International Journal of Marine Engineering Innovation and Research, Vol. 11(3), Sept. 2026. 973-983
(pISSN: 2541-5972, eISSN: 2548-1479)

Implementation of A Geofence-Based Anti-Theft System and Real-Time Notifications on USV

Setyawan Ajie Sukarno[1*], Jenaya Aurielle Feriwijaya[2], Dini Hadiani[3], Wahyudi Purnomo[4], Riky Adhiharto[5]

(Received: 10 June 2026 / Revised: 12 June 2026 / Accepted: 17 July 2026 / Available Online: 1 September 2026)

Abstract— Unmanned Surface Vehicles (USVs) are increasingly deployed due to technological advancements, yet their physical security remains significantly under-explored. While anti-theft frameworks are widely adopted for land vehicles, these systems rely on passive mechanisms that only alert the owner, failing to prevent the physical removal of the asset. To address this critical gap, this study proposes an active anti-theft system for USVs featuring a dual-layer detection mechanism utilizing spatial geofencing, physical attitude anomaly detection, and real-time notification. First, the USV was equipped with these sensors and connected to an onboard edge computing unit to continuously monitor spatial and attitude data. Second, upon detecting a geofencing breach, the system automatically triggers a Return-to-Launch (RTL) maneuver while transmitting a real-time notification to alert the operator. Third, an attitude anomaly breach transmits an immediate alert about the vessel's unusual tilt. Finally, the complete architecture was evaluated through controlled and real-world environment testing to validate evasion success and communication latency. Testing demonstrated that the system reliably executes autonomous return protocols with low-latency communication. By transitioning asset protection from passive monitoring to active defense, this multi-layered framework establishes a novel foundation for physical security in USVs.

Keywords— Autonomous Self-Preservation, Edge Computing, Geofencing, Low-Latency Telemetry, Maritime Asset Protection.

**Corresponding Author : ajie@ae.polman-bandung.ac.id*

I. INTRODUCTION

Driven by technological advancements, the capabilities of Unmanned Surface Vehicles (USVs) have significantly increased. USVs are introduced to higher levels of automation, such as deep learning applications, coordinated control, and collision avoidance [1], [2], [3], [4]. Modern USVs also integrate advanced broadband telemetry and autonomous navigation software, enabling operators to execute complex and real-time decision-making from remote locations [5]. As these USVs become central to ocean digitalization and long-range missions, they have evolved into highly sophisticated and valuable operational assets [2], [6], [7].

Despite these advancements, USV security research remains significantly underexplored compared with navigation and control [8]. Although the onboard crew's removal effectively reduces human operational error [9], but this physical absence creates a serious risk. With the absence of crew, the ship is completely exposed to physical dangers such as piracy and hardware tampering [10].

Existing security solutions—primarily designed for land vehicles—rely heavily on passive anti-theft mechanisms. For instance, land transport security systems heavily utilize IoT-based tracking and alarm systems. These effectively notify the owner about an ongoing theft, but they rarely stop the asset from being physically removed [7], [10], [11], [12]. Similarly, Unmanned Aerial Vehicles (UAVs) frequently use geofencing to restrict movement, keeping the drone from straying from its designated route or entering prohibited areas [13]. However, the translation of these systems into the maritime domain, specifically for USV, remains underdeveloped and underexplored in current literature. Most marine tracking systems still rely on basic, passive GPS modules that periodically send location updates without any autonomous defensive capabilities [4].

This absence of active anti-theft research in USVs creates a critical operational vulnerability. While passive tracking might be adequate for land and aerial vehicles, where the owners or authorities can quickly intercept the theft, it is fundamentally unfeasible in vast and remote open-water environments [6], [14]. If a USV is intercepted, a simple delayed notification leaves the vessel highly vulnerable to theft before operators can launch a recovery mission [15]. Therefore, there is an urgent need to transition from passive monitoring to an active defense system, allowing the USV to utilize its own computational and propulsion capabilities to actively resist theft [8].

To address this critical gap, the primary objective of this study is the development of an active anti-theft system integrated with a dual-layer detection mechanism. Unlike existing passive anti-theft architecture, this study utilizes spatial geofencing and physical attitude anomaly detection. This system is designed to autonomously trigger the vehicle's

Setyawan Ajie Sukarno. Departement of Automation Engineering, Politeknik Manufaktur Bandung, Bandung, 40135, Indonesia. E-mail: ajie@ae.polman-bandung.ac.id
Jenaya Aurielle Feriwijaya. Departement of Automation Engineering, Politeknik Manufaktur Bandung, Bandung, 40135, Indonesia. E-mail: jenayaaurielle@gmail.com
Dini Hadiani. Departement of Automation Engineering, Politeknik Manufaktur Bandung, Bandung, 40135, Indonesia. E-mail: dinibhs@polman-bandung.ac.id
Wahyudi Purnomo. Departement of Automation Engineering, Politeknik Manufaktur Bandung, Bandung, 40135, Indonesia. E-mail: yud_prn@yahoo.com
Riky Adhiharto. Departement of Automation Engineering, Politeknik Manufaktur Bandung, Bandung, 40135, Indonesia. E-mail: riky@polman-bandung.ac.id

propulsion to counter unauthorized movement via a Return-to-Launch (RTL) maneuver [16]. Additionally, this system is designed to detect physical attitude anomaly by calculating the USV's tilt on a certain limit to distinguish a theft attempt from natural waves. Simultaneously, the on-board edge computing unit transmits real-time telemetry notifications to the operator's Web-based Ground Control Station (Web-GCS), which subsequently triggers an alert on the operator's interface whenever a violation is detected. By combining autonomous physical evasion with real-time remote operator alerts, this proposed architecture aims for the USV to be effectively secured and retrieved to safety. At present, no existing literature integrates spatial geofencing and physical attitude detection into a closed-loop, active defense mechanism for USV. Consequently, this architecture constitutes a novel approach to USVs' physical security.

II. METHODS

The proposed anti-theft system for the USV is divided into two primary subsystems: the On-Board System and the On-Land System. The On-Board System exists on the USV itself. It handles direct sensing, computation, and actuation. Integrating microcontroller, autopilot module, and propulsion system [5], [17]. Additionally, the On-Land System serves as the monitoring hub, interfacing directly with the Web-based Ground Control Station (Web-GCS) to provide real-time situational awareness and telemetry tracking [18], [19]. The system is illustrated in Fig. 1.

