CEN

WORKSHOP

AGREEMENT

CWA 18150

October 2024

ICS 03.220.50; 49.020

English version

Unmanned aircraft systems - Counter UAS - Testing methodology

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 18150:2024 E

Contents

Page

Table of Figures

Table of Tables

European foreword

This CEN Workshop Agreement (CWA 18150:2024) has been developed in accordance with the CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid way to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by the Workshop CEN "Courageous", the secretariat of which is held by "ASRO" consisting of representatives of interested parties on 2024-09-04, the constitution of which was supported by CEN following the public call for participation made 2023-06-20. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2024-10-07.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

- Ecole Royale Militaire – Koninklijke Militaire School (RMA), Belgium

- Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO), Netherlands

- Police Grand-Ducale (PGD), Luxembourg

- Kentro Meleton Asfaleias (KEMEA), Greece

- Police Federale Belge (PFB), Belgium

- Ministerio del Interior (SMI), Spain

- Politsei- ja Piirivalveamet (PPA), Estonia

- Hellenic Police (HP), Greece

- The International Criminal Police Organization (INTERPOL), France

- Serviciul de Protecţie şi Pază (SPP), Romania

- Wojskowa Academia Techniczna im.jaroslawa dabrowskiego (WAT), Poland

- Universidad de Sevilla (USE), Spain

- Rheinmetall Air Defence AG, Switzerland

- RUAG MRO Schweiz, Switzerland

- Federal Office of Communications OFCOM, Switzerland

- OIP Sensor Systems, Belgium

- DFS Deutsche Flugsicherung GmbH, Germany

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patent". CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

Introduction

This document seeks to develop a standardized test methodology for UAS detection, tracking and identification systems. It has been developed within the framework of the project COURAGEOUS (Building a common understanding of the effectiveness of counter-UAS solutions) funded by European Union's Internal Security Fund Police under Grant Agreement 101034655. This standardized test methodology is based upon a series of standard user-defined scenarios representing a wide set of use cases. At this moment, these standard scenarios are geared towards civil security end users (e.g. prison & airport security, critical infrastructure protection, border security, drugs & human trafficking, etc). However, as the domain of counter-UAS is highly dual-use-oriented, more military scenarios are certainly also highly relevant. Therefore, this standard provides an open architecture where the standard scenarios are modularly provided as examples in annexes, providing the standard users the possibility to easily add new scenarios. For each of these scenarios, operational needs & functional performance requirements are provided. Using this information, an integral test methodology is presented that allows for a fair qualitative and quantitative comparison between different counter-UAS systems. This test methodology was validated during three user-scripted validation trials.

It is the aim that this standardized test methodology will lead to a much better understanding of the capabilities of counter-UAS systems within the EU network of law enforcement agencies. This is urgently needed, as member states are facing an increase in drone threats and there are no cohesive policies being developed across the region to try and manage the threat. It should be highlighted though that the most EU LEAs do not have a complete and detailed drone response strategy.

It should be highlighted that this standard test methodology focuses totally on the detection, tracking and identification (DTI) aspect of the counter-UAS "kill chain" and does not cover neutralisation aspects. The standard test methodology also concentrates on the qualitative and quantitative evaluation of DTI systems, configured as integrated solutions (so, not as individual sensors) as they are presented to end users. While the test methodology includes an end-user steered qualitative evaluation of the interface of the counter-UAS solutions, a full useability analysis of the Command & Control interface is not within the scope of this standard test method.

This document can be subdivided in 4 main parts:

- Part I (Clauses 1 – 4), providing a general introduction

- Part II (Clauses 5 - 8), focusing on the standard scenarios

- Part III (Clauses 9 - 11), focusing on performance requirements

- Part IV (Clauses 12 - 13), focusing on the actual standard test methodology

The scope of this document is wide. It targets different stakeholders, such as the counter-UAS industry, law enforcement agencies and policy makers, with actionable insights.

Main take-aways for the counter-UAS industry:

- Insight in operational needs and performance requirements of end users, to drive the design of the counter-UAS solutions

- A standardised way of testing and communicating performance specifications and capabilities of their products.

Main take-aways for end-users:

- Insights in the counter-UAS landscape (incidents, gaps, technologies)

- A way of developing and validating requirements specifications for better procurement decisions

- A standardised approach for performance measurements in order to better match selected counter-UAs solutions with the operational needs

Main take-aways for policy makers:

- Insights in the counter-UAS landscape (incidents, gaps, technologies)

- A better understanding of the capabilities counter-UAS systems, through standardised testing methods.

1 Scope

This document develops a standardized test methodology for assessing the performance of solutions for the detection, tracking and identification of drones in order to protect the lower airspace. This standardized test methodology is based upon a series of standard user-defined scenarios representing a wide set of use cases (e.g. prison & airport security, aviation safety, critical infrastructure protection, border security, drugs & human trafficking, etc).

For these scenarios, operational needs and functional performance requirements were extracted by end-users. Using this information, an integral test methodology was developed that allows for a fair qualitative and quantitative comparison between different counter-UAS systems.

The scope of this document focuses on sensors for detection, tracking and identification, integrated in a C2 system and does not cover the defeat or disable aspects, as indicated by the figure below.
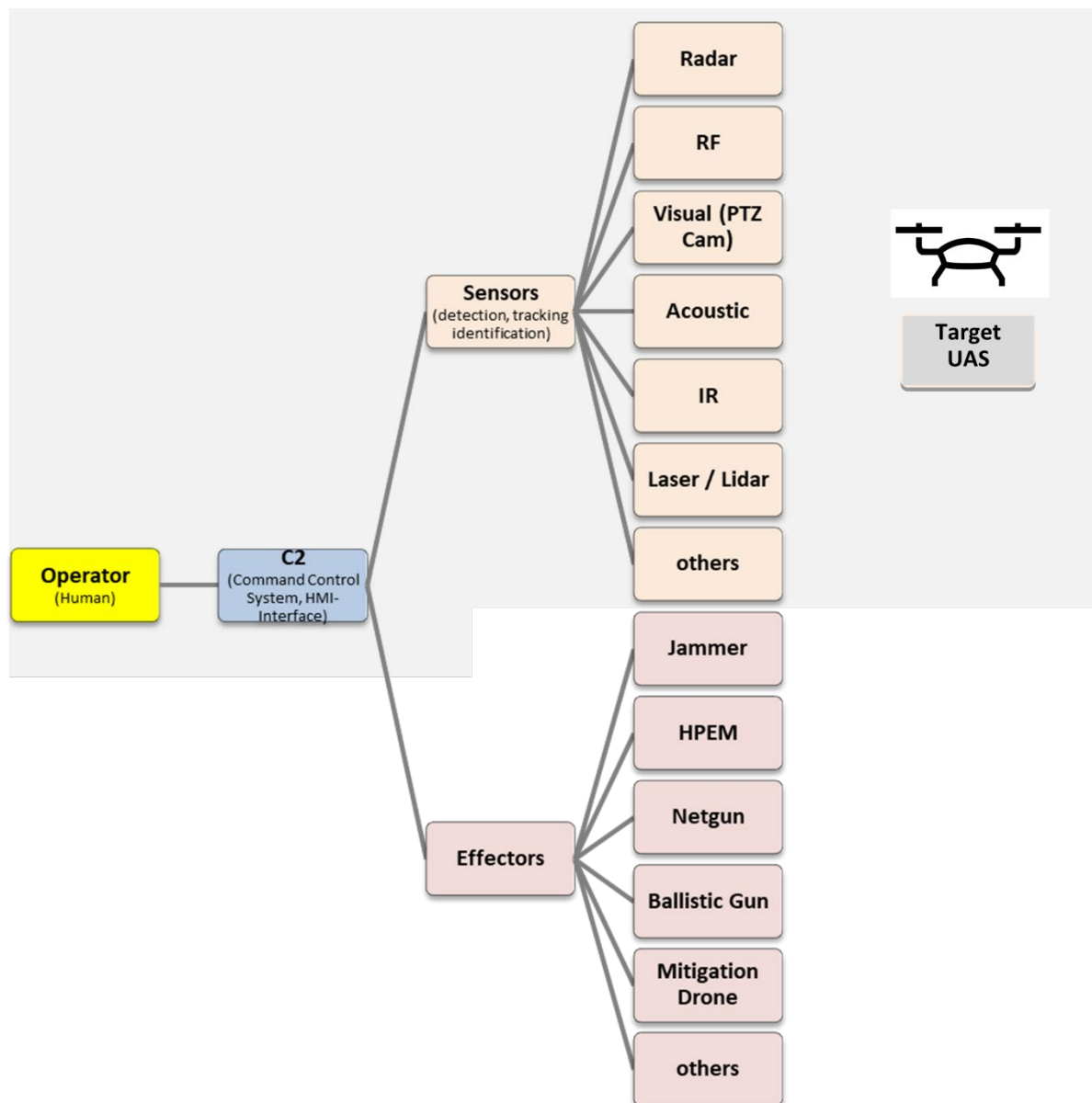
Figure 1— C-UAS system overview

2   Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 21384-4, *Unmanned aircraft systems — Part 4: Vocabulary*

ISO 21895, *Categorization and classification of civil unmanned aircraft systems*

3   Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21384-4, ISO 21895 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/

- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
unmanned aircraft system (UAS)

unmanned aircraft (an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft) and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot to operate safely and efficiently in the airspace system

3.2
counter unmanned aircraft system (C-UAS)

system or device capable of lawfully and safely detect, track, identify, disable, disrupt, or seize control of an unmanned aircraft or unmanned aircraft system

3.3
absolute coverage of a C-UAS system

stacked coverage of all integrated sensors

3.4
classification

ability to classify the object (e.g. airplane, balloon, drone)

3.5
detection

instance of a sensor system reacting to a stimulus and initiate processing of data, possibly generating an alarm

3.6
detection point

range at which the UAS is sensed by the C-UAS solution

Note 1 to entry: The detection point is characterized by coordinate referenced from C-UAS location

3.7

detection volume

three-dimensional (3D) plot of the Detection Point coordinates that creates a volume during which the sensor can be expected to initiate an alarm caused by the presence of the UAS stimulus

3.8

drone detection system

function that detects unmanned aircraft systems in space and, if possible, locates, tracks, classifies and identifies them

[SOURCE: DIN 5452-9]

3.9

probability of detection

probability that the C-UAS is able to detect a UAS of a certain size at a certain distance from the detection system

3.10

identification

ability to describe the object in detail (e.g. DJI Phantom 4, DJI Mavic Air 2)

3.11

tracking

displaying or recording of successive positions of the moving UAS

Note 1 to entry: Tracking position information includes providing the current location of the UAV at least every second.

3.12

localisation

range at which 2D or 3D coordinates of the UAS are obtained by the C-UAS location

3.13

verification

confirmation and assessment of the potential danger posed by the drone based on external characteristics such as payloads (cameras, explosive devices, transport boxes, etc.), e.g. visually by an operator

[SOURCE: DIN 5452-9]

3.14

swarm

group of drones that carry out tasks cooperatively

Note 1 to entry: This cooperation can take place in flight by the drones based on predefined rules among themselves, through coordinated control inputs from the remote pilots during the flight or before the flight through coordinated planning of the missions to be flown

[SOURCE: DIN 5452-9]

4 Abbreviations and symbols

For the purposes of this document the following abbreviations apply.

AGL	Above Ground Level
AoI	Area of Interest
ATM	Air Traffic Management
BLOS	Beyond (Visual) Line of Sight
BSF	Border Security Force
BTS	Base Transceiver Station
CBRN	Chemical, Biological, Radiological, Nuclear
C&C	Command and control
CEN	The European Committee for Standardization
CIP	Critical Infrastructure Protection
CNB	Central Narcotics Bureau
COTS	Commercial Off The Shelf
C-UAS	Counter Unmanned Aerial System/Counter Unmanned Aircraft System
CWA	CEN Workshop Agreement
DESCA	Development of a Simplified Consortium Agreement
DoA	Description of Action
DTI	Detection-Tracking-Identification
EASA	European Union Aviation Safety Agency
EC	European Commission
EM	Electro-Magnetic
EMP	Electro-Magnetic Pulse
EO	Electro-Optical
ERC	European Research Council
EU	European Union
FAR	False Alarm Rate
FAQ	Frequently Asked Questions
GA	General Assembly
GCS	Ground Control Station
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface
ID	Identification
IED	Improvised Explosive Device
IMU	Inertial Measurement Unit
INTERPOL	The International Criminal Police Organization
IP	Intellectual Property
IR	Infrared Radiation
ISF	Internal Security Fund

ISFP	Internal Security Fund Police
KPI	Key Performance Indicator
LAN	Local Area Network
LEA	Law Enforcement Agency
LCEG	Law Enforcement Agency Community Engagement Group
LUC	Light UAS operator certificate
MAR	Missed Alarm Rate
ML	Machine Learning
MS	Member State
MSL	Mean Sea Level
MTOM	Maximum Take-off Mass
NATO	North Atlantic Treaty Organisation
NTP	Network Time Protocol
POD	Probability Of Detection
RBW	Resolution Bandwidth
RCS	Radar Cross Section
RF	Radio Frequency
SAB	Security Advisory Board
UAS	Unmanned Aircraft System/Unmanned Aerial System
UAV	Unmanned Aircraft Vehicle
UC	Use Case
UTM	UAS Traffic Management
VLOS	Visual Line of Sight
VTOL	Vertical Take-off and Landing
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
2D	Two-Dimensional
3D	Three-Dimensional
4G	Fourth generation broadband cellular network
5G	Fifth generation broadband cellular network

5   Incidents analysis and identification of gaps

5.1 General

The analysis of previous drone incidents and identification of gaps has been created to help understand the evolving incident landscape involving drones and to identify gaps in current responses to such threats. Over the last five years drones have become a more common and emerging threat used by criminals, terrorists as well as the public who are usually clueless, careless, or uninhibited in their use of the drone.

The threat from drones is increasing. In the past years, drones have become more accessible and acquirable for most people. This has also been driven by companies, such as DJI, making and marketing drones as a tool for everyone to take aerial photos and videos. The commercial drone industry has

seen rapid development and investment as the technology becomes cheaper, accessible, and more reliable. With this, the criminal and terrorist elements of society have also adapted their response to include drones to carry out attacks, surveillance, and menace within member states.

One major outcome is there is not a coordinated approach to drone incident reporting within member states and many different entities have different roles and responsibilities in this area. For example, if a traditional crime is committed, it is reported to the police, and they investigate the crime. If successful they arrest, charge, and try the suspect. However, in drone incidents, the police, civil aviation authority and owner of the building or area where the drone threat exists must be involved. This is usually because, majority of the time, the drone is classed as an aircraft.

As drone becomes a more prevalent part of everyday life, the likelihood of a drone incident becomes more likely. Member states, as well as the region, should employ the right technology to detect, track and locate drones within an airspace and then utilize the appropriate response to the incident.

The use of countermeasures to detect, track and locate a drone within an airspace should be paramount as a first line of defence but this should also be supported by other initiatives such as public awareness, collaborative entities to share data and information around drone threats, and the appropriate training for law enforcement and associated entities to respond to such incidents.

Eight hundred and twenty-three drone incidents from across the globe have been gathered and has analysed to identify trends and any gaps that should be filled to ensure a coherent and cohesive approach to the drone threat across member states.

The following incident areas were identified (see Table 1).

Table 1 — Incident Areas/Environment

Incident Area	Description
Airports	The area in and around an airport including sightings by aircraft or members of the public within the vicinity of the airport environment
Energy/Utilities	Installations such as power plants, water treatment plants or communication hubs and critical infrastructure
Entertainment/Media	Film sets or filming of environments or incidents by media outlets
Government/Military	Army, navy or aircraft bases and government offices or parliament buildings
Defence & Aerospace	Attacks or intelligence gathering (stationary or mobile) on dismounted troops, single vehicles, platoons or fixed installations
Landmarks	Landmarks or public/government buildings
Law Enforcement/First Responders	Incidents where drones have affected or resulted in law enforcement, medical or fire services to adapt their response to an incident or event
Prisons	Area in and around a prison where drones are used to smuggle contraband into the prison
Private/Non-Corporate	Areas of non-commercial locations or private residences
Stadiums	Locations where sporting events or concerts are held and there is a public mass gathering.
Hospitality/Real Estate	
Transportation (non-airports)	
Technology	
International Summit / international meeting of heads of states or government	

The three main areas for incidents are Airports, Law Enforcement/First Responders and Private/Non-Corporate. This is possible since there is a lot of awareness around drones in the vicinity of airports. Drone pilots wishing to capture a one-in-a-million shot of law enforcement or first responder incidents such as a siege or forest fire could be another possible explanation. The private/non-corporate area is a huge proportional as most incidents happen in this area due to drones flying above residential properties and areas. Majority of the incidents in this category seem to be caused by residents who are living local to the site of incident. When the incident involves acts such as harassment or intimidation, this is seen as a premediated attack and is interpreted as such. This means that the person brought the drone and flew a drone in a particular area to cause distress or to intimidate an individual.

The drone incidents can be categorized by following incident types (see Table 2).

Table 2 — Types of incidents

Incident Type	Description
Activity Interruption	Where the day-to-day operations or activities in a location was affected by a drone incursion
Attack	Use of a drone to carry out an attack on an individual or building (non-explosive)
Crash	A drone has crashed into a building, object, or the ground
Explosion	A drone was used to deliver and detonate an explosive to a target or area
Harassment	A drone was used to cause aggressive pressure or intimidation.
Injury	A drone was used to cause injury to member of the public or target
Near Miss	A drone was part of a near collision with a vehicle, aircraft, or ship
Smuggling	A drone was used to carry prohibited or illegal substances into a prohibited area, cross country or across a border
Spying / Espionage / Intelligence	Drones were used to spy or gain intelligence from a location or individual
Terrorist/Civilian Threat	Drones were used to threaten or cause panic by criminals or terrorists
Trespassing	Drones flying in a designated no fly zone, no drone area or private property

According to the type of threat the following identified categories are described below:

Table 3 — Drone Threat Classification

Drone Threat Classification	Description
Clueless	Operator is ignorant of, or does not acknowledge regulations, no fly zones, and requirements by flying wherever and however they please.
Careless	Operator, most of the time, complies with regulations, flies safely, yet occasionally ventures out of these boundaries (flying above maximum altitude or outside permitted zones)
Compliant	Operator complies with the regulation, staying within the approved flying zones and visual requirements (VLOS/daytime)
Uninhibited	Operator continuously pushes regulatory boundaries, intentionally flies in restricted airspace yet rarely means harm or menace
Criminal	Operator flying a drone with an intent to carry out an illegal act (e.g., Prison contraband, illegal surveillance)
Terrorist	Operator within terrorist cells utilizing any means to accomplish their potentially lethal or destructive objective.
Military	Operator flying a drone to gather intelligence, deploy explosives, assess battle damage or the like.

Most incidents were caused by uninhibited drone pilots who pushed the boundaries of the drone to enter restricted area, no fly zones, or just wanted to see what the drone could do and how it could be utilised. Most drone pilots are novices and just want to capture or utilise the drone in a way that they have seen on social media, in movies, or are just curious about what they can accomplish with the drone.

The criminal and terrorist elements are using drones to accomplish definitive outcomes such as smuggling illicit goods, surveillance of areas or to cause panic and damage to buildings or individuals. This element seems to be increasing year on year as the accessibility and cost of drones becomes more accessible and available.

The ease of operation of drones is also a factor. When drones first became a consumer product, the skill and prowess to control a drone was still relatively high. However, as drones have become more automated and easier to control, the number of drone pilots have also increased.

Along with the number of drones in the market, the sizes and capabilities of them have also increased. For instance, when many countries introduced regulations stating that any drone above 250 grams will need to be registered, a company released a drone with obstacle detection and avoidance that weighed 249 grams thus circumventing the need for registration.

These budget drones also attract the clueless, careless, or uninhibited drone owners as the entry to market is low. The need to adhere to member country regulations such as having to take a test or register the drone is also minimal.

In the analysis, sometimes it has been difficult to categorize the incident under a particular drone threat category. Hence, when such an issue occurs, the incident it is analysed and based on information supplied it is categorised depending on the location of the incursion, if anyone was injured, if it interfered with operational activities and if a suspect was apprehended as result of the incident. If the incident was intentional, such as harassment of a target or individual then this would have been classed as criminal rather than clueless/careless or uninhibited since the drone was aimed as a specific target or individual.

When a drone incident has taken place in a specific environment but could be classed in more than one environment then the primary environment is considered. For example, if a drone is flown above a stadium, it will be classed under stadium and not Entertainment/Media or Private/Non-Corporate.

All incidents have been classed as one type, but it is possible that it could be multi category. For the purpose of this analysis, the process have been simplified as using more than one type of incident would have blurred the analysis and may have caused a misinterpretation of results. For instance, a drone flying above a stadium where a sporting event is taking place could be classed as civilian threat and activity interruption and so based on identifying the primary threat was evoked. If a drone is flying above a stadium and the sport event is delayed or stopped then this would be classed as activity interruption and if the report does not identify that the stadium attendees or athletes were under threat, or the drone indicated a threat to the people or athletes then this would be classed as activity interruption rather than a civilian threat.

NOTE The data collected was from numerous resources such as news sites, drone specialist sites, drone countermeasure bulletins and companies such as DroneSec, Dedrone, DG HOME's "Overview of noteworthy security/safety incidents involving unmanned aircraft systems (UAS)", and agencies located within member states/countries such as France, Germany, Singapore United Kingdom and United States.

5.2 Criteria for incident analysis

The scope of this section is to establish a set of criteria playing key roles in the analysis of the incidents. The following criteria were identified:

Criterion 1 – Environment

Table 4 — Types of environments

Type of Environment	Definition
Rural	Rural areas are areas that are open and spread out with a small population.
Surburban	Suburban areas are areas that are mainly residential area with a larger population than rural areas.
Urban	Urban areas are areas that consists of both living and working areas and have high population.
Not Available	Not Available

Criterion 2 – Time of day

Table 5 — Definition of the time of day

Time of Day	Definition
Day	Incident occurred during daylight hours
Night	Incident occurred at night
Not Available	Time of incident is unknown

Criterion 3 – Weather

Table 6 — Definition of the weather conditions

Weather	Definition
Sunny	A sunny day with little or no cloud coverage
Cloudy (including rainy)	A day with lots of clouds that also might include rain
Not Available	Unknown weather condition

Criterion 4 – Presence of other aircrafts/UAVs in the nearby airspace

Table 7 — Definition of the presence of other aircraft

Presence of other aircraft or UAV	Definition
Yes	Evidence of other UAVs or aircraft present
No	No evidence of other aircraft or UAVs present
Not Available	No information available around the presence of other aircraft or UAVs

Criterion 5 – Type of UAV

Table 8 — Definition of the types of drones

Type of UAV [1]	Definition
Multirotor	Multirotors are UAVs that use more than two rotors with fixed pitch spinning blades that generate lift. By changing the speed of the rotors so that the thrust generated is greater than, equal to or less than the forces of gravity and drag acting on the aircraft, the drone can be made to ascend, hover or descend.
Fixed Wing	Fixed-wing drones (as opposed to 'rotary wing', i.e., helicopters) use a wing like a normal aeroplane to provide the lift rather than vertical lift rotors. Because of this they only need to use energy to move forward, not hold themselves up in the air, so are much more efficient.
Not Available	Type of drone could not be verified

Criterion 6 – Number of UAV

Table 9 — Definition of the number of drones

No of UAVs	Definition
1	Only one UAV was present at incident
<3	2 or 3 drones present at the incident
Swarm	More than 3 drones were present at incident
Not Available	Sufficient information was not available to ascertain the number of drones involved at the incident

Criterion 7 – Custom or Commercial

Table 10 — Definition of the category of drones

Category	Definition
Commercial	A drone that can be brought off the shelf and requires no or small modifications to operate
Custom	A drone that is assembled by the owner from different components that require self-assembly to create the drone
Not Available	Drone type cannot be confirmed

---

[1] The configuration in cruising status defines the type of UAV, not the take-off or landing configuration. Typically, hybrid vertical take-off and landing drones would thus qualify as fixed wing drones

Criterion 8 – Payload

Table 11 — Definition of the payload characteristics

Payload	Definition
Camera	Drone was carrying a camera as its payload that can be used to take photographs or film
Contraband	A prohibited item ('contraband') is anything introduced or found into an area that is not permitted. A prohibited item ('contraband') is anything introduced or found that is not permitted. Examples of contraband are drugs, weapons, or mobile phones (Prison environment)
Weapon (CBRN, IED etc)	An explosive, chemical or radiological weapon that is intended to cause harm or death
Not Available	Payload cannot be confirmed

Criterion 9 – Available DTI systems

Table 12 — Definition of the presence of DTI systems

DTI Present	Definition
Yes	System that can detect, track, identify a drone is present
No	No system that can DTI present
Not Available	No information available around DTI system present

Criterion 10 – Type of flight area (Restricted / Un-restricted)

Table 13 — Definition of the restricted flight area denomination

Restricted flight area	Definition
Yes	Drone was flown in designated restricted area such as 5km of an airport etc.
No	No flight restrictions
Not Available	No information available around no-fly zone available

Criterion 11 – Severity of the incident

Table 14 — Definition of the drone incident severity levels

Severity of Incident	Definition [2]
Catastrophic	Infrastructure destroyed; Loss of lives; Sever disruption to services and confidence in the system.
Critical	A large reduction in safety margins, physical distress or a workload such that operational personnel cannot be relied upon to perform their tasks accurately or completely; Serious injury; Major equipment damage; Major disruption to services and confidence in the system
Serious	A significant reduction in safety margins, a reduction in the ability of operational personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency; Serious incident; Injury to persons; Substantial disruption to services and confidence in the system
Marginal	Nuisance; Operating limitations; Use of emergency procedures; Minor incident; Minor disruption to services and confidence in the system.
Negligible	Few consequences; No disruption to services

5.3 Gap Identification and Analysis

Appropriate processing of more than 200 drone related incidents that took place within the European territory led to the identification of gaps and needs in the current establishment of technical countermeasures used by the relevant authorities as well as the potential offensive drone capabilities and patterns. The following analysis is based on the identification of common characteristics and listing gaps as challenges for the current state of play in the field of illegal drone detection resulting from:

- The limitations of the DTI systems
- The capabilities of UAVs
- The intrinsic characteristics of the field of action

Table 15 — Gaps and challenges

DTI systems	Besides the fact that most incidents do not explicitly report the existence of a DTI system operating at the area of interest, only a 5% of the incidents report existing DTIs established in the nearby area or infrastructure.
Urban areas	DTIs face several limitations in performing satisfactorily in congested areas. The dense populated RF spectrum challenge the capabilities of drone RF detectors while the crammed buildings offer the appropriate hiding set for a rogue drone.
No weather preference	It seems that there is no weather-related preference when acting illegally using a drone. More commercial drones are now becoming rain-resistant pushing DTIs to perform under all weather and lighting conditions.

---

[2] Based on EASA's risk consequences table in "Drone Incident Management at Aerodromes" document

Presence of other UAVs/aircrafts	Presence of other UAVs in the area where the incident is taking place is quite possible, rendering the detection of the illegal drones a demanding task for DTIs as these have to distinguish between hostile and harmless drones.
Incidents in non-restricted areas	Most incidents were reported in restricted areas. Nevertheless free-access areas are more susceptible to illegal activities as technologies of surveillance and detection are difficult to deploy e.g. due to legislation.
Custom products	Custom drones are not being present in the majority of the incidents, nevertheless they constitute a real threat indeed, as their custom set up (e.g. communication frequencies) can elude from certain components of the DTIs.
Payload	While most incident reports describe a camera being used as payload at the drone, the capability of drones to carry a wide range of payloads (e.g weapons, IEDs, CBRN) that are not easily classified from a distance, constitutes this fact a significant threat and challenge that should be addressed from the DTIs despite their infrequent use.

Nevertheless, further from environmental and technical obstacles that hinder the effective and prompt detection of mischief drones, it should be highlighted that there are quite a few factors that can be exploited in favour of the DTI systems. These factors are listed below as strengths.

Table 16 — Strengths

Rural areas	DTIs perform better in sparse populated areas where the background RF signals can not obscure a drone's communications and the open space of the scenery can easily reveal a drone to a radar or electro-optical sensor.
Lighting conditions	It seems that the majority of the illegal drone related events are happening in daytime hours, offering a better chance for the sunlight-based sensors to make a detection.
Type of UAV	Preference in a single type of UAV i.e. multirotor, further assists the DTIs to exploit the specific attributes of this type of UAV.
Incidents in restricted areas	Most incidents were reported in restricted areas. These areas are usually under a surveillance status and is relatively easier to apply additional measures for drones' detections. Being a restricted area also means that a system can be effective in distinguish between hostile and cooperative drones, having in mind the upcoming implementation of U-Space.
Number of UAVs	In the vast majority of reported cases, only one UAV is involved in the incident making easier the tasks of DTI systems.
Commercial products	Off-the-self UAVs are currently preferred for illegal actions as these can be easily purchased while providing a range of capabilities. This fact is also a positive point for DTI systems as commercial drones have more possibilities to be detected, identified and tracked.

6 Review of Current C-UAS Frameworks (Methods & Technologies)

6.1 General

With the rise of drone incidents member states and law enforcement will have to adapt their response to such threats from criminals, uninhibited, clueless, or careless drone pilots, while military forces will have to adapt their response to emerging aerial threats, for military operations other than war as well as for the battlefield. As the threat is asymmetrical, this is not easy as the drone would most likely be airborne when it is first spotted, so an appropriate response is required. Many member states have or are developing such responses, but this takes time to implement. There is also a need to educate and train the responders to the drone incident on handling and police the incident alongside ensuring public safety and security. Many agencies are implementing programs to respond to drone incursions but as drone technology evolves faster than the required response this will always be a constant developing situation.

Drone technology and drones are becoming more widespread as the cost and efficiency in using drones are starting to be realised. For instance, drones are used to deliver vital medical supplies, mail and test samples from the mainland to island communities and hospitals. This is a quick and efficient way to deliver supplies across a country. Every month there are new uses for drones such as 3D mapping, remote surveillance, landscape evaluations to detect deforestation or human activity, and remote security/border patrols. As these applications of drone technology expands, so does the threat from them.

European Union member states are moving toward U-Space, a collection of digitalised and automated functions and processes aimed at providing safe, efficient, and fair access to airspace for the growing number of civilian drone operations. U-Space provides a framework to facilitate the implementation of all types of operation in all classes of airspace and all types of environments, while ensuring an orderly coexistence with manned aviation and air traffic control.

As U-Space is adopted, the need to detect, identify, and locate both the drones and the operators also increases. Legislation in member states should safeguard and prevent most drone incidents. Still, if you have a clueless, careless, or criminal drone operator who does not obey the regulations, then the U-Space's effect could be catastrophic. Collision or crash that will not only damage the drones but also cause damage to the local infrastructure or injure members of the public in the vicinity of the accident.

While the evolution of technology of drones gathers pace, it can be observed the following effects on the capability of drones in general:

- Ease of Use: Operating a drone is rather straightforward. Many drone systems today ensure that anyone can pilot it. These systems can range from detecting and avoiding obstacles to point-to-fly where one can set a location and the drone will fly there.
- Cost: The cost to buy, own and run a drone is relatively low especially in second-hand markets.
- Battery Life: Batteries used to be an issue for drones as flight times were limited to fifteen minutes. But now drones can fly up to half an hour on a single charge or even longer if using multiple battery cells.
- Non-Commercial Solutions: Building a drone from scratch using off the shelf components is easily available and one can build it without any experience. Many websites and online tutorial videos offer step-by-step instructions ranging from required tools and software to build a drone.
- Drone Community: A thriving online community is available to share knowledge and expertise. They are ever willing to answer any questions one may have regarding drones and its associated technology through online forums and sites.
- Availability of Advanced Materials: Drone manufacturers are making their materials more commonly available as they try to reduce the weight and fragility of drone and its associated components.
- Use of Off the Shelf Systems: Most of the incidents involve off-the-shelf solutions that anybody can purchase online or from a shop.

- Lack of Detection of Drone Incursions: Many sensitive sites such as major airports, power stations and security sensitive sites lag behind in their physical security.
- Drone Capabilities: Most of the incidents seem to use multi-rotor drones as they are easy to fly compared to fixed wing or VTOL drones.
- Adaption of Drone Capabilities: Many of the drone incidents seem to use off the shelf drones with no modifications. Most modifications will utilise the existing drone frame and electronics and just add a release mechanism to drop the contraband or explosives and these mechanisms are very primitive.

Due to the above arguments, the need to develop anti-drone systems, i.e. systems that will independently detect, track and identify a passing drone, is important. Producers of such systems develop their technologies faster and faster. The development of drones' DTI technology is a positive phenomenon, but due to the variety of technologies used and their combinations in one system, the end user of such a system may have a growing problem with selecting the C-UAS system appropriate to their needs. Therefore, it seems logical to systematise the drones' DTI systems and unify the possibility of choosing such a system for the needs of specific units or critical infrastructures. Due to above needs, it is important to review the C-UAS systems available on the market in terms of framework and technology.

There is a very wide variety of different technologies used in the field of drone detection, e.g. via RF spectrum monitoring, radars, daylight cameras, thermal cameras, and acoustic sensors. The goal of this section is not to extensively analyse each and every available technology and its developments, but rather to develop procedures that can empirically demonstrate their utility on specific targets and in specific scenarios. In order to enhance the readability of the document, the focus is on the main (most used) detection, tracking and identification (DTI) technologies available today.

The 7 most used types of technologies used to detect, track and identify unmanned aircraft systems (UAS) are: radars, visible light (VIS) cameras, thermal imaging cameras, infrared (IR) sensors, laser distance finders – lidars, frequency monitoring devices and acoustic sensors. The above technologies are described in this document. After a review of solutions available on the market for DTI of drones, a summary table of companies and their system solutions was created (it is included in Table of available C-UAS). The basic parameters of the technology are given, such as: ranges, fields of view (in elevation and azimuth), frequencies they use, are those technologies omnidirectional or the number of sectors covered by the technology field of view, whether the system detects the drone, its operator or the communication between them, is the system equipped with artificial intelligence, or has it the ability to learn in a new given environment, etc. In addition, the operational parameters of the systems are also given, such as: mobility of the system (is it fixed, mobile, handheld, vehicular), whether it contains control software, type of power supply, the possibility of extending a given system with other technologies, the number of operators necessary to operate it, the difficulty of using the user interface, or the time needed to set up the equipment.

The quality, ranges, the multitude of sensors used for C-UAS and finally the choice of a given technology for a specific application is a big challenge. In addition, there are no metrics that would make it possible to compare the necessary parameters of various technologies with each other. Another problem is the possibility of using several different technologies in one C-UAS solution.

Therefore, this clause has the objective of developing comparative metrics for C-UAS solutions. In addition, this clause indicates the legitimacy of using a given technology or combination of technologies in a specific application. Also, it is an introduction to proposing a methodology for conducting field tests of selected C-UAS solutions, as it indicates the limitations resulting from the physical basis of the technology as well as the limitations resulting from the design and usability of the technology.

6.2 Analysis of available C-UAS solutions and response methodologies

6.2.1 General

Existing C-UAS solutions use various technologies for detection. The purpose of each is to enable maximal detection, identification, and tracking of UAS. For the purpose of this document, the following definitions are presented to establish a clear and shared understanding. The three concepts presented earlier are defined first: UAS detection, identification, and tracking.

6.2.2 Existing C-UAS solutions analysis

6.2.2.1 Available C-UAS solutions

Identification and analysis of available C-UAS solutions in the market in terms of the key technologies used in C-UAS: detect, track and identification.

When mentioning UAS detection, this section refers to detecting a moving or stationary UAS in the air using any technology. Depending on the size of the UAS, its distance, and atmospheric conditions, the probability of detection for the same technology will differ. The probability of detection will also vary depending on the technology used. In addition to detecting the UAS, the detection system should be able to determine its position in space, speed, and direction of movement.

When mentioning UAS identification, this document refers to the functionality of the C-UAS that allows to independently determine its size, type, name of the manufacturer and model (in the case of mass-produced devices), as well as in some cases to determine the size and type of payload carried by UAS. Identification is carried out with a certain probability, depending on the technology, weather conditions, and UAS distance.

Lastly, when mentioning UAS tracking, this document refers to the functionality of the C-UAS that allows, over a range of distances or in a well-defined space, to continuously determine the position, speed, and direction of the UAS. Suppose the C-UAS solution is equipped with cameras - the tracking function shall be capable of controlling the PT mechanism of the camera so that the UAS being tracked remains within the field of vision of the camera.

6.2.2.2 Detection and identification ranges

Analysis in terms of the detection and identification ranges of the C-UAS vs. sizes of drones and grouping of those systems.

The choice of technology when selecting C-UAS is particularly important. Each of the methods of detecting and identifying drones has its limitations resulting from specific physical phenomena used in the operation of given devices.

As part of the technological reconnaissance carried out, it should be clearly indicated that the commercial market is dominated by 7 main technologies that are used in C-UAS. These include: microwave radars, visible light cameras, thermal imaging cameras, infrared sensors, lasers/ range-finding lidars, frequency monitoring systems, acoustic sensors. Most C-UAS solutions use frequency monitoring; there are 92 of them among the relevant C-UAS found. The second most used are microwave radars – seventy-nine. Sixty-seven systems use visible light cameras. Thermal cameras are used in 51 systems. The other technologies used are:

- three infrared sensors,
- six lasers (more precisely lidars – for distance measurement), and
- Seventeen systems based on the operation of acoustic sensors.

The discussed technologies are graphically presented in Figure 2.
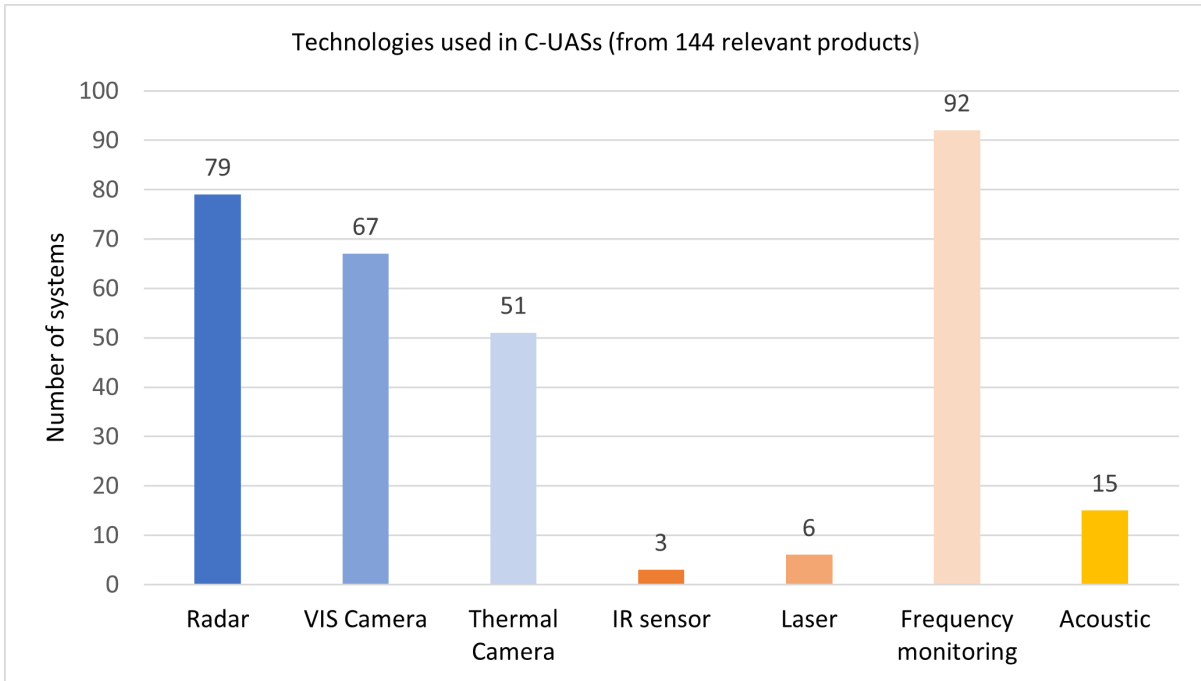
Figure 2 — Technologies used to detect, track and identify (*DTI*) in C-UAS solutions, in numbers

The diagram in Figure 3 shows the frequency bands these technologies operate.
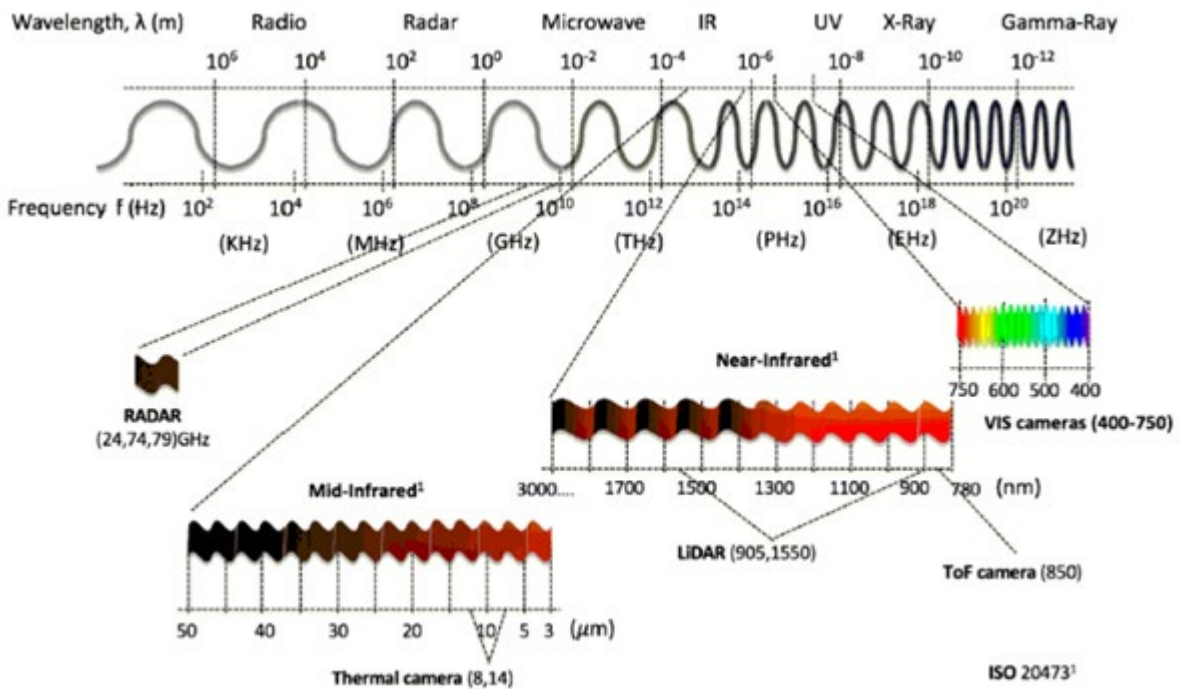
Figure 3 — Wavelengths of technologies used in C-UAS solutions, *ISO 20473:2007(e), Optics and Photonics—Spectral Bands, i. O. F. Standardization. 2007*

Due to the significant differences in the physical basis of the operation of individual types of detection devices, it is worth highlighting the main shortcomings of the systems:

- not all detection methods enable 24/7 operation, especially at night;
- the specificity of operation, particularly IR (infrared sensors) and VIS (daylight) cameras, do not allow detection in satisfactory imaging zones with appropriate resolution. These technologies are mainly used to implement other functions: tracking and identification;
- as an active detection method, the range of microwave radiation requires a thorough analysis of the possibility of using radar devices in terms of approval for use (power, frequency) in a given use scenario. Moreover, according to the properties of such radiation, a clear, defining characteristic of a given device with respect to atmospheric conditions (rain, fog) is to be expected;

In the case of measurements in the range of acoustic and radio frequencies, the background level in the test environment plays a crucial role in proper detection, which is essential in some scenarios of using the technology. Additionally, systems based on radio frequency analysis are ineffective in detecting objects that do not maintain any communication.

It should be noticed that in the realm of radio devices, compliance with European Union (EU) legal norms is imperative, particularly in ensuring the safety of usage. Any operation or utilisation of radio equipment must strictly adhere to the regulatory standards set forth by the EU, with a specific focus on safety considerations. These guidelines encompass aspects such as frequency allocation, technical specifications, and electromagnetic compatibility, aiming to establish a harmonized and interference-free radio spectrum while prioritizing user safety.

Similarly, when dealing with devices harnessing laser radiation, strict adherence to EU legal standards is indispensable, emphasizing the crucial aspect of safety. The use of laser-emitting devices must comply with regulations concerning safety, emission levels, and potential health hazards. EU directives provide a comprehensive framework to safeguard both public health and environmental concerns associated with laser technology, promoting the secure and responsible usage of such devices.

In conclusion, whether dealing with radio devices or those utilizing laser radiation, it is crucial to abide by the established norms within the European Union, with a heightened emphasis on safety considerations. Adherence to these regulations not only ensures the seamless functioning of technology but also prioritizes the safety and well-being of individuals and the environment. Compliance is paramount in fostering a secure and standardized technological landscape within the EU.

Due to the above-described shortcomings of the primary measurement/ detection technologies, the market offers the enrichment of devices and systems with elements of modern signal analysis and construction of integration interfaces in the form of software functionalities. Among the relevant products, C-UAS solutions have functionalities that use artificial intelligence technologies or have a related functionality so-called "Machine Learning," which allows systems to be adapted to the conditions in a given location or the type of detected drone.
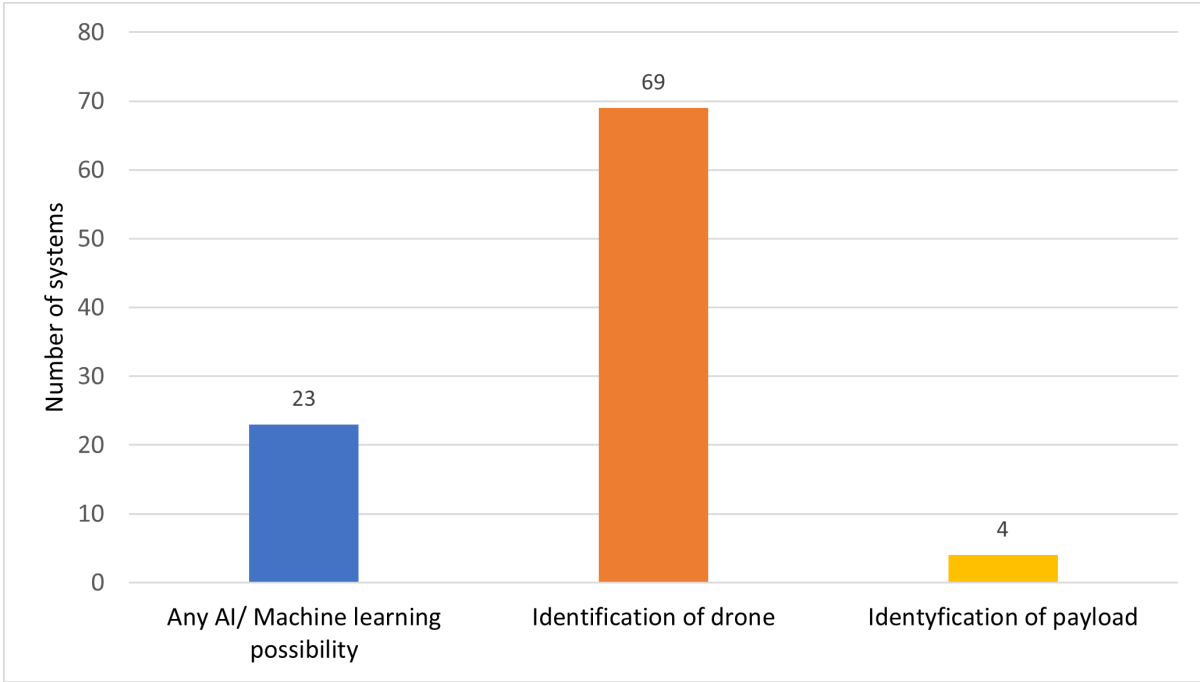
Figure 4 — Additional functions (except DTI) that C-UAS solutions allow
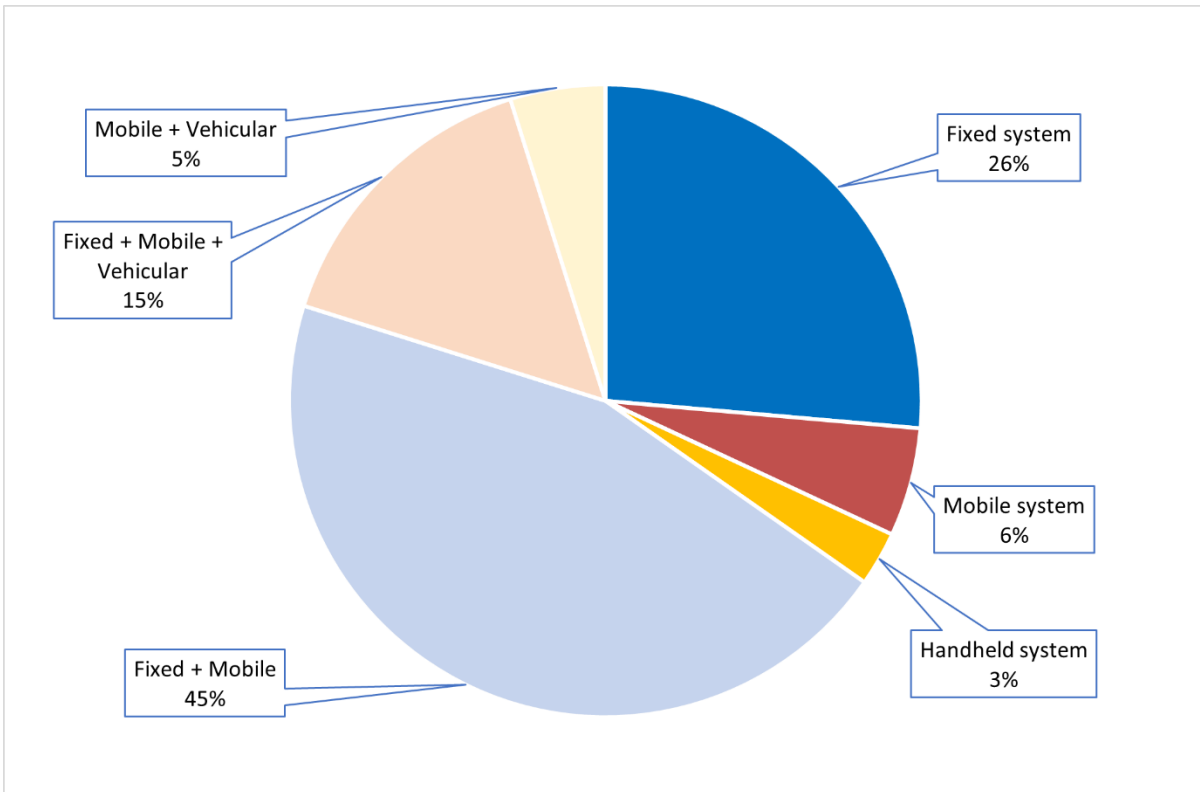
Figure 5 — Pie chart of how mobile C-UAS solutions are (from 144 relevant products)

Considering the set of system parameters, one of the basic logistic parameters is the operability of the use of C-UAS. This factor is crucial in defining constant and equal comparative conditions. It is understandable that adding additional degrees of freedom to the assembly devalues the detection parameters. On the other hand, in some usage scenarios, the ease of installation of any system and its mobility is essential for any application. In other words, depending on where C-UAS is to be used, it

may be necessary to install it permanently, for a short time, or it will not be possible to use this system other than in a mobile/ driving form. Therefore, on the basis of the obtained data, a percentage breakdown of the technology in terms of the possible assembly method is presented in Figure 5.

The analysis shows that most C-UAS (74%) are systems that can be permanently installed in one location, even though many also feature mobile versions (48% of all relevant products). Many products can be mounted on a car or trailer (17%). Therefore, as a conclusion for further work, it should be stated that any testing methodology must reflect the same assembly conditions.
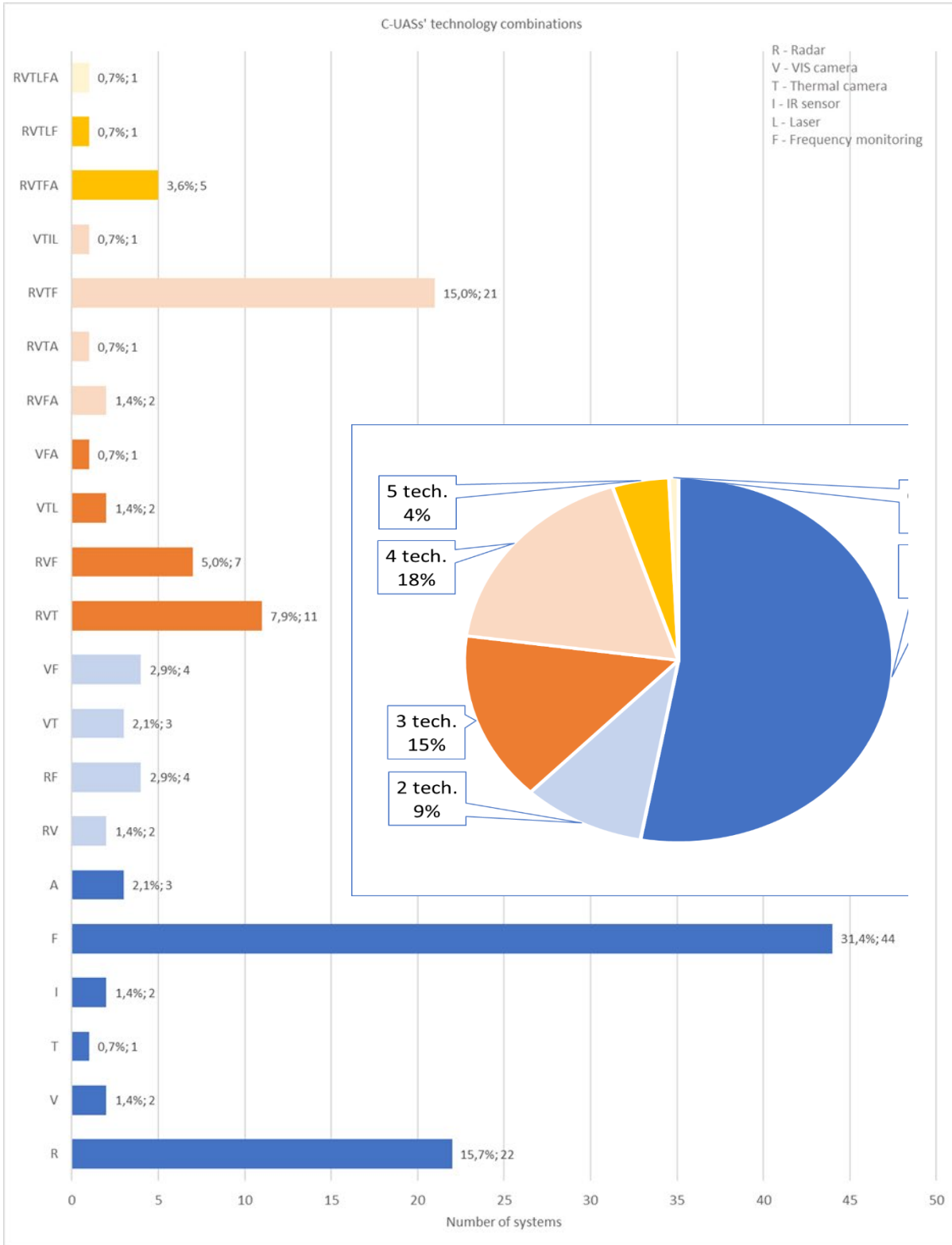
Figure 6 — Combinations of technologies used in C-UAS solutions

As mentioned, the detection technologies that can be used are a finite set characterized by various parameters and offering different functionalities. It results directly from the range of the used electromagnetic spectrum or ranges of acoustic waves. According to the theory of external protection systems, the most effective system, defining an alarm signal with high probability, is a multispectral system. The analysis of the characteristics of the detected object, in various spectral ranges, with well-matched integration principles supported by numerical analysis, always gives the best result. With this in mind, on the basis of the market analysis, the finite set of available combinations of detection technologies offered on the market as a system was extracted, as shown in the diagram in Figure 6.

When it comes to multi-technology systems, it can be seen that microwave radars and/ or visible light cameras are most often combined with other technologies. Such a large spread of the systems offered, including various sets of detection and tracking technologies, is due to several factors:
- restriction of property rights to key technologies,
- lack of consolidation of producers due to competitiveness and a different business strategy,
- sale of systems mainly for budget entities covered by the Public Procurement Acts, for which the provisions of niche technology parameters may exclude potential competitors from the competition,
- the production market of thermal imaging cameras is limited to a few global market players.

The presented analysis defines only the set of the offered complete systems. In addition to the list, there is a set of mixed solutions, understood as the use of various detection and tracking technologies (compiled ad-hock) under the name of integrating software. Hence, it should be concluded that the developed methodology and test procedure in the field of standardization and generalization must include conditions adapted to any other configuration. The aforementioned test methodology and procedures must therefore take into account:

- evaluation of the detection effectiveness in terms of detection correctness,
- evaluation of the detection range depending on the type, size and speed of the object,
- assessment of system ailments, extraction of conditions of resistance to false indications,
- evaluation of the system functionality in selected operating scenarios,
- assessment of resistance to changing environmental conditions
- assessment of sensor data fusion.

Therefore, it seems reasonable to assess the required field conditions in terms of detection ranges.

The next three graphs, i.e., Figure 7, Figure 8 and Figure 9, are the maximum ranges of the three selected technologies: microwave radars, thermal imaging cameras and frequency monitoring. Selected lists are presented on one scale, the range is given in kilometres. Selected DTI technologies can work continuously during the day and at night, i.e., they can raise the alarm for detected objects, continuously, without much impact of lighting conditions 24/7 which is crucial in assessing the suitability of C-UAS.
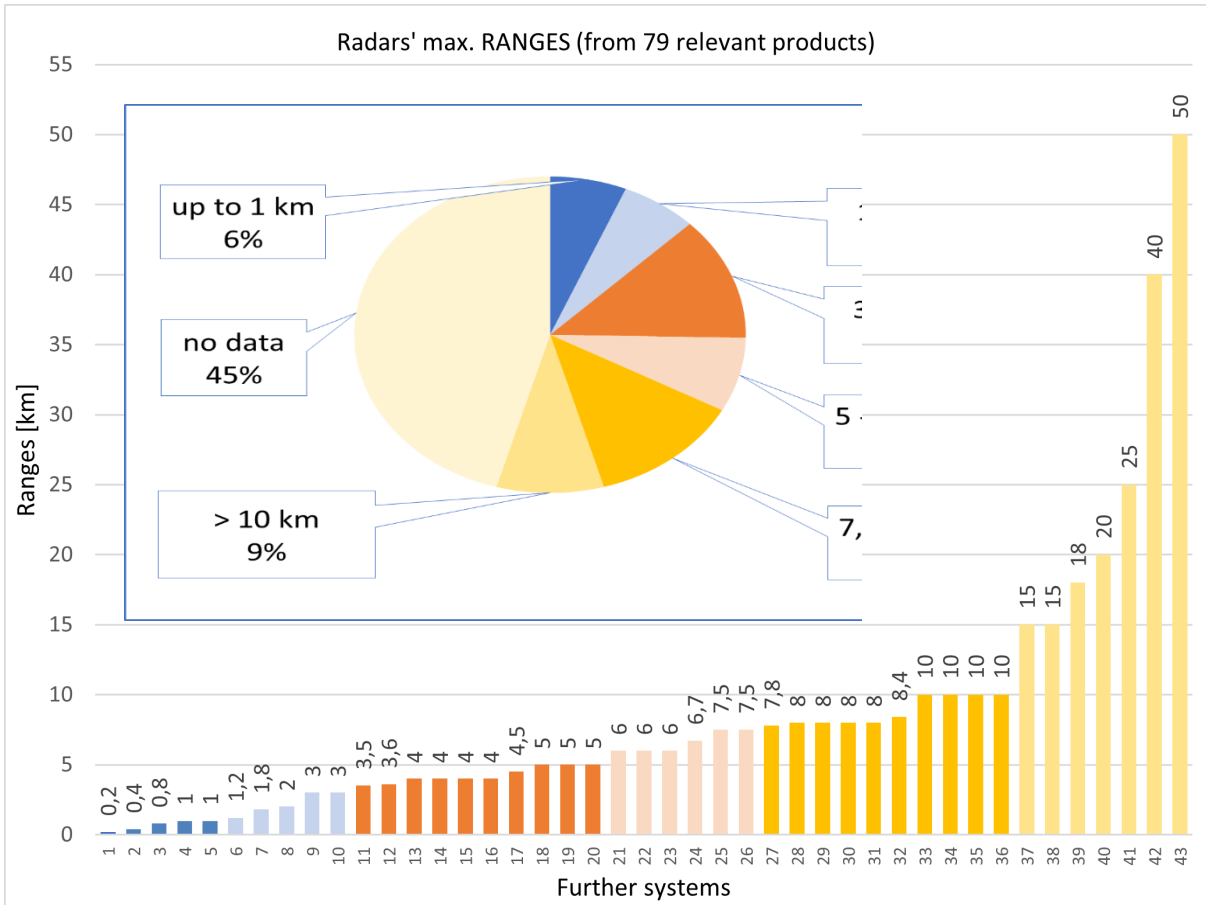
Figure 7 — Maximum ranges of radars

The chart in Figure 7 shows the range information of radar technologies according to the maximum detection ranges stated by the manufacturers. As shown in the chart (Figure 7), information on radar ranges is available only from 43 C-UAS manufacturers. Producers of 45.57% of microwave radars do not provide information about the ranges of their products (out of 79 relevant radars). The radar range is dependent on different factors (Radar Design, RCS of the target, atmospheric conditions), therefore the radar sensor selection is a subject to the use case. In the case of microwave radars, there is definitely no key information to assess the presented range parameters in terms of:

- the size of the object,
- speed of the object during the test,
- the direction of movement of the test object, or
- atmospheric parameters.

Therefore, the presented list should be treated as an approximation of what can be expected in terms of field requirements for measurement conditions.

Thermal cameras' max. RANGES (from 51 relevant products)
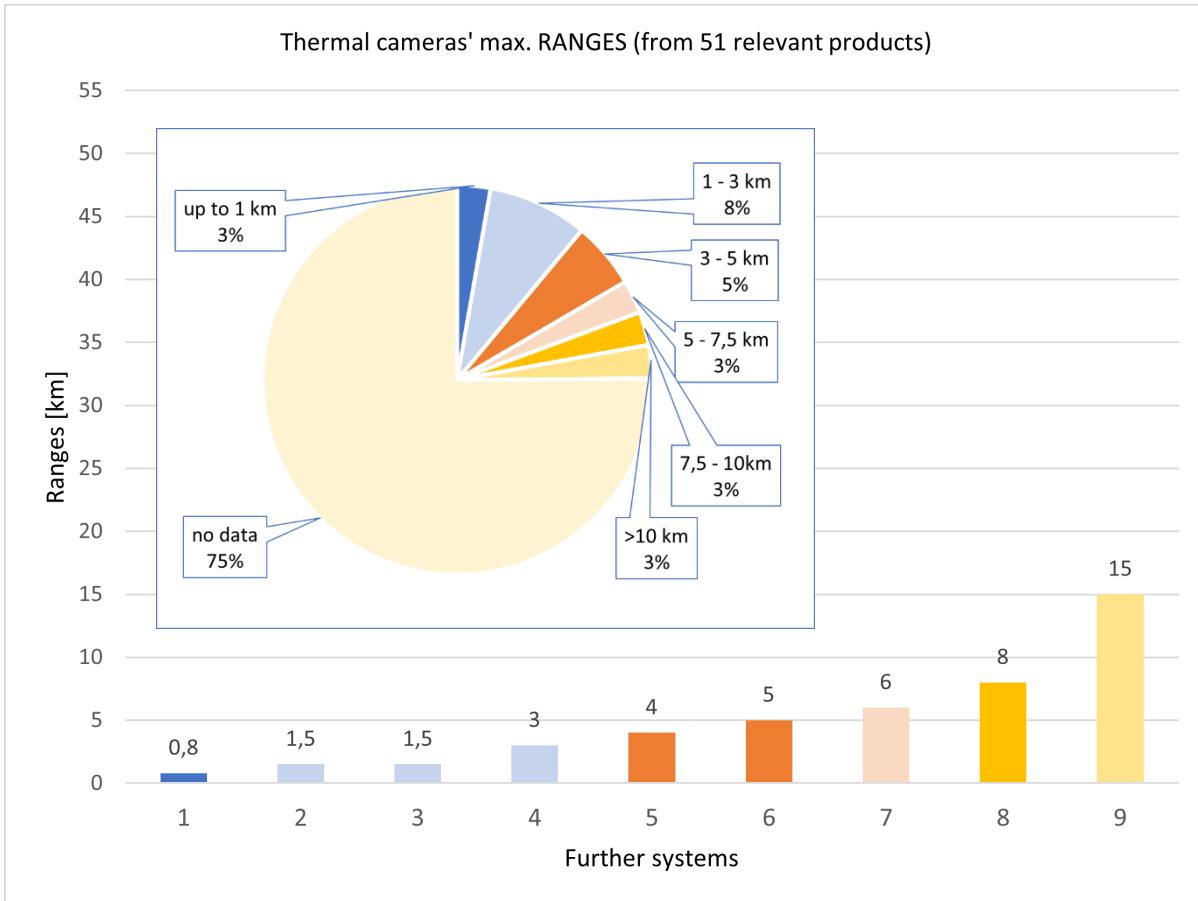
Figure 8 — Maximum ranges of thermal cameras

The diagram in Figure 8 displays information regarding the ranges of nine thermal cameras. Consequently, there is no information about the ranges of 75% of 51 thermal imaging cameras. As you can see, the ranges of thermal imaging cameras are much smaller than the ranges of microwave radars or frequency monitoring sensors. It should be emphasised, however, that thermal imaging cameras are mainly used for tracking and identification processes. Their usefulness in the detection process is limited as opposed to the so-called "Thermal Radars" included in the group of IR sensors. The published parameters clearly show that they are much lower than microwave radars, offering a limited field of view and adjusting to the appropriate image resolution by using optical zoom. The range of thermal sensors are dependent of different factors (Sensor design, thermal energy emission of the target, atmospheric conditions), therefore the thermal sensor selection is a subject to the use case.

Figure 9 — Maximum ranges of frequency monitoring devices

In summary, the three charts in Figure 7, Figure 8 and Figure 9 provide a general overview of the expected DTI ranges for the three key technologies. On this basis, it be concluded the total expected C-UAS ranges. The testing methodology must provide on how to organize the tests of these systems, i.e., how large the test site must be to evaluate the specific properties of C-UAS. How big or how far to place the detection system from the raid site in the selected test scenario.

The systems with a maximum range of up to 5 km are the largest reach group - that is 34% of the relevant products. A slightly smaller group of 30% are systems with a range of up to 3 km. The association of this information with the standard usage scenarios must be consistent in order to cover the largest possible group of products. If it is not possible to use a sufficiently large test site (over a 12 km), it should be reflected in the test methodology, including it with the requirements of the expected scenario. The adopted procedure will reflect the range assessment of C-UAS solutions from the scenario requirements, useful for the given interservice stakeholders and not defining within the procedures only the maximum capabilities of the system depending on the requirements of the scenarios, useful for given stakeholders, and not defining the maximum capabilities of the system.

6.2.2.3 Detection and identification methodologies

6.2.2.3.1 General

As mentioned above, various technologies are used to detect UAS. Each of them has certain limitations that may lower the probability of UAS detection.

6.2.2.3.2 Radars

To detect an object, microwave radars use an electromagnetic wave of a specific frequency. Frequencies in the X band (8-12 GHz) are most commonly used. It is also often possible to find radars operating in the Ku and K bands. Less frequent is the use of higher frequencies due to their strong attenuation caused by precipitation. Lower frequencies are also used less frequently, e.g., the S band due to the long wavelength, in some cases comparable to the size of the detected objects.

The strength of the signal received by the radar when the transmitter and receiver are at the same location is given by the following formula (1.) (*David Herres "Inverse square law and radar: what is the difference?"*):

$$P_r = \frac{P_t G_t A_r \sigma F^4}{(4\pi)^2 R^4 L^2}$$

(1.)

where:
P_t is the transmitter power,
G_t is the gain of the transmitting antenna,
A_r is the receiving antenna area (aperture),
σ is the radar cross section (RCS),
F is the propagation factor,
R is the distance between the radar and the target,
L is the attenuation factor between the radar and target.

The above formula shows that the strength of the signal received by the radar, and thus the detection probability, significantly decreases with increasing distance of the target from the radar (the strength of the received signal decreases inversely to the fourth power of the distance!). The attenuation factor of the signal between the radar and the target also significantly affects the strength of the signal received by the radar. Microwave attenuation can increase significantly in rain. Generally, the higher the radar frequency, the more it is attenuated in rain. The dependence of attenuation on the amount of rainfall and frequency is shown in the Figure 10.
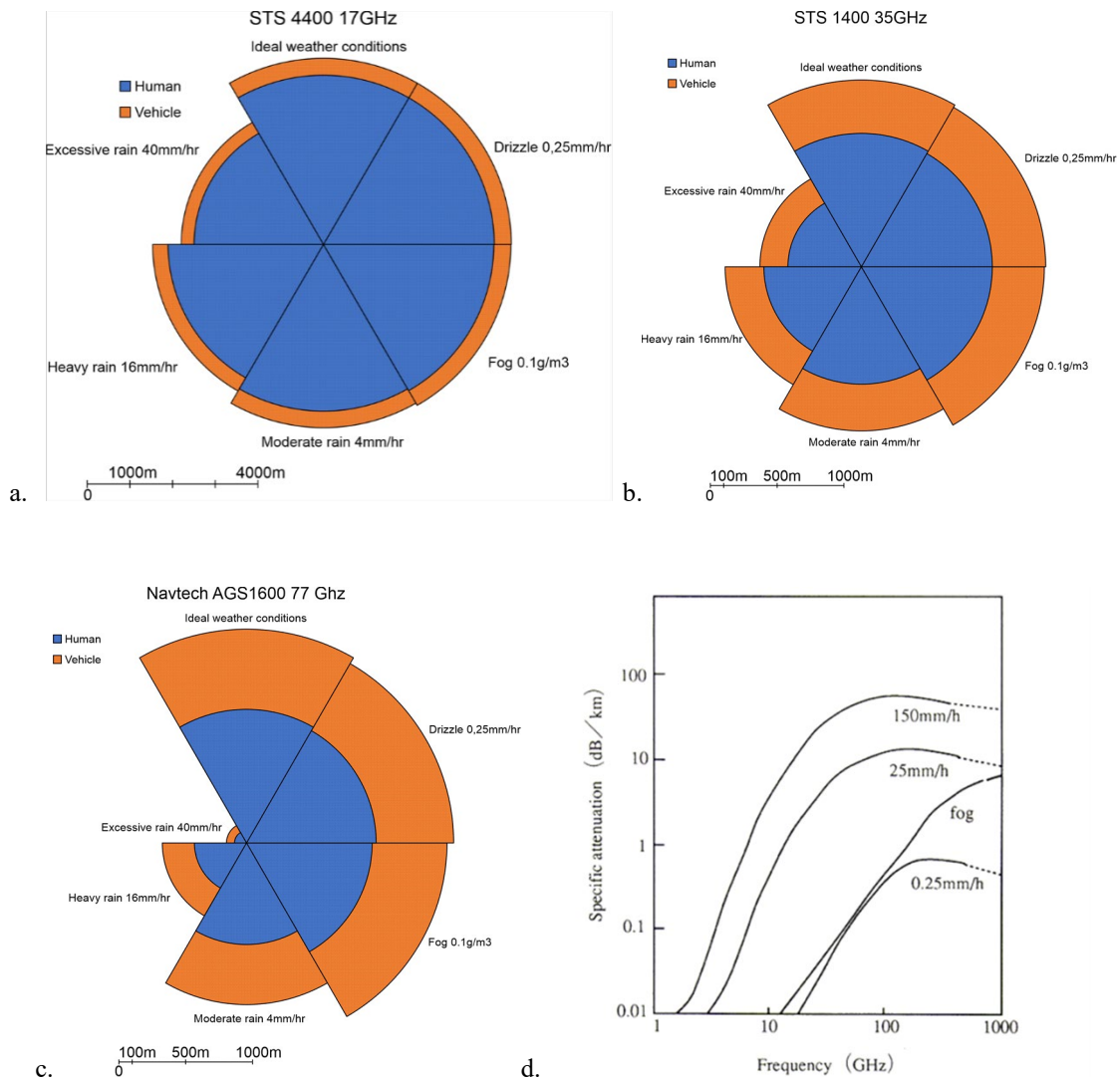
Figure 10 — Dependence of attenuation on the amount of rainfall and frequency, *M. Życzkowski, M. Szustakowski, W. Ciurapiński, M. Karol, P. Markowski, "Integrated radar-camera security system – range test"*

It is up to the radar manufacturers to make a difficult decision in what frequency range the device should operate to ensure the best range and the possibility of UAS detection.

The limitations of radars resulting from the physical phenomena related to their operation are:

- Active detection method – possible interference with the radar signal.
- Active detection method – it is possible to detect the presence of a radar.
- The response characteristics of radars, depending on the weather conditions, strongly depend on the frequency use. In general, the higher the frequency, the greater the attenuation on water molecules (fog, rain).
- The lower the frequency of the radars, the more difficult it is to detect small objects.
- For continuous wave (CW) radar movement of the object crosswise to the radar is under certain conditions difficult to detect, especially for low-power radars.
- The disturbance may come from the multiplication of the real object in the case of echo reflection from the earth's surface or the atmosphere.
- In many cases the interference signal reaching the radar receiver coming from longer distances exceeds the echo level of the useful target in its power. Only on the quality of the firmware (analysing) depends the final performance properties of the detection system.
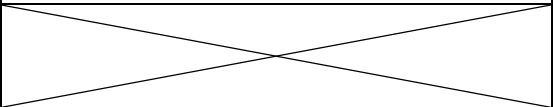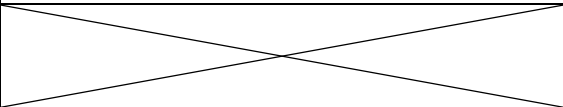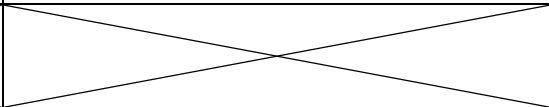
- Due to the shorter distance travelled by the interference signal (the useful signal must travel two times - from the transmitter to the interference source and back again - compared to the interference emitted by the target), the power emitted by the interference transmitter may be much smaller to effectively interfere with the working radar.
- The use of SPFA systems that can control the detection level, in the presence of environmental disturbances, can significantly reduce the detection range.
- False alarm rates: It is a challenge to adjust the proper detection level to see the real targets and have no false alarms (depending on radars Signal to Nosie Ratio - Detection Threshold and Signal Processing of the receiver).
- A radar is not designed to detect a target directly above the radar antenna. This gap is known as the cone of silence (depending on radar antenna design).

Due to the design and use, additional radar limitations are given below:

- Restrictions on the use of frequencies (including legal ones).
- Restrictions on the permissible radiation power.
- Possible impact of the radar device on other subsystems of the user (interference, disruptions) and vice versa – the interference of the radar operation is directed at the frequency of the device and comes from external sources, and the reason for its use is usually masking specific targets. Interference may be intentional (used as radio-electronic warfare) or unintentional, accidental (in the case of using radio transmitters operating at a similar or the same frequency as the operating radar). It is considered to be an active source of interference from the moment it is initiated by external elements unrelated to the useful radar signal.
- Any non-standard change of the radar position results in the disturbance of the measurement, hence the necessity to mount the radars permanently and securely on elements that do not cause or are not subject to displacement.
- A swarm of drones can be detected as a single object, especially when the objects are moving one after the other.
- Radars have a blind spot usually a few meters from the radar (this varies depending on the type of radar). The object to be detected must be away from the radar.

Table 17 — Tests' requirements for radars

Radar	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Provide legal access to use the frequency and power of the tested devices. 2. Provide measurements of atmospheric conditions and electromagnetic background. 3. Provide a test field with single trees in the detection zone. 4. Provide a test field with a forest wall in the detection field. 5. Provide a test field with buildings in the detection area. 6. If possible, provide a radar jamming station or a second radar of the same type. 7. Provide commercial drones of different sizes. 8. Ensure the presence of a falconer with a bird or birds. 9. Make sure it is necessary to insure the drone against damage by bird attacks?	1. Detection of UASs with single trees in the detection field. 2. Detection of UAS with forest wall in the detection field. 3. Detection of UASs with buildings in the detection field. 4. Detection of UASs moving towards / from the radar. 5. Detection of UASs moving across the radar beam. 6. Perform radar detection range tests depending on the size of the object (UAS: mini, micro, small). 7. Perform tests at which maximum / minimum speed of UASs are detected. 8. Perform bird / UAS discrimination tests. 9. Check whether the operation of the station is automatic or manual. 10. Check whether the detection angles given by the manufacturer (horizontal and vertical) are consistent with those obtained during the tests.	1. Check the time to set up and start the devices. 2. Check whether it is necessary to calibrate the radar once / each time it is turned on and how long it takes. 3. Provide the service of the falconer. 4. Provide power and elements necessary for the construction of the station. 5. Provide service for the jamming station, if used. 6. Provide the possibility of adjusting the sensor mounting height if the manufacturer allows it. 7. Provide drone operators.
Tracking	1. Provide legal access to use the frequency and power of the tested devices. 2. Provide measurements of atmospheric conditions and electromagnetic background.	1. Test whether the detected UAS will be recognized as the same after stopping and moving again after a short pause. 2. Tracking the UAS with single trees in the detection field.	As above.

