Abschlussbericht zum Vorhaben

6G-CAMPUS

Effiziente und sichere 6G-Industrie-Campusnetze

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

Zuwendungsempfänger: **NXP Semiconductors Germany GmbH**	Förderkennzeichen: FKZ 16KISK190K
Teilvorhaben: Sichere und zuverlässige Hardware-Plattformen für industrielle 6G-Campusnetze	
Projektleiter: **Dr. Christian Fellenberg**	Tel: +49 160 96237827 E-Mail: christian.fellenberg@nxp.com
Laufzeit des Vorhabens: **Von: 01.09.2022**	**bis: 31.12.2025**
Berichtszeitraum des Vorhabens: **Von: 01.09.2022**	**bis: 31.12.2025**

NXP Semiconductors Germany GmbH

Erstellt am 18.05.2026

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Abbildungsverzeichnis 3
1 Kurze Darstellung der Voraussetzungen, unter denen das Projekt begonnen wurde 4
1.1 Voraussetzungen 4
1.2 Wissenschaftliche und/oder technische Arbeitsziele des Vorhabens 4
1.3 Stand der Wissenschaft und Technik 4
1.4 Planung und Ablauf des Vorhabens 5
1.5 Zusammenarbeit mit anderen Stellen 5
1.6 Ergebnisse des Gesamtvorhabens aus Sicht von NXP 6
2 Eigehende Darstellung der Vorhabensergebnisse 7
2.1 Arbeitspaket 1: Management und Technische Koordination 7
2.2 Arbeitspaket 2: Anforderungsanalyse und Spezifikation der Key Performance Parameters 7
2.3 Arbeitspaket 3: Systemarchitektur und Schnittstellendefinition 8
2.4 Arbeitspaket 4: Joint Communication and Sensing (JC&S) in industrieller Umgebung 9
2.5 Arbeitspaket 5: Netzwerksteuerung mit KI-Methoden 12
2.6 Arbeitspaket 6: Sicherheit und Authentifizierung 14
2.7 Arbeitspaket 7: Konzeptnachweis (PoC) und Aufbereitung der Ergebnisse 19
Referenzen 20

Abbildungsverzeichnis

Abbildung 1: Radar-Heatmap 10
Abbildung 2: i.MX 9 Prozessor für JC&S Demonstrator. 11
Abbildung 3: Proof-of-Concept-Board 12
Abbildung 4: Komponenten Integrated Small Cell (ISC) 13
Abbildung 5: Erfolgreiche Authentifizierung in Abhängigkeit des Phasenoffsets 15
Abbildung 6: Ableitung der STRIDE-Entitäten für den JC&S Anwendungsfall 17

1 Kurze Darstellung der Voraussetzungen, unter denen das Projekt begonnen wurde

1.1 Voraussetzungen

Die Entwicklung von 6G-Technologien gewinnt weltweit an Dynamik, wobei der Fokus bisher stark auf öffentlichen Netzen liegt. Der Ausbau industrieller Campusnetze gewinnt insbesondere in Deutschland zunehmend an Bedeutung und rückt verstärkt in den strategischen Fokus. Diese Netze bieten Unternehmen die Chance, sichere, adaptive und effiziente Kommunikation innerhalb ihrer Liegenschaften zu realisieren, wobei industriespezifische Funktionen wie präzise Lokalisierung, digitale Zwillinge oder Radar-ähnliche Sensorik integriert und dynamisch an betriebliche Abläufe angepasst werden können. Aktuelle Mobilfunklösungen sind für diesen Zweck jedoch ungeeignet: Sie sind kostenintensiv, überdimensioniert und bieten keine offenen Schnittstellen für industrielle Zusatzfunktionen. Das Projekt 6G-CAMPUS setzt genau hier an. Ziel ist die Entwicklung neuer 3GPP-kompatibler Komponenten und Architekturen, die durch den Verzicht auf unnötige Funktionen und die Integration industrierelevanter Erweiterungen deutlich kosteneffizienter und nutzerfreundlicher sind. Damit soll ein neues Marktsegment für europäische Anbieter erschlossen werden, der technologisch souverän und wirtschaftlich attraktiv ist. Die Vision ist die Schaffung einer zukunftsweisenden, offenen und sicheren 6G-Campusnetz-Technologie, die speziell auf die Anforderungen industrieller und institutioneller Campusumgebungen zugeschnitten ist.

1.2 Wissenschaftliche und/oder technische Arbeitsziele des Vorhabens

Im Projekt 6G-CAMPUS wurden innovative Lösungen für industrielle 6G-Campusnetze entwickelt, die Sicherheit, Effizienz und neue Funktionalitäten vereinen. Ein Schwerpunkt lag auf Joint Communication and Sensing (JC&S), das eine gleichzeitige Datenübertragung und Umgebungserfassung ermöglicht. Dafür wurden neue Wellenformen und Signalverarbeitungsverfahren entworfen, ergänzt durch KI-Methoden zur Erstellung digitaler Zwillinge für Anwendungen wie Navigation, Kollisionsvermeidung und Prozessoptimierung. Parallel wurden umfassende Sicherheits- und Authentifizierungskonzepte umgesetzt. Dazu zählen hardwarebasierte Mechanismen, sichere UICC-Komponenten mit virtuellen eSIMs sowie Physical-Layer-Security-Ansätze zur Manipulationserkennung. Ergänzend wurden Verfahren zur Tamper-Detection und KI-gestützten Anomalieerkennung integriert, um die Resilienz in verteilten Netzarchitekturen zu erhöhen. Die entwickelte OpenXG-Architektur bietet eine 3GPP-kompatible, reduzierte Ende-zu-Ende-Lösung mit offenen Schnittstellen für Zusatzfunktionen wie Device-to-Device-Kommunikation und KI-basierte Netzsteuerung. Alle Komponenten wurden in realen industriellen Szenarien demonstriert und evaluiert. Damit trägt das Projekt entscheidend zur technologischen Souveränität bei und schafft die Grundlage für die sichere Einführung von 6G in der Industrie.

1.3 Stand der Wissenschaft und Technik

Der aktuelle Stand der Technik zeigt, dass bestehende Mobilfunklösungen für industrielle Campusnetze oft ungeeignet sind. Kommerzielle 3GPP-Systeme sind komplex, proprietär und auf öffentliche Netzbetreiber zugeschnitten. Für kleine und mittlere Unternehmen (KMU) stellt dies eine erhebliche Hürde dar. Zudem fehlt ein offenes Ende-zu-Ende-Managementmodell, das Core

Network, Radio Access Network und Endgeräte integriert. Im Bereich Sicherheit existieren keine einheitlichen Standards für Netzwerkauthentifizierung in privaten Netzen. Stattdessen dominieren Insellösungen mit begrenzter Fernwartungsfähigkeit. Auch die Hardware-Sicherheit ist unzureichend: Schutz vor Manipulationen ist teuer oder technisch nicht ausgereift. Die Integration von zellulären 3GPP- und WLAN-Technologien ist bislang nur konzeptionell vorhanden. Die Wireless Broadband Alliance hat erste Architekturvorschläge gemacht [WBA2021], jedoch ohne konkrete Implementierungen. Zukünftige 6G-Netze sollen JC&S-Funktionalitäten bieten, die über die Ortungsfähigkeiten von 4G/5G hinausgehen. Dafür sind höhere Frequenzbereiche wie Millimeterwellen und Terahertz notwendig, die präzisere Umgebungswahrnehmung ermöglichen [Sedunova2021]. Das Projekt 6G-CAMPUS adressiert diese Lücken mit dem OpenXG-Ansatz: einer offenen, abstrahierten API, die Komplexität reduziert, Sicherheit erhöht und die Integration heterogener Technologien ermöglicht, speziell für industrielle Anwendungen.

