Autoren	Hinterkircher, Dennis – PHYSEC GmbH Jansen, Kai – PHYSEC GmbH Zenger, Christian– PHYSEC GmbH Sabanovic, Kevin – Technische Universität Dortmund Arendt, Christian – Technische Universität Dortmund Boshoff, Marius – Ruhr-Universität Bochum Luong, Tommy – Ruhr-Universität Bochum Moldovan, Christian – comnovo GmbH
Veröffentlichungsdatum	21.06.2024
Schlüsselwörter	5G, 5Guarantee, Anomaliedetektion, Basisstationen, Campusnetz, Convolutional Neural Network, funktionale Sicherheit, Kommunikationsadapter, Orchestrator, Performance Level, physische Angriffe, Retro-Fit, Sicherheit, Sicherheitsmaßnahmen, Wi-Fi 6

IT-Sicherheit-Handlungsempfehlungen zur Nutzung von 5G-Lösungen

Dennis Hinterkircher (dennis.hinterkircher@physec.de), Kai Jansen (kai.jansen@physec.de), Christian Zenger (christian.zenger@physec.de), Kevin Sabanovic (kevin.sabanovic@tu-dortmund.de), Christian Arendt (christian.arendt@tu-dortmund.de), Marius Boshoff (boshoff@lps.ruhr-uni-bochum.de), Tommy Luong (luong@lps.ruhr-uni-bochum.de), Christian Moldovan (moldovan@comnovo.de)

I. Motivation

Durch das erste Aufkommen von 5G sind neue Möglichkeiten der drahtlosen Kommunikation entstanden. Begriffe wie eMBB (enhanced Mobile Broadband), mMTC (massive Machine Type Communication) sowie URLLC (Ultra Reliable Low Latency Communications) versprechen einen hohen Datendurchsatz, eine hohe Verfügbarkeit sowie eine hohe Dichte an Geräten. Mit der Vergabe im Frequenzbereich 3,7 bis 3,8 GHz wurde in Deutschland zusätzlich der Weg für kostengünstige 5G-Campusnetze geebnet, wodurch ein Einsatz in industriellen Umgebungen immer attraktiver zu werden scheint. Während der oft genannte URLLC-Anwendungsfall des automatisierten vernetzten Straßenverkehrs einen breiten 5G-Ausbau erfordert, sind hochmobile Szenarien auf Firmengeländen deutlich zeitnäher umzusetzen und erlauben es 5G „Marketing-Claims“ zu validieren. Aber auch vielgenannte Negativbeispiele wie der mögliche Einfluss von 5G bzw. Funkwellen auf Personen und Umwelt lassen sich mit einem eigenen 5G-Campusnetz untersuchen. Da Basisstationen nun auch in ungeschützten Umgebungen, wie z. B. an Hauswänden, installiert werden können, sind neue Sicherheitsmaßnahmen zu treffen. Dies stellt einen Paradigmenwechsel dar, da gewohnte Schutzmaßnahmen nicht mehr ausreichend sind. So müssen neue Maßnahmen ergriffen werden, die neben digitalen Angriffen auch physische Angriffe auf die Systeme berücksichtigen. Besonders in Zeiten fortgeschrittener Angreifer, wird der Fokus nicht ausreichend genug auf die (physische) Sicherheit von 5G gelegt. Oftmals hängt ein sicherer Betrieb davon ab, wie ein System aufgebaut wurde und wie man mit Zugriffen sowohl intern als auch extern umgeht.

Abbildung 1: Vision einer vernetzten Industrieumgebung mithilfe eines 5G-Campusnetzes.

II. Aufbau des Whitepapers

Das Ziel dieses Whitepapers ist die Zusammenfassung der wesentlichen Ergebnisse und Handlungsempfehlungen aller beteiligten Konsortialpartner aus Sicht der (IT-)Sicherheit.
In Kapitel III wird der Erfahrungsbericht beim Aufbau und der Nutzung von 5G-Campusnetzen des RUB-LPS für den Retro-Fit Use-Case dargestellt. Die TU Dortmund stellt in Kapitel IV ein Konzept zur Anomaliedetektion im Frequenzbereich von 5G-Campusnetzen vor, wodurch unerwünschte Störungen von erwünschten Nutzsignalen unterschieden werden können. Im Anschluss wird in Kapitel V von comnovo erörtert, ob 5G ausreichend zuverlässig ist, um Gefahren für Personen, Umwelt und Infrastruktur zu minimieren. Den Abschluss bildet Kapitel VI, in welchem die PHYSEC einen 5G-Orchestrator nutzt, um IT-Sicherheitsangriffe zu detektieren.

III. Erfahrungsbericht beim Aufbau und Nutzung von 5G-Campusnetzen (LPS - RUB)

In der Lern- und Forschungsfabrik (LFF) des Lehrstuhls für Produktionssysteme (LPS) wurde im Rahmen des Forschungsprojektes 5Guarantee ein lokales 5G-Campusnetz aufgebaut, um verschiedene Anwendungsszenarien in einer industrienahen Produktionsumgebung zu erproben [1]. Für die Integration von Endgeräten wie Produktionsanlagen, Sensoren oder Robotern in ein 5G Netz wird ein 5G Kommunikationsadapter benötigt, der idealerweise nach dem Plug-and-Play Prinzip funktioniert und die Nachrüstung älterer Maschinen ermöglicht. Im Zuge des Projektes wurden daher verschiedene Hardwarelösungen für die Anbindung diverser Endgeräte in der LFF erprobt.
Der vorliegende Erfahrungsbericht ist in die Kategorien *Hardware-Integration*, *Inbetriebnahme* und *Quality-of-Service* (QoS) gegliedert. Es wird sowohl auf die im Einsatz aufgetretenen Stärken als auch auf die Schwächen eingegangen. Dadurch kann ein Vergleich zwischen den anfänglichen Marketingaussagen und der tatsächlichen Implementierung des 5G-Campusnetzes durchgeführt werden. Weiterhin wird verdeutlicht, dass 5G zwar technologisch die Möglichkeit bietet, Anwendungsszenarien mit zuverlässiger, drahtloser Kommunikation zu realisieren, jedoch die höhere Komplexität eine große Hürde darstellt. Der Erfahrungsbericht wurde auf Basis der Nutzung einer softwarebasierten 5G-Lösung von CableFree erstellt und dient nicht als Referenz für Lösungen von Herstellern oder Netzanbietern wie Ericsson oder Telekom. Dennoch ist zu beachten, dass Erfahrungen mit der Nutzung von 5G auch bei der Entscheidungsfindung für die Planung einer Netzinfrastruktur eine wichtige Rolle spielen können, selbst wenn softwarebasierte Lösungen eingesetzt werden.

