Scientific Research Publishing

Open Journal of Acoustics, 2025, 13(1), 1-16
https://www.scirp.org/journal/oja
ISSN Online: 2162-5794
ISSN Print: 2162-5786

Andros: An Acoustic Anti Drone System

Adam Mlynarczyk[1], Andreas Constantinides[1], Marcello Coradini[1], George A. Danos[2], Andrea M. Di Lellis[1], Enrico Flamini[1*], Kyriakos Michail[1]

[1]Space Systems Solutions (S3) Ltd., Nicosia, Cyprus
[2]Cyprus Space Exploration Organisation (CSEO), Nicosia, Cyprus
Email: *enricoflam51@gmail.com

How to cite this paper: Mlynarczyk, A., Constantinides, A., Coradini, M., Danos, G.A., Di Lellis, A.M., Flamini, E. and Michail, K. (2025) Andros: An Acoustic Anti Drone System. *Open Journal of Acoustics*, **13**, 1-16.
https://doi.org/10.4236/oja.2025.131001

Received: December 4, 2024
Accepted: March 28, 2025
Published: March 31, 2025

Abstract

The project's general objectives were to develop a system that intercepts drones using audio and radio frequencies. This project provides a complete solution, integrating state-of-the-art passive and active detection technologies. We have produced a prototype and field-tested the technology; we are heading toward developing a market-ready model after completing a Patent request. We aim to have an Anti-Drone system that can operate stealthily without emitting eM noise. The innovative use of Sodar and Beamforming devices makes our system unique and operable to protect a predefined perimeter in the most different conditions.

Keywords

Drone, Sodar, Beamforming

1. Introduction

1.1. Early Events

On July 15, 1849 drones as a military tool were first flown by the Habsburg Austrian Empire launched against the citizens of Venice. 200 pilotless balloons armed with bombs flew over the skies of Venice [1]. The same strategy was adopted by both the Union and the Confederate Armies during the American Civil War. Balloons loaded with explosives and time-sensitive triggers were sent over their opponents; however, these attacks did not determine the fate of any battle [2].

In 1930, the British Royal Navy developed a radio-controlled drone that it used as a flying target for training its pilots [3].

Between Nov. 1944 and Apr. 1945, Japan released more than 9000 bomb-laden balloons across the Pacific, intending to cause forest fires and panic in the Western United States in Operation "Fu-Go". Most balloons caused minimal damage or

fell in the Pacific Ocean, but more than 300 entered the U.S. and Canadian skies. The U.S. government, in concert with the American press, decided to keep the Japanese balloons a secret. Hence, the Japanese believed the tactic was ineffective and abandoned the project [4].

Companies have developed dozens of drone models, ranging in size from large solar-powered fixed-wing aircraft to small hummingbird-mimicking helicopter-like drones. They all have a wide variety of capabilities and cost from $600 to at least $103.7 million per drone. In 2013, the starting price for a weaponized drone was about $15 million [5].

The two most widely used weaponized drones have been the MQ-1 Predator (which the U.S. military officially retired on Mar. 9, 2018) and the upgraded MQ-9 Reaper, both developed by military contractor General Atomics Aeronautical Systems. The Predator drones were first flown in June 1994 and deployed by NATO in 1995 in the Balkans during the Bosnian War (1992-95), while the Reaper was first deployed in Oct. 2007 in Afghanistan [6].

Drones are rapidly proliferating. Over 90 countries and non-state groups operate drones today, and even more are certain to do so in coming years. These actors are beginning to employ drones in novel ways according to their interests, opportunities, and constraints. As drones move beyond a niche capability used for surveillance and strike to an integral component of modern militaries, they could have an unanticipated impact on crisis stability, escalation dynamics, and norms regarding state sovereignty.

1.2. Perimeter Security

As drone technology keeps evolving at lightning speed, it introduces new and complex challenges to drone perimeter security, fundamentally altering the landscape for critical infrastructure protection. What is perimeter security? Perimeter security is the first line of defense for safeguarding physical spaces, assets, and infrastructure. It involves a strategic arrangement of barriers, surveillance, and detection systems to monitor and control access to a defined area, typically around critical infrastructure or restricted facilities.

Effective drone perimeter security relies on technologies like cameras, motion detectors, and sensors, as well as advanced tools like radar and radio frequency systems to detect unauthorized access or breaches. In today's environment, with the rise of increasingly sophisticated drones threats, perimeter security also includes counter-UAS measures and AI-driven surveillance to address evolving risks.

Rapid response when drones cross protected perimeters, either through an unintended breach or for malicious purposes, every second matters. When drones are capable of causing significant damage or scoping targets before a theft, closing the window of vulnerability continues to remain a high priority.

However, many commercial drones are now able to reach incredibly high top speeds (currently meeting an average of 50 mph). They can also bypass secure perimeters and enter secure airspace exceptionally quickly. This presents security

teams with the task of responding to new risks in essentially real time.

1.3. Intelligent Onboard Systems

With onboard intelligence equipping drones with the benefits of AI, it is no longer necessary for human pilots to control drones. For law enforcement teams, this presents a new challenge, how to identify the drone's owner if there's no location data available to be intercepted.

This is an ongoing concern and one that we are actively involved in tackling through our close collaboration with UK law enforcement, defense research, and other sectors.

1.4. Drones Can Harm

Drones can cause significant harm to people, property, or wider environments, such as when entering the turbines of passenger jet engines or falling from great heights into crowded areas. There are several documented incidents of drones causing bodily harm and more.

Drones are also capable of presenting other forms of unique harm to security. Their use for smuggling illegal contraband into prisons has already been flagged as a serious risk, while new abilities for deploying payloads through various means, including chemical dispersions, are a constant battle for security teams (Table 1).