1.4 Planung und Ablauf des Vorhabens

Das Projekt 6G-CAMPUS wurde unter Leitung von NXP Semiconductors Germany GmbH durchgeführt. Um die bestmögliche Zusammenarbeit zu gewährleisten, wurde der Ablauf des Projekts durch folgende Arbeitsstrukturen bestimmt:

- Regelmäßige (halbjährliche) Projekttreffen mit allen Projektteilnehmern.
- Regelmäßige (monatliche) Telefonkonferenzen zur Klärung des weiteren Vorgehens.
- Regelmäßige (monatliche) Telefonkonferenzen innerhalb der einzelnen Arbeitspakete.
- Workshops einzelner Arbeitspakete zur detaillierten technischen Abstimmung.
- Spontane Treffen oder Telefonkonferenzen sobald einzelne technische Punkte zwischen Partnern geklärt werden mussten.

Aufgrund einer bewilligten Laufzeitverlängerung wurde die ursprünglich vorgesehene Projektlaufzeit vom 01.09.2022 bis 31.08.2025 auf den 31.12.2025 verlängert. Die Arbeiten und Demonstratoraktivitäten wurden entsprechend im verlängerten Zeitraum abgeschlossen.

1.5 Zusammenarbeit mit anderen Stellen

Im Rahmen des Projekts arbeitete NXP intensiv mit mehreren Partnern zusammen, um verschiedene Arbeitspakete erfolgreich umzusetzen:

- R3 Solutions war ein zentraler Partner bei der Hardwareentwicklung für Arbeitspaket 3 und 5. Gemeinsam mit NXP wurden Schaltpläne und Layouts für einen Mischer erstellt und die Inbetriebnahmen der gefertigten Proof-of-Concept-Boards erfolgreich durchgeführt.

- Für die Integration der Small Cell basierend auf NXP Hardware in die Campusnetz-Softwarearchitektur wurde in enger Kooperation mit MECSware Anpassungen des Interfaces vorgenommen. Die erfolgreiche Integration wurde durch einen Demonstrator mit Small-Cell-Steuerung durch die MECSware Plattform demonstriert.

- Im Bereich Machine Learning (Arbeitspaket 4) führte NXP Analysen eigener Hardware durch und stimmte sich eng mit dem Projektpartner Merantix Momentum ab, um geeignete Modelle auszuwählen.

- Für Arbeitspaket 5 stellte NXP der RPTU zwei Evaluation Kits mit i.MX 8M Plus Prozessoren zur Verfügung. Die RPTU analysierte diese Hardware hinsichtlich ihrer Eignung für KI-basierte Ressourcenverteilung, unterstützt durch NXP.

- In Arbeitspaket 6 hat NXP bei der wissenschaftlichen Publikation zur „Physical Layer Authentication within 6G Campus Networks“ mitgewirkt. Das Paper zu innovativen PLA-Verfahren erfolgte in Zusammenarbeit mit PHYSEC und der RPTU. Das gemeinsame Paper wurde als Poster auf der EuCNC & 6G Summit 2025 in Poznan, Polen präsentiert [Weinand2025].

- Zusätzlich leitete NXP eine umfassende Sicherheitsanalyse der Campusnetze aller Partner basierend auf der STRIDE-Methodik für den JC&S Anwendungsfall.

1.6 Ergebnisse des Gesamtvorhabens aus Sicht von NXP

Das Projekt 6G-CAMPUS kann aus Sicht von NXP trotz leichter Verzögerungen im Gesamtprojekt als voller Erfolg gewertet werden. Die wesentlichen Ergebnisse aus Sicht von NXP sind:

- Analyse industrieller Anwendungsfälle für Campusnetze und Ableitung der Sicherheitsanforderungen
- Entwicklung eines Mischers, der die Funkkommunikation von WiFi-Hardware im 3,7-GHz-Campusband erlaubt. Präsentation des Mischers auf der Hannover-Messe 2024 und der Berlin 6G-Konferenz. Entwicklung eines Demonstrators.
- Entwicklung und Implementierung einer vollständigen echtzeitfähigen Machine-Learning-Pipeline für vorverarbeitete Radar-Heatmaps, die in realen industriellen Szenarien aufgenommen werden. Entwicklung eines Demonstrators.
- Erweiterung des Small-Cell Software Stack um Funktionalitäten der OpenXG-API zu unterstützen. Identifikation von Hardwareanpassungen, die eine schnelle und dynamische Umkonfiguration ermöglichen und bei Bedarf in zukünftige Hardwareversionen übernommen werden können. Entwicklung eines Demonstrators.
- Sicherheitsanalyse des JC&S Anwendungsfall basierend auf der STRIDE-Methodik.
- Zwei Veröffentlichungen zu 6G-CAMPUS
    - A. Weinand; A. Hasani, A. Ahmad, S. B. Mallikarjun; J. Wilking, M. Hafner, J. V. Gomez, H. Master; H. D. Schotten, „Physical Layer Authentication Within 6G Campus Networks“, 2025 EuCNC & 6G Summit
    - German Perspective on 6G - Use Cases, Technical Building Blocks and Requirements, Insights by the 6G Platform Germany, White Paper

2 Eingehende Darstellung der Vorhabensergebnisse

2.1 Arbeitspaket 1: Management und Technische Koordination

Das Projekt 6G-CAMPUS wurde unter Leitung von NXP Semiconductors Germany GmbH durchgeführt. Diese umfasste unter anderem folgende Punkte:

- Planung und Durchführung des Kick-Off Meetings bei NXP in Hamburg
- Koordination der Ausarbeitung des Kooperationsvertrags
- Regelmäßige (monatliche) Telefonkonferenzen zur Klärung des weiteren Vorgehens
- Planung und Leitung der Konsortialtreffen
- Bereitstellung von Meilensteinen und Dokumentation des Projektfortschritts
- Koordination der Beiträge aller Partner zu den 6G-Konferenzen in Berlin
- Koordination der Beiträge zum Whitepaper „German perspective on 6G“
- Koordination der Erstellung eines Videos mit den Ergebnissen des Projektes

2.2 Arbeitspaket 2: Anforderungsanalyse und Spezifikation der Key Performance Parameters

NXPs Beiträge in Arbeitspaket 2 lagen im Wesentlichen in Aufgabe T-AP 2.3 „KPI & Maßnahmen Definitionen: Sicherheit & Authentifizierung“.

2.2.1 T-AP 2.3: KPI & Maßnahmen Definitionen: Sicherheit & Authentifizierung

Im Rahmen des zweiten Arbeitspakets wurden zwei zentrale Use Cases im Kontext eines 6G-basierten Campusnetzwerks eingebracht, die sich mit der nahtlosen Integration unterschiedlicher Funktechnologien sowie der sicheren Einbindung neuer Geräte befassen.

Use Case 1: Nahtloses Handover zwischen WiFi und 6G

Dieser Use Case adressiert die Herausforderung, in einem heterogenen Campusnetzwerk mit verschiedenen Funkzugangstechnologien – insbesondere WiFi und 6G – einen unterbrechungsfreien Übergang zwischen diesen Technologien zu ermöglichen. In heutigen Netzwerken entscheidet das Endgerät selbst über die zu verwendende Funktechnologie, was beim Wechsel zu einer anderen RAT (Radio Access Technology) zu einer Trennung der Verbindung und einem Neuaufbau führt. Dies bringt IP-Adressänderungen und QoS-Einbußen mit sich.

