Check for updates

METHOD ARTICLE

Methodological Approach for the Development of Standard C-UAS Scenarios

[version 1; peer review: 2 approved with reservations, 2 not approved]

Paraskevi Petsioti[1], Marek Życzkowski[2], Konrad Brewczyński[2], Krzysztof Cichulski[2], Kamil Kamiński[2], Roman Razvan[3], Ali Mohamoud[4], Christopher Church[5], Alexios Koniaris[1], Geert De Cubber[6], Daniela Doroftei[6]

[1]Center for Security Studies (KEMEA), Athens, Greece
[2]Military University of Technology, Warsaw, Poland
[3]Protection and Guard Service, Bucharest, Romania
[4]Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek, Den Haag, Netherlands Antilles
[5]International Criminal Police Organization, Lyon, France
[6]Royal Military Academy, Brussels, Belgium

v1 **First published:** 30 Oct 2024, **4**:240
https://doi.org/10.12688/openreseurope.18339.1
Latest published: 30 Oct 2024, **4**:240
https://doi.org/10.12688/openreseurope.18339.1

Abstract

The integration of unmanned aircraft systems (UAS), commonly referred to as drones, into various sectors including agriculture, healthcare, and military operations has transformed industries and services. While drones offer numerous benefits, they have also been exploited by terrorists and criminals for illicit activities, such as smuggling and surveillance. Incidents involving drones flying over restricted airspaces or sensitive locations have highlighted the vulnerabilities of critical infrastructure and limitations of current law enforcement capabilities. To address these challenges, there is a growing need for effective counter-UAS (C-UAS) systems including detection, tracking, and identification technologies. However, evaluating the capabilities of these systems poses a significant challenge, leading to the demand for standardized test methodologies. The COURAGEOUS project seeks to fill this gap by developing standardized scenarios covering various use cases, such as airport security, critical infrastructure protection, and border security. These scenarios are informed by a systematic approach involving a literature review, analysis of previous incidents, assessment of current C-UAS frameworks, and gathering feedback from end users. The resulting standardized test methodology aims to enhance the understanding of C-UAS system capabilities, improve preparedness against evolving threats, and facilitate the global dissemination of project results. Through validation trials and feedback from law

Open Peer Review

Approval Status ? ✗ ? ✗

	1	2	3	4
version 1 30 Oct 2024	? view	✗ view	? view	✗ view

1. **Tijeni Delleji**, Science and Technology for Defense Lab (STD), Aouina, Tunisia
2. **Omar Alharasees**, Budapest University of Technology and Economics, Budapest, Hungary
3. **Sofia Mateou**, Prince Sultan University, Riyadh, Saudi Arabia
4. **Abdulhadi Shoufan**, Khalifa University, Abu Dhabi, United Arab Emirates

Any reports and responses or comments on the article can be found at the end of the article.

enforcement agencies, the COURAGEOUS project strives to contribute to a broader network of counter-UAS initiatives, ultimately enhancing the lower airspace security.

Plain Language Summary

The use of drones, or unmanned aircraft systems (UAS), has become common in sectors like agriculture, healthcare, and the military, offering many benefits. However, drones are also being misused for illegal activities, such as smuggling and unauthorized surveillance. This misuse poses risks to critical infrastructure and exposes gaps in current law enforcement abilities to counter these threats. To address these issues, there is a growing focus on counter-UAS (C-UAS) systems, which help detect, track, and identify drones. However, testing these systems effectively is challenging. The COURAGEOUS project aims to create standardized testing scenarios for different use cases, including airport and border security. By analyzing past incidents, reviewing existing C-UAS systems, and gathering feedback, the project hopes to establish a reliable testing method that can improve drone threat response. Ultimately, this will help strengthen airspace security and promote international collaboration in counter-UAS efforts.

Keywords

C-UAS, methodology, standardization, scenarios, factors, validation

Corresponding author: Paraskevi Petsioti (p.petsioti@kemea-research.gr)

Author roles: Petsioti P: Conceptualization, Formal Analysis, Methodology, Writing – Original Draft Preparation; **Życzkowski M**: Writing – Review & Editing; **Brewczyński K**: Writing – Review & Editing; **Cichulski K**: Writing – Review & Editing; **Kamiński K**: Writing – Review & Editing; **Razvan R**: Writing – Review & Editing; **Mohamoud A**: Writing – Review & Editing; **Church C**: Writing – Review & Editing; **Koniaris A**: Writing – Review & Editing; **De Cubber G**: Project Administration, Writing – Review & Editing; **Doroftei D**: Project Administration

Competing interests: No competing interests were disclosed.

Grant information: This project has received funding from the European Union's Internal Security Fund Police, ISFP-2020-AG-CUAS, UAS countermeasures under grant agreement No 101034655 Building a common understanding of the effectiveness of counter-UAS solutions (COURAGEOUS).

Copyright: © 2024 Petsioti P *et al*. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Petsioti P, Życzkowski M, Brewczyński K *et al.* **Methodological Approach for the Development of Standard C-UAS Scenarios [version 1; peer review: 2 approved with reservations, 2 not approved]** Open Research Europe 2024, **4**:240 https://doi.org/10.12688/openreseurope.18339.1

First published: 30 Oct 2024, **4**:240 https://doi.org/10.12688/openreseurope.18339.1

Introduction

Over the last few decades, unmanned aircraft systems (UAS) and drones have been used in various shapes and sizes, ranging from handheld micro-UASs to medium-sized tactical systems to fully grown and Remotely Piloted Aircraft (RPA)[1]. UAS have found applications in agriculture, health, and military purposes[2,3]. Aside from their practical uses, such as search and rescue, surveillance, traffic monitoring, weather monitoring, firefighting, drone-based photography, videography, even delivery services, to name a few, drones continue to make headlines for their ability to additionally engage in all manner of recreational uses[4–6]. Unfortunately, terrorists and criminals are proving as innovative as their industry counterparts in finding novel uses for UAS[7]. The increasingly common use of drones by terrorists to launch strikes abroad has raised concerns that domestic male factors may plan and execute similar attacks. Meanwhile, some criminal actors use drones to smuggle drugs across borders and prisons or to support their nefarious enterprises[8]. These incidents, as well as others (which include unauthorized flights over sports stadiums or in controlled airspaces near airports), have exposed both the vulnerability of sensitive facilities and critical infrastructures to hostile or recklessly operated UAS, as well as serious shortcomings in the capabilities of law enforcement and national security agencies to address these threats[9].

The need to protect people, infrastructure, and assets signifies the importance of counter Unmanned Aerial Systems, including detection, tracking, and identification systems[1]. As the availability of UAS or drones increases, law enforcement agencies face the unique challenge of regulating access to the lower airspace. Although commercial solutions are available, the evaluation of the capabilities of these systems is challenging. This results in end users struggling to match appropriate tools to specific use cases. 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[10].

The operational needs and subsequent operational capability gaps that these standardized scenarios are called upon to address stem from the limitations of the C-UAS. Specifically, these limitations refer to the technical and non-technical obstacles faced by the detection and mitigation technologies used for C-UASs[11].

To address this issue, the COURAGEOUS project aimed to create a standardized test methodology for detecting, tracking, and identifying malicious drones using countermeasure systems to safeguard the lower airspace. The proposed methodology relies on standard user-defined scenarios, covering diverse use cases, such as prison and airport security, critical infrastructure protection, border security, and combating drugs and human trafficking. COURAGEOUS end-users will extract the operational and functional performance requirements for these scenarios, forming the basis for developing a comprehensive test methodology. This methodology enables fair qualitative and quantitative comparisons of different counterUAS systems. Validation trials conducted in Greece, Belgium, and Spain confirm the effectiveness of the test methodology.