Table 1. Type of harm depending on drone size.

Threats Mapped to Types of Drones					
Types of Drones		Privacy	Physical Attacks	Crime	Cyber Attacks
	Video Streaming	Carrying Surveillance Equipment			
Nano (90 m range)			Targeted assassination	Targeting homes for burglaries	
Micro (5 km range)		3D mapping using a radio transceiver MITM attacks against cellular networks Tracking a person according to his/her devices	Carrying radioactive sand- and chemicals/biological	Smuggling goods into prison yards	
Mini (25 km range)	>/	V	Carrying a bomb colliding with an airplane	Hijacking radio-controlled devices smuggling goods between countries	Establishing a covert channel
Swarm			Multiple casualty incidents	Cyberwarfare	

1.5. The Reaction

A wide range of counter-drone solutions has been proposed, from conventional radar to using trained eagles to attack the aircraft. Spectrum RF monitoring to

detect and geolocate drone control signals is one solution that has become popular in recent years. Spectrum RF monitoring has also been developed as an essential technique in a comprehensive counter-drone system. However, active radar techniques may not be used, such as when the drone flies at a few meters altitude from the ground or in airport proximity where interferences with control tower communications must be avoided, or when RF techniques fail because the drone flies in unattended & GPS driven silent mode, minimizing its RF emissions, the Audio methods may provide the ancillary (proper) solution. Indeed, whatever the drone may try to camouflage, such as its radar reflectivity, or minimize its RF emissions, it cannot avoid those significant turbulences and large detectable signals unavoidable to sustain its weight in flight. Moreover, the audio signal signatures generated by the multiple number and complexity of the rotors may provide an actual mean for their classification.

Table 2. Anti Drone most used techniques.

Technique	Pros	Cons
Audio Detection	• Can detect drones without any RF control signal • Can cover a wide range of installation from single buildings to major airports • Short to long-range depending on the number of "towers".	• Interference prone in very noisy environments
Infrared Detection	• Can detect drones without any RF control signal	• Most small drones produce very little heat • Most airborne vehicles (not drones) are heat sources, as well as big birds • Not operable with the Sun in the background • Limited range • Operational difficulties (like optical & lidar detection)
Radar Detection	• Can detect drones without RF control signal • Long-range	• Difficult to detect low flying drones • Problems distinguishing from other small objects • EM Electromagnetic interference
Radio Frequencies RF Detection	• Long-range in absence of background RF noise • Can locate controller and drone • Lends itself to signal jamming and intercept	• Requires drone to be emitting RF signal (*i.e.* amateur or commercial drones) • Autonomous drones cannot be detected

As the number of drones flying in the sky, dangers and risks also rise in parallel. Technologies capable of finding, tracking, and alerting will score the highest gains in the coming years. The existing solution for this kind of threat is typically the use of anti-air missiles but wasting an expensive missile on an inexpensive drone is not scalable and poses a threat to the nearby area, so anti-drone detection systems are the solution. The global anti-drone market is segmented based on system, technology, and end-user. By type, the market is categorized into neutralizing and detection systems. The neutralizing system segment is classified into laser, drone rifles, jamming, drone capture nets, and interception. The detection system segment includes active optics, passive optics, RF emissions, radar-based, and acoustics. The technology segment comprises electronic, laser, and kinetic systems. By the end-user, the market includes government, military and defense, commercial, critical infrastructure, households, public venues, and others. Following Table 2 describes the vast applications that need an Anti-Drone Detection System with low-height flights.

Today in the market, producers of all-acoustic devices use a microphone array to detect drones by analyzing the noise of the rotors or detect drones based on comparing a drone's captured acoustic signature with other signatures stored in a database of previously collected sound signatures, **none use the combination of passive and active listening using SODAR technology (S3 exclusive technology).**

1.6. Current Unsolved Issues

- No identification of low-flying UAVs and drones
- Avoidance of interferences with control tower communications (for example Airport proximity). No identification of drone flies in un-attended & GPS-driven silent mode, minimizing its RF emissions. Radio Frequency techniques fail (Figure 1).

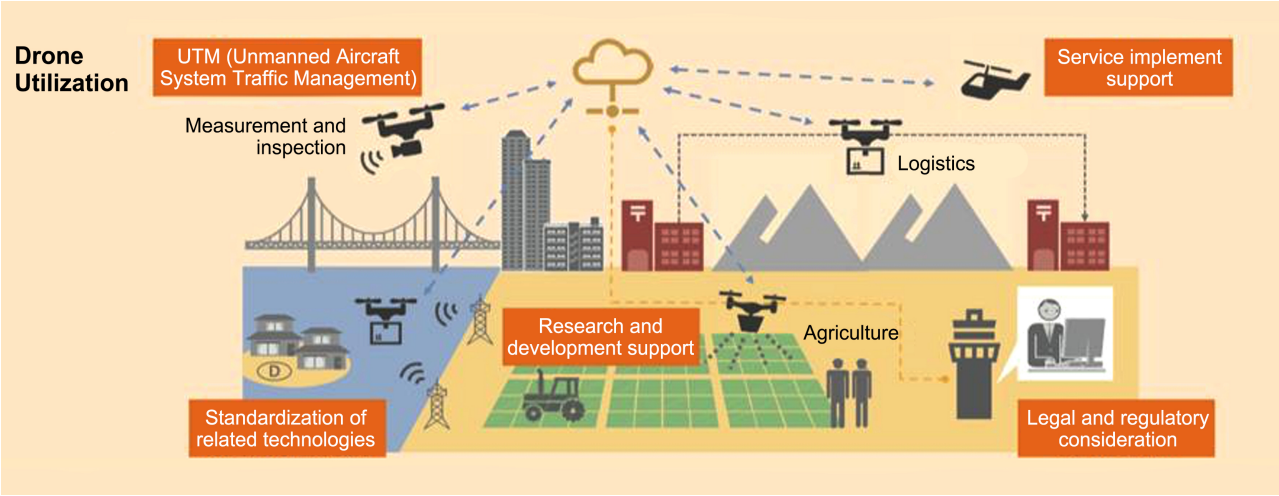

Figure 1. Drone fly zones and utilizations [7].

