*Rev. Roum. Sci. Techn.– Électrotechn. et Énerg.*
Vol. **71**, *1*, pp. 555–560, Bucarest, 2026



# DESIGN AND IMPLEMENTATION OF AN INTEGRATED SURVEILLANCE SYSTEM FOR MARITIME ANTI-PIRACY

SERGIU LUPU[1], OVIDIU CRISTEA*[1], CLARA-GEORGETA LIȚU[1], ANDREI POCORA[1], NICOLAE-SILVIU POPA[1], CLAUDIA LAURENȚA POPESCU[2]

**Keywords: Maritime security; Anti-piracy; Integrated surveillance; Object detection; Autonomous tracking; Raspberry Pi.**

**The phenomenon of piracy remains a critical priority for global maritime security. This article introduces an innovative concept for anti-piracy countermeasures, inspired by conventional methods but automated through an integrated surveillance system. The solution correlates and processes data from navigation devices and multiple sensors, eliminating the need for armed Vessel Protection Detachments or private security guards. The system used to simulate efficiency includes a Raspberry Pi 4 Model B, two cameras, proximity sensors, power actuators, and a laser for deterrence. On a real-life scale, the architecture is adaptable to each vessel, optimizing existing on-board hardware resources for autonomous and efficient protection.**

## 1. INTRODUCTION

A video surveillance system represents the main instrument used for ensuring security, monitoring, and control within public and private spaces. It represents an assembly of hardware and software components with the main purpose of supervising certain areas.

An integrated surveillance system is based on interconnecting more devices, which results in expanding its field of applications and capabilities. For example, a simple system of this type can record images in real time, automatically detect if something looks suspicious, and save and store images for a predetermined period. Also, the images can be transmitted not only locally (wired display, through wi-fi connection, etc.), but also over long distances (via applications or specific programs).

Modern monitoring equipment is engineered to function reliably across diverse environmental settings. This inherent versatility allows these systems to be deployed both indoors and outdoors, withstanding direct exposure to harsh meteorological elements-such as heavy precipitation, snow, or intense solar radiation-in urban landscapes as well as in demanding maritime environments aboard ships. Regarding global shipping safety, the demand for visual monitoring solutions has surged in recent years. This trend is primarily driven by a growing frequency of both executed and thwarted piracy threats against commercial vessels navigating high-risk zones, particularly around the African continent, South America, and Southeast Asian routes like the Singapore Strait. Data provided by the International Chamber of Commerce (ICC) through its International Maritime Bureau highlights a significant escalation in these maritime crimes.

Recent annual statistics indicate a peak of 137 combined successful and attempted incidents, representing a notable rise compared to the preceding three-year period-specifically, reflecting an increase of 22 cases relative to 2022, 17 more than in 2023, and surpassing the 2024 figures by 21 events [1]. According to the same organization, on 15th and 16th of January 2026, two more incidents were reported, the first in the Philippines and the second in the Singapore Strait [2]. Even though these attacks have evolved and are now more concentrated on theft rather than harming the crew, there are still incidents that involve armed forces, harming the crew, and even kidnapping [3,4].

Approximately 90% of global trade is carried by sea. Piracy is one of the most well-known threats while navigating through straits or narrow waterways, especially the Malacca or Singapore Straits, Suez or Panama Canal, and the Strait of Bab el-Mandeb[5]. Incidents of piracy directed at commercial shipping do more than just disrupt global supply chains and inflict severe financial damages on international commerce; they also constitute a profound danger to the overall security of maritime navigation[6,7].

While transiting these dangerous areas, the ship's crew must adopt some basic safety measures. These include increasing the ship's speed to at least 18 knots to improve lookout effectiveness and better observe any approaching suspect vessel. Also, the water cannons must be prepared to be started, an action that is generally taken to slow down the attacks.

Regarding the safety of the ship's crew in the circumstances mentioned above, a CCTV (Closed Circuit Television) system became a necessity on board, not only to improve the threat detection capabilities, but also to review and analyze the events that are happening during such an incident.

