INTRUSION IDENTIFICATION SYSTEM BASED ON 360 THERMAL CAMERAS AND POST-PROCESSING USING ARTIFICIAL INTELLIGENCE MODELS

Mª Cinta Urgel Fernández
ICAI – Universidad Pontificia Comillas

ABSTRACT This paper presents an innovative perimeter video surveillance system designed to optimize security and operational efficiency in facilities, such as photovoltaic plants and electrical substations, as part of the ongoing industrial digital transformation. The central proposal involves replacing fixed thermal cameras with 360-degree thermal cameras integrated with a YOLOv11 Artificial Intelligence (AI) model for image post-processing. Substantial improvements in intrusion detection, minimization of false alarms, and cost optimization are demonstrated. Simulation results confirm a 70% reduction in devices and a 65% saving in overall system costs, including acquisition, installation, and maintenance. This approach not only enhances the reliability of the security system but also drives digital transformation and resource efficiency, key elements in the evolution towards a smarter industry.

KEY WORDS Perimeter Security, Video Surveillance, Thermal Cameras, Intrusion Detection, Artificial Intelligence, YOLOv11.

I. INTRODUCTION

The current era is defined by the digital transformation that has permeated all sectors, giving rise to a new paradigm in industry, often referred to as Industry 4.0. In this modern industrial landscape, characterized by the interconnection of systems, advanced automation, massive data management, and artificial intelligence, the perimeter security of infrastructures, such as photovoltaic plants (Figure 1) and electrical substations, acquires fundamental strategic importance. These facilities, often the backbone of the energy and productive matrix, are inherently vulnerable to intrusions that can lead to material damage, operational disruptions, or even risks to personnel safety.

Figure 1: Photovoltaic plant

Traditional surveillance of these infrastructures has relied on systems employing a large number of fixed thermal cameras and domes with manual tracking.

While these technologies have offered valid solutions, they present significant limitations within this evolving industrial context. The necessity of deploying numerous devices to ensure comprehensive coverage of extensive perimeters considerably increases acquisition, deployment, and maintenance costs, while also complicating system management. More critically, these systems are highly susceptible to false alarms caused by environmental factors or wildlife. This excessive volume of irrelevant alerts overloads security personnel, compromises their productivity, and, most dangerously, heightens the risk of real intrusions going unnoticed.

In response to these deficiencies and aligning with the principles of industrial advancement, this work proposes an evolutionary strategy in perimeter surveillance. The solution involves integrating 360-degree thermal cameras with an advanced AI model for image post-processing. This approach aims to transform industrial security through the digitalization of surveillance processes, optimizing coverage with fewer devices, minimizing false alarms, and automating response. The proposed system promises not only greater efficiency and reduced investment and maintenance costs but also ensures an automated and more precise response capability to real threats. It is thus configured as a pillar in the operational cyber-resilience and efficiency optimization within the digital industrial landscape.

II. STATE OF THE ART

The use of thermographic cameras has been a widely adopted solution for perimeter surveillance. However, the fixed thermographic cameras commonly used present several challenges. These challenges underscore the limitations of traditional systems and highlight the necessity for innovative approaches aligned with the tenets of the digital industrial transformation:

- ➢ Limited Coverage:

Fixed thermal cameras possess a restricted field of view. This limitation necessitates the installation of a multitude of units to adequately cover the entirety of an installation's perimeter. Such extensive deployment considerably escalates acquisition, installation, and maintenance costs, while also increasing the overall complexity of the surveillance system.

- ➢ High Rate of False Alarms:

These cameras are susceptible to generating a high number of erroneous detections. Alarms can be triggered by non-relevant movements, such as wildlife, environmental changes or strong backlighting. This excessive volume of non-critical alerts increases the workload for security personnel and elevates the risk of real intrusions going unnoticed due to the overwhelming number of false positives. The constant need for manual verification and filtering of these alarms leads to operational inefficiency and potential resource exhaustion.

In recent years, technological advancements have driven the industry towards more integrated and intelligent solutions.

360-degree thermal cameras represent a significant leap forward, addressing the limitation of limited coverage by enabling the surveillance of larger areas with fewer devices and at reduced costs. Furthermore, the pervasive issue of high false alarm rates is being mitigated through the application of advanced Artificial Intelligence (AI) models to the images captured by these cameras. This intelligent post-processing allows for a more precise distinction between real threats and non-critical events, thereby optimizing alert management and substantially reducing false positives. This evolution signifies a move from reactive, labor-intensive surveillance to proactive, intelligent monitoring.

