# Compact Counter-UAS System for Defeating Small UAV in Complex Environments

**Alexander Wentzel, M.Sc.**
Helmut-Schmidt University
University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
GERMANY

wentzela@hsu-hh.de

**Jan Cornils, M.Sc.**
Helmut-Schmidt University
University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
GERMANY

cornilsj@hsu-hh.de

**Marco Valentin, M.Sc.**
Helmut-Schmidt University
University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
GERMANY

valentim@hsu-hh.de

**Ralf Heynicke, Dr.-Ing.**
Helmut-Schmidt University
University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
GERMANY

heynicke@hsu-hh.de

**Gerd Scholl, Univ.-Prof. Dr.-Ing.**
Helmut-Schmidt University
University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
GERMANY

scholl@hsu-hh.de

## *ABSTRACT*

*Since the danger posed by unauthorized unmanned aerial vehicles (UAV) has risen tremendously in recent years, the demand for proper detection, tracking and countering measures to defeat such threats is at least as high and overdue. Besides RF jammers, GPS Spoofing, HP lasers, EMP and projectile guns, a Counter-unmanned aerial system (cUAS) is a very efficient and effective countermeasure against unauthorized small UAVs.*

*The cUAS covered in this paper is a fully automated, versatile and mobile deployable system capable of intercepting almost every market available small UAV utilizing an air-pressure driven net launcher. In contrast to the alternatives listed above, the developed cUAS performs independent of the operational mode of the unauthorized small UAV, i.e., manually or automated controlled, or even GNSS or RF-denied. Our multi-sensor approach (camera, LiDAR and radar sensors) together with the implemented algorithms allow the cUAS to operate in a variety of environments like open airfields, over military grounds and in urban spaces, where many radar reflections typically impede the detection and tracking of small objects. The cUAS independently approaches, tracks, and/or intercepts identified UAVs with up to 20 m/s with a success rate of over 90 %.*

*In the paper, the performance of the cUAS prototype is demonstrated and evaluated. The interception capability as well as the dogfight performance on small UAV is tested and investigated. Furthermore, we also outline specific attack and defense strategies of the system and the characteristic process phases from initial detection and classification to the final interception and removal of the unauthorized UAV, and state the advantages of the developed multi-sensor platform over existing single-sensor systems.*

# 1.0 INTRODUCTION

Small unmanned aerial vehicles (UAV), commonly known as drones, are still a rising threat for the society and many industries. While UAVs offer various benefits and opportunities for many fields of application, they also pose a tremendous risk and danger which is extremely difficult to counter.

In this paper, we present a compact Counter-UAS system including a newly developed interceptor UAS to counteract the threat of unauthorized UAVs. First, we outline the related work on reasonable countermeasures currently available on the market. Afterwards, the advertised compact Counter-UAS System is presented, while elaborating on its components (including a ground station) and its approach of countering small UAVs. In that course, the performances of the sensors of the interceptor UAS's multi-sensor platform as well as the interception strategies are presented. Finally, the overall system's performance in comprehensive, rear scenario tests are evaluated and presented to proof the countermeasure capabilities and effectiveness of the presented system.

To effectively and safely fight an unauthorized UAV in mid-air, it is necessary to physically stop and tow it away to eliminate the threat, while not letting it fall down. These requirements can only be met by an interceptor UAS, since alternative counter measures usually either cause the unauthorized UAV to crash and fall down (hard kill) or cannot ensure a fast, overall intervention in a timely manner (due to approaches like control manipulation). However, there are a variety of challenges for an automated interception UAS like the detection of small objects with light-weight sensor system, an air-to-air combat against small, agile and much lighter UAV and deploying a netgun effector with relatively small effective range.

## 1.1 Related Work

As the UAV market increases, the work and research relating counter measures increases accordingly. The counter measures are often categorized in physical and nonphysical mitigation. For each category there are different approaches to countering UAVs which are described in this section.

### 1.1.1 Nonphysical Mitigation

One approach for nonphysical mitigation is *GPS spoofing*. Valid but wrong GPS signals, that have a larger signal power than the legitimate GPS signals sent by satellites [1], are generated by the attacker and sent to the victim. Here, a clear line of sight from attacker to victim is required, since the GPS spoofing attacks rely heavily on the relative position between attacker and victim [2]. This approach includes manual and autonomous UAVs but it takes time, is very complex, often unreliable and can be nullified by manual (GPS denied) control of the UAV operator [3].

