Article

Not peer-reviewed version

Standardized Evaluation of Counter-drone Systems: Methods, Technologies, and Performance Metrics

Geert De Cubber * , Daniela Doroftei , Paraskevi Petsioti , Alexios Koniaris , Konrad Brewczyński , Marek Życzkowski , Razvan Roman , Silviu Sima , Ali Mohamoud , Johan van de Pol , Ivan Maza , Anibal Ollero , Christopher Church , Cristina Popa

Posted Date: 26 March 2025

doi: 10.20944/preprints202503.2043.v1

Keywords: counter-drone; standardization; quantitative evaluation; standard test methods; counter-UAS; performance evaluation

Article

Standardized Evaluation of Counter-Drone Systems: Methods, Technologies, and Performance Metrics

Geert De Cubber [1,†,‡,*], Daniela Doroftei [2,‡], Paraskevi Petsioti [3,‡], Alexios Koniaris [4,‡], Konrad Brewczyński [5,‡], Marek Życzkowski [6,‡], Razvan Roman [7,‡], Silviu Sima [8,‡], Ali Mohamoud [9,‡], Johan van de Pol [10,‡], Ivan Maza [11,‡], Anibal Ollero [12,‡], Christopher Church [13,‡] and Cristina Popa [14,‡]

[1] Royal Military Academy
[2] Royal Military Academy
[3] Center for Security Studies (KEMEA)
[4] Center for Security Studies (KEMEA)
[5] Military University of Technologyl
[6] Military University of Technology
[7] Serviciul de Protectie si Paza
[8] Serviciul de Protectie si Paza
[9] Nederlandse organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)
[10] Nederlandse organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)
[11] GRVC Robotics Lab, University of Seville
[12] GRVC Robotics Lab, University of Seville
[13] INTERPOLt
[14] Asociatia de Standardizare din Romania
* Correspondence: geert.de.cubber@mil.be; Tel.: +32-244-14008
† Current address: Av. De La Renaissance 30, 1000 Brussels, Belgium.
‡ These authors contributed equally to this work.

Abstract: This paper aims to introduce a standardized test methodology for drone detection, tracking and identification systems. It is the aim that this standardized test methodology for assessing the performance of counter-drone systems will lead to a much better understanding of the capabilities of these solutions. This is urgently needed, as there is an increase in drone threats and there are no cohesive policies to evaluate the performance of these systems and hence mitigate and manage the threat. The presented methodology has been developed within the framework of the project COURAGEOUS funded by European Union's Internal Security Fund Police. 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. However, the proposed standard methodology provides an open architecture where the standard scenarios can modularly be extended, providing the standard users the possibility to easily add new scenarios. For each of these scenarios, operational needs and 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-drone systems. The standard test methodology concentrates on the qualitative and quantitative evaluation of counter-drone systems. This test methodology was validated during three user-scripted validation trials.

Keywords: counter-drone; standardization; quantitative evaluation; standard test methods; counter-UAS; performance evaluation.)

1. Introduction

The increasing proliferation of unmanned aerial systems (UAS), ranging from small consumer drones to larger tactical platforms, has led to a surge in both legitimate and malicious applications. While drones offer substantial benefits across various sectors, including agriculture, logistics, security,

 doi:10.20944/preprints202503.2043.v1

and emergency response, their misuse by criminal and terrorist actors presents significant security concerns. Reports of drones being used for smuggling contraband, conducting unauthorized surveillance, interfering with critical infrastructure, and executing targeted attacks have underscored the urgency of developing effective countermeasures [1–4]. Law enforcement agencies and security forces face the challenge of detecting, tracking, identifying, and mitigating these threats in a rapidly evolving technological landscape.

Despite the availability of numerous counter-drone solutions on the market [5–8], no widely accepted standardized methods exist for assessing their performance. This lack of standardization complicates the efforts of acquisition agencies, law enforcement entities, and other stakeholders tasked with selecting and deploying appropriate counter-drone technologies. Without objective, comparable data, end-users struggle to match specific operational requirements with the capabilities of available counter-drone systems. As a result, the selection and procurement process remains fragmented, often leading to suboptimal solutions that may fail to address real-world threats effectively.

To bridge this gap, the COURAGEOUS project [9] has developed a pre-standard document in the form of a CENELEC Workshop Agreement (CWA). This document, designated CWA 18150 [10], outlines a standardized test methodology for assessing the performance of counter-drone systems under controlled and relevant operational conditions. The methodology defines a set of evaluation scenarios designed to replicate real-world operational challenges, allowing for fair qualitative and quantitative comparisons of different counter-drone solutions. By adopting this standardized framework, security agencies, procurement bodies, and industry stakeholders can better understand system capabilities and limitations, ultimately improving the selection and deployment of counter-drone technologies.

The purpose of this paper is to provide a structured overview of the CWA 18150 document, serving as both an abstract and an introduction to the standardized test methodology it defines. This paper details the key aspects of performance assessment, including risk analysis, test environments, operational requirements, and evaluation metrics. It aims to offer a comprehensive understanding of the framework developed under the COURAGEOUS project and to facilitate its broader adoption within the security and defense communities. The full CWA document, which contains detailed methodology and implementation guidelines, can be accessed at https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf.

2. Related Work

2.1. Counter-Drone

Technical development of new counter-drone solutions is a common subject of research in the counter-drone area. The projects H2020-ALFA [11], H2020-ALADDIN [12], and H2020-SafeShore [13] are noteworthy examples, as they all created drone detection systems for particular use cases. The creation of an effective drone detecting system is generally fraught with two major challenges. First, regardless of the sensor technology employed, drone platforms typically have a very small cross section and detection baseline [14]. In fact, drones employ common radio transmission frequencies, have a small sound signature (from a relevant distance), a small visual/infrared signature, a small RADAR cross section, etc. Furthermore, it is challenging to eliminate false positives because the signatures of many drones and birds are fairly similar [15,16].

RADAR [17], acoustics [18], visual [19], infrared [20] (thermal and short-wave), radio spectrum sensing [21], LIDAR [22], and other sensing modalities can be employed to tackle the drone detection problem. Nevertheless, due to the difficulty of solving the problem under real-world operating conditions, the majority of current solutions rely on a combination of various sensing techniques to solve the drone detection problem [14] and combine conventional detection and tracking techniques [23,24] that come from computer vision to accomplish multi-sensor tracking.

The incorporation of counter-drone solutions and practices into standard operating procedures for law enforcement agencies is also a crucial factor to take into account. The projects SkyFall [25] and DroneWise [26] are pertinent in this context; they examine various counter-drone systems, integrate

 doi:10.20944/preprints202503.2043.v1

the best available systems in a law enforcement organization training, and provide a number of useful end-user-focused measures to enhance the response to UAS terrorist attacks.

2.2. Standard Testing for Counter-Drone Solutions

In terms of standard test methodology development for counter-drone solutions, there have been multiple developments in the past. To state the main problem: two opposing needs can be found in regard to the creation of standardized test techniques for assessing drone detection systems' performance [14]. In order to identify the limitations of the system being tested, it is necessary to carefully regulate the test settings because drone detection systems typically rely on intricate data fusion and processing of sensor data. This first need calls for repeatable test in controlled environments. However, since drone detection systems must function around-the-clock and in all weather situations, it is necessary to evaluate how well they operate in a variety of environmental settings. This second need calls for the evaluation of the systems in a non-controlled operational environment. Since these constraints conflict with one another, a standardized test methodology must carefully balance these two categories of needs. Therefore, the goal is to identify a validation approach that meets the needs of the platform developers for a quantitative statistically meaningful validation as well as the end users' requirement for a qualitative operational validation of the system [14].

In the realm of robotics, for example, the National Institute of Standards and Technology (NIST) in the United States has previously recommended such qualitative and quantitative validation approaches [27]. Based on the work done at NIST, a first qualitative and quantitative validation methodology was presented in [28] and validated in [29]. This methodology was applied for a first time in the framework of standardised counter-drone testing in the year 20217 and 2018 [30] in the framework of the SafeShore project [13]. In that period, the National Nuclear Security Administration of the United States Department of Energy also conducted research in the United States to build a counter-drone testing and evaluation methodology [31]. Although it never actually became a standard, the test approach outlined defines test techniques, performance measurements, UAS types tested, critical variables, and the required data analysis to reliably assess the capabilities of counter-drone technology.

The absence of a standard test method started becoming problematic from around the year 2020, when multiple counter-drone solutions became available on the market, and the performance capabilities of these systems became harder and harder to differentiate for end users. Law enforcement agencies and other government actors conducted various counter-drone equipment tests in critical infrastructure protection scenarios [32], but the problem is that these trials are highly costly for all actors involved and results are not easily transferable to other environments.

This challenge has led to multiple standardization efforts across international organizations. EUROCAE WG-115 [33] has been actively developing standards such as ED-286, which provides an Operational Services and Environment Definition (OSED) for counter-drone operations in controlled airspace, and ED-322, which sets System Performance and Interoperability Requirements for Non-Cooperative UAS Detection Systems. These efforts focus specifically on airport environments and happen in close coordination between Europe (EUROCAE) and the United States, where the Federal Aviation Administration (FAA) has initiated Special Committee SC-238 to establish comprehensive evaluation guidelines for counter-drone technologies. By working together, EUROCAE WG-115 and FAA SC-238 aim to ensure the safe integration of counter-drone systems within existing aviation structures while maintaining effective detection and mitigation capabilities.

NATO is another key player in establishing counter-drone test procedures. i) establishing a counter-drone community; ii) policy, concepts, doctrine, tactics, techniques, and procedures; iii) standardization; and iv) research, development, and operation activities are among the topics being worked on by the NATO counter-drone Working Group. The annual TIE exercises, which are designed to promote interoperability among various counter-drone assets, are a significant example [34].