	3. Provide a test field with single trees in the detection zone.	3. Tracking the UAS with the forest wall in the detection field.	
	4. Provide a test field with a forest wall in the detection field.	4. Tracking the UAS with buildings in the detection field.	
	5. Provide a test field with buildings in the detection area.	5. Check whether the operation of the station is automatic or manual.	
	6. Provide commercial drones of different sizes.		
Identification			

6.2.2.3.3   VIS cameras

Visible light cameras are often used in anti-drone systems to track and identify drones. The most common are PTZ cameras, allowing the camera to rotate and zoom, and thus follow the drone. Many manufacturers buy ready-made solutions, but some of them also produce their cameras. Currently, most of the cameras used are high definition (HD), with multiple optical and digital zoom. The ranges of these cameras allow to see the drone from a distance of up to 10 km, but the identification takes place at much shorter distances, about three times smaller.

PTZ camera   Image from camera   Drone detection   Start of drone tracking   Centered view

Sending differences in x and y axes to pan-tilt-zoom device
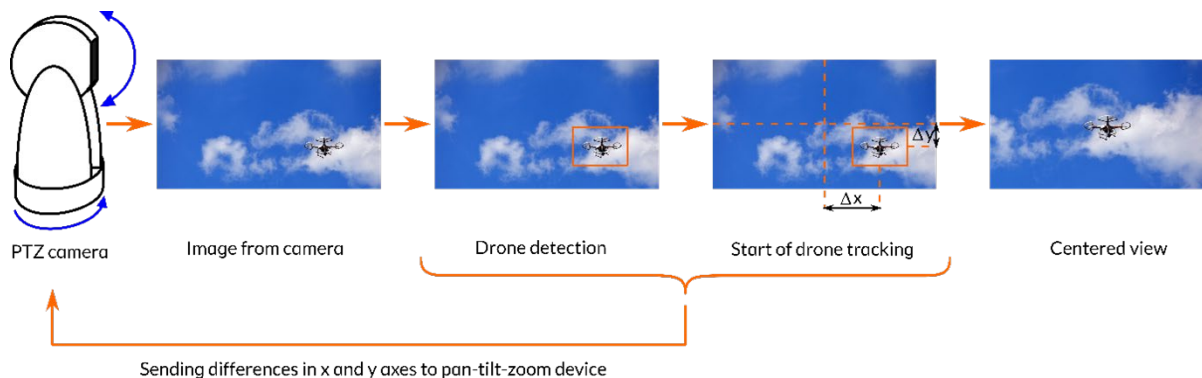
Figure 11 — How to track drone with a PTZ VIS camera

A simple diagram of the use of the PTZ VIS pan tilt camera for drone tracking is shown in Figure 11. When the drone is detected by the camera, the image is verified with the drone database, which includes photos of constructions popular on the market. When the verification is correct (i.e. in the image captured by the camera is a drone compatible with the drone images resources), it is marked on the image (most often with a characteristic bright square). In the next step, the distance of the central part of the drone from the axis (vertical and horizontal) intersecting the centre of the camera image is calculated on the image (in pixels). These distances are then transmitted to the camera pan tilt mechanism, which corrects the camera position - so that the central part of the drone coincides with the central point of the camera image. And so, these corrections are repeated with the appropriate frequency - the higher the frequency of corrections, the faster and more accurate the tracking of the drone. The above steps are used in cameras with intelligent image analysis. Without this feature, the operator of the C-UAS solution would have to confirm the detection of the drone himself and track it by controlling the camera himself. Of course, to build the C-UAS system, a camera without intelligent image analysis can be used, but then the coordinates of the drone changing its position must be detected and transmitted to pan tilt mechanism by other technology that allows to track the drone, e.g., radar, IR sensor or frequency monitoring.

The limitations of visible light cameras resulting from the physical phenomena related to their operation are:

- The systems are dedicated to imaging under constant lighting conditions in the field of observation with radiation in the range of visible light to a strictly defined level (they cannot be used at night).
- The limitations are strictly related to the choice of the lens and its parameters.
- Resolution of image detection depends on the coincidence of the resolution of the matrix and the focal length of the lens (field of observation range).
- The ability to indicate the distance of an object is limited, only to predict from the calculation of the potential size of the object.
- It is difficult (software) to indicate the coordinates of the object.
- The quality of object tracking depends on the adopted image analysis method.

- The dynamics of image lighting (clouds, sun, etc.) significantly affect the detection of the object in the image.
- Light reflections from dirt on the lens disqualify the solution from use.

Due to their design and use, additional limitations of visible light cameras are given below:

- Too slow camera pan tilt mechanism may not keep up with the tracking of the drone.
- There is a possibility of dazzling the camera.
- High computing power is required to recognize a drone.

Table 18 — Tests' requirements for VIS (*visible* range of wavelength) cameras

VIS	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Obtain consent (GDPR) to record people. 2. Check that it is possible to perform tests (or simulate conditions) in rain and fog. 3. Provide mirrors or reflectors to simulate camera glare. 4. Provide a test field with single trees in the detection zone. 5. Provide a test field with a forest wall in the detection field. 6. Provide a test field with buildings in the detection area. 7. Provide commercial drones of different sizes. 8. Ensure the presence of a falconer with a bird or birds. 9. Make sure it is necessary to insure the drone against damage by bird attacks?	1. Detection of UASs with single trees in the detection field. 2. Detection of UAS with forest wall in the detection field. 3. Detection of UASs with buildings in the detection field. 4. If possible, test the operation of the system in different weather conditions (sun, rain, fog).	1. Check the time to set up and start up the devices. 2. Provide the service of the falconer. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the weather simulation station, if such a solution is used. 5. Provide the possibility of adjusting the sensor mounting height if the manufacturer allows it. 6. Provide drone operators (minimum 3 drones).
Tracking	1. Obtain consent (GDPR) to record people. 2. Check that it is possible to perform tests (or simulate conditions) in rain and fog. 3. Provide mirrors or reflectors to simulate camera glare. 4. Provide a test field with single trees in the detection zone. 5. Provide a test field with a forest wall in the detection field.	1. Test whether the camera will follow the bird or the drone during tracking. 2. If possible, test the operation of the system in various weather conditions (sun, rain, fog). 3. Perform a tracking test depending on the size and distance of the UAS. 4. Check whether the operation of the station is automatic or manual.	As above and: 1. The operator or operators of a swarm of drones.

	6. Provide a test field with buildings in the detection area.	5. Perform UAS tracking test on straight and cross flight.	
	7. Provide commercial drones of different sizes.	6. Perform a correctness test - how long does the tracking lose the UAS.	
	8. Provide a swarm of drones.	7. Perform the targeting speed test.	
	9. Ensure the presence of a falconer with a bird or birds.	8. Perform a system behaviour test in the event of a drone swarm.	
	10. Make sure that it is necessary to insure the drone against damage by bird attacks?	9. Test the entry of different UASs from different directions.	
		10. Perform the drone swarm entry test and then split it into individual UASs.	
Identification	1. Obtain consent (GDPR) to record people.	1. Perform a bird-UAS discrimination test.	As in the line "detection".
	2. Check that it is possible to perform tests (or simulate conditions) in rain and fog.	2. If possible, conduct a UAS identification test in different weather conditions.	
	3. Provide mirrors or reflectors to simulate camera glare.	3. Perform an identification test depending on the size and distance of the object.	
	4. Provide a test field with single trees in the detection zone.	4. Check whether the operation of the station is automatic or manual.	
	5. Provide a test field with a forest wall in the detection field.	5. Check if the system allows you to take a picture or a screenshot to compare the image resolution at the time of UAS recognition or detection.	
	6. Provide a test field with buildings in the detection area.		
	7. Provide Rotakin for measuring camera resolution.	6. Test the camera resolution with the Rotakin.	
	8. Provide commercial drones of different sizes.		
	9. Ensure the presence of a falconer with a bird or birds.		
	10. Make sure that it is necessary to insure the drone against damage by bird attacks?		

6.2.2.3.4 Thermal cameras

Thermal imaging is a technology that uses for observation an electromagnetic wave of the length that is emitted by any object with a temperature above absolute zero (0K, i.e. -273.15°C). Thanks to this the image is visible both during the day and at night without the use of additional light sources. An additional advantage is the fact that the range of electromagnetic waves used in thermal imaging is slightly less attenuated by fog, dust, and precipitation than visible light thanks to which the thermal imager allows observation at a greater distance in difficult weather conditions than daylight cameras. The image obtained from a thermal imaging camera in security systems is usually black and white. Shades of gray depend on the temperature of the observed object and the material from which the object is made. Therefore, it is not possible to become completely "invisible" to a thermal camera.

The Earth's atmosphere attenuates certain wave ranges, therefore, in practice, thermal imaging cameras are used, operating in the ranges weakly suppressed by the atmosphere, in the so-called atmospheric windows.
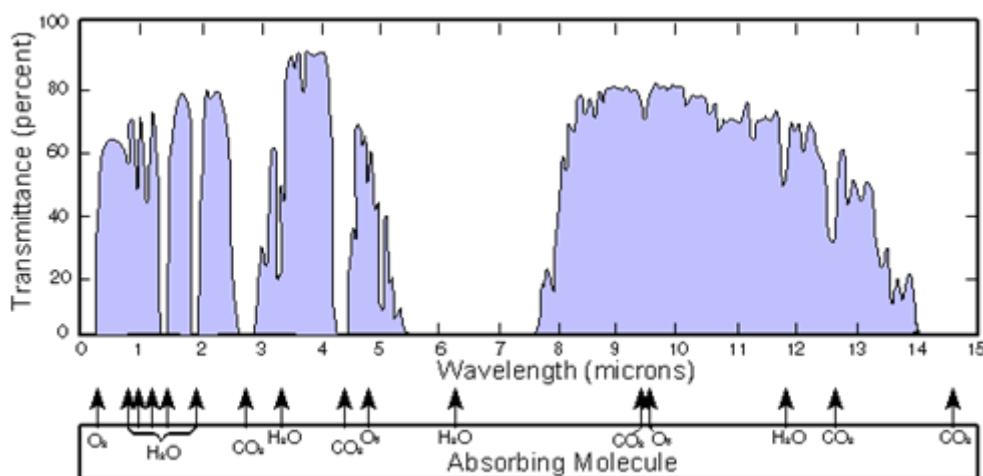
Figure 12 — Absorption of electromagnetic radiation by the earth's atmosphere without clouds, Illustration – Wikipedia

In practice, due to the attenuation of the atmosphere, thermal imaging cameras operating in two different wavelength ranges are used:

- 3-5 μm (MWIR - Short Wave Infrared),
- 7,5-14 μm (LWIR - Long Wave Infrared).

Different types of detectors are used depending on the wavelength range.

Photon detectors are used for the SW range. They are made of semiconductor materials (eg InSb – indium antimonide or MCT – mercury-cadmium telluride). The measuring signal for them is the change in electrical conductivity, caused by the passage of valence electrons in atoms to the conduction level (due to the absorption of photons of infrared energy from the observed object). In order to reduce the number of naturally thermally triggered free electrons (giving the so-called noise) and thus to expose the effect of electron triggering due to the absorption of radiation coming from the observed objects, these detectors are cooled to a low temperature during operation, usually from 60 K to 100 K (-196°C to -173°C). This is a nuisance because, after switching on the camera, the cooling device has to run for some time to reach the required temperature. Moreover, the cooling device has a limited life. Photon detectors are sensitive to shortwave radiation and are used in the construction of shortwave cameras. Their advantage is the possibility of observation over long distances (over 20 km), high sensitivity and the possibility

of achieving a high speed of image refreshment, which enables the registration of thermal images with a very high frequency.

For the LW range, thermal detectors, also known as resistive bolometers, are used. The following are most often used for their construction: a-Si - amorphous silicon or VOx - vanadium oxide. Since they do not require cooling and can operate at room temperature, they are also called uncooled detectors. The bolometer works by converting (by means of an absorber) the energy of infrared radiation into heat, which changes the resistance of the material used to build the detector. A suitable reading system detects changes in the bolometer resistance and generates a corresponding voltage signal at the output. Miniature bolometers (microbolometers) arranged in the form of a matrix with a specified number of rows and columns form a microbolometric matrix. The currently produced microbolometer arrays have better and better parameters, and they are much cheaper than cooled arrays with photon detectors. As a result, they are more and more often used in thermal imaging cameras for civil and military applications.

The most important parameters of thermal imaging cameras are:

- Spectral range.
- Resolution (number of pixels horizontally and vertically).
- The distance between the pixel centres (the so-called pixel pitch).
- NETD (Noise Equivalent Temperature) – detector sensitivity parameter, indicates the level of the signal that allows the detector to exceed the internal noise, as shown in Figure 12. The smaller value the better detector.
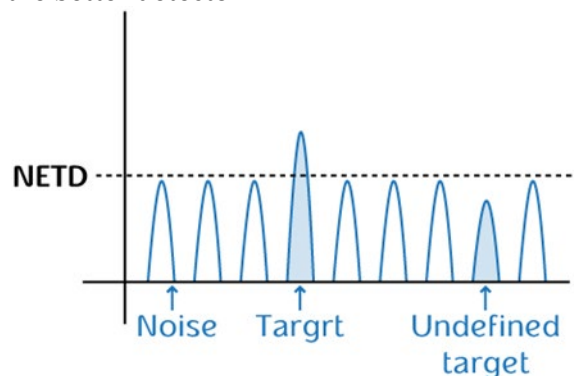
Figure 13 — Illustration of a Noise Equivalent Temperature, *Opgal company training materials*

- MRTD (Minimum Resolvable Temperature Difference) - sensitivity parameter that specifies the minimum temperature difference at which the image can be distinguished as 4 separate stripes, as shown in Figure 14. The lower the temperature the better camera.
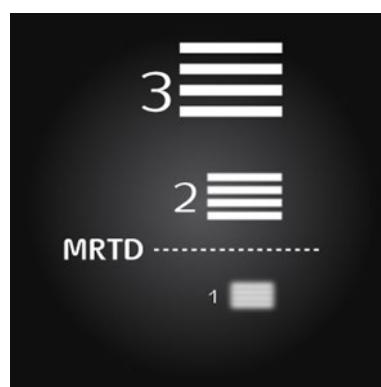
Figure 14 — Ilustration of Minimum Resolvable Temperature Difference determination, *Opgal company training materials*

- Image refresh rate.
- Type of lens (fixed focal length or zoom lens).
- The F-number (focal ratio) of the lens, specifying the amount of radiation that can reach the detector. The smaller the F number is the better the lens.
- The focal length of the lens, or more commonly the field of view (FOV) of the camera, which includes both the focal length of the lens and the detector size. FOV is given in degrees.
- The way of displaying the image (black and white, black and white with the hottest elements of the image, or the image displayed in the colour palette).

Since the temperature of the observed sky is about 210K (about -60°C), all objects with a higher temperature, such as a drone, are very clearly visible against the background when viewed with a thermal camera. Whether or not a drone is observed depends on its size, distance from the camera, and camera FOV. Theoretically, having a camera with a very narrow viewing angle a small object can be detected from a long distance. However, narrowing the viewing angle reduces the area of the observed sky. When choosing the viewing angle, it is necessary to make a compromise. A wider viewing angle will make smaller objects visible from a shorter distance. According to Johnson's criterion, for an observer to be able to perceive (detect) an object with a probability of 50 %, it must occupy 1,5 pixels on the detector matrix. It shows how strongly the probability of detection depends on the technical parameters of the camera, the selected field of view (FOV) of the camera, the size and distance of the object.

The limitations of thermal imaging cameras resulting from the physical phenomena related to their operation are:

- Poor image adjustment/sharpness, better quality available only in motor zoom systems
- Thermal imaging cameras are passive, which means they detect all infrared radiation coming from a target. This means that what is seen through the camera is not limited to the heat emitted by the object but can also be the result of energy reflected from the surface looked at but coming from other sources.
- The identification ability of thermal imaging cameras is limited by weather phenomena. Fog, snow, and rain suppress infrared waves, which reduces the range of camera effective detection and imaging.
- Cloudy conditions strongly affect the interpretation of the image, especially of small objects over long distances.
- The key parameter of a thermal imaging camera is the MRTD parameter, which means that cooled matrices are better for the imaging of objects.
- The limitation in use is closely related to the choice of the lens and its parameters.
- The resolution of image detection depends on the coincidence of the matrix resolution and the focal length of the lens (field of view range).
- The ability to indicate the distance of an object is limited only to predictions from the calculation of the potential size of the object.
- It is difficult (software) to indicate the coordinates of the object.
- The quality of object tracking depends on the adopted image analysis method.
- Firmware is most often closed under one manufacturer and the possibility of integration is limited to the functions provided by the SDK.
- The detectability of objects strictly depends on the emissivity of the material from which it was made. The ambient temperature is required to compensate for the radiation reflected from the object. If the emissivity of the object is low, then the correct setting of the ambient temperature is of key importance.
- There may be a problem with detecting and/or interpreting detected shiny objects.

Due to their design and use, additional limitations of thermal imaging cameras are given below:

- The device is susceptible to dirt on the lens.
- Higher resolution cameras are among the police/army licensed products.

- Multi-kilometre imaging requires the use of long focal length lenses and precise control with elimination of shake. Any non-standard change in the position of the camera results in a distortion of the image.
- Objects flying low over a large sunny surface (asphalt, concrete) in long-range imaging with a thermal imaging camera have artifacts from heated air.
- It is possible to deliberately blind the camera.

Table 19 — Tests' requirements for thermal cameras

Thermal	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Check if it is possible to perform tests (or simulate conditions) in rain and fog. 2. Provide a simulation of the presence of a warm object in the detection zone. 3. Provide a test field with single trees in the detection zone. 4. Provide a test field with a forest wall in the detection field. 5. Provide a test field with buildings in the detection area. 6. Provide commercial drones of different sizes. 7. Provide a flying wing type drone. 8. Ensure the presence of a falconer with a bird or birds. 9. Ensure the uniformity of camera scenarios by monitoring the sky temperature (clear / cloudy) during testing! 10. Ensure sun exposure is monitored during testing (may cause the drone to heat up). 11. Make sure it is necessary to insure the drone against damage by bird attacks?	1. Perform the UAS detection test when the camera observes the sky only and when it observes the sky and the surroundings on the ground (especially important in high ambient temperatures). 3. Perform a flying wing UAS detection test. 4. Perform a UAS detection test near a warm object (architectural object, eg a chimney or a simulator). 5. If possible, test the operation of the system in various weather conditions (sun, rain, fog). 6. Perform a UAS detection range test depending on the size of the object. 7. Tests with UASs should be carried out, which will have the same temperature before the test (think about the method of storing the drones). 8. Test if the camera detects its reflection on the water surface as the UAS.	1. Check the time to set up and start up the devices. 2. Provide the service of the falconer. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the weather simulation station, if such a solution is used. 5. Provide drone operators (minimum 3 drones).
Tracking	1. Check that it is possible to perform tests (or simulate conditions) in rain and fog. 2. Provide a test field with single trees in the detection zone.	1. Test whether the camera will follow the bird or the UAS during tracking. 2. If possible, test the operation of the system in various weather conditions (sun, rain, fog).	As above and: 1. The operator or operators of a swarm of drones.

Thermal	Test field	Testing methods / Scenarios	Tests handling
	3. Provide a test field with a forest wall in the detection field.	3. Perform a tracking test depending on the size and distance of the UAS.	
	4. Provide a test field with buildings in the detection field.	4. Check whether the operation of the station is automatic or manual.	
	5. Provide commercial drones of different sizes.	5. Perform UAS tracking test on straight and cross flight.	
	6. Provide the presence of a falconer with a bird or birds.	6. Perform a correctness test - how long does the tracking lose the UAS.	
	7. Ensure the uniformity of camera scenarios by monitoring the sky temperature (clear / cloudy) during testing!	7. Perform the targeting speed test.	
	8. Ensure that sunlight is monitored during testing (may cause the drone to heat up).	8. Perform a system behaviour test in the event of a drone swarm.	
	9. Make sure it is necessary to insure the drone against damage by bird attacks?	9. Test the entry of different UASs from different directions.	
		10. Perform the drone swarm entry test and then split it into individual UASs.	
Identification	1. Provide commercial drones of different sizes.	1. Perform a bird-UAS discrimination test.	As in the line "detection".
	2. Ensure the presence of a falconer with a bird or birds.		
	3. Ensure the standardization of camera scenarios by monitoring the sky temperature (clear / cloudy) during testing!		
	4. Ensure sun exposure is monitored during testing (may cause the drone to heat up).		
	5. Make sure it is necessary to insure the drone against damage by bird attacks?		

6.2.2.3.5   IR sensors

In this study, infrared sensors are not standard infrared detectors, as the use of such sensors would be pointless in long-range anti-drone systems. Here they are considered as infrared cameras or long-range infrared sensors, the behaviour of which resembles a radar.

a)   one-camera thermal radar-like device   b) multi-cameras thermal radar-like device
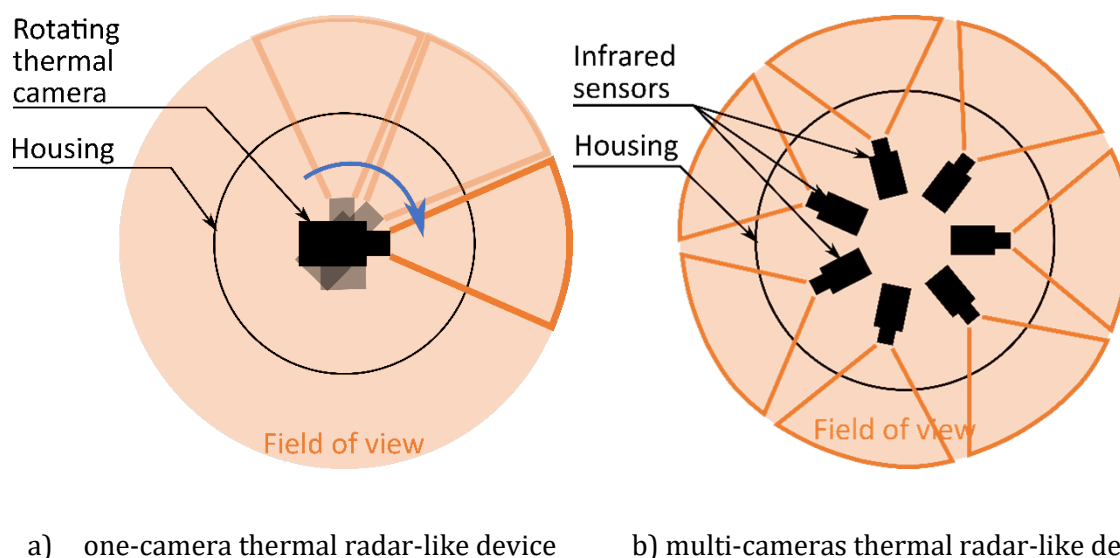
Figure 15 — IR sensors

1. First, a rapidly rotating thermal imaging camera allows for the observation of the 360° field of view (Figure 15.a).

2. The second, several IR detectors placed in a circle can observe several zones, and together they give a field of view equal to 360° (Figure 15.b).

Several of the found companies producing C-UAS offer an unusual solution for the use of thermal imaging cameras. They use two approaches in their systems:

Most often, in such solutions of thermal imaging cameras, imaging takes place in grayscale - where the objects with the highest temperature are bright, and the objects with the lowest temperature are dark. Such devices can therefore be used at night because they do not need additional lighting to work. Compared to standard radar, this technology is passive so it can't be detected.

The limitations of IR sensors resulting from the physical phenomena related to their operation are:

- The limitations are similar to the limitations of thermal imaging cameras when the IR sensor is a rotating thermal imager.
- The rotation frequency of the thermal imaging camera is limited to single Hz and the image analysis depends on comparing the sequence of image changes every second.
- Limited ability to indicate the distance of an object, only for prediction from the calculation of the potential size of the object.
- The field of view (lens) and the size of the matrix as well as mounting on a rotating platform limit the resolution of the measurement over a long distance.

Due to their design and use, additional limitations of IR sensors are given below:

- Image analysis is delayed in time with rotary cameras.
- Correlation of the detection efficiency and the drone tracking speed is related to the algorithms for combining individual frames from IR sensors.

Table 20 — Tests' requirements for IR (*InfraRed*) sensors

IR	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Provide a test field with single trees in the detection zone. 2. Provide a test field with a forest wall in the detection field. 3. Provide a test field with buildings in the detection area. 4. Provide commercial drones of different sizes. 5. Ensure the presence of a falconer with a bird or birds.	1. Perform the detector detection range tests depending on the object size (UAS: mini, micro, small). 2. If possible, test the operation of the system in various weather conditions (sun, rain, fog). 3. Test whether the detector can detect more UASs as separate drones or as one, and if separate, from what minimum distance. 4. Detection of UASs moving towards / from the radar. 5. Perform a bird-UAS discrimination test. 6. Perform a test of detection of UAS heated to the ambient temperature (for tests in autumn / winter conditions, it is worth carrying out a test for detecting a cooled drone) - only for IR detectors, not for "thermal radar".	1. Check the time to set up and start up the devices. 2. Provide the service of the falconer. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the weather simulation station, if such a solution is used. 5. Provide drone operators (minimum 3 drones). 6. Provide the drone swarm operator or operators.
Tracking	1. Provide commercial drones of different sizes.	1. Perform a test at what minimum and maximum distance the detector can track the UAS. 2. Perform a UAS tracking resolution test through the detector - develop a scenario. 3. For the thermal imaging radar, test the refresh rate of the drone's location on the map of the operator's system.	As above.
Identification			

6.2.2.3.6 Lasers (range-finding lidars)

Lidars, designed to measure the range to objects, are hard target lidars. They consist of two functional blocks: the transmitting path and the receiving path. These paths are shown in Figure 16. The basic element in the transmission path is the laser, the radiation of which is shaped by the lens system and directed into space.
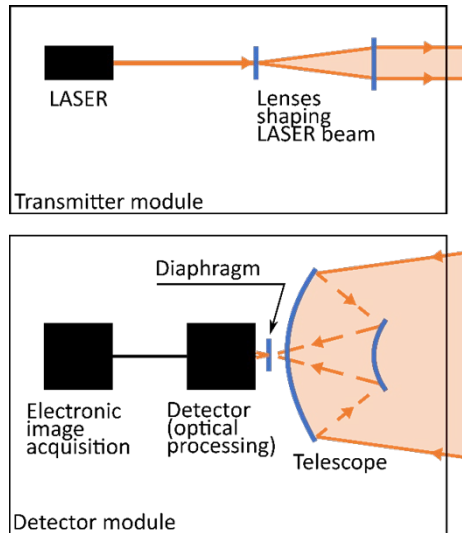
Figure 16 — Two basic functional blocks of lidar rangefinders: transmitter module and detector module

After reflection from an object in the laser propagation path (Figure 17 a), scattered radiation partially reaches the receiving system. First, the receiving lens/telescope focuses the radiation at one point, then it propagates through the field diaphragm and the optical system, and finally hits the detector. The signal received in this way is converted by an optical processing block - from an optical signal to an electrical one, and then it goes to the electronic image acquisition block.
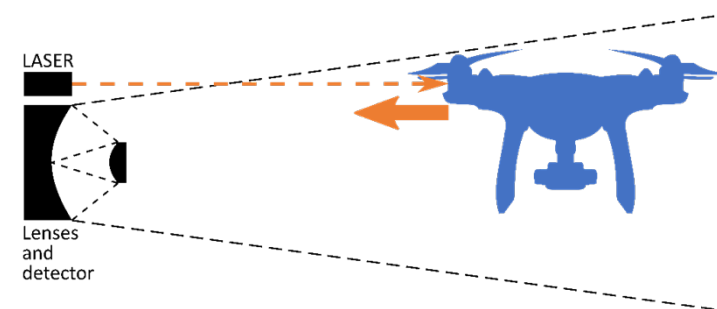
a) Hard Target LIDARs' principle of operation
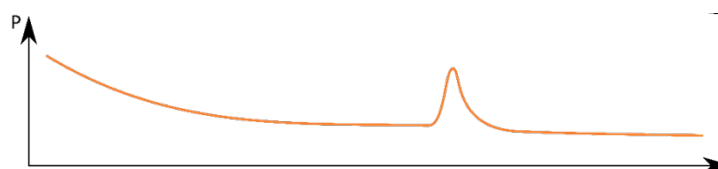
b) Corresponding dependence of reflected power on range to the detected object

Figure 17 — Reflection of radiation from a solid object

Figure 17 a) shows the measurement of the optical echo resulting from the reflection of radiation from a solid object - a drone. In Figure 17 b) is shown the corresponding graph of reflected radiation as a function of the distance from the object.

The optical echo is characterised by:

- a spectral line identical to that in the transmitted pulse,
- analogous time dynamics of transmitted and received pulses.

The limitations of the laser lidars resulting from the physical phenomena related to their operation are:

- The distance measurement may be disturbed by a drone other than intended.
- Drones cannot be tracked.
- The distance measurement may be distorted by unfavourable weather conditions: high extinction coefficient, insolation.
- The reflected power from the subject may be too low to filter out from the noise.
- The power radiated towards the object must be sufficiently high, but not too high, so as not to cause damage.
- The optical wavelength of the laser must be eye-safe (not to dazzle pilots/people, etc.).
- It is an active method, which means it is possible to detect the irradiation/lighting of the object.
- Scattering the 1 550 nm wavelength on water molecules (rainfall, fog, etc.).

Due to their design and use, additional limitations of the laser lidars are given below:

- • High precision aiming at an object over a long distance is required.

- • Distance measurement of fast-moving drones is difficult.

Table 21 — Tests' requirements for for lasers/ range finding lidars

| Laser (rangefinder)	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Check the legal requirements for the possibility of using a laser with specific parameters (power and wavelength) on the training ground and, if necessary, ensure that these requirements are met. 2. Provide a test field with single trees in the detection zone. 3. Provide a test field with a forest wall in the detection field. 4. Provide a test field with buildings in the detection field.	1. Perform the UAS distance measurement time test from the moment it was detected by another detector cooperating within the same system. 2. If possible, test the operation of the rangefinder in different weather conditions (sun, rain, fog). 3. Perform a test of the rangefinder operation depending on the speed of the UAS. 4. Perform a rangefinder resolution test if more than one UAS appears (e.g., one UAS closer to the other, both at a short distance from the laser beam axis and at what distance from the beam centre the UAS will detect the closer and farther away. 5. Checking the accuracy of the laser operation in the case of work in various field conditions (single trees, forest walls, buildings).	1. Check the time to set up and start up the devices. 2. Provide the service of the falconer. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the weather simulation station, if such a solution is used. 5. Provide drone operators (minimum 2 drones).
Tracking	1. Check that it is possible to perform tests (or simulate conditions) in rain and fog. 2. Provide a test field with single trees in the detection zone. 3. Provide a test field with a forest wall in the detection field. 4. Provide a test field with buildings in the detection area.	1. Test whether the system will follow the bird or the drone during tracking. 2. If possible, test the operation of the system in various weather conditions (sun, rain, fog). 3. Perform a tracking test depending on the size and distance of the UAS. 4. Check whether the operation of the station is automatic or manual.	As above and: 1. The operator or operators of a swarm of drones.

	5. Provide commercial drones of different sizes. 6. Provide a swarm of drones. 7. Ensure the presence of a falconer with a bird or birds.	5. Perform UAS tracking test on straight and cross flight. 6. Perform a correctness test - how long does the tracking lose the UAS. 7. Perform a tracking speed test. 8. Perform a system behaviour test in the event of a drone swarm. 9. Test the entry of different UASs from different directions. 10. Perform the drone swarm entry test and then split it into individual UASs	
Identification			

ATTENTION!
As in the analysed systems, the Laser is not a typical detector but only serves to measure the drone's distance; conducting typical tests for detection and tracking is not justified.

6.2.2.3.7 Frequency monitoring

Most drones maintain radio communication with the remote control to receive control commands or to transmit an image. The method of detecting drones using frequency monitoring is only applicable in this case.

There are many solutions that allow the detection of a drone using passive receiving devices. SDR (Software Defined Radio) receivers are most often used for this purpose. Transmission spectral patterns are used for detection and localization. The different detection and location technologies are shown in Figure 18.
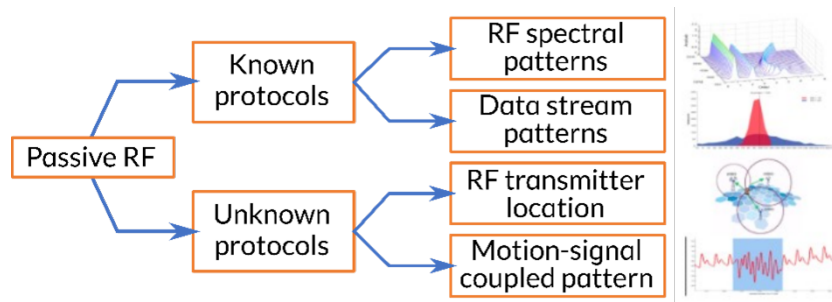
Figure 18 — Different detection and location technologies, *Jian Wang, Yongxin Liu, and Houbing Song, Senior Member, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends"*

One of the detection methods is the analysis of data transmission patterns. Based on the analysis of data packets (their length and time distribution), it is possible not only to detect, but also in some cases to identify the UAS.

Since most of the commercial drones available on the market use Wi-Fi transmission for communication, most of the available drone detection systems also analyse these bands (2.4 GHz and 5 GHz). In this case, it is possible to detect the drone by monitoring data traffic using Wi-Fi fingerprint. If the transmission protocol is known and it is possible to decode it, it is possible to recognise the drone and precisely locate it based on the location data sent by it.

In the case of unknown transmission protocols, it is possible to detect the drone based on the analysis of the radio signal and its changes thanks to the identification of unique signatures of the radio signal resulting from vibrations and shifts in the transmitted radio signals.

Signal tracking and the triangulation method are used to accurately locate the UAS and the operator station. Thanks to this, it is possible to track the location of both the drone and its operator.

It should be noted that the method of detecting and locating drones using frequency monitoring is one of the cheapest and most widely used in available commercial solutions, despite its constant imperfections. This technology is under constant development and is expected to lead the way in commercial UAS detection and location.

Limitations of frequency monitoring devices resulting from the physical phenomena related to their operation are:

- This type of systems is prone to deliberate interference.
- The background-rich electronic environment of the measurement environment significantly reduces the detection efficiency.
- Most solutions only define possible threats in the direction of without specifying the correct object distance.
- Detection, tracking and locating of objects is limited by the presence of natural and artificial terrain obstacles creating covered zones.

- The detection range drops significantly due to interference with other devices (in an urbanized area).
- Most frequency monitoring systems only detect WiFi frequencies (2.4 GHz and 5 GHz) - narrow detection range.

Due to their design and use, additional limitations of frequency monitoring devices are given below:

- It is required to set up a system of receiving antennas to locate a drone.
- Limiting the system to a single antenna results in a loss of object localization, allowing only the object to be detected. Unless the given system can decode the transmission and based on its data, provide the position of the drone.
- Transmission analysis or decoding is required to identify the object.
- There is a need to be able to follow the frequency when listening for hopping transmissions.
- A small database of drone signatures that can change depending on the software version limits the possibilities of recognition. The types of transmission are also variable.

Table 22 — Tests' requirements for frequency monitoring devices

Frequency	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Provide electromagnetic background measurements. 2. Provide non-commercial radio-controlled drones operating outside the 2.4 GHz and 5 GHz bands. 3. Provide commercial drones of various manufacturers and types to check which ones will be detected and tracked. 4. If possible, provide a station that interferes with the system operation - generating a disturbing signal of a specific frequency or broadband.	1. Perform a non-commercial radio-controlled UAS detection test. 2. Perform a detection test of commercial UASs of different manufacturers and of different types. 3. Perform a detection test of more than one UAS. 4. Perform a drone swarm detection test. 5. Perform a UAS detection test in the event of disturbing the frequency of communication with the drone.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide service for the jamming station, if used. 5. Provide drone operators (minimum 3 drones) and a swarm of drones.
Tracking	1. Provide electromagnetic background measurements. 2. Provide non-commercial radio-controlled drones operating outside the 2.4 GHz and 5 GHz bands. 3. Provide commercial drones of various manufacturers and types to check which ones will be detected and tracked. 4. If possible, provide a station that interferes with the system operation - generating a disturbing signal of a specific frequency or broadband.	1. Perform a non-commercial UAS tracking test. 2. Perform a tracking test of commercial UASs that can be tracked and check the refresh rate of the UAS position on the operator's map. 3. Test the accuracy of the UAS positioning in case of triangulation. 4. Perform a test of the accuracy of determining the operator's position based on triangulation. 5. Perform a UAS tracking test in case of disturbing the frequency of communication with the drone.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide service for the jamming station, if used. 5. Provide drone operators (minimum 3 drones). 6. Check if the system is reading the drone's position based on the read data from the communication or based on triangulation, by analysing the uncertainty on the position measurement

Frequency	Test field	Testing methods / Scenarios	Tests handling
			7. Check the minimal signal strength at which the system can track the UAS transmission
Identification	1. Provide electromagnetic background measurements. 2. Provide commercial drones of various manufacturers and types to check which ones will be detected and tracked.	1. Perform a commercial UAS identification test of different manufacturers and of different types. 2. Check whether the identification takes place automatically or whether action is required by the system operator.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide drone operators (minimum 3 drones).

6.2.2.3.8   Acoustic sensors

Acoustic drone detection systems use directional microphones to capture the sound generated by a flying drone. Acoustic analysis allows, under certain conditions, not only to detect, but also to identify and track the drone.
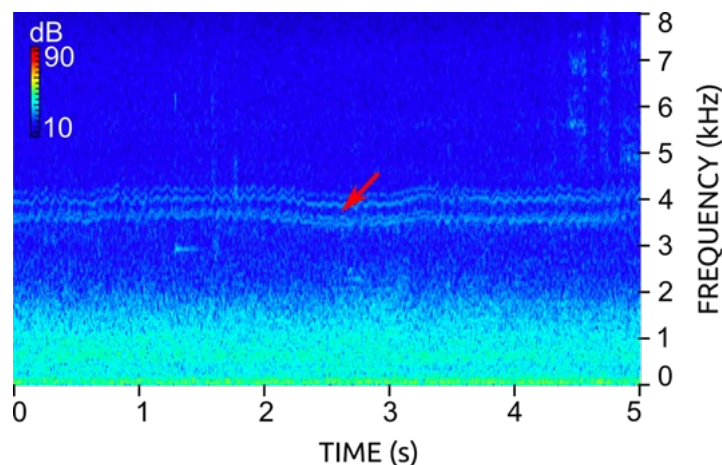
Figure 19 — Spectrogram from the directional microphone directed at the drone, *Busset, Jo, Perrodin, Florian, Wellig, Peter, Ott, Beat, Heutschi, Kurt, et al. 2015 "Detection and tracking of drones using advanced acoustic cameras"*

The four oscillating horizontal lines at about 4 kHz (red arrow) correspond to the sound emission of the four propellers of a quadrocopter.

In order to detect UASs, arrays of microphones are usually used, from 4 to even 120, evenly distributed in an omnidirectional arrangement. This solution has two advantages. It allows, with appropriate software, to determine the azimuth, direction of movement of the drone or more drones, and, in some cases, the height at which the UAS is moving. The second advantage of using more microphones is the increase in the signal-to-noise ratio thanks to the background noise analysis. To locate the drone more precisely, some solutions use more microphones and a triangulation technique.

In order to achieve the best possible detection results, digital signal processing with the use of various algorithms is used. The software allows both the probability of UAS detection and its recognition to be improved. Drone recognition, offered by some solutions, uses previously saved acoustic signatures assigned to a specific type of drone. Unfortunately, due to the multitude of solutions and construction changes of drone manufacturers, the recognition is not fully effective. Currently, the best results in detection are achieved using machine learning (ML) systems.

The advantage of using acoustic sensors is their passivity and relatively low cost. However, it should be noted that the best results are obtained by using a larger number of good quality microphones, which affects the price of the solution.

The detection range depends to a large extent on the environmental conditions and acoustic signature of the target. Wind, rain and high levels of background noise significantly reduce the range of this solution. Currently, effective ranges of acoustic systems range from 150 to 300 m for small class 1 multirotors.

Figure 20 — AMBOS acoustic drone detection system developed at the Fraunhofer Institute, *https://www.fkie.fraunhofer.de/en/departments/kom/ambos.html#1514342531*

The limitations of acoustic sensors resulting from the physical phenomena related to their operation are:
- This type of sensor has range limitations, when used as single Point Defence sensor.
- Detection range can be affected by refraction caused by wind and atmospheric temperature variations.
- Detection range is reduced when the ambient acoustic noise floor(level) is increased (e.g. in urban environments/areas).
- The elimination of non-linear acoustic disturbances, which hinders the interpretation of the tested signals, is problematic.

Due to their design and use, additional limitations of acoustic sensors are given below:
- Minimization of noise and the system's own acoustic disturbance as well as vibration during object detection is required.
- There is a need to collect background recordings or calibration each time in a new environment where the sensor is to be located.
- There is a need for a large database of background recordings and known acoustic signatures.
- There may be a background sound (e.g., cars, airplanes, mowers) that may cause false alarms.
- A number of microphones are required, among others to determine the direction to the sound source and eliminate interference.
- The more data in the database, the more time it takes to compare the signatures and the actual detection - a lot of computing power is required (if there is no machine learning used for target identification).

Table 23 — Tests' requirements for acoustic sensors

Acoustic	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Provide a test field with single trees in the detection zone. 2. Provide a test field with a forest wall in the detection field. 3. Provide a test field with buildings in the detection area. 4. Provide background noise measurements. 5. Provide a device that generates sounds that disrupt the detector operation. 6. Provide non-commercial UASs. 7. Provide commercial UASs of various manufacturers and of various types and weight classes.	1. Detection of UASs with single trees in the detection field. 2. Detection of UAS with forest wall in the detection field. 3. Detection of UASs with buildings in the detection field. 4. If possible, test the operation of the system in different weather conditions (sun, rain, fog). 5. Perform single UAS detection range test. 6. Perform a detection test of more than one UAS (will more than one UAS be detected?). 7. Perform a test of the influence of the speed of the UAS on the detection range (UAS moving perpendicularly). 8. Perform the UAS detection test in case of acoustic disturbances. 9. Test whether a false alarm can be triggered if any devices that may interfere with the operation of the system are used in the vicinity of the detector (e.g., mower, blower, hammer drill, etc.) 10. Perform a test of the system's behaviour in the event of a swarm of drones.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the interfering device, if used. 5. Provide drone operators (minimum 3 drones) and a swarm of drones.

Acoustic	Test field	Testing methods / Scenarios	Tests handling
Tracking	1. Provide a test field with single trees in the detection zone. 2. Provide a test field with a forest wall in the detection field. 3. Provide a test field with buildings in the detection area. 4. Provide background noise measurements. 5. Provide a device that generates sounds that disrupt the detector operation. 6. Provide non-commercial UASs. 7. Provide commercial UASs of various manufacturers and of various types and weight classes.	1. Perform the UAS tracking test - indication of the direction in which the UAS is located and possibly the distance (if possible). 2. Perform a tracking test of more than one UAS. 3. Perform the UAS tracking test in case of acoustic disturbance.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide support for the interfering device, if used. 5. Provide drone operators (minimum 3 drones) and a swarm of drones.
Identification	1. Provide background noise measurements. 2. Provide non-commercial UASs. 3. Provide commercial UASs of various manufacturers and of various types and weight classes	1. Perform a commercial UAS identification test of different manufacturers and of different types - if the system offers such functionality. 2. Perform a non-commercial UAS identification test - if the system offers such functionality. 3. Perform a drone swarm identification test (does the system identify individual drones in the swarm or displays information about the detection of a swarm or a single drone). 4. Check whether the identification is done automatically or whether an action is required by the system operator (screening identification).	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide drone operators (minimum 3 drones) and a swarm of drones.

6.2.2.4 Relevant C-UAS parameters

Defining relevant C-UAS parameters based on the data contained in available documents and data sent in response to the inquiry. Identification of eventual discrepancies in the collected technical parameters.

Technologies used in anti-drone systems can be divided into active and passive, i.e., those that send a signal into space to detect an echo reflected from the object and those that detect the signal coming from the object without the need to "illuminate" it first. Active technologies include radars and lidars – they account for 28.6% of the available technologies (Figure 21 a.). In contrast, 71.4% are passive technologies. When this data is multiplied by the number of devices used in the found C-UAS solutions, active technologies are 27%, passive technologies are 73% (Figure 21 b.). Therefore, for a group of active systems constituting 1/4 of all systems, the necessary analysis of the approval for use in a given test environment and use scenario should be considered. Such analysis must result from the methodology of tests and the need to measure the parameters of electromagnetic radiation declared by the manufacturers should also be considered.

Technology type		
Active	Passive	
R		79
	V	67
	T	51
	I	3
L		6
	F	92
	A	15

a) Table format

Technology type

Active (R, L) 27%

Passive (V, T, I, F, A) 73%
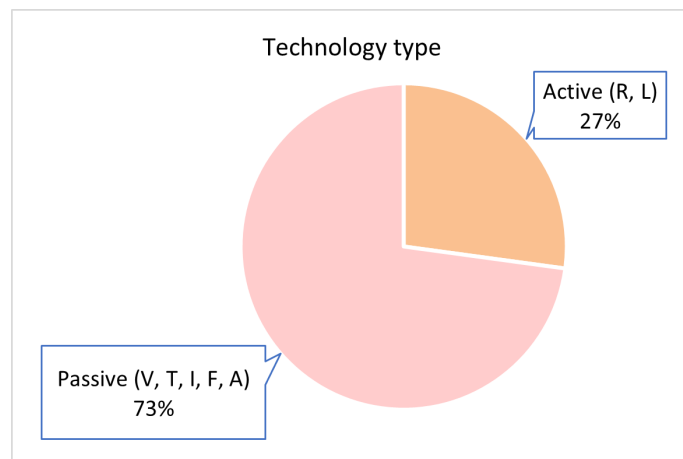
b) Pie chart format

Figure 21 — Division of technologies (Radars, VIS cameras, Thermal cameras, IR sensors, Lasers/ lidar rangefinders, Frequency monitoring devices, Acoustic sensors) into passive and active types

From a practical point of view, it is known that manufacturers are able to adjust the range of emitted electromagnetic radiation to legal requirements. The key, in this case, is to include the standardization of requirements in the proposed measurement methodology to be compatible

with practical possibilities vs. real test results. It should, therefore, be clearly declared what frequencies and radiation power are allowed in a given country and scenario for active detection.

Table 24 — Noise impact on certain technologies (Radars, VIS cameras, Thermal cameras, IR sensors, Lasers/ lidar rangefinders, Frequency monitoring devices, Acoustic sensors) used in C-UAS solutions

Technology	No. of systems	Noise impact					
		Atmospheric				Electronic (frequency)	Drone signature (for chosen detection)
		Wind	Rain	Fog	Insolation		
R	79	-	+/-	+/-	-	+/-	+/- *
V	67	-	+	+	+/-	-	-
T	51	-	+/-	+/-	+/-	-	-
I	3	-	+/-	+/-	+/-	-	+/-
L	6	-	+/-	+/-	+	-	-
F	92	-	-	-	-	+	+/- **
A	15	+	+	-	-	-	+/-

*small drones
**ineffective in the absence of transmission

-	95,2%	29,4%	34,2%	59,4%	45,4%	39,6%
+	4,8%	26,2%	23,3%	1,9%	29,4%	0,0%
+/-	0,0%	44,4%	42,5%	38,7%	25,2%	60,4%
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

The graphs in Figure 22 a)-c) are a graphical representation of the data in Table 24 regarding the impact of disturbances on the given technologies used in C-UAS production. Three types of markings are used in Table 24: [+] indicates a strong influence of a given noise on a given technology, [-] no impact of a given noise on technology, [+/-] indirect or dependent on test conditions, effect of a given type of interfering factor on the performance of a given DTI technology.

Only one technology can be drowned out by strong winds, i.e., acoustic sensors, the influence of the wind on other technologies is not noticeable. Rain may disrupt the operation of VIS cameras and acoustic sensors, or partially disrupt the operation of radars, thermal imaging cameras, IR sensors and lasers (lidars). Frequency monitoring is not prone to rain or fog. Strong sunlight may affect the correct operation of 4 types of technologies: VIS and thermal imaging cameras, IR sensors and lasers (lidars). Sensors that are vulnerable for frequency/ electronic interference are (to a greater extent) frequency monitoring sensors and (to a lesser extent) radars. Incorrect selection of the drone's signature may have an impact on the correct detection for 4 technologies: radars, IR sensors, frequency monitoring and acoustic sensors.

Hence, it is necessary to introduce (or not) the distinguished constraints to the test methodology. If not, the normative interference monitoring conditions, as added to the test results, should be clearly indicated for the purpose of any comparison of the results. The difficulty in organising many kilometres of outdoor tests with the same weather and environmental conditions is understandable. This may be the basis for negating the test results and the methodology itself for a given scenario. Hence, the key is to decide on the strictly defined test conditions and the method of their monitoring.
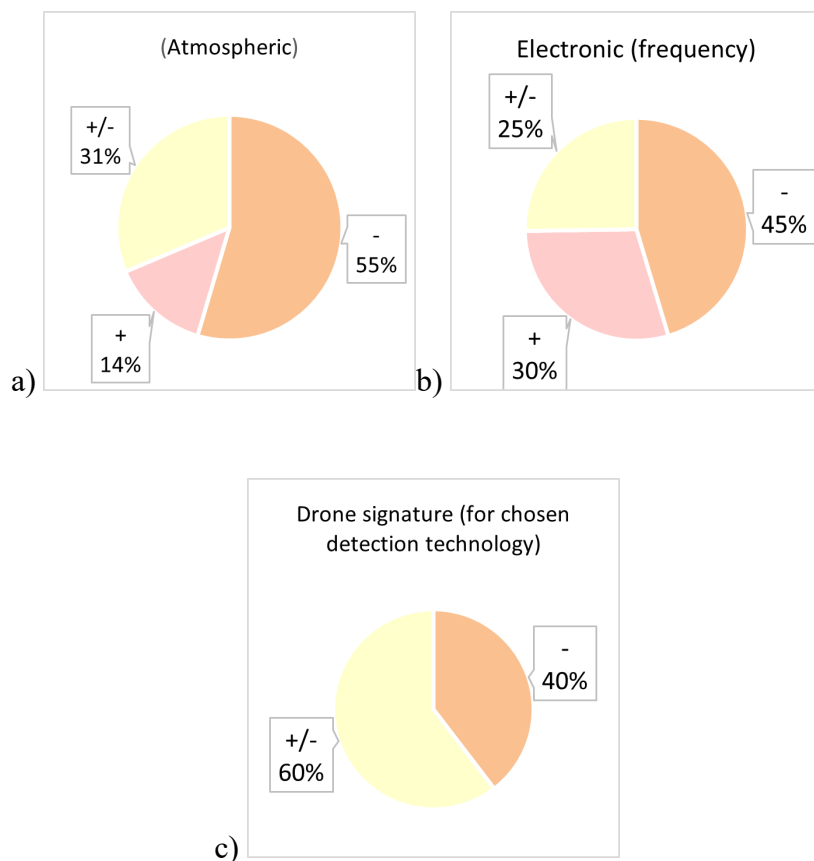
Figure 22 — Impact of noise on certain technologies used in C-UAS solutions

To sum up, for nearly 50% of devices, the influence of atmospheric conditions, electromagnetic interference or factors related to the signature of the object related to a given detection technology is significant and cannot be ignored. Detailed explanation of the measurement conditions in the selected test methodology is crucial in the representative evaluation of the usability of the C-UAS solution.

Table 25 — Abilities of technologies used in C-UAS solutions resulting from physical phenomena

Technology	No. of systems	Detection	Speed	Direction	Altitude	Size	Distance
R	79	+	+	+	-	+/-	+
V	67	+/-	+	+/-	+	+/-	+/-
T	51	+/-	+	+/-	+	+/-	+
I	3	+	+	+	+	+	+/-
L	6	-	+/-	-	+/-	-	+
F	92	+	-	+	+	-	+
A	15	+	-	+/-	+/-	+/-	+/-

Table 25 presents the possibilities of various technologies for detecting drones, their speed, direction of flight, altitude at which they are flying, their size and the possibility of giving the distance to the sensors.
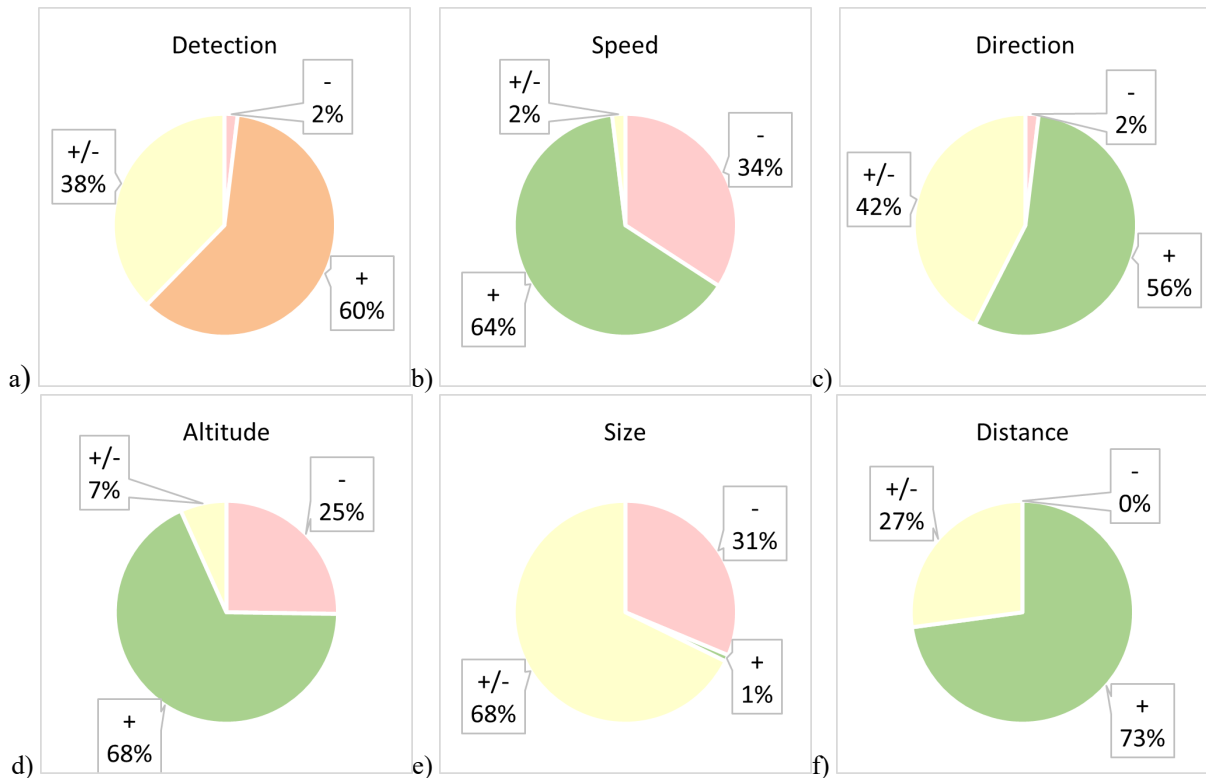
Figure 23 — Abilities of technologies used in C-UAS solutions arising from physical phenomena – resulting from Table 25

The charts in Figure 23 a)-f) are a graphical visualisation of Table 25. Additionally, in Figure 23 a)-f), the percentages depend on the number of devices offered in the given technology.

Four technologies can be used for detection: microwave radars, IR sensors, frequency monitoring, acoustic sensors. If VIS and thermal imaging cameras do not have additional intelligent image analysis, they cannot be used to detect passing objects. Two out of the seven technologies, i.e., frequency monitoring and acoustic sensors, cannot cope with speeds (if there are additional signal decoding algorithms in frequency monitoring sensors, the speed might be detected – there is no information about this solution in the gathered review). Lidar-laser devices will not detect the direction of drones' flight. Radars are unable to measure/ give the height of passing drones. Laser-lidar devices and frequency monitoring cannot give the size of the drone. When stating the distance to the drone, most technologies have no significant problems, but physically it is possible thanks to 4 technologies: radars, thermal imaging cameras, lasers-lidars, and frequency monitoring.

Table 26 — Abilities of certain technologies (Radars, VIS cameras, Thermal cameras, IR sensors, Lasers/ lidar rangefinders, Frequency monitoring devices, Acoustic sensors) to D detect, T track and I identify

Technology	No. of systems	D	T	I
R	79	+	+	-
V	67	+/-	+/-	+
T	51	+/-	+/-	+
I	3	+	+	+
L	6	-	-	-
F	92	+	+	+
A	15	+	-	+

Table 26 shows the dependence of detection, tracking, and identification on the physical properties of a given technology. Symbol: [+] means trouble-free detection, [-] no detection, [+/-] detection possible with additional software or intelligent image analysis (for VIS and thermal imaging cameras).

Thus, radar technology enables both UAS detection and tracking but does not allow for the identification of the object.

VIS light and thermal imaging cameras do not enable detection or tracking by themselves, but after applying appropriate image analysis algorithms and rotating pan-tilts, they can detect and track an object. The cameras are a great identification tool (of course, at the right distance from the drone).

Infrared sensors (to put it simply – in terms of the mode of operation: "infrared radars", enabling omnidirectional operation) can handle both detection and tracking as well as identification.

Lasers (in the sense of range-measuring lidars) cannot be used as detection, tracking, or identification devices. Hence, this technology never stands alone in C-UAS solutions (see Figure 6).

Table 27 — Abilities of certain technologies (Radars, VIS cameras, Thermal cameras, IR sensors, Lasers/ lidar rangefinders, Frequency monitoring devices, Acoustic sensors) to detect certain things (* depending on the specific solution, and chosen technology)

Technology	No. of systems	Detection of:			
		Min. speed	Max. speed	Flight direction	
				Towards sensor ↓	Across sensor →
R	79	+	+	+/- *	+/- *
V	67	-	-	+/-	-
T	51	-	-	+/-	-
I	3	+/-	+/-	+/-	+
L	6	+	+	-	-
F	92	-	-	+	+
A	15	-	-	+/- *	+/- *

Table 27 shows the physical ability of technologies to detect specific variables. If a given technology enables the detection of a given variable resulting from the movement or size of the drone, the symbol [+] appears in the given cell, or a symbol [-] if the technology does not enable detection of a given variable. If the technology itself does not enable the detection of a given variable, but there are algorithms/ computer programs with the help of which the detection is possible, then the symbol [+/-] appears in the given cell.

Radar technology has no problem detecting a slow or fast object, but it does not always detect movement towards the radar. It depends strictly on the physical properties of the given radar. This vulnerability in the radar operation can be circumvented by software, hence the symbol appears in the table. Each radar will detect movement across the sensor.

Both VIS and thermal imaging cameras will not detect the drone if it moves too slowly or too fast or if it moves across the camera's view direction. However, if the drone moves towards the camera, programmatically, using the so-called intelligent image analysis, it can detect a flying drone. However, these analytics should be tested in the field tests of C-UAS solutions.

Infrared sensors should not have any problems with detecting slow objects or any problems with detecting fast objects. In addition, they should distinguish the direction of flight of the drone – certainly if it moves across the sensor.

Lasers-lidars during tracking will define the distance to both – slow and fast-moving drones. They will not distinguish the direction of the drone's movement.

The frequency monitoring sensors do not distinguish the speed of the drone hence the symbol appears in both boxes – minimum speed and maximum speed.

When it comes to acoustic sensors, it is difficult to detect the direction in which the drone is moving – it can only be predicted by estimating the zone. It is difficult, with this technology, to detect a slow-moving drone. The acoustic sensor will not distinguish it if the drone moves fast enough.

6.2.3 C-UAS methods

6.2.3.1 Identification of the methods used in C-UAS

This clause is dedicated to the possibilities of integrating the tested C-UAS solutions with external analysis and control systems. The most popular way of integration is the so-called Application Programming Interface (API). It is a set of rules that closely describes how programmes or subroutines communicate with each other.

A good API makes it easier to build software, reducing it to the programmer combining blocks of elements in a set convention. It is defined at the source code level for software components, e.g., applications, libraries, operating systems. The purpose of the application programming interface is to provide the appropriate specifications for subroutines, data structures, object classes, and the required communication protocols. One of the most popular types of API is web APIs. It is a type of API where functions are made available as a resource on the web. Current web API systems allow to easily integrate information from the web with applications, extending their functions or enabling interoperability.

However, in the case of the integration of C-UAS systems, which are an autonomous element that develops a decision on e.g., detection or identification, it is not necessary to transmit raw data from the cameras. Therefore, in this case, it is much more efficient to use the SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) standard. It allows you to send the developed decisions from the autonomous elements of the system. An HTTP-based REST API would overburden bandwidth, while SAPIENT sends binary data to a TCP socket (server socket), which is more efficient. If you need to take a screenshot from a camera, for example, it is possible to send the URL of the photo to the server, i.e. it is not sent directly. Taking into account the above information, SAPIENT is a much more tailored solution for the integration of C-UAS systems than REST API.

6.2.3.2 Methods of working out the alarm signal

Producers of the analysed C-UAS do not write much about integration methods with external systems, only paying attention to whether their C-UAS has such functionality (Figure 24). Only two manufacturers specify the possibility of integration with radar, camera, and mitigation systems. However, only one describes the API interface used, which can be accessed via JSON and gRPC. Nevertheless, it can be safely assumed that most of the systems that allow integration with external systems use the API interface due to its current universality.
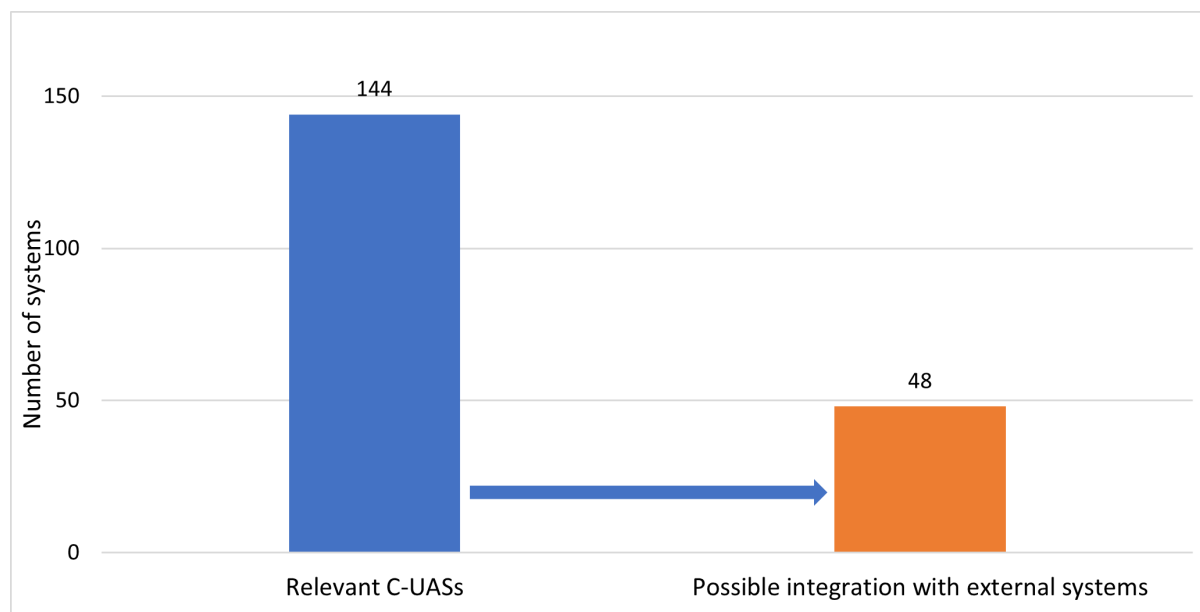
Figure 24 — Integration of the C-UAS solution with external control and analysis systems

6.2.3.3 Correlation methods of signals from selected technologies

Regarding C-UAS solutions, the correlation should be understood as a measure of the interconnection between technologies present in a given system (called features in this section). Due to the method of analysis, the correlation can be divided into:

- Simple - examining the relationship between two features.
- Partial - informing about the relationship of two features, excluding the third.
- Multiple - informing about the relationship between one feature and several features taken together.

Due to the result of the relationship between the features, the following are distinguished:

- Positive correlation – it can be said about it when the values of the variables change in the same direction. So, if one grows, the other behaves the same way.

- Negative correlation – in this case, the situation is entirely different. A negative correlation means that the values of dependent variables change in opposite directions – they are inverse. So, if one value goes up, the other goes down, and vice versa.

- No correlation is a situation in which phenomena, features, and properties that have no relation to each other are compared.

In order to quantify the degree of correlation between features, the so-called correlation coefficients. The most popular of them is the so-called Pearson's linear correlation coefficient. It determines the level of linear dependence between the features. The correlation coefficient value is in the closed range [-1, 1]. The greater its absolute value, the stronger the linear relationship between the variables. 0 - means no linear relation, 1 - means a positive relation, and -1 - means a negative relation between features.

C-UAS solutions very often make it possible to make decisions about detection, identification, or tracking using only one technology for this purpose; however, additional technology performing the same task can improve the efficiency of this process. However, the condition is that the results of individual classifications are similar, as a significantly weaker classifier may adversely affect the final result of the task. It is possible that C-UAS manufacturers use additional technologies to limit the set of results initially and then decide by another technology or by applying weights of the results obtained from individual technologies. Unfortunately, the manufacturers do not

describe the details of this process. Figure 25 shows the likely possible correlations between the pairs of technologies used by C-UAS producers.
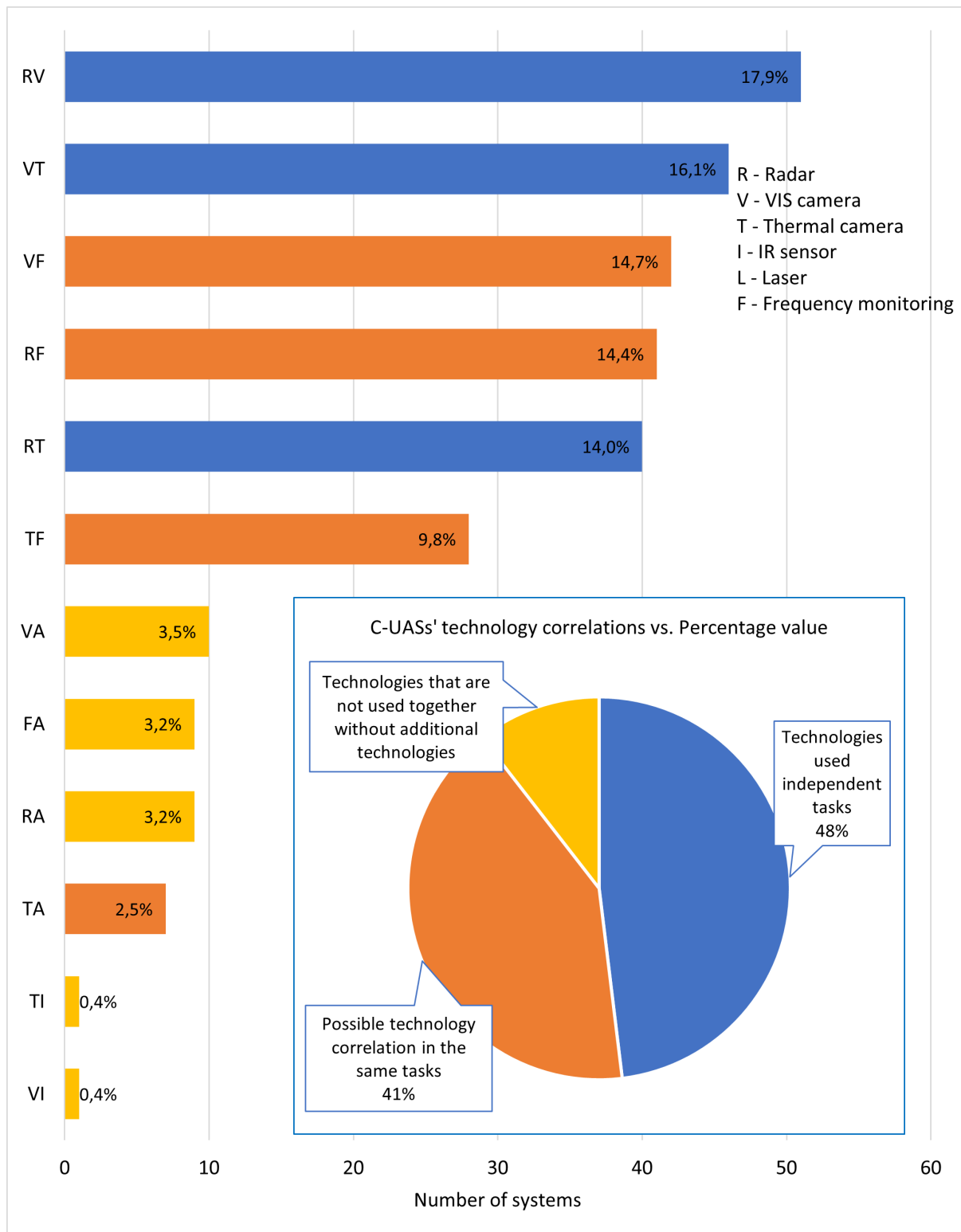
Figure 25 — C-UAS technology correlation

6.2.3.4 Identification methods

Analysis of the used identification methods, including the use of companies' authors' signatures of objects

In the compared C-UAS solutions, sensors from the EO sensor range are most often used during identification. These sensors include both HD low light sensors as well as MWIR, LWIR, and SWIR thermal sensors. The data obtained from the sensors are then used in the decision-making process, often supported by machine learning, to decide UAS identification. This allows a positive distinction between drones and other airborne objects such as planes or birds. The compared C-UAS solutions also contained information about systems enabling quick identification of types and models of drones by their visual signature, including drones from all major manufacturers. There was also information about the possibility of simultaneous recognition of many drones at the same time, which is a significant advantage of these systems.

The analysis of information about available products indicates that the other most popular method of UAS identification is monitoring and analysing the communication between the drone and the operator. Indeed, this solution is flawed because it does not apply to drones following a pre-programmed path and not maintaining communication with the operator. Detection of communication beyond the commonly used frequencies may also be a problem. The vast majority of solutions analyse communication in the 5GHz and 2,4GHz bands typical of popular commercial solutions. Few systems analyse and monitor other frequency ranges, and these are usually solutions intended for the military market.

After detecting communication between the drone and the operator, the detection system operating on this principle analyses the transmitted signals. The transmitted data includes information about the manufacturer and model of the device and information from the location system (GPS, GLONASS, etc.), making it possible to precisely locate the drone. With multiple receiving antennas and triangulation, some systems allow for an approximate determination of the operator's position. Solutions of this type are passive and usually less expensive than others using sensors, thanks to which, despite their limitations, they can be used in practice in the case of objects where commercial drones used irresponsibly may be a threat, e.g., at the airports.

The object identification process is one of the most advanced elements implemented on C-UAS solutions. For this reason, it is necessary to take into consideration numerous limitations that result from the correct performance of this process. Such restrictions include, but are not limited to:

- weather conditions,
- lighting conditions,
- distance to the tested object,
- the size of the object,
- the presence of terrain covered zones that make it difficult to detect the drone,
- the frequency and method of communication with the drone and much more.

These elements have been subjected to a broader analysis in terms of identification in tables summarizing individual technologies described in subclause 6.2.1.2.

Figure 26 shows that 69 producers of C-UAS inform that their systems enable the identification of drones, while only 30 of them specify what exactly is the subject of identification.
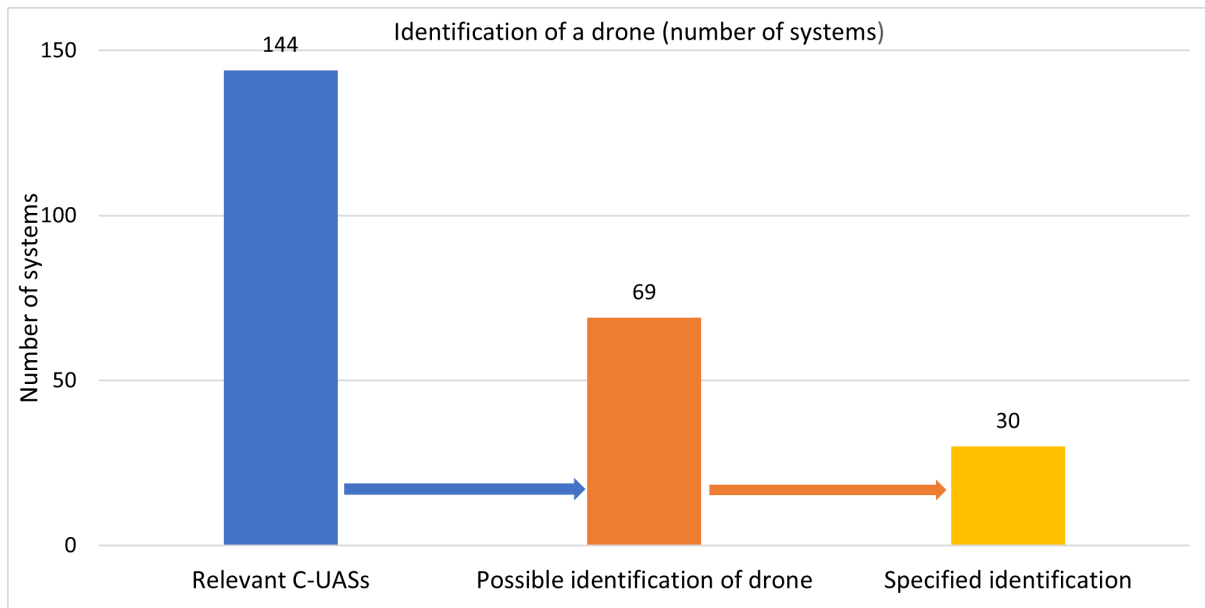
Figure 26 — Identification of a drone (number of systems)

The analysis of the collected data shows that the producers of C-UAS inform that their products enable [3], among others:

- drone model identification;
- identification of the drone producer;
- identification of the cargo/ payload;
- using internal drone base;
- detecting/ distinguishing homemade drones;
- resistance to false alarms, e.g., bird identification as a drone;
- drone operator identification.

The numerical list of this specification is presented in Figure 27. Among the tested C-UAS solutions, there are systems equipped with a different number of functionalities related to identification (1 - 6 functionalities).

---

[3] It should be noted that in some cases producer statements on this topic are not 100% reliable.
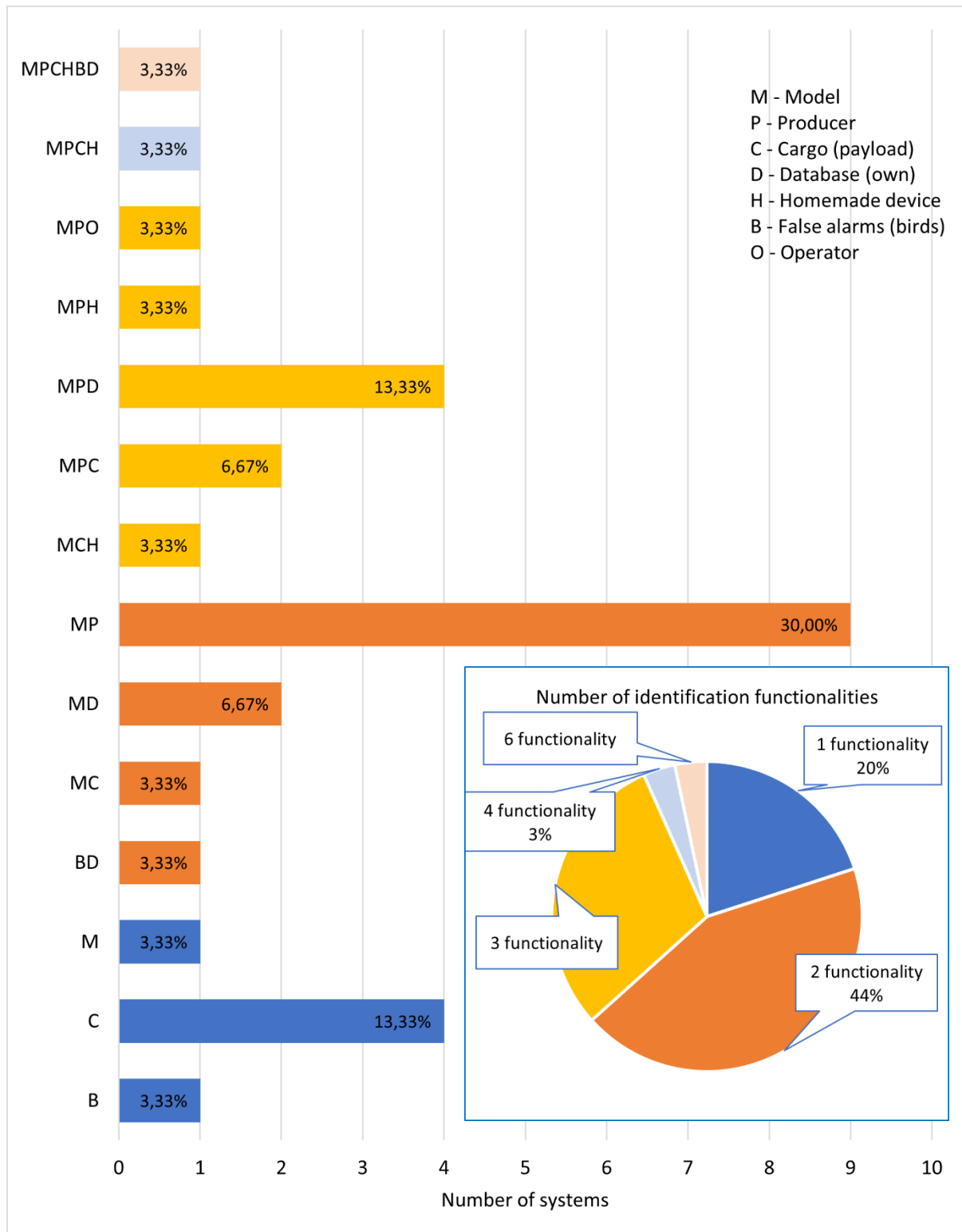
Figure 27 — Types of identification functionalities

6.2.3.5   Artificial Intelligence

6.2.3.5.1   Elaborating the role of AI in detection and identification

The compared C-UAS solutions often contain information about the use of artificial intelligence and machine learning both when supporting the process of object detection and drone tracking.

