TESTUDO

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES
IN INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

www.testudo-project.eu

NEWSLETTER 2

SEPTEMBER 2025

Contents:

Dear Reader,

Welcome to the second issue of the TESTUDO Newsletter. Our consortium is continuing with the efforts of developing new tools and capabilities focused on enhancing the surveillance and protection of the European Critical Infrastructure to ensure their reliable and robust operation.

We would like to present you our work and accomplishments in the second year of the project implementation.

If you are interested in updates on the project, you can follow us on our social media channels, check the News section on our webpage and subscribe to the next issues of the Newsletter.

TESTUDO project team

TESTUDO use cases

TESTUDO aims to equip CI operators and other relevant agencies with a **novel data-driven and process-oriented surveillance and intelligence platform** for increased autonomy and improved situation awareness that will enable optimal response and prediction/prevention of various threats.

To evaluate the functionality of the **TESTUDO** solutions, a set of use case scenarios tailored to the real operational needs were co-created with relevant stakeholders, to ensure that the tools developed fit seamlessly with current and proposed future operational processes.

This year the project has entered its pivotal phase, when each **TESTUDO** prototype will be validated under the scope of tests and trials under real operational scenarios defined by the end-users, which focus on deploying either partially or the entire prototype, escalating the developments based on the complexity of the real scenarios.

The example scenarios include:

Use Case #1: Disruptive online events in water reservoirs

Scenario: During night time, the management system of a water treatment facility is attempted to be hacked. A potential hacker is connected to the management system targeting to affect the smooth operation of the facility by interfering with the CBRN installation. The intension is to cause panic among the personnel and if possible, to release major amounts of chemicals which otherwise are beneficial for water quality in small quantities.

Solution: Cyber-threat detection service for identification and prevention of the hacker attempt

Result: Visualisation of the incident evolution based on the operator's decisions

Use Case #2: Chemical fire in tunnel provoked by an electric vehicle

Scenario: Due to heavy rains in the last days, part of the roof of a tunnel in the highway collapses. An electric vehicle which enters the tunnel, tries to avoid the rocks in the road, losses the control and crashes into the wall. As some of the components of the battery were damaged, the car fire starts. Although the exhaust systems react, they are not able to completely remove harmful smoke from the tunnel. People start to get out of the cars and head for the emergency exits. Moreover, a truck with hazardous substances is blocked near the fire.

Solution: Mobile sensors for threat detection

Result: Situation awareness supported by Digital Twins, Extended Reality and Human-Machine Interface technologies

Use Case #3: Synchronized attack on water treatment facilities

Scenario: During his/her daily activities, a remote operator of a water tank receives abnormal CBRN indications causing the distraction of the existing personnel. In parallel, a group of individuals, possible terrorists, clamber the fence of the facility and move towards the water tank in order to contaminate the water inside the tank with a CBRN substance. In order to ease their entrance, the illegal trespassing is performed from a location with no surveillance capabilities due to obstacles that prevent a proper connection.

Solution: UAVs and UGVs for area patrolling

Result: Threat detection, assessment and visualisation

At the end of each full-scale and cross-sectorial demonstrator, the findings guide the next development circles to conclude to the final trial where the prototype will be deployed for a long period and cover multiple scenarios to prove the effectiveness and robustness of the proposed solution.

Summary and accomplishments of the second project year

In the second year the consortium focused on efforts for the design, implementation and evaluation of the first prototype of the **TESTUDO** platform.

On 26th and 27th of November **TESTUDO** 2nd physical plenary meeting was held in Athens (Greece), hosted by EYDAP and Centre for Research & Technology Hellas (CERTH).

The meeting was focused on discussing the preparation for the upcoming UC1 and further planning for execution of UC3. All partners have been familiarised with the areas of operations and potential constraints for the trials implementation.

As part of the meeting, the consortium had an occasion to visit and learn about the EYDAP's assets in the Attica region to understand operational processes and protocols of an example infrastructure to better prepare for the implementation of the trials validating **TESTUDO** technological solutions via selected use-cases.