2. Method (Technical Approach and Solution)

Our technical objectives were to exploit a system that intercepts drones using audio and radio frequencies.

Our final goal was to provide a complete solution, integrating state-of-the-art passive and active detection technologies with an optional, commercially available, jamming active counter system that can completely stop communications and onboard GPS signal processing.

2.1. The Project Developed through the Following General Objectives (GO)

Go I: To design, develop, and certify a commercial demonstration model (DM) for intercepting drones where the DM will be used to verify the efficiency of the target identification algorithms and assess the Audio & Radio frequency antenna layout configuration and orientation. This development will conclude with a local test campaign to verify the performances and finalize all the interface aspects in similar environmental conditions. The achieved results will be consolidated via a critical design review, which will clarify the needed upgrades of the DM to be promoted as the following final model.

Go II: To design, optimize, and produce an upgraded version of the DM into the final deliverable mast model, namely the Final Model, herein FM, which will fulfill all the given user requirements, including customer-required camouflaging. So far, the FM will be simply an upgrade and ready-for-market model of the DM, supporting the complete set of the expected system mast and running the final validated software on the Central Station. Part of the DM hardware will be part of the FM hardware.

Go III: To promote and commercialize a system named ANDROS, to the global market to trigger potential customers and attract further investments. To develop system procurement and production capabilities in Cyprus. Training of engineering team(s) capable of assembling, integrating, and installing the required system on-site. After installation, the team will test the overall system, guarantee the performance commissioning, and provide clear instructions, tutorials, and procedures for daily operations.

2.2. Technical Solution

An innovative integration of passive long-range acoustic detection with the use of an adapted SODAR (Sonic Detection and Ranging system) and short-range high-resolution detection & beam forming.

The goal is to detect drones at a distance of up to 1.0 km, below the radar level.

The system needs to be modular and much cheaper than a radar system. It also needs to be capable of operating day and night and remain undetectable by drones (passive, non-emitting).

Furthermore, the system must be discrete and stealthy, and not interfere with existing infrastructure operating EM systems at various wavelengths.

A "sodar," is an acoustic pulse-echo probe that mimics in the acoustic wavelenghts domain a radar. The first sodars, which appeared in the early 1970s, emitted an acoustic pulse in a single vertically pointing beam as shown in Figure 2. The sodar geometry shown, with the acoustic source and receiver collocated, is common and is known as a "monostatic" sodar (A less common geometry has the receiver separated horizontally from the transmitter and is called a "bistatic" sodar).

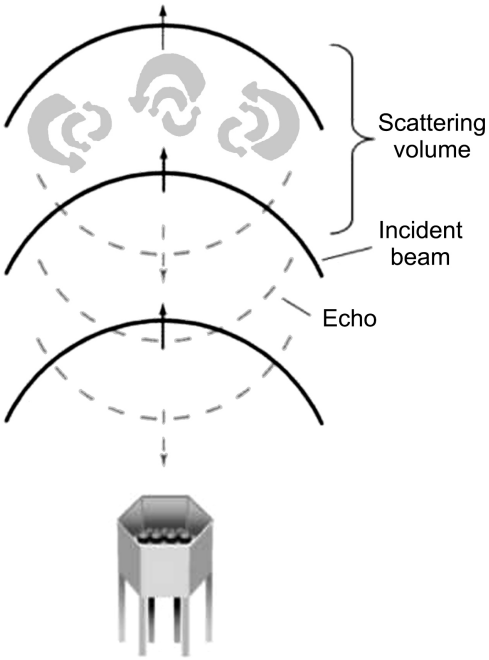

Figure 2. Sound Detection and Ranging—SODAR It can operate in passive (just listening) or active (sending sound pulses and listening to the echoes) mode [8].

With monostatic a SODAR, the part of the acoustic wave scattered back toward the ground, the echo, is detected using the same transducers that produced the prime wave. The principle of a SODAR (sonic detection and ranging) is to transmit acoustic waves vertically and measure the backscattered signals. The backscattered signals are affected by temperature and humidity fluctuations in the atmosphere. By analyzing the Doppler shift in the backscattered signals, Sodars can measure wind speed, temperature structure, and other atmospheric properties. This is the prime utilization of Sodars, and their dimensions are very sizeable. We are using the same principle to detect fast-moving flying objects but using an ultra-miniaturized version of the apparatus.

In fulfillment of the above requisites, we have integrated a high-reliability active & passive Audio automated system, coupled with the most recent RF receivers, capable of successfully detecting and tracking drones without interfering with ground infrastructure tracking and communications systems. This is an integrated market-ready solution having a vast RF jamming range and high jamming accuracy. The maximum capacity of jamming is up to 1500 meters. Our system

can block GPS, BeiDou, and GLONASS signals, by effectively targeting, at the same time, the latest military drones. The main challenge is discriminating a single sound source in a loud (noisy) environment, such as a flying drone in a city context or a conversation between two criminal people monitored by a Police task force in a crowded context. Both such problems may be tackled adequately with the help of the "Beamforming technology", which not only may properly focus on single sound emission sources but is scalable towards multi-source problems such as the follow-up of a multi-drone attack. The information on detected drones can be used to neutralize drone attacks.

