

KI-GESTÜTZTER ENTWURF UND CYBERSECURITY-ANALYSE EINES 'DIGITAL TWINS' AM BEISPIEL FUTURE COMMUNICATIONS INFRASTRUCTURE

H. Flühr, A. Ciobîcă, A. P. Dacumos, D. Koren¹, K. Gebeshuber, M. Pamsl, S. Rappl²

¹ Institut Luftfahrt/Aviation, ² Institut Informatik und Künstliche Intelligenz,
FH JOANNEUM, 8020 Graz, Österreich

Zusammenfassung

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 ATN-Demonstrators sowie die Entwicklung von Cyber-Angriffsszenarien auf ein modernes IP-System, wie sie bei FCI zum Einsatz kommen.

Keywords

Flugsicherungstechnik; Künstliche Intelligenz; Cyber-Sicherheit; ATN/OSI; FCI; LLM; Prompt Engineering

1. EINLEITUNG

Aktuelle Arbeiten aus unterschiedlichsten wissenschaftlichen Disziplinen (exemplarisch seien hier [1],[2],[3],[4] genannt) 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.COM¹ (KI-gestützter Entwurf und Cybersecurity-Analyse eines 'Digital Twins' am Beispiel Future Communications Infrastructure) 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. Das bisher im Schichtmodell der ISO/OSI standardisierte aeronautische Telekommunikationsnetzwerk (ATN/OSI) ist derzeit in einer schrittweisen Übergangsphase in das ATN/IPS [5]. ATN/IPS verwendet die Internet Protocol Suite (IPS), schafft eine zukunftsfähige Kommunikationsplattform und ermöglicht eine bessere Integration moderner Netzwerk- und Kommunikationsdienste. Das ATN/IPS stellt die Grundlage für ein leistungsfähiges und langfristig skalierbares aeronautisches Netzwerk dar.

Im Rahmen der FCI soll die bodenseitige Kommunikationsinfrastruktur durch das NewPENS gebildet werden. Für die Luft-Boden-Kommunikation sind drei komplementäre Datenlinks vorgesehen: AeroMACS, LDACS und SATCOM. Über diese Kommunikationspfade sollen die erforderlichen flugsicherungstechnischen Dienste zuverlässig und interoperabel bereitgestellt werden. FCI integriert dabei ATC-Controllerarbeitsplätze, Airline-Dispatch und die flugzeugseitige Avionik über die Funkschnittstelle und das aeronautische Telekommunikationsnetzwerk hinweg in das ATN/IPS als Gesamtnetzwerk.

¹ Das Projekt KI.DI.COM wird im Rahmen des FTI-Programms Take Off durch das Bundesministerium für Innovation, Mobilität und Infrastruktur gefördert und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt.

