Project 740859

D4.19 – Report on standardisation, regulation, and SOTA progress V7

Deliverable Identifier: D4.19
Delivery Date: November 30th, 2020
Classification: PUBLIC
Editor(s): IDS, CS GROUP
Document version: 1.0 – 2020

Contract Start Date: 1st September 2017
Duration: 40 months
Project coordinator: CS GROUP (France)
Partners: CERTH (GRC), Fraunhofer IDMT (DEU), PIAP (POL), VUB (BEL), CS GROUP (FRA), IDS (ITA), SIRC (POL), MC2 (FRA), HGH (FRA), FADA (ESP), KEMEA (GRC), Acciona ACCI (ESP), MIF (FRA), Home Office CAST (GBR), PJ (PRT), MIPS (ITA), ADM (ESP).

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 740 859

Document Control Page

Title	Report on standardisation, regulation, and SOTA progress V7	
Editors	Name	Partner
		IDS
		CS GROUP
Contributors	Name	Partner
Peer Reviewers	Name	Partner
		CS GROUP / FADA
		CERTH / ACCIONA
Security Assessment	☒ passed ☐ rejected	
Format	Text - Ms Word	
Language	English-UK	
Work-Package	WP4	
Deliverable number	D.4.19	
Due Date of Delivery	30/11/2020	
Actual Date of Delivery	30/11/2020	
Dissemination Level	☐ Public ☒ Confidential (only Consortium members + EC) ☐ EU Restricted	
Rights	ALADDIN Consortium	
Date	30/11/2020	
Revision	None	
Version	1.0	
Edited by	IDS, CS GROUP	
Status	☐ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	19/08/2020	Initiation of Document	IDS
0.2	24/11/2020	Update with inputs from partners	IDS
1.0	30/11/2020	Version for submission	CS GROUP

Executive summary

The project **ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization** is funded by the European Commission (EC) through the European H2020 research and innovation programme with Grant Agreement 740859.

This document, ***Deliverable D4.19 – Report on standardisation, regulation, and SOTA progress V7***, is an extract of the sixth release of six reports issued on a biannual basis throughout the whole duration of the ALADDIN project.

Unmanned Aerial Vehicles (UAV) or Systems (UAS), commonly termed drones, are becoming an ordinary presence in everyday citizens' life, with a continuous market increase in a growing number of useful applications. The drone proliferation is however generating serious security issues. In recent years, newspapers and mass media have reported dozens of incidents involving drones flying over restricted areas and around critical infrastructures, such as airports, nuclear plants, official buildings, or during public events, including the alleged use of drones for terroristic purposes. Drone technology has evolved at a faster rate than imagined, leaving regulation and counter-drone capability far behind.

The recent incidents of small **drones flying too close to UK airports** (Gatwick in December 2018, during Christmas holiday and Heathrow in early January 2019) **and in Spain** at Adolfo Suárez Barajas airport (February 2020) caused a huge flight service disruption. These safety incidents, like the recent **drone near-miss with Trump' plane** in August 2020, demonstrated to the public the severe impact of the drone threat in everyday life and prompted an acceleration in both regulatory activities and Counter UAV business development.

The availability of open international standards is a key enabling factor for the development of markets in all business sectors, including the **Security** sector. Since the beginning of this decade, the European Commission is pointing out the necessity to address the gaps in the standardisation and regulation framework for an innovative and competitive Security Industry.

A number of standardization and regulation bodies are currently working on filling these gaps on UAV and counter-UAV (C-UAV) related topics, such as producing harmonized standards and regulation for the ***safe operation of UAVs*** in different zones of the airspace, according to their category. The most important standardization bodies dealing with UAV-related topics include EUROCAE work group WG-105 at European level, ISO technical committee ISO/TC 20/SC 16 and ICAO RPAS Panel at International level. There is an increasing effort to harmonize European standards with standardization activities outside Europe, such as those of the ASTM technical committee F38 and the RTCA special committee SC-228.

Current EUROCAE hottest topics include Specific Operations Risk Assessment (SORA), UAS Traffic Management (UTM), UAS E-Identification and UAS Geo-Fencing. Most importantly, in 2019 EUROCAE launched WG-115 **Counter UAS (C-UAS)**, with the mandate to develop standards to support the safe and harmonised implementation of Counter-UAS Systems into airport and Air Navigation Service Provider (ANSP) systems. The activities of the various EUROCAE working groups concerned with UAS and C-UAS (WG 105 and WG 115) are progressing, with some relevant standards published in June 2020, such as those on UAS Geo-Fencing and geo-caging, while others are under approval, such as those on UAS E-Identification and UAS safety analysis for the Specific category.

UTM is also the core of current ISO standardization activity within ISO/TC 20/SC 16, along with more general topics, such as UAS operational procedures included in the ISO standard published in 2019. ASTM standards include, among others, those published in 2018 on UAS Registration and Marking, and BVLOS Small UAS Operations, or in 2019 on UAS Remote ID and Tracking, while other standards are still in preparation, including those concerning Operation over People.

Important standardization and regulation activities affecting C-UAV technology are also those pertaining to ***electromagnetic emissions*** – relevant to radar and RF sensing or neutralization, as well as ***Privacy and personal data protection*** **–** mostly relevant to Electro-Optical sensors. Concerning electromagnetic emissions, apparently there is a lack of applicable standards for radar used in drone detection application. Furthermore, given the ambiguous legality of radio frequency (RF) jamming technologies, there does not appear to be European standards applicable to such neutralization equipment. The recent adoption of the General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679, which became enforceable from 25 May 2018, could speed up the development of standards for privacy and personal data protection management in support of Union's security industry.

Concerning the regulation progress, the European Aviation Safety Agency (EASA) is working at an unprecedented pace to improve the ***drone safety regulation*** thus overcoming the current fragmented regulatory framework especially for the smaller UAS. In the EU framework up to 2018, Regulation (EC) No 216/2008 (the 'Basic Regulation') established the main principles and common rules for civil aviation in the EU and defined the area of competence of the EU and of its Member States (MSs). According to it, most of EU Member States adopted national regulations to ensure the *safe operations* of civil drones (UAS) below 150 kg, but there were no harmonized rules at EU level. EASA has been working actively towards a revision of the Basic Regulation to extend the scope of the EU competence to regulate UAS even below 150 kg, also to allow free circulation of UAS throughout the EU. Following the Notice of Proposed Amendments issued in May 2017 (NPA 2017-05 - open and specific category) and the publication on the 06/02/2018 of EASA **Opinion 01/2018,** approval of the new EU regulation was expected by 2018-2019. A notable progress in this direction is the publication on the 22nd August 2018 of **Regulation (EU) 1139/2018**, (the new 'Basic Regulation') which repeals Regulation (EC) No 216/2008 with effect from 11 September 2018. In June 2019, the European Commission adopted the Delegated Regulation **(EU) 2019/945** and Implementing Regulation **(EU) 2019/947** (the 'UAS Regulation'), containing technical and operational requirements for drones. The publication by EASA of **Decision 2019/021/R** containing the relevant Acceptable means of compliance (AMC) and Guidance material (GM) completed the process. The EU regulation will be applicable in one year to give Member States and operators time to prepare and implement it. Following EASA **Opinion No 05/2019** on standard scenarios in the specific category, amendments to the EU drone regulation have been issued in May - July 2020, namely: Commission Implementing Regulation **(EU) 2020/639** and **(EU) 2020/746** and Commission Delegated Regulation **(EU) 2020/1058**. The purpose is to include the above-mentioned standard scenarios, along with postponing dates of application of certain measures in the context of the COVID-19 pandemic. Ongoing regulatory activities are concerned with U-Space, whose first step is the publication on 13th March 2020 of **Opinion on U-space** by EASA.

Member States are preparing for transposing the EU regulation into national implementation in the coming 3 years after its entry into force. Meanwhile, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) facilitates harmonisation of standards within the EU Member States and other participating authorities.

As stated previously, the main progress regarding ***Privacy and personal data protection*** is the entry into force on 25 May 2018 of the **General Data Protection Regulation** (**GDPR**) - Regulation (EU) 2016/679. However, within the scope of ***Preventing and countering the UAV threat***, the use of *detection technology* by law enforcement for the detection of the criminal use of drones may be exempted from the field of application of the GDPR by Recital 19. Instead, such use may fall under the ambit of **Directive (EU) 2016/680** (**Police and Criminal Justice Data Protection Directive**), which covers the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regarding the use of *neutralization technologies*, most regulations are not at the European Union level because matters relating to public security are generally within the competence of member state law. The legal regimes allowing state authorities to make use of otherwise banned technologies (radio frequency jamming, for instance) may vary significantly between countries. The recent escalation of the drone threat, as publicly demonstrated by the serious incidents of drone sighting at Gatwick, Heathrow and Adolfo Suárez Madrid-Barajas airports, will likely trigger tougher regulation and heavier restrictions with impacts on Privacy and personal data protection. For instance, the *Air Traffic Management and Unmanned Aircraft Bill* (2019) will give more power to the Police for countering the drone threat in UK. This Bill is not scheduled to become law until 2021. The legal debate on countering the drone threat is active also outside Europe. In August 2020, the US Government has issued an advisory document providing guidance on the legal framework applicable to counter drone technology in the US. Specifically, this advisory addresses two categories of federal laws: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does not address state and local laws, nor potential civil liability flowing from the use of UAS detection and mitigation technologies.

In addition to the progresses in standardization and regulation, the document provides also the ***State Of The Art (SOTA) analysis*** of C-UAV technology as reported by published reports and online sources. Mini-UAV threat appeared as important in 2014, when many companies started to propose anti-UAV solutions. Single domain solutions focused on one aspect of the problem, either detection or neutralization of the threat. Detection mainly involves radar and/or electro-optical/infrared sensors whereas countering the threat mainly involves radio-frequency piloting and jamming of the UAV communication links. On the other hand, complete C-UAV systems are based on integration of (at least one) sensor, tracker/identifier and a neutralization effector (usually jammer). A number of systems and subsystems (sensing and neutralization equipment, data processing and data fusion techniques, cartographic and other supporting software) are currently available on the market. However, the threat is evolving very quickly and is mainly unpredictable: hence, single domain solutions are inadequate and should be integrated in flexible systems, able to accept different sensors and effectors. The overall trend is therefore toward multi-sensor integration and enhanced automation, although many points, such as drone versus bird discrimination, remain challenging tasks.

Additionally, new trends are gaining interest. The main one is related to swarms of drones either as a most frightening threat requiring superior detection and neutralization capabilities or even as potential countermeasure if employing sophisticated algorithms (currently a topic of academic research) to form a self-organized network of defence drones to intercept the intruder drone. Recent developments with potential impact on C-UAS systems include the requirement for integration with U-Space services/UTM systems and technological progresses of Artificial Intelligence/Machine Learning.

The latest surveys of C-UAS equipment appeared in the market confirm the trend to provide a multi-layer solution, with some equipment incorporating artificial intelligence (AI) algorithms or capabilities to detect and/or neutralize swarms of hostile drones. Additionally, growing partnerships are being signed for developing rogue drone detection capabilities for integration within civil UTM networks.

The constant stream of announcements in the specialised press of C-UAS system enhancements and new partnerships between C-UAS manufacturers or sellers demonstrate a high dynamism, especially by the global big players, both in improving the system performances and in seizing new market segments.

Table of Contents

List of Figures

List of Tables

1 Introduction

The project **ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization** is funded by the European Commission (EC) through the European H2020 research and innovation programme with Grant Agreement 740859. It will be implemented in compliance with the Description of Action (DOA): Annex 1 - Part A (description of the work plan) and Annex 2 – Part B (narrative description of the action) [AD1].

This document, ***Deliverable D4.19 – Report on standardisation, regulation, and SOTA progress V7***, is an extract of the sixth release of six reports issued on a biannual basis throughout the whole duration of the ALADDIN project.

1.1 Purpose of the Document

This document aims at providing an overview of the State-Of-The-Art (SOTA) progress in countering malicious drones from a standardisation, regulation and technological perspective, performed by the ALADDIN project within *Task 4.2 Standardization, regulation, and technological monitoring*.

Version V7 of the Deliverable (D4.19) accounts for the analysis performed since the beginning up to the sixth semester of the ALADDIN project, and reports relevant information accessed from public sources up to August 2020.

1.2 Scope and Intended audience

This document is an extract of the sixth release of six reports on standardisation, regulation, and SOTA progress issued on a biannual basis throughout the whole duration of the ALADDIN project.

The intended audience of the document are the project stakeholders (European Commission DG HOME, Research Executive Agency (REA), ALADDIN Consortium executive members) and the project team (Consortium staff).

This public version is aimed to be disseminated to a larger audience.

According to the preliminary security scrutiny in the DOA Part B [AD1], this deliverable was classified as **PU = Public**.

1.3 Structure of the Document

The structure of this document (besides the current Section) is as follows:

- **Section 2** presents a general overview of the drone threat and the ALADDIN response within the EU counter-drone policy;
- **Section 3** contains a summary of the standardisation status at beginning of the project and its progress up to present.
- **Section 4** contains a summary of the regulation status at beginning of the project and its progress up to present.
- **Section 5** contains a summary of the technological SOTA at beginning of the project and its progress up to present.
- The **last two Sections** contain the main Conclusions and References to relevant bibliographic material.

2 The ALADDIN Project in the EU counter-drone policy

2.1 The UAV growth: opportunities and threats

Unmanned Aerial Vehicles (UAV) or Systems (UAS), commonly termed drones, are becoming an ordinary presence in everyday citizens' life, with a continuous market increase in a growing number of useful applications. The civil UAV market comprises three main groups:

- **Civil government UAVs** for uses ranging from border security to law enforcement to research on wildlife.
- **Commercial UAVs** for uses including construction, agriculture, insurance, internet communications, and general photography.
- **Consumer/hobbyist UAVs**, which are mass-produced, particularly in China, for low-end UAV applications. These are low cost and may or may not use a camera. They are not engaged in commercial activity.

Recent reports ([BD1], [BD2], [BD3], [BD4]) confirm the soaring of UAV production worldwide, making it one of the three growth industries revolutionizing the world (**Figure 2.1.1** and **Figure 2.1.2**), with the highest number of units worldwide of the rotorcraft type, followed by the fixed-wing type, and the nano-type.

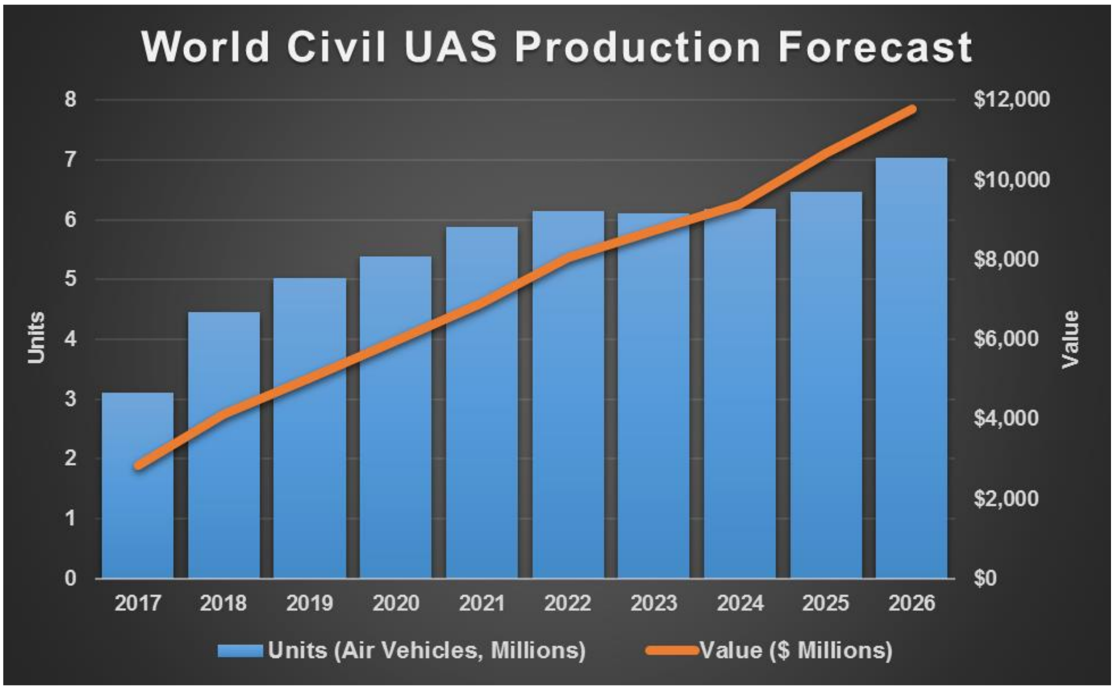


Figure 2.1.1: World civil UAS production forecast ([BD1])

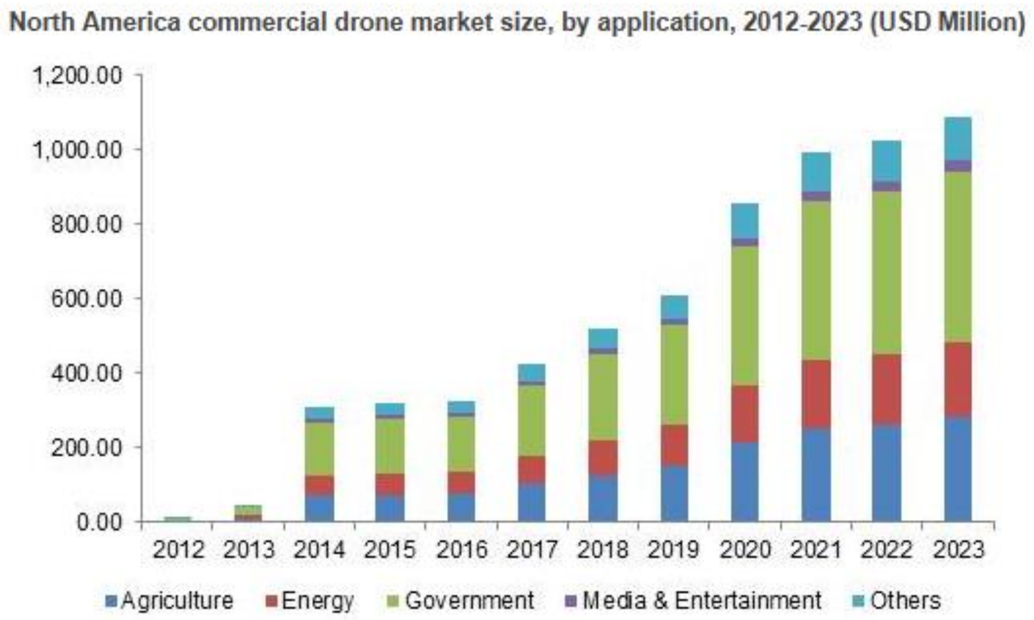


Figure 2.1.2: North America commercial drone market size forecast ([BD4])

According to the 2016 ***SESAR European Drones Outlook Study*** ([BD5]), drone market and capabilities are expanding rapidly also in Europe (**Figure 2.1.3**, **Figure 2.1.4**). *"The growing drone marketplace shows significant potential, with European demand suggestive of a valuation in excess of EUR 10 billion annually, in nominal terms, by 2035 and over EUR 15 billion annually by 2050. […] The development of the civil drone industry is dependent on the ability of drones to operate in various areas of the airspace, especially at very low levels that today are generally defined as being below 150 metres. […] Commercial and professional users are expected to demand drones in both rural and urban settings and will be reliant on beyond visual line of sight capabilities to be permitted. […] Unlocking the full potential of the market and maintaining the high standards of safety of EU aviation will require increased levels of European support. […] An estimated total of at least EUR 200 million in additional R&D over the next 5-10 years, based on expectations of the market, is required to address remaining gaps related to Very Low Level (VLL) activities that represent the majority of future drone operations. This boost in R&D capabilities would complement on-going efforts for the integration of drones into controlled airspace.*

According to the replies received on a UAS operators questionnaire issued by the European Aviation Safety Agency (EASA) in 2016 ([ND24]), in the segment of small-UAS of less than 25 kg, more than 90% of them have a maximum take-off mass (MTOM) between 0 and 4 kg. Of course, the above estimates do not take into account model and privately built aircraft, mainly used by hobbyists. Apart from being fast evolving, the UAS market is characterized by the presence of many actors relatively new to the aviation sector, especially for the small-size segment. Indeed, concerning UAS manufacturers, an important market share is accounted for by companies that are not familiar with aviation regulation. Drones in the small-size segment, especially those privately built, are likely the most susceptible for illegal activities.

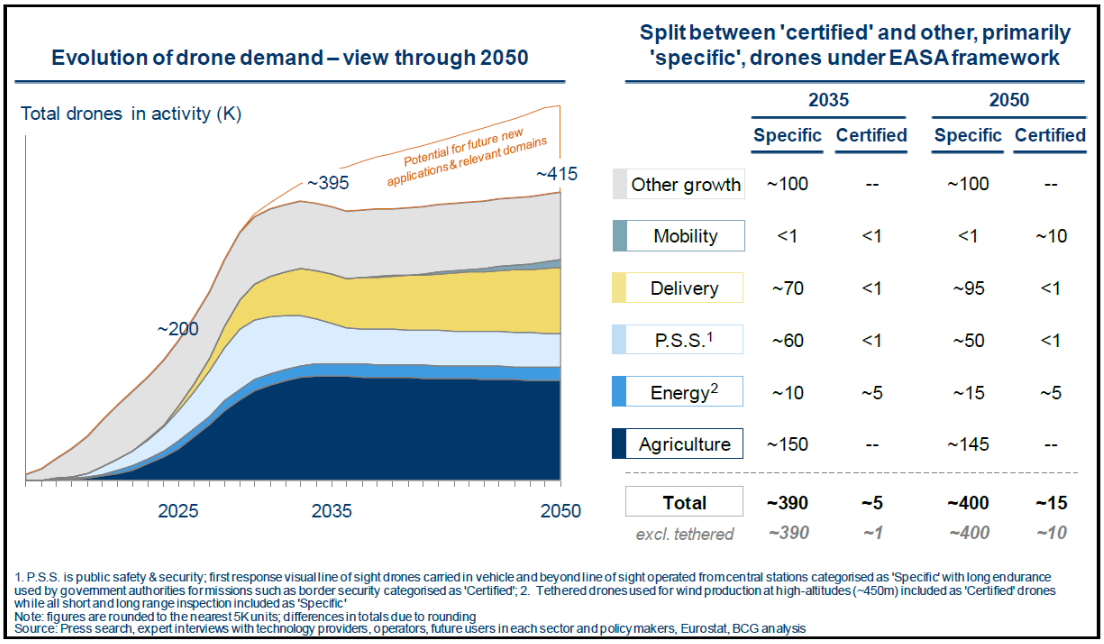


Figure 2.1.3: Europe drone demand forecast by industry domain ([BD5])

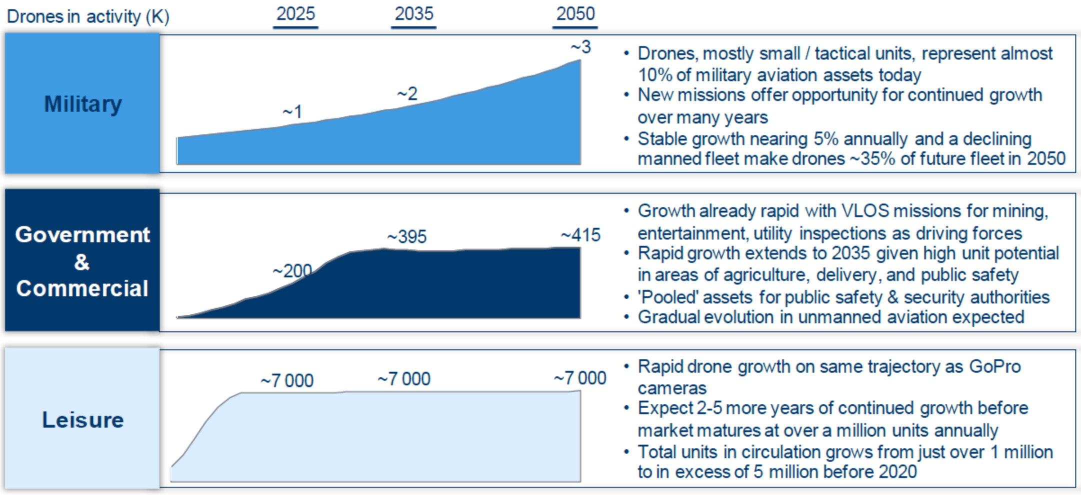


Figure 2.1.4: Europe estimate of total UAS fleet size ([BD5])

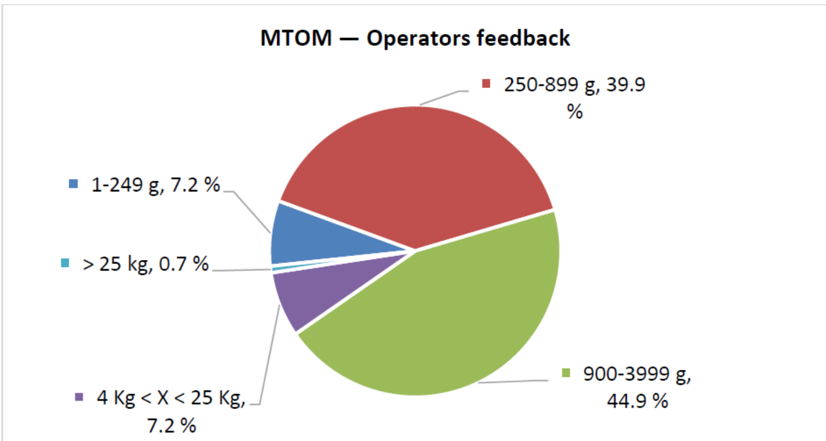


Figure 2.1.5: Distribution of drone mass according to EASA UAS operators questionnaire 2016 ([ND24])

The drone proliferation is however generating serious security issues. In recent years, newspapers and mass media have reported dozens of incidents involving drones flying over restricted areas and around critical infrastructures, such as airports, nuclear plants, official buildings, or during public events (§ 2.3). Drone technology has evolved at a faster rate than imagined, leaving regulation and counter-drone capability far behind. Hence, it is critical that governments work with regulators and industry to develop an effective Counter UAV (C-UAV) framework. Prisons, airports, sporting venues, public buildings and other sensitive sites are at serious risk, and correctly understanding the multitude of challenges that drones present is central for the effective protection of critical infrastructures and citizens.

While concern is growing about the kind of threats posed in a world filled with small, but increasingly versatile UAVs (§ 2.3), hundreds of millions of dollars are being devoted worldwide to develop Counter UAV (C-UAV) technologies, either for Military/Defence or Critical Infrastructure Protection (CIP) applications ([BD6], [BD7]). The worldwide market for counter-drone technology is expected to grow from $342.6million in 2016 to $1.5billion by 2023, according to a July 2017 research report from MarketsandMarkets ([BD8], [BD9]), with non-kinetic electronic systems estimated to grow at the highest rate during the forecast period.

The drone threat is relatively new and it is a necessity to provide a thorough solution on the detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas, even if this happens before the completion of the relevant regulatory framework. In this specific case, the fact that the criminal organisation groups and the terrorists have the absolute advantage of surprise maximises the impact of illicit activities with vast consequences to the society and the economy worldwide.

Unfortunately, facing such threats is not straightforward for various reasons. Firstly, the regulatory framework about the usage of UAVs and the legal responses to such threats is not clear and homogenous. Secondly, the operational capacity of law enforcement agencies is limited in human, equipment, and financial resources.

Despite the growing and rapidly evolving C-UAV market, before the start of the ALADDIN project there were no off-the-shelf C-UAV solutions effective enough in all operational contexts that can reliably detect, localize, identify and mitigate the threat of suspicious and potentially multiple UAVs, while taking into account the regulatory framework and the decision chain.

To address the drone threat the European Commission (EC) opened a specific call within the Horizon 2020 (H2020) research and innovation programme: *‘**SEC-12-FCT-2016-2017 - Sub-topic 2**: Detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas and involving as beneficiaries, where appropriate, the operators of infrastructure’*.

In response to this call, the project **ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization** has been awarded to a Consortium of 18 European partners with Grant Agreement 740859 (https://aladdin2020.eu/). The ALADDIN project will be implemented in compliance with the Description of Action (DOA): Annex 1 - Part A (description of the work plan) and Annex 2 – Part B (narrative description of the action) [AD1].

Through a holistic approach and thanks to a Consortium of world-leading technical partners (industrial companies, small-medium enterprises, research centres and academic institutes) and end-user representatives of Law Enforcement Agencies

(LEAs) and constructors/operators of critical infrastructures, ALADDIN's ambition is to provide an unprecedented and evolving solution to the emerging **drone threat**, completely in line with the scopes of the call:

1. *New knowledge and targeted technologies for fighting both old and new forms of crime and terrorist behaviours supported by advanced technologies*
2. *Test and demonstration of newly developed technology by LEAs involved in proposals*
3. *Innovative curricula, training and (joint) exercises to be used to facilitate the EU-wide take-up of these new technologies*

2.2 ALADDIN project overview and main objectives

The main objective of the ALADDIN project is to **study and develop a state-of-the-art, global, and extensible system to detect, localise, classify, and neutralise suspicious, and potentially multiple, light UAVs over restricted areas**. This system will be tailored to operational constraints such as easiness of use and deployment, quality of detection, or safety, in order to deliver unprecedented tools for operational support, including investigations, and training.

ALADDIN will also assess relevant technologies, threat trends, regulations, and other important issues such as societal, ethical, and legal (SoEL) frameworks in order to develop new knowledge made available to LEAs and infrastructure designers, constructors, and operators through innovative curricula.

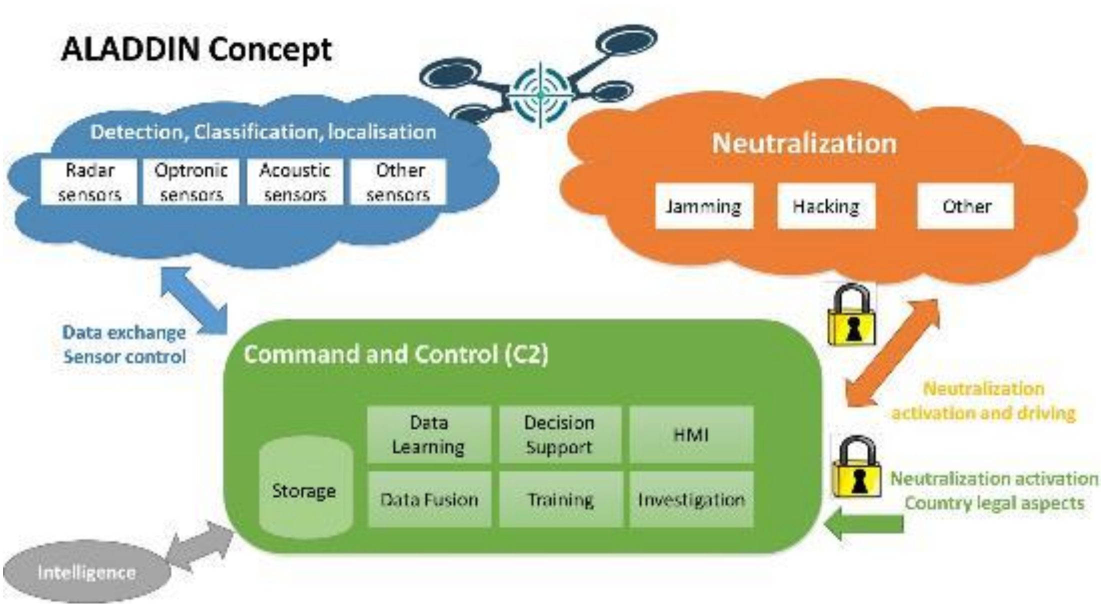


Figure 2.2.1: The ALADDIN platform concept

The **overall concept** of the ALADDIN project is the development of a seamless, tightly integrated system for countering malicious drones. The ALADDIN platform (**Figure 2.2.1**) will tightly integrate multiple modules materializing the three core sub-systems:

- the **detection, classification, and localisation** sub-system
- the **advanced command and control (C2)** sub-system
- the **neutralization** sub-system

ALADDIN is an ambitious research and innovation project racing against organised criminal groups and terrorism and facing important challenges at the technological and integration level as well as barriers in the non-technological domains, including **political and economic barriers** in adopting new technologies and **legislative or cultural differences at national level** in terms of privacy and other legal constraints. The SWOT Analysis presented in **Table 2.2.1** summarizes the position of the ALADDIN project.

