Enhancing Robustness and Security of Edge AI Systems for Safety-Critical Applications

WP5 – Impact Maximization: Dissemination, Exploitation, and Certification Roadmap

D5.1: Project Website

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101168067. 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.

Document Information

GRANT AGREEMENT NUMBER	101168067	**ACRONYM**	GuardAI
FULL TITLE	Enhancing Robustness and Security of Edge AI Systems for Safety-Critical Applications		
START DATE	1st October 2024	**DURATION**	36 months
PROJECT URL	https://www.kios.ucy.ac.cy/guardai/		
DELIVERABLE	D5.1 – Project Website		
WORK PACKAGE	WP5 – Impact Maximization: Dissemination, Exploitation, and Certification Roadmap		
DATE OF DELIVERY	**CONTRACTUAL** 12/2024	**ACTUAL**	12/2024
TYPE	Report	**DISSEMINATION LEVEL**	PU
LEAD BENEFICIARY	UCY-KIOS CoE		
RESPONSIBLE AUTHORS	Christos Kyrkou, Antonis Savva		
CONTRIBUTIONS (FROM)	Christos Kyrkou (UCY), Antonis Savva (UCY), Kseniia Guliaeva (UNIVIE), Stelios Erotokritou (8BELLS), Erion-Vasilis Pikoulis (ATHENA), Nikos Piperigkos (ATHENA), Aris Lalos (ATHENA)		
ABSTRACT	This deliverable presents an overview of the GuardAI project website, designed to facilitate information sharing, stakeholder engagement, and dissemination of results and updates. The website includes sections on project goals, use cases, Consortium members, news, publications, and communication materials, alongside interactive features such as a contact form. This deliverable provides an overview of the website with detailed descriptions, screenshots, and an analysis of the website's functionality.		

Document History

VERSION	ISSUE DATE	STAGE	DESCRIPTION	CONTRIBUTOR
V 1.0	20/12/2024	Final	Final Submitted Deliverable	Christos Kyrkou, Antonis Savva, Kseniia Guliaeva, Stelios Erotokritou, Erion-Vasilis Pikoulis, Nikos Piperigkos, Aris Lalos

Disclaimer

Copyright message

Table of Contents

Executive summary

This deliverable provides an overview of the GuardAI website which is designed to share essential information about the project, its goals, use cases, Consortium members, and ongoing developments, while also engaging stakeholders and supporting efficient dissemination of results and updates.

The website features the following sections:

- **About** – Detailing the project's goals, objectives, concept, work packages, and anticipated outcomes,
- **Use Cases** – Where comprehensive descriptions of the three use cases are given, highlighting their scenarios, attack surfaces, and innovative approaches.
- **Consortium** – Introducing project members, including their logos and concise descriptions,
- **Publications** – The publications of project results in peer-reviewed conferences and journals
- **News –** Updates on project activities and events.
- **Communication** – Includes material such as press releases, blog articles, as well as project's brochure, posters or videos.
- **Synergies** – Specific synergies with other EU projects, stakeholders and Key European Initiatives on AI.
- **Contact** – An interactive contact form and direct communication details for project coordinators.

The website is implemented using a visually appealing design with user-friendly navigation, social media integration and data privacy protection measures according to GDPR. It enhances accessibility and engagement through its simple design, inclusion of Consortium member logos and multimedia links.

This report includes screenshots, descriptions of the website's sections and a description of its functionality.

1. Introduction

The project website serves as the main communication hub presenting the project's objectives and progress and facilitating communication with the project Consortium. This deliverable provides an overview of the website's structure, content, and functionality, with accompanying screenshots illustrating its key features.

1.1. Website Structure and Content

1.1.1. Home

The homepage (https://www.kios.ucy.ac.cy/guardai/) provides a concise introduction to the project, including:

- A brief overview of the project's mission and goals (Figure 1),
- Summaries of the three use cases being developed during the project (Figure 2),
- Visual representation of all Consortium members (Figure 3), and
- Footer which includes links to all major website sections, social media links (X, YouTube, LinkedIn) and direct link to the privacy policy (Figure 4).

