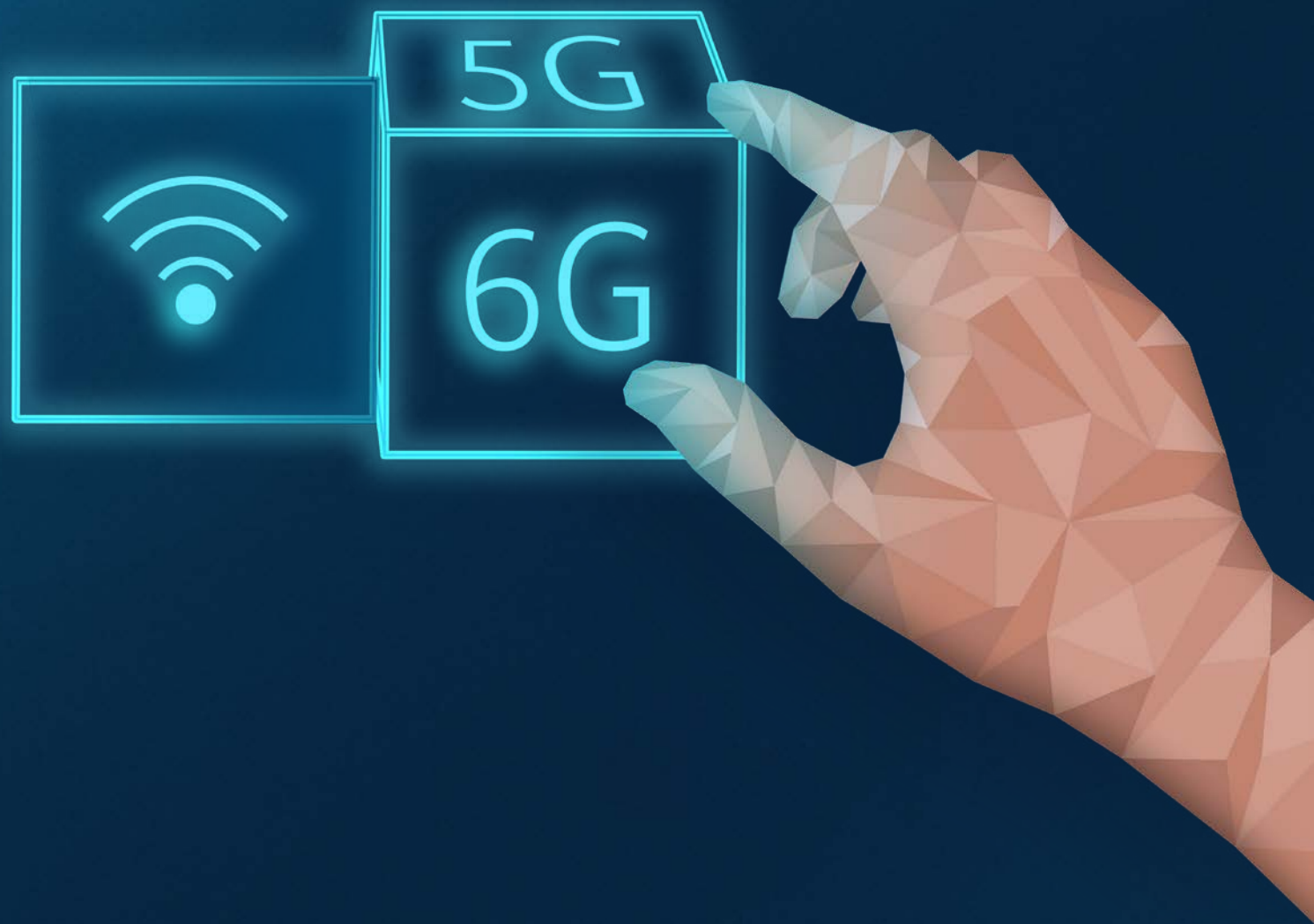
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Projektkatalog zur Fördermaßnahme „Cyber-Sicherheit und digitale Souveränität in den Kommunikations-technologien 5G/6G“



Vorwort

Liebe Leserin, lieber Leser,

mit unserem Projektkatalog behaltet ihr den Überblick zum Förderprogramm „Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G."

Wir als BSI sehen das große Potenzial von 5G/6G, die Digitalisierung zu beschleunigen. Um dabei das Vertrauen in neue Technologien zu stärken, braucht es Informationssicherheit, die von Anfang an mitgedacht wird. Mit unserem Förderprogramm wollen wir Innovation und Digitalisierung voranbringen. Wir unterstützen mit den geförderten Projekten den sicheren, technologischen Wandel und gehen Schritt für Schritt in Richtung digitale Souveränität. Zusammen mit den Projekten in fünf vielfältigen Themenschwerpunkten kommen wir dem Ziel näher, Angreifern den entscheidenden Schritt voraus zu sein. Hierfür testen die Projekte ganz praktisch neuartige Testaufbauten und -szenarien oder arbeiten an der Weiterentwicklung von Werkzeugen für Sicherheitsprüfungen im 5G-Bereich. Andere entwickeln Produkte, Lösungen, Methoden oder Verfahren, die den sicheren Einsatz von 5G/6G unterstützen und die Resilienz von Infrastrukturen erhöhen. Es beteiligen sich Start-ups und KMUs an der Forschung und Entwicklung zu Lösungen, die IT-Sicherheit im Open-RAN erhöhen oder Schnittstellen absichern.

Den Überblick über alle Projekte habt ihr mit unserem Projektekatalog. Ihr findet hier zum einen allgemeine Infos zum Förderprogramm Zum anderen erfahrt ihr nach Themenschwerpunkten sortiert mehr über alle seit Beginn 2023 geförderten Projekte. Jedes Projekt nimmt euch mit und zeigt, welche Motivation, welches Ziel und welche Vision hinter dem eigenen Projekt steckt.

Ich wünsche viel Freude beim Lesen und bleibt auch über unsere Webseite auf dem neuesten Stand.

Claudia Plattner

Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

Das Förder-programm

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fördert im Auftrag des Bundesministerium des Innern und für Heimat (BMI) Forschungs- und Entwicklungsvorhaben im Bereich „Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ im Rahmen des „45. Elements“ des Konjunkturprogramms der Deutschen Bundesregierung.

Das Förderprogramm stärkt die Innovationskraft von Unternehmen, fördert die digitale Souveränität Deutschlands und trägt dazu bei, dass Deutschland bei 5G und 6G in der Weltspitze eine führende Rolle als Technologieanbieter einnimmt. Insgesamt stehen – vorbehaltlich der Haushaltslage – bis zu 60 Millionen € für die Förderungen zur Verfügung.

Die geförderten Projekte unterstützen die folgenden übergreifenden Ziele:

- nationale Betreiber- und Hersteller-Ökosysteme für moderne Netztechnologien im Kontext der IT-Sicherheit stärken,
- moderne Netztechnologien zur Stärkung der Resilienz und Erhöhung der Netzsicherheit entwickeln und erproben,
- Markteintrittsbarrieren für moderne und sichere Netztechnologien abbauen,
- Risiken für den Einsatz moderner Netztechnologien minimieren und Sicherheitslücken schließen sowie
- sichere Anwendungsfälle für moderne Netztechnologien in der Digitalisierung zur Stärkung der IT-Sicherheit identifizieren und etablieren.

Das Programm richtet sich an Unternehmen der gewerblichen Wirtschaft (beispielsweise Netzbetreiber, Campus-Netzbetreiber, Herstellerfirmen, Integratoren, Beratungs- und Schulungsunternehmen), an Kommunen, Hochschuleinrichtungen sowie an außeruniversitäre Bildungs- und Forschungseinrichtungen. In Themenschwerpunkt 5 wird ein Fokus auf die Förderung von jungen Unternehmen sowie kleinen und mittleren Unternehmen (KMU) gelegt.

Um die IT-Sicherheit und digitale Souveränität in Deutschland zu stärken, findet die vorwettbewerbliche Förderung für den Mittelstand statt. Im Fokus des Förderprogramms steht die Entwicklung von innovativen Lösungen, die neue Geschäftsfelder in den Unternehmen ermöglichen.

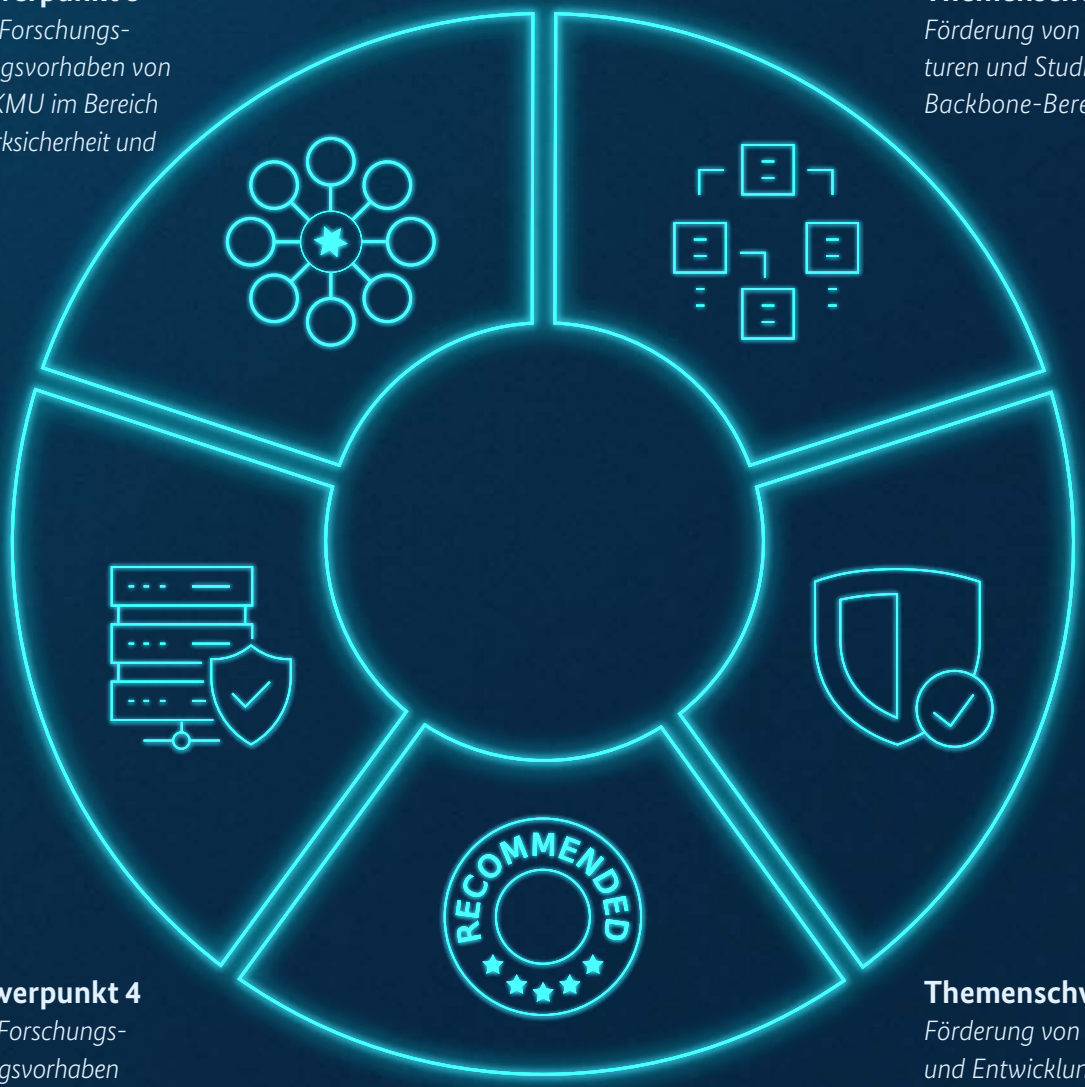
Die fünf Themenschwerpunkte richten sich an Unternehmen der gewerblichen Wirtschaft, Kommunen und Kommunalverbände, Verbände, gemeinnützige Organisationen, Hochschulen, Universitäten sowie öffentliche und nicht-öffentliche Forschungsinstitutionen.

Für eine gute Einbindung der entwickelten Lösungen in den Markt werden die Vorhaben in den fünf Themenschwerpunkten nach Möglichkeit von Unternehmen geführt und als Einzel- oder Verbundvorhaben umgesetzt.

Vorstellung der fünf Themenschwerpunkte

Themenschwerpunkt 5
Förderung von Forschungs- und Entwicklungsvorhaben von Start-ups und KMU im Bereich 5G/6G-Netzwerksicherheit und Open RAN

Themenschwerpunkt 1
Förderung von Test-Infrastrukturen und Studien im 5G/6G-Backbone-Bereich



Themenschwerpunkt 4
Förderung von Forschungs- und Entwicklungsvorhaben zur Sicherheit und Resilienz von 5G/6G-Technologien und Infrastrukturen

Themenschwerpunkt 2
Förderung von Forschungs- und Entwicklungsvorhaben zur Cyber-Sicherheit in 5G/6G-Digitalisierungsfeldern (Nutzungsszenarien)

Themenschwerpunkt 3
Förderung von Forschungs- und Entwicklungsvorhaben zum Aufbau von 5G/6G-Prüf- und Zertifizierungsstellen

Förderprogramm im Überblick

Programmstatus

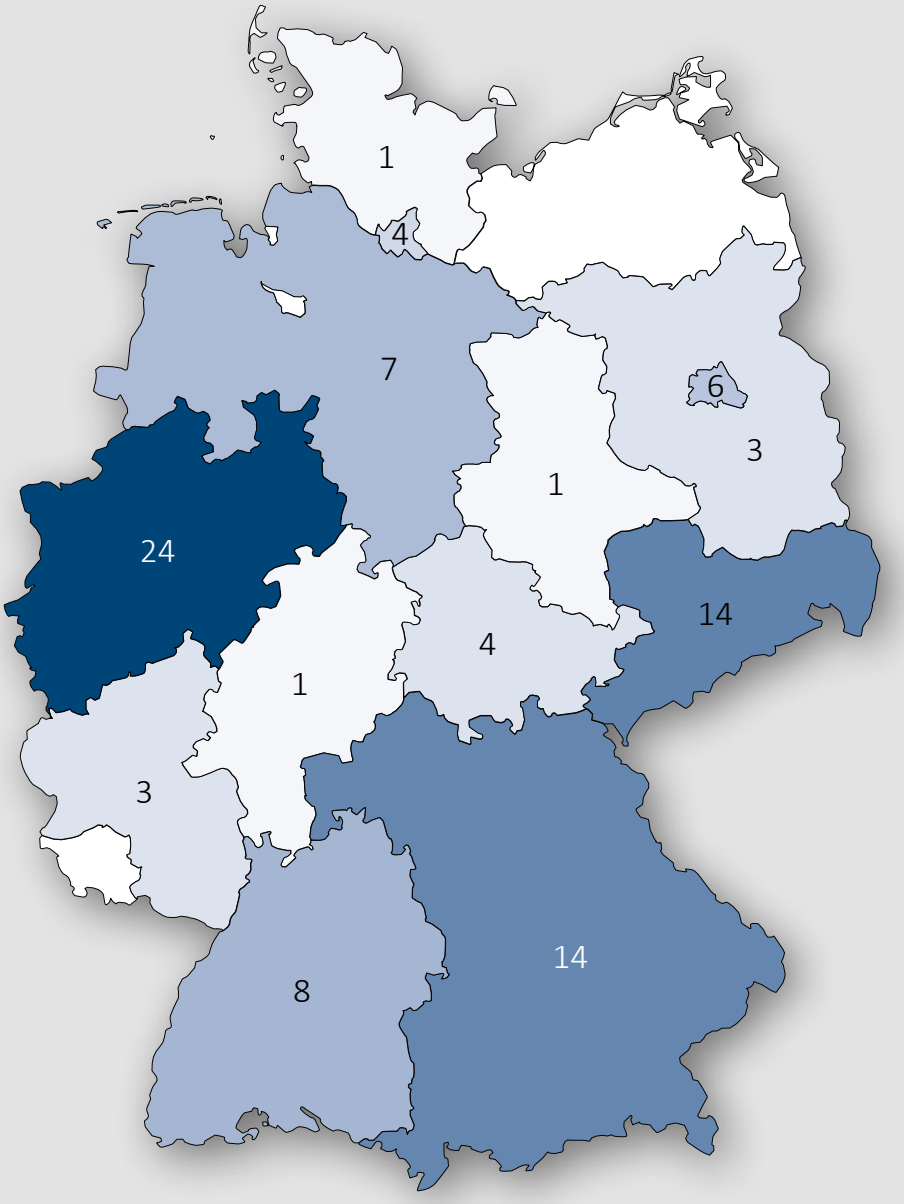
Das BSI fördert im Rahmen des Fördervorhabens „Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G“ insgesamt 90 Zuwendungsempfänger in 31 Projekten mit einem Gesamtfördervolumen von 38,852 Mio. €. Die Projekte und ihre Fördernehmer verteilen sich auf das gesamte Bundesgebiet.

52 % der Fördersumme gehen an Akteure der Wirtschaft und Städte, darunter 44 % an kleine und mittelständische Unternehmen (KMU). 48 % fließen an Bildungseinrichtungen und Forschungsinstitutionen.

Über die Hälfte der Fördermittel (56 %) entfallen dabei auf Projekte des TSP 4 (Förderung von Forschungs- und Entwicklungsvorhaben zur Sicherheit und Resilienz von 5G/6G-Technologien und Infrastrukturen). Die Projekte des TSP2 (Forschungs- und Entwicklungsvorhaben zur Cyber-Sicherheit in 5G/6G-Digitalisierungsfeldern [Nutzungsszenarien]) erhalten 15 % des Fördervolumens. Die TSP 1 (Forschung und Entwicklung für Test-Infrastrukturen und Studien im 5G/6G-Backbone-Bereich), 3 (Forschungs- und Entwicklungsvorhaben zum Aufbau von 5G/6G-Prüf- und Zertifizierungsstellen) und 5 (Forschungs- und Entwicklungsvorhaben von Start-ups und KMU im Bereich 5G/6G-Netzwerksicherheit und Open RAN) werden mit jeweils 10 % der Fördermittel unterstützt.

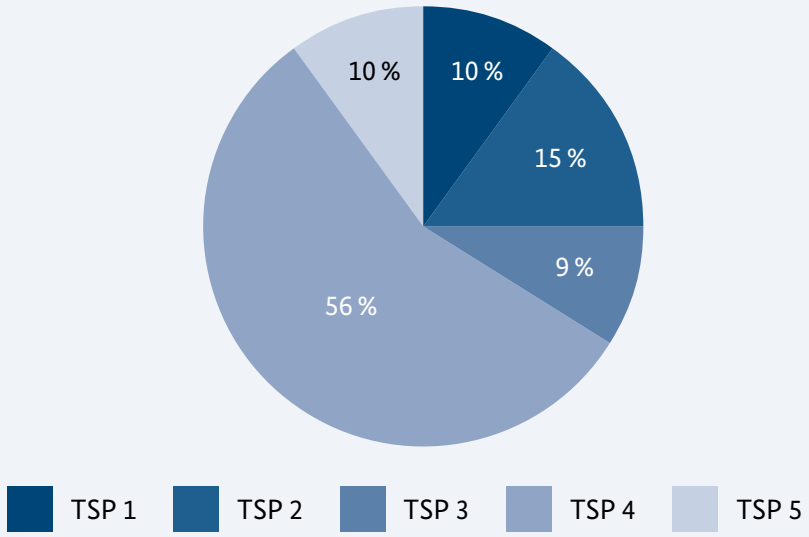
53 % der Zuwendungsempfänger sind Akteure der Wirtschaft und Städte. Hierunter fallen sieben junge Unternehmen mit einem Alter von bis zu drei Jahren, 12 Scale-Ups (4 – 10 Jahre alt), 18 KMU, 9 Großunternehmen plus die Städte Hamburg und Aalen. 47 % der Zuwendungsempfänger sind Bildungseinrichtungen und Forschungsinstitutionen.