AI is also used during image recognition, so that a specific type, brand, or model of the drone can be identified. In addition, the use of AI should also be distinguished in the process of holistic determination of a detected object as a threat. In the air defense business, such a process is called a "threat evaluation," which provides decision support (which improves command and control as well as situational awareness) and is designed to improve the operational velocity of operators. In this case, the system, takes into consideration numerous information from available sensors, such as:

- microwave radars (impulse and FMCW),
- acoustic detection systems,
- passive systems that detect communication between the drone and the operator and decode the information transmitted
- systems using video signal analysis from daylight cameras and thermal imaging cameras
- thermal imaging radars,
- lidars,
- measurement of the speed of the object,
- measurement of the size of the object,
- crossing the zone not allowed by the object,
- time of the object occurrence in relation to projects implemented in the observed area,
- detection of carried loads by the drone.

All these elements, thanks to the appropriate correlation mentioned in subclause 6.2.2.2 and perceived as a whole, may allow the system to qualify the object to the adopted threat level. When correlating information from different sources, one of the key elements is the correct selection of information. For this purpose, artificial intelligence algorithms are very useful.

However, in many cases there is only a stripped-down description of the machine learning methods used, among them also traditional statistical methods. The most common methods of supporting decision-making during both detection and identification of drones are presented below:

- Expert systems,
- Bayesian inference,
- PCA (Principal Component Analysis),
- SVM (Support Vector Machines),
- Clustering (e.g., K-means),
- GPU Accelerated DNN (cuDNN),
- Supervised, Unsupervised learning.

Unfortunately, the use of artificial intelligence is now a "fashionable" trend that is often used only as a sales method, so in some cases it is possible that manufacturers exploit this concept. Below is a list of manufacturers of C-UAS solutions that use artificial intelligence methods when making decisions. In the vast majority of cases, there is no information about the classification methods used during the detection and identification of drones. Manufacturers of systems relying on machine learning algorithms need to provide this information and require themselves deep knowledge of the machine learning methods used and of the C-UAS problem they intend to solve.

In cases where training is used to feed classifiers, it is also important for an end-user to know:

1) Who bears the costs for producing testing data;

2) What consequences do bad training data have on false negatives;

3) How to evaluate a system where machine learning is an integral part, and what risks it entails.
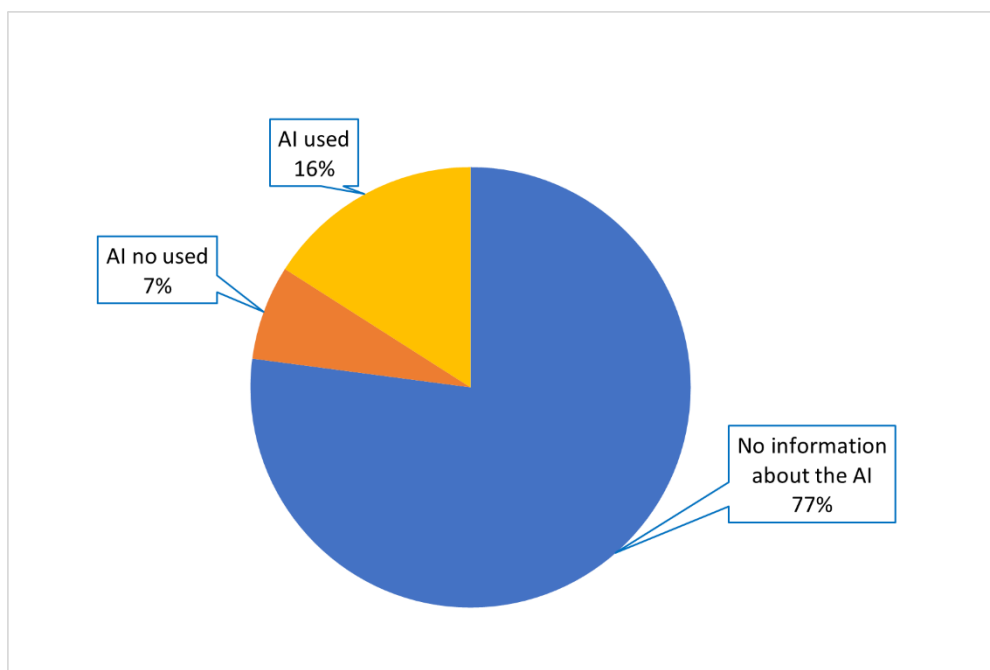
Figure 28 — The use of AI in the detection and identification of drones (number of systems)

6.2.3.5.2 Expert systems

An expert system is a program or set of computer programs that supports the use of knowledge and facilitates decision making. It uses inference procedures to solve those problems that are so difficult that they normally require significant expert judgment. Knowledge along with inference procedures can be considered as a model of expertise normally possessed only by the best specialists in a given field. Expert systems can support or replace human experts in a given field, they can provide advice, recommendations and diagnoses on problems in this field. In the case of C-UAS, expert systems can independently decide e.g., to identify a drone or provide valuable situational analysis about a detected object, supporting identification by an expert.

The components of the expert system are:

- The backbone of the system consists of:
    - User interface. The user uses the system by communicating with it via the user interface. It usually comes down to asking questions, providing information to the system, and receiving answers and explanations from the system.
    - Knowledge base editor. Thanks to the built-in editor, it is possible to modify the knowledge contained in the system, which allows for the expansion of the system.
    - Inference engine. It is the most important component of the expert system; its task is to draw conclusions from the premises and questions entered by the user and generate answers.
    - Explanation system. This mechanism makes it possible to explain, at the user's request, why the system provided such and not another answer, or why the system asked the user a specific question.
- Knowledge base. It is the second most important component of the system. The knowledge base contains knowledge extracted from human experts in a specific field. This knowledge is usually written in a chosen way of knowledge representation, for example in terms of rules or a framework.
- Case specific data: working storage. It is an auxiliary database in which the conclusions obtained by the system during its operation are stored. This database makes it possible

to recreate the system's inference method and present it to the user by means of an explanatory mechanism.

Generally, knowledge engineers are involved in extracting knowledge from experts. This is usually a long and arduous process because the knowledge used by human experts is usually practical and intuitive.
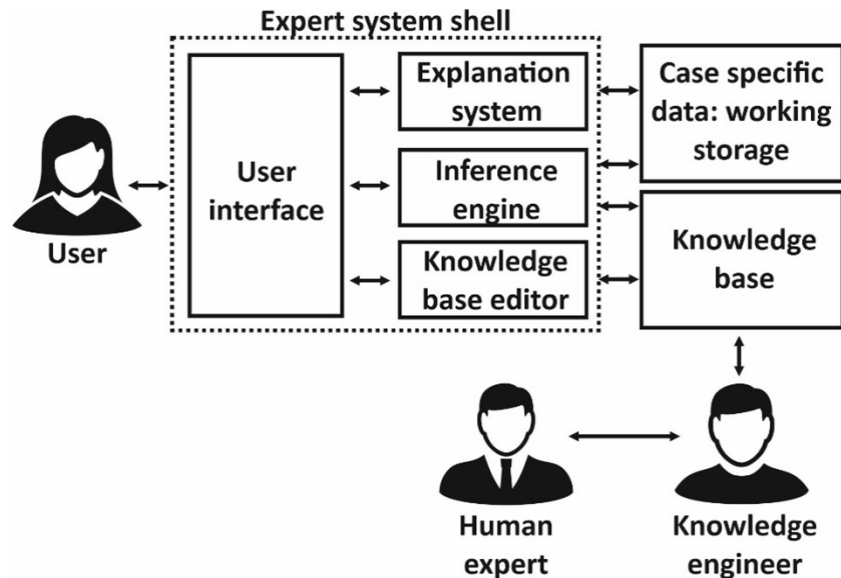
Figure 29 — Scheme of operation of the expert system

6.2.3.5.3   Bayesian classifiers

Bayesian classifiers, based on Bayesian theorems, are probabilistic classifiers and are one of the machine learning methods used to solve the classification problem. The task of the Bayes classifier is to assign a new case of observation to one of the predefined classes, and the set of decision classes must be finite and complete. According to Bayesian theory, the most likely class to which a new object should be assigned is the class that maximises the conditional probability. This class is marked as maximum a posteriori.

One of the known and currently used methods of Bayesian classification are the so-called Gaussian mixture models GMM, which are perfect for modelling multidimensional data, which for easier visualisation were projected and presented in two dimensions as points (see Figure 30). They constitute training data in the process of creating Gaussian mixture models. In the training process, the linear combination of Gaussian distributions adapts to the training data, adjusting its parameters so as to generalise the considered data with the highest probability.
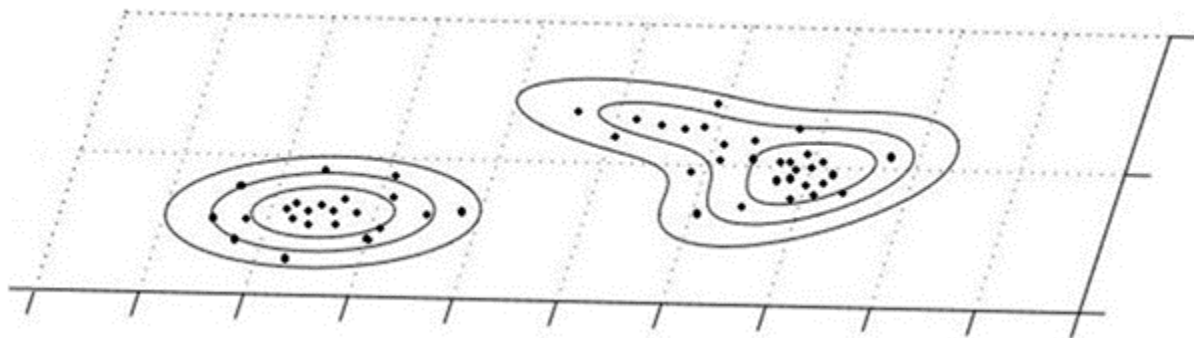
Figure 30 — Visualisation of the training data of the object on a 2-dimensional plane, *K. Kamiński, "Automatic speaker recognition system based on Cepstral speech signal analysis and Gaussian mixture models", PhD thesis, WAT*

Then, in the identification stage, a check is made of the belonging of the recognised object (its extracted distinctive features) to the models in the database. As shown in Figure 30, an exemplary model of the object (drone) A is not well suited to the distinctive features of the recognised object. In the case of model B, a much greater degree of similarity of the model to the identified object is visible, which may prove its correct identification.
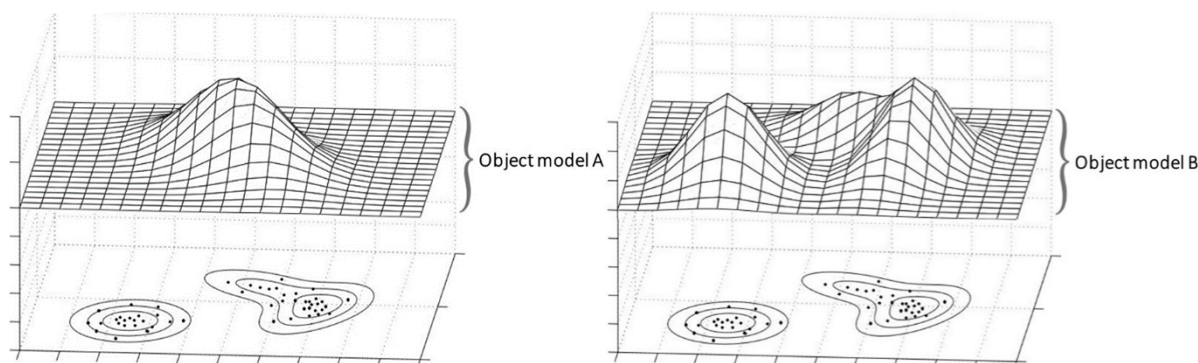
Figure 31 — Visualisation of the object (drone) identification process with the use of Gaussian mixture models, *K. Kamiński, "Automatic speaker recognition system based on Cepstral speech signal analysis and Gaussian mixture models", PhD thesis, WAT*

The last stage of the system's operation is the decision-making system, which allows to determine the scale of model similarity and compare it with the empirically determined threshold. This allows you to avoid a situation in which the recognised object, e.g., a bird, would be forcibly matched to the drone model that is most similar to.
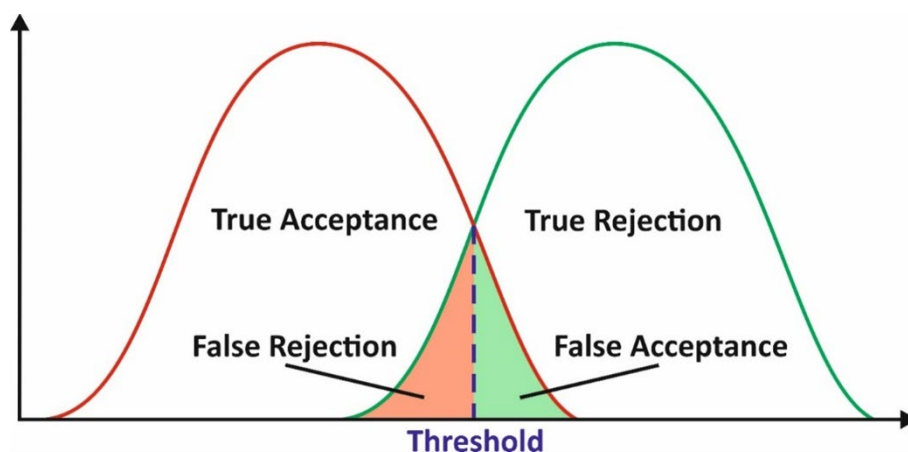
Figure 32 — Probability density distributions for an object from outside the base (red distribution) and for an object located in the drone base (green distribution)

6.2.3.5.4 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is one of the most popular dimension reduction algorithms. In general, it is about projecting data to a space with fewer dimensions to best preserve the structure of the data.

It is mainly used to reduce the variables describing a given phenomenon and to discover possible regularities between the features. A thorough analysis of principal components enables the identification of those initial variables that have a large impact on the appearance of individual principal components, i.e. those that make up a homogeneous group.

PCA analysis consists in determining the so-called principal components, which are linear combinations of its coordinates, where successive components are mutually uncorrelated,

ordered in descending order and so defined as to maximise variability that was not captured by the previous components. Each principal component "explains" some of the variability in the input fields. The total variance is the sum of all eigenvalues.

There are two practical implications from this:

- The coordinates of vectors can be treated as new uncorrelated features, where when constructing a classifier, their number is usually limited to only a few of those whose values are their own are the greatest,
- The graphic representation of all cases in the two or three-dimensional space of the first PCA coordinates can be used, which will allow for a collective assessment of all the considered features and any of their subsets, and the selection of the best subset of features (Figure 33).
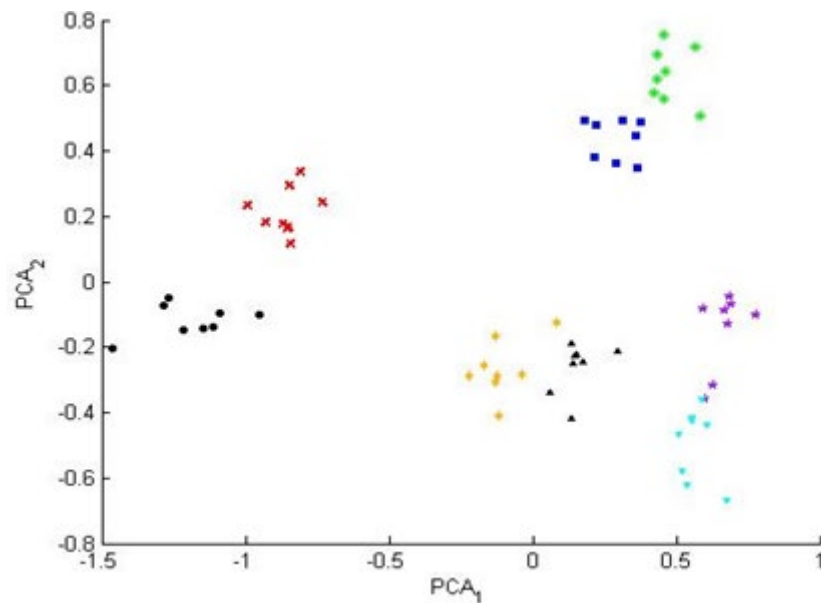
Figure 33 — Distribution of cases in the space of the first two principal components for 8 objects (drones)*, E. Majda, "Automatic system of reliable speaker recognition based on Cepstral analysis of the speech signal", PhD thesis, WAT*

6.2.3.5.5   Support Vector Machine (SVM)

The SVM network technique called the Support Vector Machine technique is understood as a type of neural network using a special training method which comes down to quadratic programming. In general, in SVM networks the classification and approximation tasks are distinguished. The primary goal of the SVM network is to maximise the distance of the separating hyperplane from the nearest points of opposite classes.

SVM networks are trained on a set of training data, like classic networks. However, in contrast to the classical techniques of training neural networks, thanks to the use of non-linear programming methods, the learning process practically always leads to finding the minimum global error function.

The SVM algorithm can work in multiclass mode using one of the following strategies:

- One against all: the classifier decides whether the sample belongs to a given class or to other classes.
- One against one: for each binary classifier, the selected class scores a point, and the k-class decision is to select the class with the most points.

The most optimal shall be deemed the hyperplane that maximises the margin of separation between the two classes. The separation margin is the area between two parallel hyperplanes, inside which no teaching points lie. The interpretation of the optimal hyperplane is shown in Figure 34.

a)   b)
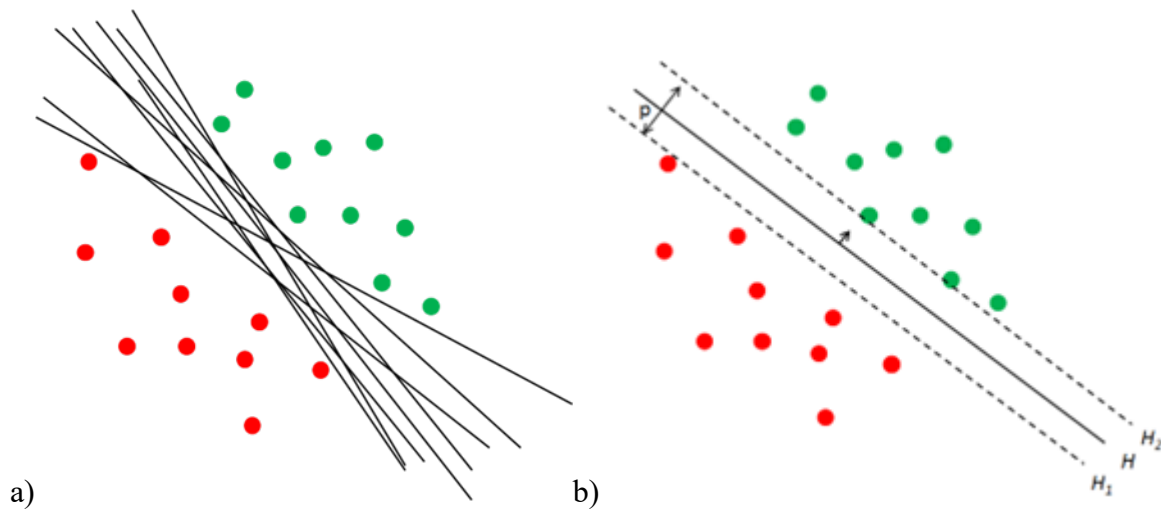
Figure 34 — Examples of multiple discriminant hyperplanes a), Interpretation of the position of the optimal hyperplane – an attempt to search for a hyperplane characterised by the maximum distance p b), *E. Majda, "Automatic system of reliable speaker recognition based on Cepstral analysis of the speech signal", PhD thesis, WAT*

6.2.3.5.6   NVIDIA CUDA Deep Neural Network (cuDNN)

Deep learning – machine learning method in the structure of which there are distinguished many layers that implement non-linear transformations. The layers represent the successive levels of abstraction creating a hierarchical model. The lowest layers represent the simplest features of the input signal, while the higher layers generate more general concepts based on relationships from previous layers.
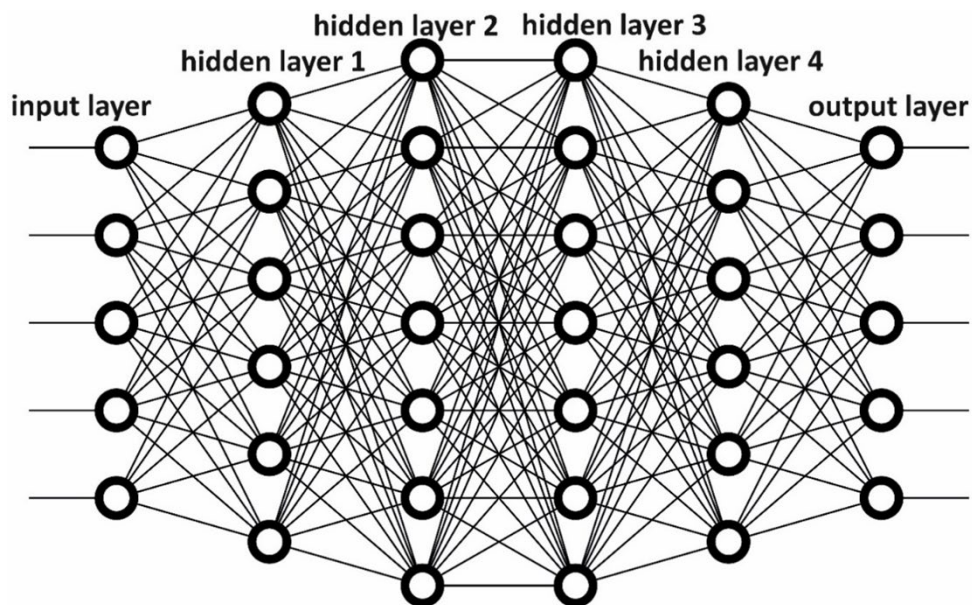
Figure 35 — Multilayer neural network

The layers can be organized hierarchically so that in the successive layers, the data is processed from a lower level, and the results are passed on to the next layer. In this way, more and more complex, high-level information can be gradually obtained from relatively simple low-level input data. It turns out that during the training process, a neural network can learn some complex properties found in the input data, e.g., specific neurons activate (i.e., the activation function takes values much greater than zero) when certain specific patterns are present in the data. These types of learning methods are called deep learning because networks with many layers are learned, and elements in each layer learn to detect and represent certain non-obvious (deep), complex data properties that have been used in the training process, in subsequent layers, folding these complex properties from simpler elements, in a sense. This is one of the most important properties for the success of deep learning. Deep learning algorithms can learn the most important complex features on their own, significantly accelerating the work of scientists – machine teachers, saving their time, reducing the chances of making a mistake, enabling the application of these solutions to many real problems, including, for example, the detection and identification of drones. However, often, much more data is needed than in the case of expert intervention, so that the neural network can learn the necessary features well enough, more computing power is also needed, which is why calculations in neural networks are currently accelerated most often with the use of graphics cards.

The NVIDIA CUDA Deep Neural Network Library (cuDNN) is a GPU-accelerated library for deep neural networks. Deep learning scientists and framework developers around the world rely on cuDNN for high-performance GPU acceleration. This allows them to focus on training neural networks and developing applications instead of spending time fine-tuning GPU performance. cuDNN works with the following Caffe2, Chainer, Keras, MATLAB, MxNet, PaddlePaddle, PyTorch, and TensorFlow implementation environments.

The following Table 28 contains requirements for the tests' field, testing methods as well as tests handling in completing the AI tests on the C-UAS solutions.

Table 28 — Tests' requirements for AI (*Artificial Intelligence* algorithms)

AI	Test field	Testing methods / Scenarios	Tests handling
Detection	1. Provide a test field with single trees in the detection zone. 2. Provide a test field with a forest wall in the detection field. 3. Provide a test field with buildings in the detection area. 4. Provide non-commercial UASs. 5. Provide commercial UASs of various manufacturers and of various types and weight classes. 6. Provide the presence of a falconer with a bird or birds.	1. Detection of UASs with single trees in the detection field. 2. Detection of UAS with forest wall in the detection field. 3. Detection of UASs with buildings in the detection field. 4. Test the behaviour of the system in the case of a group of drones, a swarm and several drones coming from different directions. 5. Perform bird / UAS discrimination tests. 6. Check whether it is possible to mark as safe objects that are legally entered for flights (functionality and interface to the air traffic supervision system). 7. Check the existence and operation of key system functionalities, such as: recording history, quality, event handling speed, history loading speed, etc. 8. Check the possibility of exporting data to external systems or integration with external systems (e.g., via API or SDK).	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide the service of the falconer. 5. Provide drone operators (minimum 3 drones).
Tracking	1. Provide a test field with single trees in the detection zone. 2. Provide a test field with a forest wall in the detection field. 3. Provide a test field with buildings in the detection area.	1. Test how long the system keeps the target (UAS) and whether it loses it after some time. 2. Perform a UAS flight test behind an object (e.g., a building or a chimney) and check whether the system detects the same object, or the UAS appears as a new object when the UAS reappears.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station.

	4. Provide non-commercial UASs. 5. Provide commercial UASs of various manufacturers and of various types.	3. Perform a test to recognize the switch of the tracked UAS after its temporary hiding (no visibility, e.g., behind a chimney or a building).	4. Provide drone operators (minimum 3 drones).
Identification	1. Provide non-commercial UASs. 2. Provide commercial UASs of various manufacturers and of various types. 3. Provide the UAS with payload or payloads to be attached to the UAS.	1. Perform a re-identification test of the same object (whether the system recognizes that it is a UAS that was previously detected). 2. Make an attempt to identify a non-commercial UAS. 3. Perform the identification test of the arriving UAS in different ways (from different angles). 4. Perform the UAS identification test with the load (whether the system recognizes that the load is attached. 5. Perform a test to identify the type of payload attached to the UAS.	1. Check the time to set up and start up the devices. 2. Check whether it is necessary to calibrate the system once / after each start-up and how long it takes. 3. Provide power and elements necessary for the construction of the station. 4. Provide drone operators (minimum 3 drones). 5. Provide various standard loads.

6.2.3.6 Elaborating methods of objects' tracking

In case of drone tracking methods, C-UAS manufacturers provide very little information. Only 20 manufacturers admit that their product allows this functionality, while only 8 indicate the possible angular tracking accuracy.
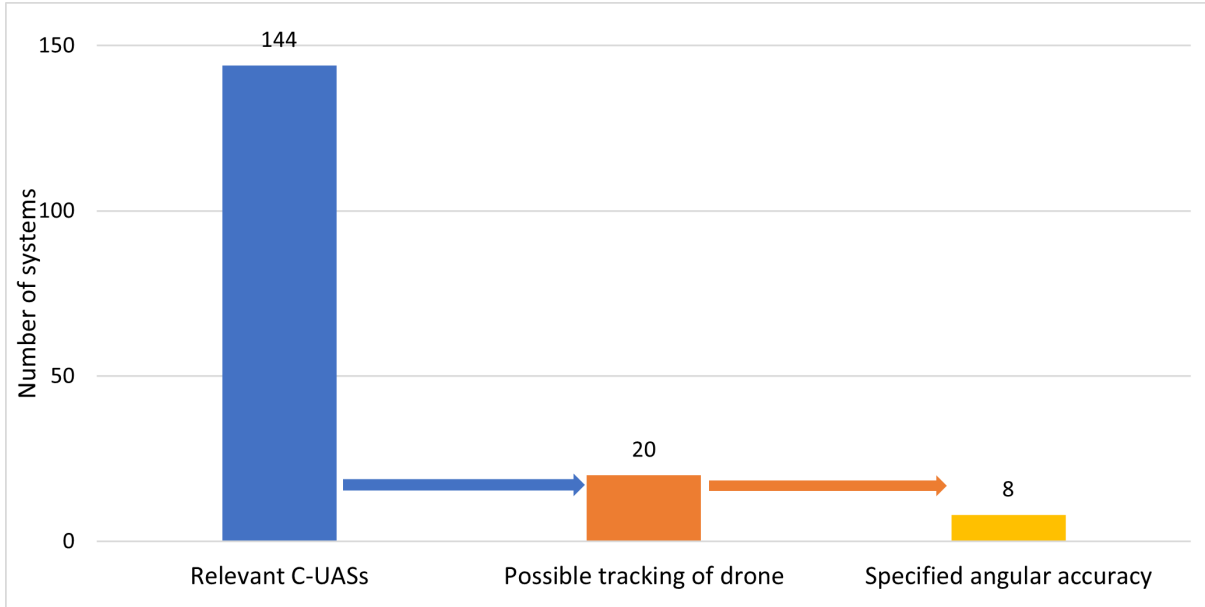
Figure 36 — Tracking of a drone ability among C-UAS solutions

The percentage of angular tracking accuracy for the manufacturers that specifies it is shown in Figure 37.
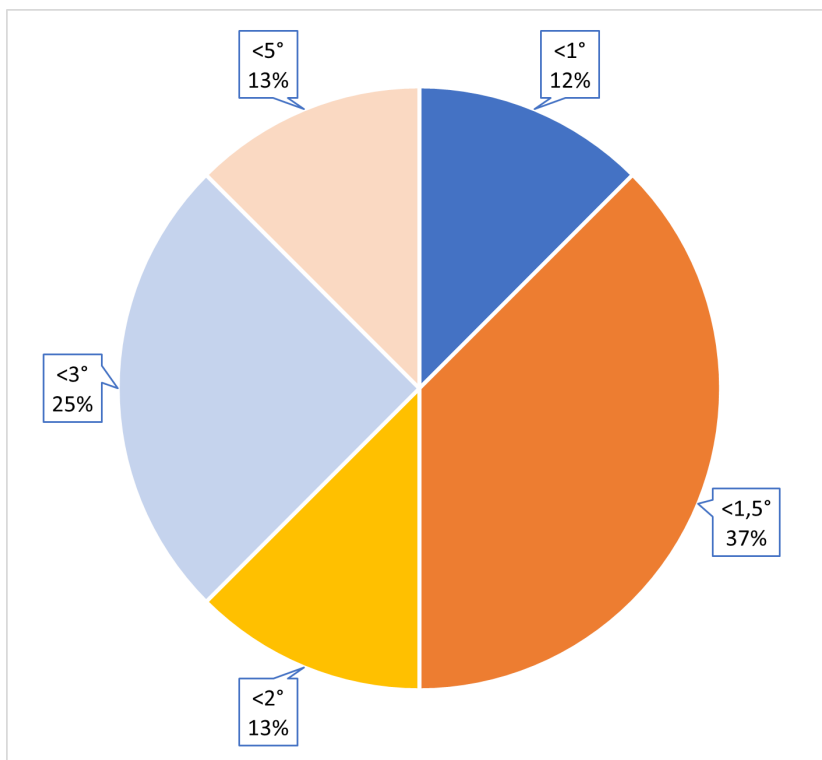
Figure 37 — Drone tracking angular accuracy

Taking into account the above angular accuracy results, it will be reasonable to include in the test scenario the possibility of checking the accuracy declared by C-UAS manufacturers. This implies the need to include in the adopted test methodology a possible deviation during the drone tracking process. This value depends on the distance from the tracked object adopted in the scenario and the declared angular accuracy, e.g. for the weakest of the declared accuracies (5°) from Figure 37 and an example tracking distance of 1 km, the deviation will be 87.5 m, which results from the formula:

$$a = b \cdot \tan\alpha \tag{2}$$

In addition, 26 C-UAS manufacturers define the possible number of targets that can be tracked. The numerical set of such an analysis is shown in Figure 38.
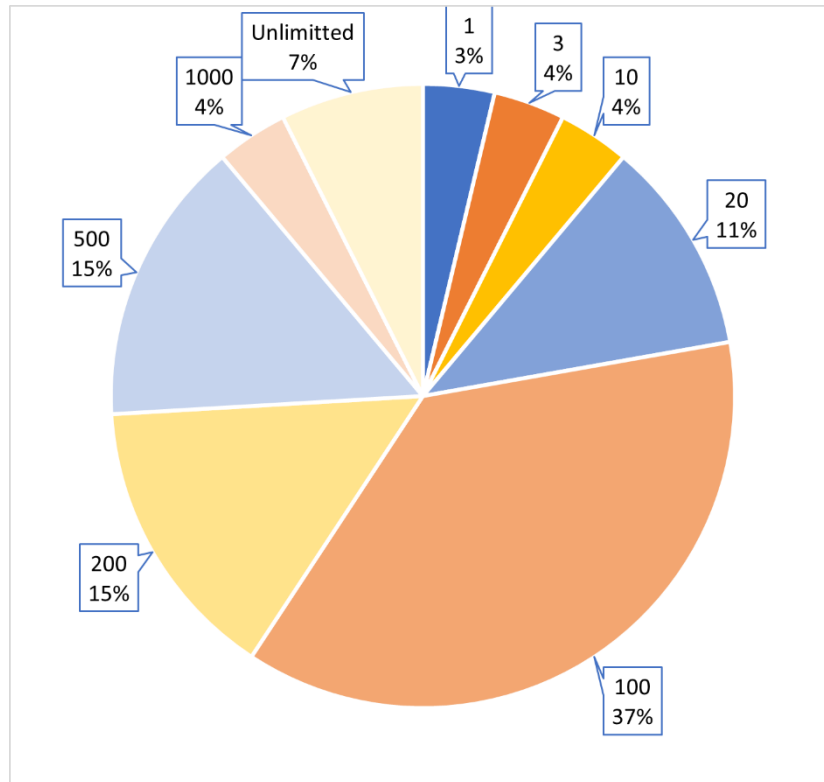
Figure 38— Number of tracking targets

When testing C-UAS it will also be necessary to assume a reasonable number of targets to be tracked. As shown in Figure 38 there is a large discrepancy in the number of tracked targets declared by C-UAS manufacturers. Adoption of the requirement of 1 000 tracked targets in the test methodology would be quite a logistic challenge, therefore it will be reasonable to adopt a compromise value, but not less than 20 targets, which will allow checking the limit declared parameters for at least ¼ of the C-UAS manufacturers, who have specified the tracking process.

6.2.3.7 Identification of logistical challenges in C-UAS use

This clause provides preliminary conditions that should be included in the future measurement methodology for radars, VIS and thermal cameras, IR sensors, lasers-lidars, frequency monitoring, acoustic sensors:

1. Check the time to set up and start up the devices.

2. Check whether it is necessary to calibrate the radar once/ each time it is turned on and how long it takes.

3. Provide the service of the falconer.

4. Provide power and elements necessary for the construction of the station.

5. Provide service for the jamming station, if used.

6. Provide the possibility of adjusting the sensor mounting height if the manufacturer allows it.

7. Provide support for the weather simulation station, if such a solution is used.

8. Provide drone operators (minimum 3 drones).

9. Provide the operator or operators of a swarm of drones.

10. Provide support for the interfering device, if used.

11. Provide various standard payloads for drones.

12. How to check if the system is reading the drone's position based on the read data from the communication or based on triangulation?

13. How to check at what signal strength the system can detect the transmission (distance and elevation or other terrain obstacles)?

These conditions result from Table 15 to Table 22 and Table 28.

6.2.4 Technological and methodological factors

Definition of technological and methodological factors influencing the test scenarios and the new C-UAS solutions' evaluation methodology

C-UAS tests, for practical reasons, can only take place in an external environment. For various reasons, it is not possible to develop and compile laboratory conditions that would allow for multi-kilometres drone detection tests to be carried out. On the other hand, conducting tests in an external environment carries with it the possibility of significant deviations from the measurement conditions and the associated measurement uncertainties. It should be clearly emphasized that it is very difficult to repeat the tests in the same conditions, in particular in different places, at different times and in different weather conditions related to this place. The aforementioned changes in the weather, but also changes in the environment caused by the vegetation of plants and human activity, as well as changes in the electromagnetic background and other factors related to the measurement method, mean that reliable comparative tests of various solutions, using the same procedure of potential tests, must take into account the changes of these factors.

Accordingly, there are two basic factors that will influence the outcome of the tests. Technological factors – related to the compilation of the test environment, and methodological factors – closely related to the method of test execution and the developed interpretation of the results.

Technological factors can be divided into those related to the tested technology, i.e., those that will have an impact on the test results only in the case of a specific technology, and general factors.

For the test results to be comparable, it is, first of all, necessary to provide test objects/drones with the same technical and operational parameters for all tests. For example, from the micro and mini groups, three types of drones should be selected and defined the following parameters for them. Drones with defined parameters should be used in all tests to make them comparable.

Significant technical parameters of drones, specifying the technology for which they will affect:

- size (daylight cameras, thermal cameras, infrared detectors, laser rangefinder),
- radar cross-section (RCS) or reflectance (radars with strictly selected ranges of microwave radiation, rangefinders/laser scanners – laser radiation of the near infrared range),
- surface emissivity (thermal imaging cameras, infrared detectors),
- acoustic signature (acoustic detectors),
- frequency and method of radio communication (frequency monitoring systems).

In addition, as a critical condition for each potential test scenario, it is necessary to clearly define the way the test object moves in the area of the expected detection field in terms of speed, slope and

flight path in relation to the detection system (depending on the detection method, flight parameters have a huge impact on the measurement results) and flight height.

In general, according to the theory of measurement methodology, the testing process should take into account the minimum necessary number of repetitions of a single test, enabling the statistical processing of measurement results – in the sense of one method of flying in a given scenario.

In practice, selected drones of a specific manufacturer and type should be used for all tests. Due to the future design changes of drones, in future tests, it is necessary to choose structures similar to the above-mentioned parameters to the previous models.

For comparable test results for different technologies, in accordance with the diagnosis of C-UAS technology and the analysis of the parameters of these systems, it is necessary to provide the following factors influencing the repeatability and reliability of tests for a given technology.

For detection systems using radars:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles,
- jamming stations or other jamming devices with the same technical parameters for all test sites.

For detection systems using daylight cameras:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles,
- dazzle devices and/or systems with the same characteristics and positioned in the same way for all tests,
- precipitation simulation devices of the same intensity and arranged in the same way for all tests,
- measuring devices (Rotakin) arranged in the same way for all tests.

For detection systems using thermal imaging cameras:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles,
- ensure a constant temperature of drones at the beginning of each test,
- dazzling devices for infrared cameras with the same parameters and arranged in the same way for all tests,
- precipitation simulation devices of the same intensity and arranged in the same way for all tests.

For detection systems using infrared detectors:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles,
- ensure a constant temperature of the drones at the beginning of each test.

For systems using laser rangefinders:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles.

For detection systems using frequency monitoring:

- jamming stations or other jamming devices with the same technical parameters for all test sites.

For detection systems using acoustic detectors:

- polygons (open terrain, forest, urban terrain) with the most similar terrain and the distribution of obstacles,

- jamming devices with the same technical characteristics and positioned in the same way for all tests.

Methodological factors are closely related to the subsequent interpretation of the results and have an influence on the comparison of the test devices. Due to the fluctuating conditions in field testing, there are many external factors that will influence the test results. During the tests, a sufficient number of tests of the same detectors under changing conditions should be carried out in order to be able to experimentally link the test result to changing environmental conditions.

In the case of all types of detectors, the weather conditions should be monitored on an ongoing basis:

- air temperature,
- air humidity,
- wind speed and direction,
- type and intensity of precipitation,
- cloudiness,
- visibility range.

For different types of C-UAS systems, it is also important to monitor other environmental parameters.

For radar-based detection systems, the following measurements should be taken during the tests:

- electromagnetic background, especially at the radar operating frequency.

For detection systems using daylight cameras, the following measurements should be taken during the tests:

- light intensity,
- the type of cloud cover.

For detection systems using thermal imaging cameras, the following measurements should be taken during the tests:

- sky temperature in the drone detection directions,
- insolation.

For detection systems using infrared detectors, the following measurements should be taken during the tests:

- sky temperature in the drone detection directions,
- insolation.

For systems using laser rangefinders, the following measurements should be taken during the tests:

- light intensity (in the direction of the raid),
- air humidity measurement (radiation scattering on water droplets in the air).

For detection systems using frequency monitoring, the following measurements should be taken during the tests:

- electromagnetic background, in particular at the operating frequency of C-UAS.

For detection systems using acoustic detectors, the following measurements should be taken during the tests:

- background acoustic wave intensity considering the spectral distribution.

Failure to measure and control the above-mentioned parameters and not taking them into account in the test results will lead to their distortions. It is important to ensure that all tests are conducted in similar atmospheric conditions, monitored as part of the developed test procedure, and recorded and reported together with the measurement results.

To sum up, the technological, functional, and methodological factors indicated in the study must be reproducible for each type of test in a given scenario. The test results themselves must have statistical characteristics and contain a strictly standardized description of test conditions, including flight conditions, weather conditions and environmental conditions associated with the action of additional physical fields.

Such an approach to tests will enable the following of the developed test procedures to follow the potential evaluation of C-UAS solutions, including the emergence of new detection technologies.

7 Development of standard scenarios

7.1 General

The purpose of this clause is to present a detailed description of a set of standard scenarios related to malicious UAS behaviour. In order to ensure consistency and comprehensiveness, this activity involved the identification of the needs for standardized scenarios based on clause 5 and clause 6.

Over the last decades, UAS have been present in a variety of shapes and sizes, ranging from handheld micro-UAS to medium-sized tactical systems to fully grown and Remotely Piloted Aircraft (RPA). At the same time, drones continue to make headlines for their ability to engage in all manner of recreational, but also practical uses, such as search and rescue, surveillance, traffic monitoring, weather monitoring, firefighting, drone-based photography, videography, agriculture, even delivery services, to name a few. Unfortunately, terrorists and criminals are proving as innovative as their industry counterparts in finding novel uses for UAS. The increasingly common use of drones by terrorists to launch strikes abroad has raised concerns that domestic malefactors may plan and execute similar attacks. Some criminal actors, meanwhile, are using drones to smuggle drugs across the border or into prisons, or otherwise to support their nefarious enterprises. These incidents, as well as others (which include unauthorized flights over sports stadiums or in controlled airspace near airports) have exposed both the vulnerability of sensitive facilities and critical infrastructures to hostile or recklessly operated UAS, as well serious shortcomings in the capabilities of law enforcement and national security agencies to address these threats. The necessity to protect people, infrastructure, and assets signifies the importance of counter UAS systems, including DTI systems. In order to be able to evaluate DTI systems, there is a need to develop a set of appropriate standardized scenarios to encapsulate as best as possible the elements involved in the countering of malevolent actions launched by UAS.

The operational needs, and subsequent operational capability gaps that these standardized scenarios are called upon to address, stem from limitations related to C-UAS. Specifically, these limitations refer to technical and non-technical obstacles faced by the detection & mitigation technologies used for C-UAS purposes.

1. Minimizing False Negatives and False Positives
To be useful, C-UAS detection systems need to generate low levels of false negatives and false positives. This is not an easy feat, since C-UAS detection elements must be sensitive enough to detect all drones operating within the area of use, but systems that are too sensitive may create an overwhelming number of false positives, rendering the system unusable.

2. Distinguishing Legitimate and Illegitimate UAS Use
In operating environments where legitimate drone use is common, it is increasingly important for C-UAS operators to be capable to differentiate between legitimate and rogue drones. Particularly given the potential hazards of mitigating a drone in civilian environments, C-UAS operators will need to develop means to rapidly and reliably determine the threat level of an incoming UAS based on the limited information provided by existing detection technologies.

3. Making it within the Response Window

Counter-drone operators may only have a very brief window of time during which to decide whether an incoming drone is indeed malicious. Thanks to advances in propulsion technologies, commercially available drones will become much faster in the years ahead, further reducing the viable response window for C-UAS.

4. Improving Interdiction Effectiveness

Like detection systems, no interdiction system is 100 percent effective and all interdiction systems have specific drawbacks. Following is a brief description of these systems, as well as their limitations:

•Physical capture (i.e. Nets, Projectiles, Collision Drones): entails physically disabling or blocking a flying object. This method is burdened by high costs, but most importantly by running the risk of being destructive. All kinetic systems may struggle against drones that are moving quickly or in unpredictable patterns. When they do indeed work as intended, they may destroy components of the drone that are necessary for forensic investigations.

•High-Power EMP: disrupts the logic of circuits within the flying UAS by directing pulses of high intensity microwave energy, disabling the aircraft's electronic systems and rendering it unable to fly. This approach again runs the risk of destruction and also of leaking electromagnetic energy.

•RF Jamming: disrupts the radio frequency link between the drone and its operator by generating large volumes of RF interference. Once the RF link, which can include WiFi links, is severed, a drone will usually either descend to the ground or initiate a "return to home" manoeuvre. However, this technique has no effect against drones that operate without an active RF link. Many signal jammers also have a limited effective range of a few hundred meters, meaning that the system must be very close to the intruding UAS to successfully mitigate it, and are not effective without a direct line-of-sight to the UAS. Jammers that are capable of operating at long ranges and beyond line-of-sight must be significantly more powerful, but more powerful jammers also pose a higher risk of interference to legitimate communications.

•Hacking: seizes the root privileges of the UAS's operating system and issues appropriate operations. The drawback of this method is that it only deals with specific operating systems and network protocols and, as with RF Jamming, it interferes with other ISM band devices.

•Spoofing: allows one to take control of or misdirect the targeted UAS by feeding it a spurious communications or navigation link. Spoofing systems, however, are technically very difficult to build and implement, and may not be universally effective against all UAS. Unmanned aircraft that have been built with protected communication links, for example, could be resistant to spoofing attacks.

5. Avoiding Interdiction Hazards

Most C-UAS interdiction techniques can be dangerous in certain circumstances. UAS that have their flight interrupted by kinetic means may fall to the ground with considerable force. Interdiction elements must be incredibly precise to hit a moving drone and could be dangerous to bystanders if they miss. Long-range effectors such as lasers and high-powered microwaves could pose a serious threat to aircraft operating above a targeted UAS. Jamming systems, meanwhile, can interfere with legitimate communications links in their vicinity (i.e. an airport). The use of GPS jamming or spoofing systems, in particular, is especially dangerous in areas where other entities rely on reliable GPS navigation (for example, manned aircraft at an airport).

6. Keeping up with advances in UAS Technology

Drone technology is an ever-evolving field, with innovations in this area presenting new challenges for C-UAS systems. As the UAS market expands and the range of easily available aircraft types becomes more diverse, C-UAS systems will need to be flexible enough to detect and neutralize drones that come in a wide variety of shapes and sizes. These could span from large, unmanned aircraft

capable of carrying heavy payloads at very high speeds to low-flying micro surveillance drones that might only weigh a few grams. Not all of these advances are motivated by a desire to make drones harder to counter. In fact, many of these innovations are driven by efforts to make drones safer.

7. Tackling the lack of Operational Data

There is a distinct lack of information regarding the operational track record of deployed systems. This information vacuum makes it difficult for would-be C-UAS owners to know what actually works and what doesn't, anticipate potential issues, and select a system that is best suited to their needs.

8. Facing C-UAS Costs

Counter-drone technology is expensive. Personnel training, maintenance, and staff time to operate the counter-drone system all incur significant additional costs.

9. Achieving Legality

In the U.S. and many other countries, C-UAS systems share a common drawback, in that they may not always be legal. In many instances, there is significant confusion and ambiguity as to the exact legal dimensions of C-UAS technology use. This is because the technology is often subject to numerous overlapping laws that were drafted to address other technologies, long before C-UAS technology existed. Adding to this ambiguity is the fact that most governments have not yet established comprehensive C-UAS-specific policies, while airspace regulators continue to develop regulations that may, in turn, have a bearing on C-UAS. Such legal restrictions and ambiguities are mirrored around the globe.

10. Dealing with the lack of Standards

No international standards exist for the proper design and use of C-UAS systems. This means there may be significant variances between the performance and reliability of systems that might, at the spec-sheet level, appear to be very similar. Some firms appear to be working to capitalize on the growing interest in this technology before properly maturing or field-testing their products. The absence of standards also raises questions about the safety of these systems. Particularly in civilian environments, a malfunctioning C-UAS system might present a public safety threat.

11. Protecting Privacy

Because counter-drone detection systems are a form of surveillance technology, they potentially pose a risk to privacy if misused or if the data that they collect is not handled properly. So far, there have been relatively few efforts to evaluate how to mitigate privacy risks that could arise from the use of these systems.

The aforementioned operational needs and operational capability gaps faced by LEAs in their C-UAS efforts, point to an underlying need to develop standardized scenarios, which will address and, hopefully, help overcome or mitigate the obstacles and shortcomings connected to countering malicious actions launched by UAS.

7.2 Methodology for extraction and development of standard scenarios

This subclause describes the methodology used for the development of standard scenarios.

Four specific steps were used for gathering and analyzing data related to the development of the standard scenarios; namely:

- Need for standardization Scenarios/Literature review
- Having defined the scope of the literature review, the deliverable focused on searching and collecting relevant literature. The literature analysis was the base of identifying the need for standardization scenarios.
- Previous incidents & identification of gaps (see Clause 5)
- Previous incidents and identification of gaps were used to identify the factors related to these incidents and their repetition.

- Current C-UAS framework (methods & technologies) (see Clause 6)
- The current framework of methods and technologies regarding C-UAS were used to identify the context of the scenarios that could be developed.
- End-User Questionnaire (see Annex B)

The methodology is described in Figure 39. In this diagram, the four techniques that were used for the development of the first draft of the 10 standard scenarios are represented. These four techniques are applicable to all possible environments and relevant to all security authorities and will account for the range of UAS threat types

The scenarios that are described in this subclause were evaluated, updated and refined by the consortium's End-Users and relevant Stakeholders in a dedicated workshop organized by KEMEA after the first execution.

Each step, among the four specific steps introduced earlier in this subclause, has its own use and purpose and complements the need elicitation process in its own characteristic way, while their combination ensures the effective collection process. The approach on defining the standard scenarios and their added value is presented in the below figure.
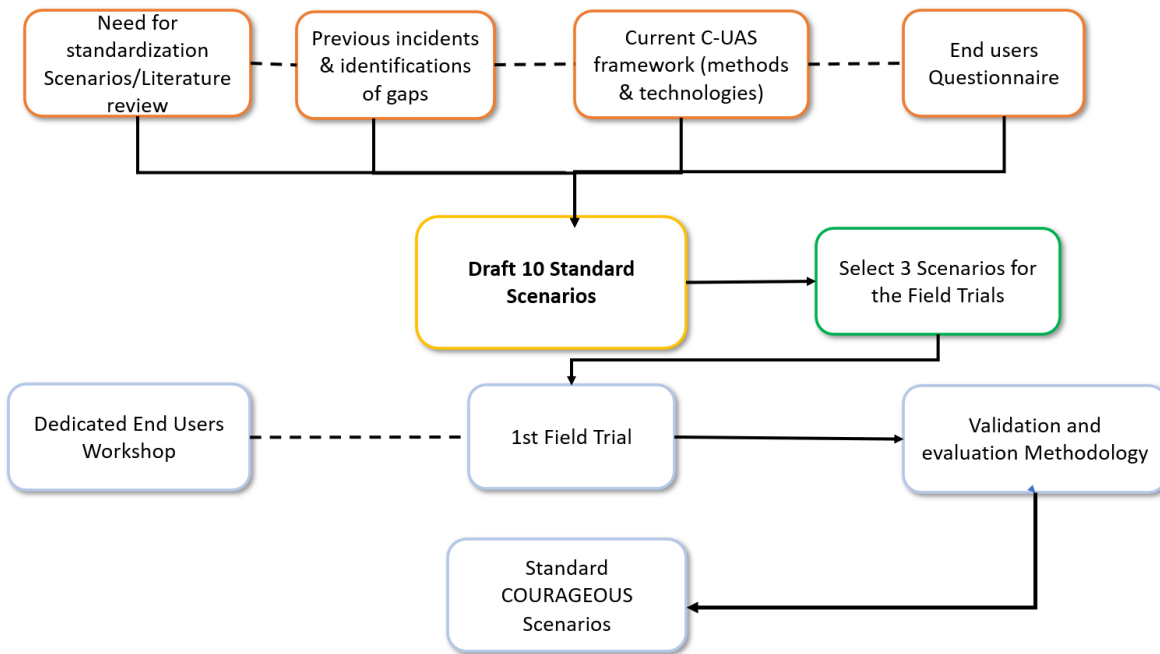
Figure 39— Scenarios definition approach

According to the four steps, the factors comprising an incident and a scenario are described below in Table 29. In this table, the major factors concerning incidents, as well as their subcategories are presented. For example, the subcategories of the Weather factor are: Sunny, Cloudy, Rainy, Foggy, Windy, Stormy, Smoke, Dusty, Snowy and Clear.

Table 29 — Scenario factors

Target	Weather	Type of UAS	Maximum take-off mass of UAS	Altitude	UAS Speed	Environment	Lighting Conditions	Presence of other aircrafts/UASs in the nearby airspace
Critical Infrastructure	Sunny	Multirotor	<250g	0-5m	0-10km/h	Rural	Sunrise	Not Classified
Government Building	Cloudy	Fixed Wing	<900g	5-20m	10-30km/h	Suburban	Sunset	Not Controlled
VIP	Rainy	Flapping-wing Ornithopters	<4kg	20-50m	30-60km/h	Urban	Daylight	Own Fleet
Public Event	Foggy	Gliders	<25kg	50-100m	<60 km/h		Darkness	Friend
Means of Transportation	Windy	Single Rotor	<100kg	100-120m	60-120 km/h			Authorized
Urban - Not Specified	Stormy	Hybrid	>100kg	>120m	120-160 km/h			Stolen
Border	Smoke				>160 km/h			Alleged Infringer
	Dusty							Threat
	Snowy							Escaped
	Clear							Neutralized

Number of UASs	Flight Mode	Radio Frequencies used for Remote Control and / or Video Stream	Flight Behaviour	Pilot Location	Payload	Custom or Commercial	Dimensions of UAS	Direction of Arrival
1	Manual	2.4GHz	Direct flight	Known	Optical camera	Recreational custom-made UAS	<30cm	
2	GPS	5.8GHz	Obscured	Unknown	LiDAR	Wrong-doing custom-made UAS	30-50cm	
Swarm	Waypoints	RC model aircraft frequencies (depending on national regulations)	Drop from High Altitude		Thermal sensor	Commercial	50-70cm	
	Inertial Navigation Systems	4G/LTE			Explosives/IEDs		>1m	
	4G/LTE	Other			Gun			
					CBRN			
					Objects for Commercial Distribution			
		None			Sprayers			
					Noise Generators			
					Jamming Devices			
					Different Domestic Payloads			
					Dazzling Laser			
					Illicit Package			

Terrain	EM Environment	Birds	Vegetation	UAS Signature
Flat	Rural	Low Bird presence	None	Strong
Irregular	Suburban	Normal Bird presence	Low	Normal
Mountainous	Urban	High Bird presence	Average	Low
	Dense/Crowded		Meadowland	None
			Wood / Forest	

In addition, in order to create a standard scenario, the Pilot's Intention (Deliberate or Accidental), has to be taken into account also. The subcategories of the pilot's intention are the following:

- Negligence

  ➢ Clueless Individuals

  Characterised as such when the pilot does not know of or understand the applicable regulations and restrictions. As a result, they fly their drones over sensitive or prohibited areas. Their stance can be described as "Clueless", since they have no intention of causing any disruption.

  ➢ Careless Individuals

  Characterised as such when the pilot knows of the applicable regulations and restrictions but breaches them through fault or negligence. As a result, they fly their drones over sensitive or prohibited areas, but these individuals have no intention of causing any disruption.

- Gross Negligence

  ➢ Reckless Individuals

  Characterised as such when the pilot knows of the applicable regulations and restrictions, but deliberately does not follow the rules in order to pursue personal or professional gain (e.g. aggressive spotters). Their behaviour can be characterised as "reckless", because they cause a disruption by totally disregarding the consequences of their actions.

  ➢ Activists / Protesters

  Pilots who, regardless of whether they know the applicable regulations and restrictions, actively seek to use drones to cause a disruption. To maximise impact, these individuals might even act as a group. While their actions might have disruptive consequences, they have no intention of endangering human lives.

- Criminal / Terrorist

  Pilots who, regardless of whether they know the applicable regulations and restrictions, actively seek to use drones to cause a disruption. Because their actions are deliberate and show no regard for human life and property, these individuals are to be regarded as being criminally motivated or even regarded as terrorists.

  The factors that could comprise a scenario are identified and described in Table 30. The following step for the development of the standard scenarios is to combine these Factors with Pilot Intent. In this context, a table was created in which Pilot Intent is found on Axis Y, whereas the Factors that could comprise a UAS attack can be found on Axis X, as well as their Sub-Categories. By selecting a specific value from Pilot Intent and then a specific value for each of the Factors, a unique scenario can be defined. Hence, based on to this table, one could have as many scenarios as are decided upon. To facilitate this, the table has drop-down menus in order to be adaptable for every user.

Table 30 — Scenarios development methodology

Categorisation of intention-motivation of pilots of unauthorised drones/ Important scenario factors	Target	Weather	Type of UAS	Maximum take-off mass of UAS	Altitude	UAS Speed	Environment	Lighting Conditions	Presence of other aircrafts/UASs in the nearby airspace
Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Gross Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Criminal/ terrorist motivation	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Clueless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Careless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Reckless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Activists/ Protesters	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

Categorisation of intention-motivation of pilots of unauthorised drones/	Number of UASs	Flight Mode	Radio Frequencies used for Remote Control and / or Video Stream	Flight Behaviour	Pilot Location	Payload	Custom or Commercial	Dimensions of UAS

Important scenario factors								
Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Gross Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Criminal/ terrorist motivation	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Clueless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Careless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Reckless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Activists/ Protesters	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

Categorisation of intention-motivation of pilots of unauthorised drones/ Important	**Terrain**	**EM Environment**	**Birds**	**Vegetation**	**UAS Signature**

scenario factors					
Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Gross Negligence	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Criminal/ terrorist motivation	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Clueless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Careless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Reckless Individuals	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.
Activists/ Protesters	Choose an item.	Choose an item.	Choose an item.	Choose an item.	Choose an item.

In order to determine the selection of the most relevant scenarios, were taking into account the following variables:

- Difficulty for the DTI Systems
- Severity of the Incidents.
- Availability of the test sites
- Ability for the test sites to accommodate to a given scenario.

Each scenario (see Annex A) received a value between 0 to 5 (Very Low, Low, Medium, High, Very High) in terms of Difficulty for DTI Systems and also received a value between 0 to 5 (Very Low, Low, Medium, High, Very High) in terms of the Severity of each Incident. The following table presents a matrix with the two values and the final score.

Table 31 — Scenario matrix

	Scenario	DTI Difficulty	Severity of the Incidents	Total Value
Sensitive Sites/Critical National Infrastructure	Prison	3	2	5
	Airport	3	3	6
	Nuclear plant	4	4	8
	Government building	3	2	5
Public spaces protection/Events	Stadium	3	3	6
	Outdoor concert	4	3	7
	Outdoor political rally	4	4	8
	International Summit	3	3	6
Border Protection	Land Border	4	4	8
	Maritime border	4	3	7

According to Table 31, the 5 most "important" scenarios that are interesting to evaluate are:

- Category: Sensitive Sites/Critical National Infrastructure, Scenario: Nuclear Plant
- Category: Public Spaces Protection/Events, Scenario: Outdoor concert
- Category: Public Spaces Protection/Events, Scenario: Outdoor Political Rally
- Category: Border Protection, Scenario: Land Border.
- Category: Border Protection, Scenario: Maritime Border.

8 Risk analysis and metrics definition

8.1 General

The purpose of this clause is to present and analyze the level of risk of the standard scenarios related to malicious UAS behaviour. In order to ensure consistency, coherence and comprehensiveness, this

activity involved the identification of the basic principles of threat and risk via literature analysis and based on analysis of the output from the Clause 5, Clause 6 and Clause 7.

8.2 The threat of UAS - Basic principles

8.2.1 General

The presentation of basic principles of the threat introduced by unmanned aerial systems (UAS) initiates readers to the notion of risk analysis and metrics aiming to fortify the security of the assets from an evolving UAS threat.

8.2.2 Threat Understanding

This study intends to analyze the current and future threats posed by UAS. To achieve this scope, it is of prior importance to conceptualize the terms "risk", "threat" and "vulnerability". According to EU COM (2006) 787[4]: "Risk" is the likelihood of loss, damage, or injury in regard to the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and the likelihood that a specific vulnerability will be exploited by a particular threat.

A threat is a function of capability and intent. Risk is a function of likelihood (taking into account threat and vulnerability) and impact (taking into account mitigation measures) of the threat occurring. Impact considers a range of physical, financial, psychological, reputational and operational factors as well as the level of vulnerability and any mitigation measures already in place.
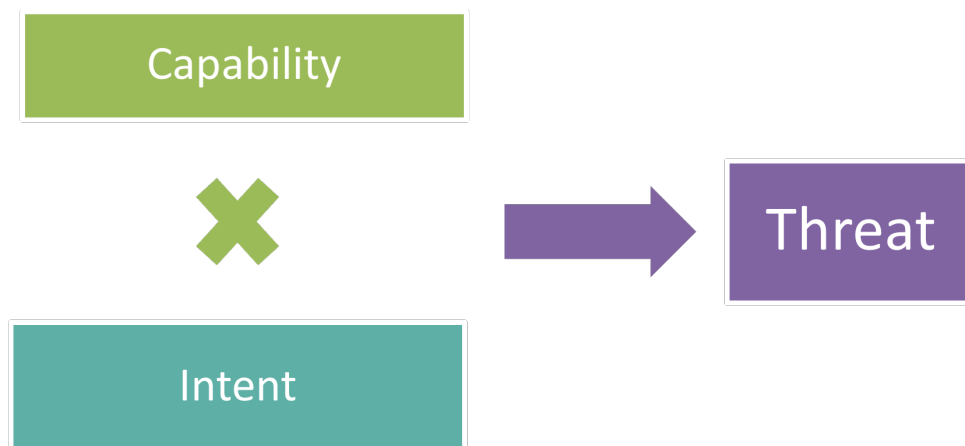
Figure 40 — Threat as a function of capability and intent

"Vulnerability" refers to a characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure.

The level of risk is calculated as follows:

Risk = Likelihood (Threat x Vulnerability) x Impact[5]

(3)

---

[4] Commission of the European Communities (2006), COM/2006/0787 final "Proposal for a directive of the council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection" https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006PC0787&from=BG

[5] Center for Security Studies (2018), Manual – Trainings for the protection of Critical Infrastructures http://www.ciprotection.gr/index.php/el/

A "risk" is a function of a threat, a vulnerability, the likelihood of the threat attacking the vulnerability, and the potential impact of the attack."[6]

UAS, although unmanned, relate to man-made threats occurring by accident or with malicious intent. The U.S. Department of Homeland Security defines as a credible threat UAS that:

- Cause physical harm to a person.
- Damage property, assets, facilities, or systems.
- Interfere with the mission of a covered facility or asset, including its movement, security, or Protection.
- Facilitate or constitute unlawful activity.
- Interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons.
- Result in unauthorized surveillance or reconnaissance or
- Result in unauthorized access to or disclosure of classified, sensitive, or otherwise lawfully protected
- Information.

A UAS can also be used in malicious ways:

- Hostile Surveillance.
- Smuggling or Contraband Delivery.
- Disruption of Government Business.
- Weaponization.

8.2.3   Threat Assessment

A UAS can cause damage, loss or other adverse effects. A UAS threat exploits the vulnerabilities of a system to attack it. These vulnerabilities can be reduced or controlled with appropriate precautionary measures. Risk analysis and metrics development, which are presented in this deliverable, aim to facilitate in the avoidance and/or confrontation of a UAS hazard. Standardized scenarios in addition are crucial in testing the resilience of an infrastructure or asset when it comes to a UAS attack.

A risk scale can be developed based on various specifications of the UAS. The rule that states "the more advanced the UAS, the more dangerous" applies in UAS risk assessment. Identifying specific characteristics such as attainable height, visibility capabilities, authorization, and operator's capacity are taken into consideration in the categorization of aerial systems, characterizing them as low, medium, or high risk.

Damage metrics are an extra element in the assessment of a UAS' risk. Damage-impact analysis is a preventive procedure that encodes information and indications of an aerial threat scenario. Schematically, the information that is elaborated for the assessment of impact-damage primarily includes the type of UAS, the perpetrator, the target and the environment in which the aerial system operates.

Specifications and damage metrics assessment warn security systems about an imminent UAS threat. In addition, the surveillance of unknown flying objects provides a better understanding of the threat's severity. When the incident is categorized as high risk, an alarm situation is raised in the threatened area.

---

[6] *Wallace, Ryan & Loffi, Jon. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. International Journal of Aviation, Aeronautics, and Aerospace. Volume 2. 10.15394/ijaaa.2015.1084.*

8.2.4 Threat Confrontation

The next principle in the spectrum of a UAS threat is its confrontation. Being in an alarm situation, countermeasures are launched towards the hostile flying system. For efficiency purposes, the measures must be integrated in relevance with the level, type, and damage-metrics of the risk. At this stage, a successful threat assessment is crucial, prior to the countermeasure process. Development of standardized confrontation scenarios further enhance safety and security plans.

Countermeasures can be passive or active:

Passive countermeasures do not interfere with the drone and can include the closing of blinds, moving of protected assets, or temporarily shutting down operations.		Active countermeasures are typically illegal for enterprises and individuals, since destroying or intercepting a drone is against the law in many countries. However, exceptions may exist when drone intrusion are a matter of national security.

8.2.5 Crisis management

Even though a facility was defended against a hostile UAS, damages and/or casualties may have occurred. The existence of an individual crisis response plan results in the mitigation of losses. Damage-metrics help security staff and first responders to initially assess and then to intervene in the ensuing emergency, using standard operating procedures and means. A UAS crisis response plan contains:
- Crisis Teams:
  - Emergency Team
  - Crisis management Team
  - Communication Team
- Crisis Procedures:
  - Preparation and Prevention Procedures
  - Management Procedures
  - Recording of crisis results and evaluation

8.2.6 Continuity

Having successfully dealt with the crisis of a drone attack, the facility starts implementing its standard continuity plan. This aspect is very important in the analysis of cases in which UAS targets a critical infrastructure in the industry of transport or energy. In the case of the real scenario of a drone disrupting the route of a passenger airplane and forcing the suspension of air-traffic for security reasons, to minimize its commercial losses, the threatened airport implements a standard plan of processes and procedures to assure the continuation of its operability. To continue providing services to its customers, the infrastructure continuity plan shall preserve a minimum level of operation in terms of its:
- Personnel
- Archives and information systems
- Buildings and equipment
- Transportation
- Logistics and financials
- Supply Chain

To summarize, basic principles are indispensable in better understanding, identifying, assessing and countering an unmanned but, at the same, manmade threat. In that framework, the threat posed by

a highly sophisticated aerial technology can be delineated in a scale of basic principles that must be followed in order to proceed with holistic risk management.

Figure 41 — UAS Threat Scale

8.3 Analysis of the scope of a confrontation of an UAS attack

The increasingly common use of UAS provide terrorists and criminals with innovative new ways of operating (as it does for their industry counterparts of course; namely LEAS) and in finding novel uses for UAS with little to no necessary modifications.

The categories of illicit UAS use by criminals are the following [7]:

- **Nuisance**. The most common and harmless illicit use of UAS is various forms of interference that they could cause in a public area. Such actions of interference are those which affect a property owner's rights to use and enjoy their property without substantial or unreasonable interference and are reflected in criminal, civil or tort law [8]. Furthermore, UAS can elicit fear or adversely affect an individual's perceptions of security or safety.
- **Monitoring Threat.** The most important concern regarding UAS are their ability to silently monitor and record their surroundings. Anyone with a pilot certificate and access to a UAS has the capability of conducting aerial surveillance.
- **Surveillance.** With the widespread availability of highly automated UAS, anyone can purchase an aerial monitoring platform which has high resolution camera capabilities. Privacy intrusion occurrences by UAS are becoming more frequent. While most operators make use of their UAS devices for fun and as they are, out of the box, others may have inappropriate observation intentions, such as invading privacy.
- **Reconnaissance.** Is an activity derived from military terminology that involves collecting intelligence on a known "enemy" target. UAS can rapidly produce geo-references (GPS accurate) or 3D maps that are often more detailed and faster than satellite imagery. UAS automation allows operators to conduct illicit monitoring activities at a sizable standoff distance, effectively preserving their anonymity from potential criminal investigation. Such illicit monitoring actions allow criminals or terrorists to assess for "soft" targets, vulnerabilities in critical infrastructures, government sites, businesses, and private citizens alike.
- **Airspace Interference.** UAS platforms present a genuine threat to the safe utilization of airspace. The FAA has logged dozens of reports of near misses between airliners and UAS platforms being improperly operated near airports across the country. An airborne UAS creates a collision threat to aircrafts and could adversely impact normal and emergency aviation operations. It is conceivable that terrorists or criminals could employ UAS craft to disrupt drug interdiction, law enforcement, or medical aircraft with the intended purpose of curtailing tracking, emergency response, or disaster mitigation capabilities.

---

[7] Wallace, Ryan & Loffi, Jon. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. International Journal of Aviation, Aeronautics, and Aerospace. Volume 2. 10.15394/ijaaa.2015.1084.

[8] Soloman, E.D. (2014). Part two: Unmanned aircraft systems ("UAS") – aka drones legal issues: Where are we headed. Blank & Rome. Retrieved from http://www.blankrome.com/index.cfm?contentID=37&itemID=3338

- **Kinetic/Kamikaze.** Even without armaments, a drone is capable of causing damage or injury to people or property on the ground or in the air. While many UAS accidents are likely inadvertent rather than intentional, the risk is the same. While the incidents appear unintentional, they demonstrate the destructive potential of UAS systems. Should criminal or terrorist elements wish to carry out an attack, an out-of-the-box UAS platform has the potential to deliver a lethal kinetic blow to soft targets, while having the potential added benefit of appearing as accidental or negligent.

- **Payload Threat/Smuggling.** UAS platforms can also be exploited as a transportation mechanism for illegal contraband or cargo. Use of these platforms allow terrorists or criminals to bypass traditional security barriers such as fences, walls, and detection measures. Essentially, drones add a skyward dimension to security considerations.

- **Weaponized Threat.** Perhaps the most fearsome threat produced by terrorist or criminal entities involve the deliberate construction or modification of UAS systems to carry and employ weapons. This application of UAS platforms has received the bulwark of speculation and even fear mongering among industry experts but is well-justified considering the relative ease in which a UAS platform can be weaponized to produce devastating results.

- *Non-Lethal Systems.* While the use of non-lethal systems is not generally associated with criminal activity, the production of such systems is already underway for law enforcement and security purposes. Mounting a drone with systems capable of firing rubber bullets, tear gas, or taser nodes has several promising applications for law enforcement organizations (Kersey, 2012). It is not unreasonable to speculate that terrorist or criminal elements could foreseeably gain access to such systems through either proliferation or theft.

- *Projectile Threats.* While the prospect of UAS platforms carrying firearms or other lethal projectile weapons might seem particularly troubling, the likelihood of such a modification is reasonably low compared to other weaponization efforts. The development of an effective projectile weapon system such as a gun or missile requires highly specialized engineering and fabrication expertise. Without engineering expertise, access to these types of UAS systems is generally limited to a select group of special operations or military organizations. Moreover, such technology generally remains tightly guarded against physical theft or proliferation, making the acquisition of such systems by terrorists or criminal elements extremely improbable. Despite the complications, some individuals have self-produced UAS projectile systems that show alarming ingenuity.

- *IED/Explosive.* The use of drones as a delivery system for improvised explosive devices (IEDs), incendiary devices, or other combustibles remains high. Terrorists in particular have shown great ingenuity in crafting rudimentary explosives.

- *Weapons of Mass Destruction (WMD).* Weapons of mass destruction represent particularly lethal threats stemming from the use of hazardous materials including Chemical, Biological, Radiological, and Nuclear (CBRN) substances. Use of UAS platforms as a delivery system for CBRN substances is particularly troublesome, as such delivery systems could easily bypass traditional security measures. Moreover, such systems can effectively cause mass casualties without the need for precision flying. A drone could merely fly over the target area where a CBRN substance could be deployed in aerosol form, or a dispensing mechanism could be dropped from the aircraft.

- *Electronic Attack.* A particularly novel threat presented by drones is the potential to use them as platforms to commit an electronic attack or electronic theft. The device bears a striking similarity to the Stingray phone tracking system, with substantially enhanced capabilities. It is conceivable that such technology would be highly sought-after by intelligence agencies and law enforcement entities and could be easily adapted by unscrupulous elements to be used for identity theft, blackmail, corporate espionage, or any number of other illicit activities.

8.4 Specific Operations Risk Assessment (SORA)

The risk assessment methodology, known as SORA (Specific Operations Risk Assessment), is developed by EASA, because when conducting an operation not covered by an STS or a PDRA, applicants are required to conduct a risk assessment, identify mitigations and comply with safety objectives. EASA published the SORA as an Acceptable means of compliance to Article 11 of Regulation (EU) 2019/947.

SORA is a methodology for the classification of the risk posed by a drone flight in the specific category of operations and for the identification of mitigations and of the safety objectives. It helps the operator to identify operational limitations, training objectives for the personnel essential for the operation (e.g remote pilots, observers, maintainers etc.), technical requirements for the drone and to develop the appropriate operational procedures that will be part of the operator manual.

SORA is a 10-step process starting with the description of the operation and the evaluation of ground risk and air risk.

The ground risk is related to the risk posed to persons, properties, or critical infrastructures, being struck by a drone. It is affected by:

- population density
- the type of operation
- Visual Line of Sight – VLOS; or
- Beyond Visual Line of Sight – BVLOS
- the drone's size
- the mitigations applied.

The air risks determination considers the probability of encountering manned aircraft in the airspace. This is derived from:

- the density of manned air traffic in the airspace
- the mitigations applied

By combining the air and ground risk value, the intrinsic risk values of the full operation - called SAIL (Specific assurance integrity level) – are then defined.

A high value SAIL represents an operation with high potential risk. Once the SAIL is determined, the applicant needs to go through the 24 operational safety objectives (OSOs) and to show compliance with a level of robustness that increases as SAIL of the operation increases (e.g., operations with higher SAIL, meaning with higher intrinsic risk, will be required to show compliance with higher levels of robustness, meaning more demanding standards and showing compliance to the NAA).

The last point is to assess the level of risk of the area adjacent to the area of operation and comply with the requirements to protect such area and contain the drone in the operational area in case of a fly away.[9]

---

[9]   https://www.easa.europa.eu/en/domains/civil-drones-rpas/specific-category-civil-drones/specific-operations-risk-assessment-sora#Risk%20assessment%20of%20the%20intended%20operation%20%E2%80%93%20SORA
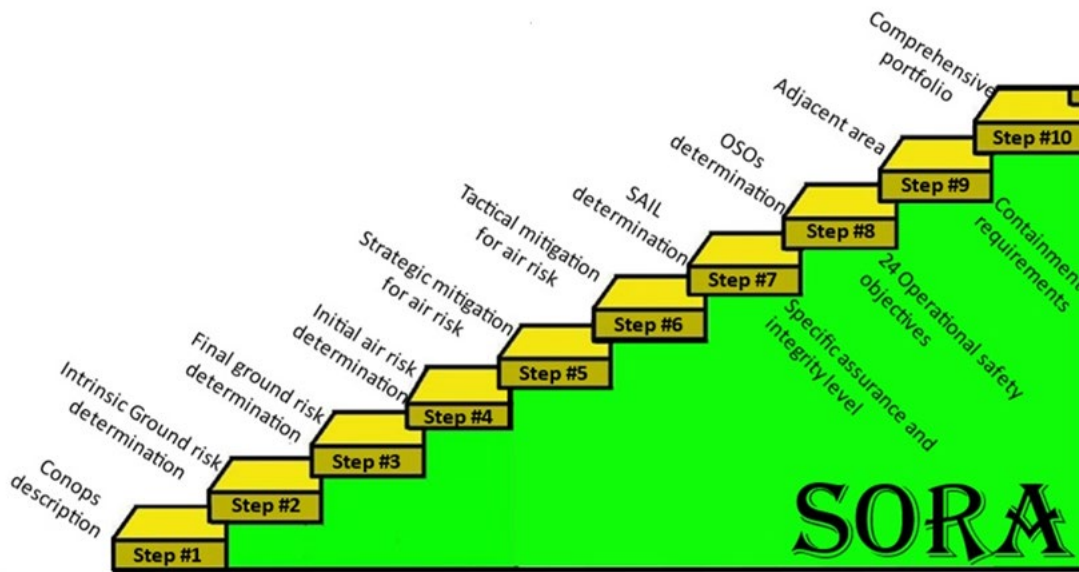
Figure 42— SORA methodology - 10 steps

8.5 Risk analysis and Metrics development

In this subclause, the risk of each factor will be analyzed. The level of risk is calculated according to the formula (3) from subclause 8.2.

For each factor, the average of Likelihood has been multiplied by the average of Impact. The resulting risk of each factor is presented in Table 32. From the results below, factor "Target" has the highest risk value compared to "Presence of the Birds" and "Vegetation" which have the lowest risk values. In general, when a factor has a high frequency (Likelihood) combined with a low Impact and vice versa, the risk is mitigated. Therefore, from the Environment factor, subcategory "Urban" has the highest risk value, whereas from factor "Altitude", subcategory "0-5m" has the lowest risk value.