a. Flexible Hardware-Integration und Retro-Fit-Ansatz

Für die Integration der kompakten Kommunikationsadapter hat sich der LPS nach Evaluierung mehrerer Hardwarekomponenten gängiger Hersteller für ein USB-Carrier-Board mit M2-Schnittstelle für das 5G-Modul entschieden. Dieser Hardwareaufbau ermöglicht eine flexible Anbindung von Endgeräten und unterstützt verschiedene Endgerätetypen oder Plattformen mit 5G über eine USB-Schnittstelle. Insbesondere spielt Flexibilität bei der Integration von 5G in die Flugrobotik eine wichtige Rolle [2]. Dabei sind Gewicht und Abmaße des Kommunikationsadapters kritische Faktoren, um eine optimale Funktionalität zu gewährleisten (siehe Abbildung 2). Der Ansatz der Edge-Server-Architektur wurde genutzt, um die Drohne mittels 5G zuverlässig mit einer zentralen Recheneinheit zu steuern.

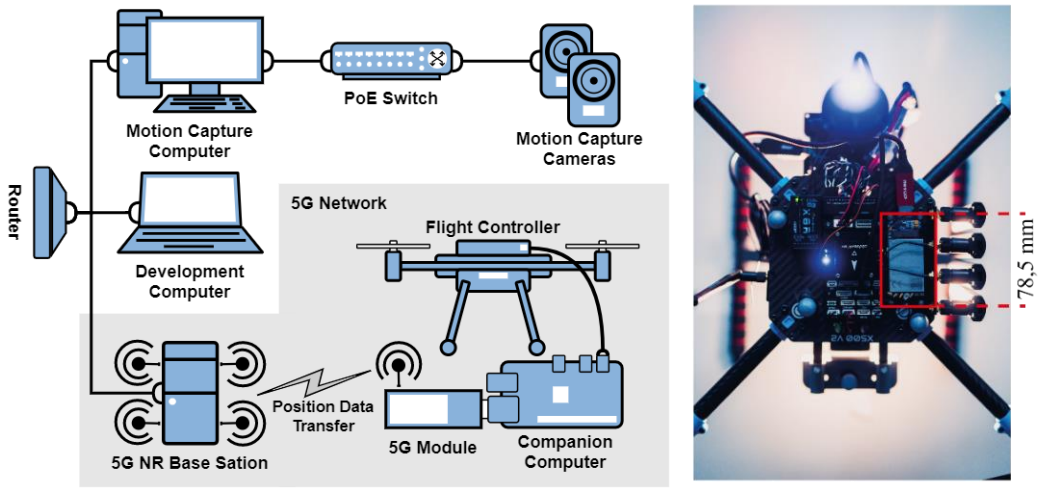


Abbildung 2: Beispiel für eine kompakte Integration des 5G-Kommunikationsadapter für die Indoor-Flugsteuerung [2].

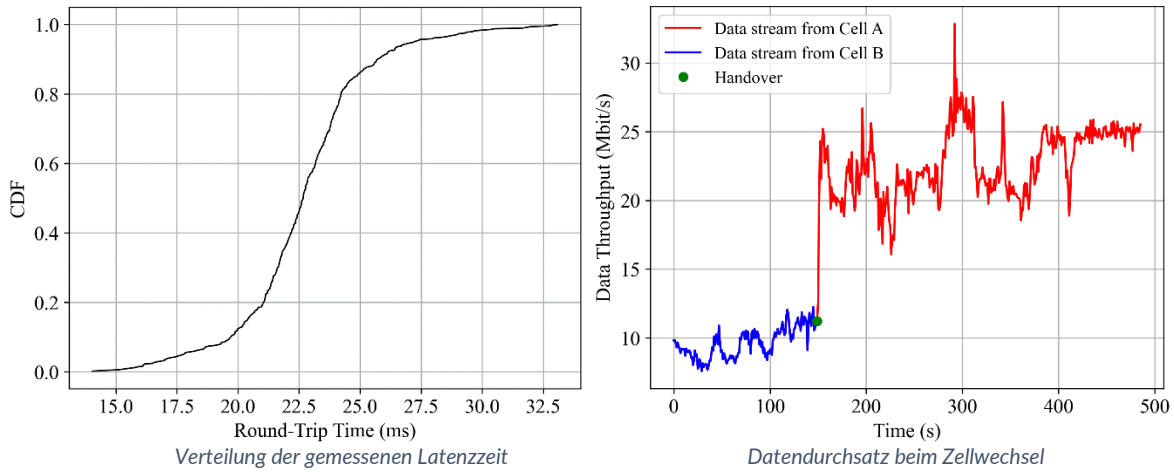
Weitere Anwendungsinnovationen wie etwa das visuelle Referenzieren von Roboterplattformen, die Integration relevanter Prozessinformationen eines Hochgeschwindigkeitsroboters sowie eine vergleichende Validierung unter Berücksichtigung 5G-spezifischer Leistungsparameter, wurden mit dem USB-Carrier-Board als Demonstratoren in der LFF umgesetzt. Für solche Architekturen kann ebenfalls der Retro-Fit-Ansatz als zusätzliche Integration von weiteren Rechnern genutzt werden, um ältere lokale Endgeräte über 5G zu vernetzen.

b. Hohe Komplexität bei der Inbetriebnahme

Erfahrungen haben gezeigt, dass die Inbetriebnahme von 5G-Endgeräten für Endanwender ohne kommunikationstechnischen Hintergrund zumeist komplex ist. Häufig müssen softwareseitige Kompatibilitätsprobleme mit unterschiedlichen Betriebssystemen für die jeweiligen Endgeräte gelöst werden, bevor eine einwandfreie Kommunikation mit der Peripherie hergestellt werden kann. Ebenfalls zeigte sich, dass auch eine erfolgreiche Erstinbetriebnahme keine Garantie für einen laufenden Betrieb ist. Es können anwendungsspezifische Kommunikationsprobleme auftreten, insbesondere bei der Konfiguration des Frequenzbereichs und der Signalstärke während der Eigenverwaltung des 5G-Netzes, um eine ordnungsgemäße Abdeckung der Halle zu gewährleisten. Verglichen mit Wi-Fi erweist sich 5G auch aufgrund der aufwendigeren Planung, wie dem Genehmigungsverfahren für die Frequenzzuteilung und der damit verbundenen festgelegten Platzierung der 5G-Antenne, allgemein als komplexer. Erfahrungen am LPS haben daher innerhalb des Forschungsprojektes in vielen Stellen die Abhängigkeit des Nutzers vom Anbieter der Campusnetzlösung aufgezeigt.