Another approach is the *RF Jammer*, that focus on paralyzing radio communication by interfering RF signals. High-power RF signals are either sent in a broad frequency spectrum [4, 5] or intelligently in the currently used frequency spectrum [6] to interfere remote control and GPS signals of the UAV. This interference causes UAVs to enter a failsafe mode or loses control, but has little to no effect on autonomous UAVs [7]. In general, the effect and consequence of the disruption is basically unpredictable.

Additionally, there are *High-power (HP) Electromagnetic (EM)* waves used to impair the UAVs electronic systems. Here, it is distinguished between wideband and narrowband EM [8]. The narrowband EM also referred as HPEM transmits high-power on a single frequency. After determining the UAVs exact frequency of operation, the HPEM will be used for that frequency and results in irreversible damage to the UAVs electronics [9]. The wideband EM transmits short pulses in time domain which requires accurate direction of the EM waves, since there will be a low lethality rate otherwise [10].

Another nonphysical mitigation approach is using *Lasers* that can be used with low and high power. Low power lasers dazzle the UAV's sensitive electro optical (EO) or infrared (IR) sensors. High-power lasers ionize the path to the UAV and emits an electrical current down the conducting track of the ionized plasma [9, 11], which can destroy the UAV. For using lasers accurate aiming and tracking of the UAV is required [10].

### 1.1.2 Physical Mitigation

Using *Projectiles* like machine guns, sniper rifles and guided missiles is the traditional approach to neutralize UAVs, due to the reaction possibility. But either the costs for special munition is very high or the accuracy is extremely low and this harsh method may cause collateral damage [10, 11, 7].

Another approach is to use *Nets* that are either ground based and shot at the UAV [12, 13, 14, 15] or deployed in mid-air. However, the handheld approach has a very limited range for mitigation. To overcome the range limitations UAVs are equipped with nets, sensors and artificial intelligence (AI) to autonomously intercept UAVs and are referred to as Counter-UAS. These Counter-UAS can detect, track, chase and shoot a net at the UAV. The shot nets have a drag-chute or a parachute attached to lower the shot UAVs descend rate and minimize damage [16, 17, 18, 19, 20]. Other counter UAS that shoot nets have a rope attached to net so that the intercepted UAV can be transported to a safe location [21, 19, 20]. There are also Counter-UAS that have loose-hanging nets or threads to intercept UAVs [22, 23, 24].

The last approach is to use *Collision UAVs* equipped with sensors and AI that intercept the UAV's trajectory and crash into it which will cause both UAVs to fall to the ground [25].

## 2.0 COMPACT COUNTER-UAS SYSTEM

The Counter-UAS system presented in this paper consists of an interceptor UAS and a ground station with detection and control capability (see Figure 1).

The interceptor UAS is designed to automatically perform an intercept of a small intruder UAV on its own. It is based on an off the shelf UAV with a payload capacity of about 10 kg. An NVIDIA Jetson Xavier NX companion computer is attached to the UAV, which handles the data processing and communication with the UAV's flight controller unit (FCU). In addition, a wireless data link is attached to communicate with the ground station. Self-developed net launchers are applied to catch the opponent UAV. A multi sensor system including an Echodyne EchoFlight airborne radar, a Blickfeld Cube 1 LiDAR and an Intel Realsense D415 stereo camera is gathering the data for the algorithms running on the companion computer. The whole interceptor UAS weights less than 20 kg and is smaller than 80 cm in all dimensions (packed).

The ground station consists of a detection system and a control unit. The Echodyne EchoGuard radar used as the detection system, which weighs about 1 kg, can be connected to the ground station via Ethernet. The detection system is equipped with GPS and position sensors to automatically determine its location and position. Thus, the ground station can be used mobile and with very little setup needed. The radar classifies UAVs automatically and reports them to the command-and-control software (laptop).

The ground station offers system wide control options to the operator. The interception process can be monitored and controlled at any time, including catch authorization, drop zones or no-fly zones. A color image, received from the interception UAS, is displayed to the operator to be able to capture the interception process from a birds-eye perspective.