This article proposes a study on an integrated surveillance system installed on board. It combines the cameras, the radars, the AIS (Automatic Identification System), and the water cannons into a larger system to prevent and protect the vessel from piracy incidents. The primary objective of this architecture is to synchronize the visual feeds from exterior cameras with the navigational data already available on the ship's bridge. In the event of a recognized threat, the system is programmed to automatically trigger the water cannons, establishing a defensive barrier to protect the vessel and its personnel against potential hostiles, functioning effectively both underway and at anchor.

Furthermore, the long-term reliability and efficiency of such maritime surveillance systems heavily depend on the underlying electronic and sensor technologies. Recent advancements in semiconductor materials indicate that tuned doping in SiC nanostructures can achieve robust electronic and magnetic behavior, making materials like Al- and Ga-doped SiC nanotubes strong candidates for developing highly durable, next-generation spintronic sensors and electronic devices.[8]

[1] Romanian Naval Academy "Mircea cel Bătrân", Constanța, Romania.
[2] National University of Science and Technology Politehnica Bucharest, Romania.
E-mails: sergiu.lupu@anmb.ro; ovidiu.cristea@anmb.ro (corresponding author); lituclara24@gmail.com; andrei.pocora@anmb.ro; silviu.popa@anmb.ro; claudia.popescu@upb.ro

DOI: 10.59277/RRST-EE.2026.4.1

## 2. GENERAL INFORMATION

The first part of the procedure contains the detection and identification of squatters as they approach the vessel [9,10]. The second part involves automatically tracking and identifying the vessel approaching (to avoid unnecessary alerts), as well as constantly measuring the distance to it and taking actions only with human approval.

In case an unknown vessel is approaching, at a distance that is pre-established considering the type of vessel, the identification process is started. Once the appurtenance is established, the Officer of the Watch is going to be alerted. He can also determine, by observation, whether the alarm is accurate.

The subsequent phase of the protocol is initiated once a target, definitively classified as hostile, breaches the predefined security perimeter of the defending vessel. Upon receiving manual authorization from the ship's master, the system deploys the water cannons, automatically directing them toward the exact bearing of the incoming threat.

Considering that realizing a simulation of this system on board a ship was not possible, the project was adapted and mounted on a couple of buildings printed with a 3D printer. To demonstrate the efficiency of this study, the hardware components of this system were placed strategically to ensure that, during the simulation, the intruder is successfully detected, tracked, and stopped from its intended action. For this to be possible, the first proximity sensor is placed at the furthest point to detect the approaching item in time.

Positioned adjacent to the initial sensor on the first structure, the primary camera handles the automated identification process by cross-referencing visual data with a predefined database. Meanwhile, the secondary sensor is situated at the base of the second building, functioning specifically to calculate the exact range and approach distance of the target.

Lastly, the electromechanical assembly is placed on the top of the second building. Its principal roles are to detect and classify the intruder and to automatically track it [11]. Also, after a manual command, it should activate the whole system to turn on the countermeasures.

## 3. TECHNICAL STRUCTURE

For the simulation, many hardware components were used, as follows: a Raspberry Pi 4 Model B [12–14], two proximity sensors (US-020), a Raspberry Pi Camera Module 3 NoIR, a CMOS (Complementary Metal Oxide Semiconductor) Camera Module, and an electromechanical assembly formed with two power actuators (SG90 for pan and tilt movement) and a laser. At a larger scale, the proximity sensors used for this simulation are represented by the radar and the AIS, devices mostly used for safe navigation. The two cameras are a CCTV system, and the assembly represents the water cannons.

When transposed to the scale of an actual vessel, each component of the simulated architecture corresponds to hardware already present, or readily deployable, on-board commercial ships, allowing the system to be implemented without introducing entirely new categories of equipment. The two proximity sensors used in the demonstrator are functionally replaced by the ship's radar and AIS, both of which already provide continuous range and bearing data on approaching vessels. The identification camera, tasked in the small-scale model with cross-referencing visual data against a known database, corresponds to the ship's existing CCTV system, whose feeds would instead be processed through the same object-detection pipeline described in this study. Finally, the electromechanical assembly is replaced at full scale by the vessel's water cannon system, which is likewise repositioned and activated only after manual authorization from the Officer of the Watch or the ship's master, preserving the human-in-the-loop principle validated in the demonstrator.

