Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

Schlussbericht zum Teilvorhaben

Vorhaben: Mission Critical Dienste zur sicheren Vernetzung heterogener Breitnetze in anspruchsvollen KRITIS-Umgebungen, Teilvorhaben: Sichere heterogene Breitbandnetze (MissionXconnect)
Projektpartner: Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. / Fraunhofer FKIE
Förderkennzeichen: 16BEC0048
Laufzeit: 16.09.2024 bis 30.06.2026 (inkl. kostenneutraler Laufzeitverlängerung)

Gefördert durch:

Bundesministerium
des Innern

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhaltsverzeichnis

Abbildungsverzeichnis		**3**
Tabellenverzeichnis		**3**
I.	**Kurzdarstellung**	**4**
I.1	Problemstellung	4
I.2	Voraussetzungen, unter denen das Vorhaben durchgeführt wurde	4
I.3	Planung und Ablauf des Vorhabens	4
I.4	Wissenschaftlicher und technischer Stand	5
I.5	Kurzdarstellung der wichtigsten Vorhabenergebnisse	5
I.6	Nutzen und zukünftige Anwendungsmöglichkeiten der Vorhabenergebnisse	6
II.	**Eingehende Darstellung**	**7**
II.1	Erzielte Ergebnisse im Einzelnen	7
II.1.1	AP-Nr. 1 – Systemdefinition und Betrachtungshorizont des Vorhabens	7
II.1.2	AP-Nr. 2 – Risikoanalysen und Sicherheit	8
II.1.3	AP-Nr. 3 – Vorbereitung Demo und Sicherheitsinfrastruktur	9
II.1.4	AP-Nr. 4 – Demonstration Use-Case	12
II.1.5	AP-Nr. 5 – Maßnahmen und Handlungsempfehlungen	14
II.2	Beitrag zu Zielen der Fördermaßnahme, voraussichtlicher Nutzen und Verwertbarkeit	15
II.2.1	Wirtschaftliche Erfolgsaussichten nach Vorhabenende	18
II.2.2	Wissenschaftliche und/oder technische Erfolgsaussichten nach Vorhabenende	19
II.2.3	Wissenschaftliche und wirtschaftliche Anschlussfähigkeit	20
III.	**Anlagen**	**22**
III.1	Wichtige Positionen des zahlenmäßigen Nachweises	22
III.2	Zusammenarbeit und Projektmanagement	23
III.2.1	Zusammenarbeit im Konsortium	23
III.2.2	Zusammenarbeit mit der BDBOS und VDI/VDE Innovation + Technik GmbH	24
III.3	Übersicht der Maßnahmen der Öffentlichkeitsarbeit	24
III.3.1	Innovationsforum 2024	24
III.3.2	Virtuelle Roadshow	25
III.3.3	Demonstration der technischen Realisierungen	25
III.3.4	Innovationsforum 2026	26
III.4	Übersicht der Schutzrechtsanmeldungen	26

Abbildungsverzeichnis

Abbildung 1. Initiale Version des passiven Sensors, wie in AP4 auf der FrOSCon verwendet 11
Abbildung 2. Verwendetes abschließbares Gehäuse zum Schutz vor Manipulation 12
Abbildung 3. Hinweisschild, das auf jedem Sensor angebracht wurde.....12
Abbildung 4. Durchschnittliche gemessene WiFi-Kanalauslastungen je über 2 Stunden. 13
Abbildung 5. Exemplarische Messergebnisse für einen Kanal und einen Standort. 13
Abbildung 6. Weiterentwickelte deutlich kompaktere Version des passiven Sensors 14
Abbildung 7. Redebeitrag von Prof. Michael Rademacher zu den Ergebnissen des Vorhabens auf dem 2. Innovationsforum in Berlin 26

Tabellenverzeichnis

Tabelle 1. Übersicht der Arbeitspakete 4
Tabelle 2. Verwertungsplan.....17

I. Kurzdarstellung

I.1 Problemstellung

BOS- und KRITIS-Anwendungen haben zunehmenden Bedarf an breitbandigen Diensten über reine Sprachkommunikation hinaus, die zugleich jedoch hohe Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit und Resilienz erfüllen müssen. Besonders herausfordernd ist dies bei WiFi als Zugangstechnolgie, da es in unlizenziertem Spektrum betrieben wird und damit Störungen, konkurrierenden Netzen und gezielten Angriffen unterliegt.

Ziel des Vorhabens war die Bewertung der Eignung heterogener Breitbandnetze – insbesondere WiFi und ergänzend 5G-Zugänge – für einsatzkritische Kommunikationsdienste. Dabei wurden moderne WiFi-Standards auf ihre Eignung geprüft und bewertet, ein passives Messverfahren zur Erfassung der Kanalauslastung entwickelt, Messungen durchgeführt und ausgewertet, sowie Handlungsempfehlungen für BOS- und KRITIS-nahe Szenarien abgeleitet.

I.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Vorhaben wurde im Verbund mit der **Frequentis Deutschland GmbH** als **Koordinatorin**, der **ELARA Leitstellentechnik GmbH**, der **ATS Elektronik GmbH**, der **NKMG mbH** und der **RWTH Aachen University** mit der Juniorprofessur für Sicherheit und Datenschutz in industrieller Kooperation durchgeführt. Zusätzlich war die **Fraport AG** als assoziierter Partner beteiligt. Auf Seiten des **Fraunhofer FKIE** war das Vorhaben in der Forschungsgruppe „Secure Mobile Communication“ verankert.

Als wesentliche Randbedingung war die ursprünglich vorgesehene Nutzung der Flughafeninfrastruktur des Fraport für standortspezifische Analysen und Messungen im Projektverlauf nicht möglich. Die passiven Messungen wurden daher in Abstimmung mit dem Projektträger generisch und datensparsam – mit direkter Anwendbarkeit auf diverse KRITIS/BOS-Standorte – entwickelt, und zur Gewinnung belastbarer Auslastungsdaten in einem Szenario mit flughafenähnlichem Personenaufkommen erfolgreich durchgeführt. Eine weitere Rahmenbedingung war der verzögerte Projektanlauf infolge des späten Eingangs des Zuwendungsbescheids.

I.3 Planung und Ablauf des Vorhabens

Das Vorhaben war entlang der in Tabelle 1 dargestellten Arbeitspakete strukturiert.

Tabelle 1. Übersicht der Arbeitspakete

Arbeitspaket (AP)	Name	Leitung
AP-Nr. **1**	Systemdefinition und Betrachtungshorizont des Vorhabens	Frequentis
AP-Nr. **2**	Risikoanalysen und Sicherheit	RWTH Aachen
AP-Nr. **3**	Vorbereitung Demo und Sicherheitsinfrastruktur	Frequentis
AP-Nr. **4**	Demonstration Use-Case	Frequentis
AP-Nr. **5**	Maßnahmen und Handlungsempfehlungen	Fraunhofer FKIE

Die Laufzeit wurde aufgrund der veränderten Rahmenbedingungen kostenneutral bis zum 30.06.2026 verlängert; offene Arbeitspakete wurden dabei mit Genehmigung des Projektträgers auf die neue Projektlaufzeit fortgeschrieben. Auf diese Weise konnten durch das FKIE alle Arbeitspakete in der vorgesehenen fachlichen Tiefe und Qualität abgeschlossen werden. Wesentliche Änderungen der Ausgaben- und Kostenplanung ergaben sich nicht. Zum Zeitpunkt der Berichtserstellung ist für die Teilvorhaben einzelner Partner darüber hinaus eine weitere Verlängerung beantragt, die die Arbeiten des FKIE nicht berührt.
Eine eingehende Darstellung der einzelnen Arbeitspakete erfolgt unter Punkt II.

I.4 Wissenschaftlicher und technischer Stand

Das **Fraunhofer FKIE** stützte sich auf umfangreiche Vorarbeiten zur Skalierbarkeit und Sicherheit drahtloser Kommunikationssysteme wie WiFi und 5G und verantwortete die Bewertung der Eignung von WiFi für einsatzkritische Kommunikation, das passive Messverfahren zur Kanalauslastung sowie die Leitung des Arbeitspaketes zu Maßnahmen und Handlungsempfehlungen.
Die **Frequentis** brachte langjährige Erfahrung in sicherheitskritischen Kommunikations- und Kontrollraumsystemen, MCX-Lösungen und Standardisierung ein und übernahm die Verbundkoordination, die MCX-Systemarchitektur und Interworking. Die **ELARA** brachte Leitstellen-Know-how und das System ASGARD ein und bearbeitete die leitstellenseitige Anbindung an MCX. Die **ATS** stellte mithilfe ihrer umfangreichen Erfahrung in Planung und Betrieb von TETRA- und 5G-Campusnetzen die netztechnische Demonstrationsumgebung sowie 5G-/WiFi-Integration bereit. Die **NKMG** brachte ihre Expertise ein, um die Anforderungs- und Use-Case-Analyse, sowie die Bewertung sicherer Kommunikationslösungen für BOS und KRITIS zu unterstützen. Die **RWTH Aachen** stützte sich auf Vorarbeiten zur Cybersicherheit drahtloser und industrieller Kommunikationsnetze und bearbeitete insbesondere Fragen der Ende-zu-Ende-Sicherheit.