Im angestrebten 6G-Campusnetz übernimmt die Netzwerkintelligenz im 6G-Core die Verwaltung der Kommunikationsressourcen. Ziel ist es, einen nahtlosen Übergang zwischen WiFi und 6G zu gewährleisten, bei dem aktive Datenverbindungen erhalten bleiben und die Identifikation sowie die Qualität der Verbindung (QoS) gesichert sind. Der Ablauf sieht vor, dass ein Endgerät eine Datenübertragung startet und sich zwischen WiFi- und 6G-Abdeckungsbereichen bewegt. Die Campusnetzwerkintelligenz initiiert daraufhin den Handover, der ohne Unterbrechung erfolgt.

Die Systemanforderungen beinhalten, dass sowohl WiFi als auch 6G dem Campusnetzbetreiber gehören müssen. Die Steuerung des Roamings und der Richtlinien erfolgt über die Campusnetzwerkintelligenz (OpenXG). Technisch wird eine Datenrate von 100 Mbit/s bis 1 Gbit/s

sowie eine Latenz von 10–50 µs angestrebt. Nutzerseitig handelt es sich um „Data Only“-Geräte, wobei optional auch Notfall- und kritische Verbindungen berücksichtigt werden können. Als Maßnahme wird die Entwicklung von Richtlinien für die Netzwerkintelligenz sowie die Sicherstellung der eindeutigen Identifikation der Endgeräte genannt.

Use Case 2: Sichere Provisionierung und Onboarding von vorvertrauenswürdigen Geräten

Der zweite Use Case befasst sich mit der sicheren Einbindung neuer Geräte in ein privates Campusnetzwerk. In sicheren Netzwerken muss jedes Kommunikationsgerät dem 6G-Core bekannt sein, wobei die Identifikation über die SIM-Karte erfolgt. Während in öffentlichen Netzen der Netzbetreiber Zugriff auf den privaten Schlüssel der SIM hat, ist dieser in privaten Campusnetzen ausschließlich dem Gerätehersteller bekannt. Daraus ergibt sich die Notwendigkeit, einen sicheren Weg zu schaffen, wie Betreiber von Campusnetzen Geräte vertrauenswürdig „onboarden“ können – auch wenn deren SIMs nicht vorab bekannt sind.

Ziel ist es, neue Geräte zu erkennen, eine initiale Vertrauensbasis zu schaffen und eine sichere Kommunikation zwischen Campusnetz und Gerätehersteller zu etablieren. Der Ablauf beginnt mit einer Zugriffsanfrage eines neuen Geräts. Der Core prüft, ob das Gerät bekannt ist, und fragt bei vertrauenswürdigen Herstellern nach. Bei positivem Abgleich erfolgt die Provisionierung, wobei Authentifizierungsdaten und Schlüssel generiert werden. Das Gerät wird anschließend zur Liste der bekannten Geräte hinzugefügt und erhält Zugang zum Netzwerk.

Die Systemanforderungen beinhalten die Verfügbarkeit einer Liste neuer, noch nicht provisionierter Geräte, die Möglichkeit zur Provisionierung von USIM-Informationen sowie die Fähigkeit des Campusnetzes, vertrauenswürdige Hersteller zu identifizieren. Hersteller müssen ihrerseits sichere Provisionierungsportale bereitstellen. Nutzerseitig muss das Gerät einem vertrauenswürdigen Hersteller zugeordnet sein, und die Anfrage zur Provisionierung muss an diesen gesendet werden. Als Maßnahme wird die Verbindung zu einem vertrauenswürdigen Server mit Provisionierungsinformationen genannt.

Beide Use-Cases sind nicht in die Umsetzung der Demonstratoren eingeflossen, wurden jedoch in der vorgeschlagenen Architektur der 6G-Campus Netze berücksichtigt.

2.2.2 T-AP 2.4: KPI & Maßnahmen Definitionen: Sicherheit & Authentifizierung

Zusätzlich zu T-AP 2.3 unterstützte NXP im Rahmen von T-AP 2.4 die fortlaufende Bewertung der Systemarchitektur hinsichtlich der definierten Sicherheitsanforderungen und KPIs. Die in AP2 eingebrachten Use Cases dienten dabei als Referenz für Architekturentscheidungen in AP3 sowie für die Bewertung der Sicherheits- und Integrationsaspekte in AP6 und AP7.

2.3 Arbeitspaket 3: Systemarchitektur und Schnittstellendefinition

NXPs Beiträge in Arbeitspaket 3 lagen in T-AP 3.4 „Non-3GPP Integration“.

2.3.1 T-AP 3.4: Non-3GPP Integration

Die Arbeiten im Rahmen von T-AP 3.4 konzentrierten sich auf die Integration sowie die gezielte Weiterentwicklung vorhandener Technologiebausteine, um deren Einsatz im lizenzierten 3,7-GHz-Campusband zu ermöglichen. Ziel war es, bestehende Systemkomponenten so zu

erweitern, dass sie in einem Campusband zuverlässig betrieben und zugleich effizient in übergeordnete Netzarchitekturen eingebunden werden können.

Gemeinsam mit dem Projektpartner R3 Solutions entwickelte NXP hierfür einen Mischer, der den Betrieb vorhandener WiFi-Hardware von R3 Solutions, basierend auf einem NXP-WiFi-Chip für das 2,4-GHz-Band, im 3,7-GHz-Campusband ermöglicht. Der Mischer übernimmt die Frequenzumsetzung und konvertiert das Ausgangssignal von 2,4 GHz auf 3,7 GHz. Damit steht eine praxisnahe und insbesondere kosteneffiziente Lösung zur Verfügung, um etablierte WiFi-basierte Systeme ohne grundlegende Hardware-Neuentwicklung auch in lizenzierten Frequenzbereichen einsetzen zu können.

Ergänzend dazu erfolgte eine enge Abstimmung mit MECSware und der RPTU zur OpenXG-Schnittstelle und deren Integration in einer Small Cell auf Basis von NXP-Hardware, so dass die Steuerung relevanter Netzwerkfunktionen nutzbar gemacht werden kann. Dabei wurden die notwendigen Anforderungen an Schnittstellenlogik, Datenfluss und Steuerinformationen betrachtet, um eine konsistente Einbindung in die Systemlandschaft zu gewährleisten.

In einem Demonstrator konnte schließlich erfolgreich nachgewiesen werden, dass die WiFi-Hardware von R3 in ein Campusnetz integriert und über das 6G-Core-Netzwerk zentral gesteuert werden kann. Das 6G-Core-System von MECSware übermittelt hierzu die erforderlichen Steuerinformationen über die Small Cell und die neu definierte Schnittstelle OpenXG an die WiFi-Komponenten. Damit wurde eine durchgängige Kette von der 6G-Core-basierten Steuerung bis zur WiFi-Funkebene demonstriert und die technische Machbarkeit des Integrationsansatzes im Zielband überzeugend belegt.

Neben der Hardwarelösung zur Frequenzumsetzung wurden die für die Non-3GPP-Integration relevanten Schnittstellen und Steuerflüsse analysiert. Dadurch konnte gezeigt werden, wie heterogene Funkzugangstechnologien über die OpenXG-Architektur in ein gemeinsames Campusnetzmanagement eingebunden werden können.