III. TECHNOLOGY DESCRIPTION

360° THERMAL CAMERAS AS ADVANCED IIOT SENSORS

360° thermal cameras are fundamental components of the Industrial Internet of Things (IIoT) infrastructure, functioning as intelligent sensors that collect critical operational data for security purposes. Their primary advantage lies in their ability to provide a complete 360-degree panoramic view, which contrasts with the limited field of view of conventional fixed cameras. This feature is key to the digitalization of perimeter monitoring, as it allows for covering significantly larger areas with a reduced number of devices.

The operation of these cameras is based on detecting the infrared radiation emitted by objects due to their temperature. This capability allows them to operate effectively in zero-visibility conditions, such as total darkness, or under adverse weather conditions like fog, where traditional optical cameras would fail. This robustness in data capture is crucial for ensuring continuous monitoring and system reliability.

For this project, the InfiRay XSENTRY-UM619 model, [1], has been selected, Figure 2.

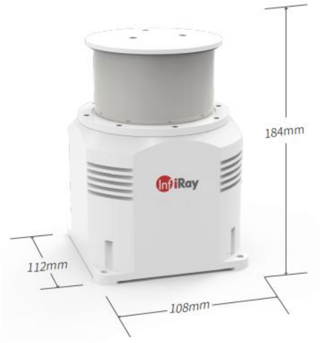

Figure 2: InfiRay XSENTRY 360° Thermal Camera

This camera provides detailed thermal images for precise intrusion detection. It generates high-resolution panoramas (up to 13000x512) for comprehensive coverage. Its multiple focal lengths (13mm, 19mm, and 25mm) allow detection of people up to 750 meters and vehicles up to 1500 meters with the longest-range lens. Compatibility with Power over Ethernet (POE) facilitates its integration into industrial networks. Its robust design ensures reliable outdoor performance.

DOME (PTZ) CAMERAS FOR AUTOMATED VERIFICATION AND TRACKING

PTZ (Pan-Tilt-Zoom) cameras, commonly known as dome cameras, play a crucial complementary role in the proposed system, undertaking detailed visual verification and automated event tracking. While 360° thermal cameras focus on initial detection across wide areas, dome cameras provide the capability to precisely inspect any point of interest. This marks a significant evolution from previous systems, which required manual intrusion tracking, often leading to inefficiencies and delayed responses.

The PTZ functionality (Pan for horizontal movement, Tilt for vertical movement, and Zoom for zooming in/out) provides these cameras with superior operational flexibility, allowing for panoramic sweeps, angle adjustments, and detailed close-ups. In the context of the Smart Industry, this capability translates into an efficient and automated response. Once the 360° thermal camera detects a potential intrusion, the dome camera automatically positions itself at the precise location of the event and initiates autonomous tracking, accelerating situation assessment and decision-making by security personnel.

The Hikvision DS-2DF9C435IH-DLW model from the DarkFighterX series, [2], has been selected. This series stands out for its innovative dual-sensor technology (infrared light and visible light) and its bi-spectrum image fusion, which provides bright and sharp colour images even in extremely low light conditions. This capability is vital for obtaining clear and detailed visual information of an intrusion during the night or in low-light environments.

The DS-2DF9C435IH-DLW model was chosen for its superior features in infrastructure applications. It offers an extended infrared range that significantly enhances coverage in darkness. Its high sensitivity to light ensures quality images even in very dim conditions. Furthermore, its powerful optical zoom is crucial for identifying details at long distances, and its high resolution contributes to sharper captured images. These robust capabilities ensure the dome can provide precise verification and reliable autonomous tracking, integrating seamlessly into a digitalized security system.

Figure 3: Hikvision DS-2DF9C435IH-DLW Dome Camera

ARTIFICIAL INTELLIGENCE (AI) AND COMPUTER VISION FOR INTELLIGENT POST-PROCESSING

Artificial Intelligence (AI) stands as the central component that equips the video surveillance system with "intelligence", enabling it to simulate and execute human cognitive processes such as learning, understanding, and real-time decision-making. Within AI, Computer Vision, [3], is the discipline that empowers machines to interpret and comprehend the visual world. Its objective is to derive meaningful information from digital images and videos, replicating human ability to identify and understand people, objects, and patterns.