Verteilung der Zuwendungsempfänger nach Standorten je Bundesland



Baden-Württemberg	8	Nordrhein-Westfalen	24
Bayern	14	Rheinland-Pfalz	3
Berlin	6	Sachsen	14
Brandenburg	3	Sachsen-Anhalt	1
Hamburg	4	Schleswig-Holstein	1
Hessen	1	Thüringen	4
Niedersachsen	7		

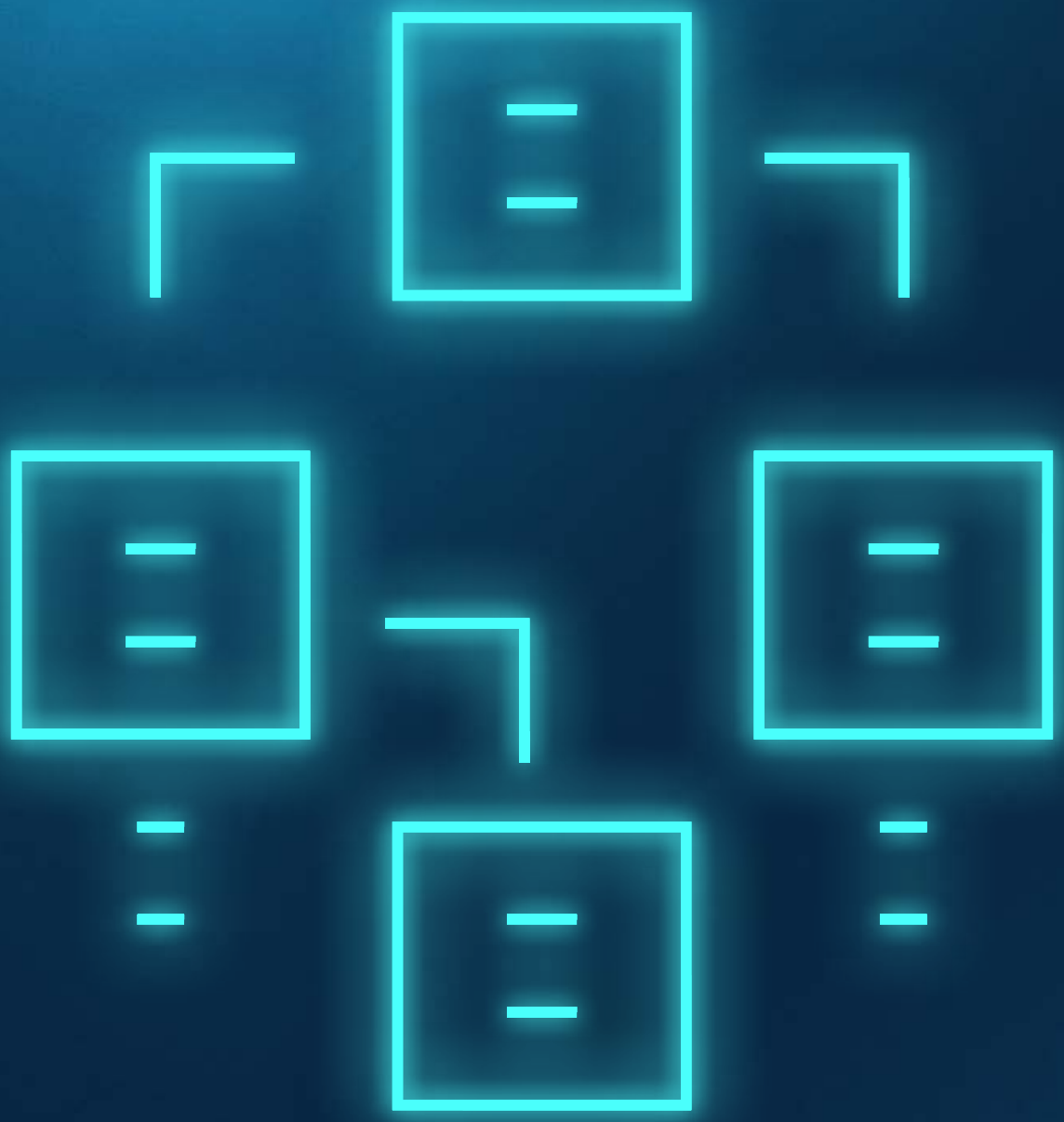
Verteilung der Förderung über die Themenschwerpunkte



Projekte in den Themenschwerpunkten						
	Gesamt	*TSP 1*	*TSP 2*	*TSP 3*	*TSP 4*	*TSP 5*
Förderaufruf 1	20	2	4	2	7	5
Förderaufruf 2	11	1	0	3	6	1
Gesamt	31	3	4	5	13	6

Projekte in den Themenschwerpunkten						
Themen-schwerpunkte	Gesamt	*TSP 1*	*TSP 2*	*TSP 3*	*TSP 4*	*TSP 5*
Förderung in €	38,852 Mio.€	3,769 Mio. €	5,887 Mio. €	3,724 Mio. €	21,642 Mio. €	3,829 Mio. €
Förderung in %	100 %	10 %	15 %	10 %	56 %	10 %

Themen-schwerpunkt 1



Forschung und Entwicklung für Test-Infrastrukturen und Studien im 5G/6G-Backbone-Bereich

Dieser Themenschwerpunkt deckt zwei Bereiche ab:

1a: Test-Infrastrukturen für Forschung und forschungsnahe Entwicklung

Es werden Test-Infrastrukturen im Bereich der Backbone-Architektur der 5G/6G-Netze gefördert, die der Forschung und der forschungsnahen Entwicklung dienen. Das Bundesministerium unterstützt den Aufbau übergreifender Test-Infrastrukturen in Verbundvorhaben, sodass eine verbesserte Vernetzung von Akteuren im Bereich 5G/6G möglich ist.

1b: Forschungs- und Entwicklungsvorhaben mit Bezug zur Sicherheit von 5G/6G-Backbone-Komponenten und Netzen

Projekte, die Sicherheitsaspekte im 5G/6G-Backbone beleuchten, werden ebenfalls gefördert. Das können sowohl Untersuchungen von einzelnen Komponenten als auch von Netzen als Ganzes sein. In den Forschungs- und Entwicklungsvorhaben oder auch in den Durchführbarkeitsstudien dieses Schwerpunkts sollen Angriffsmöglichkeiten und Absicherungsstrategien analysiert, entwickelt, getestet und bewertet werden. Dafür können vorhandene Testnetze weiterentwickelt oder neue Testnetze aufgebaut werden.

Projekte im Themenschwerpunkt 1:

- **B5GCyberTestV2X** - Beyond 5G: Virtuelle Umgebung für Cyber-Sicherheitstests von Vehicle-to-Everything -Systemen
- **RealSec5G** - Uniting Realtime Safety and Security in 5G
- **RIS4NGWB** - Resilienz und Security im Next-Generation Wireless Backhaul mit rekonfigurierbaren und intelligenten Oberflächen

Ansprechpartner für fachliche Fragen

Jan Schwabe
E-Mail: kopa45@bsi.bund.de

B5GCyberTestV2X - Beyond 5G: Entwicklung eines Basissystem und Evaluation einer virtuellen Umgebung für Cyber-Sicherheitstests von Vehicle-to-Everything-Systemen

Abstract
Die Absicherung von Vehicle-to-Everything (V2X)-Technologien bedarf innovativer Lösungsansätze, zum Schutz vor V2-XJamming und V2X-Spoofing. In dem Projekt werden die Anforderungen an 6GV2X-Sicherheitsmechanismen untersucht. Durch die umfangreichen Simulationen können realistische Szenarien geschaffen und somit effektive Schutzmechanismen entwickelt werden.

Motivation
Autonomes Fahren sorgt für einen drastischen Rückgang der Verkehrsunfälle, effizientes und umweltfreundliches Fahren und Zeitersparnis für den Fahrenden. Zudem ergeben sich Geschäftsfelder im Bereich Mobility-as-a-Service (MaaS) für unzählige neue transportbezogene Unternehmen. Dabei sorgt eine sichere kollektive Wahrnehmung für koordiniertes Fahren. In diesem Projekt wird eine Lücke auf dem Gebiet des autonomen Fahrens in Bezug auf die Cybersicherheit geschlossen.

Vision
Angestrebt wird zuverlässiges autonomes Fahren durch sichere V2X-Kommunikation.

Zielstellung
Ziele sind die Entwicklung einer virtuellen Open-Source-Umgebung für Cybersicherheit in V2X-basierten Anwendungen und die Entwicklung von Methoden zum Schutz vor Jamming und Spoofing sowie die Validierung der verschiedensten Szenarien zu einem Bruchteil der Kosten eines realen Aufbaus mithilfe einer virtuellen Simulationsumgebung.

Angestrebte Ergebnisse
Die Bereitstellung der virtuellen Open-Source-Cybersicherheitsumgebung „B5GCyberTestV2X“ zur Validierung von V2X-Algorithmen und Anwendungsfällen für autonome Fahrzeuge wird anvisiert. Der Schwerpunkt der TITUS Research GmbH liegt auf der Validierung der Entwicklungsergebnisse sowohl der virtuellen als auch der experimentellen Validierung.

Erwarteter Impact
Verschiedenste virtuell getestete und evaluierte Szenarien werden zu einem Bruchteil der Kosten eines realen Aufbaus mithilfe einer Simulationsumgebung gemimt. Die neuartige Beyond-5G-basierte V2X-Architektur für V2X unter Berücksichtigung der Informationssicherheit wird angewandt und ermöglicht B5G-basierte V2X-Validierung von Algorithmen und Anwendungsfällen.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	1,8 Mio. €
Partner:	Hochschule Hamm-Lippstadt, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Titus Research GmbH
Projektleitung:	Prof. Dr.-Ing. João Paulo Javidi da Costa, Hochschule Hamm-Lippstadt
Website:	www.b5gcybertestv2x.hshl.de

RealSec5G - Uniting Realtime Safety and Security in 5G

Motivation
Das Projekt RealSec5G möchte im Rahmen einer Durchführungsstudie erproben, inwieweit es heute schon möglich ist, die beiden Anforderungen Security und Safety kostengünstig und effizient in Kommunikationsgeräten für 5G/6G-Infrastrukturen umzusetzen.

Vision
Erschließung neuer, zukunftsträchtiger Anwendungsfelder für Security und Safety in Kommunikationsgeräten für 5G/6G-Infrastrukturen.

Zielstellung
Ziel ist es, die Anforderungen der funktionalen Sicherheit (Safety) in Form von Echtzeitfähigkeit, Redundanz und Übertragungsgarantien sowie der Datensicherheit (Security) in Form der Linespeed-Verschlüsselung gleichzeitig in einem kostengünstigen und einfach zu integrierenden System zu erfüllen, welches als Basis für zukünftige 5G/6G-Infrastrukturkomponenten dienen kann. Aktuell werden diese Anforderungen nur getrennt betrachtet. Im Rahmen einer Umsetzungsstudie soll ein Systemkonzept durch die geeignete Kombination von echtzeitfähigen, deterministischen TSN-Baugruppen (Safety) mit einer effizienten, die Bandbreite ausreizenden Verschlüsselung (Security) auf Basis von MACsec entworfen, realisiert und erprobt werden.

Angestrebte Ergebnisse
Integration eines kombinierten IP-Cores aus bereits bestehenden Cores für Time-Sensitive Networking (TSN) und MAC Layer Security (MACsec). Aufbau eines Demonstrators unter Verwendung von Cots-Komponenten zur Evaluation des Gesamtsystems auf Basis FPGA-basierter SmartNICs.

Erwarteter Impact
Die gewonnenen Erkenntnisse bieten die Möglichkeit einer industriegetriebenen Weiterentwicklung von Produkten und entsprechender Beratungstätigkeiten sowie öffentlich-geförderter Anschlussprojekte. Des Weiteren sind wissenschaftliche Veröffentlichungen und die Qualifizierung wissenschaftlich-technischen Nachwuchses geplant. Das Fraunhofer IPMS nimmt zudem aktiv an internationalen Testbeds des Industrial Internet Consortiums (IIC) und des Labs Networks Industrie 4.0 (LNI) für Konformitäts- und Kompatibilitätstests teil. Die internationalen Organisationen stellen ideale Plattformen für den Test neuer Projektergebnisse dar und bilden zusätzlich den Zugang zu zahlreichen zukünftigen nationalen und internationalen Kunden.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 1,1 Mio. €

Partner: albis-elcon system Germany GmbH, Fraunhofer-Institut für Photonische Mikrosysteme (IPMS)

Projektleitung: Dr. Tim Lackorzynski, albis-elcon system Germany GmbH

Website: realsec5g.albis-elcon.com

RIS4NGWB - Resilienz und Security im Wireless-Backhaul von 5G/6G-Netzwerken mit rekonfigurierbaren und intelligenten Oberflächen

Abstract
Das Team von „RIS4NGWB“ bietet wichtige Entwicklungen im Bereich Physical Layer Security (PLS). Die Integration von reflektierenden intelligenten Oberflächen (RIS) in 5G- und 6G-Netzwerken macht nicht nur ein drahtloses Backhaul-Netzwerk möglich, sondern erhöht auch die Sicherheit. Dies wird durch die Nutzung von mm-Wave-Frequenzen erreicht. Die Resilienz des Netzes wird durch rekonfigurierbare Oberflächen (RIS) gesteigert, da diese in der Lage sind, sich an Änderungen in der Umgebung anzupassen.

Motivation
Die drahtlosen Punkt-zu-Punkt-Netzwerkinfrastrukturen (Wireless Backbone) für 5G/6G sind an vielen Stellen unverzichtbar, aber besonders gefährdet für absichtliche oder unabsichtliche Störungen und Abhörungen. Mit zunehmender Wichtigkeit von mobilen Netzen müssen auch der Schutz und die Resilienz dieser Infrastruktur verbessert werden.

Vision
Neue Netzwerkelemente, in diesem Fall rekonfigurierbare intelligente Oberflächen (reconfigurable intelligent surfaces - RIS), sollen zukünfig dazu beitragen, alternative Verbindungswege für Punkt-zu-Punkt-Netzwerkinfrastrukturen zu ermöglichen. Um diese Netzwerkelemente für verschiedene Verbindungen gemeinsam nutzbar zu machen, müssen sie im Netzwerkmanagement als Ressource ansteuerbar sein. Dies wird über Software-definierte Netze (software defined networking SDN) realisiert.

Zielstellung
Das vorgeschlagene Prinzip soll in einer beispielhaften Einsatzumgebung, dem Testcenter des Fraunhofer IIS, untersucht und demonstriert werden. Außerdem sollen mögliche Anwendungsszenarien, Anforderungen und Systemarchitekturen entwickelt werden.

Angestrebte Ergebnisse
Im Projekt wird von den Partnern ein Katalog an möglichen Anwendungsszenarien, daraus resultierenden Anforderungen sowie eine Systemarchitektur für Hardware- und SDN-Komponenten erarbeitet.

Erwarteter Impact
Das Projekt stärkt das Konsortium und sein Netzwerk am Standort Deutschland durch neu erworbene Lösungskompetenz zur Gewährleistung der neuen und hohen Anforderungen bei Sicherheit und Resilienz im Kontext von Wireless Backhaul. Es erlaubt den zielgerichteten Transfer der Ergebnisse durch Qualifikation wissenschaftlichen Personals, Abschlussarbeiten, wissenschaftliche Veröffentlichungen sowie ggf. Patente, Anwendungsszenarien in Zusammenarbeit mit einzelnen Unternehmen und Verbänden wie NGMN, 5G-ACIA, BDEW, UP-KRITIS und Standardisierung wie 6G (z .B. über 3GPP).

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme	0,9 Mio. €
Partner:	TU Clausthal, Fraunhofer IIS, FAU Erlangen-Nürnberg
Projektleitung:	Prof. Dr.-Ing. habil. Niels Neumann, TU Clausthal
Website:	www.iis.fraunhofer.de/ris4ngwb

Themen-schwerpunkt 2

Forschung und Entwicklung zur Cyber-Sicherheit in 5G/6G-Digitalisierungsfeldern (Nutzungsszenarien)

In Themenschwerpunkt 2 werden Forschungs- und Entwicklungsvorhaben gefördert, die nachhaltig sichere IoT-Anwendungen für Smart Cities - also vor allem für kommunale IoT¬Infrastrukturen - zur Absicherung von Lieferketten oder Verkehrsanalysen für die Personen- und Warenbeförderung betrachten. Voraussetzung ist die Nutzung moderner Mobilfunkinfrastrukturen aus dem 5G/6G-Bereich sowie die Entwicklung marktfähiger Lösungen und deren nachhaltige Umsetzung zur Stärkung der Cyber-Sicherheit.

Projekte im Themenschwerpunkt 2:

- **PIA5** - Public-Key-Infrastruktur (PKI) in Infrastrukturen für industrielle Automatisierungstechnik mit 5G

- **PlusMoSmart** - Planbare und sichere Mobilfunk-IoT-Konnektivität für die Daseinsvorsorge in Smart Cities

- **safe hAAven 5G++** - Cybersichere und datenschutzkonforme IKT-Infrastruktur mit 5G-Zentrale zur Ende-zu-Ende-Verkehrsflussoptimierung in Smart-Cities

- **SILKOSTU** - Sicherheit in der intelligenten Kommunikation zwischen Verkehrsteilnehmenden und städtischer Infrastruktur

Ansprechpartner für fachliche Fragen

Björn Flubacher
E-Mail: kopa45@bsi.bund.de

PIA5 - Cyber-Sicherheit und digitale Souveränität in den 5G/6G Campus-Netzwerken mittels Public-Key-Infrastructure (PKI)

Abstract
Über das Projekt „PIA5“ unterstützt das Fraunhofer-Institut für Angewandte Informationstechnologie (FIT) in Zusammenarbeit mit weiteren Partnern die Entwicklung einer sicheren und zuverlässigen Infrastruktur für 5G-Campus-Netzwerke. Dabei sollen modernste Technologien wie Operational Technology und Multi-Access Edge Computing eingesetzt werden. Um die Sicherheit der Datenübertragung zu gewährleisten, wird auch eine Public-Key-Infrastructure (PKI) implementiert. So wird gewährleistet, dass nur autorisierte Personen Zugriff auf die Daten haben. Das Projekt geht somit einen wichtigen Schritt hin zur digitalen Souveränität von Unternehmen und öffentlichen Einrichtungen.

Motivation
Die Einführung von 5G-Campus-Netzwerken in den Produktionsbereich führt dazu, dass klassische Automatisierungstechnik (OT) und Informationstechnik (IT) zusammenwachsen. Diese neue Architektur erfordert neuartige Security-Mechanismen zu einem sicheren Betrieb. Gleichzeitig bietet dieses Zusammenwachsen die Chance für den Aufbau neuer Industrie 4.0-Konzepte und innovativer Geschäftsmodelle wie „Pay-per-Use“.

Vision
Die Ergebnisse des Projekts sollen eine sichere übergreifende Kommunikation zwischen Informationstechnologie (IT) und Operational Technology (OT) sicherstellen. Dabei gelten 5G-Campus-Netzwerke als IT-Lösung unter Einsatz von Multi-Access Edge Computing (MEC) und Automatisierungstechnik mit den klassischen Feldbussen. Dies wird als Operational Technology (OT) bezeichnet. Das Projekt PIA5 demonstriert den sicheren Betrieb einer Produktionslinie über den gesamten Lebenszyklus der integrierten Komponenten bis hin zu ausgelieferten und beim Kunden betriebenen.