In the short term, the COURAGEOUS standardized test methodology will enhance LEAs' understanding of counterUAS system capabilities. This knowledge will not only benefit COURAGEOUS partners but also contribute to the broader EU network of LEAs and the global dissemination of project results, which will be facilitated by the International Criminal Police Organization (INTERPOL).

Methods

The methodology for developing standard scenarios in the COURAGEOUS project involves four key steps (Figure 1), each aimed at systematically gathering information and insights to inform the creation of scenarios for countering unmanned aerial system (UAS) threats. A more detailed description of each step is provided below:

1. *Literature Review / Need for Standardization Scenarios*:
This step involved a comprehensive literature review to define the project scope. The focus is on collecting relevant literature related to UAS threats and analyzing them to identify the need for standardization scenarios. This initial review helps establish a foundation for the knowledge and understanding of existing research and practices in the field.

2. Previous Incidents & Identification of Gaps:
Building upon the literature review, this step involves analyzing previous incidents involving UAS threats. By studying

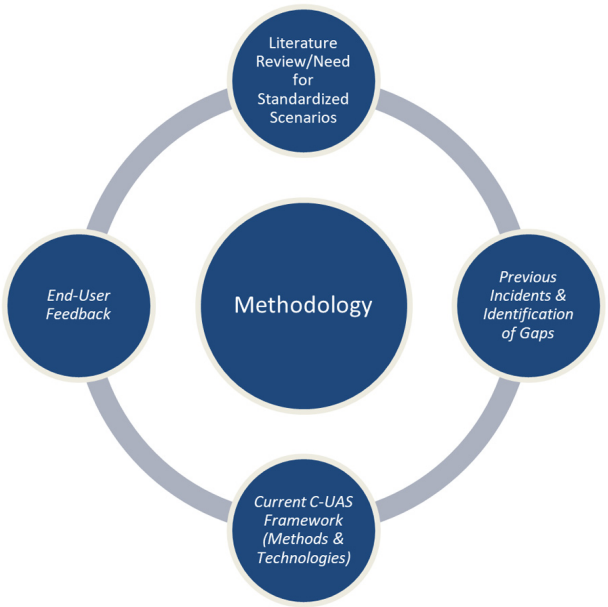

Figure 1. Methodology diagram.

past incidents, the project team aims to identify the common factors associated with these incidents and the gaps in the existing approaches to countering them. Recognizing patterns from past incidents is crucial for developing effective strategies for mitigating future threats.

3. Current C-UAS Framework (Methods & Technologies):
In this step, the project team examined the current framework of the (C-UAS) methods and technologies. This examination helps understand the existing landscape of tools, techniques, and technologies used for countering UAS threats. By assessing the current state-of-the-art, the team can identify areas for improvement and innovation in the C-UAS capabilities.

4. End-User Feedback:
This step involves gathering feedback from end users, including security authorities and other stakeholders involved in countering UAS threats. A questionnaire was created and distributed to COURAGEOUS partners, particularly end users. The feedback obtained helps to identify specific factors that should be considered when developing C-UAS scenarios. By incorporating end-user perspectives, scenarios can be tailored to meet the practical needs and requirements of those implementing them.

The integration of these four techniques ensures a comprehensive and systematic approach to scenario development that is applicable to various environments and security authorities. By selecting one scenario for each execution, the project aims to focus on developing high-quality relevant scenarios to address UAS threats effectively. Each step serves the specific purpose of gathering information and insights, ultimately contributing to the overall effectiveness of the scenario collection process.

Need for standard scenarios/literature review

The rapidly expanding C-UAS industry serves as a crucial defense against rogue UAS activity, with systems designed to locate, track, and neutralize such threats. This demand extends across the commercial and law enforcement sectors, owing to the escalating threat posed by unidentified UAS in civil and law enforcement scenarios. Despite this, there remains an absence of international standards for C-UAS design, and not all systems perform as advertised, necessitating the development of global standards and policies as technology evolves[12]. Predictions estimate the global C-UAS market will reach two billion dollars by 2024, as highlighted in a comprehensive report titled "Report on 537 Anti-Drone Systems Shows How Wild the Market Has Become," showcasing a wide array of anti-drone technologies[13]. Notably, Bard College has contributed to the discourse on counterdrone Systems[14].

C-UAS systems encounter specific challenges when dealing with small unmanned aerial vehicles (sUAVs), where detection plays a crucial role in providing initial threat information[15]. Various approaches, such as radiofrequency (RF) detectors[16], active radars[17], optoelectronic (OE) detectors[18,19] coupled with AI-based classification systems[20], LIDAR detectors[21], and acoustic detectors[22], offer early warning information about incoming UAVs. A methodology for evaluating different types of detectors, accompanied by an experimental test using the active radar system ReGuard developed by Retia, was formulated[23]. Furthermore, Doroftei[24] presented a test methodology for qualitatively and quantitatively assessing the performance of multimodal drone detection systems. However, this test method focused on one specific detection system[25] and lacked generality to enable its application to a wide range of C-UAS systems.

Effective C-UAS solutions require collaboration among numerous stakeholders, as demonstrated by the European Commission's Joint Research Centre (JRC) in its development of a handbook based on experience gained from the DRONE project[26]. This collaborative effort involved targeted consultations and workshops with key stakeholders, providing advice on safeguarding against malicious UAS activities and offering guidelines across various stages, from detection to neutralization. These efforts align with the Commission's C-UAS package, announced under the Commission communication 'A drone strategy 2.0, for a smart and sustainable unmanned aircraft ecosystem in Europe[27].

Continuing its support, the JRC has produced two handbooks, one outlining a five-phased approach to C-UAS solution development, and the other containing recommendations for assessing risks associated with the malicious use of UAS[28]. Additionally, a paper titled "The Methodology of Counter-UAS System Comparison" aimed to develop a method for comparing UAS detection systems, ensuring compatibility with diverse situations[29].

By harmonizing European legislation and integrating unmanned aircraft systems into the common airspace (U-space), addressing unauthorized UAS operations in restricted areas is imperative. The paper titled "Procedures for Prevention of Unauthorized Incursion into UAS Geographical Zones" aims to establish a methodology and verify its functionality for intervening against unauthorized drone intrusion[30]. However, during the literature review, limited literature was found on the methodology for developing standard scenarios for C-UAS testing.

UAS have evolved significantly in size and application, raising concerns regarding their misuse by criminals and terrorists. C-UAS aims to address these threats but faces various operational needs and capability gaps[31] (Table 1). Project COURAGEOUS collected data on over eight hundred and twenty-three drone incidents globally, revealing gaps and needs in the current technical countermeasures used by authorities[32]. While most incidents occur in restricted areas, free-access areas remain susceptible to illegal activities owing to challenges in deploying surveillance and detection technologies, which are often hindered by legislative barriers.

Although custom drones are not predominant in reported incidents, they pose a significant threat because of their

Table 1. Operational Needs and Capability Gaps.