I.5 Kurzdarstellung der wichtigsten Vorhabenergebnisse

Das Teilvorhaben wurde erfolgreich abgeschlossen. Wesentliche Ergebnisse sind:

- **Moderne WiFi-Standards wie WiFi 6(E) und 7** bieten großes Potenzial für einsatzkritische Kommunikation durch Mechanismen wie OFDMA, MU-MIMO, MLO und das 6GHz-Band, Grenzen liegen bisher vor allem in der Verfügbarkeit praktikabler Implementierungen;
- Das aktuelle Sicherheitsverfahren **WPA3-Enterprise** bietet deutliche Sicherheitsgewinne zu veralteten Versionen und ist **für einsatzkritische Netze zu bevorzugen**, Angriffe auf die Verfügbarkeit bleiben jedoch weiterhin besonders relevant und sind nicht zu vernachlässigen;
- Verfügbarkeit eines passiven, datenschutzkonformen und auf andere Standorte übertragbaren **Messverfahrens zur Erfassung der WiFi-Kanalauslastung**;
- **Praktische Erprobung dieses Verfahrens** in einer realitätsnahen Hochlastumgebung mit rund 2.000 Personen und drei Messpunkten; selbst im Spitzenzeitfenster lag die durchschnittliche

Belegung des am stärksten genutzten Kanals nur bei rund 35 %, mehrere weitere Kanäle lagen deutlich darunter;

- Ableitung konkreter technischer und organisatorischer **Handlungsempfehlungen** für den Einsatz von WiFi in BOS- und KRITIS-nahen Szenarien in einem konsolidierten Dokument.

I.6 Nutzen und zukünftige Anwendungsmöglichkeiten der Vorhabenergebnisse

Die Ergebnisse können unmittelbar für die Planung, Bewertung und Weiterentwicklung breitbandiger Kommunikationsinfrastrukturen in BOS- und KRITIS-nahen Umgebungen genutzt werden. Sie liefern eine belastbare Entscheidungsgrundlage für die Eignung von WiFi, ein auf andere Standorte übertragbares Messverfahren zur Vor-Ort-Bewertung der Kanalauslastung sowie konkrete sicherheitstechnische Handlungsempfehlungen. Damit sind die Ergebnisse unter anderem für Flughäfen, Bahnhöfe, Veranstaltungsstätten und andere kritische Standorte anschlussfähig.

Für das Fraunhofer FKIE ergeben sich Verwertungsperspektiven insbesondere in Form von Forschungs- und Entwicklungsleistungen, Beratungs- und Evaluationsleistungen, Schulungs- und Transferformaten sowie als Grundlage für Anschlussvorhaben. Eine produktbezogene Vermarktung steht nicht im Vordergrund; die Verwertung erfolgt primär über Methoden-, Technologie- und Know-how-Transfer.

II. Eingehende Darstellung

II.1 Erzielte Ergebnisse im Einzelnen

In den folgenden Abschnitten werden die erreichten Ergebnisse der einzelnen Arbeitspakete (AP) unter Berücksichtigung der vorgegebenen Ziele aus der Teilvorhabenbeschreibung erläutert.

II.1.1 AP-Nr. 1 – Systemdefinition und Betrachtungshorizont des Vorhabens

Im ersten Arbeitspaket hat das Fraunhofer FKIE die fachliche Grundlage für die weiteren Arbeiten geschaffen. Im Zentrum standen die systematische Betrachtung moderner drahtloser Zugangsnetze, die Ableitung relevanter Bewertungsdimensionen für einsatzkritische Dienste sowie die Einordnung der technischen Randbedingungen.

Ein Schwerpunkt lag auf der **theoretischen Analyse der Eignung von WiFi für MCX-Dienste**. Dazu wurden die Eigenschaften der Standards WiFi 5, WiFi 6(E) und WiFi 7 hinsichtlich Leistungsfähigkeit, Latenzverhalten, Robustheit, Priorisierungsfähigkeit und Störanfälligkeit gegenübergestellt. Als wesentliche positive Entwicklungen wurden insbesondere OFDMA, MU-MIMO, BSS-Coloring, das 6-GHz-Band sowie perspektivisch MLO identifiziert. Gleichzeitig zeigte die Analyse, dass diese Vorteile in der Praxis stark von der konkreten Implementierung des Access Points, von der Qualität des Schedulers, von der Signalstärke und vom Gerätemix abhängen.

Darüber hinaus wurden die grundsätzlichen Herausforderungen des Betriebs von WiFi in unlizenzierten Bändern analysiert. Dazu zählen Interferenzen durch andere WiFi-Netze, andere Funksysteme im selben Spektrum, Altgeräte, schlechte Signal-Rausch-Verhältnisse sowie regulatorische Einschränkungen, insbesondere im 5-GHz- und 6-GHz-Band. Auch die Möglichkeit gezielter Angriffe auf die Verfügbarkeit, Vertraulichkeit und Integrität von WiFi-Infrastruktur wurde in diesem Arbeitspaket initial betrachtet.

Ergänzend wurde dargestellt, unter welchen Voraussetzungen ein 5G-Campusnetzwerk sicher in bestehende KRITIS- und BOS-nahe Infrastrukturen eingebunden werden kann. Als wesentliche Voraussetzungen wurden hierbei insbesondere ein kontrollierter beziehungsweise eigenbetriebener Netzansatz, eine sichere Konfiguration von Kernnetz und Funkzugang, die sichere Segmentierung und – soweit genutzt – belastbare Absicherung von Slices sowie die zusätzliche Absicherung der Anwendungskommunikation und der Endgeräte herausgearbeitet.

Im Projektverlauf war die ursprünglich vorgesehene direkte Nutzung der Fraport-Infrastruktur nicht möglich. Das FKIE wich deshalb nicht von den Zielen des Arbeitspakets ab, sondern **konkretisierte die Arbeiten in Richtung einer generischen, übertragbaren Technologieanalyse**. Dies erwies sich als fachlich sinnvoll, da die Ergebnisse dadurch nicht auf einen Einzelstandort beschränkt blieben, sondern in eine breitere Bewertungsmethodik für BOS- und KRITIS-Standorte überführt werden konnten. Zugleich wurde die ursprünglich am Flughafen vorgesehene Zielumgebung in einen modularen, auf Partnerinfrastrukturen basierenden Test- und Demonstrationsansatz mit zentralem MCX-Server und gekoppelten Teilnetzen überführt.

Als zentrale Erkenntnis aus AP1 wurde deutlich, dass WiFi für einsatzkritische Kommunikation aus einer rein theoretischen Perspektive nicht pauschal bewertet werden kann. Vielmehr ist eine differenzierte

Betrachtung erforderlich, die technologische Fähigkeiten, lokale Spektrumsituation, Sicherheitsmechanismen, Angriffsszenarien und betriebliche Einsatzszenarien zusammenführt.

II.1.2 AP-Nr. 2 – Risikoanalysen und Sicherheit

Im zweiten Arbeitspaket bearbeitete das FKIE die sicherheitstechnische und risikoorientierte Bewertung drahtloser Zugangsnetze, insbesondere von WiFi-basierten Zugängen. Ziel war es, die wesentlichen Bedrohungen, vorhandenen Sicherheitsmechanismen und verbleibenden Restrisiken einer Nutzung von WiFi im BOS-/KRITIS-Kontext systematisch zu analysieren und zu bewerten. Im Projektverlauf zeigte sich, dass die Untersuchung von Angriffen auf WiFi-Infrastrukturen fachlich besonders anspruchsvoll ist, da die praktische Relevanz und Ausnutzbarkeit einzelner Angriffsszenarien wesentlich von den eingesetzten Standards, Sicherheitsverfahren, Konfigurationen sowie der konkreten Kombination aus Access Points und Endgeräten abhängt. Da für einsatzkritische Kommunikation insbesondere die Sicherstellung von Verfügbarkeit, Vertraulichkeit und Integrität von zentraler Bedeutung ist, wurde in AP2 ein besonderer Schwerpunkt auf die vertiefte Analyse praktisch relevanter Angriffsszenarien gegen WiFi sowie auf die Einordnung geeigneter Schutzmaßnahmen gelegt.

Dazu wurden die aktuellen Sicherheitsstandards **WPA2**, **WPA3** sowie **OWE** analysiert und hinsichtlich ihrer Eignung für einsatzkritische Kommunikationsszenarien bewertet. Parallel dazu wurde eine strukturierte Betrachtung realistischer Angriffsszenarien vorgenommen. Im Fokus standen dabei:

- passives Abhören der Kommunikation,
- Evil-Twin- und Man-in-the-Middle-Angriffe,
- Passphrasen- und Downgrade-Angriffe,
- Deauthentication- und Flooding-basierte Denial-of-Service-Angriffe,
- Angriffe auf Schicht 1 wie Jamming, Reactive Jamming und BeamSteal.

Die Analyse zeigte, dass moderne Sicherheitsstandards die Sicherheit im Vergleich zu älteren Verfahren deutlich erhöhen, die Eignung für kritische Kommunikation aber maßgeblich vom **konsequenten Einsatz aktueller Standards und sauberer Implementierungen** abhängt. Als besonders geeignet wurde **WPA3-Enterprise ohne Transition Mode** identifiziert. Gleichzeitig wurde herausgearbeitet, dass auch bei modernen Standards insbesondere die **Verfügbarkeit** weiterhin ein kritischer Aspekt bleibt, da weitaus effizientere und effektivere praktikable DoS-Angriffe auf WiFi bekannt sind als nur klassisches Jamming.