Table 2.2.1 SWOT Analysis for the ALADDIN project

SWOT Analysis for the ALADDIN project	
STRENGTHS	**WEAKNESSES**
Consortium composition and size Collaboration and cooperation capacity of partners Accumulated Expertise in ICT Security domain Use of diverse and state-of-the-art sensors and software Hands-on involvement of end-users Very strong return on experience on real and practical use case with leads to a clear understanding of the UAV solution to be developed Adaptability and flexibility	Lack of knowledge on the new forms of criminal and terrorism activities involving UAVs (to be improved via the workshops, the Advisory Board, the discussion between LEAs…) Study of a broad set of crimes rather than on specific types (i.e. smuggling, drug dealing etc.)
OPPORTUNITIES	**THREATS**
Active role in participating in the definition of the Regulatory framework Improve investigation capabilities Reduce time to crime resolution Prevent terrorism endeavours Update current LEA practices and capabilities Boost EU Security Industry Decipher the use of UAVs in criminal and terrorism activities	Lack of Regulatory framework for the operation of UAVs/drones Fluid policy and legislation environment Adoption readiness by users Change in current LEA practices Vendor and market response Potential erosion of goodwill and commitment of users Poor reception by civil society Uncertainty around EU Data Protection Directives

ALADDIN follows an **iterative and incremental** development in order to implement a **user-centred design process** all along the project duration. Continuous implication of end users and iterative evaluation of the project results aims at ensuring that the work is addressing real operational needs and constraints. This methodology will enable the regular revision of the user needs, technical design, scientific approaches, and prototypes as well as the early implementation of corrective actions.

The work plan consists of **nine work packages** with an overall project duration of 40 months enabling **two main iterations**, leading to two incremental releases of the ALADDIN system (**Figure 2.2.2**). Each one of the two main phases (**beta** and **final**) is a **complete development cycle** composed of requirement collection, platform design, development, integration, and end-user testing and evaluation.

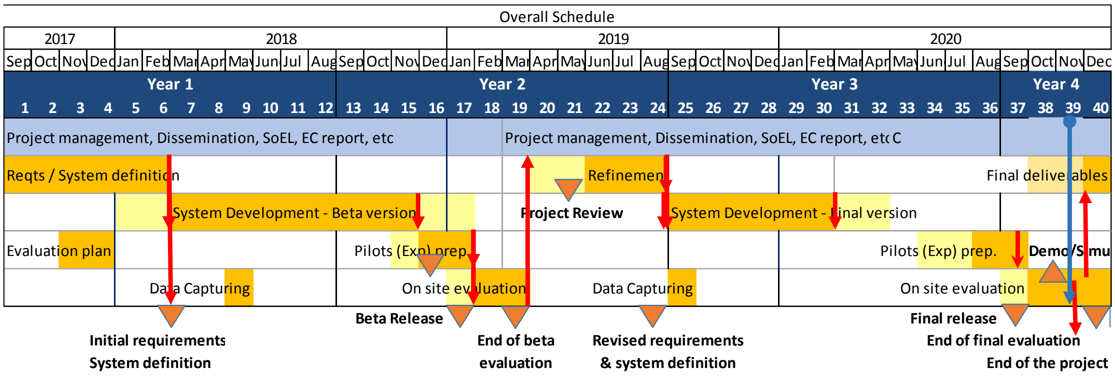


Figure 2.2.2: Schedule of the ALADDIN Project

2.2.1 Standardisation, regulation, and technological evolution: monitoring and impact

One of the main purposes of the ALADDIN project is the assessment of relevant technologies, threat trends, regulations, and other societal, ethical, and legal (SoEL) issues to improve the LEAs' capability in facing the emerging drone threat. According to the **ALADDIN user-centred** approach, as stated in the DOA [AD1], one of the main **Expected Impacts** of the ALADDIN project is: "*LEA officers provided with better tools to help them on their (specialized) daily work".* To this aim, *the ALADDIN project will closely monitor the evolution of threats, technologies and regulations throughout the project, keeping LEA activities and tools up-to-date.*

According to the DOA Annex 1 - Part A, work package **WP4** - **Mission, Operational & System Requirements** *will gather and refine end-user's requirements and constraints, while monitoring relevant standardisation initiatives and technological evolution, in order to define and refine pilot scenarios as well as functional specifications and system architecture.*

In particular, task **T4.2 – Standardization, regulation, and technological monitoring** will produce internal reports to *inform the project about external technology and product evolutions as well as relevant working group activities, standardisation and regulation initiatives, which will be fed into the design process* of the ALADDIN system. *During the whole project, great attention will be paid to international standards and emerging technologies/research results/projects/products in order to determine, in agreement with end-users, which of them are the most relevant to use or to comply/interoperate with […].*

Task T4.2 is complementary to task **T2.3 – Contribution to standardisation and regulations**. *This task aims at organising and carrying out the activities related to the dissemination of the project results towards the standardisation initiatives […]* and *the appropriate actions to disseminate WP3 results towards the regulation initiatives relevant to UAVs in order to propose changes in laws and regulations aiming to better control UAV threats and simplify LEAs operations, including investigation.* This activity may include Dissemination of WP3 results that may derive from those included in D3.1 "Data protection, Social, Ethical and Legal frameworks" [AD2] and in other WP3 public deliverables.

The monitoring activity of T4.2 aims primarily to help the Consortium in designing the system architecture and functional specifications of the ALADDIN platform in order to develop the most advanced, yet user-friendly, counter-drone system fit for the purpose of **Civilian Security** and compliant with current European regulation and standards, allowing its interoperability with third-party components.

Secondarily, the monitoring activity of T4.2 will have a positive impact on the entire European community by providing an up-to-date overview of the standardization, regulation, and technological state of the art (SOTA) related to drone and counter-drone emerging topics. In addition, the active participation of ALADDIN partners to standardisation and regulation initiatives within T2.3 will contribute to addressing the most urgent problems and barriers in order to ensure the European technical leadership and competitiveness in the security domain.

A summary of the internal reports about standardization, regulation, and technological monitoring will be included in the biannual Deliverable "*Report on standardisation, regulation, and SOTA progress"*. Although not exhaustive, the various issues of this Deliverable aim to provide an overview of the evolution of the major (counter-) drone topics on the standardization, regulation, and technological perspectives. More in-depth information may be found in the relevant literature and referenced material.

2.3 Threat analysis

UAVs can represent both **passive** threats, unintentionally disrupting ordinary citizen lives, and **active** threats of criminal activities or terrorism, with high destabilization potential. Passive threats include possible airborne collisions of drones flying too close to aircrafts. A study of the US Federal Aviation Administration (FAA) into drone safety has suggested that collisions with aircraft are more damaging than bird strikes[1]. The FAA study ASSURE recreated a collision between a drone and an airplane using a computer simulation and the models of two types of drone (the DJI Phantom 3 Standard quadcopter and a fixed-wing Precision Hawk Lancaster Hawkeye III). The Final Report of the study[2] pointed out that windscreens on aircraft were particularly vulnerable to damages. A similar study in the UK, conducted by military research firm Qinetiq on behalf of the UK government, suggested that drone strikes could cause critical damage to planes. Other drone threats include the collection of sensitive data by un-malicious users and the possible misuse of such data[3], causing high legal and ethical concerns. The huge impact on everyday life of this kind of UAV threat (passive) became apparent in December 2018 - January 2019, when two major incidents of drones sighting caused huge flight disruptions at the two biggest UK airports.

Active threat include the possibility of using (mini and small) UAV for criminal activities, such as smuggling of drugs/cigarettes or other illegal goods into prisons or across borders, and for terroristic purposes, by carrying spy cameras or powerful explosives.

---

[1] http://www.bbc.com/news/technology-42238115, 5 December 2017

[2] ASSURE UAS Airborne Collision Severity Evaluation Final Report http://assureuas.org/projects/deliverables/sUASAirborneCollisionReport.php

[3] https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html; https://gcn.com/Articles/2017/11/29/DJI-drone-snoops.aspx; http://securityaffairs.co/wordpress/66351/intelligence/dji-drones-cyberespionage.html

The statement that *"Terrorist Drone Attacks are not a matter of IF but WHEN"*[4] indicates the severity of the asymmetric threat on the prosperity, the political stability and the well-being within the European Union (EU).

On the military side, there is a lot of concern about the potential for small, weaponized drone swarms, demanding for a multilayer detection capability with either electronic or kinetic mitigation, depending on the area of operations and rules of engagement. The potential threat from small UAVs in the hands of terrorists has attracted the attention of regulatory agencies not only in Europe but also in America, such as US FAA, which launched its Pathfinder Program in May 2015 as a partnership with industry to explore the next steps in unmanned aircraft operations.[5]

An interesting commentary in the Unmanned Airspace website[6] looks at the different types of actors behind the rogue drone threat, pointing out that "the difference between a drone being a toy or a weapon is the decision made by the operator," as a speaker said at a recent counter-UAS event in London. According to the expert (Tony Reeves of Level 7 Expertise): *What has become strikingly apparent is there is a close similarity between the nefarious drone operators above to similar groups operating in the cybersecurity world. Perhaps the way that nefarious actors behave is a human trait rather than being defined by the tool.* In his analysis, he divides the ***nefarious drone operators*** in the following categories:

- **Uninformed hobbyist**: This person doesn't know they're doing anything wrong; they don't know enough to check what is and what is not allowed, and where they are allowed to fly.
- **Disruptors**: This is a wide-ranging group, divided into a number of sub-categories but all characterised by knowing that they shouldn't be flying where, when or how they are.
    - Disruptive (1) – Shortcut / risk taker.
    - Disruptive (2) – Deliberately outside the rules, for reputation.
    - Disruptive (3) – Deliberately unsafe.
    - Disruptive (4) – Deliberately disruptive.
- **Protestors.** Protestors tend to carry or broadcast a strong message, and are not averse to being apprehended and/or arrested on live video.
- **Criminals.** The criminal use of drones is largely confined to activities connected to financial gain. The primary issue faced is the use of drones to smuggle contraband (usually mobile phones, drugs or money) into prisons. [ ] There is a new sub-group which has appeared recently, utilising drones to film live sporting events and place "in-play" bets.
- **Terrorists.** A committed terrorist is incredibly hard to stop, and there is a near-continuous 'leakage' of terrorist / insurgent drone tactics from the Middle East conflict areas – in particular Iraq / Syria and Yemen / Saudi Arabia. [ ] The

[4] Terrorist drone attacks are not a matter of 'if' but 'when', 2016. http://europe.newsweek.com

[5] J.R. Wilson 2016. *The dawn of counter-drone technologies.* Military & Aerospace Electronics, November 1, 2016. http://www.militaryaerospace.com/articles/print/volume-27/issue-11/special-report/the-dawn-of-counter-drone-technologies.html

[6] "The drone threat: a guide to the bad and the very bad actors", May 31, 2019 https://www.unmannedairspace.info/commentary/the-drone-threat-a-guide-to-the-bad-and-the-very-bad-actors/

terrorist's intent is to achieve their objective at all costs. [ ] Hard to detect, deliberately covert until the moment of attack, operating in small cells and highly motivated; the terrorist presents the hardest challenge for security organisations.

- **Other hostile actors i.e. Nation States or sponsored / supported actors**. Houthi-backed rebels have launched drone attacks on Saudi airports, using commercially available drones with a payload of explosives. Press reports says Saudi authorities have shot down the drones.

2.3.1 Escalation of the drone threat

During the lifetime of the ALADDIN project, the world has witnessed an escalation of the drone threat, either passive or active.

2.3.1.1 Drone incidents: aircraft near misses and airport security

UAV-related incidents have often been reported as causing hazards to aircraft, or to people or property on the ground. Safety concerns have been raised due to the potential for an ingested drone to rapidly disable an aircraft engine, and several near-misses and verified collisions have involved hobbyist drone operators flying in violation of aviation safety regulations[7].

The recent **incidents of drone sighting at UK airports** demonstrated to the public the severe impact of the drone threat in everyday life and prompted an acceleration in both regulatory activities (§ 4.2.1) and Counter-UAV business development.

Recent news in UK and worldwide mass media report two big incidents of drone sighting at the major UK airports:

- **Gatwick**, which in the run-up to Christmas was repeatedly forced to close between 19 and 21 December 2018 due to reported drone sightings[8], with about 800 flights cancelled, affecting 120000 people[9].
- **Heathrow**, which was forced to ground departures with an emergency one-hour halt because of a drone sighting on 8 January 2019[10].

These incidents have received high emphasis in the websites of UK-based C-drone conferences: **Countering Drones 2019** (10-11 July 2019, London, UK) and **Counter UAS 2019** (16 - 18 April 2019, London, UK), designed exclusively for the military.

The **Countering Drones** website[11] highlights that *the **drone incident at Gatwick Airport** has brought the threat of malicious drone use into the mainstream, and the serious economic and personal impact that this has had on businesses and private*

[7] https://en.wikipedia.org/wiki/List_of_UAV-related_incidents

[8] https://www.theguardian.com/uk-news/video/2018/dec/20/thousands-stranded-at-gatwick-airport-due-to-drones-video 21/12/2018

[9] https://www.theguardian.com/uk-news/2018/dec/20/tens-of-thousands-of-passengers-stranded-by-gatwick-airport-drones 21/12/2018

[10] https://www.theguardian.com/uk-news/2019/jan/08/heathrow-airport-departures-suspended-after-drone-sighting 08/01/2019

[11] https://counteringdrones.iqpc.co.uk/

individuals cannot continue to be ignored. Following the incident at Gatwick, we now expect investment and real commitment to tackle the issues (including improvements to the regulatory environment)*, in order to assure businesses and the public of an effective response to future incidents*. These incidents confirm the concerns expressed earlier when Defence IQ published global airport drone threat map[12]. *The threat posed by drones to airports is real. Even though regulations have been recently updated in some countries and countermeasures currently trialled, the safety risk they pose along with the potential financial loss they could cause is still present.*

The **Counter UAS 2019** website[13] emphasize the supporting role of military C-UAS capabilities in the capacity of Military Assistance to a Civilian Authority (MACA). *The recent **incident at London Gatwick Airport** has also highlighted the role the military has to play in supporting civilian organisations during crises until more effective Counter-UAS capabilities are procured by civilian operators of Critical National Infrastructure.*

Related newspaper articles announce new anti-drone powers handed to Police in response to Gatwick incidents[14], and millions investment in further anti-drone systems by Heathrow and Gatwick airports[15].

In response the government has announced a package of measures which include plans to give police the power to land, seize and search drones. The Home Office will also begin to test and evaluate the use of counter-drone technology at airports and prisons.

According to the press[16], during the Heathrow drone sighting the armed forces were called in to protect the UK's busiest airport using "specialist equipment", probably the Israeli-developed Drone Dome C-UAS system, which the United Kingdom had procured in August 2018[17]. *The selection of the Drone Dome comes eight months after it was demonstrated to the UK government in January. According to its manufacturer Rafael, the United Kingdom is to receive the radar detection, electro-optical (EO) identification and communication jamming elements of the system, but not the hard-kill laser. The radar usually has a detection range of about 50 km for a target the size of a transport aircraft, but for the class of target that it is looking for in its Drone Dome application the radar would typically provide a detection range of between 3.5 km and 10 km.*

---

[12] Drones and airports: Global threat map https://counteringdrones.iqpc.co.uk/downloads/drones-and-airports-global-threat-map?-ty-m; Defence IQ publishes global airport drone threat map, https://www.unmannedairspace.info/counter-uas-systems-and-policies/defence-iq-publishes-global-airport-drone-threat-map/, 3/10/2018

[13] https://counteruas.iqpc.co.uk/

[14] https://www.theguardian.com/technology/2019/jan/08/police-handed-new-anti-drone-powers-after-gatwick-disruption 08/01/2019

[15] https://www.theguardian.com/world/2019/jan/03/heathrow-and-gatwick-millions-anti-drone-technology 03/01/2018

[16] https://www.theguardian.com/uk-news/2019/jan/08/heathrow-airport-departures-suspended-after-drone-sighting 08/01/2019

[17] https://www.janes.com/article/82347/uk-signs-for-drone-dome-c-uas-system 14/08/2018

Subsequent news[18] mention the decision to install the AUDS UAV Defense System to protect Gatwick airport, for a cost of around € 900,000. This is not surprising as AUDS is a UK-developed anti-drone system used also by the US military.

Other news[19] announce *Drone jamming system to protect European airports, public spaces*, according to the chief technology officer of Danish anti-drone firm MyDefence.

In early 2019, on the emotional wave caused by the incidents at UK airports, the media attention on the drone threat has a special focus on **near misses (Airprox) incidents** with ordinary aircraft. The latest figures published for 2018 by the UK Airprox Board (UKAB) and reported on the UAS Vision website[20] show a continued rise of incidents involving drones and civil aircraft (**Figure 2.3.1**). There were 120 near misses between drones and aircraft reported in 2018, up 29% than in 2017. Several of the incidents involved airliners, which were approaching Heathrow.

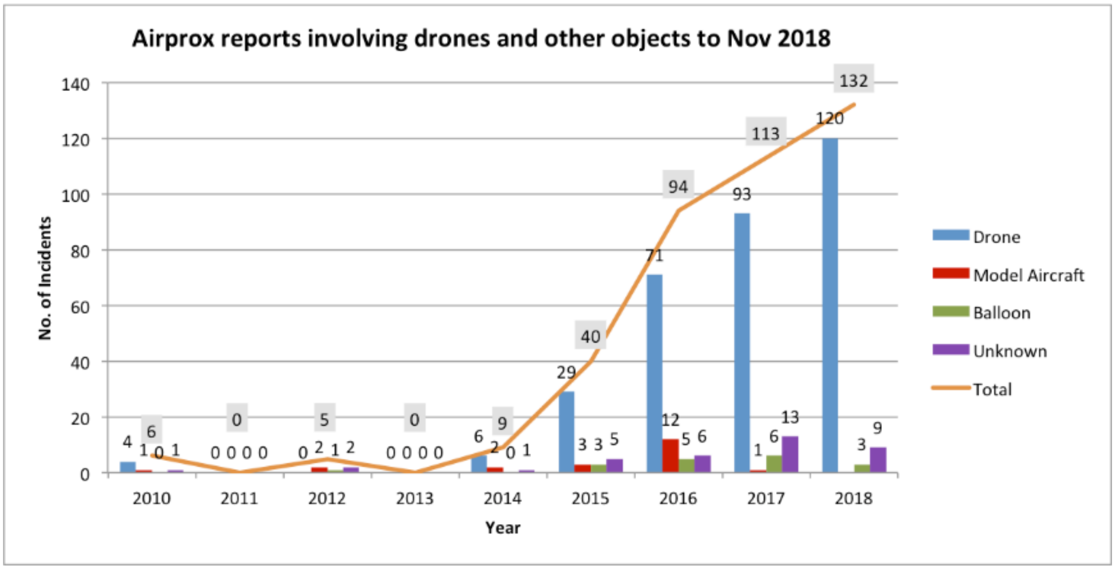


Figure 2.3.1: Near misses of drones and civil aircraft in UK (Source: UK Airprox Board)

In early 2020, other incidents confirmed the drone threat at airports. In Spain, at **Adolfo Suárez Madrid-Barajas** airport on 3rd February 2020, a set of drones forced air traffic to be deviated to other nearby airports and limited take-offs during one hour[21]. The airport was closed during almost 2 hours due to the apparent presence of drones

[18] https://www.quadricottero.com/2019/01/a-gatwick-installato-il-sistema-anti.html 13/01/2019

[19] https://phys.org/wire-news/308899455/drone-jamming-system-to-protect-european-airports-public-spaces.html 14/01/2019

[20] "UK Airprox Board Reports 30% Rise in Drone Incidents", 25/01/2019 https://www.uasvision.com/2019/01/25/uk-airprox-board-reports-30-rise-in-drone-incidents/

[21] https://elpais.com/politica/2020/02/03/actualidad/1580732176_100077.html

around[22]. Spain's State Air Safety Agency (AESA) confirmed in a tweet that "flying drones in the vicinity of an airport is a serious infraction that comes with a penalty fine of up to €90,000".

In August 2020, news report that US President Donald **Trump's jet was nearly hit by a small drone**[23] as it approached an air base near Washington Sunday night, according to several people aboard Air Force One. The article states that this is among the thousands of such safety incidents involving unmanned devices in the U.S. that have prompted calls by law enforcement and homeland security agencies for greater measures to rein in their use. Government research suggests that the damage from a drone could be greater than that from a similar-sized bird, which could shatter a cockpit windshield or damage an engine, although none of the instances in which drones actually struck aircraft have resulted in a serious crash or injuries, according to National Transportation Safety Board data. Drone sightings have occasionally disrupted operations at major airports in USA, such as in January 2019. The FAA hopes to unveil regulations requiring that civilian drones transmit their location and identity by the end of the year. The new requirement is designed to help prevent the devices from being used by terrorists and to reduce the risks they pose to traditional aircraft.

2.3.1.2 Criminal and terroristic use of drones

An article of the World Security Report (March / April 2019)[24] summarizes the recent escalation of the drone threat in just three months:

In recent months, drones have been wreaking havoc; whether they are used to infiltrate someone's privacy by recording from above, flying illicit contraband into prisons, exposing the security shortcomings of a critical infrastructure site or closing Gatwick Airport airspace for 33 hours. In that 33 hours over 1,000 flights were disrupted affecting 140,000 passengers and a suggested total cost to the airport and industry anywhere between £50 – 100 million! [ ] These are the off-the-shelf hobbyist drones used by petty criminals for unauthorised surveillance, malicious actors intent on causing trouble, activists proving a point or maybe just a simple error from a hobbyist in a field. Recently Greenpeace dropped smoke bombs from a drone onto the roof of a building containing irradiated fuel to prove a point that the Orano La Hague Nuclear Power Facility is not sufficiently protected. [ ] Hence the frenzied interest in Anti Drone technology. [ ] This article looks at just some of the myriad of options now available to counter drone threats. Among the anti-drone options, the article includes Black Knight by IDS Corporation, member of the ALADDIN consortium, and a number of other systems (AUDS, etc.).

---

[22] https://www.thelocal.es/20200203/airspace-closed-at-madrids-barajas-airport-after-drone-sighting 3 February 2020

[23] https://www.bloomberg.com/news/articles/2020-08-17/trump-s-plane-nearly-hit-by-small-drone-on-sunday-witnesses-say 17 August 2020

[24] Karen Kingham, "From Eagles to Lasers – the Evolving Business of the Anti-Drone Market", World Security Report, March / April 2019, p.14

The risk of terroristic use of drones is confirmed by news from Spain in September 2017[25]: "*The police arrested a man in Merida (Badajoz) on Friday for his alleged integration into Dáesh's I+D+I technological apparatus, for which he was looking for drones and other equipment, in addition to participating in financing the terrorist organization*."

More recent news refer to an alleged shock assassination plot against **Venezuelan President Nicolas Maduro** using two flying drones loaded with explosives on 4th August 2018[26]. The worldwide echo of this event highlights risk of drone strikes[27] and that such kind of attacks will not be the last[28]. This attack has prompted concerns that such terror tactics could become more and more common in the future, especially against easy targets, such as airports and *"large stadiums full of people, including rock concerts and football matches"*, according to an associate professor at the University of the West England, in Bristol[29]. Experts say the psychological effects of a small but successful attack could far outstrip the actual physical damage, accomplishing the goal of spreading terror that many militant groups have made their mission.

Various sources evidence the asymmetric nature of this emerging threat:

The proliferation of inexpensive commercial UAS democratises capabilities previously held by militaries, and enhances asymmetric threats.[30]

The asymmetric nature of the sUAS, especially when considering swarm tactics, makes the technology difficult to defend against[31]*.*

At dawn of 2020, the use of weaponized drones is becoming a dramatic reality: an example is **the killing of Iranian General Q. Suleimani by a US drone** in an overnight airstrike at the Baghdad airport on 02/01/2020[32]. Although military applications are outside the scope of this report, the entire world fears that this event could trigger an

[25] http://www.rtve.es/noticias/20170922/detenido-merida-hombre-financiar-buscar-drones-para-daesh/1621622.shtml, 22 September 2017

[26] The Guardian, 05/08/2018. *Venezuela's Nicolás Maduro survives apparent assassination attempt.* https://www.theguardian.com/world/2018/aug/04/nicolas-maduros-speech-cut-short-while-soldiers-scatter

[27] Reuters, 05/08/2018. *Apparent attack in Venezuela highlights risk of drone strikes.* https://www.reuters.com/article/us-venezuela-politics-drones/apparent-attack-in-venezuela-highlights-risk-of-drone-strikes-idUSKBN1KQ0MG

[28] Wired, 04/08/2018. *The Explosive-Carrying Drones in Venezuela Won't Be the Last*. https://www.wired.com/story/venezuela-drones-explosives-maduro-threat/

[29] Express, 05/08/2018. *Venezuela-style DRONE TERROR will SURGE with airports and football stadiums 'easy targets'.* https://www.express.co.uk/news/world/999209/Venezuela-drone-assassination-terror-Maduro-attack-terrorism

[30] https://counteruas.iqpc.co.uk/

[31] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_30-35_Tingle-Tyree.pdf

[32] U.S. Strike in Iraq Kills Qassim Suleimani, Commander of Iranian Forces https://www.nytimes.com/2020/01/02/world/middleeast/qassem-soleimani-iraq-iran-attack.html

increased uses of drones for terroristic purposes, as "*Iranian leaders issued strident calls on Friday for revenge against the United States"*[33].

Concerning the threat evolution, experts agree that the next generation of drone threats will be swarms and completely autonomous drones. Since swarms are multiple drones employed simultaneously to complete a common goal, they require a C-UAS system that can effectively mitigate the threats at an extremely rapid rate. Completely autonomous drones, which operate without using radio frequencies, GPS, WiFi, Bluetooth or any other form of signal communication, require a multi-layered defence system, that can detect and locate both RF and non-RF emitting drones through different types of sensors, and then mitigate the threat through appropriate means.

2.4 The role of drones in the near future

While in bad hands drones can pose a nasty threat, like all disruptive technologies they are destined to revolutionize everyday life and to play a crucial role as powerful allies of humanity in facing unexpected challenges, especially in global health emergency and crisis situations.

An article by **Drone Industry Insights** points out 5 key trends on drone discussion topics in 2020[34]:

1. ***Counter drone technology*** – Due to security concerns, the counter-drone market has grew rapidly in recent years and is expected to continue to grow in 2020 and beyond.
2. ***Urban Air Mobility (UAM)*** – Following the start of drone deliveries (food, medicine, etc.) last year, the expectation is that the drone delivery industry develops even further in 2020, whereas the development of passenger drones will need more time and more funding to get certified, before the passenger drones market will rise.
3. ***Unmanned Traffic Management (UTM)*** **–** Following the FAA opinion on UTM published in December 2019 and EASA opinion about Remote ID and U-Space initiative in the first quarter of 2020, it will be interesting to see how the European rules will differ from the US rules.
4. ***Adoption and Automation*** – Increased automation and better workflow integration will make drone adoption easier, which is reflected in the growing drone market forecast for the next five years.
5. ***ISO Standards*** – After the release of the first ISO approved drone safety standards at the end of 2019, safety management system will become a major regulatory topic in 2020.

[33] The Killing of Gen. Qassim Suleimani: What We Know Since the U.S. Airstrike https://www.nytimes.com/2020/01/03/world/middleeast/iranian-general-qassem-soleimani-killed.html

[34] Millie Radovic, Global Drone Outlook 2020: What's on the Agenda, 2020-01-07 https://www.droneii.com/global-drone-outlook-2020

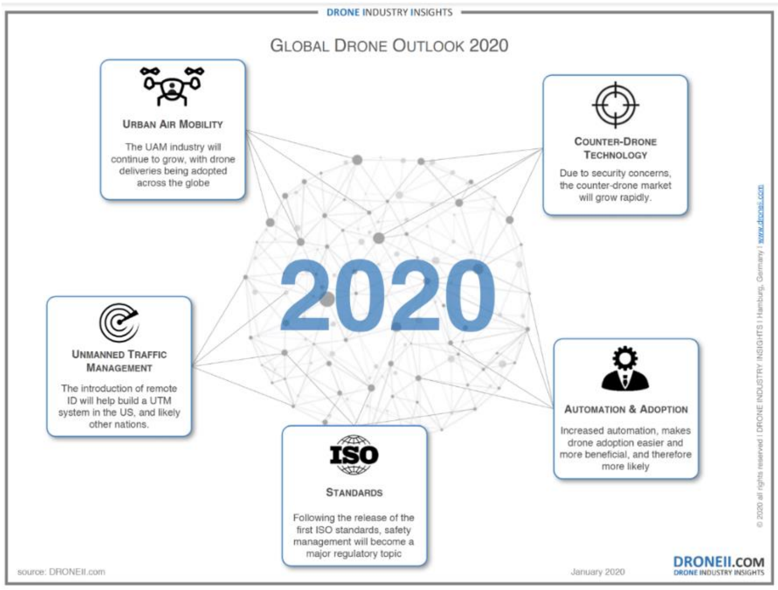


Figure 2.4.1: Global Drone Outlook 2020 (Source: DRONEII.com)

The game-changing role of drones became apparent in the recent **global pandemic COVID-19**, which is affecting the daily life of everyone, causing major disruptions globally from travel restrictions to event cancellations and impacting the stock market as well. The big impact of drones became visible during the Coronavirus outbreak[35], demonstrating their high potential in this novel situation, thanks to their quick response and ability to operate autonomously. A number of articles in specialized press and media describe the benefits of Aerial Mobility during COVID-19[36] [37] and the opportunity of using drones for improving life with tech innovation[38]. COVID-19 is accelerating the deployment and development of aerial mobility technology in various ways:

Surveillance drones **–** Several examples in the world (China, Spain[39] [40], Italy[41] [42] and many more) demonstrate the use of surveillance drones to support the enforcement of quarantines and curfews, broadcasting the invitation to stay at home and monitoring social distancing in public places.

---

35 https://www.amsterdamdroneweek.com/news/articles/the-impact-of-drones-during-the-corona-virus 13 March 2020

36 https://transportup.com/editorials/aerial-mobilitys-attack-on-coronavirus/ 09 March 2020

37 https://www.amsterdamdroneweek.com/news/articles/the-benefits-of-aerial-mobility-during-covid19 25 March 2020

38 https://www.amsterdamdroneweek.com/news/articles/improving-life-with-tech 06 April, 2020

39 https://www.youtube.com/watch?v=J7ZAXFGWpEc

40 https://www.independent.co.uk/news/world/europe/coronavirus-spain-police-lockdown-drones-latest-cases-a9403771.html 16 March 2020

41 https://www.euronews.com/2020/03/23/coronavirus-italy-approves-use-of-drones-to-monitor-social-distancing 23/03/2020

42 https://www.enac.gov.it/news/utilizzo-droni-provvedimenti-governativi-emergenziali

Corollaries in disaster relief – Drones are significantly faster than ground-based Search and Rescue (SAR) methods in natural disaster relief scenarios and in the fight against COVID-19 are being used for disinfectant spraying or remote temperature check[43].

Rapid transport of medical goods – Since the start of the outbreak, various companies are offering drone transport services for the anti-epidemic effort. Rapid transport via air taxi ranges from the safe transport of medical samples and quarantine supplies in China to the delivery of goods and aid in hazardous conditions without putting humans at risk, up to transportation of human organs in critical scenarios.

Food delivery drones – COVID-19 is forcing the progress of larger scale drone deliveries, making universally clear the benefits of a large network that could transport food, consumables, and emergency/disaster relief equipment in a scenario such as a hurricane, earthquake, or virus outbreak.

In summary, the related article by Drone Industry Insights[44] states that *while on the one hand economists are asserting that this will undoubtedly impact our economies for years to come, tech experts will agree that this global health crisis (like many before it) could bring about a new momentum for potentially lifesaving technologies like drones.*

As in most sad massive global events, these hard times are prompting for great progress in technological advancements, giving the opportunity to implement innovations in the drone industry and in many other fields that could benefit the society.