c. Evaluation der QoS der 5G-Campusnetzlösung am LPS

Im Rahmen von 5Guarantee wurde eine qualitative Evaluierung der Zuverlässigkeit der Latenzzeit für eine kontinuierliche Videoübertragung bei einem Zellwechsel einer zu überwachenden mobilen Roboterplattform zwischen zwei benachbarten Basisstationen untersucht. Abbildung 3 zeigt im linken Bild die Verteilung der gemessenen Latenz und im rechten Bild den gemessenen Datendurchsatz während der Videoübertragung [3]. Besonders relevant ist hier die Latenz, da die Realisierung einer autonomen, mobilen Roboterplattform eine zuverlässige Datenübertragung erfordert. Es wurde festgestellt, dass bei einem Wechsel der Funkzellen durch das Endgerät, sowohl die Latenz als auch der Datendurchsatz nahezu keine Unterbrechung aufweisen.



Verteilung der gemessenen Latenzzeit *Datendurchsatz beim Zellwechsel*

Abbildung 3: Ergebnisse für eine qualitativen Untersuchung hinsichtlich der Zuverlässigkeit eines Zellwechsels in 5G [2].

Es hat sich gezeigt, dass der Datenpaketaustausch mit dem Kommunikationsprotokoll von 5G eine stabile mittlere Latenzzeit im Bereich von unter 30 ms bietet. Dies liegt an Latenzschwankungen, die im Vergleich zu Wi-Fi deutlich geringer sind. Der Grund dafür sind die unterschiedlichen Methoden der Kanalzugriffe beider Technologien. 5G besitzt feste Zeitintervalle, in

denen der Datenaustausch stattfinden kann, ähnlich wie bei den Vorgängern der Mobilfunktechnik. Bei der Implementierung der Demonstratoren wurde festgestellt, dass die von der 3GPP versprochenen Spezifikationen hinsichtlich des höheren Datendurchsatzes und der geringeren Latenz für die Campusnetzlösung in der LFF nur teilweise erfüllt werden [4]. Dies könnte derzeit einer Entscheidung für den Einsatz von 5G-Campusnetzen zur industriellen Modernisierung entgegenstehen.

IV. Funktionsmuster für Konzept der Anomaliedetektion in 5G-Campusnetzfrequenzbereichen (TUDo)

Mit dem Zuwachs von privaten 5G-Campusnetzen im industriellen Umfeld kommen neue und potenziell unbekannte Bedingungen hinzu, welche Betrachtung finden müssen. Verschiedene Formen von Störeffekten, beispielsweise elektromagnetischer Strahlung durch Schweiß- oder ähnliche Produktionsprozesse oder eine fehlerkonfigurierte Nachbarzelle, können die Leistungsfähigkeit und Konnektivität von privaten Netzen einschränken. Im Zuge dessen ist eine lokale Erkennung von möglichen Störquellen eine wichtige Form der Qualitätssicherung und Gewährleistung einer reibungslosen Nutzung von privaten 5G-Campusnetzen.

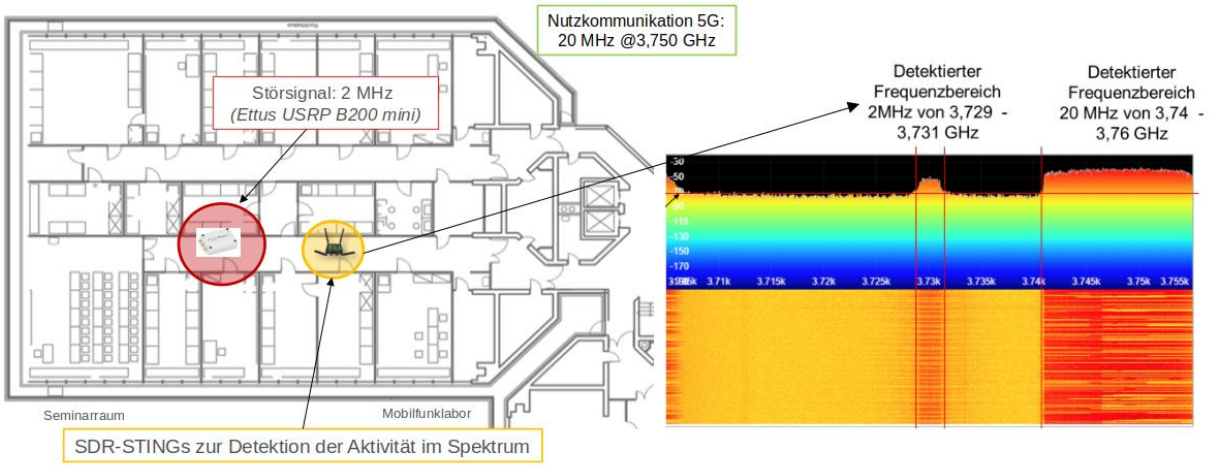


Abbildung 4: Überblick des Funktionsmusters zur Anomaliedetektion

Vor diesem Hintergrund wurde im 5Guarantee Projekt ein Funktionsmuster zur Anomaliedetektion entwickelt (vgl. Abbildung 4), das durch den Einsatz mobiler SDR-Lösungen eine lokale Analyse des Frequenzspektrums ermöglicht. Dies ermöglicht die Identifizierung von 5G-Nutzsignalen und die Unterscheidung von potenziellen Anomalien im Frequenzband. Die Unterscheidung zwischen gewünschten Nutzsignalen und unerwünschten Störungen/Anomalien ist dabei von entscheidender Bedeutung. Im Rahmen des 5Guarantee Projektes wurde dazu ein Machine-Learning-gestützter Ansatz entwickelt, welcher darauf abzielt, jedes bekannte Nutzsignal zu erkennen und so davonabweichende Empfangssignaturen als Anomalie identifizieren zu können.