In der Bearbeitung wurde die Sicherheitsanalyse gezielt auf die für das FKIE-Teilvorhaben relevanten Fragestellungen fokussiert. Die Gründe hierfür lagen in der klaren Spezialisierung des Teilvorhabens auf Zugangsnetze und deren praktische Nutzbarkeit für MCX-Dienste. Die Konsequenz war eine inhaltlich vertiefte und sehr anwendungsnahe Sicherheitsbewertung, die später direkt in die Handlungsempfehlungen aus AP5 einfloss.

Ein wesentliches Ergebnis des Arbeitspakets war damit die Erkenntnis, dass WiFi für einsatzkritische Kommunikation **nur unter klar definierten technischen und organisatorischen Randbedingungen** in

Betracht gezogen werden sollte, einschließlich moderner Sicherheitsstandards, konsequentem Patch-Management, separierter Netzinfrastruktur und standortspezifischer Risikobewertung.

II.1.3 AP-Nr. 3 – Vorbereitung Demo und Sicherheitsinfrastruktur

Im Teilvorhaben wurde durch das FKIE eine Messkampagne zur Evaluation der Nutzbarkeit von WiFi für einsatzkritische Kommunikation geplant und praktisch durchgeführt. Das AP 3 diente dabei der Planung sowie Implementierung der Messungen und war dazu in vier Unterarbeitspakete aufgeteilt, auf die in den folgenden Abschnitten einzeln eingegangen wird.

II.1.3.1 AP-Nr. 3.1 – Anforderungen an Demo und Tests

In AP3.1 konkretisierte das FKIE die Anforderungen für die geplanten Messungen und Tests. Dabei wurden die in AP1 und AP2 erarbeiteten Erkenntnisse in messbare Kriterien überführt.
Als zentrale KPI wurde die **zeitliche Kanalauslastung** bzw. Busytime eines WiFi-Kanals festgelegt. Ergänzend wurden weitere Messgrößen definiert, insbesondere:

- Anzahl aktiver Geräte bzw. sichtbarer MAC-Adressen,
- Anzahl detektierter SSIDs,
- Größenklassen beobachteter Frames.

Die Definition dieser Kennzahlen erfolgte mit Blick auf die praktische Frage, ob in realen Hochlastsituationen genügend freie Ressourcen für eine robuste einsatzkritische Kommunikation vorhanden sind. Das FKIE stellte damit sicher, dass die geplanten Messungen nicht nur Rohdaten erzeugen, sondern direkt auf die Bewertungslogik des Projekts einzahlen.
Im Projektverlauf ergab sich eine fachlich sinnvolle Schärfung der ursprünglich sehr breiten Metrikdiskussion: Statt möglichst vieler Einzelgrößen wurden die in der Praxis besonders belastbar und interpretierbar erfassbaren Größen priorisiert. Diese Fokussierung erhöhte die Aussagekraft und Umsetzbarkeit der späteren Feldmessung.

II.1.3.2 AP-Nr. 3.2 – Eignungsprüfungen Sicherheitsmaßnahmen

In AP3.2 bewertete das FKIE, inwieweit die für den Einsatz drahtloser Zugangsnetze relevanten Sicherheitsmaßnahmen geeignet sind, die identifizierten Risiken in einem kritischen Anwendungskontext angemessen zu adressieren. Aufgrund des nicht abzubildenden Zugriffs auf die Infrastruktur eines Flughafens wurden analog zu AP1 auch hier die Analysen auf eine generische und übertragbare Technologiebetrachtung hin konkretisiert.
Die Eignungsprüfung erfolgte insofern nicht als isolierter Penetrationstest einzelner Komponenten, sondern als **strukturierte Plausibilitäts- und Wirksamkeitsbewertung** der vorgesehenen Schutzmaßnahmen im Lichte der identifizierten Bedrohungen. Bewertet wurden insbesondere:

- Netztrennung zwischen einsatzkritischen und sonstigen WiFi-Diensten,
- Nutzung moderner Standards und Ausschluss veralteter Geräte,
- Einsatz von WPA3-Enterprise ohne Transition Mode,
- Bedeutung regelmäßiger Updates und hinreichender Herstellerunterstützung,

- Notwendigkeit einer szenariobezogenen Risikobewertung bei erwartbaren Verfügbarkeitsangriffen,
- Erfordernis zusätzlicher Rückfallebenen.

Das Ergebnis war eine klare Aussage: Die betrachteten Sicherheitsmaßnahmen sind für den Einsatzzweck **geeignet, wenn sie konsequent und vollständig umgesetzt werden**. Gleichzeitig wurde betont, dass WiFi trotz moderner Schutzmechanismen nicht per se dieselben Garantien bieten kann wie exklusiv kontrollierte und priorisierbare Zugangsnetze. Deshalb ist die Entscheidung für oder gegen WiFi stets im konkreten Nutzungsszenario zu treffen.

Die Arbeiten in AP3.2 dienten unmittelbar als inhaltliche Brücke zwischen der theoretischen Risikoanalyse und den späteren praxisorientierten Handlungsempfehlungen.

II.1.3.3 AP-Nr. 3.3 – Detailplanung der Tests

In AP3.3 plante das FKIE die praktische Messkampagne im Detail. Aufgrund der nicht verfügbaren Fraport-Infrastruktur wurde ein alternativer, aber fachlich geeigneter Messort ausgewählt: die Konferenz **FrOSCon 2025** an der Hochschule Bonn Rhein-Sieg mit rund 2000 Teilnehmenden.

Die Wahl dieses Szenarios war aus Sicht des FKIE fachlich sinnvoll, da sich dort eine realistische mit einem Flughafen vergleichbare Hochlastsituation mit vielen Endgeräten, mehreren Access Points und dynamischen Personendichten beobachten ließ. Die Methodik wurde bewusst so ausgelegt, dass sie mit geringem Anpassungsaufwand auf einen Flughafen oder andere BOS/KRITIS-Standorte übertragbar ist.

Im Rahmen der Detailplanung wurden zwei jeweils rein passive Messmethoden vorgesehen:

- **WiFi-Survey durch Router/AP-Hardware**,
- **Monitor-Modus von WLAN-Karten**.

Beide Verfahren wurden so kombiniert, dass pro Beobachtungszeitraum definierte Kanäle erfasst und durch Sweep-Verfahren größere Spektrumsbereiche abgedeckt werden konnten. Zusätzlich wurden drei besonders aussagekräftige Messstandorte festgelegt:

- Foyer,
- Bereich vor dem Audimax,
- Bereich nahe eines zentralen Ausschanks.

Ein weiterer Schwerpunkt lag auf Datenschutz und Nichtbeeinflussung des Zielsystems. Die Messkampagne wurde vollständig passiv geplant, sodass keine aktive Interaktion mit dem vorhandenen WiFi erforderlich war.

Die Abweichung gegenüber der ursprünglichen standortspezifischen Planung bestand somit ausschließlich im Messort, nicht aber in der Zielsetzung. Das FKIE konnte dadurch ein robusteres, allgemeiner einsetzbares Messverfahren ausarbeiten.

II.1.3.4 AP-Nr. 3.4 – Vorbereitung der Tests und Demo

In AP3.4 setzte das FKIE die zuvor geplante Messinfrastruktur technisch um und validierte sie unter kontrollierten Bedingungen.

Zum Einsatz kamen handelsübliche WLAN-Karten sowie verfügbare Router-/AP-Hardware, die die notwendigen Messfunktionen unterstützten. Ergänzend entwickelte das FKIE ein verteiltes Softwareframework zur:

- Datenerfassung,
- Vorverarbeitung,
- Synchronisation,
- Visualisierung,
- redundanten Speicherung.

Ein besonderer Fokus lag auf der datenschutzkonformen Ausgestaltung. Identifizierende Merkmale wie MAC-Adressen wurden nicht dauerhaft gespeichert, sondern nur in aggregierter Form ausgewertet. Damit wurde ein praxisgerechter und für sensible Umgebungen geeigneter Messansatz geschaffen.

Zusätzlich wurden die Sensoren in robuste Gehäuse integriert (siehe Abbildung 1 und Abbildung 2), um die Geräte gegen Manipulation oder unbeabsichtigte Einflüsse zu schützen. In enger Zusammenarbeit mit dem Betreiber der FrOSCon wurden die Positionierungen der Sensoren präzisiert, wobei die Gewinnung aussagekräftiger Messdaten, die Verfügbarkeit von Strom- und Netzwerkversorgung, organisatorische Aspekte sowie der Ausschluss von Gefahren wie Stolperfallen für anwesende Personen im Fokus standen. Die Sensoren wurden mit einem Hinweisschild ausgestattet, um interessierte Personen auf das Projekt aufmerksam zu machen und über den Umfang erhobener Daten zu informieren (siehe Abbildung 3).

Als letzter Arbeitspunkt in AP3.4 wurde die Funktionalität des Gesamtsystems erfolgreich getestet. Die entwickelte Messinfrastruktur bildete die unmittelbare Grundlage für die Durchführung der Feldmessungen in AP4.

