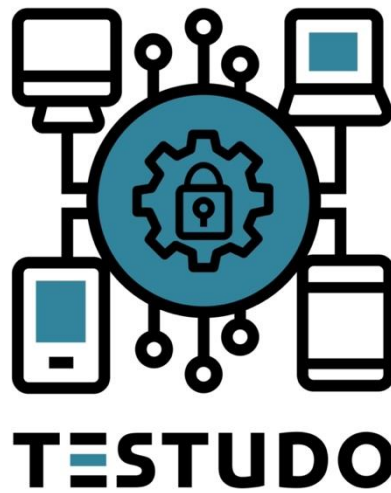




TESTUDO

HORIZON-CL3-2022-INFRA-01- Grant Agreement No. 101121258

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

TESTUDO: Final Policy Recommendations



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

These policy recommendations translate the market, operational, and regulatory insights from TESTUDO into actionable strategies to promote the wider use of advanced technologies for Critical Infrastructure protection. They are based on the market analysis in Chapter 3, WP12's exploitation and stakeholder engagement activities, lessons learned from the project pilots' technical and operational experiences, and the policy discussions outlined in the TESTUDO policy briefs.

The project's findings indicate a generally positive environment for adopting AI-powered, autonomous, and cyber-physical security solutions. Growing demand for advanced Critical Infrastructure Protection tools is driven by stricter regulatory requirements under the CER and NIS2 Directives, which bolster the case for investing in resilience. Additionally, related markets such as autonomous systems, AI-driven surveillance, and Digital Twins - covered by TESTUDO - are experiencing rapid growth. However, moving from successful demonstrations to everyday operational use is still hindered by regulatory hurdles, inconsistent validation practices, interoperability issues, procurement challenges, and organisational capacity constraints in incorporating increasingly autonomous technologies into sensitive settings.

These issues are especially important for TESTUDO because its main benefit is not based on one technology, but on combining diverse capabilities: autonomous aerial and ground units, fixed sensors, AI-driven detection, multimodal data fusion, predictive analytics, Digital Twins, CBRN detection, cybersecurity, and advanced operator interfaces. The policy challenge is to establish a supportive framework that allows these integrated solutions to be tested, evaluated, procured, and operated with clear legal regulations, interoperability, safety, cybersecurity, and public trust.

1. Policy gaps identified through market and impact analysis

1.1. Fragmented validation and assurance pathways

A key issue is the lack of a unified approach for validating integrated AI- and autonomy-based solutions for protecting critical infrastructure. While individual technologies might already meet specific standards in products, aviation, cybersecurity, or data protection, operators implementing a combined cyber-physical system must navigate multiple regulatory and assurance requirements at once.

This creates a gap between technical validation in an operational pilot and the regulatory or procurement readiness required for large-scale deployment. TESTUDO's pilot experience highlights the need to assess not only individual model accuracy but also factors such as interoperability, system stability, latency, human-machine interaction, alert management, and overall operational effectiveness. The second TESTUDO Policy Brief noted that the lack of common validation and certification pathways is a key obstacle to wider adoption. It also emphasised that successful technical integration alone does not resolve operational challenges, including alert overload, inconsistent correlation of sensor data, and the need for clearer information prioritisation for operators.

A future assurance framework should go beyond certifying individual components and focus on how the entire system behaves in real-world operating conditions.



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

1.2. Regulatory complexity across interconnected technology domains

TESTUDO technologies operate within a complex regulatory environment that includes the CER Directive, NIS2 Directive, AI Act, GDPR, Cyber Resilience Act, civil UAS legislation, U-space rules, product safety standards, and, where relevant, the Machinery Regulation and sector-specific laws. These regulations aim at different legitimate objectives. For CI operators or technology providers, navigating the interactions among these rules can create uncertainty about which requirements apply to specific deployments, responsibilities, and the evidence needed to prove compliance throughout the system's lifecycle.