Operational Needs and Capability Gaps.	Explanation
Minimizing False Negatives and Positives	C-UAS detection systems must balance sensitivity to detect all drones with minimizing false positives and false negatives to ensure effective operation.
Distinguishing Legitimate and Illegitimate UAS Use	In environments with common drone use, C-UAS operators need to differentiate between legitimate and rogue drones quickly and reliably.
Meeting Response Window Constraints	Counter-drone operators have a limited time to assess and respond to potentially malicious drones, and the increasing speed of commercial drones further reduces this response window.
Improving Interdiction Effectiveness	Various interdiction methods have limitations, such as the potential destructiveness of physical capture and risks associated with high-power Electromagnetic Pulse (EMP), Radio Frequency (RF) jamming, hacking, and spoofing.
Avoiding Interdiction Hazards	C-UAS techniques can be dangerous, posing risks to by-standers and legitimate communication systems, emphasizing the need for precision and safety.
Keeping up with UAS Technology Advances	The dynamic nature of drone technology requires C-UAS systems to adapt to a wide range of drone shapes, sizes, and capabilities.
Tackling the lack of Operational Data	The absence of information on the performance of deployed C-UAS systems makes it challenging for users to make informed decisions.
Facing C-UAS Costs	Counter-drone technology incurs significant expenses, including per-sonnel training, maintenance, and operational costs.
Achieving Legality	Legal uncertainties and ambiguities surround the use of C-UAS systems, with existing laws often inadequately addressing this evolving technology.
Dealing with the lack of Standards	The absence of international standards for C-UAS design and use raises concerns about performance variations, safety, and potential misuse.
Protecting Privacy	Counter-drone detection systems, as forms of surveillance technology, pose privacy risks if misused or if data handling practices are inadequate.

ability to evade certain detection components with custom setups, thereby presenting challenges for the C-UAS systems. Additionally, the capability of drones to carry various payloads, including weapons or hazardous substances, presents a significant challenge for detection systems[32,33].

Addressing these operational needs and capability gaps necessitates the development of standardized scenarios to improve the effectiveness of C-UAS systems in countering malicious actions launched by UAS.

Previous incidents & identification of gaps

The escalating occurrence of drone incidents has necessitated law enforcement agencies (LEAs) to adapt their responses to combat the diverse threats posed by criminals, uninhibited hobbyists, and inexperienced or reckless drone pilots. Through COURAGEOUS research, which meticulously analyzed over 800 global drone incidents spanning from May 2015 to August 2021, a clear need for education and training of responders has emerged. The analysis underscores the prevalence of uninhibited drone pilots as the most common threat actors, often pushing the boundaries of drone capabilities to infiltrate restricted areas or to satisfy their curiosity.

These incidents are meticulously categorized into three primary areas (airports, law enforcement, first responders, and private/non-corporate), revealing discernible patterns and characteristics. Most incidents occur in urban settings, predominantly during daylight hours, and involve multi-rotor UAVs equipped with a single commercial camera payload. Notably, most incidents are of marginal severity and cause disruptions rather than catastrophic outcomes. Europe and the United States bear the brunt of these incidents, whereas the Middle East confronts the threat of terrorism by employing UAVs[34].

Further examination of more than 200 drone-related incidents in Europe shed light on the gaps and challenges prevalent in current technical countermeasures and offensive UAV capabilities. These challenges include the limitations of Drone Threat Intelligence (DTI) systems, difficulties encountered in congested urban environments, lack of weather-related preferences for illegal drone activities, potential complications arising from the presence of other UAVs, and prevalence of incidents in non-restricted areas. Additionally, the emergence of custom drones and diverse payloads present formidable obstacles for DTI systems[35–37].

However, despite these challenges, DTI systems exhibit strengths, particularly in rural locales with favorable lighting conditions during daytime incidents, a preference for multirotor UAVs, incidents occurring in restricted areas under surveillance, and a predominance of off-the-shelf commercial

drones that are relatively easier to detect. It is imperative to address the identified challenges comprehensively to bolster the effectiveness of countermeasures against malicious drone activities.

Current C-UAS framework (methods & technologies)

The COURAGEOUS project conducted an exhaustive examination of C-UAS frameworks, focusing specifically on the methods and technologies utilized for detecting, tracking, and identifying unmanned aerial systems (UAS). The analysis encompassed 260 anti-drone systems, shedding light on prevalent technologies and their operational characteristics[38–40].

Detection Technologies: Frequency monitoring has emerged as the most commonly employed technology, utilized by 35.4% of the systems under review. Following closely are Microwave radar (30.4%), visible-light cameras (25.8%), and thermal cameras (19.6%). Other technologies included infrared (1.15%), lidar (2.3%), and acoustic sensors (6.5%).

Shortcomings of Systems: Several systems lack the capability for 24/7 operation, particularly during nighttime. Certain technologies, such as infrared sensors and visible-light cameras, exhibit limitations in terms of the range and image quality. Microwave radar analysis requires approval, and is susceptible to atmospheric conditions. Moreover, acoustic- and radio-frequency-based systems depend on the background noise level in the testing environment.

Operability and Mobility: The majority of C-UAS systems (74%) are designed for permanent installation, with a substantial portion also offering mobile versions (48%). In addition, some systems could be mounted on vehicles or trailers (17%).

Combination of Technologies: Multispectral systems are regarded as the most effective for defining alarm signals. While the majority of systems rely on a single technology (53%), with frequency monitoring being the most prevalent (31.4%), a notable percentage utilizes multi-technology configurations, integrating various detection and tracking technologies.

Challenges and Considerations for Standardization: This analysis underscores the necessity of a standardized methodology that considers detection effectiveness, range, resistance to false indications, system functionality in diverse scenarios, and resilience to changing environmental conditions. Technologies can be categorized as either active (e.g., radar and lidar) or passive (e.g., cameras), with passive technologies dominating C-UAS solutions.

Environmental Impact on Technologies: Environmental factors, such as rain and strong sunlight can disrupt the operation of certain technologies. For instance, rain may impede the functioning of Visible Imaging Sensor (VIS) cameras and acoustic sensors, whereas strong sunlight can affect VIS, thermal imaging cameras, infrared (IR) sensors, and lidars. However, the frequency monitoring remains unaffected by rain or fog.

Object Identification Process: The object identification process faces numerous challenges, including weather conditions, lighting, distance, object size, and terrain-covered zones. A clear definition of the movement of a test object within the detection field is crucial for accurate testing.

In conclusion, this study underscores the complexity involved in selecting and implementing C-UAS technologies, highlighting the significance of a standardized methodology that considers various operational parameters and environmental conditions[3,41].

Law enforcements feedback

A pivotal step involves the creation and circulation of a comprehensive questionnaire among the end users within the consortium. This questionnaire aimed to gather insights into the prevalent factors and components inherent in the UAS threat scenarios. By leveraging the collective expertise of stakeholders, the objective is to discern and validate the parameters crucial for shaping these scenarios, thereby ensuring their efficacy in addressing potential UAS threats[33,42].

The overarching goal was to ascertain the requisite level of detail necessary to effectively categorize these scenarios. Through rigorous data collection and analysis, this project sought to gain a nuanced understanding of the diverse contexts and circumstances surrounding UAS attacks. By collating inputs from end-users across various domains, the aim is to capture a comprehensive spectrum of potential threat scenarios encompassing different environments, operational contexts, and adversary behaviors.

This meticulous process of soliciting feedback and integrating diverse perspectives underscores a project's commitment to develop robust and adaptable standard scenarios. By aligning these scenarios with the identified parameters and stakeholders' real-world experiences, the COURAGEOUS project endeavors to enhance preparedness and response capabilities against UAS threats. Ultimately, the initiative strives to provide a structured framework that enables stakeholders to anticipate, mitigate, and effectively manage the evolving landscape of UAS-related risk.

It is emphasized that all these components must be included in scenario development, regardless of their significance, and that a scoring procedure is not suitable for this activity.

The responses collected through the questionnaire supported the creation of a UAV threat scenario element pool, thereby contributing to the definition of the standard threat scenarios.

Development of standard scenarios

Following the structured approach outlined in the methodology for developing standard scenarios in the COURAGEOUS project, Table 3 delineates the components that combine incidents and scenarios. This table serves as a comprehensive reference, and presents a detailed breakdown of the primary factors associated with incidents and their respective

Table 2. Parameters extracted from the questionnaire.