2.4 Arbeitspaket 4: Joint Communication and Sensing (JC&S) in industrieller Umgebung

NXPs Beiträge in Arbeitspaket 4 lagen in T-AP 4.1 „JC&S-Funktionen und detaillierte Anforderungen“ und T-AP 4.4 „JC&S PHY-/MAC-Layer und Schnittstellen für die Integration in das 6G-Netz“

2.4.1 T-AP 4.1: JC&S-Funktionen und detaillierte Anforderungen

Das Ziel von Arbeitspaket 4 war es, die Machbarkeit von Machine-Learning-basierten Verfahren zur Erkennung von Anomalien in industriellen Umgebungen zu demonstrieren. Der Schwerpunkt von NXP lag dabei nicht auf der Entwicklung neuer JC&S-Wellenformen, sondern auf der Bewertung geeigneter Hardwareplattformen, der Umsetzung der KI-basierten Auswertung am Netzwerkrand sowie der Validierung der Echtzeitfähigkeit auf industrietauglicher Embedded-Hardware. Zu diesem Zweck wurde eine durchgängige ML-Pipeline entwickelt, die auf JC&S-abgeleiteten Sensordaten basiert. NXP nutzte vorverarbeitete Radar-Heatmaps aus realen industriellen Szenarien, um ein One-Class-SVM-Modell zu trainieren, das zwischen

Normalzuständen und abweichenden Mustern unterscheidet, welche auf potenziell unbefugte oder sicherheitsrelevante Aktivitäten hinweisen können (siehe Abbildung 1).

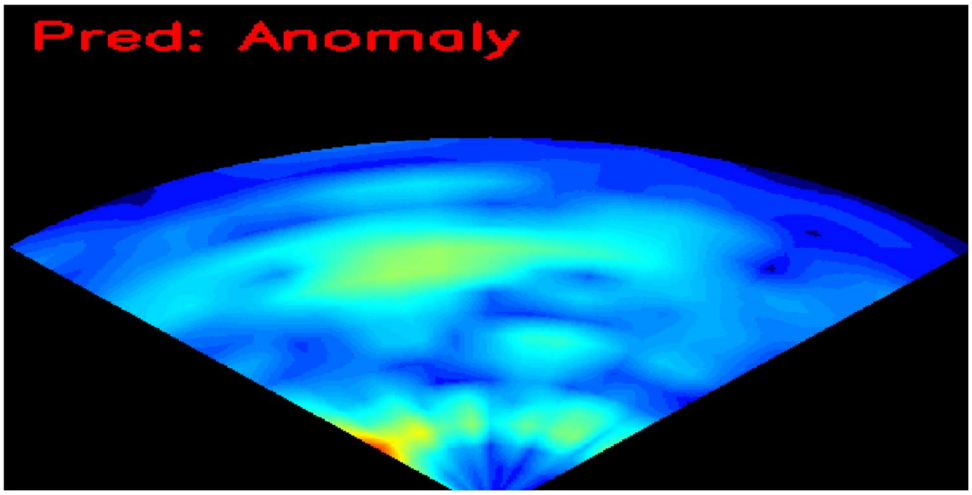

Abbildung 1: Radar-Heatmap

Die entwickelte Pipeline wurde in unterschiedlichen Anwendungsszenarien erprobt und zeigte eine zuverlässige Unterscheidung zwischen normalen und abnormalem Verhalten. Der gesamte Workflow von der Datenakquisition über die Vorverarbeitung bis hin zur Inferenz wurde erfolgreich auf der i.MX-Hardwareplattform von NXP umgesetzt. Dabei wurde die grundsätzliche Kompatibilität mit Embedded-Linux-Systemen sowie die Eignung für eine kontinuierliche, echtzeitnahe Verarbeitung nachgewiesen.

Die Tests lieferten zudem wichtige qualitative Erkenntnisse zur effizienten Nutzung der verfügbaren Hardware-Ressourcen, insbesondere im Hinblick auf die Strukturierung des Datenflusses, die Trennung zeitkritischer und nicht-zeitkritischer Verarbeitungsschritte sowie die Auswahl geeigneter Modell- und Datenparameter für den Einsatz auf Embedded-Systemen.

Darüber hinaus verdeutlicht der entwickelte Demonstrator, wie KI-gestützte Anomalieerkennung als Bestandteil eines ganzheitlichen Sicherheitskonzepts am Netzwerkrand eingesetzt werden kann. Durch die lokale Verarbeitung der Sensordaten auf der i.MX-Plattform werden kurze Reaktionszeiten, ein geringer Kommunikationsaufwand und eine hohe Systemautonomie erreicht. Die visuelle Darstellung der Erkennungsergebnisse unterstützt dabei sowohl die Systementwicklung als auch die spätere Inbetriebnahme in industriellen Umgebungen. Insgesamt unterstreicht der Demonstrator das Potenzial moderner Embedded-KI-Lösungen, Sicherheitsfunktionen effizient, skalierbar und praxisnah umzusetzen.

Die Validierung des Demonstrators auf realer i.MX-Hardware bestätigte die praktische Umsetzbarkeit von ML-basierten Anomalie- und Authentifizierungsverfahren direkt am Netzwerkrand. Gleichzeitig konnten Anforderungen und Randbedingungen für eine mögliche zukünftige Integration von JC&S-basierten Sicherheitsfunktionen in industrielle Embedded-Systeme identifiziert werden. In Abstimmung mit dem Projektpartner Merantix Momentum wurden

geeignete Machine-Learning-Modelle evaluiert, wobei die grundsätzliche technische Machbarkeit der Implementierung auf NXP-Hardware nachgewiesen wurde.

Insgesamt zeigt die Arbeit in Arbeitspaket 4, wie moderne Machine-Learning-Technologien in Kombination mit spezialisierter Hardware die Sicherheit industrieller Netzwerke erhöhen können.

In einem Demonstrator wurde das von Merantix Momentum entwickelte KI-Modell [Mollenhauer2025] erfolgreich auf einem i.MX9 Prozessor für industrielle Anwendung von NXP implementiert, wobei die Echtzeitfähigkeit der Lösung nachgewiesen werden konnte (Abbildung 2).

Abbildung 2: i.MX 9 Prozessor für JC&S Demonstrator.

2.4.2 T-AP 4.4: JC&S PHY-/MAC-Layer und Schnittstellen für die Integration in das 6G-Netz

In diesem Arbeitspaket wurden die in Arbeitspaket 3 erarbeiteten Konzepte konsequent in die Praxis überführt, um den Betrieb von WiFi im lizenzierten 3,7-GHz-Campusband mithilfe eines Mischers zu realisieren. Auf diese Weise wird die bestehende WiFi-Funktechnik um eine Frequenzumsetzung erweitert, sodass sie in einem Campusband genutzt werden kann. Gleichzeitig ermöglicht der Ansatz, relevante Kenngrößen und Zustandsinformationen des PHY-/MAC-Layers über den Übertragungskanal an das 6G-Core-Netzwerk zu übermitteln. Diese Daten können dort zentral erfasst und mittels KI-basierter Verfahren ausgewertet werden, um Störungen, Anomalien und/oder potenzielle Manipulationen frühzeitig zu erkennen und geeignete Gegenmaßnahmen abzuleiten.

In enger Zusammenarbeit mit R3 Solutions erarbeitete NXP die Schaltpläne sowie das Layout des Mischers und initiierte im Anschluss die Fertigung entsprechender Proof-of-Concept-Boards

(Abbildung 3). Damit wurde eine belastbare Hardwarebasis geschaffen, um die Frequenzumsetzung und die Systemintegration unter realitätsnahen Bedingungen zu erproben und iterativ zu optimieren.