Zielstellung
Die Projektergebnisse werden im Rahmen einer Testintegration in einer realen Produktion überprüft. Dazu erfolgt eine technische Umsetzung und Evaluierung ausgesuchter Use-Cases. Eine speziell erstellte Multi-Access-Edge-Computing-App managt die Verbindung zwischen einem industriellen 5G-Campus-Netzwerk und der Automatisierungstechnik. Ausgewählte Automatisierungskomponenten werden in das System integriert und im Rahmen eines Brownfield-Szenarios berücksichtigt, die nicht für das neue Sicherheitskonzept angepasst werden können.

Angestrebte Ergebnisse
Nach der technischen Umsetzung des Sicherheitskonzepts erfolgt am Ende des Projekts der Aufbau von zwei Testbeds, die verschiedene Best-Practise-Lösungen demonstrieren. Dies ermöglichen für interessierte Unternehmen eine praxisnahe Vorstellung des Sicherheitskonzepts.

Erwarteter Impact
Das Projekt stärkt das Konsortium und sein Netzwerk am Standort Deutschland durch neu erworbene Lösungskompetenz zur Gewährleistung der neuen und hohen Anforderungen bei der Verknüpfung von Automatisierungstechnik und 5G-Campus-Netzwerken. Es erlaubt den zielgerichteten Transfer der Ergebnisse durch eine individuelle Verwertung bei den Partnern. Durch die Einbindung von verschiedenen Verbänden wie dem VDMA, der 5G-ACIA und ausgewählten Feldbus-Gremien können direkte Anforderungen aus der Industrie berücksichtigt und entsprechende Kontakte zu potenziellen Kunden geknüpft werden.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	1,2 Mio. €
Partner:	ZIEHL-ABEGG SE, Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e. V., Hochschule Offenburg
Projektleitung:	Karl Goldmann, ZIEHL-ABEGG SE
Website:	www.pia5.de

PlusMoSmart - Planbare und sichere Mobilfunk-IoT-Konnektivität für die Daseinsvorsorge in Smart Cities – Entwicklung einer modularen Sensorplattform für die Infrastruktur von Städten

Abstract
Mit der neuen 450-MHz-Frequenz und dem 5G-Standard stehen Deutschland revolutionäre Möglichkeiten bevor. Doch damit nicht genug: Durch den Einsatz von Sensoren wird die Daseinsvorsorge (z. B. in der Wasser- und Energieversorgung) in Smart Cities auf ein neues Level gehoben. Das Projekt selbst entwickelt innovative Sensorplattformen, die speziell für die Anwendungsfälle der Daseinsvorsorge konzipiert sind.

Motivation
Eine Voraussetzung für die Smart City, insbesondere für Infrastrukturen zur Daseinsvorsorge, sind planbare und sichere drahtlose Zugangsnetzwerke. Für einen nachhaltigen Aufbau werden verschiedene Mobilfunktechnologien (LTE-M 450 MHz, 5G, 6G) diskutiert. Die zentrale Herausforderung besteht darin, die Chancen und Risiken dieser Technologien transparent zu machen, um nachhaltig Vertrauen zu schaffen und Vorbehalte im Bereich der Digitalisierung in Kommunen abzubauen.

Vision
Das Projekt soll Markteintrittsbarrieren für den sicheren Einsatz moderner Mobilfunktechnologien verringern, das Vertrauen in diese Technologien stärken, um somit die dringend benötigten Modernisierungen der IKT-Netze im Bereich der Daseinsvorsorge voranzubringen.

Zielstellung
Das Ziel von „PlusMoSmart“ ist es, Mobilfunk-IoT-Konnektivität für die Daseinsvorsorge in Smart Cities planbar und sicher zu gestalten und damit Vertrauen in diese Technologien aufzubauen. Mit Fokus auf die Anwender (Unternehmen der Daseinsvorsorge) werden Entwicklungen durchgeführt, welche die Markteintrittsbarriere für moderne Mobilfunktechnologien verringern und somit einen Beitrag zur nachhaltig sicheren Modernisierung der Netze liefern.

Angestrebte Ergebnisse
Die Entwicklung einer sicheren, modularen Sensorplattform für Anwendungsfälle der Daseinsvorsorge im Kontext von 5G-Campusnetzwerken, welche bspw. auf Betriebshöfen oder Industrieanlagen (u. a. Heizkraftwerke, Windparks, Häfen, Flughafen, Stahlwerke) errichtet werden, sowie eines 450-MHz-Mobilfunknetzes als Funknetz für die Digitalisierung kritischer Infrastrukturen. Außerdem wird eine Software für kommunale Unternehmen aus dem Bereich Smart City oder Daseinsvorsorge entwickelt, um Planungssicherheit für die Ausbringung von moderner Sensorik auf ihrem Versorgungsgebiet zu erlangen.

Erwarteter Impact
Die geplanten Arbeiten führen dazu, dass die strategischen und operativen Risiken für den sicheren Einsatz moderner Netztechnologien minimiert werden. Planbarkeit für Digitalisierungsprojekte in der Daseinsvorsorge wird hergestellt und Sicherheitslücken werden identifiziert und beherrschbar gemacht. Durch den direkten Beitrag eines Anwenders können die Entwicklungen erprobt und die Ergebnisse mit direktem Praxisbezug weiterverbreitet werden.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	0,9 Mio. €
Partner:	ATS Elektronik GmbH, Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., Bonn-Netz GmbH, Rheinisch-Westfälische Technische Hochschule Aachen
Projektleitung:	Dr. Astrid Krage, ATS Elektronik GmbH
Website:	https://www.plusmosmart.de

safe hAAven 5G++ – Sichere und datenschutzkonforme IKT-Infrastruktur mit 5G- Ende-zu-Ende-Verkehrsflussoptimierung in Smart-Cities. Zuverlässige Erfassung und strukturierte Visualisierung von aktuellen Mobilitätsinformationen

Abstract
Sichere Datenübertragung in Smart Cities wird mit dem Projekt „safe hAAven 5G++“ durch eine datenschutzkonforme Infrastruktur für die Sensorik möglich. Der Fokus liegt auf einer cybersicheren Ende-zu-Ende-Verkehrsflussoptimierung dank zentraler 5G-Technologie. Die Expertise liegt hierbei in den Bereichen Sicherheit, Datenschutz und Sensortechnologie.

Motivation
Datenvermeidung, Datensparsamkeit sowie Datenschutz- und Cyber-Sicherheit sind als Grundpfeiler der Umsetzung angesehen. Hierbei wird in allgemeinverständlichen Security-/Privacy-Policies dokumentiert.

Vision
Die Digitalisierung des Straßenverkehrs durch Echtzeit-Verkehrsflussoptimierung.

Zielstellung
Ziel von „safe hAAven 5G++“ ist es, für eine Smart-City-Umgebung Funkdatenverbindungen und zugehörige Anwendungen bzgl. ihrer Funktionalität, Cyber-Sicherheit und ihres Datenschutzes derart einfach konfigurierbar zu gestalten, sodass technikfremde Entscheider/innen deren Konsequenzen überblicken können.

Angestrebte Ergebnisse
Im Rahmen von „safe hAAven 5G++“ soll vorwettbewerblich eine cybersichere und datenschutzkonforme Lösung für kamerabasierte Sensoriken entwickelt und integriert werden. Daneben ist die Projektleitung und -koordination ebenso Teil des Aufgabenpaketes wie die Durchführung von Workshops und die Erstellung von Nutzer-Studien in Smart City Kommunen.

Erwarteter Impact
Es wird eine cybersichere und datenschutzkonforme Vernetzungslösung mit statistischer Erfassung von Bewegungsrouten zur Verkehrsoptimierung entwickelt. Die Lösungen werden in einem RealBed integriert, demonstriert und evaluiert. Weitergehend schafft die erarbeitete Lösung nicht nur einen Mehrwert für weitere Modellkommunen, sondern sie kann in Zukunft auch von Road-Side-Units genutzt werden.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 2,0 Mio. €

Partner: GEO DATA GmbH, Stadt Aalen, Hochschule Aalen - Technik und Wirtschaft, Conclurer GmbH

Projektleitung: Rudi Feil, GEO DATA GmbH

Website: https://www.safehaaven5gplus.de/

SILKOSTU – Cyber-Sicherheit in der intelligenten 5G/6G-Kommunikation zwischen Verkehrsteilnehmenden für eine lernende städtische Infrastruktur und höhere Verkehrssicherheit

Abstract
Für das Projekt „SILKOSTU“ ist Cyber-Sicherheit das A und O. In modernen Vernetzungs- und Smart-City- Szenarien spielt Datensicherheit eine entscheidende Rolle. Die Kommunikationstechnologien müssen auf höchstem Niveau arbeiten, um eine reibungslose und sichere Infrastruktur zu gewährleisten. SILKOSTU fokussiert sich auf die Umsetzung intelligenter Infrastruktur und die Vernetzung zwischen Fahrzeug-zu-Infrastruktur (V2I) und Infrastruktur-zu-Fahrzeug (I2V), um eine effizientere und sichere Nutzung der städtischen Ressourcen zu ermöglichen. Das Projekt basiert auf 5G/6G-Mobilfunk-Netzwerken und bildet den Schlüssel für städtische Infrastrukturen der Zukunft.

Motivation
Aktuell gibt es auf dem Markt keine Hardware-Software-Lösung, die alle drei Kommunikationsstandards (WLANp, C-V2X, 5G/6G) miteinander verbindet. In Europa ist noch nicht klar, welcher der Kommunikationsstandards sich durchsetzen wird. Für die Absicherung der Mobilfunkkommunikation mittels eUICC existieren parallel mehrere Standards. Existierende TEE (Trusted Execution Environment) liefern zwar hohe Sicherheit, wie sie von Anwendungen im 5G/6G-Bereich benötigt werden, sind aber aufgrund von Performance-Overheads nicht für den Einsatz im echtzeitkritischen 5G/6G-Bereich geeignet.

Vision
Vision ist die Erhöhung der Sicherheit in der intelligenten Kommunikation zwischen Verkehrsteilnehmern und städtischer Infrastruktur, die Ermöglichung von Echtzeitkommunikation als Grundstein für automatisiertes und autonomes Fahren, die Optimierung der Verkehrslage, Priorisierung von Nahverkehr und Einsatzfahrzeugen, der Schutz von vulnerablen Verkehrsteilnehmern/-innen sowie der Umweltschutz.

Zielstellung
Speziell in der Mobilität ist die direkte Vernetzung von allen Akteuren im Straßenverkehr ein essenzieller Grundbaustein für sichere, effiziente und schließlich autonome Mobilität. Um diese Vernetzung zu ermöglichen, bedarf es neuer Kommunikationstechnologien, die Verkehrsteilnehmer/-innen miteinander vernetzen und hohen Sicherheitsanforderungen gerecht werden. Hohe Sicherheit in der Kommunikation zwischen den Geräten der Verkehrsinfrastruktur kann durch zusätzliche Hardware-Sicherheitsmodule gewährleistet werden.

Angestrebte Ergebnisse
Entwicklung einer Hardware, die es erlaubt, Daten von verschiedenen Verkehrsteilnehmern/-innen zu sammeln (entweder in Form eines Steuercomputers im Fahrzeug oder am Straßenrand) und verschlüsselt in einer Cloud zu speichern. Das bedeutet, dass die Hardware durch verschiedenen Sicherheitselemente ergänzt wird, die den Ansprüchen des Datenschutzes und des IT-Sicherheitsgesetzes 2.0 genügen.

Erwarteter Impact
Durch dieses Vorhaben werden insbesondere nationale Betreiber (Smart Cities) wie auch Hersteller der Industrie und Forschungseinrichtungen gestärkt, weil die Hardware- und Softwareelemente nach hiesigen Standards entwickelt und erprobt werden und Ergebnisse später somit weiter in Deutschland verwertet werden können. Der Standort Deutschland profitiert von den Ergebnissen, da die Positionierung in Wissenschaft und Technik bezüglich sicherer Kommunikation im Automobil- und Verkehrsbereich erweitern wird. Dadurch werden Ziele wie Emissionsverminderung und Vision-Zero (keine Verkehrstoten und keine Schwerverletzten) unter Einhaltung geltender Datenschutzverordnungen unterstützt und die Städte vertiefen ihr Image als Smart Cities.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	1,8 Mio. €
Partner:	Universität zu Lübeck, consider it GmbH, Giesecke + Devrient Mobile Security GmbH, Stadt Hamburg
Projektleitung:	Dr.-Ing. Leutrim Mustafa, Universität zu Lübeck
Website	www.silkostu.de

Themen-schwerpunkt 3

Forschung und Entwicklung zum Aufbau von 5G/6G-Prüf- und Zertifizierungsstellen

Gefördert werden die Forschung und Entwicklung zu innovativen Produkten und Dienstleistungen in der 5G/6G-Zertifizierung. Darunter fallen zum Beispiel neuartige Testaufbauten und -szenarien sowie die Weiterentwicklung von Werkzeugen für Sicherheitsprüfungen im 5G/6G-Bereich. Unterstützt werden Einzel- und Verbundvorhaben mit mindestens einer Prüf- und Zertifizierungsstelle; auch jene, die bereits existierende, sicherheitstechnische Prüfungen von IT-Komponenten und -Infrastrukturen signifikant erweitern können. Führen Prüf- und Zertifizierungsstellen neuartige Prüfverfahren für die KI-basierte Netzsteuerung, Virtualisierung oder für cloudbasierte Ansätze ein, können auch diese gefördert werden.

Projekte im Themenschwerpunkt 3

- **Ag5G+** - Etablierung einer zukunftsorientierten Prüfstelle zu „Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation“ (NESAS CCS-GI)
- **MANTRA5G** - Modular, Adaptive and iNteroperable Test fRAmework for 5G/6G
- **OPNESAS** - Operationalisierung der NESAS-Zertifizierung
- **Pentest-5GSec** - Mobiles Pentesting für sichere 5G-Netze
- **UuW5G** - Untersuchung und Weiterentwicklung des 5G Zertifizierungsschemas NESAS CCS-GI; Teilvorhaben: Aufbau von NESAS CCS GI

Ansprechpartner für fachliche Fragen

Jörg Andreas
E-Mail: kopa45@bsi.bund.de

Ag5G++ - Etablierung einer zukunftsorientierten Prüfstelle mit Fokus auf Virtualisierung und Fuzzing zu „Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation“ (NESAS CCS-GI)

Abstract
Erleben Sie die Zukunft der 5G-Sicherheit mit „Ag5G+“, der Etablierung einer zukunftsorientierten Prüfstelle für NESAS CCS-GI. Mit Fokus auf Virtualisierung und Fuzzing wird die Prüfstelle dazu beitragen, dass Netzwerke höchsten Sicherheitsstandards entsprechen. Die zertifizierte und zuverlässige 5G-Verbindung wird hier von „Ag5G+“ sichergestellt werden.

Motivation
Die IT-Sicherheit der Infrastruktur von Netzbetreibern, insbesondere 5G, ist bisher kaum zertifiziert worden. Das BSI hat aus diesem Grund am 1. Juli 2022 das neue NESAS-CCS-GI-Schema gestartet. atsec hat bereits eine führende Stelle bei internationalen NESAS-Audits, viel Erfahrung mit der Evaluierung von Komponenten nach Common-Criteria sowie erste 5G-Komponenten nach dem internationalen NESAS/SCAS-Schema geprüft.

Vision
Deutsche Betreiber von 5G- und zukünftigen Netzwerkgenerationen verfügen über eine Auswahl an Netzwerkkomponenten, die nachweisbar einer unabhängigen Sicherheitsprüfung unterzogen wurden. Betreiber kritischer Infrastrukturen können so existierende Zertifizierungsanforderungen an Komponenten erfüllen. Das ermöglicht Endnutzern, Vertrauen in die Sicherheit der Anwendungen zu gewinnen und stärkt die digitale Souveränität in Deutschland.

Zielstellung
Es soll die Prüfung der herstellerunabhängigen Erfüllung aller NESAS-CCS-GI-Anforderungen mithilfe einer virtualisierten Testinfrastruktur und einem Test-Framework für gängige Funktionen von 5G-Core-Netzwerken ermöglicht werden. Dabei berücksichtigt das Projekt moderne Ansätze wie virtualisierte Netzwerkfunktionen, Infrastructure-as-a-Service und OpenRAN sowie Anforderungen an das Testing und das Fuzzing.

Angestrebte Ergebnisse
Das Projekt soll effiziente Prüfverfahren durch ein flexibles virtualisiertes Test-Framework und mobile Testaufbauten ermöglichen. Die mit einer Pilotevaluierung einer 5G-Komponente gesammelten Erfahrungen in Bezug auf Anforderungen und Methoden sollen an das zugrundeliegende NESAS/SCAS-Schema zurückgeführt werden.

Erwarteter Impact
Das Projekt zielt darauf ab, Herstellern von 5G-Produkten eine vergrößerte Auswahl an Prüfstellen im NESAS-CCS-GI-Schema anzubieten und effiziente Prüfverfahren zur Evaluierung von Komponenten zu erreichen. Außerdem profitieren Netzbetreiber und Endanwender mittels Verfügbarkeit und Einsatz zertifizierter-Komponenten von einer erhöhten Sicherheit der 5G-Core-Netze.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 0,3 Mio. €

Partner: atsec information security GmbH

Projektleitung: Dr. ret. nat. Andreas Hohenegger, atsec information security GmbH

Website: www.atsec.de/forschung/index.html

MANTRA5G - Modular, Adaptive and iNteroperable Test fRAmework for 5G/6G

Motivation

5G wird mehr und mehr Teil des täglichen Lebens und damit auch vermehrt in kritischen Infrastrukturen eingesetzt. Eine flächendeckende Verbreitung, hohe Vernetzung und eine große Anzahl an Teilnehmenden erhöhen jedoch auch die Fläche für mögliche Angriffe und deren Auswirkungen. Dies führt zu neuen Sicherheitsanforderungen und damit auch zu neuen Prüfaspekten und –abläufen, die notwendig werden, um ein definiertes Maß an IT-Sicherheit zu erreichen. IT-Sicherheitsevaluationen und -zertifizierungen stellen einen wichtigen Baustein dar, um Vertrauen in die 5G-Technologie zu generieren. Ein Zertifikat ermöglicht es Herstellern, die Einhaltung geforderter Sicherheitseigenschaften nachzuweisen. Durch gesetzliche Rahmenbedingungen wird eine Vielzahl an unabhängigen Prüfungen für kritische 5G-Komponenten erforderlich. Um einen effizienten Testablauf solcher Komponenten zu ermöglichen, sind automatisierte Testwerkzeuge zur Unterstützung des Prüfablaufes unerlässlich.

Vision

Vom BSI wurde das neue Produktzertifizierungsverfahren NESAS CCS-GI entwickelt. Darin wird unter anderem festgelegt, welche Prüfaspekte durchzuführen sind und welche IT-Sicherheitstests im Rahmen der Produktprüfung auf den Prüfgegenstand angewendet werden müssen. Um Sicherheitstests vergleichbar und effizient durchführen zu können, sind einheitliche Testtools und Prüfabläufe wünschenswert. Eine besondere Herausforderung stellt dabei die wachsende Anzahl von 5G-Komponenten und deren vielfältige Varianten dar. Nicht nur eine Betrachtung der unterschiedlichen Produktklassen, sondern auch die oft hochgradig heterogen bzw. proprietär implementierten Schnittstellen erschweren die Wiederverwendbarkeit von Testketten. Da es sich bei NESAS CCS-GI um ein neu etabliertes Schema handelt, existieren aktuell keine dedizierten Testtools, die von Prüfstellen als Werkzeug eingesetzt werden können. Diese sind jedoch für eine (teil-) automatisierte und effiziente Prüfung unerlässlich.

