

KI.DI.COM

KI-gestützter Entwurf und Cybersecurity-Analyse eines 'Digital Twins' am Beispiel Future Communications Infrastructure

Programm / Ausschreibung	WRLT 24/26, WRLT 24/26, Take Off Ausschreibung 2024	Status	laufend
Projektstart	01.01.2026	Projektende	31.12.2026
Zeitraum	2026 - 2026	Projektlaufzeit	12 Monate
Keywords	Künstliche Intelligenz; Flugsicherungstechnik;		

Projektbeschreibung

Aktuelle Arbeiten aus unterschiedlichsten wissenschaftlichen Disziplinen zeigen, dass der Einsatz von Large Language Modellen (LLM) in vielen Bereichen der FTI einen Reifegrad erreicht, um KI-Modelle als mächtiges und unterstützendes Forschungswerkzeug nutzen zu können. Dabei spielt die neue und gegenwärtig stark an Bedeutung wachsende Domäne des "Prompt Engineerings" eine zentrale Rolle, da durch gezielte Interaktion mit dem LLM die Art und Qualität der Ergebnisse beeinflusst und auf Anforderungen der Forscherinnen und Forscher optimiert werden kann.

Im Rahmen der Sondierung "KI.DI.COM" sollen Einsatzpotenziale und -szenarien von LLM und Prompt Engineering an beispielhaften Elementen der zukünftigen aeronautischen Kommunikation (Future Communications Infrastructure, FCI) und der damit verbundenen Endsysteme bei Flugsicherung, Fluglinie und Luftfahrtgerät untersucht werden. Mittels FCI werden ATC-Controllerarbeitsplätze, Airline-Dispatch und die flugzeugseitige Avionik über die Funkschnittstelle und das aeronautische Telekommunikationsnetzwerk hinweg in ein Gesamtnetzwerk integriert. In diesem Einsatzszenario werden exemplarisch Fragestellungen mithilfe von KI- bzw. LLM-Einsatz gepromptet, Lösungen erarbeitet und diese mit aktuell bereits bekannten Implementierungen anhand einer mehrdimensionalen Skala bewertet. Im Fokus stehen insbesondere die Darstellung eines X.25-basierten ATN-Demonstrators sowie die Entwicklung von Cyber-Angriffszenarien auf ein modernes IP-System, wie sie bei FCI zum Einsatz kommen. Basierend auf der Arbeitshypothese, wonach ein LLM ein valides Entwurfswerkzeug im Bereich der Flugsicherungstechnik darstellt, werden die folgenden Forschungsfragen (RQ) untersucht: RQ.1 behandelt dabei das Prompt Engineering und soll effiziente Interaktionsstrategien mit dem LLM erarbeiten. RQ.2 dreht sich um die Frage, welche Qualität ein KI-generiertes F&E-Ergebnis erreichen kann und RQ.3 betrachtet den Einfluss des verwendeten LLM auf das erzielte Ergebnis sowie die Frage, ob der FTI-Aufwand durch den Einsatz der KI maßgeblich reduziert werden kann.

Das angestrebte Ergebnisse der Sondierung ist eine qualitative und quantitative Aussage, welche technologischen Reifegrade anhand KI-getriebener FTI im Bereich der Flugsicherungstechnik und Avionik momentan erreicht werden können. Zudem soll die Frage beantwortet werden, ob ein auf OpenSource basierendes LLM vergleichbare Resultate erzielen wie eine kommerzielle Implementierung. Durch die Arbeiten an drei Fragestellungen des FCI auf unterschiedlichen

Abstraktionsebenen soll die Aussagekraft der Analyse erhöht und verallgemeinert werden. Die Ergebnisse der Sondierung sollen im Rahmen eines kooperativen F&E-Vorhabens im Themenbereich der Cybersicherheit der zukünftigen aeronautischen Kommunikation fortgesetzt werden.

Abstract

Current work from a wide range of scientific disciplines shows that the use of large language models (LLM) has reached a level of maturity in many areas of RTI that enables AI models to be used as a powerful and supportive research tool. The new and currently increasingly important domain of 'prompt engineering' plays a central role here, as the type and quality of the results can be influenced and optimised to the requirements of the researchers through targeted interaction with the LLM.

As part of the 'KI.DI.COM' exploratory project, the application potential and scenarios of LLM and prompt engineering are to be investigated using exemplary elements of future aeronautical communication (Future Communications Infrastructure, FCI) and the associated end systems for air traffic control, airlines and aircraft. Using FCI, ATC controller workstations, airline dispatch and aircraft avionics are integrated into an overall network via the radio interface and the aeronautical telecommunications network. In this deployment scenario, exemplary questions are prompted with the help of AI and LLM deployment, solutions are developed and these are evaluated with currently known implementations using a multidimensional scale. In particular, the focus is on the presentation of an X.25-based ATN demonstrator and the development of cyber attack scenarios on a modern IP system as used in FCI. Based on the working hypothesis that an LLM is a valid design tool in the field of air traffic control technology, the following research questions (RQ) are investigated: RQ.1 deals with prompt engineering and is intended to develop efficient interaction strategies with the LLM. RQ.2 revolves around the question of what quality an AI-generated R&D result can achieve and RQ.3 considers the influence of the LLM used on the result achieved and the question of whether the RTI effort can be significantly reduced by using AI.

The intended result of the exploratory study is a qualitative and quantitative statement as to which technological maturity levels can currently be achieved using AI-driven RTI in the field of air traffic control technology and avionics. The aim is also to answer the question of whether an open source-based LLM can achieve comparable results to a commercial implementation. By working on three questions of the FCI at different levels of abstraction, the significance of the analysis is to be increased and generalised. The results of the exploratory work are to be continued as part of a co-operative R&D project in the field of cyber security for future aeronautical communications.

Projektpartner

- FH JOANNEUM Gesellschaft mbH