This is especially important when AI-supported functions are integrated into broader robotic, surveillance, or command-and-control systems. In these situations, regulatory duties should be converted into practical guidance that addresses risk management, human oversight, cybersecurity, data governance, technical documentation, and change management. The emphasis is less on new laws and more on providing clearer implementation guidance within existing regulatory frameworks.

1.3. Interoperability and legacy-system integration

Market analysis shows that CI operators typically have large installed bases of CCTV, SCADA, PSIM, VMS, access-control, communications, and other monitoring systems. Replacing these is generally neither cost-effective nor operationally feasible. Therefore, the ability of advanced security technologies to scale effectively will largely rely on their capacity to integrate with existing infrastructure.

TESTUDO intentionally implemented a modular architecture and has advanced interoperable information sharing by adapting data formats and standard messaging methods. The technical efforts also explored IDMEFv2 and STIX-based systems for exchanging information related to detection, hardware, and situational awareness.

The remaining policy gap involves the lack of widely adopted common interoperability profiles designed for multi-domain CI protection. Without standardised semantics, interfaces, data models, and minimum interoperability standards, otherwise compatible solutions may rely on expensive, project-specific integration.

1.4. The pilot-to-deployment and procurement gap

TESTUDO results are expected to achieve TRL 6-7 mainly by the end of the project. The market analysis suggests a timeline of two to four years for these results to become commercially viable, with a steady shift from pilots and tests to full operational use. This reflects a common innovation gap. While demonstration projects can prove technical feasibility, traditional procurement usually demands proof of reliability, certification, maintenance plans, service continuity, cybersecurity measures, liability coverage, and lifecycle cost information - areas where emerging solutions might not yet meet requirements.

The original impact analysis expected that certification, permits, bureaucratic procedures, and new standards could delay the effective use of TESTUDO results. It also acknowledged that variations in public-private cooperation and institutional factors might impede adoption. Therefore, policy tools are necessary to bridge the gap between Horizon Europe validation and standard procurement.



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

1.5. Operational deployment of autonomous aerial systems

Autonomous and remotely operated aerial systems are well-suited for inspecting and safeguarding large, hazardous, remote, or distributed infrastructure. Nevertheless, the operations envisioned by TESTUDO may include BVLOS flights, activities near sensitive sites, and deployment in environments that demand thorough risk assessment and operational approval.

The current European UAS framework offers a foundational regulatory structure. However, expanding it would necessitate more consistent assessment of recurring CI security missions, cross-site operations, and integrated autonomous surveillance. This need grows as the EU develops its drone and counter-drone policies.

A balanced approach is required to maintain aviation and public safety while allowing legitimate CI operators to deploy trusted autonomous assets without redundant authorisation and assessment processes.

1.6. Trustworthy AI and lifecycle assurance

The AI Act offers a clearer regulatory framework for AI deployment. However, protecting CI remains challenging due to factors like environmental variations, sensor setups, datasets, adversarial tactics, and interactions among multiple models.

TESTUDO's technical work has identified challenges such as dataset quality and availability, model robustness across environments, explainability, cybersecurity, and ongoing post-integration validation. The project integrates legal, ethical, and AI trustworthiness efforts alongside technical development, rather than viewing compliance as a final step. In CI applications, policy measures should promote ongoing assurance, not just initial compliance at deployment.

1.7. Human factors, skills and organisational readiness

The advent of predictive AI, Digital Twins, multi-sensor fusion, and autonomous resources alters the operator's role. Instead of monitoring individual systems, operators must now interpret prioritised information, understand AI-driven suggestions, oversee autonomous operations, and intervene when needed.

TESTUDO pilots have observed that interface design and information prioritisation can significantly affect operational effectiveness. Too many alerts or alerts that are poorly aligned can diminish situational awareness instead of enhancing it. As a result, adopting new technology requires not only hardware and software integration but also investments in training, organisational procedures, and human-machine interaction. Additionally, operator competence should be viewed as an integral element of system readiness, not an afterthought after deployment.

