

Drei Fragen
an Sarah
Koop-Brinkmann

04

Mission
Critical
Networks

06

VDE-Gremienarbeit
im KI-Zeitalter
Reicht gesichertes
Fachwissen noch?

30

ITG news

Magazin der
**Informationstechnischen
Gesellschaft** im VDE e.V.

VDE

OKTOBER 26



Mission
Critical
Networks

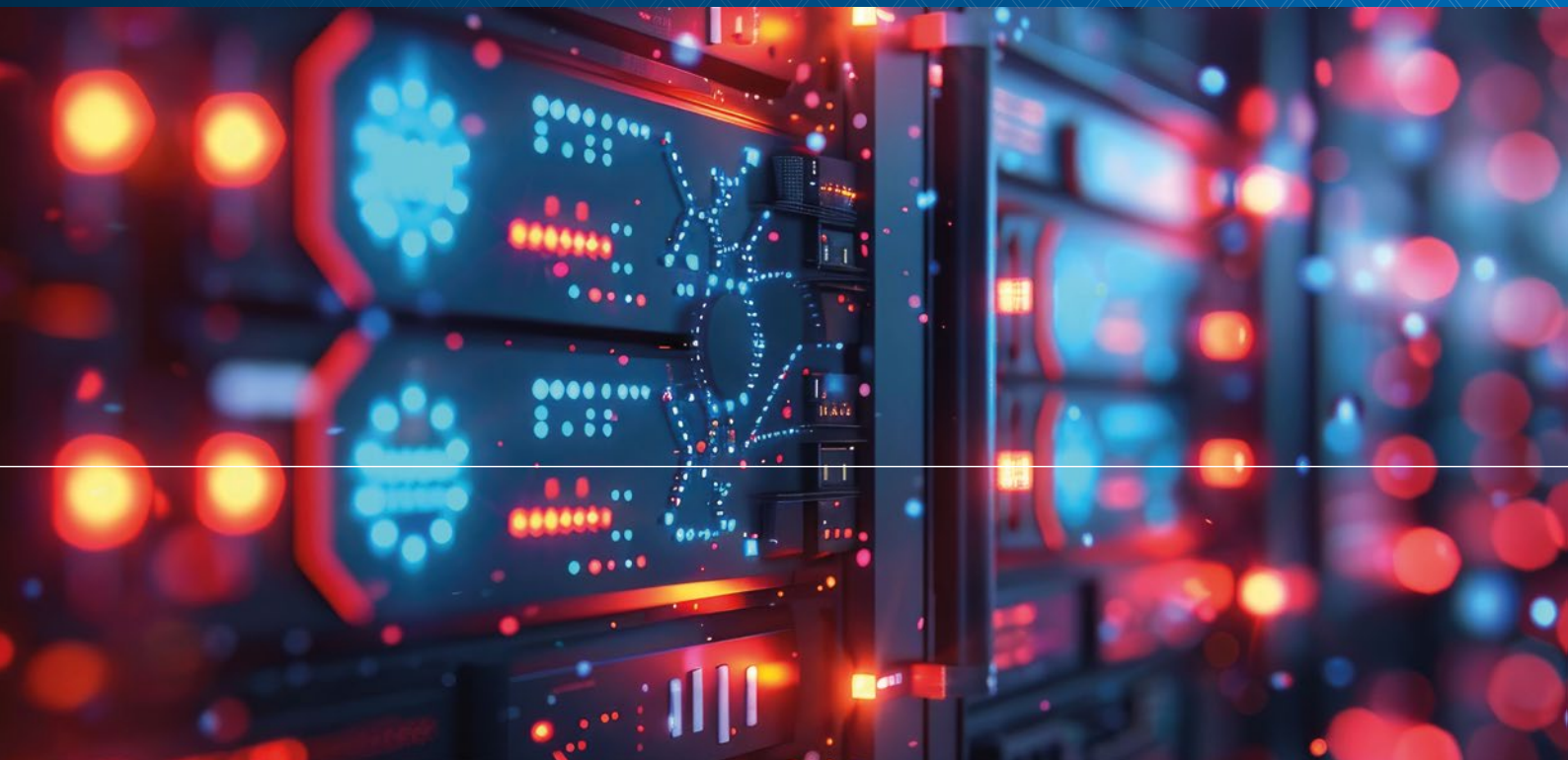
THEMA

ITGnews

Vorwort	01
Ankündigungen	02
Drei Fragen an ...	04
Thema Mission Critical Networks	06
Nachdenken & Mitreden	30
Aus den Fachgremien	32
Veranstaltungen	40
Durchstarter – Ausgründungen & Start-ups	48
Personalia	51