This correspondence indicates that the proposed architecture is not simulation-specific: the logic of detection, classification, distance-based escalation, and countermeasure activation is transferable to the ship's bridge systems with a change of sensor and actuator interfaces rather than a redesign of the underlying software. Implementing the system at full scale would primarily require integrating the Raspberry Pi, or an equivalent industrial controller, with the ship's existing NMEA 0183/2000 data bus to receive radar and AIS output, and with the water cannon's control interface to issue activation commands — both of which are standard integration points on modern commercial vessels.

### 3.1. HARDWARE COMPONENTS INTEGRATION

To maximize operational efficiency, the hardware components were segregated into two primary subsystems, drawing electrical power directly from the Raspberry Pi board alongside two independent external power supplies.

The first part is represented by the suspect approach of the vessel. For the first process to be successful, the Raspberry Pi Camera Module 3 [15] NoIR and the two proximity sensors were connected directly to the Raspberry Pi (for information and power). To automatically identify whether the vessel is a squatter or not, a database including basic information, pictures, and a short history, created from official sources, will be used.

The second scenario represents the automatic tracking and identification of the vessel within the pre-established safety area, as well as starting the defense system (the water cannon). To achieve this, the CMOS Camera Module and the assembly are connected to a Raspberry Pi for data and to two external power sources. All the connections are made through a breadboard.

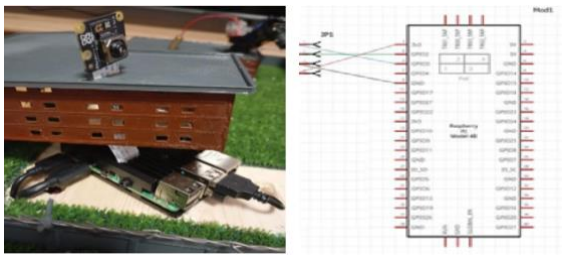


Fig. 1 – Physical and electrical connection

## 4. PHYSICAL AND ELECTRICAL CONNECTIONS

To validate the proposed concept, the physical mockup was designed to secure two scaled-down buildings, whereas the electronic schematic was modeled entirely within the Fritzing software environment. The initial hardware integration involved attaching the camera module directly to the Raspberry Pi 4 board via a dedicated ribbon cable, Fig. 1 [16]. Due to the absence of a dedicated Camera Serial Interface (CSI) module within the Fritzing environment, a

standard 4-pin header was adopted as a graphical proxy to represent the physical connections.

Additionally, a breadboard served as the intermediary platform for mounting the first proximity sensor, referred to hereafter as the primary sensor, corresponding to the unit positioned at the furthest detection point described in Section 2, and for linking it to the Raspberry Pi. The breadboard's power rails distributed the 5V supply (VCC) and the common ground (GND) to the sensor, while the TRIG and ECHO logic-signal pins were wired directly, through individual jumper connections on the same board, to dedicated GPIO pins. In this configuration, the breadboard performs no signal processing; it functions solely as a shared physical interconnection point that keeps the power distribution and the logic signaling electrically separate while using a single mounting platform. The secondary proximity sensor was connected through the same breadboard using an identical wiring logic.

While the actual physical circuit required three resistors to operate correctly, the corresponding schematic in Fritzing was designed using a pair of 1 kΩ resistors [17,18]. Also, the pins were connected through wires to the GPIO (General Purpose Input/Output) as follows: VCC to pin 2, for 5V voltage; TRIG to GPIO 23; ECHO to GPIO 24; GND to pin 6, for ground (Fig. 2).