Our solution is based on a signal processing technique used in sensor arrays for directional signal transmission or reception. This is achieved by combining elements in a microphone array in such a way as to provide a concurrent pattern of constructive/destructive interference. Beamforming is intensively used for the audio-receiving ends to achieve spatial selectivity. This improvement concerning isotropic reception/transmission is known as array directivity. When the signal of the source is sampled, as an example, by three different mics, and the signals are first appropriately delayed, the resulting signal is highly intensified. Originally developed to prevent racial choirs in a video context, such as a football stadium, this Beamforming technique was first deeply investigated and adopted by S2G Technologies/AMDL Team. The main features of the developed system are briefly described in G. Casasanta *et al.* [9], "Consumer Drones Targeting by Sodar (Acoustic Radar)", in IEEE Geoscience and Remote Sensing Letters, vol. 15, no. 11, Nov. 2018. To adequately address the problem, the best mics able to withstand such a noise level typical of football matches in a stadium but still with an exquisite sensitivity have been chosen. With a package size of only 4 mm × 3 mm × 1.2 mm, this component provides a wide dynamic range of 105 dB with a Signal-to-Noise Ratio of 69 dB (A) with less than <1% total harmonic distortions up to 128 dBSPL and can sustain an acoustic overload point at 130dBSPL. For this application, the primary "Tile" with 16 mics spaced 2.2 cm each has been already manufactured and tested. Such a tile contains the above-selected mics plus a super-correlating FPGA able to perform the local DaS (Delay and Sum algorithm) or FaS (Filter and Sum algorithm) computations. This tile is designed to be combined into a mosaic of up to 127 tiles, with the possibility to assemble a single large panel of up to 2032 mics. Besides single super-focused audio streams at a 48kHz sampling rate, the assembled system board can provide multiple audio source directions up to a total budget of 5 Gigabit/sec. The tiles have been assembled and finished into a single large array, *i.e.*, implementing a flat panel type of 8 × 2 tiles size of about 20 cm × 80 cm and containing 256 mics by using the in-house 3D printer. This system, which already includes the front-end electronics, gets connected to a local front-end computer that controls the operational mode(s) of the mosaic, namely:

1) Survey, auto scan of the front scene, trigger on Event which alerts the video system;

2) Fine auto scan, auto scan on the maximum local audio source;

3) Fixed direction sampling;

4) Servo scanning addressed by the User.

Beamforming is intensively used for the audio-receiving ends to achieve spatial selectivity. This improvement concerning isotropic reception/transmission is known as array directivity. When the signal of the source is sampled, as an example, by three different mics, and the signals are first appropriately delayed, the resulting signal is highly intensified. Hence, the best mics able to withstand such a noise level typical of football matches in a stadium but still with an exquisite sensitivity have been chosen (Figure 3).

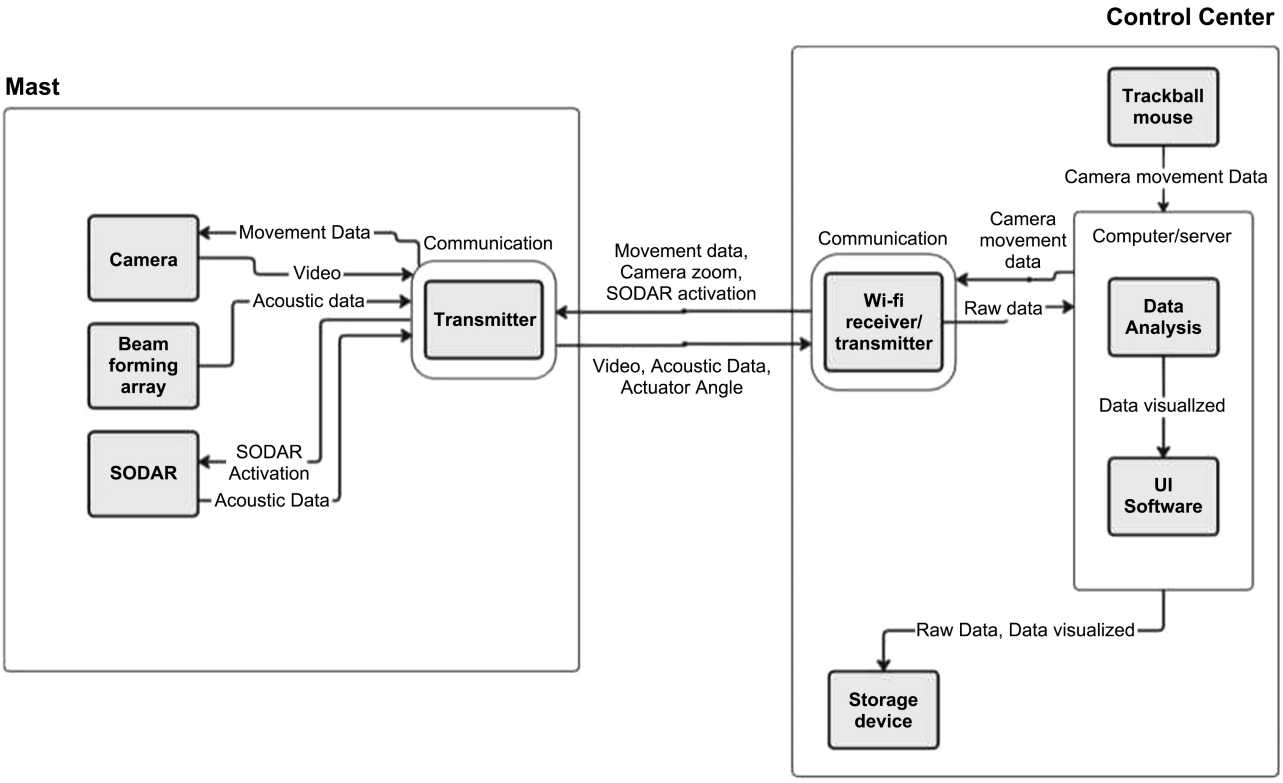

Figure 3. Functional diagram of Andros. The FPGA controls the overall system synchronizing the active direct digital synthesizer and receiver side performing all the required digitally controlled operations such as FFT. The lower part shows the analog ultra-low noise high gain processing analog chain.