VDE

OKTOBER 26





Liebe Mitglieder der ITG,

willkommen zur zweiten Ausgabe der ITG-News im neuen Erscheinungsbild, und zugleich vielen Dank für das positive Feedback zur ersten Ausgabe im neuen Design. Das ist uns ein Ansporn, auf diesem Weg weiterzugehen. Wir haben wieder – wie wir hoffen – hochinteressante Themen für Sie.

Das Schwerpunktthema dieser Ausgabe ist den einsatzkritischen Netzen (»Mission Critical Networks«) gewidmet. Für Anwendungsbereiche wie etwa Polizei, Feuerwehr und Rettungskräfte, das Militär, den Betrieb von Stromnetzen oder Bahnen, oder die Automatisierung von industriellen Produktionsprozessen sind die öffentlichen Fest- und Mobilfunknetze nicht ausreichend. Spezialfunktionen, Abdeckungsbereiche und besonders hohe Verfügbarkeit können nur von spezifischen Netzen bereitgestellt werden. Die Fachbeiträge zu diesem Thema nehmen Sie mit in die Welt einsatzkritischer Netze, die in aller Regel sehr zuverlässig funktionieren und deren Existenz nur dann sichtbar wird, wenn – selten genug – einmal Störungen auftreten, die den Betrieb des jeweiligen Anwendungsbereichs spürbar beeinträchtigen.

Ein umfangreicher Fachartikel beschreibt einen aktuellen, neuartigen Ansatz aus der Welt der Künstlichen Intelligenz: dezentrales, föderiertes Training von Machine Learning Algorithmen bietet Vorteile bei heterogenen Anwendungen mit hohen Anforderungen an Sicherheit und Datenschutz. Ein erfolgreicher Einsatz des Konzepts kann nur gelingen, wenn menschliche Faktoren von vornherein mitgedacht werden.

Die Künstliche Intelligenz steht auch im Mittelpunkt des 1. ITG Future Forum, zu dem wir Sie am 25.11.2026 ganz herzlich nach Berlin einladen. Mit dem Thema »AI-powered Networks and Networking for AI« beleuchten wir, welche Auswirkungen KI für unsere Kommunikationsnetze haben wird. Freuen Sie sich auf ein spannendes Thema, hochkarätige Sprecher, und intensive fachliche Diskussionen. Und wenn Sie schon nach Berlin kommen: am 24.11. halten wir dort die jährliche Mitgliederversammlung der ITG ab und laden Sie anschließend zum traditionellen ITG-Hauptstadtforum ein. Es steht dieses Jahr unter dem Motto »150 Jahre Telefon« – eine Erfindung, an der wir exemplarisch sehen, dass eine gute Erfindung alleine noch keinen wirtschaftlichen Erfolg garantiert. »Innovation is to turn an invention into business« – wir werden beleuchten, wie dies Alexander Graham Bell gelungen ist, was Philipp Reis fehlte, der das Telefon bereits 20 Jahre früher erfunden hatte, und was wir für unsere heutige Arbeit daraus lernen sollten.

Interessante Impulse finden Sie auch in unseren Kolumnen: wie findet eine junge Frau ihren Weg in die Hochfrequenztechnik? Was waren die Ergebnisse ausgewählter ITG-Veranstaltungen der letzten Zeit, und was ist für die kommenden Monate geplant? Und was für neue Geschäftsideen gibt es im Bereich Quantenverschlüsselung?

Wir wünschen Ihnen eine anregende Lektüre – und wir sehen uns hoffentlich in Berlin!

DR.-ING. JÖRG-PETER ELBERS
Vorsitzender der ITG

DIPL.-ING. SIGURD SCHUSTER
Projektbeauftragter des ITG Vorstandes
Management Consulting – Unternehmensberatung



EINLADUNG

VDE Hauptstadtforum 2026

24.11.2026, Berlin
Berlin-Brandenburgische
Akademie der Wissenschaften



INFOS UND ANMELDUNG
www.vde.com/hauptstadtforum

Wir schreiben »150 Jahre
Telefon« als Motto. Ist Alexander
Graham Bell der Erfinder des
Telefons oder ist es Johann
Philipp Reis?

