Welcome
First Newsletter GALICIA

Generative AI with Cybersecurity for Internet Applications development

The Project

GALICIA is a project funded by the **European Union**, within the framework of the **NGI Sargasso**.

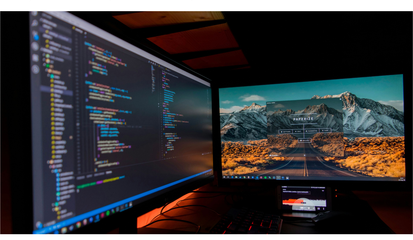
The aim of the project is to test a novel approach to digital resilience verification by testing LLM generated code for correctness and security on a set of case studies, aiming to ensure compliance with user requirements and given standards. The ambition is to verify source code generated by Generative AI and analyze its limits, thus building trust in Generative AI. GALICIA aligns with the increasing demand for compliance in industrial automation and the need for fast and low cost software production.

Main expected results:

GALICIA will provide a platform for code verification on a set of test cases in automation, encompassing a large case study of industrial maintenance, based on the Azure technology.
It will encompass a two-step verification of LLM generated code:

- Generation through use of source code, from user provided natural language functional requirements;
- Compliance verification of a formal model of the generated code with users' natural language security specifications through the NuSMV theorem prover.

Project duration: 9 months (from 5th September 2024).



Who we are:

Novareckon was born as a **spin-off** of public research to enhance the encounter between academia and companies, public bodies, the non-profit sector and citizens.

Today it is **an innovative SME** in full growth, which invests in **R&D**, hires highly qualified personnel and develops a portfolio of its business projects.

Our **network** has grown strongly over time, consolidating around the internationally recognized success of product and process **innovation projects** as well as change management models in light of (in view of) technological evolution.

website: *novareckon.it*

Mind in a Box provides real-time solutions to help organizations of all sizes make **better decisions** by getting the most value out of their data with advanced analytics and AI.

Its main solutions, Mind in a Box™, bring together hardware and software into one simple system, with Managed Services to keep things running smoothly. It makes advanced technologies easier by offering an **all-in-one**, **modular** **setup** that diminishes costs using best-of-breed open-source tools, reduces risks with licensed proprietary software, and keeps data secure.

website: *mindinabox.ai*

Since the early 1990s, **HAL Service** has been providing customized ICT and TLC solutions to businesses and public administrations.

Its goal is to accompany their clients on a continuous path of digitalization, so that they can express their full potential with the support of innovative solutions, tailor-made services, and high-quality products.
Through their WiC brand, they offer a wide range of standard and custom solutions, including connectivity, voice, network and cyber security services, cloud and data center solutions, all orchestrated by their application platforms, WiC Manager and WiC Advisor, entirely developed and managed by them.

In GALICIA project, Hal Service acts as an end user providing a critical internet application as a test case.

website: *mywic.it*

News:

GALICIA: Pioneering Secure, AI-Driven Internet Application Development

In today's digital landscape, innovation in artificial intelligence (AI) and cybersecurity is not just desirable but essential. The GALICIA project, which stands for "Generative AI with Cybersecurity for Internet Applications development," represents a bold step forward in this direction. GALICIA is committed to transforming how internet applications are created and secured by seamlessly integrating advanced generative AI with state-of-the-art cybersecurity measures. This initiative goes beyond conventional application development by building a robust framework where AI is envisioned to making them resilient against an evolving spectrum of cyber threats.

At the core of GALICIA lies a dual focus on safety and innovation. The project's AI algorithms are potentially able to not only streamline development but also embed adaptive security protocols that detect, anticipate, and mitigate cyber risks autonomously. This approach provides developers and enterprises with tools that are not only efficient but also inherently secure, reducing the need for separate cybersecurity add-ons or reactive defenses.
GALICIA is designed with a collaborative, modular approach, allowing Small and Medium-sized Enterprises (SMEs) and larger organizations alike to adapt and scale the framework to their specific needs. By empowering diverse industries with secure, AI-driven applications, GALICIA is positioned to have a lasting societal impact—enabling secure digital services and fostering trust in digital transformation processes.