In the context of today's digital industry, AI, and particularly Computer Vision, are fundamental for process optimization and the reduction of inefficiencies. Traditional video surveillance systems generated a high number of false alarms, overloading security personnel and compromising the detection of real intrusions. This is where AI provides a differential value.

For video post-processing and intelligent intrusion detection, the YOLOv11 (You Only Look Once) model is proposed. YOLO is a real-time object detection algorithm that utilizes Convolutional Neural Networks (CNNs). CNNs, Figure 4, are neural networks specialized in processing two-dimensional data like images, excelling in visual recognition tasks such as image detection, segmentation, and classification. Unlike image classification, which assigns a general label to the image, object detection identifies and locates individual elements using bounding boxes, providing the precise position of a potential intrusion.

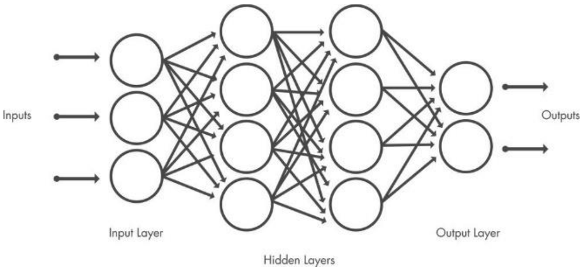

Figure 4: Convolutional Neural Network (CNN)

YOLOv11 represents the latest evolution of this series and has been selected to overcome the limitations of its predecessor, YOLOv8, which showed deficiencies in robustness and reliability under real-world conditions, generating false alarms. The improvements introduced in YOLOv11, [4], are critical for an industrial environment:

- Higher Accuracy (mAP):

The network has been redesigned for more efficient feature extraction, resulting in more reliable and consistent detections, even with partially hidden, poorly lit, or distant objects. This directly translates into a significant reduction in false positives, which is vital for the operational efficiency of security personnel.

- Greater Computational Efficiency:

YOLOv11 uses fewer parameters and operations (FLOPs). This optimization drastically reduces memory consumption and computational resources, making it ideal for implementation on edge devices (Edge AI).

- Faster Inference Speed:

The reduction in model complexity translates into lower inference times, especially noticeable on CPUs and resource-constrained devices. This is crucial for real-time processing of video streams, enabling a high response capability to security events.

Figure 5 visually demonstrates the superior performance of YOLOv11 over previous versions, particularly YOLOv8, in terms of accuracy (mAP) and inference latency.

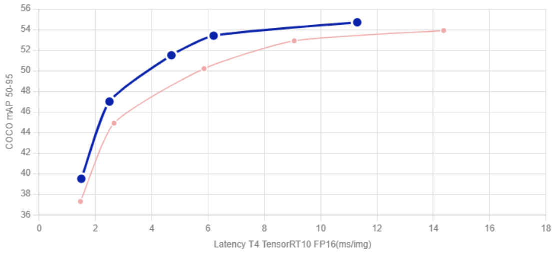

Figure 5: Performance Curve (mAP vs. Latency) of YOLOv11 and YOLOv8

The implementation of YOLOv11 ensures that the system can distinguish more precisely between real intrusions (humans or vehicles) and environmental noise sources such as vegetation or wildlife. This intelligent filtering capability is key to optimizing surveillance processes, preventing personnel overload and guaranteeing that resources are allocated to genuine threats, a primary objective in a digitally transformed industry.

INTEGRATED SYSTEM WORKFLOW

The effective synergy between these advanced technologies culminates in a streamlined and automated operational workflow, which is a hallmark of intelligent industrial processes. This intelligent interconnection not only enhances security but also drives deep operational optimization through process automation and efficient information management. Figure 6 illustrates the sequential interaction and data flow among the system's core components for real-time intrusion identification and response.