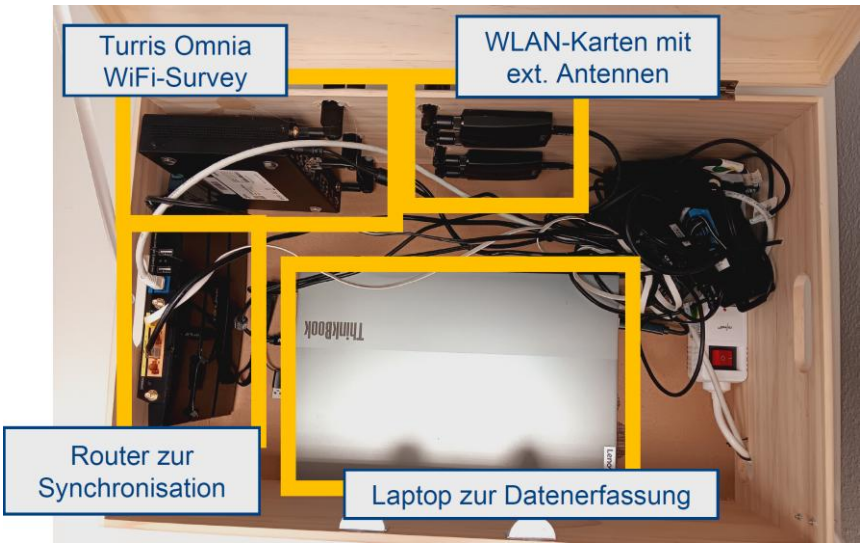


Abbildung 1. Initiale Version des passiven Sensors, wie in AP4 auf der FrOSCon verwendet

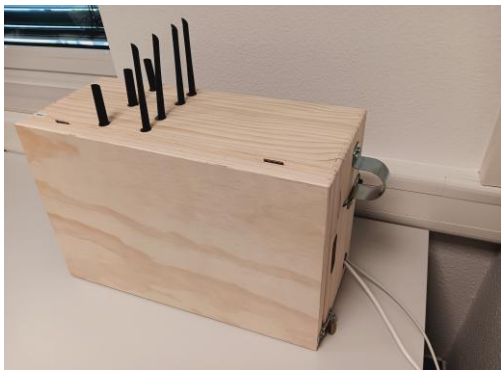


Abbildung 2. Verwendetes abschließbares Gehäuse zum Schutz vor Manipulation

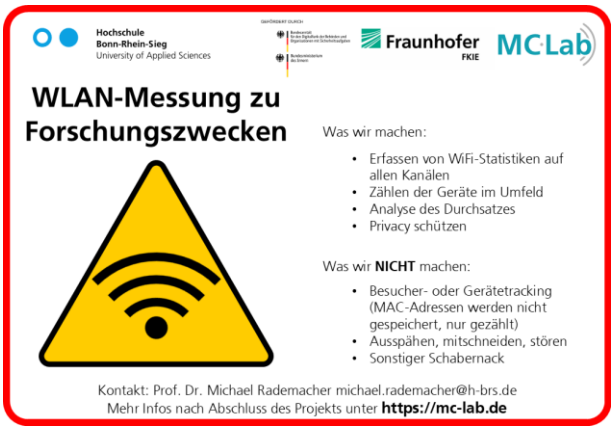


Abbildung 3. Hinweisschild, das auf jedem Sensor angebracht wurde

II.1.4 AP-Nr. 4 – Demonstration Use-Case

Im Arbeitspaket 4 führte das FKIE die geplante Feldmesskampagne erfolgreich durch. Die Messungen fanden am **16. und 17. August 2025** im Rahmen der FrOSCon 2025 statt.

Vor Ort wurden drei Messaufbauten an zentralen Punkten installiert. Erfasst wurden insbesondere:

- zeitliche Kanalauslastung,
- Anzahl beobachteter MAC-Adressen,
- Anzahl SSIDs,
- Größenordnung gesendeter Frames.

Die Messungen deckten durch parallelen Sensoreinsatz und Sweep-Verfahren die relevanten Kanäle im 2,4-GHz- und 5-GHz-Band ab. Der operative Aufbau erfolgte abgestimmt mit dem Veranstalter. Die Messgeräte waren gekennzeichnet, die Strom- und Netzversorgung war vorbereitet, und die Datenerhebung lief über den gesamten vorgesehenen Zeitraum stabil.

Die Auswertung der Daten zeigte ein klar positives Bild hinsichtlich der verfügbaren Spektrumreserven (siehe Abbildung 4 und Abbildung 5). Besonders hervorzuheben ist:

- selbst in Spitzenzeiten blieben mehrere Kanäle deutlich unter kritischer Auslastung,
- der am stärksten belastete Kanal erreichte im am stärksten ausgelasteten Zeitfenster nur rund **34–35 %** mittlere Belegung,
- mehrere Kanäle lagen selbst in 2-Stunden-Fenstern unter **15 %** durchschnittlicher Auslastung.

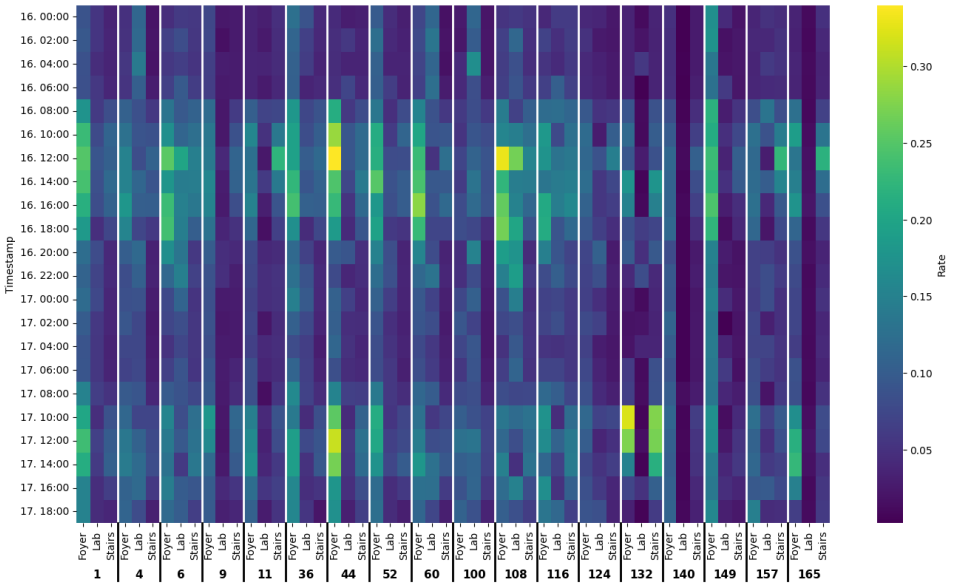


Abbildung 4. Durchschnittliche gemessene WiFi-Kanalauslastungen je über 2 Stunden. Über die Zeit (y-Achse) für verschiedene Standorte und Kanäle im 2,4GHz- und 5GHz-Spektrum (x-Achse). Die beiden Konferenztage heben sich deutlich von den Nachtzeiten mit fast keiner WiFi-Nutzung ab. Dennoch zeigt sich, dass das Spektrum auf vielen Kanälen selbst in hoch ausgelasteten Mittagszeiten noch zu einem großen Teil frei bleibt.

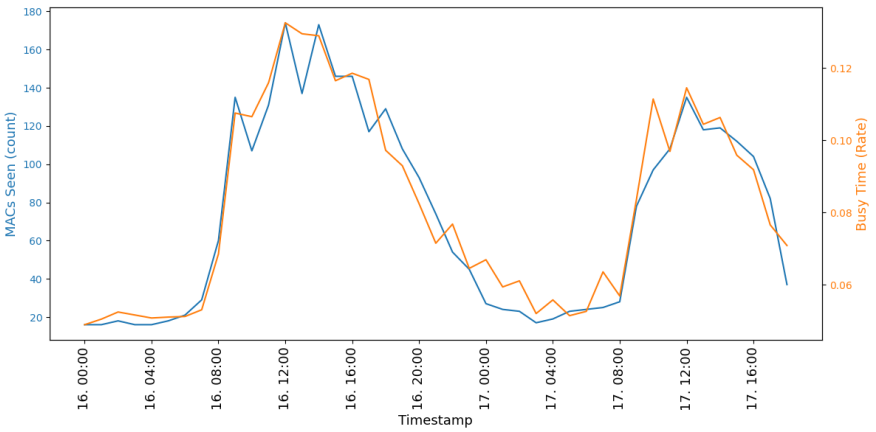


Abbildung 5. Exemplarische Messergebnisse für einen Kanal und einen Standort. Auf der x-Achse ist die Zeit dargestellt. Die y-Achse zeigt in blau die Anzahl gesehener MAC-Adressen und in orange die gemessene Kanalauslastung zum entsprechenden Zeitpunkt. Erwartungsgemäß zeigt sich, dass die Anzahl gesehener Geräte (MAC-Adressen) stark mit der gemessenen Kanalauslastung korreliert.

Für das FKIE ist dies ein zentrales Ergebnis: Selbst in hoch frequentierten Innenraumszenarien kann WiFi grundsätzlich ausreichende freie Spektrumsanteile bereitstellen, um einsatzkritische Dienste zu unterstützen – vorausgesetzt, dass Netzplanung, Standardwahl, Gerätestand und Sicherheitsmaßnahmen passen.

Die ursprünglich für den Flughafen gedachte Demonstration wurde damit erfolgreich in ein übertragbares Hochlastszenario überführt. Die Ziele des Arbeitspakets wurden vollständig erreicht.

Das Konzept der Messkampagne sowie erste vorläufige Ergebnisse wurden im Anschluss am 21. August 2025 im Rahmen der virtuellen Roadshow der BDBOS interessiertem Fachpublikum präsentiert.
Im Rahmen einer Veranstaltung am 13. Mai 2026 in Wunstorf bei der ATS Elektronik wurde ein zu diesem Zeitpunkt bereits weiterentwickelter und deutlich kompakterer Sensor praktisch demonstriert (siehe Abbildung 6), zudem wurden die abschließenden Ergebnisse der Messkampagne vorgestellt und diskutiert; auch bei diesem Termin waren diverse Anwender und Stakeholder sowie Vertreter von BDBOS und VDI/VDE präsent.