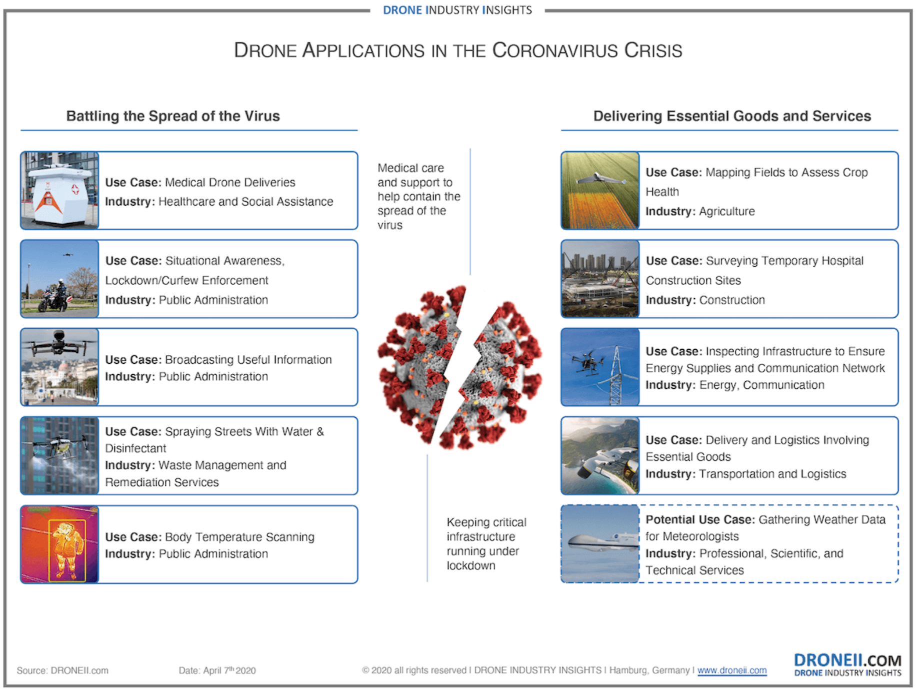


Figure 2.4.2: Drone applications in the Coronavirus crisis (Source: DRONEII.com)

43 https://www.geospatialworld.net/blogs/how-drones-are-being-used-to-combat-covid-19/ 04/20/2020

44 https://www.droneii.com/drones-and-the-coronavirus-from-crisis-to-opportunity 2020-04-06

3 Standardisation progress

This chapter reports the main standardisation progress in ALADDIN focus areas, namely those concerning:

- UAV-related topics
- Electromagnetic emissions
- Privacy and personal data protection.

In developing the ALADDIN platform, the consortium will pursue compliance with applicable standards not only for ***UAV-related topics*** – relevant to the whole project, but also to ***Electromagnetic emissions*** – relevant to radar, jamming and communications (C2), as well as ***Privacy and personal data protection*** – mostly relevant to Electro-Optical sensors.

Starting from the situation at beginning of the ALADDIN project (§ 3.1), this chapter aims at monitoring the standardisation evolution through the project lifetime (§ 3.2).

3.1 Introduction

The availability of open international standards is a key enabling factor for the development of markets in all business sectors, including the **Security** sector, since they provide sustainability and interoperability while still allowing for competition between equipment, service and content providers. Since the beginning of this decade, the EC is pointing out the necessity to address the gaps in the standardisation and regulation framework for an innovative and competitive Security Industry. This necessity is clearly stated in the EC documents: ***An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage*** ([ND1]), the ***Action Plan for an innovative and competitive Security Industry*** ([ND2]) and the recent ***European Agenda on Security*** ([ND3]). Whilst the EU must remain vigilant to other emerging threats that also require a coordinated EU response, the Agenda prioritises **terrorism, organised crime and cybercrime** as interlinked areas with a strong cross-border dimension, where EU action can make a real difference[45].

To address the gaps in the standardisation and regulation framework, in [ND1] the Commission announced the launch of a dedicated initiative on a Security Industry Policy: *The EU security industry faces a highly fragmented internal market and a weak industrial base. National regulatory frameworks differ widely and the market for security products is highly diversified, ranging from cameras to complex scanner systems. To provide a security system, manufacturers, system integrators, and service providers have to work closely together with clients. It is essential to develop a fast-track system for approval of priority technologies; to make substantial further progress on harmonisation, standardisation; to consider coordinated public procurement; and to accelerate research on security technologies including dual-use.*

The EC acknowledges the importance of certification and standardisation in the Security sector and the need to initiate a series of actions, which will enable the EU

[45] https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

industry to meet the challenges of the twenty-first century[46]. Concerning certification[47], it admits that *there are currently, no EU-wide certification systems for security technologies. National systems differ widely, thus significantly contributing to the fragmentation of the security market*. Concerning standardization[48], it recognizes that, as highlighted in [ND2], *Standards play a major role in defragmenting markets and helping industry in achieving economies of scale. Standards are also of upmost importance for the demand side, notably with regard to interoperability of technologies used by first responders, law enforcement authorities, etc. Additionally, standards are essential for ensuring uniform quality in the provision of security services. Creating EU-wide standards and promoting them on a worldwide level is also a vital component of the global competitiveness of the EU security industry. Nevertheless, the security market in Europe is a highly fragmented one with divergent national standards, which pose a major obstacle for the creation of a true internal market for security, thus hindering the competitiveness of EU industry.*

Two relevant areas identified in [ND2] for future standardization were:

- *exploiting synergies between **security and defence** technologies,*
- ***privacy and personal data protection** management.*

*The Commission considers that the development of 'hybrid standards', i.e. standards that apply both to civil security and defence technologies, should be actively pursued in areas where technologies are the same and application areas are very similar. Therefore, in close cooperation with the European Defence Agency, the Commission issued a standardisation mandate to the European Standardisation Organisations (ESOs), i.e. CEN, CENELEC and ETSI, for Reconfigurable Radio Systems (**M/512 Mandate**). In addition, the Commission committed to issue a mandate to the ESOs to develop standard(s) for privacy and personal data protection management in support of Union's security industry (**M/530 Mandate**).* Standards and regulation on this topic may affect also the development of security products for C-UAV application.

ALADDIN agrees with the global consensus on the importance of open standards and specifications with respect to the widespread adoption of applications, services and products. Therefore, ALADDIN will constantly monitor the standardization activities and will build its offered services and platform to be fully aligned with all the related standards ([AD1]).

3.1.1 Standardisation bodies

Standardization activities relevant to **UAV (and C-UAV) themes** include those carried out at different levels (European, International) within:

- work groups of the *European Organization for Civil Aviation Equipment* (EUROCAE)[49]:

[46] https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security_en

[47] https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security/certification_en

[48] https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security/standardisation_en

[49] https://www.eurocae.net/

  - **WG-105** Unmanned Aircraft Systems UAS, which replaces former WG-73 and WG-93, following the Council decision of 29 September 2016[50]
  - **WG-115** Counter UAS (C-UAS), launched in 2019
- technical committees (or sub-groups) of the *International Organization for Standardization* (ISO)[51]:
  - **ISO/TC 20/SC 16** Unmanned aircraft systems[52]
- relevant panels of the *International Civil Aviation Organization (ICAO)*[53], the *European Aviation Safety Agency (EASA)*[54], the *Joint Authorities for Rulemaking on Unmanned Systems (JARUS)*[55]*, EUROCONTROL*[56], as well as the American *Federal Aviation Administration (FAA)*[57]
- standardization discussion groups in *UAV associations* and *stakeholders unions and networks*, such as:
  - AERPAS, UVS International, IEEE Aerial Robotics and Unmanned Aerial Vehicles Technical Committee, euRobotics;
  - European Union Agency for Law Enforcement Training, European Network on Law Enforcement Services;
  - National committees or sub-groups.

EUROCAE

The EUROCAE work group **WG-105 (Unmanned Aircraft Systems UAS)** is tasked to develop standards and guidance documents that will allow the safe operation of UAS in all types of airspace, at all times and for all types of operations. It works in coordination with RTCA SC-228 (Minimum Operational Performance Standards for Unmanned Aircraft Systems). WG-105 is organized in six Focus Teams working in 6 main Focus Areas.

ISO

ISO has also an intense activity on drones regulation under **ISO/TC 20/SC 16 (Unmanned aircraft systems).** This Technical Committee was created in 2014 and includes 15 Participating members (USA - Secretariat, EU and most of Asian Countries) and 5 Observing members. It deals with standardization in the field of UAS including, but not limited to, classification, design, manufacture, operation and safety management of UAS operations. ISO/TC 20/SC 16[58] is developing ISO standards through its three working groups:

---

[50] https://www.eurocae.net/about-us/working-groups/

[51] https://www.iso.org/home.html

[52] https://www.iso.org/committee/5336224.html

[53] https://www.icao.int/

[54] https://www.easa.europa.eu

[55] http://jarus-rpas.org/

[56] https://www.eurocontrol.int/

[57] https://www.faa.gov/

[58] https://www.iso.org/committee/5336224/x/catalogue/p/0/u/1/w/0/d/0

- WG1 General
- WG2 Product manufacturing and maintenance
- WG3 Operations and procedures

The participation in ISO is through the different national standardization entities; for example is Spain is through the Spanish Association for Standardization and Certification (AENOR)[59].

ICAO

The *International Civil Aviation Organization* (**ICAO**)[60] is a specialized agency of the United Nations, created in 1944 to promote the safe and orderly development of international civil aviation throughout the world. It sets standards and regulations necessary for aviation safety, security, efficiency and regularity, as well as for aviation environmental protection. The Organization serves as the forum for cooperation in all fields of civil aviation among its Member States.

ICAO initiated work on unmanned aircraft systems (UAS) in 2007 when it established the Unmanned Aircraft Systems Study Group (UASSG). The UASSG served as the ICAO focal point for all UAS related issues until 2014, when it was superseded by the **ICAO Remotely Piloted Aircraft Systems Panel (RPASP)** to address the new challenges of UAS operating internationally under Instrument Flight Rules (IFR).

In 2011, ICAO issued *Circular 328 AN/190* ([ND4]), considered as a first attempt to develop an international regulatory framework towards global harmonisation in the regulation of UAS.

The **ICAO RPASP** coordinates and develops ICAO Standards and Recommended Practices (SARPs), Procedures for Air Navigation Services (PANS) and Guidance material for remotely piloted aircraft systems (RPAS), to facilitate a safe, secure and efficient integration of remotely piloted aircraft (RPA) into non-segregated airspace and aerodromes.[61] A useful Guidance material is the *Manual on Remotely Piloted Aircraft Systems (RPAS)* published by ICAO in 2015 ([ND5]).

In ICAO terminology, RPA is a subset of Unmanned Aircraft (UA), defined as any powered or unpowered aircraft that is flown without a pilot onboard[62] (**Figure 3.1.1**). These aircraft may operate autonomously or be remotely piloted (RPA).

---

59 http://www.aenor.es/aenor/inicio/home/home.asp

60 https://www.icao.int/

61 https://www.icao.int/safety/UA/Pages/Remotely-Piloted-Aircraft-Systems-Panel-(RPASP).aspx

62 https://www.icao.int/NACC/Documents/Meetings/2016/ANIWG3/ANIWG3P01.pdf Mexico, April, 2016

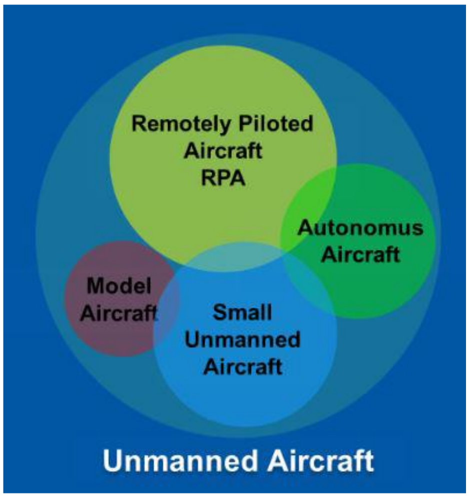


Figure 3.1.1: Unmanned Aircraft in ICAO terminology

The main objective of the RPAS Panel is to develop SARPs, procedures and guidance material specifically for RPAS, giving priority to IFR operation in controlled airspace, with the aim to maintain the existing level of safety for manned aviation.

Performance-based Standards are preferred as they provide greatest freedom of choice, allowing the most appropriate solution to be considered; however, prescriptive Standards are sometimes required (e.g. frequency spectrum).The RPASP Structure includes a large number of Members (23 States and 11 international organizations) and Observers (3 States and 5 international organizations) organized in six working groups. ICAO has developed an online **UAS toolkit**[63] to assist States in developing national regulations for domestic UAS operations.

ASTM

ASTM International (**ASTM**)[64] is a not-for-profit organization and developer of voluntary consensus standards. **ASTM F38 (Unmanned Aircraft Systems)** UAS Standards Committee was formed in 2003, with the mission to produce practical, consensus standards that facilitate UAS operations in civil airspace at an acceptable level of safety. Efforts on developing standards for small UAS (sUAS/sRPAS) began in 2010 with FAA support[65]. Many standards are being developed and finalized. The most relevant to C-UAV application include the proposed new standards under the jurisdiction of Subcommittee F38.01 Airworthiness[66] concerning Operation over People of small and micro UAS and UAS remote identification and tracking, in addition to the active ones, such as ASTM F2851-10 ([ND6]) and ASTM F3196-17 ([ND7]) with its proposed revision.

[63] https://www4.icao.int/uastoolkit/home/about

[64] https://www.astm.org/

[65] Ted Wierzbanowski, 2017. 'ASTM International Committee F38 on Unmanned Aircraft Systems', ASTM Meeting at AUVSI, Dallas, TX, 8 May 2017. https://www.astm.org/COMMIT/2017-AUVSI%20May%20Meeting.pdf

[66] https://www.astm.org/COMMIT/SUBCOMMIT/F3801.htm

RTCA

Radio Technical Commission for Aeronautics (**RTCA**, Inc.) [67] is a United States volunteer organization that develops technical guidance for use by government regulatory authorities and by industry. **RTCA SC-228** (Minimum Operational Performance Standards for Unmanned Aircraft Systems)[68], established in 2013, is working to develop the Minimum Operational Performance Standards (MOPS) in order to safely and seamlessly integrate these platforms into non-segregated airspace. These MOPS concern:

- Detect and Avoid (DAA) equipment
- Command and Control (C2) Data Link.

SESAR JU

While not a standardization body in the strict sense, *SESAR Joint Undertaking* (**SESAR JU**) has a major role in standardization concerning Air Traffic Management (ATM) and Unmanned aircraft system Traffic Management (UTM). UTM is "a specific aspect of air traffic management which manages UAS operations safely, economically and efficiently through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions"[69].

As the technological pillar of Europe's ambitious *Single European Sky (SES)* initiative, SESAR is the mechanism which coordinates and concentrates all EU research and development (R&D) activities in ATM, pooling together a wealth experts to develop the new generation of ATM[70]. SESAR-JU is the main actor in fostering the UTM system of services in Europe, known as **U-Space**[71].

GUTMA

The *Global UTM Association* (**GUTMA**)[72] is a non-profit consortium of worldwide UTM stakeholders. Its purpose is to foster the safe, secure and efficient integration of drones in national airspace systems. GUTMA is a standardization body focused on **U-Space** (also known as UTM, especially in USA). GUTMA is trying to attract non-aeronautical actors (such as cell phone and satellite service providers, UTM companies, etc.) in order to create standards that will facilitate the interoperability of different UTM systems.

ETSI, CEN-CENELEC

CEN, CENELEC and ETSI are the European Standards Organisations (ESO) responsible for producing **harmonised standards**. A harmonised standard is created following a request from the European Commission to one of these organisations.

[67] https://www.rtca.org/

[68] https://www.rtca.org/content/sc-228

[69] https://www.icao.int/safety/UA/Documents/UTM-Framework%20Edition%202.pdf

[70] https://www.sesarju.eu/discover-sesar

[71] https://www.sesarju.eu/U-Space

[72] https://gutma.org/

Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation. The references of harmonised standards must be published in the Official Journal of the European Union (OJEU).

Relevant Harmonised Standards, such as those on **Electromagnetic compatibility (EMC)** or **Radio Equipment (RED)**, are accessible through the EC website: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en.

ETSI, CEN and/or CENELEC will be responsible to elaborate the European Directive on the **CE marking** of drones for the 'Open' category of the European drone regulation.

EUSCG

For minimizing the risk of gaps and overlaps in the various standardisation activities by various organizations, considering the successful example of the EASCG which coordinates the standardisation activities in the area of Air Traffic Management (ATM), it was decided to put in place a similar arrangement in the area of UAS. Hence, the *European UAS Standards Coordination Group* **(EUSCG)**[73] was established. It had its Kick-Off Meeting on the 1st of June 2017 at the EUROCAE offices in France.

The EUSCG is a joint coordination and advisory group established to coordinate the UAS-related standardisation activities across Europe, essentially stemming from the EU regulations and EASA rulemaking initiatives. The EUSCG provides a link to bridge the European activities to those at international level, ensuring a better coordination and monitoring of the relevant activities affecting standardisation:

- rulemaking activities under EASA responsibility,
- update to ATM Master Plan by including UAS provisions,
- standardisation activities executed by the relevant standardisation bodies, including **EUROCAE WG-105** work programme.

The main deliverable of the EUSCG is the European UAS Standardisation Rolling Development Plan (RDP), which will be progressively updated to reflect the current situation.

3.1.2 Standardisation status in 2017

For **UAV-related topics** the preliminary version of the EUSGC' RDP[74], dated 20/11/2017, gives a useful overview of the status of relevant regulation and standardization activities at the end of 2017.

[73] https://www.eurocae.net/about-us/euscg/

[74] https://www.eurocae.net/media/1480/preliminary-rdp_20-nov-2017_final.pdf

Concerning **electromagnetic emissions**, [AD3] presented the main ETSI standards and EU directives relevant to ***radar*** systems ([ND8] to [ND12]), including:

- the *Radio Equipment (RED)* Directive 2014/53/EU ([ND9]), that provides the essential requirements for radio equipment also in terms of radio spectrum use "in order to avoid harmful interference";
- the Directive 2014/30/EU - *Electromagnetic Compatibility (EMC)* [ND12], that sets out the mandate for harmonization of EM standards across the EU[75].

The analysis pointed out that apparently there is a lack of applicable standards for ***radar*** used in drone detection application.

Radar systems belong to **radio equipment** using radio waves for radiodetermination or radiolocation (as defined in [ND8] and [ND9]). However, ETSI standards defining emission limits for radio equipment are organised:

- *by application*: digital broadcasting, Air Traffic Control (e.g. [ND10]), VHF air-ground communication, etc.,
- *by licence-need and application*: some radio equipment can be used as license-free apparatus if they satisfy ERC Recommendation 70-03 ([ND11]). They are called Short Range Devices (SRD) because the emission limits are very low.

UAV detection application does not appear in the list of applications regulated by ETSI standards and the radar systems for UAV detection cannot be regarded as SRD because medium (1 km) and long (5-10 km) detection ranges are required.

From a standardisation point of view, the use of **radar** systems to detect these new threats (malicious UAVs) is a new application; hence, the standards that define the emission limits[76] are not yet available in the regulatory framework of air surveillance.

Moreover, it is not clear whether the drone detection application, performed by LEAs, could be classified as a public security service (see D3.1, Section 6 [AD2]). In such case, it would fall outside the scope of the *Radio Equipment (RED)* Directive 2014/53/EU ([ND9]) that provides the essential requirements for radio equipment also in terms of radio spectrum use "in order to avoid harmful interference". Furthermore, given the ambiguous legality of radio frequency ***(RF) jamming*** technologies (see D3.1 [AD2]), there does not appear to be European standards applicable to such neutralization equipment.

Regarding **privacy and personal data protection**, [AD3] pointed out that privacy and personal data protection management is in the forefront of current European standardization and regulation activity (as foreseen in [ND2] and [ND3]). The recent adoption of the *General Data Protection Regulation (GDPR)* - Regulation (EU) 2016/679 ([ND13]), which became enforceable from 25 May 2018, could speed up the development of standards for privacy and personal data protection management in support of Union's security industry (M/530 Mandate). These 'privacy by design' standards aim to promote the embedding of high standards of security and fundamental rights at the earliest stage in technological design. These may have an impact also on C-UAV systems, affecting some of its subsystems (e.g. video cameras

[75] https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/electromagnetic-compatibility_en

[76] Emission limits in the Occupied Bandwidth (OBW), Out-of-band domain (OOB) and spurious domain. These limits do not include Electromagnetic Compatibility (EMC).

and other supporting tools for subsequent forensic analysis), although the possible classification of the drone detection application as a *security service* (if performed by LEAs) would make the GDPR not applicable.

For an overview of the relevant data-protection legislation please refer to D3.1 [AD2], and for an analysis of the application to the GDPR and other data protection law-related legal instruments to the ALADDIN project, please refer to D3.3.

3.2 Standardisation progress report (August 2020)

3.2.1 UAV-related topics

The most important standardization bodies dealing with **UAV-related topics** include various bodies at International level and **EUROCAE** work group WG-105 at European level.

After its constitution in June 2017, the *European UAS Standards Coordination Group* **(EUSCG)**[77] aims at ensuring a better coordination and monitoring of the relevant activities affecting standardisation and their connection with rulemaking activities under EASA responsibility. The Version 1.0 of the EUSCG' European UAS Standardisation Rolling Development Plan (RDP)[78], dated 17/02/2018, gives a useful overview of the status of relevant regulation and standardization activities at the beginning of 2018. In the 'Regulation' side, the RDP table refers to the EASA **Opinion No.1/2018** ([ND27]), whereas in the 'Standardisation' side it lists the Standardisation activities/deliverables (either published, ongoing or planned) relevant to the different provisions of the regulation.

In 2018, EUROCAE hottest topics include Specific Operations Risk Assessment (SORA), where ALADDIN partner FADA-CATEC plays a leading role, UAS Traffic Management (UTM), UAS E-Identification and UAS Geo-Fencing. UTM is also the core of **ISO** standardization activity within ISO/TC 20/SC 16. **ASTM** standards published in 2018 include, among others, those on UAS Registration and Marking, and BVLOS Small UAS Operations, while other standards are still in preparation, including those concerning Operation Over People and UAS Remote ID and Tracking.

The Version 3.0 of the EUSGC' RDP, dated 06/03/2019, provides an overview of the status of relevant regulation and standardization activities at the beginning of 2019. These included the themes under responsibility of EUROCAE, pursuant to its Technical Work Programme, Edition 2019 (TWP 2019), and those carried out by other standardization bodies.

EUROCAE WG-105 develops standards and guidance documents that will allow the safe operation of UAS in all types of airspaces. ASD-STAN D5WG8 is developing

[77] https://www.eurocae.net/about-us/euscg/; http://www.euscg.eu/

[78] https://www.eurocae.net/media/1514/version-10-rdp_17_02_2018.pdf; http://www.euscg.eu/media/1246/euscg-039-version-10-rdp_2018.pdf

standards covering the requirements imposed on the consumer drones intended to be operated in the 'open' category of operations.

Concerning the anticipated evolutions affecting UAS, the EUROCAE TWP 2019 anticipates that the development by SESAR JU of the so-called U-Space concept for integration into the ATM Master Plan, will drive further standardisation needs.

At the end of 2019, the most important standardization activities on **UAV-related topics** are EASA publication of Acceptable means of compliance (AMC) and Guidance material (GM) on the rules and procedures for the operation of unmanned aircraft as well as the creation of EUROCAE WG-115 Counter UAS (C-UAS).

On 10 October 2019 EASA published Decision 2019/021/R[79], which provides the first issue of AMC and GM related to Commission Implementing Regulation (EU) 2019/947 (the 'UAS Regulation'). AMC are non-binding standards useful to demonstrate compliance with the 'Basic Regulation' [ND30] and the delegated and implementing acts ([ND31] and [ND32]).

In addition to an overview on ongoing activities in the various working groups, such as WG-105 (UAS), the EUROCAE Technical Work Programme, Edition 2020 (TWP 2020)[80] includes a new paragraph specifically on Counter UAS, where it identifies the *need to contribute on the topic of detection and surveillance around the airfield, with a focus on non-cooperative UAS.* Pursuant to TWP 2020, *WG-115 is established to develop standards to support the safe and harmonised implementation of Counter-UAS Systems into airport and ANSP systems.* ALADDIN partner CS GROUP has been appointed as Secretary of the WG-115 and is actively involved in drafting the foreseen 3 standardization documents, bringing the experience gained during the project implementation. New topics, like 'Autonomy' and 'Higher Airspace Operations' (above FL 660), involving autonomous UAS and relevant to other emerging themes, such as Urban Air Mobility (UAM) and UTM, will likely influence EUROCAE standardisation activities in the longer-term.

The Version 5.0 of the EUSCG' RDP, published in July 2020, provides the latest overview of the status of regulation and standardization activities relevant to UAS-related topics. The activities of the various EUROCAE working groups concerned with UAS and C-UAS (WG 105 and WG 115) are progressing, with some relevant standards published in June 2020, such as those on UAS Geo-Fencing and geo-caging, while others are under approval, such as those on UAS E-Identification and UAS safety analysis for the Specific category.

Meanwhile other bodies, like ISO and ASTM, are continuing their standardization activities at an unprecedented pace. In 2019-20 several documents were issued: 4 standards by ISO/TC 20/SC 16 and 11 standards under the jurisdiction of the subcommittees of ASTM Committee F38 on Unmanned Aircraft Systems, including the standard on UAS Remote ID and Tracking.

[79] https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2019021r 10 October 2019

[80] https://www.eurocae.net/media/1636/eurocae-twp-2020-public-version.pdf

3.2.2 Electromagnetic emissions

Concerning **electromagnetic emissions**, ALADDIN partners performed a review of the harmonized European standards relevant to EMC and LVD directives ([ND12] and [ND28]), which apply to jamming systems. These harmonized European standards likely apply also to other technologies involving electromagnetic emissions for detection, neutralization or communications (radar, RF, C2). Additionally, radar should comply also with the standards relevant to the RED directive ([ND9]). Other applicable standards include those produced by the International Telecommunication Union (ITU) or the military standards (MIL-STD or MIL-SPEC) set by the US Department of Defense.

3.2.3 Privacy and personal data protection

Regarding **privacy and personal data protection**, the most notable event is the entry into force on 25 May 2018 of the **General Data Protection Regulation** (**GDPR**) - Regulation (EU) 2016/679 ([ND13]). Compliance to related 'privacy by design' standards will likely become an essential requirement for EU security products. Nevertheless, it should be assessed whether (and to what extent) compliance to the GDPR is requested for systems/functionalities designed for use by Civilian Security stakeholders (Law Enforcement Agencies), such as C-UAV systems or sub-systems.

In relation to UAV (and C-UAV) topics, during the **UAS Workshop on standard scenarios**, organized by EASA in July 2018, the discussion was not limited to safety but it also included privacy and security aspects, confirming that the general challenge remains compliance to related 'privacy by design' standards.

4 Regulation progress

This chapter reports the main regulation progress in ALADDIN focus areas, namely those concerning:

- UAV-related topics
- Electromagnetic emissions
- Privacy and personal data protection
- Preventing and countering the UAV threat.

In developing the ALADDIN platform and implementing the project, the consortium will conform to the applicable regulation not only for ***UAV-related topics*** – including the operation of UAVs, relevant to the whole project, but also to ***Electromagnetic emissions*** – relevant to radar, jamming and communications (C2), as well as ***Privacy and personal data protection*** – mostly relevant to Electro-Optical sensors. For additional details, please refer to Deliverable D3.1 [AD2], as this document goes into depth into the relevant regulations with respect to all the above topics.

Starting from the situation at beginning of the ALADDIN project (§ 4.1), this chapter aims at monitoring the regulation evolution through the project lifetime (§ 4.2).

4.1 Introduction

It is widely recognised[81] that unmanned aircraft (UA) is a sector of aviation that is developing very fast and has a great potential for producing new jobs and growth. UAS or RPAS - also called civil 'drones' - are increasingly being used in the EU, but under a fragmented regulatory framework.

In the EU regulatory framework before the start of the ALADDIN project, Regulation (EC) No 216/2008 (hereinafter referred to as the **'Basic Regulation'** [ND15]) establishes the main principles and common rules for civil aviation in the EU and defines the area of competence of the EU and of its Member States (MSs). Since 2014 ([ND16]), there is a visible strong political support for developing rules on drones but regulations are not harmonized yet. The *European Aviation Safety Agency* (EASA)[82] has been tasked by the European Commission to develop a regulatory framework for drone operations and proposals for the regulation of "low-risk" drone operations. In achieving this, EASA is working closely with the *Joint Authorities for Regulation of Unmanned Systems* (JARUS)[83].

Aviation regulatory bodies, such as EASA and FAA, have banned the use of UAVs keeping in view the limitations in managing air traffic on such a huge scale and the safety of the citizens. On 7 December 2015 the EC adopted the *"Aviation Strategy to Enhance the Competitiveness of the EU Aviation Sector"*, a milestone initiative to boost Europe's economy, strengthen its industrial base and contribute to the EU global leadership. The new **Aviation Strategy for Europe**[84] consists of a Communication identifying challenges and opportunities to improve the competitiveness of the EU

---

[81] https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

[82] https://www.easa.europa.eu/

[83] http://jarus-rpas.org/regulations

[84] http://europa.eu/rapid/press-release_IP-15-6144_en.htm

Aviation sector ([ND17]), a proposal for a revision of the EU's aviation safety rules in the Basic Regulation ([ND18]) and requests to negotiate comprehensive EU-level air transport agreements with key third countries. The Aviation Strategy aims - among others – to the specification of the regulatory framework for the operation of unmanned aircraft, in order to unleash its full economic potential ensuring legal certainty to investors and safety. Towards this direction, after the publication in July 2015 of an Advance Notice of proposed Amendment (**A-NPA 2015-10**, [ND19]), on 18 December 2015 EASA published a formal **Technical Opinion**[85] on the operation of unmanned aircraft [ND20], in parallel to the draft modifications to the Basic Regulation included in the Aviation Strategy. In August 2016, EASA published a "Prototype" regulation [ND21] for the operation of unmanned aircraft in the 'open' and 'specific' categories in view of the ongoing negotiations with the Parliament and the Council on the review of Regulation (EC) No 216/2008.

ALADDIN is fully aware of the principles for a *proportionate, operation-centric, risk- and performance-based, progressive, and smooth* regulatory framework for all unmanned aircraft (UA) introduced by the Technical Opinion. As stated in the DOA [AD1], *"ALADDIN consortium will maintain an open two-way communication channel with the European Aviation Safety Agency, in order to stay up-to-date with the latest regulatory principles and limitations and above all transfer the knowledge gained throughout the project lifecycle with respect to the identification and the understanding of criminal and terrorism activities, involving UAVs. In this way, ALADDIN is expected to become a key player in the elaboration of the regulatory framework for the* ***operation*** *of UAVs."*

4.1.1 Regulation bodies

International civil aviation is regulated by a number of bodies that issue the rules and establish the modalities for their respect by interested parties:

- ICAO - International Civil Aviation Organization
- EU - European Union, through its institutional bodies
- EASA - European Aviation Safety Agency
- Eurocontrol
- JARUS - Joint Authorities for Rulemaking on Unmanned Systems

National Aviation Authorities (NAAs) are responsible for the enforcement of EU legislation at a national level.

In addition to the information in § 3.1.1, a concise presentation of the main civil aviation regulatory bodies is provided below. A brief introduction of EU Regulations Stakeholders[86] as well as major EU Regulations Updates[87] may be found also in the **DroneRules.eu** website[88].

ICAO - International Civil Aviation Organization

[85] https://www.easa.europa.eu/document-library/opinions/opinion-technical-nature

[86] https://dronerules.eu/en/professional/eu_regulations_stakeholders

[87] https://dronerules.eu/en/professional/eu_regulations_updates

[88] https://dronerules.eu/en/

ICAO[89] is a specialized agency of the United Nations founded in 1947 following the Chicago Convention on International Civil Aviation (Chicago 1944). ICAO[90] works with the Convention's 193 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector.

- Based in Montreal (Canada)
- 193 Contracting States[91]
- Purpose: Policies and Rules for Air Navigation and International Air Transport
- It issues and updates the Technical Annexes to the Convention (Annexes) which contain Standards and Recommended Practices (SARPs).
- There are currently 19 Annexes covering all technical areas of civil aviation.
- Contracting States must transpose the Standards into the national regulations and enforce them by all aeronautical organizations concerned.

As stated in paragraph 3.1.1, the scope of the **ICAO RPAS Panel** is currently limited to 'certified' RPAS operating internationally under instrument flight rules (IFR) in non-segregated airspace and at aerodromes. Instead, it is not concerned with the other categories of UAS ('open' and 'specific') of the European drone regulation defined by EASA, which are the National Authority focus.

EU - European Union

In its territory, the European Union is the regulatory body for air transport, aviation safety and security and for the respect of passengers' rights.

- It issues Basic and Implementation Regulations for the aviation sector.
- European regulations are binding in all the Union; Directives must be transposed by Member States (MS). EU supervises the application of the rules by the Member States.
- The European Union set up EASA - European Agency for Air Safety.
- EU performs its regulatory role through its institutional bodies:
    - The European Parliament and the Council
    - The European Commission

The European Parliament and the Council of the European Union are the main co-decision-making bodies of the EU. Under the ordinary legislative procedure, they are responsible for the negotiation and adoption of new EU laws based on proposals from the European Commission. Since 2015, both Institutions are actively working on the adoption of the first ever EU-wide rules for civil drones[92].