Beam Forming is a unique characteristic of the Andros system. The beam forming technology is normally used in TV studios or on stage to follow acoustically someone who is speaking/singing while fast moving. We have evolved this technology to its utmost performance, making it capable of following drone intrusions at close distances and low altitudes. Our implemented beam forming technology works as a proximity sensor capable of detecting and following at low altitude (from 0 to 10 m altitude) any drone intrusion up to distances of 200 meters. This technology is a necessary complement to our "acoustic horns" technology as it covers the shortrange areas that for geometric reasons cannot be effectively covered by the long-range detection system.

2.3. Camera Systems

The technology and the production of monitoring cameras at Visual and IR and Thermal IR is immense. IR (night vision not thermal) cameras can reach incredible resolutions of Km+. However, a single camera system is not completely effective, as 360-degree azimuth and elevation monitoring are required for early detection of flying intruders. Our system offers the possibility of installing several types of cameras, depending on the customer's requirements. The camera is used to display in the user interface the image of the intruding drone, after acoustic detection has taken place.

2.4. Operability in Severe Environmental Conditions

Several measures were adopted to guarantee the optimal functioning of the system in the most diverse environmental conditions. However, we should declare upfront that in the course of an intense wind storm or in the proximity of a large number of airplanes taking off simultaneously, the system might lose effectiveness. On the other hand, in the presence of a wind storm, flying effectively a drone is almost impossible. The system can operate under rainy or snowy conditions thanks to specific meshes that protect the external part of the sensors. Should anyhow water or humidity penetrate, a specific design of the internal acoustic horns stops the water from reaching sensitive parts of the apparatus. The electronic components were tested in the laboratory under extreme temperature conditions. The system can also be adapted to the use in constant extreme temperature conditions thanks to the use of appropriate thermal protections to be discussed with the potential client.

The system is also insensitive to intense local EM disturbances as its internal electronics are protected by the tower's metallic or mesh-like structure, and the acoustic (noise) of an intruding drone has no EM coupling.

2.5. Protection of Large Perimeters

Our system consists of a minimum of three components (towers). However, the number of towers can be increased almost indefinitely to protect large perimeters such as an airport. When the number of towers and the spatial separation is large, specific communication and powering systems can be discussed with the potential client.

2.6. Stealthy Operability

The most important characteristic of our system is that when operated in acoustic passive mode, it generates zero electromagnetic noise. Hence, it can be operated in proximity to any communication or other detection system. This specificity makes our system ideal to be operated in an airport or other sensitive targets such as a communication center. Furthermore, the operation geometry of both our acoustic horns and our beam-forming apparatus covers 0 to 90 degrees of

azimuth. This makes our system perfectly appropriate to detect low-flying drones even if operated in visual navigation in areas with no GPS coverage.

3. Results

Field Testing

The initial tests focused on examining the SODAR system's response to specific frequencies. For this purpose, a sound generator was utilized, programmed to generate frequencies from 0 to 10 kHz. This sequence was repeated 10 times to minimize errors and external signals. The tests were conducted in an anechoic chamber, and the entire test lasted 20 minutes. The system's response is presented in Figure 4 below.

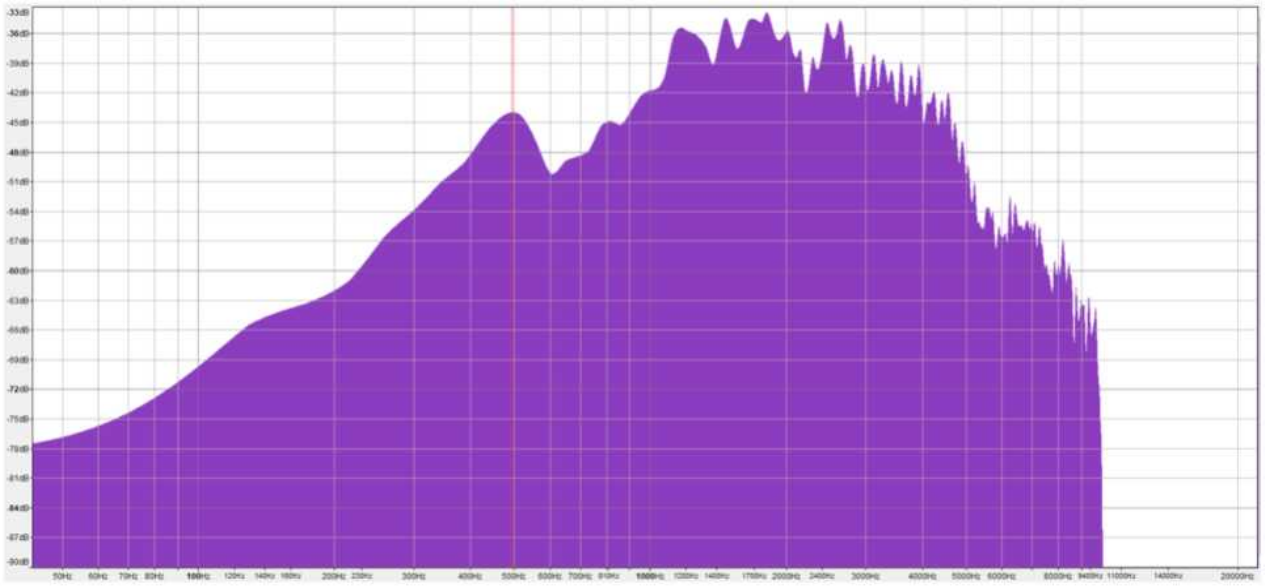

Figure 4. Sodar response to different wavelengths.