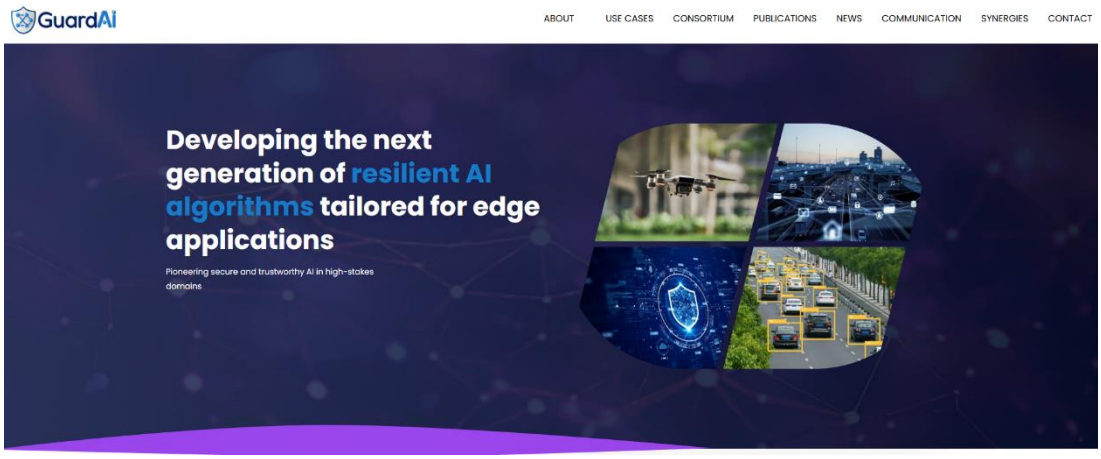


Figure 1: GuardAI's statement

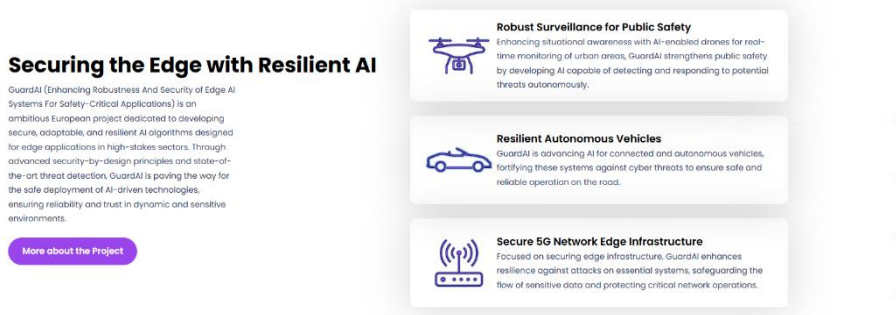


Figure 2: Brief description of Use Cases

Figure 3: Consortium member logos

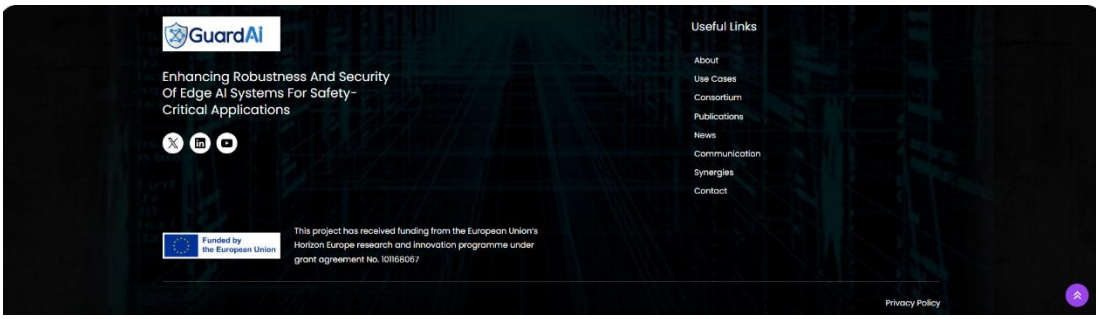


Figure 4: Website footer

1.1.2. About

This section elaborates on the foundational aspects of the project consisting of:

- The challenges that will be addressed (Figure 5),
- The overarching aim of the project and specific objectives (Figure 6),
- Explanation of the innovative ideas driving the project and the approach to be followed (Figure 7),
- Descriptions of the work packages, their scope and leader (Figure 8), and
- Highlighted achievements anticipated at the end of the project (Figure 9).

Figure 5: Challenges that GuardAI addresses

Goal

GuardAI's goal is to develop the next generation of resilient AI algorithms tailored for edge applications. In pursuit of this goal, GuardAI will engage in extensive research activities with the following aims to:

1. Develop innovative solutions to ensure the integrity, security, and resilience of these systems, ultimately fostering trust and accelerating the safe adoption of AI-driven technologies.
2. Integrate context indicators and holistic situational understanding into AI algorithms, enabling systems to adapt and make informed decisions in dynamic environments.
3. Collaborate with researchers, industry experts, government agencies, and AI practitioners to lay the groundwork for future certification schemes that promote the adoption of secure AI technology across various domains.

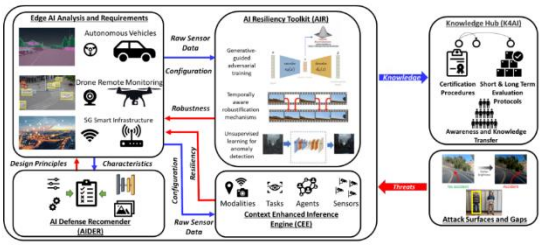
Ultimately GuardAI is committed to developing cutting-edge, secure, and robust, solutions tailored to the specific needs of edge AI safeguarding critical infrastructure and systems.

Objectives

1. Identify characteristics for AI at the edge to inform the security-by-design concept
2. Improve robustness of AI algorithms running on edge/embedded systems against adversarial attacks
3. Enhance resiliency of AI at the edge by leveraging auxiliary contextual information
4. Establish a path towards certification of security-compliant edge AI algorithms
5. Raise awareness and share knowledge with end users and decision makers on resilient AI

Figure 6: GuardAI's goal and objectives

Approach



GuardAI, comprises multiple activities aimed at **determining attack surfaces** and **identifying** potential **vulnerabilities and gaps** in AI systems. In this context, existing attack vectors and research gaps will be identified, with the existing limitations informing the **development** of **approaches**, **algorithms**, and **system optimizations**. At the application-level, **purpose-build context embedding** mechanisms will be developed that will allow an edge AI system to exploit various context indicators such as location, mapping, multi-sensory orchestrations, and multi-agent environments to **enrich** its **reasoning** capabilities. The context capabilities will change depending on the edge AI application configuration and requirements. Using the raw sensory data available in each application, **domain tailored solutions** will be developed to enable machine and deep learning for perception and analytics to operate in the presence of adversarial attacks so that the overall operation can be performed in a **trusted way** and in a **resilient manner**.

These approaches will employ unsupervised learning for anomaly detection, temporally aware robustification mechanisms, and generative-guided adversarial training. The main research work encompassing context information, situational awareness, and novel algorithms and tools for adversarial robustness will be tailored for use in edge AI applications for drones, CAVs, and edge network infrastructure. These application domains encapsulate many challenges of AI at the edge applications such as, real-time processing, sensitive data, limited resources, and mobile deployment with limited energy. Consequently, due to the complexity of designing tailored defence mechanisms for edge AI systems, an automated recommender approach will be designed to encapsulate the security-by-design concept.