The European Commission is the executive body of the EU. It has four main roles including the submission of legislative proposals to Parliament and the Council.

[89] https://www.icao.int/Pages/default.aspx

[90] https://www.icao.int/about-icao/Pages/default.aspx

[91] https://www.icao.int/MemberStates/Member%20States.Multilingual.pdf 13/4/19

[92] https://www.consilium.europa.eu/en/policies/drones/

Estimating that an action was necessary at European level to regulate the drone industry more efficiently, in 2014 the EC published the Aviation Strategy, later endorsed by the aviation community in the Riga Declaration. Today, EC services driving the ongoing reform are Directorate General Mobility and Transport[93] and Directorate General Internal Market, Industry, Entrepreneurship and SMEs[94]. The EC is also supported in its mission by EASA and other EU technical bodies.

EASA - European Aviation Safety Agency

EASA[95] is an executive agency of the EC with regulatory and executive tasks in the field of civil aviation safety (e.g. safety inspections, certification, etc.). It is the European Authority in aviation safety, with the mission to ensure the highest level of safety and environmental protection, promoting a single regulatory and certification process among Member States in cooperation with other international aviation organisations & regulators (mainly ICAO, JARUS and the U.S. FAA). EASA absorbs part of the competences of EU member states and assists the EC in negotiating international harmonisation agreements with the "rest of the world" (such as FAA) on behalf of the EU member states.

- Established in 2002 on the basis of Regulation (EC) n.1592/2002 - now replaced by Reg. (EU) 2018/1139
- Based in Cologne (Germany)
- Purpose: Aviation Safety Regulations, including:
    - Type certification of aircraft and parts
    - Certifications of non-EU organizations
    - Standardization of national authorities

EUROCONTROL - European Organisation for the Safety of Air Navigation

EUROCONTROL[96] is a pan-European, civil-military organisation dedicated to supporting European aviation.

- Intergovernmental organisation involving 41 European Member states and 2 Comprehensive agreement States outside Europe
- Founded in 1960 and based in Brussels (Belgium)
- Purpose: develop and maintain a safe and efficient air traffic management across Europe, supporting the national civil aviation authorities, the air navigation service (ANS) providers, civil and military airspace users, the industrial sector, professional organizations and the European institutions.

JARUS - Joint Authorities for Rulemaking on Unmanned Systems

JARUS[97] is a group of experts from the National Aviation Authorities (NAAs) and regional aviation safety organizations.

---

[93] https://ec.europa.eu/transport/modes/air/aviation-strategy_en

[94] https://ec.europa.eu/growth/sectors/aeronautics/rpas_en

[95] https://www.easa.europa.eu/

[96] https://www.eurocontrol.int/

[97] http://jarus-rpas.org/

- At present 61 countries, as well as EASA and EUROCONTROL, are contributing to the development of JARUS.
- Purpose: to recommend a single set of technical, safety and operational requirements for the certification and safe integration of Unmanned Aircraft Systems (UAS) into airspace and at aerodromes.
- Objective: to provide guidance material aiming to facilitate each authority to write their own requirements and to avoid duplicate efforts.

JARUS has developed several documents[98] toward the new European drone regulation, such as on the initial operation-centric approach for categories. On 28 July 2017, JARUS published the first edition of the ***JARUS guidelines on Specific Operations Risk Assessment (SORA)***[99]. This document recommends a risk assessment methodology to establish a sufficient level of confidence that a specific operation can be conducted safely.

National Aviation Authority

The European aviation safety system is based on the sharing of tasks and responsibilities between the EU and its Member States. In this system, National Aviation Authorities (NAAs) are responsible for the implementation of EU legislation and safety oversight at a national level. A list of NAAs per country is available on **DroneRules.eu** website[100].

4.1.2 Regulation status in 2017

The previous paragraphs presented an historical background on the evolution of the regulatory framework for the operation of unmanned aircraft before the start of ALADDIN project (from [ND15] to [ND21]) and introduced the main regulation stakeholders at European and International level (§ 4.1.1). For the sake of conciseness, this paragraph summarizes the regulation status at beginning of the ALADDIN project. A more detailed report may be found in **Version V1** of the Deliverable (D4.5) [AD3].

For **UAV-related topics**, as recalled in § 4.1.1, [AD3] listed the main points to be addressed by the regulatory efforts in order to overcome the current fragmentation, with EASA playing a key role in this process.

In the regulatory framework before the start of the ALADDIN project, Regulation (EC) No 216/2008 (the 'Basic Regulation' [ND15]) establishes the main principles and common rules for civil aviation in the EU and defines the area of competence of the EU and of its Member States (MSs). The scope of EU regulations, and in particular of the 'Basic Regulation' is limited to those with a maximum take-off mass (MTOM) above 150 kg that are not used for military, customs, police, firefighting, search and rescue, or experimental operations, whereas each nation is in charge of ruling the operation of

[98] http://jarus-rpas.org/publications

[99] http://jarus-rpas.org/content/jar-doc-06-sora-package; http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v1.0.pdf

[100] https://dronerules.eu/en/professional/authorities

aerial systems below 150 kg. An overview of National Regulations (October 2017) for EU MSs and other countries (such as Australia and USA) can be downloaded from the JARUS website[101].

Concerning **electromagnetic emissions**, [AD3] points out that there is no relevant applicable regulation concerning limits of **electromagnetic emissions** for sensors (such as ***radar***) that might be used for drone detection application, since this is a new application and the normative process is usually slower than technological development. As stated in previous paragraphs, if (radar) drone detection performed by LEAs could be considered as a public security service it would fall outside the scope of the *Radio Equipment (RED)* Directive 2014/53/EU ([ND9]). Furthermore, ***RF jamming*** technologies have ambiguous legality in European legislations (see D3.1 [AD2]).

Finally, concerning **Privacy and personal data protection**, the adoption of the **General Data Protection Regulation** (**GDPR**) - Regulation (EU) 2016/679 ([ND13]), enforceable from 25 May 2018, might affect also the design of drone detection subsystems (such as video cameras) and other supporting tools for subsequent forensic analysis. However, the possible classification of the drone detection application as a *security service* (if performed by LEAs) would make the GDPR not applicable.

4.2 Regulation progress report (August 2020)

4.2.1 UAV-related topics

Concerning ***UAV-related topics***, in 2018 there is a notable progress in EASA efforts to improve the **drone safety regulation** thus overcoming the fragmented regulatory framework especially for the smaller UAS. A major step forward is the publication on the 06/02/2018 of EASA **Opinion 01/2018** ([ND27]), after a four-month consultation period on the NPA 2017-05 published in May 2017 ([ND23] and [ND24]), concerning the 'Open' and 'Specific' category.

According to [ND27], the 'open' category has been defined as operations conducted:

- with a UAS with an MTOM of less than 25 kg;
- below a height of 120 m; and
- in VLOS.

It was decided to further subdivide operations in the 'open' category into three subcategories (A1, A2, A3) to allow different types of operations without the need for an authorisation.

The 'specific' category is applicable to all operations that do not comply with the limits of the 'open' category. It requires the UAS operator to perform a risk assessment and

[101] Comparison National Regulations (updated 18th Oct 2017) http://jarus-rpas.org/sites/jarus-rpas.org/files/comparison_national_fegulations_oct2017.xlsx

to propose mitigation measures that the competent authority will analyse and approve through an authorisation.

The 'certified' category is a category of UA operation that, considering the risks involved, requires the certification of the UAS, a licensed remote pilot and an operator approved by the competent authority, in order to ensure an appropriate level of safety.

Meanwhile, JARUS facilitates harmonisation of standards within the EU Member States and other participating authorities.

A major progress in the second half of 2018 is the publication on the 22nd August 2018 of **Regulation (EU) 1139/2018**[102] ([ND30]). This is the **new Basic Regulation**, which repeals the previous one, Regulation (EC) No 216/2008 ([ND15]) and shall be complemented by delegated and implementing acts by the Commission.

After the entry into force of the **new aviation safety Basic Regulation** [ND30] on 11 September 2018, important steps include the adoption of **Delegated and Implementing Regulation**, published in June 2019 ([ND31] and [ND32]), containing technical and operational requirements for drones. These rules will replace any national rules on drones that may currently exist in the different Member States. The EU regulation will be applicable in one year to give Member States and operators time to prepare and implement it. As of June 2020, operators of drones will need to register in the Member State where they have their residence or their main place of business. The European Commission is also developing an institutional, regulatory and architectural framework for the provision of U-space services, which aim to enable complex drone operations with a high degree of automation. Finally, a systematic review of all existing EU aviation rules is progressing to identify the necessary changes to improve applicability to drone operations.[103]

A major milestone in the regulation of UAS in Europe was achieved on 10th October 2019 (**Figure 4.2.1**) with the publication of **ED Decision 2019/021/R**[104] issuing Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) No 2019/947 'Rules and procedures for the operation of unmanned aircraft' (the 'UAS Regulation').

In November 2019, EASA has published the **Opinion No 05/2019** "Standard scenarios for UAS operations in the 'specific' category"[105] which is proposing amendments to the new European Drone Rules. The Opinion covers two standard scenarios to facilitate some UAS operations posing a low risk in the specific category, namely Urban VLOS and Rural BVLOS above control ground area operations. For those, drone operators will be allowed to just send a declaration to the respective authority instead of applying and waiting for an authorization.

[102] https://www.easa.europa.eu/document-library/regulations/regulation-eu-20181139

[103] https://ec.europa.eu/transport/modes/air/news/2019-05-24-rules-operating-drones_en

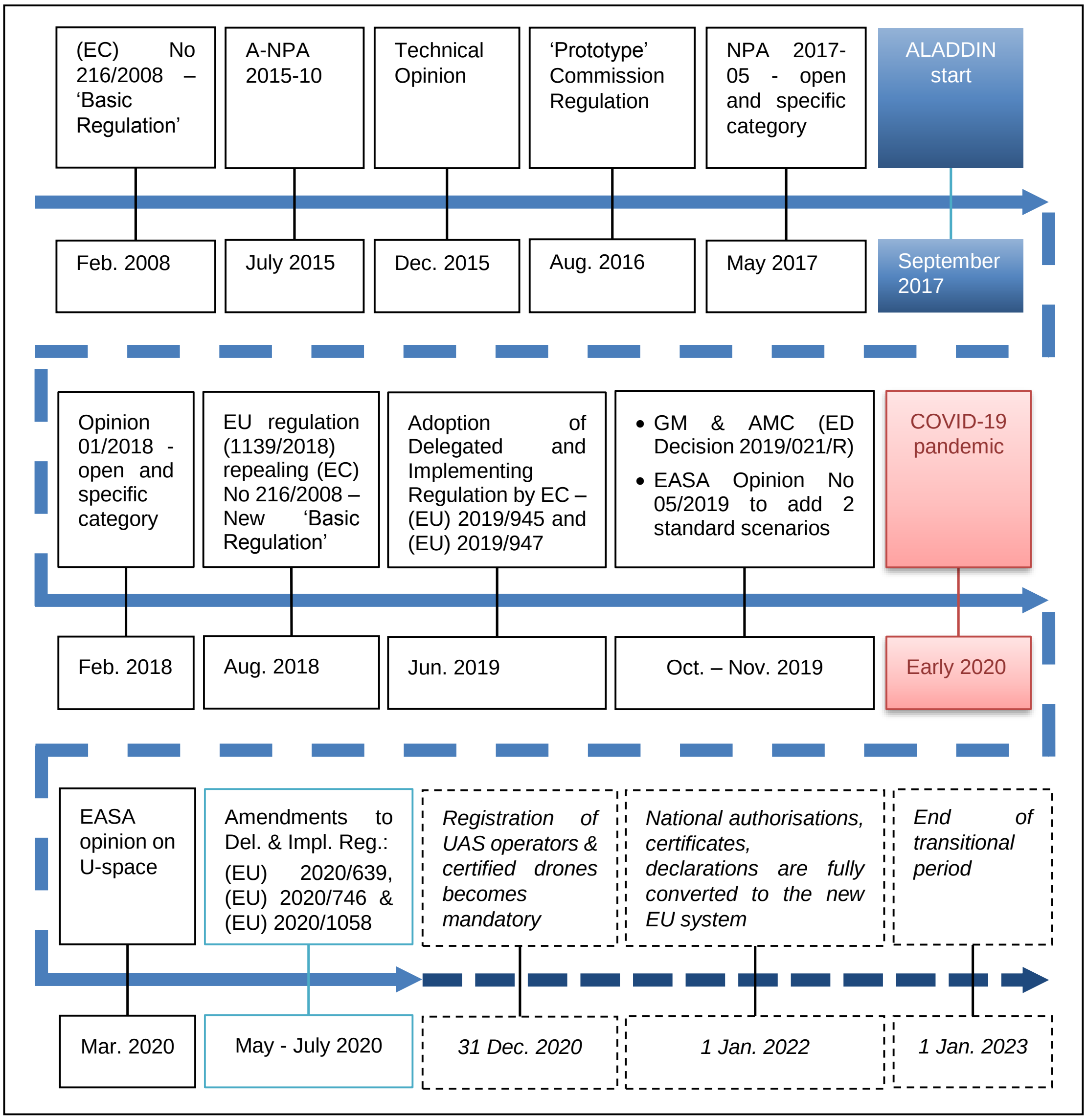
[104] https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2019021r 10 October 2019

[105] https://www.easa.europa.eu/document-library/opinions/opinion-052019 7 November 2019

Amendments to the EU drone regulation have been issued in May - July 2020 to include the above-mentioned two standard scenarios, along with postponing dates of application of certain measures in the context of the COVID-19 pandemic, namely: **Commission Implementing Regulation (EU) 2020/639** ([ND35]) and **(EU) 2020/746** ([ND36]) and **Commission Delegated Regulation (EU) 2020/1058** ([ND37]).

According to the updated EASA timeline[106], the **Opinion on U-space** by EASA (originally expected by December 2019) has been published on 13th March 2020.

The new EU 'UAS Regulation' will become gradually applicable starting from a year after publication (1st July 2020). By January 2023, the transitional period will be completed and the regulation will be fully applicable.



106 https://www.easa.europa.eu/drones-regulatory-framework-timeline

Figure 4.2.1: Evolution of EU drone regulation (August 2020)

At **national level**, European Member States are mainly focusing on increased restrictions close to airports in order to prevent disruptions to ordinary air traffic similar to those caused by the drone sightings at Gatwick and Heathrow in UK and Adolfo Suárez Madrid-Barajas in Spain, while preparing for national implementation of the provisions of the new EU regulation. In United Kingdom two executive orders, i.e. *Air Navigation amendment Order 2018 and 2019*, amend previous provisions mostly related to the remote pilot and operator of a small unmanned aircraft (SUA) and extend the flight restriction zone at and around protected aerodromes. In Spain, a drone regulation has been published in December 2017 and a calendar has been established for the transition from the national regulation to the European law. In Portugal, decree-law 58/2018, published on 23 July 2018[107], defines rules for the use of unmanned civil aircraft systems, known as drones, until the full transition to the European law. In Italy ENAC (the Italian Civil Aviation Authority) keeps updating its drone regulation to adapt to the legislative evolution in the Community context. On 21 May 2018, ENAC approved amendment 4 of the edition 2 of the Regulation on “Remotely Piloted Aerial Vehicles”. The intent was to anticipate a forecast of the next European regulation that places the operations in “specific” category in standard scenarios into the “Declaration” regime. On 11 November 2019, ENAC published the third edition of the Remotely Piloted Aircraft Regulation, now replaced by amendment 1 of the edition 3 of 14 July 2020, in order to integrate some requirements deriving from the European Regulations, such as the registration of the drone operator and the obligation of marking the single drone. A more extensive analysis of the current drone regulation at National level for some countries relevant to the ALADDIN project can be found in D3.1 [AD2] and D3.2 [AD17].

4.2.2 Electromagnetic emissions

Concerning **electromagnetic emissions**, ALADDIN partners performed a review of European and national product regulation that apply to jamming devices and likely also to other technologies involving electromagnetic emissions for detection, neutralization or communications (radar, RF, C2). Applicable European Regulation include the EMC, LVD and RED directives ([ND12], [ND28] and [ND9]). In addition, Directive 2013/35/EU ([ND29]) lays down minimum requirements for the protection of workers from risks to their health and safety arising from exposure to electromagnetic fields during their work. There are still the major concerns stated in the first version of this deliverable ([AD3]):

- For radars, the lack of specific regulation (and standards) concerning electromagnetic emissions for the particular application of drone detection and whether, as a public security service, it would fall outside the scope of the RED Directive 2014/53/EU ([ND9]);
- For jammers, their ambiguous legality in European legislations (see D3.1 [AD2]) and in National regulations. For instance, in France, there is a principle of general prohibition of jammers. Nevertheless, according to the ANFR, these

[107] https://dre.pt/web/guest/home/-/dre/115740753/details/maximized?res=en

activities are authorized exclusively for the purposes of public order, defense and national security, or the public service of justice.

4.2.3 Privacy and personal data protection

Concerning **Privacy and personal data protection**, in Europe the most notable event is the entry into force on 25 May 2018 of the **General Data Protection Regulation** (**GDPR**) - Regulation (EU) 2016/679 ([ND13]). Useful initiatives, like the *DroneRules PRO* project, will help creating a privacy culture among Europe's UA professionals, by producing and making available to the public their e-learning course and other resources on privacy and data protection, which will be useful also to the C-UAS community.

In 2020, the regulatory debate on privacy and data security in relation to drones is very topical. Experts point out that data security is the critical foundation for Remote ID of drones, which is one of the main current topics in the rulemaking process in Europe and USA. The recent COVID-19 pandemic, which has given greater powers to the police and governments including the use of surveillance drones, rises concerns about the possibility of removing privacy rights and that previous clearly-drawn lines around privacy and security are starting to become blurred.

4.2.4 Preventing and countering the UAV threat

Concerning the legislative grounds on **Preventing and countering the UAV threat**, in Europe the use of *detection technology* by law enforcement for the detection of the criminal use of drones may be exempted from the field of application of the GDPR by Recital 19. Instead, such use may fall under the ambit of **Directive (EU) 2016/680** (**Police and Criminal Justice Data Protection Directive**), which covers the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regarding the use of *neutralization technologies*, most regulations are not at the European Union level because matters relating to public security are generally within the competence of member state law. The legal regimes allowing state authorities to make use of otherwise banned technologies (radio frequency jamming, for instance) may vary significantly between countries.

Outside Europe, the regulatory debate on countering crimes using unmanned aircraft systems (UAS) became very topical in the United States after the **bipartisan Preventing Emerging Threats Act of 2018** (S.2836)**,** introduced in May 2018. Against the request for higher power to the Department of Homeland Security (DHS) and the Department of Justice (DOJ) for countering the UAS threat, advocates of the American Civil Liberties Union (ACLU) oppose granting the government broad authority to strike drones pre-emptively, on the basis that this could harm the rights to protect property and privacy. In August 2020, the US Government has issued an advisory document providing guidance on the legal framework applicable to counter drone technology in the US. Specifically, this advisory addresses two categories of federal laws: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does *not* address state and local laws, nor potential civil liability flowing from the use of UAS detection and mitigation technologies.

In the United Kingdom, the *Air Traffic Management and Unmanned Aircraft Bill* (2019) will give more power to the Police for countering the drone threat in UK. This Bill is not scheduled to become law until 2021.

In European countries it is likely that the recent escalation of the drone threat, as publicly demonstrated by the serious incidents of drone sighting at Gatwick, Heathrow and Adolfo Suárez Madrid-Barajas airports, will likely trigger tougher regulation and heavier restrictions with impacts on Privacy and personal data protection.

5 SOTA progress

This chapter reports a state of the art (SOTA) analysis and main (hardware or software) technological progress relevant to the detection and neutralization of UAVs either as individual components or as integrated counter-UAV systems, with particular reference to those involved in the ALADDIN platform concept (**Figure 2.2.1**), namely those concerning:

- Sensor technology (radar, optical, thermal and acoustic sensing, with relevant data processing techniques);
- Effector technology (jamming, hacking/spoofing and physical neutralization)
- Command and Control (C2) and Support to Operations sub-systems
- Complete counter-UAV systems, involving combination of the above components.

Starting from the situation at beginning of the ALADDIN project (§ 5.1), this chapter aims at monitoring the technological evolution through the project lifetime (§ 5.2).

This report does not generally include prices for C-UAV equipment or subsystems, unless retrieved from public sources (e.g. the price of AUDS, around € 900,000, included in paragraph 2.3.1.1). The inclusion of prices is actually quite delicate for several reasons:

1. It's difficult (not to say impossible) to obtain detailed prices or even rough order of magnitude (ROM) prices for counter-drone systems or for equipment involved in building C-UAV systems: they are specific, and unless you are a potential buyer, the companies don't publish their price.
2. There are price lists – sometimes – for standard equipment. However, there are generally negotiations and the final price may differ significantly from the price list: hence, this does not reflect correctly the real situation and any comparison or reference is biased.

Despite the reviewers' recommendation at Reporting Period 1 to include prices into the SOTA report, finally the Project Officer in consultation with the evaluators accepted ALADDIN approach for limiting the recommendation to **public prices** in the SOTA report or in the Exploitation Plan D2.13 – Business sustainability strategy V2. As suggested, the upcoming D2.13 will take into account some news of public bids of airports wishing to install counter-drone equipment. This can give an idea of the global cost, which is not the same as the individual price per equipment, but can help to better situate the SOTA market.

5.1 Introduction

In recent years, there has been an exponential proliferation in the civilian market of small UAV (sUAV), often called mini-drones. As shown in § 2.1, the highest growth potential is expected for the segment of mini UAV with a maximum take-off mass of less than 25 kg, thanks to their low investments, low operational costs, low risk potential for innocent bystanders, easy handling characteristics and unique sensing capabilities.

Unfortunately, this is coupled with a potential increase in their use for illegal purposes, including terrorist activities (§ 2.1). Mini-UAV threat appeared as important in 2014. Since then, different counter-UAV (C-UAV) solutions appeared on the market, mainly from defence systems manufacturers:

- Single domain solutions (or 'subsystems') focused on one aspect of countering the threat, mainly radio-frequency piloting and jamming of the UAV communication links. Other solutions focused only on detecting the threat, mainly through radar and/or electro-optical/infrared (EO-IR) sensors.

- C-UAV systems are based on integration of sensor, tracker/identifier, and jammer.

The needs to have a seamless, tightly integrated C-UAV system are shared by worldwide end-users. However, most **military C-UAV systems** are not suited for the civilian security sector, since they are generally cumbersome, costly and high-emission devices intended for large UAVs, using specialized radar and occasionally Infrared (IR) technology for UAV detection. Additionally, military countermeasures include both ‘hard kill’ effectors - Missiles, Shotguns, Directed Energy Weapons (DEW) including Laser and High-Power Microwave (HPM) - and ‘soft kill’ Electronic Counter-Measures (ECM), like jamming and spoofing. Most of the military neutralization effectors (such as missiles, high-power lasers, or powerful jamming devises) are of questionable legality or completely unacceptable from the Societal, Ethical and Legal perspective in the civilian security sector.

In the same time, some countries have launched R&D programs in order to fill the gap in efficient **counter-UAV systems for civilian application**. However, the market is not very large, preventing further developments, except for companies involved in R&D programs. The situation can be summarised as follow:

- The threat is evolving very quickly, with commercial devices increasingly powerful and sophisticated, posing problems to counter devices. Additionally, terrorist organisations are able to tune commercial equipment or to build homemade unmanned vehicles. Consequently, threat is mainly unpredictable.
- For countering this threat, single domain equipment is not enough. However, these partial solutions could be integrated in systems.
- The large variety of scenarios requests a very flexible solution, able to accept different sensors – different regarding performances, domain or number - and effectors.

The ALADDIN consortium aims to build the solution able to meet such needs, while seizing the business opportunity and confirming European technical leadership in the security domain.

5.1.1 Counter-UAV technology status in 2017

This paragraph provides an overview of the state of the art of C-UAV systems and subsystems appeared on the market until December 2017, as well as technological and scientific progress in related fields including data processing and data fusion.

In this section, unless stated otherwise, the term ***‘detection’*** is used in a broad sense, as the functionality aimed at revealing (sensing) the presence of a potential threat (drone) and possibly, but not necessarily, also localizing, tracking and/or classifying it. In the same broad sense are used also the terms ‘detector’ or ‘sensor’.

Also the term ***‘neutralization’*** is used in a broad sense, as the functionality aimed at mitigating the threat, either through ‘soft’ countermeasures, to make the UAV harmless without destroying it, or through ‘hard’ means, by severely damaging or even destroying it. In the same broad sense is used also the term ‘effector’.

Equipment covering just one of these functionalities, only detection or only neutralization, are termed **single-domain** C-UAV solutions or **sub-systems**, regardless of the type and number of components (sensors or effectors employed) and of the presence/absence of additional functions to command and control (C2) them. Equipment covering both functionalities, detection and neutralization, and usually provided with C2 functions to handle their mutual interaction, are termed C-UAV (integrated) **systems**.

5.1.1.1 Comparison of typical C-UAV sensor technology

Various public sources[108] present qualitative **performance comparison** of typical C-UAV sensor technology, evidencing how **multi-sensor** equipment outperforms single-sensor solutions overcoming the weaknesses of the individual sensors. The major drawback of multi-sensor solution is, of course, the increased complexity and costs. A quick overview of the underlying principles and main shortcomings in UAV detection is provided below, together with a qualitative performance comparison of typical C-UAV sensor technology (**Table 5.1.1**), although strict comparison cannot be performed without accounting for the specific characteristics and configuration of each sensor.

Table 5.1.1 Qualitative sensor performance comparison

	Acoustic	Electro-Optical	Thermal-Infrared	Passive RF	Radar
Detection (1)	Poor < 0.1 km	Fair < 1 km	Fair < 1 km	Fair < 1 km	Good ~ 5 km
Tracking (2)	Poor	Fair	Fair	Good	Good
Classification (3)	Poor	Fair/Good (in favourable visibility conditions)	Fair	Fair	Fair
Localization (4)	Poor	Fair	Fair	Fair	Fair/Good (2D/3D radar)
All weather / Day & night	Fair	Poor	Fair	Fair	Good
Autonomous target	Good	Good	Good	Poor	Good
Comments	(1) Typical detection ranges for mini-UAVs (2) EO-IR cameras typically require cue from another sensor (3) Only certain classes of RF passives can be classified (4) Localization accuracy highly dependent on sensors type and configuration				

Acoustic methods. Audio detection generally consists of monitoring external sounds and comparing them against a database of known UAV audio signatures. However, this method suffer from very short detection range (usually no more than 100 m) and

[108] See, for instance: https://anti-drone.eu/blog/anti-drone-publications/anti-drone-system-overview-and-technology-comparison.html; https://www.helpnetsecurity.com/2015/05/28/drone-detection-what-works-and-what-doesnt/; http://gryphonsensors.com/products/

can be unreliable in a noisy environment such as urban areas. Networking many (sophisticated) audio sensors allows localization and tracking of the sound source, which may be unfeasible or poorly reliable with basic sensors. Additionally, audio classification cannot guarantee reliable results due to the difficulty of building a huge database of UAV audio signatures and the risk of deception if UAVs are modified with custom propellers and engines, which would affect their audio signature.

Electro-Optical methods. Video detection uses cameras to locate moving aerial objects and attempts to differentiate UAVs from other flying objects (such as birds or other aircraft) based on size, flight path and style of movement. The main limitation is the strong susceptibility to light and weather conditions, which makes video detection useless in night hours and in foggy/rainy/smoky conditions. Although VLOS operation makes 'legal' UAVs unlikely to fly in such conditions, adverse conditions might not prevent criminal UAVs to fly, especially if suitable for autonomous operation. Even for sophisticated cameras, equipped with leading-edge processing algorithms, typical detection range do not exceed 1 km, with even shorter ranges for tracking and classifying the flying targets. Apart for panoramic devices, which continuously scan the surrounding sky, cameras typically require cue from another sensor to point in the direction where a possible target has been detected in order to perform deeper video analysis/classification of the potential threat. Even by utilizing computer algorithms that look at flight patterns, distinguishing birds from drones might be a difficult task for EO sensors.

Thermal-Infrared methods. These methods use special infrared cameras to identify the heat signature of a UAV or any other flying object. Based on thermal emissions, they are unaffected by bad weather/light conditions and hence are commonly used to complement video detection and classification. In most cases, video and thermal sensors have similar detection ranges. Thermal detection might be useful to detect larger UAVs that would typically need gas-powered engines to carry larger payloads, thus producing plenty of heat. However, thermal detection might fail in detecting very small UAVs, such as recreational drones, which have a minimal heat signature due to the construction in plastic and the use of electric motors. Due to higher heat radiated, thermal detection would pick up birds more readily than mini drones in most cases. Hence, these methods may aid the classification by detecting the heat of living creatures (birds) and distinguish them from UAVs having low thermal emission.

Radio Frequency (RF) methods. RF detection involves the monitoring of the frequencies used for UAV transmissions, typically 2.4 GHz and 5.8 GHz. Manufacturers of RF detection devices claim that this technology is the most effective way to detect drones (and discriminate them from birds), within fairly long distances (~500 m). Additionally, RF sensors would allow to gather enough data (GPS coordinates of the drone and pilot, unique identifier of the drone) to not only find the drone but to find also its operator, providing evidence for criminal prosecution. The main disadvantage of RF detection is that it is useless if the drone flies by waypoints. Therefore, although effective for prosecuting 'negligent' UAVs flying over restricted areas, this technology would be of little use for detecting 'criminal' UAVs employing different radio frequencies than those allowed by regulation or autonomous UAVs not relying on communication with the remote pilot.

Radar methods. Radar detection is based on recording the radio waves (in suitable frequency bands of the electromagnetic spectrum) emitted by transmitting antennas and reflected back by a remote target toward the receiving antennas. Sophisticated radar signal processing allows the extraction of geometric information for the localization of the detected target as well as other possible characteristics of the received signal useful for deeper analysis and classification purposes. The type and amount of information retrieved depend on a number of factors, involving both the sensor architectural design and the algorithms implemented. In particular, this technology can provide range and angular position of the potential target only in azimuth for 2D radars and both in azimuth and elevation for 3D radars. Some radars can also provide information on target velocity. Radar is the traditional sensor for detecting flying vehicles. However, radars designed for detecting standard (manned) aircraft, with relatively large radar cross-section (RCS) and high velocity, are not suitable for detecting very small and slow moving objects such as UAVs. Therefore, specifically designed radars are needed for this challenging application, ideally requiring 360-degree continuous coverage. Compared to other technologies, radar is in principle the only one able to provide long-range detection (from a few kilometres to tens of kilometres, depending on the target RCS) and almost unaffected performance in adverse weather conditions. Additionally, using advanced signal processing techniques can differentiate between birds and UAVs.

Other methods. Some of the drones are operated using Wi-Fi and many of the low-end commercial UAVs have identifiable SSIDs and MAC addresses, which are broadcast. Hence, using the latest technologies for **Wi-Fi detection** it is possible not only to detect the drone, but also take over the control. Despite the small market share of Wi-Fi operated drones (compared to the standard 2.4 GHz), combining this method with other detection technology (e.g. RF) creates additional protection from the drones.

However, most of the additional detection methods advertised in public sources, especially the low-cost and short-range ones, seems concerned with private property protection against drone intrusion rather than detection (and countering) of malicious drones with criminal or potentially terroristic intent.

5.2 SOTA progress report (August 2020)

After presenting the situation at beginning of the ALADDIN project (§ 5.1), this paragraph aims at monitoring the technological evolution through the project lifetime, by providing an overview of the state of the art of C-UAV systems and subsystems appeared on the market, as well as technological and scientific progress in related fields including data processing and data fusion.

5.2.1 Counter-UAV systems

5.2.1.1 Reviews of Counter-UAV research and technology

This paragraph introduces the main sources of information used to retrieve the relevant data presented in subsequent paragraphs in relation to C-UAV systems and subsystems on the market. It summarizes the main outcomes of recent reviews of Counter-UAV research and technology, including:

- **2015 Sandia Report** [BD58],
- CSD study 1st edition (Feb. 2018), named **2018 CSD report** [BD59] and 2nd edition (Dec. 2019), named **2019 CSD report** [BD99],

- a paper published in June 2017 as part of the H2020 SafeShore project ([BD60]),
- a scientific publication by Nassi et al. 2019 ([BD84]), which describes new societal threats to security and privacy created by drones and presents academic and industrial methods used to detect and disable drones,
- a review by ALADDIN partner CERTH (Samaras et al. 2019 [BD100]) on Deep Learning methodologies for C-UAV application.