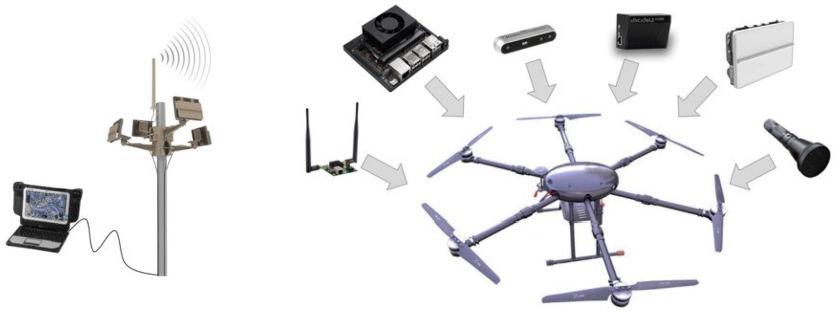

**Figure 1: Hardware components of the ground detection and control station (left) and the interceptor UAS (right) [product photos from respective manufactures].**

# 3.0 INTERCEPTION PROCESS

The interceptor UAS counteracts unauthorized UAVs by capturing them in mid-air using a net. The advantage of this approach is that it is effective regardless of the opposing UAV and its operation mode. Whether it is autonomous, mission or manually controlled, the UAV can be stopped either way, without being destroyed. The challenges of the interception approach are the high complexness and technical requirements on the interceptor UAS, which are covered in this section.

To intercept a small UAV, the interceptor UAS needs to detect and track the target UAV with its onboard sensor system at all time to allow a precise positioning relative to the target UAV. Once the netgun has been positioned at an effective position, the net will be shot at the target UAV, which then tangles itself in the net and remains tied to the inceptor UAS for safe disposal.

## 3.1 Detection

As shown in Section 2.0, the Counter-UAS system includes a ground detection unit and various onboard sensors. Object detection takes place for each sensor individually. The developed detection algorithms identify an updated object location based on its previous locations.

To test, tune and verify the sensors and object detection algorithms, they have been evaluated in a ground-based, stationary test. Major performance criteria for the interceptor UAS's sensor system are the detection ranges and reliability of the individual sensors. For this test, the individual sensors were placed on a predefined location and position while a small DJI Phantom 2 sized UAV flew a predefined path in front of the sensors. For evaluation the recall rate is determined by the ratio of successful detections over possible detections. The results are shown in Figure 2. The location of the sensors is marked with a black arrow. The flown path of the small UAV is shown in black and serves as a reference for this test. The distance between the flown UAV and the stationary sensors was in the range from 14 to 100 m. This test found that the developed object detection algorithm of the stereo camera had difficulties identifying the correct object when viewing at a poorly structured background, in this case the sky, because this creates a lot of noise and makes it difficult to identify the right object. The right graph in Figure 2 shows that the recall rate, of the object detection of the stereo camera is about 50 % at a distance of up to 30 m. From 30 m it was no longer possible to distinguish whether it was the right object or noise, which is why we decided to only test the stereo camera up to 30 m. The recall rate of the LiDAR is over 90 % at distances of up to 29 m. After that, it decreases significantly. The last detection was measured at a distance of 36 m. The radar has a dead zone from 0 to 20 m. At distances between 20 m and 100 m, the radar was able to detect the flown UAV with a mean recall rate of about 30 %.

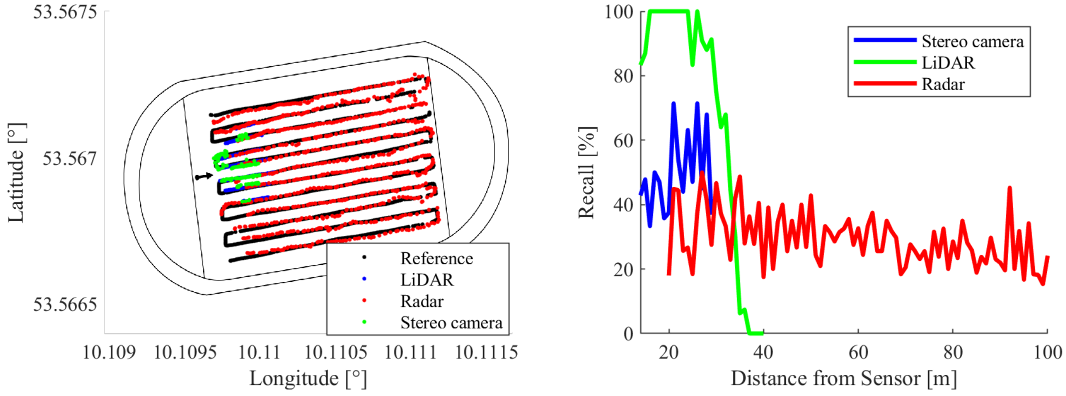

**Figure 2: Test results of ground-based sensor tests. Left, the reference positions and detected positions of a flying small UAV. Right, the detection recall for each sensor.**