Parameters	Explanation
Target	Identifying different objectives and targets of malicious UAVs.
Environment	Considering the area or environment where the UAS threat scenario occurs.
Lighting Conditions	Recognizing lighting conditions as a critical component affecting UAS threat scenarios.
Weather Conditions	Understanding how weather conditions impact both malicious UAVs and deployed countermeasures.
Presence of Other Aircrafts/UAVs	Considering the influence of nearby aircraft on UAS threat scenarios and implemented countermeasures.
Type of UAV	Recognizing the contribution of the UAV type to the development of a UAS threat scenario.
Number of UAVs	Acknowledging the critical role of the number of UAVs in UAS threat scenarios.
Custom or Commercial	Assessing how the manufacturing method of the UAS affects the risk level of a threat scenario.
Dimensions of UAV	Considering the physical dimensions of the UAV, including wingspan and rotor characteristics.
Maximum Take-Off Mass of UAV	Recognizing the impact of the maximum take-off mass on UAS threat scenarios.
Flight Mode	Understanding how the pilot's navigation method, or flight mode, contributes to the threat scenario.
Payload	Identifying the payload carried by the UAV and its role in defining mission objectives.
Altitude	Considering the altitude at which the UAV operates as a component of the threat scenario.
UAV Speed	Recognizing the impact of UAV speed on risk levels, prevention, and countermeasures.
Radio Frequencies	Identifying the radio frequencies used for remote control and video streaming as components of the UAS threat scenario.
Flight Behavior	Assessing the trajectory and behavior of the UAV during flight, which can affect established countermeasures.

subcategories. For example, within the weather factor category, the subcategories encompass various weather conditions such as Sunny, Cloudy, Rainy, Foggy, Windy, Stormy, Smoke, Dusty, Snowy, and Clear.

By systematically categorizing these factors and subcategories, the table facilitates a thorough understanding of the diverse elements that may influence incident occurrence and scenario development. Each factor and its associated subcategories provide valuable insights into the multifaceted nature of UAS-related incidents, encompassing a broad spectrum of environmental, operational, and contextual considerations.

This structured approach not only enables comprehensive documentation of incident characteristics, but also lays the groundwork for defining standardized scenarios that reflect real-world scenarios encountered by stakeholders. By providing a clear and organized framework for analyzing and categorizing incident components, Table 3 serves as a valuable tool for guiding the development of standard scenarios within the COURAGEOUS project, ultimately enhancing preparedness and response capabilities against UAS-related threats.

In the formulation of a standard scenario within the COURAGEOUS project, the pilot's intention is recognized as a critical factor, distinguishing between deliberate and accidental actions. The subcategories of the pilot's intention encompass various motivations, ranging from negligence to criminal or terrorist intent[34,43].

Under negligence, two distinct subcategories are identified:

Clueless Individuals: Pilots who are unaware of or unfamiliar with regulations fly inadvertently over sensitive areas due to a lack of knowledge.

Careless Individuals: Pilots who are aware of regulations but violate them unintentionally, flying over sensitive areas without disruptive intentions.

Moving to gross negligence, two additional subcategories are outlined:

Reckless Individuals: Pilots who knowingly disregard regulations for personal or professional gain, causing disruption.

Table 3. Scenario Factors.

Target	Weather	Type of UAV	Maximum take-off mass of UAV	Altitude	UAV Speed	Environment	Lighting Conditions	Presence of other aircrafts/ UAVs in the nearby airspace	Number of UAVs	Flight Mode	Radio Frequencies used for Remote Control and / or Video Stream	Flight Behaviour	Pilot Location	Payload	Custom or Commercial	Dimensions of UAV	Terrain	EM Environment	Birds	Vegetation	UAV Signature
Critical Infrastructure	Sunny	Multirotor	<250g	0-5m	0-10km/h	Rural	Sunrise	Not Classified	1	Manual	2.4GHz	Direct flight	Known	Optical camera	Recreational custom-made UAS	<30cm	Flat	Rural	Low Bird presence	None	Strong
Government Building	Cloudy	Fixed Wing	<900g	5–20m	10–30km/h	Suburban	Sunset	Not Controlled	2	GPS	5.8GHz	Obscured	Unknown	LiDAR	Wrong-doing custom-made UAS	30–50cm	Irregular	Suburban	Normal Bird presence	Low	Normal
VIP	Rainy	Flapping-wing Ornithopters	<4kg	20-50m	30-60km/h	Urban	Daylight	Own Fleet	Swarm	Waypoints	RC model aircraft frequencies (depending on national regulations)	Drop from High Altitude		Thermal sensor	Commercial	50–70cm	Mountainous	Urban	High Bird presence	Average	Low
Public Event	Foggy	Gliders	<25kg	50–100m	<60 km/h		Darkness	Friend		Inertial Navigation Systems	4G/LTE			Explosives/ IEDs		>1m		Dense/ Crowded		Meadowland	None
	Windy	Single Rotor	<100kg	100–120m	60–120 km/h			Authorized		4G/LTE	Other			Gun						Wood / Forest	
Urban - Not Specified	Stormy	Hybrid	>100kg	>120m	120<160 km/h			Stolen						CBRN							
Border Means of Transportation	Smoke				>160km/h			Alleged Infringer						Objects for Commercial Distribution							
	Dusty							Threat			None			Sprayers							
	Snowy							Escaped						Noise Generators							
	Clear							Neutralized						Jamming Devices							
														Different Domestic Payloads							
														Dazzling Laser							
														Illicit Package							

Activists/Protesters: Pilots who, whether aware of regulations or not, actively use drones to disrupt, potentially as a group, without harming human lives.

Finally, the criminal/terrorist motivation category encompasses pilots deliberately seeking to use drones for disruption, disregarding human life and property, and criminal or terrorist motivations.

Table 3 serves as a comprehensive reference, identifying and describing the factors that could constitute a scenario, including the pilot's intention. The next phase in developing standard scenarios involved combining these factors with the pilot's intent. A unique scenario can be defined by selecting specific values for the pilot's intent and each factor. This approach ensures adaptability to various users, allowing the creation of multiple scenarios based on specific selections, thereby enhancing the preparedness and response capabilities against a diverse range of UAS-related threats[44,45].

Standard scenarios

For the COURAGEOUS project requirements, ten standard scenarios were devised and categorized into three main groups (Figure 2):

- Sensitivity Sites/Critical National Infrastructure
- Public space protection/events and
- Border Protection (land – maritime).

Each scenario provides a real-world event example, offering an overview of the operational context and its limitations. These non-technical high-level representations aim to portray events of interest from an LEA perspective, illustrating the threat and problem spaces through narrative examples. These scenarios, along with the use cases, guide technical developments that influence technological demonstrations, trial designs, and evaluations.

In the first scenario, the test was conducted in a prison area with diverse surroundings such as small trees, private houses, and public roads. A manually operated Class I mini-category multirotor UAV carries a drug payload and takes off from a concealed position, crossing a prison fence. Notably, a "friendly" UAV is also airborne, making this scenario pertinent for addressing concerns regarding careless use of UAVs near airports. In the second scenario, the setting shifts to an airport area featuring a Class I fixed-wing UAV with an optical camera payload. This UAV operates autonomously, contending with general aviation activities, as it attempts to breach airport limits. This scenario addresses security challenges inherent in high-traffic airport environments. The third scenario involves a nuclear power plant located in an isolated rural area. During the night and under cloudy weather conditions, a custom-made multirotor UAV with an explosive payload autonomously takes off with the aim of approaching a nuclear plant via controlled waypoints. The relevance of this scenario lies in the imperativeness of securing critical infrastructure to protect against external threats. In the fourth scenario, which was situated in a large urban area, three UAVs were employed for physical attacks during an afternoon event. These UAVs, equipped with video equipment to coordinate the attack, target VIP at different frequencies. This scenario underscores the significance of security measures against potential criminal