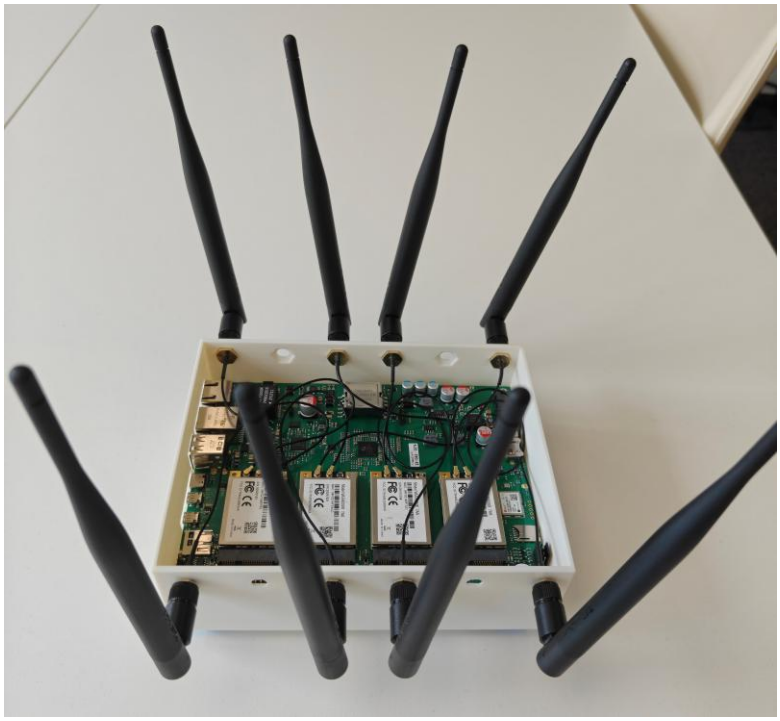


Abbildung 6. Weiterentwickelte deutlich kompaktere Version des passiven Sensors, hier ohne Abdeckung

II.1.5 AP-Nr. 5 – Maßnahmen und Handlungsempfehlungen

In AP5 führte das FKIE die eigenen Ergebnisse fachlich zusammen und leitete daraus belastbare Maßnahmen und Handlungsempfehlungen ab. Als Leiter dieses Arbeitspakets koordinierte das FKIE zudem die strukturelle Aufbereitung der Ergebnisse im Projektkontext; für den vorliegenden Bericht relevant sind die eigenen inhaltlichen Beiträge zu WLAN und WLAN-Sicherheit.
Die Ergebnisse wurden in konkrete Empfehlungen überführt. Für die **Eignung von WiFi für MCX-Dienste** wurden insbesondere folgende Maßnahmen abgeleitet:

- Nutzung moderner WiFi-Standards, mindestens WiFi 6,
- Trennung einsatzkritischer WLANs von sonstigen WLANs,
- Nutzung verfügbarer QoS-/Priorisierungsmechanismen, sofern technisch sinnvoll und implementiert,
- bevorzugte Nutzung des 6-GHz-Bandes in Innenräumen,
- hohe Netzabdeckung und gute Signalqualität im Zielgebiet,

- standortspezifische Messung der WLAN-Kanalauslastung vor einer produktiven Nutzung.

Für den Bereich **Sicherheit** wurden insbesondere folgende Empfehlungen formuliert:

- szenariobezogene Risikoeinschätzung möglicher Angreifer und Angriffe,
- Nutzung von WPA3-Enterprise ohne Transition Mode,
- konsequentes Update- und Patch-Management der eingesetzten Geräte.

Darüber hinaus wurde weiterer Forschungs- und Entwicklungsbedarf identifiziert, u. a. in den Bereichen:

- praktische Bewertung moderner Scheduler,
- Erprobung von r-TWT,
- Quantifizierung von MLO- und MU-MIMO-Effekten,
- Aufbau weiterer Referenzdatensätze an BOS-relevanten Standorten,
- Konkretisierung von Risikotaxonomien für WiFi-Angriffe im KRITIS-Kontext.

Die Arbeiten in AP5 seitens FKIE wurden vollständig abgeschlossen und stellen den inhaltlichen Schlusspunkt des FKIE-Teilvorhabens dar.

Da einige Projektpartner die Verlängerung des Projektes über Juni 2026 hinaus anstreben, ist damit zu rechnen, dass sich im Laufe der weiteren Arbeiten dieser Partner auch zusätzliche und konkretisiertere Handlungsempfehlungen ergeben. Da das FKIE keine weitere Verlängerung beantragt hat und damit ab Juli keine Projektarbeiten mehr ausführen darf und kann, wurde die weitere Leitung des AP ab Juli an die verlängernden Konsortialpartner übergeben.

II.2 Beitrag zu Zielen der Fördermaßnahme, voraussichtlicher Nutzen und Verwertbarkeit

Das Teilvorhaben hat einen unmittelbaren Beitrag zur Erreichung zentraler Ziele des Förderprogramms KoPa_45 geleistet. Dies betrifft insbesondere die **Stärkung der Resilienz und Cybersicherheit nationaler Kommunikationsinfrastrukturen** sowie die **Erprobung lokaler privater Netzzugänge** mit einem besonderen Fokus auf WiFi-Zugangsnetze. Inhaltlich wurde damit vor allem an die in der Bekanntmachung[1] benannten Interessengebiete **4 „Leitstellen, Smart Devices und sonstige Endgeräte“** und **5 „Netzbetrieb, -zugänge, -übergänge und Interworking“** angeknüpft. Aus Sicht des Fraunhofer FKIE standen insbesondere die folgenden in der Bekanntmachung veröffentlichten Forschungsfragen im Mittelpunkt[2]:

- Kommerzielle Mobilfunknetzbetreiber ergänzen mangelhafte Mobilfunkversorgung durch die 3GPP-standardisierte Option der Nutzung von WiFi-Access Points, zum Beispiel Voice over WiFi/WLAN-Call. Wie und unter welchen Voraussetzungen kann dieses Konzept analog auch für den breitbandigen Digitalfunk BOS, zumindest als „Last Resort“, genutzt werden (MC over WiFi)? (s. Frage 57)

[1] Bundesanzeiger vom 31.07.2023

[2] Die hier benannten Forschungsfragen wurden im Vergleich zu den Vorhabenbeschreibungen teils leicht angepasst und konkretisiert.

- Wie kann ein Konzept zur Nutzung von MC over Wifi für die Objektversorgung in zukünftigen Breitbandnetzen aussehen? (s. Frage 58)
- Wie zuverlässig ist eine WiFi-Nutzung durch MC-Clients unter Nutzung aktueller WiFi-Standards (WiFi 6 und WiFi 6E) und Nutzung BDBOS-eigener Access Points („Trusted non-3GPP Access“) in unlizenzierten Bändern und wie kann diese Zuverlässigkeit verbessert werden? Wie ist die Störsicherheit bei räumlicher Nähe mehrerer AP, zum Beispiel eines BDBOS-AP und eines anderen AP auf dem gleichen WiFi-Kanal? Welche Störungen und Attacken sind durch/mit handelsüblichen WiFi-Endgeräten auf private AP der BDBOS (Trusted non-3GPP Access) möglich und wie sind diese abzusichern? (s. Frage 59)

Darüber hinaus hat das Teilvorhaben auch, teils in Zusammenarbeit mit Partnern, Beiträge zur Beantwortung der folgenden Forschungsfragen geleistet:

- Wie lassen sich Anforderungen an Bandbreiten, Netzressourcen, Steuerung bei Ressourcenmangel (Sonderlagen), Verfügbarkeit, Robustheit, Nutzerverwaltung, Funktionen uvm. für die geplante Kommunikationsinfrastruktur berücksichtigen?
- Wie kann bei Großschadenslagen eine Überlastung des MC-Netzes aus Leitstellenperspektive vermieden werden und wie erfolgt dort eine Priorisierung der Kommunikation? Wie kann sichergestellt werden, dass neben der Großschadenslage noch andere Lagen bearbeitet werden können? (s. Frage 43)
- Wie und unter welcher Flexibilität können Integrationen von 5G-Campusnetzen erfolgen? Welche technischen und einsatztaktischen Anforderungen ergeben sich an den Netzbetrieb (von Teilnetzen)? (s. Frage 49)

Zugleich wurden die in der Teilvorhabenbeschreibung formulierten Ziele erreicht, nämlich die theoretische Bewertung der Eignung von WiFi und ergänzend 5G, die Analyse des unlizenzierten WiFi-Spektrums mittels eines passiven Messverfahrens, die sicherheitstechnische Einordnung der betrachteten Zugangsnetze sowie die Sicherung der Projektergebnisse und Formulierung von Handlungsempfehlungen.