Zielstellung

In diesem Vorhaben sollen Anforderungen an ein innovatives und interoperables Testframework spezifiziert werden, das in seiner finalen Ausprägung die zeit- und kosteneffiziente (teil-) automatisierte Prüfung nach dem „Network Equipment Security Assurance Scheme“ (NESAS) und dem „NESAS Cybersecurity Certification Schema – German Implementation“ (NESAS CCS-GI) für kritische 5G-Komponenten erlaubt. Im Rahmen der Projektlaufzeit soll zudem ein Demonstrator entwickelt werden, der die einzelnen Komponenten des spezifizierten Frameworks umsetzt. Dies umfasst beispielsweise die Weiterentwicklung von Open-Source-Lösungen zur Nachbildung eines 5G-Netzes, die Umsetzung einer herstellerunabhängigen Zwischenschicht (API) sowie die Implementierung und Automatisierung von Testschritten nach NESAS CCS-GI.

Angestrebte Ergebnisse
Die Ergebnisse des Projektes sollen den Aufbau von Prüfstrecken und Testketten bei Prüfstellen unterstützen, um das Vertrauen in 5G-Komponenten sowie die Vergleichbarkeit des Testens zu erhöhen. Die gewonnenen Zwischenergebnisse, wie z. B. die Erkenntnisse zur herstellerunabhängigen Umsetzbarkeit und Automatisierbarkeit der Testfälle sowie die Analyse der prüfnotwendigen Trigger können in die (Weiter-)Entwicklung vorhandener Prüfschemata und gesetzlicher Regelungen einfließen.

Erwarteter Impact
Die Untersuchungsergebnisse werden den entsprechenden öffentlichen Stellen zur Verfügung gestellt. Der entwickelte Demonstrator soll in den Räumlichkeiten von Prüfstellen direkte praktische Einsetzbarkeit bieten und mittelfristig Prüfungen nach NESAS und NESAS CCS-GI beschleunigen. Darüber hinaus werden weitere Projektergebnisse wie z. B. die weiterentwickelte Open-Source-Software anderen Parteien der 5G-Community zur Verfügung gestellt werden. Nach Abschluss des Projektes soll der Demonstrator weiterentwickelt werden, um den Funktionsumfang zu erhöhen, neue behördliche Anforderungen zu implementieren oder weitere IT-Sicherheitstests umzusetzen. Auf der Grundlage des Demonstrators werden die Projektpartner kommerzielles Testequipment entwickeln und eine führende Martkstellung für Prüfequipment im 5G/6G-Kontext anstreben.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 0,8 Mio. €

Partner: TÜV Informationstechnik GmbH, exceeding solutions GmbH

Projektleitung: Markus Wagner, TÜV Informationstechnik GmbH

Website: www.mantra5g.de

OPNESAS - Optimierung der Sicherheit für 5G-Campus-Netzwerke durch Operationalisierung der NESAS-Zertifizierung (OPNESAS)

Abstract
Das Projekt „OPNESAS“ hat die Optimierung der Sicherheit für 5G-Campus-Netzwerke zum Ziel. Mit Hilfe der Sicherheitsprüfung mittels NESAS- und SCAS-Zertifizierung wird das 3GPP-kompatible Prüflabor garantieren können, dass maximale Sicherheit für 5G-Private-Networks erreicht werden können.

Motivation
Potentielle Angriffsvektoren in öffentlichen sowie privaten 5G-Netzen stellen Risiken für alle darauf aufbauenden Anwendungen, Nutzer und Geräte dar. Ursachen für Angriffsvektoren können Spezifikations-, Implementierungs-, Konfigurations- oder Betriebsfehler sein.

Vision
„OPNESAS“ hat die Vision etablierte Security-Testing und Zertifizierungs-Methoden weiterzudenken. Hierzu werden die etablierten SCAS-Testfälle der 3GPP automatisiert und technisch weiterentwickelt. „OPNESAS“ beabsichtigt in 5G-Netzen den Security-Status während des laufenden Netzbetriebs ohne Unterbrechungen testen zu können.

Zielstellung
OPNESAS verfolgt das Ziel eines Left Shift, was bedeutet, das Prüflabor geht mit seinen Testwerkzeugen in die CI/CD-Pipelines des Herstellers. Parallel dazu wird auch der Right Shift untersucht, dies bedeutet die Testwerkzeuge werden im Livenetz eingesetzt. Mit OPNESAS wird darüber hinaus das Ziel verfolgt, möglichst ein komplettes 5G-Netz mit dessen Konfiguration zu zertifizieren.

Angestrebte Ergebnisse
Das Projekt „OPNESAS“ plant eine detaillierte Bedarfsermittlung am Markt durchzuführen, um die Möglichkeiten bezüglich 5G-Security-Testings auszuloten. Dies soll die Projektpartner in die Lage versetzen, zukunftsfähige Geschäftsmodelle im Bereich von 5G-Security zu entwickeln. Des Weiteren sollen neue technische Standards für Schnittstellen entwickelt werden, welche das automatisierte Testen möglich machen.

Erwarteter Impact
Durch „OPNESAS „können Impulse für das deutsche NESAS-CCS-GI-Schema sowie das GSMA-Schema entwickelt werden. Durch marktorientierte Zertifizierungsangebote soll das Interesse an der NESAS-Zertifizierung angekurbelt werden.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 1,2 Mio. €

Partner: secuvera GmbH, Ruhr-Universität Bochum, CampusGenius GmbH (im Unterauftrag)

Projektleitung: Sebastian Fritsch, secuvera GmbH

Website: www.opnes.as

Pentest-5GSec - Mobiles Pentesting für sichere 5G-Netze

Motivation
Die Verbreitung von 5G-Netzen erfordert eine hohe Sicherheit der einzelnen Komponenten. Insbesondere mit der zunehmenden Privatisierung des Mobilfunksektors durch Campusnetze müssen diese unter dem Aspekt der Informationssicherheit betrachtet und behandelt werden. Da Campusnetze für verschiedene Infrastrukturen, darunter auch kritische Infrastrukturen wie das Gesundheitswesen oder die Energieversorgung, genutzt werden sollen, müssen entsprechend hohe Sicherheitsstandards innerhalb des Netzes vorhanden sein. Darüberhinaus müssen auch die eingesetzten Komponenten geprüft werden, da sie letztlich den gesamten Netzverkehr innerhalb eines Netzsegments oder Campusnetzes verarbeiten.

Vor allem im Kernnetz setzen 5G-Netze auf Webtechnologien wie HTTPS, Docker, Kubernetes oder OpenAPI. Diese Komponenten ändern sich ständig und müssen neben der eigentlichen Hardware auch getestet und gehärtet werden. Aktuelle Audit- oder Pentesting-Richtlinien sind für 5G-fähige Kommunikationsgeräte nicht konform. Diese Wissenslücke muss unbedingt geschlossen werden, da immer mehr 5G-Geräte in der realen Welt eingesetzt werden. Außerdem müssen die aktuellen Bedrohungsmodelle ständig aktualisiert werden und auf der Grundlage dieser Bedrohungsmodelle müssen die Produkte in einem Laborsystem entsprechend zertifiziert werden. Derzeit gibt es in Deutschland nur zwei NESAS-CCS-GI-Testzentren, die die erwartete Anzahl der zu testenden Systeme kaum bewältigen können.

Vision
Dieses Projekt soll zu einer vielfältigen Audit-Landschaft beitragen und bestimmte Aspekte des Audit-Prozesses einer breiten Öffentlichkeit zugänglich machen. Insbesondere die Komponenten des Pentestings und der Bedrohungsmodellierung sollen innerhalb des Audit-Prozesses gestärkt werden.

Zielstellung
Ziel ist es, ein mobiles Prüflabor und Werkzeuge zu entwickeln, die zum Pentesting eines 5G-Netzwerks eingesetzt werden können. Darüber hinaus werden Erkenntnisse im Bereich der Bedrohungsmodellierung und der wirtschaftlichen Tragfähigkeit generiert.

Angestrebte Ergebnisse
Neben der traditionellen Präsentation von Forschungsergebnissen auf kompetitiven (Entwickler-) Konferenzen und in Fachzeitschriften ist insbesondere geplant, die Projektergebnisse in die (Weiter-) Entwicklung konkreter Dienstleistungen einfließen zu lassen. Um einen Technologietransfer zu gewährleisten, sollen die Ergebnisse in Form von White Papern oder Workshops auch (regionalen) Firmen zur Verfügung gestellt werden. Darüber hinaus werden die Ergebnisse einen Beitrag zur öffentlichen Diskussion und zur akademischen Lehre leisten. Es ist geplant, die Projektergebnisse als Open-Source-Software bzw. Katalog zur Verfügung zu stellen. Die Projektergebnisse haben erhebliche Auswirkungen auf die zukünftige Einwerbung weiterer Fördermittel auf nationaler wie auf EU-Ebene, zumal mit UbiTrans Vorarbeiten in diesem Bereich geschaffen werden, die in Zukunft zur Einordnung Deutschlands in den europäischen Kontext genutzt werden können. Daraus ergeben sich interessante Möglichkeiten für Folgeprojekte, insbesondere nach Projektabschluss.

Erwarteter Impact
Das Vorhaben soll einen Beitrag zum Technologietransfer sowie zur öffentlichen Diskussion und zur akademischen Lehre leisten. Darüber hinaus soll es die Resilienz moderner Kommunikationsnetzwerke stärken. Die Projektergebnisse haben erhebliche Auswirkungen auf die zukünftige Einwerbung weiterer Fördermittel auf nationaler wie auf EU-Ebene, die in Zukunft zur Einordnung Deutschlands in den europäischen Kontext genutzt werden können. Daraus ergeben sich interessante Möglichkeiten für Folgeprojekte.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 0,5 Mio. €

Partner: AWARE7 GmbH, Ruhr-Universität Bochum

Projektleitung: Dr. Matteo Große-Kampmann, AWARE7 GmbH

Website: https://aware7.com/de/forschung-entwicklung/

UuW5G - Untersuchung und Weiterentwicklung des 5G-Zertifizierungsschemas NESAS CCS-GI

Motivation
Das NESAS CCS-GI Schema startete zum 01. Juli 2022 und stützt sich weitgehend auf die Verwendung vorhandener und erprobter Testspezifikationen aus dem Mobilfunk. Ziel ist die Implementierung eines Evaluierungs- und Zertifizierungsschemas, das eine größtmögliche Sicherheit der 5G- Kommunikationsinfrastruktur durch qualifizierte Prüfung der Komponenten gewährleistet. Die Evaluierung soll hierbei durch anerkannte NESAS CCS-GI-Prüfstellen erfolgen. Die dafür notwendigen Prüf- und Zertifizierungsstrukturen befinden sich derzeit im Aufbau.

Im Rahmen dieses Projektes ist der Aufbau von Prüfkompetenzen im Bereich 5G/6G, die Effizienzsteigerung zukünftiger Evaluierungen durch die Analyse vorhandener und die Erforschung neuer Testszenarien sowie die Weiterentwicklung und Automatisierung der Methodiken und Testwerkzeuge, welche die Prüfstelle im Rahmen von Sicherheitsprüfungen in Zertifizierungsverfahren nutzten kann.

Vision
Das Projekt wird durch die Zusammensetzung des Konsortiums mit den spezifischen und sich ergänzenden Kompetenzen der einzelnen Partner, durch die Weiterentwicklung der Prüfmethodik und Prüfwerkzeuge sowie durch den Wissenstransfer sowohl untereinander als auch in das Schema zum Aufbau von Prüf- und Zertifizierungskompetenzen und -ressourcen beitragen.

Zielstellung
Das Projekt hat die Weiterentwicklung von Testszenarien und die Erforschung und Entwicklung von Werkzeugen für Sicherheitsprüfungen zum Ziel, die eine weitgehend automatisierte, standardisierte, nachvollziehbare und somit evaluationsgeeignete Prüfung von 5G-Komponenten im Rahmen des NESAS CCS-GI-Schemas unterstützen. Hierduch soll sowohl eine umfangreichere und gründlichere als auch zugleich eine effizientere Evaluierung ermöglicht werden. Der Aufbau von Prüfstellen soll erfolgen.

Angestrebte Ergebnisse
Methoden und Werkzeuge für die Evaluierung von 5G Komponenten und optimierte Prüfprozesse, die eine weitgehend automatisierte, standardisierte, nachvollziehbare und somit evaluationsgeeignete Prüfung von 5G-Komponenten im Rahmen des NESAS CCS-GI-Schemas unterstützen,

Außerdem soll im Rahmen des Projektes die Anerkennung eines NESAS-CCS-GI Prüflabors und die Durchführung einer Evaluierung in diesem Schema, wenn möglich einschließlich einer Zertifizierung, erfolgen.

Erwarteter Impact
Die Unterstützung von Herstellern und Prüfstellen beim Testen von Produkten vor und während der Zertifizierung führt zu besser getesteten und damit sichereren Produkten auf dem Markt. Der Standort Deutschland gewinnt durch die Erforschung und Entwicklung von verbesserten Testmethodiken eine höhere Testkapazität. Die Bereitstellung weiterer Prüfkapazitäten und die angestrebte Weiterentwicklung der Automatisierung auf NESAS-Spezifikationen basierender Tests und Produktgutachten soll außerdem zu einer schnelleren und höheren Verfügbarkeit für den Betrieb zugelassener Produkte führen und damit letztlich Kosten senken und Qualität steigern.

Projektlaufzeit:	01.06.2023 - 30.11.2024
Fördersumme:	0,9 Mio. €
Partner:	SRC Security Research & Consulting GmbH, Research Industrial Systems Engineering (RISE) Deutschland GmbH
Assoziierter Partner:	ZTE Deutschland GmbH
Projektleitung:	Ansgar Tessmer, SRC Security Research & Consulting GmbH
Website:	www.uuw5g.de

Themen-schwerpunkt 4

Forschung und Entwicklung zur Sicherheit und Resilienz von 5G/6G-Technologien und Infrastrukturen

4a: Sichere Lieferketten für Campus-Netze

Durch geförderte Forschungs- und Entwicklungsarbeiten wird darauf abgezielt, sichere Lieferketten für den Aufbau und Betrieb von sogenannten Campus-Netzen zu etablieren. Sichere Lieferketten in diesem Bereich können die digitale Souveränität der Bundesrepublik und der EU stärken. Technologische Entwicklungen wie Open RAN bieten dabei neue Chancen in der Funkzugangstechnologie.

Es soll erforscht werden, wie mit entwickelten Produkten und Lösungen – gegebenenfalls gemeinsam mit weiteren Anbieterinnen und Anbietern – eine sichere Lieferkette aufgebaut werden kann. Dabei soll soweit wie möglich auf Technologien und Unternehmen aus Deutschland und Europa zurückgegriffen werden und Alternativen zu aktuellen Lieferketten geschaffen werden. Zudem sollen diese marktfähig und passend für viele Firmen und Organisationen sein.

4b: Security-Innovationen zur Erhöhung der Resilienz von 5G-Infrastrukturen

Im Vordergrund steht hier die Entwicklung von Produkten, Lösungen und Dienstleistungen, aber auch von Methoden und Verfahren, die den sicheren Einsatz von 5G/6G unterstützen. Gefragt sind Innovationen zur Sicherheit, die die Resilienz von Infrastrukturen steigern können. Dazu gehören etwa die Bereitstellung von Minimalfunktionen für Netzinfrastrukturen in Störfällen oder die Entwicklung von Sensorik, um Störangriffe zu erkennen und abzuschwächen.

Durch die Einführung von 5G entstehen viele neue Anwendungsfelder wie Massive Machine Type Communications (mMTC) oder Ultra Reliable and Low Latency Communications (uRLLC). Auch für diese Anwendungsprofile spielt das Thema Sicherheit eine große Rolle. So muss beispielsweise die Resilienz von 5G-basierten Infrastrukturen gegenüber Störangriffen (sogenanntes Jamming) deutlich erhöht werden, um die 5G-Technologie für zum Beispiel automatisiertes Fahren verlässlich zu machen.

Projekte im Themenschwerpunkt 4

- **5GProSec** - IT-Security beim Einsatz von 5G im Ökosystem Produktion
- **5G-Sierra** - Sichere 5G-Infrastrukturen für resiliente Produktionssysteme und -anlagen
- **6G-ReS** - Sichere und resiliente 5G/6G-Systeme
- **ADVISIOR5G** - Ein verteilter drahtloser Schutzschirm für private 5G Netze
- **COBRA-5G** - Container-basierte resiliente Architektur für 5G Campus-Netzwerke
- **DeSiRe-NG** - DEpendable and Secure Infrastructure for Resilient Next Generation Networks
- **EMiL** - „Echtzeitfähige Machine-Learning“-Lösungen für resiliente und sichere 5G/6G-Netze am Beispiel von Automatisierungsanwendungen

- **FlexShield** - Resiliente 5G Vernetzung für industrielle Echtzeitanwendungen

- **medCS.5** – Cyber-Sicherheit für den Austausch medizinischer Daten: 5G-Campusnetz für klinische und eHealth-Anwendungen

- **MNT-Pro** - Mobile Network Protector

- **QSyncNextG** - Quantum Synchronisation for Resilient and Secure Next Generation (5G/6G) Campus Networks

- **PHYSICS** - PHY Security Innovations- for Communication Systems

- **RIOT** - Resiliente IoT – Hochverfügbare Infrastruktur für kritische IoT-Anwendungen

Ansprechpartner für fachliche Fragen

Matthias Weber
E-Mail: kopa45@bsi.bund.de

5GProSec

5GProSec - IT-Security beim Einsatz von 5G im Ökosystem Produktion

Motivation
Kommunikation dient dem Informationsaustausch. Abhängig vom Kommunikationsmedium können einige, viele oder sehr viele Informationen in kurzer Zeit ausgetauscht werden. Die ausgetauschten Informationen sollen dabei, unabhängig vom genutzten Kommunikationsmedium, unverändert und von außen nicht beeinflussbar sein. Übertragen auf den industriellen Kontext bedeutet dies, dass 5G-Technologie das Kommunikationsmedium ist, um die in der Produktion notwendigen Datenmengen zu transportieren, dabei aber mögliche äußere Einflussfaktoren bedacht werden müssen. Um hinsichtlich der Produktionstechnik auf hohem Niveau arbeiten zu können, müssen Unternehmen die Firmen-IT-Infrastruktur systematisch vor Cyberangriffen schützen und Methoden entwickeln, dies auf allen denkbaren Ebenen umzusetzen.

Vision
Wir entwickeln eine Handreichung, um ...

- ... Anwender zu sensibilisieren und in der sicheren Nutzung des Kommunikationsmediums zu unterstützen.
- ... Experten zu sensibilisieren und umfassend über nicht-technische Unsicherheitsfaktoren zu informieren und den adäquaten Umgang damit zu schulen.

Zielstellung
Ziel des Forschungsprojekts 5GProSec ist die systematische Erfassung und Beseitigung von möglichen Angriffsvektoren und unbeabsichtigten Störungen beim Einsatz von 5G speziell in der Produktion, um Hürden für den Einsatz von 5G in Unternehmen zu senken und Sicherheitsbedenken auszuräumen. Für die Erreichung des Ziels wird ein ganzheitlicher Ansatz verfolgt, indem sowohl technische als auch nicht-technische Aspekte in Bezug zu IT-Security und Resilienz von 5G-Anwendungen speziell in der Produktion betrachtet werden. Zur Erforschung von Risiken und zur Entwicklung von Methoden zur Verringerung dieser Risiken werden ein stationärer und ein mobiler Demonstrator aufgebaut, die jeweils unterschiedliche Anwendungsmöglichkeiten von 5G in der Produktion repräsentieren.

Angestrebte Ergebnisse
Anhand der Demonstratoren sollen die Auswirkungen produktionsspezifischer, technischer Störgrößen, wie z. B. eine Verringerung der Empfangsstärke von Endgeräten durch den Einsatz von Kühlschmierstoff im Maschinenraum, bewertet werden. Darauf aufbauend wird eine gezielte Entwicklung technischer Lösungen zur Verringerung dieser Störungen angestrebt. Gleichzeitig finden Befragungen und Workshops bei produzierenden Unternehmen statt, um nicht-technische Risiken, wie z. B. die Gefahr einer fehlerhaften Konfiguration von Berechtigungen, zu identifizieren und zu beseitigen.