Im Rahmen des VDE Hauptstadtforums werden Preise und Ehrungen an Personen verliehen, die eine besondere Strahlkraft in der Informationstechnischen Gesellschaft haben. Diese kommen vor allem aus dem akademischen Arbeitsbereich der Informationstechnik. Jedoch steht gerade die Zusammenarbeit zwischen Industrie und Akademia in der ITG in einem durchgängigen Kontinuum ohne Barrieren zwischen den Disziplinen oder der Arbeitsweisen. Vor diesem Hintergrund beleuchten wir im Rahmen von Vorträgen und einer Podiumsdiskussion den häufig in Deutschland besprochenen fehlenden Transfer aus der Grundlagenforschung in Anwendungen. Was ist an dem Narrativ dran, dass wir als Industrieland an Innovationskraft verlieren? Mit einem Blick in die Vergangenheit vor

150 Jahren als das Telefon für die massenhafte Nutzung in den Markt eingeführt wurde und der Perspektive in die Zukunft der Entwicklung der generativen KI für den Massenmarkt, wollen wir eine Diskussion anregen und freuen uns auf Ihre Einschätzung und Meinung dazu.

Wir freuen uns auf die Diskussion im Rahmen der Preisverleihungen. Vergessen Sie bitte nicht sich anzumelden unter www.vde.com/hauptstadtforum. Wir laden Sie herzlich zum VDE Hauptstadtforum 2026 ein, dass am Dienstag, den 24. November 2026 in der Berlin-Brandenburgischen Akademie der Wissenschaften stattfinden wird.

Erleben Sie spannende Einblicke in die Geschichte und Zukunft der Informationstechnik und nutzen Sie die Gelegenheit zum Austausch mit Expertinnen und Experten mit Unternehmerinnen und Unternehmern aus Akademia und Industrie.

Zu dem Programmablauf gehören auch die Preisverleihungen sowie die Ehrungen der ITG und das Netzwerken mit einer großen Anzahl aus prominenten Gästen aus Wissenschaft, Politik und Industrie.

PARTICIPATION

1st ITG Future Forum on AI-powered Networks and Networking for AI Systems Bridging AI and Networking

The ITG is launching its first ITG Future Forum to foster interdisciplinary dialogue, taking place on

November 25th at the Fraunhofer HHI Institute, Einsteinufer 37, Berlin the day after the VDE Hauptstadtforum.

This one-day event will unite ITG communities to explore the intersection of AI and networking, addressing how AI reshapes network design and operations while demanding robust networking for distributed training, real-time inference, and autonomous systems. Under the theme »AI-Powered Networks and Networking for AI Systems«, the forum will feature keynotes, panel discussions, workshops, and a demo zone.

Key topics include:

- » AI-native network architectures
- » Data-driven network automation
- » Edge and cloud intelligence for communication systems
- » Networking challenges for AI workloads
- » AI robustness, security, and trust in network

Join us to shape the future of interdisciplinary collaboration and register here:



INFOS UND ANMELDUNG
www.vde.com/networking-ai

EINLADUNG

Mitgliederversammlung 2026 der Informationstechnischen Gesellschaft im VDE e.V.

24.11.26, 16–17 Uhr

(vor dem VDE Hauptstadtforum)

**Berlin-Brandenburgische
Akademie der Wissenschaften,
Gendarmenmarkt, 10117 Berlin
Eingang Markgrafenstraße 38**

Aufruf für den Johann-Philipp-Reis-Preis 2027

Das 125-jährige Jubiläum der erstmaligen Präsentation seiner genialen Idee haben die Stadt Friedrichsdorf, die Barbarossa-Stadt Gelnhausen, die Deutsche Telekom und der VDE Verband zum Anlass genommen, einen mit 10.000 Euro dotierten Preis für eine herausragende, innovative Veröffentlichung auf dem Gebiet der Informationstechnik zu vergeben. Der 1987 erstmalig verliehene Preis wird seither alle 2 Jahre vergeben. Auch 2027 soll der Preis wieder an Ingenieurinnen und Ingenieure oder Naturwissenschaftlerinnen und Naturwissenschaftler (Altersgrenze 40 Jahre) verliehen werden, die mit ihrer Arbeit eine bedeutende informationstechnische Neuerung, die auch Auswirkungen auf die Volkswirtschaft hat, in Gang gesetzt haben bzw. eine solche Entwicklung erwarten lassen. Der VDE ITG Vorstand bittet, Vorschläge für den Johann-Philipp-Reis-Preis 2027 spätestens bis zum **15. April 2027** elektronisch einzureichen: www.vde.com/itg-jpr-preis

