Funded by the European Union

NGI SARGASSO

Funded by the **European Union**. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them. Funded within the framework of the **NGI Sargasso** project under grant agreement No **101092887**

Third 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.

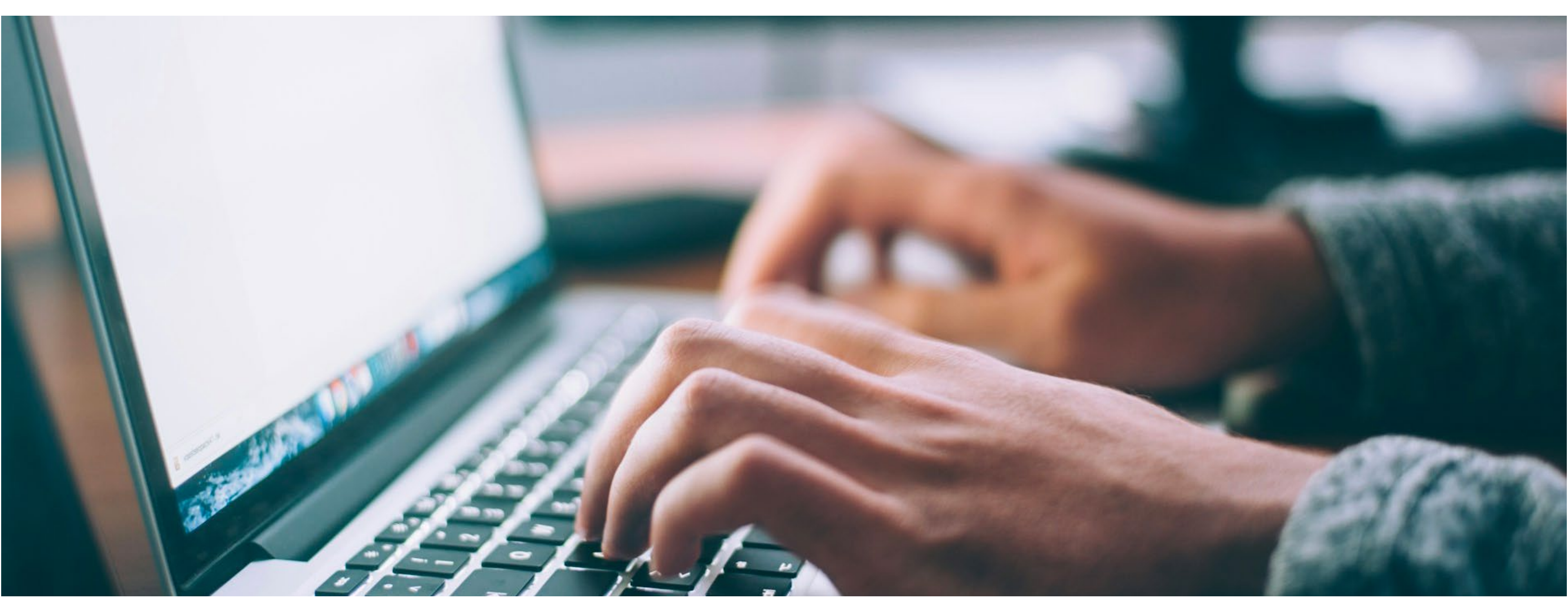
Main expected results:

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:

The GALICIA Platform Undergoes Second Round of Evaluation with Broader Panel

The second evaluation of the GALICIA platform builds upon an initial expert review conducted using the System Usability Scale (SUS). This new phase involved a broader panel of 11 evaluators, bringing diverse perspectives from both academia and industry. The focus shifted toward gathering structured, hands-on feedback to assess the platform's practical usability and potential value in real-world applications.