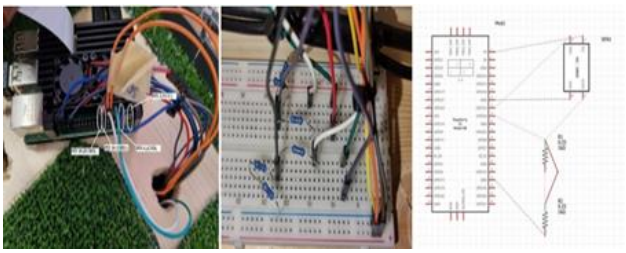


Fig. 2 – The physical and electrical connection of the first proximity sensor.

The second sensor is connected to the Raspberry Pi the same way as the first one, but the pins are linked as follows: VCC to pin 4, for 5V voltage; TRIG to GPIO 20; ECHO to GPIO 21; GND to pin 40, for ground (Fig. 3).

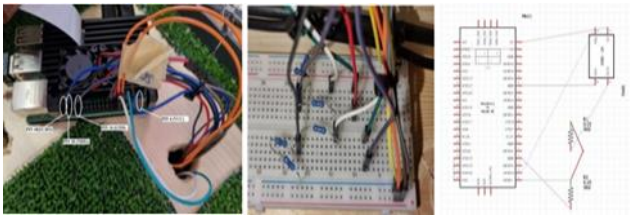


Fig. 3 – The physical and electrical connection of the second proximity sensor.

The two actuators are fixed on a camera support with horizontal and vertical movement. Both are receiving power from an external power source comprising two batteries, and the voltage is reduced by a step-down DC-DC voltage regulator. For better efficiency, the ground is connected to the Raspberry Pi pin through the breadboard (Fig. 4).

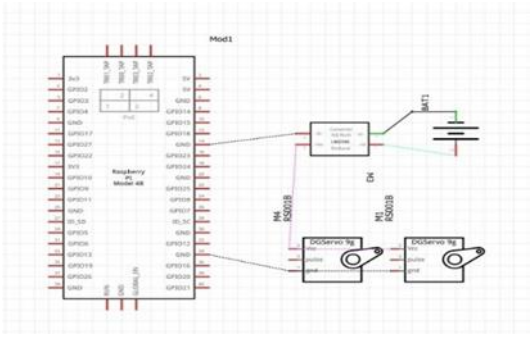


Fig. 4 – The electrical connection of the two actuators.

To maintain operational precision, the secondary camera was securely mounted onto the previously described actuator assembly. It draws energy from an independent external power supply, utilizing a DC-DC step-down regulator to adjust the voltage to 6 V. Consistent with the servomotor wiring, the camera shares a common ground connection with the Raspberry Pi. Because the device outputs an analog signal, it interfaces with the mainboard via the Raspberry Pi's USB 2.0 port [20,21] (Fig. 5).

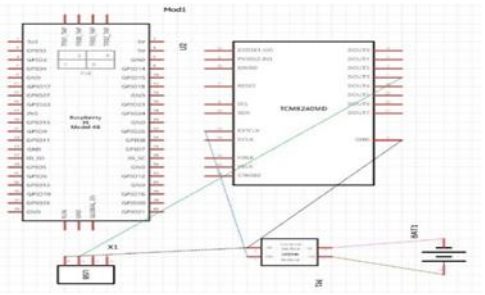


Fig. 5 – The electrical connection of the CMOS camera module.

The last element, the laser, is receiving power from the Raspberry Pi pin 1, which has a voltage of 3.3 V. As the laser functions only with a 3 V voltage, two resistors are used (Fig. 6).

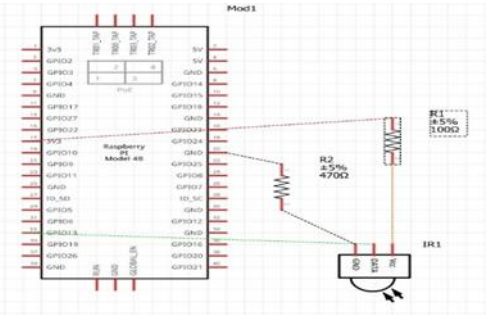


Fig. 6 – The electrical connection of the laser.