1.8. Secure data sharing and public trust

Integrated CI protection relies on sharing operational, sensor, security, and possibly personal data across various systems and organisations. This data could also be commercially or security-sensitive. At the same



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

time, AI-driven surveillance in public spaces demands careful consideration of privacy, necessity, proportionality, and fundamental rights.

A policy framework aiming for broader adoption must balance two goals: facilitating legal sharing of information needed for cross-organisational resilience and ensuring strict controls on sensitive data to protect citizens' rights. The initial TESTUDO Policy Brief also highlighted that responsible AI, privacy safeguards, and meaningful human oversight are essential for sustainable technology adoption, not external limitations.

2. Recommendations to support adoption and scale-up

The policy should focus on closing the gap between successful R&I demonstrations and reliable operational capability. TESTUDO highlights the following priorities in this context.

An EU-wide validation framework should be created for advanced CI protection technologies. This framework would set a shared evidence base for evaluating AI-supported and autonomous systems, covering both standalone components and integrated platforms. The evaluation criteria should include technical performance, false-positive and false-negative rates, latency, robustness, cybersecurity, safe degradation, interoperability, operator usability, human oversight, and resilience in real-world multi-threat scenarios. Whenever possible, evidence obtained from recognised test conditions should be reusable throughout procurement and authorisation procedures.

Europe should establish a network of realistic CI security test and validation environments. These environments should allow technology providers, CI operators, authorities, and first responders to evaluate emerging technologies in controlled yet realistic operational settings. The focus should be on multi-domain incidents where physical, cyber, environmental, and operational risks converge. When suitable, these facilities could also facilitate regulatory testing and readiness assessments.

Implementation guidance should connect the CER Directive, NIS2 and AI governance more explicitly at the operational level. Critical entities should help translate resilience obligations into technology requirements without mandating the purchase of specific technologies. Guidance could detail how tools like predictive monitoring, autonomous inspection, multi-sensor analytics, and Digital Twins can support risk assessment, contingency planning, business continuity, and incident response. It should also clarify cybersecurity, data protection, and human oversight needs.

Interoperability should become a core procurement and policy requirement. Public authorities and CI operators should promote open, well-documented interfaces, reusable data models, standardised event exchanges, and modular systems that can operate alongside legacy infrastructure. Developing common European interoperability profiles for cyber-physical CI protection would lower integration costs, encourage competition, and reduce the risk of technological lock-in.

Innovation procurement and follow-on financing should be strengthened. Horizon Europe and similar programmes effectively promote the development and validation of innovative technologies. However, additional mechanisms are necessary to support the transition of these solutions into operational products. Approaches like public procurement, pre-commercial procurement when suitable, deployment-



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

focused funding, demonstration projects, and public-private co-investment can address the TRL 7-to-market gap. Funding criteria should also account for modular deployment, enabling operators to adopt specific capabilities without an immediate full-platform commitment.

Trustworthy AI requirements should be translated into practical CI assurance procedures. These should encompass monitoring for model drift, documenting human intervention points, conducting stress tests, evaluating cybersecurity measures, maintaining audit trails, and establishing revalidation procedures following major software, hardware, or model updates. These safeguards would help ensure compliance with the AI Act and give CI operators the operational confidence necessary for environments where safety and security are critical.

Operator readiness should be addressed alongside technological readiness. EU and national capability-building programmes should promote specialised training in areas like AI-assisted decision support, autonomous systems, Digital Twins, cyber-physical security, and multi-sensor situational awareness. Additionally, joint exercises should include CI operators, first responders, and technology providers to ensure technical skills are integrated into contingency plans and operational procedures.

European industrial capacity should be supported through open but security-conscious procurement. The market analysis highlights the growing strategic importance of EU-developed solutions that combine technological excellence with compliance with European standards. Policy initiatives should promote competitive European supply chains, especially for SMEs and technology-driven firms, while maintaining procurement quality, interoperability, and competition.

