Article

ARGUS: An Autonomous Robotic Guard System for Uncovering Security Threats in Cyber-Physical Environments

Edi Marian Timofte [*] , Mihai Dimian , Alin Dan Potorac , Doru Balan , Cătălin Stratu , Daniel-Florin Hrițcan , Marcel Pușcașu , Ovidiu Chiraș

Posted Date: 25 July 2025

doi: 10.20944/preprints202507.2138.v1

Keywords: autonomous security robot; cyber-physical systems; intrusion detection; computer vision; machine learning; real-time navigation; obstacle avoidance

Article

ARGUS: An Autonomous Robotic Guard System for Uncovering Security Threats in Cyber-Physical Environments

Edi Marian Timofte *, Mihai Dimian, Alin Dan Potorac, Doru Balan, Cătălin Stratu, Daniel-Florin Hrițcan, Marcel Pușcașu and Ovidiu Chiraș

Department of Computers, Automation and Electronics, University "Ștefan cel Mare", 720229 Suceava, Romania

* Correspondence: edi.timofte@usm.ro; Tel.: +40-748-171-798

Abstract

While traditional surveillance and security methods remain widely used, they struggle to keep up with emerging threats. These systems lack autonomy, cannot process multimodal data in real time and are largely dependent on human intervention. This highlights the clear need for integrated solutions that combine autonomous robotic mobility, intelligent perception, and real-time contextual awareness, enabling faster and more effective responses to evolving security challenges. This paper presents ARGUS (Autonomous Robotic Guard System) an autonomous robotic platform for patrolling, detection, and response within cyber-physical environments. Unlike traditional systems, ARGUS operates independently, navigating, analyzing, and intervening in dynamic and potentially hazardous scenarios. The platform integrates advanced computer vision modules (facial recognition, vehicle, and bladed weapon detection), artificial intelligence for abnormal behavior assessment and contextual acoustic analysis, alongside embedded cyber protection capabilities through native Intrusion Detection Systems – IDS (Snort, Suricata). Additionally, ARGUS incorporates adaptive planning and routing algorithms (A*, D* Lite), Simultaneous Localization and Mapping (SLAM), and robust control strategies (backstepping, sliding-mode), enabling effective operation even in unstable, crowded, or unstructured environments. Beyond its autonomous functionalities, ARGUS can seamlessly integrate into a multi-agent network, coordinating real-time security responses with other mobile units and human operators. This paper details the system architecture, software and hardware components, implementation methodology, and testing scenarios, highlighting the advantages of adopting integrated robotic approaches for modern security applications.

Keywords: autonomous security robot; cyber-physical systems; intrusion detection; computer vision; machine learning; real-time navigation; obstacle avoidance

1. Introduction

In an increasingly interconnected world, critical infrastructures and smart urban environments are subjected to hybrid threats, where physical and cyber-attacks converge to destabilize essential systems [1-2]. Traditional surveillance and protection systems, relying heavily on static architectures, fragmented data acquisition, and human intervention, are increasingly insufficient in responding to these dynamic and complex threats [3]. The evolution of threats calls for integrated cyber-physical solutions capable of autonomous operation, real-time anomaly detection, and adaptive response under diverse conditions [4].

Recent advancements in autonomous robotic platforms have shown significant potential to address these challenges by combining continuous mobility, context-aware analysis, and decision-making autonomy powered by artificial intelligence [5-6]. However, most current solutions still suffer from key limitations such as lack of real-time multi-modal data fusion, insufficient adaptive learning, and rigid navigation strategies [7].

To overcome these deficiencies, this work proposes ARGUS, an Autonomous Robotic Guard System designed for uncovering security threats in cyber-physical environments. ARGUS integrates multi-modal sensors (Light Detection and Ranging - LiDAR, Passive Infrared - PIR, ultrasonic, RGB and IR cameras), real-time processing units, and advanced cybersecurity modules to offer proactive protection capabilities both at the physical and digital layers [8].

Unlike conventional systems, ARGUS operates as a distributed security agent, embedding intrusion detection systems (Snort and Suricata) directly onboard to monitor and react to network-level anomalies such as port scans, unauthorized access attempts, and Denial-of-Service (DoS) attacks [9-10]. These cyber-detections are correlated in real-time with physical observations—such as human presence, vehicle detection, and suspicious objects—enabling the identification of complex hybrid threat scenarios. The image of the functional prototype is shown in Figure 1.

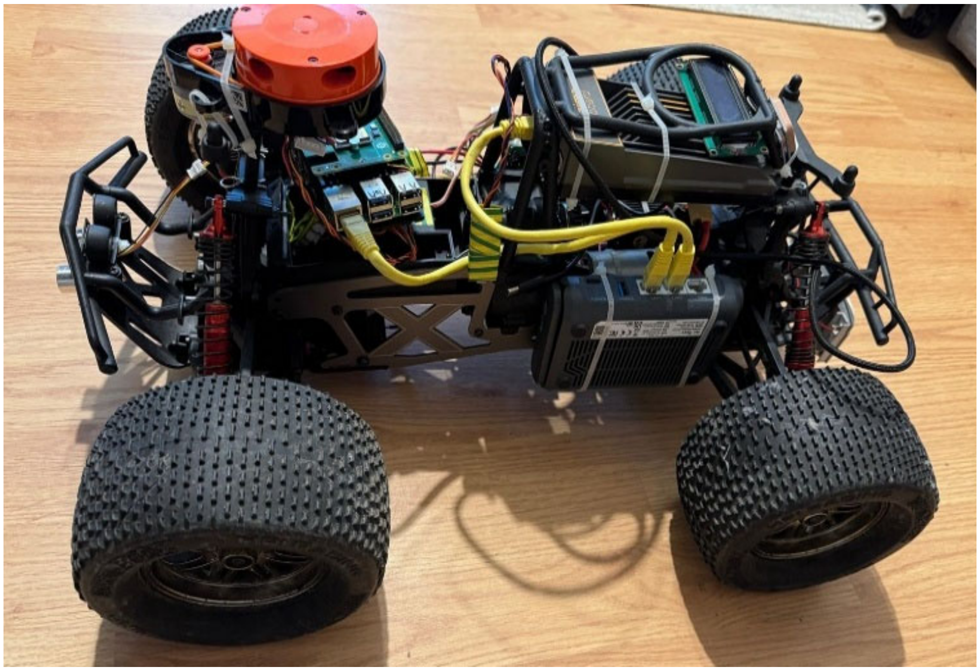


Figure 1. ARGUS image.