The design of the GALICIA mock-up

The development of secure and efficient software is crucial, and a new AI-driven application is set to redefine how developers create and verify code. This upcoming software has been conceptualized with three potential release options: Integration as an Integrated Development Environment plugin, a specialized GPT interface, or a standalone custom application. After careful consideration, the custom application approach was chosen for its flexibility and comprehensive functionality.

This application allows developers to input functional requirements in natural language. Using a backend LLM, the system generates corresponding source code and a formal model for compliance verification. The software ensures rigorous security and functionality standards by integrating with verification tools like NuSMV. If discrepancies arise, it iteratively refines the code until it meets the predefined standards, offering developers detailed feedback on every step.

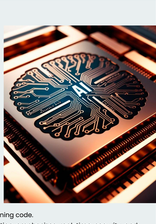
The user interface is designed for simplicity and effectiveness. Developers can:

- Enter functional requirements via text or file upload.
- Generate source code and review it on dedicated screens.
- Access detailed verification reports, including iteration history and error corrections.
- Customize settings such as the maximum number of iterations for refining code.

Unlike existing tools such as GitHub Copilot or Tabnine, this application emphasizes real-time security and compliance. It employs formal verification to ensure code correctness, making it particularly valuable for industries with stringent safety requirements.
The application features a layered architecture, separating the user interface, server logic, and LLM integration. This modular approach simplifies updates and potential expansions into other platforms, such as IDE plugins or GPT integrations.

This groundbreaking software is poised to become a game-changer in secure code development, combining ease of use with unparalleled rigor in compliance and functionality.

Stay tuned for its launch!

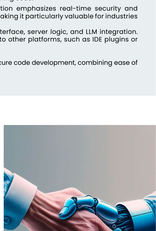


Societal Impact of AI-Driven Cybersecurity Projects

Across the EU and US, projects such as AI4CYBER, REWIRE, and CYBERSANE are advancing the use of AI for cybersecurity, targeting critical sectors from infrastructure to public services. Though many are still in the early phases, these initiatives highlight the potential for societal impact through improved cyber resilience.

- *AI4CYBER* aims to enhance vulnerability detection across sectors like finance and utilities. By deploying advanced algorithms, it lays a foundation for safer critical infrastructure, though its impact is contingent on widespread adoption of its tools.
- *REWIRE* provides a modular framework for coordinated cyber incident responses. While promising for healthcare and finance, its societal reach remains limited until it undergoes broader implementation.
- *CYBERSANE* has made headway in raising public awareness and bolstering cyber incident responses for both government and private entities. This initiative is beginning to show practical results in governmental crisis management.
- *Smart City and Transportation Resilience* initiatives, like those in Los Angeles, are delivering tangible benefits. Enhanced AI-based threat detection is already improving security in transportation, though these impacts are currently localized.

Together, these projects underscore the promise of AI-driven cybersecurity but also highlight the need for larger-scale implementation. GALICIA aligns well with these efforts, aiming to create cybersecurity frameworks that can address vulnerabilities at scale.

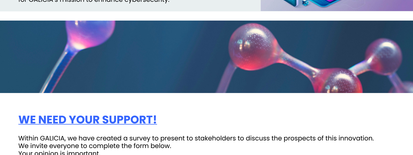


AI-Powered Code Verification Tools

A variety of European tools are tackling the verification of AI-generated code, offering developers insights into security flaws. Examples include:

- CodeChecker and SonarQube for analyzing code vulnerabilities.
- Semmle and ShiftLeft for detecting security issues across languages.
- Checkmarx and Snyk for identifying flaws in open-source dependencies.

These tools ensure AI-generated code meets security standards, essential for GALICIA's mission to enhance cybersecurity.



WE NEED YOUR SUPPORT!

Within GALICIA, we have created a survey to present to stakeholders to discuss the prospects of this innovation.
We invite everyone to complete the form below.
Your opinion is important.

Thank you!

Click here to complete the survey >

GALICIA

Visit our website:
galicia-project.eu