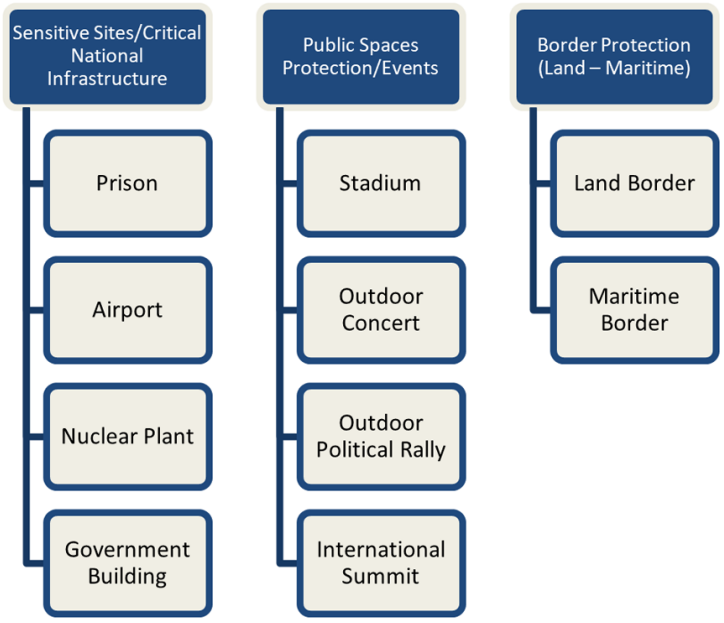

Figure 2. Standard Scenarios per category.

activity during major urban events. The fifth scenario occurred at a suburban stadium during a concert where a custom-made multirotor UAV with an aerosol-dispersing device disrupted the event. This highlights the need for robust security protocols to counter potential threats during large public gatherings. In the sixth scenario, during an outdoor concert in a bustling urban area, a non-friendly UAV equipped with a dazzling laser payload is detected and destroyed. This scenario emphasizes the importance of security measures against unauthorized UAVs in crowded settings. The seventh scenario occurs in the middle of a city during an authorized rally, when a commercial multirotor UAV carrying a noise generator payload disrupts the event. This exemplifies how criminal organizations may employ UAVs to induce panic and disturbance during public gatherings. Moving on to the eighth scenario, set at a historical international summit, a commercial fixed-wing UAV was utilized by a terrorist organization to create panic. The UAV autonomously approaches the VIPs and explodes, thereby releasing shrapnel. This underscores the significance of security measures for counteracting potential terrorism during crucial international events. In the ninth scenario, positioned at the land border, a custom-made multirotor UAV drops packages in a forested area, highlighting the challenges of combating trafficking activities at the border. Finally, the tenth scenario unfolds at the sea border, where a commercial multirotor UAV is used for surveillance to avoid coast guard boats during immigrant boat crossings. This scenario underscores the need for effective border control and surveillance by using UAVs.

These scenarios are realistic representations within the C-UAS domain, involving multiple actors, events, and activities and addressing various use cases. The presentation of standard scenarios followed the template used by the consortium partners, incorporating incident factors. Abstract Use case scenarios were described for specific areas without defining the interaction between the COURAGEOUS system and the user. The factors outlined in Table 2 were utilized to construct scenarios, with the consortium carefully selecting factors for adaptability and comprehensive coverage of the DTI system capabilities.

Methodology evaluation

The initial evaluation of standardized scenarios involved active participation from consortium members and law enforcement agencies (LEAs) within the consortium. The development process for these standard scenarios underwent rigorous discussion and received approval from the consortium. Ultimately, ten Standard COURAGEOUS Scenarios were formally presented and endorsed by the end users and consortium. Subsequently, further evaluation of these scenarios was conducted in a specialized workshop attended by consortium end users and relevant stakeholders.

During the workshop, participants engaged in discussions regarding standardized procedures within the methodology. Following these discussions, a questionnaire was distributed to gather feedback from participants.

The questionnaire comprised three key questions aimed at assessing participants' perspectives and satisfaction with the standardized scenario methodology. First, participants were asked to indicate their organization's level of interest in the Standardized Scenario Methodology, with response options ranging from "Slightly interesting" to "Extremely interesting." The majority of respondents (80%) rated their interest level as either "Very interesting" or "Extremely interesting."

Second, participants were asked whether the scenarios met their requirements, with response options being "Yes," "No," or "Maybe." Maybe. The overwhelming majority (80%) indicated that the scenarios met their requirements.

Finally, participants were requested to score their agreement with the extent to which standardized procedures were followed for each scenario. The scoring options ranged from strongly disagree' to strongly agree. ' The resulting responses, depicted in Table 4, illustrate the consensus among participants regarding adherence to standardized procedures for each scenario.

Results

In this article, validation trials were conducted across multiple locations, including Greece, Belgium, and Spain. These trials confirmed the effectiveness of the standardized testing methodology developed by the project. For instance, the methodology enabled the fair, qualitative, and quantitative comparison of various counter-UAS (C-UAS) systems under different operational environments (e.g., prisons, airports, critical infrastructures). The validation trials produced key data that demonstrated how well these systems performed in diverse use cases like prison area drug smuggling or airport security breaches.

Use cases

The project created 10 standard scenarios covering areas like critical infrastructure protection, public event security, and border control (both land and maritime). For example, one scenario involves a drone carrying an explosive payload attempting to breach a nuclear power plant, which simulates a real-world threat to critical infrastructure. These scenarios not only address various threat levels but also inform the broader design of C-UAS systems, making them more adaptable to different real-life applications. This section should highlight how these scenarios reflect the COURAGEOUS project's practical implementations, even before full validation is completed.

Implementation expectations

The COURAGEOUS project provides a structured approach to scenario development, based on insights from over 800 global drone incidents and extensive feedback from law enforcement agencies (LEAs). The methodology aims to address key gaps in C-UAS capabilities, such as improving the detection of small, custom drones and reducing false positives/negatives in detection systems. These standardized scenarios offer a framework for future research and system development, ensuring

Table 4. Evaluation Question 3 – Results.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Prison	-	-	-	60%	40%
Airport	-	-	-	80%	20%
Nuclear Plant	-	-	-	80%	20%
Government Building	-	-	-	40%	60%
Stadium	-	-	-	40%	60%
Outdoor Concert	-	-	-	60%	40%
Outdoor Political Rally	-	-	-	40%	60%
International Summit	-	-	20%	40%	40%
Land Border	-	-	20%	40%	40%
Maritime Border	-	-	20%	40%	40%

C-UAS systems can be evaluated consistently across different countries and operational contexts. Peer review will further help refine and adapt the methodology, adding value to the field by promoting international collaboration and enabling the global dissemination of results through bodies like INTERPOL.

Conclusions

In conclusion, the COURAGEOUS project endeavors to establish a unified understanding among Member State authorities regarding the effectiveness of technical systems designed for detecting, tracking, and identifying noncooperative drones. This project focused on creating a uniform test methodology using a set of standard scenarios that describe situations that require protection against malicious UAS. The key outcomes of COURAGEOUS research include a collection of standard scenarios and use cases, which forms the basis for future trials in the project. The project methodology involves a comprehensive approach, starting with a literature review to define the scope and identify the need for standardization scenarios. The analysis of previous incidents, identification of gaps, examination of the current C-UAS framework, and an end-user questionnaire contributed to the development of standard scenarios. The identified parameters from the questionnaire covered a wide range of factors, including the target, environment, lighting conditions, presence of other aircraft, and more, ensuring a holistic approach to the scenario development. The evaluation process involved both consortium members and LEAs within the consortium to ensure the relevance and effectiveness of standardized scenarios. Ten standard scenarios were developed and endorsed by end users, representing diverse use cases such as critical infrastructure protection, public event security, and border protection.

The COURAGEOUS project recognizes the evolving nature of drone technologies and challenges faced by LEAs in countering malicious drone activities. By addressing operational needs and capability gaps through standardized scenarios, the project aims to enhance the effectiveness of C-UAS in responding to potential threats. The developed scenarios not only serve as a foundation for upcoming trials, but also contribute to the broader EU network of LEAs, facilitating knowledge sharing and dissemination of project results. Moving forward, a standardized test methodology and scenarios will be applied to a broader range of commercial C-UAS systems to provide valuable quantitative data for informed design decisions.