The open field tests took place in various locations, using various types of drones following different flight paths. Tests were carried out at various stages of product development. To minimize the possible signal ambiguity during initial tests, we made sure the weather was favorable, *i.e.*, the absence of strong winds. The ambient background noise was accurately measured to best calibrate the captured signals (Figure 5).

The first DM test consisted of three flights: 1.1—towards the protected zone with mast no. 1 on its trajectory; 1.2—in the opposite direction to the first flight; and 1.3—under the same conditions as 1.1. The distance for each flight was approximately 500 m. The second test was conducted between masts 1 and 2, also towards the protected zone. The last, third flight was circular, at a minimum distance of approximately 500 m from each mast. Spectrograms of the flights are shown in Figure 6 and labeled "flight 1, 2, 3".

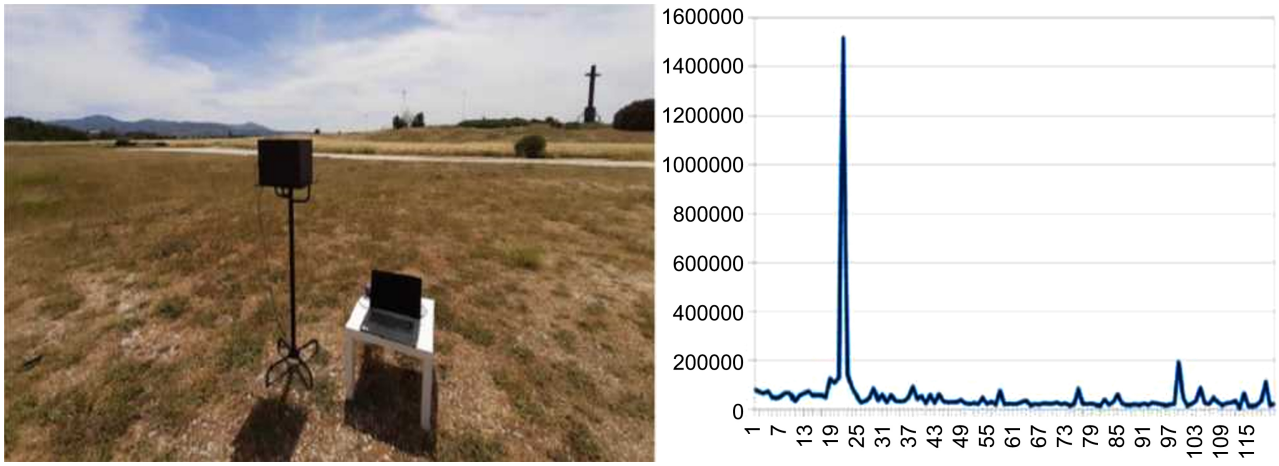

Figure 5. Image of one prototype receiving station (left) and signal detected at 150 m.

The recording of the entire measurement session is shown in the spectrogram in **Figure 6**. It contains three complete recordings for the entire measurement session with marked moments of flights 1, 2, and 3. Audio data during the flight and when the drone mission was not being performed were recorded and used as input data for machine learning (**Figure 6**).

Figure 6. The trajectories of drone flights (upper left figure), their corresponding spectrograms (upper right figure), and a spectrogram of the entire measurement session (lower figure).

4. Discussion

The input data were spectrograms of sounds from various drones recorded in diverse environmental conditions. Each sound lasted 1 second. The analysis aimed to investigate the effectiveness of CNN (Convolutional Neural Network) in recognizing drone sounds based on their spectrogram representation (Figure 7).

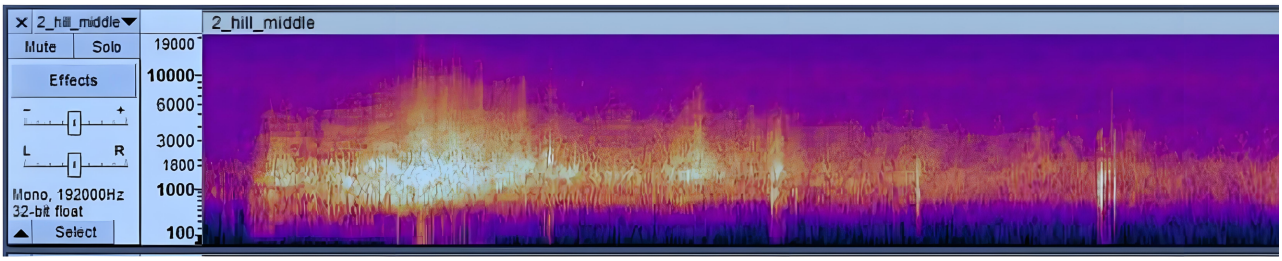

Figure 7. The results of drone sound analysis conducted using a convolutional neural network (CNN).

