RPAS COMMITTEE OF THE AESA

WORKING GROUP 1.3. TECHNOLOGY AND SECURITY

Working Subgroup SGT 1.3. C3 Communications Requirements for RPAS (Remotely Piloted Aircraft Systems) and Cyber-security

Document 1.3_02

Date: **21 November 2018**

Subject: ***Security requirements of the basic communications equipment of RPAS***

Summary: Document defining the security requirements (including measures against illegal interference) of the basic communications equipment of RPAS

Comments:

CONTENTS

1 PURPOSE AND SCOPE OF THE DOCUMENT

This document describes the security requirements and specifications that must be met by the basic equipment of an **RPAS** (*Remotely Piloted Aircraft System*) in order to ensure the continuity of communications links, especially in the event of deliberate interference. The basic communications equipment only includes the Telemetry and Telecontrol (or Telecommand) subsystems of RPAS.

Royal Decree (RD) 1036/2017, of 15 December, regulating the civilian use of aircraft piloted by remote control, specifies in ***Art. 13.1*** that: "***the command and control link forming part of the RPAS must ensure the execution of these functions with the continuity and reliability necessary in relation to the operations area***". ***Art. 13.2*** also mentions that: "***The command and control link must comply with the current regulations regarding the use of the radio spectrum and deploy frequencies appropriately selected to minimise the possibility of interference, voluntary and involuntary, that may affect the security of operations, subject to its authorisation by the Ministry of Energy, Tourism and Digital Agenda when appropriate in accordance with the applicable regulations***."

This document is written in keeping with the objective of the RPAS Committee to implement the regulations of the new RD on RPAS, with a special emphasis on the articles mentioned above. More specifically, this document addresses the problem of the possible voluntary and illegal interference that may be suffered by the C2 communications link of an RPA and, by extension, any type of voluntary, deliberate or illegal action affecting the entire RPAS (including the RPA and the RPA control station), carried out by unauthorised persons with the aim of taking control of the RPA or the entire RPAS. This document briefly lists the potential cyber-security vulnerabilities of RPAS and contains a section at the end on measures to "secure" the communications link, as well as the entire RPAS. SGT 1.3 has also produced an Appendix to this document that shows a list of operating scenarios and, for each operating scenario, describes which "security" measures are most appropriate to apply.

When the RPAS Committee of the AESA was formed in 2017, the SORA (Specific Operations Risk Assessment) methodology developed by the JARUS organisation to conduct risk assessments on RPAS operations still did not contemplate conducting assessments of the safety risks introduced or caused as a result of deliberate attacks or cyber attacks on RPA. That is, in 2017, the SORA methodology did not include security issues that could influence the safety aspects of operations. ***This omission of security from the SORA methodology was one of the reasons why the RPAS Committee of the AESA asked Subgroup SGT 1.3 to prepare this report***. In October 2018, a proposal arose within JARUS to introduce within SORA an assessment methodology for the security risks that could affect or influence the safety of RPAS operations in any way (see [1] in the Bibliography section), in order to somehow overcome the aforementioned omission. However, on the date on which this report was written, November 2018, this proposal has still not been implemented within the JARUS forums and even if its implementation were to be successful, it is unlikely that this implementation would be carried out in the next few months or even years. Thus, and ***on the date on which this report was written, November 2018, JARUS has still not resolved the issue of what security aspects may affect the safety of RPAS operations. This report is one of the few sources currently available to the RPAS Committee of the AESA on this issue and it comes closest to resolving (albeit in an initial manner) the problem of the security aspects in RPAS***. It cannot be ruled out that this report may serve as a starting point or initial document for JARUS when conducting debates aimed at developing this new methodology for the assessment of security risk that affect the safety of RPAS operations.

This document does not address the safety requirements of the communications link of the basic equipment of RPAS, given that those requirements are addressed in the document "*Doc. 1.3_01_Safety Requirements_Basic communications equipment of RPAS*" of subgroup SGT 1.3. It also does not address the requirements of other types of communications links (additional equipment and special equipment).

Moreover, this document does not address the payload links which remain outside its scope, except in those matters where, for security reasons, it is helpful to take the payload links into account.

In addition, this document is focused on describing the requirements for RPA that weigh less than 25 kg, those weighing more being outside the scope of this document.

This document does not address (as the RD excludes them from its objective scope) the following aircraft:

a) Military remotely piloted aircraft and aircraft systems (RPAS).

b) Remotely piloted aircraft (RPA) used exclusively for air shows, recreational or competitive sporting activities, as well as those whose maximum take-off mass exceeds 150 kg, unless, in the latter case:

1. They carry out customs, policing, search and rescue, fire-fighting, coastguard or similar activities.

2. They are excluded from the application of (EU) Regulation 20198/1139 of the European Parliament, of 4 July 2018, due to the occurrence of any of the circumstances specified in its appendix II.

C) Unmanned free balloons and moored balloons.

d) Flights that take place fully in completely enclosed interior spaces.

2 INTRODUCTION AND INITIAL INFORMATION

This section briefly describes RPAS, including the C2 communications link and other equipment on board the RPA.

2.1. DESCRIPTION OF THE TELECOMMAND OR TELECONTROL AND TELEMETRY LINKS OF THE BASIC EQUIPMENT, ALSO KNOWN AS C2 LINKS

Below is a simple RPAS including the fundamental components of the basic communications equipment of the RPA. More information about the basic communications equipment, C2, of an RPA can be found in the document "*Doc. 1.3_01_Safety Requirements_Basic communications equipment of RPAS".*