One of ARGUS's critical functionalities is the detection of stationary individuals in secure zones using 2D LiDAR technology [11]. By segmenting and classifying static point clouds, ARGUS can distinguish between passive objects and stationary humans potentially evading traditional surveillance. The integration of motion sensors and audio signal analysis further refines the system’s ability to reduce false positives, enhancing operational reliability in environments such as hospitals, universities, or administrative facilities [12].

To extend coverage and reduce vulnerability to predictable attack patterns, ARGUS employs advanced patrol planning mechanisms based on heatmap generation, historical incident records, and randomized routing strategies [13-14]. By prioritizing less-visited or high-risk zones dynamically, the platform minimizes patrol predictability while ensuring comprehensive surveillance. These capabilities are crucial in large, heterogeneous operational areas where static patrols are vulnerable to dynamic threat emergence [15].

The platform’s navigation autonomy is further reinforced by integrating multi-modal obstacle detection and avoidance systems, combining visual, ultrasonic, and inertial data through sensor fusion. Trajectory optimization algorithms based on probabilistic models such as A* and D* Lite allow ARGUS to anticipate and bypass potential obstructions while maintaining efficient energy consumption and minimizing mission time [16].

Combining key capabilities, ARGUS integrates voice control for hands-free command execution in enclosed environments, advanced autonomous surveillance for public and industrial spaces, and anomaly detection using machine learning (ML) models trained on specialized datasets such as University of Macau Anomaly Detection Benchmark Dataset (UMAD). Bringing together autonomous navigation, video analytics, collaborative control, and cyberattack detection, ARGUS establishes a resilient and intelligent platform that sets a new benchmark for autonomous patrol in complex cyber-physical environments [17-18].

2. ARGUS System Functionalities

Inspired by the mythological figure Argus Panoptes, a giant with a hundred eyes and constant vigilance, the ARGUS platform embodies the same core concepts of continuous monitoring, intelligent surveillance, and proactive threat detection.

In essence, this figurative concept has been turned into a fully autonomous robotic function that can analyze an environment in real-time, detect cyber intrusion, and respond to incidents that can arise [19]. ARGUS was designed to operate as a mobile patrol and reconnaissance unit designed to combine cyber-physical awareness with autonomous decision making.

To perform security operations, the platform combines numerous technologies, including artificial intelligence and computer vision for facial and object recognition, proximity and motion sensors for perimeter detection, embedded network monitoring for unauthorized scanning detection, GPS positional components to track intruders, and automatic alerts and real-time incident management.

ARGUS is more than a robot, it's a fully autonomous and integrated security solution designed to transform the approach to perimeter protection, and the protection of critical infrastructure. By virtue of conducting autonomous patrols, while providing intelligence for decision making in terms of threat assessment and cyber-physical anomaly detection, the platform is a truly future looking integrated security solution [20-22].

The following sections highlight the main operational capabilities of the ARGUS system, featuring real-world data flows and examples of the system interface [23-24].

2.1. Access Control and Monitoring

The first stage of access control involves registering individuals authorized to enter a building or secured perimeter. This process is fully automated and includes submitting personal data (such as name, photo, and role) via a web-based interface. The system extracts facial features using Google MediaPipe and stores them in a centralized database, as is shown in Figure 2.

doi:10.20944/preprints202507.2138.v1

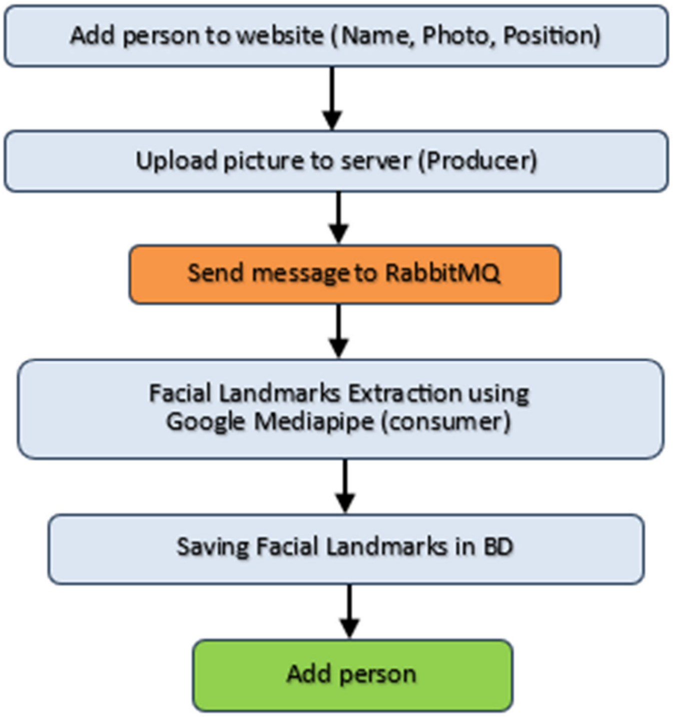

Add person to website (Name, Photo, Position)
Upload picture to server (Producer)
Send message to RabbitMQ
Facial Landmarks Extraction using Google Mediapipe (consumer)
Saving Facial Landmarks in BD
Add person

Figure 2. Access control – adding authorized individuals.

In the second stage, ARGUS continuously monitors entry points, detecting in real time any person attempting to access the secured zone. Video streams are transmitted via RabbitMQ to the processing module, where facial recognition algorithms analyze the captured images. Detected features are compared with those in the database to verify access rights.

If access is granted, the system permits entry. Otherwise, an alert is triggered, both through system logs and notifications sent to assigned security personnel. This ensures a rapid and automatic response to unauthorized access efforts.

By combining facial identification, real-time video processing, and automatic identity verification, ARGUS replaces traditional authentication methods with a self-interaction, reference-aware access control platform. Each effort is logged, and alerts are issued when intruder is detected.

Every individual who accesses the area is also recorded using a timestamp and an image, for traceability of both successful and unsuccessful access. Those records are then securely stored and can be viewed via the administrative interface, in the same way, you would review historical console logs. ARGUS also has rule-based access scheduling, such that, access permissions can be time-limited or context-specific based on prior security policy constructs.