The knowledge accumulated by the consortium expertise and the novel knowledge that will be created will be digitized in a knowledge hub specialized for resiliency and robustification. Through this knowledge hub, GuardAI will derive evaluation protocols and standardized metrics that offer robustness guarantees for AI systems. These metrics will serve as means to assess the effectiveness of the developed security mechanisms and provide confidence in the reliability and safety of edge AI applications. Furthermore, the knowledge hub will act as the main medium for active engagement with the actors, enabling the creation of a wide network of experts, dialogue amongst stakeholders with aligned interests and capturing and diffusing of existing and new knowledge.

Figure 7: GuardAI's approach

GuardAI ABOUT USE CASES CONSORTIUM PUBLICATIONS NEWS COMMUNICATION SYNERGIES CONTACT

Explore GuardAI's six work packages (WPs)

WP Number	WP Name	WP Description	WP Leader
WP1	Use Cases Requirements and System Architecture	Provide the basis for requirement analysis and design of the Use Cases to ensure that the solutions address the specific needs and objectives of its intended users. Derive specifications and architecture for the GuardAI solutions to enhance their ability to withstand potential threats and vulnerabilities.	ATHENA
WP2	Comprehensive Toolkit for Robust Edge AI	Identify challenges beyond the state-of-the-art. Develop algorithms and methodologies for enhancing AI systems' robustness against adversarial attacks. Create context-aware AI models that can respond appropriately to diverse and changing situations. Develop anomaly detection algorithms to identify unusual patterns or outliers.	UCY-KIOS CoE
WP3	Enhanced Protection and Security-by-Design Principles for Secure Edge AI	Perform a comprehensive evaluation of potential attack vectors and conduct a detailed analysis of existing risks/threats to AI security. Develop a defence recommender system that is not only risk-aware but also capable of suggesting proactive security measures. Implement secure practices for handling both models and data, addressing key components of security-by-design principles.	CERTH
WP4	Use Cases Implementation, Evaluation and Demonstration	Establish a robust set of evaluation methods. Integrate the developed algorithms into their intended applications and efficiently deploy them to ensure practical usability. Derive certification criteria that are driven by benchmarking. Showcase the algorithms' capabilities and evaluate their key outcomes.	CERTH
WP5	Impact Maximization: Dissemination, Exploitation, and Certification Roadmap	Design and implement European-wide strategies for disseminating, communicating, and exploiting GuardAI's outputs and tools to maximize their impact. Increase social awareness, acceptance, and scalability of GuardAI's research and innovation solutions. Take actions towards standardisation of GuardAI results.	EIGHT BELLS LTD
WP6	Project Coordination and Management	Coordinate and monitor the technological and scientific work of the GuardAI project, including communication and coordination with the partners and the European Commission (EC).	UCY-KIOS CoE

Figure 8: GuardAI's work packages

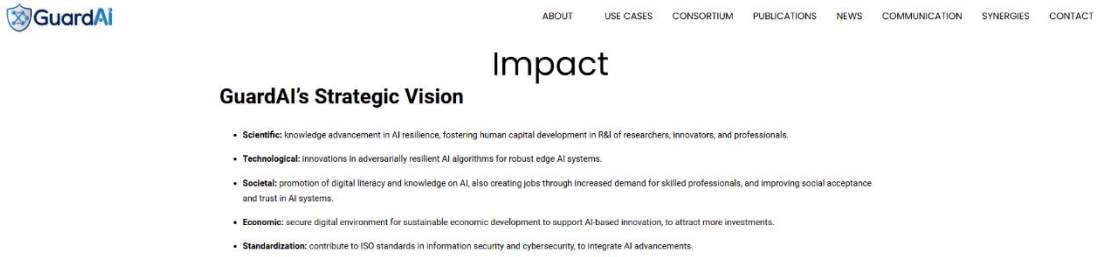


Figure 9: GuardAI's strategic vision for impact

This information is divided into three subpages, i.e.,

- Concept: https://www.kios.ucy.ac.cy/guardai/concept/
- Work Packages: https://www.kios.ucy.ac.cy/guardai/work-packages/
- Impact: https://www.kios.ucy.ac.cy/guardai/impact/

which are accessible by hovering over "About" tab (Figure 10).

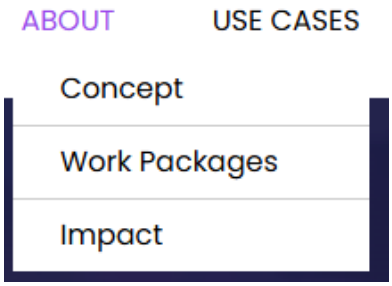


Figure 10: Subpages to better illustrate key information about the project

1.1.3. Use Cases

This page (https://www.kios.ucy.ac.cy/guardai/use-cases/) elaborates on the three use cases (Figure 11 – Figure 14) by providing additional and structured details including:

- A high-level description,
- The identification of potential vulnerabilities and scenarios addressed within the project, and
- The specific advancements and contributions each use case aims to achieve.

