Cognitive and Predictive Intelligence for threat identification and operational support in Critical Infrastructure Protection

Stella Parisi, Konstantinos Ioannidis, Stefanos Vrochidis, Ioannis Kompatsiaris

Centre for Research and Technology Hellas, 6th km Charilaou-Thermi Rd, P.O. Box 60361, Thermi, GR 57001 Thessaloniki, Greece

Keywords: *Critical Infrastructure Protection, Cognitive Intelligence, Predictive Intelligence, Evaluation of threats and vulnerabilities, Surveillance of environment, Autonomous resource allocation*

Abstract

The TESTUDO project addresses the growing demand for autonomous solutions in Critical Infrastructure (CI) protection, motivated by the increasing vulnerability of the European territory to complex and interconnected risks. TESTUDO combines cognitive and predictive intelligence, aiming to provide a scalable and resilient architecture capable of continuous threat detection, autonomous resource allocation, and real-time decision support for CI operators. The system integrates a swarm of unmanned ground and aerial vehicles, multispectral sensors, and advanced detection algorithms to enhance the situation awareness of its users across diverse operational environments. TESTUDO will validate its effectiveness in detecting, preventing, and mitigating a range of CI risks though a series of operational and cross-sectorial trials. This paper outlines the architecture, implementation approach, and expected results while addressing key challenges, including AI-related vulnerabilities and future work on prototype development.

Introduction

In recent years, Europe has faced several complex challenges that have threatened the stability, security, and prosperity of its communities [1]. These challenges significantly impact Critical Infrastructures (CI), essential to the European well-being and economic stability. The European Commission's Security Union Strategy emphasises the need for reliable, robust, and independent operation of these infrastructures. [2]. However, as CIs become more digitised and interconnected, they also grow more vulnerable to complicated threats/risks, such as cyber-attacks and physical disruptions [3]. The failure of one CI can trigger a ripple effect across interconnected networks, endangering both the CI and the first responders tasked with managing these incidents [4]. Therefore, CI operators require innovative and sometimes autonomous solutions that adjust to diverse operational demands, and support critical decision-making for timely and efficient response to such challenges [5]. Although a wide range of established technologies for CI operations and risk reduction exist, there is currently no integrated, holistic solution capable of utilising diverse autonomous assets for complete CI security. This gap presents a significant opportunity for the advancement of technological capabilities.

The TESTUDO project seeks to improve CI protection via a comprehensive architecture that integrates a network of Unmanned Ground Vehicles (UGVs), Unmanned Aerial Vehicles (UAVs), and fixed sensors to facilitate rapid threat detection, autonomous allocation of resources, and predictive modelling that can proactively mitigate developing incidents. Designed for various circumstances, ranging from urban infrastructures to remote, inaccessible areas, TESTUDO enables CI operators to respond efficiently to complex threats and risks. To this end, TESTUDO incorporates numerous cognition capabilities to facilitate continuous autonomous threat detection and decision-making assistance for CI operators. The project will design and implement a data-driven and process oriented platform that prioritises scalability, resilience, and real-time situation awareness via a multi-layered approach. The high-level architecture comprises of layers that include Data Collection & Edge Processing, Autonomous Functionality Services, Processing & Detection Services, Secure Communications and Network Manager, and the User Interface Applications, as depicted in Figure 1.

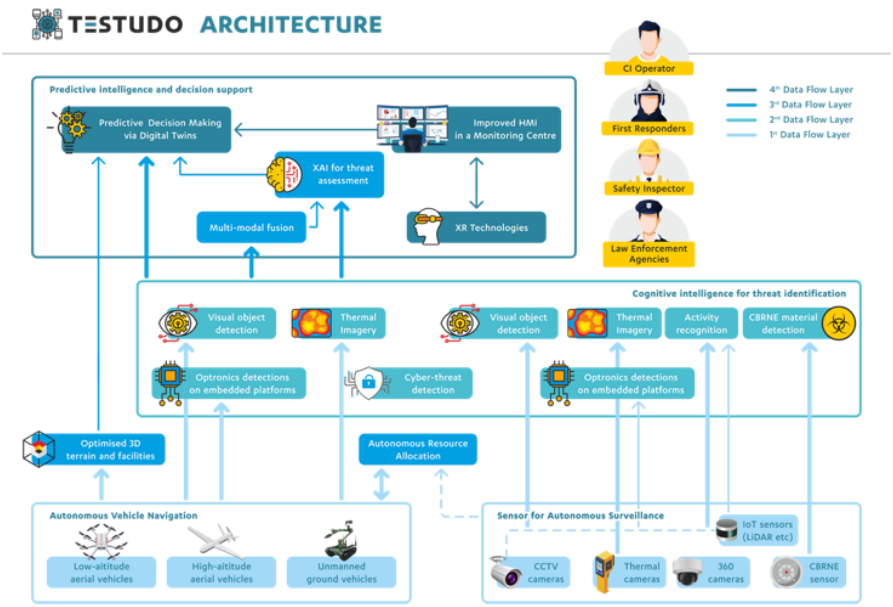

Figure 1: Preliminary, high-level depiction of the TESTUDO architecture, comprised of multiple key layers, each with distinct responsibilities for seamless integration and optimized data exchange across the system..