TESTUDO 2nd physical plenary meeting in Athens

The second year of **TESTUDO** implementation brought the definition of the initial platform architecture and establishment of strong foundational frameworks to support future development phases. Also, the legal, ethics and privacy requirements relevant to **TESTUDO** were identified.

The developed initial functional modules were validated in alignment with the project's architecture and objectives – the Autonomous Fleet Coordinator module and a robust communication layer for cross-asset integration. Some significant advancements were made in AI-driven detection tools as well as on intelligence capabilities through predictive modelling and data fusion. Additionally, novel HMI technologies for improved situational awareness were developed. In parallel, comprehensive evaluation methodologies and KPI frameworks were established whilst undertaking preparatory activities for upcoming pilot demonstrations and drafting of user training plans to ensure effective testing and validation of the **TESTUDO** platform.

The key achievement in year 2 were the integration activities of modules and delivery of the first prototype, which has been evaluated through an operational test.

Overall, four project milestones were accomplished, marked with the submission of 9 deliverables and the first project Periodic Report.

The first **TESTUDO** Review Meeting was held on May 13-14, 2025 at the Research Executive Agency's premises in Brussels, Belgium. All the progress and achievements of the reporting period (until month 18) have been presented to the Project Officer and appointed Reviewers.

Three of the project deliverables with PUBLIC dissemination level have been accepted, so they could be released via the project webpage and can be accessed on the Deliverables & publications subpage.

Dissemination and clustering activities

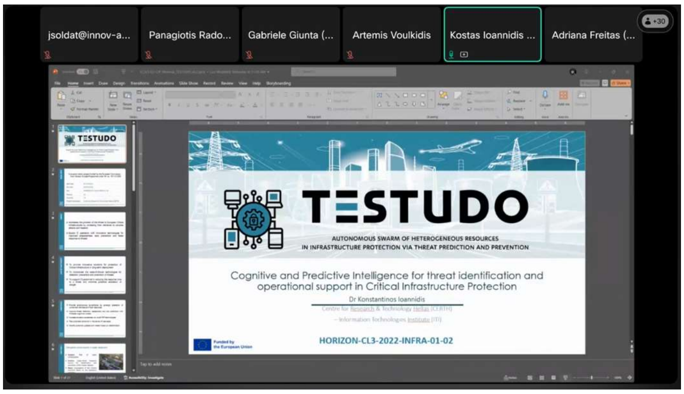
While **TESTUDO** progressed with all its technical goals, the consortium has also made efforts to promote the project results and foster an enhanced stakeholder awareness and collaboration, supporting knowledge transfer and maximising TESTUDO's societal and technological impact.

On September 20th 2024, Dr Konstantinos Ioannidis from CERTH presented the **TESTUDO** project on behalf of the coordinator, Dr. Stefanos Vrochidis (Researcher Grade B') during the EU CIP & ECSCI Webinar: The Double-Edged Sword of AI in Critical Infrastructure Protection.

The purpose of the webinar was to explore how Artificial Intelligence can enhance the resilience of critical infrastructures, while addressing potential risks introduced by AI systems. Experts and stakeholders from various industries actively participated, engaging in an interactive discussion and sharing their insights and experiences.

During the presentation, Dr. Ioannidis highlighted the challenges posed by cognitive and predictive intelligence for threat/risk identification and operational support in critical infrastructure protection. Focusing primarily on robotic platforms, he introduced the innovative solutions offered by **TESTUDO** to tackle these challenges.

These solutions include visual and multispectral detection, object recognition on embedded systems, activity recognition, cyber threat identification, explainable AI (XAI) for threat assessment, and prediction models using Digital Twins. The positive reception and active participation from stakeholders emphasized the importance and relevance of **TESTUDO** to the future of critical infrastructure protection. The recording of the online seminar is available here.