Erwarteter Impact
Die im Rahmen des Vorhabens erforschten Methoden bilden die Grundlage für eine erhöhte IT-Sicherheit beim Einsatz von 5G im produktionsnahen Umfeld, denn der Schutz von Infrastrukturen vor Cyberangriffen ist und bleibt für Unternehmen und Behörden eine Kernaufgabe, um das öffentliche und gesellschaftliche Miteinander zu gewährleisten. Die wissenschaftlichen Ergebnisse stellen weiterhin die Basis für weiterführende Forschungsvorhaben im Bereich der IT-Sicherheit dar. Es wird erwartet, dass die Forschungsergebnisse und erlangten Kenntnisse in anderen Drittmittelprojekten, beispielsweise Projekten zur industriellen Auftragsforschung für den Mittelstand, angewendet werden und damit unmittelbar einen zusätzlichen Benefit in der industriellen Gemeinschaftsforschung erzeugen bzw. KMU in ihren vielfältigen Herausforderungen unterstützen können.

Um Barrieren für den Einsatz von 5G in Unternehmen zu senken und Sicherheitsbedenken zu begegnen, werden mögliche technische und nicht-technische Faktoren untersucht, die speziell in der Produktion Einfluss auf die IT-Security und Resilienz von 5G-Anwendungen haben.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 0,5 Mio. €

Partner: ATS Elektronik GmbH, Leibniz Universität Hannover

Projektleitung: Dr. Astrid Krage, ATS Elektronik GmbH

Website: Gegenwärtig in Klärung

5G - Sierra

5G-Sierra – Sichere 5G-Infrastrukturen für resiliente Produktionssysteme und -anlagen

Abstract
„5G-Sierra“ ist ein Forschungsprojekt zur Entwicklung von sicheren 5G-Infrastrukturen für resiliente Produkti-onssysteme und -anlagen. Hierbei werden fortschrittliche Technologien wie Industrial-Device-Authentifikation, Anomaliedetektion, Resilienz und Redundanz genutzt, um den störungsfreien Betrieb von Produktionslagern zu gewährleisten. Darüber hinaus bietet „5G-Sierra“ fortschrittliche Funktionen wie Lokalisierung, Process-Monitoring und Remote Maintenance, um Probleme in Echtzeit zu erkennen und schnell zu beheben. Das System soll auch gegen Jamming-Angriffe geschützt werden und betont die Bedeutung von Datensicherheit und Datenschutz.

Motivation
Mit der zunehmenden Digitalisierung der industriellen Produktion entstehen neue komplexe Cyber-Security-Risiken. Zur Erhaltung der Wettbewerbsfähigkeit müssen produzierende Unternehmen die Zuverlässigkeit ihrer Systeme gewährleisten und Sicherheitslücken zielgerichtet schließen.

Vision
Die Vision des „5G-Sierra“-Projekts liegt in der systematischen Absicherung industrieller IoT-Systeme beim gleichzeitigen Einsatz von 5G/6G Kommunikationsstandards.

Zielstellung
Ziel des Projekts ist die Entwicklung von Lösungen zur Prävention, Detektion und Reaktion von Risiken, die dazu beitragen, Standardisierungsansätze und Sicherheitskonzepte zu etablieren.

Angestrebte Ergebnisse
Durch die Behebung von Sicherheitslücken sowie
die Entwicklung von Konzepten und Strategien zur Prävention, Detektion und Reaktion wird Know-how erzeugt, welches einen selbstbestimmteren Umgang mit den Kommunikationsstandards 5G und 6G fördert. Auf diese Weise wird die digitale Souveränität der deutschen Forschung und Industrie gesteigert.

Erwarteter Impact
Die Partner erwarten neben dem Erkenntnisgewinn hinsichtlich Cybersicherheit und digitaler Souveränität den Aufbau umfassender Cyber-Security-Expertise und neuer Lösungskonzepte.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	1,9 Mio. €
Partner:	oculavis GmbH, Utimaco GmbH, Swissbit AG, Rheinisch-Westfälische Technische Hochschule Aachen, Marposs GmbH, Keysight Technologies, Inc., Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung IPT
Projektleitung:	Dr. Markus Große Böckmann, oculavis GmbH
Website:	https://www.ipt.fraunhofer.de/de/projekte/5g-sierra.html

6G-ReS – Sichere und resiliente 5G/6G-Systeme

Abstract
Die Mitarbeitenden im Projekt „6G-ReS“ sind sich bewusst, dass für KRITIS-Anwendungen Vertrauenswürdigkeit und Sicherheit essenziell sind. Durch eine Gesamtsicherheitsarchitektur, Separierung und Mandantentrennung sowie Monitoring werden Daten vor Cyberangriffen geschützt. Die Virtualisierung von Ressourcen ermöglicht eine flexible Nutzung für den Mobilfunk, O-RAN und Edge-Computing.
Es wird auf Confidential-Computing gesetzt, um sensible Daten zusätzlich abzusichern. Das Ziel ist die Schaffung einer sicheren und resilienten Infrastruktur zur Digitalisierung von kritischen Anwendungen.

Motivation
Immer mehr kritische Anwendungen und Infrastrukturen benutzen 5G-Systeme als zugrundeliegende (Kommunikations-)Infrastruktur. Daher ist die Vertrauenswürdigkeit dieser Systeme — und insbesondere auch der zukünftigen 6G-Systeme — von entscheidender Bedeutung für eine erfolgreiche und zuverlässige Digitalisierung. Betrachtet man allerdings den aktuellen Status quo, so hat man es mit einer historisch gewachsenen Gesamtarchitektur zu tun, die nicht unter Berücksichtigung fundamentaler Sicherheitsparadigmen wie etwa „Security-byDesign“ oder „Zero Trust“ entwickelt wurde und insofern viel Verbesserungspotential bezüglich Vertrauenswürdigkeit, Sicherheit und Resilienz besitzt.

Vision
Die Vision des Projektes sind zukünftige 6G-Systeme mit beweisbar garantierter Vertrauenswürdigkeit als inhärente Eigenschaft. Die grundsätzliche Vertrauenswürdigkeit soll auch im Falle einer Integration von möglicherweise nicht-vertrauenswürdigen Komponenten bestehen und so die aktuell existierenden Supply-Chain-Risiken minimieren.

Zielstellung
Ziel ist die Entwicklung und Erprobung von vertrauenswürdigen 5G/6G-Systemen an Hand von ausgewählten Anwendungsfällen mit erhöhter Kritikalität. Die dabei entstehenden Konzepte und Prototypen sollen dabei insbesondere die Umsetzung von Verfügbarkeit und Resilienz adressieren. Im Rahmen dessen sollen zum einen 5G-Minimalfunktionalitäten sowie Sicheheitsgarantien vertrauenswürdiger Virtualisierungsumgebungen als Lösungsfundamente untersucht werden, insbesondere um eine sichere Integration nicht-vertrauenswürdiger Komponenten zu ermöglichen.

Angestrebte Ergebnisse
Als Ergebnisse der Projektdurchführung sollen Sicherheits- und Resilienz-Konzepte entstehen, die die oben beschriebene Zielstellung umsetzen. Darüber hinaus sollen mit Hilfe von Proof-of-Concept-Implementierungen ausgewählte Konzepte an spezifischen Anwendungsfällen erprobt werden. Dabei sollen standortübergreifende 5G-Testbeds als ein Fundament dienen. Ausgewählte Lösungsbausteine sollen zudem als Open Source zur Verfügung gestellt werden.

Erwarteter Impact
Im Rahmen der Entwicklungen sollen Lösungen entstehen, die spezifische Bedürfnisse von Anbietern und Anwender adressieren. Dazu gehört unter anderem die Entwicklung von Resilienz-Konzepten, welche providerübergreifend einen sicheren Wiederanlauf des Netzes in Krisensituationen ermöglichen. Darüber hinaus sollen Lösungen entstehen, die das Supply-Chain-Risk-Problem adressieren und so Flexibilität bei der Komponentenauswahl zurückgewinnen. Die vorgeschlagenen Konzepte sollen insgesamt einen verlässlichen und beherrschbaren Betrieb von 5G-Systemen ermöglichen und dabei gleichzeitig die Umsetzung von Diensten mit besonders hohen Sicherheitsanforderungen erlauben. Darüber hinaus wird erwartet, dass einige der entwickelten Lösungsbausteine — beispielsweise im Bereich sicherer Virtualisierungsumgebungen — auch in andere Bereiche wie beispielsweise Edge Computing oder e-Health transferiert werden können. Das Projekt strebt ferner eine aktive Beteiligung an Standardisierungsaktivitäten bezüglich der O-RAN ALLIANCE und ETSI an.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	2,5 Mio. €
Partner:	secunet Security Networks AG, Vodafone GmbH, Scontain GmbH, Barkhausen Institut gGmbH, Friedrich-Alexander-Universität Erlangen-Nürnberg
Assoziierter Partner:	Technische Universität Ilmenau
Projektleitung:	Elisabeth Rieger, secunet Security Networks AG
Website:	www.6g-res.de

ADWISOR5G

ADWISOR5G - Ein verteilter drahtloser Schutzschirm für private 5G-Netze

Motivation
Ein Ziel der Bemühungen rund um die 5G-Technologie ist die Verteilung und Diversifizierung der einzelnen Netzkomponenten eines (privaten) 5G-Netzes. Der Schwerpunkt wird dabei auf Anwendungen in der Industrie 4.0 und dem Internet der Dinge liegen.

5G- und perspektivisch 6G-Netze werden damit in Zukunft wichtige Teile kritischer Infrastrukturen sein. Die Komponenten, aus denen diese Netze aufgebaut werden, sind dabei sehr komplex. Dies macht sie wenig vertrauenswürdig. Im Besonderen gilt dies für 5G-Modems als zentrale Komponenten. Diese zeichnen sich durch eine sehr hohe Komplexität aus, bedingt u. a. durch die Verwendung vollständiger SoCs, closed-source Hard- und Softwarekomponenten, HW-Offloading bestimmter Funktionen, aber auch durch die Notwendigkeit der Kompatibilität zu alten Mobilfunkstandards.

Vision
Wir entwickeln in ADWISOR5G einen verteilten Schutzschirm, der physikalische Angriffe auf private 5G-Netze erkennt, ortet und abwehrt. Das Gesamtsystem bestehend aus Hardware und Software setzt Zero Trust für die 5G-Luftschnittstelle um.

Zielstellung
Das Ziel des Verbundprojektes ADWISOR5G ist die Entwicklung eines verteilten Schutzschilds zum Schutz privater 5G-Netzwerke. Ein Spectral Intrusion Detection (SID) dient der autonomen Erkennung von Funkpaketen und verdächtigen Störungen auf physikalischer Ebene. Mit Hilfe mehrerer Software-defined Radios (SDRs), angeordnet als verteilte Gruppenantenne, soll eine ständige Überwachung des Spektrums gewährleistet werden, um Störungen lokalisieren und entfernen zu können. Eine sichere Lokalisation erfordert eine genaue Synchronizität der verteilten SDRs. Die von Fraunhofer IIS entwickelte Funktechnologie UWIN bietet hier eine einzigartige Ultra-Reliable Low Latency Communication (URLLC) Plattform. Die Kennzahlen der Technologie, wie eine Fehlerrate kleiner als 10 hoch -8 bei Latenzen kleiner als 125 µs, ermöglichen sowohl die zeitliche Synchronisierung als auch die echtzeitfähige Übertragung der detektierten Angriffe zu einem zentralen Knoten. Um der Herausforderung gerecht zu werden, die Komplexität von 5G-Netzkomponenten zu senken, ist ein sogenanntes Hardware Abstraction Layer (HAL) hilfreich. Diese Schicht abstrahiert bestimmte Hardwareschnittstellen von der darüber laufenden Software ab und macht es so möglich, bestimmte Teile der Software ohne Modifikation auf andere bzw. neuere Hardwareplattformen zu portieren und gleichzeitig zu isolieren. Damit kann sie einen wertvollen Beitrag dazu liefern, die Softwareentwicklungsprozesse, Kosten und Sicherheit von 5G/6G-Komponenten erheblich zu beschleunigen. Schließlich wollen wir einen prototypischen Demonstrator, bestehend aus Hard- und Software, im Feld validieren.

Angestrebte Ergebnisse
Ziel ist die Entwicklung eines Gesamtsystems, welches Angriffe auf der Luftschnittstelle erkennt, ortet und abwehrt. Dazu werden vernetzte Sensoren entwickelt, welche Daten sammeln, die dann dazu dienen, das Netz zu analysieren. Des Weiteren ist es Ziel, Modelle und Trainingsdaten für typische Störer und Angreifer, wie intelligente, mobile Jammer zu erstellen. Diese dienen dann zur Lokalisierung und Abwehr von Störern. Ein praktischer Vorschlag zur Abstraktion unterschiedlicher Hardware-Schnittstellen soll erheblich zur Reduktion von Komplexität solcher Systeme beitragen.

Erwarteter Impact
Erschließung neuer Kunden- und Forschungsprojekte. Positionierung als starker nationaler bzw. innereuropäischer Anbieter von sicheren und kosteneffizienten 5G/6G-Infrastrukturkomponenten, hergestellt in Deutschland und basierend auf deutschem Know-how. Dies stärkt direkt die digitale Souveränität Deutschlands, wobei wir unseren Kunden die Wahl geben, auf außer-europäische Wettbewerber zu verzichten und damit auch erhöhten Sicherheitsanforderungen gerecht zu werden. Die Projektergebnisse werden als begutachtete Artikel international publiziert, um wertvolle Rückmeldungen aus der Wissenschaft zu erhalten. Insbesondere die Veröffentlichung der Trainingsdaten verspricht einen hohen wissenschaftlichen Nutzen, da dieser von anderen Forschern für das Training eigener KI-Systeme genutzt werden kann.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 1,7 Mio. €

Partner: albis-elcon system Germany GmbH, Fraunhofer-Institut für Integrierte Schaltungen (IIS), Hochschule Darmstadt

Projektleitung: Dr. Tim Lackorzynski, albis-elcon system Germany GmbH, Hochschule Darmstadt

Website: adwisor5g.albis-elcon.com

Cobra5G

COBRA-5G - Container-basierte resiliente Architektur für 5G-Campus-Netzwerke

Motivation

5G-Campusnetzlösungen sind ein aufstrebendes und zunehmend wichtiges Marktsegment für den Wirtschaftsstandort Deutschland, insbesondere durch den damit einhergehenden Digitalisierungsprozess in deutschen Schlüsselindustrien. Die zunehmende Komplexität von sicherheitskritischen 5G-Netzen stellt Administratoren vor neue Herausforderungen: Sie müssen nicht nur verstärkt unvorhersehbare Störfälle und Angriffe auf das System entdecken, sondern auch zeitnah auf diese reagieren. Unterschieden werden muss hierbei zwischen logischen Cyberangriffen, die zu einer Störung der eingesetzten Software führen, und physikalischen Angriffen, bei denen durch die bewusste oder unbewusste Aussendung von Störsignalen die Kommunikation von Endgeräten erschwert oder sogar verhindert wird.

Vision

Durch neue Standards wie Open-RAN ist es möglich, dass Komponenten verschiedener Provider im gleichen Netzwerk integriert sind und über vordefinierte Schnittstellen miteinander kooperieren. Weiterhin sind Netzwerkfunktionalitäten entweder in virtuellen Maschinen virtualisiert oder in Containern orchestriert und über das Netzwerk hinweg ausgerollt. Dieser Entwicklung folgend ist es notwendig, einen höheren Fokus auf die zertifizierbare IT-Sicherheit zu legen. Im Rahmen von COBRA-5G wird das Konsortium ein Ende-zu-Ende-Gesamtsystem aufbauen – Made in Germany!

Zielstellung

In diesem Projekt soll die Grundlage gelegt werden, Systemangriffe jeder Art zu erkennen. Die angestrebten Lösungen der Partner im Projekt sind auf verschiedenen Ebenen angesiedelt: von der Absicherung des virtualisierenden 5G-Servers über die Steigerung der Fehlertoleranz der Orchestrierung bis zur dezentralen Detektion von Störausfällen und Angriffen auf die Infrastruktur sowie Durchführung von Gegenmaßnahmen auf dem Gesamtsystem, um die Minimalfunktionen des Netzwerkes zu gewährleisten.

Angestrebte Ergebnisse
Es wird eine vollständige resiliente 5G-Campuslösung realisiert, deren Teilergebnisse von allen Partnern in der Verwertung nutzbar sind und neue Marktperspektiven eröffnen können. Das im Kontext von COBRA-5G ausgebaute Reallabor wird ebenfalls für zukünftige Projekte verwendet werden - der Nutzen erstreckt sich über eine Vielzahl von zukunftsrelevanten Themen, u. a. die autonome Mobilität und Smart Cities mit all ihren Herausforderungen. Die enge Kooperation mit Industriepartnern für den Nutzen und weiteren Ausbau dieser Infrastruktur (wie in COBRA-5G) ist von äußerster Wichtigkeit.

Erwarteter Impact
Das Projekt trägt zum Wissensaufbau und -transfer in den Bereichen Cybersecurity und digitaler Souveränität bei. Außerdem steigert es die allgemeine IT-Sicherheit von 5G/6G-Infrastrukturen und unterstützt den Ausbau der digitalen Souveränität Deutschlands. Sichere und robuste 5G-Infrastrukturen sind ein wichtiger Baustein, um neue Märkte, Kunden und Forschungsprojekte zu erschließen. Die Weiterentwicklung und der Ausbau von 5G-Campusnetzen sichert und schafft zukunftsträchtige Arbeitsplätze am Standort Deutschland.

Projektlaufzeit: 01.06.2023 - 30.11.2024

Fördersumme: 2,3 Mio. €

Partner: albis-elcon system Germany GmbH, GT-ARC gemeinnützige GmbH, HMF Smart Solutions GmbH, Technische Universität Berlin

Projektleitung: Dr. Amina Ayadi-Mießen, HMF Smart Solutions GmbH

Website: https://cobra-5g.de/

DeSiRe-NG
DEpendable and Secure Infrastructure for Resilient Next Generation Networks

DeSiRe-NG - DEpendable and Secure Infrastructure for Resilient Next Generation Networks

Motivation
Die Erfahrungen im Kontext von 5G-Kommunikation zeigen, dass Anwendungsunternehmen derzeit noch eine starke Zurückhaltung hinsichtlich des Einsatzes von 5G-Campusnetzen aufweisen. Die Beweggründe liegen insbesondere in der Unklarheit über deren Resilienz und Zuverlässigkeit im Produktivbetrieb.

Vision
In diesem Projekt werden Werkzeuge und Methoden entwickelt, mit denen die Leistungscharakteristik erfasst, mögliche Störungen erkannt und dadurch vermieden werden können; ebenso kann die Resilienz im eigenen 5G-Netz durch Emulation untersucht werden, um diese zu erhöhen. DeSiRe-NG hat darüber hinaus das Bestreben, die Ergebnisse auf die nächste Generation der Funktechnologien übertragbar zu entwickeln.

Zielstellung
Zielsetzung des Projektes DeSiRe-NG ist es Werkzeuge (Mess-Framework, QoS-Explorer, Digitaler Zwilling, Toolbox und Emulation) zu entwickeln, um die agile Anwendungsentwicklung in 5G- und beyond 5G-Netzen mit höherer Resilienz gegenüber Störungen und Non-Performance zu unterstützen. Dazu werden Anwendungen bzw. deren Kommunikation gezielt auf deren Resilienz hin untersucht und in kontrollierter Umgebung auf Performance und Widerstandskraft - unter verschiedensten Einflussfaktoren - modelliert und gemessen. Der Mehrwert dieser Herangehensweise ist die vereinfachte und verbesserte Entwicklung resilienter und effizienter Kommunikationsstrukturen und Anwendungen. Anhand eines relevanten Anwendungsfalls sollen die Projektrgebnisse evaluiert werden.