Table 32 — Risk calculation of each Factor

		Likelihood	Impact	RISK
Intention				
	Negligence			
	Gross Negligence			
	Criminal / Terrorist Motivation			
Target	Critical Infrastructure			
	Government Building			
	VIP			
	Public Event			
	Urban - Not Specified			
	Border			

		Likelihood	Impact	RISK
Weather	Sunny			
	Cloudy			
	Rainy			
	Foggy			
	Windy			
	Stormy			
	Smoke			
	Dusty			
	Snowy			
	Clear			
Type of UAV	Multirotor			
	Fixed Wing			
	Flapping-wing Ornithopters			
	Gliders			
	Single Rotor			
	Hybrid			
Maximum take-off mass of UAV	<250g			
	<900g			
	<4kg			
	<25kg			
	100kg			
Altitude	0-5m			
	5-20m			
	20-50m			
	50-100m			
	100-120m			
	>120m			
UAV Speed	0-10km/h			
	10-30km/h			
	30-60km/h			
	<60 km/h			

		Likelihood	Impact	RISK
	60-120 km/h			
	120-160 km/h			
	>160 km/h			
Environment	Rural			
	Suburban			
	Urban			
Lighting Conditions	Sunrise			
	Sunset			
	Daylight			
	Darkness			
Presence of other aircrafts / UAVs in the nearby airspace	Not Classified			
	Not Controlled			
	Own Fleet			
	Friend			
	Authorized			
	Stolen			
	Alleged Infringer			
	Threat			
	Escaped			
	Neutralized			
Number of UAVs	1			
	2			
	Swarm			
Flight Mode	Manual			
	GPS			
	Waypoints			
	Inertial Navigation Systems			
	4G/LTE			
Radio Frequencies used for Remote	2.4GHz			
	5.8GHz			

		Likelihood	Impact	RISK
Control and / or Video Stream	RC model aircraft frequencies (depending on national regulations)			
	4G/LTE			
	None			
Flight Behaviour	Direct Flight			
	Obscured Flight			
	Drop from High Altitude			
Pilot Location	Known			
	Unknown			
Payload	Optical Camera			
	LiDAR			
	Thermal Sensor			
	Explosives/IEDs			
	Guns			
	CBRN			
	Objects for Commercial Distribution			
	Sprayers			
	Noise Generators			
	Jamming Devices			
	Different Domestic Payloads			
	Dazzling Lasers			
	Illicit Packages			
Custom or Commercial	Recreational custom-made UAS			
	Wrong-doing custom-made UAS			
	Commercial			
Dimensions of UAV (wingspan, rotor diameter/area or maximum distance between rotors	<30cm			
	30-50cm			
	50-70cm			
	>1m			

		Likelihood	Impact	RISK
in case of multirotor)				
Terrain	Flat			
	Irregular			
	Mountainous			
EM Environment	Rural			
	Suburban			
	Urban			
	Dense/Crowded			
Birds	Low Bird presence			
	Normal Bird presence			
	High Bird presence			
Vegetation	None			
	Low			
	Average			
	Meadowlands			
	Wood/Forest			
UAV Signature	Strong			
	Normal			
	Low			
	None			

8.6 Key Risk Indicators (KRIs)

In this subclause, the key risk indicators (KRIs) are presented.

A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability and associated consequences of an event will exceed a scenario's risk appetite and have a profoundly negative impact on a scenario's ability to be successful.

Key risk indicators play an important role in risk management programs. KRIs provide the following benefits:

- Advanced notice of potential risks that could cause damage
- Insight into possible weaknesses of a scenario's monitoring and control tools; and
- Ongoing risk monitoring between risk assessments.

The Average Risk of the Factors that comprise a standard scenario constitute the relevant key risk indicators (see Annex C for application to standard scenarios). The indicators are the following:

Table 33 — Average Risk of Factors

Factor	Average Risk
Flight Behaviour	
Target	
Custom or Commercial	
Pilot Location	
Environment	
EM Environment	
Number of UAVs	
Flight Mode	
Maximum take-off mass of UAV	
Intention	
Radio Frequencies used for Remote Control and / or Video Stream	
Dimensions of UAV (wingspan, rotor diameter/area or maximum distance between rotors in case of multirotor)	
Terrain	
UAV Signature	
Altitude	
Lighting Conditions	
Payload	
UAV Speed	
Type of UAV	
Presence of other aircrafts / UAVs in the nearby airspace	
Birds	
Weather	
Vegetation	

9 Operational needs for C-UAS coverage

9.1 General

The purpose of this clause is to define the operational needs for C-UAS measures based on the standard scenarios established on clause 7. By analysing the expected results and measures needed to be imposed in order to mitigate the threats that non-cooperative UASs represents in the hands of malicious actors, general operational requirements emerged.

This clause defines a general set of operational needs based on the standard scenarios defined on clause 7. These operational needs describe what authorities need to mitigate the threats that non-cooperative UAS pose, especially in the hands of malicious actors including terrorists in order to adequately protect different sites/facilities, events and individuals. Examples of operational needs are how much early warning an authority requires in order to effectively protect a given site, how many UAS an operator needs to be able to track at any given time or operational needs related to the use of the system itself in the context of specific scenarios (e.g., how quickly do operators need to be able to deploy a C-UAS system, how many operators, should ideally be needed to work the system).

Operational requirements are those statements that "identify the essential capabilities, associated requirements, performance measures, and the process or series of actions to be taken in effecting the results that are desired to address mission area deficiencies, evolving applications or threats, emerging technologies, or system cost improvements. The operational requirements assessment starts with the Concept of Operations (CONOPS) and goes to a greater level of detail in identifying mission performance assumptions and constraints and current deficiencies of or enhancements needed for operations and mission success. Operational requirements are the basis for system requirements"[10]

There are currently no standard operational requirements for counter-UAS developed throughout technical standards and based on consensus of different parties (users, companies, and regulators). This major problem, determines a lack of mature DTI (Detect Track and Identify) tools for specific use-cases and consequently a lack of information to support rapid operational counter measures to threats. Moreover, no existing C-UAS system is perfect from a user point of view, since the user requirements and scenarios are so different. The issue is compounded by a lack of standards for design and use of C-UAS system, as well as reliable test and operational data. The problem must be seen from two perspectives:

- from the user point of view, the lack of reliable test data makes it difficult to know what actually works or not, to anticipate potential issues and select a system that is best suited to their needs. The end user must be able to formulate operational needs without knowing the system performance. It is about the difference the end users want to make in order to improve the operational challenges one is facing. So, the used approach: operational needs definition > system procurement > system validation, out in a very short/conservative way and update/prioritize the needs.
- from a producer point of view, the lack of reliable and complete operational needs, coming from the end users, and presented in a standardized manner, makes impossible the development of solutions which will fulfil later the user's expectations, for different scenarios.

A requirement is an attribute of a product, service or system necessary to produce an outcome(s) that satisfies the needs of a person, group or organization. Requirements therefore define "the problem." In contrast, "the solution" is defined by technical specifications.

---

[10]   https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/concept-development/operational-requirements

Defining requirements is the process of determining what to make before making it. Requirements definition creates a method in which appropriate decisions about product or system functionality and performance can be made before investing the time and money to develop it. Understanding requirements early removes a great deal of guesswork in the planning stages and helps to ensure that the end-users and product developers are "on the same page."

A system will be always checked/tested against functional requirements and this is addressed in Clause 10– *C-UAS system performance requirements and metrics*. Performance requirements will provide criteria against which solutions can be tested and evaluated, offering detailed metrics that can be used to objectively measure a possible solution's effectiveness, ensuring informed purchasing decisions on products, systems or services that achieve the stated operational goals.

For a better understanding of the basis for the operational needs, it is important to link these requirements with the existing technologies used in C-UAS systems. In this respect, the working hypothesis is that there is a system of systems. A C-UAS is typically composed of several complementary components interconnected in a processing chain:
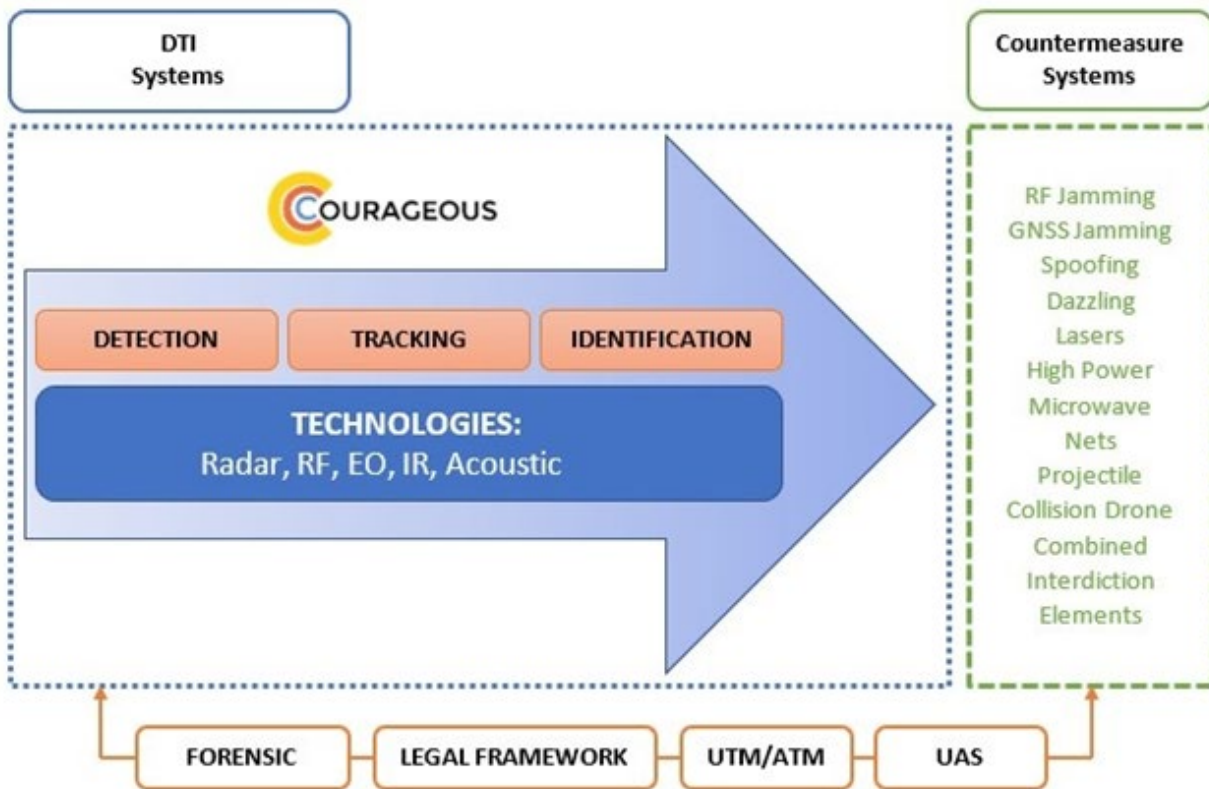
Figure 43 — The Counter-Drone kill-chain

Generally, the architecture of a complete C-UAS system, as expected by the users, is composed from two major parts:

- **DTI system – Detection, Tracking and Identification**
- **Countermeasure Systems**

Though DTI is a part of a larger solution, the scope of this document is to address only the DTI, therefore operational needs will be focused mainly on these technologies. In this respect, the needs for DTI will be grouped and presented in this clause.

However, since the C-UAS could be described as an ecosystem because it is intersecting with the countering technologies, air traffic management systems, the existing security systems, regulators

and the civil society, mentions or general requirements will be defined also in this clause, for the countering part.

The forensic part represented in the above figure, is a system functionality expected by the users and regulators, in order to collect, preserve, and analyse scientific evidence during the course of an investigation of a UAS incident. This is a general requirement (which is out the scope of the CWA), must be addressed in the near future, having in mind also the legal implication of the criminal use of UAS. Taking into the consideration the technology used for C-UAS, the forensic term must be addressed at least from the following points of view:

- Forensic video analysis is the scientific examination, comparison and evaluation of video in legal matters.
- Mobile device forensics is the scientific examination and evaluation of evidence found in mobile phones, e.g. Call History and Deleted SMS, and includes SIM Card Forensics.
- Forensic engineering is the scientific examination and analysis of structures and products relating to their failure or cause of damage.
- Digital forensics is the application of proven scientific methods and techniques in order to recover data from electronic / digital media. Digital Forensic specialists work in the field as well as in the lab.

Based on the above definitions, the C-UAS as technical systems, must be provided with adequate means for supporting the forensic activities, these needs being presented later in this deliverable.

All the major blocks mentioned above, are integrated in most of the cases in a **Command and Control System, with or without a Decision Support Functionality**, aiming the following: threat analysis, alerts, Incident Response and Neutralization Determination, documenting, trending and reporting of the data collected, provides important intelligence that will leverage in the decision support process to determine the initial response recommendation and neutralization method.

Also, the data collection process could **interface with ATM, UTM/U-space**, and other available services for exchanging of information and in this respect operational needs will be described for these issues.

The demarcation line between operational needs (as the subject of this deliverable) and the functional and performance requirements and metrics (as the subject of D3.2) is not very well defined, sometimes these being overlapped. Such, the operational needs will be considered users requirements and will be focused just on the needs in scenarios context, with generic requirements of the C-UAS system, without going into too much detail on the technical details of the sensors that make up the system.

All the needs, must be done well if the final product or system is to be judged by the end users as successful. From the International Council of Systems Engineers (INCOSE)[11], there are eight attributes of good requirements:

- **Necessary:** Can the system meet prioritized, real needs without it? If yes, the requirement isn't necessary.
- **Verifiable:** Can one ensure that the requirement is met in the system? If not, the requirement should be removed or revised.
- **Unambiguous:** Can the requirement be interpreted in more than one way? If yes, the requirement should be clarified or removed. Ambiguous or poorly worded requirements can lead to serious misunderstandings and needless rework.

---

[11] Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996.

- **Complete:** Are all conditions under which the requirement applies stated? In addition, does the specification include all known requirements?
- **Consistent:** Can the requirement be met without conflicting with any other requirement? If not, the requirement should be revised or removed.
- **Traceable:** Is the origin (source) of the requirement known, and is there a clear path from the requirement back to its origin?
- **Concise:** Is the requirement stated simply and clearly?
- **Standard constructs:** Requirements are stated as imperative needs using "shall." Statements indicating "goals" or using the words "will" or "should" are not imperatives.

For a better understanding of the operational needs structure, the Figure 3, depicts at a high level, the information flow over the whole chain processes, in a C-UAS as system of systems. The operational needs will address all the building blocks of a C-UAS as a whole.

C-UAS CAPABILITIES / C-UAS as SYSTEM of SYSTEMS

DETECTION SYSTEM

C-UAS System alerts Information on potential unauthorized UAS

DETECTION
LOCATION
TRACKING

Report of unauthorized/authorized UAS by:
- C-UAS system
- Surveillance systems
- Direct Remote Identification
- Observers

I_01 Direct Remote Identification

I_02 Surveillance systems

Provide data to CCS, CCRs and stakeholders

C-UAS System classifies and identifies threats

CLASSIFICATION
IDENTIFICATION

Incident Management Unit

I_08

Drone threat confirmed

I_04

Process Cycle determines the appropriate level of response

Forces in charge with mission area

LEAs, Regional and National Authorities

Process Cycle determines the appropriate level of response

Threat monitoring

I_03

COUNTERMEASURE SYSTEM

C-UAS System proposes most appropriate countermeasure

COUNTERMEASURES

Risk assessment

I_04

I_05

Threat neutralization

Target mitigated

Target not mitigated

No further actions

Back to normal operations

I_06

POST-INCIDENT SYSTEM

C-UAS System collects and analyses information

DATA COLLECTION
POST-INCIDENT
ACTION

I_07

Accident/Incident Reporting and sharing lessons

I_05

I_08

Key

→ Intra-system interface

→ Inter-system interface

I_0x Inter-system interface number

Figure 44 — Information flow in a C-UAS system

Starting from the above system which must address the operational needs for different standard scenarios, it was proposed the use for definition of the requirements, the ones stipulated in IEEE 29148 process terminology, one of the most used prioritization mechanisms used for user requirements. This is a widespread method, due to its acceptance from most partners across Europe and to the fact that results from previous activities/projects demonstrated its efficiency. Its central

role is to define a common baseline on how to evaluate each defined requirement. This prioritization method is reliable and offers better results when compared to simpler prioritizations approaches like high/medium/low prioritization or sequential prioritization. For this reason, it was concluded that this is the approach that will be followed for the current document. End users will categorize requirements according to their needs and technical partners will have a better understanding of what is expected, what is critical for having a successful implementation and what can bring additional value to the project in terms of functionalities/features.

- **Shall** – High priority requirements that shall be met to ensure the project meets its key objectives.
- **Should** – Medium priority requirements that should be met unless acceptable rationale for their omission is provided.
- **May** – Low priority requirements that may be considered during the project.

For the ease of understanding of all operational needs, the following form should be used:

Table 34 — Structure of the requirements and fields explanation

Field	Meaning of the field	Format
Req. Nº	*Unique code identifying each requirement for future references.*	*GR followed by two numbers - Ex. GR05, for a general requirement* *SR followed by two numbers - Ex. SR05, for a specific requirement*
Req. Name	*Concise description of the requirement.*	*Free text.*
Description	*More detailed description of the requirement, with special emphasis on the motivation behind the requirement.*	*Free text*
Importance	*Assessment by project stakeholders of the importance of each requirement for the project.*	*Value from a list:* - *Shall* - *Should* - *May*

9.2 Operational needs for Detection, Tracking and Identification

9.2.1 General operational needs for DTI

These DTI components provide real time situational awareness information to the C-UAS system by monitoring key areas according to the stakeholder needs. The main goal of these components is to support early and agile detection, location, tracking, classification and identification of UASs based on deployment of one or more sensors of the same or different type operating in a complementary manner. As the operational needs do not follow a specific technology or a mix of possible technologies, from an operational point of view, first there are some general applicable requirements. However, considering the previous defined scenarios in clause 7, it is clear that along with the general requirements, there could be some specific operational requirements for each scenario, considering the operating environment, specific UAS threats, impact and severity of an attack, etc.

The following needs are addressed:

Req. Nº	*GR01*
Req. Name	*General expected outcome*
Description	The system shall contribute to increase the protection capacity of some physical objectives by identifying and monitoring the threats represented by the use of unmanned aircraft used in illicit actions
Importance	**SHALL**

Req. Nº	*GR02*
Req. Name	*General expected outcome*
Description	The system shall contribute to strength the security capabilities by adopting new detection and neutralization technologies, through which new threats with unmanned aircraft used in illicit actions can be adequately responded to.
Importance	**SHALL**

Req. Nº	*GR03*
Req. Name	*General expected outcome*
Description	The system shall contribute in reducing vulnerabilities to new types of drone attacks.
Importance	**SHALL**

Req. Nº	*GR04*
Req. Name	*General expected outcome*
Description	The system shall contribute in countering terrorist or criminal acts in which unmanned aircraft may be involved.
Importance	**SHALL**

Req. Nº	*GR05*
Req. Name	*General expected outcome*
Description	The system shall contribute in increasing the level of cooperation between institutions with responsibilities in combating threats in which unmanned aircraft are used.
Importance	**SHALL**

Req. Nº	*GR06*
Req. Name	*General expectation – decision support facilitator*
Description	The C-UAS shall support decisions by providing information and tools for threat analysis, alerting, incident response and initial engagement
Importance	**SHALL**

Req. Nº	*GR07*
Req. Name	*Decision support*
Description	The C-UAS system may incorporate elements of autonomy and decision support to enhance its response capabilities. Intelligent algorithms, machine learning, or artificial intelligence can assist in automated threat assessment and response decision-making processes.
Importance	**MAY**

Req. Nº	*GR08*
Req. Name	*General expectation – Detect, Track, Identify*
Description	The system shall ensure through technological capabilities based on various technologies, the detection, tracking and identification of unmanned aerial vehicles that enter a well-defined hemispherical space.
Importance	**SHALL**

Req. Nº	*GR09*
Req. Name	*General expectation – Detect, Track, Identify*
Description	The system should have a sufficient detection and mitigation range to protect the desired operating area.
Importance	**SHALL**

Req. Nº	*GR10*
Req. Name	*General expectation – Detect, Track, Identify*
Description	The C-UAS system may be able to classify the type of UAS based on its size, shape, speed and other characteristics, in order to determine the appropriate response.
Importance	**MAY**

Req. Nº	*GR11*
Req. Name	*General expectation – Detect, Track, Identify*
Description	The C-UAS system may be able to predict the UAV's path and target location in order to provide a comprehensive picture of the UAV's behaviour and intentions.
Importance	**MAY**

Req. Nº	*GR12*
Req. Name	*General expectation – Prioritization*
Description	The C-UAS system may possess the capability to assess and prioritize UAS threats, by implementing an algorithm or decision-making framework based on predefined criteria, such as level of risk, proximity to sensitive areas, potential impact on safety and security, the nature of mission or operation, or potential harm to personnel or assets. This also involves adapting the prioritization based on evolving circumstances, mission objectives, or changes in the operational environment.
Importance	**MAY**

Req. Nº	*GR013*
Req. Name	*General expectation – authorization for use (legality)*
Description	The C-UAS system shall be authorized (not to be prohibited) by legal EU authorities to detect and mitigate drones in EU airspace considering the applicability of the system (e.g. government and military facilities, critical infrastructure, large events).
Importance	**SHALL**

Req. Nº	*GR14*
Req. Name	*General expectation – threat assessment*
Description	The C-UAS system may asses the threat level posed by the UAV, considering its size, speed and potential payload.
Importance	**MAY**

Req. Nº	*GR15*
Req. Name	*Technical expectation – protected airspace shape*
Description	The system should ensure through technological capabilities based on various technologies, DTI of unmanned aerial vehicles that enter a well-defined hemispherical airspace (azimuth 360^0 and elevation 180^0)*
Importance	**SHOULD**

Req. Nº	*GR16*
Req. Name	*Technical expectation – operation time*
Description	The system shall be reliable, with minimal downtime and high availability, in order to ensure 24/7 operation of all detection and/or countermeasures equipment.
Importance	**SHALL**

Req. Nº	GR17
Req. Name	*Technical expectation – UAS class*
Description	The system shall detect, track, and identify, UASs which are included in Class I (<150Kg) according to NATO classification, or from the micro, mini, small, as in EU classification
Importance	**SHALL**

Req. Nº	GR18
Req. Name	*Technical expectation – UAS shape*
Description	The system shall detect, track and identify, UASs (as defined in Req.Nº 10), regardless of their shape and colour.
Importance	**SHALL**

Req. Nº	GR19
Req. Name	*Technical expectation – UAS type*
Description	The system shall detect UASs (as defined in Req.Nº 10), regardless of their type: rotary wing, fix wing, hybrid/VTOL.
Importance	**SHALL**

Req. Nº	GR20
Req. Name	*Technical expectation – target flight mode*
Description	The C-UAS system shall detect, track, identify and counter UAS, regardless the flight navigation mode: manual navigation, GPS navigation
Importance	**SHALL**

Req. Nº	GR21
Req. Name	*Technical expectation – target flight mode*
Description	The C-UAS system should detect, track, identify and counter UAS which is flying autonomously.
Importance	**SHOULD**

Req. Nº	GR22
Req. Name	*Technical expectation – target flight path*
Description	The C-UAS shall detect, track and identify targets regardless of the flight path (e.g. hovering, low speed, high speed, etc.).
Importance	**SHALL**

Req. Nº	GR23
Req. Name	*Technical expectation – GPS denied environment*

Description	The C-UAS should be effective against drones that can operate in GPS-denied environment
Importance	**SHOULD**

Req. Nº	*GR24*
Req. Name	*Technical expectation – UAS RF link*
Description	The C-UAS should be effective against drones that operate without an active RF link.
Importance	**SHOULD**

Req. Nº	*GR25*
Req. Name	*Technical expectation – multiple targets*
Description	The system shall detect, track and identify multiple targets at the same time.
Importance	**SHALL**

Req. Nº	*GR26*
Req. Name	*Technical expectation – UAS information*
Description	The C-UAS system shall provide at least some of the following information related to detected UAS: type and serial number, position/coordinates, the route, ground speed, communication protocol, pilot/control station location.
Importance	**SHALL**

Req. Nº	*GR27*
Req. Name	*Technical expectation – data fusion approach*
Description	The system shall automatically detect, track and identify UASs, using sensors/technologies capabilities, independently or through data fusion mechanisms.
Importance	**SHALL**

Req. Nº	*GR28*
Req. Name	*Technical expectation - operation*
Description	The system shall ensure the manual, grouped and independent operation (at the decision of the operator/user), of the capabilities of all C-UAS subsystems.
Importance	**SHALL**

Req. Nº	GR29
Req. Name	Technical expectation – user interface
Description	The C-UAS system should have an intuitive and user-friendly interface, enabling operators to easily monitor and manage the system's functionalities. The interface should provide clear visualizations, alerts, and controls to facilitate efficient decision-making and response.
Importance	**SHALL**

Req. Nº	GR30
Req. Name	Technical expectation – access and configuration
Description	The system shall allow access and configuration of all settings and options of subsystems in the composition, through graphical user interface. The application will ensure the management of the sensors.
Importance	**SHALL**

Req. Nº	GR31
Req. Name	Technical expectation – auxiliary sensors
Description	The system should allow the installation of auxiliary sensors, to increase performance and/or adapt to the operational operating environment.
Importance	**SHOULD**

Req. Nº	GR32
Req. Name	Technical expectation - interconnectivity
Description	The system may allow interconnection with legacy systems/subsystems installed in other locations, including command and control, air traffic control, radar and perimeter security systems, to achieve a common operational picture.
Importance	**MAY**

Req. Nº	GR33
Req. Name	Technical expectation - adaptability
Description	The C-UAS system should be flexible enough to adapt to changing UAS threats (new models, new protocols or new specific parameters) and operating conditions.
Importance	**SHOULD**

Req. Nº	GR34
Req. Name	Technical expectation – geofence configuration
Description	The system shall offer the possibility of configuring geofence zones to establish detection (alarm) and countermeasure (interdiction) zones.
Importance	**SHALL**

Req. Nº	GR35
Req. Name	*Technical expectation – alarm functions*
Description	The system shall be provided with alarm functions through which the operator/user is warned, visually and audio, regarding the detection of UAS and their access to the geofence areas.
Importance	**SHALL**

Req. Nº	GR36
Req. Name	*Technical expectation – friend or foe*
Description	The system shall be equipped with detection capabilities and exclusion from the alarm procedure of friendly unmanned aircraft (mentioned in a dedicated list), these being visible in the graphical user interface through a different symbology/colour than the aircraft considered hostile.
Importance	**SHALL**

Req. Nº	GR37
Req. Name	*Technical expectation – malfunctions identification*
Description	The system should be provided with capabilities to identify malfunctions and alert the operator about them.
Importance	**SHOULD**

Req. Nº	GR38
Req. Name	*Technical expectation – alarms due disconnections*
Description	The system shall identify and alert the operator if any sensor is disconnected.
Importance	**SHALL**

Req. Nº	GR39
Req. Name	*Technical expectation – alarm sharing*
Description	The system shall be provided with the ability to share alerts via instant messaging such as MS Teams or WHATSAPP or email to a predefined list of phone numbers or email addresses, by including information on drone locations, the locations of their operators and the time of alarm activation.
Importance	**SHALL**

Req. Nº	GR40
Req. Name	*Technical expectation – access for diagnostic*
Description	The system shall allow local access to C-UAS sensor diagnostics and control applications.
Importance	**SHALL**

Req. Nº	*GR41*
Req. Name	*Technical expectation – access roles*
Description	The system shall ensure the possibility of assigning the following attributes/roles for users: a) For the Command and Control Centre - global administrator for access and editing of all capabilities of C-UAS sensors/subsystems, as well as user roles and permissions; b) For each fixed C-UAS system separately (in the case where several systems in different locations are interconnected) - dedicated local administrator for access and editing of all the capabilities of the C-UAS sensors/subsystems installed on them, as well as the roles and user permissions; c) User, with rights to view (read-only) all C-UAS sensors/subsystems or only certain C-UAS sensors/subsystems, in the rights functions granted by the local administrator; d) User, with rights to access the functions of the solution, all C-UAS sensors/subsystems or only certain C-UAS sensors/subsystems, in the rights functions granted by the administrator.
Importance	**SHALL**

Req. Nº	*GR42*
Req. Name	*Technical expectation – reports*
Description	The system shall ensure the possibility of creating and exporting a report that shows the recordings made by the sensors and the actions taken by the operator/user of the C-UAS software.
Importance	**SHALL**

Req. Nº	*GR43*
Req. Name	*Technical expectation – Performance Assessments*
Description	The C-UAS system may undergo regular performance assessments to evaluate its effectiveness in detecting, tracking, and neutralizing UAS threats. Performance metrics should be established to measure the system's accuracy, response time, false positive/negative rates, and overall operational success.
Importance	**MAY**

Req. Nº	*GR44*
Req. Name	*Technical expectation – data saving*
Description	The system shall ensure the permanent saving automatically as well as manually in a time interval predefined by the user, of at least the following information (logs, geographic coordinates, details about the identified UAS, sensor, etc..)
Importance	**SHALL**

Req. Nº	GR45
Req. Name	*Technical expectation – data sharing for coordinated response*
Description	Relevant information from C-UAS system shall be shared across incident management or workflow management tools to coordinate stakeholder response activities.
Importance	**SHALL**

Req. Nº	GR46
Req. Name	*Technical expectation - installation*
Description	Installation and uninstallation of detection and/or countermeasures equipment, should be done easily, through a modular and compact design.
Importance	**SHOULD**

Req. Nº	GR47
Req. Name	*Technical expectation - installation*
Description	System's components should be installed using specific clamping systems/tripods, which will offer a high degree of mobility, both during use and during maintenance and without major intervention on the infrastructure in which they will be installed. To ensure installation flexibility and avoid additional civil construction work, which must be subject to design, authorization and construction, mechanical fastening systems will be provided for each sensor.
Importance	**SHOULD**

Req. Nº	GR48
Req. Name	*Technical expectation – scalability by design*
Description	CUAS system shall be flexible and scalable by design, in order to address a specific location and environment conditions, without affecting the DTI performances. Based on location on field evaluation, the system must allow the placement of additional sensors (in terms of quantity as well as types), so as to offer the optimization of C-UAS system performance and safety in the operation of the equipment, by adapting to the specifics of a defined location.
Importance	**SHALL**

Req. Nº	GR49
Req. Name	*Technical expectation - redundancy*
Description	The C-UAS system may have built-in redundancy to ensure continuous operation of the main subsystems even if some of its components fail.
Importance	**MAY**

Req. Nº	GR50
Req. Name	*Technical expectation – connection elements*
Description	The fixed type CUAS systems shall be provided with all the connection elements necessary for the installation and safety in operation of the equipment in the installation location, both in terms of the necessary technical elements and in terms of the required quantities.
Importance	**SHALL**

Req. Nº	GR51
Req. Name	*Technical expectation – IP67 certification*
Description	Permanent installations shall be certified for use in the outdoor environment, according to the characteristics of protection class IP67.
Importance	**SHALL**

Req. Nº	GR52
Req. Name	*Technical expectation*
Description	Interconnection of C-UAS subsystems via IP architecture/networks. The interconnection of the sensors in the system composition with the command and control centre shall be done by dedicated IT equipment (switch, firewall), compatible with relevant IEEE/RFC standards and industrial connectors.
Importance	**SHALL**

Req. Nº	GR53
Req. Name	*Technical expectation*
Description	The system shall allow the ingestion and displaying in real time, of the information transmitted by all C-UAS subsystems, in a common image (integration of information from all sensors in the same interface)
Importance	**SHALL**

Req. Nº	GR54
Req. Name	*Technical expectation*
Description	The C-UAS system shall continuously report status, performance, degradation or failure
Importance	**SHALL**

Req. Nº	GR55
Req. Name	*Technical expectation*
Description	The system shall ensure the interoperability between all components of the C-UAS solution.
Importance	**SHALL**
Req. Nº	GR56
Req. Name	*Technical expectation*

Description	The system shall automatically assign C-UAS subsystems once they are connected to the C-UAS software.
Importance	**SHALL**

Req. Nº	*GR57*
Req. Name	*Technical expectation*
Description	The system shall allow operation without an Internet connection, using the connection in a dedicated local network
Importance	**SHALL**

Req. Nº	*GR58*
Req. Name	*Technical expectation*
Description	The system shall have an adaptable open architecture for C&C application software.
Importance	**SHOULD**

Req. Nº	*GR59*
Req. Name	*Technical expectation – privacy by design*
Description	The C-UAS system must be conceptually designed, with software mechanisms to ensure data protection
Importance	**SHALL**

Req. Nº	*GR60*
Req. Name	*Technical expectation – privacy by design*
Description	The C-UAS system will protect the data privacy against any accidental leakage or phishing.
Importance	**SHALL**

Req. Nº	*GR61*
Req. Name	*Technical expectation – Secure Communication and Information Sharing*
Description	The C-UAS system shall facilitate secure communication and information sharing. This includes robust data cybersecurity measures, data encryption, secure communication protocols, and access controls to prevent unauthorized access or data breaches.
Importance	**SHALL**

Req. Nº	GR62
Req. Name	*Technical expectation – GDPR compliance*
Description	The C-UAS shall be compliant with EU GDPR regulation regarding all digital data and information which are used and obtained during system operation: aircraft's registration number, video streams, etc.
Importance	**SHOULD**

Req. Nº	GR63
Req. Name	*Technical expectation – GDPR compliance*
Description	The C-UAS should allow the override of technical GDPR compliance mechanisms regarding all digital data and information which are used and obtained during system operation (aircraft's registration number, video streams, etc.), if an imminent threat with high risks is in place. The public interest will prevail.
Importance	**SHALL**

Req. Nº	GR64
Req. Name	*Conformity with the applicable regulations regarding the regime of products and services that can endanger life, health, security and the environment*
Description	This applies to new, used or reconditioned non-food products and services that may endanger life, health, work safety and environmental protection, not regulated by specific normative acts regarding the conditions for introducing products, respectively services, into the market. The introduction of new, used or refurbished non-food products and services on the market is allowed only under the conditions that they do not endanger life, health, work safety and environmental protection.
Importance	**SHALL**

Req. Nº	GR65
Req. Name	*Conformity with the applicable national regulations regarding the use of radio spectrum.*
Description	The system shall comply with 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.
Importance	**SHALL**

Req. Nº	**GR66**
Req. Name	*Conformity with the electrical safety directives/regulations*
Description	The system shall be compliant to Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonization of the laws of Member States relating to electrical equipment and electrical appliances designed for use within certain voltage limits.
	This directive addresses the safety aspects of electrical appliances, such as household appliances, but also for industrial equipment, laboratory instruments as well as information technology apparatus and all apparatuses within a defined voltage range on an external connection.
	While the directive addresses only apparatus that are supplied by electricity in common main networks, the hazards concerned are much wider. Besides electrical shock and the effects of short circuit, overheating, radiation and mechanical hazards are also part of the safety assessment, as well as documentation, both of applied components, but also safety documents and operation manual shall be delivered as part of the apparatus sold.
Importance	**SHALL**

Req. Nº	**GR67**
Req. Name	*Conformity with the regulation regarding the restriction of the use of certain hazardous substances in electrical and electronic equipment*
Description	The system shall be compliant to Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (recast)
Importance	**SHALL**

Req. Nº	**GR68**
Req. Name	*Conformity regarding eco-design requirements for computers and computer servers*
Description	The system shall be compliant to Commission Regulation (EU) No 617/2013 of 26 June 2013 implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to eco-design requirements for computers and computer servers
Importance	**SHALL**

Req. Nº	**GR69**
Req. Name	*Conformity with MIL-STD-810 H – Environmental Engineering Consideration and Laboratory tests*
Description	Emphasizes tailoring an equipment's environmental design and test limits to the conditions that it will experience throughout its service life, and establishing chamber test methods that replicate the effects of environments on the equipment rather than imitating the environments themselves. MIL-STD-810 addresses a broad range of environmental conditions that include: low pressure for altitude testing; exposure to high and low temperatures plus temperature shock (both operating and in storage); rain (including wind-blown and freezing rain); humidity, fungus, salt fog for rust testing; sand and dust exposure; explosive atmosphere; leakage; acceleration; shock and transport shock; gunfire vibration; and random vibration. Applicable only for equipment intended to be used outdoor.
Importance	**SHALL**

Req. Nº	*GR70*
Req. Name	*Marking and identification*
Description	Each component of the system shall be marked clearly and visibly. The labels shall contain all the mandatory information provided by international regulations (name, PN and series). The labels shall be resistant to the action of the weather and not allow accidental damage during handling, transport and storage
Importance	**SHALL**

Req. Nº	*GR71*
Req. Name	*Safety marking*
Description	In the documentation that accompanies the product and directly on the product, there will be warnings regarding possible dangers that may arise for people and equipment in the event of unauthorized interventions
Importance	**SHALL**

Req. Nº	*GR72*
Req. Name	*Product quality*
Description	The equipment shall be new, fully equipped and ready for immediate use. The equipment shall not include EoL (end of life) and/or EoS (end of service) products. Technical and quality specifications shall be supported by relevant documentation
Importance	**SHALL**

Req. Nº	*GR73*
Req. Name	*Maintenance plans*
Description	Maintenance shall be carried out in units approved by the manufacturer, during the entire service life of the product. The equipment supplier will detail the list with the contact details of the service units agreed to carry out maintenance work (during the warranty and post-warranty period). The supplier shall provide the preventive maintenance diagram, by complexity level, together with the information related to periodicity, volume of works, maintenance costs, including the list of necessary materials
Importance	**SHALL**

Req. Nº	*GR74*
Req. Name	*Logistic support*
Description	The products shall be purchased and delivered in compliance with the following logistic support program: free service and support during the warranty period; service and technical support against the cost after the expiration of the warranty period, for the entire life of the equipment
Importance	**SHALL**

Req. Nº	*GR75*
Req. Name	*Product warranty*
Description	The product warranty shall be at least 2 years (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0044), without a limit on operating hours. In case of equipment failure for any reason during the warranty period, the supplier must replace the product without additional costs, repair it or replace it within a maximum of 7 working days from receiving the notification. In the event that an equipment is replaced, it will benefit from an additional warranty period, equal to the number of days in which the equipment was unavailable. The replacement shall be done only with new components, according to the configuration in the documentation. If a piece of equipment is taken over by the supplier for repair, during the time it is unavailable, the supplier must make available to the beneficiary, a piece of equipment with performance at least like that of the product taken over for repair, to ensure the operation of the product at the set values.
Importance	**SHALL**

Req. Nº	*GR76*
Req. Name	*Reception of the product*
Description	Upon receipt of the product, shall be accompanied by all the accessories necessary for operation at the required parameters. The product will be accompanied by a list of all components, warranty certificate, declaration of conformity, operating, knowledge and maintenance documentation. The reception will be done, through inspections and tests, to verify the conformity of the product with the specified requirements.
Importance	**SHALL**

Req. Nº	*GR77*
Req. Name	*Product documentation*
Description	The documentation accompanying the product shall include at least the following: user manual, installation, administration and maintenance manual. The documents will be in the mother tongue of the beneficiary or in English.
Importance	**SHALL**

Req. Nº	*GR78*
Req. Name	*The life of the product*
Description	The life of the product shall be at least 5 years, or as it is stipulated in the national accounting regulations
Importance	**SHALL**

Req. Nº	*GR79*
Req. Name	*Software licensing*
Description	If the software solution consists of a desktop application, the application installation kit should be transferred to the beneficiary at no additional cost.
Importance	**SHOULD**

Req. Nº	*GR80*
Req. Name	*Software licensing*
Description	The supplier should provide perpetual usage licenses.
Importance	**SHOULD**

Req. Nº	*GR81*
Req. Name	*Software licensing*
Description	The provider shall ensure the possibility of migrating perpetual licenses from a workstation/processing unit to another computer of the Beneficiary, without additional costs. The migration will be done in the event of a workstation failure, or during the period in which it is under maintenance
Importance	**SHALL**

Req. Nº	*GR82*
Req. Name	*Software licensing*
Description	The supplier shall provide all updates and patches necessary to fix non-functionalities and vulnerabilities for a period of at least 5 years;
Importance	**SHALL**

Req. Nº	*GR83*
Req. Name	*Painting and colour markings*
Description	The C-UAS system painting scheme, shall be adapted on client requirements, to cover the operational needs, even for covert operations.
Importance	**SHALL**

Req. Nº	*GR84*
Req. Name	*Cost-effectiveness*
Description	The C-UAS system should be cost-effective. The system should be able to operate efficiently and require minimal maintenance and repair costs.
Importance	**SHOULD**

Req. Nº	*GR85*
Req. Name	*Functional Safety*
Description	The system may be compliant with IEC 61508.
Importance	**MAY**

Req. Nº	*GR86*
Req. Name	*Countermeasures directionality*
Description	The countermeasures should be directed at the target.
Importance	**SHOULD**

Req. Nº	*GR87*
Req. Name	*Conformity with the applicable national regulations regarding the use of radio spectrum*
Description	The system shall comply with the national frequency allocation plan.
Importance	**SHALL**

Req. Nº	*GR88*
Req. Name	*Conformity with the applicable international legislation*
Description	The C-UAS system shall comply with the applicable provisions of the European AI legislation as soon as this legislation enters into force (New AI Act).
Importance	**SHALL**

Req. Nº	*GR89*
Req. Name	*Subsystem calibration*
Description	Calibration process of the subsystems and the system should be supported by the C2 and therefore should be tested
Importance	**SHALL**

Req. Nº	*GR90*
Req. Name	*Built in Test*
Description	The start-up process shall include an overall system health check (not only BIT of Subsystems).
Importance	**SHALL**

Req. Nº	*GR91*
Req. Name	*Operator training*
Description	System operation should be intuitive and require minimal training (provided by the manufacturer or integrator)
Importance	**SHALL**

Req. Nº	GR92
Req. Name	Administrator training
Description	System administration may require advanced knowledge that may be proven by skill certificates.
Importance	**MAY**

9.2.2 Operational needs for the counter measures

Additional requirements/needs must be addressed. Below are presented just several basic requirements from an operational point of view, considering the link with the DTI capabilities.

Req. Nº	CM01
Req. Name	Countermeasure requirements – multiple targets
Description	The C-UAS system shall counter simultaneously one or multiple UAS
Importance	**SHALL**

Req. Nº	CM02
Req. Name	Countermeasure requirements – jamming
Description	The jamming system (if any) of the C-UAS system shall not interfere with legitimate communications links
Importance	**SHALL**

Req. Nº	CM03
Req. Name	Countermeasure requirements - spoofing
Description	The spoofing system (if any) of the C-UAS system shall not interfere with legitimate communications links
Importance	**SHALL**

Req. Nº	CM04
Req. Name	Countermeasure requirements – GPS jamming
Description	The GPS jamming system (if any) of the C-UAS system shall not interfere with legitimate communications links
Importance	**SHALL**

Req. Nº	CM05
Req. Name	Countermeasure requirements – protocol manipulation
Description	The take-over system/ protocol manipulation (if any) of the C-UAS system shall not interfere with legitimate communications links
Importance	**SHALL**

Req. Nº	*CM06*
Req. Name	*Countermeasure requirements – man in the loop*
Description	The counter measures shall be activated by a trained operator only
Importance	**SHALL**

Req. Nº	*CM07*
Req. Name	*Countermeasure requirements -safety of use*
Description	The counter measures shall minimize the threat for safety of the people, as set out by the member state/regional regulation board for the safety of the users/operators and general public that may come in to contact or within the vicinity of the system
Importance	**SHALL**

Req. Nº	*CM08*
Req. Name	*Countermeasure requirements - integration with DTI*
Description	The counter technologies, shall be integrated with the DTI capabilities
Importance	**SHALL**

Req. Nº	*CM09*
Req. Name	*General expectation – Multi-layer Countermeasures*
Description	The C-UAS System may develop a multi-layered approach to counter UAS threats, based on predefined criteria, such as level of risk, proximity to sensitive areas, potential impact on safety and security, the nature of mission or operation, or potential harm to personnel or assets.
Importance	**MAY**

9.2.3 Operational needs for the integration with other technologies

Req. Nº	*In01*
Req. Name	*ATM integration*
Description	The C-UAS system should be able to interface with existing ATM system for exchange information on cooperative UAS.
Importance	**SHOULD**

Req. Nº	*In02*
Req. Name	*Open standards*
Description	The C-UAS system should support open standards to allow the connection with existing or new systems, to assure future scalability.
Importance	**SHOULD**

Req. Nº	*In03*
Req. Name	*Alternative links for interconnection*
Description	The C-UAS system's components (e.g. sensors, command & control, effectors) should use as alternative links for interconnection, the existing wired and wireless open infrastructure of the beneficiary
Importance	**SHOULD**

Req. Nº	*In04*
Req. Name	*Open API*
Description	The C-UAS system shall have an open API that allows end-users or third-party vendors to add additional sensors or mitigation capabilities
Importance	**SHALL**

Req. Nº	*In05*
Req. Name	*Open standards*
Description	The interconnection of the C-UAS system's components (e.g. sensors, command & control, effectors) should be open according to the wired and wireless open standard (e.g. Ethernet IETF protocols and 3GPP protocols)
Importance	**SHOULD**

Req. Nº	*In06*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system should allow integration into any existing security infrastructure
Importance	**SHOULD**

Req. Nº	*In07*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system shall not compromise the existing aviation safety and security levels in the deployment and operation area
Importance	**SHALL**

Req. Nº	*In08*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system shall not affect current operations of Communication, Navigation and Surveillance systems
Importance	**SHALL**

Req. Nº	*In09*
Req. Name	*Integration in existing C2 (command and control) infrastructure*
Description	The C-UAS system should be compatible with the SAPIENT-interface in order to be interoperable with NATO, should it ever become necessary.
Importance	**SHALL**

9.2.4 Operational needs for post-action forensic evidence

Req. Nº	*FE01*
Req. Name	*Forensic evidence requirement*
Description	The C-UAS system shall record all events, which can be used later on for analysis, measure the effectiveness of the full C-UAS process cycle, training, and forensic processes.
Importance	**SHALL**

Req. Nº	*FE02*
Req. Name	*Forensic evidence requirement*
Description	The C-UAS system shall preserve all digital information needed for forensic investigations.
Importance	**SHALL**

Req. Nº	*FE03*
Req. Name	*Forensic evidence requirement*
Description	The C-UAS system's components shall be tamper-proof.
Importance	**SHALL**

10 C-UAS system performance requirements and metrics

10.1 General

The functional and performance requirements of C-UAS systems result directly from the operational needs described in clause 9. The described requirements allow for defining the minimum requirements for C-UAS applicable to various scenarios and directly refer to them. Each area of C-UAS application will have slightly different requirements regarding operating parameters, power supply, type of detected UAS and conditions in which they are to work.
On the basis of the described requirements, metrics were defined that will verify whether the previously defined requirements are met and to what extent.

The requirements and metrics described in this clause will allow for estimating the suitability of a given system for specific applications corresponding to the assumed threat scenarios.

Requirements serve as criteria against which solutions can be tested and evaluated. They offer detailed metrics that enable an objective measurement of the potential solution's effectiveness, ensuring well-informed purchasing decisions regarding products, systems, or services that achieve the stated operational goals. A thorough requirements analysis can unveil hidden needs and identify common issues across programs and various operational components. Detailed operational

requirements will guide product development, ensuring that solution specifications actively address the identified problems.

This clause proposes a set of detailed functional and performance requirements that detection, tracking, and identification (DTI) systems should meet, along with the metrics by which they can be measured. The requirements definition will use the IEEE 29148 process terminology:

- Must (Shall) – high-priority requirements that must be met for the project to achieve its key objectives.
- Should - medium-priority requirements that must be met unless an acceptable reason is provided for omitting them.
- May - low-priority requirements that should be considered during the project.

The proposal for prioritization is included in the current definition of requirements, but its appropriateness will be assessed at a later stage. The requirements presented in this document are divided into the following types:

- DTI General System Requirements (O)
    - Detection (sub)system requirements (D)
    - Tracking (sub)system (T)
    - Identification (sub)system (I)
- System architecture requirements (A)
- Safety requirements (S)
- Logistics requirements (L)
- Human-Machine Interface Requirements (H).

Individual requirements for different scenarios are sequentially numbered. For each scenario, a different alphabetical abbreviation is adopted alongside the point number.

The numbering scheme looks as follows:

XXYY ZZ where:

- XX – two letters indicating the type of requirement:
    - FR – Functional Requirements
    - PR – Performance Requirements
- YY – two letters specifying the scenario name:
    - PR – PRison
    - AP – AirPort
    - NP – Nuclear power Plant
    - GB – Government Building
    - ST – events STadium
    - OC – Outdoor Concert
    - OR – Outdoor political Rally
    - IS – International Summit
    - LB – Land Border
    - MB – Maritime Border
- ZZ – the consecutive number of the requirement on the list for a specific scenario.

This numbering method facilitates easy identification of the requirement on the list and allows for referencing it in other documents if needed.

In the next section of the document, technical parameters of C-UAS systems for their objective comparison are also presented. The proposed methods and indicators allow for measurable comparisons of C-UAS systems, minimising the impact of technologies used in those systems when choosing the suitable one for the given area. These metrics are a logical extension of earlier functional and performance requirements. A consistent methodology for describing object specifications, environmental conditions, and test locations enables the maintenance of similar test conditions, crucial for an unbiased comparison of C-UAS systems.

10.2 Functional requirements of C-UAS systems

10.2.1 General

In this subclause, the functional requirements of C-UAS systems are presented. Properly formulated functional requirements enable a clear determination of what C-UAS systems shall, should, or may perform. The essence of functional requirements is focused on meticulously defining specific guidelines for C-UAS systems in terms of the types of tasks they perform, aligning with the needs of a given scenario.

In annex E, diverse usage scenarios of C-UAS systems have allowed for the formulation of dedicated functional requirements tailored to each scenario. These requirements are closely aligned with the real needs that arise during the execution of a specific scenario, to which specific functionalities of C-UAS systems respond. Additionally, functional requirements have been categorized according to the types described in subclause 10.1 (O/D/T/I/A/S/L/H).

This subclause also serves as the foundation for the performance requirements described in the 10.3. Performance requirements often measurably determine how tasks are executed by C-UAS systems, as specified by the functional requirements.

10.2.2 Descriptive definition of functional requirements for C-UAS systems

The functional requirements describe what the system shall/should/can do in order to detect UAS and provide this information to the system operator. They are a consequence and result directly from the operational needs described in clause 9.

It is not always possible to directly translate operational needs into functional requirements. In some cases, one operational need is matched by two or more functional requirements. On the other hand, some of the needs are so general, but necessary from the user's point of view, that it is not possible to translate them directly into functional requirements. However, the assumptions contained in them are taken into account when creating other requirements. For example, the operational need described as "The system shall contribute to increase the protection capacity of some physical objectives by identifying and monitoring the threats represented by the use of unmanned aircraft used in illicit actions" is referenced in the requirements to identify and track UAS.

The main assumption is that the requirements describe in detail the tasks to be performed by C-UAS in order to meet the operational needs of the user.

As part of this document, a list of functional requirements for each of the 10 scenarios was created in accordance with the best knowledge of the authors and in cooperation with the users involved in this project. Subsequently, this list, containing about 80 items, was unified in order to give a single wording to the provisions relating to individual requirements. The functional requirements for C-UAS for each scenario have been selected from this list to be relevant to the specific case described in one of them.

10.2.3 Brief analysis of operational needs in terms of selection of functional requirements

Clause 9 lists the operational needs that C-UAS needs to meet from the user's point of view. The document includes:

- list of basic operational needs for DTI of C-UAS,
- list of operational needs for countermeasure systems (jamming systems, spoofing, GPS jamming etc.),
- list of operational needs for the integration of DTI systems with countermeasure systems,
- list of operational needs for forensic evidence, and
- list of specific operational needs for different scenarios developed by the COURAGEOUS project.

Functional requirements for countermeasure systems are not included in the scope of this document. Describing the functional requirements for these systems in accordance with the logic would require the development of performance requirements and metrics for them, which would significantly extend the document. However, since C-UAS do not operate in isolation from reality, it seemed necessary to the authors of this document to include requirements regarding the possibility of their integration with countermeasure systems.

When developing functional requirements, all operational needs described in clause 9 were considered, taking into account their share in relation to individual scenarios. The functional requirements are assigned to individual scenarios, and the possible separation of those that are universal, basic regardless of the type of scenario is planned at a later stage of developing this document after the tests that will be carried out as part of the project and which will show the importance of individual requirements.

10.2.4 C-UAS functional requirements with description and justification

Below is a description of the functional requirements in the further part of the document with their justification. Each of these requirements may have a different "Importance" (shall/should/may) depending on the user's requirements/expectations for a given scenario.

Table 35 — Description of functional requirements

Type of requirements	Requirement	Description and justification of the requirement
Detection	detect UAS that is appearing in the observation area	In order to meet this requirement, the system shall/should/can detect a UAS that appears in the observation area adopted in the considered scenario. The expected result of this requirement is the immediate detection of the UAS regardless of the existing observation processes conducted by the C-UAS system.
Detection	detect multiples UAS in the observation area	In order to meet this requirement, the system shall/should/may allow multiple detection of UAS. The expected result of this requirement is the ability to multi-thread, system operation in terms of detection, without compromising system performance
Human-Machine Interface	alarm the system operator to the appearance of UAS in the observation area	In order to meet this requirement, the system shall/should/may alert the system operator to the presence of a UAS in the observation area via the user interface. The method of providing information should be prompt and unambiguous for the C-UAS system operator

Type of requirements	Requirement	Description and justification of the requirement
Tracking	track UAS that is moving in the observation area	In order to meet this requirement, the system shall/should/can track the UAS that moves within the observation area, with and without the operator confirmation, while ensuring the uninterrupted operation of the processes already running in the C-UAS system. The method of tracking the object should be continuous and reproducible by the system operator.
Tracking	track multiples UAS in the observation area	In order to meet this requirement, the system shall/should/may allow multiple detection of UAS. The expected result of this requirement is the ability to multi-thread, system operation in terms of tracking, without compromising system performance.
Identification	identify UAS that is in the observation area	In order to meet this requirement, the system shall/should/can identify a UAS within the observation area by comparing its shape to the current base of commercial UAS patterns. The expected result is immediate and unambiguous information for the operator about the identified UAS, considering the probability of correct identification.
Identification	identify multiples UAS in the observation area	In order to meet this requirement, the system shall/should/may allow multiple detection of UAS. The expected result of this requirement is the ability to multi-thread, system operation in terms of identification, without compromising system performance.
Human-Machine Interface	give the system operator the ability to identify the UAS within the observation area	In order to meet this requirement, the system shall/should/may allow the operator to self-identify the UAS based on the parameters and images displayed in the user interface.
Detection	detect a single class C1 UAS (weight <900g - according to Commission Delegated Regulation (EU) 2019/945 of 12 March 2019)	In order to meet this requirement, the system shall/should/may detect a single UAS in the observation area adopted in the considered scenario, meeting the requirements of class C1 in accordance with Commission Delegated Regulation (EU) 2019/945 of March 12, 2019). The expected result of this requirement is the immediate detection of the UAS regardless of the existing observation processes conducted by the C-UAS system.
Detection	detect a load carried by UAS weighing ...	To meet this requirement, the system shall/should/may detect the load transported by the UAS, weighing ..., storing the time and place of its detection in the database, allowing for later retrieval of this information.
Detection	detect UAS flying at speed of up to ...	In order to meet this requirement, the system shall/should/may immediately detect a UAS moving in the observation area adopted in the scenario, ensuring the possibility of its detection for the speed of UAS movement up to ...
Detection	detect UAS flying at an altitude of up to ...	To meet this requirement, the system shall/should/can immediately detect a UAS moving within the observation area at a flight altitude of ...
System architecture	enable simultaneous processing of	In order to meet this requirement, the system shall/should/can process information from sensors using

Type of requirements	Requirement	Description and justification of the requirement
	information from sensors using different technologies	different detection/tracking/identification technologies to achieve synergistic results (data fusion algorithms. The obtained detection/tracking/identification results should be more effective when using different technologies than in the case of single technologies.
Identification	distinguish between friend or foe UAS (IFF)	To meet this requirement, the system shall/should/can provide the operator with Identification Friend or Foe (IFF) by being able to enter and tag their own UAS in the system database. The result of this will be the unambiguous identification of only potentially hostile/unknown UAS.
Detection	be immune to false alarms caused by flying birds	In order to meet this requirement, the system shall/should/can be immune to false alarms caused by flying birds, so that when detecting UAS they are not confused with birds flying in the observation area assumed in the scenario. The expected result of this requirement is the selection of only UAS from all detected flying objects, rejecting detected birds, which will significantly improve the readability of the situational analysis conducted by the C-UAS system operator.
Identification	be immune to false alarms caused by flying birds	To meet this requirement, the system shall/should/can be immune to false alarms caused by flying birds, so that when identifying UAS they are not confused with birds flying in the observation area assumed in the scenario. The expected result of this requirement is to identify only commercial UAS according to the current UAS database, reject flying birds.
Tracking	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	To comply with this requirement, the system shall/should/may allow the system operator to assign a unique identifier in the database to a detected and then tracked UAS. This allows for selective and unambiguous observation of the most interesting objects from the point of view of the operation.
Tracking	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	To meet this requirement, the system shall/should/may ensure the ability to continue tracking the UAS after a temporary loss of its visibility, resulting, for example, from terrain obstacles. The expected result of this requirement is that the UAS continues to be tracked under the same unique identifier, rather than broadcasting a new one after temporarily losing visibility of the tracked object.
Tracking	provide the ability to determine the coordinates of the location of the pilot of the detected UAS	In order to meet this requirement, the system shall/should/can provide the ability to immediately determine the coordinates of the location of the pilot detected UAS and continuously track changes in its position.
Identification	identify the load carried by the UAS	In order to meet this requirement, the system shall/should/can identify the type of cargo carried by the UAS, unambiguously classifying it to the cargo class specified in the database.
Identification	identify that the UAS is carrying load	In order to meet this requirement, the system shall/should/may immediately recognize a situation in

Type of requirements	Requirement	Description and justification of the requirement
		which a UAS moving in the observation area is carrying a load or no longer has a load (it has been dropped).
Detection	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	In order to meet this requirement, the system shall/should/can allow continuous and uninterrupted UAS detection, despite the currently running tracking process of a previously detected UAS. The expected result of this requirement is the ability to multi-thread, uninterrupted system operation in terms of detection and tracking, without compromising system performance.
Detection	be able to detect UAS in the observation area regardless of the obstacles and environment	In order to meet this requirement, the system shall/should/may be able to detect UAS behind building and obstacles indifferent of environment. The expected result of this requirement is the ability detect UAS, in various environments without compromising system performance.
Human-Machine Interface	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	In order to meet this requirement, the system shall/should/may immediately alert the system operator via the user interface of the appearance of another UAS in the observation area and prompt the operator to decide friendly, foe or false, while the tracking process of the previously detected UAS is continuously carried out.
Human-Machine Interface	possibility to train operators with an embedded training system/Simulator	In order to meet this requirement, the system shall/should/may incorporate means to train operators in the chain detection-tracking- identification-reporting-recording and after-math evaluation.

10.3 Performance requirements of C-UAS systems

10.3.1 General

In this subclause, performance requirements for C-UAS systems are presented. In most cases, they are closely related to the functional requirements described in subclause 10.2. They provide a detailed and complementary description of the previously specified required functions of C-UAS systems in terms of how a given task should be performed. However, not all functional requirements are directly and simply linked to performance requirements. Sometimes, one functional requirement corresponds to two or more performance requirements. They are often accompanied by numerical values that serve as performance requirement thresholds. Additionally, the requirements include information about their "importance" (must/should/may) depending on user expectations for a given scenario. Performance requirements have also been categorised according to the types described in 10.1 (O/D/T/I/A/S/L/H). Due to the performance requirements outlined in this clause, it is possible to subsequently create metrics that describe the physical parameters subject to measurement and evaluation. Therefore, it is necessary to define the scope of certain performance requirements that are acceptable from the user's perspective.

10.3.2 Descriptive definition of performance requirements and their relationship to functional requirements

Performance requirements describe, based on functional requirements, what the system shall/should/may do. Individual performance requirements were created based on the corresponding functional requirements.

As with operational needs and performance requirements, it is not always possible to translate one requirement directly to another. In some cases, two or more performance requirements correspond to one functional requirement. In others, it is not possible to directly transfer a notation from functional to performance requirements, and it is necessary to transfer the idea of one notation to another in a different way.

It is important that the sense of the functional requirements is transferred to the performance requirements because it is on the basis of the ideas contained in them that the metrics are built.

As in the case of functional requirements, a list containing about 80 items was created for performance requirements. Performance requirements were selected from it and assigned to individual scenarios.

10.3.3 Descriptive translation of functional requirements into performance requirements

The functional requirements prepared for individual scenarios assume checking the C-UAS in specific conditions similar to real ones and reflecting the assumptions of a given scenario. These requirements describe what the system shall/should/may do.

Performance requirements describe what a system shall/should/may be. Performance requirements should result directly from functional requirements, although such a direct connection will not always be possible. Sometimes one functional requirement will be matched by two or more performance requirements.

Performance requirements will define the criteria against which the C-UAS will be tested and then evaluated in order to obtain an objective measure of the effectiveness of the C-UAS when used in a particular scenario.

Examples:

1. Functional requirement:
   - *The C-UAS must detect a UAS that appears in the observation area*

   translates into performance requirements:

   - *The C-UAS must detect all UAS with no missed detections in the observation area,*
   - *The C-UAS must detect Class I, Micro category UAS in the observation area.*

2. Functional requirement:
   - *The C-UAS must track the UAS that is moving within the observation area*

   translates into performance requirements:

   - *The C-UAS must indicate the position of the object without significant non-real deviations.*

Properly formulated performance requirements will allow for the development of metrics that will allow for an objective, based on measurements of physical quantities, comparison of different C-UAS in different conditions and for different test objects.

10.3.4 C-UAS performance requirements with a brief description and justification

In this subclause is a description of the performance requirements with their justification. Each of these requirements may have a different "Importance" (shall/should/may) depending on the user's requirements/expectations for a given scenario.

Table 36 — Description of performance requirements

Type of requirements	Requirement	Description and justification of the requirement
System architecture	ensure that all signals are recorded in native resolution (continuously and efficiently)	In order to meet this requirement, the system shall/should/may record all signals at native resolution continuously and efficiently. The expected result of this requirement is uninterrupted effective recording of events and the possibility of retrieving them at any time.
System architecture	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	In order to meet this requirement, the system shall/should/may have the resources to record all detections. The user should be able to access the storage space/capacity of each detection at any time.
System architecture	have access to above mentioned storage space/capacity in real time	In order to meet this requirement, the system shall/should/may provide the user with access to the history of events on demand at any time.
System architecture	have guaranteed manufacturer support in the field of UAS databases	In order to meet this requirement, the system shall/should/may cooperate with the system manufacturer in the field of ongoing updating of the UAS database. The expected result of this requirement is that the system has an up-to-date UAS database.
System architecture	Operate 24 hours a day, 7 days a week	In order to meet this requirement, the system shall/should/may operate reliably, continuously, have an alternative power supply and be provided with regular maintenance inspections.
System architecture	use DTI technologies that does not affect the object infrastructure systems	In order to meet this requirement, the system shall/should/may not interfere with the existing devices of the protected facility. The expected solution is noise-free operation.
System architecture	transmit D, T, I signals over long distances to the system operator ...	In order to meet this requirement, the system shall/should/may be provided with encrypted means of communication (e.g., satellite, radio). The expected result is the continuity of operation, uninterrupted control of the operator over the system and protection against attempts to take control.
Detection	be resistant to severe weather conditions: strong winds, precipitation, fog, salty air, etc	In order to meet this requirement, the system shall/should/may be resistant to various weather conditions that cannot interfere with the operation of the C-UAS in any way. The expected result of this requirement is uninterrupted unmissable recording of all detections regardless of adverse weather conditions.

Type of requirements	Requirement	Description and justification of the requirement
Detection	detect all UAS with no missed detections	In order to meet this requirement, the system shall/should/may detect UAS that have appeared in the observation area. The expected result of this requirement is the immediate detection of all UAS regardless of the previous observation processes conducted by the C-UAS system.
Detection	detect objects with technology that does not interfere with the communication systems of government security (not necessarily RF)	In order to meet this requirement, the system shall/should/may not interfere with the existing devices of the protected facility. The expected solution is noise-free operation.
Detection	have enough RAM (processing resources and storage resources) to ensure detections 24 hours a day, 7 days a week	In order to meet this requirement, the system shall/should/may have operational memory resources ensuring continuous uninterrupted UAS detection. The expected result of this requirement is uninterrupted non-missing logging of all detections.
Detection	detect multiples UAS in the observation area	In order to meet this requirement, the system shall/should/may allow multiple detection of UAS. The expected result of this requirement is the ability to multi-thread, system operation in terms of detection, without compromising system performance
Human-machine interface	have an appropriate API enabling communication with other systems	In order to meet this requirement, the system shall/should/may have the possibility of cooperation with the existing and planned systems of the protected facility. The expected result of this requirement is the ability to fully integrate the facility's security systems.
Identification	enable UAS identification in difficult weather conditions, at night	In order to meet this requirement, the system shall/should/may be resistant to harsh weather conditions and be able to be identified at any time. The expected result of this requirement is uninterrupted unmissable identification of detected objects in continuous mode.
Identification	enable UAS identification in difficult weather conditions, during fog	In order to meet this requirement, the system shall/should/may be resistant to harsh weather conditions and be able to identify when fog occurs. The expected result of this requirement is uninterrupted unmissable identification of detected objects in continuous mode.
Identification	have enough resources (processing resources and storage resources) to ensure identification 24 hours a day, 7 days a week	In order to meet this requirement, the system shall/should/may have operational memory resources ensuring continuous uninterrupted identification of detected objects. The expected result of this requirement is uninterrupted, unmistakable identification of detected objects, which will not raise false positives.

Type of requirements	Requirement	Description and justification of the requirement
Identification	identify the birds distinguishing them from the UAS	In order to meet this requirement, the system shall/should/may identify all detected objects. The expected result of this requirement is uninterrupted unmistakable identification of detected objects that will not trigger false alarms due to bird detections in the observation area.
Logistics	be easy deployable (determine the number of people, their training and tools necessary to set up and run the system)	In order to meet this requirement, the system shall/should/may precisely determine the number of human resources and the level of competence necessary to run the system. The expected result of this requirement is that the system is simple to set up and commissioned by selected trained personnel.
Logistics	operate in an area without access to the mains	In order to meet this requirement, the system shall/should/may operate without access to the power grid using other dedicated self-sufficient energy resources. The expected result of this requirement is continuous, trouble-free operation.
Logistics	operate 24 hours a day, 7 days a week	In order to meet this requirement Integrated Logistics Support (ILS) issues have to be taken into consideration to achieve the desired Operational Availability.
Logistics	provide prior to test all the frequencies used by equipment	In order to meet this requirement, the provider shall/should/may provide the necessary information such that the operator can apply – if necessary – for frequency clearances at national OFCOM.
Tracking	constantly track a given number of UAS simultaneously	In order to comply with this requirement, the system shall/should/may allow continuous and uninterrupted tracking of several UAS. The expected result of this requirement is the ability to multi-thread, uninterrupted system operation in terms of detection and tracking, without compromising system performance.
Tracking	indicate the position of the object without significant unreal deviations	In order to meet this requirement, the system shall/should/may accurately display to the operator of the UAS that is moving within the observation area. The expected result of this requirement is the ability to precisely determine the coordinates of the tracked UAS in real time.

10.4 Determination of acceptable ranges for performance requirements

Performance requirements describe what the system shall/should/may be and are the basis for creating metrics – a description of physical parameters that will be subject to measurement and evaluation. For this reason, it is necessary to specify a range for some of the performance requirements that is acceptable from the user's point of view. If the specified parameters are outside the defined range, they are unacceptable and C-UAS is useless.

The range of parameters must be agreed with the users and ultimately their opinion will be binding in this respect.

In particular, it is proposed to define acceptable ranges for:

- be resistant to severe weather conditions - strong wind - the user will specify the acceptable range of wind speeds,
- detect communication between the UAS and the pilot on supposed frequencies - the user will specify the frequency range monitored by C-UAS,
- detect the dropping of the load - the user will specify the size of the load, the dropping of which is to be detected by the system,
- detect UAS flying at a speed of up to … - the user will specify the maximum UAS speed at which it must be detected,
- detect UAS flying at an altitude of above … - the user will specify the lowest possible height at which the UAS is to be detected,
- detect UAS flying at an altitude of up to … - the user will specify the highest possible height at which the UAS is to be detected,
- enable the detection of UAS within the time (distance) that allows the implementation of security procedures - a very important parameter that depends largely on the provisions of the protection plan for a specific site. Considering the fact that in the event of an attack using a UAS, security procedures provided for in the facility security plan must be implemented, the time needed for their implementation is an important factor. The time depends on the maximum speed at which the attacking UAS can move and the shortest distance from which it can take off. The protection plan should take into account what type of UAS can be used to attack a given object and what is the minimum distance from which it can start, i.e. at what distance from sensitive places on the site its foreground is not monitored and it is possible to start the UAS without the knowledge of security services of the facility. Without taking these factors into account, it is not possible to simply specify the time in which C-UAS will detect a threat in performance requirements.
- Alarm the system operator of a malicious UAS with a false positive rate (FPR) of no more than … - the user should specify the maximum allowable FPR value,
- Alarm the system operator of malicious UAS with a False Negative Alarm Rate (FNR) of no less than … - the user should specify the maximum allowable FNR value.

Performance requirements for various scenarios presented in this document have been described above based on functional requirements. Their correct description determines the parameters to be measured during the tests. These parameters are described in 10.5.

Note that the performance requirements detail the C-UAS parameters for the specific uses envisaged in the scenarios. Ultimately, a set of these requirements can be used by the user to create specifications for ordering the required solution for specific applications. They can also be used in the creation of public procurement by entities operating on the basis of the Public Procurement Act.

10.5 Technical parameters of C-UAS systems relevant for their comparison and methods of their measurement

10.5.1 General

In this subclause, technical parameters of C-UAS systems are provided to facilitate their objective comparisons. The proposed methods and indicators enable a measurable assessment of the quality

of tested C-UAS systems. These metrics have been prepared to minimize their dependency on the technologies employed by C-UAS. They represent a logical continuation of previously developed functional and performance requirements. By employing a standardized methodology for describing the specifications of the object under examination, environmental conditions, and test locations, it will be possible to maintain similar test conditions for C-UAS systems, essential for conducting an objective comparison. Every factor, whether related to the object under study, the location, or the test conditions, has a significant impact on the effectiveness of C-UAS systems. These metrics aim to uphold the principles of "fair play" in testing C-UAS systems, ensuring that each provider can present their solution under the same conditions. Additionally, end-users of C-UAS can be confident that the system performs correctly not only in laboratory conditions but also in real-world scenarios.

The above describes the quantities that should be measured during the tests to be able to reliably compare different C-UAS. It should be noted that the environmental conditions in which they are tested (weather and terrain conditions) and the test objects are particularly important for comparing different systems. It is difficult to compare two systems, one of which would be tested during rainfall in a heavily urbanized area and the other during good windless weather in a rural area. Likewise, it would be difficult to compare systems if different test objects of significantly different sizes were used for testing.

After testing under this project, it is planned to develop a weighting scale that will enable estimation of the measurement results for different conditions. However, for this to be possible, it is necessary to precisely measure all parameters that affect the operation of the C-UAS during the planned tests.

It is important to note that selected conditions described in operational needs, operational requirements, and performance requirements can be applied collectively or independently by users to define the conditions that must be met by the C-UAS solution they require. Based on all these conditions, metrics have been developed in this document. The application of these metrics will enable the comparison of different systems and determine their suitability for specific objectives.

In order for test results to yield benefits in the form of recommendations for various solutions, parameters, and requirements for specific objects and threat scenarios, it is necessary to conduct credible, scientifically justified measurements that clearly demonstrate differences between various technologies and solutions used in C-UAS systems.

This document presents the functional and performance requirements of C-UAS systems, along with technical parameters for their objective comparison. Functional requirements precisely specify what C-UAS systems must, should, or may accomplish, focusing on various usage scenarios. Performance requirements closely align with functional ones, detailing how tasks should be executed. Both types of requirements are categorised according to types described in subclause 10.1 (O/D/T/I/A/S/L/H). Subsequently, metrics are introduced to facilitate the evaluation of tested systems, independent of specific technologies. A shared methodology for describing object specifications, environmental conditions, and test locations ensures similar test conditions, crucial for an unbiased comparison of C-UAS systems. These metrics, adhering to the principles of "fair play," enable providers to showcase their solutions in comparable testing conditions, providing end-users with confidence that the system operates not only in laboratory conditions. This document serves as an essential foundation for developing a weighted evaluation system for individual factors within the tests. This will enable obtaining a numerical and clear assessment of a specific instance of the C-UAS system and facilitate a straightforward comparison with competitive solutions under conditions specified by the end-user.

10.5.2 Introduction to the measurement of C-UAS parameters during tests with justification

Based on a defined set of standard scenarios and related operational needs, then developed into detailed functional and performance requirements that UAS detection, tracking and identification systems must meet, a set of metrics has been developed with which to measure them.

In order for the metrics to objectively evaluate individual systems and have added value in the project, it is necessary to develop them in such a way that they are as universal and transparent as possible. Can be used for different C-UAS and for equal measurement conditions - test environment.

For this purpose, four thematic groups have been distinguished in the metrics:

1. test facility specification (UAS),
2. environmental conditions,
3. specification and equipment of the test site,
4. parameters subject to testing for detection, tracking and identification,

A separate problem is the development of such test methods to obtain objective and comparable results for each of the tested C-UAS. For this purpose, it is necessary to describe in detail the method of conducting tests and UAS raid routes.

Within each of the metrics, ranges have been defined for which weighting points will be assigned, resulting in a numerical value that will determine the quality of the proposed solution.

C-UAS systems are designed to detect various drones. In order to ultimately be able to compare them, it is necessary to define the requirements for test objects (UAS). This clause specifies which parameters should be measured and specified for test objects in order to compare the capabilities of the C-UAS.

In order to be able to compare different C-UAS tested in different environmental conditions, it is necessary to measure them (temperature, wind force, air humidity, electromagnetic background, etc.). Parameters to be measured and methods of measurement are described in subclause 10.5.7.

Since the measurements will take place in different places, it is also necessary to take into account the parameters related to the test site (degree of urbanization, afforestation, uneven terrain, etc.). The deployment area of the C-UAS sensors must be taken into consideration (e.g. predefined area for RF sensors, Radars etc.). To compare different systems the exact position, their height and also the number of sensors have to be taken into account.

The target effect of the measurements during the tests will be to determine the quality parameters of the C-UAS operation (speed range of detected objects, number of objects detected simultaneously, time from the appearance of the UAS to its detection, etc.).

An important factor, as mentioned earlier, that should be considered when conducting tests is also how the UAS will appear in the field of view of the C-UAS (distance, way of flying, hiding behind an object, etc.). Testing requirements must be defined in order to be able to compare test results for different C-UAS.

10.5.3 Environmental conditions

The table lists the environmental conditions measured when testing the C-UAS systems. This allows for objective testing in similar conditions, which has a significant impact on the operation of devices included in the C-UAS systems. The measured parameters were divided into 3 parts. The first is meteorological conditions (determined on the basis of the Manual on Automatic Meteorological Observing Systems at Aerodromes), the second is electromagnetic conditions, and the third is acoustic conditions. For all conditions, the accuracy with which the measurement should be carried out is given.

Table 37 — Environmental conditions

No.	Type of conditions	Sub no.	Parameter	Unit	MEASUREMENT RESULT
1. Specification of environmental conditions				
1.	Meteorological conditions	1.	Medium surface wind	Direction: ± 10° Speed: ± 0,5 m/s (1 kt) to 5 m/s (10 kt) ± 10% above 5 m/s (10 kt)	
		2.	Visibility	± 50 m to 600 m ± 10% between 600 m to 1 500 m ± 20% above 1 500 m	
		3.	The amount of cloud cover	± 1 okta	
		4.	The height of the cloud base	± 10 m (33 ft) to 100 m (330 ft) ± 10% above 100 m (330 ft)	
		5.	Air temperature and dew point temperature	±1°C	
		6.	Pressure value (QNH, QFE)	± 0,5 hPa	
		7.	Average wind measured at test altitude (drone or mast measurement)	Direction: ± 10° Speed: ± 0,5 m/s (1 kt) to 5 m/s (10 kt) ± 10% above 5 m/s (10 kt)	
		8.	Air temperature measured at the test altitude (measurement from the drone)	±1°C	
		9.	Water body temperature, if the scenario assumes its occurrence	±1°C	
		10.	Illuminance	± 3% (<10 000 lux) ± 4% (>10 000 lux)	
2.	Electromagnetic conditions	1.	The average intensity of the electromagnetic field in the considered frequency range (with no additional disrupting devices)	Power density S: ± 1 W/m2 Electric component E: ± 1 V/m Magnetic component H: ± 0,01 A/m	
		2.	The peak intensity of the electromagnetic field in the considered frequency range (with no additional disrupting devices)	Power density S: ± 1 W/m2 Electric component E: ± 1 V/m Magnetic component H: ± 0,01 A/m The frequency of the peak value of the	

				Power density S: ± 1 W/m2 Electric component E: ± 1 V/m Magnetic component H: ± 0,01 A/m electromagnetic field strength: ± 1 Hz	
		3.	Average intensity of the electromagnetic field in the considered frequency range (additional interference devices activated) * The frequency of the interfering signal must be convergent with the UAS operating frequency	Power density S: ± 1 W/m2 Electric component E: ± 1 V/m Magnetic component H: ± 0,01 A/m	
		4.	Peak electromagnetic field strength in the considered frequency range (additional disturbance devices activated) * The frequency of the interfering signal must be convergent with the UAS operating frequency	Power density S: ± 1 W/m2 Electric component E: ± 1 V/m Magnetic component H: ± 0,01 A/m The frequency of the peak value of the electromagnetic field strength: ± 1 Hz	
3.	Acoustic conditions	1.	Average sound level (no additional jamming devices)	Average sound level: ± 1 dB	
		2.	Peak sound level and frequency at which it occurs (no additional jamming devices)	Peak sound level: ± 1 dB The frequency of the peak sound level: ± 1 Hz	
		3.	Average sound level (additional jamming devices activated) * The jamming signal frequency must be convergent with the UAS operating frequency	Average sound level: ± 1 dB	
		4.	Peak sound level and frequency at which it occurs (additional jamming devices activated) * The jamming signal frequency must be convergent with the UAS operating frequency	Peak sound level: ± 1 dB The frequency of the peak sound level: ± 1 Hz	

10.5.4 Test object specification (UAS)

In order to be able to compare different C-UAS, it is necessary to specify the parameters of the test objects (UAS) that these systems will detect. The lack of unification in this respect means that the test results for different test objects will be incomparable.

