Kurzfassung des Abschlussberichtes

zum Vorhaben 6G-CAMPUS

Effiziente und sichere 6G-Industrie-Campusnetze

mittels KI-gestützter Joint-Communication-&-Sensing-Verfahren

NXP Semiconductors Germany GmbH, FKZ 16KISK190K

Die Entwicklung von 6G-Technologien gewinnt weltweit an Dynamik. In der industriellen Praxis rückt dabei zunehmend die Frage in den Vordergrund, wie sich leistungsfähige Funkkommunikation in Campusnetzen sicher, wirtschaftlich und mit offenen Schnittstellen betreiben lässt. Industrielle Campusnetze sollen nicht nur eine robuste Datenübertragung bereitstellen, sondern auch campusspezifische Mehrwertfunktionen ermöglichen, etwa präzise Lokalisierung, digitale Zwillinge von Produktionsumgebungen, zeitkritische Steuerkommunikation oder radarähnliche Umfelderfassung.

Das Vorhaben 6G-CAMPUS adressierte diese Herausforderungen mit dem Ziel, eine 3GPP-kompatible, funktional reduzierte und kostenoptimierte Ende-zu-Ende-Architektur für industrielle 6G-Campusnetze zu entwickeln. Im Zentrum standen offene Schnittstellen (OpenXG-Ansatz) zur Steuerung und Erweiterung von Funk- und Kernnetzfunktionen, die Integration heterogener Funktechnologien sowie die Einbettung zusätzlicher Industriefunktionen.

Die Beiträge von NXP konzentrierten sich auf die technische Machbarkeit und Demonstration zentraler Bausteine. Dabei wurden sowohl prototypische Hardwarekomponenten als auch softwareseitige Erweiterungen entwickelt und in Demonstratoren in realitätsnahen industriellen Szenarien evaluiert.

Systemarchitektur und Schnittstellendefinition: Non-3GPP Integration. Ein Schwerpunkt von NXP war die gezielte Weiterentwicklung vorhandener Funkbausteine, um deren Einsatz im 3,7-GHz-Campusband zu ermöglichen. Gemeinsam mit R3 Solutions entwickelte NXP einen Frequenzmischer, der das Ausgangssignal bestehender WiFi-Hardware (2,4 GHz) in das lizenzierte 3,7-GHz-Band umsetzt. Dadurch steht eine praxisnahe, kosteneffiziente Lösung zur Verfügung, um etablierte WiFi-basierte Systeme ohne grundlegende Hardware-Neuentwicklung in lizenzierten Frequenzen zu betreiben. Die erforderlichen Schaltpläne und Layouts wurden erarbeitet, PoC-Boards gefertigt und in Betrieb genommen.

Joint Communication and Sensing (JC&S) in industrieller Umgebung Im Kontext von JC&S erarbeitete NXP eine durchgängige Machine-Learning-Pipeline für vorverarbeitete Radar-Heatmaps aus realen industriellen Szenarien. Auf Basis eines One-Class-SVM-Ansatzes wurde eine Anomalieerkennung umgesetzt, die Normalzustände von abweichenden Mustern unterscheidet und so potenziell sicherheitsrelevante Aktivitäten identifizieren kann. Der Workflow von Datenakquisition über Vorverarbeitung bis zur Inferenz wurde auf NXP i.MX-Hardwareplattformen realisiert und hinsichtlich Echtzeitnähe und Ressourceneffizienz untersucht. Zusätzlich wurde ein KI-Modell auf einem i.MX9-Prozessor demonstriert; damit wurde die grundsätzliche Eignung moderner Embedded-KI für kontinuierliche Auswertung direkt am Netzwerkrand belegt. Die lokale Verarbeitung reduziert Kommunikationsaufwand und ermöglicht kurze Reaktionszeiten sowie hohe Systemautonomie.

Netzwerksteuerung mit KI-Methoden: Ziel war die Erweiterung des 5G Software-Stacks der Small Cell zur Unterstützung von OpenXG-Funktionen wie Frequenzwechsel, Bandbreitenanpassung und Slot-Konfiguration. Die Integration in die Campusnetz-Architektur erfolgte gemeinsam mit Vicinity Technologies und MECSware und wurde im Demonstrator erfolgreich gezeigt. Notwendige Anpassungen der Hardware für eine dynamische Umkonfiguration während des Betriebes wurden identifiziert und können in zukünftigen Versionen einfließen.