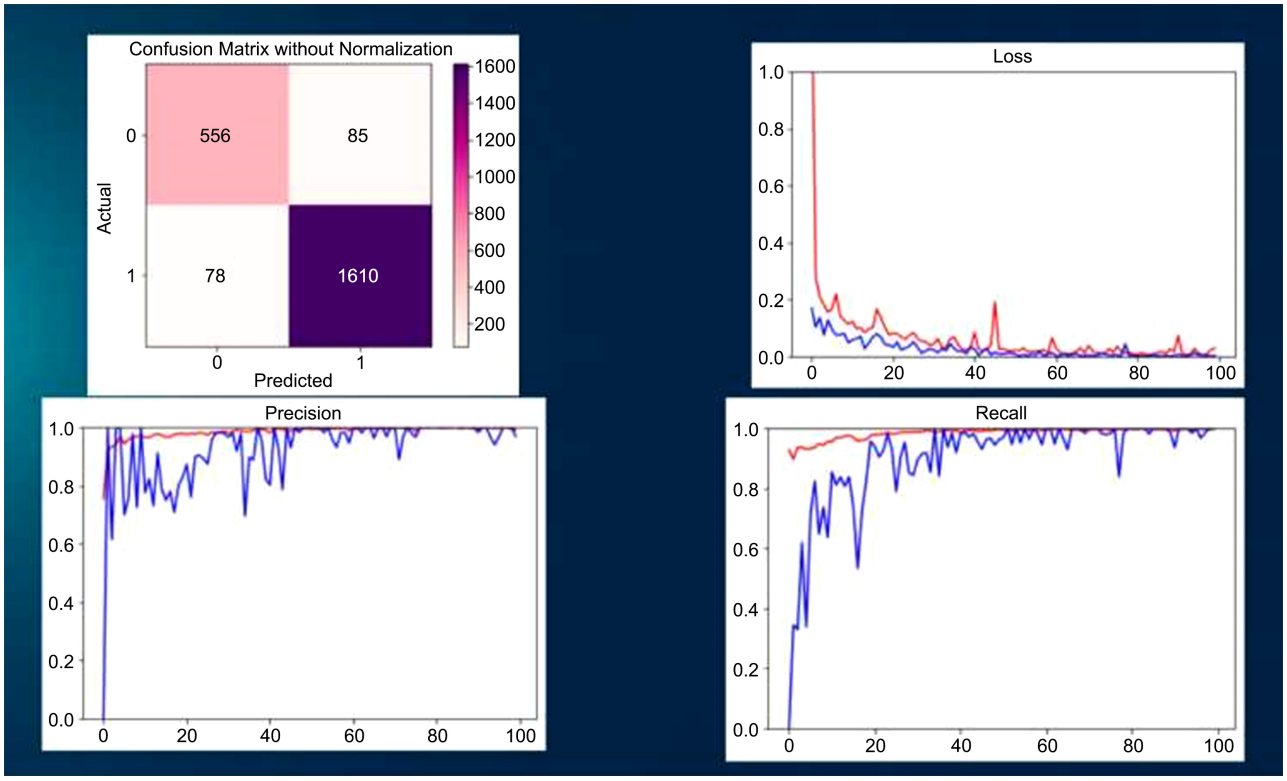

Figure 8. The confusion matrix is shown in the upper left corner, and the remaining graphs illustrate the loss, precision, and recall of the model depending on the number of training epochs.

Based on the confusion matrix (Figure 8), it can be observed that the CNN achieved high accuracy in the classification of drone sounds, as shown by the following results: True Positive (TP): 1610, True Negative (TN): 556, False Positive (FP): 85, False Negative (FN): 78. The approach and the achieved results of this methodology are resumed in the above pictures. The audio-recorded traces with and without Drone presence at different distances and in different environmental

conditions have been taken to collect a statistical meaningful data set to initially train the Andros Convolutional Neural Network (A-CNN). Then traces have been analyzed by professional freeware audio processing tools such as the popular "Audacity" to produce Spectrograms (image on the left) in which real-time spectra are shown versus time (Figure 9).

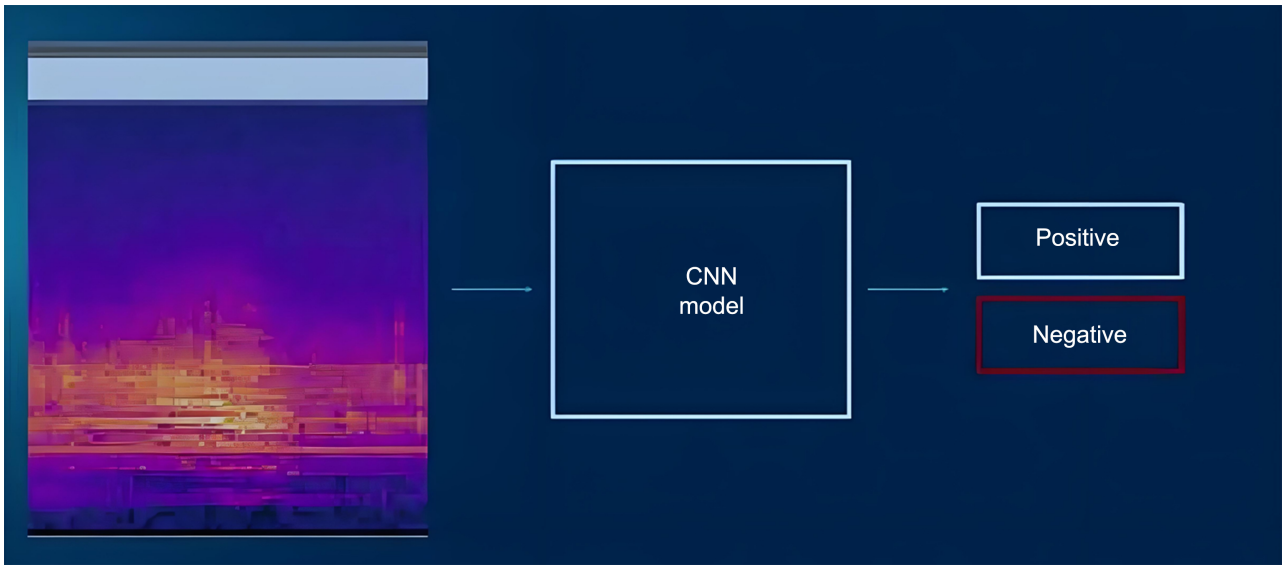

Figure 9. Data flow during the use of the model shown in Figure 8. A spectrogram is passed to the CNN, which, after calculation, classifies the result as positive or negative.