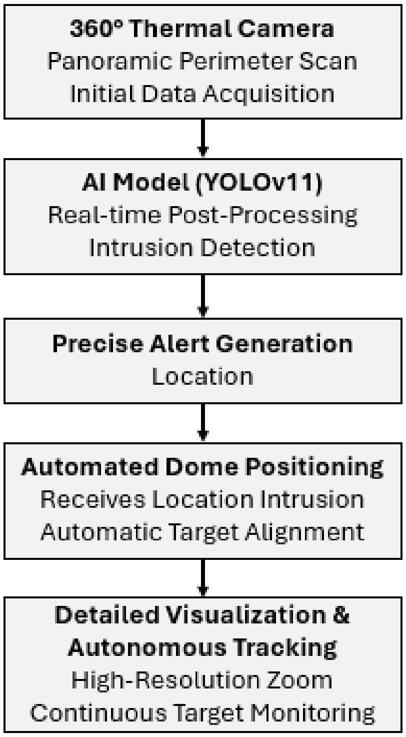

Figure 6: Workflow System

IV. RESULTS AND CONCLUSIONS

This Master's Thesis successfully addresses the challenge of optimizing security in facilities, such as photovoltaic plants, by proposing an innovative perimeter video surveillance system aligned with digital industrial transformation. The project's objectives, aiming to overcome the limitations of conventional systems with inefficient coverage and high false alarm rates, have been effectively met.

Key findings validate the proposed solution's feasibility and advantages. Firstly, perimeter coverage optimization is achieved through 360-degree thermal cameras. Simulations demonstrate an approximate 70% reduction in necessary devices to cover the same area, transitioning from fifteen fixed cameras to just four 360-degree units. This significant reduction is visually depicted in comparative simulations (Figure 7 and Figure 8).

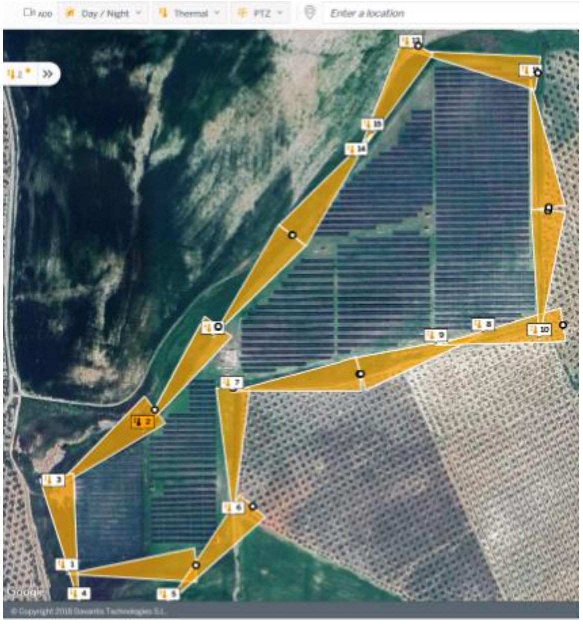

Figure 7: Fixed Thermal Camera Simulation

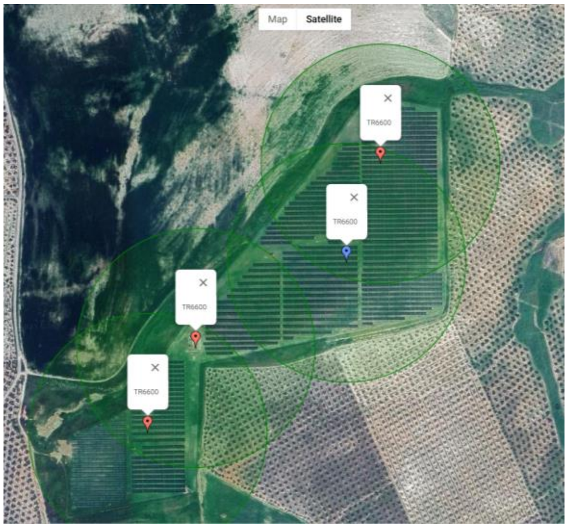

Figure 8: 360-degree Thermal Camera Simulation

Beyond direct economic savings, device reduction yields substantial operational benefits crucial for modern industrial environments:

- Deployment Simplification: Fewer installation points reduce labour hours and materials, streamlining system commissioning.
- Increased System Reliability: Fewer components mean lower failure risks, cutting corrective maintenance costs and enhancing operational resilience.
- Optimized Resource Utilization: Maximizing each 360° camera's field of view and eliminating redundancies ensures efficient resource use, contributing to smarter asset management.

Secondly, false alarm minimization is achieved through advanced Artificial Intelligence models. While YOLOv8 had reliability limitations, generating false positives, the proposed YOLOv11 significantly improves intrusion detection accuracy. Its architectural optimizations yield higher accuracy (mAP), greater computational efficiency, and faster inference, enabling better discrimination between real intrusions and environmental noise.