Freely accessible reports on C-UAV detection and neutralization technologies include the **2015 Sandia Report** [BD58] published by the Sandia National Laboratories (USA) and the **2018 CSD report** [BD59] published by the Center for the Study of the Drone at Bard College (USA). The second edition, published in December 2019 (**2019 CSD report** [BD99]) includes latest updates on the worldwide market of Counter-Drone Systems with a special mention to the ALADDIN project. *This second edition of "Counter-Drone Systems" provides background on the growing demand for C-UAS technology, describes how the technology works, presents our database of known C-UAS products from around the globe, and explains some of the challenges surrounding counter-drone technology use.* Although referring to worldwide manufactured equipment, the above market surveys are mainly oriented to the American market.

A scientific paper focusing on ***Counter Remotely Piloted Aircraft Systems*** (C-RPAS or C-UAV) was published in June 2017 as part of the H2020 SafeShore project ([BD60]). It provides an overview of the various issues (legal, technological, etc.) of C-RPAS systems: *The designing process of an effective Counter Remotely Aircraft System needs to benefit from a systemic approach, starting from the legal aspects, and ending with the technical ones. From a technical point of view, the system has to work according to the five "kill chain" model starting with the detection phase, going on with the classification, prioritization, tracking and neutralization of the targets and ending with the forensic phase.*

In the paper' Figure 1 the authors propose a conceptual C-RPAS architecture, while in their Figure 2 they propose a flowchart for detection, classification and risk level assessment, including as essential block the data fusion and processing module. *Once information about a potential target has been acquired by one or multiple sensors this information is sent to a specialized module for intelligent fusion and processing, target validation and alarm generation.*

Furthermore, in the paper' Table II (reproduced in **Table 5.2.1**) they compare the effectiveness of current sensors used as detection options for the three types of RPAS or flying objects (Glider, Quadcopter, Jet turbine) evaluated by the Sandia National Laboratories in the already cited 2015 Sandia Report [BD58].

Table 5.2.1 Effectiveness of current sensors used as detection options ([BD60])

TABLE II. EFFECTIVENESS OF CURRENT SENSORS USED AS DETECTION OPTIONS

Sensor	Remarks	Flying objects		
		Glider	Quadcopter	Jet
Active radar	The radar cross section (RCS) for two small commercially available platforms was measured to be -15dBm2 and is theorized to be -30dBm2 if the RPA is constructed with an RF transparent material [4].	Poor	Mild	Between poor and mild
Passive radar [8]	It uses existing "electro smog" generated by GSM or WiFi systems as a source of illumination. It could be effective for large surfaces [8].	Mild	Mild	Mild
Passive optics (video, thermal or infrared cameras)	Imaging commercially available quadcopters with EO/IR visible, MWIR, and LWIR resulted in low contrast images, and the amount of data required to provide a reasonable response time is very large [4].	Mild	Mild	Between poor and mild
Active optics (LIDAR)		Mild	Mild	Poor
Acoustics	Acoustic detectors were successfully demonstrated and identified a UAS from 25 meters at an elevation of 10 meters using a microphone array [4]. Last projects relieve that acoustic sensors through an effective acoustical sensor network could detect commercial drones (DJI Phantom Drone) up to 300m [7].	Poor	Mild	Mild
EM emissions	RF detection is promising since currently available COTS RPAS technology requires a transmission and receive signal from a human user [13]. On the other hand, the detection of RF becomes highly complicated if a RPAS uses open source software or is programmed to require no human interaction.	Mild	Mild	Between poor and mild
B-field detection	Disturbances within the magnetic field around a RPA has potential to be detected, but it is dependent on the materials used and the physical size of the system.	Poor	Poor	Poor

A scientific publication by **Nassi et al. 2019** ([BD84]) describes new societal threats to security and privacy created by drones and presents academic and industrial methods used to detect and disable drones. In the paper, the authors provide a comprehensive review of *Threats, Challenges, Solution Mechanisms, and Scientific Gaps*, including also aspects that are missing in previous reviews, such as the challenges that arise from allowing drones to fly over populated areas.

> *In our SoK, we review 120 methods proposed by the academic and industrial sectors that were designed to detect and disable drones flying in areas where drone presence is restricted, as well as areas where drones are allowed. We compare the methods' effectiveness at drone detection. We also present the scientific gaps that exist as a result of allowing drones to fly over populated areas and discuss future research directions.*

The paper includes interesting tables, such as Table IV with threats mapped to types of drones (**Figure 5.2.1**) and Table VI (**Figure 5.2.2**), listing ALADDIN partner HGH Infrared Systems among the companies manufacturing commercial devices for drone detection.

The paper is cited in an article of SmartCitiesWorld website[109]:

> *An open-skies policy that allow drones to fly over populated areas pose significant risks in terms of security and privacy within society, a new study warns. And without additional safeguards, could result in attacks by malicious entities and be exploited for use in cyber-attacks, terrorism, crime and invasion of privacy.*

[109] "Drones pose cyber-security and privacy threats, says report", 28 March 2019, https://www.smartcitiesworld.net/smart-cities-news/smart-cities-news/drones-pose-cyber-security-and-privacy-threats-says-report-4014

TABLE IV
THREATS MAPPED TO TYPES OF DRONES

	Privacy		Physical Attacks	Crime	Cyber Attacks
	Video Streaming	Carrying Surveillance Equipment			
Nano	✓		Targeted assassination [45]	Targeting homes for burglaries [46]	
Micro	✓	3D mapping using radio transceiver [47] MITM attacks against cellular networks [48] Tracking a person according to his/her devices [49]	Carrying radioactive sand [50]	Smuggling goods into prison yards [12]	
Mini	✓	✓	Carrying a bomb [16]; colliding with an airplane [51], [52]	Hijacking radio controlled devices [53], [24] Smuggling goods between countries [13], [14], [15]	Establishing a covert channel [54], [55]
Swarm	✓	✓	Multiple casualty incidents [56]	Cyber warfare [57]	

Figure 5.2.1: Threats mapped to types of drones (Source: Nassi et al. 2019)

TABLE VI
CHARACTERISTICS OF COMMERCIAL DEVICES FOR DRONE DETECTION

		Radio		Optical				Acoustic	Features				
Company Name	Product Name	Radar	RF Scanner	Camera	LiDAR	Electro-optical Camera	Thermal	Microphone	Detection Range (KM)	Identification	Angle	Locating	Mobility
3DEO	Rogue Drone Detection & Mitigation [103]				✓				2			✓	
Aaronia	Drone Detection System [82]	✓		✓			✓		50	✓		✓	✓
Anti-Drone.eu	GROK [83]	✓							4	✓		✓	
	Droneshield [104]							✓	0.5				
Aveillant	Gamekeeper 16U - Holographic Radar [84]	✓							5			✓	
Black Sage - BST	UAVX [85]	✓		✓			✓		0.5		90	✓	✓
C speed LLC	LightWave Radar [86]	✓										✓	
CACI	SkyTracker [105]		✓							✓			
CerbAir	DroneWatch [106]		✓						1			✓	✓
Chess Dynamics Ltd	AUDS [87]	✓				✓	✓		10		180	✓	✓
DeDrone.com	DroneTracker [107]		✓	✓						✓			✓
DeTect	DroneWatcher [108]		✓						1.6-3.2	✓			✓
	HARRIER DSR [88]	✓		✓				✓	3.2	✓		✓	
Digital Global Systems	SigBASE [109]		✓										✓
DroneShield	FarAlert/WideAlet Sensors [110]						✓	✓	1		30		✓
Gryphon Sensors	Skylight [89]	✓	✓			✓	✓		3-10		360	✓	✓
HGH Infrared Systems	UAV Detection & Tracking [111]			✓	✓		✓				360		
Kelvin Hughes Limited	SharpEve SxV Radar [90]	✓		✓			✓		1.5		360	✓	✓
MAGNA	Drone Detection [112]			✓			✓	✓	0.5-1				
Microflown AVISA	Skysentry AMMS [113]		✓					✓	0.4-1		360	✓	
Mistral Solutions	Drone Detection and Classification System [114]		✓	✓			✓		1	✓			
ORELIA	Drone-Detector [115]							✓	0.1		360		
Quanergy Systems	Q-Guard - LiDar X-Drone [116]				✓				0.1				
Rinicom	SKY PATRIOT [117]			✓		✓	✓		0.8	✓			
Rinicom and METIS Aerospace	SKYPERION [118]		✓					✓					
ROBIN Radar Systems	ELVIRA [91]	✓		✓								✓	✓
Rohde and Schwarz	R&S ARDRONIS-I [119]		✓						1-2	✓			
SAAB Group	Giraffe AMB Radar - ELSS [92]	✓							30-470		360	✓	✓
Sensofusion	AIRFENCE [120]		✓										✓
SpotterRF	A2000 Radar UAVX [93]	✓							0.2-1		45/90	✓	✓
Squarehead Technology	DiscovAir [121]							✓					
TCI International	BlackBird [122]		✓										✓
Thales	SQUIRE [94]	✓					✓		48			✓	✓

Figure 5.2.2: Characteristics of commercial devices for drone detection (Source: Nassi et al. 2019)

Amongst the latest reviews of C-UAV research and technology, it is worth mentioning a scientific paper by ALADDIN partner CERTH, published in November 2019 on MDPI Sensors journal ([BD100]). The scientific publication by **Samaras et al. 2019** ([BD100]) provides a systematic review of Deep Learning on Multi Sensor Data for Counter UAV Applications, which is one of the emerging research topics in this field.

In the introduction, the paper declares that *recent advances in counter UAV (c-UAV) solutions offer systems that comprise a multi-sensory arsenal in an effort to robustly maintain situational awareness and protect a critical infrastructure or an important event.*

Characteristics

Detection Methods	Range	Position accuracy	Classification	Autonomous targets	Multiple targets	Low visibility conditions	Price
Human surveillance	**	***	*****	✓	✗	✗	****
Passive Electro-optical/infrared	***	****	****	✓	✗	✗	*
Acoustic	*	**	**	✓	✓	✓	***
Active Radar	****	****	***	✓	✓	✓	**

Figure 5.2.3: Comparison of key characteristics between individual components of counter-UAV systems (Source: Samaras et al. 2019)

The authors show a comparison of key characteristics between individual components of counter-UAV systems (**Figure 5.2.3**), pointing out that most of the state-of-the-art C-UAV systems do not exploit their full potential.

A considerable drawback in multi-sensory c-UAV applications is that the information from the different sensors is not fused to produce a result but instead the alert signals are used independently from each system component to provide multiple early warnings that are later confirmed by a human operator. [ ] The system can be fully automatic by leveraging recent advances in data fusion techniques without a considerable trade off in classification capability. Data fusion techniques have gathered significant attention in recent years mainly due to the interest of combining information from different types of sensors for a variety of applications.

Along with the soaring of research publications related to UAV detection and classification over the past few years (from 10 in 2015 to over 90 in 2019 based on Google scholar's search), there is an increasing interest in the use of deep learning based methodologies to tackle multi-sensor learning tasks for generic objects.

Yet applying deep learning for UAV detection and classification is considered a novel concept. Therefore, the need to present a complete overview of deep learning technologies applied to c-UAV related tasks on multi-sensor data has emerged. The aim of this paper is to describe deep learning advances on c-UAV related tasks when applied to data originating from many different sensors as well as multi-sensor information fusion. This survey may help in making recommendations and improvements of c-UAV applications for the future.

5.2.1.2 Commercial C-UAV systems

The evolution of worldwide C-UAV market is monitored by looking at the above-mentioned C-UAV reports and (scientific) reviews, as well as specialized websites.

The **2015 Sandia Report** [BD58] lists the detection technologies more frequently used to detect and identify low, slow, and small (LSS) unmanned aerial systems (UAS) and discusses their positive and negative attributes. In 2015, the Sandia Report lists 10 manufacturers/sellers of detection and identification products.

At the beginning of 2018, the situation has evolved a lot, with a stratospheric expansion of the C-UAS market sector in the latest three years, according to the **2018 CSD report** [BD59]. To grasp the scale and form of the counter-drone market, the researchers assembled a comprehensive database of publicly known counter-drone systems consisting of 235 products sold by 155 firms and partnerships from 33 different countries. This list includes both systems that are on the market and systems that are in active development, as well as existing products designed for other purposes (such as Doppler radars) that have been retooled for C-UAS.

In the second edition, published in December 2019 (**2019 CSD report** [BD99]) the author states: *Today, less than five years later* (after the **2015 Sandia Report** [BD58]), *we have tallied as many as 537 systems on the market. In that interim, the technology itself has also advanced considerably and the knowledge-base for how to employ it has matured. However, significant challenges remain unsolved.*

An overview of C-UAS products listed in the two editions of the **CSD Report** ([BD59] and [BD99]) is included in **Table 5.2.2**.

Table 5.2.2 Overview of C-UAS products listed in the CSD Report

C-UAS products at-a-glance	1st edition (February 2018)	2nd edition (December 2019)
Number of Products	235	537
Number of Manufacturers	155	277
Countries of Origin	33	38
Systems for Detection Only	88	175
For Interdiction Only	80	214
For Detection and Interdiction	67	138

As the author says, the difference in the two editions does not represent absolute growth in the sector: 24 products and 9 manufacturers were removed from the original database because they no longer appear to be active, while a small number of products in the new database appear to have already been on the market before February 2018.

The database does not include software products, such as command and control products that are used to manage incoming data from sensors.

As in previous analysis, RF and radar are the most common detection elements, followed by EO and IR systems, which are usually used in conjunction, whereas Jamming (both RF and GNSS) is the most common interdiction method.

In addition to the comprehensive reports mentioned earlier, a further source of useful information is the website: **Unmanned Airspace**[110], the information portal for unmanned air system traffic management (UTM) and counter-UAS (C-UAS) systems. Interesting news are continuously reported in the section *Counter-UAS systems and policies*[111], including mention to the 2018 CSD report.

Additionally, in the *Counter-UAS industry directory*[112] the Unmanned Airspace website lists major global equipment manufacturers, with outline product and contact information. The May 2018 issue[113] lists over 140 products from over 130 suppliers of counter UAS equipment: most of them are included in the 2018 CSD report, whereas nearly 30 are new entries.

The November 2018 issue of the *Counter-UAS industry directory*[114] lists over 190 suppliers of counter UAS equipment: 140 of them were included in the previous issue (May 2018), whereas nearly 50 are new entries (although most of them are already included in the 2018 CSD report). Additionally, for a number of them the description has been updated with new product information, including information on where the systems are being used in service or displayed at exhibitions (such as Eurosatory 2018).

The August 2020 issue in the *Unmanned Airspace* counter-UAS directory[115] lists over 230 suppliers of counter UAS equipment and provides the latest update on C-UAS technologies that are available in the open market and research programmes in the public domain.

The survey highlights the growing dominance of US industry in this sector (especially in areas such as directed energy weapons research) and the emergence of new industries in Europe and Asia. Amongst European countries, UK, France and Germany are those with the most prolific and varied C-UAS industrial bases outside of USA, Israel and Russia. UK has apparently the most rapid growth, whereas new entries include India, Austria and Ukraine.

The August 2020 list of C-UAS manufacturers includes some ALADDIN partners:

- **CS Group** as manufacturer of *Boreades* high-performance scalable multi-sensor and multi-effector system.

---

[110] https://www.unmannedairspace.info/

[111] https://www.unmannedairspace.info/category/counter-uas-systems-and-policies/

[112] https://www.unmannedairspace.info/counter-uas-industry-directory/

[113] https://www.unmannedairspace.info/wp-content/uploads/2018/05/Counter-UAS-directory.-May-2018.-v1.docx.pdf

[114] https://www.unmannedairspace.info/wp-content/uploads/2018/11/Counter-UAS-directory.-November-2018.-v2.pdf

[115] https://www.unmannedairspace.info/wp-content/uploads/2020/08/Counter-UAS-directory.-August-2020.v2.pdf August 2020

- **IDS** as manufacturer of *Black Knight* UAV detection radar and partner, through its subsidiary IDS North America, with the US ***34 North Drones*** to offer the *NO-DRONE* counter drone system for the civilian market[116]. The NO-DRONE radar system can be upgraded with an optional "slew to cue" EO/IR turret and an RF detector to enhance drone tracking and identification capabilities.
- **HGH** as manufacturer of an improved version of the *Spynel-S* and *Spynel-X* long-range detection systems to meet the high demand for drone and micro-drone detection. Additionally, it is mentioned that ***MBDA*** had reportedly integrated HGH's Infrared tracking camera into its *Licorne* C2 lightweight and mobile air defence command and control system now with integrated anti-drone capabilities.

It is worth noting that on 16 June 2020 the **ALADDIN** project is mentioned in the *Unmanned Airspace* website. The article[117] announces *ALADDIN counter drone demo to include SkyWall Patrol net capture solution* by the UK firm ***OpenWorks Engineering*** during the forthcoming demonstration in Greece later in 2020 in the final phase of the programme[118].

The previous outcomes agree with the findings of the **Counter-Drone Market report 2020** that was recently presented by DroneII[119]. The report confirms that, after USA and Israel, the most active European countries in Counter-drone technology are UK and France. Additionally, 80% of the offered solutions include non-kinetic countermeasures, with nearly half of the counter-drone systems offering only interdiction, one third only detection and nearly 20% offering both detection and interdiction means.

5.2.1.3 ALADDIN project to address drone threat

The need for a military intervention in the crises of drone sightings at the UK airports in December 2018 and January 2019 (§ 2.3.1.1), as well as at Madrid-Barajas airport in Spain in February 2020, has evidenced a **gap in the civilian capacity to countering this emerging threat in an effective and holistic way**. This gap has been the motivation for the specific topic in the H2020 call, answered by the ALADDIN proposal.

Therefore, it is not a coincidence that, following the above events, ALADDIN project has received attention for the first time in the public awareness. On 9th January 2019 an article titled ***'ALADDIN project to address drone threat'***[120] has been published in the Defence & Security News of **Government Europa**, a web journal dedicated to EU Government Policy News.

---

116 https://www.unmannedairspace.info/counter-uas-systems-and-policies/34-north-drones-teams-with-ids-to-offer-counter-drone-system/ November 15, 2019

117 https://www.unmannedairspace.info/counter-uas-systems-and-policies/aladdin-counter-drone-demo-to-include-skywall-patrol-net-capture-solution/ June 16, 2020

118 https://openworksengineering.com/2020/06/17/skywall-patrol-integrated-as-part-of-aladdin-project-2020/ 17 June 2020

119 https://www.droneii.com/product/counter-drone-market-report-2020

120 https://www.governmenteuropa.eu/aladdin-project-drone-threat/91807/ 09/01/2019

The ALADDIN project – which stands for Advanced hoListic Adverse Drone Detection, Identification and Neutralisation – is funded by the European Commission through the Horizon 2020 research funding initiative. It intends to address the growing issue of drone misuse in crime and terrorism. The consortium administering the project consists of 18 technical, law enforcement and end user infrastructure partners from nine EU Member States: France, Germany, Greece, Italy, Poland, Portugal, Spain and the UK.

As production and procurement of drones has soared in recent years, so have incidents of airport disruption, threats to critical infrastructure and criminal activity involving drones. In December the UK's Gatwick airport was shut down for two days after drone sightings, disrupting 1,000 flights; yesterday saw Heathrow – the second busiest airport in the world – shut down for an hour over drone fears. The ALADDIN project was devised to assess emerging technologies and current developments in order to formulate a comprehensive anti-drone system to detect and neutralise potential drone threats.

As expected, the ALADDIN system has received higher attention in the media after the successful test and demonstration of ALADDIN Beta release at the Spanish Test Flight Centre ATLAS in early 2019. This fact is documented by the increased number of cites of ALADDIN in other websites and specialized press (included in D2.10 - [AD16]). An example is the article in the Spanish consultor **Sousa website**, dated 6/02/2019[121], highlighting the role of Spanish partners (FADA-CATEC, ACCIONA and especially Policía Municipal de Madrid), in the successful demonstration of ALADDIN beta release at ATLAS Test Centre in Spain. Additionally, also ALADDIN subsystems (sensor, neutralization and support components) are receiving the media attention, such as IDS' Black Knight radar. An example is the announcement in the Italian press[122] [123] [124]of the procurement of IDS' Black Knight radar by the Italian Air Force for the fight against the illegitimate use of drones, evidencing that Italy is "*among the leading countries in Europe in the fight against the threat of drones"*.

At the end of 2019, ALADDIN sets itself at the forefront of C-UAV research and technology, as demonstrated by recent appraisals in scientific publications and renowned reports, both by consortium member and external sources (such as the **2019 CSD Report** [BD99]).

It should be remembered that the systematic review on Deep Learning by **Samaras et al. 2019** ([BD100]), presented in § 5.2.1.1, is the result of the research efforts of the ALADDIN project, which aims to include in a holistic approach not only state-of-the-art multi-sensor and effector technology, but also leading-edge detection, classification and data-fusion methodologies.

---

[121] https://sousa79.webnode.es/l/aladdin-nos-ayudara-a-encontrar-al-genio-del-lhampadron/ ALADDIN, nos ayudará a encontrar al "GENIO DEL HAMPADRON", 06/02/2019

[122] https://www.lagazzettadelmezzogiorno.it/news/puglia-con-le-stellette/1097319/gli-scali-inglesi-investono-in-sistemi-anti-drone-italia-all-avanguardia-nel-contrastare-la-minaccia.html 04/01/2019

[123] http://www.aeronautica.difesa.it/comunicazione/notizie/Pagine/16-stormo-capacit%C3%A0-c-uos.aspx 04/01/2019

[124] http://spazio-news.it/ami-e-ids-il-16-stormo-rafforza-le-capacita-anti-drone 07/01/2019

An evidence of ALADDIN primary role in advancing scientific research is the workshop on **Vision-Enabled UAV and Counter-UAV Technologies for Surveillance and Security of Critical Infrastructures (UAV4S)**, organized by ALADDIN partner CERTH within the12th International Conference on Computer Vision Systems (ICVS 2019), held in Thessaloniki, Greece, in September 2019. Partners CERTH, IDS, FADA and HGH contributed with 5 papers on the main scientific results achieved within the ALADDIN projects, which have been published in the Conference proceedings **CVS 2019** as part of the **Lecture Notes in Computer Science** book series (LNCS, volume 11754)[125].

With regard to external sources, apart for the updated Counter-Drone Systems Database, the most interesting contribution of the **2019 CSD Report** [BD99] is the analysis of <u>challenges of countering drones</u>, both of technical and non-technical nature. These include:

- Detection Effectiveness
- False Negatives and False Positives
- Distinguishing Legitimate and Illegitimate Drone Use
- Response Window
- Interdiction Hazards
- Interdiction Effectiveness
- Advances in Drone Technology
- Lack of Operational Data
- Cost
- Legality
- Lack of Standards
- Privacy

Concerning <u>Legality</u> and <u>Privacy</u>, the **2019 CSD Report** [BD99] acknowledges the contribution of ALADDIN to these subjects, including ALADDIN deliverable "D3.1 – Data protection, Social, Ethical and Legal Frameworks" ([AD2]) in the suggested reading list.

Explicit mention of the ALADDIN contribution on Legality and Privacy issues is contained also in the **PRIO Paper 2020**[126] [BD118]: *The EU-funded ALADDIN project published a preliminary study on the different data protection, social, ethical and legal frameworks in Europe that have legal implications for the C-UAS problematique.* In another page, ALADDIN is mentioned as a notable example of the EU's framework programmes for security and defence R&D: *the EU has recently started to fund projects and initiatives that advance research on C-UAS technology. These initiatives include the above-mentioned ALADDIN project […] KNOX and other C-UAS-related projects, such as ALFA, SAFESHORE, DEFENDER and SafeSky* (5.2.2.1.2).

After the release of the new deliverable D3.2 [AD17] and of the public version of the SOTA report D4.9[127] [AD18], we expect a greater resonance of ALADDIN's

[125] https://link.springer.com/book/10.1007/978-3-030-34995-0?page=2#toc

[126] https://www.prio.org/Publications/Publication/?x=12245

[127] https://aladdin2020.eu/wp-content/uploads/2020/07/D4_9_Report_StandardRegulSOTA_progress_V1_0_PU.pdf 22 July 2020

contribution in the debate on ethical and legal aspects, as well as on the general state of the art in terms of standardization, regulation and technological anti-drone solutions.

5.2.2 Drone detection systems

5.2.2.1 Radar sensing

The **2018 CSD report** ([BD59]) includes 63 products using Radar sensing for drone detection (31 in single-sensor systems and 32 in multi-sensor ones), representing 41 % of detection products.

It is worth noting that ALADDIN partner IDS produces a 2D drone detection radar integrated into its **Black Knight** system, featuring also EO-IR detection and jamming. The system has been showcased at the Eurosatory exhibition in Paris on June 2018[128]. Although absent in the 2018 CSD Report ([BD59]), IDS Black Knight is included in the second edition (2019 CSD Report [BD99]) and in the August 2020 issue of the *Unmanned Airspace* counter-UAS directory[129], along with IDS' *NO-DRONE* counter drone system for the civilian market.

An extensive SOTA analysis on radar sensors for C-UAV application has been performed as part of the activities of WP5 – Task T5.1 Radar Capability. The outcome is included as **ANNEX C** of the **Deliverable D5.1** ([AD5]), issued in November 2018 and in version V2 of February 2020.

5.2.2.1.1 Drone recognition with FMCW radar signals

Most of the radars used for UAV detection, including the 2D radar by IDS and 3D radar by SIRC included in the ALADDIN platform (**Figure 2.2.1**), are Frequency Modulated Continuous Wave (FMCW) radar. The techniques that can be applied for classification and recognition of drones using FMCW radar signals ([BD10] - [BD11]) depend on the type of radar. There are mainly two types of radar:

- A *surveillance radar*, operating with a rotating antenna to discover, detect and track multiple targets ([BD10] - [BD11]), that can work with global features describing the signature of the targets, such as Radar Cross Section (RCS) and Signal-to-Noise Ratio (SNR), along with the information related to the position and the trajectory (kinematic features). As a surveillance radar is designed to constantly seek the space to find new targets, the time on target (that is the time for which the target is seen by the radar) is usually very small, in the order of 10ms ([BD10] - [BD11]). The above mentioned features can be successfully exploited to classify drones from false alarms [BD16], or maybe even to distinguish fixed wings drones from rotatory wings drones.
- A *tracking radar*, illuminating a single target for a fairly longer time, in the order of 1 s, that can provide features describing the intrinsic movements of the target through the analysis of the time variations of the Fourier spectra of received signals, which is called the micro-Doppler analysis [BD15]. The intrinsic movements of the targets could describe the rotation of rotor blades of a rotatory

[128] http://www.eurosatory.com/?lang=en

[129] https://www.unmannedairspace.info/wp-content/uploads/2020/08/Counter-UAS-directory.-August-2020.v2.pdf August 2020

wings drone or of a helicopter, the propulsion turbine of a jet, the flapping of the wings of a bird, and can be statistically described by the radar micro-Doppler signature. Thus, using a radar which holds its antenna in the direction of a single target, it could be possible not only to distinguish drones from false alarms, and rotatory / fixed wings drones, but also to recognize the type of drone ([BD15] - [BD14]).

For both types of radar, the received raw signal can also be exploited for classification by resorting to the Range Profiles matrix ([BD10] - [BD17]).

State-of the art methods for classification of drones include two main categories, essentially depending on the duration of target illumination:

1. Classification of drones based on **signature and kinematic features** ([BD12] - [BD17])
2. Classification of drones based on **micro-Doppler signature** ([BD18] - [BD28])

Providing additional details on these classification methods is beyond the scope of this document. They have been included in the relevant deliverables of WP5 Detection, Localisation, and Classification (D5.5 and D5.6). The ALADDIN project is exploring both possibilities, according to the availability of suitable radar data, trying to implement the most suitable classification approaches to the chosen system architecture. Main results have recently been presented at the UAV4S workshop and included in the publication by Messina and Pinelli, 2019 ([BD101]).

5.2.2.1.2 Scientific research

Recent C-UAV research projects involving radar sensing include the H2020 projects:

- ***SafeSky*** - *Integrated system for critical infrastructure and personal sphere monitoring and protection against aerial threats* (from July to October 2015) [130], leading to the **CTRL+SKY Radar** by Advanced Protection Systems (Poland).
- ***KNOX*** - *Cost advantageous and scalable drone alarm and protection system for urban contexts* (from August 2017 to July 2019)[131] related to the **EAGLE radar** by MyDefence (Denmark).

Another relevant H2020 project for drone detection in maritime environment is the project funded under the H2020-BES-2015 scheme:

- ***SafeShore*** - *System for detection of Threat Agents in Maritime Border Environment* (from May 2016 to October 2018)[132], which does not include radar sensors, but is very relevant in the context of multi-sensor data fusion.

Focusing on low cost and "green" technologies for maritime border protection, the SafeShore core solution is to integrate a 3D LIDAR with passive acoustic sensors, passive radio detection and video analytics in the visual and thermal domain. ALADDIN will take into account the research outcome of the SafeShore project ([BD46], [BD47] and [BD60]), especially those concerning data processing and data fusion, as well as other scientific publications on these subjects (§ 5.2.6 and [AD3]).

[130] https://cordis.europa.eu/project/rcn/197958_en.html

[131] https://cordis.europa.eu/project/rcn/211671_en.html; http://www.mydefence.dk/research-development/horizon-2020/

[132] https://cordis.europa.eu/project/rcn/203302_en.html; http://safeshore.eu/

5.2.2.2 Optro and thermal sensing

According to the 2018 CSD Report, Electro-optical and Infrared (EO-IR) is the most common dual-sensor combination for drone detection, followed by Radar-EO-IR combined technologies. EO-IR dual sensors account for 10% of C-UAV systems with detection capabilities. Likely military products are those including Laser as neutralization technology and the two UAV-borne systems.

Only a few products involve only one of these two technologies (either EO or IR), as a standalone detector or in combination with other technologies.

According to the November 2018 issue[133] of the Unmanned Airspace Counter-UAS-directory, at Eurosatory 2018 MBDA[134] demonstrated its **Licorne** C2 lightweight and mobile air defence command and control system now with integrated anti-drone capabilities. In the concept system on display, MBDA had reportedly integrated **HGH's Infrared tracking camera**, a Sagem electro-optical camera and a Konsortium Engineering Activities System's (KEAS's) UAS jammer.

HGH Infrared Systems is mentioned also in the **2019 CSD Report** [BD99] and in the publication by **Nassi et al. 2019** ([BD84], **Figure 5.2.2**). HGH' main results on *UAV localization using panoramic thermal cameras* have recently been presented at the UAV4S workshop and included in the publication by Thomas et al. 2019 ([BD102]).

Main SOTA progress concerning optical and thermal sensing is included in the relevant deliverable **D5.3 Optro-Thermal Panoramic Capability** ([AD6]), issued in November 2018 and in version V2 of February 2020.

5.2.2.3 Acoustic sensing

The 2018 CSD report ([BD59]) includes 21 products using Acoustic sensing for drone detection (8 in single-sensor systems and 13 in multi-sensor ones), representing 14 % of detection products.

Main SOTA progress concerning acoustic sensing is included in the relevant deliverable **D5.5 Acoustic Capability** ([AD7]), issued in November 2018 and in version V2 of February 2020. A number of references therein list the recent improvements in the fields of signal processing and machine learning, especially concerning *Neural Network-based Acoustic Source Localization*. An extensive SOTA analysis of acoustic hardware and processing algorithms is beyond the scope of this document, whereas a concise summary is provided below.

5.2.2.3.1 Microphone array hardware for outdoor application

Organized arrays solutions: Organized arrays represent any determined arrangement of microphones, often restricted to one carrier unit. Some standard configurations of organized arrays are planar (2D) or spatial (3D, i.e. cubical or spherical). While 2D arrays often are used for measuring of emissions (e.g. acoustic camera), 3D arrays enable the user to locate acoustic source in its surrounding.

---

[133] https://www.unmannedairspace.info/wp-content/uploads/2018/11/Counter-UAS-directory.-November-2018.-v2.pdf

[134] www.mbda-systems.com

Distributed and sparse arrays: The emergence of small, low cost and low-power sensor technologies that possess on-board signal processing and wireless communication capabilities has stimulated great interests in utilization of distributed sensor networks in a wide variety of applications [BD29]. These distributed sensor networks offer a new and promising paradigm for security surveillance, reconnaissance and situation awareness in urban terrain [BD30]. Additionally, there has been considerable attention to develop miniature sensitive microphones for many applications that require acoustic data collection over larger bandwidths for proper signal detection and identification. Several important properties of the randomly distributed acoustic sensors have been studied [BD31] for detection, tracking and localization of moving sources.