Main Concept and Challenges

TESTUDO is designed to maximize system autonomy, enabling CI operators to focus on their main responsibilities or even manage facilities remotely, if required. It integrates autonomous platforms composed of unmanned vehicles and fixed sensors, seamlessly integrating with existing facilities and legacy systems through a versatile data model tailored to CI operations. This model allows the platform to function both as a complement to existing systems and as an independent external component.

To support seamless operations across diverse conditions, TESTUDO processes multimodal data streams through advanced detection, monitoring, and prediction tools, which provide operators with real time insights and support them in complex decision-making scenarios. The project's user-centered approach involves stakeholders at each development stage, ensuring the system's functionality aligns closely with operator needs and performance requirements, as well as with relevant insights from the EU Security market study [6].

CI protection in the 21st century requires securing interconnected structures, monitoring large territories and defending against advanced cyber-attacks [5]. The TESTUDO solution aims at addressing several of these critical issues, focusing on detection, prediction and prevention of threats and hazardous events. Such challenges include improving the operational needs of CI operators and ensuring the use of different types of sensors, including existing infrastructure and legacy systems. The system must be capable of identifying diverse threats and suspicious events, even in low connectivity scenarios and hardly reachable territories. Compliance with the AI Act (Regulation (EU) 2024/1689), commission directives, and a risk-driven approach to ICT and security is essential. Other challenges include the unavailability of hardware components due to global logistic problems and ensuring that AI tools do not violate data protection or privacy regulations.

Main Cognitive and Predictive Intelligence Innovations

To correspond to these challenges, it is essential that protective methodologies evolve accordingly. The TESTUDO project aims to integrate innovative cognitive and predictive solutions to improve CI protection and redefine how CI operators detect and respond to threats. By combining autonomous

systems with sophisticated data processing and analysis, TESTUDO equips operators with knowledge that enhances situational awareness and supports timely decision-making.

Visual Detection: TESTUDO provides 24/7 object detection from visual data using deep learning models that process streams from visual spectrum cameras. The input includes images, videos, and real-time streams, which are converted into structured data outputs containing object classes, confidence levels, and bounding boxes. The detection results are delivered as annotated images, videos, and streams, ensuring that CI operators receive real-time information about detected threats, which improves situation awareness and decision-making.

Multispectral Detection: TESTUDO uses multispectral detection capabilities to maximize operational support in diverse and low visibility conditions, ensuring continuous threat detection, regardless of environmental conditions. This includes the processing of streams from thermal and infrared cameras, which provide reliable detection outcomes even in challenging environments. The structured data outputs consist of messages with confidence levels and location information. The results are overlayered images, videos, and streams with the detection outcomes.

Visual Object Recognition on Embedded Devices: TESTUDO exploits on-board computing capabilities to perform visual object recognition on embedded devices, such as UAVs and UGVs, which process visual streams locally. The system integrates custom algorithms suitable for on-edge computing, providing efficient detection from cameras. The output includes information on space occupancy via the video stream data and detection of possible threats, with the goal to achieve Autonomy on the Edge (AoE).

Activity Recognition Models: TESTUDO uses activity recognition models designed to recognize predefined actions and detect potential threats based on video content. The system processes raw videos and metadata from visual and multispectral object detection to classify activities such as panic behaviour, violent behaviour, and abandoned objects. By using both deep learning and rule-based methods, these models generate action and threat classifications along with confidence scores, helping CI operators to identify critical situations and respond effectively.

Cyber Threat Identification: TESTUDO integrates an AI module that dynamically assesses ICT infrastructure to identify vulnerabilities and detect potential cyberattacks. This module uses an anomaly-based intrusion detection system built on AI primitives, capable of identifying vulnerabilities or ongoing cyberattacks, indicating the potential impact of identified threats, and proposing countermeasures. The system processes network traces information as input, generating a library of cyber-attack indicators, including domain names, IP addresses, file hashes, and log indicators. The result is a real-time assessment of cyber threats, enabling the system to autonomously determine the best course of action to mitigate attacks, providing robust protection for the digital infrastructure of critical systems.

Explainable AI for Threat Assessment: TESTUDO uses explainable AI to identify and understand critical attacks on autonomous systems, such as drones and robots, focusing on how these attacks modify AI behaviour. By employing deep compression of AI models, the system enables non-invasive defence development. Artificial Neural Networks (ANN) are used for graph representations, mapping AI behaviour changes to generate countermeasures adapted to the target AI system, ultimately enhancing security through better AI functionality understanding.

