Second 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 relevance, based on the Azure technology.
It will encompass a two-step verification of LLM generated code:
- Generation through Azure 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.

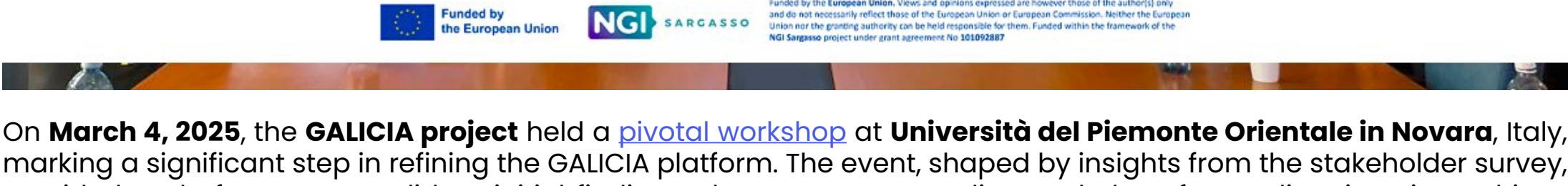**Project duration: 9 months** *(from 5th September 2024).*

Click here for more information >

News:

GALICIA Workshop: Advancing AI-Driven Verification & ValidationPioneering Secure, AI-Driven Internet Application Development

*Pioneering Secure, AI-Driven Internet Application Development*

On **March 4, 2025**, the **GALICIA project** held a **pivotal workshop** at **Università del Piemonte Orientale in Novara**, Italy, marking a significant step in refining the GALICIA platform. The event, shaped by insights from the stakeholder survey, provided a platform to consolidate initial findings, showcase case studies, and chart future directions in AI-driven verification and validation (V&V).

A key highlight was the introduction of the GALICIA V&V platform, demonstrating its innovative integration of formal methods and Large Language Models (LLMs). Presentations included a keynote by **Franco Alberto Cardillo** (CNR) on theoretical and practical applications, alongside benchmark demonstrations by **Lorenzo Vandoni** (*Hal Service*) and **Alberto Stefanini** (*Novareckon*). **Jérémie Farret** (*Mind-in-a-Box*) also provided remote insights into GALICIA's hybrid LLM infrastructure and its commercial potential.

The event culminated in a structured roundtable discussion, where stakeholders identified key technical objectives, industry adoption opportunities, and an initial roadmap for GALICIA's future. These discussions reinforced the platform's alignment with industry needs, compliance automation, and emerging regulatory frameworks.

By fostering meaningful engagement among industry leaders, SMEs, and research institutions, the workshop strengthened GALICIA's role as a catalyst for trust and reliability in AI-driven software verification. The event set the stage for further refinement, expanded case studies, and strategic collaborations, ensuring GALICIA evolves into a robust, industry-ready solution for compliance verification in AI-generated software.