Figure 11: GuardAI's focus areas for the use cases

Figure 12: GuardAI's Use Case 1

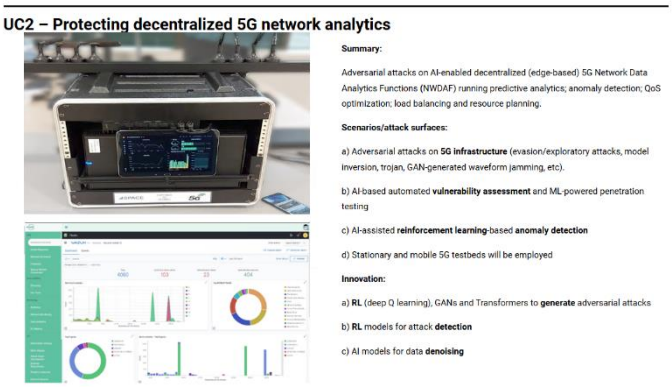


Figure 13: GuardAI's Use Case 2

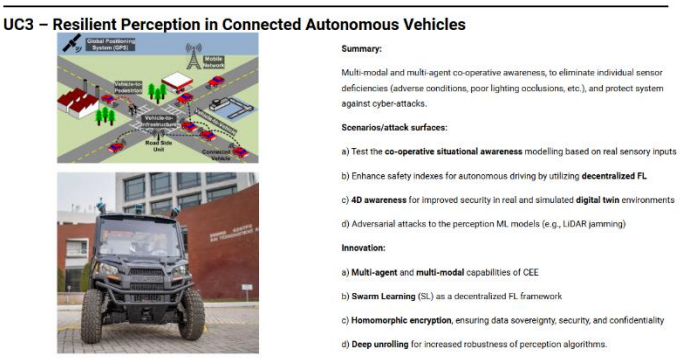


Figure 14: GuardAI's Use Case 3

1.1.4. Consortium

This page (https://www.kios.ucy.ac.cy/guardai/consortium/) introduces GuardAI's Consortium members by providing high-resolution logos for easy recognition of each Consortium member, along with brief information about the expertise and role of each partner in the project.

GuardAI

ABOUT USE CASES CONSORTIUM PUBLICATIONS NEWS COMMUNICATION SYNERGIES CONTACT

Consortium

KIOS Research and Innovation Center of Excellence
University of Cyprus

The University of Cyprus (UCY) is the oldest and largest public university in Cyprus, and participates in this proposal via the KIOS Research and Innovation Center of Excellence (KIOS CoE). The KIOS CoE operates within the University of Cyprus and was established in 2008, advancing into a European Research and Innovation Center of Excellence in 2017. It is the largest research and innovation center in Cyprus and conducts research and innovation activities emphasizing monitoring, control, management and security of critical infrastructures. The goal of the Center is to conduct outstanding interdisciplinary research and innovation and produce new knowledge and tools that can be applied to solve real-life problems.

For GuardAI, KIOS CoE will develop algorithms for enhancing the robustness of machine learning models and will also lead the use-case related to surveillance and monitoring with AI-enabled drones to showcase the solutions.

https://www.kios.ucy.ac.cy/

iSi INDUSTRIAL SYSTEMS INSTITUTE
ATHENA Research & Innovation Information Technologies

The Industrial Systems Institute (ISI) was established in Patras, Greece, in 1998. It is a leading R&D organization of excellence conducting basic & applied research and exploratory development on Information and communications technology (ICT) for the Greek and European industry. ISI has been part of the Research and Innovation Centre in Information, Communication, and Knowledge Technologies "ATHENA", since 2003. ATHENA is involved in the GuardAI project through ISI's Autonomous Interactive Systems and Machine Intelligence group. Founded in 2019, the group employs 20 research staff members, and brings its extended expertise in machine learning, signal processing, and computer vision in applications related to autonomous driving, cyber-physical systems and human-robot collaboration. Over the past five years, the group has co-led or contributed to over 10 EU and national projects, collaborated on three industrial subcontracts with Panasonic Automotive Europe, and published more than 100 papers in international journals and leading conferences.

ATHENA has the overall technical oversight of the project and will contribute to GuardAI with cutting-edge AI-empowered solutions for high-performance, efficient, robust, and resilient multimodal cooperative perception in connected and autonomous mobility (UC3).

https://www.isi.gr

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

The Centre for Research and Technology-Hellas (CERTH) is the only research centre in Northern Greece and one of the largest in the country founded in 2000. It is a legal entity governed by private law with non-profit status, supervised by the General Secretariat for Research and Innovation (GSRI) of the Greek Ministry of Development and Investments. Its mission is to promote the triplet Research – Development – Innovation by conducting high quality research and developing innovative products and services while building strong partnerships with industry and strategic collaborations with academia and other research and technology organisations in Greece and abroad. CERTH consists of five (5) Institutes and the Central Directorate and is governed by its Board of Directors. The institutes are: the Information Technologies Institute (ITI), the Chemical Process & Energy Resources Institute (CPERI), the Hellenic Institute of Transport (HIT), the Institute of Applied Biosciences (INAB), and the Institute of Bio-Economy and Agri-Technology (iBO).

The Information Technologies Institute (ITI) is one of the leading Institutions of Greece in the fields of Informatics, Telematics and Telecommunications, with long experience in numerous European and national R&D projects. It is active in a large number of application sectors (energy, buildings and construction, health, manufacturing, robotics, (cyber)security, transport, smart cities, space, agri-food, marine and blue growth, water, etc.) and technology areas such as data and visual analytics, data mining, 5G/6G, SDN, machine and deep learning, virtual and augmented reality, image processing, computer and cognitive vision, human computer interaction, IoT and communication technologies, navigation technologies, cloud and computing technologies, distributed ledger technologies (blockchain), (semantic) interoperability, system integration, mobile and web applications, hardware design and development, smart grid technologies and solutions and social media analysis.

Within the scope of the GuardAI project, CERTH-ITI will contribute to the enhanced protection and security-by-design principles for secure Edge AI, and use case implementation, evaluation, and demonstration.

https://www.iti.gr/iti/en/home/

universität wien

The University of Vienna, founded in 1365, is the oldest public research university in the German-speaking world and one of Europe's largest institutions of higher education. In October 2017, the Department of Innovation and Digitalization in Law was established within the University's Law School to address the emerging legal challenges posed by rapid technological advancements.

The Department serves as a nexus between legal scholarship and the digital revolution, focusing on critical areas such as information technology law, intellectual property law, privacy and data protection, copyright, e-commerce, consumer protection (from European and comparative perspectives), and Legal Tech innovations.

Committed to an interdisciplinary approach, the Department actively collaborates on multidisciplinary research projects, particularly in healthcare and law enforcement, to deliver comprehensive solutions to the legal, ethical, and societal questions stemming from technological progress.