In Germany, DIN is working on DIN 5452-9 [35], which focuses on drone detection, as well as an attachment that defines conformance test procedures. These efforts aim to create a robust testing framework that allows for systematic evaluation of counter-drone effectiveness. Similarly, the UK's

 doi:10.20944/preprints202503.2043.v1

National Protective Security Authority (NPSA) is developing a "counter-drone Testing and Evaluation Standard," which aims to provide a structured methodology for performance assessment.

The International Standardization Organisation ISO is also contributing to the standardization landscape with ISO/CD 16746 [36], which provides guidance to end-users on the deployment of counter-drone equipment, and ISO/CD 16747 [37], which supports manufacturers in producing effective and compliant counter-drone solutions. These standards seek to harmonize best practices and technical specifications, ensuring consistency and interoperability across different jurisdictions.

These initiatives demonstrate the global recognition of the need for standardized test methodologies. However, disparities in national regulations and differing operational requirements present ongoing challenges. The CWA 18150 developed under the COURAGEOUS project aims to maximize the usage of work being done in many countries and complements these efforts by providing a structured approach to performance evaluation while ensuring compatibility with emerging international standards. By aligning with these ongoing standardization initiatives, CWA 18150 seeks to provide acquisition agencies and security stakeholders with a reliable framework for assessing and comparing counter-drone technologies in a transparent and repeatable manner.

2.3. Organization of this Paper

The remains of this paper is organized as follows: In order to provide a clear grasp of the problem, section 3 provides an analysis of incidents related to UAS and an analysis of identified gaps in counter-drone capabilities. To further analyse the current playing field, section 4 investigates the current technologies and methods used for counter-drone operations. Based on the ground work in the previous sections, section 5 proposes 10 standard counter-drone scenarios. These standard scenarios will serve as a guideline throughout the whole standardization process. For each of the standard scenarios, a risk analysis is performed, as explained in section 6. In a parallel line of work and through discussions with end-users of counter-drone solutions, a set of *operational needs for counter-drone coverage* were devised in section 7, together with a series of *counter-drone system performance requirements and metrics*. Based on all this input, a counter-drone System Evaluation Method was developed in section 8. This methodology was validated during three large-scale trials in Greece, Belgium and Spain, as discussed in section 9. Section 10 concludes this paper by investigating and discussing the results obtained and by identifying remaining gaps and directions for future research.

3. Incidents Analysis and Identification of Gaps

3.1. Incident and Threat Analysis

The increasing proliferation of drones has led to a rise in security concerns globally. Unauthorized drone activities have been reported in various environments, ranging from airports to government facilities, often leading to operational disruptions or security breaches. In order to obtain a good overview of the problem, a systematic review of more than 200 drone-related incidents in the European territory was performed, analyzing recent drone incidents, categorizing threat actors, and highlighting the gaps in counter-drone measures:

- **Targeted Locations:** Airports, government buildings, military installations, and critical infrastructure remain prime targets for unauthorized drone activities.
- **Incident Types:** The most common incidents include unauthorized surveillance, smuggling, near-miss collisions with manned aircraft, and weaponized drone deployments.
- **Operational Environments:** Dense urban areas present unique challenges due to radio frequency (RF) congestion and limited line-of-sight detection capabilities.
- **Technological Capabilities:** Advances in commercial drone technology, including autonomous navigation and payload adaptability, have outpaced current counter-drone countermeasures.

Analysis of drone-related incidents reveals that the majority of cases involve uninhibited operators, followed by criminal activities. Figure 1 categorizes these threat actors into six main groups:

 doi:10.20944/preprints202503.2043.v1

- **Uninhibited** (55%): Operators who frequently violate regulations but do not necessarily have malicious intent.
- **Criminal** (25%): Drones used for illicit activities such as smuggling contraband.
- **Terrorist** (10%): Drones employed in attacks or reconnaissance by hostile entities.
- **Careless** (7%): Operators who occasionally breach airspace restrictions unintentionally.
- **Clueless** (2%): Operators unaware of regulations, often leading to airspace violations.
- **Compliant** (0.3%): Law-abiding drone users who adhere to regulations.

The data indicates that while regulatory violations are common, a significant number of incidents involve intentional misuse of drones for criminal or terrorist purposes.

Drone-related incidents have been observed across various sectors. Figure 2 provides an overview of the distribution of incidents across different environments:

- **Private/Non-Corporate** (24%): Drones flown over residential areas, often leading to privacy violations.
- **Airports** (24%): Incidents causing flight delays and safety concerns.
- **Government/Military** (16%): Unauthorized surveillance or potential attacks.
- **Law Enforcement/First Responders** (13%): Interference with emergency operations.
- **Prisons** (10%): Drones used for smuggling contraband.
- **Stadiums** (6%): Uncontrolled drone operations during events.

The high occurrence of incidents in airports and private properties suggests an urgent need for robust counter-drone strategies.

3.2. Gaps Analysis for Counter-Drone Measures

Despite advancements in drone detection and mitigation, several gaps remain unaddressed.

Legislation governing counter-drone operations varies significantly across jurisdictions, creating ambiguity regarding permissible countermeasures. Additionally, free-access areas, such as public spaces and private properties, pose enforcement difficulties due to privacy and regulatory limitations. Furthermore, there is no unified response framework for handling drone incursions.

Despite the availability of various DTI technologies, only 5% of reported incidents indicate the presence of an operational detection system. Furthermore, these systems exhibit reduced efficacy in RF-dense environments, adverse weather conditions, and scenarios involving multiple airborne objects.

While off-the-shelf drones account for the majority of incidents, the increasing prevalence of modified and custom-built UAVs presents a growing concern. Such drones often utilize non-standard communication protocols, rendering conventional RF-based detection methods less effective.

A significant proportion of incidents involve drones carrying undefined payloads, raising uncertainties regarding their intent and threat level. Distinguishing between benign and hostile drones remains a major challenge, especially in areas where multiple UAS operate simultaneously.

A unified incident reporting mechanism is lacking across member states, hindering data-driven policy formulation and response coordination. The absence of structured information-sharing frameworks limits the development of proactive countermeasures.

4. Review of current counter-drone frameworks

The field of counter-drone has seen significant advancements, driven by the increasing use of drones for both commercial and military applications. This section provides an overview of the existing detection, tracking, and identification (DTI) technologies and their combinations in counter-drone solutions.

4.1. Technologies for Detect, Track, and Identify (DTI) in Counter-Drone Solutions

For this study on counter-drone technologies, information on 260 anti-drone systems was initially collected. This initial dataset was downscaled to 144 systems based on the level of detail and the

 doi:10.20944/preprints202503.2043.v1

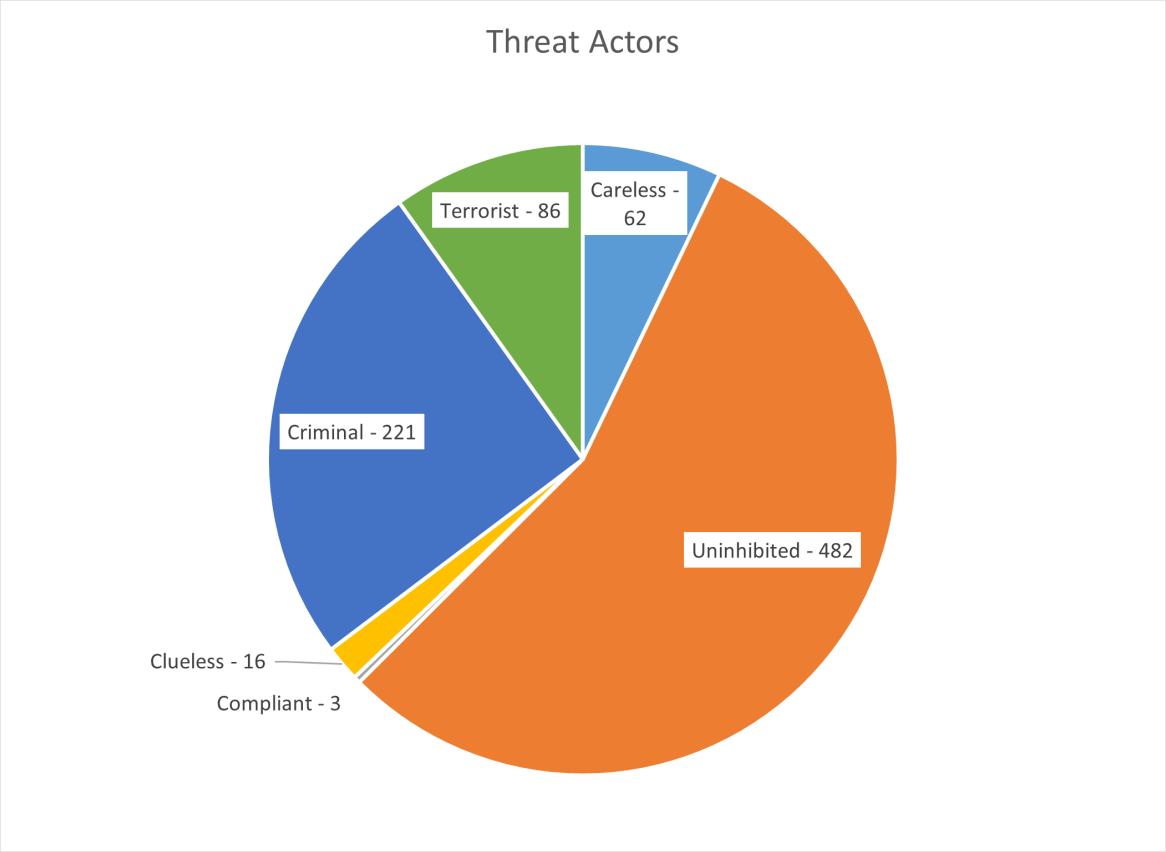

Figure 1. Categorization of threat actors in drone incidents.

