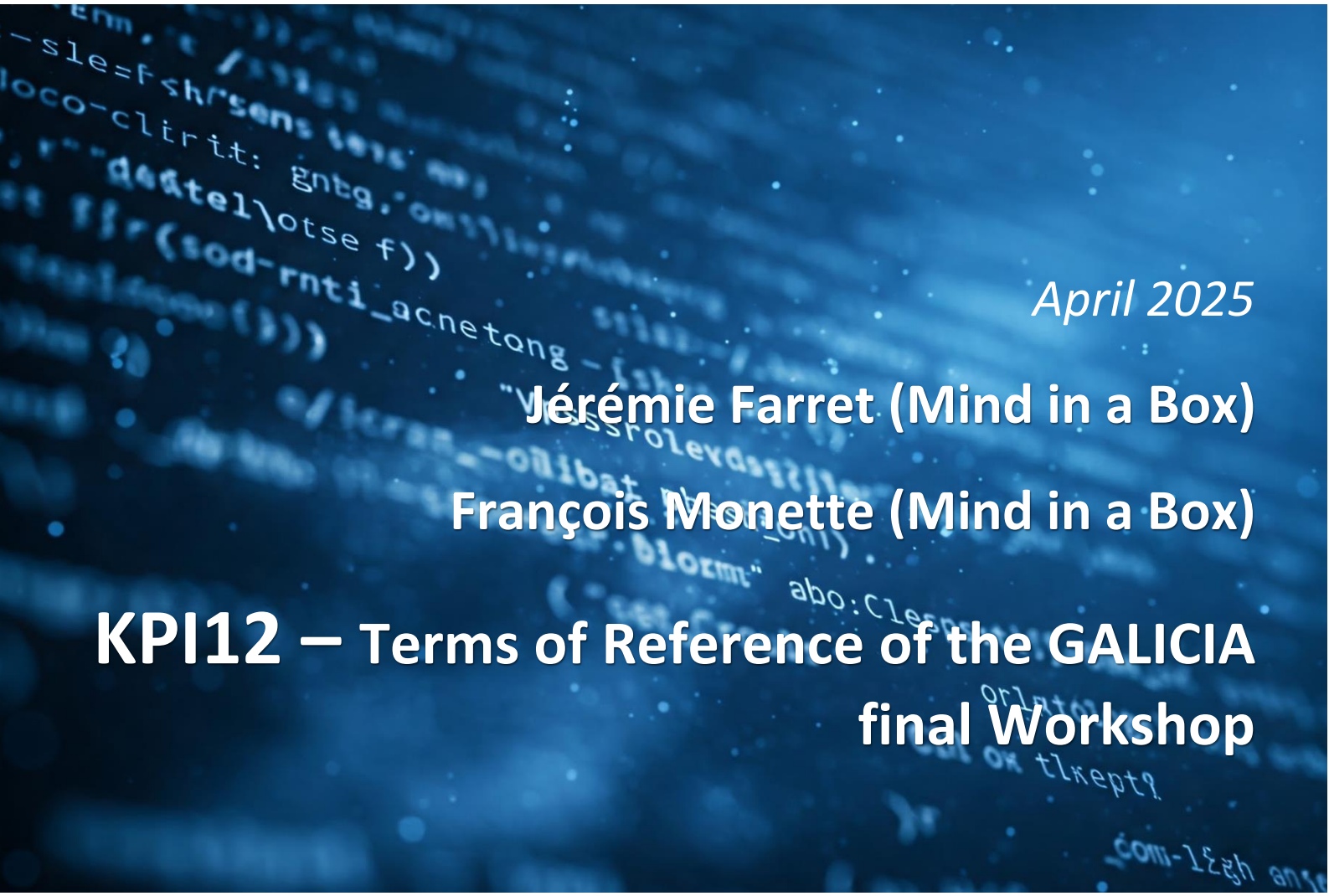

April 2025

Jérémie Farret (Mind in a Box)

François Monette (Mind in a Box)