From this test it can be concluded that the radar is a good way to detect UAVs over long distances. At distances smaller than 30 m, the LiDAR has proven to be a reliable sensor. The stereo camera is suitable as an additional sensor for short distances with a slightly larger field of view than the LiDAR. However, the stereo algorithms have difficulties at less structured backgrounds, which makes the sensor far less reliable. Finally, combining these sensors into a multi-sensor platform for the interceptor UAS, lowers the weaknesses of every single sensor and improves the overall performance over a wider detection range.

## 3.2 Strategy

The overall goal of the interceptor UAS is to bring its effector in an advantageous position to fight and stop the intruder. In general, there are two major strategies for the interceptor UAS to deploy: Attack and Defend.

For the air pressure driven netgun effector, the most advantageous strategy is to attack the target UAV from behind. This is because the target can be chased in a safe distance, until there is an appropriate situation to catch up, bring the netgun into an advantageous position and shoot the net at the target. The limit of this strategy is a considerably fast-moving target, because strong headwinds will interfere with the net and lower its effective range, or, if the target is moving even faster than the intruder UAS could. In these cases, the interceptor UAS may intersect the target's trajectory in a defence manner, and deploys the net at its flight path, so that the target is flying into the net. The challenge of this defence strategy is the exact timing and a precise long-range detection. However, in this paper, the focus is on the attack strategy and the automation of its interception process.

Because of the choice and configuration of the interceptor UAS's sensor system for tracking the small UAV during the interception process, the attack strategy can be split in five phases with different characteristics and priorities: Stop, Search, Approach, Chase, Catch. Figure 3 shows the conditions of each phase and the transitions between the phases.

Each phase has an individual goal, which usually leads to the transition to the next phase. This goal is basically to reach a new relative position to the unauthorized UAV, further referred to as target object, to either get better detection results, or deploy the netgun. The newly desired relative position is calculated globally and called destination position. Algorithms continuously update the destination position using the newest data on the target object. Depending on the phase, the destination position is either approach as fast as possible, or while keeping the target object in sensor view, or any other constrains.

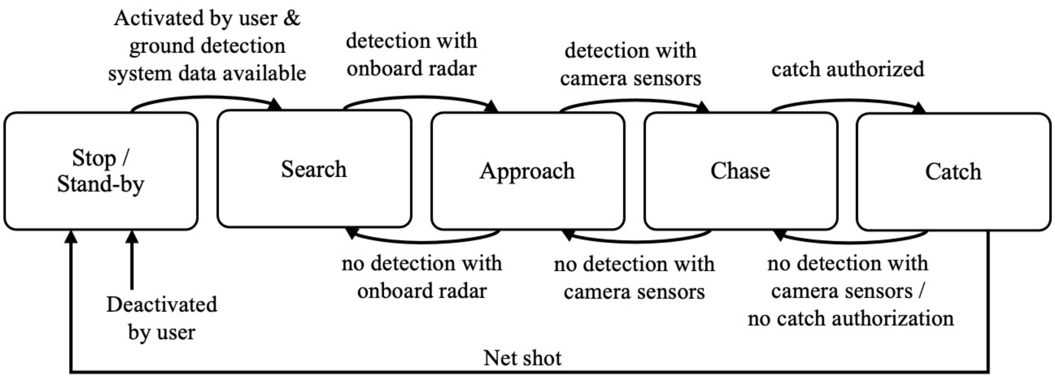
Activated by user & ground detection system data available
detection with onboard radar
detection with camera sensors
catch authorized
Stop / Stand-by
Search
Approach
Chase
Catch
no detection with onboard radar
no detection with camera sensors
no detection with camera sensors / no catch authorization
Deactivated by user
Net shot

**Figure 3: Phases of the interception process and their conditions.**

# 4.0 INTERCEPTION PERFORMANCE

The above concepts (detection and interception) have been brought together and deployed to an interceptor UAS for a full system test. The evaluation and data records are presented below.