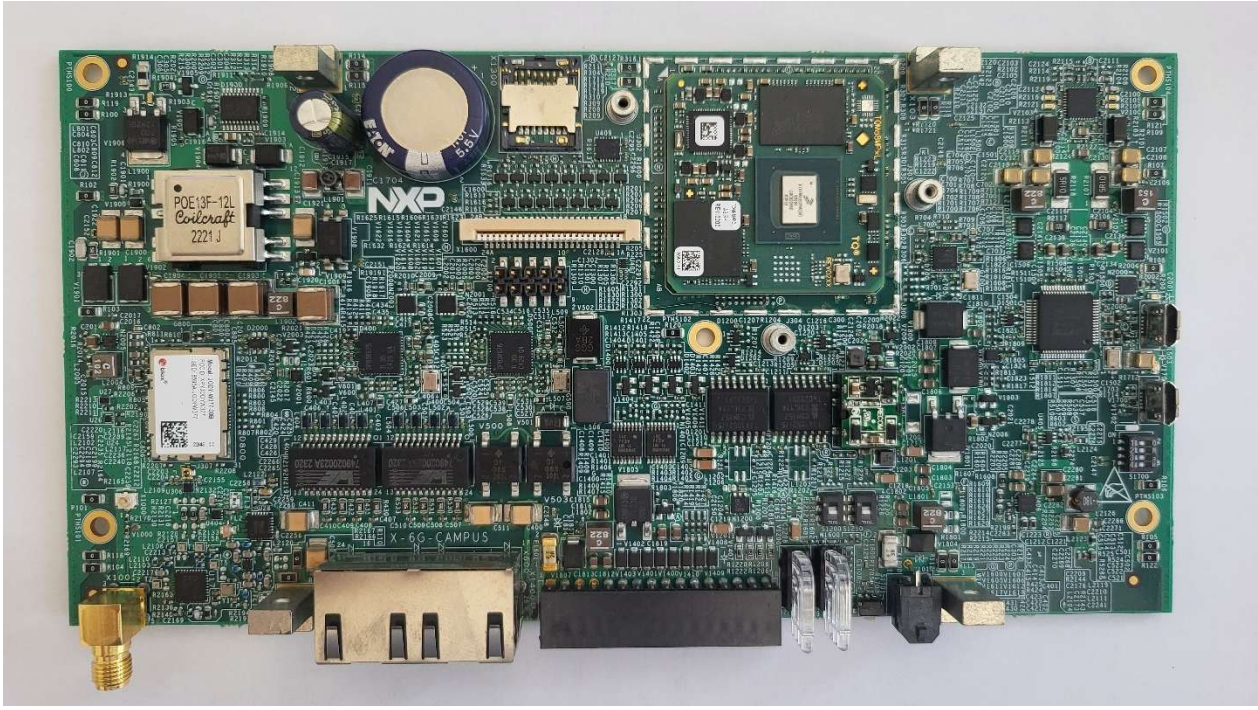

Abbildung 3: Proof-of-Concept-Board

Die entstandenen Prototypen wurden gemeinsam mit R3 Solutions auf der Hannover Messe 2024 präsentiert. Die Inbetriebnahme erfolgte unter der Leitung von R3 Solutions; NXP unterstützte dabei insbesondere bei der Fehlersuche, bei notwendigen Überarbeitungen der Boards sowie durch die Bereitstellung von Messtechnik und Laborressourcen. Hierzu zählte insbesondere die Nutzung des Terahertz-Labors in Hamburg. Auf der 6G-Konferenz in Berlin 2024 konnte schließlich das Sendespektrum erfolgreich demonstriert werden, womit die grundlegende Funktionalität der Lösung und die Eignung für den Einsatz im Campusband eindrucksvoll belegt wurden.

2.5 Arbeitspaket 5: Netzwerksteuerung mit KI-Methoden

NXPs Beiträge in Arbeitspaket 5 lagen in T-AP 5.1 „Entwicklung eines KI-Frameworks inkl. Schnittstellen zur OpenXG API“

2.5.1 T-AP 5.1: Entwicklung eines KI-Frameworks inkl. Schnittstellen zur OpenXG API

Im Rahmen des Arbeitspakets 5 wurden umfangreiche Arbeiten zur Weiterentwicklung und Integration der Small Cell durchgeführt, die auf NXP-Technologie basiert. Die Small Cell nutzt zwei zentrale Komponenten (Abbildung 4):

- Layerscape Access LA122x Baseband-Prozessor - zuständig für die physikalische Verarbeitung der Mobilfunksignale.
- Layerscape LX2160A Host-Prozessor - übernimmt die höheren Protokollschichten, konkret Layer 2 und Layer 3 des 5G-Kommunikationsstacks.

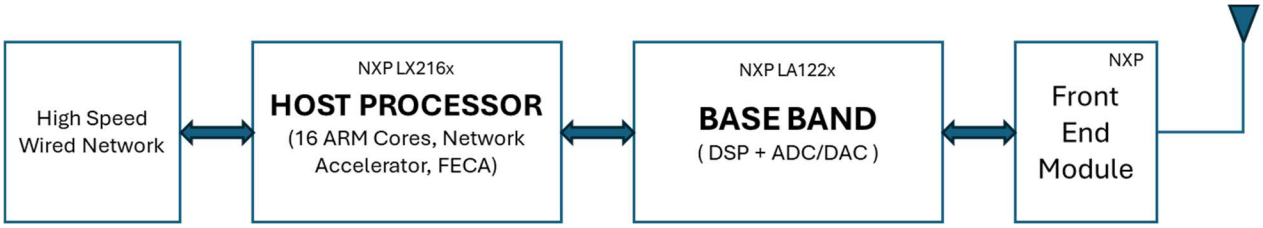

Abbildung 4: Komponenten der Integrated Small Cell (ISC)

Ziel war es, die Funktionalität der Small Cell im Hinblick auf die Unterstützung der OpenXG-API zu erweitern. Die 6G-CAMPUS OpenXG API folgt den O1-Schnittstellenspezifikationen zur Verwaltung von 3GPP-RAN-Komponenten. Während des Projekts wurde ein Kernsatz von Managementfunktionen festgelegt, die für den Betrieb eines Campusnetzwerks erforderlich sind, um die Projektziele zu erreichen:

OXGM → RAN Configuration Functions

- Set Mobile Country Code (MCC)
- Set Mobile Network Code (MNC)
- Set Physical Cell ID (PCI)
- Set Cell Global Identity (CGI)
- Set Frequency Band
- Set Center Frequency
- Set Bandwidth
- Set Transmit Power
- Set DL:UL Ratio
- Set Synchronization Parameters

Dazu wurden spezifische Softwareänderungen implementiert, die unter anderem Funktionen wie Frequenzwechsel, Bandbreitenanpassung und Slot-Konfiguration ermöglichen. Diese Erweiterungen wurden gezielt auf die Anforderungen der definierten Use Cases abgestimmt und in mehreren Testreihen evaluiert.

Für die Einbindung in die bestehende Campusnetz-Softwarearchitektur arbeitete NXP mit dem langjährigen und spezialisierten externen Partner Vicinity Technologies zusammen. In dieser Kooperation wurden die notwendigen Interface-Anpassungen zusammen mit MECSware vorgenommen und dokumentiert, um eine reibungslose Einbindung zu ermöglichen. Die Integration wurde erfolgreich demonstriert, wobei die Steuerung der Small Cell durch MECSware in einem Demonstrator gezeigt wurde. Das übergeordnete Ziel dieser Maßnahme war es, eine europäische Hardwarelösung mit starker deutscher Präsenz in das Projekt einzubringen. Damit

soll die technologische Souveränität Europas im Bereich der 5G-Netzwerktechnologie gestärkt werden.

