impossible. Unfortunately, no universal solution or procedure guarantees a success. Following anti-drone weapons or procedures can serve as active defensive measures:

1. Net guns
   (a) From ground
   (b) From another drone / drones

   One of the easiest way how to restrict an unauthorized drone from flying is to catch it into a net. Of course, it is applicable only on small, slowly flying, light UAs (e.g. a copter). Main advantages are a low cost and the simplicity.

2. Drone-downing birds Basically, this option works for the same types of UAs which can be stopped by a

net. Training of drone-hunting birds is very expensive and complicated though. According to NL Times, the Netherlands was the first country in the world that started using birds of prey against unauthorized unmanned aircrafts and eventually dropped the project by the end of 2017. [6]

3. Radio-frequency jamming tools
   (a) To jam communication between GCS and UAV
   (b) To jam GPS signals

   The radio jammers serve well for defense of certain areas and are able to stop even bigger and faster hostile UAs, which could neither be stopped by a net nor by specially trained birds of prey. If communication with an operator is jammed, the UA activates pre-set mode depending on current system setting. Commercial copters usually either activate the home-return mode or keep following a pre-programmed trajectory. If a UAV flies autonomously, only GPS signals can be jammed, which usually means fail-safe mode activation. From the engineering point of view, the success of signal jammers closely depends on three factors – transmit power (of both UAV and GCS), antenna gain (higher antenna gain can extend the effective range of a jammer) and radio-frequency noise level in the environment. Nevertheless, jamming works only as long as the RF noise level from the signal jammer is above the signal from the control antenna. Therefore, once it is below, an operator can again take over the control.

4. Control take over
   (a) To hack a command channel
   (b) To hack a communication and fake GPS signals

   This method is likely applicable only to commercial drones with generally-known and easily hackable remote control protocols. Concerning that fact, it is almost impossible to take down a UAV with professionally encrypted communication. Another limitation is, that you cannot take over UA while flying autonomously. In this case, it is possible to fake GPS signals and thus influence the further trajectory of the UA. The main advantage of this method is the possibility to take control of an unauthorized UA and land it safely on a convenient place for a hacker. Because the hacking is targeted on the particular unmanned aircraft, there is no risk of jeopardizing other electronic devices in the vicinity (which is certainly an advantage over the signal jammers).

5. Anti-aircraft weapons Anti-aircraft weapons are mainly targeted to bigger unmanned aircrafts of a medium, heavy or super heavy weight category. Therefore, its application is more applicable in the military sector. Concerning the small UAs, this method is kind of inappropriate. The use of such technique is very expensive, and moreover, it would be almost impossible to target the missile to a small UA.

6. Firearms

Firearms represent another low-cost and simple way how to quickly destroy a hostile UAV. It comes even more effective since the commercial UAs are usually made from cheap and non-resistant materials. On the other hand, this method is limited by the range of a shotgun and by potential negative impact on safety. Should the unmanned aircraft was shot down, the area of the subsequent crash must be considered as well as the fact, that the shooting shall not pose any threat for surroundings.

Each aforementioned active-defense method has its pros and cons and its effectiveness is closely related to many circumstances and conditions. Thus, the countermeasure should be always chosen appropriately according the certain situation.

4. Conclusion

UAV boom and its impact on safety and security clearly brings up many concerns which should not be omitted. Both safe and secure operation of UAVs is fundamental for general sustainability of public safety. The UAs' operation will never be under complete control, but the relevant steps have been already undertaken. The legislation regulating UAs' market is progressively being put in place. Nevertheless, the regulation seems to be insufficient in terms of requirements on safety integrity level of control systems. Moreover, the manufacturers of UAS continuously evolving more advanced solutions and technologies. The market with defensive systems is also going forward. However, despite a list of such anti-drone weapons is quite long, they are apparently not efficient enough unless being a part of complex defensive system (combination of sensors, technologies and procedures).

Since development of modern technologies is making huge strides forward, the sophisticated algorithms will be soon replaced by complete artificial intelligence. While all competent aviation authorities are currently working hard on legislation for UAVs, the parallel works should be immediately targeted on preparation of regulatory framework for swarms. The era of swarms is just around the corner and it certainly poses even bigger security threat to the global community than a single unmanned aircraft.

References

[1] Federal Aviation Administration. Federal aviation administration, 2018. URL https://www.faa.gov/uas/.

[2] EASA. Civil drones, 2018. URL https://www.easa.europa.eu/easa-and-you/civil-drones-rpas.

[3] DroneRules. Dronerules.eu, 2018. URL http://dronerules.eu.

[4] International Electrotechnical Commission. Functional safety: Essential to overall safety, 2018. URL http://www.iec.ch/about/brochures/pdf/technology/functional_safety.pdf.

[5] Charlotte Adams. Safety-critical software for mission-critical applications to get boost with release of do-178c, 2010. URL https://www.militaryaerospace.com/articles/2010/10/safety-critical-software.html.

[6] Janene Pieters. Dutch police drops drone-hunting eagles project, 2017. URL https://nltimes.nl/2017/12/07/dutch-police-drops-drone-hunting-eagles-project.