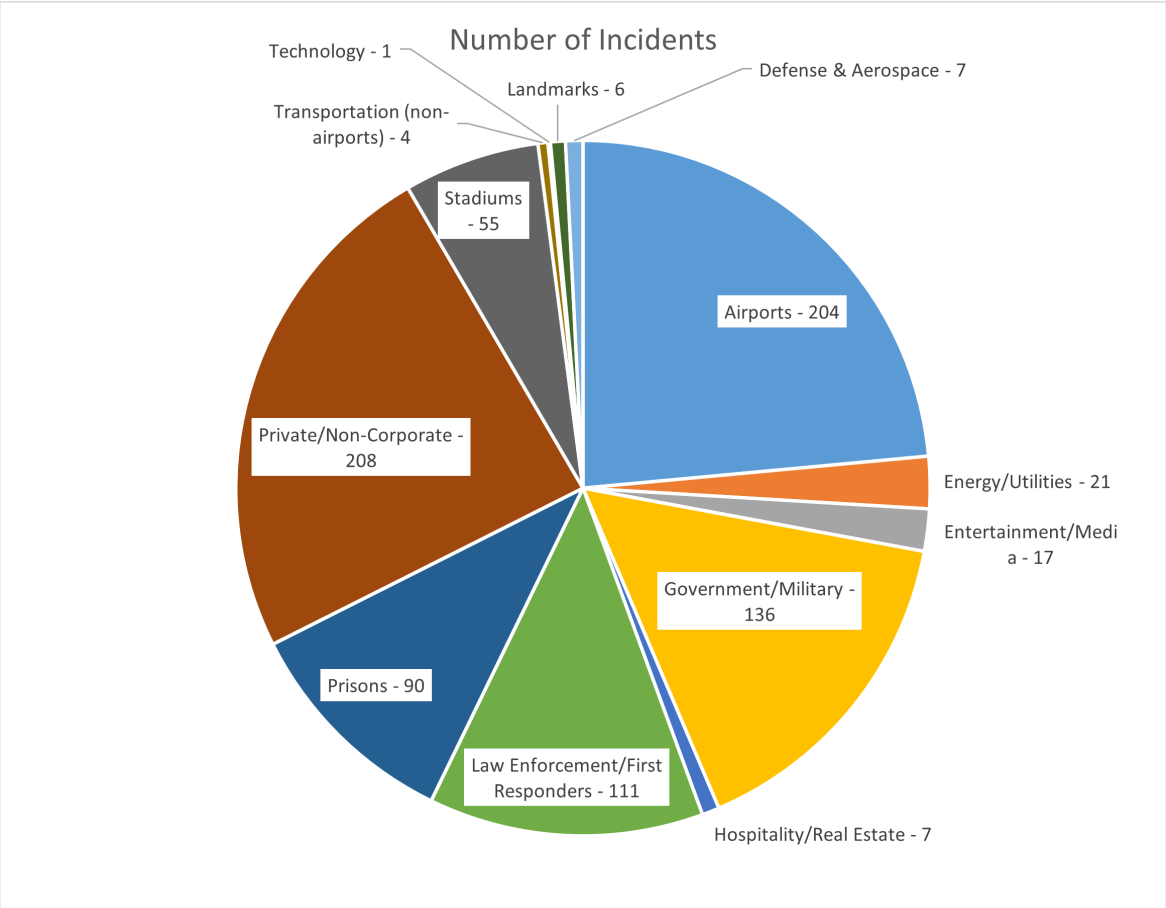

Figure 2. Distribution of drone incidents across different environments.

 doi:10.20944/preprints202503.2043.v1

appropriateness of the data that could be obtained for the systems. These counter-drone solutions utilize multiple technologies for detecting, tracking, and identifying drones. Figure 3 illustrates the distribution of these technologies. The most widely used methods include [38]:

- **Microwave radars:** Employed in 55% of the systems, radars detect drones through active radio wave emissions and reflections.
- **Visible light (VIS) cameras:** Used in 47% systems, VIS cameras enable optical detection and visual tracking, very often as a secondary sensing modality to support the identification of the drone threat or to provide a visual cue for the operators.
- **Thermal imaging cameras:** Integrated into 35% systems, these cameras detect drones based on infrared signatures.
- **Frequency monitoring devices:** Present in 64% systems, these devices detect and analyze radio frequency emissions from drones and their controllers.
- **Acoustic sensors:** Used in 10% systems, these sensors capture and analyze the sound signatures of drone propellers.
- **Infrared (IR) sensors and lidar systems:** Less commonly used, with 2% and 4% implementations respectively.

The prevalence of these technologies indicates a trend toward multi-sensor fusion for enhanced reliability and robustness.

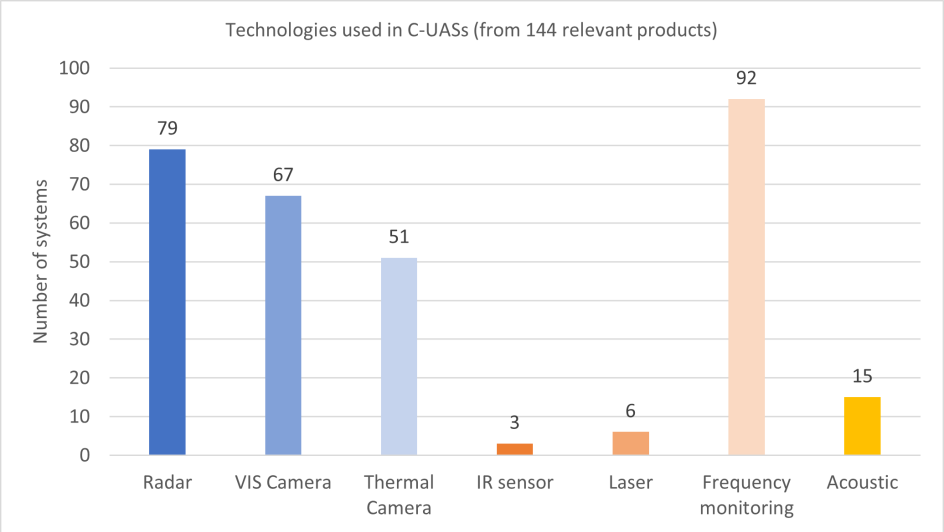

Figure 3. Technologies used for detect, track, and identify (DTI) in counter-drone solutions.

4.2. Combination of Technologies in Counter-Drone Solutions

Modern counter-drone solutions often integrate multiple detection technologies to improve detection probability and tracking accuracy. Figure 4 presents the percentage distribution of different technological combinations within counter-drone solutions. The breakdown is as follows:

- **Single-technology systems:** 53% of counter-drone solutions rely on one detection method, primarily frequency monitoring or radar-based detection.
- **Two-technology systems:** 9% of solutions combine two methods, such as radar and VIS cameras.
- **Three-technology systems:** 15% of solutions incorporate three distinct technologies, enhancing multi-modal detection.
- **Four or more technology systems:** 23% of solutions employ four or more technologies, typically integrating radars, cameras, RF monitoring, and additional sensors.

The trend toward multi-technology systems highlights the need for robust data fusion methodologies to effectively mitigate false positives and negatives.

 doi:10.20944/preprints202503.2043.v1

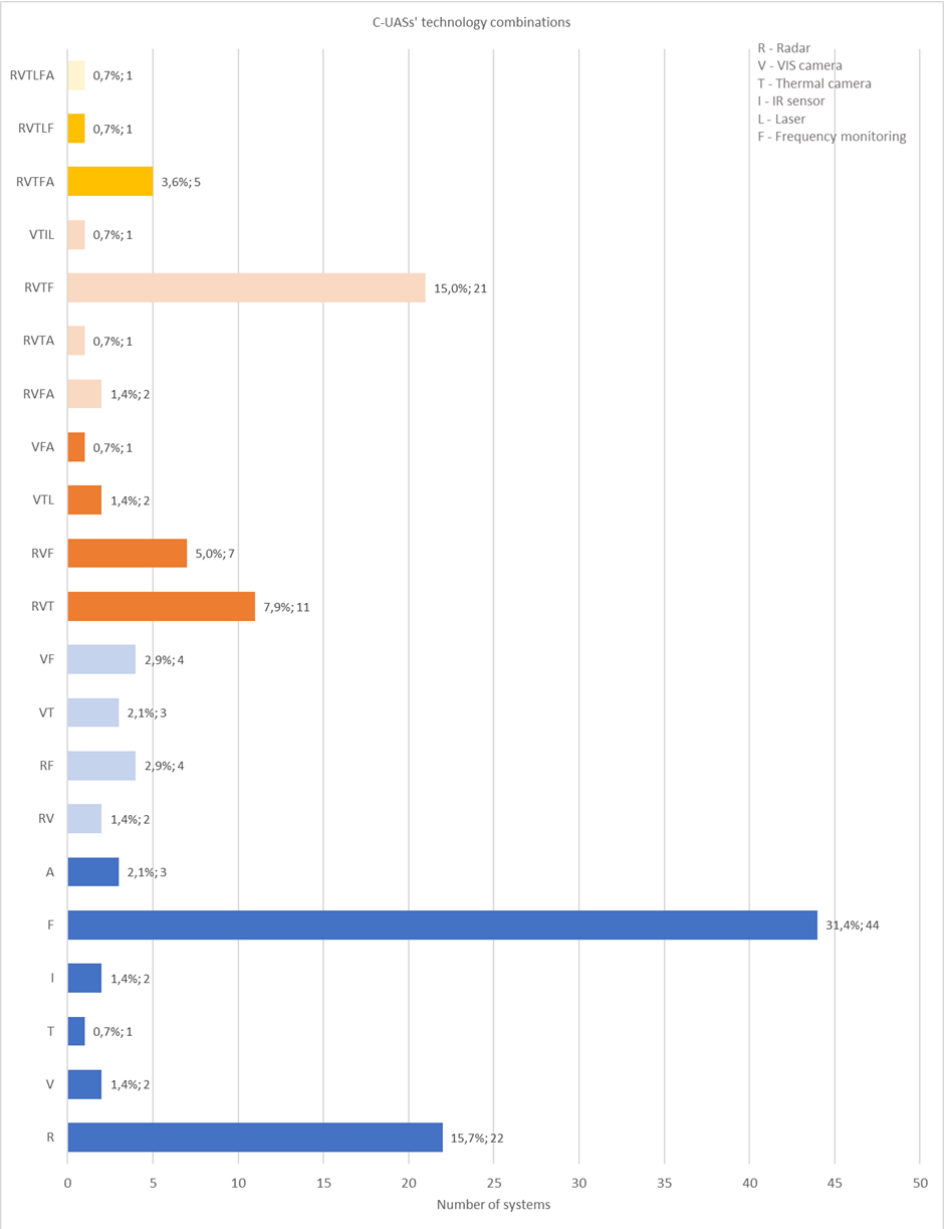

Figure 4. Combinations of technologies used in counter-drone solutions.