Vector-based acoustic sensors: The Acoustic Vector Sensor or (AVS) is a device that is capable of measuring acoustic particle velocity as well as pressure as in a standard microphone. This combination makes it possible for the device to measure the complete sound field. The AVS device has great advantages since it allows determining the direction of arrival of an acoustic source in 3D. The most important aspect of this is the ability for the device to accomplish this task on its own, without the aid of an additional microphone. By using the AVS in an array configuration, better results for localization can be achieved.

Outdoor application: For outdoor microphones, there are several products on the market available, e.g. Norsonic, B&K. But all those microphones are Analog Microphones that have special needs to protect them from the influence of outdoor environments. There is no outdoor microphone array known, neither for analog nor for digital microphones.

5.2.2.3.2 Acoustic processing for drone detection and localization

ALADDIN aims for the development of an outdoor applicable detection, localization and tracking solution. Consequently, harsh noisy acoustic conditions are expected which need to be addressed to enable high system performance.

Pre-processing techniques include various single-channel signal enhancement algorithms that can be divided into two main categories, the cancellation and the filtering approach. An even better enhancement can be achieved by using beamforming for spatial filtering and multi-channel algorithms for localization.

Acoustic Event Detection (AED) is increasingly used in various application fields. Examples include detection and classification of emergency situations in public environments, such as siren detection, recognition of screams and improvement of speech recognition. Various approach are reported in the recent literature. Recent scientific research shows that combining these approaches with appropriate signal pre-processing methods leads to high detection and classification results and increase the overall robustness of AED systems [BD32].

Acoustic source localization of moving objects is crucial for the estimation of flight trajectories in order to assess the character of the UAV flight. For localization many algorithms have been developed. They can be divided into three categories based on their increasing computational complexity: Time-delay-based methods [BD33], spectral-based methods and parametric methods ([BD34], [BD35]).

In time-delay-based methods the Time-Difference-Of-Arrival (TDOA) is obtained from the phase differences of microphones. For a full 3D localization at least four microphones in a 3D aperture are necessary.

Parametric methods have high computational cost and thus are not suitable for real-time processing, while spectral-based methods (such as the MUSIC, Root-MUSIC and ESPRIT algorithms) are computationally attractive, while providing high accuracy.

The practical disadvantage of these traditional approaches is that spurious peaks in the localisation function may have greater amplitude than the peak caused by the true source, so that simply choosing the maximum peak to estimate the source location may not give accurate results. A promising approach that overcomes the drawback and increases tracking capabilities of traditional methods is to use a state-space approach based on particle filtering (PF), as recently described [BD36]. Related work on using particle filters to track multiple moving targets can be found [BD37]. Particle filtering and variants (such as extended Kalman particle filtering [BD38]) can be used in conjunction with any of the direct and indirect localization methods.

5.2.2.4 Other sensors

Out of the 155 C-UAV products with detection capabilities listed in the 2018 CSD Report over 60 products (~40%) are based on RF detection, either as standalone detectors (41 products) or in combination with other technologies. Most of the single-sensor RF systems are produced in USA (26) or Israel (8), and the remaining in Europe or other countries (like the Australian RfOne and Faralert Sensor by DroneShield).

5.2.3 Drone neutralization systems

5.2.3.1 Jamming

Jamming (both RF and GNSS) is the most common interdiction method ([BD59], [BD99]). The UAVs are remotely controlled by a person using several frequencies. The common frequencies are in the ISM bands (2.4 -2.5 GHz and 5.725 - 5.875 GHz). Nowadays, it is possible to build a UAV by yourself. In this case, the frequencies used are 433 MHz and 868 MHz due to the facilities of buying emitters and receivers. If a transmission issue happens, the drone uses the satellite navigation to get back to the take-off location. Depending on the country, it uses the GPS, Galileo, GLONASS or Beidou.

The 2018 CSD report ([BD59]) includes 97 products with RF/GNSS jamming capability (66 % of the neutralization products), 51 of them with interdiction capability only and the rest integrated in complete C-UAS systems.

The SOTA analysis performed by MC2 in February 2018[135] includes a number of jammer solutions available on the market, divided into:

- Fixed jammer solutions: 19 products, including MC2' **Scrambler 1000**
- Mobile jammer solutions: 14 products, including MC2' **Scrambler 300**

Although absent in the 2018 CSD Report ([BD59]), MC2 jammers (Scrambler 1000, Scrambler 300, Nerod F5 and Reconfigurable Jamming System) are included in the second edition (2019 CSD Report [BD99]).

[135] MC2, 08/02/2018. ALADDIN internal report (180208-ALLADIN.doc)

5.2.3.2 Other effectors (Hacking, Physical neutralization capabilities, etc.)

The 2018 CSD report ([BD59]) includes 12 products with **spoofing** capability (8 % of the neutralization products), most of them from USA; the only European spoofing devices are manufactured by the Irish Chenega Europe and the German Dronefence.

Other 41 C-UAS products (27 % of the neutralization products) include some form of **physical neutralization** (sometimes in addition to jamming): 10 products involve the use of net (or net shotgun shells) launched by ground-based, hand-held or UAV platforms. The majority of these devices are produced in Europe, including the two lines of products (Skywall series from the UK Open Works Engineering and DroneCatcher by the Dutch Delft Dynamics) already mentioned in D4.5 ([AD3]).

Around twenty systems employing **other effectors** (Kinetic, Laser, Electromagnetic Pulse, Projectiles) are mainly from Defence manufacturers.

Main SOTA progress concerning Neutralization is included in the relevant deliverables, issued in November 2018:

- **D6.1 Jamming Module** [AD8]
- **D6.3 Hacking Module** [AD9]
- **D6.5 Physical neutralization capabilities** [AD10]

Based on the REA recommendations, main updates and improvements are included in version V2 of February 2020.

Innovative approaches of physical neutralization include the recourse to **defence UAV swarm** to surround the intruder drone: the practical feasibility of this approach requiring advanced mathematical algorithms is currently a novel research topic (§ 5.2.5.1).

Within ALADDIN, FADA-CATEC is conducting research on the use of drone interceptors as a physical neutralization option for countering malicious drones. The main results on *Minimal-time trajectories for interception of malicious drones in constrained environments* have recently been presented at the UAV4S workshop and included in the publication by García et al. 2019 ([BD103]).

5.2.4 Command and Control (C2)

Command and control (C2) software is the heart of C-UAV systems. It connects data from sensors and helps for classification and threat mitigation. The level of integration and automation depends on each system objectives. Human-Machine Interfaces (HMI) are generally based on mapped representation, mostly satellite picture.

The data used for mapped representation are usually from 3rd party providers (satellite image providers, GIS data providers, map providers). The networking and interoperability components ensure that the C-UAV platform can use those data and adapt to the most common exchange standards.

The mapping of the area is constructed through these data as a 2D picture or a 3D representation of the scene (including the altitude information).

The ALADDIN platform will use networking and interoperability components to allow accessibility to most common geographic data and exchange standards.

5.2.4.1 New interoperability standards

As of 09/2017, OGC (the main standardisation body in geospatial data field) acknowledged a new standard for storing and visualising 3D layers. This standard may allow new types of data providers.

5.2.4.2 Displays

One of the display means considered in ALADDIN is Augmented Reality head-up devices. This branch of the technology is a rapidly evolving one.

For the current period, Microsoft issued information about the planned new version of its device Hololens, including increased hardware specification for more fluid rendering.

Main SOTA progress concerning Command and Control (C2) and additional components is included in the relevant deliverables, issued in November 2018 and in version V2 of February 2020:

- **D7.1 C2+API** ([AD11])
- **D7.3 Mixed Reality cartographic module** ([AD12])
- **D7.7 Networking and Interoperability modules** ([AD13])

5.2.5 Support to Operations sub-systems

The virtual training and support to investigation capability is a tool that can simulate a virtual 3D scene animated by a scenario (either by replaying an existing event or by playing an imaginary event) and feed the C2 with the relevant information.

The ALADDIN project will employ virtual training to provide LEAs and end users with innovative tools. Additionally, it will make use of sophisticated algorithms and state of the art methods to provide unprecedented system performance, including Deep Learning and Data Fusion techniques, as described in the following paragraphs.

Main SOTA progress concerning Support to Operations sub-systems is included in the relevant deliverables, issued in November 2018 and in version V2 of February 2020. Main topics are related to Data processing methods, including Deep Learning methodologies for UAV detection and classification, summarised in § 5.2.6. Additional topics are included below.

5.2.5.1 Novel topics: drone swarms and Internet of Things (IoT)

The November 2018 issue[136] of the Unmanned Airspace Counter-UAS-directory includes two C-UAS systems employing novel approaches for UAV detection and neutralization: **swarms of drones** to neutralize an intruder drone and **Internet of Things (IoT)** for drone tracking.

5.2.5.2 Novel topics: UTM/U-Space and cooperative target recognition

ALADDIN consortium makes every efforts to provide a solution at the forefront of the C-UAV market, incorporating also features to address novel requirements coming out from the vibrant debate in this sector at various levels. One of these novel topics is related to Unmanned Traffic Management (UTM) for the safe integration of drones in the low-altitude airspace, represented in Europe by the ongoing U-space initiative fostered by SESAR JU.

A major benefit of interoperability with U-Space services, starting from the possibility of using the e-identification information within ALADDIN C-UAV system, would be the invaluable opportunity of an improved drone classification, incorporating also a feature similar to the functionality known as *Identification Friend or Foe (IFF)* for ordinary aircraft. The e-identification information would allow the identification of *'Friend'* drones (through a sort of cooperative target recognition), thus helping to single out the potentially malicious or *'Foe'* drones among the total set of targets detected by ALADDIN suite of sensors and classified as 'drones' by ALADDIN classifier (acting as 'non-cooperative target recognition').

CS GROUP has already done preliminary work to demonstrate the feasibility of including UTM tracks on ALADDIN display for complementing standard Air Traffic Control (ATC) services in airport environments, particularly vulnerable to the drone threat. As described in D2.10 ([AD16]), at SIAE International Paris Air Show 2019, CS GROUP presented a large display of C-UAV technologies. A simulated situation, with attacking drones on Le Bourget airport and counter-measures, were displayed. Links with ATC situation (drones tracks displayed on ATC screen) and UTM (UTM tracks on ALADDIN display) were shown.

In addition to integration with U-Space Service/UTM Systems, other recent developments gaining increasing interest in the UAS and C-UAS world include Artificial Intelligence/Machine Learning (§ 5.2.6.2).

5.2.6 Data processing methods

5.2.6.1 Conventional methodologies for UAV detection and classification

A literature study on UAV detection systems before the Deep Learning era is presented here for multiple modalities, including optronics, radar and acoustic sensors.

[136] https://www.unmannedairspace.info/wp-content/uploads/2018/11/Counter-UAS-directory.-November-2018.-v2.pdf

Optronics modality

Rozantsev [BD39] proposed an approach using optro-sensing to detect flying objects such as UAVs and aircrafts when they occupy a small portion of the field of view, possibly moving against complex backgrounds, and are filmed by a camera that itself moves. A regression-based approach to motion stabilization of local image patches that allows effective classification on spatio-temporal image cubes is deployed.

Pedro Alexandre Prates et al. proposed in [BD61] a method for UAV detection and localization extracted from video sequences captured by a camera when facing upwards towards the sky. A Background Subtraction algorithm is deployed to differentiate detected objects from a fairly stagnant environment such as the sky. Clouds are considered part of the background but all other objects (e.g. planes, birds, UAVs) are handled as foreground. The irregular motion patterns of the UAV, are used to create a movement signature that distinguishes the UAV from other objects. The signature is classified as an entropy metric obtained from the resulting optical flow over a number of past frames. A tracking algorithm based on a Kalman filter was developed to further improve the detection rate. Experimental results obtained from a dataset encompassing 12 diverse videos showed the ability of the computer vision algorithm to perform the tracking of the UAV with an average performance of 93.4%.

In [BD62], Eren Unlu developed an autonomous drone detection and tracking system that is discriminating birds from targets (UAVs). The authors have used 2-dimensional scale, rotation and translation invariant Generic Fourier Descriptor (GFD) features and classified targets as a drone or bird by a neural network. For the training of this network, a large dataset composed of birds and drones was gathered from open sources. The proposed method has achieved up to 85.3% overall correct classification rate.

Li Xiaoping et al. presented in [BD63], a novel method of UAV detection based on graph theory and HOG-FLD feature fusion. A selective search of the image segmentation and similarity is producing the candidate areas of the UAV. The resulting features are extracted through the method of gradient orientation histogram (HOG) and Fisher linear discriminant analysis (FLD) fusion. These features are employed to train a SVM classifier. The method can detect the UAV quickly and accurately under complicated background and circumstances of various positions and angles. Compared with the sliding window method based on image segmentation and HOG+SVM, the experimental results show that the speed of this method has been obviously improved with the same recognition accuracy. An average performance of 95.75% is reported.

Radar modality

The subject of UAV detection, localisation and classification using radar sensors was explored in the framework of the Dutch Radar Centre of Expertise (D-RACE), a strategic alliance of Thales Nederland B.V. and TNO [BD40]. This alliance has produced a joint dataset in the field of C-UAV systems, when monitored by a radar sensor. The resulting dataset has led the research on UAV detection and classification.

The main ingredient of radar sensing solutions is the micro Doppler signature. When, in addition to the constant Doppler frequency shift induced by the bulk motion of a radar target, the target or any structure on the target undergoes micro-motion dynamics, such as mechanical vibrations or rotations, the micro-motion dynamics induce Doppler modulations on the returned signal, referred to as the micro-Doppler effect [BD41]. The micro Doppler signature is extracted with the Short Time Fourier Transform, and the resulting spectrograms are often used as discriminant features for classification.

In [BD42], Molchanov proposed a UAV classification method based on extraction of intrinsic features from micro-Doppler signature. Eigenpairs extracted from the correlation matrix of the signature are used as informative features for classification. Planes, quadricopters, helicopters and stationary rotors as well as birds are considered for classification. The dataset consists of 11 classes captured within the framework of D-RACE. Classification accuracies exert 95% with a SVM classifier. Important to note is that targets were monitored within 30 m of distance away from the radar.

In [BD14], De Wit et al. studied a feature extraction method based on three main features to allow quick classification of mini UAVs versus birds: target velocity, spectrum periodicity, and spectrum width. It has been shown that these features can be extracted from spectrograms in a robust manner using singular value decomposition (SVD). The used dataset was created for a challenge in 2012 International Micro Air Vehicle (IMAV) Conference in Braunschweig.

In [BD23], Harmanny et al. recommended spectrograms and cepstrograms to easily extract key features for automatic or visual recognition of LSS-targets versus bio-life.

Ren et al. proposed in [BD43] a robust signal representation (2-D regularized complex-log-Fourier transform and an object-oriented dimension-reduction technique) subspace reliability analysis. The proposed signal representation addresses the problems of the existing feature representations by making full use of both magnitude and phase information of the first Fourier transform, enlarging the weak micro-Doppler signature and suppressing the noise in the log-spectrogram. The proposed subspace reliability analysis is specifically designed for UAV-detection problem. The proposed approach significantly reduces the equal error rate of the second-best approach, cadence velocity diagram, from 6.68% to 3.27%. The dataset used was provided by Thales and the classifier was Support Vector Machine (SVM).

Beom-Seok Oh et al. proposed in [BD64], an empirical-mode decomposition (EMD)-based method for automatic multiclass mini unmanned aerial vehicle (UAV) classification. The radar echo signal is first decomposed into a set of oscillating waveforms by EMD. In order to capture the phenomenon of blade flashes eight statistical and geometrical features are extracted from the oscillating waveforms. A nonlinear support vector machine is trained for target class label prediction after feature normalization and fusion. Their empirical results on real measurement of radar signals show encouraging mini-UAV classification accuracy performance. The equal error rate of the proposed method is 3.43 which is lower than similar methods on the same dataset.

Acoustic modality

In [BD65], Brendan Harvey envisioned a non-cooperative aircraft collision avoidance system based on acoustic sensing. An unmanned aerial vehicle (UAV) fitted with two microphones was flown in the vicinity of another airborne UAV to determine the maximum distance at which the intruding aircraft could be detected. A two-dimensional analytical model to approximate the minimum detection distance required to facilitate an avoidance manoeuvre for a given spatial configuration was presented. A method to increase detection distances by exploiting the harmonic nature of acoustic signals generated by propeller-driven aircraft was also presented. The method significantly increases the detection distances compared to the commonly used incoherent spectral mean. It was found that a small gasoline-powered UAV could be detected at distances up to 678 m, which is more than double the minimum required to avoid a head-on collision.

Xianyu Chang et al. introduced in [BD66], a feature extraction method based on Direction of Arrival (DOA) estimation algorithm using an acoustic array. They proposed a novel algorithm to estimate the DOA of an intruding drone by exploiting its acoustic feature, which is mainly reflected in the strength distribution of the harmonics of the received acoustic signal. Specifically, this algorithm first estimates the harmonic frequencies of the drone's acoustic signal in frequency domain. Then, multiple signal classification is used to estimate the DOAs of all the selected harmonics. Finally, weighted sum of these DOA estimates are taken as the drone's DOA estimate, where the weights are proportional to the energy of the corresponding harmonics. The performance of the proposed algorithm is verified by both simulation and field experiments.

In [BD67], Muhammad Zohaib Anwar et al. proposed the novel machine learning (ML) framework for detection and classification of amateur drones (ADr) sounds out of the various sounds like bird, airplanes, and thunderstorm in the noisy environment. In order to extract the necessary features from ADr sound, they implemented Mel frequency cepstral coefficients (MFCC), and linear predictive cepstral coefficients (LPCC) feature extraction techniques. Afterwards, SVM with various kernels are adopted to accurately classify these sounds. The experimental results verify that SVM cubic kernel with MFCC outperform LPCC method by achieving around 96.7% accuracy for ADr detection. Moreover, the results verified that the proposed ML scheme has more than 17% detection accuracy, compared with correlation-based drone sound detection scheme that ignores ML prediction.

5.2.6.2 Deep Learning methodologies for UAV detection and classification

Deep Learning methodologies are among the latest advances of scientific research in various applications, yet applying deep learning for UAV detection and classification is considered a novel concept. ALADDIN partner CERTH is working on applying deep learning methodologies not only to single-sensor data processing but also to multi-sensor data fusion for UAV detection and classification, which is considered a rapidly emerging research field. The recent paper by **Samaras et al. 2019** ([BD100]), published by CERTH within the ALADDIN project, contains a systematic literature review on this subject. Most of it is based on the SOTA analysis reported in previous version of this deliverable and summarised here for single sensor modalities as well as in § 5.2.6.3 for multi-modal data fusion. A more comprehensive review may be found in the CERTH paper ([BD100]) and references therein. Deep Learning methodologies are also the focus of two papers presented by CERTH at the UAV4S workshop and included in the publications by Samaras et al. 2019b ([BD104]) and Diamantidou et al. 2019 ([BD105]).

Deep Learning is part of a broader family of machine learning methods based on learning data representations. A deep neural network (DNN) is an artificial neural network (ANN) with multiple hidden layers between the input and output layers [BD44]. An ANN is based on a collection of connected units called artificial neurons. Neurons have state, a real number often between 0 and 1, and weights, which control the learning process. Typically, neurons are organized in layers. Different layers may perform different kinds of transformations on their inputs [BD45]. DNNs can model complex non-linear relationships. DNN architectures generate compositional models where the composition of features from lower layers is modelling complex data with fewer units. Deep architectures include many variants of a few basic approaches. Each architecture has found success in specific domains. It is not always possible to compare the performance of multiple architectures, unless they have been evaluated on the same data sets. Convolutional Neural Networks (CNNs) are feedforward networks in which data flows from the input layer to the output layer without looping back. They are particularly used in computer vision applications. On the other hand, in

Recurrent Neural Networks (RNNs), data can flow in a recurrent way. Long Short-Term Memory (LSTM) layers are particularly effective in applications where temporal patterns are involved. In general, whenever the term of time comes into the picture RNNs and LSTMs, in particular, are very popular in literature.

There are only a handful of deep learning approaches on solving the problem of detection, localization and classification of UAVs. The majority of them came into light in recent years. Hence, the subject itself is considered novel. As far as the modalities are concerned, optronics and radar sensing are the leading sources of data, which are being tackled by the aforementioned deep learning architectures.

The problem of the UAV detection and tracking is considered by the “SafeShore” project, funded by the European Commission under the “Horizon 2020” program. It aims to cover existing gaps in coastal border surveillance by preventing cross-border crime, such as trafficking in human beings and the smuggling of drugs, with the use of unmanned aerial robotic vehicles or drones ([BD46]). The “SafeShore” consortium launched the “drone-vs-bird detection challenge to encourage work on the topic of detecting UAVs from optical sensors [BD47]. The prominent ingredient of the solutions that have been proposed is the use of neural networks and deep learning approaches.

At beginning of the ALADDIN project UAV detection systems based on Deep Learning remain few and mostly include information analysis on optronics, radar and acoustic modalities. A SOTA report on deep learning (DL) methodologies that led to the development of the unimodal DL modules that are present in ALADDIN has been performed as part of the activities of WP5 – Task 5.4 Unimodal Deep Learning Filtering and Analysis. This work is included in **D5.7 – “Deep Learning Filters + C2 Modules + Reports V1”** [AD14]. Recently, a variety of scientific articles were published with terms UAV or drone detection and/or classification in their title. A summary of the most notable DL methodologies per module follows. As stated earlier, most of them are included in the systematic review by **Samaras et al. 2019** ([BD100]).

Optronics modality

The current SOTA on the subject of designing a UAV detection system using optro-sensing with deep learning methods is evaluated here. Saqib et al. [BD48] have considered Faster R-CNN [BD49] with publicly available pre-trained models for most of the object detectors. There were too few images in the shared challenge dataset to learn a deep model from scratch. Therefore, to take full advantage of network architectures, the authors have used transfer learning from ImageNet to fine-tune the models. The fine-tuning process helps the system to converge faster and perform better. Various network architectures have been tested such as ZF [BD50], VGG16 and VGG M 1024 [BD51] to train the system (see details in the papers) and evaluate the performance on the test dataset.

Aker and Kalkan [BD52] have used an end-to-end object detection method based on CNNs to predict the location of the drone in the video frames. In order to be able to train the network, the authors created an artificial dataset by combining real drone and bird images with different background videos. The results show that the variance and the scale of the dataset make it possible to perform well on drone detection problem.

Farhadi and Amandi [BD53] have proposed Faster RCNN with the VGG16 model. Therein, moving object detection is combined with single deep neural network object detector; along with finding of moving objects, object detection step applies on each frame using three classes: drone, bird, other. If the detection accuracy is higher than a threshold and related to the previous step, the algorithm accepts it but if the detection is out of the predicted bound, the result of the object detection is rejected.

Schumann et al. [BD54] have proposed a detection framework composed of two core modules: the first module detects regions that are likely to contain a UAV, followed by a classification module to distinguish each hypothesis into UAV or distractor classes, such as birds. To detect regions that are likely to contain an UAV, two complementary detection techniques are considered which exhibit promising results on video sequences containing UAVs at different distances. Depending on whether the video images are recorded by static cameras or moving cameras, median background subtraction or a deep learning based method are applied, respectively. To reduce the high number of false alarms, a CNN classifier is also used. In general, the classification of UAVs in real world data is a challenging task due to varying object dimensions (in the range of less than ten to hundreds of pixels), large variety of existing UAVs, and often lack of training data. Furthermore, the classification is impeded by varying illumination conditions, differing backgrounds, and localization errors of the detector. To address the various object dimensions, in [BD54] it is proposed to use a small network that is optimized to handle low-resolution objects such as UAVs at large distances. A proprietary dataset is used to train the CNN classifier. The dataset is composed of crawled and self-acquired UAV images, bird images of a publicly available dataset and crawled background images to account for the large variety of existing UAVs, other distracting flying objects, and varying illumination conditions and backgrounds.

Sonyou Hwang et al. proposed in [BD68] a vision-based aircraft detection method based on a deep convolutional neural network using a single camera sensor. The proposed method considers not only UAVs but all kinds of aircrafts and detects the objects based on the Single Shot Detector (SSD) network. They verified the system performance using test videos consisting of a total of 17,000 frames. On the test data, the model achieved over 83% of detection rate and 0.899 precision. The system operates at over 28 frames per second.

Hu et al. [BD87] designed a DL based detection method named DiagonalNet for UAV images, which does not include anchor boxes and detects targets by directly detecting diagonal lines in the input RGB image. The utilized backbone network is a modified hourglass network architecture with squeeze and excitation blocks for better performance. The authors achieved faster detection results than Faster-RCNN and more accurate than YOLO in their dataset. Jin et al. [BD88] approached drone detection with optical sensors through pose estimation. They proposed a quadcopter 6D pose estimation algorithm based on keypoints detection (only need keypoints annotation), relational graph network and perspective-n-point (PnP) algorithm, which achieved state-of-the-art performance in both simulation and real scenario. The proposed network is a light two-stage detector that detects drone and its keypoints simultaneously with an Xception like backbone network. Finally, Xiaoping et al. [BD89] proposed a non-DL dynamic detection method based on two consecutive inter-frame differences to extract the region of interest. The position of the target that appears on the image is obtained by the method of two consecutive inter-frame difference, and the UAV is detected by a trained SVM classifier. This simplistic UAV detection method is fast and relatively accurate in complex background and in different position and angle circumstances. Comparison against traditional HOG+SVM sliding window detection method is performed showing that the detecting speed with the proposed methods is improved while the recognition accuracy is comparable.

Within ALADDIN, the optro DL submodule is developed to handle the unimodal DL analysis of PIAP's PTZ camera. It is developed based on the Faster-RCNN [BD49] methodology. Faster-RCNN is one of the fastest and highest performing object detection algorithms. It enables both the detection and classification of multiple objects within a single, unified CNN. The optro DL submodule utilizes a part of MobileNet [BD76], as its base CNN. MobileNet is a lightweight classification CNN that offers a good trade-off between accuracy and test speed.

Thermal modality

The development of the thermal DL submodule is similar to the implementation of optro DL submodule. Faster-RCNN combined with a higher capacity classification CNN based on residual blocks [BD77] was utilized. The base CNN is a modified version of ResNet-50, designed to offer real-time performance with panoramic, high resolution 360° images. Utilizing thermal imagery for UAV detection and classification is a very novel concept and not many scientific publications are produced. As stated earlier HGH' main results on *UAV localization using panoramic thermal cameras* included in the publication by Thomas et al. 2019 ([BD102]) is the most recent related work.

Radar modality

The current literature on UAV detection systems using radar-sensing data with deep learning methods is described here. The main idea is to extract the spectrogram from the radar signal in order to produce the micro Doppler signature (MDS) of the detected object. Those spectrograms can be handled as images and the problem translates to image classification.

Kim, et al. in [BD55] used CNN to learn directly from the spectrogram. They also deployed the frequency domain representation of MDS called as cadence-velocity diagram (CVD). The proposed approach is tested and verified in two different environments, anechoic chamber and outdoor. Different numbers of operating motor and aspect angle of a drone are tested. The proposed method improved the accuracy from 89.3% to 94.7%. Two types of drone at the 50 and 100 m height are classified and showed 100% accuracy due to distinct difference in the result images. The GoogleNet architecture was used.

Wang et al. [BD85] proposed a CNN based target detection algorithm on the Range-Doppler spectrum and compared their method against traditional CFAR detector showing promising results. The detection problem was handled as a classification task between target and clutter classes where a fixed size window slides over the complete Range-Doppler matrix so that all Range-Doppler cells are checked. The authors validated their method on artificial data simulating that of a continuous wave radar. Chen et al. [BD86] proposed a non DL probabilistic motion model estimation method based on calculating the time-domain variance of the model occurrence probability in order to classify between UAVs and birds with data originating from a surveillance radar. The authors utilized moving direction, velocity and position of the target information to build their motion estimation models and proposed a smoothing algorithm on top of a Kalman filter tracking to enlarge the gap between the estimations of target model conversion frequency for birds and UAVs. They validated their approach on simulated and real data showing promising results.

Within ALADDIN, the 2D radar DL submodule is developed to handle the unimodal DL analysis of IDS's 2D radar. The basic building block of the 2D radar DL submodule are the Convolutional Neural Networks (CNNs) [BD75]. The CNNs have found great success on computer vision and signal processing tasks. The most notable similar work to the 2D radar DL submodule deploys the use of CNNs on the Range Doppler matrix [BD17] for target detection. While the 2D radar DL submodule utilizes the CNNs on the Range Profile matrix for target classification. This method is described in detail in *UAV classification with Deep Learning using surveillance radar data* which is the subject of the publications by Samaras et al. 2019b ([BD104]).

Acoustic modality

In [BD69], Dong Hyun Lim et al. analysed the effectiveness of a simple neural network for the task of determining, by sound, if small unmanned vehicles are carrying potentially harmful payloads. The authors operated under a minimal cost constraints to enable eventual adoption at scale by law enforcement agencies. Their system classifies payload carrying vs. non-payload carrying DJI Phantom II UAVs by presenting sound spectrum data to a simple Convolutional Neural Networks (CNN). These networks, along with a simple voting system, provided a 99.92% recognition rate for this problem without a need to violate the minimal cost constraint.

Recent advances in computer vision deep neural networks showed significant improvement, compared to 1D CNNs or sequential RNNs, when classifying audio signals in the presence of background noise [BD78]. A similar work is considered by the Acoustic DL submodule of ALADDIN. The spectrograms of the acoustic signals are used as input to the Xception network architecture [BD79] in order to tackle the classification problem of T5.4.

Al-Emadi et al. [BD90] presented a comparison between three DL based methods for UAV detection and classification, namely Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) and Convolutional Recurrent Neural Network (CRNN). These algorithms are utilized to exploit the unique acoustic fingerprints of the flying drones in order to detect and identify them. The audio clips are converted into spectrograms to allow for training with the DL methods. The authors proved that CNN based method is performing the best at their dataset both for detection and classification task. Another study [BD91] introduced a real-time drone detection and monitoring system using the k-nearest neighbours and plotted image learning algorithms to learn from properties of the Fast Fourier Transform spectrums. Recently, Kim et al [BD93], using an artificial neural network increased the accuracy of the proposed system from 83% to 86%.

Bowon Yang et al. introduced in [BD92], a UAV detection system with multiple acoustic nodes using machine learning models along with an empirically optimized configuration of the nodes for deployment. Features including MFCC and short-time Fourier transform (STFT) were used for training. SVM and CNNs were trained with the data collected in person. Experiments were conducted in order to evaluate models' ability to find the path of the UAV that was flying. Sensing nodes were placed in four different configurations and the best of test set was chosen which maximizes the detection range without blind spots. STFT-SVM model showed the best performance and a semi-circle formation with 75 meters distance between a node and the protected area was found to be the optimized configuration. The aforementioned system can be easily deployed in public and scaled by adding more, very affordable, nodes.

5.2.6.3 Multi-modal data fusion

Data fusion is the process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source [BD56]. Data fusion processes are often categorized as low, intermediate, or high, depending on the processing stage at which fusion takes place [BD57]. Low-level data fusion combines several sources of raw data to produce new raw data. The expectation is that fused data is more informative and synthetic than the original inputs. For example, sensor fusion is also known as (multi-sensor) data fusion and is a subset of information fusion.

In the framework of “SafeShore” the consortium will integrate the 3D LIDAR with passive acoustic sensors, passive radio detection and video analytics in the visual and thermal domain to improve UAV detection. Important to note is that instead of focusing on singular detection technologies, “SafeShore” aims to develop data fusion methodologies, as indicated on **Figure 5.2.4**, for cross-sensor data combination in order to maximize the detection ratio, while minimizing the false positive ratio [BD46].