Anomalien werden detektiert, indem ein auf Adversarial Autoencoders (AAE) basierter Algorithmus angewandt wird [5]. Dieser versucht auf Basis von aufgezeichneten Empfangsleistungsdichtedaten die zeitlich folgenden Werte zu prädizieren und vergleicht diese mit den tatsächlich auftretenden nächsten Empfangsleistungsdichten. Bei zu großer Abweichung wird davon ausgegangen, dass eine Anomalie besteht.
Der hier vorgestellte Ansatz verfolgt eine ähnliche Methodik, stützt jedoch die Detektion nicht auf eine Prädiktion, sondern auf das direkte Erkennen von Nutzsignalen in einem sogenannten Wasserfalldiagramm. Bei gleicher bis besserer Erkennungsgenauigkeit, ist eine Erweiterung durch zusätzliche Nutzsignale dabei einfacher umzusetzen [5].
Die Autoren einer vergleichbaren Forschungsarbeit nutzen, ähnlich dem hier vorgestellten Ansatz, ein Convolutional Neural Network (CNN) [6]. Dabei wird sich jedoch auf das Erkennen und

Lokalisieren von verschiedenen Nutzsignalen (bspw. LTE und 5G) beschränkt. Bei kurzen Trainingszeiten werden bis zu 98% Genauigkeit bei der Lokalisierung von Aktivitäten im Spektrum erreicht. Der im 5Guarantee-Projekt entwickelte Ansatz ist in der Lage, ebenfalls mit hoher Genauigkeit 5G Signale festzustellen, jedoch wird diese Funktion in einem weiteren Schritt dazu genutzt, anormale Signale vom Nutzsignal zu unterscheiden und so eine Detektion durchzuführen.

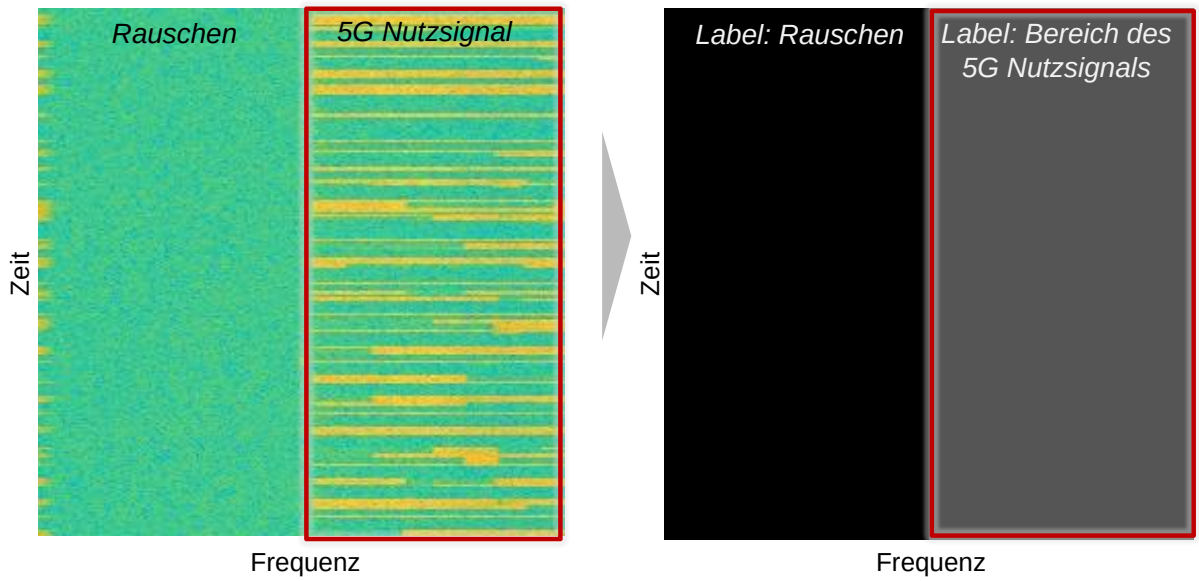


Abbildung 5: Wasserfalldiagramm (Links) von 5G-Nutzsignalen | Segmentierungsmaske (Rechts) mit eingefärbten Bereichen (schwarz = Hintergrundrauschen, grau= 5G-Signal).

Das im 5Guarantee-Projekt entwickelte SDR-basierte System ermöglicht es, in Szenarien wie Produktionsstätten periodisch Wasserfalldiagramme des Spektrums aufzunehmen, wie auf der linken Seite der Abbildung 5 zu sehen ist. Diese Diagramme stellen die Leistungsdichte sowohl über die Frequenz als auch über die Zeit aufgelöst dar. Die Daten werden durch Segmentierung und Post-Processing auf der Grundlage einer bekannten Wissensbasis über die Konfiguration des Campusnetzes analysiert, um Anomalien zu erkennen.

In der Bildklassifizierung werden typischerweise CNN als Machine Learning Modelle verwendet. Als solches wurde das sogenannte U-NET [7] gewählt da sich dieses schon bei vielen Bildsegmentierungsanwendungen, wie zum Beispiel in der Medizin, bewährt hat. Da es sich bei U-NET um ein CNN handelt, ist Supervised Learning nötig, um das Netz zu trainieren. Mithilfe der insgesamt über 2000 erhobenen Datensätzen aus kontrollierter Umgebung, wurden diverse Modelle mit verschiedenen Hyperparametern trainiert, um optimale Ergebnisse zu ermöglichen. Jeder Datensatz besteht aus einem aufgenommenen Wasserfalldiagramm und einer Segmentierungsmaske, wie in Abbildung 5 zu sehen ist. Dabei wurden die Trainingssets randomisiert in Trainings- und Validierungsset geteilt, mit einem 80/20 Split.

Der Post-Processing-Schritt beinhaltet einen Vergleich der Segmentierung des CNN und einer sogenannten Ground-Truth-Maske (GT-Maske) (siehe Abbildung 5, rechte Seite). Diese Maske kann erstellt werden, da bekannt ist, welches Frequenzband betrachtet wird und wo sich die Nutzsignale befinden. Die GT-Maske beschreibt also immer das Frequenzband im Soll-Zustand (ohne Anomalie). Diese beiden Bilder werden im nächsten Schritt spaltenweise auf

Abweichungen untersucht. Dies wird durchgeführt, um eine differenzierte Erkennung zu gewährleisten, da viele Bereiche der Segmentierung im Normalfall identisch sind und so kleine Abweichungen untergehen.
Im Falle, dass für eine Spalte eine gewisse Menge an Unterschieden überschritten wird, wird das gesamte Frequenzband als Anomalie behaftet bewertet. Der Grenzwert, der angibt, ab welcher Abweichung eine Anomalie vorhanden ist, stellt einen optimierbaren Parameter für die untersuchte Umgebung dar.

Für die Evaluierung der Anomalieerkennung wurden etwa 700 zusätzliche Datensätze erhoben, die mit diversen randomisierten synthetischen Störquellen aufgenommen wurden. Dabei wurde darauf geachtet, dass drei verschiedene Bandbreiten als Störung verwendet wurden, die neben und überlappend zu dem Nutzsignal positioniert waren.