Moreover, the platform offers enhanced reliability through two or more verification attempts in a narrow time window to mitigate false negatives resulting from temporary occlusion or low lighting. Upon detecting one or more failed attempts, ARGUS escalates by triggering an additional response layer, (e.g., an acoustic alert, or message broadcast to the nearby units). The full process is illustrated in Figure 3.

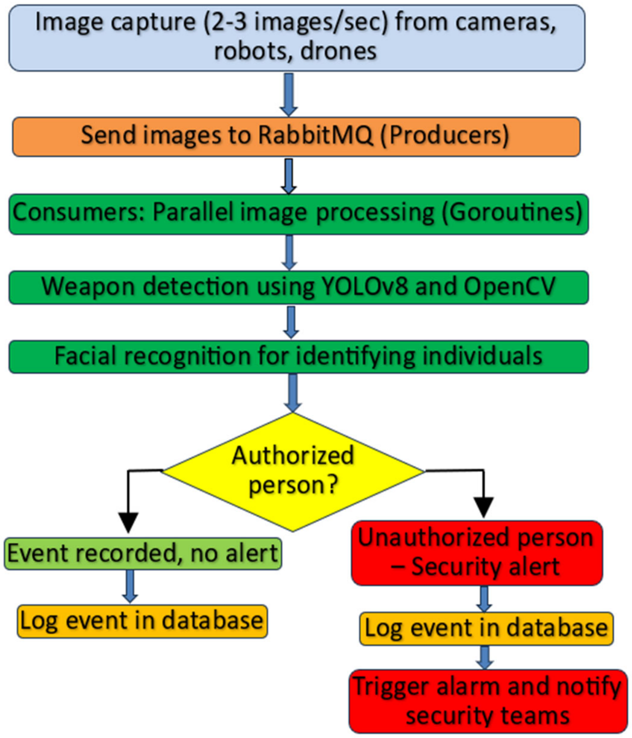


Image capture (2-3 images/sec) from cameras, robots, drones
Send images to RabbitMQ (Producers)
Consumers: Parallel image processing (Goroutines)
Weapon detection using YOLOv8 and OpenCV
Facial recognition for identifying individuals
Authorized person?
Event recorded, no alert
Log event in database
Unauthorized person – Security alert
Log event in database
Trigger alarm and notify security teams

Figure 3. Real-time access monitoring.

The system merges biometric identification with network-distributed decision logic, to provide an extensible, adaptive access control regime. This is seizing the opportunity inherent in environments where risk levels constantly change, and human oversight is limited.

2.2. Incident Management

ARGUS integrates advanced capabilities for managing vehicle access within secured perimeters, using real-time visual detection algorithms such as YOLO and SSD. Surveillance cameras capture video streams, which are transmitted asynchronously via RabbitMQ to processing modules. These modules detect vehicles and verify their authorization against a secure database. If validation is successful, access mechanisms (e.g., barrier gates) are activated automatically. Otherwise, alerts are triggered, events are logged, and optional notifications are sent to external systems such as parking management or incident reporting platforms.

In addition to vehicle control, the platform supports real-time detection of physical threats, including facial recognition and identification of bladed weapons. Video feeds from drones, fixed cameras, or mobile patrol robots are processed in parallel through a scalable architecture based on Goroutines. When a dangerous object is detected, ARGUS cross-checks the individual's identity against the authorized personnel database. Unauthorized or unknown individuals immediately trigger safety alerts and start escalation protocols.

For efficient events reaction, the system includes an analytics module that classifies events based on the source (robot or camera) and provides them with priority levels. Incidents of low-priority are stored for later review, while high-risk detections trigger alarm and collect security resources. In important circumstances, the system can react autonomously or coordinate to neutralize hazards with operators, ensuring a complete and reference-intensive safety response (see Figure 4).

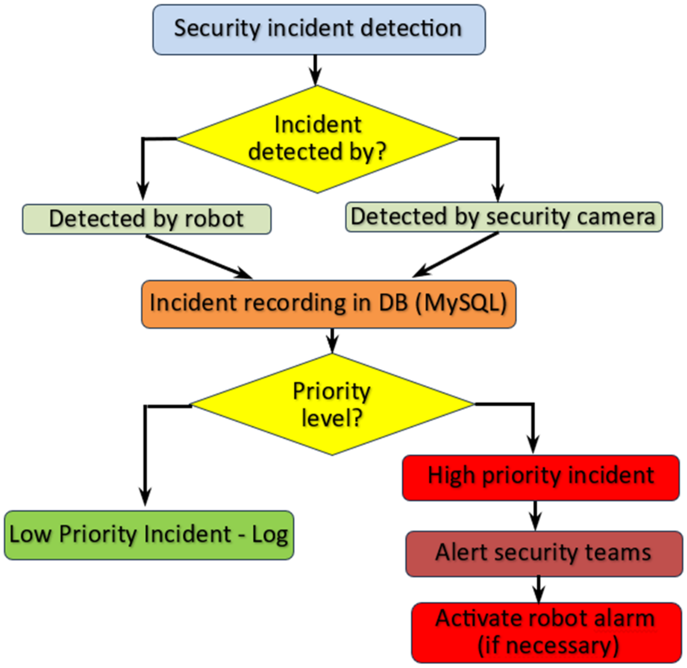

Security incident detection
Incident detected by?
Detected by robot
Detected by security camera
Incident recording in DB (MySQL)
Priority level?
High priority incident
Low Priority Incident - Log
Alert security teams
Activate robot alarm (if necessary)

Figure 4. Security incidents.

To optimize situational awareness, ARGUS preserves a real-time record of events, with contextual metadata that reflects the location, time of detection, kind of threat, and response status of a system. These records are displayed through the command interface, and the operator can filter, monitor, and interpret occurrences over time. When opportunities for pattern analysis of event histories arise, such as unauthorized vehicle access attempts occurring in the same area several times or the same object detected in the same location over months, the system will recommend altering patrol routes or increasing monitoring of that location.