Different detection technologies measure different kinds of physical quantities to detect UAS. For example, for the currently most widespread detection technology, microwave radars, the parameter that will be responsible for the possibility and quality of detection will be radar cross section (RCS). Since it is very difficult to determine this parameter before the measurement, one of the parameters that make up the RCS was adopted for the purposes of this study - the area occupied by the UAS when viewed from above.

Similarly for other detection technologies it is necessary to compare for different UAS used during testing:

- grey level of the UAS colour – for detection systems using daytime cameras,
- UAS surface emissivity and UAS temperature during launch - for detection systems using thermal imaging cameras and for thermal imaging radars,
- the maximum volume of the UAS (measured at a distance of 1m from the object) and the frequency with the highest volume - for acoustic detection systems.

For passive systems that use monitoring of the frequency on which the UAS communicates with the pilot for detection, it will be important on what frequency the communication takes place and what communication protocol is used in it.

All these parameters are listed in the table below.

Table 38 — Test object specification (UAS)

2 Specification of the test object - UAS				
No	Parameter	Unit	Remarks	MEASUREMENT RESULT
1	UAS height	m		
2	Diameter (diameter of the smallest circle into which the test object can be entered)	m		
3	UAS weight	g		
4	Equivalent Radar Cross Section (RCS) calculated by the product of the height and diameter	m^2		
5	Surface colour converted to grayscale	%		
6	Surface emissivity (measurement with a thermal camera)	W/m^2 Hz		
7	The maximum volume of sound generated by the UAS	dB	Measured at a distance of 1 m from the UAS	
8	The frequency at which the sound is at its maximum	Hz		

9	The frequency at which the UAS communicates with the operator	Hz		
10	Type of wireless communication (communication protocol) between the UAS and the operator	description		
11	For a swarm of drones, the amount that can work at the same time	pcs.		

10.5.5 Ways of conducting tests

This subclause presents diverse methodologies employed in the evaluation of Counter-Unmanned Aircraft Systems (C-UAS). It provides a detailed exploration of various parameters and scenarios that facilitate a comprehensive understanding of how C-UAS systems respond to different conditions and challenges.

Table 39 serves as a structured guide, outlining specific parameters and their corresponding sub-categories. These parameters play a crucial role in simulating real-world situations, allowing for a thorough examination of the capabilities and limitations of C-UAS technologies.

Some key parameters presented in the table:

- **Flight Direction:** Explore scenarios where drones approach the system, move across it, follow mixed patterns, or move away from the system.
- **Additional Drone Inclusion:** Consider how the introduction of another drone during testing impacts the system's performance.
- **Flight Patterns:** Address different flight patterns based on end-user requirements.
- **Starting Point of Drones:** Examine scenarios where drones start from various positions, such as out of field of view (FOV), behind obstacles, or without any obstacles.
- **Cooperation with a Falconer:** Evaluate the system's response when a falcon enters the flight zone, conducting differentiation tests.
- **Cooperation with Jamming Systems:** Assess the system's performance in the absence of interference, with various disruptive technologies activated, or in a noisy environment.
- **Buildings in Flying Zone:** Explore flights behind different obstacles like buildings and trees to test the system's ability to track drones.
- **Checking Systems' FOV (Angles):** Investigate flights from one FOV limit to another, both horizontally and vertically, to understand when the drone is detected or lost by the DTI system.
- **Tests with Systems' Operator Participation:** Evaluate scenarios with no operator (autonomous system) or with one operator.
- **Flights on Different Ranges of Technologies:** Test the system's performance at minimum, medium, maximum, and above-maximum ranges, as well as through the full range to check for any limitations.
- **Tests Near Warm Objects:** Examine the system's performance in detecting drones near warm objects like architectural structures, chimneys, or simulators.
- **Detection of Drones' Reflections from Water Surface:** Assess the system's ability to classify reflections from water surfaces as drones.
- **Detection of Drones' Reflections from Glass Surface:** Evaluate the system's response to reflections from glass surfaces, such as buildings.

This subclause aims to provide a comprehensive guide for conducting tests that mimic real-world scenarios, offering valuable insights into the effectiveness and adaptability of C-UAS systems across a spectrum of operational conditions.

Table 39 — Parameters for ways of conducting tests

3. Ways of conducting tests				
No.	**Parameter**	**Sub no.**	**Description**	**CHOOSE MOST ACCURATE DESCRIPTION**
1.	Flight direction	1.	Towards the system.	
		2.	Across the system.	
		3.	Not defined.	
		4.	Mixed.	
		5.	Moving away from the system.	
2.	Adding another drone to the test	1.	Towards the system.	
		2.	Across the system.	
3.	Flight pattern (if there is a need from the end user, add patterns)	1.		
4.	Place of drone start	1.	Out of FOV.	
		2.	In FOV - from behind a terrain obstacle.	
		3.	In FOV - from behind a building.	
		4.	In FOV - from behind a tree.	
		5.	In FOV - without any obstacles.	
5.	Cooperation with a falconer, differentiation tests	1.	None.	
		2.	Falcon entering the flight zone.	
6.	Cooperation with jamming systems	1.	None (tests in quiet area).	
		2.	Station disrupting various technologies activated.	
		3.	Tests in a noisy environment (lawn mower / jackhammer / blower).	
7.	Buildings in flying zone	1.	None.	
		2.	Flights behind buildings to check if the DTI system loses the drone.	
		3.	Flights behind the tree to check if the DTI system loses the drone.	
		4.	Flights behind trees/ forest to check if the DTI system loses the drone.	

8.	Checking systems' FOV (angles)	1.	Flights from one FOV limit to another (right - left) to see when the drone is detected and when it is lost by the DTI.	
		2.	Flights from one FOV limit to the other (up and down) to see when the drone is detected and when it is lost by the DTI.	
9.	Tests with systems' operator participation	1.	No operator (the system works autonomously).	
		2.	One operator.	
10.	Flights on different ranges of different technologies	1.	Minimum for technology.	
		2.	Medium technology range.	
		3.	Maximum for technology.	
		4.	Above the maximum for technology.	
		5.	Flights from the minimum to the maximum range of the technology to check if the DTI system loses the drone.	
11.	Tests near warm objects (architectural objects, chimneys, simulators)	1.		
12.	Tests of detection of drones' reflections from water surface (checking if this reflection is classified as a drone)	1.	Flights above water.	
		2.	None.	
13.	Tests of detection of drones' reflections from glass surface e.g., building (checking if this reflection is classified as a drone)	1.	Flight near a glass building.	
		2.	None.	

10.5.6 Specification and equipment of the test site

The table below summarizes the parameters to consider when evaluating a test site. The degree of urbanization, topography or vegetation are factors that can make C-UAS operation more difficult or easier. In order to be able to compare different systems, it is necessary to take these parameters into account. Considering the factors contained in the table will allow in the future, based on tests, to select the appropriate system for a specific facility with characteristic terrain factors.

The table also includes information on equipping the test site with equipment to simulate various weather conditions and factors that hinder the operation of the C-UAS.

Table 40 — Specification and equipment of the test site

4. Specification of the test site

No.	Parameter	Sub No.	Description	CHOOSE MOST ACCURATE DESCRIPTION
1.	Type of terrain including radio interference	1.	Rural, sparsely urbanized area, forests or fields.	
		2.	Suburban area, moderately urbanized.	
		3.	Urban area with a high degree of urbanisation.	
		4.	Area near the industrial plant.	
		5.	The site in the vicinity of a power plant, power station or transmission line.	
		6.	The area in the vicinity of a radio broadcasting station or radar station.	
		7.	Land near the BTS station.	
2.	Type of terrain in terms of topography	1.	Flat terrain (terrain unevenness below 1m).	
		2.	Uneven terrain (uneven terrain from 1m to 10m).	
		3.	Hilly terrain (uneven terrain from 10m to 100m).	
		4.	Mountainous terrain (uneven terrain over 100m).	
		5.	A river with a width of more than 5 m or a water reservoir with an area of more than 10.000m².	
3.	Buildings in the test site	1.	Individual buildings on the test site (up to 3	

			buildings with a height of up to 6 m on the test site).	
		2.	Buildings on the test site (over 3 buildings up to 6m high or buildings higher than 6m, industrial plants, industrial structures, e.g., masts, poles).	
		3.	Built-up area (village with more than 10 houses or a city).	
4.	Vegetation in the test site	1.	Open area (no trees).	
		2.	Individual trees in the test site (tree density does not obscure UAS).	
		3.	Partially wooded area (there are places in the test site with groups of trees covering the UAS.	
		4.	Wooded area (in the test area there is a border of forest cover obscuring the incoming UAS).	
5.	Equipping the test site with radar jamming stations or devices			
6.	Equipping the test site with devices that disrupt or hinder the operation of systems using frequency monitoring (including devices that use Wi-Fi connectivity to disrupt systems using Wi-Fi fingerprint technology)			
7.	Equipping the test site with devices that disrupt the operation of acoustic systems			
8.	Possibility to use birds (falconer) to test the recognition of bird drones by C-UAS systems			
9.	Terrain map with ranges for different C-UAS technologies			

10.5.7 Testable parameters for detection, tracking and identification

Below is a list of testable parameters. The parameters are included in 3 tables for detection (Table 41), tracking (Table 42) and identification (Table 43) and divided into parameters resulting from the characteristics of the system and parameters measured during tests. Such definition of parameters will allow for an objective assessment of the technical capabilities of the C-UAS and its effectiveness. Testable parameters include, among others, the system response time to an emerging threat, determining the maximum and minimum operating ranges, the ability to track UAS and transfer it in the manner expected by the operator, and the ability to identify UAS in detail.

10.5.7.1 Detection

Table 41 — Testable parameters for detection

5. Specification of parameters to be measured - DETECTION					
	No.	Types of parameters	Sub no.	Parameter	Unit	CHOOSE MOST ACCURATE DESCRIPTION

	No.	Types of parameters	Sub no.	Parameter	Unit	CHOOSE MOST ACCURATE DESCRIPTION
Detection	1.	Parameters resulting from the characteristics of the system	1.	Time when an object was detected by a given detection system	s	
			2.	Time of displaying a detected object on the map	s	
			3.	Indication of coordinates of detected objects	Y/N	
			4.	Indication of UAS equivalent objects as distinct from birds	Y/N	
			5.	Detection of terrain obstacles in determining the alarm signal (manual mode/automatic mode)?	Y/N	
			6.		manually/ automatically	
			7.		3D/2D	
			8.	Defined minimum speed of the detected object	m/s	
			9.	Defined maximum speed of the detected object	m/s	
			10.	Determining the minimum range of the technology used on map display	Y/N	
			11.	Determining the maximum range of the technology used on map display	Y/N	
			12.	Determination of detection angles (horizontal and vertical)	Y/N	
			13.	Determination of the camera rotational speed (detection)	deg/s	
			14.	Determination of the current field of view angles of the VIS camera, dynamically regarding focus and zoom	Y/N	
			15.	Determination of the current field of view angles of the IR camera, dynamically regarding focus and zoom	Y/N	

			16.	Indication of the frequency of refreshing the UAS location on the map of the operator's system	Y/N	
			17.	Indication of the dominant technology determining the coordinates	Y/N	
			18.	Does the system have a Laser Rangefinder for determining distances?	Y/N	
			19.	The frequency of refreshing the UAS position on the operator's map	Hz	
			20.	Detection of the second object or group of objects appearing in the detection field	Y/N	
			21.	Whether the system is able to determine the UAS-operator communication channel	Y/N	
			22.	Continuity of assigning events to one object when detection is lost	Y/N	
2.		Parameters measured during tests	23.	System detection time (time when an object flying into the zone was detected)	s	
			24.	Signalling time at the detection operator station		
			25.	Coordinates of the detected object	Y/N	
			26.	Measurement of the minimum speed of the detected UAS	m/s	
			27.	Measurement of the maximum speed of the detected UAS	m/s	
			28.	Measurement of the minimum UAS detection distance	m	
			29.	Measurement of the maximum UAS detection distance	m	
			30.	Compliance of the obtained detection ranges with the requirements of the scenario		

			31.	Compliance of the UAS flight speed with the requirements of the scenario		
			32.	Measure the frequency of refreshing the UAS position on the operator's map	Hz	
			33.	Determine the method of communication between the UAS and the operator		
			34.	The maximum number of objects to be detected	pcs.	

10.5.7.2 Tracking

Table 42 — Testable parameters for tracking

				5. Specification of parameters to be measured - TRACKING		

	No.	Type of parameters	Sub no.	Parameter	Remarks	CHOOSE MOST ACCURATE DESCRIPTION
Tracking	1.	Parameters resulting from the characteristics of the system	1.	Is a given technology able to track, follow quickly moving objects?		
			2.	Does the system specify the minimum speed of a detected and tracked object?		
			3.	Does the system determine the maximum trackable speed of a detected object?		
			4.	Does the system indicate the target's speed as it travels from/to and across the detection zone?		
			5.	Does the system graphically visualize the object's flight path?		
			6.	Does the system indicate the coordinates of the object's flight path?		
			7.	Does the system measure object tracking time?		
			8.	Does the system lose the target behind the terrain obstacle?		
			9.	Determination of tracking angles (horizontal and vertical)		

2.	Parameters measured during tests		13.	Measurement of refreshing the UAS location on the operator system map during tracking		
			15.	Does the technology track two or a group of objects?		
			1.	Measurement of the minimum speed of a tracked object		
			2.	Measurement of the maximum speed of a tracked object		
			3.	Measurement of the speed of the tracked object in flight from / to and across the detection zone		
			4.	Measurement of the minimum tracking distance of an object		
			5.	Measurement of the maximum tracking distance of an object		
			6.	Measurement of the maximum imaging distance of the object		
			7.	Visualisation of the object's flight path		
			8.	Coordinates of the object's flight path		
			9.	Determine the tracking time of the object	min/max	
			10.	Check if the system loses the target flying behind the terrain obstacle, the building, the electromagnetic and acoustic influence zone		
			11.	Is the rediscovered (lost from tracking) object indicated as new or old?		
			12.	Measure the above parameters for the second detected object		
			13.	Check that the entry of the second UAS into the tracking zone of the first alters system operation		
			14.	Specify the maximum number of tracked objects	individually/collectively, automatically/manually	

10.5.7.3 Identification

Table 43 — Testable parameters for identification

5. Specification of parameters to be measured - IDENTIFICATION						
	No.	Type of parameters	Sub no.	Parameter	Unit	CHOOSE MOST ACCURATE DESCRIPTION
Identification	1.	Parameters resulting from the characteristics of the system	1.	Does the system measure UAS size?	Y/N, cm^2	
			2.	Does the system communicate with the UAS base?	Y/N	
			3.	Does the system have its own database?	Y/N	
			4.	Is the system able to recognize the UAS payload?	Y/N	
			5.	Is the system able to identify the UAS, taking into account the measured parameters?	Y/N	
			6.	Does the system identify UAS as a new object after the UAS enters the occluded zone and its reappearance?	Y/N, further description	
			7.	Can the system recognise non-commercial UAS?	Y/N	
	2.	Parameters measured during tests	1.	Specify the type, kind and name of the UAS (at maximum / minimum speed and different traffic directions)	description	
			2.	Identify the load carried by the UAS	Y/N	
			3.	Determine the coordinates of the UAS operator	Y/N	
			4.	Determine whether, after the UAS enters the occluded zone and its reappearance, identifies UAS as a new object	Y/N	
			5.	Specify the maximum number of objects to be identified	Y/N, further description	
			6.	Measurement of system response time from detection to identification	s	

			7.	UAS battery status visualisation (radio passive systems)	%	
			8.	UAS flight time visualisation (radio passive systems)	s	
			9.	Operator position information (radio passive systems)	coordinates	
			10.	Information on the type of UAS (radio passive systems)	description	
			11.	Information on the frequency and type of radio communication between the UAS and the operator	Hz/description	

11 C-UAS system evaluation framework

11.1 General

Based on the requirements and metrics previously defined in clause 9 and clause 10, an evaluation framework will be developed, which aim to provide a structured tool by which to systematically document, review, compare and evaluate test results.

This clause aims to present a common framework by which Member States working in coordinated, voluntary fashion can test and share data regarding the performance of different C-UAS systems with one another. The evaluation framework is intended to create a common baseline understanding amongst Member State authorities concerning the effectiveness of different C-UAS solutions, which in turn shall support decision-making at national level regarding the development, procurement and/or operational deployment of different systems.

The evaluation framework can be considered an ecosystem, since multiple factors are involved, many dependencies can lead to a success or a failure. The evaluation is not a matter of a single entity, not even of two entities (a company vs. the end user). As the expected outcome of the test could affect in the future the C-UAS applicability to a certain attack scenario in a certain operational environment at a specific time, it is important to make objective judgments based on qualitative and quantitative comparison between different counter-UAS tools.

The evaluation framework described in this clause was created considering the needed flexibility for the evaluation of different C-UAS systems, with different technical components, the multitude of usage scenarios for different interested stakeholders, the diversity of environmental context, etc. The framework is not intended to serve as an evaluation methodology targeting a specific C-UAS solution, but rather as an adaptable tool based on a scientific approach and the envisioned user expectations regarding the effectiveness of different C-UAS solutions, this being one of the major interests since most of the procurement will be from public funds where the best value for money is a major goal.

11.2 The Evaluation Framework

11.2.1 Fundamentals

An Evaluation Framework is a tool that presents a systematic and concise overview of the evaluation methodology and process. A well-thought-out Evaluation Framework can assist greatly with identifying the planned evaluation activities and help clarify the scope of the evaluation.

Generally, the Evaluation Framework supports communication between the evaluation team and the evaluation commissioners/clients. In this case, it will support the communication between Member State authorities (as potential buyers of C-UAS solutions) and the manufacturers of the technical systems. The Evaluation Framework as a tool links the evaluation objectives to areas of enquiry, detailed questions, data collection, to mention but a few. The Evaluation Framework is extremely important since it is used as an evidence trail, i.e., it demonstrates how evaluation activities will lead to producing evidence on the outcomes and impacts of an intervention. It is both a guide for the evaluation team prior to the evaluation as well as a checklist to be referenced during the evaluation. It should be noted that the evaluation methodology must be an iterative process, based on concrete data and information provided by manufacturers, respectively measurable and verifiable by users, in a very well-defined operating context. Through a consultative process, the evaluation team (potential buyers) will agree on the scope of each evaluation with the manufacturer (vendor).

The effectiveness of different C-UAS solutions requires an Evaluation Framework tailored to:

- the purpose for which the evaluation will be used (public tender, technology scouting, development, etc.);
- the intended audience of the evaluation (user profile, concept of operation);
- the types of activities (specific use cases);
- the scale and significance of these activities (qualification tests, acceptance tests, etc.).

The Evaluation Framework must be seen as a simple tool which helps the interested stakeholders to:

- organize the thinking and foreseen activities of the evaluation team;
- relate intervention activities to the expected results;
- set indicators/detailed questions that enable a thorough understanding of the scope of the evaluation;
- allocate responsibilities among the evaluation team and key stakeholders;
- communicate information on the evaluation from/to the key stakeholders.

The 1st step for the development of the Evaluation Framework, is the clear definition of the product/program/action to be evaluated (i.e., the intended short-, medium- and long-term outcomes, and the potential external factors that may affect the process and outcomes, constraints, causal linkages, the critical success factors, etc.). From the above process, the purpose, scope and use for the evaluation will be clarified.

The 2nd step is the definition of the evaluation type. There are three major types of evaluations with the following general specifications:

1. Evaluation based on questionnaires:
   a. The use of key/standard evaluation questions starting from the user requirements (i.e., Terms of References)
   b. identification of all types of information required to answer to the evaluation questions, including performance criteria and indicators;
   c. a clear determination of the methods for obtaining information on indicators is needed;
   d. data sources and methods must be clearly identified;
   e. judgement criteria must be clearly defined.
2. Evaluation based on results:
   a. identification of the expected results for the action being evaluated;
   b. development of detailed questions that will enable the assessment of the presence or lack of the expected results is mandatory;
   c. determination of methods for obtaining information on indicators is mandatory;
   d. data sources and methods must be clearly identified;

e. judgement criteria must be clearly defined.

3. Evaluation based on a thematic area;
    a. identification of the specific thematic area being evaluated;
    b. development of detailed questions that will enable the assessment of the contribution of the defined thematic areas;
    c. determination of methods for obtaining information on indicators is mandatory;
    d. data sources and methods must be clearly identified;
    e. judgement criteria must be clearly defined.

The 3rd step is the definition of the evaluation matrix, which will be based on some template documents, filled in with the specific information some of which may include but are not limited to:

- Evaluation Question/Results/Thematic Area
- Detailed Questions
- Evaluation methods/tools
- Evaluation Criteria
- Value Judgement
- Roles and responsibilities
- Timeline
- Budget
- Assumptions/Risks and Mitigation measures

The 4th step is the definition of the evaluation conclusions, which will include also a detailed explanation of the key findings, including also a SWOT analysis. This tool will be further used for additional evaluations between different solutions. The used evaluation criteria and the field test values will be included also in the document.

There are some key elements with direct impact for a good evaluation framework:

- It must be developed through a consultative process;
- It must describe in detail the scope of the evaluation, including the target group, expectations, use cases, requirements, etc.;
- It must describe in detail the methodological approach of the evaluation, including the evaluation questions, the performance criteria and indicators, the type of data to be collected, how data will be collected, analysed and interpreted, and who will be involved in the evaluation process.
- It must consider the context of the activity (including for instance the constrains, the political, social, economic or cultural contexts) in order to understand how this has affected the process and the outcomes of the evaluation.

Taking into consideration the expected outcomes of this document, the vast field of technological and functional C-UAS systems, the case for the use of drones for malicious purposes, operating contexts and types of missions, the wide range of manufacturers, ensuring impartiality towards different manufacturers, as well as a quantifiable measurement of results, resulted the following evaluation methodology, described below.

11.3 Evaluation methodology

11.3.1 General

For the evaluation methodology, it is proposed the following structure.

1	**Purpose of the evaluation** Key Stakeholders Purpose and Focus Stakeholder Needs
2	**Background and context** Considerations Evaluation Context Goal & Objectives Participatory Approach
3	**The Evaluation Plans** Approach to Evaluation The Evaluation Plan
4	**Evaluation Questions** Considerations Finalized Questions
5	**Data Collection** Data Collection Plan Questionnaires based data Field test-based data Managing Potential Ethical Issues
6	**Data Management** Data Management Plan
7	**Data Synthesis, Judgments, and Conclusions** Approach to Data Synthesis Forming Judgments Reaching Conclusions Feedback and follow-up
8	**Reporting and Dissemination plan**

11.3.2 Purpose of the evaluation

Key Stakeholders
The first step to write the evaluation plan is to decide which stakeholders to include. Stakeholders are consumers of the evaluation results. As result users, they will have a vested interest in the results of the evaluation. In general, stakeholders are those who are: 1) interested in the action and would use evaluation results (such as clients, community groups, officials); 2) those who are involved in running the evaluation, such as (staff, partners, management, the funding source); and 3) those who are benefit by the final results (the general public). Others may also be included as these categories are not exclusive. Stakeholders in an evaluation can have many benefits. In general, stakeholders

include people who will use the evaluation results, support or maintain the evaluation action, or who are affected by the activities or evaluation results.

Table 44 — Stakeholder Mapping Matrix

Stakeholder	Focus and scope	Key role in the evaluation action	Key role in the plan drafting	Key role in evaluation tests/questionnaires	Key role in evaluation judgements, conclusions	Key role in evaluation reporting and dissemination
A						
B						
……..						

An overview of key stakeholders and their roles is presented below:

- **Government Agencies:**
  - Regulatory Oversight: Government agencies are responsible for regulating the use of C-UAS systems and ensuring compliance with relevant laws and regulations.
  - Procurement: Some government agencies may procure C-UAS systems for their own use, such as for security or defence purposes.
  - End-User: Government entities may also serve as end-users of C-UAS systems in protecting critical infrastructure and public safety.

- **C-UAS Manufacturers and Developers:**
  - System Development: Manufacturers and developers create and innovate C-UAS technologies and solutions.
  - Testing and Validation: They may participate in testing and validation of C-UAS systems to ensure their efficacy.
  - Compliance: Manufacturers must ensure their products comply with legal and regulatory standards.

- **Independent Evaluators and Experts:**
  - Assessment: Independent experts are often engaged to conduct third-party evaluations of C-UAS systems, providing impartial assessments.
  - Research and Development: They may contribute to research and development efforts to advance C-UAS technologies and evaluation methodologies.
  - Validation: Independent evaluators validate the performance and effectiveness of C-UAS systems to enhance transparency and credibility.

- **End-Users (e.g., Security Agencies, Military, Critical Infrastructure Operators):**
  - Operational Deployment: End-users are responsible for deploying and operating C-UAS systems to protect critical assets and facilities.
  - Feedback: They provide feedback on the usability, performance, and effectiveness of C-UAS systems in real-world scenarios.
  - Compliance: End-users ensure that their C-UAS deployments comply with regulatory and legal requirements.

- **Regulatory Bodies and Compliance Organizations:**
  - Standard Setting: These organizations contribute to setting standards and best practices for C-UAS technology and operation.
  - Compliance Verification: They may verify that C-UAS systems adhere to established standards and regulations.
  - Advisory Roles: Regulatory bodies provide guidance on the lawful and ethical use of C-UAS systems.

- **Academic and Research Institutions:**
  - Research and Development: Academic institutions conduct research and contribute to the development of C-UAS technologies and methodologies.
  - Education and Training: They may provide education and training for C-UAS operators and professionals.

- **Public and Community Representatives:**
  - Advocacy and Awareness: These stakeholders may advocate for public awareness and education regarding the use of C-UAS systems and their potential impact on communities.
  - Liaison with Authorities: They act as intermediaries between the public and relevant authorities, conveying concerns and feedback related to C-UAS usage.

- **Commercial and Private Operators:**
  - Non-Military End-Users: Operators of C-UAS systems in commercial and private sectors play a role in providing feedback and input into the evaluation process.
  - Regulatory Compliance: They ensure that their C-UAS operations comply with legal and regulatory requirements.

- **Law Enforcement Agencies:**
  - Operational Use: Some law enforcement agencies use C-UAS systems for law enforcement and public safety.
  - Evaluation Input: Law enforcement agencies may provide input based on their experiences with C-UAS technologies.

- **Local and National Governments:**
  - Regulation and Oversight: Governments at various levels are responsible for regulating and overseeing the use of C-UAS systems within their jurisdictions.
  - Public Policy: They set public policy and guidelines for the responsible and lawful operation of C-UAS systems.

- **Privacy Advocacy Groups:**
  - Advocacy and Education: These groups advocate for privacy rights and may provide input on the privacy implications of C-UAS usage.
  - Policy Influence: They may seek to influence policies related to C-UAS system usage in relation to privacy concerns.

The involvement of these diverse stakeholders ensures a comprehensive and balanced evaluation process for C-UAS systems. Their collective input helps shape the evaluation framework, address regulatory compliance, and promote responsible and effective use of C-UAS technologies.

Purpose and Focus

Here must be included brief statement, regarding the evaluation scope. Why is needed? It has to describe why the evaluation is needed (i.e., market consultation, public tender, qualification, marketing activity, research, TRL demonstration, etc.). A shared understanding of what the evaluation can and cannot deliver is essential to the success of implementation of evaluation activities and the use of evaluation results. The stakeholders must agree upon the logic model and the purpose(s) of the evaluation. Understanding the purpose of the evaluation and the rationale for prioritization of evaluation questions and activities is critical for transparency and acceptance of evaluation findings. It is essential that the evaluation address those items of greatest interest and the priority for the users of the evaluation.

The purpose and focus of the C-UAS (Counter-Unmanned Aircraft Systems) evaluation framework may be as follows:

- Assessment of C-UAS Effectiveness: The primary purpose of the framework is to systematically assess the effectiveness of C-UAS systems in countering unauthorized unmanned aircraft threats. It aims to determine how well these systems can detect, track, and identify potential threats to critical infrastructure, public safety, and privacy.

- Informed Decision-Making: The primary purpose of the framework is to provide stakeholders, including government agencies, end-users, manufacturers, and regulatory bodies, with the necessary information to make informed decisions regarding the development, procurement, and operational deployment of C-UAS systems.

- Promotion of Transparency and Accountability: Another purpose is to promote transparency in the evaluation process, ensuring that results are unbiased and can be trusted by all stakeholders. This transparency enhances accountability for C-UAS systems' performance and compliance with regulations.

- Legal and Ethical Compliance: The framework serves the purpose of assessing the legal and ethical compliance of C-UAS systems. It helps ensure that these systems are used within the boundaries of relevant laws, regulations, and ethical considerations.

- Continuous Improvement: The framework facilitates continuous improvement in C-UAS technology by identifying areas for enhancement. It supports the evolution of C-UAS systems to address emerging challenges and evolving UAS threats effectively.

Stakeholder Needs

Here must be included a short description of stakeholder needs, as general statements for definition of the evaluation context idea. Which are the general needs? It has to define for what the evaluation is done (i.e., a border authority which was previously defined as a stakeholder has to evaluate a C-UAS solution needed for the protection of a seashore, against the use of drones for smuggling). Also, this clause will describe the stakeholders' needs during the entire evaluation cycle, from drafting the evaluation framework, to managing findings and reporting.

Table 45 — Evaluation Framework

Stage	Required Areas of Knowledge and Understanding
Initial Orientation	
Developing the Framework	
Implementing the Framework	
Managing findings and reporting	

Understanding these diverse stakeholder needs is essential to develop an evaluation framework that serves the interests of all parties involved and ensures responsible, effective, and ethical use of C-UAS systems:

- **Government Agencies:**
  - Security and Public Safety: Government agencies need to ensure the security and safety of their citizens, critical infrastructure, and sensitive sites.
  - Data Protection: Government agencies need to safeguard sensitive data and ensure data protection while countering UAS threats.

- **C-UAS Manufacturers and Developers:**
  - Product Development: Manufacturers need feedback to enhance their C-UAS systems, improve their effectiveness, and stay competitive.
  - Regulatory Compliance: They need clear evaluation criteria to ensure their products comply with legal and regulatory requirements.
  - Market Understanding: Feedback helps them understand the market's needs and challenges better, guiding their research and development efforts.

- **Independent Evaluators and Experts:**
  - Data and Metrics: They require access to reliable data and well-defined evaluation metrics to conduct thorough assessments.

- **End-Users (e.g., Security Agencies, Critical Infrastructure Operators):**
  - Effective Defence: End-users need to know if the C-UAS systems they deploy are capable of effectively countering UAS threats.
  - Operational Feedback: They seek insights into how well the system works in real-world scenarios and how to optimize its performance.

- **Regulatory Bodies and Compliance Organizations:**
  - Regulatory Oversight: Regulatory bodies need evaluation results to create and enforce regulations that govern C-UAS system usage.
  - Standards Development: They use insights to develop and update industry standards and best practices.

- **Academic and Research Institutions:**
  - Education and Training: They require information to develop educational programs and training courses related to C-UAS systems.

- **Public and Community Representatives:**
  - Transparency and Accountability: They need transparent evaluation results to ensure that the use of C-UAS systems aligns with public interests and values.

- **Commercial and Private Operators:**
  - Operational Feedback: Operators need to know how C-UAS systems perform in various operational scenarios to optimize their usage.

- **Law Enforcement Agencies:**
  - Effective Operations: Law enforcement agencies need to ensure the effectiveness of C-UAS systems in addressing security and public safety challenges.

- **Local and National Governments:**
  - Public Safety: They need assurance that C-UAS systems are used to enhance public safety and protect critical infrastructure.

- **Privacy Advocacy Groups:**
  - Privacy Protection: These groups seek to protect privacy rights and need insights into the privacy implications of C-UAS technology.

11.3.3 Background and context

Considerations

A description of the general problem which must be solved. The stakeholders must agree from the beginning about the nature of the problem or goal, who is generally affected, how big is the problem and whether and how is changing. For instance, if a Law Enforcement Agency, specialized in the protection of high rank dignitaries, has the intention to implement a C-UAS solution in its daily operations, here must be mentioned some general consideration regarding the nature of the problem. The information is needed for the other stakeholders involved in the evaluation to fully understand the problem which must be solved. Relevant drone incidents and gap analysis could be included as explanatory notes.

Evaluation Context

This clause must contain introductory explanations about the evaluation context. They describe what the evaluation has to accomplish to be considered successful. For most programs, the accomplishments exist on a continuum (first, the aim is to accomplish X... then, to do Y...). Therefore, they should be organized by time ranging from specific (and immediate) to broad (and longer-term) consequences. The description of the evaluation's context also considers the important features of the environment in which operates. This includes understanding the activity field, geography, social and economic conditions, and also what other organizations have done. A realistic and responsive evaluation is sensitive to a broad range of potential influences. An understanding of the context lets users interpret findings accurately and assesses their generalizability. For example, a C-UAS system to protect a government building in an inner-city neighbourhood might have been a tremendous success for a LEA, but would likely not work in open space environment, without significant changes. Relevant concept of operation must be mentioned here.

Goal & Objectives

Developing clear goals and objectives will help you to clarify problems, issues and opportunities. Goals are general guidelines that explain what you want to achieve, and they are usually long-term and represent the global vision. The goals must be defined based on the user profile (i.e., LEA, critical infrastructure administrators, airport operators, border authority, prisons administrators, etc.). Goals will not be achieved if they exist in a vacuum or compete with other user goals. For instance, UAS threat mitigation has a far greater chance for success when its goals are effectively integrated into other community goals. Combining goals in this manner can lead to a "win-win" situation where everyone benefits. The following goals are mentioned as examples.

Table 46 — Goals

#	Goals	Notes
G1	*Protect the life and health of persons carrying out activities in a critical infrastructure, against malicious use of UAS.*	
G2	*Provide adequate warning in case of malicious use of UAS against the protected area.*	
G3	*Provide adequate response and mitigation actions against the UAS attacks.*	
G4	*Maintain the essential services provided by the critical infrastructure.*	
G5	*Enhance the community security.*	
G6	*Raise the citizens awareness.*	
....		

Objectives define strategies or implementation steps to attain the identified goals. Unlike goals, objectives are specific, measurable, and have a defined completion date. They are more specific and outline the "who, what, when, where, and how" of reaching the goals. Plans and actions based on clear goals and objectives are more likely to succeed in meeting the user needs. Objectives are developed

to help achieve goals by dividing them into manageable components. For example, "Protect the life and health of persons carrying out activities in a critical infrastructure, against malicious use of UAS" would be a goal. A supporting objective could be "installation of a system for detecting, identifying and neutralizing the UAS threat in an urban environment." This objective establishes an action that will lead to the protection of life or health, as described in Goal 1. Successful completion of multiple objectives is needed for each individual goal. Some objectives may themselves have components that can be expressed as "action steps," but it is vital to eventually identify in the plan all the details that will guide and encourage concrete actions to be taken.

The following objectives are mentioned as examples:

Table 47 — Objectives

#	Objectives	Observations
O1	*Installation of a system for detecting, identifying and neutralizing the UAS threat in an urban environment, for the protection of the Ministry of Foreign Affairs building.*	
O2	*The C-UAS system components will be installed on the infrastructure related to the protected objective, without other major additional construction works.*	
O3	*The C-UAS system detects and identifies all rotary UAS flights in the surrounding area of the building, from a specific distance.*	
O4	*The C-UAS system automatically alerts the security personnel for all detected UAS, within an appropriate time frame.*	
O5	*The C-UAS system automatically provides adequate neutralization measures.*	
….		

The evaluation framework must be developed through a participatory approach, for all the involved stakeholders, since it demonstrates how evaluation activities will lead to producing evidence on the outcomes. Common understanding and considering the priorities and concerns of all different stakeholders impact the evaluation planning, communication strategies during and after the evaluation and support the utilization of evaluation findings. Stakeholders are people or organizations that have something to gain or lose from what will be learned from an evaluation, and also in what will be done with that knowledge. Evaluation cannot be done in isolation. Almost everything involves partnerships - alliances among different organizations, board members, those affected by the problem, and others. Therefore, any serious effort to evaluate C-UAS systems must consider the different values held by all partners. Stakeholders must be part of the evaluation to ensure that their unique perspectives are understood. When stakeholders are not appropriately involved, evaluation findings are likely to be ignored, criticized, or resisted. However, if they are part of the process, they are likely to feel the ownership for the evaluation process and results. They will probably want to develop it, defend it, and make sure that the evaluation really works.

11.3.4 The evaluation plans

As the evaluation aims to assess the appropriateness, effectiveness, efficiency, impact and sustainability of a C-UAS solution, before starting the activities, the entire group should be very clear about the answers to the following questions:
1. What will be evaluated?
    Evaluation Goals: The goals of the evaluation must be clearly defined. These goals include assessing C-UAS effectiveness, ensuring regulatory compliance, and enhancing transparency and accountability.
    Goal Prioritization: The goals should be ranked based on their importance and relevance to stakeholders to provide a clear focus for the evaluation.

2. Which is the test approach?

Data Sources: The sources of data required for evaluations must be determined, including test scenarios, real-world simulations, historical data, and operational feedback.

Data Instruments: This includes the data collection instruments and tools necessary to gather relevant information during evaluations.

Existing Standards and Practices: An examination of the existing standards and best practices related to C-UAS technology and evaluation methodologies is mandatory in order to understand what is already in place and where there may be gaps.

3. Where and when the evaluation will take place?

Scenario Variations: To ensure the framework is robust, the entire group must account for different operational scenarios, environmental conditions, and UAS threat scenarios.

4. Who and what resources will be provided?

The resources may consist of budget, personnel, equipment, or materials, required for each activity.

5. What criteria will be used to judge program performance?

Performance Metrics: The key metrics and indicators that will be used to measure C-UAS performance will must be known. These include metrics related to detection accuracy, false alarm rates, response times, and tracking accuracy.

6. What standards of performance on the criteria must be reached for the evaluation to be considered successful?

Standardization: The metrics must be standardized to allow consistent and repeatable evaluations across different C-UAS systems.

7. What evidence will indicate performance on the criteria relative to the standards?

Benchmarking: Benchmarks and reference points will be established for comparing C-UAS systems against industry standards and operational requirements.

Transparency Measures: Reporting processes must ensure transparency in evaluation results and methodologies.

Accountability: Specific mechanisms must be defined to hold C-UAS manufacturers and operators accountable for the results of evaluations.

8. What conclusions about program performance are justified based on the available evidence?

The problem approach logic provides a structured framework for addressing the complex challenges related to C-UAS technology and ensuring that the evaluation framework serves its intended purposes effectively. It involves a collaborative and iterative process that engages stakeholders, respects ethical considerations, and promotes accountability and transparency. It typically helps identify and prioritize activities, allocate resources, and establish clear responsibilities. The evaluation framework, at the end, will give answers to all these questions and the first step from a participatory approach point of view is the definition of general aspects. In this respect, a planning matrix is a first key element.

Table 48 — Participatory planning matrix

Evaluation scope:	*As defined above*
Evaluation planning timeframe:	*The stakeholders will agree on the time period allocated for the entire evaluation, including the evaluation plan preparation, answers to the questionnaires and the field demonstrations.*
Field test demonstration date:	*The stakeholders will agree on the field test date.*
Alternative field test demonstration date:	*The stakeholders will propose also an alternative field test demonstration date.*

Field test demonstration location:	*The stakeholders will agree on the location for field tests*
Dissemination level	☐ PU: Public ☒ CO: Confidential for the involved stakeholders ☐ RE: RESTREINT UE (Commission Decision 2015/444/EC) *The stakeholders will agree on the dissemination level of the activities and outcomes (i.e. commercially confidential issues may arise)*
Status	☒ Draft ☐ Reviewed ☐ Finally reviewed ☐ Accepted

Stakeholder	Organization type	Role in the evaluation	Contact details	General activities	Allocated resources	Associated documents
A						
B						
....						

An iterative approach is necessary, in order for the framework to continually improve based on feedback and the results of testing.

> *General activities will describe the committed activities for each involved stakeholder. For instance, a LEA will specify the needs, explain the context, will prepare the questionnaire, will make available the test infrastructure, will participate in data collection and at the end will make data synthesis, judgments and formulate conclusions.*
> *Allocated resources – each involved stakeholder will mention the committed resources allocated for the evaluation. For instance, a C-UAS developer will mention here what products from his portfolio it will allocate, for how long and in which circumstances, how many technicians will be involved, what costs will be covered for the evaluation, etc.*
> *Associated documents – here it is useful to include relevant documents as a proof for the committed activities and resources (i.e. management declarations, support letters, availability statements, etc.).*

The next logic step in the evaluation framework is the description of the evaluation plan. A description clarifies the evaluation's activities, capacities, implementation context and steps. A shared understanding of what the evaluation can and cannot deliver is essential to the successful implementation of evaluation activities and use of evaluation results. Stakeholders must agree upon the logic model. This work will set the stage for identifying the evaluation questions and activities focusing the evaluation design, and connecting planning, testing and evaluation. A logic model may be used to succinctly synthesize the main elements of an evaluation program. While a logic model is not always necessary, a program narrative is. The evaluation program description is essential for focusing the evaluation design and selecting the appropriate methods.

The description section often includes a logic model to visually show the link between activities and intended outcomes. It is helpful to review the model and to ensure a shared understanding of the model and that the logic model is still an accurate and complete reflection of the evaluation. The logic

model should identify available resources (inputs), what the program is doing (activities), and what you hope to achieve (outcomes). It is important also the challenges and constraints (the program's context or environment).

Logic model elements should include:

- Inputs: data and resources necessary for the implementation
- Activities: the actual actions that the evaluation implements in order to achieve the outcomes
- Outputs: results obtained from the evaluation activities
- Outcomes (short-term, intermediate, long-term): the changes, impacts, or results of evaluation implementation (activities and outputs)

Inputs: *all information needed from all stakeholders in the evaluation context. They can be considered as deliverables in a project management approach.*

1. *User concept of operation (type of mission, threats, location, environment conditions, etc.)*
2. *User requirements (operational, legal, etc.)*
3. *Expected KPIs and acceptance criteria*
4. *Technical specification of the C-UAS system (detailed information for the technical components)*

Activities: *the description of all evaluation activities. The activities description and the responsibilities are mandatory for each item. Also, a Gantt chart is recommended.*

1. *Definition of the evaluation questions*
2. *Analysis of the answers to evaluation questions*
3. *Definition of the field test activities (test scenarios)*
4. *Definition of the measurements and data recording*
5. *Evaluation test execution*
6. *Data collection and management*
7. *Data synthesis, Judgments, and Conclusions*
8. *Reporting and dissemination*
9. *Evaluation management and logistics*

Outputs:

1. *Resulted input deliverables (user requirements, KPIs and acceptance criteria, etc.)*
2. *Activities deliverables (evaluation questions and answers, test scenarios, collected data, synthesis and conclusions)*

Outcomes:

1. *User satisfaction/rejection*
2. *Procurement preparation*

Table 49 — Outcomes

OUTPUTS	SHORT-TERM OUTCOMES	MEDIUM-TERM OUTCOMES	IMPACTS

11.3.5 Evaluation questions

In this step, it is important to solicit evaluation questions from the involved stakeholders, based on the stated purposes of the evaluation. The questions should then be considered through the lens of the logic model/program description. Evaluation questions should be checked against the logic model and changes may be made to either the questions or the logic model, thus reinforcing the iterative nature of the evaluation planning process.

The amount of information you can gather is potentially limitless. Evaluations, however, are always restricted by the number of questions that can be realistically asked and answered with quality, the methods that can be employed, the feasibility of data collection, and the available resources. The scope and depth of any evaluation is dependent on stakeholder priorities; available resources, including financial resources; staff and contractor availability; and amount of time committed to the evaluation. All evaluation staff should work together to determine the priority and feasibility of these questions and identify the uses of results before designing the evaluation plan.

This step facilitates conceptualizing what the evaluation can and cannot deliver. It is important to collaboratively focus the evaluation design with the identified purposes, context and logic model. Additionally, issues of priority, feasibility, and efficiency need to be discussed with the responsible for the implementation of the evaluation. Transparency is particularly important in this step. Stakeholders and users of the evaluation will need to understand why some questions were identified as high priorities while others were rejected or delayed.

In this part of the plan, the purposes of the evaluation, its uses, and the evaluation description to narrow the evaluation questions and focus the evaluation for improvement and decision making were applied. Useful evaluations are not about special research interests or what is easiest to implement, but about what information will be used by the stakeholders and decision makers to make decisions.

The questions are drafted by the end-users (i.e., a LEA which aims to assess a C-UAS solution in a given concept of operation). The evaluation needs to answer their specific questions. Users are the specific individuals (representing an organization) who will receive evaluation findings. They will directly experience the consequences of inevitable trade-offs in the evaluation process. For example, a trade-off might be having a relatively modest evaluation to fit the budget with the outcome that the evaluation results will be less certain than they would be for a full-scale evaluation. Because they will be affected by these trade-offs, intended users have a right to participate in choosing a focus for the evaluation. An evaluation designed without adequate user involvement in selecting the focus can become a misguided and irrelevant exercise. By contrast, when users are encouraged to clarify intended uses, priority questions, and preferred methods, the evaluation is more likely to focus on things that will inform (and influence) future actions.

Drafting questions encourages stakeholders to reveal what they believe the evaluation should answer. The process of developing evaluation questions further refines the focus of the evaluation. In this respect, for this evaluation stage, it was proposed the use of a centralized table with all evaluation questions based on the user requirements (defined in the previous activities), grouped

under 5 domains: appropriateness, effectiveness, efficiency, impact and sustainability. The answers will be later compared with the results measured or observed during the field tests or experiments.

Table 50 — Evaluation questionnaire

Domains	Evaluation questions	Evaluation answers
Appropriateness	Q1	
	Q2	
	Q3	
	.....	
Effectiveness	Q1	
	Q2	
	Q3	
	.....	
Efficiency	Q1	
	Q2	
	Q3	
	.....	
Impact	Q1	
	Q2	
	Q3	
	.....	
Sustainability	Q1	
	Q2	
	Q3	
	.....	

11.3.6 Data collection

Credible evidence is the raw material of a good evaluation. The information should be seen by stakeholders as believable, trustworthy, and relevant to answer their questions. This requires thinking broadly about what counts as "evidence." Such decisions are always situational; they depend on the question being posed and the motives for asking it. For some questions, a stakeholder's standard for credibility could demand having the results of a randomized experiment. For another question, a set of well-done, systematic observations or tests will have high credibility. The difference depends on what kind of information the stakeholders want and the situation in which it is gathered. In some situations, it may be necessary to consult also independent evaluation specialists. This may be especially true if concern for data quality is especially high. In other circumstances, LEA's operational personnel may offer the deepest insights. Regardless of their expertise, however, those involved in an evaluation should strive to collect information that will convey a credible, well-rounded picture of the evaluation program and its efforts.

Having credible evidence strengthens the evaluation results as well as the recommendations that follow from them. Although all types of data have limitations, it is possible to improve an evaluation's overall credibility. One way to do this is by using multiple procedures for gathering, analysing, and interpreting data. Encouraging participation by stakeholders can also enhance perceived credibility. When stakeholders help define questions and gather data, they will be more likely to accept the evaluation's conclusions and to act on its recommendations.

Sources of evidence in an evaluation may be people, documents, observations/measurements during tests. More than one source may be used to gather evidence for each indicator. In fact, selecting multiple sources provides an opportunity to include different perspectives and enhances the evaluation's credibility. For instance, an inside perspective may be reflected by internal documents and comments from staff or managers; whereas clients and those who do not support the program

may provide different, but equally relevant perspectives. Mixing these and other perspectives provides a more comprehensive view of the evaluation.

The criteria used to select sources should be clearly stated so that users and other stakeholders can interpret the evidence accurately and assess if it may be biased. In addition, some sources provide information in narrative form (for example, a person's experience when taking part in the program) and others are numerical (distances, time, etc.). The integration of qualitative and quantitative information can yield evidence that is more complete and more useful, thus meeting the needs and expectations of a wider range of stakeholders.

Quality of the data refers to the appropriateness and integrity of information gathered in an evaluation. High quality data are reliable and informative. It is easier to collect if the indicators have been well defined. Other factors that affect quality may include instrument design, data collection procedures, training of those involved in data collection, source selection, coding, data management, and routine error checking. Obtaining quality data will entail trade-offs (e.g., breadth vs. depth); stakeholders should decide together what is most important to them. Because all data have limitations, the intent of a practical evaluation is to strive for a level of quality that meets the stakeholders' threshold for credibility.

Quantity of the data refers to the amount of evidence gathered in an evaluation. It is necessary to estimate in advance the amount of information that will be required and to establish criteria to decide when to stop collecting data - to know when enough is enough. Quantity affects the level of confidence or precision users can have. It also partly determines whether the evaluation will be able to detect effects. All evidence collected should have a clear, anticipated use.

Logistics is an important aspect for data collection. The main components of logistics are the methods, timing, and physical infrastructure or equipment for gathering and handling evidence. All these must be detailed with the involved stakeholders and mentioned in the evaluation plan.

Data collection procedures should also ensure that confidentiality is protected.

Methods for Data Collection

1. Controlled Test Scenarios:

Purpose: Controlled test scenarios must be used in a controlled environment to assess specific aspects of C-UAS system performance.

Description: Controlled tests allow for the precise measurement of C-UAS capabilities under known conditions. These tests can involve stationary or moving UAS targets, varying altitudes, and different threat scenarios.

Examples: Controlled tests might involve drones equipped with different payloads (e.g., cameras, hazardous materials) to assess the system's ability to neutralize threats.

2. Field Testing in Realistic Environments:

Purpose: Field tests must be conducted in real-world environments to evaluate C-UAS systems under operational conditions.

Description: Field tests replicate scenarios that security forces or agencies might encounter in the field, including urban settings, critical infrastructure protection, and public events.

Examples: Field tests could involve the deployment of C-UAS systems at airports to evaluate their effectiveness in countering rogue drones near runways.

3. Simulation:

Purpose: Simulations should be used to assess C-UAS system performance in complex and potentially dangerous scenarios without real-world risk.

Description: Advanced computer simulations model various threat scenarios and environmental conditions. This approach enables the evaluation of C-UAS effectiveness and response strategies without physical equipment.

Examples: Simulations can assess the system's ability to counter multiple coordinated UAS threats or evaluate the impact of interference from other electronic devices.

4. User Experience Feedback:
Purpose: The feedback from end-users, operators, and system administrators will help the group assess the practical usability and human factors of C-UAS systems.
Description: Using surveys, interviews, or focus groups with individuals who have experience operating or interacting with the C-UAS system would result in gaining insights into usability issues, interface design, and operational challenges.
Examples: Collect feedback from military personnel, law enforcement officers, or security personnel who have used C-UAS systems in real-world situations.

Data Sources
1. Sensors and Instrumentation:
Install sensors, cameras, radar systems, and other specialized equipment on the C-UAS system to collect data during evaluations. These sensors provide real-time information on UAS detection, tracking, and neutralization.

2. Test Ranges and Facilities:
Collaborate with dedicated test ranges and facilities equipped with controlled environments for C-UAS testing. These facilities provide controlled airspace, test infrastructure, and safety measures.

3. Drone Fleet:
Maintain a fleet of drones, including different UAS types and sizes, to serve as targets during evaluations. These drones can be equipped with various payloads to simulate different threat scenarios.

4. Operational Data:
Collect data from operational deployments of C-UAS systems in real-world scenarios. This data can include reports of successful interceptions, false alarms, and system performance during actual incidents.

Data Collection Plan.
In this stage of the evaluation is very important to establish a procedural framework for data collection, to extract the right data, in the right format. Everything should be clearly stated from the beginning and be known to all parties involved. It is consider as relevant two data categories: data resulted from the answers to the question in the early stages of the evaluation and the data resulted from the field tests. All of them will offer the opportunity for a clear and impartial judgment. Data collection tools must be specified:

Table 51 — Data Collection Tools

	Questionnaires	**Field tests**
Purpose		
Focus		
Sampling		
Implementation		
Potential Ethical Issues		

Collected data must be later evaluated, using standard evaluation criteria, with well specified methods, responsibilities, and timings.

Table 52 — Evaluation of collected data

Evaluation criteria	Summary	Focus of Evaluation	Evaluation Method	Method Implementation	Who is Responsible	When
Appropriateness						
Effectiveness						
Efficiency						
Impact						
Sustainability						

Questionnaires based data.

The questionnaires filled with the answers will be the basis for the first stage of the evaluation.

Table 53 — Evaluation criteria

Criteria	Excellent	Good	Adequate	Poor	Justification
Appropriateness:					
1.					
2.					
3.					
.....					
Effectiveness:					
1.					
2.					
3.					
.....					
Efficiency:					
1.					
2.					
3.					
.....					
Impact:					
1.					
2.					
3.					
.....					
Sustainability:					
1.					
2.					
3.					
.....					

Field test-based data

The method or methods chosen for field evaluations must be in line with the questionnaires data and need to fit the evaluation question(s) and not be chosen just because they are a favoured method or specifically quantitative or experimental in nature. A misfit between evaluation question and method can and often does lead to incomplete or even inaccurate information. The method needs to be appropriate for the question in accordance with the evaluation criteria.

The field-based data must support the conclusions, so it is important to be accurate, correctly measured and stored, relevant for the tests and to validate the questionnaires-based data. In simple wording, the field test will demonstrate the answers to the questionnaires.

In this clause the following examples are presented:

EXAMPLE 1   TEST ENVIRONMENT

Coverage areas:

Monitoring area:
- o   Map of the monitoring area
- o   Horizontal and vertical coverage

Interdiction area:
- o   Map of the interdiction area
- o   Horizontal and vertical coverage

Environmental conditions:
- o   Scenario number
- o   Location name
- o   GNSS coordinates of sensors
- o   Describing the weather (e.g., sunny, rainy, foggy, clear or cloudy)
- o   Describing the ground (e.g., dry, wet, snow covered)
- o   Average air temperature
- o   Average wind speeds
- o   Average wind direction
- o   Air humidity
- o   Noise level
- o   Description of the surrounding obstacles and height profile of the test area (e.g., buildings, other antennas, cars, fences, powerlines, metallic reflectors)
- o   Pictures from each cardinal point

C-UAS system configuration:
- o   *System hardware configuration:*
- -   System type
- -   Hardware version
- -   Sensors type
- o   *System software configuration:*
- -   Software version
- -   Firmware version

UAS configuration:
- o   Drone class, type and version
- o   Drone firmware
- o   Available telemetry data
- o   Drone downlink/uplink output power
- o   Drone downlink/uplink bandwidth
- o   Drone downlink /uplink frequency
- o   Remote controller type and version
- o   Remote controller firmware
- o   Remote controller output power
- o   Remote controller transmitter bandwidth

- o Used frequency band
- o Average speed of the drone
- o GNSS position of the pilot

Flight scenario:
- o Time interval for test execution
- o Sequences description
- o Flight height
- o Direction of flight
- o Flight profile
- o Speed

EXAMPLE 2   TESTS RESULTS

One of the most important data necessary for the evaluation are the data resulted from the tests, coming from the C-UAS system. The test plans must consider all technical and logistic issues, necessary for precise measurement and data recording during the live tests. It is important that the envisioned C-UAS system will be used in real operational conditions which are not the same all the time, as in tests. Biases may arise and, in this respect, it is important to make the tests as relevant as possible for the expected operational environment. If the field test data are not measured correctly or some data are missed, the test result may be seriously affected making them inappropriate.

The tests must be planned to offer the opportunity for assessing each requirement, in the right way, with the right means and in the best conditions.

For the field test data it was used the same format as for operational requirements but with additional fields for the results.

Table 54 — Template for requirements

Field	Meaning of the field	Format
Req. Nº	*Unique code identifying each requirement for future references.*	*GR followed by two numbers - Ex. GR05, for a general requirement* *SR followed by two numbers - Ex. SR05, for a specific requirement*
Req. Name	*Concise description of the requirement.*	*Free text.*
Description	*More detailed description of the requirement, with special emphasis on the motivation behind the requirement.*	*Free text*
Importance	*Assessment by project stakeholders of the importance of each requirement for the project.*	*Value from a list:* • *Shall* • *Should* • *May*
Parameters and performance limits	*The minimum and maximum limits within which the requirement must be complied with shall be specified. If the requirement comes from a legal provision or standard, the applicable legislation/standard will be specified.*	
How to quantify the fulfilment	*The method of verification of the parameter: inspection, analysis, demonstration, or testing shall be specified.*	

All the data acquired during tests will be stored appropriately, for the next steps in the evaluation methodology.

Managing Potential Ethical Issues

Ethics in evaluation is focused on what it means for evaluators to "do the right thing." Although there is considerable controversy about what "the right thing" means, in philosophy as well as practice, there is general agreement that ethical challenges are common in all phases of the evaluation process, from initial contracting to the reporting and use of the findings. Every stage of an evaluation can present ethical conflicts, from the entry/contracting phase to utilization of results. The most frequent challenge reported by evaluators is pressure from stakeholders to misrepresent findings. Strategies for preventing and responding to ethical problems include actively managing the entry/contracting stage, applying professional guidelines, consulting with colleagues, being sensitive to culture and context, and examining one's own values.

Table 55 — Management of Potential Ethical Issues

Data type	Potential Ethical Issues	Mitigation actions
Personal information of the evaluation participants (all involved stakeholders)	*Describe here what sort of data will be collected, processed, stored, etc. Check the GDPR regulations and perform a Data Privacy Impact Assessment.*	*Describe the measures you take to mitigate the ethical issues.*
Documents (technical sheets, electronic correspondence, etc.)	*Same as above*	*Same as above*
Reports	*Same as above*	*Same as above*
Pictures	*Same as above*	*Same as above*
Metadata from UAS used in tests	*Same as above*	*Same as above*
Metadata from the C-UAS during tests	*Same as above*	*Same as above*
Tests participants	*Same as above*	*Same as above*
Other	*Same as above*	*Same as above*

11.3.7 Data management

11.3.7.1 Data Management Plan

Data management plan is extremely needed for the test methodology. The principles to be followed are mainly focused to data protection and ethics. All data which are used in the evaluation methodology may lead to privacy issues or classified information handling. All stakeholders are interested to deal with correct data and to protect their interest, whether is about the protection of commercial interests in the case of technology providers, or about sensitive data that can be extracted from the expected operational requirements and performance parameters, in case of the end users. If one of the parties protects its data by hiding it, the test results will be erroneous or inconsistent.

To avoid this situation, the evaluation methodology must include a data management plan, which will be seen as a legal document, with specific contractual/procedural rules for information management.

11.3.7.2 Data Synthesis, Judgments, and Conclusions

- **Data aggregation** involves the collection of all the data gathered during the evaluation, including raw data, performance metrics, benchmarks, and user feedback, by ensuring that data is properly organized and stored securely to prevent unauthorized access.

The collected data must be reviewed for accuracy and completeness. Any data anomalies or inconsistencies should be resolved before proceeding with the analysis.

- **Analysis and synthesis** are methods to discover and summarize an evaluation's findings. They are designed to detect patterns in evidence, either by isolating important findings (analysis) or by combining different sources of information to reach a larger understanding (synthesis). Mixed method evaluations require the separate analysis of each evidence element, as well as a synthesis of all sources to examine patterns that emerge. Deciphering facts from a given body of evidence involves deciding how to organize, classify, compare, and display information. These decisions are guided by the questions being asked, the types of data available, and especially by input from stakeholders and primary intended users. By applying the defined performance metrics and benchmarks to the collected data, the results will derive into meaningful insights and conclusions about the C-UAS system's performance.

Below is a detailed description of the data analysis process, including the use of metrics and benchmarks.

<u>Performance Metrics</u>

1. Detection Rate:
Purpose: Measure the system's ability to detect unauthorized UAS within a given range.
Calculation: Detection Rate (%) = (Number of Detected UAS / Total Number of UAS) x 100
Benchmark: Compare the detection rate to industry standards or the system's stated capabilities.

2. False Alarm Rate:
Purpose: Evaluate the system's propensity to generate false alarms or mistakenly identify non-threat objects as UAS.
Calculation: False Alarm Rate (%) = (Number of False Alarms / Total Number of Alarms) x 100
Benchmark: Compare the false alarm rate to acceptable levels defined by operational requirements.

3. Tracking Accuracy:
Purpose: Assess the system's ability to accurately track UAS movements, including speed, direction, and altitude.
Calculation: Tracking Accuracy (%) = (Number of Accurate Trackings / Total Number of Trackings) x 100
Benchmark: Compare tracking accuracy to predefined standards or requirements.

4. Response Time:
Purpose: Measure the system's speed in detecting UAS threats.
Calculation: Response Time (in seconds) = Time from drone take-off to detection
Benchmark: Compare response times to operational requirements or industry best practices.

5. Interference with Other Systems:
Purpose: Evaluate whether the C-UAS system disrupts or is disrupted by other critical electronic systems or communications.
Measurement: Assess the impact on/from nearby electronic devices, including radar systems, GPS, and communication networks.
Benchmark: Ensure that interference remains within acceptable limits as defined by relevant regulations and standards.

Benchmarks for Comparison

1. Historical Data:
Purpose: Compare current evaluation results with historical data from previous evaluations or deployments of the same or similar C-UAS systems.
Benchmarking Process: Analyse whether the system's performance has improved or declined over time and identify trends.

2. Industry Standards:
Purpose: Reference established industry standards or guidelines for C-UAS system performance.
Benchmarking Process: Ensure that the system meets or exceeds benchmarks set by recognized industry organizations or regulatory bodies.

3. Operational Requirements:
Purpose: Align the C-UAS system's performance with the specific operational requirements of the deploying stakeholder.
Benchmarking Process: Ensure that the system's performance metrics meet the operational needs and objectives defined by the stakeholder.

4. Competitor Analysis:
Purpose: Compare the performance of the evaluated C-UAS system with competing systems or solutions in the market.
Benchmarking Process: Evaluate how the system fares in terms of detection rate, false alarm rate, response time, and other critical metrics compared to alternatives.

5. User Feedback and Surveys:
Purpose: Use feedback from end-users and operators as benchmarks for user satisfaction and usability.
Benchmarking Process: Analyse user feedback to identify areas where the C-UAS system excels or requires improvement in comparison to user expectations.

- **Data interpretation** is the effort to figure out what the findings mean. Uncovering facts about a system's performance is not enough to make conclusions. The facts must be interpreted to understand their practical significance. Interpretations draw on information and perspectives that stakeholders bring to the evaluation. They can be strengthened through active participation or interaction with the data and preliminary explanations of what happened.

Table 56 — Data interpretation

Evaluation Question	Indicator/ Performance Measure	Method	Data Source	Frequency	Responsibility

- **Forming Judgments**

Judgments are statements about the merit, worth, or significance. They are formed by comparing the findings and their interpretations against one or more selected standards/criteria. Because multiple standards/criteria can be applied to a given program, stakeholders may reach different or even conflicting judgments. For instance, a C-UAS solution that increases the security of a critical infrastructure by 50% from the previous year may be judged positively by managers, based on standards of improved performance over time. LEA's operational personnel, however, may feel that

despite improvements, a minimum threshold of security has still not been reached, since their expectation is around 90%. Their judgment would therefore be negative. Conflicting claims about a C-UAS's quality, value, or importance often indicate that stakeholders are using different standards or values in making judgments. This type of disagreement can be a catalyst to clarify values and to negotiate the appropriate basis (or bases) on which the evaluation should be judged.

Table 57 — Forming judgments

Criteria	Evaluation Question:					
	Data Synthesis	Standards				Evaluative Judgments
		Excellent	Good	Adequate	Poor	

- **Reaching Conclusions**

Justifying conclusions in an evaluation is a process that involves different possible steps. For instance, conclusions could be strengthened by searching for alternative explanations from the ones you have chosen, and then showing why they are unsupported by the evidence. When there are different but equally well supported conclusions, each could be presented with a summary of their strengths and weaknesses. Techniques to analyse, synthesize, and interpret findings might be agreed upon before data collection begins.

Three things might increase the chances that recommendations are relevant and accepted:
- ✓ Sharing draft recommendations
- ✓ Soliciting reactions/feedback from multiple stakeholders
- ✓ Presenting options instead of directive advice

Table 58 — Reaching conclusions

Evaluation questions criteria	Data Synthesis	Evaluative Judgments	Evaluative Conclusions
Appropriateness			
Effectiveness			
Efficiency			
Impact			
Sustainability			

Table 59 — Processing conclusions

Evaluative Conclusions	Recommendations	Lessons

Recommendations are actions to consider as a result of the evaluation. Forming recommendations requires information beyond just what is necessary to form judgments. If recommendations are not supported by enough evidence, or if they are not in keeping with stakeholders' values, they can really undermine an evaluation's credibility. By contrast, an evaluation can be strengthened by recommendations that anticipate and react to what users will want to know.

• **Feedback and follow-up**

Feedback is the communication that occurs among everyone involved in the evaluation. Giving and receiving feedback creates an atmosphere of trust among stakeholders; it keeps an evaluation on track by keeping everyone informed about how the evaluation is proceeding. Primary intended users and other stakeholders have a right to comment on evaluation decisions. From a standpoint of ensuring use, stakeholder feedback is a necessary part of every step in the evaluation. Obtaining valuable feedback can be encouraged by holding discussions during each step of the evaluation and routinely sharing interim findings, provisional interpretations, and draft reports.

Table 60 — Providing feedback

Conclusions	Recommendations
Include here each conclusion	*Insert here the feedback*

Follow-up refers to the support that many users need during the evaluation and after they receive evaluation findings. Because of the amount of effort required, reaching justified conclusions in an evaluation can seem like an end in itself but it is not. Active follow-up may be necessary to remind users of the intended uses of what has been learned. Follow-up may also be required to stop lessons learned from becoming lost or ignored in the process of making complex or technical decisions. To guard against such oversight, it may be helpful to have someone involved in the evaluation serve as an advocate for the evaluation's findings during the decision-making phase. Facilitating the use of evaluation findings also carries with it the responsibility to prevent misuse. Evaluation results are always bounded by the context in which the evaluation was conducted. Some stakeholders, however, may be tempted to take results out of context or to use them for different purposes than what they were developed for. For instance, over-generalizing the results from a single case study to make decisions that affect all sites in a national program is an example of misuse of a case study evaluation. Similarly, program opponents may misuse results by overemphasizing negative findings without giving proper credit for what has worked. Active follow-up can help to prevent these and other forms of misuse by ensuring that evidence is only applied to the questions that were the central focus of the evaluation.

Table 61 — Follow-up template

Follow-up action	Initiation date	Who initiated the process?	To whom?	Conclusions
Include here the description of the follow-up action	*When the follow-up action was initiated*	*The name of the party who initiated the action*	*The name of the targeted party*	*Conclusions after the action*

11.3.8 Reporting and dissemination plan

Dissemination is the process of communicating the results or the lessons learned from an evaluation to relevant audiences in a timely, unbiased, and consistent fashion. Like other elements of the evaluation, the reporting strategy should be discussed in advance with intended users and other stakeholders. Planning effective communications also requires considering the communication channels, timing, style, message source and format of information. Regardless of how communications are constructed, the goal for dissemination is to achieve full disclosure and impartial reporting.

Along with the uses for evaluation findings, there are also uses that flow from the very process of evaluating. These "process uses" should be encouraged. The people who take part in an evaluation can experience profound changes in beliefs and behaviour. For instance, an evaluation challenges

staff member to act differently in what they are doing, and to question assumptions that connect evaluation activities with intended effects. Evaluation also prompts staff to clarify their understanding of the goals. This greater clarity, in turn, helps staff members to better function as a team focused on a common end. In short, immersion in the logic, reasoning, and values of evaluation can have very positive effects, such as basing decisions on systematic judgments instead of on unfounded assumptions.

The evaluation findings must be clearly included in reports, which will be disseminated later to the interested stakeholders. In this respect, a clear record of the reports, the recipients and the level of access to information must be kept.

Table 62 —Report template

Report Type	Due Date	Audience & their Interests	Overall Focus	Contents	Dissemination
Formal Reports					
Ad Hoc and Event Reports					

Reporting Evaluation Results

- Executive Summary: the report will begin with an executive summary that provides a concise overview of the evaluation's key findings, conclusions, and recommendations. This summary should be accessible to non-technical stakeholders.
- Detailed Analysis: the detailed analysis of the C-UAS system's performance must be presented, including results for each performance metric.
- Benchmark Comparison: a comparison of the system's performance against established benchmarks, historical data, industry standards, and operational requirements, while highlighting areas where the system meets or exceeds expectations and areas that require improvement.
- User Feedback: the report must include summaries of user feedback and survey results, emphasizing user experiences, satisfaction, and usability insights. If applicable, showcase user testimonials to add credibility to the evaluation.
- Anomalies and Challenges: any anomalies or challenges encountered during the evaluation process and how these were addressed and their potential impact on the system's performance.
- Recommendations: clear, actionable recommendations for improvements, if necessary. These recommendations should be based on the evaluation results and should offer practical guidance for enhancing system performance.
- Lessons Learned: insights gained from the evaluation process that could benefit future assessments or inform best practices in C-UAS evaluations.

12 Test Environment

12.1 General

The COURAGEOUS test methodology and performance evaluation contains two main parts:

- Test environment covering use of standard scenarios, stimuli (e.g., UAS types and behavior), environmental conditions, DTI systems under test and test templates for test execution
- Performance evaluation dealing with a comparative functional evaluation of DTI systems both at component level and system level.

This clause presents the test environment for DTI systems which is composed of the following main elements

- Standard scenarios that form the baseline for the field test scenarios and use cases for the evaluation of DTI systems.
- Stimuli and environmental conditions and elements that have an influence on the operation and outputs of the DTI systems. Here, the main actors of the test environment are presented, along with their properties, making special emphasis in these elements that can be relevant to test the performance of the DTI systems.
- In order to assess the performance of the DTI systems, the test environment also includes relevant equipment, tools and associated procedures, such as facilities for time synchronization of all the devices logging data, GNSS trackers for relevant actors during the tests, weather stations and radiofrequency spectrum analyzers.

12.2 Standard field test scenarios

In Clause 7 (Standard Scenario Development) ten standard scenarios were identified and clustered into three main categories: Sensitive Sites/Critical National Infrastructure, Public Spaces Protection/Events and Border Protection (Land - Maritime). In some scenarios, figures such as the number of drones, size of the area of interest, required detection ranges and payload or altitude of the drone are provided as a reference.

These parameters were complemented with the information in Clause 6 (Review of Current C-UAS Frameworks) that contains relevant values such as the typical detection ranges of the DTI systems in the market.

From the standard test scenarios, it was analyzed how they can be implemented (totally or partially) in the COURAGEOUS project field trials. The relevant standard test scenarios for a given test site were translated into test scripts that were followed during the trials.

In the test scripts, the information in Clause 6 (Review of Current C-UAS Frameworks) about common state of the art commercial DTI specifications was taken into account, e.g., relevant values such as the typical detection ranges of the DTI systems in the market. The goal was to achieve a trade-off between LEA's requirements for the DTI systems in the standard scenarios and the specifications of the commercial products when the tests are carried out.

In Clause 7 (Standard Scenario Development), of the ten standard scenarios mentioned above, a subset has been selected to validate the test methodology, at the three different test sites (Greece, Belgium and Spain). For the first test site execution, that was held in Greece, the scenario chosen was the "Outdoor Political Rally". Other operationally relevant scenarios (e.g., Maritime and Land border) were the use cases used in the Belgium (at the Lombardsijde military base) and Spain (at the ATLAS Flight Test Center) trials.

12.3 Stimuli and environmental conditions

12.3.1 General

This section presents the main actors of the test environment, along with their properties, making special emphasis in these that can be relevant to test the performance of the DTI systems. It should be noted that their locations and evolution in time will be decoupled and addressed in the following sections. Two main categories will be described in the following subsections:

- Unmanned Aerial Systems (UAS): the objects of interest in the environment that the DTI systems should detect, their properties (e.g., types, behaviour) will be analysed in detail.

- Environmental conditions: the rest of actors in the test environment that could affect the performance of the DTI systems. Ideally, this environmental clutter should be replicable in different test sites. However, in the COURAGEOUS field trials, it is studied how this could be achieved to the maximum possible extent in practice. Environmental conditions are broad and cover not only physical aspects but also other relevant constraints.

12.3.2 Unmanned Aerial Systems

There are two main classifications of UAS which are relevant within the scope of COURAGEOUS. The first one from NATO is interesting, since it is usually referred to in reports about C-UAS systems in the military field. But since the scope of project COURAGEOUS is European, the classification of UAS from the EU Aviation Safety Agency (EASA) and its linked civil UAS European regulation framework was taken into consideration in 12.3.2.8.

NATO categorizes UAS into three dedicated classes (see Table 63):

- Class I (<150 kg) for micro (<66J potential energy), mini (<15 kg) and small ones (>15 kg)
- Class II (150 kg – 600 kg) for medium-sized, tactical systems
- Class III (>600 kg) for Medium-Altitude Long-Endurance (MALE) and High-Altitude Long-Endurance (HALE) aircraft.

By comparing the three different classes, their application, size, and operating altitude alone, it can be concluded that countering this spectrum of UAS requires a multitude of different, class-specific approaches. The size and complexity of NATO Class I category is quite comparable to commercially available consumer models and therefore require a similar approach when having to counter them.

Table 63 — NATO UAS taxonomy (Source: NATO ATP-3.3.8.1, Ed. B, Ver. 1 (NATO Standardization Office (NSO), 2019)

Class	Category	Normal employment	Normal Operating Altitude	Normal Mission Radius
Class III (>600 kg)	Strike/Combat	Strategic / national	Up to 65000 ft MSL	Unlimited (BLOS)
	HALE	Strategic / national	Up to 65000 ft MSL	Unlimited (BLOS)
	MALE	Operational / Theatre	Up to 45000 ft MSL	Unlimited (BLOS)
Class II (150 kg-600 kg)	Tactical	Tactical Formation	Up to 18000 ft AGL	200 km (LOS)
Class I (<150 kg)	Small (>15 kg)	Tactical Unit	Up to 5000 ft AGL	50 km (LOS)
	Mini (<15 kg)	Tactical Sub-unit (manual or hand launch)	Up to 3000 ft AGL	Up to 25 km (LOS)
	Micro (< 66 J)	Tactical Sub-unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)

12.3.2.1 Types of UAS

Figure 45 shows four UAS designs with examples from different companies or research centres. There are three main designs for UAS: fixed wing, rotocopter or a combination of both designs. Fixed wing designs have a motor(s) and propeller(s) to create propulsion in a roughly horizontal direction and the flight path is determined by the manipulation of the flight control surfaces on the wings and tail. Rotocopters have two or more propellers that generate lift in a roughly vertical direction and the flight path is determined by independently adjusting the rotation speed of the propellers.

The range of operation of fixed wing designs is larger compared to rotocopters but they do not have hovering and vertical take-off and landing capabilities. Then, there are different hybrid designs that try to combine the advantages of fixed wing and rotocopters in the same aircraft: by using tilting rotors that can change from vertical to horizontal direction during flight or by using wings, horizontal and vertical rotors and changing the thrust from vertical to horizontal rotors and vice versa for take-off and landing, respectively. However, in hybrid designs, the flight range is significantly reduced when hovering several times during the operation.

In addition, there are also bioinspired designs such as the nano hummingbird by AeroVironment, the dragonfly (BionicOpter), the flying fox (BionicFlyingFox), the herring gull (SmartBird), and others by Festo for instance. Current research in this area is being conducted in the GRIFFIN[12] ERC Advanced Grant.

Aerial biomimetic platforms can serve a role in more advanced malicious C-UAS modus operandi. There are a few providers selling these systems, mostly for wildlife management (in airports, oil & gas, agriculture and mining operations), but more recently the market is moving towards more interesting operational use cases, such as unobtrusive surveillance (anti-poaching, border control, law enforcement and defense – SOF).
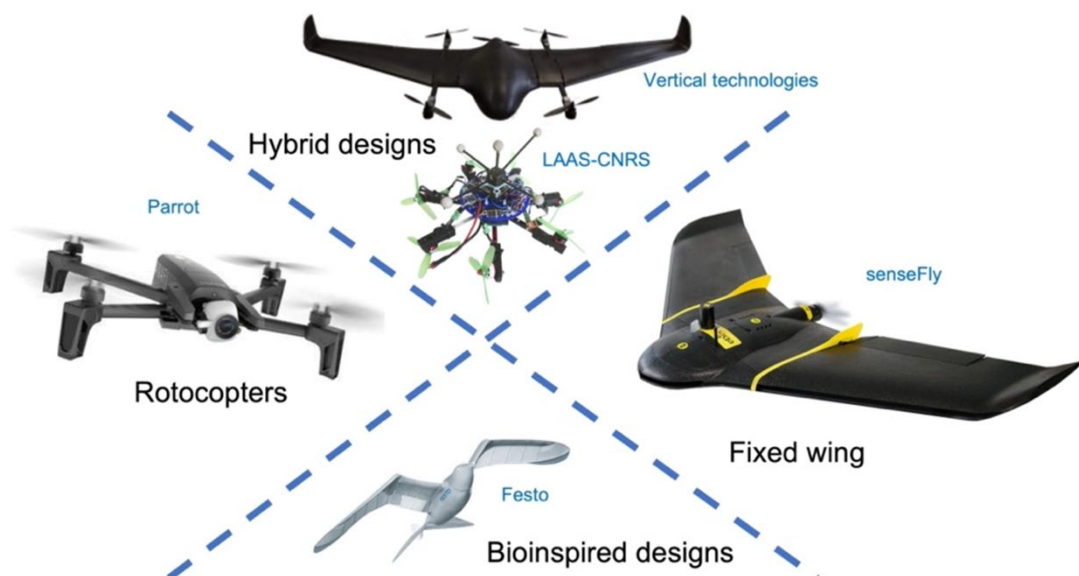
Figure 45 — Different UAS designs with examples from different companies or research centers

12.3.2.2 Size, geometry, and material

The geometry of the UAS, its size, and materials define the RCS (Radar Cross Section) have an impact on the performance on DTI systems based on radar. These features also affect the performance of

---

[12] https://griffin-erc-advanced-grant.eu/

DTI systems based on EO and infrared cameras. Some of the materials used in the manufacture of UAS are plastic, aluminum, and carbon fiber.