The Department of Innovation and Digitalization in Law ensures that GuardAI Consortium adheres to legal, ethical, and data protection regulations, including the European Charter of Fundamental Rights. UNIVIE also offers guidance on ethical considerations in project research and identifies potential regulatory challenges for implementing GuardAI solutions.

https://id.univie.ac.at/en/

CNIT (National, Inter-University Consortium for Telecommunications, www.cnit.it) is a non-profit consortium, established in 1995, bringing together 42 public Italian universities to perform research, innovation and education/training activities in the field of the Information and Communication Technology. CNIT operates 50 Research Units, one for each member university, plus eight other units belonging to institutes of the National Research Council (CNR, the largest public research institution in Italy) that reached a cooperation agreement with CNIT. CNIT also operates eight National Laboratories: Photonic Networks & Technologies (located in Pisa); Radar & Surveillance Systems (located in Pisa); Multimedia Communications (located in Napoli); Smart, Sustainable and Secure Internet Technologies and Infrastructures (located in Genova); Wireless Communications (located in Bologna/Cesena/Ferrara); Network Assessment, Assurance and Monitoring (located in Rome); Context – Oriented Networking (located in Catania/Cosenza/Palermo/Reggio Calabria). More than 1,300 professors and researchers, belonging to the member universities, collaborate within CNIT, together with more than 115 CNIT own employees. CNIT participated in hundreds of research projects, including EU coordinated projects, ERC grants and Italian nation-wide initiatives. In H2020 European program the CNIT has obtained 61 projects and coordinated 15 of them, while in HORIZON EUROPE the CNIT has obtained 24 projects and coordinated 9 of them. CNIT has also a significant experience in the organization of scientific events and conferences.

CNIT will contribute to the application-level resiliency framework leveraging federated and split learning to enhance privacy, security, and reliability in a data-intensive context like drone imagery processing. Based on a resilience analysis and deficiencies identified of AI systems for object recognition, CNIT will design new "security" functions to mitigate these threats at the AI level. CNIT will define and evaluate the robustness of the enhance AI-system in UC1.

https://www.cnit.it/

SPACE HELLAS S.A. is a dynamic, leading System Integrator and Value-Added Solution and Service Provider, based in Athens (Greece). The company – certified according to ISO 9001:2015 quality standard and ISO 27001:2013 for its information security management system – mainly focuses on System integration, surveillance and security systems and services, telecommunication services at national and international level, IT Applications and Services. SPACE Hellas S.A. R&D Department has extensive experience in the field of various domains including cybersecurity, software development and integration through its participation in many EU, ESA, and National collaborative R&D projects, as well as in national large-scale system integration projects, for which it develops cutting-edge technologies, products and services for the enterprise, government and defence sectors.

In GuardAI, SPACE Hellas S.A., is leading Use Case 2 for Protecting Decentralized 5G Network Analytics, by developing cutting-edge AI techniques.

https://www.space.gr/en

EXUS AI Labs, the R&D department of EXUS, is where we design and develop robust and trustworthy AI solutions that allow us to leverage the untapped potential of big data analytics across multiple verticals. For more than **35 years**, EXUS has gained substantial experience in managing research activities, from the ideation to the realisation phase, taking advantage of a highly professional and diverse team. Currently, EXUS AI Labs coordinates and participates in projects funded under EU Research and Innovation Programmes, such as Horizon Europe and European Defence Fund. Our department is developing AI solutions for numerous large-scale Research and Innovation Projects in various sectors such as Security (Physical and Digital), Health, Defence and Creativity with our core competence being around AI, data analytics, real-time systems engineering, complex event processing, and large-scale cloud implementations.

Within GuardAI, EXUS is responsible for the development of the AI Defence Recommender, a tool aiming to fortify edge AI systems against evolving challenges while enhancing their reliability and integrity.

www.exusailabs.eu

Eight Bells stands as a pioneering independent high-tech enterprise, based in Nicosia, Cyprus and in Athens, Greece dedicated to pioneering advancements in Information and Communication Technology. Our expertise spans diverse technological fields, including 5G/6G Telecommunications, Cybersecurity, and Artificial Intelligence. At the core of our offerings lie custom-designed solutions tailored to meet the demands of emerging technologies. The company also designs and builds high-performance thermal cameras for various industrial and security applications, ensuring precise and reliable thermal imaging solutions.

The company's multidisciplinary team of experts is committed to bridging the gap between academic research and practical applications, transforming innovative ideas into impactful technological solutions. Whether helping organizations enhance their digital infrastructures or providing strategic guidance, Eight Bells is dedicated to driving technological progress and improving operational efficiency for its clients. With a rich background in system engineering, R&D consultancy, and network design, we actively participate in and have led numerous Horizon, EDIDP/EDF, ESA, and National-funded research initiatives.

Eight Bells acts as the Work Package leader for Dissemination, Exploitation and Certification roadmap (WP5), overseeing the project's overall communication and developing the exploitation strategy to ensure impactful outreach and engagement. Additionally, Eight Bells contributes significantly to the project's technical aspects, including the elaboration of Use Cases and system requirements analysis, the design of the overall architecture, and conducting risk analysis and threat modeling.

https://www.8bellsresearch.com/

Cyprus Organization for Standardization (CYS) is the National Standardization Body of Cyprus, and a full member of international and European standardization bodies, including: **ISO** (International Organization for Standardization), **ITU** (International Telecommunication Union), **CEN** (European Committee for Standardization), **CENELEC** (European Committee for Electrotechnical Standardization), **ETSI** (European Telecommunications Standards Institute).

CYS's mission is to effectively represent Cyprus in the global standardization landscape, advancing the national interests in international and European standardization activities. It focuses on promoting standards that enhance the competitiveness of Cypriot businesses, ensure consumer protection, and safeguard environmental sustainability and public health. CYS is responsible for the management of the National Standardization System, which includes developing national standards and annexes of European Standards and facilitating the public enquiry of draft European and International standards.