Further, the platform supports multiple escalation layers: if a cyber alert along with a physical anomaly occurs within the same cadence, the ARGUS system can tie both alerts into the same collection of action responses. The linking of events and the ability for operators to analyze them across time and space allows constant situational intelligence when time matters. This intelligence provides ARGUS not only with the capability to respond to ongoing extraordinary threats, but also with the flexibility to learn and adapt to compound security challenges and multi-faceted incidents.

2.3. Perimeter Monitoring and Report Generation

ARGUS not only comes equipped with the physical and cyber surveillance capabilities previously described, but it also has an audio threat detection system. Through contextual sound detection, it features high risk sound detection capability (e.g., gunshots, human screams) and treats such sounds as incidents. When ARGUS detects a high risk sound, it will automatically invoke the alerting mechanism: begin capturing video and audio, emit a local alert tone, and if required will forward the event to some or all other units, using a distributed message broker. These agents consume events and execute appropriate responses, thereby establishing a cohesive multi-agent framework capable of rapid and coordinated action.

To facilitate operational traceability and continuous oversight, ARGUS enables automated reporting as illustrated in Figure 5.

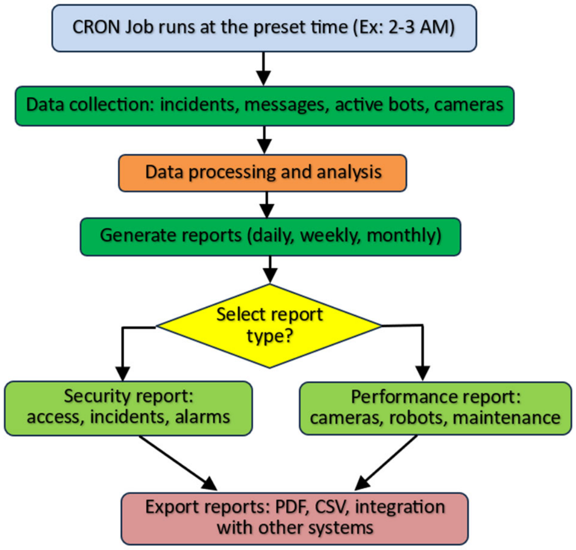

CRON Job runs at the preset time (Ex: 2-3 AM)
Data collection: incidents, messages, active bots, cameras
Data processing and analysis
Generate reports (daily, weekly, monthly)
Select report type?
Security report: access, incidents, alarms
Performance report: cameras, robots, maintenance
Export reports: PDF, CSV, integration with other systems

Figure 5. Automated report generator module.

This module runs CRON jobs at EDT intervals (for example, 2-3 AM), during which all or a selection of data will be obtained from system logs, detection events, status of the robots, and surveillance images. This information will be processed internally and subsequently produce regular daily, weekly, or monthly reports, with users electing the report, security (access, incidents, or alerts) or performance (system health, maintenance history, etc.). The reports can be exported in PDF or CSV format for aggregation with other systems, ensuring legislative efficiencies and interoperability.

In order to provide perceptibility in operations, every report contains logs with timestamps, system status snapshots, and summary statistics: the number of access attempts, alerts fired, anomalies detected, and uptime percentages. The reports are also tailored for the user role, e.g., a security manager gets a different report than an IT administrator or maintenance staff, so they only receive information pertinent to their role.

Additionally, ARGUS can automatically generate and distribute reports via email or secure file transfer at any defined point in time or time interval, so that less manual monitoring is necessary and, critical information is presented to designated parties in a timely manner. All reports are tampered evident, digitally signed and archived in a legally defensible manner, as well as for regulatory purposes.

In operations where there is mandatory compliance (i.e., critical infrastructure, public sector), there is a substantial administrative reduction using an automated report process and achieve a high degree of accountability and traceability. As reports accumulate over time, they generate a great many trend lines, which can also help inform strategic improvements on patrols, placement of sensors, or equipment maintenance intervals.

3. Methodology

The ARGUS system architecture was designed based on a customized, modular, and extensible robotic structure to accommodate a wide range of integrated functionalities, from physical detection of human presence and facial recognition to network monitoring and protection against cyber attacks in the real environment. Such designs allow for easy expansion of features and reconfiguration depending on the conditions of the operational environment. Regarding the hardware level, ARGUS combines the performance of specialized integrated platforms, such as Raspberry Pi, ZimaBoard and Arduino microcontrollers. Each of them performs a specific function in sensor processing, network interfacing or algorithm exclusivity. This layered approach significantly contributes to the robustness of the system and its resilience in critical security scenarios.

3.1. Integrated hardware and sensors

Towards hardware, the ARGUS robot is equipped with the following components:

- The Raspberry Pi board video interface management, facial identification, and responsible for local processing of real-time data currents;
- Dedicated to network traffic analysis and infiltration detection on a ZimaBoard, running Snort and Suricata in parallel;
- An Arduino microcontroller that is used to interface with temperature, acoustic and touch/speed sensors;
- A comprehensive sensor suit, which includes ultrasonic sensor, 2D lidar, PIR, a directional microphone and an infrared camera, which are all climbed on an autonomous mobile chassis.

This structure ensures logical separation of tasks and allows parallel processing, thus increasing the reliability of the system under real operational conditions.

3.2. Software Architecture and Technologies Used

The ARGUS software system has been developed in the Python and follows a hybrid distributed, event-powered architecture. It takes advantage of local microservice and asynchronous communication to ensure modularity and scalability. Each application runs in an isolated container and communicates through a lightweight REST API or via RabbitMQ using asynchronous message queues.

The system incorporates the following technologies:

- OpenCV and MediaPipe for real-time video stream processing and facial recognition tasks;
- YOLOv8, manually trained, for detecting bladed weapons, suspicious objects, and vehicles;
- Snort and Suricata, deployed on the ZimaBoard, for identifying unauthorized scans and malicious traffic;
- CRON jobs for scheduled and automated report generation;
- Flask to manage the local API interface and inter-module communication;
- RabbitMQ as the backbone for asynchronous messaging between system components.

3.3. Operational Flow and Data Management

All data collected by the system, including images, alerts, incident records, and robot statuses, is stored within a local private cloud, accessible via a secure web-based graphical interface. ARGUS follows an edge-first processing model, where data analysis is performed locally, at the edge of the network, to minimize latency and reduce exposure to external threats.