## 5. SOFTWARE COMPONENTS

The Raspberry Pi 4 Model B utilizes Raspberry Pi OS as its primary operating system. This software environment is engineered specifically to complement the board's hardware architecture, ensuring seamless driver integration, optimized resource management, and overall system reliability [22,23]. The operating environment provides a comprehensive software stack, anchored by a Linux-based kernel and supplemented by an extensive array of system libraries and development utilities. Beyond the core kernel, the OS includes a graphical user interface (GUI) and pre-integrated software modules designed to streamline system

administration and software engineering tasks. Furthermore, the platform natively supports wireless connectivity through dedicated Bluetooth and Wi-Fi management tools.

The control logic for the peripheral hardware is implemented using Python (version 3.11.2). This programming language was selected for its native compatibility with the OS and its vast ecosystem of specialized libraries, which significantly optimized the development cycle. In the initial phase of the software design, several key libraries were utilized to bridge the gap between hardware and software: ultralytics was employed for the object recognition models, picamera2 served for direct optical sensor management, and pigpio was used for the efficient processing of sensor data via the GPIO pins. Standard Python modules, such as time and os, were also integrated to handle timing operations and user-interface interactions (Fig. 7).

The second module of the program retains many of these core libraries but introduces JSON (JavaScript Object Notation) and NumPy to the architecture. Specifically, JSON is used to define and store the operational boundaries and reference parameters for the actuators, while the NumPy library provides the computational power required for real-time numerical analysis and motion calculations (Fig. 7).

```
from ultralytics import YOLO
from picamera2 import Picamera2
import pigpio
import cv2
import time
import os
```

```
import cv2
import json
import pigpio
import numpy as np
from time import sleep
from gpiozero import DistanceSensor, LED
import os
```

Fig. 7: Libraries used to program the system

The database for this simulation was created online, using the Roboflow site. It was created using a YOLO (You Only Look Once) model. The pictures for it were taken with the Raspberry Pi 3 Camera NoIR and were transferred to a laptop using the app FileZilla [24–26].

As mentioned above, all the electrical connections were realized using the Fritzing program [27].

To ensure better control over the programming process, the RealVNC app was used [28,29].

## 6. SYSTEM OPTIMIZATIONS

When it comes to surveillance systems, the optimizations must be complex, and they address a large scale of components. Within this project, the optimizations are applied to each one.

To avoid overloading the board, the powering of the hardware devices was divided. To do this, some components were powered directly from it, and the others were powered using external power supplies. As the initial voltage was not suitable for the second category mentioned above, step-down voltage regulators were used. Also, to stabilize the signal within the circuit, the grounding was common for all the hardware components.

Regarding the software optimization, the two most important improvements are starting the recording only when something is detected in the proximity and the automatic identification system starting only when necessary. These two improvements represent a major advantage when it comes to energy and resource consumption. In terms of functionality, the second camera was programmed to automatically track the moving object, and the laser is activated only when necessary, for short periods of time, and all the information (identification data, pre-established messages, and alarms) can be seen on the same display.

To create a user-friendly program, the interface is intuitive. All the principal folders and the scripts are well organized; all the functions can be tested individually, and the execution can be manually terminated.

## 7. SOFTWARE-HARDWARE INTEGRATION

To achieve a high functionality rate of the integrated system, the hardware devices chosen are compatible with the Raspberry Pi 4 Model B. To ensure electrical compatibility, external sources of power, step-down voltage regulators, and electrical resistors were used. Logical compatibility is ensured, as mentioned above, through the use of the correct libraries.

The logical control is from only one source, which gives the system more coordination. The main board controls all signals coming from and transmitted to the proximity sensors, the two cameras, the two actuators, and the laser, as well as the process of analyzing and transmitting the alarms.