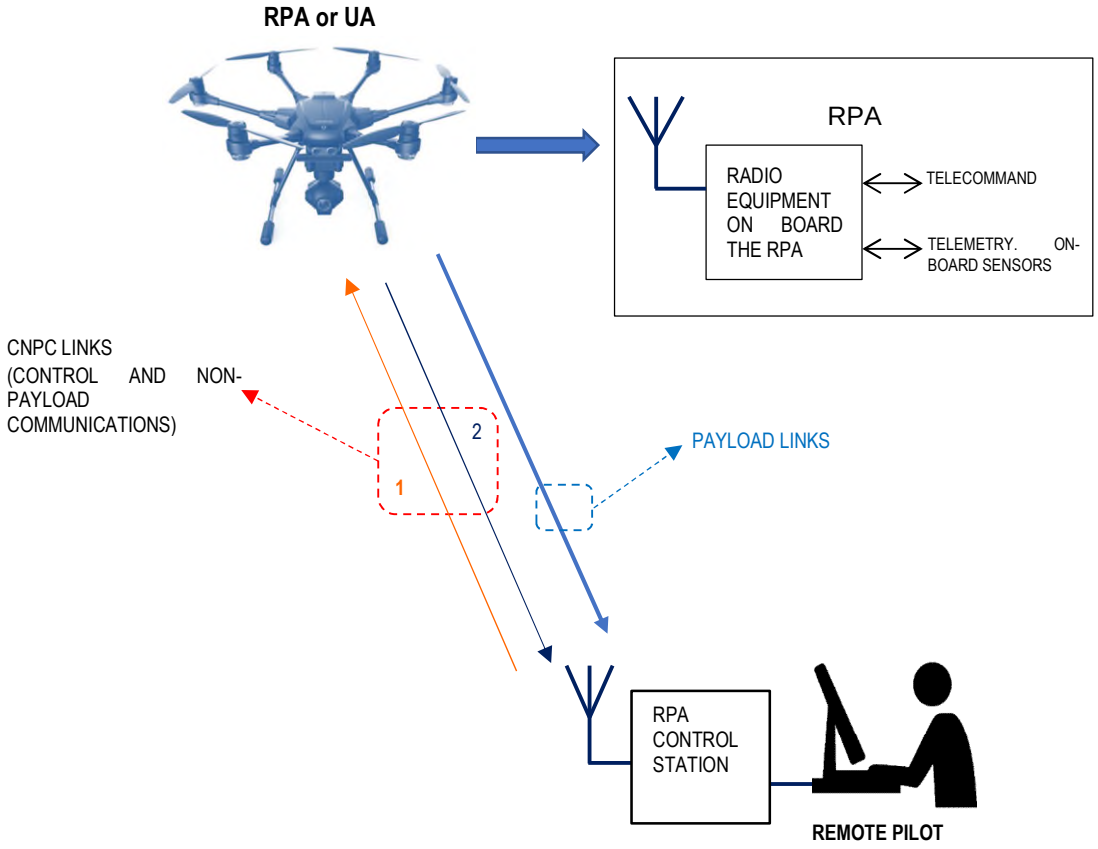

Fig 1. SIMPLE RPAS WITH BASIC COMMUNICATION EQUIPMENT ON BOARD THE RPA. C2 LINK

As can be seen in the above figure, a simple RPAS would consist of an RPA with basic communications equipment on-board. This ***basic equipment would only allow the use of Telemetry and Telecommand (or Telecontrol) communications, or C2 links***. In the above figure, these links are 1 and 2. These links are also called ***CNPC*** (*Control and Non-Payload Communications*) links. The basic communications equipment only includes these C2 links but not the ATC and ATS links with air traffic control. When remotely piloting through the control station, communication with the RPA is through the above links.

This basic equipment has been designed in this way, as there are commercial operational scenarios created by SGT 2.2 that use RPA and do not include communications with air traffic control.

This document will focus on the security aspects that affect the C2 links or CNPC links. It also addresses the security aspects involving the payload link, also been shown in the above figure, and deals with security aspects that affect other RPAS subsystems.

Moreover, the control station from where the remote pilot controls the RPA may range from a complex room with various people to a portable computer operated by a single person, with other options including through laptops or tablets with specific software for controlling the RPA. See the following figure obtained from document [2].

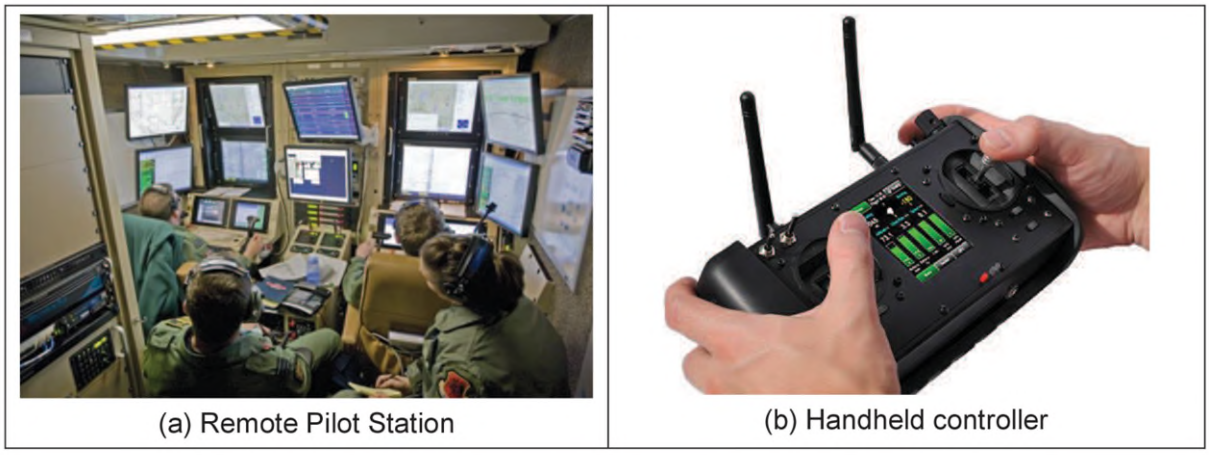

Fig 2. TYPES OF RPA CONTROL STATION IN ACCORDANCE WITH EUROCAE DOCUMENT ER-012

The radiocommunications equipment in figure 1 solely and exclusively transmits the links:

* ***Telecontrol*** (telecommands from the control station to the RPAS). *Art. 13.1 of RD.*

* ***Telemetry*** (RPAS status data sent from the RPAS to the control station). *Art. 13.1 of RD.* From among all the information transmitted to the control station, it is worth highlighting the following:

  - Flight parameters of the RPAS: speed, height above ground, direction, latitude, longitude, pitch, yaw and roll parameters, etc.
  - Charge status of the batteries on board
  - If applicable, status of the fuel tanks
  - Data on monitoring the health status of the data link itself. See NOTE
  - Data from the other sensors on board the RPA

NOTE: According to [3], *Section 11.1.3, Chapter 11*, the C2-C3 link must support a range of **functions for monitoring the health status of the data links**, including the pulse, or positive and negative acknowledgements of receipt of the messages exchanged in any direction. These functions can be used to provide information about the condition of the data link to the remote pilot.

2.1. BASIC SUBSYSTEMS OF THE RPA AND RPA's CONTROL STATION

This section briefly describes the different subsystems making up the RPA and the control station of the RPA itself. These systems are illustrated in the following figure obtained from article [4].