## 4.1 Interception

Two interception processes have been recorded and are evaluated below. One being an unauthorized intruder UAV that enters a protected area in a straight flight. The other being an unauthorized intruder UAV, which is flying an arbitrary route, potentially trying to escape the interceptor UAS. Here, a DJI Phantom 2 sized UAV was used as intruder.

The two interception processes show and proof the functionality, the emphasized strategy and phases of the developed Counter-UAS interceptor system. To start the interceptor and during search phase, the ground detection system sends the rough position of the unauthorized intruding UAV. Further down the process, the interceptor UAS's onboard sensors take over and the system operates completely on its own.

### 4.1.1 Straight Line Intruder

An unauthorized UAV is moving on a straight line at about 8.5 m/s ground speed and about 20 m height. The interceptor UAS has been activated as the ground detection system detects the unauthorized intruder UAV at a distance of 200 m.

In the following diagrams, the travelled path of both UAVs, the velocities and relative distances to each other are shown. The arrows show the start positions of the unauthorized UAV (red) and the interceptor UAS (green). The red cross indicates the interception points, where the shot net hits the unauthorized UAV.

The interceptor UAS takes about 13 seconds and accelerates up to 12 m/s to get that close to the 200 m away unauthorized UAV that the onboard radar locks on to the target object and the interceptor is able to proceed without any information from the ground detection system. From that time, it took a little less than 30 seconds for the interceptor UAS to catch the unauthorized UAS. It took about 16 seconds to safely approach from about 100 m distance to less than 20 m distance, where the other onboard sensors took over. Shoot authorization has been given immediately, so that the catch phase started already about 2 seconds after the chase phase. About 8 seconds later, the interceptor UAS reached the final position to effectively deploy the net at about 5 m horizontal distance and 3 m above the target object. So, all in all, the unauthorized UAV has been caught less than 45 seconds after it has been detected at 200 m distance.

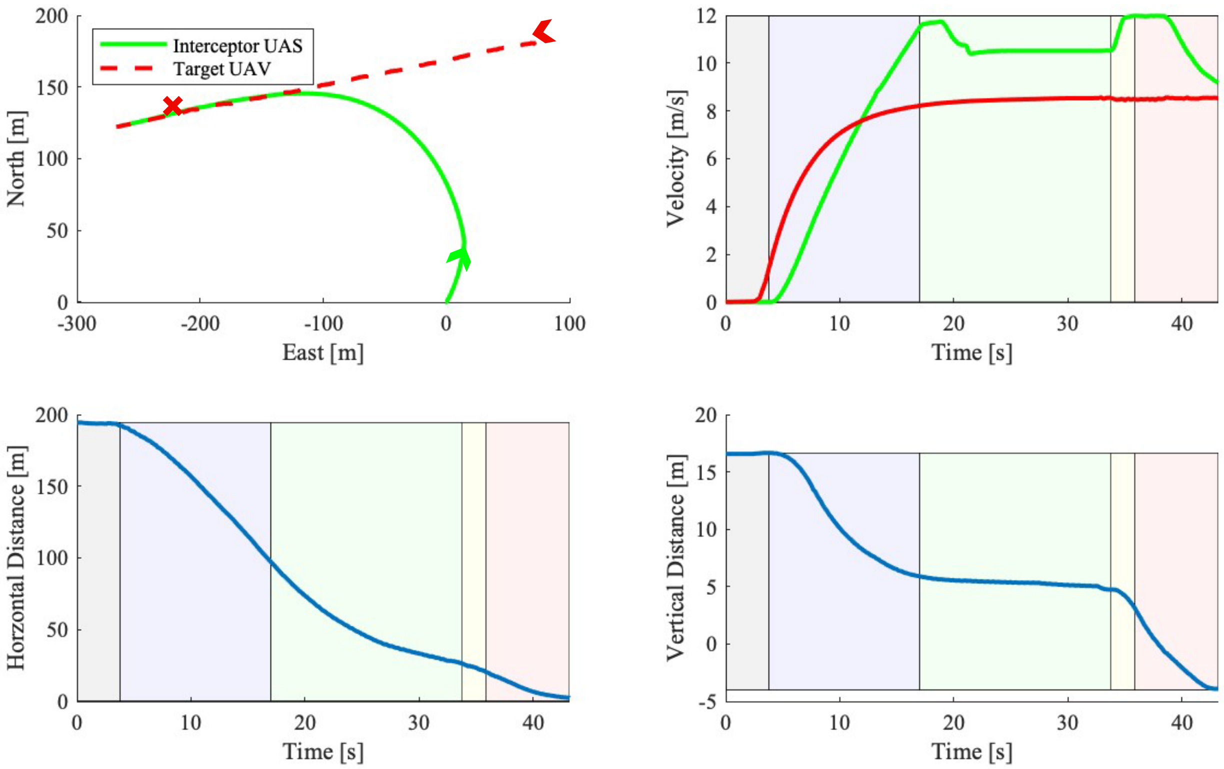

**Figure 4: Recorded data from straight line intruder interception process (travelled path, velocities, distances between interceptor UAS and unauthorized UAV).**