GALICIA Test Case Landscape: Advancing Formal Verification
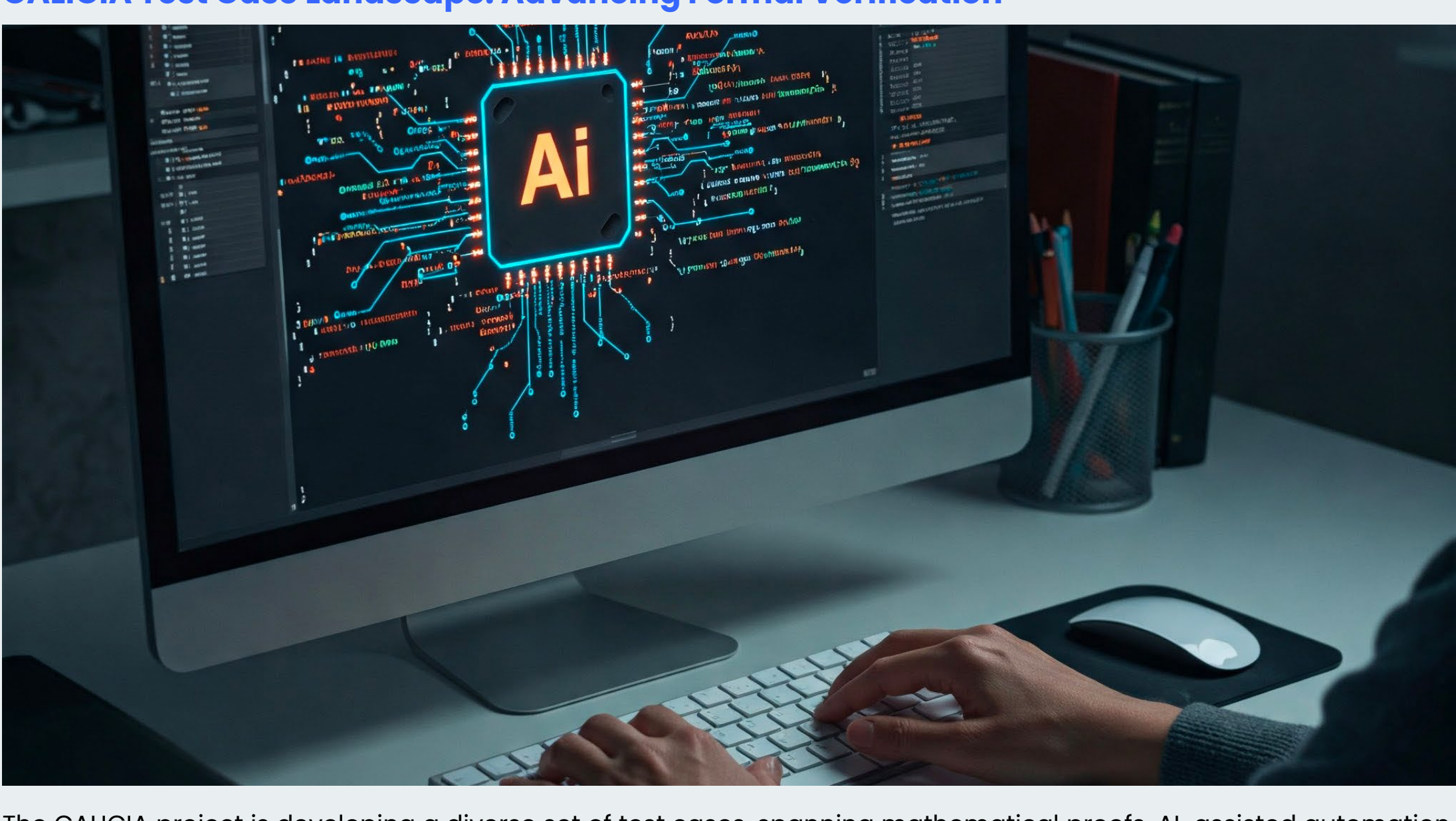
The GALICIA project is developing a diverse set of test cases, spanning mathematical proofs, AI-assisted automation, and network protocols. Current studies include formalizing the Fibonacci sequence, Euclid's geometry, specific functionalities of HAL's WiC Advisor, and implementing the handshake mechanism of the TCP/IP protocol.

WiC Advisor Test Cases
The project examines the CRUD functions (Create, Read, Update, Delete) within WiC Advisor, enabling secure IoT service management through querying, external resource creation, and remote diagnostics. Another case study focuses on coverage verification, cross-referencing address-based service availability from multiple providers (e.g., TIM, Open Fiber, FastWeb). Additional functionalities include a guided service quote generator and a ticketing system for end-to-end technical support tracking.

Formalizing Euclid's Theorem
GALICIA explores Euclid's geometric axioms using formal methods, representing fundamental postulates in first-order logic. The study includes proving equilateral triangle construction in Prolog and validating the model in Coq and Python B, ensuring rigorous verification.

TCP/IP Protocol Analysis
By modeling and verifying the handshake mechanism, the project assesses network communication integrity, identifying correctness and security considerations.

Key Takeaways
GALICIA demonstrates that formal verification, traditionally requiring months of manual effort, can now be completed in days with Large Language Models (LLMs). These AI-driven approaches support modeling paradigm selection, completeness checks, and implementation guidance. While results are promising, further large-scale validation is necessary to refine these methodologies and confirm their robustness in complex real-world applications.