Während der Tests zeigte sich, dass dynamisches Frequenzumschalten sowie die Rekonfiguration von Frequenzbereichen zu einem Verlust der zeitlichen Synchronisation der Frames führten. In der Folge gingen umfangreiche, zeitkritische Abtastwerte verloren; zudem schlugen aktive Verfahren zur Verbindungswiederherstellung durchgängig fehl. Das System ließ sich erst durch einen vollständigen Neustart der Komponenten der physikalischen Schicht wieder in einen stabilen Betriebszustand überführen. Eine vertiefte Analyse ergab, dass für die zuverlässige Handhabung von Echtzeit-Konfigurationsänderungen im Funkspektrum zusätzliche, spezialisierte Hardwareunterstützung auf den untersten physikalischen Ebenen erforderlich ist. Insbesondere das fehlende Feedback bestimmter Schaltungskomponenten sowie das Ausbleiben von Echtzeit-Informationen zum RX/TX-Pufferstatus erschwerten die korrekte Zustandsführung der Datenwarteschlangen und trugen maßgeblich zur beobachteten Instabilität bei. Als temporäre Lösung wurde ein Mechanismus etabliert, bei dem Module gezielt neu gestartet werden, um veraltete Queues zu bereinigen und die neuen Konfigurationen zuverlässig zu propagieren. Zudem wurden Hardwareanpassungen identifiziert, die eine schnelle und dynamische Umkonfiguration ermöglichen und in zukünftige Hardwareversionen übernommen werden können.

Darüber hinaus stellte NXP der RPTU zwei Evaluation Kits (EVKs) mit i.MX 8M Plus Prozessoren zur Verfügung. Diese Prozessoren wurden speziell für maschinelles Lernen entwickelt und verfügen über integrierte Hardware-Beschleuniger zur effizienten Ausführung entsprechender Algorithmen. Die EVKs ermöglichen eine unkomplizierte Anbindung an externe Peripheriegeräte und bieten somit eine geeignete Plattform für erste Evaluierungen. Die RPTU analysierte die Hardware im Hinblick auf ihre Eignung für KI-basierte Verfahren zur Ressourcenverteilung. NXP unterstützte diese Arbeiten durch technische Informationen zu den Plattformen und deren Beschleunigerfunktionen.

2.6 Arbeitspaket 6: Sicherheit und Authentifizierung

NXPs Beiträge in Arbeitspaket 6 lagen in T-AP 6.1 „Authentisierung und Sicherheitskonzepte von Netzwerkteilnehmern“ und T-AP 6.2 „Hardware- und Sensingbasierte Sicherheit“

2.6.1 T-AP 6.1: Authentisierung und Sicherheitskonzepte von Netzwerkteilnehmern

Im Rahmen des Arbeitspakets 6 (AP6) des Projekts 6G-CAMPUS hat NXP wesentliche Beiträge zur Erforschung und Entwicklung von Verfahren zur Authentifizierung auf physikalischer Ebene geleistet. Der Fokus lag dabei insbesondere auf sogenannten Physical Layer Authentication (PLA)-Techniken, die eine zusätzliche Sicherheitsschicht direkt auf der Übertragungsebene bieten sollen. Diese Ansätze sind besonders relevant für zukünftige 6G-Netzwerke, in denen eine hohe Sicherheit bei gleichzeitig niedriger Latenz und hoher Energieeffizienz gefordert wird.

Ein zentraler Bestandteil der Arbeiten war die Mitwirkung an der wissenschaftlichen Publikation „Physical Layer Authentication within 6G Campus Networks“ [Weinand2025]. In dieser Publikation wird ein Überblick über bestehende PLA-Methoden gegeben, wobei zwischen verdeckten und nicht-verdeckten Verfahren unterschieden wird. NXP konzentrierte sich dabei auf die Entwicklung

und Validierung eines innovativen aktiven PLA-Verfahrens, das auf der Einbettung von Wasserzeichen in die Phasen von OFDM-Symbolen basiert.

Der neuartige Ansatz unterscheidet sich von früheren Methoden dadurch, dass die Wasserzeichen nicht in kritische Symbole im Frequenzbereich eingebettet sind, sondern in den Phasen weniger kritischer Symbole im Zeitbereich. Die Wasserzeichen werden durch gezielte Phasenoffsets eingeführt, die auf einem geheimen Schlüssel zwischen Sender und Empfänger basieren. Nur die Entität, die im Besitz dieses Schlüssels ist, kann die Offsets rekonstruieren und somit die Echtheit der Nachricht verifizieren.

Die Leistungsfähigkeit des vorgeschlagenen Verfahrens wurde durch Simulationen und Messungen evaluiert (Abbildung 5). Dabei zeigte sich, dass bei einem Signal-Rausch-Verhältnis (SNR) von 15 dB bereits ab einem Phasenoffset von 10 Grad eine effektive Authentifizierung möglich ist. Bei niedrigeren SNR-Werten nimmt die Authentifizierungsrate erwartungsgemäß ab, was auf eine erhöhte Fehleranfälligkeit bei der Entfernung der Wasserzeichen zurückzuführen ist.

Die Ergebnisse dieser Arbeiten bilden eine vielversprechende Grundlage für die Integration von PLA-Techniken in zukünftige 6G-Netzwerke und demonstrieren die Innovationskraft von NXP im Bereich sicherer Kommunikationssysteme. Die entwickelten Konzepte sollen in weiteren Publikationen vertieft und durch zusätzliche Messungen validiert werden.