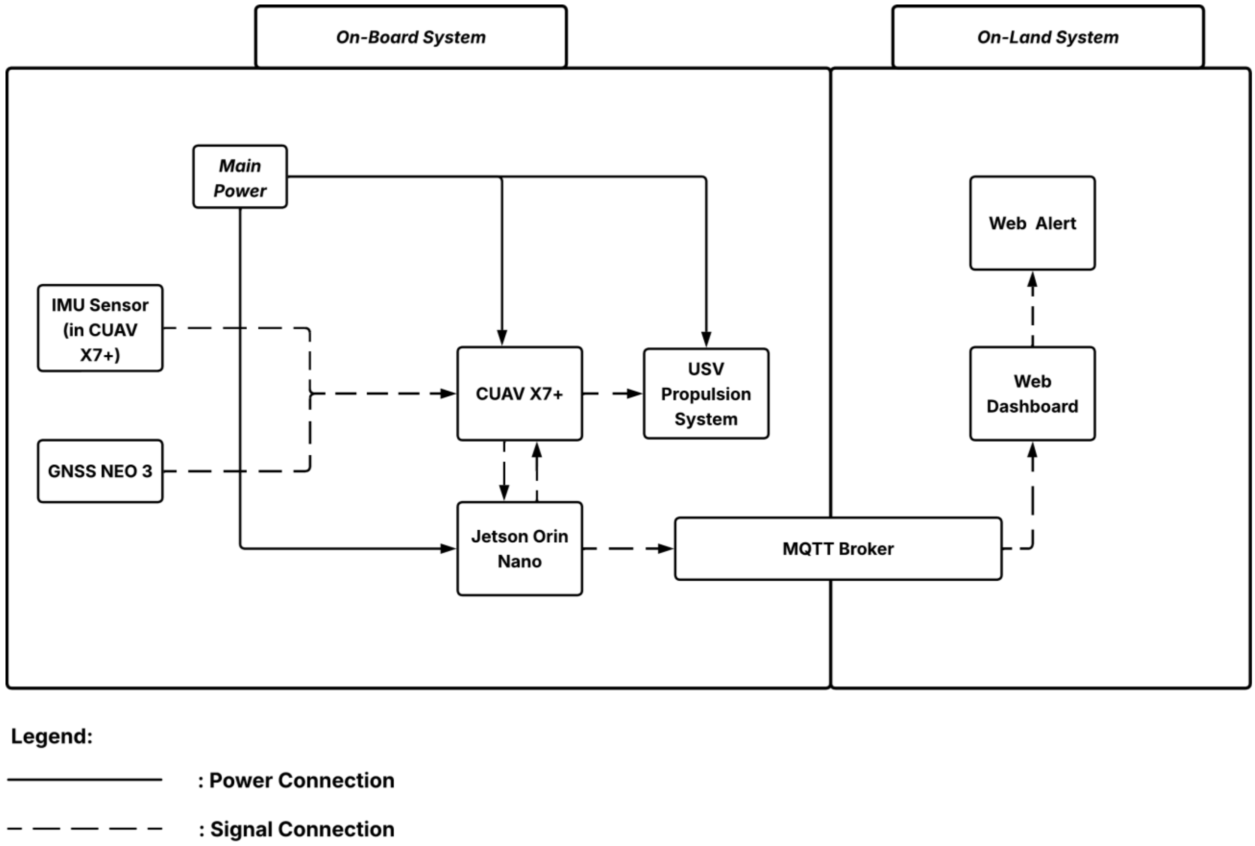


Figure 1 On-Board and On-Land System of The Anti-Theft

A. Hardware Configuration

The hardware is divided into two component groups based on its operational environment to ensure robust physical security and reliable communication.

1) On-Board Components: To handle the computational load of anti-theft logic and real-time data processing, an NVIDIA Jetson Orin Nano is integrated into the system. It utilizes its Gigabit Ethernet port to transmit high-bandwidth telemetry data streams from the USV to the Web-GCS with minimal latency [20]. CUAV X7+ was selected due to its triple-redundant IMU ability, which ensure high fault tolerance [21]. In the event of a primary IMU failure, the backup sensor is automatically activated to maintain stability [21]. It is paired with NEO 3 GNSS module to provide a wide range selection of satellites (GPS, GLONASS, Galileo, and Beidou) . This module is designed to minimize electromagnetic interference from other onboard electronics, ensuring highly accurate positional data [22]. This configuration minimizes communication latency and ensures rapid, bounded-latency decision-making for the active defense system, which has been proven effective for real-time autonomous maritime operations [23].
2) On-Land Components: A laptop or PC monitoring station with a Web-GCS dashboard makes up the On-Land System components. The design guarantees immediate notification through the operator's device, successfully alerting the

monitoring staff without compromising the system's awareness to the intruder.

B. Software Implementation

The software implementation consists of ArduPilot firmware, MQTT Broker, ROS 2-based environment, and MAVProxy. The autopilot operates on ArduPilot firmware, which has been widely proven for robust autonomous navigation in marine vehicles [24]. To handle the data transfer—such as IMU and GPS coordinate—between the USV and the Web-GCS, MQTT Broker is used. The use of MQTT is based on its ability to provide reliable publish-subscribe messaging and its design minimizes code size, memory use, and network overhead [25]. A ROS 2-based environment running on the companion computer to execute the security script. By acting as a hardware abstraction layer, it translate the script into specific commands for each hardware component, ensuring the seamless operation of the anti-theft system [26]. To efficiently manage the data stream, a MAVProxy routing is integrated in the computer companion. It distributes incoming MAVLink serial stream from the autopilot into multiple UDP endpoints, enabling simultaneous data access for the ROS 2 environment and the MQTT communication [27].

C. Anti-Theft Protocol and Defense Mechanisms

The core anti-theft architecture of the USV relies on a multi-layered security approach, comprising dual detection parameters and an automated response system. The anti-theft protocol and defense mechanisms consists of virtual geofencing logic (spatial detection), tilt anomaly logic (attitude detection), and active defense and real-time notification (response & alert).

1) Virtual Geofencing (Spatial Detection)

The primary layer of security is a predefined virtual perimeter established via the Web-GCS. To establish this boundary, the NEO 3 GNSS module continuously monitors the USV's global coordinates. This positional data is fed to a radius-bounding algorithm implemented in Python, which computes spatial deviations in real-time.

First, to determine the absolute distance (d) between the USV's current position and its authorized waypoint, the algorithm utilizes the Haversine formula [28]:

$$d = 2r\times\arcsin(\sqrt{[\sin^2(\Delta\phi/2)+\cos(\phi_1)\times\cos(\phi_2)\times\sin^2(\Delta\lambda/2)]}) \quad (1)$$

Where r is the Earth's radius, $\Delta\phi$ is the difference between latitude in radians ($\phi_2 - \phi_1$), and $\Delta\lambda$ is the difference between longitude in radians ($\lambda_2 - \lambda_1$).

Second, to monitor lateral drift from the designated route, the system calculates the Cross-Track Error (CTE) [29]:

$$CTE = \text{asin}(\sin(d_{13}/r)\times\sin(\theta_{13} - \theta_{12}))\times r \quad (2)$$

Where r is the Earth's radius, d_{13} is the Haversine calculation, θ_{13} is the bearing from home location to current USV's location, and θ_{12} the bearing from home location to designated location.