Thirdly, expedited response to real intrusions is ensured by the intelligent integration of 360-degree thermal cameras with dome-type cameras. The 360-degree camera handles initial detection, while the selected Hikvision dome automatically positions for detailed and autonomous target tracking. This optimizes human resource utilization and enhances immediate decision-making.

These factors collectively reinforce the proposed system's economic, technical, and operational viability, offering a more efficient, robust, and sustainable approach to perimeter security for infrastructures, and establishing it as a model for process optimization driven by digital technology.

V. FUTURE PERSPECTIVES

Despite current challenges, Artificial Intelligence has solidified its position as a cross-cutting and strategic technology with an expanding transformative potential. Its impact will continue to redefine how industries operate, interconnect, and make decisions, directly influencing future enhancements for our intelligent surveillance system.

- Edge AI (Artificial Intelligence at the Edge):

This trend, [5], shifts data processing and intelligence directly from centralized data centers (the cloud) to end devices or "edge devices", such as our 360° thermal cameras and dome cameras. For our industrial perimeter security system, Edge AI is revolutionary:

  - Reduced Latency:

    Local processing eliminates cloud data transfer, drastically reducing latency for near-instantaneous decision-making in real-time intrusion scenarios.

  - Bandwidth Optimization:

    Processing data at the source alleviates network load by sending only relevant alerts, crucial for remote sites and industrial network efficiency.

  - Enhanced Privacy and Security:

    Sensitive video data remains within the facility, bolstering privacy and cybersecurity by reducing external exposure and ensuring data residency compliance.

  - Energy Efficiency:

    Specialized hardware (e.g., NVIDIA Jetson, Google Coral) enables energy-efficient Computer Vision models. Deploying refined YOLOv11 directly on our thermal cameras would optimize resources and enhance system resilience.

- Augmented Intelligence:

This trend, [6], emphasizes symbiotic human-AI collaboration. AI acts as a strategic ally, enhancing human capabilities and automating repetitive tasks for security personnel. Our project's AI already automates detection and tracking. Future developments would further augment operators with advanced real-time insights, predictive analytics, and suggested response protocols, enabling focus on critical decision-making and strategic oversight.

- Explainable Artificial Intelligence (XAI):

As AI integrates into critical industrial systems, understanding how and why a model makes decisions becomes fundamental. XAI develops methods to interpret, justify, and audit AI system behavior, even in complex architectures. For our intrusion detection system, XAI would be invaluable, providing operators with explanations for specific alarms. This fosters trust in the automated system and aids rapid, informed decision-making during critical security events, crucial for validation, continuous improvement, and broad acceptance of AI in industrial security.

The horizon of AI in Smart Industry is a future where technology optimizes processes and empowers humans, creating autonomous, intelligent, and collaborative systems. This evolution is essential for addressing future security, efficiency, and sustainability challenges, directly informing the development of intelligent surveillance solutions like ours.

VI. REFERENCES

[1] Visiotech, «IRS-XSENTRY-UM619». Available: https://www.visiotechsecurity.com/en/products/ip-cctv-1/thermal-411/infiray-774/irs-xsentry-um619-detail#tab=prod_0. [Last Access: 1 June 2025]

[2] Hikvision, «9-inch 4 MP 35X DarkFighterX IR Network Speed Dome». Available: https://www.hikvision.com/my/products/IP-Products/PTZ-Cameras/Ultra-Series/DS-2DF9C435IH-DLW/. [Last Access: 4 June 2025]

[3] IBM, «What is Computer Vision». Available: https://www.ibm.com/think/topics/computer-vision. [Last Access: 24 June 2025].

[4] Ultralytics, «YOLO11 vs YOLOv8: comparación detallada». Available: https://docs.ultralytics.com/es/compare/yolo11-vs-yolov8/. [Last Access: 6 July 2025].

[5] C. L. Chowdhary, M. L. Alazab, A. L. Chaudhary, S. L. Hakak y T. R. Gadekallu, «Real-time face mask detection on edge IoT devices,» de Computer Vision and Recognition Systems Using Machine and Deep Learning Approaches Fundamentals, Technologies and Applications.

[6] Forbes, «The 10 Biggest AI Trends Of 2025 Everyone Must Be Ready For Today». Available: https://www.forbes.com/sites/bernardmarr/2024/09/24/the-10-biggest-ai-trends-of-2025-everyone-must-be-ready-for-today/. [Last Access: 29 June 2025]