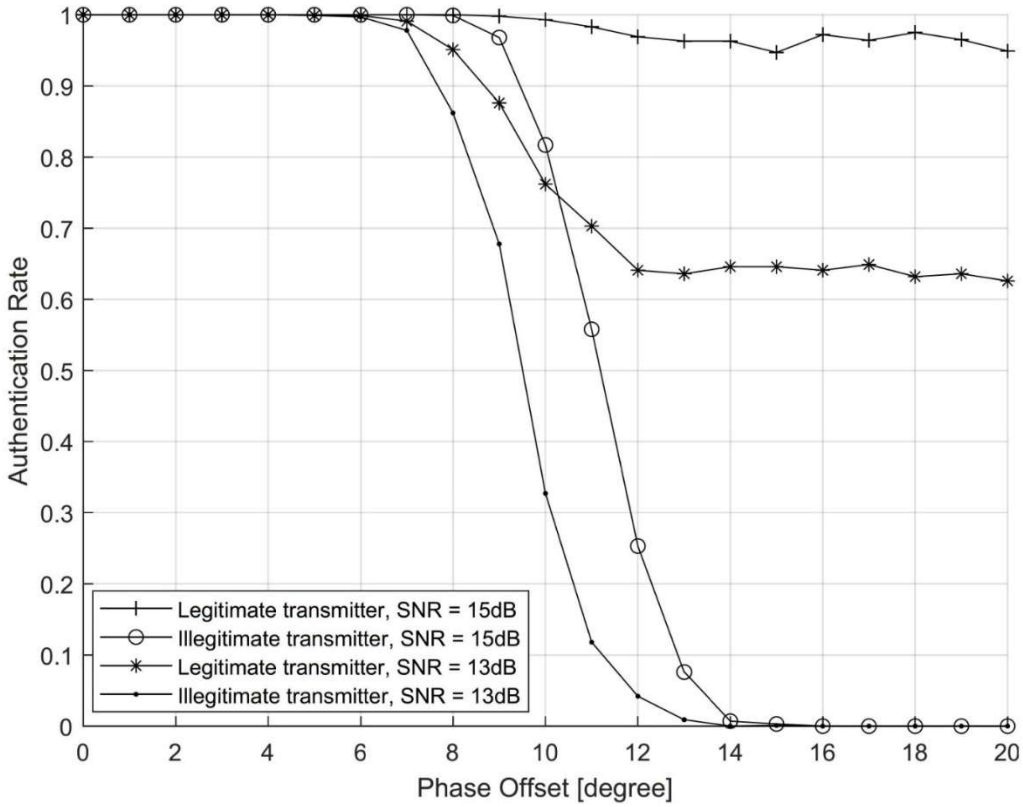

Abbildung 5: Erfolgreiche Authentifizierung in Abhängigkeit des Phasenoffsets

2.6.2 T-AP 6.2: Hardware- und Sensingbasierte Sicherheit

Im Rahmen von Arbeitspaket 6 wurde eine umfassende Sicherheitsanalyse gemeinsam mit allen Partnern unter der Leitung von NXP durchgeführt, die sich auf die STRIDE-Methodik stützt. STRIDE ist ein von Microsoft entwickeltes Modell zur systematischen Identifikation von Sicherheitsbedrohungen in IT-Systemen [Kohnfelder1999]. Es steht für:

- Spoofing (Identitätsfälschung)
- Tampering (Manipulation)
- Repudiation (Abstreitbarkeit)
- Information Disclosure (Informationspreisgabe)
- Denial of Service (Dienstverweigerung)
- Elevation of Privilege (Privilegienerweiterung)

Diese Kategorien wurden genutzt, um potenzielle Bedrohungen innerhalb der 6G-CAMPUS Systemarchitektur zu identifizieren und zu bewerten. Ergänzend wurde das DREAD-Modell verwendet, um die Risiken zu quantifizieren und zu priorisieren. DREAD bewertet Bedrohungen anhand von fünf Kriterien: Schaden, Reproduzierbarkeit, Ausnutzbarkeit, betroffene Nutzer und Entdeckbarkeit.

Für bestehende 5G-Architekturen wurden bereits umfassende Risikoanalysen durchgeführt. Daher konzentriert sich die vorliegende Analyse ausschließlich auf die neue JC&S-Funktionalität und den entsprechenden Anwendungsfall.

Vorgehensweise der Analyse

Die STRIDE-Analyse begann mit einer Vereinfachung der Systemarchitektur für JC&S, um sicherheitsrelevante Komponenten zu isolieren. Diese wurden in einem Bedrohungsmodell dargestellt. Anschließend wurden reale Systembestandteile durch STRIDE-Entitäten ersetzt, um eine abstrahierte Sicht auf potenzielle Bedrohungen zu erhalten (Abbildung 6).

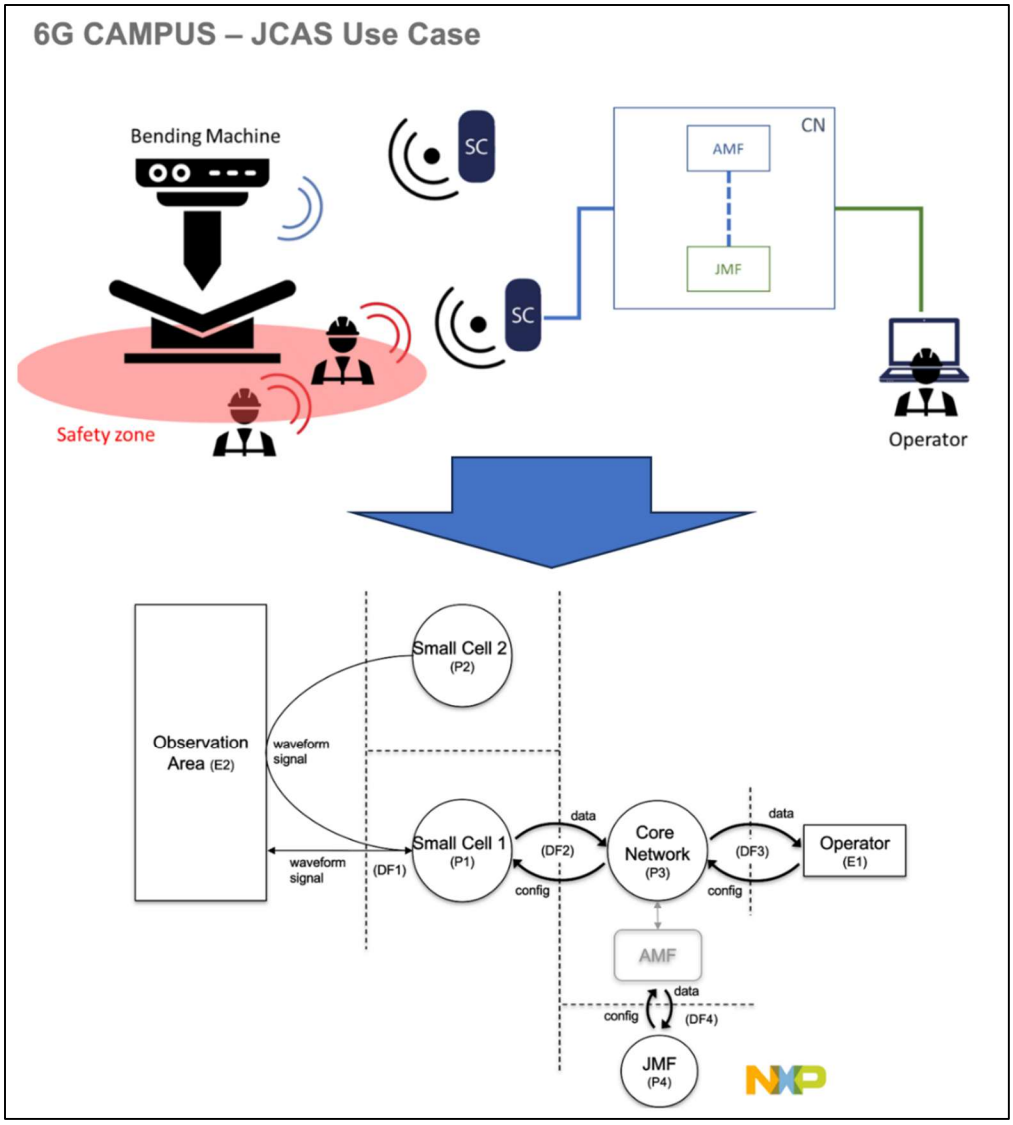

Abbildung 6: Ableitung der STRIDE-Entitäten für den JC&S Anwendungsfall

In einem Workshop wurden konkrete Bedrohungen entlang der STRIDE-Kategorien identifiziert und mit dem DREAD-Modell bewertet. Bedrohungen mit einem DREAD-Wert von 2 oder höher wurden als „kritisch genug“ eingestuft, um Gegenmaßnahmen zu definieren. Diese Maßnahmen wurden in einem weiteren Workshop erarbeitet.