Looking ahead, the COURAGEOUS test methodology will be applied to a broader range of commercial counter-UAS systems in the medium to long term. This extended testing will provide developers with quantitative data, enabling them to make informed design decisions based on the performance metrics.

Abbreviations

The following abbreviations are used in this paper:

CBRN	Chemical, Biological, Radiological, or Nuclear substance
C-UAS	Counter – Unmanned Aerial System
DTI	Detection-Tracking-Identification
EC	European Commission
EMP	Electromagnetic Pulse
EU	European Union
IEDs	Improvised Explosive Devices
IR	Infrared

ISFP	Internal Security Fund Police
LEAs	Law Enforcement Agencies
OE	Opto Electronic
RF	Radio Frequency
sUAV	Small Unmanned Aerial Vehicles
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
VIS	Visible Imaging Sensor

Ethics and consent

The participants who responded to the questionnaire are partners (end-users) of the EU-funded project entitled COURAGEOUS. An informed consent procedure was strictly followed to ensure voluntary participation and lawful data processing. In line with research ethics, all respondents were fully informed about the study and provided their consent prior to the completion of the questionnaire. Specifically, participants were asked to carefully review the Information Sheet, which detailed, among others, the study's purpose, participants' rights and contact details of the lead researchers. Informed consent was obtained through tick boxes, freely checked by the participants after having reviewed this information.

Data availability statement

Due to the sensitive nature of the COURAGEOUS project and the limited dissemination of relevant project reports, strict limitations are placed on the release of survey data. Public access to this data may pose privacy and security (misuse) risks, potentially compromising data protection and confidentiality and exposing sensitive information relating to the project. Requests for data access can be submitted to the authors via email for consideration.

While the sensitive nature of the COURAGEOUS project imposes some restrictions on data sharing, we are committed to supporting reproducibility. Researchers interested in accessing anonymized data from the validation trials, such as performance metrics or scenario descriptions, can request access by contacting the corresponding author. This process is designed to protect participant confidentiality while enabling further research and validation of the methodology.

References

1. Wang J, Liu Y, Song H: **Counter-Unmanned Aircraft System(s) (C-UAS): state of the art, challenges and future trends.** *IEEE AESS Syst Mag.* 2020; 12–15.
Publisher Full Text
2. Ayamga M, Akaba S, Nyaaba AA: **Multifaceted applicability of drones: a review.** *Technol Forecast Soc Change.* 2021; **167**: 120677.
Publisher Full Text
3. Tan CS, Van Bossuyt DL, Hale B: **System analysis of Counter-Unmanned Aerial Systems kill chain in an operational environment.** *Systems.* 2021; **9**(4): 79.
Publisher Full Text
4. Kim SJ, Jeong Y, Park S, *et al.*: **A survey of drone use for entertainment and AVR (Augmented and Virtual Reality)**. *Augmented Reality and Virtual Reality: empowering human, place and business*. 2018; 339–352.
Publisher Full Text
5. Nonami K: **Drone technology, cutting-edge drone business, and future prospects.** *J Robot Mechatronics.* 2016; **28**(3): 262–272.
Publisher Full Text
6. Restas A: **Drone applications for supporting disaster management.** *World J Eng Technol.* 2015; **3**(3): 316–321.
Publisher Full Text
7. Pledger TG: **The role of drones in future terrorist attacks.** Association of the United States army, 2021.
Reference Source
8. Schmersahl AR: **Fifty feet above the wall: cartel drones in the US-Mexico border zone airspace, and what to do about them.** Diss. Monterey, California: Naval Postgraduate School, 2018.
Reference Source
9. **https://www.heritage.org/technology/report/establishing-legal-framework-counter-drone-technologies**.
10. Mohamed N, Al-Jaroodi J, Jawhar I, *et al.*: **Unmanned aerial vehicles applications in future smart cities.** *Technol Forecast Soc Change.* 2020; **153**: 119293.
Publisher Full Text
11. **Unmanned aircraft systems detection and mitigation systems aviation rule-making committee**. Final Report, FAA, 2024.
Reference Source
12. Carter C: **Understanding C-UAS purpose and process.** Counter Unmanned Aircraft Systems Technologies and Operations, 2020.
Reference Source
13. Gault M: **Report-on-537-anti-drone-systems-shows-how-wild-the-market-has-become.** (2019, December 13).
Reference Source
14. Holland AM: **Counter-Drone systems.** 2nd Edition, 2019; **3**(4): 7–13.
Reference Source
15. Buric M, De Cubber G: **Counter Remotely Piloted Aircraft Systems.** MTA Review, Military Technical Academy Publishing House, 2017.
Reference Source
16. Sit YL, Nuss B, Basak S, *et al.*: **Real-time 2D+velocity localization measurement of a simultaneous-transmit OFDM MIMO radar using software defined radios.** In: *2016 European Radar Conference (EuRAD)*. 2016; 21–24.
Reference Source
17. Li CJ, Ling H: **An investigation on the radar signatures of small consumer drones.** *IEEE Antenn Wirel Propag Lett.* 2017; **16**: 649–652.
Publisher Full Text
18. Rozantsev A: **Vision-based detection of aircrafts and UAVs.** Master's thesis, EPFL, Lausanne, 2017.
Publisher Full Text
19. Andraši P, Radišić T, Muštra M, *et al.*: **Night-time detection of UAVs using thermal infrared camera.** *Transport Res Procedia.* iNAIR 2017, 2017; **28**: 183–190.
Publisher Full Text
20. Coluccia A, Ghenescu M, Piatrik T, *et al.*: **Drone-vs-Bird detection challenge at IEEE AVSS2017.** In: *Advanced Video and Signal Based Surveillance (AVSS). 2017 14th IEEE International Conference on*. IEEE, 2017; 1–6.
Publisher Full Text
21. de Haag MU, Bartone CG, Braasch MS: **Flight-test evaluation of small form-factor LiDAR and radar sensors for sUAS detect-and-avoid applications.**

In: *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC).* 2016; 1–11.
Publisher Full Text

22. Mezei J, Molnár A: **Drone sound detection by correlation.** In: *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI).* 2016; 509–518.
Publisher Full Text

23. Časar J, Starý V, Hanuš V: **Evaluation methodology for counter un-manned aerial system detectors.** *2023 International Conference on Military Technologies (ICMT).* IEEE, 2023.
Publisher Full Text

24. Doroftei D, De Cubber G: **Qualitative and quantitative validation of drone detection systems.** *International Symposium on Measurement and Control in Robotics ISMCR2018.* 2018.
Publisher Full Text

25. De Cubber G, Shalom R, Coluccia A, *et al.*: **The SafeShore system for the detection of threat agents in a maritime border environment.** *IARP Workshop on Risky Interventions and Environmental Surveillance.* IARP, 2017.
Publisher Full Text

26. **EU Science Hub.**
Reference Source

27. **Commission communication – A drone strategy 2.0 for a smart and sustainable un-manned aircraft eco-system in Europe**. COM(2022) 652 final.
Reference Source

28. Hansen P, Pinto Faria R: **Protection against Unmanned Aircraft Systems**. 2023.
Publisher Full Text

29. Tlučhoř T, Kraus J, Hulínská Š: **The methodology of Counter-UAS System comparison.** *Proceedings of 25th International Scientific Conference. Transport Means 2021.*
Reference Source

30. Kleczatský A, Hulínská Š, Kraus J: **Procedures for prevention of un-authorized incursion into UAS geographical zones.** *2020 New Trends in Civil Aviation (NTCA).* IEEE, 2020.
Publisher Full Text