CYS leads the standardization efforts within the GuardAI project by coordinating the review of the existing state-of-the-art included in European and International standards related to AI robustness, by providing training on standardization processes, by linking the project with the European and international ecosystem aiming to influence the development and revision of standards for AI security and robustness, and by providing a standardisation and certification roadmap for the project outputs.

https://www.cys.org.cy/en/

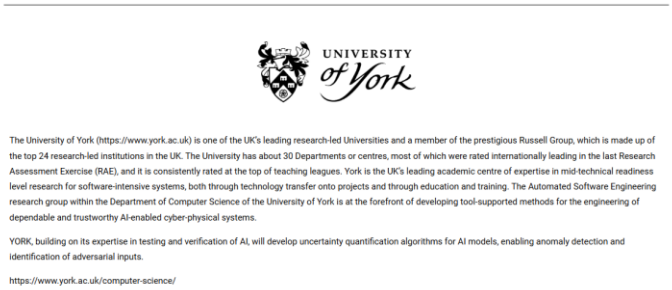


Figure 15: Consortium members' logos and description

1.1.5. News

This section (https://www.kios.ucy.ac.cy/guardai/news/) will feature announcements related to the project as it progresses, such as updates on plenary meetings and the achievement of major milestones (Figure 16).

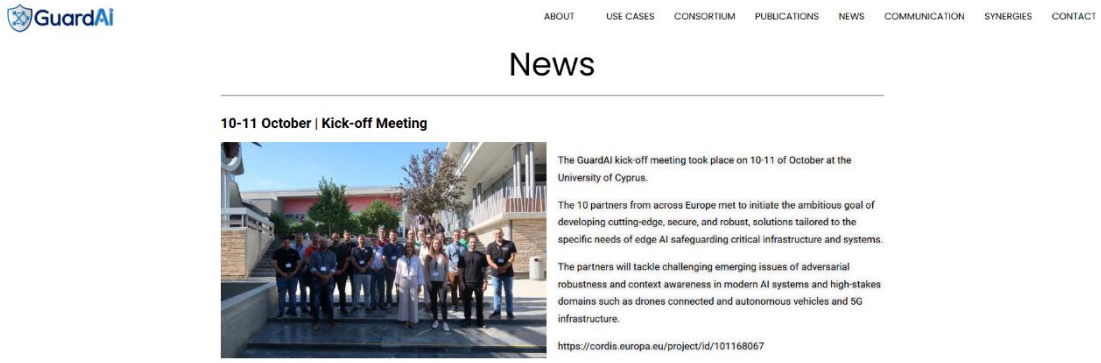


Figure 16: News page

1.1.6. Publications

This page (https://www.kios.ucy.ac.cy/guardai/publications/) will host all project-related publications, including links to open access peer-reviewed journal articles and conference proceedings, as well as deliverables (as appropriate) and public reports (Figure 17).

Figure 17: Publications page

1.1.7. Communication

This page (https://www.kios.ucy.ac.cy/guardai/communication/) will include press releases, blog articles, and communication material such as the project's brochure, posters or videos to maximize the reach of project activities and therefore its impact (Figure 18).

Figure 18: Communications page

1.1.8. Synergies

This page (https://www.kios.ucy.ac.cy/guardai/synergies/) will report specific synergies with other EU projects and Key European Initiatives on AI as the project progresses (Figure 19).

Figure 19: Synergies page

1.1.9. Contact

A dedicated page (https://www.kios.ucy.ac.cy/guardai/contact/) has been created for communication where Users can reach the project coordinators by submitting their name, email, and message. A checkbox option ensures that the Users have been informed on the privacy policy prior to submitting their message. Furthermore, direct email and phone contact details of project coordinators are available (Figure 20).

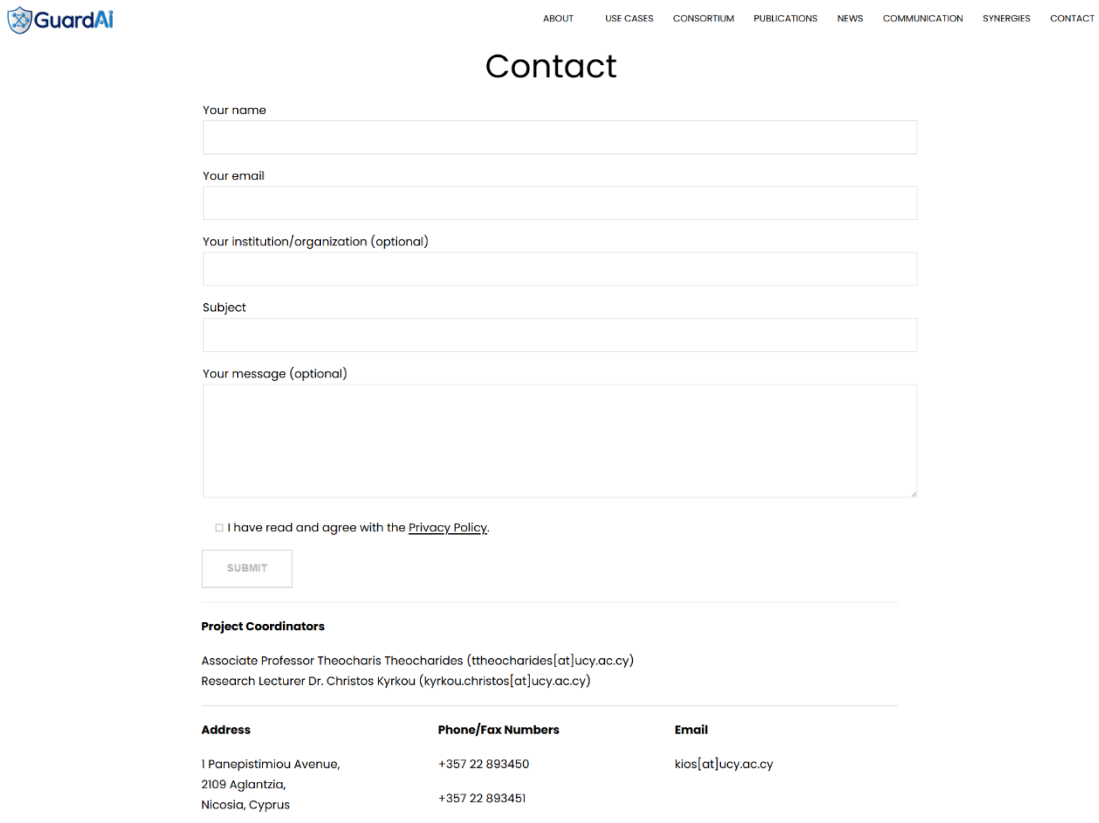


Figure 20: Contact page

1.2. Functionality

The project website is developed to provide a user-friendly interface that is also appealing to the visitors. It has a clear navigation panel to allow the user to easily navigate the website and its major sections. These are also easily accessible from the main menu bar (Figure 21) as well as the quick links provided at the bottom of each page (Figure 4).