By continuously evaluating these two metrics, the system indentifies a potential unauthorized relocation [30]. If either the USV's absolute distance or the XTE exceeds a predefined spatial threshold (e.g 3 meters), the algorithm instantly overrides the current navigation commands and executes a RTL maneuver.

2) Tilt Anomaly Logic (Attitude Detection)

As a secondary layer to prevent physical lifting within the secure zone, the system monitors the vessel's pitch and roll data from the CUAV X7+ IMU. To filter out natural wave oscillations, an anomaly is only flagged if the inclination exceeds a critical angle (e.g., 10°) continuously for a specific temporal threshold (e.g., 5 seconds) [31].

3) Active Defense and Real-Time Notification (Response & Alert)

Depending on the kind of the threat, the system initiates a certain multi-tiered action. A geofence breached initiates an immediate active defense respond, which is RTL. The propulsion system performs an autonomous RTL maneuver to navigate back to safety [32]. An attitude anomaly triggers an alert on the Web-GCS and disarmed the propulsion system. Simultaneously, the NVIDIA Jetson Orin Nano processes these breaches and transmits real-time notifications to the operators via the monitoring website, ensuring instantaneous situational awareness [33].

D. Experimental Setup and Testing Procedure

The data utilized in this research are quantitative, sourced directly from the telemetry logs and sensor readings of the On-Board System. Data retrieval is conducted in real-time through the Web-GCS during two progressive testing phases: a controlled environment test and a real environment test. The collected data are analyzed to determine the system's operational reliability, response latency, and overall defensive effectiveness. The testing phase follows a systemic workflow as illustrated in Fig. 2.

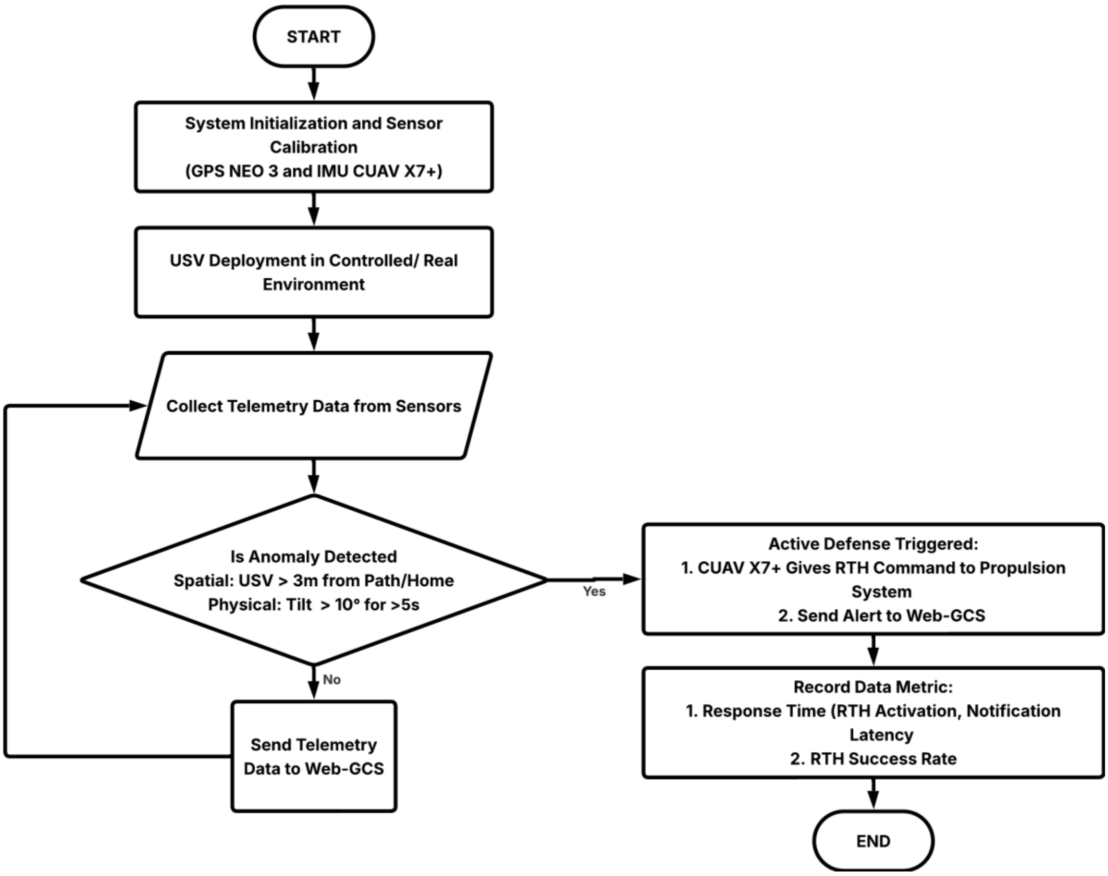


Figure 2 Experimental Setup and Testing Procedure Flowchart

1) Controlled Environment Test

The USV is deployed in a calm water environment with minimal wind and water currents. This phase has two primary objectives: first, to evaluate the accuracy of the NEO 3 GNSS module in recognizing the virtual geofence boundaries; and second, to validate the attitude anomaly detection algorithm by physically simulating an unauthorized lifting attempt. Key metrics collected include the system's response time—specifically, the temporal delay between the threshold breach (either spatial or physical) and the exact moment the thrusters actively initiate the RTL maneuver.

2) Real Environment Test

To assess robustness, the USV is deployed in an natural lake environment. This setting exposes the system to real-world dynamic disturbances, including natural water ripples and unpredictable surface currents. The primary objective of this test is to measure the overall success rate of the active defense mechanism under actual operational stress. The collected data demonstrate the capability of the autopilot system to maintain navigational stability and successfully complete the RTL maneuver back to the designated secure zone despite external natural interferences.

E. Performance Metrics and Data Analysis

The collected quantitative data are analyzed using descriptive statistic to evaluate the system's performance against predefined baseline parameters. The analysis focuses on four main aspects:

1) Geofencing Positional Accuracy

The coordinates recorded by the NEO 3 GNSS module during the breach are compared against the predefined virtual boundaries [34]. To determine the system's spatial precision, the positional error margin is calculated in meters using the Haversine formula and the XTE formula, which accurately measures the great-circle distance between two points on the Earth's surface [35]. Furthermore, the distance calculated by the On-Board system is cross-validated using the Google Maps Distance Measurement Tool as a benchmark to ensure the reliability of the data [36].

2) Maneuver Success Rate

The success of the active defense mechanism is evaluated by calculating the percentage of successful RTL executions under real environmental disturbances compared to the total number of attempts. The system validation is treated as a deterministic state-transition problem.

$$\text{Success Rate (SR)} = (N_{Success}/N_{attempt}) \times 100\% \quad (3)$$

Where $N_{success}$ is the number of times the USV successfully detected a geofence breach and executing RTL, and N_{total} is the total number of valid planned test.