Angestrebte Ergebnisse

In Zusammenarbeit mit den Projektpartnern werden ein Messsystem für 5G-Campusnetze und eine Störungsemulation konzipiert und entwickelt. Die so zu sammelnden Daten werden in einem operationalen Digitalen Zwilling gespeichert, aufbereitet und umgerechnet in statistische Größen, die einer zu entwickelnden Toolbox zugeführt werden. Diese Toolbox erlaubt die Nachbildung der 5G-Netzwerkcharakteristika, um künftige Applikationen unter diesen zu testen und agil hinsichtlich der Resilienz entwickeln zu können. Die DiSiRe-NG-Infrastruktur ermöglicht es außerdem, im laufenden Betrieb Störungen zu erkennen, die Ursachen zu untersuchen und Kompensationen einzuleiten.

Erwarteter Impact

Das hohe Marktpotential der industriellen Anwendung neuer Funktechnologien liefert die Basis für das Verwertungspotential von DeSiRe-NG, das - insbesondere für den Mittelstand und KMU - einen wichtigen Beitrag zur Beherrschbarkeit der 5G-Technologie leistet. Die Projektergebnisse fließen in Lehrveranstaltungen an den beteiligten Hochschulen ein und werden in akademischen Publikationen und Forschungsbeiträgen verbreitet und durch Bachelor-, Master- und Promotionsarbeiten weiter vertieft. Aus den Projektergebnissen sollen komerzielle Beratungsdienstleistungen für KMUs und Industrie sowie Produktpotential für resiliente 5G-Lösungen abgeleitet werden. Die Projektergebnisse sollen sowohl regional als auch überregional in Richtung anderer Transfereinrichtungen und 5G-Netz-Anwendern (insbesondere KMUs) verbreitet werden.

Projektlaufzeit:	01.06.2023 - 30.11.2024
Fördersumme:	1,4 Mio. €
Partner:	NUROMEDIA GmbH, Technische Universität Ilmenau, Technische Hochschule Ostwestfalen-Lippe, Lufthansa Industry Solutions AS GmbH, InnoZentOWL e.V.
Projektleitung:	Lukas Dalhoff, InnoZent OWL Konsortialführung: Christian Tismer, NUROMEDIA GmbH
Website:	https://desire-ng.net/

EMiL – „Echtzeitfähige Machine-Learning“- Lösungen für resiliente und sichere 5G/6G-Netze am Beispiel von Automatisierungsanwendungen

Abstract
„EMiL“ ist eine neueologie, die das Potential hat, das Mobilfunknetz der Zukunft zu revolutionieren. In Zeiten von Industrie 4.0 und Automatisierungen wird die Bedeutung von stabilen und sicheren Netzwerken immer größer. Doch was passiert, wenn es zu Netzstörungen kommt? Hier kommt Machine Learning ins Spiel! „EMiL“ ermöglicht die Echtzeit-Bewertung von Störungen im Netzwerk und gibt Empfehlungen, um diese schnell und effektiv zu beheben. Damit wird eine zuverlässige Netzwerkleistung gewährleistet, die gerade für kritische Anwendungen wie Internet-of-Things von entscheidender Bedeutung ist.

Motivation
Die Angriffe auf die kritische Infrastruktur steigen weltweit stark an. Der wachsende Datenverkehr über Mobilfunknetze führt dazu, dass auch hier die Angriffe zukünftig häufiger werden.

Vision
Angriffe auf Mobilfunknetze sollen zukünftig mittels Machine Learning (ML) zuverlässig erkannt werden. Mit Hilfe von ML wird dabei rechtzeitig auf alternative Mobilfunkressourcen in ungestörten Frequenzbändern ausgewichen.

Zielstellung
Um die IT-Sicherheit und Resilienz von 5G/6G-Netzen zu verbessern, werden im Projekt geeignete Methoden des maschinellen Lernens zur Erkennung und Vorhersage von Störungen, deren Klassifizierung und dem Einleiten von Gegenmaßnahmen untersucht und prototypisch umgesetzt.

Angestrebte Ergebnisse
Es werden Algorithmen für lokale und verteilte
Angriffserkennung mittels Machine Learning (ML) auf Edge-Servern/-Devices und ein hierarchischen Steuerungs- und Reporting-System im 5G/6G-Core entwickelt.

Erwarteter Impact
Mit dem Roll-out der 5G-Netze ist eine stärkere Nutzung von Mobilfunknetzen für IOT-Anwendungen zu beobachten. Eine Absicherung gegen Angriffe wird die Nutzung von 5G-Netzen für viele zusätzliche Anwendungen ermöglichen.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 1,5 Mio. €

Partner: Exelonix GmbH, Merantix Labs GmbH (Merantix Momentum), IHP GmbH – Innovations for High Performance Microelectronics/ Leibniz-Institut für innovative Mikroelektronik

Projektleitung: Dr. Matthias Stege, Exelonix GmbH

Website: https://www.merantix-momentum.com/casestudy/emil#chal

FlexShield - Resiliente 5G-Vernetzung für industrielle Echtzeitanwendungen

Motivation
Sichere 5G-basierte Innovationen in der Industrie 4.0 sind von entscheidender Bedeutung für die Digitalisierungsstrategie Deutschlands. Sie stärken die digitale Souveränität des Landes und ermöglichen eine führende Rolle als Technologieanbieter im globalen 5G/6G-Wettbewerb. Derzeit ist der Einsatz fahrerloser Transportsysteme in logistischen Prozessen auf vordefinierte Trajektorien beschränkt. Die Teleoperation als Handover-Technologie zur Übernahme von kritischen Tätigkeiten durch einen Teleoperationsagenten verspricht eine vielversprechende Weiterentwicklung, bringt jedoch verschiedene Herausforderungen mit sich.

Durch einen Teleoperator könnten verschiedene Fahrzeuge wie LKWs, Gabelstapler oder andere Flurförderfahrzeuge von einer einzigen Person gesteuert werden. Während die Teleoperation Logistikmitarbeiter dementsprechend entlastet und gleichermaßen das Unfallrisiko verringert, birgt diese auch Herausforderungen, denn der Einsatz teleoperierter Transportsysteme unterliegt einer angriffs- und dienstqualitätsanfälligen Mobilfunkinfrastruktur.

Vision
Standardisierte 5G-Campus-Systeme bieten im Grundsatz eine für teleoperierte Transportsystem ideale Infrastruktur. Im Rahmen von FlexShield sollen die Risiken für den Einsatz dieser modernen Netztechnologien geprüft und minimiert werden.

Zielstellung
In diesem Projekt werden Resilienzinnovationen erforscht und demonstriert, die die 5G-basierte kontinuierliche Diensterbringung für kritische Industrieanwendungen stärken sollen. Im Kern dieser Innovationen liegen vier Konzepte: die Redundanz von 3,7 GHz und 26 GHz 5G Radiosystemen, die Erprobung von 5G-Relais-Drohnen, der Einsatz echtzeitfähiger, programmierbarer Time-Sensitive Networking-Übertragungsmechanismen und letztendlich der Einsatz von Hardware-basierter Authentifizierung und Mechanismen der Softwareintegritätsüberprüfung zur Laufzeit. Das Resultat ist eine Ausschöpfung der Effizienz entlang der Wertschöpfungskette durch die Kombination von Automatisierung und Teleoperation für komplexe Tätigkeiten in Logistikprozessen.

Angestrebte Ergebnisse
Das Resultat des Vorhabens ist eine Steigerung der Effizienz entlang der Wertschöpfungskette durch die Kombination von Automatisierung und Teleoperation für komplexe Tätigkeiten in Logistikprozessen. Eines der Ziele besteht darin, den gesamten Prozess mittels 5G zu optimieren, wodurch manuelle Arbeitsschritte zwischen Lagerung, Beladung und Entladung entfallen.

Kompetenzen im Bereich der Planung, des Aufbaus und der Optimierung von resilienten 5G-Campusnetzen werden verbessert, um diese an Industriestandorten in Deutschland auch für andere Branchen zur Verfügung stellen zu können. Ein besonderer Fokus liegt dabei auf der resilienten Architektur des Netzwerks, um Campusnetze noch besser in der Industrie einzusetzen.

Die Ergebnisse des Vorhabens werden auf verschiedenen Ebenen genutzt. Es werden Arbeits- und Prozessabläufe unter Berücksichtigung des resilienten 5G-Netzes und der Teleoperationsplattform optimiert. Dabei werden modifizierte Prozessabläufe an die Arbeits- und Infrastrukturbedingungen angepasst. Des Weiteren ist die langfristige Schaffung neuer Arbeitsprofile geplant, die im Zusammenhang mit mobiler Robotik, Teleoperation von Fahrzeugen und Robotern stehen. Dadurch sollen langfristig höherwertige Arbeitstätigkeiten in den Fokus gerückt und Tätigkeitsfelder in der Logistik attraktiver gestaltet werden.

Erwarteter Impact
Die gesammelten Erkenntnisse und Erfahrungen des 5G-Netzes werden genutzt, um weitere Forschungsaktivitäten der nächsten Generation mit flexibler Integration heterogener Technologien in 5G-Netzen zu initiieren.

Projektlaufzeit:	01.06.2023 - 30.11.2024
Fördersumme:	1,9 Mio. €
Partner:	TRIOPT GmbH, Universität Duisburg-Essen, VCK Logistics SCS GmbH, V-Tron GmbH
Projektleitung:	Jonas Piepke, TRIOPT GmbH
Website:	Gegenwärtig in Klärung

medCS.5 – Cyber-Sicherheit für den Austausch medizinischer Daten: 5G-Campusnetz für klinische und eHealth-Anwendungen

Abstract
Das Projekt „medCS.5“ setzt neue Maßstäbe in puncto Datenaustausch von medizinischen Daten: Durch die Verwendung von 5G und LiFi in einem speziellen Campusnetzwerk wird höchste Datensicherheit und Geschwindigkeit gewährleistet. Die Simulation von Sicherheitsbedrohungen ermöglicht eine ständige Verbesserung des Systems. Auch die Patientendatensicherheit wird durch Quantum-Key-Distribution (QKD) gewährleistet. Durch die Analyse von Verkehrsdaten können Behandlungsprozesse optimiert werden und die Resilienz des Systems steht jederzeit im Vordergrund.

Motivation
Neue Kommunikationstechnologien wie 5G/6G werden in der Versorgungswirklichkeit eine zunehmend größere Rolle spielen: bedingt sowohl durch moderne Diagnose- und Behandlungsverfahren als auch das mobile Patientenmonitoring. Damit ergeben sich aber auch große Herausforderungen an die Resilienz der Infrastruktur sowie an die Datensicherheit, vor allem für die sensibelsten Daten: gesundheitsbezogene Informationen des einzelnen Menschen. Gerade dafür muss eine hinreichend geschützte Verarbeitung sichergestellt werden.

Vision
Ein sicheres und zuverlässiges IoT-Netzwerk im Dienst des Patienten. Dabei ermöglicht die 5G-LiFi-Netzwerkinfrastruktur die Einbeziehung aller relevanten Datenquellen entlang der Behandlungsstationen eines Patienten in einem Krankenhaus. Dadurch verbessert sich auch die Patientenversorgung, -sicherheit und -erfahrung.

Zielstellung
Das Ziel des Projektes „medCS.5“ ist die Patientendatensicherheit und Resilienz von 5G-Infrastrukturen im medizinischen Bereich zu analysieren, Bedrohungspotenziale zu identifizieren und daraus abgeleitet Empfehlungen für Sicherheit, Design und Betrieb solcher Netze zu formulieren. Dazu werden verschiedene komplementäre Methoden, innovative Technologien sowie neuartige Algorithmen und Tests entwickelt, validiert und eingesetzt. Darüber hinaus wird gezeigt, wie die Resilienz des Netzes durch ergänzende neue Technologien und Entwicklungen weiter gestärkt werden kann.

Angestrebte Ergebnisse
Der Anforderungskatalog für einen sicheren Datenaustausch in klinischen Campusnetzwerken entlang des Patientenpfades soll erstellt werden. Hinzu kommt die Entwicklung einer Software zur simulativen Resilienzbewertung von Netzwerken im Klinik- und Praxisbereich. Ferner werden selbstlernende Methoden zur Erfassung von Anomalien und Angriffen in 5G – und Cloudsystemen konzipiert. Die Integration von Li-Fi-Technologien zur Versorgung kritischer Bereiche und Verhinderung von Angriffen auf die Funkinfrastruktur (Jamming) sowie die Sicherung der 5G-Edge-Cloud-Lösung durch Quantenschlüsselverteilung und diverse Integrationstests von Algorithmen, Simulationen und Technologien in einer 5G-Testumgebung von medizinischen Einrichtungen werden als Ergebnis angestrebt.

Erwarteter Impact
Das Projekt „medCS.5“ soll über verschiedene komplementäre Methoden, Technologien, Algorithmen und Tests die Datensicherheit und Resilienz von 5G-Infrastrukturen im medizinischen Bereich analysieren und daraus abgeleitet Empfehlungen für Design und Betrieb solcher Netze formulieren. Dabei wird die Patientendatensicherheit in medizinischen Campusnetzwerken durch neuartige KI-basierte Überwachungsalgorithmen und Quantenverschlüsselungen gesteigert und neue Anwendungsbereiche für Technologien wie LiFi im eHealth-Bereich erschlossen. Darüber hinaus stellen die simulative Resilienzbewertung von medizinischen Campusnetzwerken und die damit verbundenen Fortschritte in Wissenschaft und Technik einen zentralen Schritt in der Entwicklung smarter Krankenhäuser in Deutschland dar. In diesem Zusammenhang verbessert sich nicht nur die Sicherheit der patientenbezogenen Daten in medizinischen genutzten 5G-Netzwerken, sondern auch die Sicherheit, Versorgungsqualität und Erfahrung der Patienten selbst.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 2,1 Mio. €

Partner: ITPower Solutions GmbH , Fraunhofer Heinrich-Hertz-Institut (HHI), Brandenburgische Technische Universität Cottbus-Senftenberg (BTU)

Projektleitung: Sadegh Sadeghipour, ITPower Solutions GmbH

Website: www.hhi.fraunhofer.de/abteilungen/pn/projekte/med.html

MNT-Pro - Mobile Network Protector

Abstract
Sichere und resiliente Mobilfunknetze der Zukunft, das ist das Ziel von „MNT-Pro“. Es wird mit innovativen Ansätzen gearbeitet, um 5G- und 6G-Netze vor DDoS-Attacken und Störsignalen wie Jamming zu schützen. Dabei wird ein umfassendes Security-Framework entwickelt, dass die Sicherheit der Netze auf allen Ebenen gewährleistet. Besonders wichtig ist dabei die Resilienz des Netzes. Die Entwickler/innen setzen auf fortschrittliche Technologien wie Künstliche Intelligenz (KI) und Maschinelles Lernen (ML), um das Netzwerk zu optimieren und das Risiko von Angriffen zu minimieren.

Motivation
Durch die zunehmende Digitalisierung und Vernetzung stehen in Mobilfunknetzen neue Möglichkeiten des Informationsaustauschs zur Verfügung. Der Einsatz neuer Kommunikationstechnologien birgt Risiken. Diese Risiken werden durch Analyse und Bewertung, die der Mobile-Network-Protector ermöglicht, minimiert.

Vision
Eine ganzheitliche Lösung, die verschiedenste Techniken beherrscht und flexibel erweiterbar ist, schafft Sicherheit sowohl in Industrie und Unternehmen als auch für Privatnutzer.

Zielstellung
Es wird ein System entwickelt, das Betreibern den sicheren Betrieb von 5G- und 6G-Mobilfunknetzen ermöglicht. Dies wird zum einen dadurch realisiert, dass die Kommunikation im Netz an entscheidenden Punkten analysiert und Schwachstellen sichtbar gemacht werden.

Angestrebte Ergebnisse
Ein Demonstrator zur Analyse und Bewertung der Netzsicherheit eines 5G-Mobilfunknetzes.

Erwarteter Impact
Die Schaffung der Grundlagen für ein Sicherheitsanalyse-Systems und die Befähigung zur Weiterentwicklung und Verbreitung.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 1,4 Mio. €

Partner: ipoque GmbH, TU Chemnitz

Projektleitung: Tim-Oliver Kittel, ipoque GmbH - A Rohde & Schwarz Company

Website: www.mobile-network-protection.de

PHYSICS – Sicherheit durch Innovationen im Physical Layer (PHY-Security Innovations for Communication Systems)

Abstract
Die Zukunft der Kommunikationstechnologie hängt von Innovationen im Physical Layer ab. „PHYSICS“ konzentriert sich auf die Entwicklung von PHY-Security-Innovations für Kommunikationssysteme. Durch die Verwendung von Li-Fi und Optical-Wireless können Angriffe minimiert werden. Der Channel-Estimation-Prozess macht es möglich, System zu vernetzen und autonome Fahrzeuge zu steuern. Die Forschung ist der Schlüssel zu einer sicheren Zukunft der drahtlosen Kommunikation.

Motivation
Kommunikationsnetze werden durch mehr Geräte
immer dichter und heterogener, integrieren immer mehr Funktionen wie Kommunikation, Lokalisierung, Sensing und Verarbeitung/AI miteinander und operieren in immer höheren Frequenzbereichen (mmWave, THz). Dies stellt besonders bei den Anwendungen im Verkehr zum vernetzten und autonomen Fahren mit hohen Gefahrenpotential neue Anforderungen an die verschiedene Schutzziele wie Vertraulichkeit, Integrität, Authentizität und Resilienz von Kommunikationssystemen.

Vision
Kommunikationsnetze für autonomes Fahren weisen ein hohes Maß an Sicherheit und Resilienz auf, Angriffe werden frühzeitig möglicherweise vor dem Schadenseintritt auf Ebene des Physical Layer (PHY) erkannt und Gegenmaßnahmen werden nahtlos ohne Verlust der Kommunikationsqualität eingeleitet.

Zielstellung
Ziel ist die Erforschung und Entwicklung von neuartigen und integrierten Erkennungs-, Abschwächungs-, und Kompensationsstrategien bei Angriffen auf den PHY von Kommunikationsnetzen, insbesondere im Kontext des sicherheitskritischen Vernetzten und Autonomen Fahrens. Die Erkennung erfolgt dabei durch eine Analyse des Ausbreitungskanals und die Kanalschätzung von verschiedenen Parametern sowie durch Verfahren des Machine Learnings (ML) zur Klassifikation der Angriffsvektoren.

Angestrebte Ergebnisse
Es wird angestrebt einen Demonstrator mit verschiedenen Angriffsvektoren auf den PHY bei einer V2X-Kommunikation aufzubauen, mit dem es möglich ist, die Art des Angriffs zu erkennen und durch die Klassifizierung eine geeignete Auswahl zu treffen und geeigneten Gegenmaßnahmen einzuleiten.

