TESTUDO: Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention

Stella Parisi[1], *Konstantinos Ioannidis*[1], *Stefanos Vrochidis*[1], *Ioannis Kompatsiaris*[1]

[1] *Centre for Research and Technology Hellas, 6th km Charilaou-Thermi Rd, P.O.*

Box 60361, Thermi, GR 57001 Thessaloniki, Greece.

Keywords: *Critical Infrastructure Protection, Emergency Services, Evaluation of threats and vulnerabilities, Robotics, Tele-Robotics & Autonomous Systems, Surveillance of environment, Autonomous resource allocation*

Extended Abstract

In recent years, Europe has faced a range of complex challenges, both internally and in its adjacent territories, which have affected the stability, security, and prosperity of local communities [1]. These changes, combined with technological advancements and emerging threats, pose significant risks to Critical Infrastructures (CI). Such structures are vital for the security, economic growth, innovation and well-being of European citizens. Ensuring their reliable, resilient, and autonomous operation is paramount, particularly in light of the European Commission's Security Union Strategy, which emphasizes the importance of safeguarding such systems [2]. However, as CIs become more digitized and interconnected, they are increasingly vulnerable to sophisticated threats, including cyberattacks and physical disruptions [3]. The failure of one CI can cascade through interconnected networks, potentially endangering both the infrastructure and the first responders involved in managing such incidents [4].

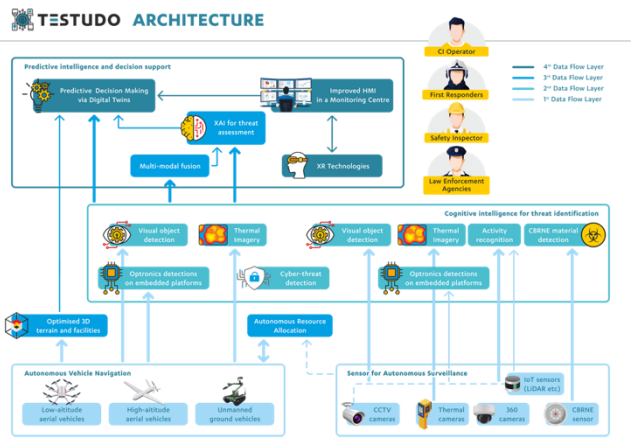

Figure 1. Preliminary, high-level depiction of the TESTUDO architecture.

To address these challenges, CI operators require innovative solutions that can operate autonomously, adapt to varying operational needs, and support effective decision-making in the face of hazardous events [5]. Despite the availability of mature technologies that assist in CI operations and risk mitigation, there is currently no integrated, holistic solution that leverages heterogeneous autonomous assets for comprehensive CI protection. This gap presents a significant opportunity for technological advancement. The TESTUDO project is designed to fill this gap by delivering an innovative prototype solution for CI protection that emphasizes autonomy, long-term deployment, and resilience. The project aims to design, implement, validate, and deliver a system capable of meeting diverse operational challenges, utilizing a three-pillar approach:

(i) Novel sensing components for enhanced and diverse detection capacities, including the use of dynamic sensors on unmanned assets and fixed sensors in remote and challenging environments.

(ii) AI-driven knowledge extraction and machine learning (ML) frameworks to enhance decision-making capabilities.
(iii) Advanced prevention and prediction models to minimize the impact of hazardous events and support recovery efforts.

These technologies will collectively create a robust and flexible CI monitoring and protection system, capable of autonomous operation in complex and unpredictable environments as depicted in Figure 1.

The primary objective of TESTUDO is to deliver a prototype at Technology Readiness Level 7 (TRL-7), which will be capable of autonomously managing CI protection in challenging environments. TESTUDO's two strategic objectives are Autonomy on the Platform (AoP) and Autonomy on the Edge (AoE). AoP will focus on integrating autonomous functionality into a system of heterogeneous assets, such as unmanned vehicles (UxVs) and a network of fixed sensors. This platform targets to enhance preparedness, prevention, and response capabilities by enabling detection, identification, and coordinated response to potential threats. AoE, on the other hand, will deliver AI-based offline cognitive capabilities that can operate in remote areas with limited or no connectivity, ensuring that the system remains functional even in the absence of communication links.

By leveraging state-of-the-art AI technologies, TESTUDO will enable high-level autonomy, reducing the need for human intervention in CI protection operations. The system will also incorporate a variety of advanced sensing and detection technologies, ensuring a robust and reliable monitoring framework capable of identifying threats early and supporting effective prevention and mitigation strategies. Through a combination of real-time decision-making tools, secure communication systems, and AI-powered threat assessment models, TESTUDO will deliver a comprehensive framework for enhanced situation awareness and optimal response to hazardous incidents.

Moreover, each TESTUDO prototype will be tested and validated through in short and long-term deployments in one operational trial and two large-scale and cross-sectorial trials. These trials will demonstrate the system's ability to handle a wide range of threats to CI, such as natural disasters, terrorist attacks, and incidents involving hazardous materials. Each version of the prototype will undergo rigorous testing in both short-term and long-term scenarios to evaluate its ability to protect, prevent, and predict critical events and validate the robustness, flexibility, and resilience of the TESTUDO solution. The trials will provide critical information to CI operators and first responders, ensuring that the system can function autonomously over extended periods and adapt to varying operational conditions.

In conclusion, TESTUDO will demonstrate a highly flexible and modular platform that can be tailored 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 critical infrastructures across Europe.

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 Un-ion 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.