Aufruf für den VDE ITG Studienpreis 2027

Die ITG im VDE e.V. schreibt den VDE ITG Studienpreis aus. Nominierungen sind herzlich willkommen. Für herausragende Master und Diplomarbeiten der Informationstechnik einschließlich Studienleistungen und weiterem Engagement für das Fachgebiet wird der VDE ITG Studienpreis an junge Wissenschaftlerinnen und Wissenschaftler jährlich verliehen. Besonderer Wert wird bei der Beurteilung der Arbeiten auf Originalität, die theoretische und praktische Behandlung des Themas, die Darstellungsweise und Form sowie die Bedeutung der Arbeit gelegt. Die Bewerbenden sollen zum Zeitpunkt des Studienabschlusses nicht älter als 28 Jahre sein. Ausnahmen sind in besonderen Fällen möglich, können aber nur berücksichtigt werden, wenn sie bei der Antragstellung stichhaltig begründet wurden. Der VDE ITG Studienpreis ist verbunden mit einer Geldprämie von 500 EUR, einer einjährigen beitragsfreien Mitgliedschaft in der VDE ITG, einer beitragsfreien Teilnahme an einer VDE ITG Tagung und einer Urkunde. Stichtag: **16. April 2027**

Aufruf für den VDE ITG Dissertationspreis 2027

Seit 1994 verleiht die Informationstechnische Gesellschaft im VDE (ITG) jährlich bis zu drei Dissertationspreise. Mit diesem Preis werden besonders herausragende Dissertationen junger Wissenschaftlerinnen und Wissenschaftler sowie Ingenieurinnen und Ingenieure auf dem Gebiet der Informationstechnik gewürdigt. Die Bewerberinnen und Bewerber müssen der VDE ITG spätestens zum Zeitpunkt der Einreichung angehören. Jeder Preis ist mit einer Geldprämie von 2.000 EUR sowie einer Urkunde verbunden. Einsendeschluss ist der **11. März 2027**.

Aufruf für den VDE ITG Preis 2027

Seit dem Jahr 1956 wird der Preis der VDE ITG für besonders hervorragende Publikationen auf dem Gebiet der Informationstechnik an Wissenschaftlerinnen und Wissenschaftler sowie Ingenieurinnen und Ingenieure verliehen. Jeder Preis ist mit einer Gesamtpremie von 3.000 EUR sowie einer Urkunde verbunden. Die VDE ITG Geschäftsstelle bittet um elektronische Einreichung der Unterlagen. Einsendeschluss ist der **11. März 2027**.

Weitere Informationen und Einzelheiten zu den verschiedenen Preisen der VDE ITG finden Sie unter www.vde.com/itgpreise



pickablu®

Ihre Meinung ist gefragt!

Das Layout der ITG News hat sich verändert. Wie zufrieden sind Sie damit? Und möchten sie das Magazin lieber gedruckt in den Händen halten oder digital am Bildschirm lesen? **Ihre Rückmeldung ist uns als Editoren besonders wichtig.** So können wir gemeinsam die ITG News weiterentwickeln und Ihren Erwartungen gerecht werden. Die Umfrage umfasst nur zwei Fragen und ist schnell beantwortet. **Bitte den QR-Code scannen oder darauf klicken.** Es werden keine persönlichen Daten erhoben oder gespeichert. <https://flow.pickablu.de/r/154>