12.3.2.3 Propulsion system

Most of the designs for small drones are based on propellers powered by one or multiple electric motors connected to an on-board rechargeable battery. Other alternatives include internal combustion engines, hybrid gas-electric systems, or turbines. If the drone is a glider, there is no propulsion system. The propulsion system has an impact on the noise and thermal signatures of the UAS, and hence can affect DTI systems based on acoustic or thermal sensors.

12.3.2.4 Manufacturer and model

The technology used by the DTI to compute these properties can be relevant since it would be possible to hack the information related to the UAS model in the communication protocol in order to scam DTI systems that identify the model based on the analysis of data frames transmitted by the UAS.

12.3.2.5 Payload

Payloads may be innocuous or may be malicious. The following payloads can be found in the literature: cameras, sensors, aerosol dispersers, medical supplies, explosives, chemical, biological or radiological substances, or other weapons, hazardous materials, radiofrequency transmitters or receivers, surveillance equipment, etc. It should be mentioned that novel payloads such as robotic arms (Ollero et al., 2021) can be found for applications such as inspection by contact.

12.3.2.6 Communication system

If the navigation system is autonomous, the drone does not use any communication system during the flight. In other cases, different communication links for control and data transmission can be present: ISM specific band, 3G, 4G, 5G, etc. In addition, Satellite Communication (SATCOM) can be also used since this technology is becoming more affordable because an increasing number of companies are providing satellite communication and are trying to test their services for the UAVs. In (Zolanvari et al., 2020) the following examples are listed: InmarSAT, Iridium NEXT, Globalstar, Orbcomm Generation 2, OneWeb, O3b Networks and SpaceX.

The directivity of the antennas used in the UAS has an effect on the C-UAS sensors based on RF. In particular, for the uplink some UAS can be equipped with directional antennas that can make more difficult to locate the pilot with RF sensors if the UAS communication protocol is not available.

12.3.2.7 Navigation mode

The navigation mode of the drone may have an impact on the performance of DTI systems. The three common navigation modes used by drones are:

- Manual navigation: the drone is directly controlled in real time by a remote, human pilot who manipulates joysticks, buttons, and/or knobs on a controller. Manual navigation is based on uninterrupted and continuous radio communication between the UAV and the controller.

- GNSS navigation: drones can be pre-programmed to fly autonomously to specified locations (also known as waypoints) or use specified flight paths. This navigation mode can be achieved without any radio emissions from the drone or the GCS, although many drones may send a "heartbeat" message that occasionally transmits telemetry, for safety reasons, back to the controller. However, this heartbeat function can be turned off to avoid radio emissions.

- Autonomous navigation in GNSS denied environments: Some drones can navigate based only on the information provided by on-board sensors such as accelerometers, gyroscopes, magnetometers, video cameras, and collision avoidance sensors. Then, navigation is not based on received signals from the GNSS system and may not emit any radio signals and may be entirely unaffected by any impediments in radio signal propagation or interference. In this mode, the drone can follow moving objects or people, fly towards a stationary object at a distance or navigate by dead reckoning.

In the test environment, it is possible to consider different navigation modes for the UAS depending on the test case.

12.3.2.8 Authorised vs non-authorised flights

This is not a characteristic of the UAS itself, but a property that depends on the acceptance by the national airspace authority of the UAS flight plan requested by the UAS operator if he/she has asked for the corresponding permission. In any case, the DTI system should have access through Internet to the list of authorised flights in the area on one hand. And, on the other hand, it should follow the UAS trajectories to detect deviations from the authorised flight plan.

In July 2018, European lawmakers passed the new Regulation (EU) 2018/1139 on common rules in the field of civil aviation, which included a new mandate for the EU Aviation Safety Agency (EASA) on drones and urban air mobility ("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, ," 2018). This regulation adopts a new comprehensive legal strategy for the drones sector and repeals Reg. (EC) 2008/216 ("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," 2008), which only concerned drones with more than 150 kg take-off weight, while drones with a maximum take-off mass under 150 kg were under Member States jurisdictions.

The new Regulation introduces specific rules for the use of drones in Section VII on "Unmanned Aircraft", that is, Articles 55 to 58, plus Annex IX on "Essential requirements for unmanned aircraft." In addition, the new regulation mandated EASA to propose technical rules for all sizes of civil drones and standards to the European Commission, which had to adopt delegated and implementing acts for the final setting up of this legal framework.

Since neither the EU Parliament nor the EU Council had any objections, both Implementing and Delegated Acts (Commission Delegated Regulation (EU) 2019/945 ("COMMISSION DELEGATED REGULATION (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems," n.d.) and Commission Implementing Regulation (EU) 2019/947 ("COMMISSION IMPLEMENTING REGULATION (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft," n.d.)) were published in June 2019 and entered into force 20 days later. The new EU regulatory framework covers all types of existing and future drone operations, enabling operators -once authorised in their state of registration to freely circulate between Member States. The purpose of introducing these new regulations is to ensure the safety of drones operations, as well as protect the privacy of EU citizens, with respect to personal data protection, and the environment while allowing free access to airspace. The new regulations establish technical and operational requirements, provisions for UAS operations and personnel (minimum requirements and operator training), including both pilots and any organization. They define UAS capabilities, types of operations, and label these into three broad risk-based categories (open, specific and certified) following the distinction suggested by EASA in the Opinion 01/2018 (Agency, 2018). These three categories of operations are based on the levels of risk involved per drone flight and each adopts a varied regulatory approach, with UAS flight operational

limitations decreasing with the requirement for greater authorisation from a Member State's national aviation authority.

Regulation 2019/947 presents a comprehensive system of unified legal regulations which classifies UAS operations into the three categories mentioned above based on different criteria:

- Open (Article 4 of Regulation 2019/947). Operations in this category shall not be subject to any prior operational authorisation, nor to an operational declaration by the UAS operator before the operation if the following conditions are met. The UAS belongs to one of the classes set out in Delegated Regulation (EU) 2019/945 or is privately built or meets the conditions defined in Article 20 of Regulation 2019/947. The unmanned aircraft has a maximum take-off mass of less than 25 kg, and the remote pilot always keeps the unmanned aircraft in VLOS except when flying in follow-me mode or when using an unmanned aircraft observer. During 'open' operations, the remote pilot ensures that the unmanned aircraft is maintained within 120 meters of the closest point on the surface of the Earth (except when it overflies an obstacle on request of its owner) and at a safe distance from people (never flying over crowds). The unmanned aircraft cannot carry dangerous goods and does not drop any material. Open operations are further divided into three subcategories: A1 (fly over people), A2 (fly close to people) and A3 (fly far from people).

- Specific (Article 5 of Regulation 2019/947). Operations fall into this category as soon as the concept of operation exceeds the limitations defined in the open category. The UAS operator shall apply to obtain an operational authorisation from the competent authority in the Member State where it is registered submitting a risk assessment including adequate mitigating measures. This risk assessment approach allows to handle new technologies and operations such as BVLOS, fully autonomous drones, urban areas, etc. However, if the operation complies with one of the standard scenarios defined by EASA, the UAS operator shall not be required to obtain the above-mentioned operational authorisation. Also, an operational authorisation or a declaration shall not be required for UAS operators holding a Light UAS operator certificate (LUC) with appropriate privileges, which is valid in all UE Member States without additional demonstrations.

- Certified (Article 6 of Regulation 2019/947). An operation is classified as being in the certified category when, according to the risk assessment, the operation cannot take place without a certificate for the operator, a certificate for the airworthiness of the UAS, and a license for the remote pilot (unless fully autonomous). In any case, the following operations are within the certified category: operations over assemblies of people with an aircraft of characteristic dimensions of 3 meters or more, transportation of people and transportation of dangerous goods if, in case of accident, they pose a high risk for third parties.

NOTE   The abovementioned text is a direct extract and reproduction of European Legislation.

Considering the different levels of risk within an Open Category operation, this category is further divided into subcategories. Each subcategory is characterized using the specific class of UAS, the area of operation, and the remote pilot competency. The UAS classes in the Open category (from C0 to C6) are mainly defined by MTOM or kinetic energy, along with technical requirements and electronic identification (ID) and geo awareness (geo fencing) requirements, but all UAS classes have MTOM below 25 kg.

The following cases can be of interest:

- Off-nominal cooperative drone: The drone is authorised to operate near the test area but it is not following its agreed flight plan yet it is a cooperative drone broadcasting its e-identification.
- Off-nominal in category Open C0: This type of drone does not need an authorisation to be operated outside of the test site and it does not need to broadcast its e-identification. It is a low-risk drone that flies away from its authorised flight zone.
- Also, the situation where there is no drone intruding the test area. This situation would be used to assess false-alarm scenarios, where the "Detect" capability would incorrectly detect an intruding drone potentially leading to the spurious activation of mitigations that could have an operational effect on the test site operations.

12.3.2.9 Behaviour of the drone

This property will depend on the particular scenario and will allow to test if the artificial intelligence of the DTI system can detect abnormal behaviour in the UAS. It is linked to the second main technical capability of a C-UAS system identified in (EUROCAE, 2021):

- Detect: capability to detect, identify and track a drone.
- Decide: capability to assess whether a detected drone could cause a risk and decide the best mitigations to be undertaken for the next step of the current operation.
- Mitigate: capability to reduce the severity of a drone threat. This capability includes technical means to neutralize the drone or means to send alarms to a remote pilot.

12.3.2.10 UAS pilot (red team)

Since the output of some DTI systems includes the estimation of the location of the pilot, it is required to log his/her position with a device such as a GNSS tracker.

It should be mentioned that the directivity of the antennas of the UAS has an impact on the capability of some DTI systems to locate the pilot. For instance, if the uplink of the UAS employs directive antennas, it could be more difficult for the RF sensors to compute the location of the pilot.

12.3.2.11 Challenges for DTI Systems depending on the type of UAS

For the NATO Class III and EASA Certified categories, a significant subset is equivalent to 'regular aircraft' without a pilot, and the qualitative difference from comparable regular air threats seems minimal. However, for most systems below these categories, there are no manned equivalents, and there cand be found relatively new types of threat, which create new challenges: much smaller designs with different forms/formats than conventional manned threats.

Both for the NATO and EASA classifications, the main challenges for DTI systems can be found in the lighter categories (NATO Class I and Open EASA category with classes C0-C6) that have smaller Radar Cross Sections (RCS), especially because larger fractions of these drones can be made from materials that are less Radio Frequency (RF) reflective. It can be assumed that the smaller the RCS of an object, the closer it needs to get to the receiver to produce a usable return signal. The detection distance may become even less due to the potentially very low flight paths of these drones in areas with a lot of background noise (cities), which prevents a line-of-sight detection independent of the RCS. This makes it very difficult for any airspace sensor to continuously detect and track them. The short detection range makes these threats a high risk in general, and it is amplified by the use of small drones in swarms or with high levels of automation.

In addition, for rotocopter, hybrid and bio-inspired designs, a stop-and-drop or rapid direction-changing flight pattern make it harder for regular radars to maintain a track. Since every sensor works within an anticipated framework of threat parameters such as RCS, speed, altitude, and manoeuvrability, novel drone designs in the lighter categories allow these parameters to be challenged.

In general, below NATO Class III and EASA certified categories, drones operate at low flight ceilings where the surrounding environment has more impact on any sensor coverage. Apart from radar, the following sensors can be found in DTI systems: optical sensors in the visual, infrared (IR) and ultraviolet (UV) bandwidth, acoustic sensors, and radio frequency passive receivers. However, both acoustic and optical sensors have relatively short ranges compared to radar sensors and can be challenged by bioinspired drones with sizes and shapes like birds and very low acoustic signatures. And depending on the background noise, acoustic detection ranges vary greatly and can be expected to range up to one kilometre in a quiet rural area, but are limited to only a few hundred meters in a noisier urban environment. Regarding the radio frequency passive detection of the drone-GCS RF data links, it is a plausible alternative or augmentation to radar active detection, especially since larger active sensors have weaknesses in short distance detection. However, if the drones are using GNSS navigation mode without heartbeat or autonomous navigation mode (see 12.3.2.7), they cannot be detected with passive RF receivers. These modes are implemented in many low-cost light drones. And, in any case, the effectiveness of RF analysers can be reduced in highly congested RF environments such as cities due to saturation.

Finally, it should be mentioned that the DTI systems should be also equipped with devices such as ADS-B/FLARM receivers for "cooperative" UAS that can be also present in any scenario. If the flight has not been authorized as it was discussed in paragraph 12.3.1.8, then it could the case of a careless pilot.

12.3.3 Environmental Clutter and conditions

12.3.3.1 General

In this subclause, additional elements in the environment that can have an impact on the performance of the DTI systems under test are considered. On one hand, there are actors that can generate false positives such as birds, rotating devices, and other aircrafts. On the other hand, obstacles, radiofrequency signals, and noise can interfere in the nominal operation of the DTI systems. Weather condition can also have an important impact on the performance of DTI systems.

12.3.3.2 Obstacles

Obstacles in the test environment are defined by the following properties:

- Geometry
- Materials such as vegetation, wood, glass, stone, concrete, bricks, reinforced concrete, metal bars, aluminium, etc.
- Static or dynamic

In Clause 6 the following obstacles are proposed for the test environment: single trees, forest walls, and buildings. Depending on the scenario, additional obstacles such as cars and trucks that can be dynamic could be also considered.

12.3.3.3 Birds

On the one hand, birds are a relevant source of false positives for most DTI systems, so their presence in the test environment should be controlled if possible and/or monitored. For instance, in Clause 6

one of the requirements for the test environment is to ensure the presence of a falconer with a bird or birds.

On the other hand, Clause 6 also mentions that it should be checked if it is necessary to insure the drone against damage by bird attacks during the tests.

12.3.3.4 Radiofrequency signals for applicable DTI sensors

Different radiofrequency signals can interfere or have an impact on the performance of DTI systems:

- Other DTI systems (power, directivity, etc.) under test
- RF jammers for VIP protection
- Cellular base stations
- Airport CNS systems (SMMS/WAM, SMR, DME, VOR, WiMAX datalinks)
- Radar and radio beacons in coastal areas
- Railway's communication infrastructure

The test environment should also include spectrum analysers to register the radiofrequency signals along time during the tests.

12.3.3.5 Noise sources

Depending on the scenario considered, different noise sources can be found such as traffic in urban environment, people in stadiums, airplanes around airports, etc. In the test environment, some devices such as large speakers can be included to simulate these noise sources if it is considered relevant to test DTI systems based on acoustic sensors.

The test environment should also include microphones to register the environmental noise along time during the tests.

12.3.4 Weather conditions

From Clause 6 and Clause 7 it can be observed that weather conditions are a relevant parameter to consider in the scenarios, since it affects the performance of most of the technologies used in DTI systems. In addition after the analysis in Clause 6, it should be emphasised that the collected information about the specifications of DTI systems is not fully reliable and comparative in technical terms. In particular, it is mentioned that, in general, there is no reference to the weather conditions during the manufacturer tests used to generate the data sheets of the products. And also in Clause 6 it is stated for many technologies the need to test the operation of the systems under different weather conditions (sun, rain, fog).

However, weather conditions cannot be controlled during the different tests, but the test environment should be equipped with a professional weather station. This station should log the evolution in time during the tests of variables and parameters.

- Wind measurement: direction and speed
- Air pressure, temperature and relative humidity
- Solar radiation
- Precipitation type (rain and snow) and intensity
- Lighting detection

12.4 Equipment and tools

12.4.1 General

Regarding logistics, the test environment should be also equipped with power supply, internet access, devices for voice communication between the personnel involved in the tests, tents, storage space for material and illumination to support night trials.

In addition, to assess the performance of the DTI systems, the test environment should include some equipment, tools and associated procedures that are described in the following.

12.4.2 Time synchronization equipment

The test environment should include some mechanism based on hardware/software and/or a procedure to ensure time synchronization among all the relevant systems involved in the tests. Time synchronization should be achieved with a level of accuracy that will depend on the maximum speed of the involved UAS. The goal is to record all the relevant data during the tests with temporal synchronization to enable the possibility to compare the estimations provided by the DTI systems with the ground truth. Ideally this ground truth will be based on the real positions of all the UAS along time during the tests with differential GNSS accuracy. However, in practice, many commercial UAS that will be used during the tests will use GNSS with lower accuracy but, in any case, the telemetry recorded should be synchronized with the clocks of other UAS and all the DTI systems.

One option to achieve this synchronization is to use the Network Time Protocol (NTP) that is widely used to synchronize a computer to Internet time servers or other sources, such as a radio or satellite receiver or telephone modem service. It can also be used as a server for dependent clients. It provides accuracies typically less than a millisecond on LANs and up to a few milliseconds on WANs, that are considered enough for the test environment. It implies to install a NTP client on the different systems involved and to connect them to a local NTP server. In the market there are many commercial NTP servers based on GNSS reception.

If it is not possible to install the NTP client in some of the systems, an alternative will be to create a procedure to be followed in the setup, so they connect to the Internet for instance until they are synchronized via a remote public NTP server. Another alternative will be to connect them to a GNSS receiver to achieve synchronization through the GNSS clock. If any of these options is available for a particular system, then a manual time synchronization procedure should be followed.

In all the cases (for the drones, the C-UAS systems, the weather and radio frequency spectrum logs, etc.), the date time of the logged data should be Zulu time: Universal Coordinated Time (UCT), sometimes called Universal Time Coordinated (UTC) or Coordinated Universal Time (but abbreviated UTC).

12.4.3 GNSS trackers

These devices allow to track the GNSS location of relevant actors during the tests such as the drones and the drone pilots if needed. It should be noticed that other elements in the environment such as moving obstacles (other vehicles) or birds will not be tracked during the tests since they are not the target of the DTI systems. The data logged is synchronized since it is based on the GNSS receiver clock.

12.4.4 Weather station

Weather is also one of variables that can impact the performance of C-UAS systems and hence hinder the comparison of different C-UAS systems. For instance, if the test takes place during a sunny day, more systems will detect, track, and identify drones efficiently and more often than on a rainy or foggy day. For more details, in Deliverable D2.2, there is a table which shows the impact of different

atmospheric conditions on certain C-UAS technologies such as radars, VIS cameras, thermal cameras, IR sensors, lasers/lidars rangefinders, frequency monitoring devices and acoustic sensors. Then, it is very relevant to log the weather data during the tests for a fair comparison.

The weather station should log the temporal evolution of variables and parameters such as:

- Wind measurement: direction and speed
- Air pressure, temperature and relative humidity
- Solar radiation
- Precipitation type (rain and snow) and intensity
- Lighting detection

In addition, a visibility detector should be also installed in the test site to measure the presence of fog and pollution affecting the level of visibility for C-UAS EO/IR sensors.

12.4.5 Radio frequency spectrum analysers

The RF spectrum analyser should log the temporal evolution of the spectrum baseline, emissions, availability, and transmission patterns during the tests. These measurements are relevant to check if none of the C-UAS systems interfere with others. Checking the frequency spectrum in the background allows to see if there are any other transmitters nearby that could spoof tested systems or interfere with them.

The basic spectrum monitoring technique is to set up a spectrum analyser, attach a suitable isotropic antenna, observe the desired part of the RF spectrum, and save traces. Traces can be saved at the end of each sweep, or if the analyser supports the option, it can save the spectrograms for the test time or save-on-event triggered by burst detection or other equivalent option. It is recommended a double trace spectrum analyser to set trace A to normal, and trace B to Max-Hold, as it shows both the current power level and the excursion limits. It is important to set the span and RBW accordingly to the desired frequency band. Usually, a mid-span is the best setting for viewing a signal that is rapidly changing. RBW and span are coupled by default, but RBW could be modified to increase resolution. However, a fast sweep with a narrow RBW would compromise amplitude accuracy.

12.4.6 Software simulation tools

There are different software applications in the market that allow to compute in simulation some parameters of interest depending on the location of the UAS and the DTI system such as: radiofrequency signal strength received from the UAS, sound levels received by the DTI, visibility check for EO/IR technologies.

12.5 Templates and scripts

12.5.1 Generic test templates and test scripts

This subclause addresses the design of the test templates and test scripts for the monitored area which is based on the standard scenarios described in Clause 7. Each of these scenarios outlines a representative real-world event to introduce the overarching operational context and limitations. The monitored area for these standard scenarios can be described with the generic top view template shown in Figure 2a) where several parameters have been considered. In all these templates, O represents the location of the sensors of a given DTI system under test and there are several parameters that define the monitored and remote areas (shown in red and green respectively in Figure 2) around it:

- Remote area defined as a circle with radius r_r. It represents the maximum extent that UAS activity may take place during the assessment.

- Monitored area of interest 1: circle with radius r_{m1}.
- Monitored area of interest 2: circular sector with an azimuth angle of coverage α and radius r_{m2}.

a) Generic configuration with $r_r > r_{m2} > r_{m1}$

b) Infrastructure protection with one level of alert ($r_{m1} = r_{m2}$)

c) Infrastructure protection with two levels of alert ($\alpha = 360^o$)

d) Border segment or perimeter protection
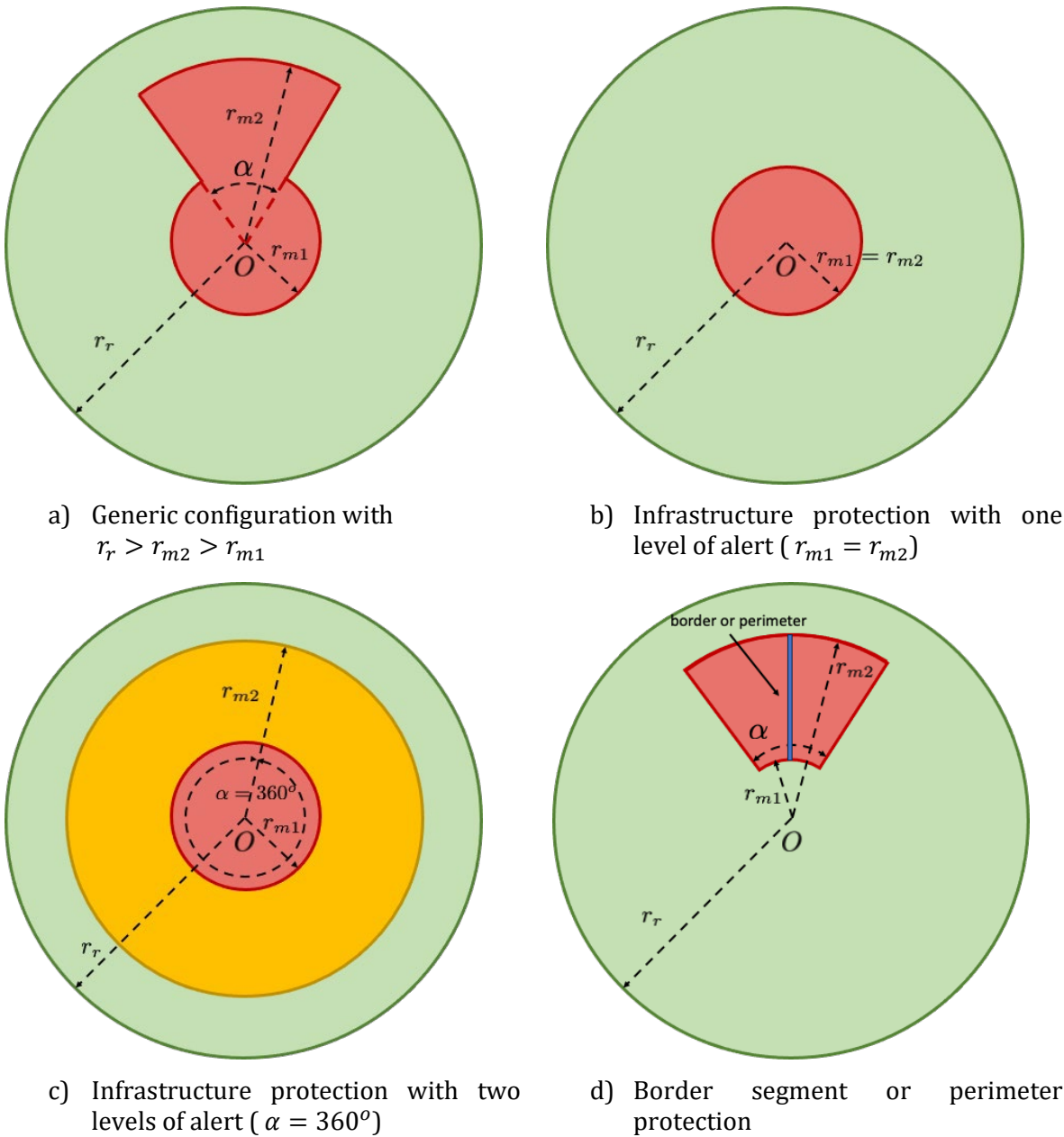
Figure 46 — Top view of some test templates for the remote and monitored areas based on the standard scenarios in Clause 7, where O represents the location of the sensors of a given DTI system and several parameters have been considered

The C-UAS equipment must declare and generate a persistent alarm for all UAS activity occurring within or entering the monitored areas, but UAS activity occurring outside of the monitored areas can be processed by the C-UAS equipment and may be declared but should not alarm. In Figure 46 b)-d) there are several examples of configurations that result for some particular values of the parameters in the generic configuration shown in Figure 46 a), which are of interest according to the standard scenarios considered in Clause 7. Then, Figure 46 b) and 46 c) represent critical

infrastructure protection templates with one and two levels of alert respectively, whereas Figure 46 d) represents a template for border or perimeter protection.

The top view of the profiles is defined in vertical from the ground up to a given altitude h Above Mean Sea Level (AMSL) for the geoid used by the GNSS logger on-board the Red Team drones as a ground truth for the tests.

It should be noticed that the sensors of the DTI system cover a 3D volume with a profile for the coverage in altitude like the one depicted in Figure 47.
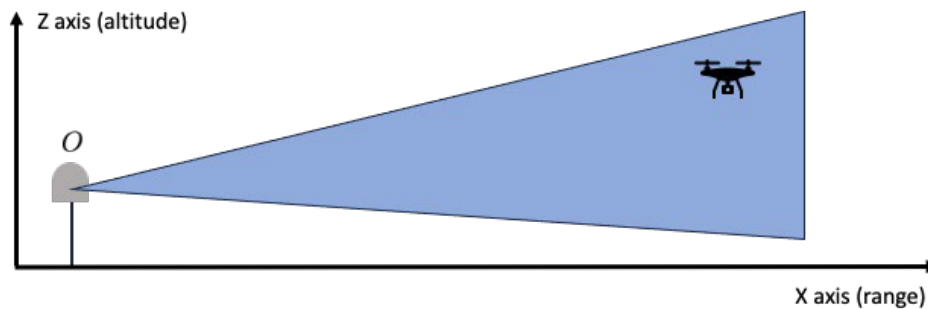
Figure 47 — Representation of the coverage in altitude by the DTI sensor located in O

It is also important to highlight that the remote and monitored volumes for a particular standard scenario such as the airports is complex as it can be seen in documents published by EUROCAE such as ED-286 (OSED for Counter-UAS in controlled airspace) and ED-322 (System Performance and Interoperability Requirements for Non-Cooperative UAS Detection Systems). However, these more complex volumes can be modelled as a combination of the volumes described in this section and can be covered using several DTI systems in real deployments.

These test templates for the remote and monitored areas are the basis for the generation of the test scripts used during the test campaigns. The methodology used during these campaigns is the Adversarial Testing, in which the Red Team behaves as a threat actor, attacking assets or locations trying to break past the defences. Test scripts define the volumes of interest (radii r_{m1}, r_{m2} and r_r, angle α and altitude h) where the drones of the Red Team will fly following different flight patterns. Figure 4 shows examples of vignettes for the test scripts for the perimeter or border protection scenario based on the test template for the remote and monitored areas depicted in Figure 2d). The trajectories of the drones are non-radial in general.

For each test script, the type of drone, its model, the values for altitude, speed, flight mode, etc. can be chosen from the values considered for each standard scenario in Clause 7.

a) Multicopter in straight line from waypoint wp_1 to wp_2 in waypoint autonomous mode at constant 90 m AMSL altitude and 20 m/s

b) Multicopters in straight lines from wp_3 to wp_4 and from wp_2 to wp_1. Both in waypoint autonomous mode at constant 60 m AMSL altitude and 15 m/s

c) Fixed wing in straight line from wp_4 to wp_3 in waypoint autonomous mode at constant 500 m AMSL altitude and 30 m/s

d) Multicopter in zig-zag pattern from wp_3 to wp_5 in manual mode at constant 100 m AMSL altitude and 20 m/s

Figure 48 — An example of possible vignettes for the test scripts

The example test scripts in Figure 48 can be generated from the test template for remote and monitored areas depicted in Figure 46d. The particular values for altitude, speed, flight mode, etc. of the drones can be chosen from the values considered for each standard scenario.

Each test script has an associated file in Keyhole Markup Language (KML) format with the list of waypoints for each drone involved. Once filled, each test script has an identifier which is a number and may have several variants labelled as Alfa, Bravo, Charlie, etc. An example with some values of a test script is shown in Table 64.

Table 64 —Example of a test script

Test script identifier	3
Variant	Bravo
Scenario	Land border protection
Test vignette	
Drone type	Multirotor
Model	DJI Matrice 300 RTK
Drone serial number	0N4DEBP0210027
On-board GPS logger S/N	50303500162
Altitude AMSL	100 m
Cruise speed	20 m/s
Flight mode	Autonomous waypoint mode
Flight plans file	Test3_bravo.kml
Flight plans visualization	

12.5.2 UAS paths

For each UAS, one or several paths can be defined with different properties (Schneider et al., 2021) such as:

- Approach pattern: includes the pattern in which the drone is flying towards the DTI system as an important part of the attack tactics. The considered patterns are straight line, zigzag path, with or without outbreaks from the sensor area, and circling.
- Approach distance horizontal: describes the horizontal distance of the UAS between the starting point and the DTI system.
- Vertical approach altitude describes the altitude of the drone when approaching the DTI system. Tests should include the same paths' shapes projected on the ground, but at different altitudes.

However, it should be noticed that the performance of the DTI system will depend on the relative paths of the UAS with respect to the location of the system. Relative position of the Sun or Moon and the DTI system with respect to the UAS trajectory may have an impact. Blinding, glares, solar EM emission, etc, can affect the DTI system performance. Another relevant aspect to consider is if the UAS are hidden by obstacles such as buildings, vehicles, vegetation, etc. partially or during the entire flight path. Regarding vegetation, systems could be affected by leaves on trees vs no leaves so testing should take place across optimum environment variables, i.e., in the summer when leaves and other fauna are at full bloom.

In the trials, different paths can be used which depend on the operational requirements from the involved end users. This can be done by means of predefined waypoints, manual flight, etc., in order to test the capabilities of the DTI systems. Curved or straight-line approach patterns as well as zigzag ones are to be used within the monitored area (see Figure 49). It should be mentioned that another critical aspect is the drone speed along the path versus the working rate of the DTI systems. Then, the same paths should be executed at different drone speeds during the tests to check the impact on the performance of the DTI systems.

For waypoint flights, the actual trajectory will depend on the on-board controller, kinematics and dynamics of the platform and environmental conditions, wind being the most significant disturbance. Then, straight segments between predefined waypoints should not be considered as the ground truth for evaluating the performance of DTI systems. Instead, the same model of GPS logger should be used on-board all the drones during the tests. The accuracy of the test will never be better than that of the ground truth.
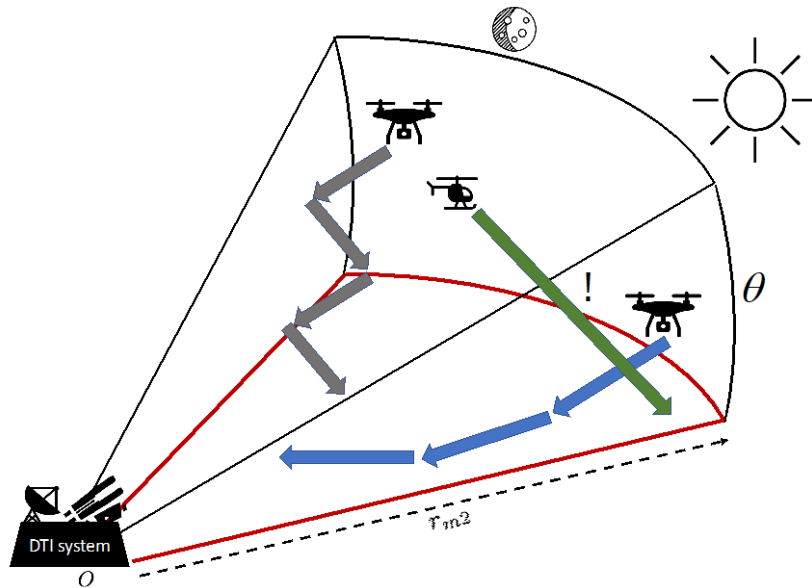
Figure 49 — Trajectories of the drones withing the volume covered by a DTI system

For example, Figure 50 shows a zig-zag flight pattern in manual control mode of a DJI 210 RTK drone during the first COURAGEOUS trial in Greece.

Figure 50 — Zig-zag flight paths of a DJI 210 RTK during a test on 8th March 2023 in the first trial used as ground truth for the DTI systems performance evaluation

For waypoint flights, the actual trajectory will depend on the on-board controller, kinematics and dynamics of the platform and environmental conditions, wind being the most significant disturbance. Then, straight segments between predefined waypoints should not be considered as the ground truth for evaluating the performance of DTI systems. Instead, the same model of GPS logger should be used

on-board all the drones during the tests. The accuracy of the test will never be better than that of the ground truth (see subclause 12.5.7).

The test script might include from one to several different types of drones flying simultaneously, according to different scenarios and threat levels. The test will evaluate the ability of the DTI system to detect, track and identify various UAS at the same time. Finally, some tests may include spoofing devices which generate "ghost" or "fake" drones to measure the impact on the DTI systems' performance.

12.5.3 Environment clutter

The following elements should be considered:

- Surrounding settlement: takes into account the settlement conditions around the asset. Possible scenarios include dense settlement (urban area), light settlement (suburban area), rural area, and industrial areas.
- Vegetation: refers to the presence of vegetation around or on the terrain of the asset to be protected as it can exert influence on the detection capability of the drone. Possible states of this factor include the options of no vegetation around the asset, isolated vegetation, or dense vegetation. In particular, Clause 6 states that single trees and forest walls should be present in the test environment.

Different obstacles can be present in the environment and will be characterized by their geometries and materials. These obstacles can be static or dynamic such as the vehicles in a highway in the vicinity.

All the clutter conditions described above should be registered during the tests, for instance building (or updating) a texturized Digital Elevation Map.

12.5.4 DTI systems under test

Ideally, all the DTI systems should be installed within the designated area in the trial field. Exact place of each sensor within the designated area should be determined by the installation specifications for the system to achieve its best performance possible combined with the end-user operational requirements. However, the installation should not interfere with other sensors in the same trial, nor affect their normal operation. In general, direct emissions from one sensor to other must be avoided or minimized. Active systems working within the same frequency range should be installed as far from each other as possible. In addition, If the power level of a DTI system is increased, then the impact on other C-UAS systems' performance within the environment should be checked to ensure no operational interference. Finally, the infrastructure needed by one system must not obstruct other systems line of sight to the monitored area.

The trial organizers must coordinate the installation efforts to assure a fair location for the sensors of the DTI systems and will ask the participants to share, before the trial dates, the installation diagrams or requirements regarding positioning, space, dimensions, frequency incompatibilities, power, internet connection, etc. Based on the real and/or simulated information about the monitored area shared with the participants, they might suggest the organizers the best installation place within the designated area. It is the responsibility of the DTI system team to provide the required information and install the system in the final designated spot.

Another important aspect to point out is that the deployment of a given DTI system during the tests will be different from the real deployment under real conditions. For instance, it is possible that in a real deployment, several sensors spatially distributed are networked to cover a greater area. Then, for DTI systems with different area coverage, the increase in the cost to achieve similar areas based on the deployment of more sensors should be taken into account for budget comparison purposes.

12.5.5 DTI output data recording

During the test, the output of the DTI system should be recorded to enable performance evaluation of these DTI systems. The data format that should be used to log the information from the DTI systems during their operation should be specified and made available for DTI companies prior to the trial. An example is given in Figure 51 and Annex H).
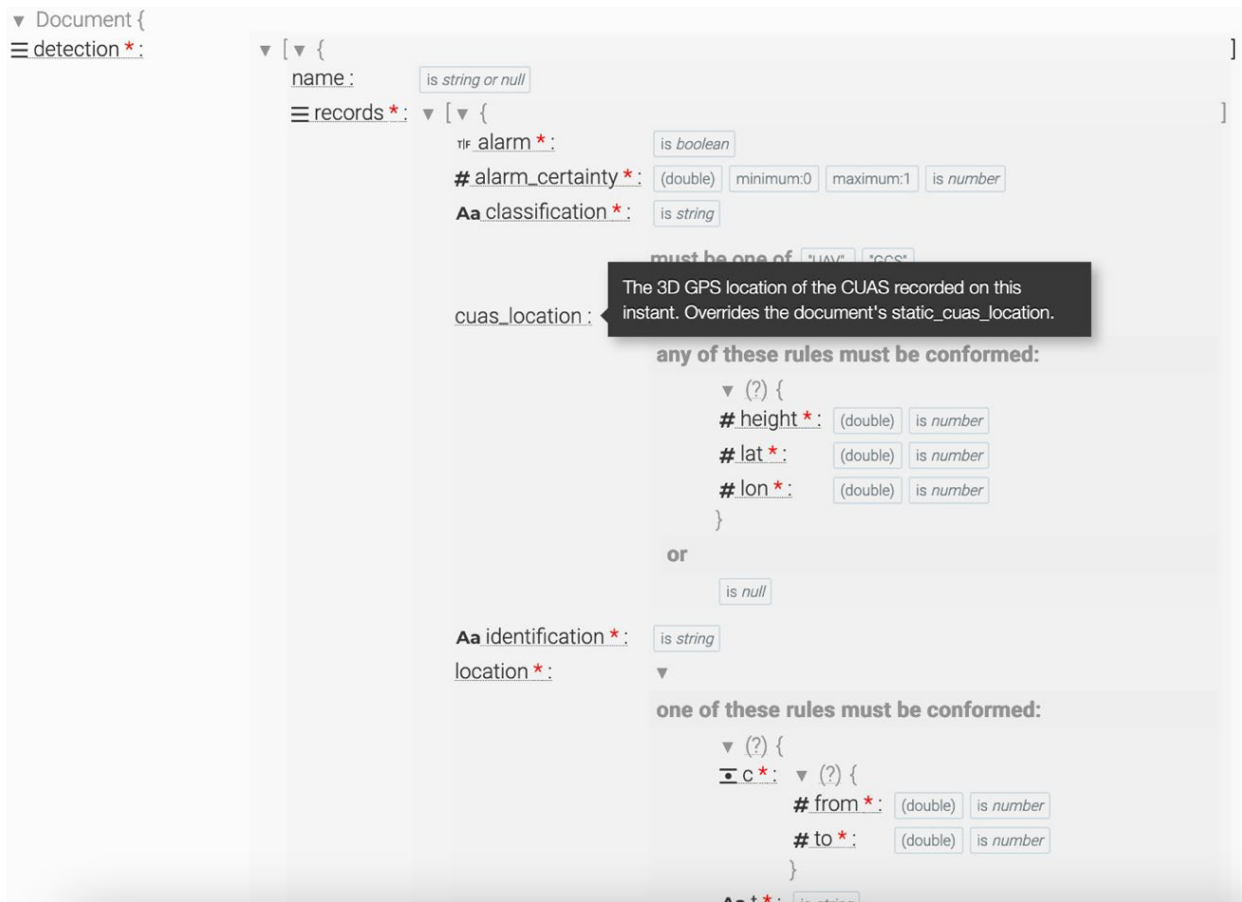
Figure 51 — An example of the data format specification for DTI companies

From the lessons learned in the COURAGEOUS trials, a structured format has been chosen as opposed to e.g., a table, as data scopes can vary. For instance, the version of the format is global to the document, whereas the elevation of a point is specific to a single data point. Using a structured format also allows easily extending it without breaking backwards compatibility. JSON format has been chosen due to its simplicity and number of libraries available for writing and parsing data.

All the DTI systems should preferably be connected in a local area network (LAN) to a storage system to log all the data for the performance evaluation.

12.5.6 Time synchronization

Time synchronization is essential to determine accuracy of detection, tracking and identification. The test environment should include some mechanism based on hardware/software and/or a procedure to ensure time synchronization among all the relevant systems involved in the tests.

Time synchronization should be achieved with a level of accuracy that will depend on the maximum speed of the involved UAS. The goal is to record all the relevant data during the tests with temporal synchronization to enable the possibility to compare the estimations provided by the DTI systems with the ground truth.

One option to achieve this synchronization is to use the Network Time Protocol (NTP) that is widely employed to synchronize a computer to Internet time servers or other sources, such as a radio or satellite receiver or telephone modem service. It can also be used as a server for dependent clients. It provides accuracies typically less than a millisecond on LANs and up to a few milliseconds on WANs, which are considered enough for the test environment. However, it implies to install a NTP client on the different DTI systems involved. If this is not possible, an alternative is to create a procedure to be followed in the setup of the DTI system, so it connects to the Internet for instance until it is synchronized via a remote public NTP server.

In all the cases (for the drones, the C-UAS systems, the weather and RF logs, etc.), the date and time of the logged data should be Zulu time: Universal Coordinated Time (UCT), sometimes called Universal Time Coordinated (UTC) or Coordinated Universal Time (but abbreviated UTC).

12.5.7 Ground truth

Ideally the ground truth will be based on the real positions of all the UAS along time during the tests with differential GNSS accuracy. However, in practice, the on-board GNSS loggers and/or the commercial UAS that will be used during the tests will provide telemetry with lower accuracy. It is a good practice to use the same model of GPS logger on-board all the drones during the tests. Also, the same GPS logger should be used to measure the global position of the sensors of each DTI system participating in the trial. In addition, the telemetry recorded should be synchronized with all the data recorded by the DTI systems. This can be achieved with the NTP server based on GPS time connected to the Local Area Network of the DTI systems and using GPS time to timestamp GPS loggers' data.

12.5.8 Evolution in time

The evolution in time of the different actors determines the following parameters:

- Number of simultaneous UAS flying. Clause 6 explains that when testing C-UAS, it will also be necessary to assume a reasonable number of targets to be tracked. It is proposed to have not less than 20 targets, because it will allow to check the declared limit parameters for at least 25% of the C-UAS manufacturers who have specified the tracking process.
- Speed of the UAS along the paths. It should be mentioned that the Clause 6 states that the maximum and minimum speed of detected UAS are not usually specified by the manufacturers.
- Radiofrequency signals and/or noise evolution over time
- Weather conditions during the tests including visibility
- Environmental lighting conditions along the day

Then, ideally all the DTI systems should be tested during the same periods, so the weather conditions and other uncontrolled variables such as environment noise, electromagnetic interference, presence of birds, etc. are the same. This is feasible for passive DTI systems, but for active DTI systems, i.e. radars, the tests should be done in sequence. Then, the evolution in time of the above mentioned stimuli should be properly logged so the test methodology can take it into account in the comparison of the DTI systems results.

13 Performance evaluation of C-UAS systems

13.1 General

Based on the scenario's provided in Clause 7, a generic performance evaluation methodology for C-UAS systems has been drawn up upon operational needs and functional & performance requirements as provided by Clause 8 and Clause 9 respectively.

The test methodology is detailed towards Detection, Tracking and Identification, taking into account relations that exist between the three. Note that identification in the context of this clause denotes classification of objects of interest (malicious drones). The test methodology covers performance evaluation for the full functionality of the DTI systems.

The test methodology is developed to enable the use of the methodology in a relevant environment, thereby taking into account any potential environmental aspect that might influence DTI system performance. In addition, the test methodology is developed with the ability to use any available realistic test terrain. The methodology is drawn up to reveal the performance of the functions in interaction with each other, takes the presence of the DTI operator into account, and supports full DTI operation either with real or simulated data.

The test methodology is based on the evaluation of the interaction between the test environment described in Clause 12 and the DTI system and is suitable both for in a simulation environment and in a relevant operational environment. The architecture presented in this clause shows how the methodology relates to the scenario and contextual information (e.g., environment), capturing of the integral DTI system output and the generation of evaluation-based and end-user weighted scores for the DTI system under test.

It should be mentioned that the consistency of the data recorded should be done on-site by gathering the trajectories recorded by the UAS during each exercise and the tracks recorded by the C-UAS. After converting them to a common format such as KML, it is possible to visualize them together a long time to detect any issues such as problems with time synchronization, different references for the altitudes, deviations from the UAS flight paths planned in the tests' scripts, etc. This consistency checking task requires a team where different responsibilities and roles are defined. An example of such division of roles during the tests can be found in https://www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf

In addition, the order in which the test scripts are executed along with the digital timestamping of the UAS and C-UAS data recorded allow to identify which test script is under execution during the exercises."

13.2 Operational needs and functional requirements

The operational needs and functional requirements that are defined in Clause 8 form the baseline for the standardized test methodology. The majority of operational needs can be translated to operational requirements and can be summarized as "the ability to detect and counter any drone, of any size, exhibiting certain behavior in different environmental conditions".

Using the operational requirements, a set of functional and performance requirements have been derived (Clause 9). The operational needs translate into functional requirements for a DTI system that can detect, track, identify (and classify) any drone, of any size, exhibiting certain behavior in different relevant environmental conditions. The functional requirements provide a baseline against which DTI systems tested and evaluated. DTI system functional breakdown, expected behavior of the system and its components are essential for defining relevant set of performance evaluation metrics. A set of operationally relevant scenarios have been chosen to verify the functional requirements.

13.3 Decomposition of DTI systems

13.3.1 General

The availability of cheap commercial off the shelf (COTS) UAS in recent years has led to potentially more threats to the traditional perimeter defence of civilian and military facilities, critical

infrastructures and public events[13]. Equally, there has been much emphasis on developing and deploying C-UAS systems capable of detecting, tracking, identifying and countering threats posed by these UAS. There is currently a wide variety of DTI systems available comprising of different subsystems and solutions. The common denominator for all DTI systems is the ability to detect an UAS at a given range, translate the detection into a track over a period of time and potentially classify the UAS. As a matter of fact, a DTI can be decomposed into three main functional components (see Figure 52):

- Detection functionality

- Tracking functionality

- Identification functionality

In the following sections, these subcomponents (detection, tracking and identification functionalities) are further detailed where emphasis is given to the relationship between the different functionalities. A high-level DTI system overview depicting the three main functionalities is given.
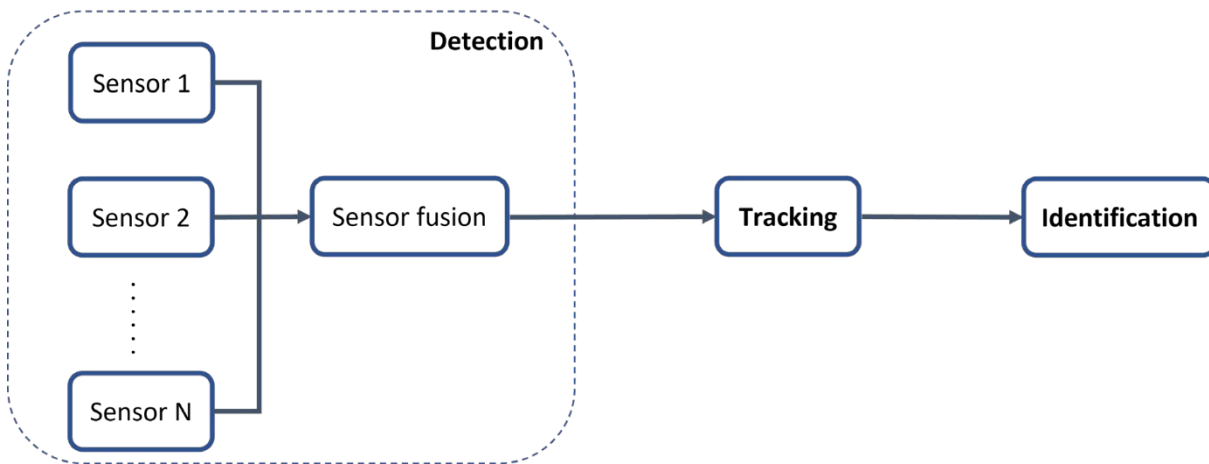
Figure 52 — DTI system decomposition

The test methodology is based on a black box approach for the DTI system. It does not interfere with the DTI's internal processing, nor will it measure and evaluate internal signals. Only if those signals are externally available and directly relate to a property that is known to the tester, it will be considered as part of an evaluated property.

13.3.2 Detection functionality

Detection of objects is performed by detection of a signal received from the object. This can either be a signal emitted by the object, or the reflection of a signal by the object. Detection can be improved by integrating a time series of this signal or by the extraction of features present in this signal. Analysis of those features leads to an estimation of object's state (e.g., position, speed, size).

One of the attributes that are relevant in detecting a UAS could be the presence of rotors (combined with the absence of flapping wings), and of course position is an overarching attribute. The attributes in turn relate to a specific domain in which the attribute is "visible" or "detectable". For the domain active and passive sensing were distinguished. Active sensing is based on detection of a signal transmitted by the DTI system and reflected by the drone, where passive sensing is either based on emission of the drone itself or on reflection by the drone of energy of another source ("daylight").

---

[13] System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment, Choon Seng Tan, Douglas L. Van Bossuyt, Britta Hale, November 2021

The domain also relates to wave domain (e.g., acoustic, electromagnetic, magnetic, seismic). For each sub-function the attribute and the domain will be derived.

Often a DTI system comprises of more than one sensor. In that case, sensor information is fed to a sensor fusion process. Sensor fusion combines all sensor signals that correspond to a given target. For that target an evaluation of each attribute is made, based on values as determined by each sensor. Every sensor has own specific attributes, e.g., radar can determine Doppler spectrum and hence rotors, camera can determine size, and communication interception can reveal ID number. The test methodology concept is domain agnostic.

13.3.3 Tracking functionality

Tracking of objects – also known as object assessment – is an important functionality of DTI systems. The tracking of objects builds upon the output of the detection functionality and can be done using a single sensor or combination of various sensors. The end result of the tracking functionality contributes to the creation of an operational picture. For a useful and comprehensive operational picture, the following features can be considered:

- Range: the range at which a DTI produces a track of an object after its detection.

- Continuity: an object shall be represented by a single track (instead of being represented by several partial tracks). A measure indicating that track number assigned to an object does not change.

- Completeness: Operational picture is complete when all objects (in the area of interest, in range) are detected and tracked.

- Accuracy: kinematic accuracy is achieved when the position and velocity of each assigned track agree with the position and velocity of the associated object.

13.3.4 Identification functionality

The identification process shall provide information that enables the end-user to make a reliable decision to start counter drone actions. This information shall be contained in the classification of the drone provided.

This function uses the attributes of the detection functionality and the related track as input and can enrich this information with historical data and data available for the drone (e.g., internet, databases). Classification of the drone might be based on Artificial Intelligence (AI) techniques that perform the required (often complex) functions. The end result of the identification functionality, in combination with the tracking functionality, constitutes to the creation of a recognized picture.

13.4 Performance evaluation of DTI systems

13.4.1 General

The main objective of the performance evaluation methodology is to enable the end-users perform a fair evaluation of DTI systems using relevant use cases and operationally relevant conditions. The test methodology should allow for an objective and standardized way to evaluate whether the DTI system under test meets the user needs. The corner stones for the test methodology and corresponding performance evaluation can be summarized in the following elements:

- Development of a test methodology for testing of integrated DTI systems and their sub systems under realistic conditions and using relevant end-user defined scenarios.
- A methodology that enables the end-users to evaluate a DTI system and thereby helps addressing whether the system meets operational needs and requirements from the end-user perspective.

- A future-proof methodology which means that the test methodology can be adjusted to test and evaluate future DTI systems and needs that may arise.

13.4.2 The DTI under test in relevant environment

The proposed test methodology is based on performance evaluation of a DTI systems under test in its actual environment which includes objects of interest (e.g., malicious drones) to be detected and other relevant actors. The interaction between the DTI system and the various aspects of the environment is shown in Figure 53.
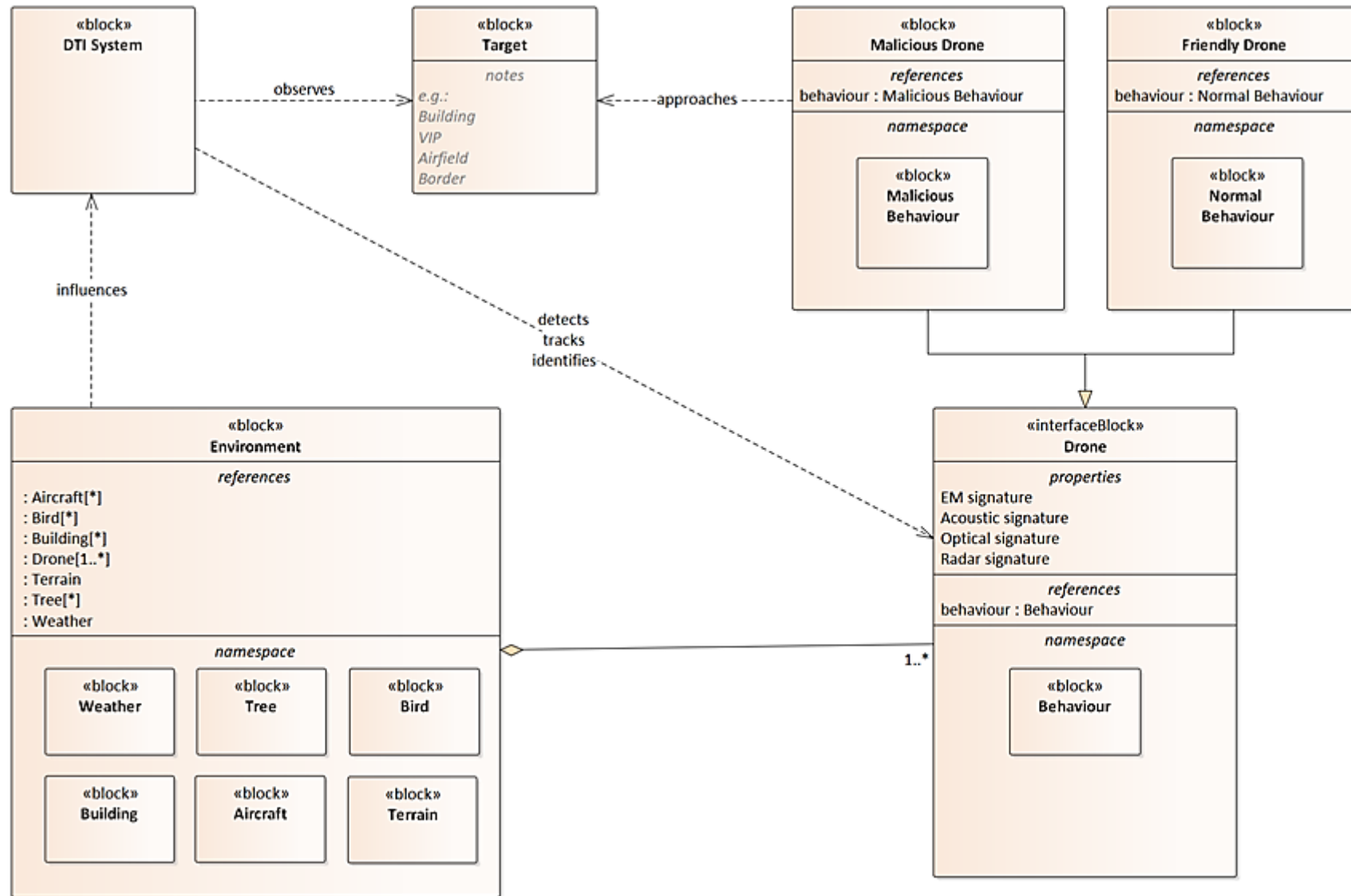
Figure 53 — DTI under test interaction with its environment

The DTI interaction with the environment overview depicted in Figure 53 contains the following components:

- DTI system representing the detection, tracking and identification system that is under test in a relevant environment
- Drones can be present in the test environment that have certain behaviour (e.g., friendly, neutral, malicious). Also, the drones can generate EM emissions. Drones can be detected based on their emissions and on the signatures, they have when illuminated (either by already present electrical, optical or acoustic radiation, or by illumination by the DTI system).
- Target (Area of Interest) depicting the area to be observed by the DTI system which is linked with a specific scenario (e.g., building, VIP, airfield, border)
- Various factors from the environment that can influence the DTI system performance (e.g., weather, buildings, birds, aircraft, terrain and trees). Moreover, the environment can be polluted by EM emissions (e.g., WLAN, 4G).

13.4.3 Flexibility in testing

The COURAGEOUS test methodology has to be flexible in the sense that it can easily be used by an end-user to evaluate C-UAS systems. This implies the test methodology can easily be applied in various test locations under various environmental conditions. The ability to adapt to conditions and test locations is a common approach for system testing. Usually, the system performance is determined under "ideal", or "standard" conditions called a baseline. Specifications are in most cases given "under standard conditions". The performance under actual conditions can then be estimated using available existing software and based on the baseline performance while adding the influence of the actual conditions. This estimated actual performance can be evaluated by actual measurements.

Example: *Radars are specified under free field conditions (nothing around that could interfere with radar performance. Also, the horizon is considered to be absent) The actual performance is then estimated, for example using the program CARPET (www.tno.nl/carpet). This program takes into account the horizon (depending on antenna height), sea and land clutter, rain, terrain shadowing etc. This calculated performance can be compared to actual measurements.*

The ideal conditions for testing DTI systems could just be just the sensor and the drone, nothing between them, even not an earth surface present (this resembles the example with radar and free field conditions). The standard condition for testing DTI systems could be flat earth with only low vegetation (with no significant influence on DTI performance. E.g., a flat desert), no birds, no people, no traffic, no buildings. Note that standard and ideal conditions resemble each other strongly. In this clause, the term "standard conditions" is used.

Note: in addition to baseline performance, manufacturers might also specify how well their system handles non-ideal conditions, e.g., how well the system suppresses nuisance alarms caused by weather conditions such as rain, or by birds.

13.4.4 Baseline testing

With the baseline testing the performance of DTI systems can be tested and evaluated under given set of (standard) conditions. Performing baseline testing is relevant for DTI manufacturers, to evaluate system specifications. It is however of little relevance to end-users; they merely use the results (system specifications) provided by manufacturers.

Baseline testing usually comprises different test for each "ideal condition". Test might be performed in an anechoic room or optical corridor (meeting the ideal condition of no interference by anything).

Other test point sensors to a location up in the sky, mimicking the absence of earth while detecting actual targets (drones, aircraft) at a distance. This phenomenon (only testing one parameter in a given set-up) renders this particular approach unsuitable for overall system tests.

13.4.5 Actual performance testing

Actual performance testing is very relevant to end-users. It determines the performance of a system taking relevant specifics into account, like actual DTI positions, actual buildings, birds and vegetation, actual sources of nuisance alarms (e.g., fans, air conditioners, cars), the presence of people and EM interference (e.g., 4/5G, Wi-Fi). Actual performance testing is less important to manufacturers, except if conditions are comparable for a multitude of similar locations (e.g., on airports, they all have runways and have to adhere to the Building Restriction Area). Actual performance test results can be compared to that of the baseline performance depending on availability, considering relevant aspects that degrade DTI performance.

13.4.6 Performance evaluation pipeline

The proposed performance evaluation is based on the following key elements:

- Use of relevant end-user defined test scenarios that contain, for instance, contextual information, objects that are to be secured and what the success criteria is.
- A set of evaluated metrics that, starting from the results of a test or a collection of tests, provide a score to the DTI system under test including its components.
- An evaluation that is updated every time a new test iteration has been executed.

The functional pipeline for the performance evaluation of DTI systems is illustrated in Figure 54.
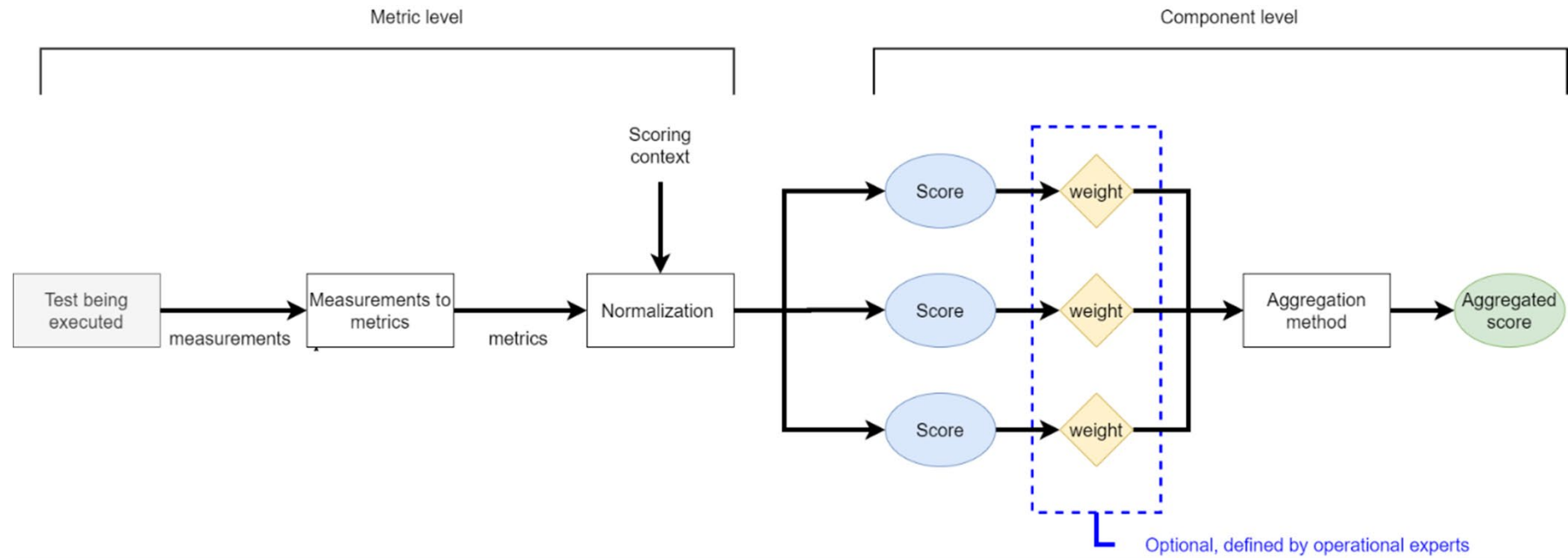
Figure 54 — Performance evaluation of DTI systems

The performance evaluation pipeline shown in Figure 54 can be grouped into two main categories, namely, metric level, and component level.

- **Metric level**: The metric level starts with tests being executed based on the scenarios. The *measurements* emanating from these tests are captured and translated into a set of *metrics*. At the metric level, the performance of a specific metric (e.g., detection range, track continuity) is evaluated. These metrics are then interpreted and normalized into a *score.* In order to know how to score the desired metric, a '*scoring context*' can be added. This scoring context provides information about what is operationally desired (success criteria) for a given metric in a given context. In the end, the *normalized* score between 0 and 1 is calculated, where 1 is the best possible score and 0 the worst score.
- **Component level**: At the component level, normalized scores calculated at the metric level are used. The component test level gathers all scores belonging to a specific functionality (detection, tracking, identification or combinations of these components). These *scores* are optionally *weighted* based on operational end-user prioritization and then aggregated. The result is an aggregated score for that specific functionality. A rating is created based on the scores of single tests, on the scores per capability and KPIs based on operational needs. The rating is updated every time a DTI system is tested.

13.4.7 Performance metrics

An overview of the metrics that are defined for the performance evaluation of DTIs is provided in this subclause. The metrics are grouped into Detection functionality metrics, Tracking functionality metrics and Identification functionality metrics.

Detection metrics: In table 65, the metrics that are defined for the DTI detection functionality are given. These metrics involve location estimation accuracy, range ratio and precision.

Table 65 — Detection functionality metrics

Metric name	Metric description
Location accuracy (2D/3D)	The location accuracy of a detection representing a true object is defined as the distance between the detection and the true object. The metric is undefined for detections which do not represent a true object.
Range ratio	The relative minimum and maximum detection range of a true object is defined as the minimum and maximum distance of the detections representing the object from the DTI system normalized for the minimum and maximum range of the true object within the Area of Interest (AoI) from the DTI system.
Precision	The precision of detections is defined as the fraction of all detections which represent a true object.

Tracking metrics: In Table 66, the metrics that are pertained to the DTI tracking functionality are provided. These metrics cover aspects of the tracking functionality that are relevant for getting a complete, continuous picture of the AoI.

Table 66 —Tracking functionality metrics

Metric name	Metric description
Track completeness	The track completeness of a true object is defined as the fraction of time in which the object is represented by at least one track.
Track continuity	The track continuity of a true object is defined as the total number of tracks representing the object. The metric is undefined if the true object has no tracks representing the object.
Track ambiguity	The track ambiguity of a true object is defined as the time-weighted average of the number of tracks representing the object during the time the object has at least one track representing the object. The metric is undefined if the true object has no tracks representing the object.
Track spuriousness	The track spuriousness is defined as the time-weighted average of the number of tracks not representing a true object at that time.
Track velocity accuracy	The track velocity accuracy of a true object is defined as the Root Mean Square (RMS) velocity difference between the tracks representing the object and the true object. The metric is undefined when no track represents the true object.
Track positional accuracy	The track positional accuracy of a true object is defined as the RMS distance between the tracks representing the object and the true object. The metric is undefined when no track represents the true object.
Longest track segment	The longest track segment of a true object is defined as the largest fraction of time in which the object was represented by the same track while being in the AoI.
Tracking immediateness	The tracking immediateness is defined as the difference between the time at which an object enters the area of interest and the time of its first associated track.

Identification metrics: A set of metrics defined for the identification functionality of the DTI is given in Table 67. These metrics cover probability of detection, false alarm rate and precision.

Table 67 —Identification functionality metrics

Metric name	Metric description
F1	The F1-score is defined as the harmonic mean of precision and recall.
False Alarm Rate (FAR)	The false alarm rate is defined as the fraction of falsely given alarms out of the total number of alarms.
Missed Alarm Rate (MAR)	The missed alarm rate is defined as the fraction of alarms the DTI did not emit out of the total number of alarms it should have emitted.
Probability of Detection (POD)	The probability of detection is defined as the number of times in which the DTI system emits the alarm (detect the object) rightfully, divided by the total number of alarms it should have emitted (i.e., times that the event happened).

Each of the metrics given earlier results in a number (a measurement) which has no evaluation yet. For example, the metric Track ambiguity measures the number of tracks assigned to a true object. If the Track ambiguity metric calculation results in 4 tracks for a true object, there is no judgement on this value yet. The evaluation is done in the scoring phase in line with the performance evaluation depicted in Figure 54.

Building upon all the components introduced in the previous clauses for the test methodology and the performance evaluation, how the methodology relates to the scenario and contextual information (e.g., environment), capturing of the integrated DTI system evaluation is illustrated in Figure 55.
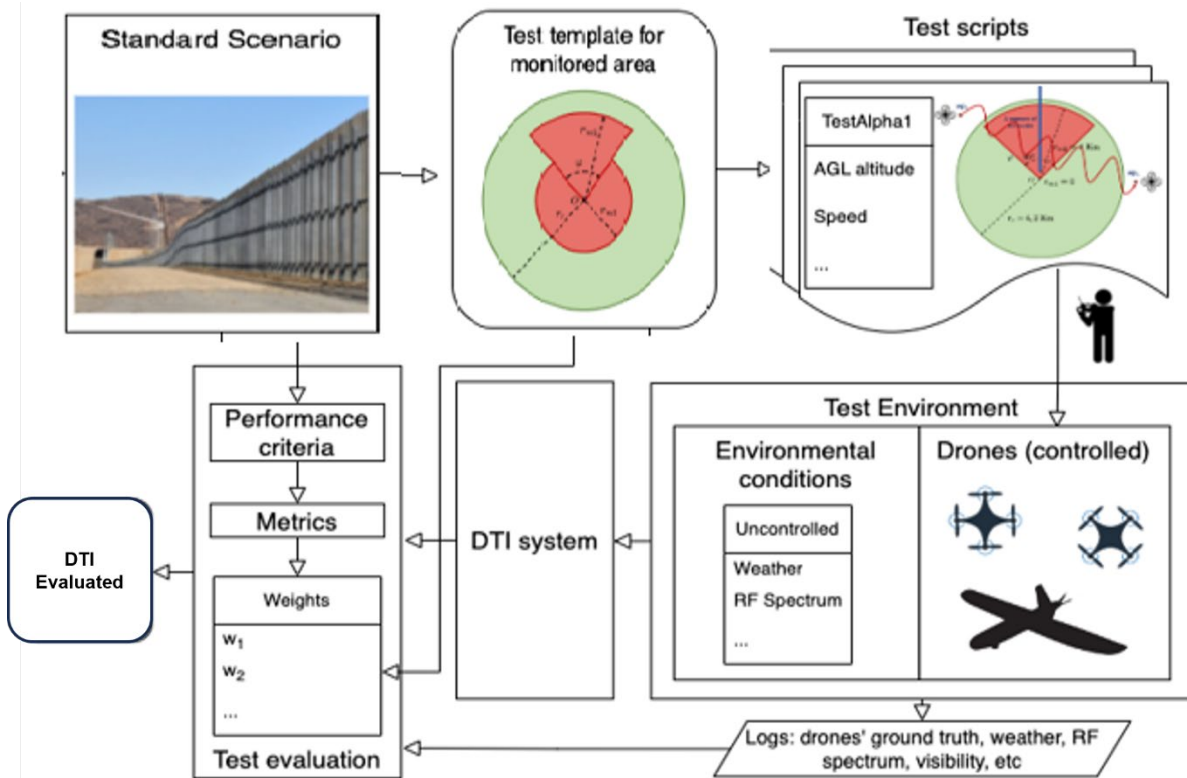
Figure 55 — Integrated performance evaluation pipeline

13.5 Validation method

In this subclause, a validation method for the test methodology and corresponding performance evaluation of DTI systems is presented. The approach contains tow main concepts:

- A simulation-based validation approach to authenticate the developed test methodology and corresponding performance evaluation in a simulation environment that facilitates sensitivity tests.

- A trial-based validation approach to verify the test methodology and corresponding performance evaluation in an operational environment with relevant scenarios.

13.5.1 Simulation based validation

13.5.1.1 DTI models

The main purpose of defining the validation method is to enable sensitivity analysis for the developed test methodology. In order to validate the test methodology, availability, and use of representative models of DTI systems is of paramount importance. These models can allow configuration of the DTI model parameters enabling sensitivity tests. The consortium has investigated the availability of such DTI models. Due to the proprietary nature of the DTI systems, no DTI models are available. In order to circumvent the unavailability of DTI models, a basic model of a generic DTI system has been defined and implemented for the validation method.

In the simulation-based validation approach, no models for Electromagnetic (EM) emission and weather-related aspects are available and hence these are not addressed. Note that, during trials, the actual EM emissions and weather conditions are recorded and considered for the evaluation of demonstration data analysis.

13.5.1.2 Simulation test framework

A concept of a test framework has been defined building upon the test methodology presented earlier. This framework enables the validation of the test methodology and the corresponding performance evaluation. The test framework depicted in Figure 56 contains the following main components:

- Test environment dealing with scenario's including environmental aspects (e.g., trees, buildings) and objects of interest (drones).

- System under evaluation representing the DTI system that is to be tested and evaluated. A basic non-physical model of a DTI system has been created with detection, tracking and identification (i.e., alarm generating) capability.

- Test suite covering the test methodology and corresponding performance evaluation using the defined metrics.
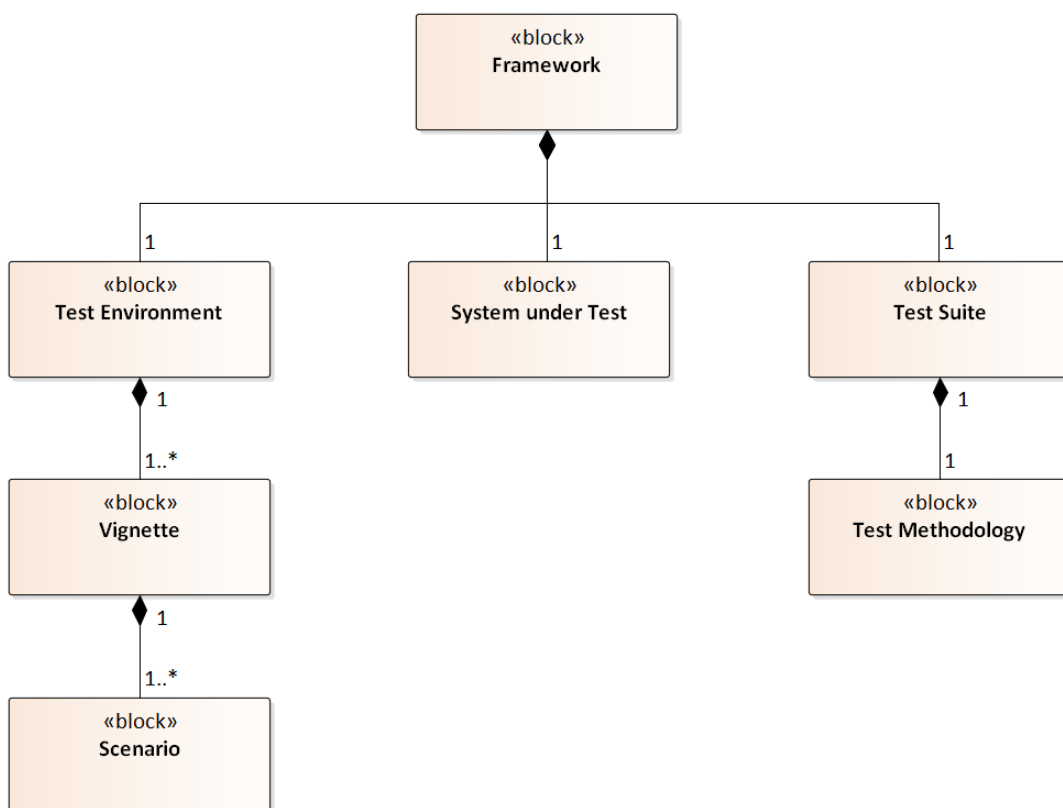
Figure 56 – Simulation test framework components

13.5.1.3 Test environment

The test environment can be virtual (a simulation environment) or a physical test terrain where the DTI system under test can be deployed for testing purposes (i.e., trial-based validation). An underlying requirement for the evaluation of the DTI system under test is the inclusion of representative environment which includes objects of interest (e.g., neutral traffic and malicious drones) to be detected and classified. The interaction between the DTI system under test and the various aspects of the environment has been given in subclause 13.4.1. This test environment concept can be used for both virtual and physical validation of DTI systems. The concept also facilitates the storing of test data (e.g., ground truth data of objects in the environment, output of DTI systems like detections, tracks, and identification) and logging of relevant settings (e.g., position of DTI systems).

13.5.1.4 Simulation test suite

A test suite tailored for the simulation-based validation has been developed. This test suite given in Figure 57 enables the execution of a number of standardized tests and generation of stimuli. After the execution of the tests, evaluation of the results of the system under test is carried out. The main components of the test suite are:

- Predefined series of tests with a range of scenarios that are executed under controlled conditions in various vignettes to derive metrics generated from results of system under test (DTI output). These metrics are used to evaluate the system in a standardized and repeatable fashion. A test-coordinator is responsible for selecting which test is executed, preparing the test environment, starting the test itself and retrieving results.
- Test environment for generating stimuli, providing the DTI model with necessary input, and producing DTI output results.
- Performance evaluation process that – based on the output of the system under test during the standardized tests – comes up with a scoring of the system of interest on all tested levels.
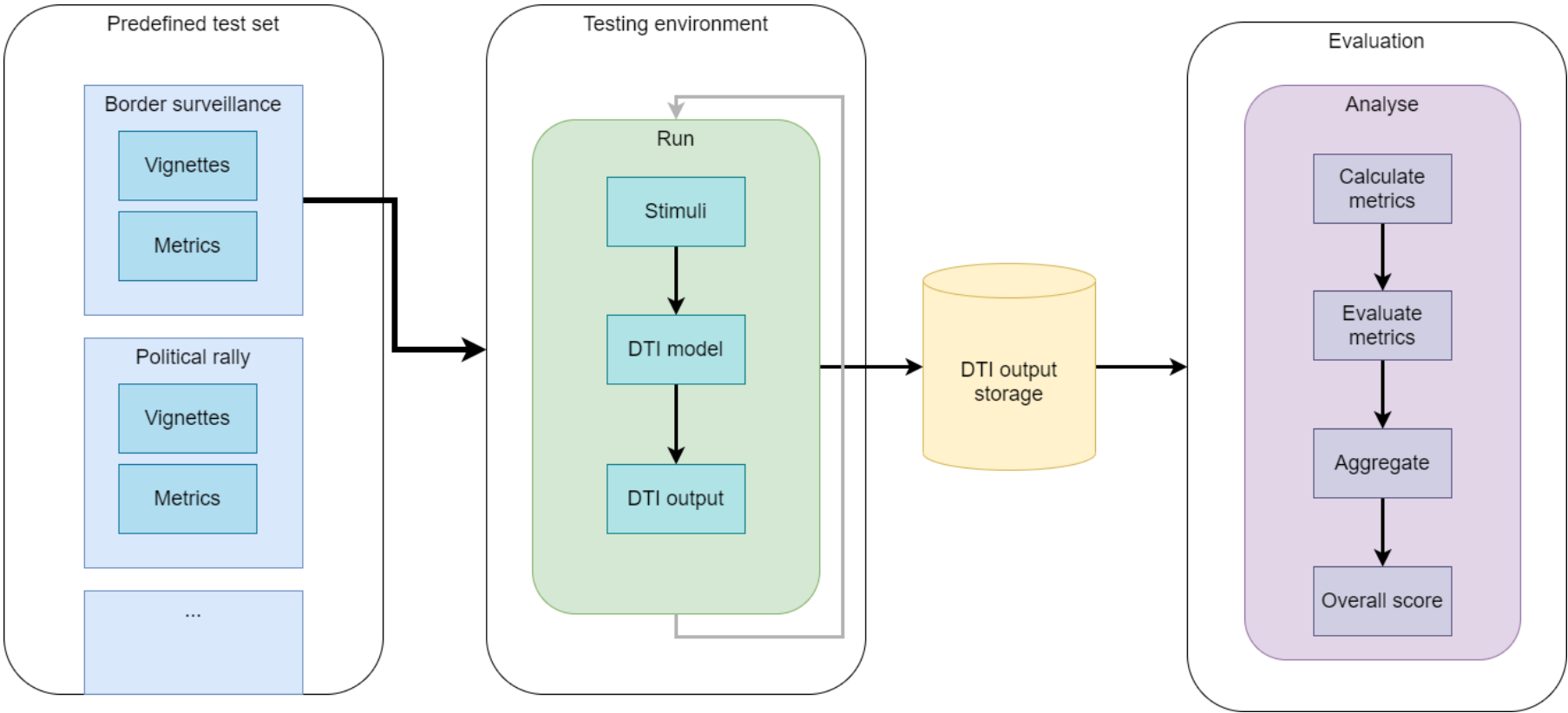
Figure 57 – Simulation test suite

From the predefined test sets, the scenarios to run and the stimuli to be created should be known. Based on this information, multiple runs of the same test can be carried out in the test suite. From each of these runs, output of the DTI model is generated and stored for the evaluation process. In this process, first the metrics are calculated and subsequently evaluated taking into account end-users' operational context. The evaluated metrics can be aggregated to come to an overall score for the DTI in that specific test scenario.