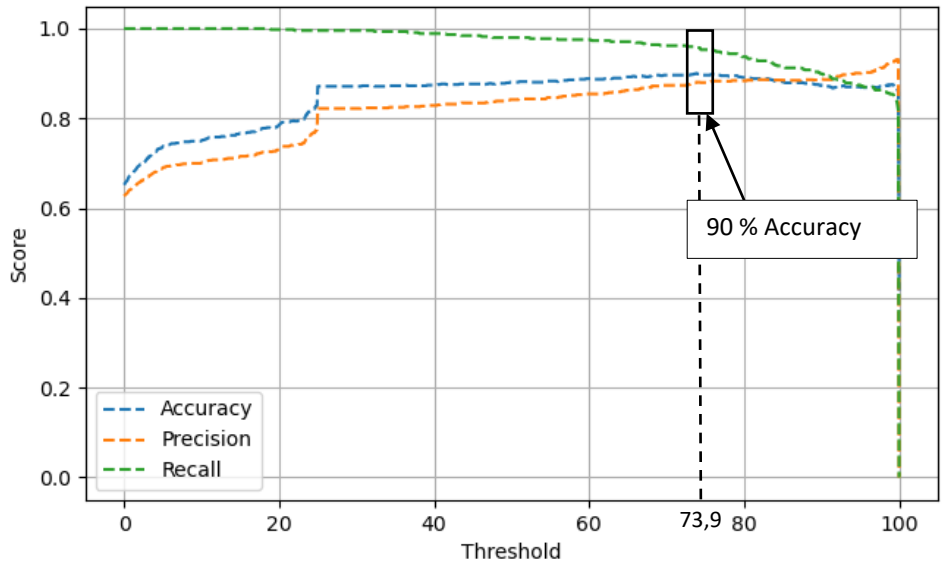


Abbildung 6: Verlauf der Accuracy, Precision und Recall für den Post-Processing-Schritt für alle möglichen Thresholds.

Die Optimierung des Grenzwerts wurde mittels Brute-Force durchgeführt, um die beste Accuracy, Precision und Recall zu bestimmen. Bei der Entscheidung des besten Wertes wurde nach der Accuracy und dem Recall optimiert. Dies dient dazu, die Menge an richtig erkannten Elementen zu maximieren und zusätzlich die Anzahl von False Negatives zu minimieren. Wie in Abbildung 6 zu erkennen ist, wurde der Threshold von 73,9 % gewählt. Dabei ergibt sich eine Accuracy von 90 % und ein Recall von 95,96 %.

Insgesamt ist das CNN in der Lage, aufgenommene Anomalien mit hoher Wahrscheinlichkeit zu erkennen. Der Algorithmus nutzt die Informationen über die Gegebenheiten und erzielt gute bis sehr gute Ergebnisse. In Zukunft ist die Erkennung von Anomalien, die vollständig im Nutzsignal liegen, ein wichtiger nächster Schritt. Darüber hinaus wäre die Kombination von Wissen aus KPIs oder Methoden aus der Nachrichtentechnik mit den Ergebnissen des CNN hilfreich, um noch robustere Ergebnisse zu erzielen. Schließlich wäre das Hinzufügen von anderen Nutzsignalen, wie zum Beispiel Wi-Fi, ein interessanter Ansatz, um den Algorithmus flexibler einsetzen zu können.

V. Ist 5G hinreichend zuverlässig, um Gefahren für Personen, Umwelt und Infrastruktur zu minimieren? (comnovo)

V.1. Einleitung

In der heutigen zunehmend digitalisierten Industrie spielen Sicherheitssysteme bei der Gewährleistung der Sicherheit von Arbeitern, der Umwelt und der Infrastruktur eine entscheidende Rolle. Besonders in Umgebungen, in denen Gabelstapler eingesetzt werden, sind zuverlässige Sicherheitsmaßnahmen von entscheidender Bedeutung, um Unfälle zu verhindern und potenzielle Risiken zu minimieren.

Traditionell verließen sich diese Sicherheitssysteme auf verdrahtete Verbindungen, die für ihre Robustheit und Zuverlässigkeit bekannt sind. Doch mit dem Fortschreiten der Technologie und der Einführung drahtloser Kommunikationstechnologien wie 5G und Wi-Fi 6 eröffnen sich neue Möglichkeiten für die Implementierung von Sicherheitslösungen.

Allerdings bringen drahtlose Netze auch ihre eigenen Herausforderungen mit sich, insbesondere in Bezug auf ihre Zuverlässigkeit. In gefährlichen Industrieumgebungen, in denen ein hohes Maß an Sicherheit erforderlich ist, ist die Gewährleistung einer kontinuierlichen und zuverlässigen Kommunikation von entscheidender Bedeutung.

Die alarmierenden Statistiken aus dem Jahr 2022 verdeutlichen die unbestreitbare Notwendigkeit einer ständigen Weiterentwicklung von Sicherheitsfunktionen [8]. In Deutschland wurden 19.758 Unfälle mit Gabelstaplern gemeldet, von denen 8 tödlich endeten. In den USA wurden 70 tödliche Unfälle im Zusammenhang mit Gabelstaplern gemeldet. Diese Zahlen unterstreichen die Dringlichkeit, fortlaufende Anstrengungen zu unternehmen, um Unfälle zu verhindern und Risiken zu minimieren.

Die Sicherheit von Arbeitern, der Schutz der Umwelt und die Erhaltung der Integrität von Infrastrukturen sind von entscheidender Bedeutung und erfordern innovative Lösungen. Angesichts dieser Herausforderungen ist es unerlässlich, dass wir kontinuierlich nach neuen Wegen suchen, um die Sicherheit zu verbessern und tragische Vorfälle zu vermeiden.

V.2. Funktionale Sicherheit

Die funktionale Sicherheit gemäß der internationalen Norm IEC 62061 ist ein grundlegendes Konzept, das darauf abzielt, korrekte Funktionen von Sicherheitskontrollsystemen in Maschinen sicherzustellen. Dieser Ansatz umfasst eine umfassende Bewertung von Risiken, um geeignete Maßnahmen zur Risikominderung zu bestimmen. Dabei wird das Performance Level (PL) als Kennzahl für die Zuverlässigkeit und Leistung von Sicherheitsfunktionen verwendet.

Ein zentrales Element, das die praktische Anwendung der funktionalen Sicherheit unterstützt, ist die ISO 13849-1. Diese Norm stellt Leitlinien für sichere Steuerungssysteme in Maschinen bereit und unterteilt die Performance Levels in fünf Stufen (PL a bis PL e). Die Auswahl des richtigen Levels hängt von verschiedenen Risikokriterien ab, darunter die Schwere potenzieller Verletzungen, die Häufigkeit der Exposition gegenüber Gefahren und die Möglichkeit der Gefahrenvermeidung.