A test is validated 'Pass' if the system successfully executes a two-stage verification: (1) accurately detecting geofence breach without false positive, and (2) autonomously triggering and completing RTL command in under 2s. On the other hand, any pre-deployment errors, such as handshake anomalies and program bugs, are considered as developmental setup faults and excluded from the operational dataset [37].

3) Tilt Sensor Responsiveness

The sensitivity of the attitude sensing mechanism is assessed by evaluating the system's ability to differentiate between genuine tampering anomalies from environmental wave disruptions. A test is validated 'Pass' if the system successfully detecting tilt anomaly > ±10° and > 5s [31].

4) Response Time Analysis

The delay between the IMU detecting a > 5 seconds tilt anomaly and the trigger of the Web-GCS alarm is measured in milliseconds (ms) [10]. Similarly, the latency of the geofence breach notification is calculated to determine the system's real-time communication reliability. The system is validated by the following framework by Jiménez Larruy [38]. The system is considered 'Pass' if it could send alarm in < 2s (< 2000ms) to the Web-GCS.

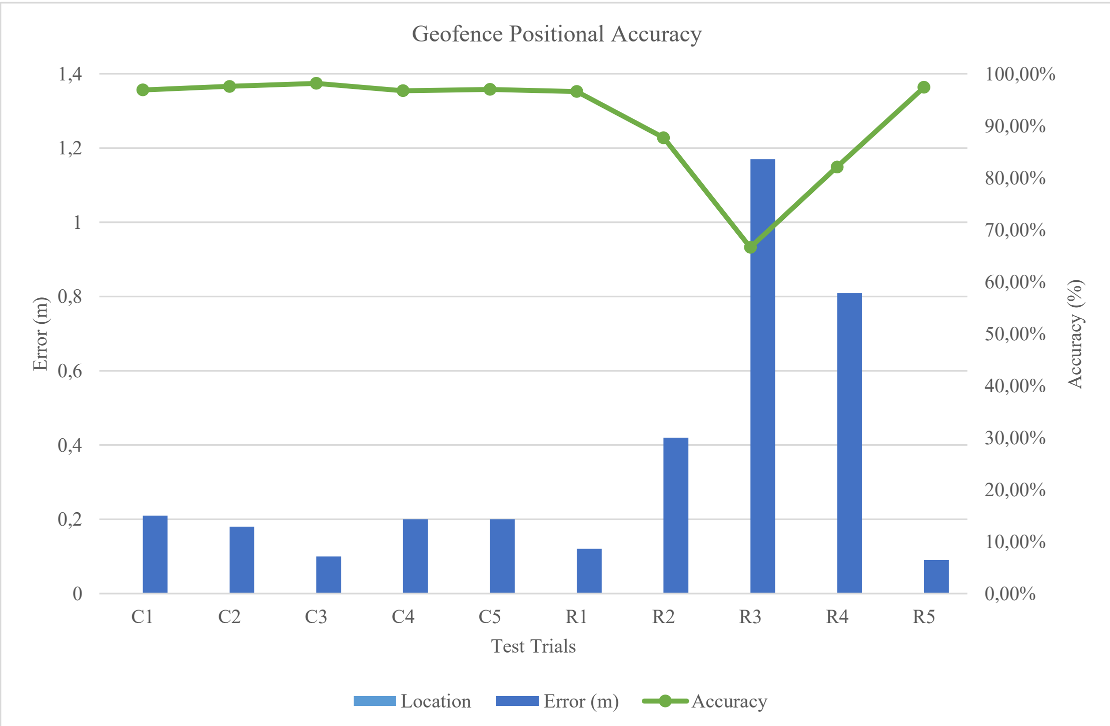
III. Results and Discussion

This section presents the performance evaluation of the integrated anti-theft system on the USV. Testing was conducted in two different phases: a controlled environment test to verify the GPS accuracy, attitude anomaly, and the system's response time, and a real environment test to measure the success rate of the anti-theft system under actual operational stress. The quantitative data gathered during both phases was analyzed using descriptive statistics to assess the system against predetermined threshold values. Following the methodology, the results and discussions are categorized into four primary areas of evaluation: geofence positional accuracy, maneuver success rate, tilt sensor responsiveness, and response time analysis.

A. *Geofence Positional Accuracy*

Table 1.
Comparison of geofence positional accuracy

Location	Geofence Boundary (m)	System's Logged Distance (m)	Benchmark Distance (m)	Error (m)	Accuracy
Controlled Environment	5	6.80	7.01	0.21	96.91%
		7.25	7.43	0.18	97.58%
		5.33	5.43	0.10	98.16%
		6.03	6.23	0.20	96.79%
		6.47	6.67	0.20	97.00%
Real Environment	3	3.94	3.82	0.12	96.90%
		3.42	3.00	0.42	87.70%
		3.50	2.33	1.17	66.60%
		3.71	4.52	0.81	82.08%
		3.45	3.36	0.09	97.40%



Graph 1 Comparison of Geofence Positional Accuracy

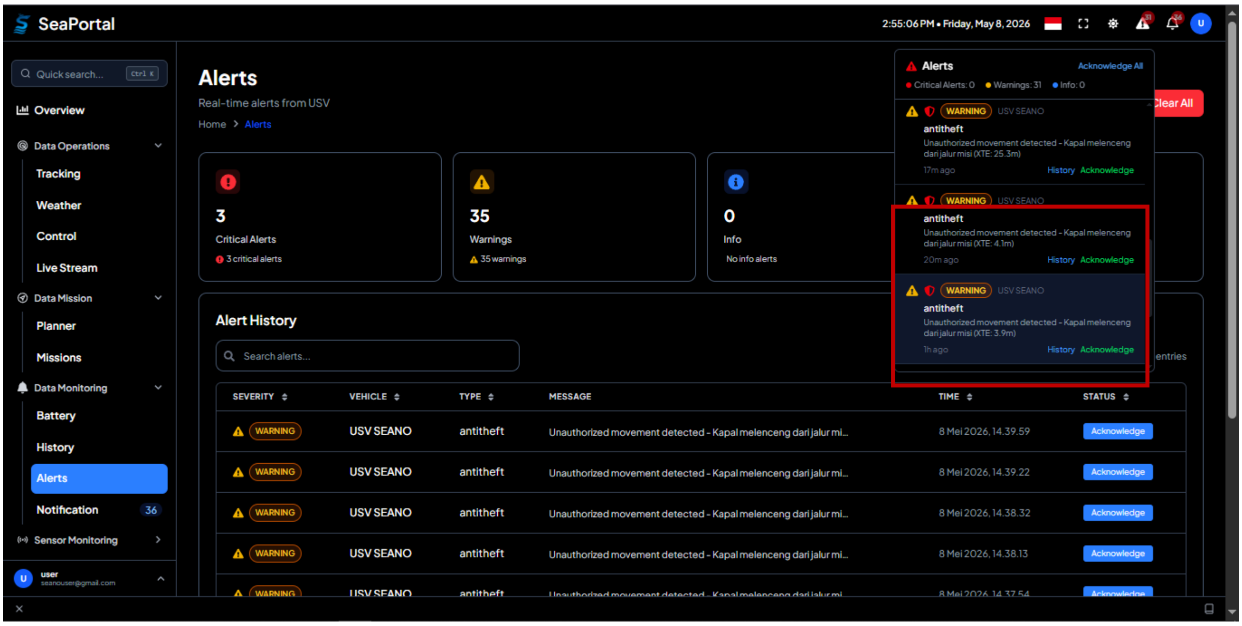


Figure 3 The Web-GCS alert for a geofence boundary breach

The data presented in Table 1 show the positional accuracy of the system's geofencing by comparing the system's logged distance against a benchmark distance. Testing was divided between controlled environment and real-world environment to isolate the impact of external disturbance on the GPS module's precision.