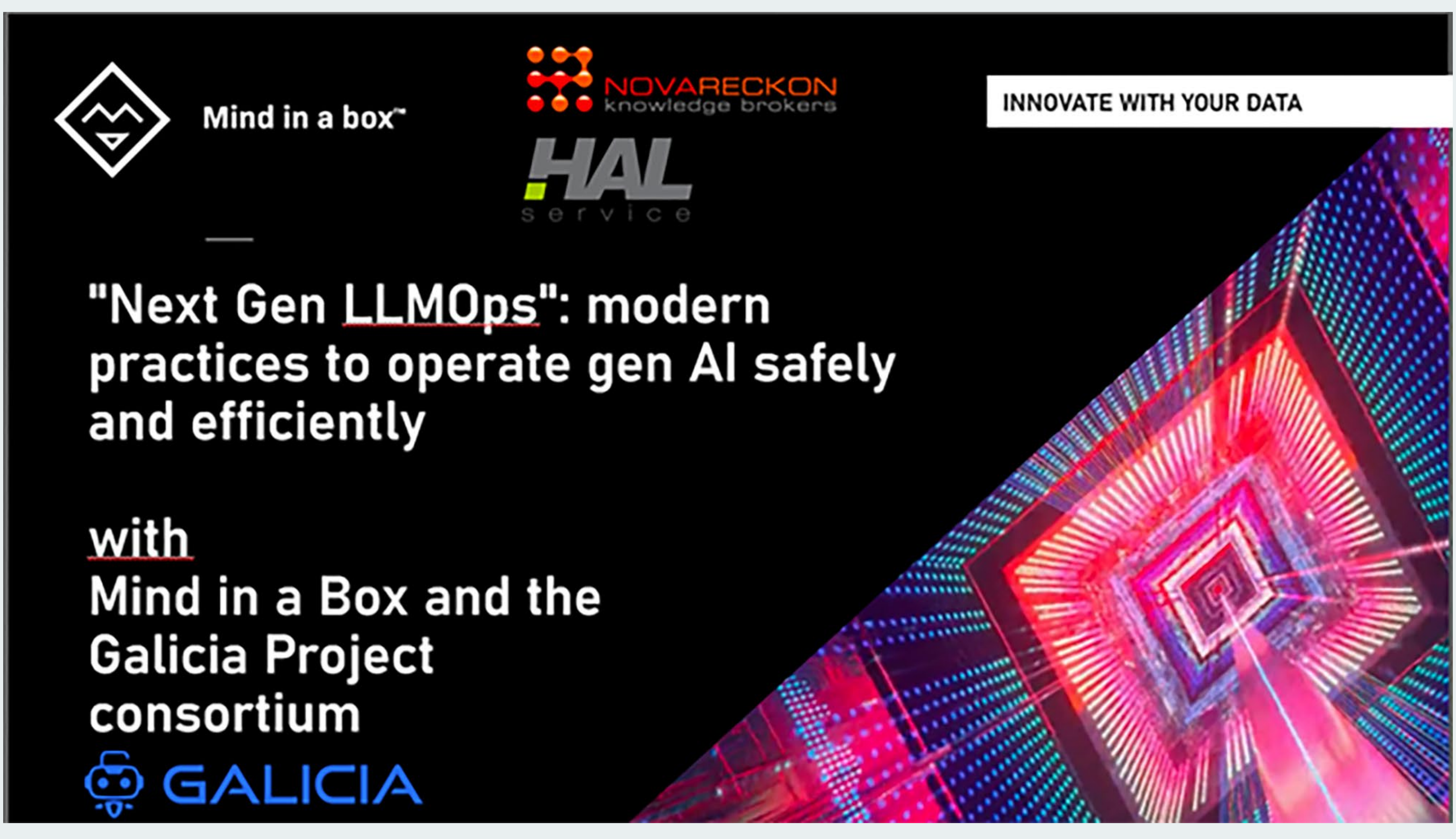
Every evaluation included:

- A **guided mini-use case**, allowing each participant to test GALICIA's core features through a real-life coding scenario.
- A **tailored Evaluation Questionnaire**, designed to collect targeted insights on user experience, clarity, transparency, and overall platform value.

The results confirmed GALICIA's increasing relevance and applicability in **operational and educational contexts**, particularly in fields such as **manufacturing, critical infrastructure, cybersecurity, and trustworthy AI**.

GALICIA at the World Summit AI:

Workshop Highlights and Community Feedback



Mind in a box™

NOVARECKON knowledge brokers

HAL service

INNOVATE WITH YOUR DATA

"Next Gen LLMOps": modern practices to operate gen AI safely and efficiently

with
Mind in a Box and the Galicia Project consortium

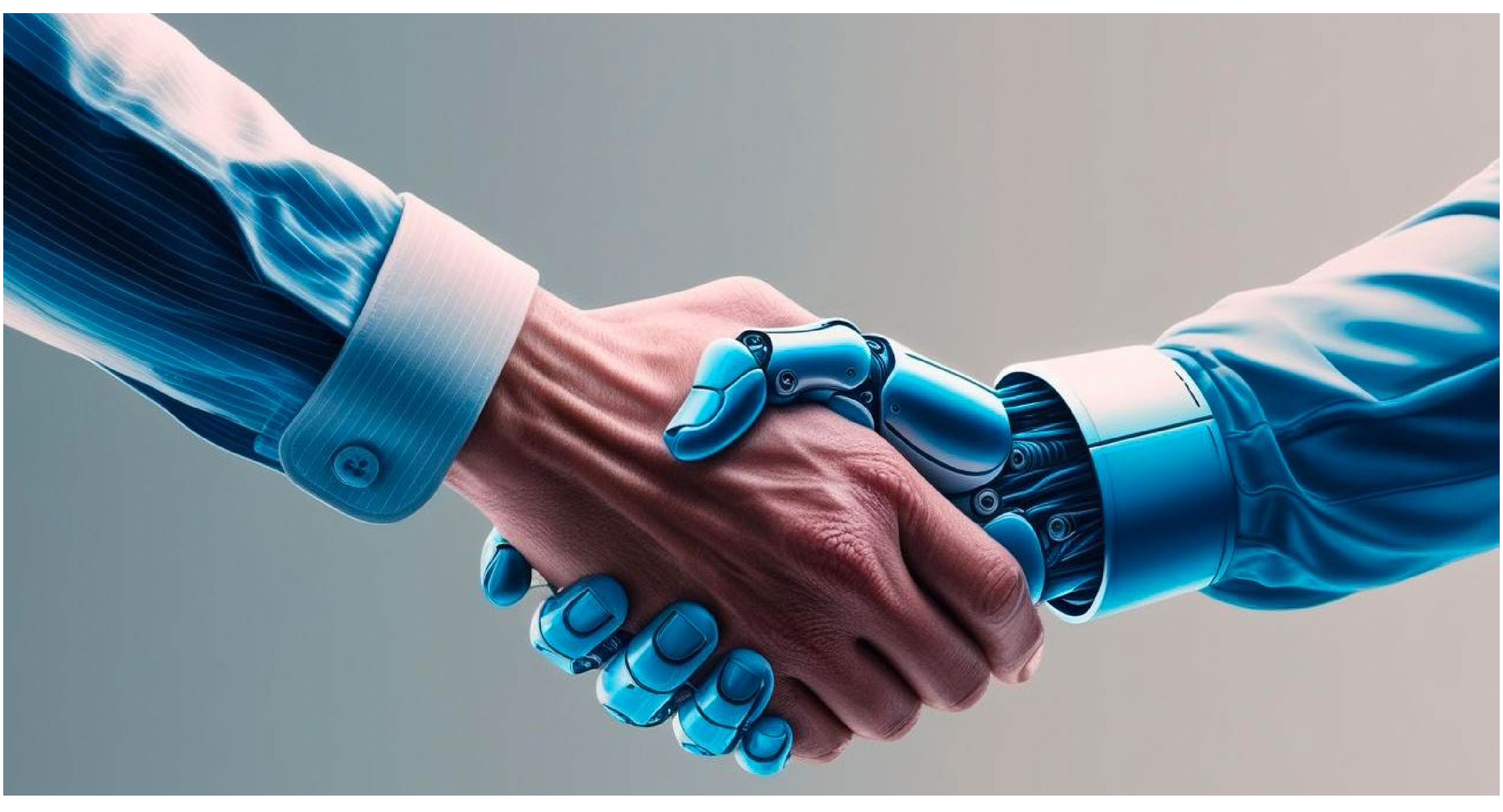
GALICIA

The **GALICIA project** was showcased in a dedicated workshop at the **World Summit AI (***WSAI***)**, one of the most prominent global events on artificial intelligence. The session, held on **April 15, 2025**, was led by **Jérémie Farret** from the GALICIA team. It was officially part of WSAI's workshop track and exceeded its scheduled time as about 15 participants remained for an extended discussion. This engagement reflected strong interest in the project's vision for next-generation infrastructure supporting **LLMOps** (*Large Language Model Operations*), thanks to **Mind in a Box's** integrated **GenAI solutions**.

Participants were particularly receptive to GALICIA's focus on building trust in generative AI, especially regarding secure and specialized code generation. Several interventions highlighted the value of adapting AI outputs to domain-specific requirements, with techniques such as **Retrieval-Augmented Generation (***RAG***)** viewed as effective strategies.

Concerns were also raised about the legal and strategic risks of relying on commercial, cloud-based AI platforms—especially in terms of intellectual property and data confidentiality. The recent controversy surrounding **DeepSeek** — a Chinese open-source project revealed to have incorporated code and data from proprietary sources without clear attribution — was cited as a cautionary case. In this context, GALICIA's on-premises AI approach, which keeps sensitive operations under full user control, was welcomed as a responsible and future-oriented alternative.