KPI12 – Terms of Reference of the GALICIA final Workshop

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**

Project Name: GALICIA
Internal Report Title: KPI12 – Terms of Reference of the final Workshop, contents and questionnaires
Authors: Jérémie Farret and François Monette (Mind in a Box)
Revised by: Jérémie Farret (Mind in a Box)
Date: 25/04/2025
Version: 2
Distribution: Internal / Limited circulation

TABLE OF CONTENTS

1 INTRODUCTION

The GALICIA project aims to establish a platform for the automated verification of Large Language Model (LLM)-generated code against predefined test cases, with a strong focus on automation and industrial applications in the telecom sector. By encompassing the complete lifecycle—from natural language functional requirements and security specifications to formal verification—GALICIA seeks to bridge the gap between AI-generated code and compliance with user-defined requirements and industry standards. The project's broader ambition is to analyze the reliability of Generative AI in software development and contribute to building trust in AI-driven automation.

This report contains the Terms of Reference (ToR) for the final workshop, which provides an opportunity for Mind in a Box to present the work of the project partners—Novareckon, Mind in a Box Inc., and Hal Service—done with the support of NGI SARGASSO, in a high-visibility context.

2 TERMS OF REFERENCE FOR THE GALICIA WORKSHOP

2.1 Format of the final workshop

In contrast to the mid-term workshop, which emphasized collaborative discussion and analysis of stakeholder survey findings, the final workshop took the form of a presentation by Mind in a Box during the World Summit AI event that took place in Montreal, Canada in April 2025. Recognized as one of the world's premier AI conferences, the event gathers thousands of global experts, innovators, policymakers, and industry leaders. It offers a strategic platform to showcase cutting-edge developments in artificial intelligence, making it an ideal venue to present the GALICIA project.

Rather than focusing on internal alignment or feedback, the final workshop aimed to position GALICIA in the international spotlight, share its technological advancements, and engage a wide array of potential stakeholders in the AI, telecom, and cybersecurity domains.

2.2 Presentation on the GALICIA Platform

The presentation highlighted the GALICIA platform's core objectives, technical architecture and preliminary results. It was integrated into a broader session given by Mind in a Box titled *Next Gen LLMOps: Modern practices to operate Gen AI safely and efficiently*, aligning seamlessly with GALICIA's mission to address operational and security challenges related to Generative AI in industrial settings.

By participating in this session, the consortium not only contributed to the global dialogue on responsible AI practices but also strengthened the visibility and credibility of the platform within a targeted audience of AI practitioners, startups, telecom specialists, academic researchers, and investors. Given Montreal's prominent role as a global hub for AI research and innovation, the workshop was uniquely positioned to generate interest, spark future collaborations, and amplify the impact of the GALICIA project.

This final workshop served both as a capstone event for the project and as a catalyst for continued exploration and deployment of AI-driven software verification solutions in high-stakes industrial contexts.

Below are a few items related to the workshop.