Die im Vorhaben erzielten Ergebnisse können in mehreren Formen verwendet werden. Erstens stellen sie eine **technische und sicherheitstechnische Bewertungsgrundlage** für die Frage bereit, unter welchen Rahmenbedingungen WiFi für einsatzkritische Kommunikation überhaupt in Betracht kommt. Zweitens liegt mit dem entwickelten passiven Messverfahren ein **übertragbarer methodischer Ansatz** vor, mit dem die Kanalauslastung an konkreten Standorten vor einem produktiven Einsatz beurteilt werden kann. Drittens liefern die Ergebnisse **konkrete Handlungsempfehlungen** für Planung, Netztrennung, Priorisierung, Sicherheitskonfiguration und standortspezifische Eignungsprüfung. Damit sind die Resultate insbesondere für Planungs-, Bewertungs- und Entscheidungsprozesse bei BOS, KRITIS-Betreibern, Integratoren und Forschungseinrichtungen nutzbar.

Die Ergebnisse wurden von den beteiligten Organisationen im Verbund aufgenommen und in die übergreifenden Maßnahmen und Handlungsempfehlungen des Projekts integriert sowie in die gemeinsame Ergebnisdarstellung aufgenommen, beispielsweise bei den Veranstaltungen in Wunstorf

und auf dem 2. Innovationsforum. Beim Fraunhofer FKIE selbst sollen die Ergebnisse zeitnah als Grundlage für fachliche Transferaktivitäten, für die Weiterentwicklung von Bewertungsansätzen sowie für die Vorbereitung weiterer Forschungs- und Beratungsleistungen eingesetzt werden. Ein produktiver operativer Einsatz bei BOS-Anwendern außerhalb des Projektkontexts war hingegen nicht Gegenstand des Teilvorhabens.

Vollständigen Zugang zu den Ergebnissen haben die beteiligten Konsortialpartner. Darüber hinaus wurden und werden die Ergebnisse im Rahmen abgestimmter Präsentationen, Berichte, Transfer- und Veröffentlichungsformate zugänglich gemacht, so ist beispielsweise die Publikation der Ergebnisse auf einer wissenschaftlichen Konferenz derzeit in Arbeit. Rückmeldungen aus dem fachlichen Austausch bestätigten insbesondere den Bedarf an belastbaren Aussagen zur Nutzbarkeit von WiFi, zu Verfügbarkeitsrisiken im unlizenzierten Spektrum und zu praktikablen Verfahren der standortspezifischen Vorabbewertung. Gemeinsame Feldversuche mit BOS-Anwendern auf der ursprünglich vorgesehenen Flughafeninfrastruktur konnten aufgrund der veränderten Randbedingungen nicht in der geplanten Form umgesetzt werden; die praktische Erprobung erfolgte deshalb in einer realitätsnahen Hochlastumgebung. Eine Weiterführung des FKIE-Demonstrators im Sinne eines dauerhaften Produktbetriebs ist nicht vorgesehen. Fachlich anschlussfähig und geplant im Sinne künftiger Folgearbeiten sind jedoch eine **Erweiterung des Messansatzes auf weitere BOS- und KRITIS-relevante Standorte** sowie die **Einbeziehung neuer WiFi-Mechanismen** und weiterer Belastungsszenarien.

Tabelle 2. Verwertungsplan

Vorhabenergebnisse und ihre Verwertung	**… aktuell**	**… voraussichtlich innerhalb der nächsten zwei Jahre**
Schutzrechte: z.B. Patente, Lizenzen, Vergabe von Lizenzen an Dritte	Nein, im Vorhaben sind keine schutzwürdigen Erfindungen oder Entwicklungen entstanden.	
Beiträge für die Standardisierung, z. B. 3GPP	Nein, das FKIE ist nicht aktiv an Standardisierungsprozessen beteiligt und kann allenfalls als Auftragsnehmer Beratungs- und Evaluationsleistungen dazu anbieten.	
Produkte: z.B. Komponentenverbesserung, Erweiterung des Produktportfolios mit neuen oder verbesserten Produkten	Nein, die Vermarktung von Produkten ist kein Teil der Strategie des FKIE.	
Technologie: z.B. verbesserter Fertigungsprozess, Messverfahren… Verfahren bei der Fertigung von Produkten bzw. Erstellung von Dienstleistungen	Verfügbares passives Messverfahren zur Beurteilung von WiFi-Spektrumsreserven in Hochlastszenarien.	Ausbau zu einem Bewertungs- und Messansatz für weitere Standorte und Szenarien.

Dienstleistungen: z.B. erweiterte Beratungs- und Zuliefermöglichkeiten… Neue oder verbesserte Dienstleistungen	Derzeit noch kein Angebot von Dienstleistungen.	Nutzung der Ergebnisse in (Auftrags-)Forschungs-, Evaluations- und Beratungsleistungen insb. für Betreiberinnen kritischer Infrastrukturen bei Interesse.
Know-how Transfer: z.B. in interdisziplinäre Bereiche, Anschlussfähigkeit an weitere Forschungs- und Entwicklungsvorhaben	Ergebnisse werden intern in Forschung und Projektanbahnung genutzt.	Anschluss an Folgevorhaben zu resilienten Breitbandnetzen, Campusnetzen, sicherer mobiler Kommunikation und MCX-nahen Infrastrukturen, falls Förderung verfügbar.
Wissenstransfer: z.B. durch Verbesserung von Forschung und Lehre, Veröffentlichungen	Projektberichte, Präsentationen und fachliche Aufbereitung im FKIE.	Fachvorträge, Lehrveranstaltungen und wissenschaftliche Publikationen bzw. transferorientierte Beiträge. Angebot von Schulungen für KRITIS-/BOS-Akteurinnen.
Netzwerk und Ökosystem: z.B. Teilnahme an Veranstaltungen	Einbindung in Roadshow- und Demonstrationsformate sowie Vernetzungsevents des Projekts.	Fortsetzung des fachlichen Austauschs mit Forschungspartnerinnen, Anwenderinnen und weiteren KRITIS-/BOS-nahen Akteurinnen; Nutzung der im Projekt entstandenen Synergieeffekte.

II.2.1 Wirtschaftliche Erfolgsaussichten nach Vorhabenende

Wie bereits in der Teilvorhabenbeschreibung dargelegt, ergeben sich die wirtschaftlichen Erfolgsaussichten des Teilvorhabens nicht primär aus einer unmittelbaren Produktvermarktung, sondern aus der Verwertung der Ergebnisse in Form von **Forschungs- und Entwicklungsleistungen**, **Beratungs- und Evaluationsleistungen**, **Transfer- und Schulungsformaten** sowie der **Einwerbung**

weiterer Drittmittel. Diese Einschätzung hat sich im Projektverlauf nicht geändert; sie wird durch die erzielten Ergebnisse nun inhaltlich konkretisiert.

Eine Konkurrenzlösung im engeren produktspezifischen Sinn wurde im Teilvorhaben nicht entwickelt. Der funktionale Vorteil der Ergebnisse liegt vielmehr in einem **herstellerunabhängigen, übertragbaren und datenschutzkonformen Bewertungsansatz**. Gegenüber rein theoretischen Eignungsbewertungen oder punktuellen Einzelmessungen besteht der Mehrwert insbesondere in der Verbindung von **Technologieanalyse, Sicherheitsbewertung und praktischer Messung**. Wirtschaftlich liegt der Vorteil vor allem darin, dass Planungs- und Investitionsentscheidungen belastbarer vorbereitet werden können und Fehleinschätzungen zur Eignung von WiFi für einsatzkritische Kommunikation verringert werden.

Ein Nutzen ergibt sich für verschiedene Anwendergruppen und Branchen am Standort Deutschland, insbesondere für **BOS-nahe Organisationen**, **Betreiber kritischer Infrastrukturen**, **Flughäfen**, **Bahnhöfe**, **Veranstaltungsstätten**, **Industrie- und Campusnetzbetreiber**, **Systemintegratoren** sowie **öffentliche und private Planungs- und Bewertungsakteure**. Die Ergebnisse können dort sowohl für Neubewertungen bestehender Infrastrukturen als auch für die Planung zukünftiger heterogener Kommunikationsarchitekturen eingesetzt werden.

Die Umsetzungs- und Transferstrategie entspricht der in der Teilvorhabenbeschreibung beschriebenen Linie und wird nun durch konkrete Projektergebnisse unterlegt. **Kurzfristig** werden die Ergebnisse in Transfergesprächen, Beratungs- und Evaluationsleistungen, Schulungsformaten und wissenschaftlichen Veröffentlichungen genutzt. **Mittelfristig** sind sie als Grundlage für Folgeprojekte, vertiefende Standortbewertungen und anwendungsnahe Forschungs- und Entwicklungsaufträge verwertbar. **Langfristig** können sie in die Planung und Bewertung kommender breitbandiger BOS-/KRITIS-Kommunikationslösungen einfließen.

Zukünftige Einsatzorte der Ergebnisse sind insbesondere Standorte mit hohem Kommunikations- und Schutzbedarf, etwa Flughäfen, Bahnhöfe, Großveranstaltungsflächen, Industrieareale und sonstige KRITIS-Standorte. Wesentliche Hürden für die Umsetzung liegen in der **standortspezifischen Heterogenität der Funkumgebungen**, in **regulatorischen und organisatorischen Zugangsfragen**, in der **begrenzten Verfügbarkeit fortgeschrittener QoS-Mechanismen in kommerziellen WiFi-Produkten**, in der **Notwendigkeit aktueller und sicher konfigurierter Hardware** sowie in den **grundsätzlichen Verfügbarkeitsrisiken unlizenzierten Spektrums**. Diese Hürden wurden im Projekt jedoch nicht nur sichtbar gemacht, sondern auch methodisch adressiert.