4.2.1. Countermeasures and Mitigation Techniques

Upon detection and identification of a drone threat, various mitigation techniques can be deployed:

- **Electronic Countermeasures:** These include RF jamming, spoofing, and protocol manipulation to disrupt drone communications or take control of the aircraft.
- **Kinetic Solutions:** Physical neutralization methods, such as net guns, interceptor drones, and high-energy laser weapons, are deployed in scenarios requiring immediate elimination of threats.
- **Directed Energy Systems:** Microwave-based and laser-based directed energy weapons provide non-contact neutralization by disabling drone electronics or structure.

4.3. Challenges and Considerations in Counter-Drone Technology Selection

Selecting an appropriate counter-drone system requires consideration of multiple factors, including:

 doi:10.20944/preprints202503.2043.v1

- **Detection range:** Different technologies exhibit varying effectiveness depending on range constraints and environmental conditions.
- **Weather resistance:** Radar and frequency monitoring are more resilient to adverse weather than optical and infrared-based systems.
- **False alarms:** Acoustic sensors and frequency monitoring devices may generate false detections due to ambient noise or RF interference.
- **Deployment feasibility:** Mobile, vehicular, and fixed installations require different logistical and operational considerations.
- **Integration with existing systems:** Many counter-drone solutions must interface with existing security frameworks, requiring compatibility with software and hardware components.
- **Regulatory constraints:** National and international regulations govern the use of certain detection and mitigation techniques, affecting system deployment.
- **Operational Environments:** Urban settings present challenges due to RF congestion and the presence of obstacles, whereas open-field environments offer improved detection and engagement opportunities.
- **Advancements in UAS Technology:** The increasing use of autonomous drones, encrypted communications, and low-observable designs necessitate continuous evolution of counter-drone methodologies.

The current landscape of counter-drone technologies reflects an ongoing arms race between drone capabilities and counter-drone solutions. Future advancements in artificial intelligence, sensor fusion, and autonomous countermeasure deployment will play a critical role in enhancing the resilience and effectiveness of counter-drone frameworks.

5. Development of Standard Scenarios

5.1. The need for Standard Scenarios

To ensure a comprehensive assessment of counter-drone capabilities, standardized scenarios must be developed. These scenarios provide a structured framework for testing detection, tracking, and identification (DTI) performance across diverse threat conditions. Without such standardization, comparisons between different counter-drone solutions remain inconsistent, hindering technological advancements and operational readiness. The establishment of well-defined scenarios enables researchers, security agencies, and policymakers to benchmark system effectiveness, identify limitations, and refine countermeasure strategies.

Standardization also supports regulatory efforts, helping define clear operational requirements and legal constraints for counter-drone deployment. By ensuring that different counter-drone technologies are tested under comparable conditions, authorities can establish baseline performance metrics and guidelines. Furthermore, standardized scenarios aid in developing training programs for law enforcement agencies, ensuring personnel are well-prepared to handle UAS threats effectively.

In addition to enhancing technical evaluations, standardized scenarios facilitate collaboration across international security agencies and industry stakeholders. By defining common testing parameters, organizations can share data and insights, driving collective improvements in counter-drone technologies and response strategies. The increasing complexity of drone threats underscores the need for a unified approach, making scenario standardization a crucial step in advancing counter-drone capabilities.

5.2. Methodology for Creating Standard Scenarios

The development of standardized scenarios within the COURAGEOUS project followed a systematic methodology incorporating multiple data sources and expert validations. The process involved four key steps:

 doi:10.20944/preprints202503.2043.v1

- **Literature Review**: An extensive review of existing counter-drone frameworks, threat assessments, and prior studies was conducted to identify recurring challenges and gaps in current methodologies.
- **Incident Analysis**: A comprehensive analysis of past UAS-related security incidents was performed to extract relevant parameters influencing scenario design, such as environmental conditions, UAS characteristics, and operational constraints.
- **Stakeholder Input**: Law enforcement agencies (LEAs) and other end-users provided valuable insights through structured questionnaires and workshops, ensuring that the scenarios aligned with real-world security concerns.
- **Iterative Validation**: The initial set of scenarios was refined through iterative discussions with experts and field trials, ensuring applicability across diverse operational contexts.

In each of these steps, a broad set of factors was considered, including drone size, speed, flight altitude, payload type, and operational intent. By incorporating these elements, the resulting scenarios comprehensively address the spectrum of UAS threats.

Beyond the methodological approach, statistical models and simulations were used to analyze potential drone threats under different conditions. Advanced modeling techniques, including Monte Carlo simulations, were applied to predict UAS behavior and potential countermeasure effectiveness. This data-driven approach ensures that the developed scenarios not only reflect historical incidents but also anticipate emerging threats in the rapidly evolving UAS landscape.

5.3. Overview of Standard Scenarios

The standard scenarios developed within the COURAGEOUS framework are categorized into three main groups: *Sensitive Sites/Critical National Infrastructure*, *Public Spaces Protection/Events*, and *Border Protection (Land – Maritime)*. Each scenario reflects a plausible threat event, outlining key operational conditions and adversarial tactics.

The ten standardized scenarios are shown on Figure 5 and can be described as follows:

1. **Prison** – Unauthorized drone activity attempting to smuggle contraband into a correctional facility.
2. **Airport** – A rogue UAS operating in restricted airspace, posing a collision risk to manned aircraft.
3. **Nuclear Plant** – Surveillance or potential sabotage by a hostile drone over critical energy infrastructure.
4. **Government Building** – Unauthorized UAS activity threatening national security at government premises.
5. **Stadium** – A drone attempting to disrupt a large public event, such as a sports match.
6. **Outdoor Concert** – Aerial surveillance or potential attack during a high-profile entertainment event.
7. **Outdoor Political Rally** – A drone deployed for surveillance or direct attack during a political gathering.
8. **International Summit** – Hostile UAS presence at a high-security diplomatic event.
9. **Land Border** – Surveillance or smuggling activity using drones to bypass border controls.
10. **Maritime Border** – UAS-assisted illegal crossing or surveillance in maritime security zones.

Each scenario is designed with specific parameters, including environmental conditions, drone capabilities, and the nature of the security challenge. These structured descriptions enable precise testing and evaluation of counter-drone performance under realistic threat conditions.

 doi:10.20944/preprints202503.2043.v1

Figure 5. Visual representation of the ten standardized scenarios.

By standardizing these scenarios, a common reference framework is established that enhances interoperability, facilitates comparative assessments, and improves the overall effectiveness of counter-drone solutions. The scenarios provide a foundation for controlled testing environments and real-world field trials, helping refine counter-drone response strategies and operational protocols.

However, it is obvious that these standard scenarios do not cater to all use cases. This is why an open architecture was used in the development of the CWA pre-standard, enabling any user to come up with new scenarios based upon the existing templates. Future research will also continue to adapt these scenarios based on evolving threats and technological advancements, ensuring that the standardized framework remains relevant and effective in countering UAS threats.

6. Risk Analysis and Risk Assessment Metrics

The risk assessment of potential UAS threats is crucial to ensuring effective mitigation strategies. A comprehensive risk assessment must consider the dynamic and evolving nature of UAS threats, which range from accidental airspace incursions to deliberate attacks. The risk evaluation process involves understanding the threat landscape, assessing vulnerabilities in existing defense mechanisms, and defining appropriate metrics to quantify risks and system performance.

This chapter presents the contributions in developing a systematic methodology for risk analysis in counter-drone applications, introducing a structured approach to evaluating threats posed by drones and provides a set of standardized risk assessment metrics tailored to different operational contexts. By leveraging empirical data, expert inputs, and analytical models, the framework enhances the ability to quantify and respond to drone-related risks effectively.

6.1. Methodological Approach to Risk Assessment

The COURAGEOUS project adopted a multi-layered methodological approach to define and evaluate the risks associated with UAS threats. The process involved the identification of key risk factors through literature analysis, historical incident evaluation, and end-user consultations. A structured questionnaire was disseminated among stakeholders, including law enforcement agencies

 doi:10.20944/preprints202503.2043.v1

(LEAs) and security professionals, to systematically assess the likelihood and impact of various UAS threat scenarios.

The risk assessment model integrates two primary indicators:

- **Likelihood**: The probability of an adversarial UAS operating within a given scenario.
- **Impact**: The potential consequences of an unauthorized UAS action, taking into account physical, financial, and operational damages.

By combining these factors, a comprehensive risk matrix was developed. This matrix allows for the classification of drone threats into different risk categories, facilitating prioritization and resource allocation for countermeasures. The methodology further considers the role of UAS capabilities, such as payload capacity, flight endurance, and autonomy, in shaping the threat landscape.