Erwarteter Impact
Die entwickelten Sicherheitslösungen sollen zur Erzeugung von redundanten Kommunikationsnetzen beitragen. Für den Einsatz in dynamischen Szenarien mit hohen Anforderungen an die Sicherheit werden dazu optischer Frontends entwickelt. Durch passgenaue Einsatzszenarien künftiger Kommunikationsnetze in Bereich autonomes Fahren sollen künftige Potenziale in verschiedenen Bereichen von Verkehr, Logistik und Industrie erschlossen werden. Es werden neuartige wissenschaftliche Erkennungsverfahren von Angreifern auf den PHY durch Kanalschätzung und ML-Methoden erwartet. Die Projektergebnisse dienen als Knowledge-Base für den erleichterten Wissens und Technologietransfer.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 1,3 Mio. €

Partner: RKW Sachsen e. V. (RKW), aeroLiFi GmbH (ALF), Dresden Elektronik Ingenieurtechnik (DDE) GmbH, Technische Universität Dresden (TUD)

Projektleitung: Steffen Mehner, RKW Sachsen e. V. (RKW)

Website: www.physics-5g.com

QSyncNextG - Quantum Synchronisation for Resilient and Secure Next Generation (5G/6G) Campus Networks

Motivation
Kommunikationsnetze stellen eine strategische Infrastruktur für den Datenaustausch, insbesondere für die intelligente Industrie der Zukunft dar. Für moderne Kommunikationsnetze und die dahinterstehenden Anwendungen ist die Verfügbarkeit und Sicherheit der Netzsynchronisation ein kritischer Faktor mit sehr hohen und permanent zunehmenden Anforderungen an die Genauigkeit. Ein Fehler in der Synchronisation innerhalb der Netze kann schnell zu Funktionseinschränkungen bzw. zum Netzausfall führen. Aus diesem Grund ist es von entscheidender Bedeutung, die Synchronisation zwischen Netzkomponenten und auch deren Verfügbarkeit für Anwendungen sicher zu stellen und vor Ausfall und Manipulation zu schützen.

Vision
Die Nutzung von Quantenphänomenen haben das Potenzial, eine wesentlich sicherere und effektivere Synchronisation zu ermöglichen. In diesem Zusammenhang zielt QSyncNextG darauf ab, eine sichere und widerstandsfähige 5G/6G-Netzwerksynchronisierung mit beispielloser Präzision zu entwickeln und zu realisieren, indem es Quantentechnologien für eine sichere, belastbare und präzise Netzwerksynchronisation einsetzt.

Zielstellung
QSyncNextG zielt darauf ab, eine Netzzeitsynchronisationspräzision zu erreichen, die über die Leistung klassischer (Nicht-Quanten) Ansätze hinausgeht. Diese neuartigen, auf Quantentechnologien basierenden Lösungen werden in einem End-to-End-Demonstrator in das 5G/6G Radio Access Network und Mobile Edge Computing integriert. QSyncNextG wird die nationalen Betreiber- und Anbieter-Ökosysteme für fortschrittliche Netzwerktechnologien im Kontext der IT-Sicherheit stärken, indem es Quantentechnologien für eine sichere, belastbare und genaue Netzwerksynchronisation nutzt.

Angestrebte Ergebnisse
Verschiedene Verwertungsmöglichkeiten sind für die Forschungsergebnisse geplant. Diese umfassen die gesamte Wertschöpfungskette für die Quantensynchronisation: von der Photonenpaarquelle über Detektionseinheiten und Synchronisationsprotokolle bis hin zum Aufbau von entsprechenden Dienstleistungs- und Serviceangeboten. Perspektivisch kann auch der Aufbau eines Lizenzgeschäfts aussichtsreich sein. Den direkt am Projekt beteiligten Mitarbeitenden werden neue Möglichkeiten zur wissenschaftlichen Qualifizierung und Weiterbildung geboten. Die Einführung der Projektergebnisse in die Lehre wird eine qualitative Verbesserung und einen größeren Praxisbezug bewirken. Zur Verbreitung der Forschungsergebnisse werden Publikationen in renommierten Fachzeitschriften und auf Konferenzen veröffentlicht.

Erwarteter Impact
QSyncNextG wird die nationalen Betreiber- und Anbieterökosysteme für fortschrittliche Netzwerktechnologien im Kontext der IT-Sicherheit stärken, indem es Quantentechnologien für eine sichere, belastbare und präzise Netzwerksynchronisation einsetzt. Hierduch werden die Markteintrittsschranken für moderne Quantennetztechnologien für Sicherheit und Ausfallsicherheit gesenkt. Die Bereitstellung von Quantensicherheit für zukünftige 6G-Industrieszenarien wird die digitale Souveränität Deutschlands, der EU und ihrer Industrie in hohem Maße erhöhen. Um die Möglichkeiten für eine spätere Nutzung und die überprüfbare Sicherheit zu erhöhen, wird auch Open-Source-Software verwendet.

Projektlaufzeit: 01.07.2023 - 30.11.2024

Fördersumme: 1,7 Mio. €

Partner: albis-elcon system Germany GmbH, Quantum Optics Jena GmbH, Technische Universität Dresden

Projektleitung: Ronald Marc Dietrich, albis-elcon system Germany GmbH

Website: qsyncnextg.de

RIOT - Resiliente IoT – Hochverfügbare Infrastruktur für kritische IoT-Anwendungen

Abstract
„RIOT“ (Resiliente IoT) ist ein Projekt, das sich auf die Schaffung einer hochverfügbaren Infrastruktur für kritische IoT-Anwendungen konzentriert. Das Ziel ist eine intelligente und sichere IoT-Konnektivität für kritische Infrastrukturen zu gewährleisten und smarte IoT-Dienste zu implementieren. Mit dem Fokus auf Robustheit, Sicherheit und Verfügbarkeit wird „RIOT“ die Nachhaltigkeit und Zuverlässigkeit von IoT-Anwendungen deutlich verbessern können. Die Entwickler/innen von „RIOT“ nutzen moderne Technologien wie Blockchain und künstliche Intelligenz (KI), um solide IoT-Dienste zu schaffen, die den betrieblichen Anforderungen entsprechen.

Motivation
Neben dem Bereich Smart-Home-Automation werden IoT-Anwendungen zunehmend auch bei der Grundversorgung und der Verkehrsinfrastruktur sowie im Klima- und Katastrophenschutz eingesetzt. Die für die Umsetzung von IoT-Diensten notwendigen Geräte und Sensoren werden hierbei oftmals drahtlos, z. B. über LPWAN- (Low Power Wide Area Networks) oder Mobilfunknetze an das Internet bzw. eine Cloudplattform angebunden. Im gleichen Maße steigt mit dem Ausbau IoT-unterstützter Applikationen die technische, gesellschaftliche und ökonomische Abhängigkeit von diesen Diensten. Fällt die Kommunikationsinfrastruktur wegen Angriffen, Katastrophenereignissen oder Bedienfehlern aus, hat dies unmittelbare Auswirkungen auf die IoT-Dienste und die darauf aufbauenden automatisierten Prozesse und Abläufe. Motivation des Projekts „RIOT - Resiliente IoT - Hochverfügbare Infrastruktur für kritische IoT-Anwendungen“ ist es deshalb, die Ausfallsicherheit von IoT Diensten zu stärken.

Vision
Die Kombination voneinander unabhängiger drahtloser Kommunikationstechnologien ermöglicht die redundante Anbindung von IoT-Geräten und Sensoren. Eine intelligente Control-Plane für das (Um-) Schalten über redundante Pfade und Cloudressourcen gewährleistet ein hohes Maß an Ausfallsicherheit der IoT-Anwendungen.

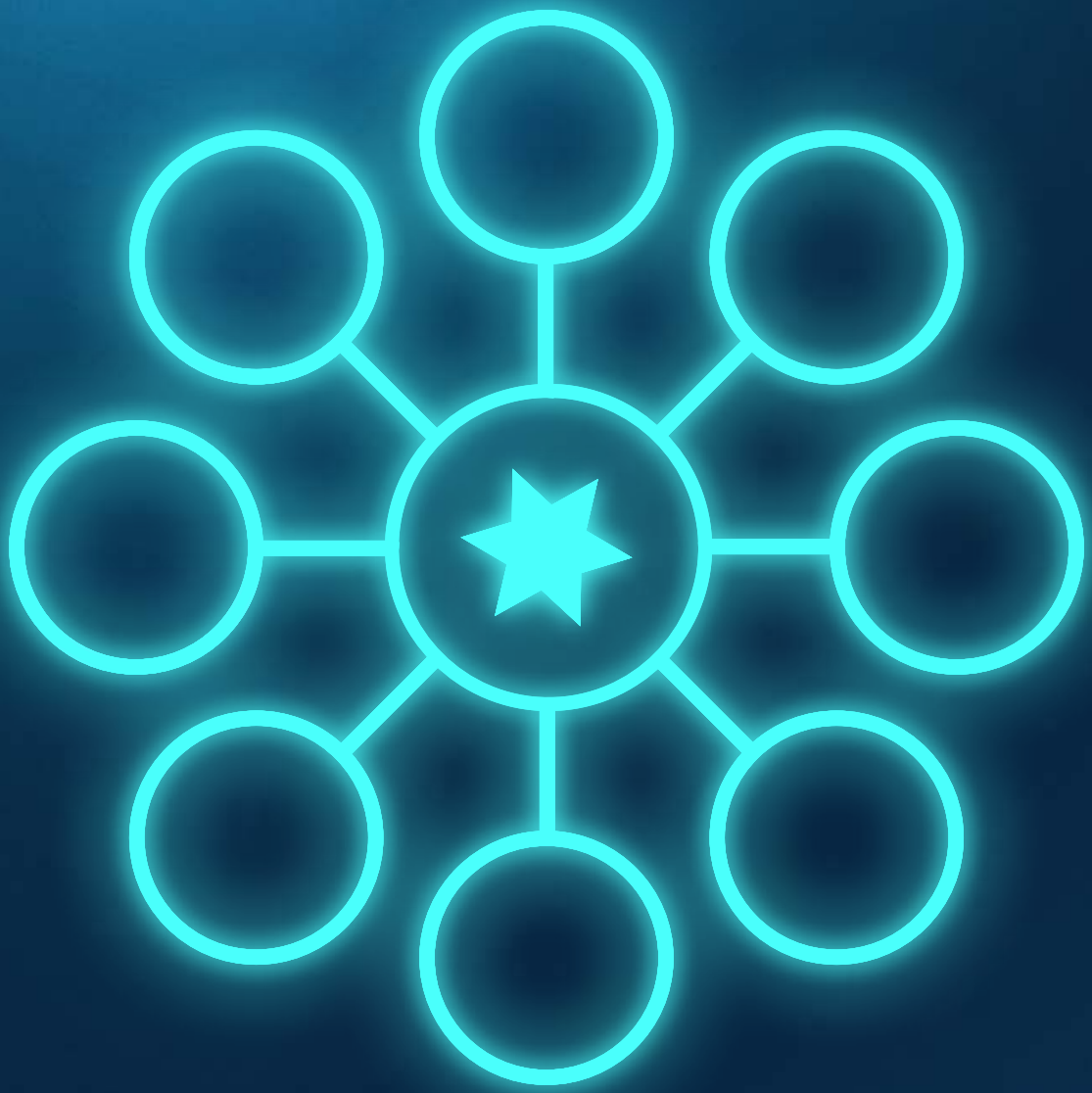
Zielstellung
Im Rahmen des Projektes werden alle Komponenten für die technische Umsetzung einer hochverfügbaren und sicheren Kommunikationsinfrastruktur für kritische IoT Dienste entwickelt. Dies umfasst alle notwendigen geräte-, netz- und cloudseitigen Hardware und Softwarekomponenten. Die Komponenten der Lösung sowie das Gesamtsystem werden innerhalb des Projektrahmens als Labordemonstrator implementiert und in einem Feldtest erprobt. Dabei sollen die entwickelten Methoden und Verfahren auf verschiedene Netzzugangstechnologien adaptiert werden können.

Angestrebte Ergebnisse
Erreicht werden soll, dass Verfahren für das Monitoring und die Erkennung und ggf. Prädiktion von Fehlern, Anomalien und Cyber-Angriffen in der OTT-Infrastruktur ausgearbeitet werden. Hinzukommen Verfahren zur automatisierten Reaktion auf erkannte (ggf. vorhergesagte) Störfälle, bspw. Ersatzschalten von Datenpfaden, Key-Change/Revocation. Außerdem soll radiotechnologieübergreifende Sicherheitsarchitektur inklusive leichtgewichtiger Verschlüsselung und Schlüsselmanagement verbessert werden. Kontrollpläne, die sowohl zentral, dezentral oder teilzentral betrieben werden können und ihrerseits eine hohe Ausfallsicherheit aufweisen, sollen genauso angestrebt werden, wie ein Überlast-Schutz des Backup-Netzes durch Reduktion der Applikationsdatenmenge bei Nutzung des Backupkanals und durch langsames Einbuchen der IoT-Geräte.

Erwarteter Impact
Mit den im Rahmen des Projekts entwickelten Lösungen sollen IoT-Anwender (z. B. Landkreise und Gemeinden, Smart-City-Projekte), aber auch Hersteller von 5G/NB-IoT/LoRaWAN Komponenten sowie von IoT-Sensoren/Aktuatoren angesprochen werden. Weiterhin sind die Projektergebnisse für Mobilnetzbetreiber und IoT-Systemintegratoren relevant. Wir sind darüber hinaus bemüht, unsere Lösungsansätze in Fachverbänden und Standardisierungsgremien einzubringen.

Projektlaufzeit:	31.12.2022 - 31.12.2024
Fördersumme:	1,4 Mio. €
Partner:	mCloud Systems GmbH, TU Chemnitz, Hochschule Koblenz
Projektleitung:	Dr.-Ing. Andreas Baumgartner, mCloud Systems GmbH
Website:	www.mcloud-systems.com/2023/03/24/riot-resiliente-iot/ www.tu-chemnitz.de/etit/kn/riot/index.php www.hs-koblenz.de/hochschule/einrichtungen/forschungsinstitute/interdisziplinaeres-institut-fuer-digitalisierung/projektbereich/riot

Themen-schwerpunkt 5



Forschung- und Entwicklung zu 5G/6G-Netzwerksicherheit und Open-RAN

Dieser Themenschwerpunkt richtet sich an Start-ups sowie kleine und mittlere Unternehmen (KMU) mit Fokus auf 5G/6G-Netzwerksicherheit und Open RAN. Gefördert werden Vorhaben auf Gebieten wie Monitoring-Tools, Schnittstellenabsicherung, Core- und RAN-Virtualisierung oder Hardware- und Embedded-Firmware-Sicherheit.

Mit dem Fokus auf Start-ups aktiviert der Themenschwerpunkt 5 über das Förderprogramm Ausgründungen, Neugründungen sowie KMUs. Gerade Start-ups aus dem technologischen Bereich können sich so etablieren. Mit innovativen Projekten zu 5G/6G-Netzwerksicherheit und Open RAN sollen neue Produkte oder neue Dienstleistungen im Unternehmen entwickelt werden. Die Förderung des BSI kann dazu beitragen, dass hierüber neue Geschäftsmodelle entstehen und sich später am Markt zeigen. Die Vorhaben sollen einzeln, in Kooperation mit gemeinnützigen Forschungsinstitutionen oder Universitäten verwirklicht werden.

Mit den ausgewählten Förderprojekten im Themenschwerpunkt 5 unterstützt das BSI die Entwicklung junger Unternehmen und Start-ups gezielt auch im Bereich der Geschäftsmodellentwicklung. Das jeweils geförderte F&E Projekt muss daher einen klaren Bezug zur Geschäftsmodellentwicklung des Jungunternehmens nachweisen, damit eine Marktdurchdringung bzw. Verwertung der Entwicklungsideen wahrscheinlicher wird. Gerade im Bereich der software- und cloudgetriebenen Core- und RAN Bereiche des 5G Netzes wird eine stärkere Diversifizierung der Hersteller- und Anbieterstrukturen erwartet. Die BSI Start-up-Förderung gilt somit als Anschubfinanzierung neuer Entwicklungsprojekte, damit sich High-Tech Ausgründungen und Jungunternehmen mit Nischen- und Speziallösungen am Markt etablieren können.

Projekte im Themenschwerpunkt

- **5G-FORAN** - IT-Forensik und Behandlung von IT-Sicherheitsvorfällen im Open RAN
- **5Guide** - Erstellung eines Leitfadens und von Werkzeugen für ein Core Pentesting von 5G Campusnetzen
- **ABAC456** - Attribute-Based-Access-Control für 5G und 6G Mobilfunknetze
- **KIMA-5G** - KI-basiertes Management und Automatisierung für 5G Open RAN
- **SECURITAS-5G** - Entwicklung eines weltweit ersten kompletten und in einer Ein-Chip Lösung realisierten 5G-millimeterwellenfähigen Connectivity Chipsets
- **SiKora** - Sichere Kommunikationsräume

Ansprechpartner für fachliche Fragen

Jörg Andreas
E-Mail: kopa45@bsi.bund.de

5G-FORAN – IT-Forensik und Behandlung von IT-Sicherheitsvorfällen im Open RAN

Abstract
„5G-FORAN“ kann die Cybersicherheit im Open-RAN-Umfeld stark erhöhen. Das Projekt kombiniert modernste 5G-Technologie mit IT-Forensik, Incident-Response und Digital Forensics. Als Teil der Cyberabwehr ist IT-Forensik ein unverzichtbarer Baustein zur schnellen Identifikation, Analyse und Abwehr von Sicherheitsvorfällen. Mit „5G-FORAN“ stellt die IT-Sicherheit im Open RAN ein neues Level dar. Das ambitionierte Projekt zielt darauf ab, IT-Forensik und die Behandlung von IT-Sicherheitsvorfällen im Open RAN zu verbessern und Cyberbedrohungen entgegenzutreten.

Motivation
Die Behandlung von IT-Sicherheitsvorfällen und die IT-Forensik moderner Netztechnologien sind noch unerforschte Gebiete. Besonders in Anbetracht der Tatsache, dass das RAN bzw. das Open RAN als konkreter Umsetzungsvorschlag innerhalb eines 5G/6G-Netzes den Großteil der Infrastruktur abdeckt, wird die Relevanz dieser Thematik in Zukunft schnell zunehmen.

Vision
Um die digitale Souveränität zu verbessern, müssen deutsche Cybersecurity-Teams in der Lage sein, schnell und effektiv Cyberangriffe auf moderne Netztechnologien abzuwehren und damit Schäden durch beispielsweise Spionage oder Sabotage zu minimieren.

Zielstellung
Das Vorhaben zielt darauf ab, eine Methode zu entwickeln, zu konzipieren und praktisch zu simulieren, wie IT-Sicherheitsvorfälle im Bereich Open RAN analysiert, behandelt und behoben werden können. Grundlage für diese Entwicklung bilden nachvollziehbare Angriffsspuren auf den Komponenten, die ebenfalls im Rahmen von „5G-FORAN“ durch eine Angriffssimulation bereitgestellt werden.

Angestrebte Ergebnisse
Zusätzlich zum Gesamtkonzept sollen die entwickelten Automatismen und die Software als Open Source veröffentlicht werden. Dadurch wird ein einfacher und direkter Zugang zu Ressourcen und Informationen ermöglicht, um die Entwicklungs- und Simulationsumgebung von „5G-FORAN“ für zukünftige Projekte wiederherzustellen, nahtlos anpassen und weiterentwickeln zu können.