Es ist wichtig zu betonen, dass das Performance Level nicht auf das gesamte System, sondern auf individuelle Sicherheitsfunktionen anwendbar ist. In Systemen mit mehreren

sicherheitsrelevanten Teilen wird das Gesamtrisiko durch die Summe der Risiken aller Teilsysteme bestimmt. Zusätzlich fließen Aspekte wie die mittlere Zeit bis zum gefährlichen Ausfall (MTTF – Mean Time To Failure) in die Bewertung ein.

Insgesamt arbeiten die Normen IEC 62061 und ISO 13849-1 zusammen, um einen Rahmen für die funktionale Sicherheit von Maschinen bereitzustellen. Sie bieten klare Richtlinien und Kriterien, die es den Herstellern ermöglichen, Sicherheitsfunktionen zu entwickeln, die den höchsten Standards entsprechen und gleichzeitig die Sicherheit von Arbeitskräften, der Umwelt und der Infrastruktur gewährleisten.

V.3. Drahtlose Sicherheitssysteme

Die Problematik bei der Implementierung von drahtlosen Sicherheitssystemen, insbesondere in Bezug auf Gabelstapler, liegt in der inhärenten Unzuverlässigkeit drahtloser Netze im Vergleich zu kabelgebundenen Netzen. In gefährlichen Industrieumgebungen, in denen ein hohes Maß an Zuverlässigkeit erforderlich ist, um die Sicherheit der Arbeiter zu gewährleisten, kann die fehlerhafte Funktionalität zu schwerwiegenden Folgen führen.

Das Performance Level (PL) wird verwendet, um die Zuverlässigkeit und Sicherheit von Sicherheitsfunktionen zu beschreiben. Allerdings gibt es keine konkrete Regelung, wie die Sicherheit von drahtlosen Netzen im Hinblick auf das PL bewertet werden soll. Dies führt zu Unsicherheiten und Herausforderungen bei der Entwicklung und Bewertung von drahtlosen Sicherheitssystemen.

Ein weiteres Problem besteht darin, dass drahtlose Kommunikation anfällig für Paketverluste ist, insbesondere bei der Verwendung von UDP (User Datagram Protocol). Ein einzelner Paketverlust kann dazu führen, dass eine potenzielle Gefahr nicht erkannt wird. Bei der Verwendung von TCP (Transmission Control Protocol) können hohe Latenzen auftreten, was dazu führen kann, dass eine Gefahr zu spät erkannt wird.

Die wichtigsten Fragestellungen sind daher, wie drahtlose Kommunikation zuverlässig aufgebaut werden kann, welcher Grad an Zuverlässigkeit erreicht werden kann und wie die Zuverlässigkeit im Sinne des PL bewertet werden kann. Es ist auch wichtig zu bestimmen, welche zukünftigen Funk Use Cases ein PL erfordern und wie die Technologien 5G und Wi-Fi 6 im Vergleich zueinanderstehen.

Trotz der Fortschritte in der drahtlosen Technologie fehlt es an hochzuverlässiger Kommunikation in industriellen Umgebungen. Es gibt keine klaren Richtlinien, wie das Performance Level für Funk-Sicherheitsfunktionen bewertet werden soll.

Als Lösung haben wir eine Methode zur Bewertung vorgeschlagen, die auf einem Warteschlangenmodell für Paketfehler basiert. Hierbei bleibt die Sicherheitsfunktion intakt, solange das nächste Paket erfolgreich übertragen wird. Das System wird erst als unsicher eingestuft, wenn eine bestimmte Anzahl aufeinanderfolgender Paketverluste auftritt. Diese Methode ermöglicht eine präzise Bewertung der Zuverlässigkeit von drahtlosen Sicherheitssystemen und trägt dazu bei, die Sicherheit in industriellen Umgebungen zu verbessern.

V.4. Evaluierung der Zuverlässigkeit von 5G und Wi-Fi 6 zur Minimierung von Gefahren für Personen, Umwelt und Infrastruktur

Die Einführung von 5G und Wi-Fi 6 hat die Diskussion über die Zuverlässigkeit drahtloser Kommunikationstechnologien in industriellen Umgebungen intensiviert und die Frage aufgeworfen, ob diese Technologien hinreichend zuverlässig sind, um Gefahren für Personen, Umwelt und Infrastruktur zu minimieren. In diesem Abschnitt wird eine detaillierte Bewertung vorgenommen, um festzustellen, inwieweit 5G und Wi-Fi 6 die Anforderungen an funktionale Sicherheit erfüllen und welche potenziellen Auswirkungen sie auf die Sicherheit in industriellen Umgebungen haben könnten.

In Bezug auf 5G zeigt sich, dass die Technologie potenziell niedrige Latenzen und hohe Datenraten bietet, was zu einer verbesserten Kommunikation und Reaktionsfähigkeit führen kann. Dies könnte dazu beitragen, Unfälle zu verhindern und die Sicherheit in gefährlichen Industrieumgebungen zu erhöhen. Dennoch bestehen Bedenken hinsichtlich der Zuverlässigkeit von 5G, insbesondere in Bezug auf den Paketverlust und die Netzabdeckung in abgelegenen oder stark strukturierten Umgebungen. Diese Unsicherheiten könnten die Fähigkeit von 5G beeinträchtigen, Gefahren rechtzeitig zu erkennen und angemessen zu reagieren.

Im Vergleich dazu bietet Wi-Fi 6 ebenfalls Verbesserungen in Bezug auf Geschwindigkeit, Kapazität und Effizienz. Die Technologie verspricht niedrigere Latenzen und eine höhere Zuverlässigkeit in der drahtlosen Kommunikation, was potenziell positive Auswirkungen auf die Sicherheit in industriellen Umgebungen haben könnte. Allerdings könnte auch Wi-Fi 6 mit ähnlichen Herausforderungen konfrontiert sein wie 5G, insbesondere in Bezug auf die Reichweite und Interferenzen in stark frequentierten Umgebungen.

Insgesamt deutet die Entwicklung von 5G und Wi-Fi 6 darauf hin, dass drahtlose Kommunikationstechnologien potenziell dazu beitragen können, die Sicherheit in industriellen Umgebungen zu verbessern. Allerdings ist es entscheidend, die Zuverlässigkeit dieser Technologien gründlich zu prüfen und sicherzustellen, dass sie den Anforderungen an die funktionale Sicherheit und den Schutz von Personen, Umwelt und Infrastruktur gerecht werden. Dies erfordert eine sorgfältige Bewertung ihrer Leistungsfähigkeit, mögliche Sicherheitsrisiken und die Entwicklung geeigneter Sicherheitsmaßnahmen, um potenzielle Gefahren zu minimieren.