KOLUMNE

Drei Fragen an SARAH KOOP-BRINKMANN

DAMIAN DUDEK Drehen wir an der »Zeitskala« und gehen zurück in die 1990-Jahre, denn in dieser Zeit galt das Schnurlostelefon und das Walkie-Talkie als die gängigen Anwendungen der Funktechnik in der Gesellschaft. Durch die Miniaturisierung elektronischer Bauelemente, eben nicht nur von Transistoren, sondern von Filtern, Induktivitäten, Kapazitäten aber auch Dioden, in Silizium vollzog sich ein Wandel getrieben aus der Forschung der Hochfrequenztechnik in die Anwendung. Allen voran der Mobilfunk für den Massenmarkt. Sie, Frau Koop-Brinkmann, haben Ihre Masterarbeit im Themenbereich der CMOS-Hochfrequenztechnik, also für integrierte Schaltungen für Mikrowellen geschrieben. Ein überaus aktueller Bereich aus wissenschaftlicher, aber auch wirtschaftlicher Perspektive. Wie kamen Sie zu diesem Themenbereich und was interessiert Sie an der Mikroelektronik insbesondere der Schaltungstechnik im Hochfrequenzbereich? Diese Frage stelle ich Ihnen vor dem Hintergrund der doch wenigen Studierenden in diesem Feld und auch mit der Intention mehr Sichtbarkeit für das Fachgebiet zu gewinnen.

SARAH KOOP-BRINKMANN Ich kann ehrlich sagen, dass ich diesen Weg selbst nicht vorhergesehen habe. Mein großes Interesse an Mathematik und insbesondere an Physik lenkte meinen Blick nach dem Abitur sowohl auf die Ingenieur- als

auch auf die Naturwissenschaften. Für mich stand früh fest, dass ich entweder Physik oder Elektrotechnik studieren wollte, da mich vor allem die elektromagnetische Feldtheorie faszinierte. Die TU Braunschweig sprach mich besonders an, weil sie Elektrotechnik und Physik in einer gemeinsamen Fakultät vereint und damit einen engen fachlichen Austausch ermöglicht. Während des Bachelorstudiums erhielt ich Einblicke in viele unterschiedliche Bereiche der Elektrotechnik. Neben der elektromagnetischen Feldtheorie entwickelte ich dabei auch große Freude an der Netzwerkanalyse und Schaltungstechnik. Meine Entscheidung, mich auf die Hochfrequenzschaltungstechnik zu spezialisieren, verfestigte sich schließlich durch das Modul »Analoge integrierte Schaltungen«. Dort wurden die theoretischen Grundlagen mit einer praktischen Entwurfsübung verbunden. Wir entwickelten beispielsweise einen Low-Noise Amplifier und einen spannungsgesteuerten Oszillator mit der Simulationssoftware »Advanced Design System« (ADS), fertigten erste Layouts an und führten elektromagnetische Simulationen durch. Diese Verbindung von Theorie und Praxis hat mich letztlich überzeugt. Gerade zu Beginn ist ein Ingenieurstudium stark von theoretischen Grundlagen geprägt. Erst wenn man selbst in Simulationen untersucht, wie sich eine Schaltung verhält und welchen Einfluss einzelne Entwurfsparameter haben, entwickelt man ein tieferes Verständnis für ihre Funktionsweise. Heute fasziniert mich besonders die Vielfalt des Schaltungsentwurfs. Der Entwurfsprozess unterscheidet sich stark abhängig von der jeweiligen Schaltung und ihrem Frequenzbereich und bietet viel Raum für eigene Ideen und kreative Lösungsansätze. Besonders spannend ist der Moment, wenn eine gefertigte Schaltung zurückkommt und erstmals vermessen wird. Die zuvor nur simulierten Signale dann zum Beispiel auf einem Spektrumanalysator zu sehen, ist für mich jedes Mal etwas Besonderes. Eine außergewöhnliche Chance war es für mich, bereits während meines Bachelorstudiums unter der Betreuung von Prof. Issakov ein Industriepraktikum bei Infineon in Villach zu absolvieren. Dort entwarf ich meine erste integrierte Schaltung in 28nm CMOS Technologie. Im Rahmen meiner anschließenden Bachelorarbeit am Institut für CMOS Design an der TU Braunschweig folgte eine weitere Schaltung in 22nm FDSOI CMOS. Beide Schaltungen konnte ich später in Messungen charakterisieren und die Ergebnisse veröffentlichen (RFIC 2024, TCAS-II 2026). Schon im Bachelorstudium den gesamten Weg vom Entwurf über die Fertigung bis zur Messung und Veröffentlichung erleben zu dürfen, ist außergewöhnlich. Für diese frühe Förderung bin ich sehr dankbar. Darüber hinaus begeistert mich, dass sich mit dem Schaltungsentwurf komplexe Systeme auf kleinster Fläche realisieren lassen und Innovationen entstehen, die nahezu alle Bereiche unseres täglichen Lebens beeinflussen.