Erwarteter Impact
Durch die Veröffentlichung der Ergebnisse als Open Source ergeben sich verschiedene Möglichkeiten zur Zusammenarbeit und Kooperation mit anderen Akteuren im Bereich Open RAN. Darüber hinaus wird durch das Vorhaben ein wichtiger Einstiegspunkt für Cybersecurity-Teams und Unternehmen geschaffen, um IT-Sicherheitsvorfälle im Open RAN zu beheben. Dies wird dazu beitragen, die Sicherheit und Stabilität des Open RAN zu verbessern und somit den Nutzen und die Akzeptanz dieser Technologie zu steigern.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 0,8 Mio. €

Partner: PROCYDE GmbH, Technische Hochschule (TH) Köln

Projektleitung: Thomas Karl, PROCYDE GmbH

Website: https://5g-foran.com

5Guide - Erstellung eines Leitfadens und von Werkzeugen für ein Core Pentesting von 5G-Campusnetzen

Motivation

Mobilfunknetze sind ein grundlegender Bestandteil der Infrastruktur unserer Gesellschaft. Die aktuelle Mobilfunkgeneration 5G verstärkt die Integration in unseren Alltag weiter und eröffnet neue Möglichkeiten durch eine höhere technische Leistungsfähigkeit. Die Sicherheit unserer Infrastrukturen spielt dabei eine fundamentale Rolle. Die Nutzung eines 5G-Netzes über bereits etablierte Web-Technologien wie HTTP/HTTPS, REST oder auch OAUTH birgt erhebliche Sicherheitsrisiken. Eine umfassende Sicherheitsanalyse von 5G-Netzen erweist sich jedoch als technisch sehr anspruchsvoll. Dies liegt an der hohen Komplexität der Netze und ihrer Komponenten. Während eine sicherheitskritische Zertifizierung von öffentlichen Netzen bereits initiiert und durch das NESAS-CCS-GI Schema spezifiziert ist, sind private Campusnetze von der verpflichtenden Anwendung ausgenommen. Durch die Bereitstellung eines dedizierten Pentesting Tools und dem erforderlichen Training soll die Zugänglichkeit von Sicherheit in der 5G-Netztechnologie erhöht und gleichzeitig die erschwerende Komplexität des Themas für Campusnetzbetreiber minimiert werden.

Vision

Wir wollen den Betreibern von 5G-Campusnetzen ein technisch ausgereiftes, skalierbares und leicht zugängliches Lösungsangebot zur Verfügung zu stellen, mit dem sie ihre kritischen Anlagen besser schützen können. Wir streben demnach an, 5G-Campusnetzbetreiber zu befähigen, die eigene Netzinfrastruktur auf sicherheitskritische Faktoren zu testen, um so einen Sicherheitsstandard im 5G-Campusnetzbereich zu schaffen, auch ohne vorherrschende Zertifizierungspflicht. Der Wert des globalen 5G-Sicherheitsmarkts wird derzeit auf 1,3 Mrd. USD (2022) geschätzt, mit einem erwarteten Wachstum auf 7,2 Mrd. USD bis 2027, was einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 41,6 % über den betrachteten Zeitraum entspricht. Dementsprechend umfasst der verfügbare Gesamtmarkt verschiedene Akteure wie kommerzielle und Campusnetzbetreiber, Ausrüstungsanbieter und Integratoren. All diesen Gruppen ist gemeinsam, dass sie verschiedene Arten von Sicherheitslösungen für ihre Infrastrukturen und Produkte benötigen. Ein Markt für 5G-Sicherheitslösungen ist im Entstehen.

Zielstellung

Ziel des Projektes 5Guide ist es, die Sicherheit von 5G-Netzen zu erhöhen, die keiner Zertifizierungspflicht unterliegen. Dies betrifft vor allem private Campusnetze, deren Betreiber das Wissen und die Mittel erhalten, um das Sicherheitsniveau während der Implementierung und des Betriebs zu erhöhen. Das Ziel kann in zwei Aspekte unterteilt werden. Ein Training ermöglicht es Campusnetzbetreibern, aber auch PentesterInnen, sich mit der Materie der 5G-Sicherheit vertraut zu machen. Das Tooling ermöglicht eine technisch unterstützte Sicherheitsbewertung von 5G-Campusnetzen, die in weiterer Folge durch gezielte Maßnahmen zu einer Verbesserung der Sicherheit führt. Damit steht ein robuster und skalierbarer Ansatz zur Verfügung, um die Kompetenz der Akteure und Verantwortlichen aufzubauen und zu erhöhen und somit die Sicherheit von 5G-Netzen zu verbessern.

Angestrebte Ergebnisse
Mit einem „Training and Tooling"-Ansatz senken wir die Eintrittsbarriere für neue und etablierte Unternehmen 5G sicher zu implementieren. Mit der technischen Entwicklung eines Demonstrators, der die bestehenden Anforderungen potenzieller Kundengruppen beantwortet, wird ein strategischer Eintritt in den Markt ermöglicht. Der entsprechende Arbeitsplan zielt auf die Evaluation verschiedener Annahmen ab, die im Falle einer positiven Verifizierung den Bedarf an den angebotenen Softwarelösungen bestätigen. So können wir kurzfristig demonstratorische Produkte an Early Adopters lizenzieren und damit die ersten Schritte des Markteintritts vollziehen. Dies beeinflusst die wirtschaftliche Tragfähigkeit des Projekts positiv, ermöglicht es uns gleichzeitig aber auch, die Eigenschaften der angebotenen Produkte an die Anforderungen der Kunden anzupassen. 5Guide bietet ein hohes Verwertungspotential. Neben der traditionellen Aufbereitung von Forschungsresultaten auf Konferenzen und in Journalen ist insbesondere vorgesehen, die Projektergebnisse in die (Weiter-)Entwicklung konkreter Dienstleistungen einfließen zu lassen. Weiterhin werden die Ergebnisse Beiträge zur öffentlichen Diskussion und zur akademischen Lehre leisten. Es ist geplant, die Projektergebnisse als Open-Source-Software zur Verfügung zu stellen.

Erwarteter Impact
Die Projektergebnisse haben signifikanten Einfluss auf die zukünftige Akquise von weiteren Mitteln sowohl auf nationaler als auch auf EU-Ebene, insbesondere da Vorarbeiten in diesem Arbeitsgebiet geschaffen werden, die zukünftig genutzt werden können, um Deutschland im europäischen Kontext zu platzieren. Hieraus ergeben sich interessante Möglichkeiten für Folgeprojekte, insbesondere nach Projektabschluss.

Statement zur Fördermaßnahme
Mit dem Projekt 5Guide soll es 5G-Campusnetzbetreibern ermöglicht werden, kritische Sicherheitsstandards im eigenen Netz zu erfüllen, auch wenn eine Zertifizierung nicht erforderlich ist. Darum entwickeln wir im Rahmen des Projektes die nötige Software und das erforderliche Training, welches die Komplexität der 5G-Netztechnologie minimieren und den praktischen sowie theoretischen Zugang zu Sicherheitstests des hauseigenen 5G-Netzes maximieren. Mit diesem Bestreben soll auf nationaler und auf EU-Ebene ein neuer 5G-Sicherheitsstandard für Campusnetzbetreiber geschaffen werden, welcher die deutsche Position im Kontext von 5G-Netz und -Sicherheit stärkt und als innovativer Vorreiter etabliert.

Projektlaufzeit:	01.06.2023 - 30.11.2024
Fördersumme:	0,7 Mio. €
Partner:	Radix Security GmbH, Westfälische Hochschule Gelsenkirchen Bocholt Recklinghausen
Projektleitung:	Dr. David Rupprecht, Radix Security GmbH, E-Mail: david@radix-security.com
Website:	www.5gui.de

ABAC456 – Attribute-Based-Access-Control für 5G- und 6G-Mobilfunknetze

Abstract
Das Zugriffsmanagement in den Bereichen Netzwerksicherheit und Identitätsmanagement ist ein branchenweites Thema. „ABAC456“ ist ein ambitioniertes Projekt, das die Leistungsfähigkeit von Attribute-Based-Access-Control (ABAC) in 5G- und 6G-Mobilfunknetzen demonstriert. Das Ziel ist es, ein sicheres und effizientes Energiemanagement zu ermöglichen. „ABAC456“ ist Open Source, um sicherzustellen, dass es für alle zugänglich und anpassbar ist.

Motivation
Die Motivation für das Projekt „ABAC456“ ist die Verbesserung der Sicherheit in den 5G/6G-Kommunikations-Stacks durch die Implementierung eines modernen Zugriffsmanagementsystems. Traditionelle Zugriffskontrollsysteme basieren auf festgelegten Rollen und sind oft statisch, was zu Schwachstellen und potenziellen Angriffspunkten führen kann. Attribute-Based Access Control (ABAC) ist dagegen flexibler und ermöglicht eine dynamische Anpassung an Änderungen in Rollen, Identitäten und Umgebungen. ABAC bietet auch die Möglichkeit, Identitäts-, Rollen- und Zugriffsmanagement auf mehrere Netzwerkteilnehmer zu verteilen, wodurch selbstsouveräne und prüfbare Identitäten eingeführt werden können. Durch die Integration von ABAC in dem Kommunikations-Stack wird das Netzwerk sicherer und widerstandsfähiger gegenüber Angriffen wie Sybil, Man-in-the-Middle und Man-at-the-Side.

Vision
Die Manipulationssicherheit als Teil des Netzwerkprotokolls durch attributbasierte Zugriffskontrolle (ABAC) und die verifizierbaren Identitäten als Kernelement der Systemsicherheit sollen künftig gegeben sein. Des Weiteren haben die User die Hoheit über Ihre Daten.

Zielstellung
Ziel ist die Implementierung von attributbasierter Zugriffskontrolle in 5G und 6G auf unteren Protokollebenen, die Minimierung von Identitäten im 5/6G-Netz, keine Dienstanfrage ohne gesicherte Identität und die Identifizierung durch selbstbestimmte und -verwaltete Identitäten.

Angestrebte Ergebnisse
Das Ergebnis dieses Projekts soll eine identitätssichernde Kommunikationsschicht für drahtlose Netze sein, die mit der Attribute-Based Access Control (ABAC) erweitert wird und die angriffsresistente Funktionalität in einem laufenden Projekt zum verteilten Energiemanagement beweisen. Die Software wird so konzipiert sein, dass sie transparent in den 5G/6G-Kommunikations-Stack integriert werden kann. Die Projektergebnisse werden als Open Source zur Verfügung gestellt und auf Konferenzen veröffentlicht.

Erwarteter Impact
Für den Anbieter erwarten wir eine erhöhte IoT-Sicherheit mit den Vorteilen der als Open Source bereitgestellten Lösung, die an den individuellen Software-Stack angepasst werden kann. Für die Nutzer erwarten wir eine erhöhte Datensouveränität durch selbstverwaltete Identitäten, eine erhöhte IoT-Sicherheit und ein robustes Authentifizierungsnetzwerk.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 0,4 Mio. €

Partner: Chainstep GmbH, Hochschule für Angewandte Wissenschaften Hamburg

Projektleitung: Mark Hebbel, Chainstep GmbH

Website: https://www.haw-hamburg.de/forschung/forschungsprojekte-detail/project/project/show/abac456/

KIMA-5G – KI-basiertes Management und Automatisierung für 5G-Open-RAN

Abstract
Im Projekt „KIMA-5G“ werden KI-basierte Technologien verwendet, um die Automatisierung von 5G-Open-RAN-Netzwerken zu ermöglichen. Mit den fortschrittlichen Maschine Learning (ML)-Tools und der Verwendung des CCO-Systems wird sichergestellt, dass das Netzwerk immer auf dem aktuellsten Stand ist. Mit ICIC kann dafür gesorgt werden, dass eine optimale Nutzung der Netzwerkressourcen erfolgt.

Motivation
Weitgehende Automatisierung des Betriebs von 5G-Campusnetzen soll mit Hilfe der Erfüllung hoher Zuverlässigkeits-, Dienstgüte- und Sicherheitsanforderungen von gemanagten Netzen und der vereinfachten Administration und Betrieb von 5G-Campusnetzen erreicht werden.

Vision
Die Vision ist die Bereitstellung eines Cloud- und KI-basierten Werkzeuges für die gemeinsame Optimierung von Netzabdeckung, Kapazität und Interferenzen von Open-RAN-basierten Campusnetzen als Baustein für ein offenes cloudbasiertes Netzmanagementsystem für 5G-Systeme.

Zielstellung

Der Demonstrator für Cloud- und ML-basiertes Werkzeug zur CCO/ICIC-Optimierung von Open-RAN-basierten 5G-Campusnetzen (rApp) wird bei AiVader mit Hilfe einer cloudbasierten Lösung zur Optimierung von Netzabdeckung, Kapazität und Interferenzen in 5G-Netzen als Ziel gesetzt. Ein Verfahren für die ML-basierte Optimierung von OpenRAN-basierten 5G-Netzen soll konzipiert werden.

Angestrebte Ergebnisse
Die Inbetriebnahme, der Betrieb und das Management von 5G-Campusnetzen, insbesondere die Erfüllung hoher Zuverlässigkeits-, Dienstgüte- und Sicherheitsanforderungen wird vereinfacht.

Erwarteter Impact
Innovativ ist die Automatisierung und Optimierung in Konflikt stehender Ziele durch ML-basierte Verfahren (Forschungsschwerpunkt der TU Ilmenau) in Campusnetzen. Der Einsatz und die Verallgemeinerung der Lösung für verschiedene Ausprägungen von 5G-Campusnetze, die Erweiterung der Netzmanagementlösung auf größere und öffentliche 5G-Netze und die Erweiterung der ML-basierten Basislösung auf weitere Use-Cases bergen hohes Transferpotential.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 0,6 Mio. €

Partner: AiVader GmbH, Technische Universität Ilmenau

Projektleitung: Zubair Shaik, AiVader GmbH

Website: KIMA-5G - KI-basiertes Management und Automatisierung für 5G OpenRAN | Technische Universität Ilmenau (tu-ilmenau.de)

SECURITAS-5G – Entwicklung des weltweit ersten kompletten und in einer Ein-Chip Lösung realisierten 5G-millimeterwellenfähigen Connectivity-Chipsets

Abstract
Die Expertinnen und Experten aus der Welt der Telekommunikation und IT-Sicherheit arbeiten zusammen mit internationalen Partnern an integrierten Schnittstellen- und Sicherheitstechnologien. Ziel ist es, eine sichere und schnelle Kommunikation im neuen Millimeterwellenmobilfunkstandard 5G zu ermöglichen. Dadurch sollen zukünftig Anwendungen wie autonomes Fahren, Augmented Reality und Virtual Reality in Echtzeit möglich sein.

Vision
Unsere Vision ist es, dass die nächste Generation von 5G, Millimeterwellen 5G, neue Maßstäbe nicht nur hinsichtlich seiner Leistungsparameter wie Datenrate oder Latenz aufstellt. Es soll gleichzeitig die Sicherheit der Kommunikation auf eine neue Stufe heben.

Zielstellung
In Securitas-5G werden wir Hardwaretechnologien entwickeln, die ein bisher nicht erreichtes Niveau an Integration erreichen, wodurch die Verwundbarkeit durch unerlaubten Zugriff auf der Hardwareebene signifikant verringert wird. Ferner wird diese Technologie die schnelle Verbreitung von Millimeterwellen 5G und damit die Verwendung von fortschrittlichen und sicheren Kommunikationsprotokollen ermöglichen.

Angestrebte Ergebnisse
Das angestrebte Ergebnis ist die Entwicklung eines kompletten, 5G-millimeterwellenfähigen und gleichzeitig kostengünstigen, energieeffizienten Connectivity Chipsets, welches weltweit erstmalig als eine integrierte Ein-Chip Lösung realisiert wird. Als Endergebnis streben wir einen funktionierenden Demonstrator eines Kommunikationslinks an.

Erwarteter Impact
Die entwickelte Technologie wird die Resilienz und Netzsicherheit erhöhen. Dank Implementierung in kostengünstiger, leicht implementierbarer 22nm CMOS Halbleitertechnologie werden Markteintrittsbarrieren verringert. Zusätzlich wird der Grundstein gelegt mit InCirT einen in Deutschland ansässigen Anbieter von zentraler 5G Millimeterwellen Mobilfunktechnologie zu etablieren und damit das nationale Hersteller-Ökosystem für moderne Netztechnologie im Kontext der IT-Sicherheit gestärkt.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 1,0 Mio. €

Partner: InCirT GmbH, RWTH Aachen

Projektleitung: Sebastian Waters, InCirT GmbH

Website: https://www.hfe.rwth-aachen.de/securitas-5g

SiKora – Sichere Kommunikationsräume durch optische Systeme zur Datenübertragung

Abstract
Das Projekt widmet das sich der Cybersicherheit in Kommunikationsräumen. Dabei kommt die neuartige Technologie Li-Fi (light fidelity) zum Einsatz, die auf sichtbarem Licht basiert, um Daten zu übertragen. „SiKora“ bietet außerdem Schutz vor gängigen Angriffen wie Jamming, Spoofing und Sniffing sowie OpenRAN und SDR-Funktionen. VLC-Technologie rundet das Sicherheitspaket ab und sorgt für schnelle und stabile Übertragungen. „SiKora“ ist eine Lösung für Unternehmen und Organisationen, die vertrauliche Daten zuverlässig und sicher schützen möchten.

Motivation
Eine lichtbasierte Kommunikation (Li-Fi) hat inhärente Vorteile gegenüber funkbasierten Systemen. Einerseits sind Zonen für die Ausleuchtung selbst in Räumen klar abgrenzbar und klassische Angriffsszenarien sind weitestgehend unwirksam. Es existieren heute keine für die lichtbasierte Kommunikation optimierten Basisband-Chipsets, daher werden proprietäre Wi-Fi- und Powerline-Chipsets begrenzt adaptiert.

Vision
Für sicherheitskritische Anwendungen soll Li-Fi zu einer ausgereiften Kommunikationslösung werden. Die Open-RAN-basierte Architektur mit über Software implementierten Protokollen und optimierten optischen Transceivern zur einfachen Anpassung an räumliche Gegebenheiten soll hierbei gegeben sein.

Zielstellung
Ziel ist der Aufbau und die Erprobung eines störsicheren optischen Systems zur Datenübertragung. Li-Fi-optimierte Software zur Implementierung von Übertragungsprotokollen auf einer SDR-Plattform ist ein Teil dessen. Die OpenRAN-Schnittstelle zum optischen Transceiver soll ausgebaut werden und Grundlagen zur Auslegung von optischen Transceivern für verschiedene Anwendungsszenarien geschaffen sowie optische Transceiver zur gezielten Ausleuchtung von definierten Bereichen entwickelt werden.

Angestrebte Ergebnisse:
Es soll eine drahtlose Kommunikationslösung für verschiedene sicherheitskritische Anwendungsbereiche, z. B. bei Banken, Krankenhäusern, Behörden und Organisationen mit Sicherheitsaufgaben sowie feste und mobile Installationen im Bereich von Krisenreaktionskräften (DRK, THW, BP, BW) bereitgestellt werden. Es soll eine zukunftssichere Plattform durch Open-RAN-Schnittstellen und softwarebasierte Protokollimplementierung konzipiert werden.

Erwarteter Impact
Es soll mit den Entwicklungen im Vorhaben eine sichere Kommunikation durch Li-Fi, Li-Fi-optimierte Transceiver- und Netzwerkarchitektur sowie eine einfache Anpassung der optischen Auslegung an Anwendungsszenarien ermöglicht werden. Durch eine transparente Integration in bestehende Netzwerke und den gewählten Open-RAN-Ansatz sind künftig längere Produktzyklen möglich. Es können weitere Anwendungsbereiche erschlossen werden. Beispielsweise können durch die neuartige Technologie die Anforderungen an erhöhten Explosionsschutz (Wasserstofftechnologie) in der chemischen Industrie und in Bereichen mit elektromagnetischen Störungen (Maschinen, MRT) erfüllt werden.

Projektlaufzeit: 31.12.2022 - 31.12.2024

Fördersumme: 0,3 Mio. €

Partner: aeroLiFi GmbH, TU Clausthal

Projektleitung: Günter Boomgaarden, aeroLiFi GmbH

Website: https://aerolifi.com/sikora-project

Impressum

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: kopa45@bsi.bund.de Internet: www.bsi.bund.de
Stand:	August 2023
Redaktion:	Bundesamt für Sicherheit in der Informationstechnik (BSI) / DLR Projektträger
Konzept und Gestaltung:	DLR Projektträger
Druck:	-
Artikelnummer:	BSI-KoPa 23/00 1
Grafiken und Bildnachweise:	Titel, Seite 7, 9, 10, 12, 20, 30, 43, 74: DLR Projektträger

www.bsi.bund.de

facebook.com/bsi.fuer.buerger
twitter.com/BSI_Bund
youtube.com/@bsi_bund
instagram.com/bsi_bund