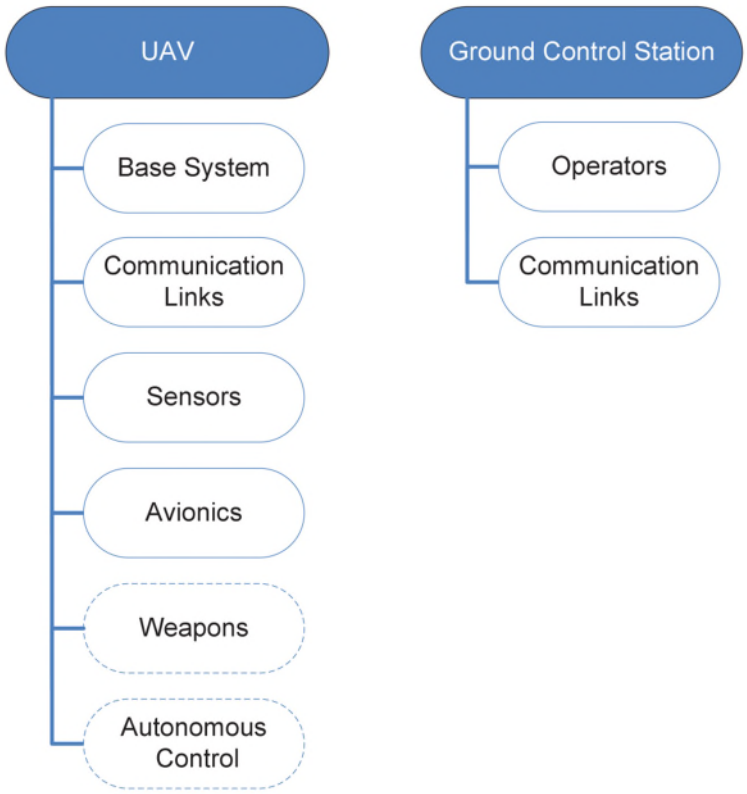

Fig 3. COMPONENT SUBSYSTEMS OF THE RPA AND THE CONTROL STATION. HARTMANN AND STEUB

In the image above, we can see the different systems (actually subsystems) comprising - schematically - the RPA (UAV - Unmanned Aerial Vehicle - in the above figure) and the ground control station.

The *Base System* is the most basic system in the RPA and allows for communication with the other components or subsystems of the RPA, as well as control of the other components: sensors, navigation, avionics, communications system, etc. This base system can be considered the "operating system" of the RPA. This base system also allows the future integration of other subsystems into the RPA, such as special sensors.

The *Communication Links* are basically the communication links between the RPA and the control station. This includes the basic communications system, or C2 link, the C3 link, all other non-payload links (CNPC links) and the payload links. See also Figure 1.

The *Sensors* cover all gauges and sensors on board the RPA, along with their pre-processing functionalities. For example, this may be a GPS signal sensor.

The *Avionics* systems are responsible for converting the signals received from telecontrol into commands to control the flight of the aircraft. That is, commands that operate the engine, the aircraft flaps (if any), the rudder, the stabilisers, etc.

The *Weapons* systems refer to the weapons systems of military RPA. This is not relevant for the civilian-type RPA described in this document. These systems are not found in civilian RPA.

The *Autonomous Control* system allows the RPA to be controlled without the intervention of the remote pilot.

Moreover, in the control station there are *Operator* systems to convert the remote pilot's actions into commands for the RPA, and there is also the *Communication Links* system to communicate with the RPA.

The following figure, also taken from article [4], shows the communications between all these subsystems. This figure does not include the weapons and autonomous control systems.

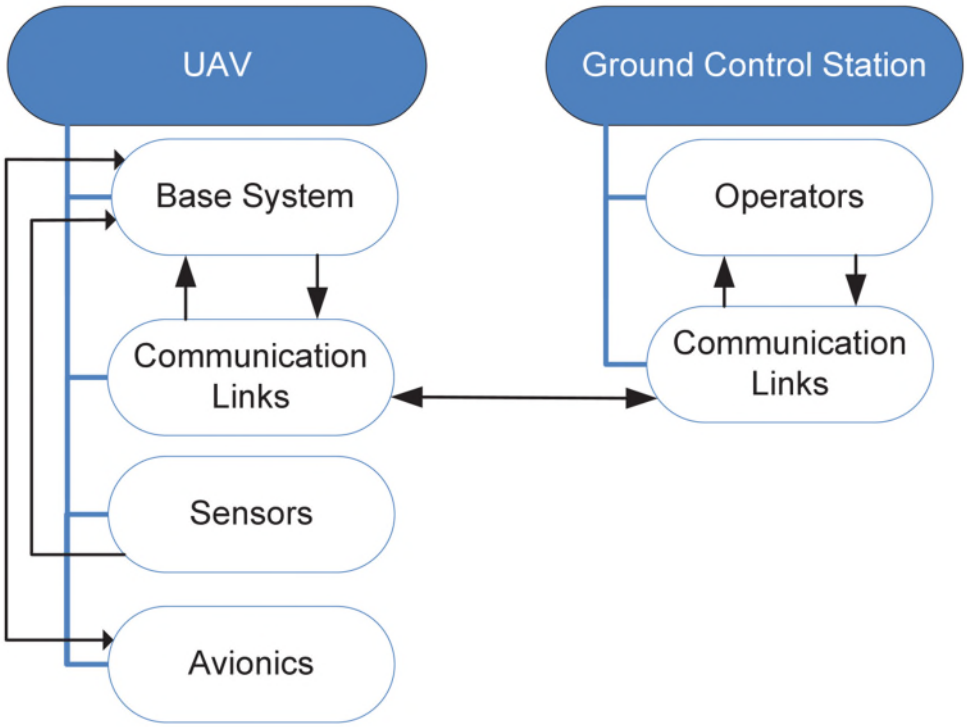

Fig 4. INFORMATION FLOWS WITHIN THE RPAS. HARTMANN AND STEUB

The information flows illustrated in the above image help to understand the types of cyber attack that may be suffered by an RPA. More information in section 3.

3 DESCRIPTIONS OF VULNERABILITIES. POSSIBLE ATTACKS ON AN RPA

This section contains a description of the possible security vulnerabilities that may be suffered by RPAS. Bear in mind that RPA, like any other system combining telecommunications and computer systems, may suffer from attacks by unauthorised users.

An RPA may be attacked in several ways. Without wishing to be exhaustive, some examples of these attacks are:

GPS Spoofing. The spoofing technique consists, in network security terms, of using techniques through which an attacker, generally for malicious or investigative reasons, passes themselves off as a different entity by falsifying the data in a communication. In the case of GPS spoofing, the attacker distracts the attention of a GPS receiver in order to spoof the original signal with the fraudulent signal from a third party, in such a way that the receiver does not realise that the origin of this signal has changed.

GPS Jamming. The jamming or flooding technique consists of disabling, saturating or interfering with the system's resources. For example, an attacker may consume the entire available memory or disk space, or send so much traffic to the network that nobody else can use it. In the case of GPS jamming, the attacker would prevent the GPS sensor on board the RPA from obtaining the location of this RPA by interfering with the satellite's RF signal.

UAV/Controller connection hijacking. The attacker would attack and take over the communication between the RPA and the aerial of the control station, or the communication between the control station and an app installed on a tablet or mobile telephone (if there are RPA control apps on a tablet).

In order to carry out a more exhaustive analysis of the vulnerabilities of RPA against attackers, the information illustrated in the following figure, which has been taken from article [5], will be used.