The most important principle of hardware-software integration is the synchronizing of all devices with the whole program. This is because each hardware device sends a signal or starts a software action, and each software action influences at least one hardware device. For instance, when the first proximity sensor detects an object within its threshold range, the software triggers the primary camera to perform identification against the trained YOLO database; if the object is not confirmed as an authorized entity, the program displays an alert and activates the second module, which governs tracking and defense. Within this module, once the target's distance falls to 20 centimeters, the code triggers the second camera to begin continuous automatic tracking, recalculating the object's position from consecutive frames. When the distance further decreases to 10 centimeters, the software flags the target as within the response perimeter and displays a request for manual authorization; only after the human operator's approval does the code command the actuators, through PWM signals, to orient the assembly toward the target and briefly activate the laser.

To obtain a well-functioning integrated system, all the signals have been adapted so that their processing is facilitated. The signals coming from the Raspberry Pi Camera, US-020 proximity sensors, and the laser are digital. The CMOS Camera Module transmits and receives an analog signal, which is the reason for using a capture card (to transform the analog signal into a digital one) [20,26]. The two actuators are controlled by PWM (pulse width modulation) signals.

## 8. VALIDATION

The efficiency of the integrated surveillance system was validated by simulating the same scenario with different objects. For this purpose, the LEGO piece was defined as “friendly,” while the other object represented the intruder.

Since the second camera, which was mounted on the actuators, was analog, it was not possible to perform object recognition using the trained YOLO model. Therefore, the code was adapted to operate within the available technical limitations. In the first scenario, the LEGO piece was used to represent the authorized person. As observed below (fig. 8),

when it entered the perimeter of the buildings, it was successfully recognized by the system, and no security measures were activated. As it approached the building where the assembly was installed, the LEGO piece was classified as an authorized person. Therefore, the system stops, and the program ends (Fig. 9).




Fig. 8 – Validation of authorized access.




Fig. 9 – Recognition and classification.

In the second scenario, a purple object represented the intruder. Both cameras detected the object, after which the required warning procedures were activated (Fig. 10).

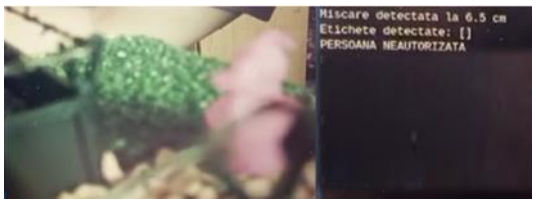



Fig. 10 – Validation of detection and classification.

Also, for the second part, the object was recognized at 20 cm and began to be tracked automatically. At 10 cm, the actuators are activated to take the final measures, with human approval (Fig. 11).



Fig. 11 – Recognition and final measures.

## 9. **CONCLUSIONS**

The development of this system demonstrates the effectiveness and feasibility of a low-cost intelligent maritime surveillance solution for countering piracy threats. During the process, numerous challenges were encountered. Some of them were represented by the compatibility between hardware and software components, adjusting the working parameters and programming each device to increase the efficiency of the system, managing the power variations, and real-time data processing.

The simulation process for validating the functionality of the surveillance system was successful. There were four simulated scenarios. During the first two, the approaching element was a friendly one, which was detected, and no actions or alarms were triggered. While simulating the last two scenarios, an intruder approached. The system automatically identified the suspect, triggering the alarms. After reaching the minimum safety distance, the message for commanding actions appeared. In the end, after human approval, auto-tracking and countermeasures went on.

The system is versatile, given that it can be used not only on-board vessels for piracy countermeasures, but also in private and public areas (after undergoing some changes), to ensure protection supply.

Furthermore, it has been proven to be an advantage in the economic field. Because of the optimizations brought to it, the system consumes less energy and resources.

Considering the importance of maritime trading for the economy, the vessels transiting risk areas and their crews need more protection. To achieve this, the integrated surveillance system is designed to enable non-lethal, deterrent actions. While this study focuses on the technical integration of hardware and software modules, subsequent research will rigorously validate the system's operational performance and overall efficiency.