3. Alignment with EU strategies and policy priorities

The proposed suggestions align with the European policy framework outlined in the D12.2 market analysis. While the regulatory and strategic environment is becoming more supportive of proactive, technology-driven resilience, it also demands greater assurance from technology providers.

The **Critical Entities Resilience Directive (EU Directive 2022/2557)** establishes the main policy framework for enhancing the resilience of vital services against various natural and human-made risks. TESTUDO supports this initiative by offering capabilities such as monitoring, early detection, prediction, autonomous inspection, and coordinated response. The above recommendations support implementation of the CER Directive by promoting evidence-based adoption of technologies that improve risk prevention, preparedness, and continuity.

The **NIS2 Directive (EU Directive 2022/2555)** supports this strategy by emphasising cybersecurity risk management and incident response. TESTUDO's combining of cyber-threat detection with physical and operational data illustrates the benefits of shifting from isolated physical-security and cybersecurity measures to a true cyber-physical system.

The **AI Act (EU Regulation 2024/1689)** is especially pertinent to the project's AI-enabled features. Its focus on risk management, traceability, technical documentation, human oversight, accuracy, robustness, and lifecycle assurance aligns with the Act's core principles. For CI operators, a primary policy goal should be



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

to prove AI compliance with evidence gathered in realistic operational settings, rather than relying solely on documentation.

The recommendations align with the **Cyber Resilience Act (EU Regulation 2024/2847)** by advocating for secure-by-design connected products, lifecycle cybersecurity, and vulnerability management. At the same time, the proposed surveillance and information-processing approach is grounded in GDPR and, where relevant, the Law Enforcement Directive, ensuring enhanced infrastructure protection does not compromise fundamental rights.

At the strategic level, TESTUDO closely aligns with ProtectEU - the European Internal Security Strategy - and the Preparedness Union Strategy. ProtectEU emphasises critical infrastructure protection and strengthening the Union's resilience and cybersecurity frameworks, while the Preparedness Union Strategy advocates for enhanced cross-sector and whole-of-society preparedness. The TESTUDO approach, bringing together technology, operators, authorities, and emergency stakeholders, serves as a practical example of how these priorities can be implemented through operational capabilities.

The EU Action Plan on Drone and Counter-Drone Security is particularly relevant. Its emphasis on preparedness, detection, coordinated response, performance standards, certification, resilience evaluation, and trusted drone technologies aligns closely with the capabilities covered in TESTUDO. Consequently, the project's experience can inform the ongoing European dialogue on evaluating the performance of drone-enabled security measures and on safeguarding critical infrastructure from malicious or uncooperative unmanned systems.

Taken together, these policy instruments increasingly point towards the same requirement: European CI resilience will depend not simply on acquiring more security technology, but on establishing trusted, interoperable, cyber-secure and operationally validated capabilities that can operate across organisational and sectoral boundaries.

4. Suggested actions for regulators, industry and stakeholders

Implementing the recommendations demands coordinated efforts from multiple stakeholder groups. Responsibility cannot be solely on regulators, as many barriers involve industrial maturity, procurement practices, organisational readiness, and interoperability.

Stakeholder	Suggested actions	Expected contribution
European Commission and EU relevant agencies	Establish shared validation principles and reference performance standards for AI- and autonomy-enabled CI protection systems. Support an EU network of operational testbeds, encourage cross-sector stress testing, and offer implementation guidance that links CER, NIS2, AI, and cybersecurity requirements. Continue advancing standardisation and interoperability efforts.	Greater regulatory certainty, reusable validation evidence and improved conditions for cross-border scale-up.



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

Member competent authorities and State regulators	Integrate advanced monitoring and predictive tools into national resilience efforts where suitable; enable risk-focused testing of autonomous systems; coordinate among aviation, cybersecurity, data protection, and critical infrastructure authorities; and support both national and cross-border exercises.	Reduced administrative fragmentation and improved transition from pilot validation to operational deployment.
Critical infrastructure operators	Implement phased deployment and risk-based approaches; clearly define operational needs; include operators and first responders in system design and testing; set up human-oversight processes; evaluate system interoperability and gather performance data.	Better technology–user fit, improved acceptance and stronger evidence for procurement decisions.
Technology providers and system integrators	Implement security, privacy, and compliance-by-design principles; keep interfaces modular and well-documented; demonstrate performance, robustness, and lifecycle support; ensure AI components are auditable and enable revalidation of major system changes.	More mature, trustworthy and procurement-ready European solutions.
Standardisation bodies and technical communities	Develop or refine interoperable event models, APIs, testing protocols, and common terminology for multi-domain CI protection. Connect standardisation efforts with lessons learned from operational pilots.	Lower integration costs and greater interoperability between products and sectors.
Research organisations and EU-funded projects	Share non-sensitive validation methods, benchmark strategies, and lessons learned; conduct cross-project testing and clustering; and advance research in AI robustness, multi-sensor correlation, human-machine interaction, and autonomous mission management.	Preserve and amplify Horizon Europe investments and accelerate the maturation of emerging technologies.
Funding bodies, investors and innovation-procurement authorities	Provide tools to transform validated prototypes into deployable products, help European SMEs scale up, and integrate demonstration funding with procurement planning and market-entry support.	Reduce the post-project financing gap and strengthen European industrial capacity.
Civil society, ethics and data-protection stakeholders	Engage in governance discussions on issues like proportionality, privacy, transparency, and acceptable uses of AI-enabled surveillance and	Stronger public legitimacy and



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

	autonomous systems. Help define safeguards and accountability measures.	sustainable societal acceptance.
--	---	----------------------------------

4.1. Implementation horizon

In the short term, efforts should prioritise developing standard validation methods, broadening realistic testing scenarios, defining interoperability requirements, and providing practical guidance for CI operators collaborating with the CER, NIS2, and AI frameworks. Additionally, systematically sharing insights from Horizon Europe projects is crucial to avoid duplicated efforts in addressing similar integration and validation issues.

In the medium term, emphasis should move toward recognised assurance and certification methods, multi-country operational demonstrations, and procurement mechanisms that facilitate the transition of validated technologies into regular service. Member States should gradually incorporate predictive and autonomous capabilities into resilience planning, especially when risk assessments show a clear operational advantage.

In the long run, Europe should establish a sustainable, mature ecosystem where authorities, CI operators, first responders, research bodies, and tech providers collaboratively evaluate emerging threats and capabilities. This ecosystem should involve regular cross-sector exercises, ongoing monitoring of deployed AI systems throughout their lifecycle, continuous enhancement of interoperability standards, and, when appropriate, mutual recognition of validation evidence among Member States.

5. Concluding policy perspective

TESTUDO shows that the technological basis for a more predictive, autonomous, and integrated approach to critical infrastructure protection is becoming more accessible. The main challenge moving forward is not only technological development but also creating an environment that enables innovative capabilities to move from research prototypes and successful demonstrations to trusted, scalable, and economically sustainable operational solutions. The market analysis shows clear demand for these capabilities, supported by the evolving EU regulatory and strategic framework, which offers strong policy incentives for adoption. Meanwhile, the TESTUDO experience demonstrates that scaling up involves more than regulatory compliance; it also requires shared validation methods, interoperability, user-friendly interfaces, trained operators, effective procurement processes, lifecycle management, and ongoing collaboration between the public and private sectors.

The main policy focus is to integrate innovation, regulation, and operational practices. This integration would help the EU enhance the resilience of critical entities, promote trustworthy AI, strengthen European technological capabilities, and maintain an open, competitive security market. Additionally, this approach aligns with TESTUDO's original goal: to use project evidence to inform long-term policy decisions and to foster fair cooperation among public authorities, critical infrastructure operators, and technology providers.



TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.