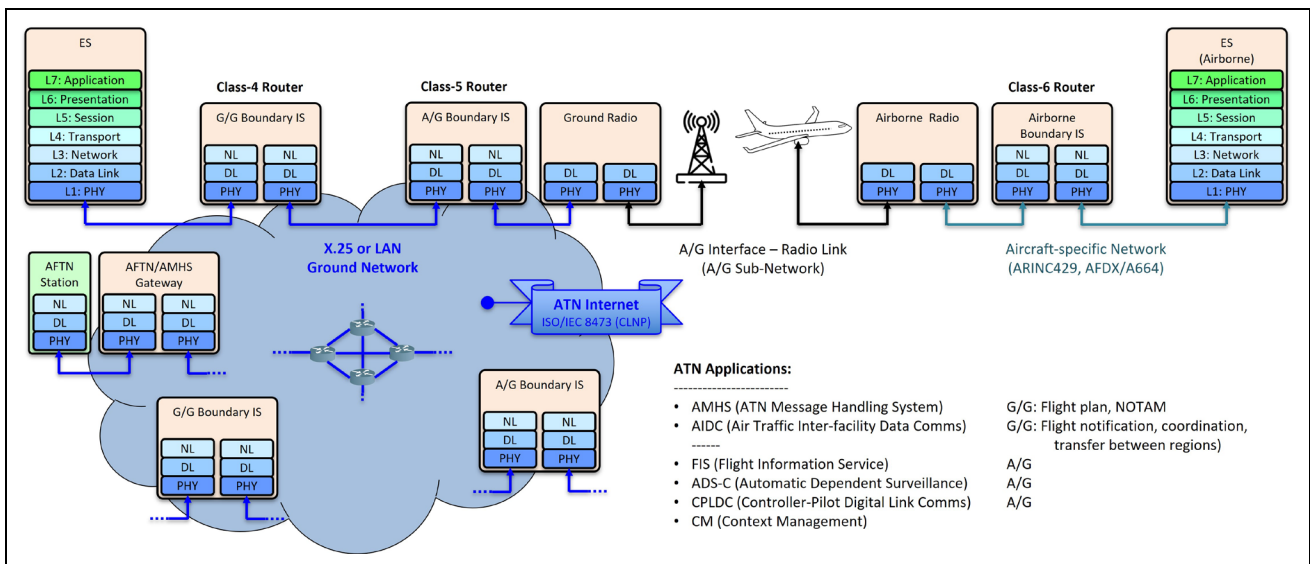


BILD 1. Architektur des aeronautischen Telekommunikationsnetzwerks (ATN) dargestellt im Schichtmodell der ISO/OSI.

In diesem Einsatzszenario werden im Rahmen von KI.DI.COM 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 ATN/OSI-Demonstrators (siehe dazu die ATN/OSI-Übersichtsdarstellung in BILD 1) sowie die Entwicklung von Cyber-Angriffsszenarien auf ein modernes IP-System, wie sie bei FCI zum Einsatz kommen. Im Rahmen des „informierenden Posters“ soll das Sondierungsvorhaben vorgestellt und mit dem Fachpublikum kritisch diskutiert werden.

2. METHODIK

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.

2.1. Große Sprachmodelle (LLM)

RQ.1 behandelt dabei LLM und deren Training anhand von Trainings- und Verifikationsdatensätzen. Welche heute bekannten Closed- und Open-Source LLM sind als Entwicklungstools im Bereich der Flugsicherungs- und IT-Technologie vielversprechend einsetzbar und welche ergänzenden Schnittstellen zu Datenbanken und Programmierertools müssen diese aufweisen?

2.2. Prompt Engineering

RQ.2 behandelt das Prompt Engineering sowie API und soll effiziente Interaktionsstrategien mit dem LLM erarbeiten. Wie können aus dem "Prompt Engineering" abgeleitete Abfragestrategien für nachrichtentechnische Aufgabenstellungen formal beschrieben werden und welche Artefakte sind dabei trotzdem zu beobachten?

2.3. Ergebnisqualität

RQ.3 betrachtet den Einfluss des verwendeten LLM auf die erzielbaren Ergebnisse. Wie unterscheiden sich bei den gewählten Use Cases die AI-basierten Ergebnisse von den mit klassischen Ingenieursmethoden erzielten Lösungen hinsichtlich deren technologischer Reife und bezüglich des Ressourceneinsatzes?

2.4. Anwendung in KI-Feldern

Das Projekt soll für den Entwurf und die Verifikation von Kommunikationssystemen und Netzwerken den unterstützenden Einsatz von KI und LLM sondieren. Für diesen Zweck wird ein aus dem aktuellen Stand des Wissens abgeleiteter digitaler Zwilling erstellt und mit LDACS (für L-Band Digital Aeronautical Communications System) als Funkschnittstelle in ein Simulationsmodell überführt. Parallel wird für drei technologische Fragestellungen auf verschiedenen Abstraktionsebenen eine mittels LLM-Tooleinsatz erstellte Vergleichslösung gepromptet und dem digitalen Zwilling gegenüber gestellt:

- Physical Layer von LDACS im FCI. Die Planung von zellulären Funknetzen und Vorhersage der erzielbaren Funkabdeckung ist aufgrund der komplexen Ausbreitungseigenschaften von elektromagnetischen Wellen bis heute ein zentrales Problemfeld. Kommerzielle Software in Zusammenspiel mit der Verfügbarkeit von Geländemodellen und der Erfahrung des Anwenders sind Schlüsselfaktoren in der Planung von möglichen

Funkstandorten. Use Case (a) ist Referenz für eine AI-Anwendung in der klassischen Flugsicherungstechnik.