	Pamela Snively, Chief Data & Trust Officer, TELUS Communications	
12:05	**HEADLINER** (12:05-12:25) **From Lab to Launchpad - Overcoming Enterprise Adoption Hurdles** Can AI truly transcend the lab and revolutionize industries? This session challenges us to move beyond theoretical potential and confront the realities of applied AI. We'll dissect the hurdles of enterprise adoption – data silos, workflow fragmentation, and the crucial element of trust – and explore how strategic partnerships can pave the way for real-world impact. But the journey doesn't stop there. We'll peer into the future of Agentic AI, questioning what it will take to unleash the power of autonomous agents within our organizations. Are we ready to redefine work itself, or will the path to agentless services remain a distant horizon? Join us to grapple with the transformative power of AI, from driving immediate value to shaping the very nature of enterprise operations. Durga Kota, Chief Technology Officer, **Fujitsu North America**	**WORKSHOP 2 – 30 mins** (12:15 – 12:45) **Next Gen LLMOps: Modern practices to operate Gen AI safely and efficiently** This workshop presents "Next Gen LLMOps", modern LLM practices to operate your gen AI model safely and harmoniously with your data, either enriching its input (RAG) or generating new data from it (Deep Data). With countless gen AI solutions emerging all over the world, the question of using these solutions safely and efficiently, as well as customizing them for a better fit with your operations, comes up more and more frequently. While terms like DevOps, DataOps, even MLOps have been coined over the years to refer to the rationalisation of practices linked to development, data processing or machine learning, LLMOps is an emerging term linked to Large Language Models practices. LLMOps aims to solve difficulties ranging from aggressive user licenses all the way to geopolitics. This workshop will focus on presenting some simple, pragmatic solutions which can help overcoming these difficulties : from deploying on premise architectures to hybrid infrastructure, we will review how gen AI models can be put to use to your benefit, while minimizing the risks. Implanted, real world examples will illustrate these solutions. Jérémie Farret, CEO/CTO, **Mind in a Box**
12:30	**HEADLINER** (12:30-12:50) **Unlocking the Power of Confidential Computing: Securing Data in Use** Confidential computing is transforming the landscape of data privacy and security by enabling the processing of sensitive data in a secure and isolated environment, even while data is actively in use. This capability is particularly critical for AI applications, which rely heavily on large volumes of sensitive data during training and inference. In this session, we will explore the key concepts and emerging technologies behind confidential computing, including trusted execution environments (TEEs), hardware-based security measures, and their real-world applications. You will gain an understanding of how confidential computing mitigates the risks of data breaches and ensures compliance with privacy regulations, empowering organizations to leverage sensitive data without compromising security. Andrej Zdravkovic, SVP, GPU Technologies and Engineering Software & Chief Software Officer, **AMD**	
12:50	**LUNCH AND NETWORKING**	
	WORLD SUMMIT AI PLENARY: Chair: Matthew Blakemore, CEO, **AI Caramba!**	**TRACK 1: AI IN ACTION: USE CASES** Chair: Alyssa Lefaivre Škopac, Director of AI Trust & Safety, **Amii**

Figure 1 – Agenda screenshot of the World Summit AI event

Figure 2 – Cover page of the workshop presentation at the World Summit AI

Figure 3 – Pictures from the workshop at the World Summit AI

2.3 Feedback from the workshop

The questions and answers from participants reflected a strong interest in the next-generation LLMOps infrastructure of the project GALICIA. It addressed existing challenges faced by the LLM research and applications community.

The workshop attendees were very appreciative of the objectives of the GALICIA project, and the need to strengthen the trust component in Generative AI code generation. Several comments were made regarding the importance of specializing code generation for specific domain constraints, with Retrieval-Augmented Generation being generally recognized as an appropriate solution to address such requirements.

There was also significant concern regarding technical property and IP risks associated with the use of cloud-based LLM solutions. The recent DeepSeek-related debate served as a unifying illustration of this concern amongst the workshop audience. There was a consensus that licensing agreements alone were insufficient guarantees, and that the on-premises LLM capability of the GALICIA project was an appropriate solution. Additionally, two pieces of feedback linked concerns about confidentiality, the reliance on US-centric cloud services, and recent developments in international trade.

2.4 Related dissemination initiative

Another event, the 7th International Conference on Advances in Signal Processing and Artificial Intelligence (ASPAI 2025), held from April 8 to 10, 2025, in Austria, was used by Mind in a Box as an additional dissemination opportunity to present the infrastructure used in the GALICIA project, including its LLMOps and the proposed context-aware Retrieval-Augmentation Generation (RAG) workflow.

A scientific paper was published at this event, along with an accompanying presentation. A recording is available here.

3 CONCLUSION

The final workshop of the GALICIA project was held within the high-profile context of the World Summit AI, marked a pivotal moment in the project's lifecycle. By presenting the GALICIA platform to a global and expert audience, the event served both as a culmination of the project's collaborative efforts and as a springboard for future engagement, adoption, and evolution.

This high-visibility opportunity not only reinforced the project's commitment to transparency, innovation, and impact in the domain of AI-generated code verification, but also underscored its relevance in addressing critical challenges in cybersecurity and software reliability.

PROJECT CONSORTIUM:

Funded by
the European Union

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**