5. Conclusions

A long test campaign has been conceived to asses the overall performances of the design, realizing two evolutive models: a Demonstration Model and a Final Model. The difference between the two models is related to the number of masts, each one including three long-range horns and three Beamforming assemblies, their electronics, and communication systems. Another difference is that on FM, optical cameras are present to show the context scenery on the screen of the control center. The test campaign was conducted in different real conditions, including various temperatures, humidity, rain, and environmental noise to measure the actual performances. From these tests, we demonstrated the capability of the system to operate and detect an approaching drone and its limits. In the best conditions, the system exceeds the requirements by 40%, reaching 1400 m. In the worst case, the reference drone, a DIJ Phantom 5, can be detected up to 600 m.

Thanks to this approach standard pictures could be used to feed the A-CNN and train the network with the audio spectrum taken in the different conditions (lower right pic).

The A-CNN training, validation, and testing accuracy achieved are shown in the above Figure 8 & Figure 9. The "convergence time" is portrayed in terms of the minimum number of epochs needed to get the highest result. The "loss" plot refers to the loss value over the training data after each epoch. And this parameter

is what the optimization process is trying to minimize with the training so, the lower, is the better. It measures the percentage of test images that were predicted as a specific class and belong to that class. "Precision" shows how the A-CNN predicted *i.e.* the percentage of test images that were predicted as a specific class (with or without drone) and belong to that class. The "recall" is calculated as the ratio between the number of Positive samples correctly classified as Positive to the total number of Positive samples, in this case, the higher it is, the better it is.

Finally, the confusion matrix is also shown. The 4 elements of the matrix represent the 4 metrics that count the number of correct and incorrect predictions the model made. Each row evidences the prediction without drones (top row), and with drones (bottom row). The top left quadrant portrays how many times the model correctly classified a Negative sample as Negative (True False), while the top right quadrant identifies how many times the model incorrectly classified a Negative sample as Positive (False Positive). Conversely, the lower bottom quadrant similarly portrays the number of False negative and True Positive.

The good scores achieved in this preliminary implementation based on picture analysis of already existing CNN models strongly encouraged us to further develop a proprietary A-CNN model that will be included in the FM directly using the time data traces which will be an object of further publications.

The main technique used during training to counteract the overfitting of the CNN model was to monitor the model's performance on a validation set during training and stop training when the performance on validation set 1 stopped improving. In reality, the amount of data (hundreds of hours of UAV flight sounds and background noise) used during training significantly exceeded the hardware capabilities, which prevented reaching a point where the network could be determined as overfitted. This avoided extensive fitting to the training data and prevented model overfitting. The diversity of the data also counteracted overfitting because it came from various sources (15 different UAVs), under different atmospheric conditions (wind, pressure, air humidity, temperature, etc.), different terrain shapes, different terrain coverage with vegetation, but also snow, ice, and water bodies), from various distances, which allowed for a large variation in amplitude concerning noise. Some of the data was artificially generated (data augmentation) by adding moving vehicles, people, speech, music, passing airplanes, etc. After the model was implemented, accuracy and reliability tests were performed in the field using visual inspection, and subsequently, the data from the device and the data from the UAV were compared analytically.

A further set of detailed tests is being carried out at the time of writing, and an acoustic localization algorithm is also under development. The results of these ongoing activities will be the subject of a second paper that will be submitted shortly.

Acknowledgement

Andros System and this paper have been developed thanks to the EU RESTART

2016-2020 Programmes, INNOVATE 1221 0048—ANDROS Contract.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Holman, B. (2009) Airminded: Airpower and British Society, 1908-1941. https://theaha.org.au/airminded-airpower-and-british-society-1908-1941-mostly/

[2] Seubsaeng, A. (2003) Drones: Everything You Ever Wanted to Know But Were Always Afraid to Ask. Mother Jones. https://www.motherjones.com/politics/2013/03/drones-explained/

[3] Hall, K. (2024) Experimental Air Power: Early British Drone Programs and Western Violence in the Interwar Period. *Critical Military Studies*, **10**, 547-561. https://doi.org/10.1080/23337486.2023.2300024

[4] Klein, C. (2012) Attack of Japan's Killer WWII Balloons, 70 Years Later. Digital Publication.

[5] Bott, I., Jones, C. and Burn-Murdoch, J. (Oct. 8, 2013) Great and Small: The Many Types of Drone. Enc. Britannica.

[6] Cole, C. (2014) Rise of the Reapers: A Brief History of Drones. Air and Space Magazine. https://dronewars.net/2014/10/06/rise-of-the-reapers-a-brief-history-of-drones/

[7] Mitsubishi Research Institute Inc. (2018) Support for the Social Implementation of Drones as Part of the "Industrial Revolution of the Sky". https://www.mri.co.jp/en/capabilities/drone.html

[8] Nappo, C.J. (2012) An Introduction to Atmospheric Gravity Waves. 2nd Edition, Academic Press.

[9] Casasanta, G., Petenko, I., Mastrantonio, G., Bucci, S., Conidi, A., Di Lellis, A.M., *et al.* (2018) Consumer Drones Targeting by Sodar (Acoustic Radar). *IEEE Geoscience and Remote Sensing Letters*, **15**, 1692-1694. https://doi.org/10.1109/lgrs.2018.2858930