The system is trained to identify and classify:

- whether a person is authorized, using multi-angle facial recognition;
- whether the individual is carrying a bladed weapon, through object classification algorithms;
- whether suspicious network activity is occurring, such as scans or unauthorized access attempts.

Based on these detections, ARGUS can:

- automatically send real-time alerts via email and SMS to designated security personnel;
- log the events in the system and activate additional ARGUS units using distributed messaging protocols.

Below is a visual representation of the ARGUS architecture in Figure 6, depicting the inter-relationships of hardware modules, AI edge processing components, and the command-and-control server, throughout the system.

doi:10.20944/preprints202507.2138.v1

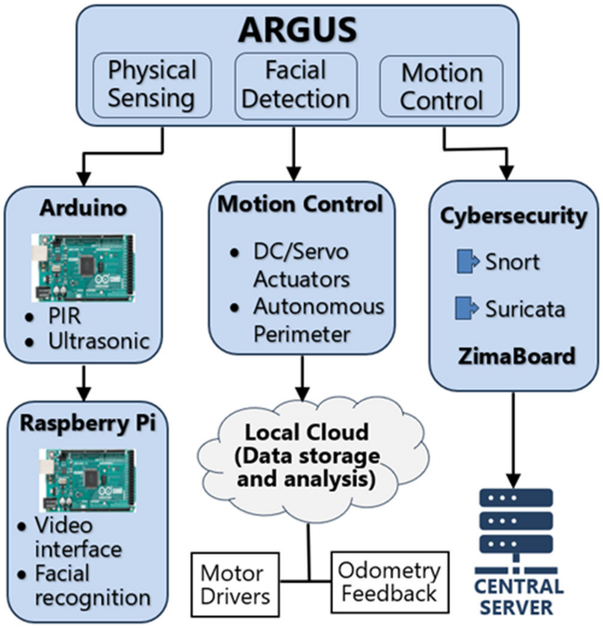


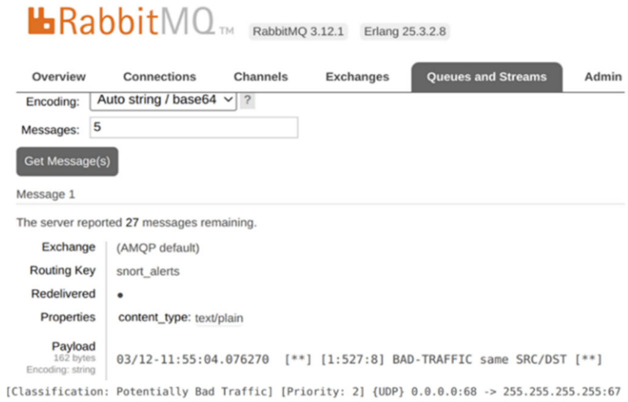
Figure 6. The functional architecture of the ARGUS system.

This diagram shows how the Raspberry Pi boards, ZimaBoard and Arduino microcontroller work in tandem to collect, analyze and transmit data. The diagram also seeks to denote the asynchronous communication flows that enable seamless operation of video analysis, AI detection, network monitoring, and alert systems as layered subsystems.

Due to the multi-layered architecture, the platform can operate independently in an isolated manner, while also synchronizing with a centralized infrastructure, allowing for incremental data aggregation and event correlation at the system-level.

4. Experimental Evolution and Results

Figure 7 depicts RabbitMQ's message monitoring console utilized by ARGUS when processing security alerts in real time, generated by the Snort intrusion detection engine. Alerts are sent along a dedicated channel using base64-encoded messages, making it an effective, reliable, quick communication channel between elements of the system.



Encoding: Auto string / base64

Messages: 5

Message 1

The server reported 27 messages remaining.

Exchange: (AMQP default)

Routing Key: snort_alerts

Redelivered: ●

Properties: content_type: text/plain

Payload
162 bytes
Encoding: string

```
03/12-11:55:04.076270  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
```

Figure 7. Snort alert stream transmitted via RabbitMQ.

The captured display shows log entries of network events classified under BAD-TRAFFIC same SRC/DST, with identical source and destination address. The phenomenon depicts UDP packets in

doi:10.20944/preprints202507.2138.v1

which both the source and destination are broadcast addresses (0.0.0.0:68 → 255.255.255.255.2555.67). Each alert may include useful metadata, such as timestamp, the protocol in use (IP/UDP), and the assigned priority level, all of which provide valuable context for assessing the nature of the threat.

Using these priority levels, ARGUS can make automatic decisions based upon low-severity and high-severity incidents. In addition to delivering immediate alerts to the operator, priority levels enable the system to dynamically learn and adjust rules as needed.

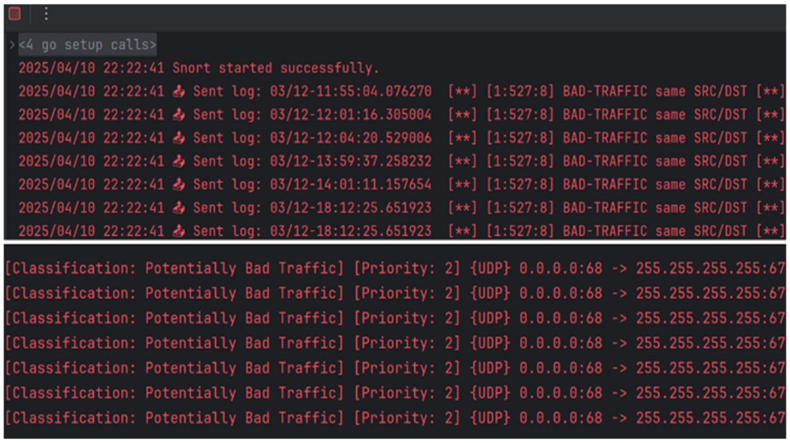
Using RabbitMQ, with the asynchronous nature of the messaging design, is beneficial to improving both the performance and scalability of this platform. Alerts are consistently processed through RabbitMQ regardless of high traffic volumes or network complexity. The critical factor is that RabbitMQ ensures no data loss or noticeable delay, maintaining continuous operational capability while working with alerts and events, even in extremely high-stress scenarios.

The results obtained in the network traffic monitoring tests confirm the efficiency of the integration of IDS modules within the ARGUS system. Abnormal traffic detections were retrieved, classified and distributed with response times below the critical threshold of 1 second, thus demonstrating the robot's ability to support active and adaptive cyber protection in real patrol scenarios.