The risk posed by UAS can be categorized into multiple dimensions, including technical, operational, and strategic risks. Technical risks involve limitations in detection, tracking, and neutralization capabilities, while operational risks stem from the complexity of deploying counter-drone systems in urban and contested environments. Strategic risks pertain to policy, regulatory, and legal challenges that influence the effectiveness of counter-drone solutions.

A structured risk assessment framework is required to systematically evaluate the probability and impact of UAS threats. The Specific Operations Risk Assessment (SORA) methodology is commonly used to analyze these risks, providing a step-by-step approach to evaluate operational safety and mitigation strategies. SORA identifies risk factors such as the likelihood of drone incursions, the potential consequences of an attack, and the effectiveness of existing countermeasures.

A core innovation in the framework is the establishment of a dynamic risk evaluation model that continuously updates based on real-time threat intelligence and evolving UAS technology trends. This ensures that the risk assessment process remains relevant and adaptable to emerging threats.

6.2. Risk assessment Metrics

To effectively quantify risk levels, several key performance indicators (KPIs) must be defined. Detection probability measures the ability of a counter-drone system to identify unauthorized drones within a defined range and timeframe. False alarm rate quantifies the occurrence of erroneous detections that may lead to operational inefficiencies. Response time evaluates the system's ability to detect, track, and neutralize a threat before it reaches its target. Mitigation success rate reflects the effectiveness of countermeasures in neutralizing hostile drones. Additionally, environmental adaptability assesses system performance under varying weather and geographical conditions.

The risk analysis for each scenario (as presented in the previous chapter) is derived from an aggregation of expert evaluations and empirical data. Each scenario is assigned a total risk score based on the weighted sum of likelihood and impact assessments. The highest risk scenario identified was the **Prison Scenario**, as it concerns a scenario in an urban environment, where it is impossible to exert a continuous total control. The lowest risk scenario was the **International Summit**, as for this type of scenario, multiple counter-drone tools can be employed and a strict control can be enforced.

The project also introduces **Key Risk Indicators (KRIs)**, which serve as benchmark values for assessing UAS threats. These indicators include (amongst others):

- Environmental complexity and operational constraints.
- The technical capabilities of adversarial UAS.
- The effectiveness of existing counter-drone measures against varying drone technologies.
- The frequency of drone incursions in specific operational environments.
- The ability of counter-drone operators to respond effectively to identified threats.

The results of this analysis directly contribute to refining counter-drone strategies. By mapping risk scores to operational response levels, security agencies can optimize resource allocation and response protocols. Furthermore, the adoption of standardized risk assessment methodologies fosters

 doi:10.20944/preprints202503.2043.v1

interoperability among European security forces, enhancing cross-border collaboration in drone threat mitigation.

7. Performance Requirements

7.1. Operational Needs and Performance Requirements

Operational needs define the essential capabilities required to counter unauthorized UAS incursions. These requirements are derived from standardized scenarios encompassing diverse operational environments, such as urban centers, airports, prisons, and maritime borders. Key operational parameters include early warning systems, real-time tracking, multi-sensor integration, and seamless interoperability with existing security infrastructure.

A critical challenge in defining operational needs is the lack of universally accepted technical standards. Consequently, operational requirements must be structured to ensure compatibility with evolving threats and emerging technologies. The ability to detect, track, and identify threats accurately remains the cornerstone of an effective counter-drone strategy, with priority considerations given to minimizing false alarms and maximizing detection range.

7.2. Methodology for Operational Needs Definition

To systematically capture the operational needs for counter-drone operations, a structured requirements definition approach was employed. The methodology adheres to best practices in system engineering and requirements management, ensuring consistency, traceability, and usability for subsequent system development phases. The approach follows a sequential process:

1. **Operational Needs Definition:** Identification of core operational requirements based on stakeholder input and analysis of real-world threat scenarios.
2. **System Procurement Considerations:** Translation of operational needs into system-level requirements to guide the selection and development of counter-drone technologies.
3. **Validation and Iteration:** Continuous refinement of requirements based on testing, feedback, and evolving operational challenges.

This iterative framework ensures that the operational needs remain aligned with real-world constraints while accommodating technological advancements and policy developments.

To standardize the requirements formulation, the IEEE 29148 process terminology was adopted. This standard is widely recognized across European partners and has demonstrated effectiveness in prior security and defense-related projects. The prioritization of requirements follows a structured classification to facilitate clear decision-making:

- **Shall:** High-priority requirements that must be met for the project to achieve its core objectives.
- **Should:** Medium-priority requirements that are desirable but not essential, allowing for trade-offs if necessary.
- **May:** Low-priority requirements that provide additional value but do not impact the fundamental operational capability of the system.

This classification enables end users to systematically articulate their needs while ensuring technical partners can effectively translate these requirements into implementable system specifications.

To facilitate clarity and traceability, operational needs were documented using a standardized template. Each requirement is uniquely identified and categorized based on its significance and intended application. The structured format includes:

- **Requirement Number:** A unique identifier for tracking and reference.
- **Requirement Name:** A concise descriptor summarizing the need.
- **Description:** A detailed explanation, including the rationale and operational context.
- **Importance:** The assigned prioritization level (Shall, Should, May).

This approach ensures that all stakeholders—ranging from system operators to technology developers—have a common understanding of the operational expectations and constraints.

 doi:10.20944/preprints202503.2043.v1

The structured requirements framework encompasses a comprehensive range of operational needs, particularly focusing on detection, tracking, and identification (DTI) capabilities. Given the diversity of deployment environments, requirements are tailored to address specific scenarios, such as:

- **General Operational Needs:** Baseline capabilities applicable across multiple deployment contexts.
- **Scenario-Specific Needs:** Custom requirements adapted to distinct security environments (e.g., airports, government buildings, public events).
- **Integration Needs:** Interoperability with existing security infrastructure and command-and-control systems.

By linking operational needs with specific deployment contexts, the approach ensures that the defined requirements remain practical and actionable.

7.3. Performance Requirements and Metrics

Performance requirements translate operational needs into quantifiable metrics. They are influenced by multiple operational factors, including the size and speed of target drones, the complexity of the operational environment, and the response time needed to neutralize threats. Detection capabilities must be comprehensive, covering a wide range of altitudes and distances while maintaining high accuracy rates. The system should effectively discriminate between drones and other airborne objects to minimize false alarms. Tracking performance must ensure continuous and stable monitoring of drone movements, even in scenarios where multiple UAS are operating simultaneously.

Identification accuracy is another critical requirement, as distinguishing between different drone models and payload types is essential for assessing threat levels. This involves integrating multispectral imaging, radio frequency (RF) analysis, and machine learning-based classification. Furthermore, mitigation effectiveness is a key factor in assessing counter-drone performance. Whether employing electronic countermeasures, physical interception, or other mitigation strategies, the system must neutralize threats reliably while minimizing collateral risks.

The COURAGEOUS framework categorizes all these requirements into:

- **Detection Performance**: The system must identify drones across various size classifications and operational altitudes.
- **Tracking and Identification**: Continuous tracking of detected UAS with high positional accuracy, distinguishing between cooperative and non-cooperative drones.
- **System Interoperability**: Compatibility with forensic analysis tools and integration with existing security networks, including air traffic management (ATM) and U-space services.
- **Robustness**: Resistance to environmental factors such as adverse weather conditions and electromagnetic interference.

Performance evaluation necessitates the development of objective metrics to assess system effectiveness across different operational contexts. Typical metrics to assess performance requirements include detection range, tracking accuracy, response time, and system resilience against environmental perturbations. Detection probability measures the likelihood of successfully identifying a drone within a given range, while the false alarm rate assesses the frequency of incorrect detections. The system's response time is a crucial metric, as rapid threat engagement is necessary to prevent unauthorized drone activity. Tracking accuracy is evaluated based on the system's ability to maintain a drone's position data over time, ensuring continuous monitoring and predictive analysis of its trajectory. Additionally, environmental adaptability examines how well a system performs under varying weather conditions, electromagnetic interference, and urban congestion. System resilience against countermeasures, such as drone evasive maneuvers and signal-jamming resistance, is also considered a vital performance parameter. The integration of artificial intelligence (AI) and advanced data fusion techniques further enhances counter-drone performance, allowing for improved decision-making and automation in real-time threat scenarios.

 doi:10.20944/preprints202503.2043.v1

7.4. Counter-Drone Evaluation Framework

The evaluation of counter-drone solutions requires a structured framework to assess their effectiveness, reliability, and operational suitability. This framework provides a standardized approach for documenting, reviewing, and comparing test results across various counter-drone solutions, facilitating informed decision-making for the development, procurement, and deployment of such technologies. The COURAGEOUS project proposes a structured evaluation methodology for assessing counter-drone effectiveness.

An effective evaluation framework must ensure objectivity through quantitative and qualitative metrics, maintain repeatability by establishing test conditions that allow consistent assessments, and be adaptable to different operational environments and evolving threats. Additionally, transparency in documentation is crucial for stakeholders and regulatory bodies to ensure compliance and trust in the evaluation process.

The proposed framework comprises a standardized testbed for performance validation, incorporating real-world scenarios to benchmark system capabilities. Evaluation methodologies include:

1. **Scenario-based testing**: Simulating realistic threats in controlled environments to analyze system responses.
2. **Quantitative metrics assessment**: Measuring system performance against predefined benchmarks, such as detection accuracy and latency.
3. **Comparative analysis**: Establishing a common baseline for evaluating different counter-drone solutions under identical testing conditions.
4. **Continuous improvement cycle**: Iterative refinement of requirements and metrics based on empirical test results.

The methodology for evaluating counter-drone performance consists of multiple stages. Initially, clear evaluation goals must be defined, focusing on aspects such as detection accuracy, response time, and mitigation effectiveness. Following this, test scenarios should be carefully selected to represent a range of operational conditions, including urban, rural, and maritime environments, ensuring that the system's adaptability is thoroughly tested.