In the controlled environment, the system demonstrated highly consistent tracking, maintaining a positional accuracy between 96.79% and 98.16%. The maximum recorded error margin in this setting was minimal, peaking only at 0.21 meter. This value confirms that the baseline logic for distance calculation and the core hardware integration are functioning correctly under ideal conditions [32], [34].

Testing in the real environment exposed the USV to the unexpected environmental variables, resulting in greater fluctuations in accuracy. Most of the iterations maintained an accuracy above 82%, while one specific reading showed an error margin of 1.17 meters, dropping the accuracy to 66.6%. Unlike the controlled test, the USV is exposed GPS interference from nearby structures in the real test as opposed to the controlled test. This factor naturally cause the vessel to drift and slightly delay the GPS update rate. This finding is supported by the research conducted Fata [32].

B. *Maneuver Success Rate*

TABLE 2.
COMPARISON OF MANEUVER SUCCESS RATE

Location	Geofence Boundary (m)	Distance from Geofence (m)	Expected	System Result	Response Time (ms)	Status
		5.01	Execute RTL	Execute RTL	37	Pass
		3.14	No Action	No Action	-	Pass
		3.91	No Action	No Action	-	Pass
		5.64	Execute RTL	Execute RTL	49	Pass
Controlled Environment	5	5.33	Execute RTL	Execute RTL	132	Pass
		4.77	No Action	No Action	-	Pass
		5.11	Execute RTL	Execute RTL	54	Pass
		5.05	Execute RTL	Execute RTL	48	Pass
		4.92	No Action	No Action	-	Pass
		4.29	No Action	No Action	-	Pass
		3.42	Execute RTL	Execute RTL	154	Pass
		3.94	Execute RTL	Execute RTL	47	Pass
		1.59	No Action	No Action	-	Pass
		2.58	No Action	No Action	-	Pass
Real Environment	3	3.33	Execute RTL	Execute RTL	56	Pass
		11.39	Execute RTL	Execute RTL	69	Pass
		25.85	Execute RTL	Execute RTL	91	Pass
		25.35	Execute RTL	Execute RTL	56	Pass
		24.47	Execute RTL	Execute RTL	6	Pass

	22.36	Execute RTL	Execute RTL	58	Pass

Note: A hyphen (-) indicates that the vessel remained within the geofence boundary, resulting in no active defense state.

Figure 4 RTL maneuver field testing at the lake

Graph 2 Comparison of Maneuver Success Rate

Table 2 shows the dataset of Maneuver Success Rate (SR) in two different environments. The total number of experiments conducted was 10 iterations for each environment. Table 2 showcase all 20 datasets to highlight the system performance across distinct spatial intervals. Based on the observed test cases presented in Table 2, the system achieved successful responses in all evaluated cases (SR = 100%).

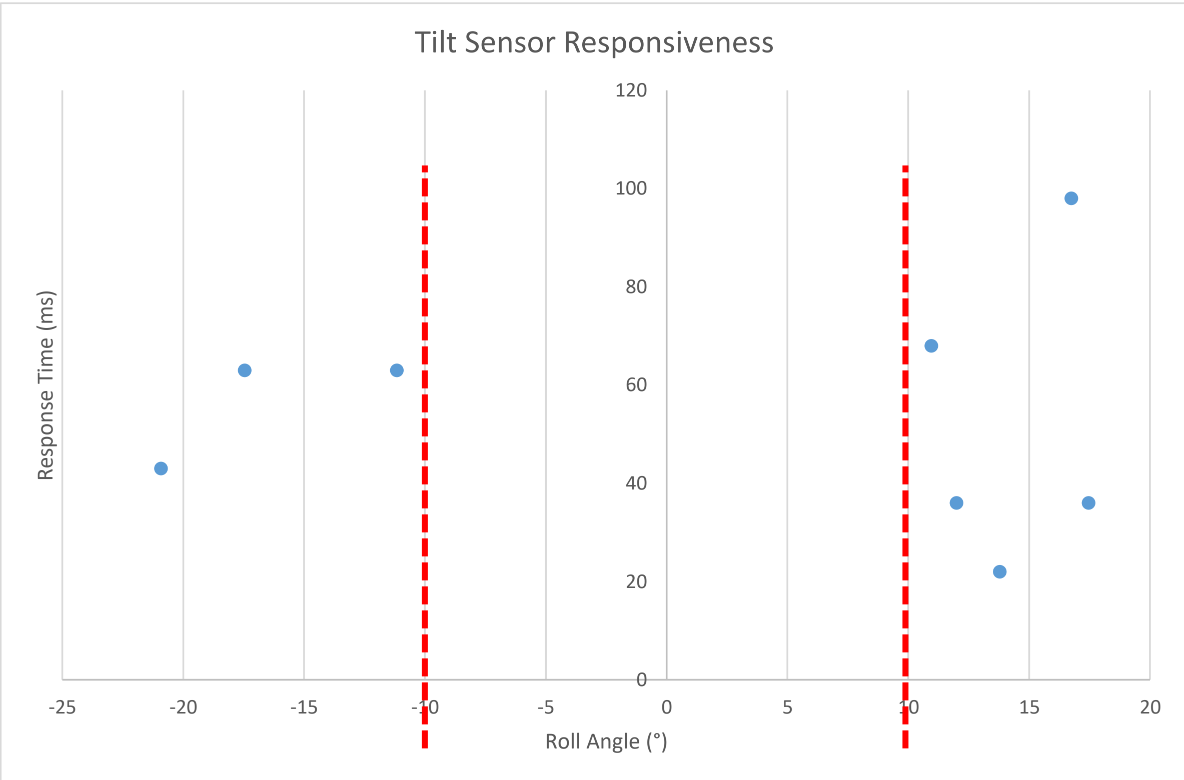
The 100% success rate is tied directly to the deterministic nature of the geofencing algorithm. Because the boundary checking logic relies on strict geospatial coordinate inequalities, the system executes predictably without logical degradation as long as telemetry remain intact. The dataset highlights exceptional boundary precision in both setups. In the controlled setup (5-meter boundary), the vehicle correctly maintained a ”No Action” status at distances close to the limit, such as 4.77 m and 4.92 m, but immediately executing RTL protocol the moment it crossed the thershold by a minor increment (e.g., 5.01 m and 5.05 m). This acute sensitivity prevents false negatives.

Furthermore, the real environment deployment successfully validated a tighter 3-meter boundary configuration, demonstrating zero false positive triggers within the safe zone (1.59 m and 2.58 m). Most notably, during extreme spatial overshoots, where distances surger up to 22.36 m and 25.85 m, the system consistently intercepted the true-positive breaches and reliably triggered the RTL command. This finding proves the algorithms’s robustness even under severe field stress.

C. *Tilt Sensor Responsiveness*

TABLE 3.
COMPARISON OF TILT SENSOR RESPONSIVENESS

Location	Delay Limit (s)	Tilt Limit (±°)	Roll (°)	Duration (s)	Expected	System Result	Response Time (ms)	Status
Controlled Environment	5	10	11.99	6	Alarm Triggered	Alarm Triggered	36	Pass
			13.78	7	Alarm Triggered	Alarm Triggered	22	Pass
			-20.92	6	Alarm Triggered	Alarm Triggered	43	Pass
			-17.46	6	Alarm Triggered	Alarm Triggered	36	Pass
			14.07	3	No Alarm	No Alarm	-	Pass
Real Environment	5	10	10.95	6	Alarm Triggered	Alarm Triggered	68	Pass
			-11.16	6	Alarm Triggered	Alarm Triggered	63	Pass
			-17.46	7	Alarm Triggered	Alarm Triggered	63	Pass
			-12.95	4	No Alarm	No Alarm	-	Pass
			16.75	6	Alarm Triggered	Alarm Triggered	98	Pass



Graph 3 Comparison of Tilt Sensor Responsiveness

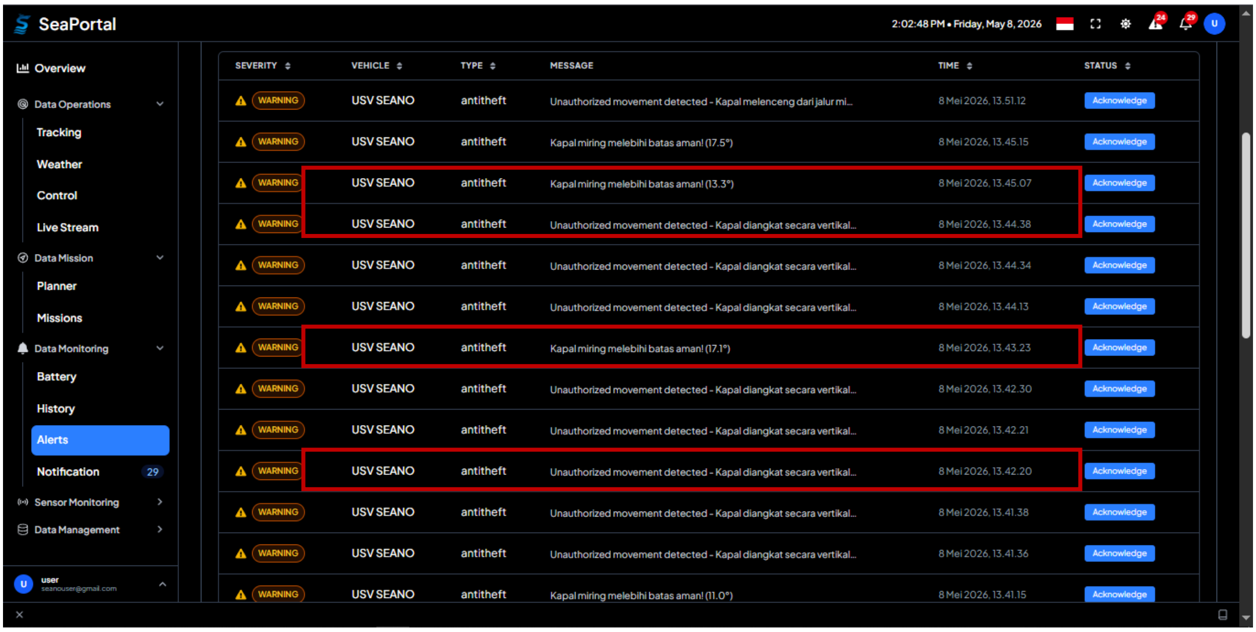


Figure 5 The Web-GCS alert logs for tilt anomalies

The tilt responsiveness test is to showcase the system's ability to detect a physical theft by lifting the USV, and to distinguish natural wave oscillation with an actual lifting attempt. Table 3 presents the dataset of Tilt Sensor Responsiveness in controlled and real environment. The total number of testing was 5 interations in each setup. The dataset shown above is a representative data to highlight the system's performance. With a high success rate of 100%, the system is able to differentiate if the USV is tilted by waves or a theft attempt.

In the controlled environment test, the highest positive number that the system detects was 14.07° at 3 seconds. Although the USV's tilt was above the tilt limit (±10°), it is considered safe because the duration of the tilt was within the safe boundary (< 5s). Similarly, the lowest positive number was 11.99 at 6 seconds. The system was able to categorized this test as a violation because it fulfilled both the criteria of a violation, which was tilted for >±10° and the duration is >5s. The system was able to send alarm to the Web-GCS, and considered as a 'Pass'.

The highest negative number that the system detects was -20.92 at 6 seconds. The system was able to detect this test as a tilt violation because the safe limit applies to positive and negative angular displacements. Furthermore, the tilted time was above the predetermined threshold (5s). By satisfying both criteria, the system successfully sent alarm to the Web-GCS, and is considered as a 'Pass'.

In the real environment test, the system detected 16.75° as the peak tilt in positive number for 6 seconds and -17.46° as the peak tilt in negative number for 7 seconds. Both test showed that the system was able to categorized them as a violation and send alarm to the Web-GCS because the criteria, tilt >±10° and duration >5s, was met. Furthermore, the system was able to detect -12.95 as a non-violation because one of the criteria of a violation was not met.

The test findings show that the system triggered an alarm when a violation occurred in both environments. Additionally, the system was able to distinguish an actual lifting attempt from natural wave oscillations, preventing false alarms from flooding the Web-GCS notifications.

D. *Response Time Analysis*

To evaluate the real-time notification and system responsiveness of the anti-theft system and the Web-GCS, network latency data was systematically captured during both geofence breaches and tilt anomalies. The validation of the test follows Jiménez Larruy [36] framework, which classifies a notification as real-time notification if the data were successfully sent in under 2s (2000ms). If the test fulfilled the condition, it can be considered as a 'Pass'.

1) Maneuver Success Rate

For the Maneuver Success Rate time response (see Table 2), the time was measured when the system detected USV's coordinates were out of the geofenced area. The time duration between the USV crossing the geofence perimeter and activating RTL protocol was instantaneous, with an average of 65.92 ms. While the USV remaining inside the boundaries (1.59 m, 3.14 m, and up to 4.92 m) correctly triggered "No Action", thus resulting in no response time.

The fastest breach response time recorded was 6 ms in the real environment test (24.47 m from geofence). The peak latency observed was 154 ms, which occurred during real environment test at a distance of 3.42 m from the geofence boundary.

Despite the real-world environmental problems causing minor latency increase compared to the controlled baseline, every single triggered response was below the critical 2 s limit with massive safety margin, therefore fulfilling the time reliability criteria of [36].

2) Tilt Sensor Responsiveness

Similarly, the tilt anomaly datasets (see Table 3) response time were measured from the moment the IMU detected an omnidirectional roll violation exceeding ±10° for a duration longer than the 5-second threshold. During the peak anomaly event (-20.92 at 6 seconds), the system successfully triggered the Web-GCS alarm in 43 ms. Overall performance of the tilt anomaly detection have the average response time of 53.63 ms.

Across all recorded tilt violations, the communication latency remained consistently low. In the controlled environment, response times ranged from a minimum baseline of 22 ms to a maximum of 43 ms. In the real environment, environmental conditions introduced slightly higher processing overhead, with the latencies ranging from 63 ms and 98 ms. Because all record intervals across both environments were well below 2000 ms threshold, the tilt alert system successfullyachieved a 'Pass' status under the validation framework [36].

IV. Conclusion

This study successfully implemented and evaluated an active, dual-layer anti-theft system for USVs. By integrating spatial geofencing with physical attitude anomaly detection, the system successfully transitioned passive tracking to an autonomous, closed-loop response to unauthorized movement.

Experimental testing verified that the system effectively triggers the vehicle's propulsion unit to execute an RTL maneuver upon a breach, preventing physical theft attempts. Additionally, the system appropriately detects a tilt violation and able to distinguish a physical theft attempt from natural waves. Simultaneously, the edge computing unit maintained reliable communication with the operator's Web-GCS, successfully delivering real-time notifications on the operator interface.

Adding autonomous physical evasion with immediate remote alerts offers a robust, layered security framework that addresses a key gap in the protection of USVs. The architecture shows high reliability in the test of controlled environment, but the environmental factor and the communication under different network conditions are the factors to be further optimized. Future work will focus on scaling the communication protocol for long-range deployment as well as enhancing the cybersecurity infrastructure of the system, focusing on securing the communication protocols against signal spoofing, data tampering, and unauthorized interception to ensure the integrity of both the geofence data and remote operator alerts.

Acknowledgements

The authors would like to express their sincere gratitude to the Ministry of Higher Education, Science, and Technology of the Republic of Indonesia (Kemdiktisaintek) for the financial support provided for this research. The authors also appreciate all parties who contributed to the completion of this study.

References

[1] H. Zheng and C. Liu, "An overview of Unmanned Surface Vehicles: Methods, practices, and applications," Control Eng. Pract., vol. 164, p. 106479, Nov. 2025, doi: 10.1016/j.conengprac.2025.106479.

[2] Y. Qiao, J. Yin, W. Wang, F. Duarte, J. Yang, and C. Ratti, "Survey of Deep Learning for Autonomous Surface Vehicles in Marine Environments," IEEE Transactions on Intelligent Transportation Systems, vol. 24, pp. 3678–3701, 2022, doi: 10.1109/tits.2023.3235911.

[3] X. Zhang, C. Wang, L. Jiang, L. An, and R. Yang, "Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state of the art survey," Ocean Engineering, vol. 235, p. 109380, 2021, doi: 10.1016/j.oceaneng.2021.109380.

[4] A. A. Priadi, T. Cahyadi, L. Barasa, S. A. Sukarno, N. Suranta, and M. Yando, "Development of IoT-Based Monitoring For Unmanned Surface Vessels (USV)," 2025.

[5] R. Kotian, P. Umesh, K. Gangadharan, and D. Shetty, "Development of Portable Ground Control Station for Real-Time Data Monitoring of an Unmanned Surface Vessel," Volume 6: Dynamics, Vibration, and Control, p., 2023, doi: 10.1115/imece2023-114071.

[6] C. Barrera, I. Padron, F. S. Luis, O. Llinas, and G. N. Marichal, "Trends and challenges in unmanned surface vehicles (Usv): From survey to shipping," TransNav, vol. 15, no. 1, pp. 135–142, 2021, doi: 10.12716/1001.15.01.13.

[7] S. Kale, "Developments in Unmanned Surface Vehicles (USVs): A Review," in International Conference on Applied Engineering and Natural Sciences, 2023, p. doi: 10.59287/icaens.1064.

[8] P. Solnør, Ø. Volden, K. Gryte, S. Petrovic, and T. Fossen, "Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field," J. Field Robot., vol. 39, pp. 631–649, 2022, doi: 10.1002/rob.22068.

[9] I. Durlik, T. Miller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzińska, "Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge?," Electronics (Basel)., p., 2024, doi: 10.3390/electronics13132654.

[10] A. Giannaros et al., "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions," J. Cybersecur. Priv., vol. 3, pp. 493–543, 2023, doi: 10.3390/jcp3030025.

[11] A.-V. Pălăcean, R. Tătăroiu, D.-C. Trancă, C. Contașel, and C. Duțescu, "IoT Enabled Optimized Architectures for GPS Anti-Theft Tracking Devices," 2021.

[12] K. Jha, "Vehicle Anti-Theft Tracking System Based on Internet of Thing(IoT)," Journal of University of Shanghai for Science and Technology, p., 2021, doi: 10.51201/jusst/21/05141.

[13] V. Vagal, K. Markantonakis, and C. Shepherd, "A New Approach to Complex Dynamic Geofencing for Unmanned Aerial Vehicles," Oct. 2021, [Online]. Available: http://arxiv.org/abs/2110.09453

[14] B. R. Page, J. DaRosa, and J. Lindler, "USV Fleet Planning Considering Logistical Constraints Using Genetic Algorithm," in OCEANS 2022, Hampton Roads, IEEE, Oct. 2022, pp. 1–7. doi: 10.1109/OCEANS47191.2022.9976967.

[15] Y. Qendah, D. Püllen, and S. Katzenbeisser, "Real-time Risk Assessment of Security Incidents for Autonomous Vehicles," in 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall), 2024, pp. 1–7. doi: 10.1109/vtc2024-fall63153.2024.10757969.

[16] H. Fadheli, S. K. A. Khalid, and L. M. Fadzil, "A Non-GPS Return to Home Algorithm for Drones using Convolutional Neural Network," Journal of Advanced Research in Applied Sciences and Engineering Technology, p., 2024, doi: 10.37934/araset.51.1.1527.

[17] F. Kilic, M. Hassan, and W. Hardt, "Prototype for Multi-UAV Monitoring–Control System Using WebRTC," Drones, p., 2024, doi: 10.3390/drones8100551.

[18] A. Poma, A. Caballero, I. Maza, and A. Ollero, "Open-Source Web-Based Ground Control Station for Long-Range Inspection with Multiple UAV s," in 2024 International Conference on Unmanned Aircraft Systems (ICUAS), 2024, pp. 1385–1392. doi: 10.1109/icuas60882.2024.10556987.

[19] F. Kilic, M. Hassan, and W. Hardt, "Prototype for Multi-UAV Monitoring–Control System Using WebRTC," Drones, vol. 8, no. 10, p. 551, Oct. 2024, doi: 10.3390/drones8100551.

[20] B. Shakya, O. El-Gayar, J. Kaabi, and K. Mamun Ahmed, "Small-Object Detection at the Edge: A Pareto-Efficient Benchmark of Lightweight YOLO Models on UAV and Overhead Datasets," IEEE Access, vol. 14, pp. 528–548, 2026, doi: 10.1109/ACCESS.2025.3648968.

[21] R. Moore, R. A. Rahimi, J. Robbins, and R. Stansbury, "A comparative study of redundant and non-redundant flight control system architectures for unmanned aircraft: key limitations and recommendations," International Journal of Vehicle Design, vol. 95, no. 1/2, pp. 75–99, 2024, doi: 10.1504/IJVD.2024.137837.

[22] G. Michieletto, F. Formaggio, A. Cenedese, and S. Tomasin, "Robust Localization for Secure Navigation of UAV Formations Under GNSS Spoofing Attack," IEEE Transactions on Automation Science and Engineering, vol. 20, no. 4, pp. 2383–2396, Oct. 2023, doi: 10.1109/TASE.2022.3208662.

[23] S. E. Tsai and C. H. Hsieh, "Glare-Aware Resi-YOLO: Tiny-Vessel Detection with Dual-Brain Edge Deployment for Maritime UAVs," Drones, vol. 10, no. 3, Mar. 2026, doi: 10.3390/drones10030226.

[24] Z. Liang et al., "DroneTest-Copilot: AGI-Powered Automated Detection and Repair of Flaws in Drone Autotest Suites," IEEE Trans. Netw. Sci. Eng., pp. 1–22, Jan. 2026, doi: 10.1109/tnse.2026.3653678.

[25] S. Gruener, H. Koziolek, and J. Ruckert, "Towards Resilient IoT Messaging: An Experience Report Analyzing MQTT Brokers," in 2021 IEEE 18th International Conference on Software Architecture (ICSA), IEEE, Mar. 2021, pp. 69–79. doi: 10.1109/ICSA51549.2021.00015.

[26] J. L. Silva Cotta, D. Agar, I. R. Bertaska, J. P. Inness, and H. Gutierrez, "Latency Reduction and Packet Synchronization in Low-Resource Devices Connected by DDS Networks in Autonomous UAVs," Sensors, vol. 23, no. 22, 2023, doi: 10.3390/s23229269.

[27] A. Toma, N. Cecchinato, G. Ferrin, I. Scagnetto, C. Drioli, and G. L. Foresti, "MAV-Link-Based Control and Coordination of a Multi-Drone Cluster for Intelligence, Surveillance and Reconnaissance Tasks," Unmanned Systems, vol. 13, no. 04, pp. 1027–1040, Aug. 2024, doi: 10.1142/S2301385025500633.

[28] A. Andreou, C. X. Mavromoustakis, J. M. Batalla, E. K. Markakis, G. Mastorakis, and S. Mumtaz, "UAV Trajectory Optimisation in Smart Cities Using Modified A * Algorithm Combined With Haversine and Vincenty Formulas," IEEE Trans. Veh. Technol., vol. 72, no. 8, pp. 9757–9769, Aug. 2023, doi: 10.1109/TVT.2023.3254604.

[29] G. Li, G. Li, X. Zhang, S. Wang, and Z. Xie, "Line-of-sight based great-circle route track-keeping control," Journal of Navigation, pp. 1–16, Apr. 2026, doi: 10.1017/S0373463326101532.

[30] N. I. M. Jalal, A. F. M. Ayob, S. Jamaludin, and N. A. Ali, "Evaluation of neuroevolutionary approach to navigate autonomous surface vehicles in restricted waters," Defence S&T Tech. Bull, vol. 16, no. 1, pp. 24–36, 2023.

[31] R. Fauzi, I. Jaya, and M. Iqbal, "Unmanned Surface Vehicle (USV) performance test in Bintan Island Waters," IOP Conf. Ser. Earth Environ. Sci., vol. 944, no. 1, p. 012013, Dec. 2021, doi: 10.1088/1755-1315/944/1/012013.

[32] T. G. Molnar, S. K. Kannan, J. Cunningham, K. Dunlap, K. L. Hobbs, and A. D. Ames, "Collision Avoidance and Geofencing for Fixed-Wing Aircraft With Control Barrier Functions," IEEE Transactions on Control Systems Technology, vol. 33, no. 5, pp. 1493–1508, Sep. 2025, doi: 10.1109/TCST.2025.3536215.

[33] A. Sathiyamurthy and S. G. S. Naidu, "Designing Edge Computing Solutions for Real-Time Vessel Tracking and Collision Avoidance," J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl., vol. 16, no. 2, pp. 863–874, Jun. 2025, doi: 10.58346/JOWUA.2025.I2.053.

[34] A. I. N. Fata, M. K. Al Ghozali, R. J. Dirgantara, A. Rusdinar, and F. Y. Suratman, "Navigation system for unmanned surface vehicle fish feeder with fuzzy logic controller," in AIP Conference Proceedings, 2024, p. 70005. doi: 10.1063/5.0207595

[35] M. M. Raikar, K. Angadi, S. Reddy, N. Naik, and A. Doddwada, "Fleet tracking and Geofencing using the Internet of Things (IoT)," in ICSCCC 2023 - 3rd International Conference on Secure Cyber Computing and Communications, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 463–468. doi: 10.1109/ICSCCC58608.2023.10176660.

[36] H. Langi, J. Pongoh, D. Sendow, Y. Lewan, and D. Kantohe, "Strengthening MSME Digital Transformation through Android-Based Geolocation Mapping: Implementation of Location-Based Services and the Haversine Formula," Journal La Multiapp, p., 2025, doi: 10.37899/journallamultiapp.v6i6.2504.

[37] P. Ramu et al., "Validity and Reliability of a Questionnaire on the Knowledge, Attitudes, Perceptions and Practices toward Food Poisoning among Malaysian Secondary School Students: A Pilot Study," Healthcare, vol. 11, no. 6, p. 853, Mar. 2023, doi: 10.3390/healthcare11060853.

[38] S. Jiménez Larruy, "Enhancing manufacturing performance through an Operator Notification app in an Industry 4.0 context," 2025.