Beyond its strictly maritime utility, the flexibility of this design allows for easy adaptation to monitor strategic objectives, such as the Port of Constanța or nuclear power plants, offering a viable solution for the early detection of drones and other emerging threats targeting critical infrastructure.

In conclusion, the proposed integrated surveillance system represents an efficient, practical method to improve maritime safety and security at sea. Offering low-cost hardware and software solutions, facile to integrate on board commercial vessels and easy to use, the system ensures early threat detection and viable automated solutions to provide more safety to the crew.

This paper represents a preliminary stage of the research. Currently, the authors' efforts are focused on developing a technological demonstrator (physical prototype), with the aim of practically implementing and validating the system under real operational conditions

## ACKNOWLEDGEMENT

The authors would like to express their gratitude to the Ministry of National Defense, through the Romanian Naval Academy "Mircea cel Bătrân", for funding the hardware components and for providing access to the Robotics and Data Transmissions laboratory, which made the practical implementation of this research possible.

## CREDIT AUTHORSHIP CONTRIBUTION STATEMENT

Sergiu LUPU: Resources, supervision, validation, writing, review and editing.

Ovidiu CRISTEA*: Methodology, supervision, writing, review, and editing.

Clara Georgeta LIȚU: Investigation, software, data curation, writing, and original draft.

Andrei POCORA: Validation, formal analysis, visualization.

Nicolae-Silviu POPA: Conceptualization, methodology, investigation.

Claudia Laurența POPESCU: Formal analysis, supervision, validation, writing, review, and editing.