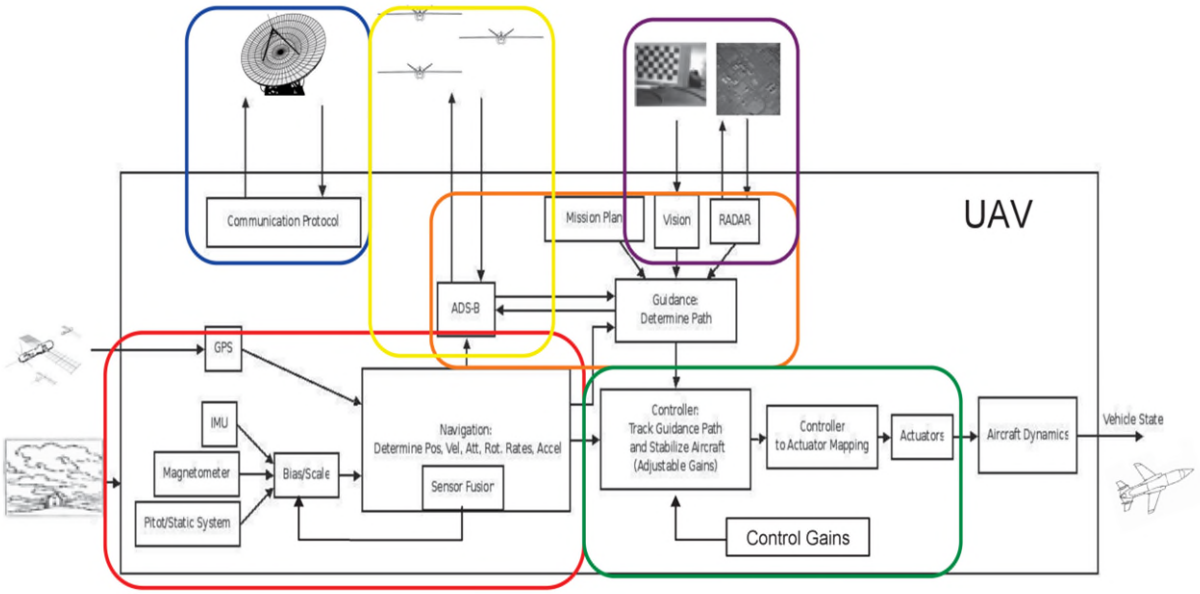

Fig 5. AUTOPILOT COMPONENTS OF AN RPA AND DATA FLOWS BETWEEN THEM. ALAN KIM ET AL.

As can be seen in the above figure, the autopilot of the RPA has various subsystems that are described below.

Guidance systems, which determine the path of the aircraft based on the status of the RPA, the way points, mission objectives, manoeuvres for avoiding collisions, monitoring of targets, etc. This system is marked in orange in the above figure.

Navigation systems. These determine the status of the RPA with information from various sensors (position, speed, height, etc.). This is marked in red in the above figure.

Control systems. These keep the RPA stable and secure in the event of possible problems. They also guide the RPA towards its target, based on the information from the guidance and navigation systems. These are marked in green in the above figure.

Communication systems. These maintain communication between the RPA and the control station. They have already been described in this document. These are marked in blue in the above figure.

ADS-B system. This is a complementary system to the guidance and navigation systems. Marked in yellow in the above figure.

Systems supporting the guidance system. These are First Person View (FPV) devices and radars that complement the guidance system. Marked in purple in the above figure.

Next, a more detailed analysis will be carried out of the possible attacks on an RPA. The autopilot system of an RPA will be taken into account for this more exhaustive analysis, as this subsystem is subject to various attacks. See the following figure, also extracted from article [5].

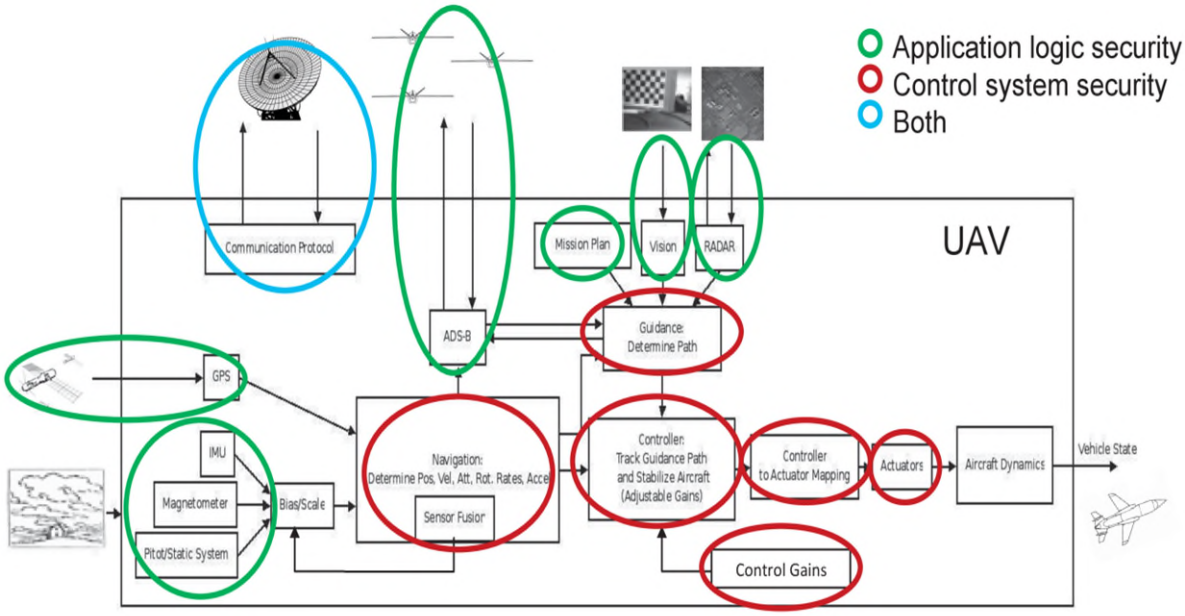

Fig 6. CURRENT VULNERABILITIES IN THE AUTOPILOT SYSTEM OF THE RPA. ALAN KIM ET AL.

The image above illustrates the vulnerabilities of an autopilot of an RPA. This figure includes:

Security in the control system. Attacks on this system will try to make the hardware/CPU of the system perform programmed. Illustrated in red in the above image.

Security in the application logic. Attacks on the logic use manipulations of sensors or the environment to supply false data to the system. Illustrated in green in the above image.

Simultaneous attacks on the control system and application logic. Illustrated in blue in the above image.

It must be taken into account that these attacks may in turn serve as input vectors for other attacks that *a priori* would not be possible from a given vulnerability. In accordance with the information described earlier in this section, a first categorisation of the attacks to which an RPAS may be exposed can be established. Some of the attacks described below are also outlined in [6].