### 4.1.2 Dynamic Intruder

An unauthorized UAV is moving on an arbitrary route which is not in any way predictable for the interceptor UAS with a groundspeed of about 7.5 m/s. The arrows show the start positions of the unauthorized UAV (red) and the interceptor UAS (green). The red cross indicates the interception points, where the shot net hits the unauthorized UAV.

The focus of this test is the interceptor UAS's chasing (dogfight) capability. Therefore, we let the interceptor UAS chase the unauthorized UAV for about 100 seconds before authorizing the catch. During this whole test, the unauthorized UAV flew arbitrary curves. From the distance graphs, it can be seen, that, while chasing, the interceptor UAS kept a steady distance of about 13 m horizontally and 4 m above the target object at all time. At the velocity recordings, there are some few irregularities compared to the previous test, which are due to the changes in direction in the curves, which are handled well by the interceptor UAS's controllers. Finally, after authorizing the catch, it took about 6 seconds for the interceptor UAS to position its netgun and shoot the unauthorized UAV. The subsequent disposal and returning home have not been recorded.

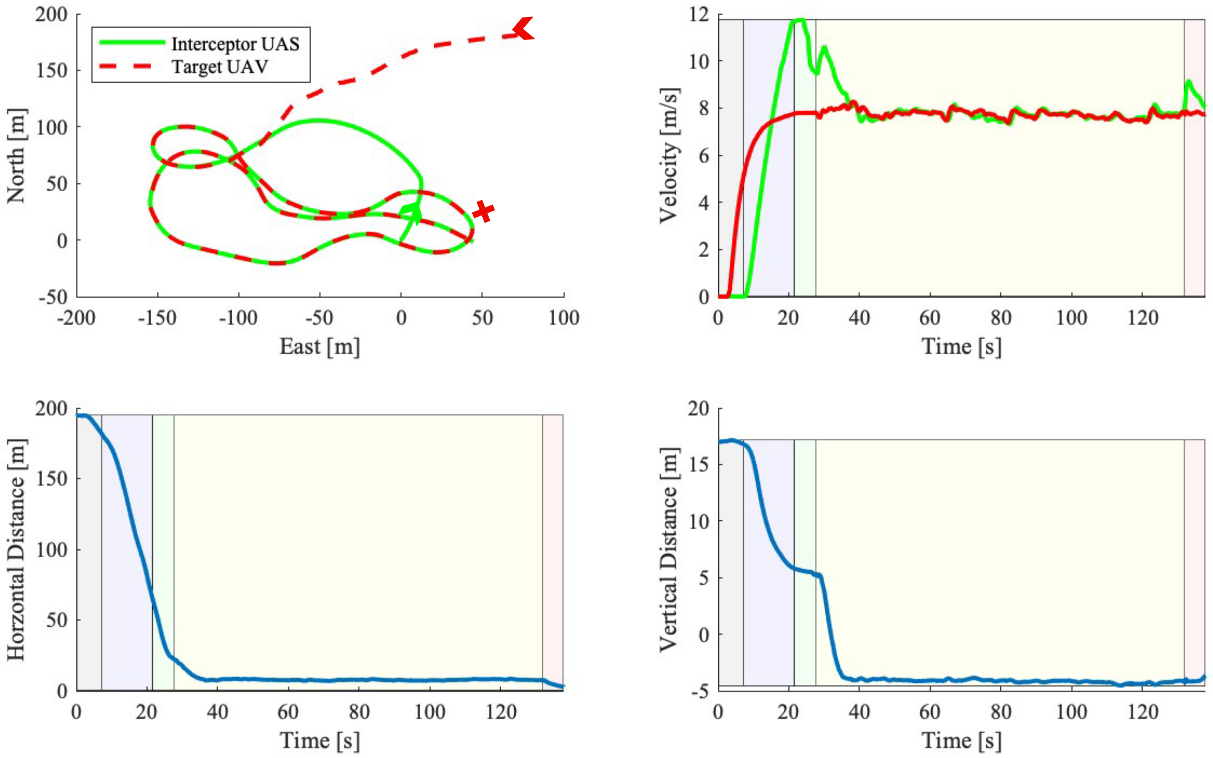

**Figure 5: Recorded data from dynamic intruder interception process (travelled path, velocities, distances between interceptor UAS and unauthorized UAV).**