- Data Link und Network Layer des ATN/OSI. Die formale Beschreibung von Netzwerken anhand derer Kernspezifikationen ist Use Case für eine abstrakte Anwendung von KI-Tools in der Technologie von Netzwerken und Routern. Aufgrund der Nähe zu formalen Beschreibungssprachen hebt sich (b) im Abstraktionsgrad deutlich vom vorherigen Anwendungsfeld ab und zeigt ein großes Potenzial für den LLM-Einsatz.
- Cyber-Security von IP-Systemen. Die missbräuchliche Verwendung von KI im Bereich der IT, etwa zur Erstellung realitätsnaher Phishing-Mails ist bekannt. Use Case (c) geht in seiner Komplexität darüber hinaus und soll untersuchen, inwieweit komplexe und automatisierte Attacken auf aeronautische Computernetzwerke geplant und erstellt werden können. Er ist somit der abstrakteste der drei beschriebenen Anwendungsfelder.

Die für die Erreichung der angestrebten Innovationen zu überwindenden Herausforderungen sind vielschichtig:

- Hohe Dynamik im Bereich der KI. Die momentan hohe Dynamik in der Weiterentwicklung der LLM - nicht zuletzt bedingt durch den Erfolg von ChatGPT und deren Entwickler openAI - erfordern eine sorgfältige Beobachtung des Sektors, um nicht den Anschluss an die aktuelle Forschung zu verlieren.
- Interaktion von Software- und Hardware-Modellen in der Simulation. Zwar ist die Methodik der Co-Simulation, dem Einsatz eines Simulationswerkzeugs im Designflow einer übergeordneten Toolkette oder mit Embedded-Hardware/Hardware-in-the-Loop bekannt, jedoch liegen in diesem Bereich nur geringe Erfahrungen zum Einsatz künstlicher Intelligenz vor.
- Training- und Verifikationsdaten, Trainingsstrategien. Eine weitere Herausforderung ist der Umstand, wie ein LLM trainiert wird: Anhand von umfangreichen Trainings- und in weiterer Folge Verifikationsdatensätzen und Ziel-Ausgaben wird das künstliche neuronale Netzwerk trainiert. Mit unterschiedlichen Ansätzen wie Backpropagation oder "Reinforcement Learning from Human Feedback" (RLHF) werden dessen Parameter adaptiert, um eine gewünschte Ausgabe zu erzielen.

3. ERWARTETE ERGEBNISSE

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 auf Open Source basierende 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.

4. LITERATUR

- [1] all-electronics: Mit künstlicher Intelligenz die Elektronikfertigung weiter vorantreiben, Hühthig Medien GmbH, zuletzt abgerufen am 12.02.2024. <https://www.all-electronics.de/elektronik-fertigung/mit-kuenstlicher-intelligenz-die-elektronikfertigung-weiter-vorantreiben-858.html>
- [2] Robert Bosch GmbH: Bosch Forschungsprojekte zum Einsatz von Künstlicher Intelligenz (KI) in der Fertigung, zuletzt abgerufen am 12.02.2024. <https://www.bosch.com/de/forschung/forschungsschwerpunkte/automatisierung/forschung-zu-industriellerautomatisierung/bosch-forschungsprojekte-zum-einsatz-von-kuenstlicher-intelligenz-ki-in-der-fertigung/>
- [3] Emha Abdillah, R., Moenaf, H., Fadullah Rasyid, L., Achmad, S., und Sutoyo, R., „Implementation of Artificial Intelligence on Air Traffic Control - A Systematic Literature Review“, 18th International Conference on Ubiquitous Information Management and Communication (IMCOM), Kuala Lumpur, Malaysia, 2024. <https://doi.org/10.1109/IMCOM60618.2024.10418350>
- [4] Plsek, Florian: Künstliche Intelligenz in der Flugsicherung: Status Quo, Potenziale und Herausforderungen, Graz, 2025. (Case Study im Rahmen des ATM-Masterlehrgangs der FH JOANNEUM, unveröffentlicht)
- [5] Internationale Zivilluftfahrtorganisation: Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocol, ICAO Document 9896, 2015.

Kontaktadresse:

holger.fluehr@fh-joanneum.at