TESTUDO

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES IN INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

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

Dr Konstantinos Ioannidis

Centre for Research & Technology Hellas (CERTH)

– Information Technologies Institute (ITI)

Funded by the European Union

HORIZON-CL3-2022-INFRA-01-02

TESTUDO presentation at the EU CIP & ECSCI Webinar

Concluding the project's dissemination activities for 2024, on 16-17 October, CERTH showcased **TESTUDO** at the Research and Innovation Symposium for European Security 2024 (RISE-SD 2024) in Chalkidiki, Greece, where **TESTUDO** was also a co-organising project of the event.

Dr. Stella Parisi presented the project, highlighting its approach, architecture, strategic objectives and development cycles for its three Use Cases. The project also disseminated its objectives via a dedicated booth featuring a roll-up banner, promotional video and brochures, allowing Dr. Parisi to engage with attendees. RISE-SD 2024 focused on EU R&D projects in areas such as Critical Infrastructure Protection, Cybersecurity and Crisis Management, with panels and workshops supported by EC officials, experts and project representatives. The event was co-organised by 40 projects and attended by around 100 participants from various sectors.

TESTUDO at RISE-SD 2024

The spring of 2025 stood out as an exceptionally dynamic period for the project's dissemination activities, with multiple partners contributing to three high-impact promotional events that showcased the project's progress and engaged diverse audiences.

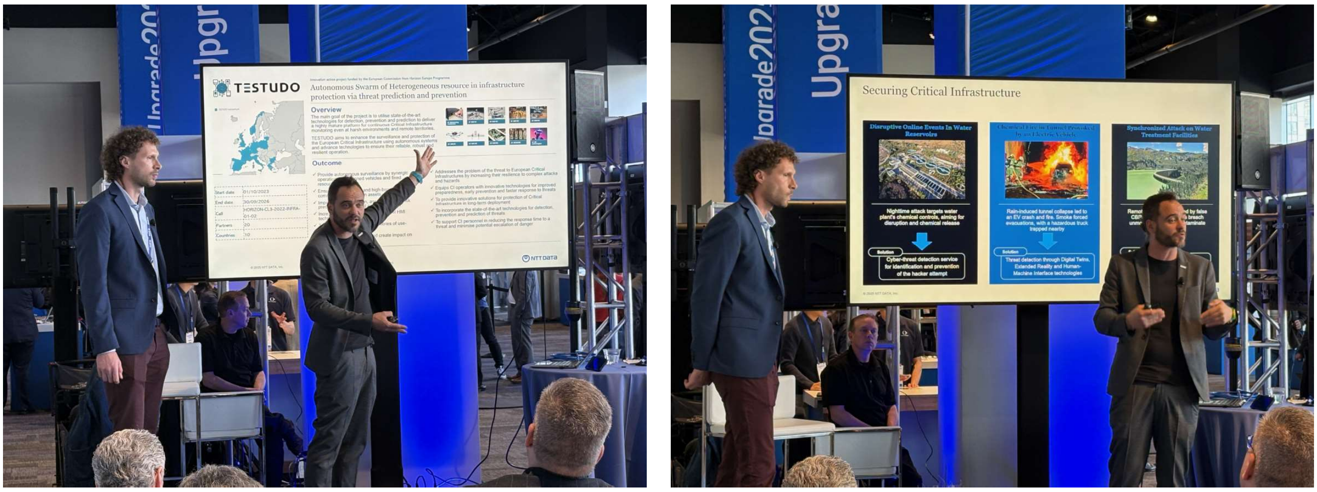
On 4-6 April 2025 Satways Ltd. (STWS) presented **TESTUDO** project on its stand at the 2025 edition of the international digital technology and innovation exhibition – BEYOND EXPO that took place in Athens, Greece.

TESTUDO at BEYOND EXPO

BEYOND event is organised in Thessaloniki since 2021 and it serves as a hub for networking, knowledge sharing, and hands-on experience with pioneering innovations.

Only a few days later, on 9-10 April 2025, partners from NTT DATA had the opportunity to present the **TESTUDO** project at the Upgrade 2025 event taking place in San Francisco, USA.