The GALICIA platform
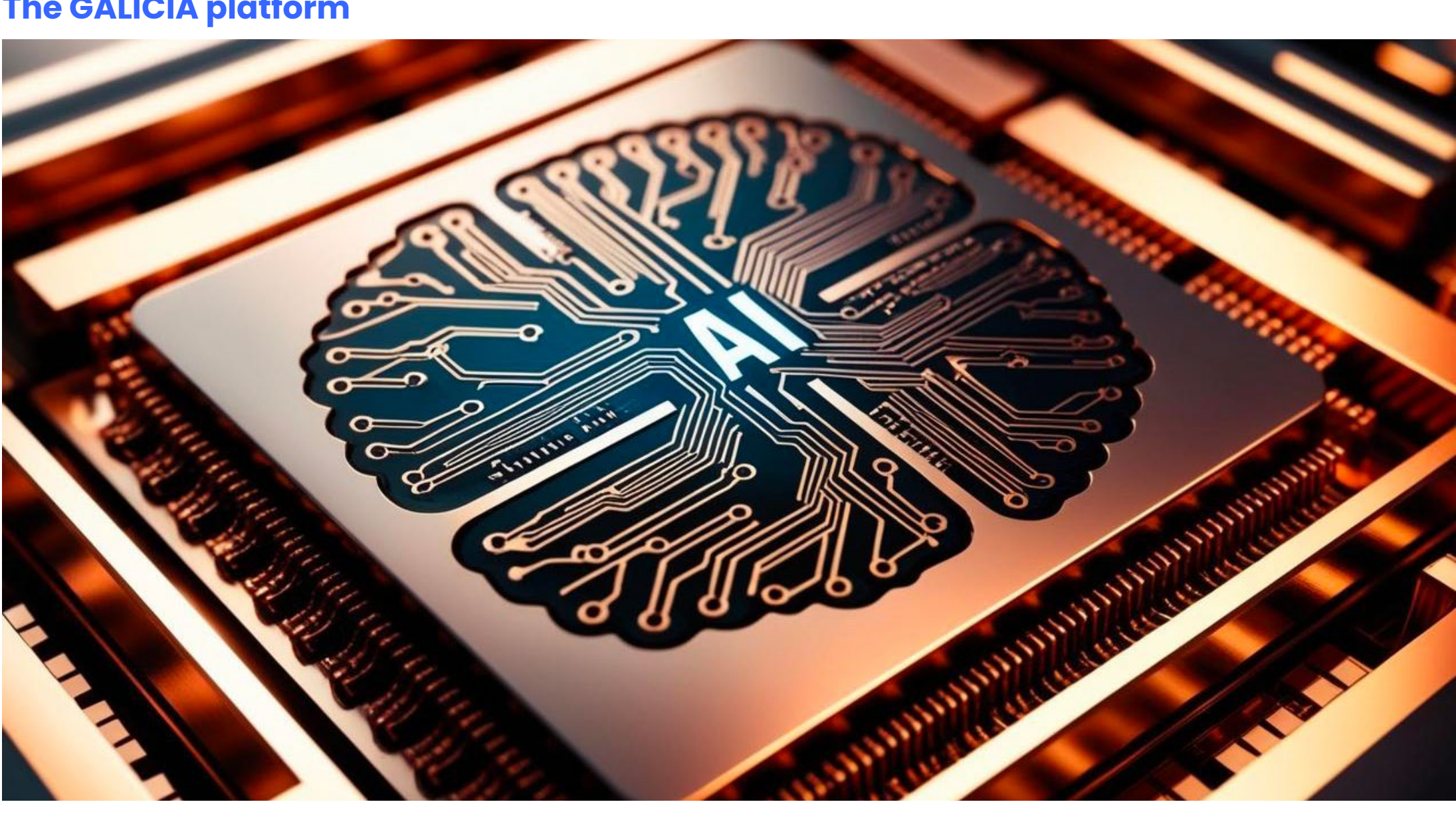
The world of software development is evolving rapidly, and the Galicia platform proposes a new approach to secure code development.

Designed to seamlessly integrate generative AI and cybersecurity, Galicia is a web application that interfaces with advanced AI platforms like Mind In a Box and popular language models such as OpenAI's GPT and LLaMA.

At its core, Galicia offers an innovative approach to code generation. When a user requests a function or script, the platform takes a structured path to ensure accuracy and security. This process involves:
- Creating a formal model of the user's request
- Generating the source code
- Crafting test cases to validate functionality
- Verifying the code against common security standards
- Refining through iterative improvements

Only after completing these rigorous steps is the final code presented to the user, with the option to review the entire development process.

To illustrate Galicia's value, consider a simple coding task: writing a function to capitalize the first letter of each word. While straightforward at first glance, common pitfalls—like handling null inputs, invalid pointers, or read-only strings—can compromise the code. Galicia ensures such challenges are addressed early in development, resulting in robust, error-free solutions.

The platform's standout feature is its guided reasoning process, built on formal modeling and iterative validation. Unlike competitors, such as GitHub Copilot or ChatGPT, Galicia focuses on security and precision, positioning it as a valuable tool for developers focused on reliability.

As Galicia evolves, the team is looking for users and projects to refine the platform further and explore its market potential. If you're interested in collaborating or experimenting with this groundbreaking tool, now is the time to get involved.

GALICIA

Visit our website:
galicia-project.eu