Prediction Models via Digital Twins: TESTUDO employs Digital Twins (DTs) to develop digital replicas of the involved CIs and the integrated assets. Using decision trees and boosting models, these DTs process detection outcomes and raw or fused data to help CI operators through predictive analysis to assess situations and make proactive choices. Outputs are shared with infrastructure systems to enable real-time re-assessment, with operators always in the loop, ensuring predictive intelligence that adapts continuously to changing scenarios and supports safe and effective threat management.

These capabilities will be integrated into a highly mature and versatile system capable of protecting CI facilities against challenges like securing interconnected systems and ensuring reliable performance in

diverse conditions. Additionally, as all TESTUDO components possess autonomous functionalities, the system will provide valuable, long-term operational insights to each CI operator.

Implementation, evaluation and main outcomes

The primary objective of TESTUDO is to deliver a prototype at Technology Readiness Level 7 (TRL-7), developed through an escalated approach to autonomously manage CI protection. This prototype will integrate the technologies mentioned above for threat detection, prevention, and prediction, supporting CI personnel in reducing response times to threats and minimizing the potential for escalation.

Each TESTUDO prototype will be tested and validated through one operational trial and two large-scale, cross-sectorial trials, encompassing both short-term and long-term deployments. These trials aim to demonstrate the system's capability to address a range of CI threats, such as natural disasters, terrorist attacks, and incidents involving hazardous materials. Each iteration will deliver one prototype that will undergo rigorous testing to evaluate its effectiveness in protecting, preventing, and predicting critical events. Each validation aims to verify the robustness, flexibility, and resilience of TESTUDO platform and its intermediate prototypes. The trials will provide vital insights for CI operators and first responders, ensuring that the system can operate autonomously for prolonged intervals and adjust to diverse operational conditions.

Conclusions, Limitations and Future Work

In conclusion, TESTUDO will demonstrate a highly flexible and modular platform that can adapt to the specific needs of different CI operators. The ultimate goal is to provide a scalable, autonomous, and resilient solution for the long-term protection of CIs across Europe. Through a combination of decision-making tools, secure communication systems, and AI-powered threat assessment models, TESTUDO will deliver a unified framework that complements autonomy functionalities for enriched situation awareness and optimal response to hazardous incidents and human-made threats.

However, while the integration of AI brings valuable autonomy, it also introduces significant vulnerabilities that TESTUDO must address. AI models, while powerful, might occasionally lack the nuanced accuracy of human judgment and mislead the operators. Additionally, malicious data manipulation, such as adversarial attacks and data poisoning, could weaken model reliability, allowing certain threats to bypass detection. Exploiting model parameters to bypass security measures also poses a serious concern, as does the risk of system integration flaws, where untested AI components may inadvertently introduce weaknesses. Failures within AI systems could jeopardise essential CI operations, with privacy and data security remaining critical due to the vast amounts of sensitive data AI requires. These potential vulnerabilities emphasize the need for thorough safeguards and ongoing assessments to ensure the safe deployment of AI in CI.

Future work entails developing countermeasures against AI vulnerabilities, including strategies to enhance the strength and reliability of AI models against malicious data manipulation. Regular model validation and accuracy assessments will also be prioritized to ensure AI components remain resilient, secure, and effective in protecting CI. The next phases in TESTUDO include developing and evaluating the first prototype through an operational test, followed by two more development/integration cycles. These cycles will deliver second and third prototypes, each adding new modules and progressing to the final, fully integrated system in the project's later stages.

Acknowledgements

TESTUDO project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121258. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

1. Felice, F., Baffo, I., & Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future.*Sustainability*. https://doi.org/10.3390/su14042233.
2. EUR-Lex - 52020DC0605 - EN - EUR-Lex (europa.eu)
3. Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, 41, 491 - 514. https://doi.org/10.1177/0967010610382687.
4. Gheorghe, A.V., & Schläpfer, M. (2006). Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures. *2006 IEEE International Conference on Systems, Man and Cybernetics, 1,* 580-584.
5. Matthews, G., Reinerman-Jones, L., Barber, D.J., Teo, G., Wohleber, R.W., Lin, J., & Panganiban, A.R. (2016). Resilient autonomous systems: Challenges and solutions. *2016 Resilience Week (RWS),* 208-213.
6. European Commission, Directorate-General for Migration and Home Affairs, *EU security market study : final report*, Publications Office of the European Union, 2022, **https://data.europa.eu/doi/10.2837/19472**
7. Alcaraz, C., & Zeadally, S. (2015). *Critical infrastructure protection: Requirements and challenges for the 21st century.* Int. J. Crit. Infrastructure Prot., 8, 53-66.