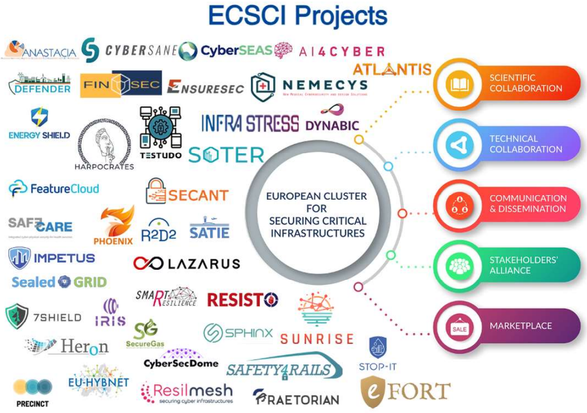
Upgrade Reality is an event hosted annually by the NTT DATA Group in the Bay Area where the latest research and innovation from NTT groups around the world are shared.


TESTUDO
Autonomous Swarm of Heterogeneous resource in infrastructure protection via threat prediction and prevention
Securing Critical Infrastructure

TESTUDO at Upgrade 2025

Next, on 29-30 April 2025, **TESTUDO** project was presented by partners from VICOMTECH at the 3rd ECSCI (European Cluster for Securing Critical Infrastructures) Workshop in Tecnalia premises in Bilbao, Spain.

The workshop was devoted to the different approaches to integrated cyber and physical security in different industrial sectors, such as energy, transport, drinking and wastewater, health, digital infrastructure, banking and financial market, space and public administration.



During the workshop sessions, various novel technologies were presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures as well as AI for resilience of critical infrastructures.

TESTUDO at 3rd ECSCI workshop

Also in April, **TESTUDO** partners from Tekniker have published a research paper in the MDPI journal *Electronics*.

The paper entitled: *Neural Network Implementation for Fire Detection in Critical Infrastructures: A Comparative Analysis on Embedded Edge Devices* is available in the Deliverables and publications section as well as directly on the journal's pages.

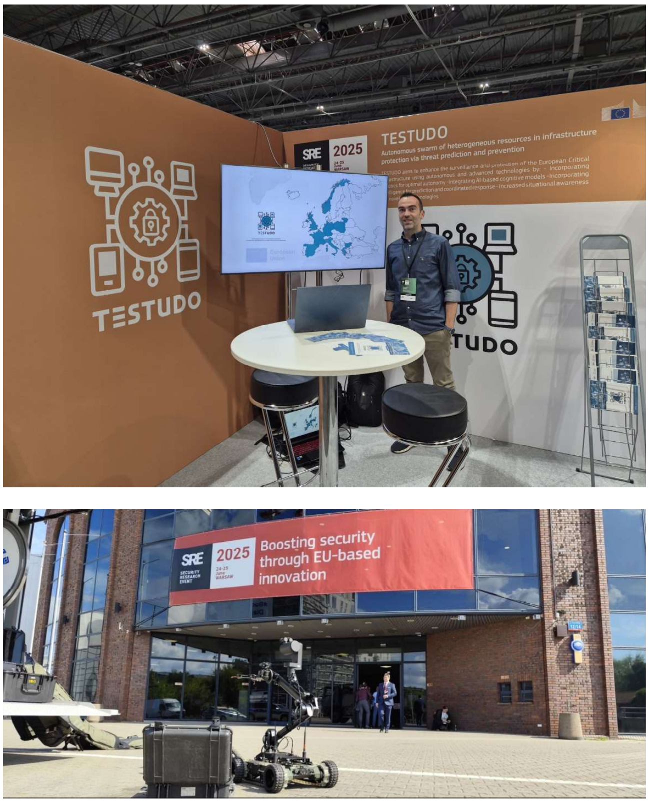
As part of the activities aimed at ensuring open access to publications and data resulting from the project, a ZENODO community has been created, where all the project dissemination materials will be made available (public deliverables, conference papers, posters, journal articles, magazine articles, brochures, etc.).