31. Global Programme on Countering Terrorist Threats against Vulnerable Targets: **Protecting vulnerable targets from terrorist attacks involving Unmanned Aircraft Systems (UAS)**. © United Nations, 2022.
Reference Source

32. Chiper F, Martian A, Vladeanu C, *et al.*: **Drone detection and defense systems: survey and a software-defined radio-based solution.** *Sensors.* 2022; **22**(4): 1453.
PubMed Abstract | **Publisher Full Text** | **Free Full Text**

33. Harrigian JL: **A comprehensive approach to countering Unmanned Aircraft Systems**. January 2021.
Reference Source

34. EASA: **Drone incident management at aerodromes, part 1: the challenge of unauthorized drones in the surroundings of aerodromes**. Germany, 2021.
Reference Source

35. INTERPOL: **Framework for responding to a drone incident for first responders and digital forensics practitioners**. 2019.
Reference Source

36. U.S. D.H.S. / Cybersecurity and Infrastructure Security Agency / Interagency Security Committee: **Protecting against the threat of Unmanned Aircraft Systems (UAS)**. 2020.
Reference Source

37. U.S. D.H.S.: **Counter-Unmanned Aircraft Systems technology guide**. 2019.
Reference Source

38. Christnacher F, Hengy S, Laurenzis M, *et al.*: **Optical and acoustical UAV detection.** *Electro-Optical Remote Sensing X.* SPIE, 2016; **9988**.
Publisher Full Text

39. Besada JA, Campaña I, Carramiñana D, *et al.*: **Review and simulation of Counter-UAS sensors for Unmanned Traffic Management.** *Sensors (Basel).* 2022; **22**(1): 189.
PubMed Abstract | **Publisher Full Text** | **Free Full Text**

40. Lykou G, Moustakas D, Gritzalis D: **Defending airports from UAS: a survey on cyber-attacks and counter-drone sensing technologies.** *Sensors (Basel).* 2020; **20**(12): 3537.
PubMed Abstract | **Publisher Full Text** | **Free Full Text**

41. Castrillo VU, Manco A, Pascarella D, *et al.*: **A review of Counter-UAS technologies for cooperative defensive teams of drones.** *Drones.* 2022; **6**(3): 65.
Publisher Full Text

42. Farlik J, Kratky M, Casar J, *et al.*: **Multispectral detection of commercial unmanned aerial vehicles.** *Sensors (Basel).* 2019; **19**(7): 1517.
PubMed Abstract | **Publisher Full Text** | **Free Full Text**

43. Martins B, Holland A, Silkoset A: **Countering the drone threat implications of C-UAS technology for Norway in an EU and NATO context**. 2020.
Reference Source

44. Joint Air PowerCompetence Centre: **A comprehensive approach to Countering Unmanned Aircraft Systems**. January 2021.
Reference Source

45. Monckton S, Sabatos D: **GOALTENDER: towards a CUAS planning tool**. DRDC-RDDC-2019-D085.
Reference Source

Open Peer Review

Current Peer Review Status: ? ✗ ? ✗

Version 1

Reviewer Report 16 January 2025

https://doi.org/10.21956/openreseurope.19817.r46155

© **2025 Shoufan A.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✗

Abdulhadi Shoufan
Khalifa University, Abu Dhabi, Abu Dhabi, United Arab Emirates

I started reading the paper with interest because I regard the topic highly relevant. Counter-drone technology will be a core requirement for protecting the airspace, the public, and the infrastructure against reckless and malicious operations. The study promises to present a “standardized test methodology”. The methods should rely on compiling data from a literature review, analysis of previous incidents, assessment of current C-UAS frameworks, feedback from end users, and validation trials.

Unfortunately, the paper lacks the expected rigor.

1. The literature review is shallow: Most literature is from 2021 and before
2. No analysis of previous incidents and the consideration ended in August 2021. Why?
3. Assessment of current C-UAS frameworks is almost completely missing
4. Feedback from the end user: no information about the questionnaire, the sample, size, etc.
5. Validation trials: completely missing.
6. No compilation of data.

I was disappointed to find out that the core contribution of the paper is Figure 2. The paper is largely written by AI.

Is the rationale for developing the new method (or application) clearly explained?
Partly

Is the description of the method technically sound?
No

Are sufficient details provided to allow replication of the method development and its use by others?
No

If any results are presented, are all the source data underlying the results available to ensure full reproducibility?
No

Are the conclusions about the method and its performance adequately supported by the findings presented in the article?
No

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: CUAS, UTM, Secure and Safe drone operations

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 09 January 2025

https://doi.org/10.21956/openreseurope.19817.r47877

© 2025 Mateou S. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

Sofia Mateou
Prince Sultan University, Riyadh, Saudi Arabia

Overview
This paper outlines the need to effectively detect and counter the illegal use of unmanned aircraft systems (UAS). It focuses on identifying and implementing a standard and systematic test methodology for scenarios to evaluate C-UAS systems in critical areas such as inter alia, border security, and protecting critical infrastructure. The research is of value to key stakeholders and contributes to the area of counter-drone capabilities. The empirical research and practical application to real scenarios are significant in light of the current and rapidly expanding developments in using UAS for illegal purposes by individuals, organizations, and entities.

Strengths:
Bridges the gap between theoretical studies and practical solutions applicable to current and real threats. The number of cases examined provides good empirical research.
The use of clear tables assists the readers in comprehending the subject matter.

General comments and suggestions:

Methodology:
The authors provide a sound systematic methodology that includes four areas: a literature review, an analysis of previous incidents to identify gaps, the current UAS framework, and feedback from

end users. The methodology could emphasize more the international collaboration and how this influenced the project.

Literature Review:
The literature review can be expanded to provide a deeper critical analysis of gaps in the literature and a more in-depth discussion of weaknesses in existing methodologies and other studies.
A more in-depth discussion of vulnerabilities and challenges, including difficulties in regulating access to lower airspace, can be included. The literature review could include a discussion on the need to have a risk-based approach with the four pillars: risk identification, risk assessment, risk control measures, and continuous monitoring and reviewing of C-UAS systems, taking into account current advancements and developments.

Validation of Results / Results:
The tables clearly depict the results. However, a more in-depth discussion and analysis of the validation of the trials held in Greece, Belgium, and Spain should be included to strengthen the study's results and validity further. This would also allow the reader to better assess the validity of the results and provide a more convincing argument regarding the effectiveness of the scenarios.

Adoption and Applicability of Findings:
Discuss the feasibility, practicalities, and /or difficulties regarding implementing the findings and adopting the standardized test methodology and the impact this would have on states being better prepared to deal with such evolving threats.
Key findings can be summarized or listed to strengthen their impact.
A discussion on how the results can be applied to additional countries will assist in achieving the objective of disseminating and applying the results globally.
Highlight how this project and the findings can impact further research.
Consider creating a database (on a European level at first) to act as a repository for reporting, accessibility, analysis and evaluation, information sharing, and lessons learned.

Weakness:
The paper does not outline or refer to the current study's limitations which diminishes the impact and reliability of the results.
The paper does not adequately discuss challenges stemming from differences in the legal and regulatory framework of EU member states and some of the many legal complexities inherent in establishing common standardized scenarios and, more specifically, in implementing the standardized test methodology to better protect lower airspace.

Is the rationale for developing the new method (or application) clearly explained?

Yes

Is the description of the method technically sound?

Partly

Are sufficient details provided to allow replication of the method development and its use

by others?
Partly

If any results are presented, are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions about the method and its performance adequately supported by the findings presented in the article?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: My research interests include legal, safety, and security issues related to the aviation industry, including, inter alia, unmanned aircraft vehicles (UAVs) and the liability of aviation professionals, including pilots, ATC, and airports following serious accidents or incidents involving commercial or unmanned aircraft.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Reviewer Report 13 December 2024

https://doi.org/10.21956/openreseurope.19817.r46739

© 2024 Alharasees O. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.