In addition, the distributed architecture based on RabbitMQ ensures not only the resilience of the information flow in case of congestion, but also the possibility of scaling the system to cover wider perimeters or integrate multiple ARGUS entities in a collaborative network.

Next, the experimental evaluations focus on the validation of the physical and visual detection components, respectively on the ARGUS capabilities of facial recognition, edged weapons identification and classification of suspicious behaviors.

Figure 8 presents a sample log output from the ARGUS module responsible for integrating intrusion detection alerts into the real-time monitoring workflow. The fragment displays the successful initialization of the Snort engine and the live forwarding of alerts, specifically BAD-TRAFFIC same SRC/DST, to the system's processing and alerting layers.



```
<4 go setup calls>
2025/04/10 22:22:41 Snort started successfully.
2025/04/10 22:22:41 🐇 Sent log: 03/12-11:55:04.076270  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-12:01:16.305004  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-12:04:20.529006  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-13:59:37.258232  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-14:01:11.157654  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-18:12:25.651923  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
2025/04/10 22:22:41 🐇 Sent log: 03/12-18:12:25.651923  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
```

```
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
```

Figure 8. Logging output of detected IDS alerts within the ARGUS platform.

These messages are handled by a dedicated custom-built application (main.go) tailored to the modular structure of ARGUS. Unlike generic integration solutions, this lightweight module ensures minimal latency and provides direct control over:

- message formatting;
- event logging and storage;
- alert prioritization logic;
- future scalability requirements.

For every detected anomaly, a structured log entry is recorded, containing the timestamp, threat type, and assigned priority level (e.g., priority 2 in the shown case).

doi:10.20944/preprints202507.2138.v1

This custom logging approach reinforces ARGUS's ability to embed IDS modules natively and manage cyber alerts efficiently, contributing to enhanced resilience against evolving network threats in autonomous security deployments.

ARGUS merges these separate paradigms onto a single, mobile platform, integrating both physical threat detection and continuous cybersecurity anomaly assessment. Compared to robotic security systems examined in recent literature [1-2], [5], which primarily focus on patrol, visual recognition [2], autonomous navigation/SLAM, and path/pathway formations [3], the ARGUS system contains not only solutions to these previous issues but also integrates security intrusion detection modules (e.g., Snort + Suricata), enabling real-time correlations of abnormal visual presence with anomalous network activity.

Unlike some architectures that are dependent on cloud-based analytics or delayed decision loops, ARGUS primarily uses an edge-based distributed computing architecture allowing processed data located at the edge to be classified in real-time, which can trigger security response protocols at predetermined times. This independence, either through software or hardware reliance no matter the scenario, provides benefits in resilience, edge rendering without dependence, and also provides improved functionality in exigent circumstances or contexts where network connectivity is scarce.

When evaluating current literature on robotic security systems as described earlier in this report, it is revealed they rely heavily on monolithic software stacks with little or nothing described around the ability to change or adapt them once deployed. In contrast, the ARGUS system is based upon containerized microservices architecture, which supports limited and multiple updates, isolated module upgrades, and can perform parallel tasks. These features are some of the most significant for ensuring long-term maintainability and mission success.

Many existing systems rely upon disjointed information streams and multi-sensory inputs are commonly classified in silos or evaluated asynchronous without situation awareness. The ARGUS system has the ability to integrate multimodal data from visual, acoustic, thermal, and cyber environments to form a complete and current operational picture. Although there are no current examples of patrol robots aggregator multimodal information in the literature, the various sensorial data the crew operates with would classify them as multiplatform surveillance dedicated agents.

The combination of autonomous navigation, real-time AI inference, embedded cybersecurity, and distributed edge computing/microservices demonstrates ARGUS's flexibility in integrating each aspect of modern security threats. This complete and integrated responsive multi-sensor/multi-modal framework demonstrates the next generation of robotic surveillance platforms.

5. Evaluation of visual detection capabilities

Within the experiments to validate the visual capabilities of the ARGUS system, two main test directions were defined:

- Facial recognition of authorized/unauthorized persons;
- Detection of edged weapons (knives, batons, blunt objects) carried by suspicious persons.

The tests were conducted in a controlled environment, replicating an access point in a secured perimeter. The ARGUS platform used RGB and infrared cameras to capture images of moving or stationary individuals.

Image processing was performed as follows:

- Face detection using the MediaPipe Face Detection model;
- Person recognition by comparing facial landmarks with the registered set;
- Weapon detection using the YOLOv8 model trained on a custom set of images (with edged weapon labels).

Figure 9 presents the comparative performance of ARGUS's visual detection modules, focusing on face recognition and weapon detection. Face recognition achieved a faster processing time of ~180 ms, while weapon detection averaged 240 ms, due to the deeper feature extraction required by models like YOLOv8. Detection precision reached 92.7% for faces and 89.3% for weapons, confirming the robustness of ARGUS visual modules even under low-light or occluded conditions.

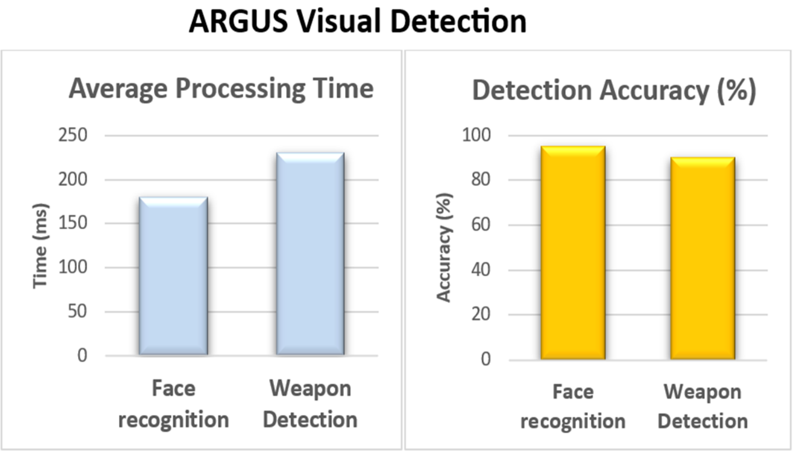


Figure 9. Performance metrics.