Zenodo is a general-purpose open-access repository developed under the European OpenAIRE program and operated by CERN. It allows researchers to deposit research papers, data sets, research software, reports, and any other research related digital artifacts. The OpenAIRE project, in the vanguard of the open access and open data movements in Europe was commissioned by the EC to support their nascent Open Data policy by providing a catch-all repository for EC funded research.

June has brought the project's participation in a major event – on 24-25 June 2025 **TESTUDO** has been showcased at this year's edition of the Security Research Event, held at EXPO XXI in Warsaw, Poland. The project was represented by the coordinator's team from the Centre for Research & Technology Hellas (CERTH).

SRE'25 was an occasion to meet and present the project to over 600 participants from across Europe and beyond — including policy makers, industry leaders, law enforcement, researchers, and civil society — to exchange insights and demonstrate our progress.

The event, themed "Boosting security through EU-based innovation", featured an exhibition of more than 50 EU-funded projects. It was a great opportunity for project representatives to connect with stakeholders, explore collaboration and contribute to shaping the future of civil security in Europe.


TESTUDO
SRE 2025
TESTUDO
Autonomous swarm of heterogeneous resources in infrastructure protection via threat prediction and prevention
Boosting security through EU-based innovation

TESTUDO at SRE'25

TESTUDO
Enhancing the autonomous surveillance and protection of European Critical Infrastructures

TESTUDO at the ADRF'25

The project's dissemination activities for year 2 were concluded with participation in two events in September 2025.

First, on September 23rd and 24th, **TESTUDO** was represented by the German Research Center for Artificial Intelligence (DFKI) at the 2025 AI, Data, Robotics Forum (ADRF'25) in Stavanger, Norway.

The event brought together around 500 researchers and practicioners from all over Europe to participate in various workshops on related topics.

Mr. Thomas Vögele presented the project at the workshop „AI-Powered Search & Rescue Robotics: Boosting European Resilience and Innovation". The objective of the workshop was to explore gaps and strategies to advance AI- and Data-driven robotics for Search & Rescue, strengthen European resilience and unlock cross-sector innovation.

Finally, on September 26th 2025 Dr. Stella Parisi from CERTH presented **TESTUDO** online at the "SAFEGUARD Workshop: Protection of Public Spaces" hosted by the Centre for Security Studies (KEMEA) in Athens, Greece. TESTUDO featured alongside PARTES project in a dedicated session focused on safeguarding public spaces through advanced threat detection and integrated security solutions.

The workshop formed part of the SAFEGUARD project activities and included pilot briefings with law enforcement partners, an expert discussion on integrated protection, platform demonstrations, and a training session, providing an excellent forum to showcase **TESTUDO**'s contributions and to engage with practitioners and researchers in the field.

HORIZON-CL3-2022-INFRA-01-02

TESTUDO

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES
IN INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

Enhancing the autonomous surveillance and protection of
Critical Infrastructures

Dr Stella Parisi | CERTH - ITI

SAFEGUARD WORKSHOP: PROTECTION OF PUBLIC SPACES

Athens, Greece , September 26th, 2025

Funded by the European Union

TESTUDO project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121258

TESTUDO at the SAFEGUARD Workshop

TESTUDO 1st Policy Brief

In the midst of the dissemination activities, on 23rd May 2025, the **1st TESTUDO Policy brief "Advancing Critical Infrastructure Resilience through Technological Innovation"** has been publicly released.

Summary: The **TESTUDO** project pioneers the integration of AI, predictive analytics, and autonomous systems to enhance the resilience of critical infrastructure. **TESTUDO** strengthens infrastructure protection through real-time threat detection and response mechanisms by addressing emerging threats such as cyber-attacks and climate-induced disasters.

The project aligns with key EU policies, including the Artificial Intelligence Act and GDPR, ensuring responsible and legally compliant technological advancements. With a focus on interoperability, ethical AI deployment, and cross-sector collaboration, **TESTUDO** is a strategic model for safeguarding Europe's critical infrastructure against evolving security challenges.