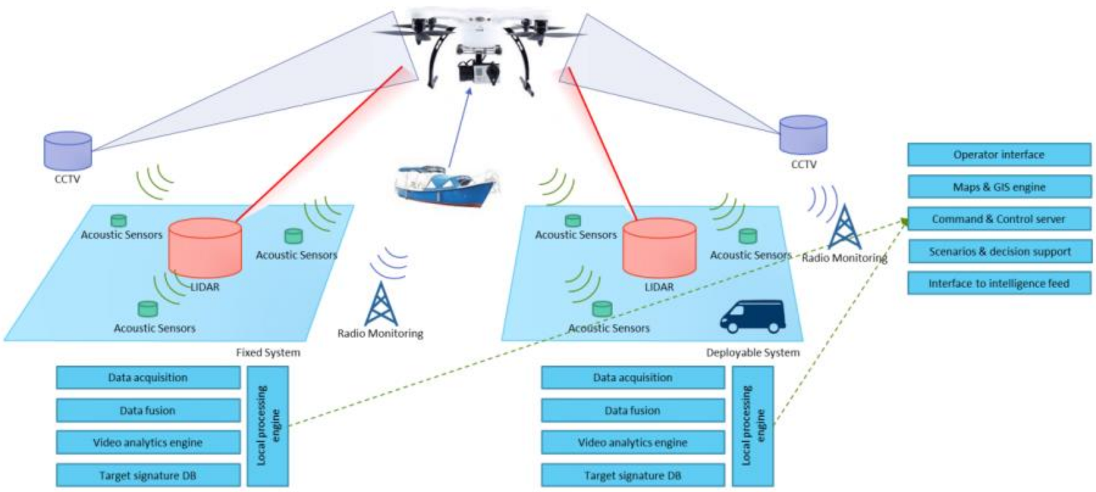


Figure 5.2.4: SafeShore system diagram, identifying the data fusion of the different detection mechanisms

Within ALADDIN, Data Fusion approaches will be explored using the available sensor data (2D and 3D radar, EO/IR and acoustic).

UAV detection systems exhibit the potential to utilize combined different modalities, such as optronics, acoustic and radar, in order to achieve increased levels of accuracy of detection. The literature presents a few studies that have been conducted using heterogeneous sensor networks in UAV detection. Image fusion techniques are the most common proposed approaches. A study of the recent data fusion methods is presented below.

Model-agnostic approaches

The available model-agnostic approaches for data fusion techniques can be classified into two categories: early fusion and late fusion as they described in [BD70]. According to this survey, early fusion yields a truly multimedia feature representation, since the features are integrated from the start. An additional advantage is the requirement of one learning phase only. A disadvantage of this approach is the difficulty to combine features into a common representation. On the other hand, late fusion focuses on the individual strength of modalities. Unimodal concept detection scores are fused into a multimodal semantic representation rather than a feature representation. Related studies describe the huge disadvantage of late fusion schemes, which is actually the computational cost in terms of the learning effort needed, as every modality requires a separate supervised learning stage.

Model-based approaches

While model-agnostic approaches are easy to implement using unimodal machine learning methods, there are also model-base approaches that are designed to perform multimodal fusion: kernel-based methods, graphical models, and neural networks as described in [BD70]. Multiple kernel learning (MKL) methods are an extension to kernel support vector machines (SVM) that allow for the use of different kernels for different modalities. An advantage of MKL is that it can be used to both perform regression and classification. One of the main disadvantages of MKL is the reliance on training data (support vectors) during test time, leading to slow inference and a large memory footprint. Regarding to graphical methods, a great example is deep belief networks, which consists of multiple hidden layers and one visible layer. The benefit of graphical models is their ability to easily exploit spatial and temporal structure of the data, making them especially popular for temporal modelling tasks. Finally, Neural Networks have been used extensively for the task of multimodal fusion. A big advantage of deep neural network approaches in data fusion is their capacity to learn from large amount of data. The major disadvantage of neural network approaches is their lack of interpretability.

Image wavelet transform fusion

K. Senthil Kumar et al. analysed in [BD71] an approach to fuse visual and thermal images for UAV tracking. They applied wavelet based image fusion with Haar transform with four level decomposition of the two images at a time. The next step was to apply an inverse transform to get back the fused image. Their system was used for UAV tracking using an optical flow technique based on Horn-Schunck method. The results were verified by experimental simulations.

Image Pyramids Fusion

A novel approach for image fusion is presented in [BD72]. The authors utilized an algorithm that combined wavelet transform and Laplacian pyramids to achieve image fusion. The proposed algorithm performed a discrete wavelet transformation. The wavelet transformation decomposed the input image to coefficients. A Laplacian pyramid was applied on every coefficient of the input image and then an inverse wavelet transformation took place to combine the decomposed levels of the image. The system was tested using performance metrics such as PSNR (Peak signal to noise ratio), average gradient and these quality measures showed a much better accuracy than the existing image fusion methods.

Neural network data fusion

In [BD73] Jiquan Ngiam et al. analysed multimodal different learning methods using neural networks. Firstly, the authors demonstrated cross modality feature learning, where better features for one modality can be learned if multiple modalities are present at feature learning time. Secondly, they showed how to learn a shared representation between modalities and evaluate it on a unique task. According to the authors, neural network data fusion has the advantage that there is no need to understand how sensors modalities relate.

In [BD74] an audio and visual data fusion for emotion recognition was proposed, using a deep convolutional neural network approach. The method was based on two individual streams, the audio network and the visual network. Each of these networks had fully connected layers and processed audio signals and visual data respectively. The output of these networks were fused in a new fusion network. The process networks were initialized on AlexNet, because of its ability in various vision tasks. The experiments were tested on RML audio-visual database and the results achieved a better performance than previous hand-crafted fusion methods in recognition tasks.

Within ALADDIN, the multi-modal fusion DL module has been developed to handle the fusion of ALADDIN modalities when utilizing DL methodologies. **D7.5 – "Multi-Sensor Information Fusion Module + Documentation V1"** [AD15] introduces a short SOTA report on (DL) methodologies dedicated to data fusion. This work describes activities performed as part of WP7 – Task T7.3 Multi-Sensor Information Fusion Component. A summary of the fusion DL methods follows.

The concepts of deep learning associated with the fusion of the extracted features are introduced in D7.5. Specifically, the Multilayer Perceptron (MLP) [BD80] is described, which is a neural network connecting multiple layers in a directed graph. The MLPs are fully connected neural networks and use backpropagation as a supervised learning technique. Because of their ability to solve classification (when the response variable is categorical) as well as regression problems, this approach is adopted for the development of the fusion DL module. Different network architectures that can be utilized to find the optimal detection results in each input combination of the modalities are illustrated. The research involved in the implementation of the training procedure of the fusion DL network is described. The choice of the optimization algorithm for the adopted deep learning model is also presented, since the optimization algorithm is the mechanism through which the network will update itself [BD81]. Two approaches are considered: the Adam optimization algorithm [BD82] as well as the stochastic gradient descent (SGD) algorithm [BD83] that has recently seen broader adoption for deep learning applications in computer vision and natural language processing.

Jovanoska et al. [BD94] presented a research about UAV detection and multi-sensor data fusion based on bearing-only as well as radar sensors for tracking and localization capabilities. For this work, a centralized data fusion system based on multi-hypothesis tracker (MHT) is implemented. The results showed that track extraction time, which is an important issue in drone detection systems, was significantly reduced. Recently, another study [BD98] proposed an automatic alignment of a 360° LiDAR system with an additional sensor (mounted on pan-tilt head) for the identification of UAVs. The classification sensor is directed by the tracking results of the panoramic LiDAR sensor. If the alignable sensor is an RGB- or infrared camera, the identification of the objects can be conducted by state-of-the-art image processing algorithms. If a higher-resolution LiDAR sensor is used for this task, algorithms have to be developed and implemented.

As stated earlier, many works related to the DL fusion task are included in the systematic review by **Samaras et al. 2019** ([BD100]). Additionally, *Multimodal Deep Learning framework for enhanced accuracy of UAV detection* is the subject of the paper by Diamantidou et al. 2019 ([BD105]).

Hengy et al.[BD95] proposed a sensor fusion scheme that aimed at detecting, localizing, and classifying incoming UAVs by utilizing optical sensors, acoustic arrays, and radar technologies. The system achieves localization accuracy with mean azimuth and elevation estimation error equal to 1.5 and − 2.5 degrees, respectively. Localization from acoustic arrays is achieved using the MUltiple SIgnal Classification MUSIC algorithms and the systems detection capability is enhanced by radar technologies to minimize false alarm rate. Finally, the authors proposed a method that combines images from short-wave infrared (SWIR) and visible sensors to achieve easier and faster detection of the UAV in the presence of clutter, smoke, or dense background on the vision sensors.

Liu et al. [BD96] presented a solution that uses both a modular camera array and audio assistance presented results of high detection precision. This drone detection device involved multiple cameras and microphones that record videos (image sequences) and sounds in all directions. The proposed method was tested against a dataset of multiple drones flying under various conditions at maximum flight altitudes of 100 m and a maximum horizontal distance of 200m. The system consisted of 30 cameras, eight workstation nodes, three microphones, and some network devices. To properly handle the multimodal data, the authors applied a synchronisation algorithm on both images and audio samples. Following this, two feature extraction methods were initialised to fuse image and audio data. The HOG feature extractor was adopted for images and the MFGG feature extractor employed for the audio data. An SVM classifier was trained to detect a drone in the image features while another SVM was trained to detect the noise produced by the drones from the audio features.

Park et al. [BD97] described a large installation of a multi-sensor fusion system concerning an airborne threat detection system combined from low cost, low power netted sensors that included a simple radar, and an acoustic microphone array. The proposed scheme is able to identify and track a potential airborne threat by employing a Kalman filter for associating the multiple sensor data to be fed to the nearest neighbor classifier for obtaining the final results. The system was able to accurately track aerial vehicles up to 800 m range, providing also a highly modular and adaptive technology setup.

ANN Image Fusion

Wang et al. propose an object detection and tracking system based on fusion of visible and thermal camera data by utilizing a CNN architecture. Their special contribution is a Cycle-GAN-based model for data augmentation of thermal images containing drones. The system is trained offline by real and augmented data on the Fast R-CNN and MDNet models and its efficiency is tested on USC drone dataset with 43.8% AUC score on the test set. This solution is the first to use deep learning technology for both the drone detection and tracking problem.

Additionally, In [BD113] a multi-frame deep learning drone detection technique is presented that is based on videos recorded from a lower-angle rotating RGB camera and a static wide-angle RGB camera. The proposed method essentially fuses the static camera's frame with the zoomed frame of the rotating camera. The wide angle camera detects the drone from afar and the detected drones that present specific motion characteristics are inspected from the lower-angle rotating camera. Both cameras use a lightweight version architecture of Yolo deep learning algorithm which is making use of the up-sampling concept in order to boost the performance for small objects detection. The classifier predicts four classes; namely drone, bird, airplane and background. The authors compared their solution with Cascaded Haar [BD114] and GMM [BD115] algorithms that were trained on the same dataset. All the algorithms resulted on a good true positive rate (0.91, 0.95. 0.98 respectively) while the authors' lightweight Yolo implementation resulted in 0.0 false alarm rate against 0.42 and 0.31 for Cascaded Haar and GMM respectively.

5.2.6.4 Latest technological updates on data processing methods

During the past year, the task of automatic UAV detection and classification using AI and DL methods has gained a lot of popularity for both single sensor (unimodal) and multi sensor (multimodal) inputs. The research community has organized workshops and challenges dedicated to the drone detection task in prestigious conferences such as the 1st Anti UAV workshop and challenge in 2020 CVPR [BD106] and the 3rd International Workshop on Small-Drone Surveillance, Detection and Counteraction Techniques in 2020 AVSS [BD107]. Although the latter was cancelled due to the COVID 19 crisis, the notice of the community is clear. This interest has resulted in multiple scientific papers which are published in 2020 extending the SOTA of data processing methods. In the following paragraph a short summary of some highlighted papers is presented.

Han Sun et al. [BD108] developed a drone detection network with tiny iterative backbone called TIB-Net in an effort to balance detection performance and model size for data originating from an optical camera. While conventional SOTA object detection methods trained with UAV data have shown promising results, they do not compensate for the small target object size. The proposed method utilizes a structure called cyclic pathway, which enhances the capability to extract effective features of small object and achieves high performance while keeping the model size at an acceptable level.

Another DL based method on optical camera data is presented by Seidaliyeva et al. [BD109]. The authors propose a two-step solution for the task at hand: the detection of moving objects and the classification of the detected object into drone, bird, and background. The moving object detection is based on background subtraction, while classification is performed using a convolutional neural network (CNN). Their experimental results showed high accuracy combined with high processing speed.

Koksal et al. [BD110] tackle the task at hand with a different perspective in mind by trying to propose a semi-automatic method to improve annotations for UAV detection dataset. They utilize YOLO v3 network for UAV detection trained with and without annotation errors in UAV thermal imagery dataset to prove their point and later propose a method to improve erroneous annotations.

The effectiveness of YOLO v3 network has also been examined by Behera et al. [BD111] for the task of UAV detection for data originating from and optical camera. In an effort to differentiate from region proposal methods such as the YOLO v3 network or the Faster R-CNN network for optical camera data Zhout et al. [BD116] examined the possibility to add a DL based method for tracking such as the Siamese – RPN. By combining the template matching of the Siamese - RPN with the output of the Faster R-CNN the proposed drone detection and tracking method can achieve a more robust outcome.

Finally, a multi-senor fusion method based on acoustic, optical and thermal cameras data is proposed by Svanstrom et al. [BD117]. The authors utilize SOTA UAV detection and tracking methods for each modality separately and then propose a multi-sensor fusion scheme based on the unimodal results to reduce false positives.

5.3 SOTA progress summary

This section presents the technological SOTA progress after the start of the ALADDIN project in late 2017 up to December 2019. Based on data from recently published reports ([BD59], [BD60] and [BD99]) and online sources, it indicates the new developments or recent updates of C-UAV systems and subsystem appeared on the market, as well as emerging topics mentioned in scientific literature or specialized press.

After a statistical analysis of the C-UAS market (§ 5.2.1), based on data from recent reports and online sources, and an extensive review of the main components (from § 5.2.2 to § 5.2.5), § 5.2.6 offers an updated literature review on the evolution of the relevant scientific research concerned with methods for data processing (including deep learning) and data fusion.

Further details on technological progresses of individual detection or neutralization subsystems or additional components are included in the SOTA analysis performed within the relevant deliverables issued in November 2018 and in their updated version of February 2020:

- Radar sensing: **ANNEX C** of **D5.1** ([AD5])
- Optical and thermal sensing: **D5.3** ([AD6])
- Acoustic sensing: **D5.5** ([AD7])
- Neutralization: **D6.1** - Jamming ([AD8]), **D6.3** - Hacking ([AD9]) and **D6.5** - Physical neutralization ([AD10])
- Command and Control (C2): **D7.1** - C2, API ([AD11]), **D7.3** - Mixed Reality ([AD12]) and **D7.7** - Networking and Interoperability ([AD13])
- Support to Operations sub-systems: **D5.7 –** Unimodal Deep Learning ([AD14]) and **D7.5** - Multi-sensor information fusion ([AD15])

In 2018, global trends indicate a rapid increase in number of C-UAS equipment appearing on the market, with Europe accounting for 40% of C-UAS manufacturers, America for 38% and the rest of the world for the remaining 22%. The technological SOTA progress in this period confirms the overall trend toward multi-sensor integration and enhanced automation. Additionally, new trends are gaining interest. One is related to swarms of drones either as a most frightening threat requiring superior detection and neutralization capabilities or even as potential countermeasure if employing sophisticated algorithms (currently a topic of academic research) to form a self-organized network of defence drones to intercept the intruder drone. Another new topic involves Internet of Things (IoT) drone tracking and safety technology.

At the beginning of 2019, the two hottest topics involve new capabilities for detecting or countering swarms of enemy drones and an increased interest toward protection of airports from the drone threat. The latest fact is somewhat a consequence of the escalation of the drone threat witnessed with the incidents of drone sighting at Gatwick and Heathrow airports in UK (§ 2.3.1.1). The increased public awareness of the reality of this threat and its high social and economic impact has brought to light the timeliness of EC initiatives to support research and innovation in this sector, giving visibility also to the ALADDIN project in online press and specialized reports (§ 5.2.1.3).

In 2019, while the clamour of the Gatwick and Heathrow incidents dominates non-technical press, also market surveys point out that manufacturers of C-UAS equipment are focusing mainly on the airport market. A number of strategic partnerships are being arranged, especially among key players of the C-UAS market, in order to enlarge the options of sensors, effectors and services provided to (military or civilian) customers within an integrated drone detection and mitigation system. Most of them are working to develop tailored solutions for airport surveillance, as one of the most vulnerable critical infrastructure, based on the exponential increase in near misses with ordinary aircraft documented in recent reports.

In 2020, global trends confirm the rapid increase in number of C-UAS equipment appearing on the market, with Europe accounting for 38% of C-UAS manufacturers, America for 36% and the rest of the world for the remaining 26%, indicating a relatively more sustained C-UAS industry growth than in Europe and America. Amongst European countries, UK, France and Germany are those with the most prolific and varied C-UAS industrial bases outside of USA, Israel and Russia. The survey highlights the growing dominance of US industry in this sector and the emergence of new industries in Europe and Asia. Many of the new systems incorporate artificial intelligence (AI) algorithms to reduce false positives to a minimum in detection systems or to assist mitigation systems, whereas some systems claim the ability to detect and/or jam/neutralize swarms of hostile UASs. This period shows growing partnership trends between niche providers of detection and mitigation systems with UAS traffic management (UTM) companies. Some of them are developing rogue drone detection capabilities for integration within civil UTM networks.

Concerning the threat evolution, experts agree that the next generation of drone threats will be swarms and completely autonomous drones. This will require an extremely rapid, multi-layered defence system, that can detect and locate both RF and non-RF emitting drones through different types of sensors, and then mitigate the threat through appropriate means.

Recent scientific publications warn about new societal threats to security and privacy created by drones. Without additional safeguards, an open-skies policy that allow drones to fly over populated areas could result in attacks by malicious entities and be exploited for use in cyber-attacks, terrorism, crime and invasion of privacy.

According to technological progress and regulatory evolution, recent developments gaining increasing interest among manufacturers of UAS and C-UAS equipment include:

- U-Space Service/UTM Systems
- Artificial Intelligence/Machine Learning

The constant stream of announcements in the specialised press of C-UAS system enhancements and new partnerships between C-UAS manufacturers or sellers demonstrate a **high dynamism** of the sector, especially by the global big players, both in improving the system performances and in seizing new market segments.

6 Conclusions

Unmanned Aerial Vehicles (UAV) or Systems (UAS), commonly termed drones, are becoming an ordinary presence in everyday citizens' life, with a continuous market increase in a growing number of useful applications. The drone proliferation is however generating serious security issues. In recent years, newspapers and mass media have reported dozens of incidents involving drones flying over restricted areas and around critical infrastructures, such as airports, nuclear plants, official buildings, or during public events, including the alleged use of drones for terroristic purposes. Drone technology has evolved at a faster rate than imagined, leaving regulation and counter-drone capability far behind.

The recent incidents of small **drones flying too close to UK airports** (Gatwick in December 2018, during Christmas holiday and Heathrow in early January 2019) **and in Spain** at Adolfo Suárez Barajas airport (February 2020) caused a huge flight service disruption. These safety incidents, like the recent **drone near-miss with Trump' plane** in August 2020, demonstrated to the public the severe impact of the drone threat in everyday life and prompted an acceleration in both regulatory activities and Counter UAV business development.

The availability of open international standards is a key enabling factor for the development of markets in all business sectors, including the **Security** sector. Since the beginning of this decade, the European Commission is pointing out the necessity to address the gaps in the standardisation and regulation framework for an innovative and competitive Security Industry.

A number of standardization and regulation bodies are currently working on filling these gaps on UAV and counter-UAV (C-UAV) related topics, such as producing harmonized standards and regulation for the ***safe operation of UAVs*** in different zones of the airspace, according to their category. The most important standardization bodies dealing with UAV-related topics include EUROCAE work group WG-105 at European level, ISO technical committee ISO/TC 20/SC 16 and ICAO RPAS Panel at International level. There is an increasing effort to harmonize European standards with standardization activities outside Europe, such as those of the ASTM technical committee F38 and the RTCA special committee SC-228.

Current EUROCAE hottest topics include Specific Operations Risk Assessment (SORA), UAS Traffic Management (UTM), UAS E-Identification and UAS Geo-Fencing. Most importantly, in 2019 EUROCAE launched WG-115 **Counter UAS (C-UAS)**, with the mandate to develop standards to support the safe and harmonised implementation of Counter-UAS Systems into airport and Air Navigation Service Provider (ANSP) systems. The activities of the various EUROCAE working groups concerned with UAS and C-UAS (WG 105 and WG 115) are progressing, with some relevant standards published in June 2020, such as those on UAS Geo-Fencing and geo-caging, while others are under approval, such as those on UAS E-Identification and UAS safety analysis for the Specific category.

UTM is also the core of current ISO standardization activity within ISO/TC 20/SC 16, along with more general topics, such as UAS operational procedures included in the ISO standard published in 2019. ASTM standards include, among others, those published in 2018 on UAS Registration and Marking, and BVLOS Small UAS Operations, or in 2019 on UAS Remote ID and Tracking, while other standards are still in preparation, including those concerning Operation over People.

Important standardization and regulation activities affecting C-UAV technology are also those pertaining to ***electromagnetic emissions*** – relevant to radar and RF sensing or neutralization, as well as ***Privacy and personal data protection*** – mostly relevant to Electro-Optical sensors. Concerning electromagnetic emissions, apparently there is a lack of applicable standards for radar used in drone detection application. Furthermore, given the ambiguous legality of radio frequency (RF) jamming technologies, there does not appear to be European standards applicable to such neutralization equipment. The recent adoption of the General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679, which became enforceable from 25 May 2018, could speed up the development of standards for privacy and personal data protection management in support of Union's security industry.

Concerning the regulation progress, the European Aviation Safety Agency (EASA) is working at an unprecedented pace to improve the ***drone safety regulation*** thus overcoming the current fragmented regulatory framework especially for the smaller UAS. In the EU framework up to 2018, Regulation (EC) No 216/2008 (the 'Basic Regulation') established the main principles and common rules for civil aviation in the EU and defined the area of competence of the EU and of its Member States (MSs). According to it, most of EU Member States adopted national regulations to ensure the *safe operations* of civil drones (UAS) below 150 kg, but there were no harmonized rules at EU level. EASA has been working actively towards a revision of the Basic Regulation to extend the scope of the EU competence to regulate UAS even below 150 kg, also to allow free circulation of UAS throughout the EU. Following the Notice of Proposed Amendments issued in May 2017 (NPA 2017-05 - open and specific category) and the publication on the 06/02/2018 of EASA **Opinion 01/2018,** approval of the new EU regulation was expected by 2018-2019. A notable progress in this direction is the publication on the 22nd August 2018 of **Regulation (EU) 1139/2018**, (the new 'Basic Regulation') which repeals Regulation (EC) No 216/2008 with effect from 11 September 2018. In June 2019, the European Commission adopted the Delegated Regulation **(EU) 2019/945** and Implementing Regulation **(EU) 2019/947** (the 'UAS Regulation'), containing technical and operational requirements for drones. The publication by EASA of **Decision 2019/021/R** containing the relevant Acceptable means of compliance (AMC) and Guidance material (GM) completed the process. The EU regulation will be applicable in one year to give Member States and operators time to prepare and implement it. Following EASA **Opinion No 05/2019** on standard scenarios in the specific category, amendments to the EU drone regulation have been issued in May - July 2020, namely: Commission Implementing Regulation **(EU) 2020/639** and **(EU) 2020/746** and Commission Delegated Regulation **(EU) 2020/1058**. The purpose is to include the above-mentioned standard scenarios, along with postponing dates of application of certain measures in the context of the COVID-19 pandemic. Ongoing regulatory activities are concerned with U-Space, whose first step is the publication on 13th March 2020 of **Opinion on U-space** by EASA.

Member States are preparing for transposing the EU regulation into national implementation in the coming 3 years after its entry into force. Meanwhile, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) facilitates harmonisation of standards within the EU Member States and other participating authorities.

As stated previously, the main progress regarding ***Privacy and personal data protection*** is the entry into force on 25 May 2018 of the **General Data Protection Regulation** (**GDPR**) - Regulation (EU) 2016/679. However, within the scope of ***Preventing and countering the UAV threat***, the use of *detection technology* by law enforcement for the detection of the criminal use of drones may be exempted from the field of application of the GDPR by Recital 19. Instead, such use may fall under the ambit of **Directive (EU) 2016/680** (**Police and Criminal Justice Data Protection Directive**), which covers the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Regarding the use of *neutralization technologies*, most regulations are not at the European Union level because matters relating to public security are generally within the competence of member state law. The legal regimes allowing state authorities to make use of otherwise banned technologies (radio frequency jamming, for instance) may vary significantly between countries. The recent escalation of the drone threat, as publicly demonstrated by the serious incidents of drone sighting at Gatwick, Heathrow and Adolfo Suárez Madrid-Barajas airports, will likely trigger tougher regulation and heavier restrictions with impacts on Privacy and personal data protection. For instance, the *Air Traffic Management and Unmanned Aircraft Bill* (2019) will give more power to the Police for countering the drone threat in UK. This Bill is not scheduled to become law until 2021. The legal debate on countering the drone threat is active also outside Europe. In August 2020, the US Government has issued an advisory document providing guidance on the legal framework applicable to counter drone technology in the US. Specifically, this advisory addresses two categories of federal laws: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does not address state and local laws, nor potential civil liability flowing from the use of UAS detection and mitigation technologies.

In addition to the progresses in standardization and regulation, the document provides also the ***State Of The Art (SOTA) analysis*** of C-UAV technology as reported by published reports and online sources. Mini-UAV threat appeared as important in 2014, when many companies started to propose anti-UAV solutions. Single domain solutions focused on one aspect of the problem, either detection or neutralization of the threat. Detection mainly involves radar and/or electro-optical/infrared sensors whereas countering the threat mainly involves radio-frequency piloting and jamming of the UAV communication links. On the other hand, complete C-UAV systems are based on integration of (at least one) sensor, tracker/identifier and a neutralization effector (usually jammer). A number of systems and subsystems (sensing and neutralization equipment, data processing and data fusion techniques, cartographic and other supporting software) are currently available on the market. However, the threat is evolving very quickly and is mainly unpredictable: hence, single domain solutions are inadequate and should be integrated in flexible systems, able to accept different sensors and effectors. The overall trend is therefore toward multi-sensor integration and enhanced automation, although many points, such as drone versus bird discrimination, remain challenging tasks.

Additionally, new trends are gaining interest. The main one is related to swarms of drones either as a most frightening threat requiring superior detection and neutralization capabilities or even as potential countermeasure if employing sophisticated algorithms (currently a topic of academic research) to form a self-organized network of defence drones to intercept the intruder drone. Recent developments with potential impact on C-UAS systems include the requirement for integration with U-Space services/UTM systems and technological progresses of Artificial Intelligence/Machine Learning.

The latest surveys of C-UAS equipment appeared in the market confirm the trend to provide a multi-layer solution, with some equipment incorporating artificial intelligence (AI) algorithms or capabilities to detect and/or neutralize swarms of hostile drones. Additionally, growing partnerships are being signed for developing rogue drone detection capabilities for integration within civil UTM networks.

The constant stream of announcements in the specialised press of C-UAS system enhancements and new partnerships between C-UAS manufacturers or sellers demonstrate a high dynamism, especially by the global big players, both in improving the system performances and in seizing new market segments.

7 References

7.1 Applicable documents

[AD1] Description of Action (DOA) Part B of Grant Agreement number: 740859 — ALADDIN — H2020-SEC-2016-2017/H2020-SEC-2016-2017-1

[AD2] D3.1 Data protection, Social, Ethical and Legal frameworks (February 2018)

[AD3] D4.5 – Report on standardisation, regulation, and SOTA progress V1 (February 2018)

[AD4] D4.6 – Report on standardisation, regulation, and SOTA progress V2 (August 2018)

[AD5] D5.1 – Radar Capability + C2 Module + Documentation V1 – Annex C (November 2018)

[AD6] D5.3 – Optro-thermal panoramic capability + C2 module + reports V1 (November 2018)

[AD7] D5.5 – Acoustic capability + C2 module + reports V1 (November 2018)

[AD8] D6.1 – Jamming Module + C2 module + reports V1 (November 2018)

[AD9] D6.3 – Hacking Module + C2 module + reports V1 (November 2018)

[AD10] D6.5 – Physical neutralization capabilities + C2 modules + reports V1 (November 2018)

[AD11] D7.1 – C2 + API + design document and documentation V1 (November 2018)

[AD12] D7.3 – Mixed Reality cartographic module + documentation V1 (November 2018)

[AD13] D7.7 – Networking and Interoperability modules + documentation V1 (November 2018)

[AD14] D5.7 – Deep learning filters + C2 modules + reports V1 (November 2018)

[AD15] D7.5 – Multi-sensor information fusion module + documentation V1 (November 2018)

[AD16] D2.10 – Dissemination, communication & standardisation activities V2 (August 2019)

[AD17] D3.2 – Data protection, Social, Ethical and Legal Frameworks – V2 (July 2020)

[AD18] D4.9 – Report on standardisation, regulation, and SOTA progress V5 – Public Version (July 2020)

7.2 Standards / Regulations

[ND1] European Commission, 2010. *An Integrated Industrial Policy for the Globalisation Era Putting Competitiveness and Sustainability at Centre Stage.* **COM(2010) 614 final**, Brussels, 28.10.2010. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1418118779571&uri=CELEX:52010DC0614

[ND2] European Commission, 2012. *Action Plan for an innovative and competitive Security Industry.* **COM(2012) 417 final**, Brussels, 26.7.2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

[ND3] European Commission, 2015. *The European Agenda on Security.* **COM(2015) 185 final**, Strasbourg, 28.4.2015. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[ND4] International Civil Aviation Organization, 2011. **ICAO Cir 328 AN/190**, *Unmanned Aircraft Systems (UAS)* https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

[ND5] International Civil Aviation Organization, 2015. *Manual on Remotely Piloted Aircraft Systems (RPAS)* First Edition (Doc 10019 AN/507).

[ND6] **ASTM F2851-10**, *'Standard Practice for UAS Registration and Marking (Excluding Small Unmanned Aircraft Systems)'*, ASTM International, West Conshohocken, PA, 2010, www.astm.org

[ND7] **ASTM F3196-17**, *'Standard Practice for Seeking Approval for Extended Visual Line of Sight (EVLOS) or Beyond Visual Line of Sight (BVLOS) Small Unmanned Aircraft System (sUAS) Operations'*, ASTM International, West Conshohocken, PA, 2017, www.astm.org

[ND8] ITU, Radio Regulation, Articles, Volume I, Edition 2012

[ND9] **Directive 2014/53/EU** of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014). (**RED Directive**) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053

[ND10] **EN 303 364 – 3** "Primary Surveillance Radar (PSR); Part 3: Harmonized Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU for Air Traffic Control (ATC) Primary Surveillance Radar sensors operating in 8500-10000 MHz frequency band (X band), PSR in X band (8500-10000 MHz)"

[ND11] ERC Recommendation 70-03, "Relating to the use of Short Range Devices (SRD)", 13 October 2017

[ND12] **Directive 2014/30/EU** of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (OJ L 96, 29.3.2014). (**EMC Directive**) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0030

[ND13] **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (**General Data Protection Regulation**). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[ND14] **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* (**Police and Criminal Justice Data Protection Directive**). https://eur-lex.europa.eu/eli/dir/2016/680/oj

[ND15] **Regulation (EC) No 216/2008** of the European Parliament and of the Council of 20 February 2008 *on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:079:0001:0049:EN:PDF

[ND16] European Commission, 2014. Communication from the Commission to the European Parliament and the Council *'A new era for aviation — Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe* *and sustainable manner'*, **COM(2014) 207 final**, dated 8 April 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0207&qid=1466071905608&from=EN

[ND17] European Commission, 2015. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *'An Aviation Strategy for Europe'*, **COM(2015) 598 final**, dated 7 December 2015. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0598&from=EN

[ND18] European Commission, 2015. Proposal for a Regulation of the European Parliament and of the Council *on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council*, **COM(2015) 613 final**, dated 7 December 2015 http://eur-lex.europa.eu/resource.html?uri=cellar:da8dfec1-9ce9-11e5-8781-01aa75ed71a1.0001.02/DOC_1&format=PDF

[ND19] EASA Advance Notice of Proposed Amendment (A-NPA) 2015-10 *'Introduction of a regulatory framework for the operation of drones'* of 31 July 2015. https://www.easa.europa.eu/system/files/dfu/A-NPA%202015-10.pdf

[ND20] EASA Technical Opinion *'Introduction of a regulatory framework for the operation of unmanned aircraft'* of 18 December 2015. https://www.easa.europa.eu/system/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf

[ND21] EASA *'Prototype' Commission Regulation on Unmanned Aircraft Operations.* 22 August 2016. https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf

[ND22] EASA *Terms of reference for rulemaking task RMT.0230 - Regulatory framework to accommodate unmanned aircraft systems in the European aviation system - ISSUE 1.* 22/12/2016. https://www.easa.europa.eu/system/files/dfu/ToR%20RMT.0230%20Issue%201.pdf

[ND23] EASA Notice of Proposed Amendment (NPA) 2017-05 (A) *'Introduction of a regulatory framework for the operation of drones - Unmanned aircraft system operations in the open and specific category'* of 4 May 2017. https://www.easa.europa.eu/system/files/dfu/NPA%202017-05%20%28A%29_0.pdf

[ND24] EASA Notice of Proposed Amendment (NPA) 2017-05 (B) *'Introduction of a regulatory framework for the operation of drones - Unmanned aircraft system operations in the open and specific category'* of 4 May 2017. https://www.easa.europa.eu/system/files/dfu/NPA%202017-05%20%28B%29.pdf

[ND25] EASA 2017. *'Rulemaking and Safety Promotion Programme including the European Plan for Aviation Safety (EPAS) 2017–2021'* European Aviation Safety Agency, 24 January 2017. https://www.easa.europa.eu/system/files/dfu/RMP-EPAS_2017-2021.pdf

[ND26] SESAR Joint Undertaking, 2017. U-Space Blueprint https://www.sesarju.eu/sites/default/files/documents/reports/U-space%20Blueprint%20brochure%20final.PDF

[ND27] EASA 2018. ***Opinion No 01/2018***: *"Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and* *'specific' categories"* of 6 February 2018. (RELATED NPA/CRD: 2017-05 — RMT.0230). https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2001-2018.pdf

[ND28] **Directive 2014/35/EU** of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (recast) (OJ L 96, 29.3.2014). (**LVD Directive**) https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:32014L0035

[ND29] **Directive 2013/35/EU** of the European Parliament and of the Council of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (OJ L 179, 29.6.2013) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0035

[ND30] **Regulation (EU) 2018/1139** of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1139&from=EN

[ND31] **Commission Delegated Regulation (EU) 2019/945** of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (OJ L 152, 11.6.2019, p. 1–40) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN

[ND32] **Commission Implementing Regulation (EU) 2019/947** of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (OJ L 152, 11.6.2019, p. 45–71) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN

[ND33] EUROCONTROL, "UAS ATM Integration Operational Concept", Edition: 1.0, 27th November 2018.