II.2.2 Wissenschaftliche und/oder technische Erfolgsaussichten nach Vorhabenende

Die in der Teilvorhabenbeschreibung dargestellten wissenschaftlichen und technischen Erfolgsaussichten bestehen unverändert fort und wurden durch die Projektergebnisse substanziell konkretisiert. Dies betrifft insbesondere die **systematische Analyse moderner WiFi-Standards**, die **strukturierte Bewertung realistischer Angriffsszenarien**, die **Entwicklung eines passiven Messverfahrens** sowie die **Erhebung und Auswertung von Messdaten in einer realitätsnahen Hochlastumgebung**.

Die Ergebnisse können in anderer Weise als über eine unmittelbare wirtschaftliche Verwertung hinaus genutzt werden. Sie eignen sich insbesondere für **öffentliche Aufgaben der technischen Bewertung und Planung**, für **wissenschaftliche Referenz- und Vergleichszwecke**, für **Transferstellen und Schulungsformate**, für **Hochschullehre und wissenschaftliche Qualifikation** sowie als Grundlage für **weitere methodische Entwicklungen** und fördern so den Wissenschaftsstandort Deutschland. Da belastbare Datensätze über die WLAN-Kanalauslastung an hochfrequentierten Orten über mehrere Tage kaum öffentlich publiziert wurden, stellen das entwickelte Messverfahren und die gewonnenen Daten eine wertvolle Referenzbasis für weitere Untersuchungen dar, etwa zur Bewertung ähnlicher Standorte oder zur methodischen Weiterentwicklung von Eignungsindikatoren für WiFi in einsatzkritischen Szenarien.

Die Perspektive für die Kooperation ist positiv. Das Vorhaben hat gezeigt, dass die Zusammenarbeit zwischen Industriepartnern, Forschungseinrichtungen und anwendungsnahen Akteuren einen hohen fachlichen Mehrwert und starke Synergieeffekte erzeugt. Für das Fraunhofer FKIE bestehen daraus konkrete Anknüpfungspunkte für weitere gemeinsame Aktivitäten mit den Verbundpartnern, insbesondere in Form von **gemeinsamen Veröffentlichungen**, **weiteren Mess- und Bewertungsarbeiten**, **fachlichem Transfer** sowie möglichen **Folgeanträgen**. Zum Zeitpunkt der Berichtserstellung liegt zwar kein bereits bewilligtes gemeinsames Anschlussvorhaben vor; die inhaltliche Kooperationsperspektive ist jedoch klar gegeben.

Der zeitliche Horizont entspricht im Wesentlichen der Einschätzung aus der Teilvorhabenbeschreibung. **Kurzfristig** sind die Ergebnisse für Berichtswesen, Transfer, Lehre und Veröffentlichungen nutzbar; insbesondere ist eine wissenschaftliche Publikation des Messverfahrens und der erzielten Ergebnisse auf einer internationalen Konferenz geplant. **Mittelfristig** sind sie anschlussfähig für Folgeforschung, Vergleichsmessungen und weitergehende Bewertungs- und Sicherheitskonzepte. **Langfristig** können sie zur methodischen Fundierung der Nutzung heterogener Zugangsnetze in einsatzkritischen Kommunikationsarchitekturen beitragen.

II.2.3 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Auch die in der Teilvorhabenbeschreibung dargestellte wissenschaftliche und wirtschaftliche Anschlussfähigkeit hat sich nicht grundlegend verändert. Die Projektergebnisse zeigen vielmehr klar, welche nächsten innovatorischen Schritte für eine erfolgreiche Umsetzung erforderlich sind. Dies betrifft insbesondere die **weitere Validierung neuer WiFi-Mechanismen** auch kommender Standards für einsatzkritische Dienste, die **Gewinnung zusätzlicher Referenzdatensätze** an BOS- und KRITIS-relevanten Standorten, die **szenariospezifische Sicherheits- und Risikobewertung** sowie die **Überführung der gewonnenen Erkenntnisse in praktisch einsetzbare Bewertungs- und Beratungsansätze**.

Weiterer Forschungsbedarf ergibt sich insbesondere in folgenden Punkten:

- praktische Bewertung der in Access Points implementierten Scheduling-Mechanismen für MCX-nahe Lastprofile,

- experimentelle Untersuchung neuer Priorisierungsmechanismen wie **r-TWT**, sobald diese breiter verfügbar sind,
- vertiefte Bewertung von **MLO**, **MU-MIMO** und weiteren neuen WiFi-Funktionen im Kontext einsatzkritischer Kommunikation,
- Erhebung zusätzlicher Referenzdatensätze in weiteren Hochlast- und BOS-relevanten Szenarien,
- Entwicklung belastbarer Kriterien und Schwellenwerte für die Eignungsbewertung von WiFi an konkreten Standorten,
- weitere Konkretisierung einer szenariospezifischen Risikotaxonomie für Angriffe und Störungen gegen WiFi-basierte Zugänge.

Insgesamt bestätigen die Ergebnisse damit die in der Teilvorhabenbeschreibung dargestellte Anschlussfähigkeit sowohl wissenschaftlich als auch wirtschaftlich. Das Vorhaben hat belastbare Ausgangspunkte für weitere Forschung, Transfer- und Bewertungsleistungen geschaffen.

III. Anlagen

III.1 Wichtige Positionen des zahlenmäßigen Nachweises

Die Ausgabenstruktur des Teilvorhabens entsprach im Wesentlichen der in der Teilvorhabenbeschreibung dargestellten Ressourcenplanung. Der größte Anteil der Fördermittel entfiel auf projektgebundene Personalausgaben. Die Sachmittel wurden demgegenüber in deutlich geringerem Umfang eingesetzt und dienten vor allem dem Aufbau des in der Teilvorhabenbeschreibung vorgesehenen Labor- und Messaufbaus für die Arbeiten in AP3 und AP4.

Mit den Fördermitteln wurde – entsprechend der Teilvorhabenbeschreibung – projektgebunden wissenschaftliches Personal für die Bearbeitung der Arbeitspakete AP1 bis AP5 finanziert. Ein Einsatz grundfinanzierten Personals war für die Durchführung des Teilvorhabens nicht vorgesehen. Die Personalmittel wurden insbesondere für die technologie- und sicherheitstechnische Analyse moderner Zugangstechnologien, die Konzeption und Implementierung des passiven Messverfahrens, die Laborerprobung, die Durchführung der Feldmessungen sowie die Auswertung und Ableitung von Maßnahmen und Handlungsempfehlungen benötigt, ebenso für die unten beschriebenen Maßnahmen der Öffentlichkeitsarbeit.

Die technischen Beschaffungen standen in unmittelbarem Zusammenhang mit den in der Teilvorhabenbeschreibung vorgesehenen Positionen für den „Messaufbau“ und den „Laboraufbau WiFi“. Tatsächlich beschafft wurden vor allem Komponenten für die Sensorik des passiven WiFi-Messsystems, für offene bzw. flexibel konfigurierbare WiFi-Clients sowie für ein kleines Labor- und Referenznetz zur Vorbereitung und Validierung der Messungen.

Die Beschaffungen lassen sich in folgende Kategorien gliedern:

- **Messsensorik und offene Client-Hardware** (1476,11€) genutzt für Konzeption, Aufbau und Erprobung des passiven Messsystems sowie für die Durchführung der Messungen:
    - 2 Router-Boards
    - 20 WiFi 6E WLAN-Karten
    - 2 Single Board Computer zur Ansteuerung der Sensoren
    - Diverses Material: Adapter, Konverter, Netzteile, USB-Hubs, Metallgehäuse
- **Laboraufbau WiFi** (809,28€) genutzt für Aufbau, Konfiguration, Validierung und öffentliche Demonstration einer aktuellen WiFi-Testumgebung:
    - 2 WiFi 7 Access Points
    - 1 Cloud Gateway Fiber
    - Gigabit-Router mit PoE
    - SFP+-RJ45-Adapter und CAT6-Patchkabel

Die tatsächlichen Beschaffungen stehen damit in klarem sachlichen Zusammenhang mit der Teilvorhabenbeschreibung. Abweichungen betrafen im Wesentlichen nicht den Zweck, sondern die konkrete Produktauswahl. Dies war in der Teilvorhabenbeschreibung ausdrücklich angelegt, da dort auf mögliche Anpassungen aufgrund von Marktverfügbarkeit, technologischer Weiterentwicklung, insbesondere WiFi 7, sowie aufgrund von Ergebnissen aus AP1 und AP2 hingewiesen wurde. Die in der

Teilvorhabenbeschreibung alternativ genannte SDR-basierte Messtechnik musste nach der methodischen Festlegung in AP3.3 nicht beschafft werden, da sich für den verfolgten passiven Messansatz handelsübliche WiFi-Hardware als fachlich geeignet und wirtschaftlich ausreichend erwies. Die Fördermittel waren notwendig, weil die Arbeiten einen zusätzlichen, projektbezogenen Forschungs- und Entwicklungsaufwand verursacht haben, der nicht innerhalb der Regelorganisation des Fraunhofer FKIE durchgeführt werden konnte. Dies betrifft sowohl den personellen als auch den sachlichen Aufwand. Das Teilvorhaben umfasste keine routinemäßigen Daueraufgaben des Instituts, sondern klar abgrenzbare zusätzliche Arbeiten im Rahmen des Förderaufrufs KoPa_45, insbesondere:

- die systematische Analyse moderner drahtloser Zugangstechnologien für einsatzkritische Kommunikation,
- die Entwicklung eines eigenständigen passiven Messverfahrens,
- den Aufbau und die Validierung eines projektspezifischen Messsystems,
- die Durchführung und Auswertung realer Messkampagnen,
- die Ableitung übertragbarer Maßnahmen und Handlungsempfehlungen,
- sowie begleitende Maßnahmen der Öffentlichkeitsarbeit.