## 4.2 Detection

On the interceptor UAS, the stereo camera and LiDAR sensor are mounted on a pan-tilt-head, which ensures the orientation of the sensors towards the target object. The radar is directly mounted to the UAS's frame and, thus, dependent on its position. The data presented below has been recorded during several interception processes. Figure 6 shows the detection ranges and the recall rates of the individual sensors.

According to the results of the previous tests, during interception, the stereo camera is only used when looking downwards (chase and catch phase) to minimize the difficulties with unstructured backgrounds (e.g. sky). This resulted in a recall rate of over 90 % for objects closer than 8 m. From 8 to 15 m, the recall rate drops significantly, as this is the transition range, where the interceptor UAS changes its position from below the target object (search and approach phase) to above the target object (chase and catch phase), when the detection algorithms do not run continuously. However, the LiDAR senor has a comparably good detection recall rate of over 70 % up to a distance of 14 m. After that, it decreases down to 12 % at 22 m, which is due to the transition from below the target object to above the target object, as the Counter-UAS's propellers temporarily interfere with the LiDAR's beams. For the radar sensor, the detection recall rate is at an improved 45 % in average for the range of 20 m (blind range) to 100 m. From the graph of Figure 6 it can also be seen how the combination of all sensor together cover the whole range of about 2 m up to 100 m.

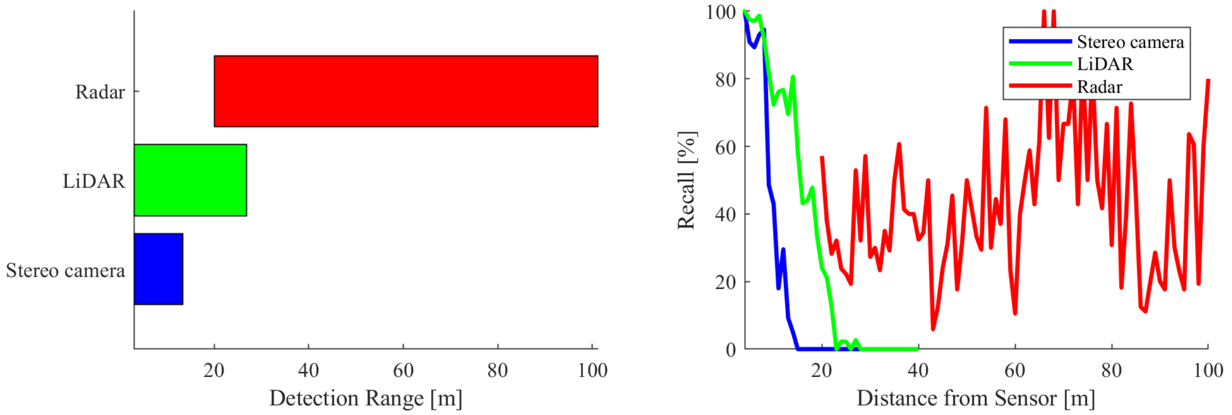

**Figure 6: Detection range (left) and recall (right) of the sensors during an interception process.**

## 5.0 CONCLUSION

Although there is a variety of countermeasures to the increasing threat of small unmanned aerial vehicles (UAVs) available on the market, most of them are ground based solutions and very limited in their field of application. To provide a new countermeasure and to offer further possibilities of intervention a compact Counter-UAS system has been developed. The system consists of a small ground station (laptop + radar) and an automated interceptor UAS and can easily be used by a mobile operations team, with minimal setup time, or stationary in an integrated system. The interceptor UAS's components have been addressed and the different sensors have been evaluated. This has shown that the multi-sensor platform achieves a good detection performance over the tested range. The developed interception strategies for the system have shown that the interceptor UAS is able to eliminate a UAV threat in a range of 200 m in less than 40 seconds. Thus, the system has been proven to be a functional, compact and effective countermeasure.