The test steps that cover all the necessary elements for the validation method are given in Figure 58:

- Test configuration: the testing starts by loading a pre-defined test configuration.
- Load environment: A configuration file that defines which scenarios are run and how many iterations per scenario are required.
- Test execution: during an iteration, a test is executed. Execution of the test in the test environment means generating stimuli (neutral and malicious drones), obstacles (trees, buildings) and providing this information to the available DTI models.
- DTI output: Upon generation of input to the DTI, the DTI models provide their output in terms of detections, tracking and generating of alerts. This output contains metrics such as detection range and track continuity.
- Store data: The output of the DTI models is stored for analysis.
- Performance analysis: Carry out performance evaluation based on the DTI output. In case the iterations of a scenario are done, a new scenario is loaded, and new tests are performed, until all tests specified in the test configuration are handled.
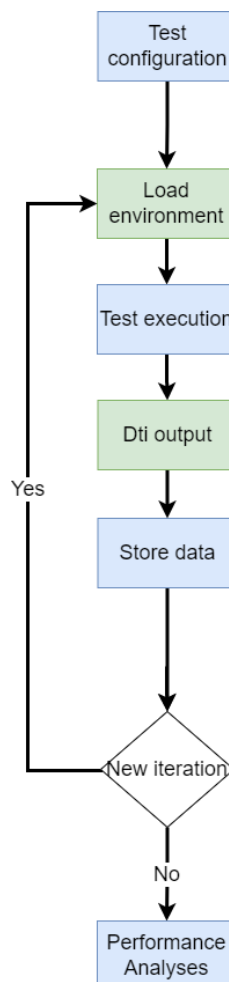
Figure 58 – Simulation test pipeline

13.5.2 Trial-based validation

13.5.3 Trial demonstration data processing and evaluation

The main objective of the trial-based validation is to authenticate the developed test methodology and corresponding performance evaluation. The insights that have been gained during the definition and development of the test framework are used as an input to the trial-based validation approach. For the trial-based validation, operational trials should be organized and executed using relevant scenarios (relevant environment, drones exhibiting both neutral and malicious behaviour) and DTI systems. A processing and evaluation pipeline for the trial data is given in Figure 59. In this pipeline, the following steps can be identified:

- Collection of DTI output (detections and tracks) and ground truth from the flying objects (e.g., drones) from the demonstration trial. Availability of reliable ground truth data is a key enabling factor of DTI system performance evaluation (see 12.5.7).
- Parsing of the collected data (i.e., DTI output and ground truth).
- Pre-processing of the data (e.g., time window filtering, transformation of coordinate system and selection of AoI).
- Association of detections and tracks to the ground truth data.
- Calculation of detection and tracking metrics.
- Inclusion of end-user context (e.g., weighting of metrics).
- Generation of a score per DTI.
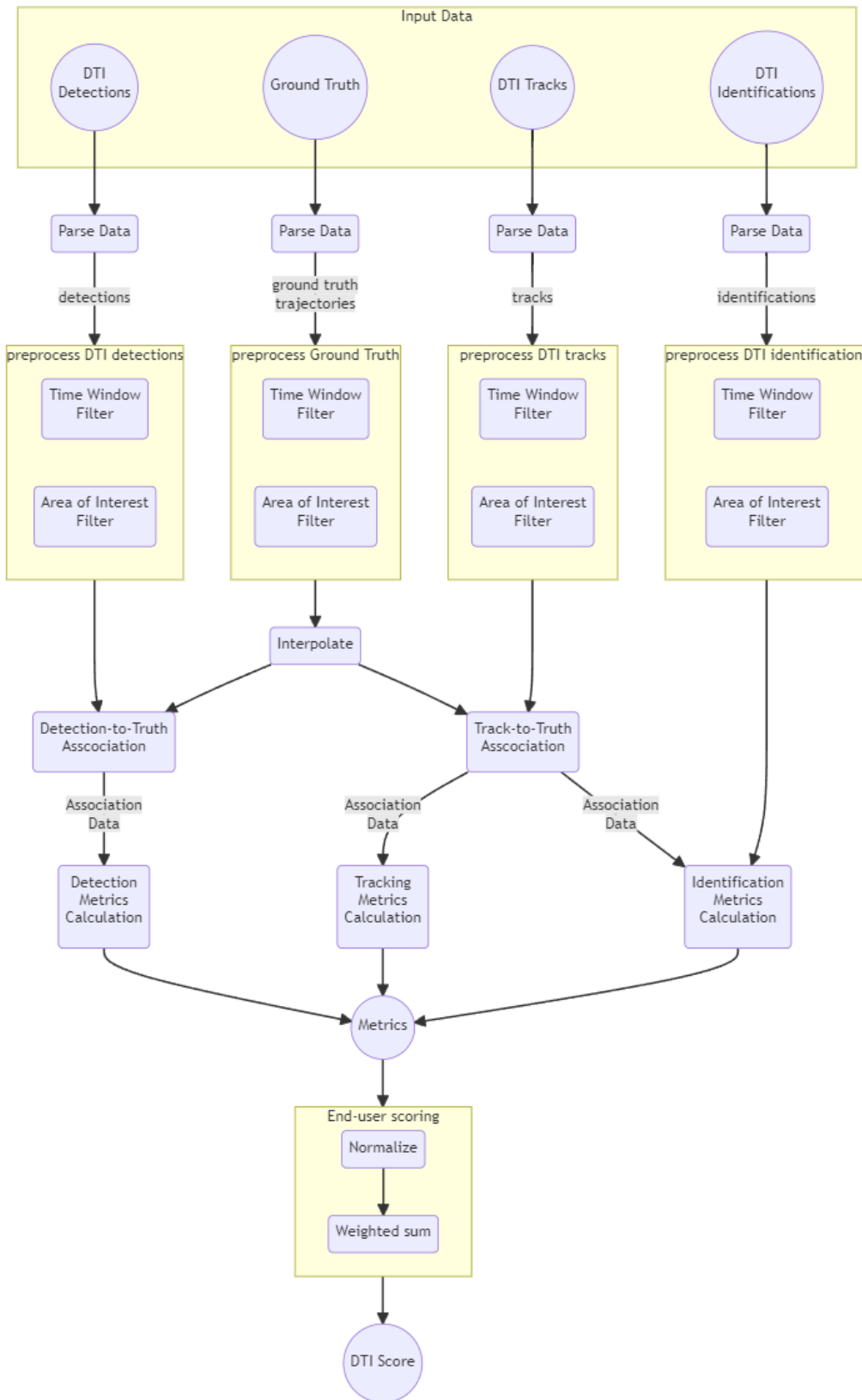
Figure 59 – Trial data processing and evaluation pipeline

Annex A
(informative)

Examples of scenarios for C-UAS systems testing methodology application

The ten (10) standard scenarios that were developed are grouped into the following three (3) main categories:

- Sensitive Sites/Critical National Infrastructure
- Public Spaces Protection/Events
- Border Protection (Land – Maritime)

These scenarios can be considered as representing realistic events occurring in C-UAS domain and involve multiple actors, incorporate one or more events or activities and address multiple use cases.

The template employed for the presentation of the standard scenarios was used by consortium partners so as to define the standard scenarios. The template includes the factors of an incident. For these areas, several use case scenarios were described in an abstract format, without defining the interaction between the system and the user. The 10 scenarios were extracted from Table 1 of the Methodology and selected by the members of the consortium. The factors that were selected for each scenario were depicted carefully from the consortium in order to be adaptable for every user and to cover all the abilities of the DTI systems.

Use Cases (UC): Capture all the possible ways that LEAs and DTI systems can interact, resulting in the user achieving their goal.

- **UC1 - Detection of target**

- **UC2 - Identification of target**

- **UC3 - Tracking of target**

- **UC4 - Classification of target**

- **UC5 - Navigation of patrol unit**

- **UC6 - Mapping of specified area**

In order to assign an overall risk value for each of the developed scenarios, a risk weight will first be assigned to each factor and its subcategories.

Sensitive Sites/Critical National Infrastructure

Sensitive Sites/Critical National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).[14] In the category of Sensitive Sites/Critical National Infrastructure four (4) different targets are analyzed:

- A Prison
- An Airport
- A Nuclear Plant
- A Government Building

---

[14] *https://www.cpni.gov.uk/critical-national-infrastructure-0*

Category	Sensitive Sites/Critical National Infrastructure
Target	Prison
	The scenario is relevant to the fight against smuggling in prisons. The test scenario will take place in a prison area, located on the outskirts of a city. There are small trees, private houses, public roads and deserted land in the area. The scenario takes place in the morning with sunny weather conditions. The threat is represented by a single multirotor UAS, Class I, of the mini category. The UAS is of a commercial recreational type, carrying a drug payload of <250 grams. The UAS takes off from a hidden position in the surrounding public area of the prison. The UAS is manually piloted by the operator, using 2.4GHz & 5.8GHz. The UAS flight trajectory from the launching point to the prison area is not linear, speed ranges between 5 to 10 km/h and the flight altitude is between 50 to 100m. The UAS crosses the prison fence flying at a flight altitude of 100m and descends to 50m. A "friendly" UAS is also in the air as the guards patrol the yard with drone.
Environment	Urban
Lighting conditions	Daylight
Weather	Sunny
Presence of other aircrafts/UASs in the nearby airspace	Friendly
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Recreational custom-made UAS
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<4kg
Flight mode	Manual
Payload	Illicit Package
Altitude	50-100m
UAS Speed	0-10km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz & 5.8GHz
Flight patterns	Drop from High Altitude
Pilot Location	Unknown
Terrain	Irregular
EM Environment	Urban
Birds	Low Bird Presence
Vegetation	Low
UAS Signature	Low
Use Cases	UC1, UC2, UC5

Category	Sensitive Sites/Critical National Infrastructure
Target	**Airport**
	The scenario is relevant to the fight against careless use of UASs in an airport vicinity by airport administrators. The test scenario will take place at an airport area, located in a suburban area, surrounded by private homes. The total airport area is over 2.000.000 sqm. There are no trees in the area. The scenario takes place in the evening with rainy weather conditions. The threat is represented by a single fixed wing UAS, Class I, of the mini category (<15Kg), carrying an optical camera as its payload. The UAS takes off from a private yard, located at a distance over 3km from the center of the runway. The UAS flies autonomously using the edited waypoints, based on GPS and inertial navigation. The UAS flight trajectory from the launching point to the airport is direct, speed ranges between 10 to 30 km/h and the flight altitude is between 100 to 120m. There are no other UASs in the area, since there are airspace restrictions in place, but there are general aviation activities (helicopters and planes), based on the active planning and in coordination with ATC services. The UAS approaches the airport limits, has a linear flight path (speed and altitude) and tries to cross it at a perpendicular direction of the glideslope.
Environment	Suburban
Lighting conditions	Sunset
Weather	Rainy
Presence of other aircrafts/UASs in the nearby airspace	Authorized / General aviation activities (helicopters and planes)
Type of UAS	Fixed Wing
Number of UASs	1
Custom or Commercial	Commercial
Dimensions of UAS	50-70cm
Maximum take-off mass of UAS	<25kg
Flight mode	Waypoints
Payload	Optical Camera
Altitude	100-120m
UAS Speed	10-30km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz
Flight patterns	Direct Flight
Pilot Location	Known
Terrain	Flat
EM Environment	Dense/Crowded
Birds	Medium Bird Presence
Vegetation	Low
UAS Signature	Low
Use Cases	UC1, UC2, UC3, UC5

Category	Sensitive Sites/Critical National Infrastructure
Target	Nuclear Plant
	The scenario is relevant to the security of very high importance infrastructures, such as nuclear plants: 173 units in Europe (https://www.euronuclear.org/glossary/nuclear-power-plants-in-europe/). The scenario takes place around the safety perimeter of a nuclear power plant, located in an isolated rural area, near a river, for access to large amounts of water, necessary for cooling. The restricted area is over 4.000.000 sqm. There is low vegetation in the area. The scenario takes place at night, with cloudy weather. The threat is represented by a single custom-made multirotor UAS, Class I, of the small category (>15kg), carrying a 3kg explosive device as its payload. The UAS takes off 1000m away from the nuclear plant, from a covert position in a glade of the surrounding forest. The UAS flies autonomously using the edited waypoints, based on GPS and inertial navigation,. The flight altitude is >120m and the speed is between 10 to 30 km/h. There are no other UASs or aircrafts flying in the area - airspace restrictions are active for all flights. The UAS approaches the nuclear plant and starts to descend at high speed into the vapor tower of the nuclear plant.
Environment	Rural
Lighting conditions	Darkness
Weather	Cloudy
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Wrong-doing custom-made UAS
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<4kg
Flight mode	Waypoints
Payload	Explosives/IEDs
Altitude	> 120m
UAS Speed	10-30km/h
Radio Frequencies used for remote control and / or video stream	4G/LTE
Flight patterns	Obscured
Pilot Location	Known
Terrain	Irregular
EM Environment	Rural
Birds	High Bird Presence
Vegetation	Average
UAS Signature	Normal
Use Cases	UC1, UC2, UC3, UC4

Category	Sensitive Sites/Critical National Infrastructure
Target	Government Building

	This scenario is relevant to the security against criminal, terrorist or hostile surveillance actions towards high importance infrastructures for the functioning of states. The scenario takes place at a building complex, located in the middle of a large urban area. The restricted area is over 200.000 sqm. There is medium vegetation in the area, major public roads on all sides, private buildings (1 – 10 floors in height), radio interference, etc. The scenario takes place in the afternoon, with clear weather conditions. The threat is represented by 3 UASs carrying video equipment payloads: two commercial multirotor UASs, Class I, of the mini and micro category and a custom-made multirotor UAS, Class I, of the small category. The goal is to carry out a physical attack against a VIP using UAS as a kinetic vector and to create panic. Two UASs are manually piloted by the operators, using 2.4GHz & 5.8GHz, whereas the custom-made one uses a nonstandard frequency. The micro-UAS takes off from a public park, located at a distance of 300-500m from the government building. It flies at a speed of 10 km/h and at a flight altitude between 50-100m. The UAS is used for reconnaissance purposes in the location, as the first phase of the attack. The second commercial UAS is used to coordinate the attack, flying outside of the location. It is manually released and piloted from the roof of a 10-floor building, located at 2-2.5km away from the government building. The 3rd UAS is used to directly be sent to the protected dignitary when he descends from the motorcade. There are no other UASs or aircrafts flying in the area - airspace restrictions are active for all flights.

Environment	Urban
Lighting conditions	Sunset
Weather	Sunny
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Multirotor
Number of UASs	3
Custom or Commercial	2 Commercial, 1 Wrong-doing custom-made UAS
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<4kg
Flight mode	Manual
Payload	Optical Camera
Altitude	50-100m
UAS Speed	0-10km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz & 5.8GHz
Flight patterns	Direct flight
Pilot Location	Known
Terrain	Irregular
EM Environment	Urban
Birds	Low Bird Presence
Vegetation	Low
UAS Signature	Low
Use Cases	UC1, UC3, UC4, UC6

The misuse of Unmanned Aerial Vehicles (UASs) in public spaces/events is a serious concern across the world as terrorists, activists and criminals adopt drone technology and develop new and creative ways in which to commit crime and terrorism.

In the category of Public Spaces Protection/Events four (4) different targets were analyzed:

- • A Stadium

- • An Outdoor Concert

- • An Outdoor Political Rally

- • An International Summit

Category	Public Spaces Protection/Events
Target	Stadium
	The scenario takes place at a stadium, which can accommodate more than 50.000 people. The location is a suburban area over 100.000 sqm, surrounded by few private homes and industrial production facilities. There are no trees in the area. The electromagnetic environment is very busy due to the large number of mobile phones in the area. The scenario takes place in the evening, with cloudy weather. During the concert, the DTI detects a custom-made multirotor UAS, Class I, of the small category (>15kg), equipped with an aerosol dispersing device as its payload. The UAS is launched from an industrial area, approaches the stadium zone flying at 100m (AGL), descends to 50m near the main stage and continues to fly at a 30m altitude above the attendants, at a slow speed (3-5 km/h) and constantly changes direction.
Environment	Suburban
Lighting conditions	Sunset
Weather	Cloudy
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Wrong-doing custom-made UAS
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<4kg
Flight mode	Manual
Payload	Sprayers
Altitude	50-100m
UAS Speed	0-10km/h
Radio Frequencies used for remote control and / or video stream	4G/LTE
Flight patterns	Obscured
Pilot Location	Known
Terrain	Irregular
EM Environment	Dense/Crowded
Birds	Low Bird Presence
Vegetation	Average
UAS Signature	Normal
Use Cases	UC1, UC3, UC4

Category	Public Spaces Protection/Events
Target	**Outdoor Concert**
	The scenario takes place at an outdoor concert area, which can accommodate more than 50.000 people. The location is in a suburban area over 100.000 sqm, where a 20m metallic stage is installed, surrounded by few private homes and industrial production facilities. There are no trees in the area. The electromagnetic environment is very busy, due to the large number of mobile phones in the area. The scenario takes place in the evening, with windy weather. The event organizer is using a single multirotor UAS, Class I, of the mini category (<15Kg), carrying a professional video camera as its payload and uses custom communication protocols – friendly UAS. The UAS flies at an altitude of 50m around the area, at a speed of 5 m/s, hovering at certain moments. The UAS flies autonomously using the edited waypoints, based on GPS and inertial navigation. During the concert, the DTI detects a second UAS in the area (not friendly UAS). It is a custom-made multirotor UAS, Class I, of the small category (>15kg) carrying as its payload a dazzling laser. The UAS is launched from an industrial area, approaches the concert zone, flying at 100m (AGL), it descends to 50m near the main stage and continues to fly at a 30m altitude above the attendants, at a slow speed (3-5 km/h) and constantly changes direction, but is mainly directed to the stage. The UAS is destroyed on impact, while crashing into one of the stage performers.
Environment	Suburban
Lighting conditions	Sunset
Weather	Windy
Presence of other aircrafts/UASs in the nearby airspace	Not classified
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Wrong-doing custom-made UAS
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<25kg
Flight mode	GPS
Payload	Optical camera
Altitude	50-100m
UAS Speed	0-10km/h
Radio Frequencies used for remote control and / or video stream	4G/LTE
Flight patterns	Obscured
Pilot Location	Unknown
Terrain	Irregular
EM Environment	Dense/Crowded
Birds	Low Bird Presence
Vegetation	Average
UAS Signature	Normal
Use Cases	UC1, UC3, UC4

Category	Public Spaces Protection/Events
Target	**Outdoor Political Rally**
	The scenario takes place in the middle of a city, during an authorized rally. The location is an urban area over 10.000 sqm, surrounded by few private homes, hotels, shops and public institutions. There are few small trees in the area. The electromagnetic environment is very busy, due to the large number of mobile devices in the area. The scenario takes place in the evening, with clear weather conditions. There are no other UASs or aircrafts flying in the area - airspace restrictions are active for all flights. The threat is represented by a single commercial multirotor UAS, Class I, of the mini category (<15kg), carrying a noise generator as its payload. The scope is for a criminal organization to create panic and cause disturbance to the event. The UAS takes off 1000m away from the center of the square, from a covert position. The UAS flies autonomously over major streets, using the edited waypoints, based on GPS and inertial navigation. The approach flight altitude is > 120m and the speed is 10 to 30 km/h. There are no other UASs or aircrafts flying in the area - airspace restrictions are active for all flights. The UAS descends to 15m over the mass gathering and continues to fly at a slow speed (<5 km/h) constantly changing direction, but heading to the stage area, harassing the speakers. The audience starts to run chaotically. The UAS continues to fly until its battery is drained and crashes in front of the stage.
Environment	Urban
Lighting conditions	Sunset
Weather	Sunny
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Commercial
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<25kg
Flight mode	Waypoints
Payload	Noise Generators
Altitude	> 120m
UAS Speed	0-10km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz
Flight patterns	Obscured
Pilot Location	Unknown
Terrain	Irregular
EM Environment	Dense/Crowded
Birds	Low Bird Presence
Vegetation	Low
UAS Signature	Normal

Use Cases	UC1, UC2, UC3, UC4
Category	Public Spaces Protection/Events
Target	**International Summit**
	The scenario takes place at an outdoor rural area, at a historical location, where an international summit is organized. The location area is over 10.000 sqm, surrounded by trees. The electromagnetic environment is very clean. The scenario takes place in the evening, with dusty weather. There are no other UASs or aircrafts flying in the area - airspace restrictions are active for all flights. The threat is represented by a single commercial fixed wing UAS, Class I, of the small category (>15kg). The scope is for a terrorist organization to create panic and cause disturbance to the event. The UAS is released at a distance of 10.000m from the location, from a grassland. The UAS flies autonomously, using the edited waypoints, based on GPS and inertial navigation. The approach flight altitude is > 120m and the speed is between 10 to 30 km/h. The UAS descends to an altitude of 100m, at a distance of 500m from the location and heads to the area where the VIPs are participating in a group photo. At a 50m distance from the photo area and at an altitude of 20m, the UAS explodes, spreading shrapnel (metal balls and nails).
Environment	Rural
Lighting conditions	Daylight
Weather	Dusty
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Fixed Wing
Number of UASs	1
Custom or Commercial	Commercial
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<25kg
Flight mode	GPS
Payload	Different Domestic Payloads
Altitude	>120m
UAS Speed	10-30km/h
Radio Frequencies used for remote control and / or video stream	RC Model aircraft frequencies
Flight patterns	Direct Flight
Pilot Location	Unknown
Terrain	Mountainous
EM Environment	Rural
Birds	High Bird Presence
Vegetation	Wood/Forest
UAS Signature	Normal
Use Cases	UC1, UC3, UC4
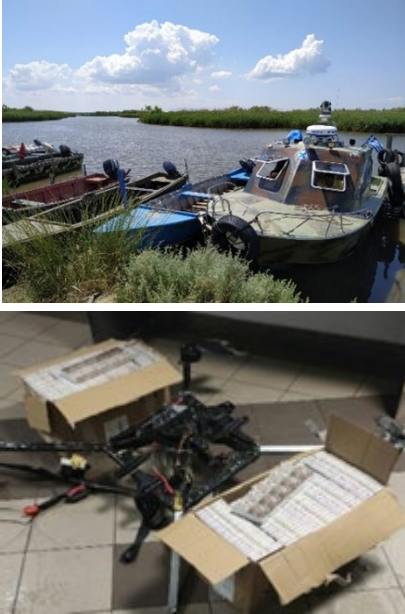
Borders consist of all air, land and maritime boundaries, including ports of entry, vast stretches of remote terrain and inland waterways. Border protection also, refers to border control measures
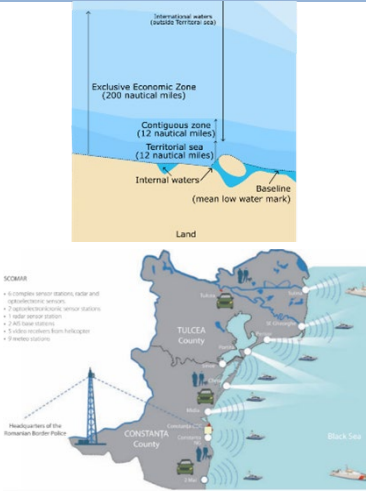
with reference to organized crime, including piracy, terrorism, migrant smuggling, trafficking in persons and arms proliferation.

In the category of Border Protection two (2) different targets analyzed:
- Land Border
- Maritime Border

Category	Border Protection
Target	Land Border
	The scenario is relevant to the fight against drug/cigarette/gun trafficking at the land border. The scenario takes place at the land border of two countries, in a curved rural area covered with dense vegetation over a length of 100km. There are no electromagnetic interferences. The scenario takes place during a misty night. There are no other UASs in the area, since there are airspace restrictions in place, but there are general aviation activities (helicopters and planes), based on active planning and in coordination with ATC services. The threat is a custom-made multirotor UAS, Class I, of the small category (>15kg), carrying a 2kg box as its payload. The UAS is used to drop packages in a forested area, away from the border patrol's control area. There is no permanent communication, given that the flight path is pre-defined. Some communication is present, in order to be able to abort the action. The UAS takes off from a remote location, at a distance of over 10km from the border. The UAS flies autonomously, using the edited waypoints, based on GPS and inertial navigation, at an altitude of under 50m and over a speed of 15km/h. It passes the LZ, drops the box and flies away, using the same flight path.
Environment	Rural
Lighting conditions	Darkness
Weather	Misty
Presence of other aircrafts/UASs in the nearby airspace	-
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Wrong-doing custom-made UAS
Dimensions of UAS	50-70cm
Maximum take-off mass of UAS	<25kg
Flight mode	Waypoints
Payload	Illicit Package
Altitude	30-50m
UAS Speed	10-30km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz
Flight patterns	Direct Flight
Pilot Location	Known
Terrain	Irregular
EM Environment	Rural
Birds	High Bird Presence

Vegetation	Average
UAS Signature	Normal
Use Cases	UC1, UC3, UC4

Category	Border Protection
Target	**Maritime Border**
	The scenario is representative of fraudulent border crossing by immigrants, using boats. The scenario takes place at the sea border at night, in clear weather conditions. The threat is represented by a commercial multirotor UAS, Class I, of the mini category (<15kg) and is used as a surveillance means to avoid the coast guard boats (it has a thermal sensor as its payload). The UAS takes off from a ship outside the territorial sea (more than 22.2 km from the border) and it is piloted, based on GPS and inertial navigation, at a flight altitude of 25m and at a speed of under 10km/h. The UAS flies in front of the immigrants' boat at a distance of 5km. The boat belongs to that of Class A boats - measuring less than 16 feet. The UAS flies back to the ship and is recovered. The guards patrol the area with UAS.
Environment	Rural
Lighting conditions	Darkness
Weather	Clear
Presence of other aircrafts/UASs in the nearby airspace	Friendly
Type of UAS	Multirotor
Number of UASs	1
Custom or Commercial	Commercial
Dimensions of UAS	30-50cm
Maximum take-off mass of UAS	<4kg
Flight mode	Manual
Payload	Thermal Sensor
Altitude	30-50m
UAS Speed	10-30km/h
Radio Frequencies used for remote control and / or video stream	2.4GHz
Flight patterns	Direct Flight
Pilot Location	Known
Terrain	Flat
EM Environment	Rural
Birds	Medium Bird Presence
Vegetation	Low
UAS Signature	Normal
Use Cases	UC1, UC3, UC4, UC5, UC6

Each scenario outlines a representative real-world event to introduce the overarching operational context and limitations. The scenarios and use cases are non-technical, high-level representations, depicting events of interest from a LEA's perspective. The intent is to illustrate the threat and the problem space through narrative examples, highlighting the importance of addressing real-world challenges.

Annex B
(informative)

Example of end-user questionnaire

The questionnaire was created and distributed to end-users participating in field trials, in order to identify the factors that comprise the C-UAS scenarios. Using this questionnaire, a set of potential values was selected for identifying the factors of a scenario.

Please tick (check) this box to indicate that you consent to taking part in this questionnaire*:

☐ **I consent to taking part in this questionnaire.**

☐ **I do not consent to taking part in this questionnaire and wish to leave the questionnaire.**

Personal Information

Full Name*:

Organization*:

Department:

Country:

E-mail Address*:

* Mandatory

1. **Has your organization taken part in a confrontation of a UAS attack? ***

☐ **Yes**

☐ **No**

2. **UAS threat scenarios can be broken down into distinct components that are the pillars around which the story is further developed e.g. time of day, type of UAV involved, environmental conditions, etc.**

According to your experience, which of the below listed components contribute to the development of a UAS threat scenario? * (multiple items can be checked)

Please add potential missing scenario components you consider important.

☐ **Intention**	
Description: The term intention refers to the UAV pilot's motivation, navigating a non-cooperative UAV. Their intention is distinguished into 3 separate categories: Negligence, Gross negligence, "Criminal/ Terrorist motivation"	[Open question] In case you consider more than the 3 categories of intention (Negligence, Gross negligence, "Criminal/ Terrorist motivation), please indicate the additional one(s): …………………………………

☐ **Target**	
Description: According to the literature, malicious UAVs could have different objectives and targets. Possible targets include: Critical Infrastructure, Governmental Buildings, VIP, Public Events, Means of Transportation, Urban – Not Specified, Border.	[Open question] Please indicate any additional target(s) that should be taken into consideration: …………………………………
☐ **Environment**	
Description: Another component that contributes to the development of a UAS threat scenario is the environment or the area that the scenario takes place in. The environment is divided into Rural, Suburban and Urban.	[Open question] If you consider necessary, please specify a more detailed categorisation and description of the environment: …………………………………
☐ **Lighting Conditions**	
Description: Lighting conditions are considered as a critical component that contribute to the development of a UAS threat. The categorisation includes Sunrise, Sunset, Daylight and Darkness.	[Open question] If you consider that a more detailed categorisation on lighting conditions would be beneficial for a UAS threat scenario, please indicate the additional categories: …………………………………
☐ **Weather**	
Description: Weather conditions could affect not only the malicious UAVs, but the deployed countermeasures that an organisation has established. Weather conditions affect UAS threat scenarios in various ways. The Weather conditions considered are: Sunny, Cloudy, Rainy, Foggy, Windy, Stormy, Misty, Smoke, Dusty, Snowy and Clear.	[Open question] Please indicate any additional weather conditions that could affect a UAS threat scenario: …………………………………
☐ **Presence of other aircrafts/UAVs in the nearby airspace**	
Description: The presence of other nearby aircraft could affect a UAS threat scenario, as well as the countermeasures that will be implemented. Information regarding the other UAVs in the nearby airspace is another component of such scenarios (U-Space), and are categorised as: Not Classified, Not Controlled, Own Fleet, Friend, Authorized, Stolen, Alleged Infringer, Threat, Escaped and Neutralized.	[Open question] Please indicate any additional categories of UAVs in the nearby airspace that could affect a UAS threat scenario: …………………………………

☐ **Type of UAV**	
Description: Another component that contributes to the development of a UAS threat scenario is the type of the UAV that each pilot uses. The categories that have been taken into consideration for the different types of UAVs are: Multirotor, Fixed Wing, Flapping-wing Ornithopters, Gliders, Single Rotor and Hybrid.	[Open question] Please indicate any additional categories of types of UAVs: …………………………………
☐ **Number of UAVs**	
Description: The number of UAVs is another critical parameter in the development of a UAS threat scenario. The different categories that are considered are: 1,2 and Swarm.	[Open question] If you consider necessary, please specify a more detailed categorisation regarding the number of UAVs: …………………………………
☐ **Custom or Commercial**	
Description: As indicated in the literature, the risk level of a UAS threat scenario could be affected by the way that it has been manufactured, as it directly affects or makes "unknown" some of its characteristics. The categories are: Recreational custom-made UAS, Wrong-doing custom-made UAS and Commercial.	[Open question] Please indicate any additional categories that should be taken into consideration: …………………………………
☐ **Dimensions of UAV (wingspan, rotor diameter/area or maximum distance between rotors in case of multirotor)**	
Description: Another component that contributes to the development of a UAS threat scenario is the actual dimensions of the UAV. The categories that are considered are: <30cm, 30-50cm, 50-70cm and >1m.	[Open question] If you consider necessary, please specify a more detailed or even another categorisation regarding the dimensions of UAVs: …………………………………
☐ **Maximum take-off mass of UAV**	
Description: Among the characteristics of a UAV that contributes to the development of a UAS threat scenario is the maximum take-off mass (MTOM). The categories that are considered are: <250g, <900g, <4kg, <25kg, <100kg and >100kg.	[Open question] If you consider necessary, please specify a more detailed or even another categorisation regarding the maximum take-off mass (MTOM) of UAVs. …………………………………

☐ **Flight mode**

Description: Another component that contributes to the development of a UAS threat scenario is the way that the pilot navigates the aircraft, meaning the flight mode. The categories that are considered for this component are: Manual, GPS, Waypoints, Inertial Navigation Systems and 4G/LTE.	[Open question] Please indicate any additional categories that should be taken into consideration regarding Flight Modes: …………………………………

☐ **Payload**

Description: Another component that contributes to the development of a UAS threat scenario is the payload that the UAV carries and indicates its missions and objectives. The categories that are considered for this component are: Optical Camera, LiDAR, Thermal Sensor, Explosives/IEDs, Guns, CBRN, Objects for Commercial Distribution, Sprayers, Noise Generators, Jamming Devices, Different Domestic Payloads and Dazzling Lasers.	[Open question] Please indicate any additional categories of payloads that should be taken into consideration: …………………………………

☐ **Altitude**

Description: The altitude that the UAV flies at is another component of the UAS threat scenario. The categories that are considered are: 0-5m, 5-20m, 20-50m, 50-100m, 100-120m and >120m.	[Open question] If you consider necessary, please specify a more detailed or even another categorisation regarding the altitude of UAVs. …………………………………

☐ **UAV Speed**

Description: The UAV speed is another component of the UAS threat scenario that affects the risk level, the prevention and the countermeasures. The categories that are considered are: 0-10km/h, 10-30km/h, 30-60km/h, <60 km/h, 60-120 km/h, 120-160 km/h and >160 km/h.	[Open question] If you consider necessary, please specify a more detailed or even another categorisation regarding the speed of UAVs. …………………………………

☐ Radio Frequencies used for remote control and / or video stream	
Description: The radio frequencies that are used to control the aircraft is another component of the UAS threat scenario. The categories that are considered are: 2.4GHz, 5.8GHz, RC model aircraft frequencies (depending on national regulations) and 4G/LTE.	[Open question] Please indicate any additional categories of radio frequencies that are used for remote control and should be taken into consideration: ……………………………………
☐ **Flight patterns**	
Description: Flight patterns refer mainly to the trajectory followed by the UAV that can be either Obvious or Obscured e.g. flight between obstacles such as trees or buildings, that could possibly affect the established countermeasures. As this component is highly dependent on the environment, there are no specific categories to distinguish the various patterns, other than: Direct Flight, Obscured flight and Drop from High Altitude.	Please indicate any additional categories of Flight Patterns to be taken into consideration: ……………………………………
☐ **Should you consider that additional scenario elements are missing, please add them below, proposing also the desirable categorization:**	

Annex C
(informative)

Risk matrix of the standardised scenarios

In this annex, each scenario was scored according to risk.

The final Risk Score of each scenario resulted from the average risk score of each factor that comprises a standard scenario, as described in 8.5. Then, for each underline standard scenario that was developed in clause 7, a risk score was assigned to each of the factor's subcategory that was selected for that specific scenario (the risk value was assigned from Table 31). Finally, the Overall Risk of each standard scenario is calculated from the aggregation of the two previous risk values.
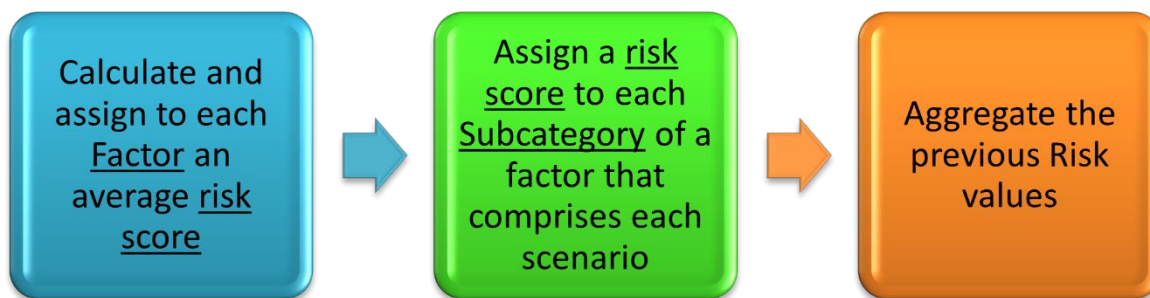
Figure C.1 — Calculation of the Overall Risk

In this context, the first scenario, whose "Target Factor" is a Prison, receives a Total Risk score of 264,3 (Table C.1).

Table C.1 — Risk of Scenario 1 - Target: Prison

Factor	Sensitive Sites/Critical National Infrastructure	Risk
Intention	Criminal	11.3
Target	**Prison**	**14.1**
Environment	Urban	17.4
Lighting conditions	Daylight	10.6
Weather	Sunny	7.0
Presence of other aircrafts/UAVs in the nearby airspace	Friendly	4.5
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Recreational custom-made UAS	12.0
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<4kg	13.9
Flight mode	Manual	14.3
Payload	Illicit Package	11.1
Altitude	50-100m	10.9
UAV Speed	0-10km/h	7.2
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Drop from High Altitude	11.7
Pilot Location	Unknown	13.7
Terrain	Irregular	11.8
EM Environment	Urban	14.2
Birds	Low Bird Presence	6.1
Vegetation	Low	6.4
UAV Signature	Low	9.6
Total Risk		**264.3**

Table C.2 — Risk of Scenario 2 – Target: Airport

Category	Sensitive Sites/Critical National Infrastructure	Risk
Intention	Gross Negligence	9.6
Target	**Airport**	**14.1**
Environment	Suburban	10
Lighting conditions	Sunset	7.6
Weather	Rainy	9
Presence of other aircrafts/UAVs in the nearby airspace	Authorized / General aviation activities (helicopters and planes)	4.7
Type of UAV	Fixed Wing	12
Number of UAVs	1	13.6
Custom or Commercial	Commercial	13
Dimensions of UAV	50-70cm	12.1
Maximum take-off mass of UAV	<25kg	10.8
Flight mode	Waypoints	10.7
Payload	Optical Camera	16.2
Altitude	100-120m	10.4
UAV Speed	10-30km/h	11
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Direct Flight	13.3
Pilot Location	Known	9.2
Terrain	Flat	10.9
EM Environment	Dense/Crowded	15.9
Birds	Medium Bird Presence	8
Vegetation	Low	6.4
UAV Signature	Low	9.6
Total Risk		253.4

Table C.3 — Risk of Scenario 3 – Target: Nuclear Plant

Category	Sensitive Sites/Critical National Infrastructure	Risk
Intention	Criminal	11.3
Target	**Nuclear Plant**	**14.1**
Environment	Rural	6
Lighting conditions	Darkness	10
Weather	Cloudy	8
Presence of other aircrafts/UAVs in the nearby airspace	-	0
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Wrong-doing custom-made UAS	10.2
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<4kg	13.9
Flight mode	Waypoints	10.7
Payload	Explosives/IEDs	10.9
Altitude	> 120m	7.7
UAV Speed	10-30km/h	11
Radio Frequencies used for remote control and / or video stream	4G/LTE	7.5
Flight patterns	Obscured	11.4
Pilot Location	Known	9.2
Terrain	Irregular	11.8
EM Environment	Rural	5.6
Birds	High Bird Presence	7.8
Vegetation	Average	8.4
UAV Signature	Normal	10.6
Total Risk		**227.3**

Table C.4 — Risk of Scenario 4 – Target: Government Building

Category	Sensitive Sites/Critical National Infrastructure	Risk
Intention	Criminal	11.3
Target	**Government Building**	**12.1**
Environment	Urban	17.4
Lighting conditions	Sunset	7.6
Weather	Sunny	7
Presence of other aircrafts/UAVs in the nearby airspace	-	0
Type of UAV	Multirotor	16.2
Number of UAVs	3	8.5
Custom or Commercial	2 Commercial, 1 Wrong-doing custom-made UAS	13
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<4kg	13.9
Flight mode	Manual	14.3
Payload	Optical Camera	16.2
Altitude	50-100m	10.9
UAV Speed	0-10km/h	7.2
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Direct flight	13.3
Pilot Location	Known	9.2
Terrain	Irregular	11.8
EM Environment	Urban	14.2
Birds	Low Bird Presence	6.1
Vegetation	Low	6.4
UAV Signature	Low	9.6
Total Risk		**252.9**

Table C.5 — Risk of Scenario 5 – Target: Stadium

Category	Public Spaces Protection/Events	Risk
Intention	Criminal	11.3
Target	**Stadium**	**15.6**
Environment	Suburban	10
Lighting conditions	Sunset	7.6
Weather	Cloudy	8
Presence of other aircrafts/UAVs in the nearby airspace	-	0
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Wrong-doing custom-made UAS	10.2
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<4kg	13.9
Flight mode	Manual	14.3
Payload	Sprayers	7.6
Altitude	50-100m	10.9
UAV Speed	0-10km/h	7.2
Radio Frequencies used for remote control and / or video stream	4G/LTE	7.5
Flight patterns	Obscured	11.4
Pilot Location	Known	9.2
Terrain	Irregular	11.8
EM Environment	Dense/Crowded	15.9
Birds	Low Bird Presence	6.1
Vegetation	Average	8.4
UAV Signature	Normal	10.6
Total Risk		**238.7**

Table C.6 — Risk of Scenario 6 – Target: Outdoor Concert

Category	Public Spaces Protection/Events	Risk
Intention	Gross Negligence	9.6
Target	**Outdoor Concert**	**15.6**
Environment	Suburban	10
Lighting conditions	Sunset	7.6
Weather	Windy	8
Presence of other aircrafts/UAVs in the nearby airspace	Not classified	8.8
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Wrong-doing custom-made UAS	10.2
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<25kg	10.8
Flight mode	GPS	12
Payload	Optical camera	16.2
Altitude	50-100m	10.9
UAV Speed	0-10km/h	7.2
Radio Frequencies used for remote control and / or video stream	4G/LTE	7.5
Flight patterns	Obscured	11.4
Pilot Location	Unknown	13.7
Terrain	Irregular	11.8
EM Environment	Dense/Crowded	15.9
Birds	Low Bird Presence	6.1
Vegetation	Average	8.4
UAV Signature	Normal	10.6
Total Risk		**253.5**

Table C.7 — Risk of Scenario 7 – Target: Outdoor Political Rally

Category	Public Spaces Protection/Events	Risk
Intention	Criminal	11.3
Target	**Outdoor Political Rally**	**15.6**
Environment	Urban	17.4
Lighting conditions	Sunset	7.6
Weather	Sunny	7
Presence of other aircrafts/UAVs in the nearby airspace	Not classified	8.8
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Commercial	13
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<25kg	10.8
Flight mode	Waypoints	10.7
Payload	Noise Generators	3.9
Altitude	> 120m	7.7
UAV Speed	0-10km/h	7.2
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Obscured	11.4
Pilot Location	Unknown	13.7
Terrain	Irregular	11.8
EM Environment	Dense/Crowded	15.9
Birds	Low Bird Presence	6.1
Vegetation	Low	6.4
UAV Signature	Normal	10.6
Total Risk		**253.4**

Table C.8 — Risk of Scenario 8 – Target: International Summit

Category	Public Spaces Protection/Events	Risk
Intention	Criminal	11.3
Target	**International Summit**	**12.5**
Environment	Rural	6
Lighting conditions	Daylight	10.6
Weather	Dusty	4.7
Presence of other aircrafts/UAVs in the nearby airspace	-	0
Type of UAV	Fixed Wing	12
Number of UAVs	1	13.6
Custom or Commercial	Commercial	13
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<25kg	10.8
Flight mode	GPS	12
Payload	Different Domestic Payloads	5.4
Altitude	>120m	7.7
UAV Speed	10-30km/h	11
Radio Frequencies used for remote control and / or video stream	RC Model aircraft frequencies	8.8
Flight patterns	Direct Flight	13.3
Pilot Location	Unknown	13.7
Terrain	Mountainous	7
EM Environment	Rural	5.6
Birds	High Bird Presence	7.8
Vegetation	Wood/Forest	8.5
UAV Signature	Normal	10.6
Total Risk		**217.3**

Table C.9 — Risk of Scenario 9 – Target: Land Border

Category	Border Protection	Risk
Intention	Criminal	11.3
Target	**Land Border**	**9.6**
Environment	Rural	6
Lighting conditions	Darkness	10
Weather	Foggy	8.2
Presence of other aircrafts/UAVs in the nearby airspace	-	0
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Wrong-doing custom-made UAS	10.2
Dimensions of UAV	50-70cm	12.1
Maximum take-off mass of UAV	<25kg	10.8
Flight mode	Waypoints	10.7
Payload	Illicit Package	11.1
Altitude	20-50m	12.2
UAV Speed	10-30km/h	11
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Direct Flight	13.3
Pilot Location	Known	9.2
Terrain	Irregular	11.8
EM Environment	Rural	5.6
Birds	High Bird Presence	7.8
Vegetation	Average	8.4
UAV Signature	Normal	10.6
Total Risk		**235**

Table C.10 — Risk of Scenario 10 – Target: Maritime Border

Category	Border Protection	Risk
Intention	Criminal	11.3
Target	**Maritime Border**	**9.6**
Environment	Rural	6
Lighting conditions	Darkness	10
Weather	Clear	7.9
Presence of other aircrafts/UAVs in the nearby airspace	Friendly	4.5
Type of UAV	Multirotor	16.2
Number of UAVs	1	13.6
Custom or Commercial	Commercial	13
Dimensions of UAV	30-50cm	11.4
Maximum take-off mass of UAV	<4kg	13.9
Flight mode	Manual	14.3
Payload	Thermal Sensor	9.9
Altitude	20-50m	12.2
UAV Speed	10-30km/h	11
Radio Frequencies used for remote control and / or video stream	2.4GHz	15.3
Flight patterns	Direct Flight	13.3
Pilot Location	Known	9.2
Terrain	Flat	10.9
EM Environment	Rural	5.6
Birds	Medium Bird Presence	8
Vegetation	Low	6.4
UAV Signature	Normal	10.6
Total Risk		**244.1**

Table C.11 — Scenarios - Total Risk

Scenario	Total Risk
Scenario 1 - Target: Prison	264.3
Scenario 2 - Target: Airport	253.4
Scenario 3 - Target: Nuclear Plant	227.3
Scenario 4 - Target: Government Building	252.9
Scenario 5 - Target: Stadium	238.7
Scenario 6 - Target: Outdoor Concert	253.5
Scenario 7 - Target: Outdoor Political Rally	253.4
Scenario 8 - Target: International Summit	217.3
Scenario 9 - Target: Land Border	235
Scenario 10 - Target: Maritime Border	244.1

Table C.12 — Risk Matrix (with values)

Impact

Likelihood	Very Low	Low	Medium	High	Very High
Very Low	110	165	220	275	330
Low	165	220	275	330	385
Medium	220	275	330	385	440
High	275	330	385	440	495
Very high	330	385	440	495	550

Table C.13 — Risk Matrix (generic)

Impact

Likelihood	Very Low	Low	Medium	High	Very High
Very Low	Very Low	Low	Low	Medium	Medium
Low	Low	Low	Medium	Medium	High
Medium	Low	Medium	Medium	High	High
High	Medium	Medium	High	High	Very High

Annex D
(informative)

Specific operational needs for the standardised scenarios

D.1   General

Standard scenarios consider different C-UAS missions, different operational environments with different operation contexts, additional to the above-mentioned needs, below, for each scenario other requirements are detailed.
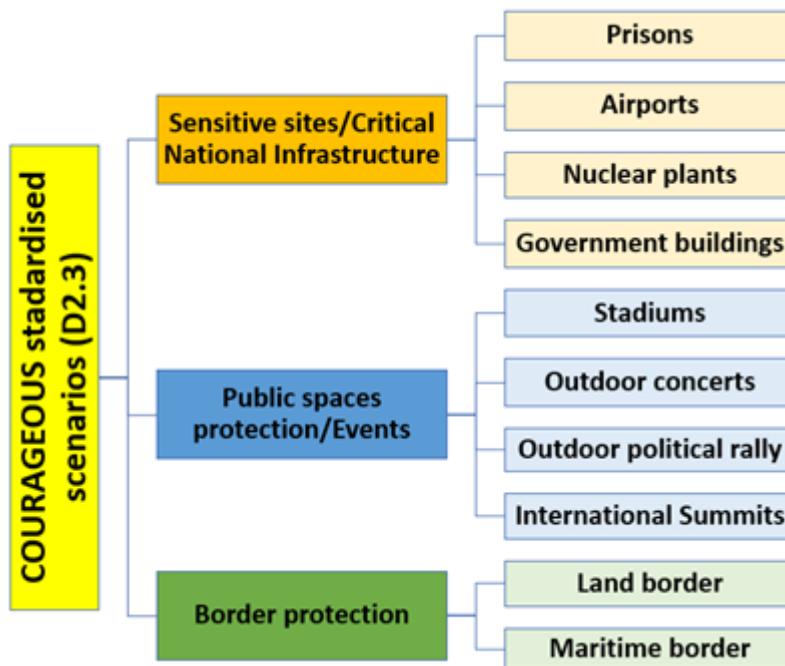
Figure D.1 — Application areas of the counter-drones technologies

D.2   Specific operational needs for standard scenario 1 - Prisons

The scenario is relevant to the fight against smuggling in prisons. The test scenario could take place in a prison area, located on the outskirts of a city, in an area with small trees, private houses, public roads. The scenario could take place in the morning with sunny weather conditions. The threat could be represented by a single multirotor UAS, Class I - mini category, commercial/recreational type, carrying a drug payload of <250 grams.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S1_GR1*
Req. Name	*Integration in the prison ecosystem*
Description	The C-UAS system shall be designed to minimize disruption to the daily operations of the prison. The system should not interfere with the communication systems or other essential operations within the prison.
Importance	**SHALL**

Req. Nº	*S1_GR2*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system should have the possibility to be integrated with other security systems within the prison, such as access control systems, CCTV cameras, and security personnel in order to improve the overall situational awareness and response times.
Importance	**SHOULD**

Req. Nº	*S1_GR3*
Req. Name	Sensor's performances – early detection
Description	A C-UAS system in a prison environment shall be able to detect and track unauthorized drones in the vicinity of the prison as early as possible. This requires sensors and detection systems that can cover the entire perimeter of the prison and identify drones that fly below the radar.
Importance	**SHALL**

Req. Nº	*S1_GR4*
Req. Name	Countermeasure's activation
Description	A C-UAS system in a prison environment may be able to respond quickly to unauthorized drones. This requires an automated response system that can take immediate action to intercept or disable the drone before it can deliver contraband or cause harm.
Importance	**MAY**

D.3 Specific operational needs for standard scenario 2 - Airports

The scenario is relevant to the fight of airport administrators, against careless use of UASs in the airport vicinity. The scenario could take place in an airport area, located in a suburban environment, with small vegetation, roads and surrounded by few private homes. The scenario could take place in the evening with rainy weather conditions. The threat could be represented by a single fixed wing UAS, Class I - mini category (<15Kg), carrying an optical camera as its payload.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S2_GR1*
Req. Name	*Integration in the airport ecosystem*
Description	The C-UAS system shall not compromise the existing aviation safety measures
Importance	**SHALL**

Req. Nº	*S2_GR2*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system shall not affect current flight operations
Importance	**SHALL**

Req. Nº	*S2_GR3*
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system shall not affect the communication and navigation systems installed in the airport area
Importance	**SHALL**

Req. Nº	*S2_GR4*
Req. Name	*System coverage*
Description	The C-UAS system shall cover the entire flight operations area, especially the approach and transition area.
Importance	**SHALL**

Req. Nº	*S2_GR5*
Req. Name	System integration
Description	The C-UAS system shall be integrated with ATC services
Importance	**SHALL**

Req. Nº	*S2_GR6*
Req. Name	Technology safety in airport area
Description	The DTI sensors based on laser technologies must not pose any risk to flight crews
Importance	**SHALL**

Req. Nº	*S2_GR7*
Req. Name	Sensor's performances
Description	If the C-UAS system includes acoustic sensors, their performances should not be affected by airport specific noise levels
Importance	**SHALL**

Req. N⁰	**S2_GR8**
Req. Name	Sensor's performances
Description	If the C-UAS system includes optic sensors, their performances should not be affected by the flying birds in the area
Importance	**SHALL**

Req. N⁰	**S2_GR9**
Req. Name	Countermeasure's activation
Description	The C-UAS system shall have the possibility to be integrated with the airport's ATC system to ensure coordination and seamless communication between C-UAS operators and air traffic controllers. The activation of countermeasures shall be done by the specialised operators only after the approval of an air traffic controller. This enables effective response without disrupting normal flight operations. Special procedures should be in place.
Importance	**SHALL**

D.4   Specific operational needs for standard scenario 3 – Nuclear plants

The scenario is relevant to the security of very high importance infrastructures, such as nuclear plants. The scenario could take place around the safety perimeter of a nuclear power plant, located in an isolated rural area, near a river, for access to large amounts of water, necessary for cooling. There is low vegetation in the area. The scenario could take place at night, with cloudy weather. The threat could be represented by a single custom-made multirotor UAS, Class I - small category (>15kg), carrying a 3kg explosive device as its payload.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. N⁰	**S3_GR1**
Req. Name	*System coverage - Critical Infrastructure Protection*
Description	The C-UAS system shall specifically focus on protecting critical infrastructure components of the nuclear plant, including reactor buildings, spent fuel storage, and other sensitive areas. It should be capable of detecting UAS attempting to approach or hover near these critical areas.
Importance	**SHALL**

Req. N⁰	**S3_GR2**
Req. Name	*Technical expectation - Secure Communication and Information Sharing*
Description	The C-UAS system shall facilitate secure communication between relevant authorities to coordinate response efforts effectively.
Importance	**SHALL**

Req. Nº	*S3_GR3*
Req. Name	*Technical expectation - Remote Monitoring and Control*
Description	The C-UAS system should allow for remote monitoring and control capabilities. This enables operators to assess threats and initiate response actions from a centralized command centre or remote locations within the plant, enhancing operational efficiency.
Importance	**SHOULD**

Req. Nº	*S3_GR4*
Req. Name	*Technical expectation - Geofencing*
Description	The C-UAS system should be able to implement a geofencing mechanism to restrict the movement of UAS within the nuclear plant's airspace. This will prevent unauthorized UAS from entering restricted areas and causing safety concerns.
Importance	**SHOULD**

Req. Nº	*S3_GR5*
Req. Name	*Technical expectation - Reliability and Redundancy*
Description	Given the critical nature of a nuclear plant, the C-UAS system may be highly reliable and resilient. It should have redundancy features in place to ensure continuous operation even in the event of system failures or disruptions.
Importance	**MAY**

Req. Nº	*S3_GR6*
Req. Name	Countermeasure's activation
Description	The C-UAS system shall have the possibility to be integrated with the power plant command and control system to ensure coordination and seamless communication between C-UAS operators and power plant operators. The activation of countermeasures shall be done by the specialized operators only after the approval of a power plant operators. This enables effective response without disrupting normal operations. Special procedures should be in place.
Importance	**SHALL**

D.5 Specific operational needs for standard scenario 4 – Government buildings

This scenario is relevant for the security against criminal, terrorist or hostile surveillance actions towards high importance infrastructures for the functioning of states. The scenario could take place at a building complex, located in the middle of a large urban area. There is medium vegetation in the area, major public roads on all sides, private buildings (1 – 10 floors in height), radio interference, etc. The scenario could take place in the afternoon, with clear weather conditions. The threat could be represented by 3 UASs carrying video equipment payloads: commercial multirotor UASs, Class I -

mini and micro category and a custom-made multirotor UAS, Class I - small category. The goal is to carry out a physical attack against a VIP using UAS as a kinetic vector and to create panic.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S4_GR1*
Req. Name	*Technical expectation - Reducing False Positives*
Description	The C-UAS system shall implement advanced algorithms and techniques to minimize false positives and reduce unnecessary disruptions to legitimate UAS operations or activities within the vicinity of the governmental building.
Importance	**SHALL**

Req. Nº	*S4_GR2*
Req. Name	*Technical expectation - Emergency Response Integration*
Description	The C-UAS system should have the possibility to be integrated with emergency response protocols and procedures to ensure coordination between the C-UAS system operators and emergency response teams during UAS incidents.
Importance	**SHOULD**

Req. Nº	*S4_GR3*
Req. Name	*Technical expectation - Integration*
Description	The C-UAS system should have the possibility to be integrated with a centralized command and control centre, enabling real-time monitoring, analysis, and coordination of UAS threats and response activities.
Importance	**SHOULD**

Req. Nº	*S4_GR4*
Req. Name	*Technical expectation - Interagency Cooperation*
Description	Collaboration and coordination channels with other governmental agencies or security organizations may be established within the governmental building and externally, to address UAS threats collectively, share intelligence, and establish response protocols.
Importance	**MAY**

D.6   Specific operational needs for standard scenario 5 - Stadiums

The scenario could take place at a stadium, which can accommodate more than 50.000 people. The location is placed in a suburban area, surrounded by few private homes and industrial production facilities. There are no trees in the area. The electromagnetic environment is very busy due to the large number of mobile phones in the area. The scenario could take place in the evening, with cloudy weather. The threat could be represented by a custom-made multirotor UAS, Class I - small category (>15kg), equipped with an aerosol dispersing device as its payload.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S5_GR1*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall be completely mobile, to allow quick manual installation in various temporary locations.
Importance	**SHALL**

Req. Nº	*S5_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall allow the connection of multiple sensors, to adapt the system's configuration and countermeasure techniques accordingly to the size and shape of protected area, considering the impact of the stadium's surrounding industrial production facilities on the C-UAS system's performance, including potential electromagnetic interference.
Importance	**SHALL**

Req. Nº	*S5_GR3*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be connected to the power lines existing in the location.
Importance	**SHALL**

Req. Nº	*S5_GR4*
Req. Name	*Technical expectation*
Description	The sensors and additional equipment shall be installed quickly, without intervention works on the existing infrastructure in the location
Importance	**SHALL**

Req. Nº	*S5_GR5*
Req. Name	*Technical expectation*
Description	The C&C software operation, shall be available on-site and remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nᵒ	**S4_GR6**
Req. Name	*Privacy Protection*
Description	Privacy protection measures shall be implemented to safeguard the privacy of individuals within and around the stadium, ensuring compliance with applicable privacy laws and regulations.
Importance	**SHALL**

Req. Nᵒ	**S5_GR7**
Req. Name	*Integration in existing security infrastructure*
Description	The C-UAS system should have the possibility to be integrated with the stadium's existing security infrastructure, including surveillance cameras, access control systems, public announcement systems, and emergency response mechanisms, allowing for timely alerts and instructions to be disseminated to stadium visitors and personnel in the event of a UAS threat or incident.
Importance	**SHOULD**

Req. Nᵒ	**S5_GR8**
Req. Name	*Collaboration with Industrial Facilities*
Description	The C-UAS system may have communication channels with surrounding industrial facilities to share information, coordinate security efforts, and address any potential UAS threats originating from or targeting those facilities.
Importance	**MAY**

Req. Nᵒ	**S5_GR9**
Req. Name	*Integration with Public Reporting Mechanisms*
Description	The C-UAS system may connect with established mechanisms for the public to report any suspicious UAS activities or concerns, providing an avenue for increased situational awareness and proactive response to potential threats.
Importance	**MAY**

D.7 Specific operational needs for standard scenario 6 – Outdoor concert

The scenario could take place at an outdoor concert area, which can accommodate more than 50.000 people. The location is in a suburban area. A 20m metallic stage is installed, surrounded by few private homes and industrial production facilities. There are no trees in the area. The electromagnetic environment is very busy, due to the large number of mobile phones in the area. The scenario could take place in the evening, with windy weather. The threat could be represented by a single multirotor UAS, Class I - mini category (15kg) carrying as its payload a dazzling laser.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S6_GR1*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall be completely mobile, to allow quick manual installation in various temporary locations.
Importance	**SHALL**

Req. Nº	*S6_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall allow the connection of multiple sensors, to adapt the performances to the size and shape of protected area and to enhance the detection and tracking capabilities in a busy electromagnetic environment.
Importance	**SHALL**

Req. Nº	*S6_GR3*
Req. Name	*Technical expectation – Laser Threat Detection*
Description	The C-UAS system should have advanced laser threat detection capabilities to identify and track unauthorized unmanned aircraft systems (UAS) equipped with dazzling lasers, distinguishing them from other legitimate UAS activities in the area.
Importance	**SHOULD**

Req. Nº	*S6_GR4*
Req. Name	*Technical expectation*
Description	The C&C software operation, shall be available on-site and remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nº	*S6_GR5*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be connected to the power lines existing in the location.
Importance	**SHALL**

Req. Nº	*S6_GR6*
Req. Name	*Technical expectation*
Description	The sensors and additional equipment shall be installed quickly, without intervention works on the existing infrastructure in the location
Importance	**SHALL**

Req. Nº	S4_GR7
Req. Name	*Privacy Protection*
Description	Privacy protection measures shall be implemented to safeguard the privacy of concert attendees, performers, and staff, ensuring compliance with applicable privacy laws and regulations.
Importance	**SHALL**

Req. Nº	*S5_GR8*
Req. Name	*Technical expectation - Communication Interoperability*
Description	The C-UAS system may ensure interoperability with the concert's communication infrastructure, local emergency services, and industrial facilities to enable information exchange and coordination during UAS threat situations.
Importance	**MAY**

Req. Nº	*S4_GR9*
Req. Name	*Technical expectation - Integration with Weather Monitoring Systems*
Description	The C-UAS system may have the possibility to be integrated with weather monitoring systems to receive real-time updates on weather conditions that may affect UAS operations and the effectiveness of countermeasures, allowing for adaptive response strategies.
Importance	**MAY**

D.8 Specific operational needs for standard scenario 7 – Outdoor political rally

The scenario could take place in the middle of a city, during an authorized rally. The location is an urban area, surrounded by few private homes, hotels, shops and public institutions. There are few small trees in the area and the electromagnetic environment is very busy, due to the large number of mobile devices in the area. The scenario could take place in the evening, with clear weather conditions. The threat could be represented by a single commercial multirotor UAS, Class I - mini category (<15kg), carrying a noise generator as its payload. The scope is for a criminal organization to create panic and cause disturbance to the event.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S7_GR1*
Req. Name	*Technical expectation*
Description	All C-UAS solution components shall be installed on a VAN/truck to allow very quick mobile operations in different urban areas (public squares, large boulevards, etc.)
Importance	**SHALL**

Req. Nº	*S7_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall be completely mobile, to allow quick manual installation in various temporary locations.
Importance	**SHOULD**

Req. Nº	*S7_GR3*
Req. Name	*Technical expectation*
Description	The C&C software operation, shall be available on-site and remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nº	*S7_GR4*
Req. Name	*Technical expectation*
Description	The C-UAS VAN/truck shall be authorized by competent authority in the field of road vehicles, road safety, environmental protection and quality assurance.
Importance	**SHALL**

Req. Nº	*S7_GR5*
Req. Name	*Technical expectation*
Description	The necessary power supply shall be provided just through VAN/truck's internal generators or mobile low noise generators.
Importance	**SHALL**

Req. Nº	*S7_GR6*
Req. Name	*Technical expectation*
Description	When installed in operational fixed mode, the power supply should be provided from external power supply sources.
Importance	**SHOULD**

Req. Nº	*S7_GR7*
Req. Name	*Technical expectation*
Description	The VAN/truck shall be equipped internally, with all the technical means of command, control and communications, which allow the operation of the system
Importance	**SHALL**

Req. Nº	*S7_GR8*
Req. Name	*Technical expectation*
Description	The internal operation room, shall be internally arranged and equipped, with all technical means to allow the operation of the system by the C-UAS team in ergonomic conditions.
Importance	**SHALL**

Req. Nº	*S7_GR9*
Req. Name	*Technical expectation – Acoustic Threat Detection*
Description	The C-UAS system should possess advanced acoustic threat detection capabilities to identify and track unauthorized unmanned aircraft systems (UAS) equipped with noise generators, distinguishing them from other legitimate UAS activities in the vicinity.
Importance	**SHOULD**

Req. Nº	*S7_GR10*
Req. Name	*Collaboration with Public institutions*
Description	The C-UAS system may have communication channels with nearby public institutions, including law enforcement agencies, emergency services, and government entities, to coordinate response efforts, share threat intelligence, and enhance overall event security.
Importance	**MAY**

Req. Nº	*S7_GR11*
Req. Name	*Technical expectation - Communication Interoperability*
Description	The C-UAS system may ensure interoperability with the rally venue's communication infrastructure, including public address systems, emergency alert systems, and event coordination platforms, for seamless information exchange and coordinated response during UAS incidents.
Importance	**MAY**

Req. Nº	*S7_GR12*
Req. Name	*Technical expectation - Geofencing*
Description	The C-UAS system should be able to implement a geofencing mechanism to establish virtual boundaries around the political rally venue and enforce no-fly zones, preventing unauthorized UAS entry.
Importance	**SHOULD**

D.9 Specific operational needs for standard scenario 8 – International Summit

The scenario could take place in an outdoor rural area, at a historical location, where an international summit is organized. The location area is surrounded by trees and the electromagnetic environment is very clean. The scenario takes place in the evening, with dusty weather. The threat could be represented by a single commercial fixed wing UAS, Class I - small category (>15kg). The scope for a terrorist organization is to create panic and cause disturbance to the event.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S8_GR1*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall be completely mobile, to allow quick manual installation in various temporary locations.
Importance	**SHALL**

Req. Nº	*S8_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS solution shall allow the connection of multiple sensors, to adapt the performances to the size and shape of protected area.
Importance	**SHALL**

Req. Nº	*S8_GR3*
Req. Name	*Technical expectation*
Description	The C&C software operation, shall be available on-site and remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nº	*S8_GR4*
Req. Name	*Technical expectation*
Description	The C-UAS solution will include pylons to install the sensors at different heights, for long range detections.
Importance	**SHALL**

Req. Nº	*S8_GR5*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be connected to the power lines existing in the location.
Importance	**SHALL**

Req. Nº	S8_GR6
Req. Name	*Technical expectation*
Description	The sensors and additional equipment shall be installed quickly, without intervention works on the existing infrastructure in the location
Importance	**SHALL**

Req. Nº	S8_GR7
Req. Name	*Collaboration with host country authorities*
Description	The C-UAS system may have communication channels with host country authorities, including relevant government agencies, law enforcement, and aviation authorities, to align security efforts and leverage their expertise in managing potential panic-inducing situations.
Importance	**MAY**

Req. Nº	S8_GR8
Req. Name	*Technical expectation - Geofencing*
Description	The C-UAS system should be able to implement a geofencing mechanism to establish virtual boundaries around the summit area to prevent unauthorized UAS entry and deter potential threats from approaching the venue, enhancing overall security.
Importance	**SHOULD**

Req. Nº	S8_GR9
Req. Name	*Technical expectation - Intelligent Alarm System*
Description	The C-UAS system may include an intelligent alarm system that can differentiate between normal environmental noise and suspicious UAS-related sounds, providing early warning alerts to security personnel in case of potential panic-inducing activities.
Importance	**MAY**

Req. Nº	S8_GR10
Req. Name	*Technical expectation - Covert Operation Capability*
Description	In order to maintain the element of surprise and prevent potential adversaries from circumventing the system, the C-UAS system may have the option for covert operation, concealing its presence and capabilities from unauthorized individuals or groups.
Importance	**MAY**

D.10 Specific operational needs for standard scenario 9 – Land border

The scenario is relevant for the fight against drug/cigarette/gun trafficking at the land border. The scenario could take place at the land border of two countries, in a curved rural area covered with dense vegetation over a length of 100km. There are no electromagnetic interferences. The scenario could take place during a misty night. The threat could be a custom-made multirotor UAS, Class I - small category (>15kg), carrying a 2kg box as its payload. The UAS is used to drop packages in a forested area, away from the border patrol's control area.

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S9_GR1*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be low consuming and must work with power from batteries or renewable sources.
Importance	**SHALL**

Req. Nº	*S9_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be controlled remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nº	*S9_GR3*
Req. Name	*Technical expectation*
Description	The external painting scheme of the equipment, shall ensure camouflage and integration into the landscape specific to the land environment (forests).
Importance	**SHOULD**

Req. Nº	*S9_GR4*
Req. Name	*Technical expectation*
Description	The C-UAS solution must allow the chaining of several systems, to ensure a linear protection of a land border area with a length of over 50 km.
Importance	**SHALL**

Req. Nº	*S9_GR5*
Req. Name	*Technical expectation - Data Sharing and Integration*
Description	The C-UAS system shall establish seamless data sharing and integration capabilities with neighbouring countries and border control agencies, enabling real-time exchange of information and facilitating coordinated response efforts.
Importance	**SHALL**

Req. Nº	S9_GR6
Req. Name	*Technical expectation - Long-Range Detection Capabilities*
Description	The C-UAS system shall incorporate long-range detection technologies, such as advanced surveillance radars or drone detection systems, to detect UAS threats from a distance, providing early warning and allowing for proactive response.
Importance	**SHALL**

Req. Nº	*S9_GR7*
Req. Name	*Technical expectation – Border Geofencing*
Description	The C-UAS system should be able to implement a geofencing mechanism that creates virtual boundaries around the border area, preventing unauthorized UAS entry and automatically triggering alerts when a UAS attempts to breach the designated airspace.
Importance	**SHOULD**

Req. Nº	*S9_GR8*
Req. Name	*Technical expectation -RailSAR*
Description	The C-UAS system may integrate foliage penetration radar technology to detect UAS threats hidden within the dense vegetation, allowing for early detection and response before the threats reach the intended drop-off location.
Importance	**MAY**

D.11 Specific operational needs for standard scenario 10 – Maritime border

The scenario is representative for fraudulent border crossing by immigrants, using boats. The scenario could take place at the sea border at night, in clear weather conditions. The threat could be represented by a commercial multirotor UAS, Class I - mini category (<15kg) and is used as a surveillance means to avoid the coast guard boats (it has a thermal sensor as its payload).

Based on this this scenario example, the following additional specific operational needs are foreseen:

Req. Nº	*S10_GR1*
Req. Name	*Technical expectation*
Description	All system components shall be tested and certified for use in a saline environment.
Importance	**SHALL**

Req. Nº	*S10_GR2*
Req. Name	*Technical expectation*
Description	The C-UAS system performances shall not be reduced due harsh meteorological conditions
Importance	**SHALL**

Req. Nº	*S10_GR3*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be low consuming and must work with power from batteries or renewable sources.
Importance	**SHALL**

Req. Nº	*S10_GR4*
Req. Name	*Technical expectation*
Description	The C-UAS system shall be controlled remotely from long distances, using secured wireless/4G communication channels.
Importance	**SHALL**

Req. Nº	*S10_GR5*
Req. Name	*Technical expectation*
Description	The external painting scheme of the equipment, shall ensure camouflage and integration into the landscape specific to the maritime environment
Importance	**SHALL**

Req. Nº	*S10_GR6*
Req. Name	*Technical expectation*
Description	The C-UAS solution must allow the chaining of several systems, to ensure a linear protection of a maritime border area with a length of over 50 km.
Importance	**SHALL**

Req. Nº	*S10_GR7*
Req. Name	*Technical expectation - Secure Communication Networks*
Description	Establishing secure and encrypted communication networks between the C-UAS system, coast guard boats, and command centres would ensure secure transmission of information, real-time updates, and operational coordination.
Importance	**SHALL**

Req. Nº	*S10_GR8*
Req. Name	*Technical expectation - Stealth Operations*
Description	The C-UAS system shall provide stealth technologies and low-signature operational practices in order to minimize the system's own detectability by potential UAS threats, reducing the risk of counter-detection or evasion.
Importance	**SHALL**

Req. Nº	*S10_GR9*
Req. Name	*Technical expectation - Real-time Video Analytics*
Description	The C-UAS system may have real-time video analytics capabilities that can analyse video feeds from various sensors and platforms, automatically detecting and highlighting potential UAS threats for quicker response and decision-making. The integration of electro-optical sensors, such as low-light cameras or image intensifiers, may complement the thermal sensor capabilities and provide enhanced visual detection and tracking of UAS threats during night-time operations.
Importance	**MAY**

Annex E
(informative)

Functional and performance requirements of C-UAS systems for the standardised scenarios

In this annex, there are presented the functional and performance requirements for each standardised scenario.