DAMIAN DUDEK Wenn Sie sich nicht gerade in Ihrem professionellen Umfeld befinden, so würde mich interessieren, wie reagieren Personen aus Ihrer Familie, Freunde oder auch diejenigen, die Sie neu kennenlernen darauf, wenn Sie von Ihrer Tätigkeit berichten? Sehen Sie hier

Zusammenhänge zu dem allgemeinen Trend, dass nicht nur in der deutschen Gesellschaft Verdrossenheit gegenüber der Informations- und Elektrotechnik oder sogar gegenüber Technik vorliegt? Es ist immer schwer aus eigenen subjektiven Eindrücken einen Trend abzuleiten, doch durch Analysen und Umfragen lässt sich belegen, dass die Sichtbarkeit und das Verständnis daran, welche Themenfelder in die Informationstechnik fallen, in der Allgemeinheit stark davon abweichen, wie die alltägliche Arbeitswelt in der Elektro- und Informationstechnik aussieht. Sehen Sie sich als Rolemodel, also als Vorbild und unabhängig davon was empfehlen Sie, um die Sichtbarkeit und die aktuellen Themenfelder der Elektro- und Informationstechnik in der Gesellschaft sichtbarer zu machen?

SARAH KOOP-BRINKMANN Einen allgemeinen gesellschaftlichen Trend kann ich aus meinen persönlichen Erfahrungen nur schwer ableiten, da ich in einem technisch geprägten Umfeld aufgewachsen bin. Meine Eltern führen ein Familienunternehmen in dritter Generation im Bereich der Haustechnik. Technikbegeisterung und die Offenheit gegenüber Innovationen gehörten daher schon früh zu meinem Alltag. Auch mein Freundeskreis, der sich durch mein Studium an der Technischen Universität Braunschweig stark aus Studierenden der Ingenieur- und Naturwissenschaften zusammensetzte, repräsentiert die breite Gesellschaft nicht. Ich beobachte allerdings, dass das allgemeine Verständnis stark vom jeweiligen Teilgebiet der Elektro- und Informationstechnik abhängt. Allgegenwärtige Themen wie Elektromobilität, Energiewende oder der Ausbau des Mobilfunks sind den meisten Menschen bekannt. Dazu haben viele bereits eine Vorstellung und häufig auch eine klare Meinung. Wenn ich auf die Frage »Was machst du eigentlich?« hingehen mit Begriffen wie »Chipdesign« oder »Mikrowellenschaltungstechnik« antworte, stoße ich häufig zunächst auf Unwissenheit. Dabei nehme ich weniger eine grundsätzliche Technikverdrossenheit als vielmehr Berührungsängste gegenüber einem vermeintlich sehr komplexen Fachgebiet wahr. Aussagen wie »das verstehe ich sowieso nicht« beenden das Gespräch manchmal, bevor eine eigentliche Erklärung beginnen kann. Das ist schade, denn die grundlegenden Zusammenhänge und insbesondere die Bedeutung dieser Technologien im Alltag lassen sich durchaus anschaulich vermitteln. Ich selbst würde mich nicht ausdrücklich als Vorbild bezeichnen. Ich würde mir jedoch insbesondere von Studierenden und Studienanfängerinnen und Studienanfängern wünschen, dass sie sich nicht von scheinbar komplexen Zusammenhängen oder vermeintlich schwierigen Themenfeldern abschrecken lassen. Ich bin sehr froh, mich für den Hochfrequenzschaltungsentwurf entschieden zu haben und hoffe, durch meine Begeisterung auch andere dazu zu motivieren, diesen Weg für sich in Betracht zu ziehen. Um die Sichtbarkeit der Mikroelektronik zu erhöhen, sollte deutlicher vermittelt werden, welche zentrale Bedeutung Halbleiter und integrierte Schaltungen für nahezu alle Bereiche unseres Alltags haben – vom Smartphone über das Automobil und die Medizintechnik bis zur Energieversorgung und Kommunikation. Einen positiven

Trend sehe ich beispielsweise in der zunehmenden medialen Berichterstattung über »Silicon Saxony« und die in Deutschland ansässige Halbleiterindustrie. Entscheidend ist dabei, nicht nur über wirtschaftliche Investitionen und Produktionsstandorte zu berichten, sondern auch verständlich zu zeigen, welche Technologien dort entwickelt werden und welche Menschen dahinterstehen.