GALICIA Final Report and Conclusions

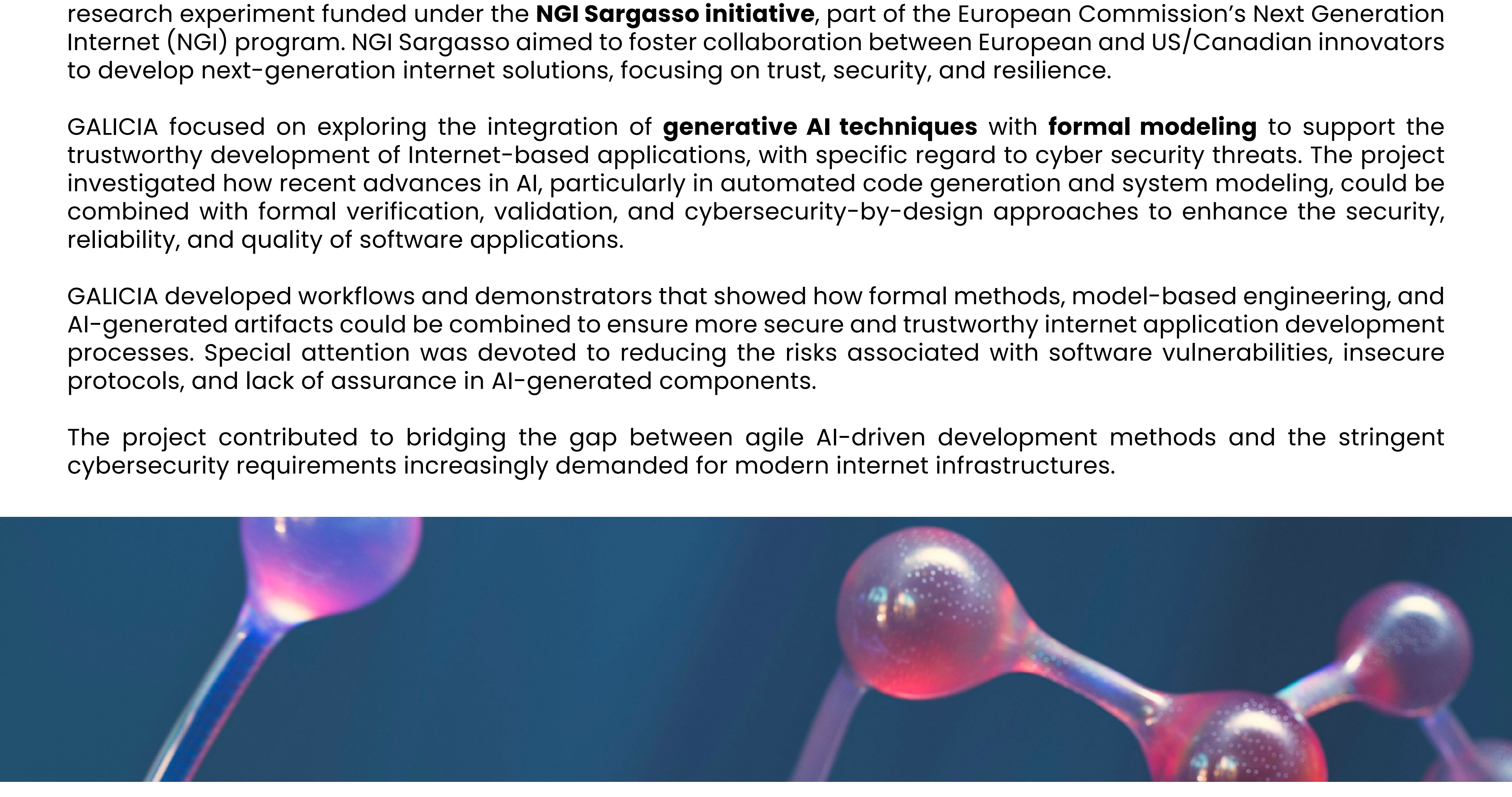


The GALICIA project **(Generative AI with Cybersecurity for Internet Applications development**) is a European research experiment funded under the **NGI Sargasso initiative**, part of the European Commission's Next Generation Internet (NGI) program. NGI Sargasso aimed to foster collaboration between European and US/Canadian innovators to develop next-generation internet solutions, focusing on trust, security, and resilience.

GALICIA focused on exploring the integration of **generative AI techniques** with **formal modeling** to support the trustworthy development of Internet-based applications, with specific regard to cyber security threats. The project investigated how recent advances in AI, particularly in automated code generation and system modeling, could be combined with formal verification, validation, and cybersecurity-by-design approaches to enhance the security, reliability, and quality of software applications.

GALICIA developed workflows and demonstrators that showed how formal methods, model-based engineering, and AI-generated artifacts could be combined to ensure more secure and trustworthy internet application development processes. Special attention was devoted to reducing the risks associated with software vulnerabilities, insecure protocols, and lack of assurance in AI-generated components.

The project contributed to bridging the gap between agile AI-driven development methods and the stringent cybersecurity requirements increasingly demanded for modern internet infrastructures.



GALICIA

Funded by the European Union

NGI SARGASSO

Funded by the **European Union**. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them. Funded within the framework of the **NGI Sargasso** project under grant agreement No **101092887**

Visit our website:
galicia-project.eu

Unsubscribe