Once scenarios are established, performance metrics are employed to measure key capabilities, such as detection probability, tracking accuracy, and neutralization success rate. Data collection and analysis play a crucial role in this process, as information is gathered from sensor logs, operator feedback, and forensic assessments to ensure a comprehensive evaluation. Comparative benchmarking is then used to establish performance baselines, enabling an objective comparison between different counter-drone systems under identical conditions.

This evaluation framework provides a transparent mechanism for stakeholders to evaluate and compare counter-drone technologies and make informed procurement decisions. The systematic approach outlined in this paper underscores the necessity of a structured framework for counter-drone development and assessment. By aligning operational needs with performance requirements and employing rigorous evaluation methodologies, the proposed methodology aims to enhance the efficacy and reliability of counter-drone benchmarking technologies.

8. Performance Evaluation and Validation

8.1. Evaluation Metrics

The proposed evaluation methodology is designed to be objective-driven, meaning that it focuses on predefined operational goals and performance criteria. It is structured around scenario-based testing, in which DTI systems are assessed under conditions that closely resemble real-world environments. These scenarios include sensitive sites and critical infrastructure such as airports, power plants, and military installations, public spaces such as stadiums and mass gatherings, and border security environments where drones may be used for illicit activities. Each scenario incorporates environmental

 doi:10.20944/preprints202503.2043.v1

variables such as weather conditions, signal interference, and varying drone behaviors, ensuring a comprehensive assessment of system performance.

The evaluation framework employs clearly defined performance metrics, as defined in Table 1 to enable standardized comparisons between different DTI solutions.

Table 1. Evaluation metrics defined in the COURAGEOUS standard test methodology [40].

Metric name	**Description**	**Equation**
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, with d_j the detection j, N_d the total number of detections, gt_i the ground truth i, and N_{gt} the total number of ground truths. The metric is undefined for detections which do not represent a true object	$A_{ij} = \begin{cases} 1, & \text{if } gt_i \text{ and } d_j \text{ associate} \\ 0, & \text{otherwise} \end{cases}$ (1) $\Delta_{ij} = \text{distance between } gt_i \text{ and } d_j$ (2) $\text{Location accuracy}(gt_i) = \sqrt{\frac{\sum_{j=1}^{N_d} A_{ij} \cdot \Delta_{ij}^2}{\sum_{j=1}^{N_d} A_{ij}}}$ (3)
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	$\Delta(x,t) = \text{Distance}(x, \text{DTI sensor})$ (4) $R_{near}(gt_i) = \frac{\max_t(\Delta(gt_i,t)) - \min_j(\Delta(gt_i,t_{d_j}) \cdot A_{ij})}{\max_t(\Delta(gt_i,t)) - \min_t(\Delta(gt_i,t))}$ (5) $R_{far}(gt_i) = \frac{\max_j(\Delta(gt_i,t_{d_j}) \cdot A_{ij}) - \min_t(\Delta_{DTI}(gt_i,t))}{\max_t(\Delta(gt_i,t)) - \min_t(\Delta(gt_i,t))}$ (6)
Preci-sion	The precision of detections is defined as the fraction of all detections which represent a true object	$\text{Precision} = \frac{\sum_{j=1}^{N_d} \max_{i=1}^{N_{gt}} A_{ij}}{N_d}$ (7)
Detection immediateness	The detection immediateness is defined as the difference between the time T at which an object enters the AoI and the time of its first detection	$\text{Immediateness}(gt_i) = T(gt_i^{start}) - \min_{j=1}^{N_d} T(d_j)$ (8)
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	$\text{Track completeness}(gt_i) = \frac{D\left(\bigcup_{j=1}^{N_t} R(A_{ij} \cdot t_j)\right)}{D(gt_i)}$ (9)

 doi:10.20944/preprints202503.2043.v1

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	$$\text{Track continuity}(gt_i) = \frac{\sum_{j=1}^{N_t}(A_{ij}^{\min}) - 1}{D\left(\bigcup_{j=1}^{N_t} R(A_{ij} \cdot t_j)\right)} \quad (10)$$
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	$$\text{Track ambiguity}(t_k) = \frac{\sum_{j=1}^{N_t} A_{ij}(t_k)}{N_{gt}(t_k)} \quad (11)$$ $$\text{Track ambiguity} = \frac{\sum_{k=1}^{K} \text{Track ambiguity}(t_k) \cdot \Delta t_k}{\sum_{k=1}^{K} \Delta t_k} \quad (12)$$
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	$$S(t_k) = \frac{N_T(t_k) - N_A(t_k)}{N_T(t_k)} \quad (13)$$ $$S = \frac{\sum_{k=1}^{K} S(t_k) \cdot \Delta t_k}{\sum_{k=1}^{K} \Delta t_k} \quad (14)$$
Track positional accuracy	The track positional accuracy of a true object is defined as the Root Mean Square (RMS) distance between the tracks representing the object and the true object. The metric is undefined when no track represents the true object	$$\Delta_{ij} = \text{distance between } gt_i \text{ and } t_j \quad (15)$$ $$\text{acc}_{ij} = \sqrt{\frac{\sum_{k=1}^{N_{k,j}} A_{ij}(k) \cdot \Delta_{ij}(k)^2}{N_{k,j}}} \quad (16)$$ $$\text{TPA(gti)} = \sqrt{\frac{\sum_{j=1}^{N_t} D(A_{ij}) \cdot \text{acc}_{ij}^2}{\sum_{j=1}^{N_t} D(A_{ij})}} \quad (17)$$
Track velocity accuracy	The track velocity accuracy of a true object is defined as the RMS velocity difference between the tracks representing the object and the true object. The metric is undefined when no track represents the true object	$$\Delta_{ij} = \text{velocity difference between } gt_i \text{ and } t_j \quad (18)$$ $$\text{TVA (gti)} = \sqrt{\frac{\sum_{j=1}^{N_t}\sum_{k=1}^{N_{k,j}} A_{ij}(k) \cdot \Delta_{ij}(k)^2}{\sum_{j=1}^{N_t}\sum_{k=1}^{N_{k,j}} A_{ij}(k)}} \quad (19)$$
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.	$$\text{Longest Track Segment (gti)} = \max_{j=1}^{N_t} \frac{D(A_{ij})}{D(\text{gti})} \quad (20)$$
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	$$\text{TI}(gt_i) = T(gt_i^{start}) - \min_{j=1}^{N_t} T(t_j^{start}) \quad (21)$$

 doi:10.20944/preprints202503.2043.v1

F1 score	The F1-score is the harmonic mean of precision and recall. It is calculated by measuring the number of True Positives (TP), False Positives (FP) and False Negatives (FN). The TP are calculated as the duration of the truth trajectories in which there was at least a single identified track associated to the truth. The value for the FP constitutes to the duration of the tracks trajectories in which there was no associated truth, but the track was identified as positive. The value for the FN constitutes to the duration of the truth trajectories in which there was not an identified track associated to the truth.	$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$ (22) $\text{F1} = \frac{2TP}{2TP + FP + FN}$ (23)
False Alarm Rate (FAR)	The false alarm rate is defined as the fraction of falsely given alarms out of the total number of alarms	$\text{FAR} = \frac{\text{FP}}{\text{FP} + \text{TN}}$ (24)
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	$\text{MAR} = \frac{\text{FN}}{\text{TP} + \text{FN}}$ (25)
Probability of Detection (PoD)	The probability of detection is defined as the number of times in which the DTI system emits the alarm rightfully (true positives), divided by the total number of alarms it should have emitted	$\text{PoD} = \frac{TP}{TP + FN}$ (26)
Preci-sion	The precision is defined as the fraction of all detections which represent a true object, i.e. associate with a ground truth	$\text{Precision} = \frac{TP}{TP + FP}$ (27)

8.2. Evaluation Methodology

To maintain fairness and objectivity, the methodology follows a comparative performance evaluation approach. All tested systems undergo identical scenarios under controlled conditions, eliminating external biases that could influence the results. Therefore, the outputs from system tests are normalized into a score ranging from 0 (worst) to 1 (best), facilitating consistent comparisons across different DTI systems. The metric evaluation process is illustrated in Figure 6.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 March 2025 doi:10.20944/preprints202503.2043.v1

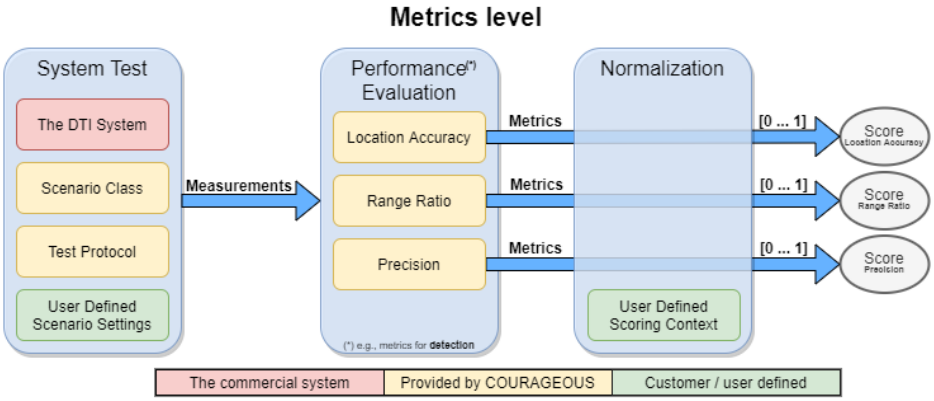

Figure 6. Performance evaluation at the metric level. The process involves executing system tests, computing raw performance values, and normalizing them into scores.

The component level integrates normalized metric scores into functional categories such as detection, tracking, and identification. Each component aggregates the relevant metric scores and applies user-defined weights based on operational priorities. This step provides an overall evaluation score for each functional component, forming the basis for system-level assessment. The process is visualized in Figure 7.