1) Attacks on the hardware of the RPA

This includes all types of actions to exploit vulnerabilities in the elements of the RPA's autopilot. The most common way is accessing the components of the hardware equipment of the RPA. Included among these types of actions are:

- Corruption of data stored on board
- Reprogramming of elements and subsystems of the equipment on board the RPA.
- Tampering with electronic components
- Modification of the firmware of subsystems
- Manipulation of memory cards used in the equipment on board the RPA (for example, SD memory)
- Exploitation of vulnerabilities, taking advantage of existing back doors and those created in the product design phase

2) Attacks on software

This includes all types of actions to exploit vulnerabilities in the design and/or implementation of the software components integrated into the RPAS. Because practically all hardware components of an RPAS are ultimately controlled by some type of firmware or software, the risk level associated with a vulnerability will depend on both the component affected and the degree of integration with the other components.

Depending on the severity of the vulnerability exploited, attacks such as the following could be expected:

- Denial of service of any of the components, forcing them to be restarted or even disabling them (in the event of affecting the flight control system of the RPA, this could cause it to go off course and eventually crash).
- Remote code injection, in order to alter the behaviour of the RPAS or orchestrate it in some way (for example, installing a back door).
- Disclosure of confidential information protected by it (including authentication and encryption codes, information related to the operator and its location, etc.).

3) Attacks on communications

This includes all types of actions that may compromise the security of the communication links (base, additional, payload equipment links, etc.) of the RPAS. When trying to implement measures against these types of attack it is important to analyse the technologies used in the communication links, both transmission (protocol, frequency, modulation, etc.) and security (authentication, encryption, etc.). Possible attacks on communications will depend directly on the basic characteristics of a secure communication, namely:

- Attacks on availability: including, for example, illegal interference or saturation of the communications channel.
- Attacks on confidentiality: includes any attack that aims to bypass the encryption mechanism, either because it is too weak or by illegally obtaining the encryption code.
- Attacks on integrity: ranging from the manipulation of legitimate traffic between the elements of the RPAS to traffic injection and replay attacks.

4) Attacks on sensors

This includes all types of actions to generate false data to be captured by the sensors of the RPA so the aircraft acts on the basis of those false data. These attacks can be classified firstly by the sensor attacked (GPS, systems for vision, radar, sonar, lidar, thermal sensors, etc.), and secondly by the purpose of the attack, namely:

- Denial of service attacks: these aim to disable a sensor so that the RPAS can no longer depend on it.
- Spoofing attacks: these aim to inject data that has been tampered with into a sensor so that the RPAS interprets them as legitimate.

A typical example of attacks on sensors is interference with the GPS sensor on board the RPA, either through GPS jamming or GPS spoofing. Depending on the type of attack, the RPA could switch to inertial or attitude mode. In this way, the RPA could maintain its stability in flight but not its position. If the RPA were flying close to an airport or sensitive area, the risk caused by the attack could be significant.

This type of interference in the GPS sensor may be reduced if the RPA has a positioning system that uses various satellite navigation systems: GPS, GLONASS, GALILEO, etc.

4 GUIDE ON SECURITY MEASURES AGAINST RPA ATTACKS. BASIC SECURITY REQUIREMENTS IN RPAS

This section presents a brief ***list of security measures that will have to be implemented in order to "secure" the C2 communications link, the RPA itself and the control station of the RPA, that is, the entire RPAS.***

This list of measures may constitute the foundation for preparing a ***future guide on cyber security measures for the RPAS.*** This future guide would aim to establish the minimum security requirements with which RPAS must comply in order to achieve the objectives of the RPAS Committee in matters of security. The preparation of this future guide could be entrusted to an independent third party.

In principle, a security risk analysis should be carried out before each operation which would result in a series of security measures to be implemented in each operation. The measures described in Appendix II of this report may be helpful when conducting this risk analysis. In Appendix II, there is a list of standard operational scenarios and the relevant minimum security measures are established for each scenario. These measures in Appendix II come from the list of measures detailed below.

NOTE: The list of security measures outlined below refer solely to the communication link (C2 link). The aforementioned security analysis must also consider establishing these security measures for the payload link, as long as there is direct or indirect communication between the payload subsystem and the C2 communications subsystem.

The list of security measures for an RPAS is outlined below. This list comprises 5 groups of security measures, where each group includes a series of measures.

1. Mitigation measures against jamming

Because the correct operation of the RPAS depends at all times on the maintenance of the C2 link between the RPA and the control station, the RPA must have mechanisms for protection against attacks on the availability of this link, such as, for example:

- Use of spread spectrum modulations (FHSS, DSSS, etc.)
- Use of a backup band that would initially be disabled and would be used in the event of an attack

Although jamming attacks can be mitigated to a certain extent, an attacker determined to interrupt the C2 link can always do so if they have the appropriate means. Therefore, the RPA must be able to suitably respond to the disappearance of the C2 link. On the date of writing this document, in November 2018, the most common strategies that have already been implemented by most commercial RPAS are:

- Keeping the RPA in the same position until the C2 link is re-established.
- Return to home, meaning that the RPA returns to a certain pre-established position if the positioning sensors allow it to.
- If possible, a controlled landing at the same point where the C2 link signal was lost.

2. Continuous activity log (Flight log registration)

Because in many situations it is very difficult to determine in time whether a system has been compromised, the RPAS must implement a continuous activity log system (log files) for subsequent analysis.

This log should be difficult to modify and easy to recover, and should record any suspicious or unusual activity. The log messages must include an updated time stamp that allows us to determine when they were sent.

On the date of writing this report, November 2018, most commercial RPA devices already include this measure.

3. Encryption of the communication channel (C2 link), regardless of the technology and modulation used

NOTE: It has previously been explained that the encryption of the payload link should be considered as long as there is any direct or indirect communication between the payload subsystem and the C2 link subsystem. Regardless of this encryption for security reasons, the payload channel may be encrypted if the RPA operator deems it appropriate (see examples in Appendix II).

In order to maximise the confidentiality of communications, an end-to-end encryption scheme is recommended, that is, messages exchanged between the RPA and the control station must be encrypted before their transmission and decrypted only when received. RPAS must allow the encryption keys to be modified by the operator, also avoiding the presence of default keys shared by all products from the same range. In [7], figure 2, page 26, we can see an example of an RPAS that consists of an end-to-end IPsec Security subsystem to encrypt the telemetry and telecommand information.

