Consortium

Coordinator

University of Cyprus

KOIOS Research and Innovation Center of Excellence

iSi Industrial Systems Institute

ATHENA Research & Innovation Information Technologies

CERTH Centre for Research & Technology Hellas

universität wien

cnit consorzio nazionale interuniversitario per le telecomunicazioni

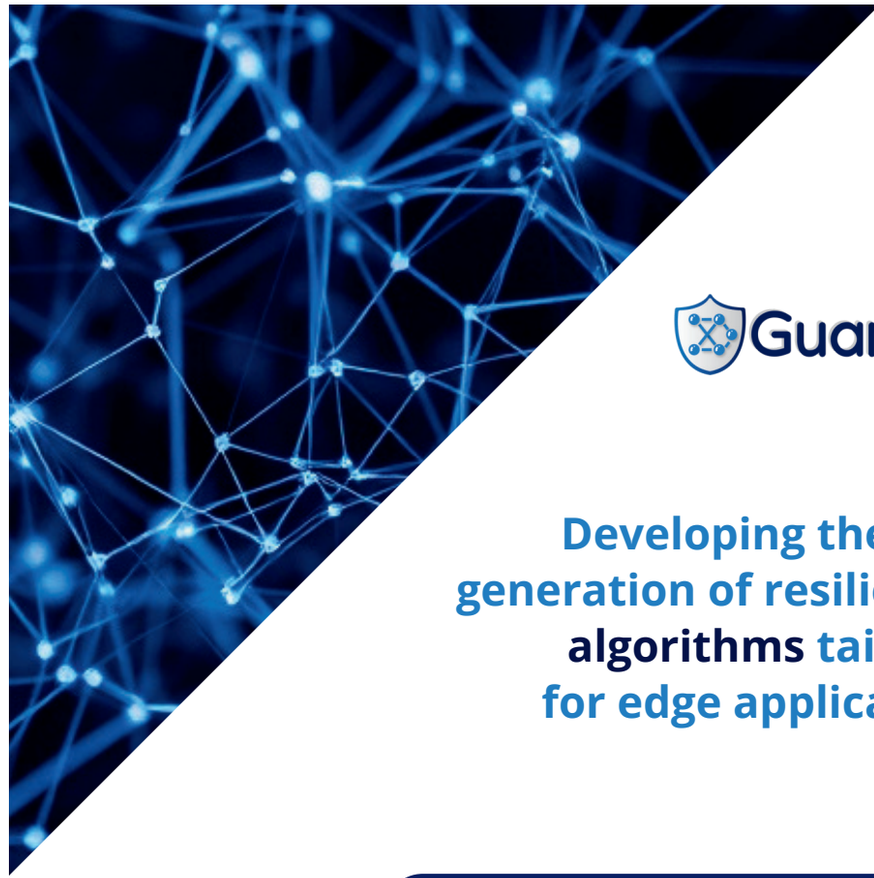
SPACE

Cyprus Organisation for Standardisation

EXUS AI LABS

EIGHTBELLS

University of York



GuardAi

Developing the next generation of resilient AI algorithms tailored for edge applications

Robust Surveillance for Public Safety

Resilient Autonomous Vehicles

Secure 5G Network Edge Infrastructure

Get in touch

GuardAi

Follow us

/guardai-eu-project

/guardai.bsky.social

@GuardAI-EU

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement 101168067.

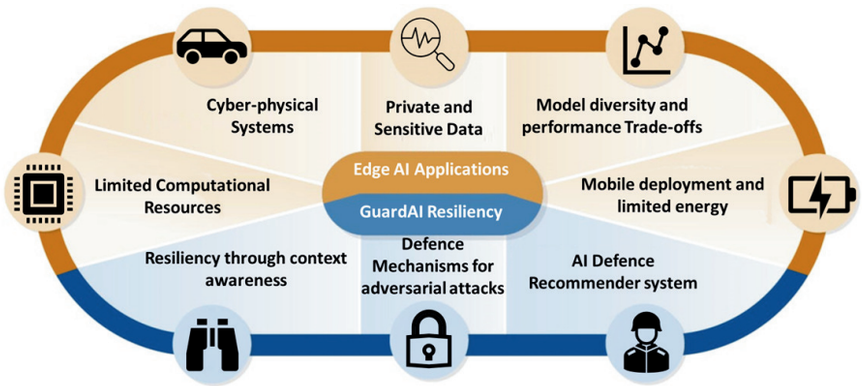
Funded by the European Union

About GuardAI

GuardAI is a 3-year European research project, bringing together leading experts from academia, industry, and public institutions across Europe to shape the future of secure and resilient AI at the edge. The project focuses on advancing trustworthy AI technologies capable of operating under real-world constraints and adversarial conditions.

Through combined expertise in machine learning, cybersecurity, autonomous systems, legal frameworks, and standardization, GuardAI delivers practical solutions that protect critical infrastructure and foster confidence in next-generation AI systems.

GuardAI Concept: Building Resilient AI at the Edge



GuardAI creates targeted solutions to address the unique challenges of AI systems, such as **drones**, **connected and autonomous vehicles**, and **5G network edge infrastructure**. Machine learning algorithms in these systems may be prone to errors caused by even minor variations, random noise, or anomalies in the data they process.

To meet these challenges, GuardAI introduces a layer of resiliency grounded in three core innovations:

- Context awareness to help AI interpret dynamic environments.
- Defence mechanisms to counter adversarial threats.
- An AI Defence Recommender System to guide the selection of appropriate safeguards.

Expected Outcomes

- Innovative solutions that protect the integrity and reliability of edge AI systems.
- Context-Aware AI capable of making intelligent, real-time decisions in complex environments.
- Robust, Attack-Resilient Algorithms designed to defend against adversarial threats.
- Foundations for Certification to support safety-critical AI applications.
- A Collaborative Knowledge Network connecting researchers, industry, and policy stakeholders.




Impact

Scientific breakthroughs in designing AI systems that remain reliable under real-world threats and uncertainty.

Technological innovations that raise the standard for resilient edge AI applications.

Greater public trust in AI through knowledge-sharing, transparency, and responsible development.

A more secure digital landscape that fosters economic growth and supports AI-driven innovation.

Influence on global standards, contributing to ISO efforts in cybersecurity and trustworthy AI.