To further improve the system, the defence strategy needs to be adequately evaluated and tuned next. This would improve the system's difficulties on fast moving objects and thus, makes it suitable for even more scenarios. Furthermore, an improved netgun or even other effectors may facilitate a wider range of applications.

## 6.0 REFERENCES

[1] N. O. Tippenhauer, C. Pöpper, K. Rasmussen and S. Capkun, "On the requirements for successful GPS spoofing attacks," 2011.

[2] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi and Y. Kim, "Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing," *ACM Transactions on Privacy and Security,* Bd. 22, pp. 1-26, April 2019.

[3] S. Khan, M. Mohsin and W. Iqbal, "On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions," *PeerJ Computer Science,* Bd. 7, p. e507, May 2021.

[4] K. Pärlin, M. Alam and Y. Le Moullec, "Jamming of UAV Remote Control Systems Using Software Defined Radio," 2018.

[5] K. Grover, A. Lim and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad Hoc and Ubiquitous Computing,* Bd. 17, p. 197, January 2014.

[6] K. Dabcevic, “Intelligent jamming and anti-jamming techniques using Cognitive Radios,” 2015.

[7] S. Park, H. Kim, S. Lee, H. Joo and H. Kima, “Survey on Anti-Drone Systems: Components, Designs, and Challenges, spoofing, high-power, projectiles,” *IEEE Access,* Bd. PP, pp. 1-1, March 2021.

[8] W. A. Radasky, C. E. Baum and M. W. Wik, “Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI),” *Electromagnetic Compatibility, IEEE Transactions on,* Bd. 46, pp. 314-321, September 2004.

[9] B. Zohuri, “RETRACTED CHAPTER: High-Power Microwave Energy as Weapon,” in *RETRACTED BOOK: Directed-Energy Beam Weapons*, Cham, Springer International Publishing, 2019, p. 269–308.

[10] H. Kang, J. Joung, J. Kim, J. Kang and Y. Cho, “Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems, spoofing, high-power, projectiles,” *IEEE Access,* Bd. 8, pp. 168671-168710, January 2020.

[11] V. Castrillo, A. Manco, D. Pascarella and G. Gigante, “A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones, spoofing, high-power, projectiles,” *Drones,* Bd. 6, p. 65, March 2022.

[12] OpenWorks, “Skywall,” Sep. 2023. [Online]. Available: https://openworksengineering.com/skywall-auto/.

[13] Koller Engineering, “DRONEGUN MKIII,” Sep. 2023. [Online]. Available: https://www.koller.engineering/produkt/dronegun-mkiii/.

[14] UAVOS, “Drone-capture net system,” Sep. 2023. [Online]. Available: https://www.uavos.com/products/uas-payloads/interception-system-for-uav/.

[15] Pacem Defense, “SKYNET Mi-5,” Sep. 2023. [Online]. Available: https://www.lesslethal.com/products/12-gauge/als12skymi-5-detail.

[16] Theiss UAV Solutions, “Excipio Aerial Netting System,” Sep. 2023. [Online]. Available: http://www.theissuav.com/counter-uas#excipio-aerial-netting-system.

[17] Airobotics, “Iron Drone,” Sep. 2023. [Online]. Available: https://www.airoboticsdrones.com/iron-drone/.

[18] SKYSEC, “Sentinel,” Sep. 2023. [Online]. Available: https://www.skysec.ch/#section-sentinel-catch.

[19] DelftDynamics, “DroneCatcher,” Sep. 2023. [Online]. Available: https://dronecatcher.nl/.

[20] Fortem Technologies, “DroneHunter F700,” Sep. 2023. [Online]. Available: https://fortemtech.com/products/dronehunter-f700/.

[21] SCI Technology, “AeroGuard,” Sep. 2023. [Online]. Available: https://www.sci.com/aeroguard/.

[22] EAGLE.ONE, “drone hunter,” Sep. 2023. [Online]. Available: https://eagle.one/en/about.

[23] ROBOTICAN, “Goshawk,” Sep. 2023. [Online]. Available: https://robotican.net/goshawk-autonomous-drone-interceptor/.

[24] Search Systems, “Sparrowhawk,” Sep. 2023. [Online]. Available: http://www.searchsystems.eu/sparrowhawk.html.

[25] Skylock, “Drone interception system,” Sep. 2023. [Online]. Available: https://www.skylock1.com/modular-components/counter-drone-mitigation-systems/dronelock/.