E.1 Functional requirements for the standardized scenarios

Scenario 1: Sensitive places / National critical infrastructure – Prison

Table E.1 —Functional requirements - scenario 1

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Functional requirements				
FRPR 1	D	Shall	detect UAS that is appearing in the observation area	
FRPR 2	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRPR 3	T	Shall	track UAS that is moving in the observation area	
FRPR 4	I	Should	identify UAS that is in the observation area	
FRPR 5	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRPR 6	D	Shall	detect a single class C1 UAS (weight <900g - according to Commission Delegated Regulation (EU) 2019/945 of 12 March 2019)	
FRPR 7	D	Should	detect a load carried by UAS weighing … (value next column)	t.b.d.
FRPR 8	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRPR 9	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
FRPR 10	A	Shall	enable simultaneous processing of information from sensors using different technologies	

FRPR 11	I	Should	distinguish between friend or foe UAS (IFF)	
FRPR 12	D	Shall	be immune to false alarms caused by flying birds	
FRPR 13	I	Should	be immune to false alarms caused by flying birds	
FRPR 14	T	Shall	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRPR 15	T	Shall	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	
FRPR 16	T	Should	provide the ability to determine the coordinates of the location of the pilot of the detected UAS	
FRPR 17	I	Should	identify the load carried by the UAS	
FRPR 18	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRPR 19	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRPR 20	T	Shall	track all detected UAS moving in the observation area	
FRPR 21	H	Shall	display messages / prompts about detected UAS	
FRPR 22	H	Should	display messages about detected birds	
FRPR 23	H	Shall	provide the possibility to inform the system operator in a legible manner about the currently detected UAS and their location	
FRPR 24	A	Shall	ensure that all information displayed to the operator by the user interface are to be stored	
FRPR 25	A	Shall	provide the ability to offer a standard tracking interface and location data to the other systems	
FRPR 26	A	Shall	enable operation on emergency power supply from batteries or other power source	

FRPR 27	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRPR 28	H	Should	display UAS status change ("with load" to "load dropped")	
FRPR 29	H	Should	indicate the coordinates of the place of dropping the load	
FRPR 30	H	Should	enable entering into the database of procedures for handling the identification of a given type of load	
FRPR 31	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRPR 32	H	Should	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FRPR 33	H	Shall	have easy intuitive GUI	
FRPR 34	H	May	display UAS status change ("with load" to "load dropped")	

Scenario 2: Sensitive places / National critical infrastructure – Airport

Table E.2 — Functional requirements - scenario 2

Func. Req. ID	Type of Req.	Import ance	Description of the requirement	Value
Functional requirements				
FRAP 1	D	Shall	detect UAS that is appearing in the observation area	
FRAP 2	D	Shall	enable UAS detection in the dark	
FRAP 3	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRAP 4	D	Shall	detect UAS class I, category <15 kg and UAS class I, category> 15 kg, appearing in the observation area	
FRAP 5	D	Shall	detect a UAS flying autonomously	
FRAP 6	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRAP 7	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRAP 8	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRAP 9	T	Shall	track UAS that is moving in the observation area	
FRAP 10	I	Should	identify UAS that is in the observation area	
FRAP 11	I	Shall	identify the commercial UAS that are in the observation area	
FRAP 12	I	Shall	distinguish UAS under observation from other general aviation activities (helicopters and airplanes)	
FRAP 13	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRAP 14	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRAP 15	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRAP 16	T	Shall	track all detected UAS moving in the observation area	
FRAP 17	H	Shall	display messages / prompts about detected UAS	

FRAP 18	D	Shall	detect all UAS in an environment with strong electromagnetic interference	
FRAP 19	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FRAP 20	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRAP 21	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRAP 22	H	Should	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FRAP 23	H	Should	enable the system operator to handle the incident for future analysis	

Scenario 3: Sensitive places / National critical infrastructure – Nuclear power plant

Table E.3 — Functional requirements - scenario 3

Functional requirements				
Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
FRNP 1	D	Shall	detect UAS that is appearing in the observation area	
FRNP 2	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRNP 3	T	Shall	track all detected UAS moving in the observation area	
FRNP 4	I	Should	identify UAS that is in the observation area	
FRNP 5	I	Shall	identify the commercial UAS that are in the observation area	
FRNP 6	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRNP 7	D	Shall	detect a single class I small UAS (<15 kg) equipped with an optical camera as load	
FRNP 8	D	Shall	detect a load carried by UAS weighing … (value next column)	t.b.d.
FRNP 9	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRNP 10	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
FRNP 11	A	Shall	enable simultaneous processing of information from sensors using different technologies	
FRNP 12	D	Shall	enable UAS detection in the dark	
FRNP 13	T	Shall	enable UAS tracking in the dark	
FRNP 14	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRNP 15	T	Shall	track UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRNP 16	D	Shall	detect a UAS flying autonomously	
FRNP 17	I	Shall	distinguish between friend or foe UAS (IFF)	

FRNP 18	D	Shall	be immune to false alarms caused by flying birds	
FRNP 19	I	Shall	provide the ability to identify the UAS belonging to the event service (distinguish friend or foe UAS)	
FRNP 20	T	Shall	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRNP 21	T	Shall	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	
FRNP 22	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRNP 23	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRNP 24	T	Shall	track all detected UAS moving in the observation area	
FRNP 25	H	Shall	display messages / prompts about detected UAS	
FRNP 26	H	Shall	provide the possibility to inform the system operator in a legible manner about the currently detected UAS and their location	
FRNP 27	A	Shall	ensure that all information displayed to the operator by the user interface are to be stored	
FRNP 28	A	Shall	provide the ability to offer a standard tracking interface and location data to the other systems	
FRNP 29	A	May	enable operation on emergency power supply from batteries or other power source	
FRNP 30	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRNP 31	H	Should	provide the possibility of informing about UAS flight parameters	
FRNP 32	H	Shall	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FRNP 33	H	Shall	provide the possibility to inform the system operator in a legible manner about the currently detected UAS and their location	

Scenario 4: Sensitive Sites / Critical National Infrastructure – Government building

Table E.4 — Functional requirements - scenario 4

Functional requirements				
Func. Req. ID	**Type of Req.**	**Importance**	**Description of the requirement**	**Value**
FRGB 1	D	Shall	detect UAS that is appearing in the observation area	
FRGB 2	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRGB 3	D	Shall	track all UAS in an environment with strong electromagnetic interference	
FRGB 4	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRGB 5	D	Should	be immune to false alarms caused by flying birds	
FRGB 6	T	Shall	track UAS that is moving in the observation area	
FRGB 7	T	Shall	track all detected UAS moving in the observation area	
FRGB 8	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FRGB 9	T	Shall	enable UAS tracking in the dark	
FRGB 10	T	Shall	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRGB 11	T	Shall	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	
FRGB 12	I	Shall	identify UAS that is in the observation area	
FRGB 13	I	Shall	identify the load carried by the UAS	
FRGB 14	I	Shall	identify all UAS in an environment with strong electromagnetic interference	
FRGB 15	I	Shall	enable UAS identification in the dark	
FRGB 16	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRGB 17	H	Shall	give the system operator the ability to identify the UAS within the observation area	

FRGB 18	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRGB 19	H	Shall	display messages / prompts about detected UAS	
FRGB 20	H	Shall	provide the possibility of informing about UAS flight parameters	
FRGB 21	H	Shall	have easy intuitive GUI	
FRGB 22	H	Shall	estimate the position of the UAS as soon as it is detected in real time	
FRGB 23	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRGB 24	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRGB 25	H	Should	display messages about detected birds	
FRGB 26	H	Should	have guaranteed manufacturer support in the field of UAS databases	
FRGB 27	H	May	keep logs of detected objects together with their classification by the operator - false alarm / threat	

Scenario 5: Public spaces protection / Events – Stadium

TableE.5 — Functional requirements - scenario 5

Functional requirements				
Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
FRST 1	D	Shall	detect UAS that is appearing in the observation area	
FRST 2	D	Should	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRST 3	D	Shall	detect a load carried by UAS weighing … (value next column)	t.b.d.
FRST 4	D	Should	be immune to false alarms caused by flying birds	
FRST 5	D	Shall	detect a UAS flying autonomously	
FRST 6	D	May	detect frequency on which a UAS is controlled	
FRST 7	D	Shall	detect the discharge of a possible load on the basis of the characteristic feature related to the technology used	
FRST 8	D	Should	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRST 9	D	Shall	detect UAS class I, category <15 kg and UAS class I, category> 15 kg, appearing in the observation area	
FRST 10	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
FRST 11	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRST 12	D	Shall	enable UAS detection in the dark	
FRST 13	D	Shall	provide the user with the ability to detect in non-commercial UAS the modules used (radio, GPS, controller etc)	
FRST 14	D	Shall	track all UAS in an environment with strong electromagnetic interference	
FRST 15	T	Should	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRST 16	T	Shall	enable UAS detection in the dark	
FRST 17	T	Should	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	

FRST 18	T	May	provide the ability to determine the coordinates of the location of the pilot of the detected UAS	
FRST 19	T	Should	track all detected UAS moving in the observation area	
FRST 20	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FRST 21	T	Shall	track UAS that is moving in the observation area	
FRST 22	I	Should	be immune to false alarms caused by flying birds	
FRST 23	I	Shall	distinguish between friend or foe UAS (IFF)	
FRST 24	I	Shall	enable UAS detection in the dark	
FRST 25	I	Shall	identify that the UAS is carrying load	
FRST 26	I	Should	identify the commercial UAS that are in the observation area	
FRST 27	I	Shall	identify the load carried by the UAS	
FRST 28	I	Shall	provide the ability to identify the UAS belonging to the event service (distinguish friend or foe UAS)	
FRST 29	I	Shall	track all UAS in an environment with strong electromagnetic interference	
FRST 30	A	Should	enable operation on emergency power supply from batteries or other power source	
FRST 31	A	Should	enable simultaneous processing of information from sensors using different technologies	
FRST 32	A	Should	ensure that all information displayed to the operator by the user interface are to be stored	
FRST 33	A	May	provide the ability to offer a standard tracking interface and location data to the other systems	
FRST 34	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRST 35	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRST 36	H	Shall	alert the system operator that the UAS is approaching the critical zone of the facility	
FRST 37	H	Should	alert the system operator to the likely type of load being transferred	

FRST 38	H	Shall	alert when the load is dropped	
FRST 39	H	May	be able to give the system operator the access to the history of detected events and/or system logs	
FRST 40	H	Shall	display messages / prompts about detected UAS	
FRST 41	H	May	display UAS status change ("with load" to "load dropped")	
FRST 42	H	May	enable entering into the database of procedures for handling the identification of a given type of load	
FRST 43	H	May	enable the system operator to handle the incident for future analysis	
FRST 44	H	May	enable the system operator to independently identify the non-commercial UAS that is in the area of observation, by preparing a set of prompts containing the identification of individual commercial UAS components	
FRST 45	H	Should	enable the system operator to manually run the adopted procedures	
FRST 46	H	Shall	estimate the position of the UAS as soon as it is detected in real time	
FRST 47	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRST 48	H	Shall	have easy intuitive GUI	
FRST 49	H	Should	have guaranteed manufacturer support in the field of UAS databases	
FRST 50	H	Shall	indicate the coordinates of the place of dropping the load	
FRST 51	H	Shall	indicate the place where the tracked object disappears in the observation area	
FRST 52	H	Shall	provide the possibility of informing about UAS flight parameters	
FRST 53	H	Shall	provide the possibility to inform the system operator in a legible manner about the currently detected UAS and their location	
FRST 54	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	

Scenario 6: Public spaces protection / Events – Outdoor concert

Table E.6 — Functional requirements - scenario 6

Functional requirements				
Func. Req. ID	**Type of Req.**	**Importance**	**Description of the requirement**	**Value**
FROC 1	D	Shall	detect UAS class I, category <15 kg and UAS class I, category> 15 kg, appearing in the observation area	
FROC 2	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FROC 3	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FROC 4	D	Shall	enable UAS detection in the dark	
FROC 5	I	Shall	distinguish between friend or foe UAS (IFF)	
FROC 6	T	Should	enable UAS detection in the dark	
FROC 7	H	Should	alert the system operator that the UAS is approaching the critical zone of the facility	
FROC 8	T	Should	track UAS that is moving in the observation area	
FROC 9	I	Should	identify the commercial UAS that are in the observation area	
FROC 10	I	Should	identify the load carried by the UAS	
FROC 11	H	Should	alert the system operator to the likely type of load being transferred	
FROC 12	H	Should	enable entering into the database of procedures for handling the identification of a given type of load	
FROC 13	H	Shall	enable the system operator to independently identify the non-commercial UAS that is in the area of observation, by preparing a set of prompts containing the identification of individual commercial UAS components	
FROC 14	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	

FROC 15	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FROC 16	T	Shall	track all detected UAS moving in the observation area	
FROC 17	D	Should	detect the discharge of a possible load on the basis of the characteristic feature related to the technology used	
FROC 18	H	Shall	display messages / prompts about detected UAS	
FROC 19	H	Shall	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FROC 20	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FROC 21	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FROC 22	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FROC 23	H	Should	enable the system operator to manually run the adopted procedures	

Scenario 7: Public spaces protection / Events – Outdoor political rally

Table E.7 — Functional requirements - scenario 7

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Functional requirements				
FROR 1	D	Shall	detect UAS that is appearing in the observation area	
FROR 2	T	Shall	track all UAS in an environment with strong electromagnetic interference	
FROR 3	H	Shall	alert the system operator that the UAS is approaching the critical zone of the facility	
FROR 4	T	Shall	track UAS that is moving in the observation area	
FROR 5	I	Shall	identify UAS that is in the observation area	
FROR 6	I	Should	identify that the UAS is carrying load	
FROR 7	H	Should	alert the system operator to the likely type of load being transferred	
FROR 8	H	Should	enable entering into the database of procedures for handling the identification of a given type of load	
FROR 9	H	May	give the system operator the ability to identify the UAS within the observation area	
FROR 10	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FROR 11	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FROR 12	T	Shall	track all detected UAS moving in the observation area	
FROR 13	T	Shall	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	
FROR 14	D	Should	detect the discharge of a possible load on the basis of the characteristic feature related to the technology used	
FROR 15	H	Shall	display messages / prompts about detected UAS	
FROR 16	H	Shall	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FROR 17	D	Shall	track all UAS in an environment with strong electromagnetic interference	

FROR 18	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FROR 19	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FROR 20	H	Should	enable the system operator to manually run the adopted procedures	

Scenario 8: Public spaces protection / Events – International Summit

Table E.8 — Functional requirements - scenario 8

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Functional requirements				
FRIS 1	D	Shall	detect UAS that is appearing in the observation area	
FRIS 2	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRIS 3	D	Shall	detect a UAS flying autonomously	
FRIS 4	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRIS 5	D	Shall	enable UAS detection in the dark	
FRIS 6	D	Should	be immune to false alarms caused by flying birds	
FRIS 7	T	Shall	track UAS that is moving in the observation area	
FRIS 8	T	Shall	track all detected UAS moving in the observation area	
FRIS 9	T	Shall	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRIS 10	T	Shall	ensure the possibility of continuing the UAS tracking despite its temporary loss of sight	
FRIS 11	T	Shall	enable UAS tracking in the dark	
FRIS 12	I	Shall	identify UAS that is in the observation area	
FRIS 13	I	Shall	identify the load carried by the UAS	
FRIS 14	I	Shall	enable UAS identification in the dark	
FRIS 15	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRIS 16	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRIS 17	H	Shall	estimate the position of the UAS as soon as it is detected in real time	

FRIS 18	H	Shall	provide the possibility of informing about UAS flight parameters	
FRIS 19	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRIS 20	H	Shall	have easy intuitive GUI	
FRIS 21	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRIS 22	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRIS 23	H	Should	display messages about detected birds	
FRIS 24	H	Should	have guaranteed manufacturer support in the field of UAS databases	
FRIS 25	H	May	provide the possibility of informing about UAS flight parameters	
FRIS 26	H	Should	have guaranteed manufacturer support in the field of UAS databases	
FRIS 27	H	May	provide the possibility of informing about UAS flight parameters	
FRIS 28	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRIS 29	T	Shall	track UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRIS 30	I	Shall	identify UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRIS 31	H	Should	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FRIS 32	I	Should	distinguish between friend or foe UAS (IFF)	
FRIS 33	H	Should	keep logs of detected objects together with their classification by the operator - false alarm / threat	

Scenario 9: Sensitive places / National critical infrastructure – Land border

Table E.9 — Functional requirements – scenario 9

Func. Req. ID	Type of Req.	Import ance	Description of the requirement	Value
			Functional requirements	
FRLB 1	D	Shall	detect UAS that is appearing in the observation area	
FRLB 2	D	Shall	enable UAS detection in the dark	
FRLB 3	D	Shall	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRLB 4	D	Shall	detect in a difficult environment - afforestation	
FRLB 5	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRLB 6	T	Shall	track UAS that is moving in the observation area	
FRLB 7	I	Should	identify UAS that is in the observation area	
FRLB 8	D	Shall	detect a single class I mini UAS (<15 kg) equipped with an optical camera as load	
FRLB 9	D	Should	detect a load carried by UAS weighing … (value next column)	t.b.d.
FRLB 10	D	Shall	detect a UAS flying autonomously	
FRLB 11	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRLB 12	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
FRLB 13	I	Should	identify that the UAS is carrying load	
FRLB 14	I	Should	identify the load carried by the UAS	
FRLB 15	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRLB 16	D	Shall	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRLB 17	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	

FRLB 18	T	Shall	track all detected UAS moving in the observation area	
FRLB 19	D	Shall	detect the discharge of a possible load on the basis of the characteristic feature related to the technology used	
FRLB 20	H	Shall	indicate the coordinates of the place of dropping the load	
FRLB 21	H	Shall	alert when the load is dropped	
FRLB 22	H	Should	display UAS status change ("with load" to "load dropped")	
FRLB 23	H	Shall	display messages / prompts about detected UAS	
FRLB 24	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRLB 25	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	
FRLB 26	H	Should	keep logs of detected objects together with their classification by the operator - false alarm / threat	
FRLB 27	H	Shall	have easy intuitive GUI	
FRLB 28	H	Shall	enable the system operator to handle the incident for future analysis	
FRLB 29	A	Shall	enable operation on emergency power supply from batteries or other power source	
FRLB 30	A	Shall	ensure that all information displayed to the operator by the user interface are to be stored	

Scenario 10: Border Protection – Maritime border

Table E.10 — Functional requirements - scenario 10

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
			Functional requirements	
FRMB 1	O	Shall	provide the possibility of observation regardless of the state of the sea	
FRMB 2	D	Should	be able to detect another UAS in the observation area, while a previously detected UAS is already being tracked	
FRMB 3	D	Should	be immune to false alarms caused by flying birds	
FRMB 4	D	Shall	detect a single class I mini UAS (<15 kg) equipped with an optical camera as load	
FRMB 5	D	Should	detect a UAS flying autonomously	
FRMB 6	D	Shall	detect frequency on which a UAS is controlled	
FRMB 7	O	Shall	be resistant to severe weather conditions - strong wind	
FRMB 8	D	Should	detect UAS appearing in the observation area in poor visibility conditions caused by adverse weather conditions	
FRMB 9	D	Shall	detect UAS class I, category <15 kg and UAS class I, category> 15 kg, appearing in the observation area	
FRMB 10	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
FRMB 11	D	Shall	detect UAS flying at speed of up to … (value next column)	t.b.d.
FRMB 12	D	Shall	detect UAS that is appearing in the observation area	
FRMB 13	D	Shall	enable UAS detection in the dark	
FRMB 14	D	Should	provide the user with the ability to detect in non-commercial UAS the modules used (radio, GPS, controller etc)	
FRMB 15	T	Should	allow an unchanging unique identifier to be assigned to the detected and then tracked UAS	
FRMB 16	T	Shall	enable UAS detection in the dark	
FRMB 17	T	Shall	provide the ability to determine the coordinates of the location of the pilot of the detected UAS	
FRMB 18	T	Shall	track all detected UAS moving in the observation area	
FRMB 19	I	Should	be immune to false alarms caused by flying birds	
FRMB 20	I	Shall	enable UAS detection in the dark	

FRMB 21	I	Shall	identify the commercial UAS that are in the observation area	
FRMB 22	I	Shall	identify UAS that is in the observation area	
FRMB 23	A	Shall	enable operation on emergency power supply from batteries or other power source	
FRMB 24	A	Should	enable simultaneous processing of information from sensors using different technologies	
FRMB 25	A	Should	ensure that all information displayed to the operator by the user interface are to be stored	
FRMB 26	A	Should	provide the ability to offer a standard tracking interface and location data to the other systems	
FRMB 27	H	Shall	alarm the operator of a malicious UAS with a false positive rate (FPR) of no greater than (value next column)	
FRMB 28	H	Shall	alarm the system operator to the appearance of another UAS in the area of observation, while a previously detected UAS is already being tracked	
FRMB 29	H	Shall	alarm the system operator to the appearance of UAS in the observation area	
FRMB 30	H	Should	be able to give the system operator the access to the history of detected events and/or system logs	
FRMB 31	H	Shall	display messages / prompts about detected UAS	
FRMB 32	H	Should	enable the system operator to handle the incident for future analysis	
FRMB 33	H	May	enable the system operator to independently identify the non-commercial UAS that is in the area of observation, by preparing a set of prompts containing the identification of individual commercial UAS components	
FRMB 34	H	Should	enable the system operator to manually run the adopted procedures	
FRMB 35	H	Shall	estimate the position of the UAS as soon as it is detected in real time	
FRMB 36	H	Shall	give the system operator the ability to identify the UAS within the observation area	
FRMB 37	H	Should	have easy intuitive GUI	
FRMB 38	H	Should	have guaranteed manufacturer support in the field of UAS databases	

FRMB 39	H	Shall	provide the possibility of informing about UAS flight parameters	
FRMB 40	H	Shall	provide the possibility to inform the system operator in a legible manner about the currently detected UAS and their location	
FRMB 41	H	Should	provide the system operator the possibility to choose any events to be currently displayed on the screen, even historical ones	

E.2 Performance requirements for the standardized scenarios

Scenario 1: Sensitive places / National critical infrastructure – Prison

Table E.11 — Performance requirements - scenario 1

Func. Req. ID	Type of Req.	Import ance	Description of the requirement	Value
PRPR 1	A	Shall	operate 24 hours a day, 7 days a week	
PRPR 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRPR 3	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRPR 4	I	Should	have sufficient computing power to ensure identification 24 hours a day, 7 days a week	
PRPR 5	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRPR 6	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	
PRPR 7	I	Should	have enoughRAM (processing resources and storage resources)to ensure identification 24 hours a day, 7 days a week	
PRPR 8	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRPR 9	A	Shall	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PRPR 10	D	Shall	detect all UAS with no missed detections	
PRPR 11	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRPR 12	T	Shall	indicate the position of the object without significant unreal deviations	
PRPR 13	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	
PRPR 14	D	Shall	enable the detection of UAS class C1 (with a mass <900g - in accordance with Commission Delegated	

			Regulation (EU) 2019/945 of 12 March 2019) from a distance of not less than (to be completed)	
PRPR 15	D	Shall	detect communication between the UAS and the pilot on supposed frequencies	
PRPR 16	D	Shall	detect UAS flying at a speed of up to … (value next column)	t.b.d.
PRPR 17	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
PRPR 18	D	Shall	detect the dropping of the load	
PRPR 19	D	Shall	determine the moment of dropping the load with accuracy (to be completed)	t.b.d.
PRPR 20	S	Shall	cover an area of at least … (value next column)	t.b.d.
PRPR 21	D	Should	detect the presence of birds in the set of detected objects	

Scenario 2: Sensitive places / National critical infrastructure – Airport

Table E.12 — Performance requirements - scenario 2

Func. Req. ID	Type of Req.	Import ance	Description of the requirement	Value
			Performance requirements	
PRAP 1	A	Shall	operate 24 hours a day, 7 days a week	
PRAP 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRAP 3	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRAP 4	I	Shall	have sufficient computing power to ensure identification 24 hours a day, 7 days a week	
PRAP 5	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRAP 6	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	
PRAP 7	I	Shall	have enoughRAM (processing resources and storage resources)to ensure identification 24 hours a day, 7 days a week	
PRAP 8	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRAP 9	D	Shall	detect all UAS within the detection area, within the range of the aircraft approach to the glide path from the entire airport area	
PRAP 10	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRAP 11	T	Shall	indicate the position of the object without significant unreal deviations	
PRAP 12	A	Shall	use DTI technologies that does not affect the object infrastructure systems	

Scenario 3: Sensitive places / National critical infrastructure – Nuclear power plant

Table E.13 — Performance requirements - scenario 3

Performance requirements				
Func. Req. ID	Type of Req.	Import ance	Description of the requirement	Value
PRNP 1	A	Shall	operate 24 hours a day, 7 days a week	
PRNP 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRNP 3	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRNP 4	I	Should	have sufficient computing power to ensure identification 24 hours a day, 7 days a week	
PRNP 5	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRNP 6	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	
PRNP 7	I	Should	have enoughRAM (processing resources and storage resources)to ensure identification 24 hours a day, 7 days a week	
PRNP 8	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRNP 9	A	Shall	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PRNP 10	D	Shall	detect all UAS with no missed detections	
PRNP 11	T	Shall	constantly track a given number of UAS simultaneously (value next column)	
PRNP 12	H	Shall	have an appropriate API enabling communication with other systems	
PRNP 13	T	Shall	indicate the position of the object without significant unreal deviations	
PRNP 14	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	
PRNP 15	D	Shall	detect UAS class I small (> 15 kg) from a distance not less than (to be completed)	t.b.d.
PRNP 16	D	Shall	detect UAS flying at a speed of up to … (value next column)	t.b.d.
PRNP 17	D	Shall	detect UAS flying at an altitude of above …	t.b.d.

PRNP 18	D	Shall	enable UAS detection in difficult weather conditions, at night	
PRNP 19	T	Shall	enable UAS detection in difficult weather conditions, at night	
PRNP 20	I	Should	enable UAS identification in difficult weather conditions, at night	
PRNP 21	D	Shall	enable UAS detection in difficult weather conditions, during fog	
PRNP 22	I	Should	enable UAS identification in difficult weather conditions, during fog	
PRNP 23	S	Should	estimate the place of the attack based on the UAS flight trajectory	
PRNP 24	S	Shall	cover an area of at least … (value next column)	t.b.d.
PRNP 25	S	Shall	enable such installation so that its operation does not affect the infrastructure of the facility and its functioning	
PRNP 26	S	Shall	enable such installation so that the facility's infrastructure does not affect system operation	

Scenario 4: Sensitive Sites / Critical National Infrastructure – Government building

Table E.14 — Performance requirements - scenario 4

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements				
PRGB 1	A	Shall	operate 24 hours a day, 7 days a week	
PRGB 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRGB 3	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRGB 4	D	Shall	detect all UAS with no missed detections	
PRGB 5	D	Shall	detect UAS flying at a speed of up to … (value next column)	t.b.d.
PRGB 6	D	Shall	detect UAS class I, mini category	
PRGB 7	D	Shall	detect UAS class I, micro category	
PRGB 8	A	Shall	use DTI technologies that does not affect the object infrastructure systems	
PRGB 9	T	Shall	operate 24 hours a day, 7 days a week	
PRGB 10	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRGB 11	T	Shall	indicate the position of the object without significant unreal deviations	
PRGB 12	I	Should	classify the tracked UAS with the percentage of false positive alarms at a level not more than (value next column)	t.b.d.
PRGB 13	I	Should	classify the tracked UAS with the percentage of false negative alarms of no less than (value next column)	t.b.d.
PRGB 14	I	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRGB 15	I	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRGB 16	I	Shall	operate 24 hours a day, 7 days a week	
PRGB 17	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	

PRGB 18	S	Shall	enable such installation so that the facility's infrastructure does not affect system operation	
PRGB 19	S	Shall	enable such installation so that its operation does not affect the infrastructure of the facility and its functioning	
PRGB 20	L	Should	be easy deployable (determine the number of people, their training and tools necessary to set up and run the system) (value next column)	t.b.d.
PRGB 21	L	Should	be quickly deployable in time of … (value next column)	t.b.d.
PRGB 22	H	Should	alarm the system operator of a malicious UAS with a false positive rate (FPR) of no more than (value next column)	t.b.d.
PRGB 23	H	Should	alarm the system operator of malicious UAS with a False Negative Alarm Rate (FNR) of no less than (value next column)	t.b.d.
PRGB 24	H	Should	have an appropriate API enabling communication with other systems	
PRGB 25	O	Shall	use the frequency bands permitted in a given country (for a given technology)	
PRGB 26	O	Shall	use the transmission power permitted in a given country (for a given technology)	
PRGB 27	A	Should	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PRGB 28	H	May	provide the possibility of informing the system operator about the state of the UAS battery	
PRGB 29	H	May	provide the possibility of informing the system operator about how long the UAS is airborne/ in the air (from its start)	
PRGB 30	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRGB 31	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	

Scenario 5: Public spaces protection / Events – Stadium

Table E.15 — Performance requirements - scenario 5

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements				
PRST 1	O	Shall	ensure the stability of observations under nighttime conditions	
PRST 2	O	Shall	use the frequency bands permitted in a given country (for a given technology)	
PRST 3	O	Shall	use the transmission power permitted in a given country (for a given technology)	
PRST 4	D	Shall	detect all UAS with no missed detections	
PRST 5	D	Should	detect communication between the UAS and the pilot on supposed frequencies	
PRST 6	D	Shall	detect the dropping of the load	
PRST 7	D	Should	detect the presence of birds in the set of detected objects	
PRST 8	D	Shall	detect UAS class I small (> 15 kg) from a distance not less than (to be completed)	t.b.d.
PRST 9	D	Shall	detect UAS class I, mini category	
PRST 10	D	Shall	detect UAS flying at a speed of up to … (value next column)	t.b.d.
PRST 11	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
PRST 12	D	Should	determine the moment of dropping the load with accuracy (to be completed)	
PRST 13	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	
PRST 14	D	Shall	enable UAS detection in difficult weather conditions, at night	
PRST 15	D	Shall	provide the ability to detect UAS at equal distances around the stadium … (value next column)	t.b.d.
PRST 16	D	Shall	run continuously for 12 hours	
PRST 17	T	Should	determine the place of dropping the load with accuracy (to be completed)	
PRST 18	T	Shall	enable UAS detection in difficult weather conditions, at night	

PRST 19	T	Shall	ensure the ability to track the UAS despite the temporary loss of signal for a time not shorter than … (value next column)	t.b.d.
PRST 20	T	Shall	indicate the position of the object without significant unreal deviations	
PRST 21	T	Shall	run continuously for 12 hours	
PRST 22	I	Shall	classify the tracked UAS with the percentage of false negative alarms of no less than (value next column)	t.b.d.
PRST 23	I	Shall	enable UAS detection in difficult weather conditions, at night	
PRST 24	I	Should	identify the birds distinguishing them from the UAS	
PRST 25	I	Shall	run continuously for 12 hours	
PRST 26	A	Shall	be resistant to being drowned out by loud noise during the concert … (value next column)	t.b.d.
PRST 27	A	Shall	be resistant to stimuli that may accompany the event	
PRST 28	A	Should	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PRST 29	A	Should	have access to above mentioned memory in real time	
PRST 30	A	Should	have guaranteed manufacturer support in the field of UAS databases	
PRST 31	A	Should	provide the ability to monitor the radio spectrum	
PRST 32	S	Shall	cover an area of at least … (value next column)	t.b.d.
PRST 33	L	Should	be easy deployable (determine the number of people, their training and tools necessary to set up and run the system) (value next column)	
PRST 34	L	Should	operate in an area without access to the mains	
PRST 35	H	Shall	alarm the system operator of malicious UAS with a False Negative Alarm Rate (FNR) of no less than (value next column)	t.b.d.
PRST 36	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the type of transmission between UAS and the system operator	
PRST 37	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS location	

PRST 38	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS type	
PRST 39	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information with the geo-positional module used	
PRST 40	H	May	have an appropriate API enabling communication with other systems	
PRST 41	H	May	provide the possibility of informing the system operator about the state of the UAS battery	

Scenario 6: Public spaces protection / Events – Outdoor concert

Table E.16 — Performance requirements - scenario 6

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements				
PROC 1	T	Shall	run continuously for 12 hours	
PROC 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PROC 3	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PROC 4	A	Shall	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PROC 5	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PROC 6	S	Shall	cover an area of at least … (value next column)	
PROC 7	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	
PROC 8	D	Should	detect the presence of birds in the set of detected objects	
PROC 9	I	Should	identify the birds distinguishing them from the UAS	
PROC 10	T	Should	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PROC 11	T	Shall	indicate the position of the object without significant unreal deviations	
PROC 12	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS location	
PROC 13	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS type	
PROC 14	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the type of transmission between UAS and the system operator	

PROC 15	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information with the geo-positional module used	
PROC 16	D	Should	determine the moment of dropping the load with accuracy (to be completed)	t.b.d.
PROC 17	T	Should	determine the place of dropping the load with accuracy (to be completed)	t.b.d.

Scenario 7: Public spaces protection / Events – Outdoor political rally

Table E.17 — Performance requirements - scenario 7

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements
PROR 1	T	Shall	run continuously for 12 hours	
PROR 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PROR 3	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PROR 4	A	Shall	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PROR 5	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PROR 6	S	Shall	cover an area of at least … (value next column)	
PROR 7	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	t.b.d.
PROR 8	D	Should	detect the presence of birds in the set of detected objects	
PROR 9	I	Should	identify the birds distinguishing them from the UAS	
PROR 10	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PROR 11	T	Shall	indicate the position of the object without significant unreal deviations	
PROR 12	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS location	
PROR 13	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS type	
PROR 14	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the type of transmission between UAS and the system operator	

PROR 15	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information with the geo-positional module used	
PROR 16	D	Should	determine the moment of dropping the load with accuracy (to be completed)	
PROR 17	T	Should	determine the place of dropping the load with accuracy (to be completed)	

Scenario 8: Public spaces protection / Events – International Summit

Table E.18 — Performance requirements - scenario 8

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
PRIS 1	A	Shall	operate 24 hours a day, 7 days a week	
PRIS 2	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRIS 3	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRIS 4	D	Shall	detect all UAS with no missed detections	
PRIS 5	A	Shall	use DTI technologies that does not affect the object infrastructure systems	
PRIS 6	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRIS 7	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	
PRIS 8	T	Shall	operate 24 hours a day, 7 days a week	
PRIS 9	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRIS 10	T	Shall	indicate the position of the object without significant unreal deviations	t.b.d.
PRIS 11	I	Shall	operate 24 hours a day, 7 days a week	
PRIS 12	I	Shall	have sufficient computing power to ensure identification 24 hours a day, 7 days a week	
PRIS 13	I	Shall	have enoughRAM (processing resources and storage resources)to ensure identification 24 hours a day, 7 days a week	
PRIS 14	I	Should	classify the tracked UAS with the percentage of false positive alarms at a level not more than (value next column)	t.b.d.
PRIS 15	I	Should	classify the tracked UAS with the percentage of false negative alarms of no less than (value next column)	t.b.d.
PRIS 16	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRIS 17	A	Shall	have access to above mentioned memory in real time	

PRIS 18	S	Shall	enable such installation so that its operation does not affect the infrastructure of the facility and its functioning	
PRIS 19	S	Shall	enable such installation so that the facility's infrastructure does not affect system operation	
PRIS 20	L	Shall	be easy deployable (determine the number of people, their training and tools necessary to set up and run the system) (value next column)	t.b.d.
PRIS 21	L	Shall	be quickly deployable in time of … (value next column)	t.b.d.
PRIS 22	H	Should	alarm the system operator of a malicious UAS with a false positive rate (FPR) of no more than (value next column)	t.b.d.
PRIS 23	H	Should	alarm the system operator of malicious UAS with a False Negative Alarm Rate (FNR) of no less than (value next column)	t.b.d.
PRIS 24	H	Should	have an appropriate API enabling communication with other systems	
PRIS 25	O	Shall	use the frequency bands permitted in a given country (for a given technology)	
PRIS 26	O	Shall	use the transmission power permitted in a given country (for a given technology)	
PRIS 27	D	Should	detect all UAS with no missed detections	
PRIS 28	A	Should	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRIS 29	A	Shall	ensure that all signals are recorded in native resolution (continuously and efficiently)	

Scenario 9: Sensitive places / National critical infrastructure – Land border

Table E.19 — Performance requirements - scenario 9

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements				
PRLB 1	A	Shall	operate 24 hours a day, 7 days a week	
PRLB 2	L	Shall	operate in an area without access to the mains	
PRLB 3	L	Shall	operate in an area without access to the telecommunications network	
PRLB 4	L	Shall	transmit D, T, I signals over long distances to the system operator … (value next column)	
PRLB 5	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRLB 6	T	Shall	have sufficient computing power to ensure tracking 24 hours a day, 7 days a week	
PRLB 7	I	Should	have sufficient computing power to ensure identification 24 hours a day, 7 days a week	
PRLB 8	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRLB 9	T	Shall	have enoughRAM (processing resources and storage resources)to ensure tracking 24 hours a day, 7 days a week	
PRLB 10	I	Should	have enoughRAM (processing resources and storage resources)to ensure identification 24 hours a day, 7 days a week	
PRLB 11	A	Shall	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRLB 12	S	Shall	cover an area of at least … (value next column)	t.b.d.
PRLB 13	D	Should	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	t.b.d.
PRLB 14	D	Shall	enable detection in inaccessible rural areas covered with dense vegetation	
PRLB 15	T	Shall	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRLB 16	T	Shall	indicate the position of the object without significant unreal deviations	

PRLB 17	D	Shall	be resistant to severe weather conditions - strong wind	
PRLB 18	D	Shall	enable UAS detection in difficult weather conditions, at night	
PRLB 19	D	Shall	enable UAS detection in difficult weather conditions, during fog	
PRLB 20	T	Shall	be resistant to severe weather conditions - strong wind	
PRLB 21	T	Shall	indicate the position of the object without significant unreal deviations	
PRLB 22	T	Shall	enable UAS detection in difficult weather conditions, at night	
PRLB 23	T	Shall	enable UAS detection in difficult weather conditions, during fog	
PRLB 24	I	Should	be resistant to severe weather conditions - strong wind	
PRLB 25	I	Should	identify the birds distinguishing them from the UAS	

Scenario 10: Border Protection – Maritime border

TableE.20 — Performance requirements - scenario 10

Func. Req. ID	Type of Req.	Importance	Description of the requirement	Value
Performance requirements				
PRMB 1	O	Shall	ensure the stability of observations under nighttime conditions	
PRMB 2	O	Should	use the frequency bands permitted in a given country (for a given technology)	
PRMB 3	O	Should	use the transmission power permitted in a given country (for a given technology)	
PRMB 4	D	Shall	detect all UAS with no missed detections	
PRMB 5	D	Shall	detect communication between the UAS and the pilot on supposed frequencies	
PRMB 6	D	Shall	detect objects with technology that does not interfere with the communication systems of government security (not necessarily RF)	
PRMB 7	D	Should	detect the presence of birds in the set of detected objects	
PRMB 8	D	Shall	detect UAS class I, mini category	
PRMB 9	D	Shall	detect UAS flying at a speed of up to … (value next column)	t.b.d.
PRMB 10	D	Shall	detect UAS flying at an altitude of up to … (value next column)	t.b.d.
PRMB 11	D	Shall	enable the detection of UAS within the time (distance) that allows the implementation of security procedures	
PRMB 12	D	Shall	enable UAS detection in difficult weather conditions, at night	
PRMB 13	D	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRMB 14	D	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRMB 15	D	Shall	operate 24 hours a day, 7 days a week	
PRMB 16	D	Should	provide the ability to detect UAS at height up to … (value next column) m, right above sea level	
PRMB 17	T	Should	constantly track a given number of UAS simultaneously (value next column)	t.b.d.
PRMB 18	T	Shall	enable UAS detection in difficult weather conditions, at night	
PRMB 19	T	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	

PRMB 20	T	Shall	indicate the position of the object without significant unreal deviations	
PRMB 21	T	Shall	operate 24 hours a day, 7 days a week	
PRMB 22	T	Should	provide the ability to detect UAS at height up to ... (value next column) m, right above sea level	t.b.d.
PRMB 23	I	Shall	classify the tracked UAS with the percentage of false negative alarms of no less than (value next column)	t.b.d.
PRMB 24	I	Shall	classify the tracked UAS with the percentage of false positive alarms at a level not more than (value next column)	t.b.d.
PRMB 25	I	Shall	enable UAS detection in difficult weather conditions, at night	
PRMB 26	I	Shall	have enoughRAM (processing resources and storage resources)to ensure detections 24 hours a day, 7 days a week	
PRMB 27	I	Shall	have sufficient computing power to ensure detection 24 hours a day, 7 days a week	
PRMB 28	I	Should	identify the birds distinguishing them from the UAS	
PRMB 29	I	Shall	operate 24 hours a day, 7 days a week	
PRMB 30	I	Should	provide the ability to detect UAS at height up to ... (value next column) m, right above sea level	t.b.d.
PRMB 31	A	Should	ensure that all signals are recorded in native resolution (continuously and efficiently)	
PRMB 32	A	Should	have a server with sufficient memory to provide detection recording for the period required by the user and access to this memory in real time	
PRMB 33	A	Should	have access to above mentioned memory in real time	
PRMB 34	A	Should	have guaranteed manufacturer support in the field of UAS databases	
PRMB 35	A	Shall	provide the ability to monitor the radio spectrum	
PRMB 36	S	Shall	cover an area of at least ... (value next column)	t.b.d.
PRMB 37	L	Shall	transmit D, T, I signals over long distances to the system operator ... (value next column)	t.b.d.
PRMB 38	H	Shall	alarm the system operator of malicious UAS with a False Negative Alarm Rate (FNR) of no less than (value next column)	
PRMB 39	H	Should	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the type of transmission between UAS and the system operator	

PRMB 40	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS location	
PRMB 41	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information about the UAS type	
PRMB 42	H	May	be able to integrate with an external UAS counteraction system by issuing an API providing access to information with the geo-positional module used	
PRMB 43	H	Should	have an appropriate API enabling communication with other systems	
PRMB 44	H	May	provide the possibility of informing the system operator about how long the UAS is airborne/ in the air (from its start)	
PRMB 45	H	May	provide the possibility of informing the system operator about the state of the UAS battery	

E.3 Correlations between the functional and performance requirements and the operational needs for the standardized scenarios

The functional and performance requirements of C-UAS systems are linked to operational needs described in Clause 9. The described requirements allow for defining the minimum requirements for C-UAS systems applicable to various scenarios and directly refer to them. Each application area of the C-UAS system will have slightly different requirements regarding operating parameters, power supply, type of detected UAS, and the conditions in which they are to operate.

This annex presents direct correlations or their absence, along with reasons for the lack of correlation, between operational needs and functional and performance requirements.

Table E.21 — Association table

No.	Operational needs	Functional requirements	Performance requirements	Remarks
1.	GR01	**Scenario 1**: FRPR 11, FRPR 4, FRPR 20, FRPR 3 **Scenario 2**: FRAP 11, FRAP 10, FRAP 16, FRAP 9 **Scenario 3**: FRNP 17, FRNP 5, FRNP 4, FRNP 19, FRNP 24 **Scenario 4:** FRGB 12, FRGB 7, FRGB 6 **Scenario 5**: FRST 23, FRST 26, FRST 28, FRST 19, FRST 21 **Scenario 6**: FROC 5, FROC 9, FROC 16, FROC 8 **Scenario 7**: FROR 5, FROR 12, FROR 4 **Scenario 8**: FRIS 32, FRIS 12, FRIS 8, FRIS 7 **Scenario 9**: FRLB 7, FRLB 18, FRLB 6 **Scenario 10**: FRMB 21, FRMB 22, FRMB 18	-	-
2.	GR02	-	-	The provision concerns neutralisation systems that are not the subject of the Courageous project
3.	GR03	**Scenario 1:** FRPR 10 **Scenario 3:** FRNP 11 **Scenario 5:** FRST 31 **Scenario 10:** FRMB 24	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
4.	GR04	**Scenario 2:** FRAP 5, FRAP 3, FRAP 2 **Scenario 3:** FRNP 16, FRNP 14, FRNP 12 **Scenario 4:** FRGB 4 **Scenario 5:** FRST 5, FRST 8, FRST 12, FRST 13 **Scenario 6:** FROC 3, FROC 4 **Scenario 8:** FRIS 3, FRIS 4, FRIS 5 **Scenario 9:** FRLB 10, FRLB 3, FRLB 2 **Scenario 10:** FRMB 5, FRMB 8, FRMB 13, FRMB 14	-	-
5.	GR05	-	-	The provision concerns types of attacks using UAS (terrorist or criminal acts). Functional requirements, on the other hand, focus on describing the requirements for DTI systems, ignoring the nature of the attack.
6.	GR06	**Scenario 1:** FRPR 25 **Scenario 3:** FRNP 28 **Scenario 5:** FRST 33 **Scenario 10:** FRMB 26	-	The provision mentions increasing the level of cooperation between institutions. The technical parameter related to this is the ability to exchange data with other systems, as indicated in this table.
7.	GR07	**Scenario 1:** FRPR 31 **Scenario 2:** FRAP 23, FRAP 21 **Scenario 3:** FRNP 30	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
		Scenario 4: FRGB 24 **Scenario 5:** FRST 45, FRST 54, FRST 43 **Scenario 6:** FROC 23, FROC 22 **Scenario 7:** FROR 20, FROR 19 **Scenario 8:** FRIS 22 **Scenario 9:** FRLB 28, FRLB 25 **Scenario 10:** FRMB 32, FRMB 34, FRMB 41		
8.	GR08	**Scenario 1:** FRPR 1, FRPR 4, FRPR 20 **Scenario 2:** FRAP 1, FRAP 10, FRAP 16 **Scenario 3:** FRNP 1, FRNP 4, FRNP 24 **Scenario 4:** FRGB 1, FRGB 12, FRGB 7 **Scenario 5:** FRST 1, FRST 19 **Scenario 6:** FROC 16 **Scenario 7:** FROR 1, FROR 5, FROR 12 **Scenario 8:** FRIS 1, FRIS 12, FRIS 8 **Scenario 9:** FRLB 1, FRLB 7, FRLB 18 **Scenario 10:** FRMB 12, FRMB 22, FRMB 18	-	-
9.	GR09	-	**Scenario 4:** PRGB 25, PRGB 26 **Scenario 5:** PRST 2, PRST 3 **Scenario 8:** PRIS 25, PRIS 26 **Scenario 10:** PRMB 2, PRMB 3	The regulation concerns the legality of using the C-UAS system in the EU. Some provisions of the Performance Requirements refer to this issue.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
10.	GR10	-	-	The provision concerns neutralisation requirements that are not covered by the COURAGEOUS project.
11.	GR11	-	**Scenario 1:** PRPR 1 **Scenario 2:** PRAP 1 **Scenario 3:** PRNP 1 **Scenario 4:** PRGB 1 **Scenario 8:** PRIS 1 **Scenario 9:** PRLB 1 **Scenario 10:** PRMB 15, PRMB 21, PRMB 29	-
12.	GR12	**Scenario 2:** FRAP 3 **Scenario 3:** FRNP 14, FRNP 15 **Scenario 4:** FRGB 4 **Scenario 5:** FRST 8 **Scenario 6:** FROC 3 **Scenario 8:** FRIS 4, FRIS 30, FRIS 29 **Scenario 9:** FRLB 3 **Scenario 10:** FRMB 8, FRMB 1	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
13.	GR13	**Scenario 1:** FRPR 6 **Scenario 2:** FRAP 4 **Scenario 3:** FRNP 7 **Scenario 5:** FRST 9 **Scenario 6:** FROC 1 **Scenario 9:** FRLB 8 **Scenario 10:** FRMB 4, FRMB 9	-	In Operational Needs, the UAS classification according to NATO was adopted, and in Functional Requirements, according to the EU.
14.	GR14	-	-	The condition applies DTI of UAS regardless of shape and colour. In Functional Requirements, this condition is taken as obvious, without being described.
15.	GR15	-	-	The condition applies DTI of UAS due to the type (rotary, wing, etc.). In Functional Requirements, this condition is taken as obvious, without being described.
16.	GR16	**Scenario 2:** FRAP 5 **Scenario 3:** FRNP 16 **Scenario 5:** FRST 5 **Scenario 8:** FRIS 3 **Scenario 9:** FRLB 10 **Scenario 10:** FRMB 5	-	The condition concerns the method of UAS air navigation. The Functional Requirements assume that manually navigated UAS are the most common case and additional conditions have been adopted for them. Automatic navigation was treated exceptionally, and the following provisions apply to it.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
17.	GR17	**Scenario 2:** FRAP 5 **Scenario 3:** FRNP 16 **Scenario 5:** FRST 5 **Scenario 8:** FRIS 3 **Scenario 9:** FRLB 10 **Scenario 10:** FRMB 5	-	Note as above in GR16.
18.	GR18	-	-	The condition applies to UAS detection regardless of the flight path. For Functional Requirements this is an obvious condition.
19.	GR19	-	-	The condition applies to UAS detection in a GPS-free environment. The Functional Requirements include one condition regarding autonomous flights.
20.	GR20	-	-	The condition applies to UAS detection without an active RF link. The Functional Requirements include one condition regarding autonomous flights.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
21.	GR21	**Scenario 1:** FRPR 18, FRPR 19 **Scenario 2:** FRAP 14, FRAP 1 **Scenario 3:** FRNP 22, FRNP 23 **Scenario 4:** FRGB 2, FRGB 18 **Scenario 5:** FRST 2, FRST 34 **Scenario 6:** FROC 14, FROC 15 **Scenario 7:** FROR 10, FROR 11 **Scenario 8:** FRIS 2, FRIS 16 **Scenario 9:** FRLB 16, FRLB 17 **Scenario 10:** FRMB 2, FRMB 28	-	-
22.	GR22	**Scenario 1:** FRPR 16 **Scenario 4:** FRGB 22 **Scenario 5:** FRST 13, FRST 46, FRST 18 **Scenario 8:** FRIS 17 **Scenario 10:** FRMB 14, FRMB 35, FRMB 17	**Scenario 1:** PRPR 15 **Scenario 4:** PRGB 29, PRGB 28 **Scenario 5:** PRST 5, PRST 41 **Scenario 10:** PRMB 5, PRMB 44, PRMB 45	Some of the provisions relating to this Operational Need are included in the Functional Requirements and some in the Performance Requirements.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
23.	GR23	**Scenario 1:** FRPR 10, FRPR 2, FRPR 20, FRPR 3 **Scenario 2:** FRAP 8, FRAP 11, FRAP 16, FRAP 9 **Scenario 3:** FRNP 11, FRNP 2, FRNP 5, FRNP 24 **Scenario 4:** FRGB 16, FRGB 7, FRGB 6 **Scenario 5:** FRST 31, FRST 35, FRST 26, FRST 19, FRST 21 **Scenario 6:** FROC 9, FROC 16, FROC 8 **Scenario 7:** FROR 12, FROR 4 **Scenario 8:** FRIS 15, FRIS 8, FRIS 7 **Scenario 9:** FRLB 5, FRLB 18, FRLB 6 **Scenario 10:** FRMB 24, FRMB 29, FRMB 21, FRMB 18	-	-
24.	GR24	-	-	The Functional and Performance Requirements do not contain this provision directly, but they are indicated by other, detailed requirements.
25.	GR25	-	-	The Functional and Performance Requirements do not contain this provision directly, but they are indicated by other, detailed requirements.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
26.	GR26	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	-
27.	GR27	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	From the Functional Requirements side, the provisions of GR26 and GR27 will meet the same points.
28.	GR28	**Scenario 1:** FRPR 2 **Scenario 2:** FRAP 8 **Scenario 3:** FRNP 2 **Scenario 4:** FRGB 16 **Scenario 5:** FRST 35, FRST 36 **Scenario 6:** FROC 7 **Scenario 7:** FROR 3 **Scenario 8:** FRIS 15 **Scenario 9:** FRLB 5 **Scenario 10:** FRMB 29	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
29.	GR29	**Scenario 1:** FRPR 2 **Scenario 2:** FRAP 8 **Scenario 3:** FRNP 2 **Scenario 4:** FRGB 16 **Scenario 5:** FRST 35, FRST 36 **Scenario 6:** FROC 7 **Scenario 7:** FROR 3 **Scenario 8:** FRIS 15 **Scenario 9:** FRLB 5 **Scenario 10:** FRMB 29	-	From the Functional Requirements side, the provisions of GR28 and GR29 will meet the same points.
30.	GR30	**Scenario 1:** FRPR 11 **Scenario 3:** FRNP 17 **Scenario 5:** FRST 23 **Scenario 6:** FROC 5 **Scenario 8:** FRIS 32	-	-
31.	GR31	-	-	The Functional and Performance Requirements do not contain this provision directly, but they are indicated by other, detailed requirements.
32.	GR32	-	-	The Functional and Performance Requirements do not contain this provision directly, but they are indicated by other, detailed requirements.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
33.	GR33	-	-	The provision was omitted when creating the Functional Requirements and Performance Requirements because constant maintenance of the system was assumed during its use.
34.	GR34	-	-	The provision was omitted because it was assumed that diagnostics were the domain of the factory service.
35.	GR35	-	-	Functional and Performance Requirements are related to scenarios and do not contain detailed requirements related to access to the system.
36.	GR36	**Scenario 1:** FRPR 27, FRPR 32 **Scenario 2:** FRAP 20, FRAP 22 **Scenario 3:** FRNP 32 **Scenario 4:** FRGB 23, FRGB 27 **Scenario 5:** FRST 39 **Scenario 6:** FROC 21, FROC 19 **Scenario 7:** FROR 18, FROR 16 **Scenario 8:** FRIS 21, FRIS 31 **Scenario 9:** FRLB 24, FRLB 26 **Scenario 10:** FRMB 30	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
37.	GR37	**Scenario 1:** FRPR 32 **Scenario 2:** FRAP 22 **Scenario 3:** FRNP 32 **Scenario 4:** FRGB 27 **Scenario 6:** FROC 19 **Scenario 7:** FROR 16 **Scenario 8:** FRIS 31 **Scenario 9:** FRLB 26	**Scenario 1:** PRPR 8 **Scenario 2:** PRAP 8 **Scenario 3:** PRNP 8 **Scenario 4:** PRGB 17 **Scenario 6:** PROC 5 **Scenario 7:** PROR 5 **Scenario 8:** PRIS 16 **Scenario 9:** PRLB 11 **Scenario 10:** PRMB 32	-
38.	GR38	-	**Scenario 5:** PRST 36, PRST 37, PRST 38, PRST 39 **Scenario 6:** PROC 14, PROC 12, PROC 13, PROC 15 **Scenario 7:** PROR 14, PROR 12, PROR 13, PROR 15 **Scenario 10:** PRMB 39, PRMB 40, PRMB 41, PRMB 42	-
39.	GR39	-	**Scenario 4:** PRGB 20 **Scenario 5:** PRST 33 **Scenario 8:** PRIS 20	-
40.	GR40	-	**Scenario 4:** PRGB 20 **Scenario 5:** PRST 33 **Scenario 8:** PRIS 20	From the Performance Requirements side, the provisions of GR39 and GR40 will meet the same points.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
41.	GR41	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	The provision is very similar to point GR26.
42.	GR42	-	-	General provision regarding the system's connecting elements. It is not applicable in Functional and Performance Requirements that are related to scenarios.
43.	GR43	-	-	General provision regarding the resistance of devices to environmental conditions. It is not applicable in Functional and Performance Requirements that are related to scenarios.
44.	GR44	-	-	General provision regarding the connection of C-UAS components via an IT network. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
45.	GR45	**Scenario 1:** FRPR 33 **Scenario 4:** FRGB 21 **Scenario 5:** FRST 48 **Scenario 8:** FRIS 20 **Scenario 9:** FRLB 27 **Scenario 10:** FRMB 37	-	-
46.	GR46	-	-	Provision is related to maintaining the proper operation of equipment and in this respect it is similar to the operational need of GR34.
47.	GR47	-	**Scenario 5:** PRST 36, PRST 37, PRST 38, PRST 39 **Scenario 6:** PROC 14, PROC 12, PROC 13, PROC 15 **Scenario 7:** PROR 14, PROR 12, PROR 13, PROR 15 **Scenario 10:** PRMB 39, PRMB 40, PRMB 41, PRMB 42	The requirement is similar in meaning to GR38.
48.	GR48			Provision refers to the automatic configuration of the system at startup. It is not applicable in Functional and Performance Requirements that are related to scenarios.
49.	GR49	-	**Scenario 9:** PRLB 3	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
50.	GR50	-	-	General provision regarding the system architecture. It is not applicable in Functional and Performance Requirements that are related to scenarios.
51.	GR51	-	-	General provision regarding the system architecture. It is not applicable in Functional and Performance Requirements that are related to scenarios.
52.	GR52	-	-	General provision regarding the system architecture. It is not applicable in Functional and Performance Requirements that are related to scenarios.
53.	GR53	-	-	General provision regarding the system's compliance with GDPR regulations. It is not applicable in Functional and Performance Requirements that are related to scenarios.
54.	GR54	-	-	General provision regarding the system's compliance with GDPR regulations. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
55.	GR55	-	-	A general provision regarding the system's compliance with regulations regarding products that may pose a threat to life, health, occupational safety and environmental protection. It is not applicable in Functional and Performance Requirements that are related to scenarios.
56.	GR56	-	-	A general provision regarding the system's compliance with electromagnetic compatibility regulations. It is not applicable in Functional and Performance Requirements that are related to scenarios.
57.	GR57	-	-	General provision regarding the system's compliance with regulations regarding safe work with electrical devices. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
58.	GR58	-	-	A general provision regarding the system's compliance with regulations regarding restrictions on the use of certain hazardous substances in electrical and electronic equipment. It is not applicable in Functional and Performance Requirements that are related to scenarios.
59.	GR59	-	-	A general provision regarding the system's compliance with regulations relating to eco-design requirements for computers and servers. It is not applicable in Functional and Performance Requirements that are related to scenarios.
60.	GR60	-	-	General provision for compliance with the military standard for performing environmental testing of the system. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
61.	GR61	-	-	General provision on how to label individual system elements. It is not applicable in Functional and Performance Requirements that are related to scenarios.
62.	GR62	-	-	A general provision on how to label individual system elements related to the possible threats they cause. It is not applicable in Functional and Performance Requirements that are related to scenarios.
63.	GR63	-	-	A general record of the time in which the devices were manufactured and the product specifications attached to them. It is not applicable in Functional and Performance Requirements that are related to scenarios.
64.	GR64	-	-	General record of how maintenance is carried out. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
65.	GR65	-	-	General provision regarding manufacturer's logistic support. It is not applicable in Functional and Performance Requirements that are related to scenarios.
66.	GR66	-	-	General product warranty provision. It is not applicable in Functional and Performance Requirements that are related to scenarios.
67.	GR67	-	-	General record of receipt of the product. It is not applicable in Functional and Performance Requirements that are related to scenarios.
68.	GR68	-	-	General provision regarding product documentation, including user manuals. It is not applicable in Functional and Performance Requirements that are related to scenarios.
69.	GR69	-	-	A general record of the duration of use of the product. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
70.	GR70	-	-	General provision regarding software licensing. It is not applicable in Functional and Performance Requirements that are related to scenarios.
71.	GR71	-	-	General provision regarding perpetual software licenses. It is not applicable in Functional and Performance Requirements that are related to scenarios.
72.	GR72	-	-	General provision regarding software license migration. It is not applicable in Functional and Performance Requirements that are related to scenarios.
73.	GR73	-	-	A general provision regarding the time in which software updates should be available. It is not applicable in Functional and Performance Requirements that are related to scenarios.
74.	GR74	-	-	General provision regarding product painting schemes. It is not applicable in Functional and Performance Requirements that are related to scenarios.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
75.	In01	-	**Scenario 5:** PRST 37 **Scenario 6:** PROC 12 **Scenario 7:** PROR 12 **Scenario 10:** PRMB 40	-
76.	In02	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	-
77.	In03	-	-	Detailed requirement regarding the connectivity of system components. The Functional and Quality Requirements do not include this condition and focus on DTI functions.
78.	In04	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	Provision functionally similar to In02.
79.	In05	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	Provision functionally similar to In02.

No.	Operational needs	Functional requirements	Performance requirements	Remarks
80.	In06	-	**Scenario 3:** PRNP 12 **Scenario 4:** PRGB 24 **Scenario 5:** PRST 40 **Scenario 8:** PRIS 24 **Scenario 10:** PRMB 43	Provision functionally similar to In02.
81.	In07	-	**Scenario 2:** PRAP 12 **Scenario 4:** PRGB 8 **Scenario 8:** PRIS 5	-
82.	In08	-	**Scenario 3:** PRNP 25 **Scenario 4:** PRGB 19 **Scenario 8:** PRIS 18	-
83.	FE01	**Scenario 1:** FRPR 32 **Scenario 2:** FRAP 22 **Scenario 3:** FRNP 32 **Scenario 4:** FRGB 27 **Scenario 6:** FROC 19 **Scenario 7:** FROR 16 **Scenario 8:** FRIS 31 **Scenario 9:** FRLB 26	-	-

No.	Operational needs	Functional requirements	Performance requirements	Remarks
84.	FE02	**Scenario 1:** FRPR 32 **Scenario 2:** FRAP 22 **Scenario 3:** FRNP 32 **Scenario 4:** FRGB 27 **Scenario 6:** FROC 19 **Scenario 7:** FROR 16 **Scenario 8:** FRIS 31 **Scenario 9:** FRLB 26	-	Provision functionally similar to FE01.
85.	FE03	-	-	Functional and Performance Requirements are related to scenarios and do not contain detailed requirements related to securing data against manipulation.

Annex F
(informative)

Preliminary questionnaire template

Trial ID	
DTI company name	
Date	

1.	**General expected outcome**	
1	Capability to assess and prioritize UAS threats by implementing an algorithm or decision-making framework based on predefined criteria, such as level of risk, dimensions, etc.	YES or NO
2	Authorization by legal EU authorities to detect and mitigate drones in EU airspace	YES or NO
3	Threat assessment, considering drone size, speed and potential payload.	YES or NO
4	DTI of unmanned aerial vehicles that enter a well-defined hemispherical airspace (azimuth 360° and elevation 180°)	YES or NO
2	**Technical expectation**	YES or NO
1	Operation time - system needs to have minimal downtime and high availability, in order to ensure 24/7 operation of all detection and/or countermeasures equipment	YES or NO
2	Weather conditions - ensure the operation in the outdoor environment and in any weather conditions.	YES or NO
3	UAS class - detect, track, and identify, UASs which are included in Class I (<150Kg) according to NATO classification	YES or NO
4	UAS shape - detect, track and identify, UASs, regardless of their shape and colour.	YES or NO
5	UAS type - system shall detect UASs, regardless of their type: rotary wing, fix wing, hybrid/VTOL.	YES or NO
6	Target flight mode - detect, track and identify UAS, regardless the flight navigation mode: manual navigation, GPS navigation	YES or NO
7	Target flight mode - detect, track and identify UAS which is flying autonomously.	YES or NO
8	Target flight path - detect, track and identify targets regardless of the flight path	YES or NO

9	GPS denied environment - be effective against drones that can operate in GPS-denied environment	YES or NO
10	UAS RF link - be effective against drones that operate without an active RF link.	YES or NO
11	Multiple targets - detect, track and identify multiple targets at the same time.	YES or NO
12	UAS information - provide at least some of the following information related to detected UAS: type and serial number, position/coordinates, the route, ground speed, communication protocol, pilot/control station location	YES or NO for: Type - Serial number - UAS Location - UAS route - Speed - Com. Protocol - Pilot location -
13	Data fusion approach - automatically detect, track and identify UASs, using sensors/technologies capabilities, independently or through data fusion mechanisms.	YES or NO
14	Operation - ensure the manual, grouped and independent operation (at the decision of the operator/user), of the capabilities of all C-UAS subsystems.	YES or NO
15	User interface - provide clear visualizations, alerts, and controls to facilitate efficient decision-making and response.	YES or NO
16	Access and configuration - allow access and configuration of all settings and options of subsystems in the composition, through graphical user interface.	YES or NO
17	Auxiliary sensors - allow the installation of auxiliary sensors, to increase performance and/or adapt to the operational operating environment	YES or NO
18	Interconnectivity - allow interconnection with legacy systems/subsystems installed in other locations, including command and control, air traffic control, radar and perimeter security systems, to achieve a common operational picture	YES or NO
19	Adaptability - adapt to changing UAS threats (new models, new protocols or new specific parameters) and operating conditions	YES or NO
20	Geo-fence configuration - offer the possibility of configuring geo-fence zones to establish detection (alarm) and countermeasure (interdiction) zones	YES or NO
21	Alarm functions - provided with alarm functions through which the operator/user is warned, visually and audio, regarding the detection of UAS and their access to the geo-fence areas.	YES or NO
22	Friend or foe - be equipped with detection capabilities and exclusion from the alarm procedure of friendly unmanned aircraft	YES or NO

23	Malfunctions identification - be provided with capabilities to identify malfunctions and alert the operator about them.	YES or NO
24	Alarms due disconnections - identify and alert the operator if any sensor is disconnected	YES or NO
25	Alarm sharing - provided with the ability to share alerts via instant messaging such as MS Teams or WHATSAPP or email to a predefined list of phone numbers or email addresses	YES or NO
26	Access for diagnostic - allow local access to C-UAS sensor diagnostics and control applications.	YES or NO
27	Access roles - ensure the possibility of assigning the following attributes/roles for users: global administrator, local administrator, read only, etc.	YES or NO
	Reports - ensure the possibility of creating and exporting a report that shows the recordings made by the sensors and the actions taken by the operator/user of the C-UAS software.	YES or NO
28	Data saving - ensure the permanent saving automatically as well as manually in a time interval predefined by the user, for at least the following information (logs, geographic coordinates, details about the identified UAS, sensor, etc..)	YES or NO
29	Data sharing for coordinated response – possibility for information from UAS system to be shared across incident management or workflow management tool	YES or NO
30	Installation - Installation and uninstallation of detection and/or countermeasures equipment, should be done easily	YES or NO
31	Scalability by design - be flexible and scalable by design, in order to address a specific location and environment conditions, without affecting the DTI performances	YES or NO
32	Redundancy - have built-in redundancy to ensure continuous operation of the main subsystems even if some of its components fail.	YES or NO
33	Connection elements - The fixed type CUAS systems shall be provided with all the connection elements necessary for the installation and safety in operation	YES or NO
34	IP67 certification - Permanent installations shall be certified for use in the outdoor environment, according to the characteristics of protection class IP67.	YES or NO
35	Internet - allow operation without an Internet connection, using the connection in a dedicated local network	YES or NO
36	Privacy by design - be conceptually designed, with software mechanisms to ensure data protection	YES or NO

37	Secure Communication and Information Sharing - facilitate secure communication and information sharing (encryption, secure protocols, etc.)	YES or NO
38	GDPR compliance - be compliant with EU GDPR regulation regarding all digital data	YES or NO
39	Conformity with the applicable regulations regarding the regime of products and services that can endanger life, health, security and the environment	YES or NO
40	Marking and identification - Each component of the system shall be marked clearly and visibly. The labels shall contain all the mandatory information provided by international regulations.	YES or NO
41	Product quality - The equipment shall be new, fully equipped and ready for immediate use	YES or NO
42	Software licensing - If the software solution consists of a desktop application, the application installation kit should be transferred to the beneficiary at no additional cost.	YES or NO

Annex G
(informative)

C-UAS system evaluation framework template

G.1   Evaluation methodology contents

1	**Purpose of the evaluation** Key Stakeholders Purpose and Focus Stakeholder Needs
2	**Background and context** Considerations Evaluation Context Goal & Objectives Participatory Approach
3	**The Evaluation Plans** Approach to Evaluation The Evaluation Plan
4	**Evaluation Questions** Considerations Finalized Questions
5	**Data Collection** Data Collection Plan Questionnaires based data Field test-based data Managing Potential Ethical Issues
6	**Data Management** Data Management Plan
7	**Data Synthesis, Judgments, and Conclusions** Approach to Data Synthesis Forming Judgments Reaching Conclusions Feedback and follow-up
8	**Reporting and Dissemination plan**

G.2 Purpose of the evaluation

G.2.1 Key Stakeholders

Please identify the key stakeholders and fill in the table below:

Table G.1 — Stakeholder mapping matrix

Stakeholder	Focus and scope	Key role in the evaluation action	Key role in the plan drafting	Key role in evaluation tests/questionnaires	Key role in evaluation judgements, conclusions	Key role in evaluation reporting and dissemination
A						
B						
....						

Note: examples of key stakeholders:
1. Government Agencies;
2. C-UAS Manufacturers and Developers;
3. Independent Evaluators and Experts;
4. End-Users (e.g., Security Agencies, Military, Critical Infrastructure Operators);
5. Regulatory Bodies and Compliance Organizations;
6. Academic and Research Institutions;
7. Public and Community Representatives;
8. Commercial and Private Operators;
9. Law Enforcement Agencies;
10. Local and National Governments;
11. Privacy Advocacy Groups;

G.2.2 Purpose and Focus

Here must be included brief statement, regarding the evaluation scope. Why is needed? It has to describe why the evaluation is needed (i.e., market consultation, public tender, qualification, marketing activity, research, TRL demonstration, etc.). A shared understanding of what the evaluation can and cannot deliver is essential to the success of implementation of evaluation activities and the use of evaluation results. The stakeholders must agree upon the logic model and the purpose(s) of the evaluation. Understanding the purpose of the evaluation and the rationale for prioritization of evaluation questions and activities is critical for transparency and acceptance of evaluation findings. It is essential that the evaluation address those items of greatest interest and the priority for the users of the evaluation.

G.2.3 Stakeholder Needs

Here must be included a short description of stakeholder needs, as general statements for definition of the evaluation context idea. Which are the general needs? It has to define for what the evaluation is done (i.e., a border authority which was previously defined as a stakeholder has to evaluate a C-UAS solution needed for the protection of a seashore, against the use of drones for smuggling). Also, this clause will describe the stakeholders' needs during the entire evaluation cycle, from drafting the evaluation framework, to managing findings and reporting.

G.3 Background and context

G.3.1 Considerations

A description of the general problem which must be solved. The stakeholders must agree from the beginning about the nature of the problem or goal, who is generally affected, how big is the problem and whether and how is changing. For instance, if a Law Enforcement Agency, specialized in the protection of high rank dignitaries, has the intention to implement a C-UAS solution in its daily operations, here must be mentioned some general consideration regarding the nature of the problem. The information is needed for the other stakeholders involved in the evaluation to fully understand the problem which must be solved. Relevant drone incidents and gap analysis could be included as explanatory notes.

G.3.2 Evaluation Context

This clause must contain introductory explanations about the evaluation context. They describe what the evaluation has to accomplish to be considered successful. For most programs, the accomplishments exist on a continuum (first, the aim is to accomplish X... then, to do Y...). Therefore, they should be organized by time ranging from specific (and immediate) to broad (and longer-term) consequences. The description of the evaluation's context also considers the important features of the environment in which operates. This includes understanding the activity field, geography, social and economic conditions, and also what other organizations have done. A realistic and responsive evaluation is sensitive to a broad range of potential influences. An understanding of the context lets users interpret findings accurately and assesses their generalizability. For example, a UAS system to detect, track and identify the UASs near a government building in an inner-city neighbourhood might have been a tremendous success for a LEA, but would likely not work in open space environment, without significant changes. Relevant concept of operation must be mentioned here.

G.3.3 Goal & Objectives

Developing clear goals and objectives will help you to clarify problems, issues and opportunities. Please fill in the table below with the goals of the test: (*examples*)

#	Goals	Notes
G1	*Protect the life and health of persons carrying out activities in a critical infrastructure, against malicious use of UAS.*	
G2	*Provide adequate warning in case of malicious use of UAS against the protected area.*	
G3	*Provide adequate response and mitigation actions against the UAS attacks.*	
G4	*Maintain the essential services provided by the critical infrastructure.*	
G5	*Enhance the community security.*	
G6	*Raise the citizens awareness.*	
….		

Objectives define strategies or implementation steps to attain the identified goals. Unlike goals, objectives are specific, measurable, and have a defined completion date. They are more specific and outline the "who, what, when, where, and how" of reaching the goals. Please fill in the table below with the objectives of the test: (*examples*)

#	Objectives	Observations
O1	*Installation of a system for detecting, identifying and neutralizing the UAS threat in an urban environment, for the protection of the Ministry of Foreign Affairs building.*	
O2	*The C-UAS system components will be installed on the infrastructure related to the protected objective, without other major additional construction works.*	
O3	*The C-UAS system detects and identifies all rotary UAS flights in the surrounding area of the building, from a specific distance.*	
O4	*The C-UAS system automatically alerts the security personnel for all detected UAS, within an appropriate time frame.*	
O5	*The C-UAS system automatically provides adequate neutralization measures.*	
….		

G.3.4   Participatory Approach

The evaluation framework must be developed through a participatory approach, for all the involved stakeholders, since it demonstrates how evaluation activities will lead to producing evidence on the outcomes. Evaluation cannot be done in isolation. Almost everything involves partnerships - alliances among different organizations, board members, those affected by the problem, and others. Therefore, any serious effort to evaluate C-UAS systems must consider the different values held by all partners.
Please fill in a description of the stakeholder's involvement in the development of the test methodology, their general contribution, their specific requirements and their expected results.

G.4   The evaluation plans

G.4.1   Approach to Evaluation

Please fill in the table below:

Table G.2 — Participatory planning matrix

Evaluation scope:	*As defined above*					
Evaluation planning timeframe:	*The stakeholders will agree on the time period allocated for the entire evaluation, including the evaluation plan preparation, answers to the questionnaires and the field demonstrations.*					
Field test demonstration date:	*The stakeholders will agree on the field test date.*					
Alternative field test demonstration date:	*The stakeholders will propose also an alternative field test demonstration date.*					
Field test demonstration location:	*The stakeholders will agree on the location for field tests*					
Dissemination level	☐ **PU: Public** ☒ **CO: Confidential for the involved stakeholders** ☐ **RE: RESTREINT UE (Commission Decision 2015/444/EC)** *The stakeholders will agree on the dissemination level of the activities and outcomes (i.e. commercially confidential issues may arise)*					
Status	☒ **Draft** ☐ **Reviewed** ☐ **Finally reviewed** ☐ **Accepted**					
Stakeholder	**Organization type**	**Role in the evaluation**	**Contact details**	**General activities**	**Allocated resources**	**Associated documents**
A						
B						
……..						

General activities *will describe the committed activities for each involved stakeholder. For instance, a LEA will specify the needs, explain the context, will prepare the questionnaire, will make available the test infrastructure, will participate in data collection and at the end will make data synthesis, judgments and formulate conclusions.*

Allocated resources *– each involved stakeholder will mention the committed resources allocated for the evaluation. For instance, a C-UAS developer will mention here what products from his portfolio it will allocate, for how long and in which circumstances, how many technicians will be involved, what costs will be covered for the evaluation, etc.*

Associated documents *– here it is useful to include relevant documents as a proof for the committed activities and resources (i.e. management declarations, support letters, availability statements, etc.).*

G.4.2   The evaluation plans

This section can be multiplied for each individual test or scenario.

Inputs: *all information needed from all stakeholders in the evaluation context. They can be considered as deliverables in a project management approach.*

1. *User concept of operation (type of mission, threats, location, environment conditions, etc.)*
2. *User requirements (operational, legal, etc.)*
3. *Expected KPIs and acceptance criteria*
4. *Technical specification of the C-UAS system (detailed information for the technical components)*

Activities: *the description of all evaluation activities. The activities description and the responsibilities are mandatory for each item. Also, a Gantt chart is recommended.*

1. *Definition of the evaluation questions*
2. *Analysis of the answers to evaluation questions*
3. *Definition of the field test activities (test scenarios)*
4. *Definition of the measurements and data recording*
5. *Evaluation test execution*
6. *Data collection and management*
7. *Data synthesis, Judgments, and Conclusions*
8. *Reporting and dissemination*
9. *Evaluation management and logistics*

Outputs:

1. *Resulted input deliverables (user requirements, KPIs and acceptance criteria, etc.)*
2. *Activities deliverables (evaluation questions and answers, test scenarios, collected data, synthesis and conclusions)*

Outcomes:

1. *User satisfaction/rejection*
2. *Procurement preparation*

Note*: TEST ENVIRONMENT description should cover at least:

- **Coverage areas:**

Monitoring area: Map of the monitoring area, Horizontal and vertical coverage;
Interdiction area: Map of the interdiction area, Horizontal and vertical coverage;

- **Environmental conditions:**

Scenario number, Location name, GNSS coordinates of sensors, Describing the weather (e.g., sunny, rainy, foggy, clear or cloudy), Describing the ground (e.g., dry, wet, snow covered), Average air temperature, Average wind speeds, Average wind direction, Air humidity, Noise level, Description of the surrounding obstacles and height profile of the test area (e.g., buildings, other antennas, cars, fences, powerlines, metallic reflectors), Pictures from each cardinal point;

- **C-UAS system configuration:**

System hardware configuration: System type, Hardware version, Sensors type;

System software configuration: Software version, Firmware version;

- **UAS configuration:**

Drone class, type and version, Drone firmware, Available telemetry data, Drone downlink/uplink output power, Drone downlink/uplink bandwidth, Drone downlink /uplink frequency, Remote controller type and version, Remote controller firmware, Remote controller output power, Remote controller transmitter bandwidth, Used frequency band, Average speed of the drone, GNSS position of the pilot;

- **Flight scenario:**

Time interval for test execution, Sequences description, Flight height, Direction of flight, Flight profile, Speed.

- **Time plan:**

Activity	Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

G.5   Test results

The tests must be planned to offer the opportunity for assessing each requirement, in the right way, with the right means and in the best conditions.

Req. Nº	
Req. Name	
Description	
Importance	
Parameters and performance limits	
How to quantify the fulfilment	

The collected data must be reviewed for accuracy and completeness. Any data anomalies or inconsistencies should be resolved before proceeding with the analysis. Aggregation data must be properly organized and stored securely to prevent unauthorized access.

G.5.1 Data analysis

The data analysis process involves the use of metrics and benchmarks.
Some of the most important performance metrics are: Detection Rate, False Alarm Rate, Tracking Accuracy, Response Time and Interference with Other Systems.
The benchmarks will include: Historical Data, Industry Standards, Operational Requirements, Competitor Analysis, User Feedback and Surveys.
By applying the defined performance metrics and benchmarks to the collected data, the results will derive into meaningful insights and conclusions about the DTI system's performance.

G.5.2 Data interpretation

Uncovering facts about a system's performance is not enough to make conclusions. The facts must be interpreted to understand their practical significance.

Evaluation Question	Indicator/ Performance Measure	Method	Data Source	Frequency	Responsibility

G.5.3 Reaching Conclusions

Evaluation questions criteria	Data Synthesis	Evaluative Judgments	Evaluative Conclusions
Appropriateness			
Effectiveness			
Efficiency			
Impact			
Sustainability			

Recommendations are actions to consider as a result of the evaluation. Forming recommendations requires information beyond just what is necessary to form judgments. If recommendations are not supported by enough evidence, or if they are not in keeping with stakeholders' values, they can really undermine an evaluation's credibility. By contrast, an evaluation can be strengthened by recommendations that anticipate and react to what users will want to know.

G.5.4 Reporting and dissemination

Regardless of how communications are constructed, the goal for dissemination is to achieve full disclosure and impartial reporting.
The evaluation findings must be clearly included in reports, which will be disseminated later to the interested stakeholders.
The Executive Summary, Detailed Analysis, Benchmark Comparison, User Feedback, Anomalies and Challenges, Recommendations, Lessons Learned should be part of the Evaluation Results Reporting.

Report Type	Due Date	Audience & their Interests	Overall Focus	Contents	Dissemination
Formal Reports					
Ad Hoc and Event Reports					

Annex H
(informative)

Data log format for DTI systems

H.1 Data log format for DTI systems

From the lessons learned in the first trial in Greece, a structured format has been chosen as opposed to e.g., a table, as data scopes can vary. For instance, the version of the format is global to the document, whereas the elevation of a point is specific to a single data point. Using a structured format also allows easily extending it without breaking backwards compatibility. JSON has been chosen due to its simplicity and number of libraries available for writing and parsing data.

The format is specified in a JSON Schema. A visualization of the format is available on this page, and the schema can be found at https://grvc.us.es/courageous/ and is listed in this Annex below. JSON Schema validators can be found online, such as this one.

Figure H.1 — JSON format

Bibliography

[1]   ISO/IEC/IEEE 29148, Systems and software engineering — Life cycle processes — Requirements engineering

[2]   ISO 20473:2007, Optics and photonics — Spectral bands

[3]   M. Życzkowski, M. Szustakowski, W. Ciurapiński, M. Karol, P. Markowski, "Integrated radar-camera security system – range test"

[4]   Jian Wang, Yongxin Liu, and Houbing Song, Senior Member, "Counter-Unmanned Aircraft System(s) (C-UAS):State of the Art, Challenges and Future Trends"

[5]   Busset, Jo, Perrodin, Florian, Wellig, Peter, Ott, Beat, Heutschi, Kurt, et al. 2015 "Detection and tracking of drones using advanced acoustic cameras"

[6]   MBOS acoustic drone detection system developed at the Fraunhofer Institute, https://www.fkie.fraunhofer.de/en/departments/kom/ambos.html#1514342531

[7]   K. Kamiński& E. Majda, "Automatic speaker recognition system based on Cepstral speech signal analysis and Gaussian mixture models", PhD thesis, WAT

[8]   E. Majda, "Automatic system of reliable speaker recognition based on Cepstral analysis of the speech signal", PhD thesis, WAT

[9]   EASA, Drone Incident Management at Aerodromes

[10]   Center for Security Studies (2018), Manual – Trainings for the protection of Critical

[11]   Infrastructures http://www.ciprotection.gr/index.php/el/

[12]   Wallace, Ryan & Loffi, Jon. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis. International Journal of Aviation, Aeronautics, and Aerospace. Volume 2. 10.15394/ijaaa.2015.1084.

[13]   Soloman, E.D. (2014). Part two: Unmanned aircraft systems ("UAS") – aka drones legal issues: Where   are   we   headed.   Blank   &   Rome.   Retrieved   from http://www.blankrome.com/index.cfm?contentID=37&itemID=3338

[14]   https://www.easa.europa.eu/en/domains/civil-drones-rpas/specific-category-civil-drones/specific-operations-risk-assessment-sora#Risk%20assessment%20of%20the%20intended%20operation%20%E2%80%93%20SORA

[15]   https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/concept-development/operational-requirements

[16]   Kar, Pradip and Bailey, Michelle. Characteristics of Good Requirements. International Council of Systems Engineers, Requirements Working Group. INCOSE Symposium, 1996

[17]   https://griffin-erc-advanced-grant.eu/

[18]   System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment, Choon Seng Tan, Douglas L. Van Bossuyt, Britta Hale, November 2021

[19]   https://www.cpni.gov.uk/critical-national-infrastructure-0