Omar Alharasees
Budapest University of Technology and Economics, Budapest, Hungary

Methodology Improvement:
- Simplify the methodology section by clearly explaining the purpose and integration of each step. Break down how international collaboration shaped the methodology, ensuring that readers understand how the multi-country context influenced the process.
- Add diagrams, flowcharts, or step-by-step visuals to illustrate the scenario development process, which will improve comprehension.

Expand Literature Review:
- Broaden the scope of the literature review to include human factors models like HFACS, OODA loop, and other UAS-focused conceptual frameworks.
- Incorporate recent studies and advancements in the field to provide a more comprehensive backdrop. This will demonstrate a deeper engagement with current research and enhance the academic value of the article.

Strengthen Results:

- Provide more detailed statistical or qualitative analysis of the validation trials, with clear data on how the C-UAS systems performed in different scenarios.
- Include visualizations, such as heatmaps, comparative graphs, or tables, to illustrate key findings from the scenarios. This will make the results more digestible and scientifically rigorous.

Highlight International Collaboration:

- Elaborate on the international aspect of the project, especially how the involvement of multiple countries (e.g., Greece, Spain, Belgium) shaped the methodology, validation, and application of findings. Discuss how this collaboration influenced the development of standardized scenarios and how the findings might be generalized or applied across different regions.

Address Limitations and Future Work:

- Include a section dedicated to discussing the limitations of the current work, such as geographical constraints, technological limitations, or potential challenges in testing.
- Propose future work, such as integrating AI-based detection technologies or refining human factors assessments in the context of C-UAS systems. This will show that the work is part of an ongoing research agenda.

Visual Enhancements:

- The article lacks sufficient visual content. Adding figures, tables, or conceptual diagrams would greatly improve the clarity and scientific robustness of the article. Consider adding a diagram to illustrate the scenario development process or a table summarizing key results from the trials.

Broader Implications:

- Discuss how the standardized scenarios contribute to global C-UAS policies and their potential to influence future research and development. Highlight how this project fits into broader international efforts to combat malicious drone activities.

  The article makes a valuable contribution to the field of counter-UAS systems by presenting a methodology for standardized testing. However, more detailed descriptions, data, and visualizations are required to strengthen the scientific rigor of the work. By addressing the gaps in the methodology, expanding the literature review, providing data transparency, and including visual enhancements, the article could be significantly improved and made suitable for indexing.

Is the rationale for developing the new method (or application) clearly explained?

No

Is the description of the method technically sound?

No

Are sufficient details provided to allow replication of the method development and its use by others?

No

If any results are presented, are all the source data underlying the results available to ensure full reproducibility?

Partly

Are the conclusions about the method and its performance adequately supported by the findings presented in the article?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: The article requires further mandatory revisions before it can be considered fully scientifically valid. While the methodology and objectives are of value, the lack of detailed technical descriptions, insufficient data transparency, and inadequate support for conclusions make it unsuitable for approval in its current form.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to state that I do not consider it to be of an acceptable scientific standard, for reasons outlined above.

Reviewer Report 12 December 2024

https://doi.org/10.21956/openreseurope.19817.r46154

© 2024 Delleji T. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

Tijeni Delleji
Military Research Center, Science and Technology for Defense Lab (STD), Aouina, Tunisia

General Overview
This manuscript addresses a critical challenge in the domain of counter-Unmanned Aircraft Systems (C-UAS) by presenting a comprehensive methodology for developing standardized scenarios. The relevance of this work is underscored by the growing misuse of drones for malicious purposes and the pressing need for effective countermeasures. The authors display academic rigor and practical insights, making this paper a valuable contribution to the field. While the paper is well-structured and insightful, some areas require improvement to enhance its clarity, consistency, and impact. Below are detailed recommendations:

Major Comments

1. **Table Descriptions**
   - The descriptions for **Table 2** and **Table 3** need to be systematically ordered. Clear and concise annotations for each table component will enhance readability and utility.
2. **Abbreviation Duplication**
   - The abbreviation “DTI” is used ambiguously for both *Drone Threat Intelligence* and *Detection-Tracking-Identification*. This needs to be resolved by introducing a distinct acronym for one of the terms.
3. **Introduction Improvement**
   - In the second line of the introduction, replace “and drones” with “or drones” to align with linguistic precision.

4. **Terminology Standardization**
    - Replace "optoelectronic (OE) detectors" with "Electro-Optic or Electro-Optical (EO) detectors" for consistency with defense and surveillance terminologies.
    - Revise the phrase:
      "Technologies can be categorized as either active (e.g., radar and lidar) or passive (e.g., cameras), with passive technologies dominating C-UAS solutions"
      to
      "Technologies can be categorized as either active (e.g., radar and lidar) or passive (e.g., visual and thermal cameras)."
5. **Consistent Nomenclature**
    - Replace the following terms throughout the manuscript:
        - *Visible Imaging Sensor (VIS) cameras* → *Visible Imaging Sensor (VIS)*
        - *Thermal imaging cameras* or *thermal cameras* → *Thermal Infrared Imaging Sensor*
        - *Infrared (IR) sensors* → *Reflected Infrared Imaging Sensor*
6. **Metrics and Evaluation Criteria**
    - Include detailed metrics and evaluation criteria used for validation trials in Greece, Belgium, and Spain. This will reinforce the study's credibility and reproducibility.
7. **Global Context Expansion**
    - Address the regulatory and threat variations outside Europe, such as in North Africa, the Middle East, or Asia. This inclusion would extend the study's relevance to a global audience.
8. **Reproducibility Limitations**
    - The data-sharing restrictions imposed by the COURAGEOUS project limit transparency. Include a discussion on how anonymized data could be shared to support reproducibility without compromising security.
9. **Annex Addition**
    - Add an annex listing the anti-drone systems utilized in the study for reference and transparency.
10. **Proposed Enhancements for Scenario Comprehension**
    - Incorporate **flowcharts** or **decision trees** to illustrate scenario execution. These visuals can aid practitioners in understanding complex processes intuitively.
11. **Roadmap for Emerging Threats**
    - Propose a roadmap for adapting the methodology to emerging threats, such as drone swarms or AI-enhanced UAVs.
12. **Scenario Development**
    - Introduce more details on tailoring scenarios for diverse operational environments and threat levels. Highlight how these scenarios can adapt dynamically to reflect evolving drone capabilities.

Additional Suggested Literature

To enhance the study's comprehensiveness, consider referencing the following works:

- *"A C4 Software for Anti-Drone Systems"*
- *"Video Data Analytics Dashboard for Anti-Drone Systems"*
- *"An Upgraded-YOLO with Object Augmentation: Mini-UAV Detection Under Low-Visibility Conditions by Improving Deep Neural Networks"*
- *"Deep Reinforcement Learning-Based Car-Following Control for Active Visual Tracking From a*

Pan-Tilt Platform"
- *"Real-Time Implementation of SDR-Based RF Source Detection and Localization in Restricted Areas."*

Is the rationale for developing the new method (or application) clearly explained?
Yes

Is the description of the method technically sound?
Partly

Are sufficient details provided to allow replication of the method development and its use by others?
Partly

If any results are presented, are all the source data underlying the results available to ensure full reproducibility?
Partly

Are the conclusions about the method and its performance adequately supported by the findings presented in the article?
Partly

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: My research interests include avionics, computer vision, EO/IR imaging (NIR, SWIR, MWIR, LWIR), thermography, Polarimetric imagery, anti-drone and military applications. In addition, I am engaged in the application of ML/DL techniques, including tasks such as dataset preparation, object detection, RF-based drone detection, image classification, spectrogram image classification and multi-object tracking.

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.