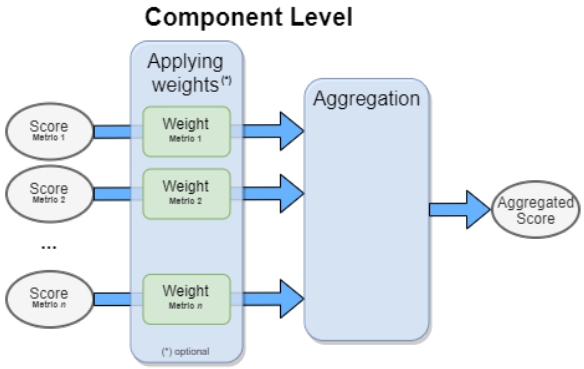

Figure 7. Performance evaluation at the component level. This stage aggregates metric scores into component-level evaluations, allowing prioritization based on operational requirements.

The combination of metric and component evaluations ensures that system performance is assessed holistically, accounting for individual function effectiveness and overall operational utility. This structured methodology supports data-driven decision-making in selecting optimal DTI solutions for specific use cases. The methodology ensures that results are not only accurate and repeatable but also actionable, enabling decision-makers to make informed choices when selecting DTI solutions. For a more detailed description of the test methodology, including the experimental setup and specific evaluation procedures, refer to [40].

9. Validation

Ensuring the reliability and applicability of the test methodology requires a structured validation process. Validation is conducted in two key stages: simulation-based verification and operational field trials. Simulation-based verification serves as the initial step, allowing for controlled testing of different scenarios in a virtual environment. This stage is crucial for refining performance metrics, optimizing detection algorithms, and identifying potential system limitations before real-world deployment. By simulating a wide range of conditions, including adverse weather, electronic interference, and varying drone speeds, this approach provides a preliminary assessment of system robustness and adaptability.

Following successful simulation-based verification, the methodology underwent validation through real-world operational field trials. These trials are conducted in diverse environments to

 doi:10.20944/preprints202503.2043.v1

evaluate system adaptability under actual deployment conditions and in different geographical context. Therefore, field trials were organized in Greece, Belgium and Spain, as depicted in Figure 8.

(**a**) (**b**) (**c**)

Figure 8. Validation of the standardized evaluation methodology took place in different test sites with a wide range of drones and a wide range of counter-drone solutions, in order to assess the robustness of the performance assessment. The figures show snapshots of the tests being performed in: (**a**) Greece (Athens Airport). (**b**) Belgium (Lombardsijde Military Base). (**c**) Spain (ATLAS test centre).

During the trials, different types of drones were used to test the performance of the DTI systems. The ground truth used to measure this performance was the drone trajectory recorded by GPS logger devices installed on-board the drones. In addition, the telemetry data registered by the drone autopilot was also logged to have an additional source of information in case any data inconsistency were detected after processing the logs.

The counter-drone companies provided their data in a standard data format that was designed specifically to log the information from the DTI systems during their operation. For this data format, 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. This data format is open source and can be found at https://grvc.us.es/courageous/.

A range of Custom-Of-The-Shelf and homebuilt drones were used during the trials. All the drones were equipped with GPS loggers and were able to fly pre-programmed flight paths. A range of flight operations were planned based upon the scenarios described above, cycling through the available drones and combining several changing parameters such as altitude and speed. In addition, there were also blind free flight missions carried out by police units in order to simulate more erratic flight movements.

Given the output of the tested DTI systems as well as the corresponding ground truth, a comparative analysis of the collected data and ground truth was performed. In a first step, data pre-processing was performed through time window filtering, transformation of coordinate systems and selection of areas of interest. In a second step, the detection tracks are associated with the ground truth and finally the resulting performance metrics are calculated and normalized. These metrics are used to generate an an aggregated score, separately per tested DTI system. This data was then compared to the data provided by the counter-drone companies participating to the trials.

These field trials allowed for the assessment of DTI performance in uncontrolled settings, where factors such as urban density, environmental noise, and unpredictable drone behavior influence results. Additionally, operational trials provide empirical performance benchmarks, ensuring that the test methodology remains relevant and practical for real-world applications. The iterative nature of this validation process allows for continuous improvements, enabling refinements based on field observations and feedback from end-users.

By combining simulation-based verification with live operational trials, the validation methodology ensures that the testing framework is both scientifically rigorous and operationally relevant. The integration of these two stages provides a holistic evaluation approach, mitigating risks associated with system deployment and ensuring that performance assessments remain accurate and actionable.

 doi:10.20944/preprints202503.2043.v1

For a detailed discussion of the validation process, including specific trial designs and performance analysis methods, refer to [41].

10. Conclusions

This paper presented a standardized evaluation methodology for counter-drone solutions, developed within the framework of the COURAGEOUS project. The increasing threat posed by unauthorized drone activity, coupled with the lack of widely accepted performance assessment methods, necessitates a rigorous and repeatable testing framework for counter-drone technologies.

The proposed methodology defines a set of standardized test scenarios designed to reflect real-world operational challenges across diverse environments, including critical infrastructure protection, public event security, and border surveillance. A comprehensive evaluation framework was developed, integrating both qualitative and quantitative performance metrics. These metrics, including detection accuracy, tracking stability, response time, and false alarm rates, ensure a structured and objective assessment of counter-drone capabilities.

To validate the methodology, extensive field trials were conducted in multiple locations, including Greece, Belgium, and Spain. These trials demonstrated the applicability and robustness of the evaluation framework, confirming its ability to differentiate system performance across various operational conditions. The integration of structured data logging and standardized reporting formats further enhances the transparency and repeatability of the assessment process.

The presented result is a pre-standard, which is open and free to consult for everyone. However, more work is required to transform this pre-standard into a full standard, which will be the subject of future research. More research is indeed required for refining standardized testing protocols, particularly in addressing evolving threats posed by increasingly autonomous and stealthy drones. Moreover, the limitation adopted in the presented work of only considering the DTI aspect of the counter-drone kill chain, is highly artificial and cannot be maintained in the furure. Indeed, from a client's perspective, counter-drone tools need to provide holistic solutions to the UAS incursion problem, and this does mean incorporating a clear link between detection, tracking, identification *and* neutralisation / interception and - not to be forgotten - forensics and training. Future research should thus focus on linking DTI and neutralisation aspects, expanding test scenarios, and enhancing interoperability with existing security infrastructures. By aligning with ongoing international standardization initiatives, the COURAGEOUS framework provides a critical step toward the objective benchmarking and certification of counter-drone technologies, ultimately supporting more informed decision-making for security and defense stakeholders.

Author Contributions: Conceptualization, methodology, writing—review and editing, validation, formal analysis D. Doroftei, P. Petsioti, A. Koniaris, K. Brewczyński, M. Życzkowski, R. Razvan, S. Sima, A. Mohamoud, J. van de Pol, I. Maza, A. Ollero, C. Church and C. Popa; writing—original draft preparation, project administration, X.X.; funding acquisition, G. De Cubber. All authors have read and agreed to the published version of the manuscript.

Funding: This project has received funding from the European Union's Internal Security Fund Police under Grant Agreement 101034655 (COURAGEOUS).

Institutional Review Board Statement: This study did not require ethical approval.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The datasets presented in this article are not readily available because the performance data of counter-drone tools that protect critical infrastructure is security-sensitive data and cannot be shared. However, the CEN/CENELEC Workshop agreement, which is a pre-standard document that extensively details the presented work and includes a detailed methodology and implementation guidelines for assessing the performance of drone-drone solutions, can be accessed freely at https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf.

 doi:10.20944/preprints202503.2043.v1

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

C-UAS	COunter Unmanned Aerial Systems
CWA	CENELEC Workshop Agreement
DIN	Deutsches Institut für Normung
DTI	Detection, Tracking, Identification
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
KPI	Key Performance Indicator
KRI	Key Risk Indicators
LEA	Law enforcement agency
NATO	North Atlantic Treaty Organization
ISO	International Standardization Organisation
NIST	National Institute of Standards and Technology
NPSA	National Protective Security Authority
OSED	Operational Services and Environment Definition
RF	Radio Frequency
UAS	Unmanned Aerial Systems

References

1. Ashok, V.; Kumar, N.; Sarkar, S.; Degadwala, S. Security Threats of Unmanned Aerial Vehicles; *Springer International Publishing*, **2023**; pp 133–164. [Online] Available: https://doi.org/10.1007/978-3-031-33631-7_5.
2. Buric, M.; De Cubber, G. Counter Remotely Piloted Aircraft Systems. *MTA Review* **2017**, *27* (1).
3. Assessing the Threat: Autonomous Commercial Drones and Its Potential for Mass Civilian Casualty Attacks. **2024**. [Online] Available: https://doi.org/10.62293/irij-455ct.
4. De Cubber, G. Explosive drones: How to deal with this new threat? *International workshop on Measurement, Prevention, Protection and Management of CBRN Risks (RISE).* **2019**, Les Bon Villers, Belgium.
5. Kang, H.; Joung, J.; Kim, J. Y.; Kang, J.; Cho, Y. S. Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems. *IEEE Access.* **2020**, 8, 168671–168710. [Online] Available: https://doi.org/10.1109/ACCESS.2020.3023473.
6. González-Jorge, H.; Aldao, E.; Fontenla-Carrera, G.; Veiga-López, F.; Balvís, E.; Ríos-Otero, E. Counter Drone Technology: A Review. **2024**. [Online] Available: https://doi.org/10.20944/preprints202402.0551.v1.
7. Sirohi, H. S.; Khairnar, C. N.; Kumar, P.; Kumar, A. A Comprehensive Review of Modern Counter-Drone Technologies: Trends, Challenges, and Future Directions. *International Journal For Science Technology And Engineering.* **2024**, *12 (5)*, 4405–4418. [Online] Available: https://doi.org/10.22214/ijraset.2024.62594.
8. Wang, J.; Liu, Y.; Song, H. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends. *IEEE Aerospace and Electronic Systems Magazine.* **2021**, *36 (3)*, 4–29. [Online] Available: https://doi.org/10.1109/MAES.2020.3015537.
9. De Cubber, G.; Petsioti, P.; Roman, R.; Mohamoud, A.; Maza, I.; Church, C. The COURAGEOUS Project Efforts Towards Standardized Test Methods for Assessing the Performance of Counter-Drone Solutions. In *Proceedings 11th Biennial Symposium on Non-Lethal Weapons*, **2023**, p. 44.
10. CEN Workshop Agreement - CWA 18150 - Unmanned aircraft systems - Counter UAS - Testing methodology. European Standardization Committee. **2024**. [Online] Available: https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa-18150.pdf
11. Van den Broek, B.; Van der Velde, J.; Van den Baar, M.; Nijsten, L.; Van Heijster, R. Automatic Threat Evaluation for Border Security and Surveillance. In *Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies III*; SPIE, **2019**, *Vol. 11166*, pp. 113–122. https://doi.org/10.5281/zenodo.3460244.
12. Baptista, M.; Fernandes, L.; Chaves, P. Tracking and Classification of Aerial Objects. In *Intelligent Transport Systems. From Research and Development to the Market Uptake*; Martins, A., Ferreira, J., Kocian, A., Eds.;