Critical infrastructure (CI) is essential to public safety, economic stability, and social well-being. However, increasing threats such as cyber-attacks, climate change-induced disasters, and other disruptions necessitate innovative solutions to enhance resilience.

The **TESTUDO** project, funded by the European Commission under Horizon Europe, integrates artificial intelligence (AI), predictive analytics, and autonomous systems to protect CI through real-time threat detection and response.

Key highlights:

- **Technological Innovation: TESTUDO** employs AI-driven surveillance, digital twins, and cybersecurity tools to improve situational awareness and predictive threat analysis.
- **Autonomous Swarm Systems:** Aerial, ground, and cyber assets work collaboratively to prevent threats and ensure rapid response.
- **Regulatory Alignment:** Ensures compliance with the EU Artificial Intelligence Act, General Data Protection Regulation (GDPR), Cybersecurity Act, and other key directives.
- **Interoperability & Scalability:** Designed for seamless integration across multiple sectors, including energy, transportation, and water supply.

Strategic Policy Recommendations

1. Accelerate AI Adoption: Promote investment in AI-based security solutions to modernize CI protection.

2. Strengthen Regulatory Frameworks: Standardize security protocols across the EU to ensure consistent protection measures.

3. Enhance Cross-Sector Collaboration: Facilitate information-sharing and partnerships between public and private sectors to improve security coordination.

Concerning ethical and legal considerations, **TESTUDO** prioritizes ethical AI deployment, privacy, and cybersecurity compliance. It incorporates explainable AI models and human oversight to foster trust and accountability while adhering to EU data protection laws.

TESTUDO is a pioneering initiative that enhances CI resilience through cutting-edge technology while maintaining ethical and legal standards. To maximize its impact, EU policymakers, industry leaders, and stakeholders must support AI-driven security solutions, establish robust regulatory frameworks, and promote cross-sector collaboration.

You can read the full version of the 1st Policy Brief here.

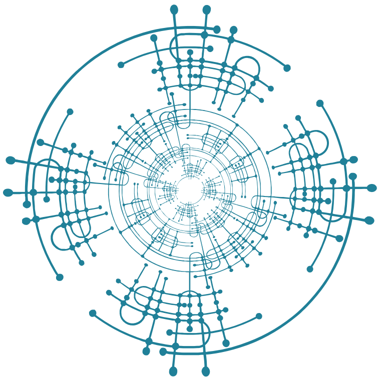
TESTUDO Stakeholders Community

One of the goals for the **TESTUDO** consortium is to **establish a broad dialogue with all the stakeholders of the project** on the solutions developed and collect feedback on expectations as well as on the outcomes via building a large community around the **TESTUDO** project encompassing various end-users and stakeholders interested in **the progress of the project, its conclusions and results.**

For that reason the **Stakeholders Forum** has been established, coordinated by the project partner T4i engineering under a dedicated project task.

The committed members of the Forum may support and influence the project via **participation in workshops, trials and demonstrations**, providing feedback and contribution to dissemination of the project and its results.

If you would like to **join the TESTUDO Stakeholders Community** and **become a member of the Stakeholders Forum** please contact: **testudo@t4ieng.com**



TESTUDO

Start date	01/10/2023
End date	30/09/2026
Call	HORIZON-CL3-2022-INFRA-01-02
GA no.	101121258
Partners	20
Countries	11
Project Coordinator	Centre for Research & Technology Hellas (CERTH)

Partners

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS · ACCELIGENCE · satways · NTT DATA · CENTRIC Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research · EYDAP · cea

ENGINEERING THE DIGITAL TRANSFORMATION COMPANY · Łukasiewicz PIAP · T4i engineering Extraordinary design · Robust engineering · Technology made simple · PROSEGUR SECURITY · vicomtech MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE · SINTEF

dfki ai · Bizkaia interbiak · Tekniker MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE · DRAXIS · adscensus · LAW AND INTERNET FOUNDATION · DBC diadikasia

Contact

/TESTUDOproject

contact@testudo-project.eu
www.testudo-project.eu

/testudo-project

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.