ARGUS effectively identified authorized individuals and triggered real-time alerts for unauthorized persons. For edged weapons, detection remained reliable in various lighting conditions, with minor degradation under low visibility. The system's rapid alerting mechanisms, including instant email and SMS notifications to the control centre, were validated successfully. Experimental analysis confirms ARGUS's high accuracy and low latency (<250 ms) across both detection tasks, supporting its readiness for autonomous security deployments, as is illustrated in Table 1.

Table 1. ARGUS Visual Performance Comparison Table.

Characteristic	Face Recognition	Weapon Detection
Average Processing Time (ms)	180	240
Detection Accuracy (%)	92.7	89.3
False Positive Rate (%)	3.2	4.1
False Negative Rate (%)	4.1	5.8
Testing Conditions	Natural and Artificial Light	Natural and Artificial Light

However, the tests highlighted certain limitations in low-light conditions or partial exposure of objects, where the recognition accuracy slightly decreases, indicating the need to implement additional mechanisms, such as:

- integration of additional IR cameras;
- improvement of the training dataset with low-light images;
- adaptation of AI models through fine-tuning techniques for various environmental conditions.

Overall, the results validate the viability of the ARGUS system in autonomous patrol scenarios, with clear optimization perspectives to expand the scope of applicability and operational robustness.

6. Conclusions and Future Work

This paper has detailed the conceptualization, design, development, and experimental validation of ARGUS, an advanced autonomous robotic platform tailored for proactive security patrolling in cyber-physical infrastructures.

By embedding multimodal sensing, real-time artificial intelligence analysis, distributed cyber threat monitoring, and autonomous decision-making mechanisms into a unified modular architecture, ARGUS demonstrates that a mobile robotic agent can effectively substitute and complement traditional static surveillance systems.

doi:10.20944/preprints202507.2138.v1

The experimental outcomes have validated the robustness and operational maturity of ARGUS in diverse threat scenarios, ranging from unauthorized network scanning to physical intrusion and weapon detection. The combination of real-time anomaly identification, autonomous patrol routing, distributed intelligence, and active response capabilities positions ARGUS as a pioneering solution ready to reshape the paradigm of intelligent security in sensitive environments.

The system's modularity and scalability further underline its potential adaptability across various operational theatres, from critical national infrastructure to smart urban spaces.

Although ARGUS has achieved a notable level of operational autonomy and threat detection proficiency, the dynamic evolution of security challenges necessitates continuous technological refinement. Future development efforts will target the enhancement of visual perception under extreme environmental conditions through the integration of thermal and hyperspectral imaging modalities.

Additionally, the extension of ARGUS into a fully collaborative multi-agent framework, leveraging decentralized consensus algorithms, will enable cooperative behaviour among multiple units, amplifying area coverage and resilience.

Edge AI optimization, via advanced model compression techniques, will further improve processing efficiency and energy sustainability, particularly for long-duration missions.

Security auditing will be fortified through the deployment of blockchain-based immutable event recording, ensuring verifiability and tamper-proof traceability of all critical incidents. Furthermore, adapting ARGUS to operate seamlessly over 5G low-latency networks will enhance remote operability and real-time cloud synchronization.

Finally, incorporating predictive behavioural analysis modules, capable of pre-emptively flagging suspicious activities, will transition ARGUS from a reactive security platform to a proactive threat anticipation system.

In summation, the ARGUS platform embodies a breakthrough in autonomous mobile security robotics, offering a resilient and intelligent response framework for the complex threats characterizing modern cyber-physical environments.

Through its seamless integration of AI-driven analytics, distributed cyber threat monitoring, and autonomous operational capabilities, ARGUS paves the way for the next generation of security infrastructure solutions.

Future expansions and real-world deployments will not only validate its technological superiority but will also set new standards for adaptability, resilience, and proactive threat management in critical sectors.

Author Contributions: Conceptualization, E.M.T. and M.D.; Methodology, E.M.T., A.D.P., D.B., C.S. and M.P.; Software, E.M.T., D.B., C.S, D.F.H, M.P. and OC..; Validation, E.M.T., A.D.P., C.S., and D.B.; Investigation, E.M.T., D.B., C.S, D.F.H, M.P. and OC.; Resources, E.M.T., C.S., O.C., and D.B.; Writing—original draft, E.M.T.; Visualization, E.M.T.; Supervision, M.D., A.D.P. and D.B.; Project administration, E.M.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

doi:10.20944/preprints202507.2138.v1

Abbreviations

The following abbreviations are used in this manuscript:

ARGUS	Autonomous Robotic Guard System
DoS	Denial-of-Service
IDS	Intrusion Detection Systems
LiDAR	Light Detection and Ranging
ML	Machine Learning
PIR	Passive Infrared
SLAM	Simultaneous Localization and Mapping
UMAD	University of Macau Anomaly Detection Benchmark Dataset

References

1. R. Soler, A. Moudni, G. Roskowski, X. Yu, M. Gormov and J. Saniie, "Autonomous Patrol and Threat Detection Through Integrated Mapping and Computer Vision," 2024 IEEE International Conference on Electro Information Technology (eIT), Eau Claire, WI, USA, 2024, pp. 398-403, doi: 10.1109/eIT60633.2024.10609884.
2. J. Zhou, X. Wang, M. Chang, K. Chen, H. Li and Z. Xu, "Design and Implementation of an Intelligent Security Patrol Robot with Nighttime Dynamic Object Detection Functionality," 2024 China Automation Congress (CAC), Qingdao, China, 2024, pp. 5409-5414, doi: 10.1109/CAC63892.2024.10865469.
3. Z. Zhang, P. Wang and K. Zhang, "Research on Path Planning Optimization for Patrol Robot based on Sparse Subspace Clustering Algorithm," 2024 International Conference on New Power System and Power Electronics (NPSPE), Dalian, China, 2024, pp. 154-159, doi: 10.1109/NPSPE62515.2024.00033.
4. C. Choe, S. Lee and N. Sung, "Scene Change Detection for Robotic Patrol System," 2024 Eighth IEEE International Conference on Robotic Computing (IRC), Tokyo, Japan, 2024, pp. 114-115, doi: 10.1109/IRC63610.2024.00029.
5. M. S. Sepeeh, S. A. -L. Nagarajan, M. E. O. Nguba, H. F. Jamahori, S. A. Zulkifli and R. Jackson, "Development of Autonomous Mobile Robot Based IoTs Integration for Surveillance Guard," 2024 IEEE 22nd Student Conference on Research and Development (SCOReD), Selangor, Malaysia, 2024, pp. 323-327, doi: 10.1109/SCOReD64708.2024.10872765.
6. V. V. Kumar, M. Shrimali, N. Shaik, R. K. N, N. Garg and R. Maranan, "Navigating the Dark: Advances in Robotic Night Patrol with D-Block Mask Electric EEL Dense Nested R-CNN for Enhanced Safety," 2024 4th International Conference on Sustainable Expert Systems (ICSES), Kaski, Nepal, 2024, pp. 1034-1041, doi: 10.1109/ICSES63445.2024.10763086.
7. B. Yaragani, S. S. Raju, S. R. Ragi, S. V. Cheemala and A. Lohith, "Women Safety Night Patrolling Robot Using Raspberry Pi 3," 2024 International Conference on Computing and Intelligent Reality Technologies (ICCIRT), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICCIRT59484.2024.10921944.
8. S. -H. Lee, Y. Jung and S. -W. Seo, "Imagination-Augmented Hierarchical Reinforcement Learning for Safe and Interactive Autonomous Driving in Urban Environments," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 12, pp. 19522-19535, Dec. 2024, doi: 10.1109/TITS.2024.3457776.
9. H. Mochizuki and R. Kiyohara, "Stationary Human Detection Method Using 2D LiDAR," 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC), Osaka, Japan, 2024, pp. 1699-1704, doi: 10.1109/COMPSAC61105.2024.00268.
10. C. -W. Chen, G. -Y. Lee and J. -S. Liu, "Human-Robot Collaboration in Unmanned Aerial Vehicle River Patrol Application," 2024 International Conference on Advanced Robotics and Intelligent Systems (ARIS), Taipei, Taiwan, 2024, pp. 1-6, doi: 10.1109/ARIS62416.2024.10679963.
11. W. Zezhao, C. Haitao, H. Zhenkun, K. Lingyu and W. Luyao, "Application of UAV Autonomous Flight Path Planning Technology in Power Inspection System," 2024 IEEE 4th International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 2024, pp. 1208-1212, doi: 10.1109/ICETCI61221.2024.10594591.

12. D. Zhang, Z. Liu, X. Wang, J. Qi, Y. Zhou and Q. Zhou, "Research on Aircraft Patrol Inspection Method Using UAV Based on YOLO Algorithm," 2024 4th International Conference on Electronic Information Engineering and Computer (EIECT), Shenzhen, China, 2024, pp. 412-415, doi: 10.1109/EIECT64462.2024.10866925.
13. L. Echefu, T. Alam and A. A. R. Newaz, "Randomized Multi-Robot Patrolling with Unidirectional Visibility," 2024 21st International Conference on Ubiquitous Robots (UR), New York, NY, USA, 2024, pp. 324-329, doi: 10.1109/UR61395.2024.10597540.
14. M. Xu, C. Li, C. Liu, S. Wang and Y. Tian, "Autonomous Location and Obstacle Avoidance of Inspection Robots Based on Multi-modal Information," 2024 3rd International Conference on Energy, Power and Electrical Technology (ICEPET), Chengdu, China, 2024, pp. 1948-1954, doi: 10.1109/ICEPET61938.2024.10626217.
15. M. S. Azim Mohd Saufi, W. Nurshazwani Wan Zakaria and R. Tomari, "Security Patrolling System for Autonomous Navigation of Service Mobile Robot," 2024 IEEE 2nd International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT), Jember, Indonesia, 2024, pp. 308-313, doi: 10.1109/ICEECIT63698.2024.10859336.
16. C. Li and S. Guo, "Study on the Backstepping Sliding Mode-Based Tracking Control Method for the SUR," 2024 IEEE International Conference on Mechatronics and Automation (ICMA), Tianjin, China, 2024, pp. 1759-1764, doi: 10.1109/ICMA61710.2024.10632882
17. N. R, P. U. S, M. Mohan, N. S, A. Mohan and J. Samuel, "Voice Controlled Moving Robot for Smart Surveillance," 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, 2024, pp. 354-359, doi: 10.1109/I4C62240.2024.10748473.
18. D. Li, L. Chen, C. -Z. Xu and H. Kong, "UMAD: University of Macau Anomaly Detection Benchmark Dataset," 2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Abu Dhabi, United Arab Emirates, 2024, pp. 5836-5843, doi: 10.1109/IROS58592.2024.10802194.
19. Q. Zhang et al., "E-Argus: Drones Detection by Side-Channel Signatures via Electromagnetic Radiation," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 11, pp. 18978-18991, Nov. 2024, doi: 10.1109/TITS.2024.3432977.
20. Fen Xu, ZhengXi Li and Kui Yuan, "The design and implementation of an autonomous campus patrol robot," 2007 IEEE International Conference on Robotics and Biomimetics (ROBIO), Sanya, 2007, pp. 250-255, doi: 10.1109/ROBIO.2007.4522169.
21. S. -W. Hsiao and C. -N. Wu, "A KE, DSM and ISM Based Approach for Patrol Robot Development," 2018 International Conference on Control and Robots (ICCR), Hong Kong, China, 2018, pp. 30-34, doi: 10.1109/ICCR.2018.8534486.
22. Jihong Lee et al., "Operating a six-legged outdoor patrol robot," 2007 International Conference on Control, Automation and Systems, Seoul, Korea (South), 2007, pp. 1034-1039, doi: 10.1109/ICCAS.2007.4407050.
23. Q. Yang, F. Xu, D. Qu, Y. Hong and Y. Zhuang, "Ground Moving Target Tracking for a Patrol Robot Based on Monocular Vision," 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Honolulu, HI, USA, 2017, pp. 159-163, doi: 10.1109/CYBER.2017.8446095.
24. F. Lastname, "Design and Implementation of Intelligent Patrol Robot for Secondary Equipment Based on Lidar Technology," 2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, China, 2019, pp. 1-4, doi: 10.1109/APPEEC45492.2019.8994663.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.