Hinzu kommt, dass die hierfür benötigte Hardware nicht der Grundausstattung des Instituts zuzurechnen war, sondern projektspezifisch für den Mess- und Laboraufbau benötigt wurde. Ohne die Förderung hätten die Arbeiten daher weder zeitnah noch in der erforderlichen fachlichen Tiefe durchgeführt werden können. Die Zuwendung war somit Voraussetzung dafür, das Teilvorhaben mit der vorgesehenen wissenschaftlich-technischen Qualität umzusetzen.

III.2 Zusammenarbeit und Projektmanagement

Im Folgenden soll kurz dargestellt werden, wie die Zusammenarbeit mit den Konsortialpartnern sowie der BDBOS und der VDI/VDE Innovation + Technik GmbH erlebt wurde.

III.2.1 Zusammenarbeit im Konsortium

Die Zusammenarbeit innerhalb des Konsortiums wurde über die gesamte Projektlaufzeit als sehr positiv erlebt. Sie war geprägt von einem partnerschaftlich, professionell, produktiv und pragmatisch gestalteten Miteinander, klaren Zuständigkeiten, hoher Verlässlichkeit und einem offenen, vertrauensvollen Austausch. Ein wesentlicher Erfolgsfaktor war die kontinuierliche Abstimmung in einer festen, in der Regel einmal wöchentlich stattfindenden Videokonferenz, ergänzt durch bedarfsorientierte bilaterale und themenspezifische Gespräche; dadurch konnten Zwischenergebnisse, technische Abhängigkeiten, organisatorische Fragestellungen und mögliche Risiken frühzeitig transparent gemacht und gemeinsam bearbeitet werden. Ergänzend wurde der Austausch durch mehrere persönliche Treffen und Demonstrationstermine vertieft, die für die gemeinsame Bewertung von Zwischenergebnissen, die Abstimmung von Schnittstellen sowie die Schärfung des gemeinsamen Projektverständnisses besonders förderlich waren. Herausforderungen ergaben sich vor allem aus externen Randbedingungen, insbesondere veränderten Infrastrukturverfügbarkeiten, technischen Abhängigkeiten zwischen den Teilbeiträgen sowie dem erhöhten Abstimmungsbedarf bei der

Zusammenführung einzelner Demonstrationsbausteine; diese wurden im Konsortium jedoch jederzeit lösungsorientiert, flexibel und gemeinsam adressiert. Verbesserungspotential bestand daher weniger in der Zusammenarbeit selbst als vielmehr in einer noch früheren verbindlichen Klärung externer Rahmenbedingungen und Verfügbarkeiten. Insgesamt hat die enge, konstruktive und zielgerichtete Zusammenarbeit wesentlich zum erfolgreichen Projektverlauf beigetragen.

III.2.2 Zusammenarbeit mit der BDBOS und VDI/VDE Innovation + Technik GmbH

Wir bedanken uns herzlich für die Organisation der Projektreihe und die damit verbundene Gelegenheit, den Digitalfunk der Zukunft in Deutschland aktiv mitzugestalten. Insbesondere das Angebot der zwei hervorragend organisierten Innovationsforen in Berlin, zu denen wir gern aktiv beigetragen haben, möchten wir positiv hervorheben. Die Möglichkeit des direkten Austausches vor Ort haben wir als sehr förderlich und motivierend für die Projektbearbeitung empfunden, zudem haben sich neue Kontakte ergeben, die nicht nur zu wertvollen Synergieeffekten für diese Förderrichtlinie geführt haben, sondern absehbar zu weiteren innovativen Vorhaben und Partnerschaften führen werden.

Positiv wollen wir auch hervorheben, dass operative Aspekte wie Verlängerungen, Mittelverschiebungen, Änderungen am Zeitplan und die Erstattung der Reise zum 1. Innovationsforum mit geringem bürokratischen Aufwand möglich waren.

Im Rückblick auf den Projektverlauf und die erreichten Ziele sowohl unseres Projektes MissionXconnect als auch der anderen Projekte der Förderrichtlinie sind wir überzeugt, dass KoPa_45 erfolgreich einen wichtigen Beitrag zum Digitalfunk der Zukunft liefern kann. Wir freuen uns bereits darauf, den positiven Einfluss der Erkenntnisse aus der Förderrichtlinie in absehbarer Zukunft in wegweisenden Entscheidungen zum Digitalfunk verwirklicht zu sehen.

III.3 Übersicht der Maßnahmen der Öffentlichkeitsarbeit

Im Projektverlauf wurde die breite Öffentlichkeit in diversen Veranstaltungen über den Verlauf und die zum jeweiligen Zeitpunkt vorliegenden Ergebnisse des Vorhabens informiert.

III.3.1 Innovationsforum 2024

Datum	12.-14. Juni 2024
Ort	Berlin, Tagungswerk
Maßnahme / Veranstaltung	1. Innovationsforum der BDBOS zu KoPa_45
Art	Posterpräsentation
Zielgruppe	Fachöffentlichkeit, Förderumfeld (inkl. BDBOS, VDI/VDE), interessierte Anwender
Inhalt (aller Konsortial-partner)	Darstellung des Projekts und der Projektziele auf einem gemeinsamen Poster; Teilnahme von Vertretern einiger Projektpartner auf Panels
FKIE-Beitrag	Darstellung des Projekts und der Projektziele auf Poster

III.3.2 Virtuelle Roadshow

Datum	21. August 2025
Ort	online
Maßnahme / Veranstaltung	Virtuelle Roadshow der BDBOS zu KoPa_45 Thema 2: Einsatzkritische und -unterstützende Applikationen & MCX
Art	Folienpräsentation
Zielgruppe	Fachöffentlichkeit, Förderumfeld (inkl. BDBOS, VDI/VDE), interessierte Anwender
Inhalt (aller Konsortial-partner)	Darstellung des Projektverlaufs aller Konsortialpartner: Vorstellung der Projektthemen und -ziele, Konkretisierung von Lösungsansätzen, geplante und bereits begonnene Implementierungen, bereits erzielte Zwischenergebnisse
FKIE-Beitrag	Darstellung der FKIE-Ergebnisse zur Nutzung von WiFi für MC-Services, technologischen Chancen und Grenzen sowie zum Messansatz

III.3.3 Demonstration der technischen Realisierungen

Datum	13. Mai 2026
Ort	Wunstorf, Räumlichkeiten der ATS Elektronik
Maßnahme / Veranstaltung	Demonstration der Projektergebnisse
Art	Folienpräsentationen, Diskussion, praktische Demonstrationen, Postersession
Zielgruppe	Förderumfeld (inkl. BDBOS, VDI/VDE), Stakeholder, interessierte Anwender. Gäste
Inhalt (aller Konsortial-partner)	Darstellung der Projektergebnisse und technischen Realisierung: Vorstellung der Projektpartner, -themen und -ziele; Diskussionen mit Anwendern und Stakeholdern zu Anforderungen; technische Erläuterung und Vergleich möglicher Lösungsansätze und Darstellung der gewählten Ansätze; praktische technische Demonstration der Funkkopplung anhand zweier Showcases: a) Direkte Kopplung, b) Kopplung via Leitstelle ASGARD; Herausforderungen der Ende-zu-Ende-Sicherheit sowie WiFi-Nutzung
FKIE-Beitrag	Postersession mit Vorstellung der Ergebnisse und Schlussfolgerungen aus den durchgeführten Messungen; praktische technische Demonstration der Auslastungsmessungen; Diskussion zur Nutzbarkeit von WiFi für einsatzkritische Dienste im Hinblick auf Gütekriterien, Störfaktoren sowie Angriffsszenarien

III.3.4 Innovationsforum 2026

Datum	8. - 10. Juni 2026
Ort	Berlin, Tagungswerk
Veranstaltung	2. Innovationsforum der BDBOS zu KoPa_45
Art	Posterpräsentation, Folienpräsentationen, Teilnahme an Panels, Workshops
Zielgruppe	Förderumfeld (inkl. BDBOS, VDI/VDE), Stakeholder, interessierte Anwender
Inhalt (aller Konsortial-partner)	Darstellung der Projektergebnisse mittels gemeinsamem Poster sowie in Präsentationen zum Lösung/Technik-Panel sowie zum Zukunftspanel. Einbringen der Schlussfolgerungen und Erfahrungen aus dem Projekt in Paneldiskussionen sowie Themenworkshops.
FKIE-Beitrag	Darstellung des Projekts und der Projektergebnisse im Bezug auf die Nutzbarkeit von WiFi auf dem Poster, in einer Präsentation sowie in der Diskussion zum Zukunftspanel (s. Abbildung 7). Einbringen der Schlussfolgerungen und Erfahrungen aus dem Projekt im Themenworkshop „Netzbetrieb, -zugänge & -übergänge“.  **Abbildung 7.** Redebeitrag von Prof. Michael Rademacher zu den Ergebnissen des Vorhabens auf dem 2. Innovationsforum in Berlin

III.4 Übersicht der Schutzrechtsanmeldungen

Im Rahmen dieses Teilvorhabens sind seitens FKIE keine Schutzrechte angemeldet worden; ebenso bestehen keine Bestrebungen dazu.