VI. 5G-Orchestrator für 5G-Anwendungen (PHYSEC)

Noch vor einigen Jahren wurde die Informations- bzw. Datenverarbeitung auf bekannten, vertrauensvollen Servern durchgeführt, die entweder bei einem Unternehmen selbst oder einem Partner standen. Doch bereits 2025 können bis zu 75 % aller Daten außerhalb bekannter Strukturen verarbeitet werden [9]. Dies ist auch bei dem Mobilfunkstandard 5G der Fall. Sowohl die Basisstationen bei 5G als auch bei 5G-Campusnetzen müssen nicht mehr in einer speziell geschützten Umgebung installiert werden, sondern können in Produktionshallen und an Hauswänden platziert werden. Dadurch, dass die Hardware damit auch von nicht-autorisierten Personen passiert werden kann, könnten theoretisch Änderungen an der Hardware vorgenommen werden. Das sorgt dafür, dass neue Möglichkeiten geschaffen werden müssen, um Hardware zu schützen. Neben dem Perimeterschutz gilt es Zugriffsversuche zu erkennen, um darauf reagieren zu können.

Um diese Fragestellung zu untersuchen, wurde eine Versuchsreihe konzipiert, in der eine Auswahl von Angriffsszenarien untersucht werden sollten. Zur Untersuchung wurde ein Cluster mit sechs APUs aufgesetzt, wovon eine APU als 5G-Campusnetz-Orchestrator fungiert, eine weitere APU stellt das Bindeglied zwischen der Cloud und dem Feld dar (Worker) und die letzten vier simulieren 5G-Geräte im Feld (Edge). Die APUs stammen von der Firma Advanced Micro Devices (AMD) und besitzen vier Kerne mit 4 GB RAM. Es soll untersucht werden, ob bspw. Services der APU auch unter Volllast noch erreichbar sind oder Ausfälle auftreten können sowie Verteidigungsmaßnahmen bei bestimmten Angriffen erfolgreich sein können. Bei dem letzten Punkt, attackiert ein Angreifer das Cluster.

Beim Stresstest wurden APUs der drei Kategorien Orchestrator, Worker und Edge auf volle Systemauslastung provoziert. Dabei fielen folgende Punkte auf:

a) Die CPU-Auslastung des Orchestrators liegt höher als bei der Worker-APU oder den Edge-APUs.
b) Unter Volllast sind die Edge-Geräte sowie die darauf laufenden Services zu jederzeit erreichbar und laufen stabil.
c) Es traten während des Tests keine Fehler oder Seitenkanäle im Betriebssystem auf.
d) Es traten keine Probleme durch den Temperaturanstieg auf.

Der Grund für die höhere CPU-Auslastung bzw. Ressourcenauslastung unter Punkt a) liegt darin begründet, dass der Orchestrator weitere wichtige Services zum Erhalt des Clusters ausführt. Diese Last hat aber keinen negativen Einfluss auf die Performance des Orchestrators. Durch die positiven Ergebnisse (Punkt b) – c)) war ein weiterer Einsatz der APUs sowie des Clusters gewährleistet, wodurch nun mögliche Angriffsszenarien formuliert und durchgeführt werden konnten.

Wie bereits eingangs erwähnt, stehen 5G-Basisstationen und wichtige Prozesseinheiten mittlerweile in öffentlichen Umgebungen oder Produktionsstätten, in welchen sich nicht nur autorisiertes und geschultes Personal aufhält. Unter dieser Annahme wurden vier mögliche Angriffsszenarien erörtert und untersucht:

a) **Szenario 1.** Der Angreifer versucht Zugriff auf ein Edge Node zu erhalten.
b) **Szenario 2.** Der Angreifer gelangt erfolgreich auf ein Edge Node.
c) **Szenario 3.** Der Angreifer kompromittiert das gesamte Cluster.
d) **Szenario 4.** Der Angreifer kann die Kommunikation zwischen Cloud und Edge stören.

In den beschriebenen Szenarien wird immer davon ausgegangen, dass die Cloud-Seite kryptografisch stark geschützt ist und damit nicht attraktiv genug für einen Angriff ist.

Im ersten Szenario zieht ein Angreifer das Netzwerkkabel aus dem Edge Node und versucht das Gerät darin auszubauen, um an Informationen zu gelangen. Die Cloud-Einheiten bekommen von dem Angriff nichts mit, doch Sensorik im Gerät erkennt einen möglichen Einbruchsversuch. In diesem Fall versucht das Gerät mögliche Zugriffe zu verhindern, indem Partitionen, Anwendungen und Zertifikate auf dem Edge Node gelöscht werden. In der Praxis würde damit eine 5G-Basisstation ausfallen, allerdings wird damit verhindert, dass der Angreifer an Daten kommt oder an der Kommunikation teilnehmen kann. Die Cloud-Seite überprüft alle 5 Sekunden, ob alle Geräte der Edge-Seite aktiv sind. Nach 5 Minuten startet der Orchestrator seinen Prozess, um ein neues Gerät mit Zertifikaten und Anwendungen auszustatten und die Lücke zu schließen. Der Wert von 5 Minuten kann jederzeit angepasst werden und wurde aus Gründen der Netzlastreduzierung gewählt.
Im zweiten Szenario wird davon ausgegangen, dass der Angreifer in der Lage war, den Perimeterschutz auf dem Edge Node zu deaktivieren und damit vollen Zugriff auf das Gerät zu erhalten. Dieses Mal merkt die Cloud-Seite allerdings den Zugriff und versucht den Schaden zu minimieren und dem Angreifer die Zugriffe zu entziehen. Der Orchestrator würde nun versuchen Anwendungen, die noch nicht kompromittiert wurden, auf andere Systeme umzuziehen. Dies dauert aber mindestens 11 s bis hin zu 61 s, sofern keine Priorisierung der Anwendung vorgenommen wurde. Wenn alle Anwendungen umgezogen wurden oder dies nicht möglich war, wird die Verbindung zum kompromittierten Edge Node aufgelöst. Da der Angreifer aber noch gültige Zertifikate besitzen könnte, besteht die Chance, dass er dem Cluster wieder beitreten kann. Dies kann verhindert werden, indem die Cloud-Seite ein neues Zertifikat aushandeln lässt.
Die nächsthöhere Stufe ist die Kompromittierung des gesamten Clusters. Da es hier je nach Clustergröße für den Orchestrator nahezu unmöglich ist den Angriff zu identifizieren, leitet er eine Notfallwiederherstellung ein. In dieser werden alle Edge Nodes zurückgesetzt und damit gezwungen sich mit neuen Zertifikaten beim Orchestrator zu melden. Für die betrachtete Clustergröße würde ein Neustart an die 2 min dauern.
Das vierte Szenario beschreibt einen sogenannten Man-in-the-Middle Angriff. Bei dieser Art Angriff platziert sich der Angreifer logisch zwischen der Edge- und der Cloud-Seite und liest die Kommunikation mit. Die Voraussetzung dafür ist aber, dass es dem Angreifer gelungen ist die aktuellen Zertifikate oder Kommunikationsschlüssel in seinen Besitz zu bringen. Bei diesem Angriff kann es sein, dass nicht bemerkt wird, dass die Kommunikation kompromittiert wurde. Das ist deshalb gefährlich, weil die Kommunikation nun jederzeit mitgelesen oder verfälscht werden kann. Da der Angreifer in diesem Fall weder Zugriff auf die Geräte in der Cloud- noch auf der Edge-Seite hat, kann dieser Angriff dadurch unterbunden werden, indem neue Zertifikate ausgehandelt werden. Dies wird von der Cloud-Seite dann getriggert, sobald der Angriff entweder bemerkt wurde oder das Zertifikat abgelaufen ist. Sobald neue Zertifikate vorhanden sind, ist der Angreifer ausgesperrt und er müsste erst erneut an ebenjene Kommunikationsschlüssel gelangen. Der Austausch der Zertifikate dauert lediglich wenige Sekunden.