The simplicity involved in securing the link depends on the communications technology used. The most important cases to keep in mind are:

- **Direct WiFi link**: in this case, the RPA acts as a WiFi access point to which the control station may connect. The use of open or WEP networks must be avoided at all times, instead using a more advanced security protocol such as WPA2 (which for this particular situation would perform as an end-to-end encrypted channel). Given that various attacks on WPA2 and WPA3 had come to light by January 2018, they have still not been included in any commercial device. They should be complemented by another encryption scheme at the application level to improve their security.
- **Bluetooth link**: multiple attacks against Bluetooth are known to have taken place, so we recommend disabling discovery mode insofar as is possible. We also recommend complementing the use of this protocol with another encryption scheme at the application level.
- **Customised RF links**: mandatory end-to-end encryption scheme. Some IoT wireless communication protocols such as SigFox do not implement any type of encryption at the connection level, so this absence must be compensated for with encryption at application level.

In cases where, due to limitations in the technology used in the communication link, an encryption scheme must be implemented, we recommend:

- **For symmetric encryption**: as of January 2018, AES 128 is still considered secure and provides an appropriate level of confidentiality at an acceptable computational cost.

- **For asymmetric encryption**: we recommend the use of elliptic curve encryption with a key length from 224 bits, or alternatively RSA from 2048 bits. Due to its high computational cost, this tends to be used for exchanging an ephemeral symmetrical key of a strong scheme (such as AES 128 or AES 256) in the context of a PKI (Public Key Infrastructure). In addition to a high level of confidentiality associated with this mode, it also delivers a secure authentication mechanism and integrity of information.

4. Bastioning the embedded system of the RPA

The bastioning of a system includes all measures aimed at reducing its attack surface. It is very common to find embedded Linux systems with a fairly large attack surface, sometimes with open and password-free fundamental ports, or with passwords that are obvious and published on the network.

This bastioning includes, among many others, the following measures:

- Elimination of unnecessary services or software.
- In the event of the presence of TCP or UDP services, filtering of all ports not necessary for communication with the control station.
- Elimination of default administration passwords and back doors introduced during the development process.
- Implementation of an automatic update mechanism.
- Elimination of debug ports (JTAG) and serial ports in the RPA hardware.

5. Verification of the integrity of the information, at connection or message level. Verification of system performance

The messages exchanged between the RPA and control station must be authenticated with digital identities or any other standardised technique. The ultimate objective of these measures is to protect against attacks on the integrity of the communications, such as reply or man-in-the-middle (MITM) attacks.

This requirement would have two possible levels of application:

1. At communication level between the RPA and the ground control station, signing the messages exchanged or using message authentication codes (HMAC).

2. At communication level between the systems on board, verifying at all times that the information received is consistent with the previous history and the information received by other sensors (GPS, sonar, lidar for measuring distance to the ground, Pitot tube, barometer, etc.).

For the particular case of GPS (whose communications lack appropriate authentication or integrity mechanisms), the integrity of the information received may be verified based on heuristics such as:

- Monitoring the signal strength received from the GPS, both absolute and relative values.
- Separately monitoring the signal strength received from each GPS satellite.
- Monitoring the satellite identification codes and the number of GPS satellite signals received.
- Reviewing the time intervals in which the RPA receives the GPS signal.
- Performing time comparisons.
- Performing tests to check the “health” of the GPS system.

Some of these heuristics involve the introduction of an additional logic in the GPS receiver that may increase the final price of the aircraft, therefore a compromise must be sought between practicability and the strength of the heuristics.

In the particular case of GPS and generally, in the event of attacks on the navigation systems on board the RPA, ***redundancy may be established in the navigation systems installed in the RPA***. With this measure, more than one satellite navigation system (GPS, GLONASS, GALILEO, etc.) can be used, so that even if an attacker were able to attack one navigation system, the others would guarantee the correct position of the RPA.

In addition to the above measures at connection or message level, a new measure is established to verify the integrity of the information at system level and not only in an isolated manner in each subsystem.

NOTE: Earlier in this section it was mentioned that a list of security measures proposed in this report could constitute the foundation of a ***future guide on cyber security measures for RPAS***, whose preparation and updating could be entrusted by AESA to any independent organisation. For this future work, the proposals on security described in report [8], section 6.2, Security Framework, could help.

These measures proposed in [8] completely exceed the objective and scope of this report. However, they are mentioned here as they could be taken into account as initial information or as a starting point for preparing the European EASA regulations on security measures relating to RPAS operations.

In the Appendix at the end of this document, there is more information about the security framework proposed in [8].

5 CONCLUSIONS

This section contains the main conclusions emerging from the report.

1. This document is written in accordance with the objective of the RPAS Committee to implement the regulations for the new Royal Decree, RD 1036/2017, of 15 December, on RPAS with special emphasis on ***developing measures against the problem of possible voluntary and illegal interference that may be suffered by the C2 communication link of an RPA and, by extension, any type of voluntary, deliberate or illegal action affecting the entire RPAS*** - including the RPA and the RPA control station- carried out by unauthorised persons with the aim of taking control of the RPA or the entire RPAS.

2. In its initial design, this document was only intended to develop security measures to protect the C2 communication link of RPAS, but one of the consequences of the studies conducted during the drafting of this report is ***that the security of an RPAS, in order to be truly effective, must be considered globally, including not only the C2 link but also the other subsystems of the RPAS that directly or indirectly communicate with the C2 link***.

3. When the RPAS Committee of the AESA was created in 2017, ***the SORA methodology of the JARUS organisation did not include security issues*** that could influence the safety aspects of operations. ***This omission of security from the SORA methodology was one of the reasons why the RPAS Committee of the AESA asked Subgroup SGT 1.3 to prepare this report***. In October 2018, a proposal arose within JARUS to introduce within SORA an assessment methodology for the security risks that could affect or influence the safety of RPAS operations in any way. Although this proposal might be implemented, the implementation work within JARUS may be delayed by months or years. Thus, and on the date on which this report was written, November 2018, JARUS has still not resolved the issue of what security aspects may affect the safety of RPAS operations. ***This report is therefore one of the few sources currently available to the RPAS Committee of the AESA on this issue and it is closest to resolving (albeit in an initial manner) the problem of the security aspects in RPAS***. It cannot be ruled out that this report may serve as a starting point or initial document for JARUS when conducting debates aimed at developing this new methodology for the assessment of security risk that affect the safety of RPAS operations.

4. Section 3 of this report contains a description of vulnerabilities and possible cyber attacks on an RPAS, using the most up-to-date bibliography available.

5. Following the guidelines of the RPAS Committee, section 4 of this report contains a series of security measures to be applied to RPAS. Appendix II of this document shows a list with the main operational scenarios developed by the RPAS Committee and outlines, for each operational scenario, the measures described in section 3 that are considered most appropriate to implement. The information on security measures outlined in section 4, and the application of these measures in the scenarios in Appendix II, are submitted for consideration by the RPAS Committee.

6. The security measures outlined in section 4 may constitute the basis for preparing a ***future guide on cyber security measures for RPAS***. This future guide would aim to establish the minimum security requirements with which RPAS must comply in order to achieve the objectives of the RPAS Committee in matters of security. The preparation of this future guide could be entrusted to an independent organisation (INCIBE, CCN, CNI, etc.). The relevant steps for developing that future guide with the help of an independent organisation is submitted to the consideration of the RPAS Committee of AESA.

7. In the report [8] there is a description of a series of security measures for RPAS that entirely exceed the objective and scope of this report. However, they are mentioned here as they could be taken into account **as initial information or as a starting point for preparing the European EASA regulations on security measures relating to RPAS operations.** Report [8], in its Recommendation 6, proposes establishing a security framework for the authentication of the RPA

and the integrity of the data transmitted by the RPA at a European level. This framework, very briefly, would consist of the following elements.

- PKI for each national aviation security administration to guarantee the authenticity of the RPA and the other RPAS subsystems, the integrity of the information transmitted to/from the RPA and the confidentiality of the information that flows between the RPA and the control station of the RPA. In this infrastructure, each national authority acts as a Certification Authority (or CA) within the scope of its responsibility.

- In turn, there would be a ***European Root Certification Authority*** (CA) hierarchically above the national CAs. See figure 6 in Appendix I.

- This series of European PKI would consist of many elements. Among all these elements it is worth mentioning *electronic identification*.

8. The European security framework proposed in report [8] could also be taken into account for future updates of the ***guide on cyber security measures for RPAS*** mentioned in conclusion 6. Submitted to the RPAS Committee for consideration is whether the AESA takes into account the information appearing in [8] to create and update this guide.

6 BIBLIOGRAPHY

- [1] NUAIR Alliance. 2018. *"JARUS Safety Impacts of Cyber Vulnerabilities Applied to SORA v8_Landscape".*

- [2] EUROCAE. June 2015. *"EUROCAE_ER-012_Command control and ATC communications operational concept (C3 CONOPS) for Remote Piloted Aircraft Systems (RPAS)"*

- [3] OACI. 2015. Doc. 10019. "*Manual sobre sistemas de aeronaves pilotadas a distancia (RPAS)*"

- [4] Kim Hartmann and Christoph Steub. 2013. 5th International Conference on Cyber Conflict. K. Podins, J Stinissen, M. Maybaum (Editors). 2013 NATO CCD COE Publications Tallinn. "*The Vulnerability os UAVs to Cyber Attacks - An Approach to the Risk Assesment*"

- [5] Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang and Hal Aldrige. American Institute of Aeronautics and Astronautics. 2012. "*Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles*"

- [6] Nils Rodday, July 2015. University of Twente, The Netherlands. Doctoral thesis on "*Exploring Security Vulnerabilities of Unmanned Aerial Vehicles*".

- [7] Ivan Vidal, Francisco Valera, Miguel A. Diaz and Marcelo Bagnulo. IEEE Communications Magazine. October 2014, pages 22-29. "*Design and Practical Deployment of a Network-Centric Remotely Piloted Aircraft System*".

- [8] Gianmarco Baldini and Eduardo Cano-Pons. Joint Reserch Centre. European Commission. 2017. JRC105305. "*Study on techniques addressing security and privacy aspects of civil operations of drones in Europe*"

APPENDICES

The following Appendices show additional information about the matters addressed in the sections of this document.

APPENDIX I. SECURITY STRUCTURE ACCORDING TO THE JOINT RESEARCH CENTRE, EUROPEAN COMMISSION, 2017

6.2 Cybersecurity framework

The objective of this section is to investigate the potential solutions and implementation challenges for the safe identification of drones, and support for the integrity of the messages transmitted by the drones.

The transparency of drone operations (as described in section 3) requires the identification of the drone and other information (for example, the flight plan) to be transmitted to all interested parties. The transmission of the ID is requested through various requirements in section 3 and is recommended in the recent EASA "Prototype" Commission Regulation on unmanned aircraft operations [84] in Appendix I.6.c, as shown in figure 5 below.

I.6.c Electronic identification

'Electronic identification' shall mean a function to identify a UA in flight without direct physical access to that aircraft. The system shall transmit the following data as applicable according to standards acceptable to EASA:

(a) the registration of the operator,

(b) the class of the UAS,

(c) the type of UA operation,

(d) the status of its geofencing, and

(e) its position and height.

Fig 5. ELECTRONIC IDENTIFICATION ACCORDING TO [84]

None of these requirements explicitly require the integrity of the data transmitted by the drone. As a consequence, this section is speculative and is written for information purposes in order to inform the reader of the advantages or disadvantages of implementing a trust model based on encryption solutions to support authentication and integrity.

The objective of the proposed trust model is to address the following potential requirements:

1. Integrity of the data transmitted by the drone

2. Authentication of the identity of the drone

The requirements must be addressed for the entire European market. In other words, all drones passing the certification stage and being registered (as described in [84]) must comply with the two above requirements. This involves the definition of a security framework or trust model, where the drones are equipped with encryption material that can be used to support integrity and authentication.

The potential number of drones that may be involved in terms of configuring the security framework to address the requirements could be very large. Thus, the scalability of the security framework is of the utmost importance.

There are parallel activities in other domains that have similar characteristics and requirements in terms of geographic scope (that is, Europe) and scalability (that is, millions of devices).

In the road transport sector, the application of the Digital Tachograph (EC Regulation 165/2014) and the current Cooperative Intelligent Transport System (C-ITS) [85] require a similar trust model for a large number of devices (for example, millions of vehicles) and similar security requirements on a European level.

In both cases, the proposed encryption model is based on a public key infrastructure (PKI).

A public key infrastructure (PKI) is the key management environment for the public-key information of a public-key encryption system.

A PKI is based on the concept of public key encryption (or asymmetric encryption) where pairs of keys are produced and used: a public key, which can be publicly disseminated, and a private key known only to the owner. An essential problem in public key encryption is establishing the trust that a particular public key is genuine, in terms of it being correct and belonging to the right person or entity and not manipulated or replaced by a malicious third party. The usual solution to this problem is to use a public key infrastructure (PKI) where a certification authority certifies ownership of the pairs of keys.

Public key encryption can support (at least) the following three main security services:

1. Authentication: the certainty for an entity that the other entity is who they say they are.

2. Integrity: the certainty for an entity that the transmitted data have not been altered.

3. Confidentiality: the guarantee for an entity that nobody can read a particular fragment of data, except the explicitly planned recipient(s).

In the context of drones, we only address security services 1) and 2) because they are associated with the previously defined requirements.

Integrity and authentication can be implemented using public key encryption and the digital signature concept.

To create a digital signature, a device (a drone and the software running on it) creates a unidirectional hash of the electronic data that must be signed. The user's private key is used to encrypt the hash, returning a value that is unique to the hash data. The encrypted hash, together with other information such as the hash algorithm, forms the digital signature. Any change to the data (even a single bit) results in a different hash value. The receiving side uses the known public key of the signatory to decipher the hash. If the deciphering does not work, the signature was created with a private key that does not match the public key presented by the signatory (indicating an authentication error) or the data have been altered in some way (indicating an integrity failure). As a consequence, when using public key encryption, it is possible to address both previously defined requirements.

Thus, a PKI must be configured to generate and distribute the certificates to ensure that the public keys are correct.

We have identified the following main components in a PKI system:

- A certification authority (CA) that issues and verifies digital certificates. This is the head of trust. The CA may have a hierarchical structure.

- A registration authority (RA) that accepts and verifies the identity of the users who request information from the CA. Once the user's identity has been authenticated, the request is resent to the CA. In many cases, the CA will trust the requests received through the RA without further validation.

■ A central directory or repository of certificates, which is a secure location where keys/certificates are stores and indexed.

■ Certificate distribution system, to distribute certificates.

■ Policies. There are policies defined for managing the PKI system, or generating and distributing certificates. These can be sub-categorised into Certificate Policies, which impose requirements on to the final entities that must be met in order to obtain certificates, and Certification Practice Statements, which are statements from a CA operator about the practices that will be followed in order to guarantee correct results.

A distribution mechanism must also be implemented to distribute the private keys and certificates in the drones, which are used to implement the digital signature. This may be implemented in the production stage and after the compliance assessment process and

the keys/certificates can be associated with a drone in the registration stage (a pre-installed private key is associated with a drone identifier).

The PKI can be implemented as in the digital tachograph with a single root CA at the European level, or can be based on a Certificate Trust List (CTL) with multiple root CAs as proposed in [85].

Since a single European Root CA is easier to implement and deploy, we propose the following architecture for the security framework and the trust model of the drones.

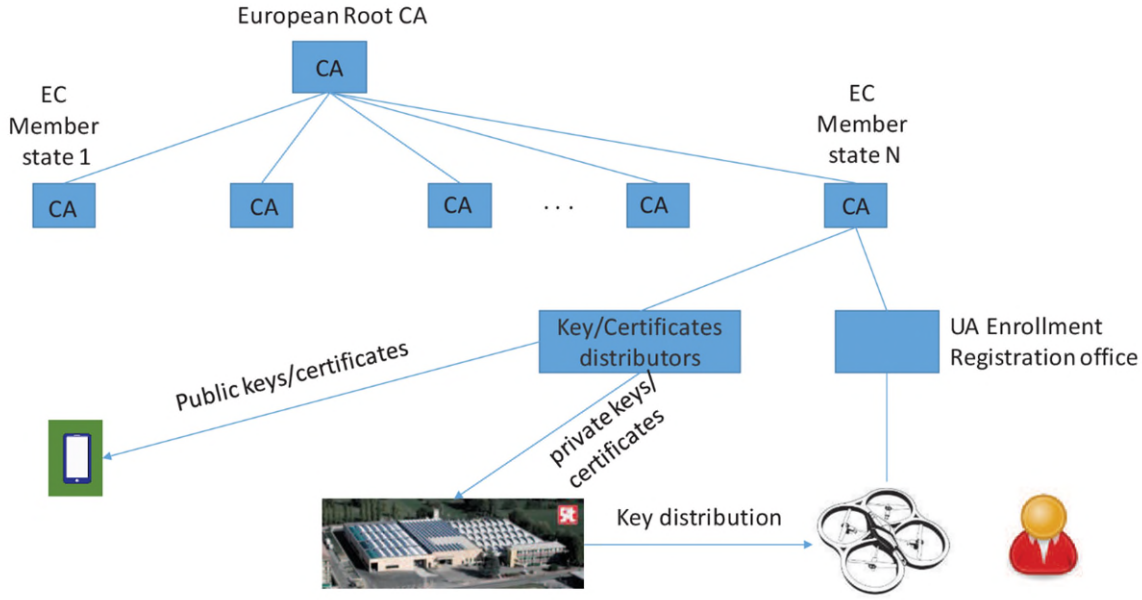

Fig 6. RELIABLE MODEL AND SECURITY FRAMEWORK FOR DRONE OPERATIONS

The key components and processes of the trust model described in Figure 6 are as follows:

■ The Root CA, which is comprised of the single European Root CA and a set of CAs from intermediate member states. The final certificate to be distributed to users is the combination of the root CA certificate and the CA certificate from the intermediate member states. This structure would support complete interoperability on a European level. For example, a drone purchased in Germany can be deployed and send messages in the other European countries.

■ The private key and certificates (secure encryption material) must be stored in the computer platform of the drones in the manufacturing stage or after the compliance assessment process in a secure workshop. A secure channel must be established in order to ensure the secure distribution of secure encryption material to drones. The

drones must also be equipped with tamper protection or secure storage for the encryption material, similar to smart cards or a mobile telephone.

■ The privacy codes can be associated with the identification of the drone in its registration stage. Drone manufacturers may receive a set of private keys and certificates in advance. The association between a specific private key and the identification of the drone can therefore then be carried out in the registration stage.

■ Mobile telephones or other devices used to interrogate or receive drone identification messages should also receive the public keys and certificates associated from a public website, which can be set up either on a European level or by the member states.

■ Appropriate certification and security policies should be written and configured to support the governance and maintenance of the system as a whole.

Bear in mind that this is a very simplistic view of a European trust model and that many aspects are not described, including the revocation of drones from a security viewpoint, the definition and migration of the encryption algorithms used in the trust model, and so on.

The following challenges have been identified for setting up and deploying the security framework:

1. A certificate and security policy must be defined on a European level.

2. A European trust model must be established with all necessary entities. This is not a simple task taking into account the large number of drones sold in Europe. A root CA with intermediate member states. The CA must be set up in accordance with the defined certificate and security policy.

3. The distribution channel for private keys, public keys and certificates must be implemented by a private or public entity.

4. Drone manufacturers must accept the additional costs of implementing the encryption algorithms and storing the encryption material.

6.3 Recommended actions

Based on the previous analysis, we highlight the need to implement security measures for drone operations. The messages sent by the drone for electronic transparency/identification can be easily modified if no security measures are established. If a drone is used for commercial activities where the manipulation of messages may provide economic incentives, the absence of security measures may cause market distortion and have an impact on fair competition. Taking into account that drone operations also have security aspects, the absence of integrity controls in 4-D geodefence and electronic identification may also generate a potential hazard. Section 6.2 of this report describes the security requirements, which must be supported, and a possible security framework. The implementation of this framework is not free from costs and consequences (for example, at a technical and organisational level), but it may be necessary to guarantee the strength of the system against hacking for malicious purposes.

Recommendation 6: A security framework should be established for the authentication of the drone and the integrity of the data transmitted by the drone at a European level.

APPENDIX II. SECURITY MEASURES FOR OPERATIONAL SCENARIOS

This Appendix II is shown in a separate document.