*Received on 27 April 2026*

## REFERENCES


1. "ICC International Maritime Bureau piracy and armed robbery against ships report for the period." [Online]. Available: www.icc-ccs.org.
2. "IMB piracy & armed robbery map 2026": https://icc-ccs.org/map/
3. Z. He, C. Wang, J. Gao, and Y. Xie, "Assessment of global shipping risk caused by maritime piracy," Heliyon, **9**, *10* (October 2023).
4. S.A. Samya, V. Nagarajan, A. Appathurai, and S.E. Suniram, "Software cost effort and time estimation using dragonfly whale lion optimized deep neural network," Revue Roumaine des Sciences Techniques Série Électrotechnique et Énergétique, **69**, *4*, pp. 431–436 (November 2024).
5. W. Akhahenda, H. Kim, W.J. Son, J.S. Lee, and I.S. Cho, "Analysis of maritime piracy trends and patterns using spatial autocorrelation in Africa," Journal of International Maritime Safety, Environmental Affairs, and Shipping, **8**, *1–2* (2024).
6. Z. He, C. Wang, J. Gao, and Y. Xie, "Assessment of global shipping risk caused by maritime piracy," Heliyon, **9**, *10* (October 2023).
7. N.J. ECE and H. KURT, "Analysis of maritime piracy by using qualitative methods," Mersin University Journal of Maritime Faculty, **3**, *2*, pp. 37–50 (December 2021).
8. V.N. Jafarova et al., "Prediction of electronic, magnetic, and structural stability characteristics in Al- and Ga-doped single-walled SiC nanotubes: ab initio study using DFT," Physical Chemistry Chemical Physics, **27**, *48*, pp. 25980–26010 (December 2025).
9. S.N. Jyothi, K.V. Vardhan, "Design and implementation of real-time security surveillance system using IoT," International Conference on Communication and Electronics Systems (ICCES), IEEE (2016).
10. D. Mathew, G. Kirubasri, K. Vijay, I. Eugene Berna, and K.R. Sowmia, "System for detecting intrusions using Raspberry Pi," in 2023 International Conference on Computer Communication and Informatics (ICCCI 2023), Institute of Electrical and Electronics Engineers Inc. (2023).
11. T. Yathavi, R. Ajay, P.R. Hariesh Varshan, J.A. Timothy, "Development of auto tracking and target fixing gun using machine vision," International Conference on System, Computation, Automation and Networking (ICSCAN), pp. 1–5, IEEE (2020).
12. Raspberry Pi Ltd., "Raspberry Pi 4 Model B – Raspberry Pi", https://www.raspberrypi.com/products/raspberry-pi-4-model-b/
13. "Datasheet: Raspberry Pi 4 Model B" (2024). Accessed: April 27, 2026, https://www.raspberrypi.org
14. C.-G. Dumitrache, C. Viorel Marian, G. Predusca, F.M. Barbu, and M. Neferu, "Wireless authentication system for Internet of Things using FreeRADIUS and blockchain," Rev. Roum. Sci. Techn. – Électrotechn. et Énerg., **70** (2025).
15. "Buy a Raspberry Pi Camera Module 3 – Raspberry Pi," Accessed: April 27, 2026, https://www.raspberrypi.com/products/camera-module-3/
16. "Raspberry Pi Camera Module 3: Standard, NoIR, Wide, and Wide NoIR" (2023), https://datasheets.raspberrypi.com/camera/camera-module-3-product-brief.pdf
17. "US-020 ultrasonic sensor module for Raspberry Pi Arduino robot, new." Available: https://everythingpi.co.uk/products/us-020-ultrasonic-sensor-module-for-raspberry-pi-arduino-robot-new-1
18. V. Atanasov, "Hybrid architecture for real-time object detection from UAV video streams using external ROI processing and embedded optimization," in 2025 19th International Conference on Electrical Machines, Drives and Power Systems (ELMA 2025), Proceedings, Institute of Electrical and Electronics Engineers Inc. (2025).
19. H. Zou, H. Jiao, and C. Fu, "Realization of intelligent monitoring system based on Raspberry Pi," in 2024 IEEE 2nd International Conference on Electrical, Automation and Computer Engineering (ICEACE 2024), pp. 317–320, Institute of Electrical and Electronics Engineers Inc. (2024).
20. *2KM NTSC product specification*, datasheet of the CMOS camera module – 728×488 (SparkFun SEN-11745): https://cdn.sparkfun.com/datasheets/Sensors/LightImaging/32KM_spec.docx.pdf
21. S.K.B. Sangeetha, P. Anitha Rajakumari, A.A. Pandian, S. Kumar, and N.M. Deshpande, "Deep learning-based object detection across multiple visual domains," in 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI 2025), pp. 805–808, Institute of Electrical and Electronics Engineers Inc. (2025).
22. O. Cristea, N.S. Popa, M.G. Manea, and C. Popa, "About the automation of an autonomous sail-propelled search drone," Engineering, Technology and Applied Science Research, **13**, *6*, pp. 12334–12341 (December 2023).
23. L. Wang, Y. Huang, and Y. Yang, "Drone-RGBT: multispectral small object detection based on early fusion," Institute of Electrical and Electronics Engineers (IEEE), pp. 29–33 (January 2026).
24. D.R. Arun, C.C. Columbus, A. Bhuvanesh, and A.S. Sumithra, "Smart crowd monitoring system using IoT-based YOLO-Ghost," Revue Roumaine des Sciences Techniques Série Électrotechnique et Énergétique, **69**, *3*, pp. 345–350 (September 2024).
25. C. Yang, J. Wang, K. Li, Y. Feng, and L. Shi, "An improved YOLOv8 with AFPN for maritime UAV object detection," Institute of Electrical and Electronics Engineers (IEEE), pp. 158–162 (January 2026).
26. K. Yamashita, H. Murakami, L. Chansomphou, M. Okuyama, "Ultrasonic array sensor using piezoelectric film on silicon diaphragm and its resonant-frequency tuning," in TRANSDUCERS'03 – 12th International Conference on Solid-State Sensors, Actuators and Microsystems, 1, p. 939, IEEE (2003), https://www.sciencedirect.com/science/article/abs/pii/S0924424703006502
27. "Fritzing." Available: https://fritzing.org/
28. "RealVNC: The world's most trusted remote access software." Available: https://www.realvnc.com/en/.
29. "RealVNC Connect: Simple, secure, ready-to-use remote access and support software." Accessed: April 27, 2026. [Online]. Available: https://www.realvnc.com/en/connect/.