Beispiele für identifizierte Bedrohungen und Gegenmaßnahmen

Kategorie	Bedrohung	Code / DREAD	Beschreibung	Gegenmaßnahme
Physikalische Bedrohungen	Absorbierende Materialien	E2-S / 2.5	Störung der Sensorik durch funkabsorbierende Materialien	Antennendiversität, KI-basierte Hintergrundmodellierung
	Jamming	E2-D / 2.3	Unterbrechung der Kommunikation durch Störsender	Frequenzsprung-verfahren, Notfall-abschaltung bei Breitbandstörung
	Hardware-Vandalismus	P1-T / 2.8	Manipulation oder Zerstörung von Basisstationen	Zugangskontrollen, Videoüberwachung, TPMs zur Datensicherung
Logische Bedrohungen	Manipulation von Konfigurations-daten	E1-T2 / 2.2	Veränderung von Konfigurationsdaten zur Auslösung unerwünschter Aktionen	Verschlüsselung, Authentifizierung
	Fehlende Benutzer-autorisierung	E1-E2 / 2.3	Unzureichende Rechteverwaltung	Netzwerk-segmentierung, rollenbasierte Zugriffskontrolle
	Sniffing vertraulicher Daten	E1-I4 / 2.0	Abhören von Netzwerkverkehr	VPNs zur Verschlüsselung der Datenübertragung
Kernnetzwerk-Bedrohungen	Manipulation von SMF & SMAE	P4-T2 / 2.0	Manipulation der Sensorik-Koordination	Kryptografische Prüfungen, Authentifizierung auf Betriebssystemebene
	Denial of Service durch Datenüber-flutung	P4-D / 2.2	Überlastung der KI-Modelle durch gefälschte Daten	KI-basierte Anomalieerkennung, Redundanz-mechanismen
Bedrohungen für den Betreiber	Unverschlossene Konsolen bei Feueralarm	E1-I/S-2 / 2.2	Gefahr durch ungesicherte Terminals bei Feueralarm	Automatische Abschaltung, Zertifikatswiderruf
	Passwörter auf Stickern	E1-I/S-1 / 2.9	Physische Preisgabe von Zugangsdaten	Zwei-Faktor-Authentifizierung, sichere Passwortverwaltung

Fazit

Die STRIDE-Analyse im 6G-CAMPUS Projekt zeigt, dass Sicherheitsaspekte bereits in der Architekturphase berücksichtigt werden müssen. Durch die Kombination von STRIDE und

DREAD konnten konkrete Bedrohungen identifiziert und priorisiert sowie wirksame Gegenmaßnahmen definiert werden. Die Analyse bildet eine solide Grundlage für die Implementierung sicherer 6G-Systeme und demonstriert die Bedeutung von Sicherheitsdesign in frühen Entwicklungsphasen.

2.7 Arbeitspaket 7: Konzeptnachweis (PoC) und Aufbereitung der Ergebnisse

Im Rahmen des Arbeitspakets 7 des 6G-CAMPUS Projekts hat NXP eine Reihe von vorbereitenden und unterstützenden Maßnahmen zur Realisierung der Demonstratoren durchgeführt.

Zur Demonstration des 6G-Campus-Konzepts wurden im Projekt zwei zentrale Demonstratoren realisiert. Der erste zeigt das Prinzip des Network-of-Networks, bei dem sämtliche Netzkomponenten - einschließlich Non-3GPP-Systeme - über das 6G-Kernnetz gesteuert werden können. Dadurch wird eine effiziente, KI-basierte Netzwerksteuerung ermöglicht, die wesentliche Kenngrößen aller beteiligten Komponenten berücksichtigt. Der zweite Demonstrator widmet sich Joint Communication & Sensing (JC&S) und verdeutlicht, wie die Umgebung mithilfe von Radar-Heatmaps erfasst und anschließend zur Anomaliedetektion genutzt werden kann.

Da die Demonstratoren in einem industriellen Umfeld vorgeführt wurden, hat NXP den Dreh eines Videos organisiert, um die Ergebnisse auch über diesen Rahmen hinaus demonstrieren zu können. Das Video wurde auf der 6G-Konferenzen in Berlin 2025 präsentiert.

Ein zentraler Beitrag zu den Demonstratoren seitens NXP bestand in der Bereitstellung einer Small Cell für den Network-of-Networks Demonstrator, welche speziell für die Anforderungen des Projekts angepasst wurde. Die Small Cell wurde mit den notwendigen Softwaremodifikationen versehen, um eine nahtlose Integration in die Projektarchitektur zu ermöglichen. Durch die Bereitstellung einer europäischen Lösung durch NXP wird ein wichtiger Beitrag zur technologischen Souveränität Deutschlands und Europas geleistet. Dies stärkt die Position Europas im Bereich der Campusnetze und unterstreicht die strategische Bedeutung des Projekts.

Außerdem stellte NXP die Hardware für die WiFi-basierte Funktechnologie von R3 Solutions im Campusband zur Verfügung. Diese beinhaltete insbesondere einen speziell entwickelten Mischer, der es ermöglicht, die bestehende WiFi-Technologie von R3 Solutions im Campusband bei 3,7 GHz zu betreiben. Die Entwicklung des Mischers wurde bereits im Rahmen von Arbeitspaket 3 und 4 detailliert beschrieben, da dort die technische Spezifikation und das Layout erfolgte. In einem Demonstrator wurde erfolgreich gezeigt, dass die WiFi-Hardware von R3 in ein Campusnetz integriert und über das 6G-Core-Netzwerk gesteuert werden kann. Das 6G-Core-System von MECSware übermittelt dabei die erforderlichen Steuerinformationen mittels der Small Cell über die neu definierte Schnittstelle an die WiFi-Komponenten.

In dem zweiten Demonstrator zu Joint Communication & Sensing wurde das von Merantix Momentum entwickelte KI-Modell erfolgreich auf einem i.MX9 Prozessor für industrielle Anwendung von NXP implementiert, wobei die Echtzeitfähigkeit der Lösung nachgewiesen werden konnte.

Zusammenfassend lässt sich festhalten, dass NXP im Rahmen von Arbeitspaket 7 maßgeblich zur technischen Infrastruktur der Demonstratoren beigetragen hat. Die Bereitstellung und Anpassung der Small Cell, die Integration der WiFi-basierten Lösung mit dem Mischer und die Implementierung der KI- Algorithmen auf Prozessoren für industrielle Anwendungen sind zentrale Bausteine für die Umsetzung der geplanten Demonstratoren und tragen wesentlich zur Zielerreichung des Projekts bei.

Referenzen

WBA2021	WBA 5G Work Group, „5G and Wi-Fi RAN Convergence”, Wireless Broadband Alliance, 2021
Sedunova2021	E. Sedunova, N. Maletic, L. Wimmer, D. Cvetkovski, E. Grass and B. Lankl, „Utilizing Beamsteering at Millimeter Waves for Indoor Object and Room Geometry Detection," 2021 IEEE 4th 5G World Forum (5GWF), 2021
Mollenhauer2025	Mattes Mollenhauer, Nicole Mücke, Dimitri Meunier and Arthur Gretton. "Regularized least squares learning with heavy-tailed noise is minimax optimal". Advances in Neural Information Processing Systems, Vol. 39, 2025.
Weinand2025	A. Weinand; A. Hasani, A. Ahmad, S. B. Mallikarjun; J. Wilking, M. Hafner, J. V. Gomez, H. Master; H. D. Schotten, „Physical Layer Authentication Within 6G Campus Networks“, 2025 EuCNC & 6G Summit
German2024	German Perspective on 6G - Use Cases, Technical Building Blocks and Requirements, Insights by the 6G Platform Germany, White Paper
Kohnfelder1999	Loren Kohnfelder and Praerit Garg, „The threats to our products“, Microsoft Interface, April 1, 1999.