[ND34] EASA 2019. ***Opinion No 05/2019***: *"Standard scenarios for UAS operations in the 'specific' category"* 6.11.2019 (RMT.0729). https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2005-2019.pdf

[ND35] **Commission Implementing Regulation (EU) 2020/639** of 12 May 2020 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight (OJ L 150, 13.5.2020, p. 1–31) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R0639&from=EN

[ND36] **Commission Implementing Regulation (EU) 2020/746** of 4 June 2020 amending Implementing Regulation (EU) 2019/947 as regards postponing dates of application of certain measures in the context of the COVID-19 pandemic (OJ L 176, 5.6.2020, p. 13–14) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R0746&from=EN

[ND37] **Commission Delegated Regulation (EU) 2020/1058** of 27 April 2020 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new unmanned aircraft systems classes (OJ L 232, 20.7.2020, p. 1–27) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1058&from=EN

[ND38] EASA 2020. ***Opinion No 01/2020***: *"High-level regulatory framework for the U-space"* 13.3.2020 (RMT.0230). https://www.easa.europa.eu/sites/default/files/dfu/Opinion%20No%2001-2020.pdf

7.3 Bibliography

[BD1] Teal Group, 2017. *2017 World Civil Unmanned Aerial Systems Market Profile & Forecast*. http://tealgroup.com/images/TGCTOC/WCUAS2017TOC_EO.pdf

[BD2] *3 growth industries revolutionizing the world*, November 2014. http://blogs.marketwatch.com/cody/2014/11/17/3-growth-industriesrevolutionizing-the-world/

[BD3] Grand View Research, 2016. *Commercial UAV Market Analysis By Product (Fixed Wing, Rotary Blade, Nano, Hybrid), By Application (Agriculture, Energy, Government, Media & Entertainment) And Segment Forecasts To 2022*. April 2016. (Report ID: 978-1-68038-584-7). https://www.grandviewresearch.com/industry-analysis/commercial-uav-market

[BD4] Global Market Insights, Inc. 2016. *Unmanned Aerial Vehicles (UAV)/Commercial Drone Market Size By Product (Rotary Blade, Fixed Wing, Nano Drone, Hybrid), By Application (Government, Media & Entertainment, Agriculture, Energy), Industry Outlook Report, Regional Analysis, Application Development, Price Trends, Competitive Market Share & Forecast, 2016 – 2023*. March 2016. (Report ID: GMI115). https://www.gminsights.com/industry-analysis/unmanned-aerial-vehicles-UAV-commercial-drone-market

[BD5] SESAR Joint Undertaking, 2016. *European Drones Outlook Study - Unlocking the value for Europe.* November 2016. (published 13th Dec 2016) http://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf

[BD6] MarketsandMarkets, 2016. *Anti-Drone Market by Technology (Laser System, Traditional Kinetic System, Electronics System), Type (Detection Systems, Detection and Disruption), Vertical and Region - Global Forecast to 2022*. January 2016.

[BD7] MarketsandMarkets, 2016. *Critical Infrastructure Protection Market by Security Technology (Network, Physical, Radars, CBRNE, Vehicle Identification, Secure Communication, SCADA, Building Management), by Service, by Vertical & by Region - Global Forecast to 2021*, June 2016.

[BD8] MarketsandMarkets, 2017. *Anti-Drone Market by Technology (Laser, Kinetic, And Electronics), Application (Detection And Detection & Disruption), Vertical (Military & Defense, Homeland Security, And Commercial), And Geography - Global Forecast to 2023*. July 2017. (Report Code: SE 4129) https://www.marketsandmarkets.com/Market-Reports/anti-drone-market-177013645.html

[BD9] MarketsandMarkets, 2017. *Critical Infrastructure Protection Market by Security Technology (Network Security, Physical Security, Radars, CBRNE, Vehicle Identification, Secure Communication, SCADA, Building Management), Service, Vertical, and Region - Global Forecast to 2022*. July 2017. (Report Code: TC 3249) https://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html

[BD10] P. Tait, "Introduction to Radar Target Recognition", IET Digital Library, 2005. http://digital-library.theiet.org/content/books/ra/pbra018e
[BD11] R. Sullivan, "Radar Foundations for Imaging and Advanced Concepts", Stevenage: The Institution of Engineering and Technology, 2004. - 505 p. http://cds.cern.ch/record/1619408
[BD12] H. Ghadaki, R. Dizaji, "Target Track Classification for Airport Surveillance Radar (ASR)", 2006 IEEE Conference on Radar, 2006.
[BD13] R. Dizaji, H. Ghadaki, "Classification System for Radar and Sonar Applications", Patent US7 567 203.
[BD14] J. J. M. de Wit, R. I. A. Harmanny and P. Molchanov, "Radar micro-Doppler feature extraction using the Singular Value Decomposition," 2014 International Radar Conference, Lille, 2014, pp. 1-6.
[BD15] V. Chen, "The Micro-Doppler Effect in Radar" – Artech House Radar Library, 2012.
[BD16] N. Mohajerin, J. Histon, R. Dizaji and S. L. Waslander, "Feature extraction and radar track classification for detecting UAVs in civillian airspace," 2014 IEEE Radar Conference, Cincinnati, OH, 2014, pp. 0674-0679.
[BD17] Vojtech Micka, "Objects identification in signal processing of FMCW radar for Advanced Driver Assistance Systems", Diploma Thesis Assignment, Czech Technical University in Prague, Faculty of Electrical Engineering. January 9, 2017.
[BD18] D. Tahmoush, "Review of micro-Doppler signatures", IET Radar, Sonar & Navigation, 2015, 9, (9), p. 1140-1146.
[BD19] S. H. Park, "Automatic Target Recognition Using Jet Engine Modulation and Time-Frequency Transform", Progress in Electromagnetics Research M, Vol. 39, 151-159, 2014.
[BD20] P. Tait, "Automatic Target Recognition: Helicopters and Range-Doppler Imaging", STO-EN-SET-172-2013, 6.
[BD21] R. Melino, C. Bourne, H. T. Tran, "Modelling Helicopter Radar Backscatter", Electronic Warfare and Radar Division, Defense Science and Technological Organization, DSTO-TR-2547, 2011.
[BD22] J. J. M. de Wit, R. I. A. Harmanny and G. P. Cabic, "Micro-Doppler analysis of small UAVs," 2012 9th European Radar Conference, Amsterdam, 2012, pp. 210-213.
[BD23] R. I. A. Harmanny, J. J. M. de Wit and G. P. Cabic, "Radar micro-Doppler feature extraction using the spectrogram and the cepstrogram," 2014 11th European Radar Conference, Rome, 2014, pp. 165-168.
[BD24] P. Molchanov, K. Egiazarian, J. Astola, R. I. A. Harmanny and J. J. M. de Wit, "Classification of small UAVs and birds by micro-Doppler signatures," 2013 European Radar Conference, Nuremberg, 2013, pp. 172-175.
[BD25] A. Balleri, A. Al-Armaghany, H. Griffiths, K. Tong, T. Matsuura, T. Karasudani, Y- Ohya, "Measurements and Analysis of the Radar Signature of a New Wind Turbine Design at X-Band", IET Radar, Sonar and Navigation, 2013, Vol. 7, Iss. 2, pp. 170-177.
[BD26] M. Ritchie, F. Fioranelli, H. Borrion, H. Griffiths, "Multistatic micro-Doppler radar feature extraction for classification of unloaded/loaded micro-drones", IET Radar, Sonar & Navigation, 2017, 11, (1), p. 116-124.
[BD27] M. Ritchie, F. Fioranelli, A. Balleri and H. D. Griffiths, "Measurement and analysis of multiband bistatic and monostatic radar signatures of wind turbines," in Electronics Letters, vol. 51, no. 14, pp. 1112-1113, 7 9 2015.
[BD28] M. Ritchie, F. Fioranelli, H. Griffiths and B. Torvik, "Monostatic and bistatic radar measurements of birds and micro-drone," 2016 IEEE Radar Conference (RadarConf), Philadelphia, PA, 2016, pp. 1-5.

[BD29] Xin Zhang, Jingchang Huang, Enliang Song, Huawei Liu, Baoqing Li, Xiaobing Yuan, Xin Zhang,Jingchang Huang, Enliang Song, Huawei Liu, Baoqing Li and Xiaobing Yuan, Design of Small MEMS Microphone Array Systems for Direction Finding of Outdoors Moving Vehicles", Sensors 2014, 14(3), 4384-4398;

[BD30] M. R. Azimi-Sadjadi, Y. Jiang and G. Wichern, "Properties of Randomly Distributed Sparse Acoustic Sensors for Ground Vehicle Tracking and Localization", Proc. SPIE 6201, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V, 62011L (10 May 2006);

[BD31] J. Davis and N. Berry, "Wireless Sensor Network Applications and Impact on MOUT", Proc. of the SPIE'04 Defense and Security Symposium, vol. 5417, pp. 435-443, April 2004.

[BD32] Jens Schröder, Niko Moritz, Benjamin Cauchi, Marc René Schädler, Kamil Adiloglu, Jörn Anemüller, Simon Doclo, Birger Kollmeier, and Stefan Goetze. On the Use of Spectro-Temporal Features for the IEEE AASP Challenge 'Detection and Classification of Acoustic Scenes and Events'. In IEEE Workshop on Applications of Signal Processing to Audio and Acoustics (WASPAA), New Paltz, NY, USA, Oct. 2013.

[BD33] Mohan,S.;Lockwood,M.E.;Kramer,M.L.;Jones,D.L.Localization of multiple acoustic sources with small arrays using a coherence test. J. Acoust. Soc. Am. 2008, 123, 2136–2147

[BD34] Bohme, J. Estimation of source parameters by maximum likelihood and nonlinear regression. In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, San Diego, CA, USA, 19–21 March 1984; pp. 271–274.

[BD35] Stoica, P.; Nehorai, A. MUSIC, maximum likelihood and Cramer-Rao bound. IEEE Trans. Acoust. Speech Signal Process. 1989, 17, 2296–2299.

[BD36] D.B. Ward and R.C. Williamson, "Particle filter beamforming for acoustic source localization in a reverberant environment", in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing (ICASSP-02), Orlando, FL, USA, May 2002

[BD37] C. Hue, J.-P. Le Cadre, and P. Pe ́rez, "Sequential Monte Carlo methods for mutliple target tracking and data fusion", IEEE Trans. Signal Processing, vol. 50, no. 2, pp. 309–325, Feb. 2002

[BD38] Xionghu Zhong, James R. Hopgood, Particle filtering for TDOA based acoustic source tracking: Nonconcurrent Multiple Talkers, Signal Processing, Volume 96, Part B, March 2014, Pages 382-394

[BD39] Rozantsev, Artem, Vincent Lepetit, and Pascal Fua. "Flying objects detection from a single moving camera". *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. No. EPFL-CONF-206719. 2015.

[BD40] Retrieved from thalesalerts.nl: http://thalesalerts.nl/2011/december/D-Race.doc/

[BD41] Chen, Victor C., et al. "Micro-Doppler effect in radar: phenomenon, model, and simulation study". *IEEE Transactions on Aerospace and electronic systems* 42.1 (2006): 2-21.

[BD42] Molchanov, Pavlo, et al. "Classification of small UAVs and birds by micro-Doppler signatures". *International Journal of Microwave and Wireless Technologies* 6.3-4 (2014): 435-444.

[BD43] Ren, Jianfeng, and Xudong Jiang. "Regularized 2-D complex-log spectral analysis and subspace reliability analysis of micro-Doppler signature for UAV detection". *Pattern Recognition* 69 (2017): 225-237.

[BD44] Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Deep_learning

[BD45] Haykin, S. O. (1993). *Neural Networks and Learning Machines (3rd Edition).*

[BD46] De Cubber, Geert, et al. "The SafeShore system for the detection of threat agents in a maritime border environment". *IARP Workshop on Risky Interventions and Environmental Surveillance*, Les Bons Villers, Belgium. 2017. Retrieved from safeshore.eu: http://safeshore.eu/

[BD47] Coluccia, Angelo, et al. "Drone-vs-Bird detection challenge at IEEE AVSS2017". *Advanced Video and Signal Based Surveillance (AVSS), 2017 14th IEEE International Conference on. IEEE*, 2017.

[BD48] Saqib, Muhammad, et al. "A study on detecting drones using deep convolutional neural networks". *Advanced Video and Signal Based Surveillance (AVSS), 2017 14th IEEE International Conference on*. IEEE, 2017.

[BD49] Ren, Shaoqing, et al. "Faster r-cnn: Towards real-time object detection with region proposal networks". *Advances in neural information processing systems*. 2015.

[BD50] Zeiler, Matthew D., and Rob Fergus. "Visualizing and understanding convolutional networks". *European conference on computer vision*. Springer, Cham, 2014.

[BD51] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition". *arXiv preprint arXiv:1409.1556* (2014).

[BD52] Aker, Cemal, and Sinan Kalkan. "Using deep networks for drone detection". *Advanced Video and Signal Based Surveillance (AVSS), 2017 14th IEEE International Conference on*. IEEE, 2017.

[BD53] Mohammad Farhadi and Ruhallah Amandi. “Drone detection using combined motion and shape features”. *In IEEE International Workshop on Small-Drone Surveillance, Detection and Counteraction Techniques*, Lecce, Italy, Aug. 2017.

[BD54] Schumann, Arne, et al. "Deep cross-domain flying object classification for robust UAV detection". *Advanced Video and Signal Based Surveillance (AVSS), 2017 14th IEEE International Conference on. IEEE*, 2017.

[BD55] Kim, Byung Kwan, Hyun-Seong Kang, and Seong-Ook Park. "Drone classification using convolutional neural networks with merged Doppler images". *IEEE Geoscience and Remote Sensing Letters* 14.1 (2017): 38-42.

[BD56] Hall, David L., and James Llinas. "An introduction to multisensor data fusion". *Proceedings of the IEEE* 85.1 (1997): 6-23.

[BD57] Blasch, Erik, et al. "Issues and challenges of knowledge representation and reasoning methods in situation assessment (Level 2 Fusion)". *Signal Processing, Sensor Fusion, and Target Recognition XV*. Vol. 6235. International Society for Optics and Photonics, 2006.

[BD58] Gabriel C. Birch, John C. Griffin, and Matthew K. Erdman, “UAS Detection, Classification, and Neutralization: Market Survey 2015,” Sandia National Laboratories, Sandia Report SAND2015-6365, 2015. http://prod.sandia.gov/techlib/access-control.cgi/2015/156365.pdf

[BD59] Arthur Holland Michel. “Counter-Drone Systems.” Center for the Study of the Drone at Bard College, February 20, 2018. http://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

[BD60] Buric M., and De Cubber G. (2017), “Counter Remotely Piloted Aircraft Systems”, MTA Review, Vol. 17, No. 1, June 2017 (Military Technical Academy Publishing House, Bucharest, Romania). http://safeshore.eu/wp-content/uploads/2016/06/2_Buric_Cubber_2017.pdf

[BD61] Prates, Pedro Alexandre, et al. "Vision-based UAV detection and tracking using motion signatures." 2018 IEEE Industrial Cyber-Physical Systems (ICPS). IEEE, 2018.

[BD62] Unlu, Eren, Emmanuel Zenou, and Nicolas Rivière. "Using Shape Descriptors for UAV Detection." Electronic Imaging 2018.9 (2018): 1-5.

[BD63] Xiaoping, L., Songze, L., Yanhong, W., Feng, X., & Penghui, T. Fast Aerial UAV Detection Based on Image Segmentation and HOG-FLD Feature Fusion.

[BD64] Oh, Beom-Seok, et al. "Micro-Doppler Mini-UAV Classification Using Empirical-Mode Decomposition Features." IEEE Geoscience and Remote Sensing Letters 15.2 (2018): 227-231.

[BD65] Harvey, Brendan, and Siu O’Young. "Acoustic Detection of a Fixed-Wing UAV." Drones 2.1 (2018): 4.

[BD66] Chang, X., Yang, C., Shi, X., Li, P., Shi, Z., & Chen, J. Feature Extracted DOA Estimation Algorithm Using Acoustic Array for Drone Surveilliance.

[BD67] Anwar, Muhammad Zohaib, Zeeshan Kaleem, and Abbas Jamalipour. "Machine learning inspired sound-based amateur drone detection for public safety applications." *IEEE Transactions on Vehicular Technology* 68.3 (2019): 2526-2534

[BD68] Hwang, Sunyou, et al. "Aircraft Detection using Deep Convolutional Neural Network in Small Unmanned Aircraft Systems." 2018 AIAA Information Systems-AIAA Infotech@ Aerospace. 2018. 2137.

[BD69] Lim, DongHyun, et al. "Practically Classifying Unmanned Aerial Vehicles Sound using Convolutional Neural Networks." 2018 Second IEEE International Conference on Robotic Computing (IRC). IEEE, 2018.

[BD70] Baltrusaitis, Tadas et al. "Multimodal Machine Learning: A Survey and Taxonomy", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018

[BD71] Kumar, K. Senthil et al. "Visual and thermal image fusion for UAV based target tracking", MATLAB - A Ubiquitous Tool for the Practical Engineer, 2011

[BD72] Kaur, Harmandeep et al. "Image fusion on digital images using Laplacian pyramid with DWT", 3rd International Conference on Image Information Processing (ICIIP), 2015

[BD73] Ngiam, Jiquan et al. "Multimodal Deep Learning" 28th International Conference on Machine Learning (ICML), 2011.

[BD74] Shiqing Zhang et al. "Multimodal Deep Convolutional Neural Network for Audio-Visual Emotion Recognition, International Conference on Multimedia Retrieval”, 2016

[BD75] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." nature 521.7553 (2015): 436.

[BD76] Howard, Andrew G., et al. "Mobilenets: Efficient convolutional neural networks for mobile vision applications." arXiv preprint arXiv:1704.04861 (2017).

[BD77] He, Kaiming, et al. "Deep residual learning for image recognition." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[BD78] I. McLoughlin, H. Zhang, Z. Xie, Y. Song, W. Xiao, Robust sound event classication using deep neural networks, IEEE/ACM Transactions on Audio, Speech, and Language Processing 23 (3) (2015) 540-552.

[BD79] F. Chollet. Xception: Deep learning with depthwise separable convolutions. arXiv preprint, pages 1610–02357, 2017.

[BD80] S. K. Pal and S. Mitra, "Multilayer perceptron, fuzzy sets, and classification," in IEEE Transactions on Neural Networks, vol. 3, no. 5, pp. 683-697, Sept. 1992. doi: 10.1109/72.159058.

[BD81] Dai, Hanjun and Khalil, Elias and Zhang, Yuyu and Dilkina, Bistra and Song, Le. (2017). Learning Combinatorial Optimization Algorithms over Graphs.

[BD82] Kingma, Diederik & Ba, Jimmy. (2014). Adam: A Method for Stochastic Optimization. International Conference on Learning Representations

[BD83] Ruder, Sebastian. (2016). An overview of gradient descent optimization algorithms.

[BD84] Ben Nassi, Asaf Shabtai, Ryusuke Masuoka, Yuval Elovici, 2019. “SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps”, arXiv:1903.05155v1 [cs.CR] 12 Mar 2019, https://arxiv.org/pdf/1903.05155.pdf

[BD85] Wang, Li, Jun Tang, and Qingmin Liao. "A Study on Radar Target Detection Based on Deep Neural Networks." IEEE Sensors Letters 3.3 (2019): 1-4.

[BD86] Chen, W. S., J. Liu, and J. Li. "Classification of UAV and bird target in low-altitude airspace with surveillance radar data." The Aeronautical Journal 123.1260 (2019): 191-211.

[BD87] Hu, Qintao, et al. "DiagonalNet: Confidence diagonal lines for the UAV detection." IEEJ Transactions on Electrical and Electronic Engineering (2019).

[BD88] Jin, Ren, et al. "Drone Detection and Pose Estimation Using Relational Graph Networks." Sensors 19.6 (2019): 1479.

[BD89] Xiaoping, Li, et al. "Fast Aerial UAV Detection Using Improved Inter-frame Difference and SVM." Journal of Physics: Conference Series. Vol. 1187. No. 3. IOP Publishing, 2019.

[BD90] Al-Emadi, Sara, et al. "Audio Based Drone Detection and Identification using Deep Learning." 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, 2019.

[BD91] Kim, J.; Park, C.; Ahn, J.; Ko, Y.; Park, J.; Gallagher, J.C. Real-time UAV sound detection and analysis system. 2017 IEEE Sensors Applications Symposium (SAS). IEEE, 2017, pp. 1–5.

[BD92] Matson, Eric, et al. "UAV detection system with multiple acoustic nodes using machine learning models." 2019 Third IEEE International Conference on Robotic Computing (IRC). IEEE, 2019.

[BD93] Kim, J.; Kim, D. Neural Network based Real-time UAV Detection and Analysis by Sound. Journal of Advanced Information Technology And Convergence 2018, 8, 43–52.

[BD94] Jovanoska, S.; Brötje, M.; Koch, W. Multisensor data fusion for UAV detection and tracking. 2018 19th International Radar Symposium (IRS). IEEE, 2018, pp. 1–10.

[BD95] Hengy, Sebastien, et al. "Multimodal UAV detection: study of various intrusion scenarios." *Electro-Optical Remote Sensing XI*. Vol. 10434. International Society for Optics and Photonics, 2017.

[BD96] Liu, H., Wei, Z., Chen, Y., Pan, J., Lin, L., & Ren, Y. (2017). Drone Detection Based on an Audio-Assisted Camera Array. In *Proceedings - 2017 IEEE 3rd International Conference on Multimedia Big Data, BigMM 2017* (pp. 402–406). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/BigMM.2017.57

[BD97] Park, S., Shin, S., Kim, Y., Matson, E. T., Lee, K., Kolodzy, P. J., … Hopmeier, M. (2015). Combination of radar and audio sensors for identification of rotor-type Unmanned Aerial Vehicles (UAVs). In *2015 IEEE SENSORS - Proceedings*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICSENS.2015.7370533

[BD98] Marcus H., Bjorn B., Marcus H., Michael A. “UAV detection, tracking and classification by sensor fusion of a 360° lidar system and an alignable classification sensor”, Proc. SPIE 11005, Laser Radar Technology and Applications XXIV, 110050E (2 May 2019).

[BD99] Arthur Holland Michel. “Counter-Drone Systems - 2nd Edition.” Center for the Study of the Drone at Bard College, December 2019 https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[BD100] Samaras, S.; Diamantidou, E.; Ataloglou, D.; Sakellariou, N.; Vafeiadis, A.; Magoulianitis, V.; Lalas, A.; Dimou, A.; Zarpalas, D.; Votis, K.; Daras, P.; Tzovaras, D. “Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review”. Sensors 2019, 19, 4837. https://doi.org/10.3390/s19224837

[BD101] Messina M., Pinelli G. (2019) Classification of Drones with a Surveillance Radar Signal. In: Tzovaras D., Giakoumis D., Vincze M., Argyros A. (eds) Computer Vision Systems. ICVS 2019. Lecture Notes in Computer Science, vol 11754. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-34995-0_66

[BD102] Thomas A., Leboucher V., Cotinat A., Finet P., Gilbert M. (2019) UAV Localization Using Panoramic Thermal Cameras. In: Tzovaras D., Giakoumis D., Vincze M., Argyros A. (eds) Computer Vision Systems. ICVS 2019. Lecture Notes in Computer Science, vol 11754. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-34995-0_69

[BD103] García M., Viguria A., Heredia G., Ollero A. (2019) Minimal-Time Trajectories for Interception of Malicious Drones in Constrained Environments. In: Tzovaras D., Giakoumis D., Vincze M., Argyros A. (eds) Computer Vision Systems. ICVS 2019. Lecture Notes in Computer Science, vol 11754. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-34995-0_67

[BD104] Samaras S., Magoulianitis V., Dimou A., Zarpalas D., Daras P. (2019) UAV Classification with Deep Learning Using Surveillance Radar Data. In: Tzovaras D., Giakoumis D., Vincze M., Argyros A. (eds) Computer Vision Systems. ICVS 2019. Lecture Notes in Computer Science, vol 11754. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-34995-0_68

[BD105] Diamantidou E., Lalas A., Votis K., Tzovaras D. (2019) Multimodal Deep Learning Framework for Enhanced Accuracy of UAV Detection. In: Tzovaras D., Giakoumis D., Vincze M., Argyros A. (eds) Computer Vision Systems. ICVS

2019. Lecture Notes in Computer Science, vol 11754. Springer, Cham. DOI https://doi.org/10.1007/978-3-030-34995-0_70

[BD106] The 1st Anti-UAV workshop and challenge, CVPR 2020, https://anti-uav.github.io/

[BD107] 3rd International Workshop on Small-Drone Surveillance, Detection and Counteraction Techniques (WOSDETC), AVSS 2020, https://wosdetc2020.wordpress.com/

[BD108] Sun, Han, et al. "TIB-Net: Drone Detection Network With Tiny Iterative Backbone." IEEE Access 8 (2020): 130697-130707.

[BD109] Seidaliyeva, Ulzhalgas, et al. "Real-Time and Accurate Drone Detection in a Video with a Static Background." Sensors 20.14 (2020): 3856.

[BD110] Koksal, Aybora, Kutalmis Gokalp Ince, and Aydin Alatan. "Effect of Annotation Errors on Drone Detection with YOLOv3." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2020.

[BD111] Behera, Dinesh Kumar, and Arockia Bazil Raj. "Drone Detection and Classification using Deep Learning." 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2020.

[BD112] Wang, Ye, et al. "Towards visible and thermal drone monitoring with convolutional neural networks." APSIPA Transactions on Signal and Information Processing 8 (2019).

[BD113] Unlu, Eren, et al. "Deep learning-based strategies for the detection and tracking of drones using several cameras." IPSJ Transactions on Computer Vision and Applications 11.1 (2019): 7.

[BD114] Lienhart, Rainer, and Jochen Maydt. "An extended set of haar-like features for rapid object detection." Proceedings International conference on image processing. Vol. 1. IEEE, 2002.

[BD115] Zivkovic, Zoran. "Improved adaptive Gaussian mixture model for background subtraction." Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.. Vol. 2. IEEE, 2004.

[BD116] Zhou, Huan, and Baorong Ni. "Tracking of drone flight by neural network Siamese-RPN." 2020 6th International Conference on Engineering, Applied Sciences and Technology (ICEAST). IEEE, 2020.

[BD117] Svanstrom, Fredrik, Cristofer Englund, and Fernando Alonso-Fernandez. "Real-Time Drone Detection and Tracking With Visible, Thermal and Acoustic Sensors." arXiv preprint arXiv:2007.07396 (2020).

[BD118] Martins, Bruno Oliveira; Arthur Holland Michel & Andrea Silkoset (2020) Countering the Drone Threat: Implications of C-UAS Technology for Norway in an EU and NATO Context, PRIO Paper. Oslo: PRIO. https://www.prio.org/utility/DownloadFile.ashx?id=2013&type=publicationfile

Annex A – List of Acronyms

Acronym	Meaning
AENOR	Spanish Association for Standardization and Certification (Spanish: Asociación Española de Normalización y Certificación)
AGL	Above Ground Level
AMC	Acceptable Means of Compliance
A-NPA	Advanced Notice of Proposed Amendment
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
ATOL	Automatic Taking-Off and Landing
BVLOS	Beyond Visual Line of Sight
C2	Command and Control
C3	Command, Control, Communication
CEN	European Committee for Standardization (French: Comité Européen de Normalisation)
CENELEC	European Committee for Electrotechnical Standardization (French: Comité Européen de Normalisation Électrotechnique)
C-UAS	Counter-UAS
C-UAV	Counter-UAV
DAA	Detect and Avoid
DEW	Directed Energy Weapons
DOA	Description of Action
EASA	European Aviation Safety Agency
EC	European Commission
ECM	Electronic Counter-Measures
EM	Electromagnetic
EMC	Electromagnetic compatibility
ENAC	Ente Nazionale per l’Aviazione Civile
EO	Electro-Optical
ERA	Enhanced RPAS Automation
ERC	European Research Council
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROCAE	European Organization for Civil Aviation Equipment
EUSCG	European UAS Standards Coordination Group
EVLOS	Extended Visual Line of Sight
FAA	Federal Aviation Administration
FMCW	Frequency Modulated Continuous Wave

GDPR	General Data Protection Regulation
GM	Guidance Material
GNSS	Global Navigation Satellite System
GUTMA	Global UTM Association
H2020	Horizon 2020
HMI	Human Machine Interface
HPM	High-Power Microwave
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
IR	Infra-red
ISO	International Organization for Standardisation
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LEA	Law Enforcement Agency
LSS	Low, Small, Slow
MASPS	Minimum Aviation System Performance Standards
MOPS	Minimum Operational Performance Standards
MS	Member State
MTOM	Maximum Take-Off Mass
MTOW	Maximum Take-Off Weight
NAA	National Aviation Authority
NPA	Notice of Proposed Amendment
OBW	Occupied bandwidth
OOB	Out Of Band
PANS	Procedures for Air Navigation Services
PSO	Project Security Officer
RCS	Radar Cross-Section
REC	Recommendation
RF	Radio Frequency
RMT	Rulemaking Task
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
RTCA	Radio Technical Commission for Aeronautics
SAB	Security Advisory Board
SARP	Standards and Recommended Practices
SESAR	Single European Sky ATM Research
SESAR JU	SESAR Joint Undertaking
SoEL	Societal, Ethical and Legal
SORA	Specific Operations Risk Assessment
SOTA	State of the art
SRD	Short Range Device
sRPAS	small RPAS

sUAS	small UAS
SWOT	Strengths, Weaknesses, Opportunities and Threats
TRL	Technological Readiness Level
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System; Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UTM	UAS Traffic Management
VLL	Very Low Level
VLOS	Visual Line of Sight
WP	Work Package

Annex B – Definitions

Expression	Meaning
Geofencing	Geofencing is a virtual geographic boundary, defined by GNSS technology that enable software to prevent a drone entering a defined zone ([ND26])
Radio Equipment	An electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination ([ND9])
Radiodetermination	The determination of the position, velocity and/or other characteristics of an object, or the obtaining of information relating to these parameters, by means of the propagation properties of radio waves ([ND8])
Radiolocation	Radiodetermination used for purposes other than those of radionavigation ([ND8])
Radionavigation	Radiodetermination used for the purposes of navigation, including obstruction warning ([ND8])
SOTA	State of the art (sometimes cutting edge) refers to the highest level of general development, as of a device, technique, or scientific field achieved at a particular time. It also refers to such a level of development reached at any particular time as a result of the common methodologies employed at the time. (https://en.wikipedia.org/wiki/State_of_the_art)