Figure 21: Main menu bar available at all pages

Social media platforms including X (https://x.com/GuardAI_EU), YouTube (https://www.youtube.com/@GuardAI-EU), and LinkedIn (https://www.linkedin.com/company/guardai-eu-project) have been created and incorporated on the website (Figure 22) to increase communication channels and therefore interaction with the broader audience and key stakeholders.

Figure 22: Links to social media platforms

The pages “News” and “Publications” are used to communicate the developments of the project as well as disseminate the relevant publications, respectively. Consequently, the content on these pages will be informed regularly to make sure that it is always up to date and relevant to project activities.

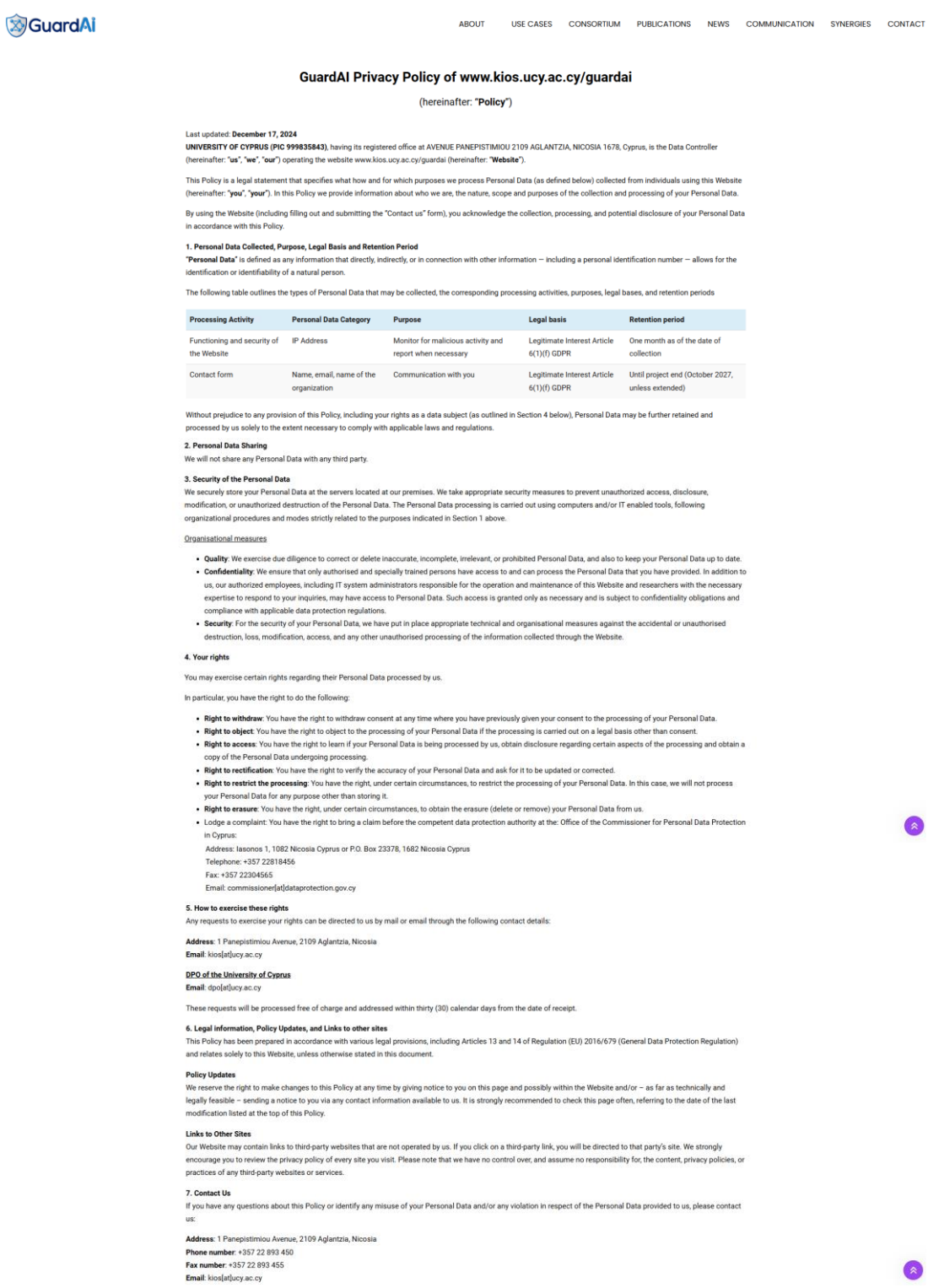
The interactive contact form helps in establishing a good means of communication with the project coordinators, providing an additional layer of user engagement. The design of the website makes it suitable for use on different devices (including desktops, tablets and mobile phones).

In the future, the website’s main menu bar will provide access to the Knowledge Hub portal (K4AI), which will include materials related to secure and resilient AI that will be developed during the project.

The website will be continuously updated, and the present deliverable reflects the website at the time of submission.

1.3. Data Protection Policy

To build user trust and ensure transparency in the handling of data, the site complies with GDPR requirements, with the adopted data protection policy (Figure 23), being clearly stated in the site, and accessible to the user via a dedicated links at the footer of each page and the “Contact” page (Figure 4 and Figure 20).