Insgesamt lässt sich sagen, dass der Orchestrator auf der Cloud-Seite in der Lage ist sein Cluster zu verwalten, wenn auch nicht uneingeschränkt zu schützen. Dies hängt damit zusammen, dass zumindest die Edge Komponenten in ungeschützten Räumen zu finden sein können. Hier hat ein Angreifer in der Regel die erste Hürde – nämlich Zugriff zum Gerät zu bekommen – überwunden. Dennoch kann der Orchestrator als Teil eines SIEM-Systems dafür sorgen, dass der Schaden in einem Cluster minimiert werden kann.

VII. Zusammenfassung

Die umfassende Analyse in diesem Whitepaper unterstreicht die transformative Kraft von 5G-Technologien in verschiedenen industriellen und kommunikativen Kontexten, betont jedoch gleichzeitig die Notwendigkeit, Sicherheit und Funktionalität in den Vordergrund zu stellen. Während die Implementierung von 5G-Campusnetzen vielversprechende Ergebnisse in Bezug auf Flexibilität und Qualität des Service zeigt, hebt sie auch die Herausforderungen hervor, die mit der technischen Komplexität und den Sicherheitsanforderungen verbunden sind. Der in Dortmund entwickelte Ansatz zur Anomaliedetektion zeigt innovative Wege auf, wie maschinelles Lernen zur Sicherung der Netzintegrität beitragen kann, während die Studien von comnovo und PHYSEC kritische Einblicke in die Zuverlässigkeit von 5G in Bezug auf den Schutz von Personen und Infrastrukturen bieten.

Diese Erkenntnisse sind besonders wichtig, da sie betonen, dass trotz der fortschrittlichen Fähigkeiten von 5G, die Sicherheit nicht als selbstverständlich angesehen werden darf. Die Implementierung von effektiven Sicherheitsmechanismen, die sowohl physische als auch digitale Bedrohungen abdecken, und die fortlaufende Überwachung und Anpassung dieser Systeme ist entscheidend, um den sich ständig weiterentwickelnden Bedrohungen einen Schritt voraus zu sein.

Abschließend fordert dieses Whitepaper zu einer ganzheitlichen Betrachtung auf: Es sollten nicht nur die technologischen Fortschritte gefördert, sondern auch eine nachhaltige Infrastruktur geschaffen werden, die Sicherheit, Zuverlässigkeit und Datenschutz in den Mittelpunkt stellt. Dies erfordert eine enge Zusammenarbeit zwischen Entwicklern, Forschern und regulatorischen Institutionen, um Rahmenbedingungen zu schaffen, die sowohl Innovation fördern als auch Schutz bieten.

Referenzen

[1] Marius Boshoff, Michael Miro, Bernd Kuhlenkötter, „Anforderungen für den Einsatz von 5G in Produktionsumgebungen“, 2022, https://doi.org/10.1515/zwf-2022-1010

[2] Gustavo Barros, Marius Boshoff, Tommy Luong, Bernd Kuhlenkötter, “Deployment of a 5G Networking Module for Robotics and IoT Applications”, Procedia CIRP, Volume 120, 2023, Pages 535-540, ISSN 2212-8271, https://doi.org/10.1016/j.procir.2023.09.033

[3] Tommy Luong, Gustavo Barros, Marius Boshoff, Christian Moldovan, David Schuster, Volker Gruhn und Bernd Kuhlenkötter, “Investigating the 5G Handover in Autonomous Mobile Robotic Applications”, 2023

[4] 3GPP, 5G System Overview, https://www.3gpp.org/technologies/5g-system-overview

[5] S. Rajendran, W. Meert, V. Lenders and S. Pollin, "Unsupervised Wireless Spectrum Anomaly Detection With Interpretable Features," in IEEE Transactions on Cognitive Communications and Networking, vol. 5, no. 3, pp. 637-647, Sept. 2019, doi: 10.1109/TCCN.2019.2911524. keywords: {Wireless communication;Data mod-els;Anomaly detection;Feature extraction;Wireless sensor networks;Hidden Markov models;Detectors;Deep learning;spectrum monitoring;anomaly detection}.

[6] C. P. Robinson, D. Uvaydov, S. D’Oro, and T. Melodia, “Deepsweep: Parallel and scalable spectrum sensing via convolutional neural networks,” 2024.

[7] O. Ronneberger et. al., “U-net: Convolutional networks for biomedical image segmen-tation”, In: Medical Image Computing and Computer-Assisted Intervention–MICCAI 2015: 18th International Conference, Munich, Germany, October 5-9, 2015, Proceed-ings, Part III 18. Springer International Publishing, 2015. S. 234-241.

[8] DGUV, Statistik—Arbeitsunfallgeschehen 2022, 2022, https://publikationen.dguv.de/widgets/pdf/download/article/4759

[9] R. van der Meulen, „What Edge Computing Means for Infrastructure and Operations Leaders”, 2018, https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders