An innovative Greek SME specialised in edge AI cybersecurity seeks an industrial IoT, critical infrastructure or space-sector SME for a Eurostars Call 11 project on anomaly detection on AI-enabled devices in critical infrastructure and space.

Summary

Profile type	Company's country	POD reference
Research & Development Request	**Greece**	**RDRGR20260705001**
Profile status	**Type of partnership**	**Targeted countries**
PUBLISHED	**Research and development cooperation agreement**	**• All countries**
Contact Person	**Term of validity**	**Last update**
Enrico FRANZIN	**5 Jul 2026** **5 Jul 2027**	**5 Jul 2026**

General Information

Short summary

A Greek innovative SME is building a Eurostars (Call 11) consortium to develop a software-defined cybersecurity layer for AI-enabled edge devices in critical infrastructure and space applications. The solution combines lightweight anomaly detection with on-device Small Language Models (SLMs) for explainable cyber threat analysis aligned with European cybersecurity and AI regulations. An SME partner is sought for pilot deployment, validation and commercialisation.

Full description

The rapid adoption of artificial intelligence and edge computing across critical infrastructure and commercial space systems has significantly expanded the cyberattack surface. At the same time, new European regulations, including the NIS2 Directive, the Cyber Resilience Act (CRA) and the EU AI Act, require operators not only to detect cyber incidents but also to provide transparent, explainable and auditable evidence supporting their response.
To address this challenge, a Greek innovative SME specialised in edge AI cybersecurity is preparing a Eurostars proposal entitled EDGE-SENTRY, aiming to develop a software-defined cybersecurity layer for AI-enabled edge devices operating in regulated industrial and space environments.
The project will develop a lightweight three-layer architecture capable of operating entirely on edge devices. The solution combines deterministic anomaly detection with an on-device Small Language Model (SLM) that automatically explains every detected anomaly using recognised threat intelligence frameworks such as MITRE ATT&CK for ICS and ESA SPACE-SHIELD. The generated outputs will support both security operators and compliance officers by providing regulator-ready evidence aligned with the requirements of NIS2, the Cyber Resilience Act and the EU AI Act.
The solution will be deployed as hardware-agnostic software capable of running on existing industrial edge devices without dependence on proprietary hardware. Validation activities will include laboratory testing followed by field pilots in representative industrial IoT and space-related operational environments, targeting technology maturation from TRL4 to TRL6.
The consortium is coordinated by the Greek SME and currently includes a research University in Brussels contributing expertise in explainable AI and edge computing. The consortium is now seeking an additional SME from a Eurostars country to strengthen the industrial validation and commercialisation activities.
The sought partner should be eligible for Eurostars funding in its own country and willing to actively participate in proposal preparation and project implementation. The deadline for Expressions of Interest is 10 August 2026, allowing sufficient time for consortium finalisation and preparation of the national funding applications before the Eurostars Call 11 deadline of 10 September 2026. The consortium welcomes expressions of interest from experienced organisations wishing to contribute to the development of next-generation trustworthy cybersecurity solutions for critical infrastructure and space applications.

Advantages and innovations

Unlike existing cybersecurity solutions that rely on cloud-based analytics or opaque AI models, EDGE-SENTRY introduces a software-defined, edge-resident cybersecurity layer capable of providing explainable threat analysis directly on AI-enabled devices.
The project combines lightweight deterministic anomaly detection with on-device Small Language Models (SLMs) that generate transparent explanations for every detected event, referencing recognised frameworks such as MITRE ATT&CK for ICS and ESA SPACE-SHIELD. This approach enables operators to understand and validate every security alert while simultaneously producing structured evidence that supports compliance with the NIS2 Directive, the Cyber Resilience Act and the EU AI Act.
As a hardware-agnostic software solution, EDGE-SENTRY can be deployed on existing industrial edge infrastructures without proprietary hardware dependencies, facilitating scalable adoption across critical infrastructure and space applications while strengthening European digital sovereignty.

Technical specification or expertise sought

The consortium is seeking an SME established in a Eurostars country (with allocated funded for the call 11) with experience in industrial IoT, critical infrastructure or space-sector technologies.
The ideal partner should have practical expertise in the deployment and integration of edge computing solutions and industrial communication technologies or equivalent industrial connectivity platforms, as well as experience in deploying cybersecurity solutions/pilot deployment in operational environments. The ideal partner should also have an interest to align the outcome of EDGE-SENTRY project to their roadmap and plans for exploitation and commercialization activities. Access to representative pilot sites or established relationships with industrial end users in sectors such as energy, transport, manufacturing, water utilities or satellite ground-segment operations would be considered particularly valuable.
Previous participation in collaborative R&D projects, including Eurostars or Horizon Europe, would be an advantage but is not a mandatory requirement.

Stage of development

Under development

Sustainable Development goals

• Goal 9: Industry, Innovation and Infrastructure
• Goal 11: Sustainable Cities and Communities

IPR Status

No IPR applied

IPR Notes

Partner Sought

Expected role of the partner

The selected partner will join the consortium as a full project partner and will play a key role in the validation and

commercialisation of the proposed solution.
The partner is expected to contribute to the development of the laboratory validation environment, support the integration of the EDGE-SENTRY software with industrial IoT infrastructures and participate in the implementation of field pilots under realistic operational conditions. In addition, the partner will actively contribute to the exploitation and dissemination activities of the project by facilitating access to end users, supporting market validation and strengthening the commercialisation strategy through its existing industrial network and customer base.
Indicative budget share is broadly comparable to the other partners within the ~€800 K total; the exact allocation and total funding depends on the national funding caps/rates and will be finalised in the consortium agreement.

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **SME <=10**
- **SME 50 - 249**
- **SME 11-49**

Call Details

Framework program

Eureka

Call title and identifier

Eurostars Call 11 for projects

Submission and evaluation scheme

Anticipated project budget

Coordinator required

No

Deadline for EoI

10 Aug 2026

Deadline of the call

10 Sep 2026

Project duration in weeks

104

Web link to the call

https://www.eurekanetwork.org/programmes-and-calls/eurostars/eurostars-call-for-projects-september-2026/

Project title and acronym

Dissemination

Technology keywords

- **01003003 - Artificial Intelligence (AI)**
- **01003008 - Data Processing / Data Interchange, Middleware**
- **01003001 - Advanced Systems Architecture**

Market keywords

- **01006001 - Defence communications**
- **01004002 - Data communication components**
- **01004008 - Other data communications**

Targeted countries

- **All countries**

Sector groups involved