Sicherheit und Authentifizierung: NXP leitete eine umfassende Sicherheitsanalyse des JC&S-Anwendungsfalls unter Verwendung der STRIDE-Methodik und nutzte ergänzend DREAD zur Risikopriorisierung. In Workshops wurden konkrete Bedrohungen identifiziert, bewertet und Gegenmaßnahmen abgeleitet. Darüber hinaus wirkte NXP an der wissenschaftlichen Arbeit „Physical Layer Authentication within 6G Campus Networks“ mit und brachte einen aktiven PLA-Ansatz ein, bei dem Wasserzeichen über geheime Schlüssel in Phasenoffsets von OFDM-Symbolen eingebettet werden. Simulationen und Messungen zeigten, dass unter geeigneten SNR-Bedingungen eine effektive Authentifizierung erreichbar ist; das Ergebnis wurde als Poster auf der EuCNC & 6G Summit 2025 präsentiert.

Konzeptnachweis (PoC) und Aufbereitung der Ergebnisse:

Im Projekt wurden zwei zentrale Demonstratoren für das 6G-Campus-Konzept entwickelt: ein Network-of-Networks-Demonstrator zur KI-gestützten Steuerung heterogener Netzkomponenten sowie ein JC&S-Demonstrator, der mittels Radar-Heatmaps die Umgebungswahrnehmung und Anomaliedetektion zeigt. NXP steuerte dafür wesentliche Komponenten wie eine OpenXG-konforme Small Cell, den WiFi-Mischer für das Campusband und i.MX-Plattformen für Embedded-KI bei. Zur übergreifenden Ergebniskommunikation organisierte NXP zudem ein Video, das die Demonstrator-Ergebnisse auch außerhalb der industriellen Vorführumgebung sichtbar macht.

Die Arbeiten wurden in enger Zusammenarbeit mit den Projektpartnern umgesetzt: Mit R3 Solutions erfolgten Entwicklung, Layout und Inbetriebnahme der Mischer-Hardware; mit MECSware wurden Integrationspunkte zur Campusnetz-Softwarearchitektur und zur Core-basierten Steuerung abgestimmt und demonstriert. Im Bereich Machine Learning wurden geeignete Modellansätze gemeinsam mit Merantix Momentum evaluiert; zudem stellte NXP der RPTU Evaluation Kits mit i.MX 8M Plus Prozessoren zur Analyse KI-basierter Ressourcenverteilung zur Verfügung. Im Sicherheitsbereich wurde die PLA-Publikation gemeinsam mit PHYSEC und RPTU erarbeitet.

In Summe belegen die Ergebnisse aus NXP-Sicht die technische Umsetzbarkeit offener, industriefokussierter Campusnetz-Konzepte. Erstens zeigt die 3,7-GHz-Integration über den Frequenzmischer einen realistischen Weg, kosteneffizient vorhandene Funktechnologie in lizenzierte Campusfrequenzen zu überführen. Zweitens demonstriert die Edge-KI-Pipeline auf i.MX-Plattformen das Potenzial, JC&S-basierte Auswertung und Anomalieerkennung direkt am Netzwerkrand zu realisieren, mit kurzen Reaktionszeiten und reduziertem Backhaul-Bedarf. Drittens ermöglicht die OpenXG-fähige Weiterentwicklung der Small-Cell-Plattform eine zentral orchestrierte, dynamische Konfiguration und ebnet den Weg zu adaptiven Funknetzen, die sich an industrielle Prozesse anpassen. Flankiert wird dies durch Security-by-Design: methodisch fundierte Bedrohungsanalyse sowie neuartige Physical-Layer-Authentifizierung als zusätzliche Schutzschicht für zukünftige 6G-Systeme. Damit trägt das Vorhaben zur technologischen Souveränität bei und schafft eine belastbare Grundlage für die sichere Einführung von 6G-Campusnetzen in der Industrie.