GuardAI

ABOUT USE CASES CONSORTIUM PUBLICATIONS NEWS COMMUNICATION SYNERGIES CONTACT

GuardAI Privacy Policy of www.kios.ucy.ac.cy/guardai

(hereinafter: "**Policy**")

Last updated: **December 17, 2024**

UNIVERSITY OF CYPRUS (PIC 999835843), having its registered office at AVENUE PANEPISTIMIOU 2109 AGLANTZIA, NICOSIA 1678, Cyprus, is the Data Controller (hereinafter: "**us**", "**we**", "**our**") operating the website www.kios.ucy.ac.cy/guardai (hereinafter: "**Website**").

This Policy is a legal statement that specifies what how and for which purposes we process Personal Data (as defined below) collected from individuals using this Website (hereinafter: "**you**", "**your**"). In this Policy we provide information about who we are, the nature, scope and purposes of the collection and processing of your Personal Data.

By using the Website (including filling out and submitting the "Contact us" form), you acknowledge the collection, processing, and potential disclosure of your Personal Data in accordance with this Policy.

1. Personal Data Collected, Purpose, Legal Basis and Retention Period

"**Personal Data**" is defined as any information that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person.

The following table outlines the types of Personal Data that may be collected, the corresponding processing activities, purposes, legal bases, and retention periods

Processing Activity	Personal Data Category	Purpose	Legal basis	Retention period
Functioning and security of the Website	IP Address	Monitor for malicious activity and report when necessary	Legitimate Interest Article 6(1)(f) GDPR	One month as of the date of collection
Contact form	Name, email, name of the organization	Communication with you	Legitimate Interest Article 6(1)(f) GDPR	Until project end (October 2027, unless extended)

Without prejudice to any provision of this Policy, including your rights as a data subject (as outlined in Section 4 below), Personal Data may be further retained and processed by us solely to the extent necessary to comply with applicable laws and regulations.

2. Personal Data Sharing

We will not share any Personal Data with any third party.

3. Security of the Personal Data

We securely store your Personal Data at the servers located at our premises. We take appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Personal Data. The Personal Data processing is carried out using computers and/or IT enabled tools, following organizational procedures and modes strictly related to the purposes indicated in Section 1 above.

Organisational measures

- **Quality**: We exercise due diligence to correct or delete inaccurate, incomplete, irrelevant, or prohibited Personal Data, and also to keep your Personal Data up to date.
- **Confidentiality**: We ensure that only authorised and specially trained persons have access to and can process the Personal Data that you have provided. In addition to us, our authorized employees, including IT system administrators responsible for the operation and maintenance of this Website and researchers with the necessary expertise to respond to your inquiries, may have access to Personal Data. Such access is granted only as necessary and is subject to confidentiality obligations and compliance with applicable data protection regulations.
- **Security**: For the security of your Personal Data, we have put in place appropriate technical and organisational measures against the accidental or unauthorised destruction, loss, modification, access, and any other unauthorised processing of the information collected through the Website.

4. Your rights

You may exercise certain rights regarding their Personal Data processed by us.

In particular, you have the right to do the following:

- **Right to withdraw**: You have the right to withdraw consent at any time where you have previously given your consent to the processing of your Personal Data.
- **Right to object**: You have the right to object to the processing of your Personal Data if the processing is carried out on a legal basis other than consent.
- **Right to access**: You have the right to learn if your Personal Data is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of the Personal Data undergoing processing.
- **Right to rectification**: You have the right to verify the accuracy of your Personal Data and ask for it to be updated or corrected.
- **Right to restrict the processing**: You have the right, under certain circumstances, to restrict the processing of your Personal Data. In this case, we will not process your Personal Data for any purpose other than storing it.
- **Right to erasure**: You have the right, under certain circumstances, to obtain the erasure (delete or remove) your Personal Data from us.
- Lodge a complaint: You have the right to bring a claim before the competent data protection authority at the: Office of the Commissioner for Personal Data Protection in Cyprus:
  Address: Iasonos 1, 1082 Nicosia Cyprus or P.O. Box 23378, 1682 Nicosia Cyprus
  Telephone: +357 22818456
  Fax: +357 22304565
  Email: commissioner[at]dataprotection.gov.cy

5. How to exercise these rights

Any requests to exercise your rights can be directed to us by mail or email through the following contact details:

Address: 1 Panepistimiou Avenue, 2109 Aglantzia, Nicosia
Email: kios[at]ucy.ac.cy

DPO of the University of Cyprus
Email: dpo[at]ucy.ac.cy

These requests will be processed free of charge and addressed within thirty (30) calendar days from the date of receipt.

6. Legal information, Policy Updates, and Links to other sites

This Policy has been prepared in accordance with various legal provisions, including Articles 13 and 14 of Regulation (EU) 2016/679 (General Data Protection Regulation) and relates solely to this Website, unless otherwise stated in this document.

Policy Updates

We reserve the right to make changes to this Policy at any time by giving notice to you on this page and possibly within the Website and/or – as far as technically and legally feasible – sending a notice to you via any contact information available to us. It is strongly recommended to check this page often, referring to the date of the last modification listed at the top of this Policy.

Links to Other Sites

Our Website may contain links to third-party websites that are not operated by us. If you click on a third-party link, you will be directed to that party's site. We strongly encourage you to review the privacy policy of every site you visit. Please note that we have no control over, and assume no responsibility for, the content, privacy policies, or practices of any third-party websites or services.

7. Contact Us

If you have any questions about this Policy or identify any misuse of your Personal Data and/or any violation in respect of the Personal Data provided to us, please contact us:

Address: 1 Panepistimiou Avenue, 2109 Aglantzia, Nicosia
Phone number: +357 22 893 450
Fax number: +357 22 893 455
Email: kios[at]ucy.ac.cy

Figure 23: Privacy policy of the project's website