 doi:10.20944/preprints202503.2043.v1

INTSYS Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer, Cham, **2020**, *Vol. 310*. https://doi.org/10.1007/978-3-030-38822-5_18.

13. De Cubber, G.; Shalom, R.; Coluccia, A.; Borcan, O.; Chamrád, R.; Radulescu, T.; Izquierdo, E.; Gagov, Z. The SafeShore System for the Detection of Threat Agents in a Maritime Border Environment. In *IARP Workshop on Risky Interventions and Environmental Surveillance*, Les Bon Villers, Belgium, **2017**.
14. Doroftei, D.; De Cubber, G. Qualitative and Quantitative Validation of Drone Detection Systems. In *International Symposium on Measurement and Control in Robotics (ISMCR2018)*, Mons, Belgium, **2018**.
15. Coluccia, A.; Fascista, A.; Schumann, A.; Sommer, L.; Ghenescu, M.; Piatrik, T.; De Cubber, G.; Nalamati, M.; Kapoor, A.; Saqib, M.; Sharma, N.; Blumenstein, M.; Magoulianitis, V.; Ataloglou, D.; Dimou, A.; Zarpalas, D.; Daras, P.; Craye, C.; Ardjoune, S.; De la Iglesia, D.; Méndez, M.; Dosil, R.; González, I. Drone-vs-Bird Detection Challenge at IEEE AVSS2019. In *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, **2019**, pp. 1–7.
16. Coluccia, A.; Ghenescu, M.; Piatrik, T.; De Cubber, G.; Schumann, A.; Sommer, L.; Klatte, J.; Schuchert, T.; Beyerer, J.; Farhadi, M.; Amandi, R.; Aker, C.; Kalkan, S.; Saqib, M.; Sharma, N.; Daud, S.; Makkah, K.; Blumenstein, M. Drone-vs-Bird Detection Challenge at IEEE AVSS2017. In *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Lecce, Italy, **2017**, p. 1–6.
17. Li, C. J.; Ling, H. An Investigation on the Radar Signatures of Small Consumer Drones. *IEEE Antennas and Wireless Propagation Letters* **2017**, *16*, 649–652. https://doi.org/10.1109/LAWP.2016.2594766.
18. Mezei, J.; Molnar, A. Drone Sound Detection by Correlation. In *Proceedings of the 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics*; **2016**, pp. 509–518. https://doi.org/10.1109/SACI.2016.7507430.
19. Rozantsev, A. Vision-Based Detection of Aircrafts and UAVs. Master's Thesis, EPFL, Lausanne, **2017**. https://doi.org/10.5075/epfl-thesis-7589.
20. Andrai, P.; Radii, T.; Mutra, M.; Ivoevi, J. Nighttime Detection of UAVs Using Thermal Infrared Camera. *Transportation Research Procedia (INAIR)* **2017**, *28*, 183–190. https://doi.org/10.1016/j.trpro.2017.12.184.
21. Sit, Y. L.; Nuss, B.; Basak, S.; Orzol, M.; Wiesbeck, W.; Zwick, T. Real-Time 2D+Velocity Localization Measurement of a Simultaneous-Transmit OFDM MIMO Radar Using Software Defined Radios. In *Proceedings of the European Radar Conference (EuRAD)*, **2016**, pp. 21–24.
22. De Haag, M. U.; Bartone, C. G.; Braasch, M. S. Flight-Test Evaluation of Small Form-Factor Lidar and Radar Sensors for SUAS Detect-and-Avoid Applications. In *Proceedings of the IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, **2016**, pp. 1–11. https://doi.org/10.1109/DASC.2016.7778108.
23. De Cubber, G.; Berrabah, S. A.; Sahli, H. Color-Based Visual Servoing Under Varying Illumination Conditions. *Robotics and Autonomous Systems* **2004**, *47* (4), 225–249. http://dx.doi.org/10.1016/j.robot.2004.03.015.
24. Enescu, V.; De Cubber, G.; Cauwerts, K.; Sahli, H.; Demeester, E.; Vanhooydonck, D.; Nuttin, M. Active Stereo Vision-Based Mobile Robot Navigation for Person Tracking. *Integrated Computer-Aided Engineering* **2006**, *13* (3), 203–222. http://dx.doi.org/10.3233/ICA-2006-13302.
25. Unmanned Airspace. EU Framework Agreement for Counter Drone Devices Features Skywall Net Capture Solution. https://www.unmannedairspace.info/counter-uas-systems-and-policies/eu-framework-agreement-for-counter-drone-devices-features-skywall-net-capture-solution/, **2021**.
26. DroneWise Consortium. DroneWISE Project. https://dronewise-project.eu/, accessed 28/03/2023.
27. Jacoff, A. Guide for Evaluating, Purchasing, and Training with Response Robots Using DHS-NIST-ASTM International Standard Test Methods. In *Standard Test Methods for Response Robots*; National Institute of Standards and Technology, **2014**.
28. Doroftei, D.; Matos, A.; Silva, E.; Lobo, V.; Wagemans, R.; De Cubber, G. Operational Validation of Robots for Risky Environments. In *8th IARP Workshop on Robotics for Risky Environments*, **2015**.
29. De Cubber, G.; Doroftei, D.; Balta, H.; Matos, A.; Silva, E.; Serrano, D.; Govindaraj, S.; Roda, R.; Lobo, V.; Marques, M. Operational Validation of Search and Rescue Robots. In *Search and Rescue Robotics - From Theory to Practice*; InTech, **2017**. http://dx.doi.org/10.5772/intechopen.69497.
30. Doroftei, D.; De Cubber, G. Using a Qualitative and Quantitative Validation Methodology to Evaluate a Drone Detection System. *ACTA IMEKO* **2019**, *8* (4), 20–27.
31. Kouhestani, C.; Woo, B.; Birch, G. Counter Unmanned Aerial System Testing and Evaluation Methodology. In *Proceedings of SPIE 10184, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XVI*, **2017**, 1018408. https://doi.org/10.1117/12.2262538.
32. Church, C. Interpol Drone Countermeasure Exercise Report. Interpol, **2022**.

 doi:10.20944/preprints202503.2043.v1

33. EUROCAE. New working group: WG-115 / Counter UAS (C-UAS). https://www.eurocae.net/news/posts/2019/october/new-working-group-wg-115-counter-uas-c-uas/ **2019**
34. NATO. NCI Agency Holds NATO's Live-Testing Counter-Drone Exercise. https://www.ncia.nato.int/about-us/newsroom/nci-agency-holds-natos-livetesting-counterdrone-exercise.html, **2022**.
35. Kretschmann, T. A Standard for C-UAS - DIN 5452-9: Improving the quality of systems and creating a level playing field. *Security 2024*. **2024**.
36. International Standardisation Organisation. ISO/CD 16746 - Unmanned aircraft systems — Counter UAS — Quality and safety for users https://www.iso.org/standard/84801.html **2025**
37. International Standardisation Organisation. ISO/CD 16747- Unmanned aircraft systems — Counter UAS — Quality and safety for manufacturers https://www.iso.org/standard/84802.html **2025**
38. Brewczyński, K. D.; Życzkowski, M.; Cichulski, K.; Kamiński, K. A.; Petsioti, P.; De Cubber, G. Methods for Assessing the Effectiveness of Modern Counter Unmanned Aircraft Systems. *Remote Sensing* **2024**, *16* (19).
39. Petsioti, P.; Życzkowski, M.; Brewczyński, K.; Cichulski, K.; Kamiński, K.; Razvan, R.; Mohamoud, A.; Church, C.; Koniaris, A.; De Cubber, G.; Doroftei, D. Methodological Approach for the Development of Standard C-UAS Scenarios. *Open Research Europe* **2024**, *4* (240).
40. Mohamoud, A.; van de Pol, J.; van Heijster, R.; Masini, B.; van den Heuvel, M.; van Keeken, A.; Hildmann; H. A performance evaluation for systems for the detecting, tracking, and identification of illicit drones. *Proc. SPIE 13207, Autonomous Systems for Security and Defence*, **2024**.
41. Borghgraef, A.; Vandewal, M.; De Cubber, G. COURAGEOUS: Test Methods for Counter-UAS Systems. In *Proceedings SPIE Sensors + Imaging, Target and Background Signatures X: Traditional Methods and Artificial Intelligence*, **2024**, p. 131990D.