DAMIAN DUDEK Der vergangene Karrierewege ist aus mancher Retrospektive nicht immer geradlinig, was sicherlich gut aber auch für einige enttäuschend ist. Eine Karriere in der Elektrotechnik anzugehen ist doch gerade in diesen unsicheren Zeiten und der Berichterstattung durch die Presse unattraktiv. Die deutsche Wirtschaft schwächelt, insbesondere verschieben sich die lukrativen technischen Bereiche immer mehr aus dem gesetzten Maschinen- und Anlagenbau, wie dem Automobilmarkt zunehmend in Richtung Elektrifizierung des alltäglichen Lebens. Damit kommen neue Geschäftsbereiche auf, die ein Umdenken erfordern und die konservativen Branchen, gerade in der Technik ablösen oder diese zur Modernisierung zwingen. Nicht selten kommen Nachrichten, dass etablierte deutschen Firmen Stellen abbauen oder diese wirtschaftlich in eine Notlage geraten. Dabei ist doch gerade dieser Wandel von den bisher eher eingefahrenen klassischen technischen Geschäftsbereichen zu mehr Elektrifizierung in der Mobilität, der Energieerzeugung, des Transports der Informationstechnik eine hervorragende Gelegenheit die Elektrotechnik für uns alle so zu gestalten, dass wir davon profitieren. Wie bewerten Sie vor diesem Hintergrund die wirtschaftliche Lage, in der wir uns derzeit befinden und wie schätzen Sie das Potential, das wir mit den Ansätzen aus Forschung und Entwicklung haben, einen Aufschwung zu erreichen? Daraus abgeleitet: Lohnt es sich Elektrotechnik zu studieren?

SARAH KOOP-BRINKMANN Ich nehme meine Antwort vorweg: Ja, gerade jetzt lohnt es sich, Elektrotechnik zu studieren. Das Studium vermittelt ein umfassendes theoretisches und technisches Verständnis und bildet genau jene Fachkräfte aus, die für die zunehmende Elektrifizierung nahezu aller Wirtschaftsbereiche benötigt werden. Ob Forschung und Entwicklung zu einem wirtschaftlichen Aufschwung beitragen können, hängt maßgeblich davon ab, ob ausreichend qualifizierte Fachkräfte zur Verfügung stehen und sie in Deutschland die notwendigen Bedingungen für Innovation vorfinden. Die gegenwärtige wirtschaftliche Schwäche sollte daher als Weckruf verstanden werden, neue Technologien konsequenter zu fördern. Andernfalls werden motivierte Fachkräfte ihre Ideen dort umsetzen, wo ihnen bessere Möglichkeiten geboten werden. ●

SARAH KOOP-BRINKMANN ist Mitarbeiterin mit Masterabschluss am Institut für CMOS Design an der Fakultät für Elektrotechnik, Informationstechnik und Physik der Technischen Universität Braunschweig.

DR.-ING. DAMIAN DUDEK ist Geschäftsführer der Informations-technischen Gesellschaft im VDE e.V. und stellte die Fragen.

Mission Critical THEMA Networks

Hochverfügbare Netze als Basis der digitalen und elektrischen Infrastruktur mit spezifischen Diensten für sicherheitskritische Anwendungen.

Das Leben in unserer digitalisierten Welt ist ohne leistungsfähige, zuverlässige Kommunikationsnetze nicht mehr vorstellbar. Sicherheitskritische Anwendungsfelder benötigen Dienste, die von den öffentlichen Kommunikationsnetzen nicht bereitgestellt werden können - zum Beispiel stellen industrielle Produktion, der Betrieb von Stromnetzen oder Eisenbahnen, Polizei, Feuerwehr und Rettungskräfte, oder das Militär jeweils besondere Anforderungen. Netzabdeckung, Sonderfunktionen, Hochverfügbarkeit und Schutzniveau gegenüber Störungen und Bedrohungen bedingen die Nutzung von einsatzkritischen Netzen (»Mission Critical Networks«). Sie werden – soweit möglich unter Nutzung kommerziell verfügbarer Technik – speziell für ihre Anwendungsfelder geplant, realisiert und betrieben, sodass die erforderlichen Kommunikationsdienste Ende-zu-Ende mit größtmöglicher Zuverlässigkeit und teils über Jahrzehnte hinweg zur Verfügung stehen. Das Schwerpunktthema dieser Ausgabe der ITG News sind Beispiele aus Forschung, Entwicklung und Betrieb von modernen einsatzkritischen Netzen in unterschiedlichen Anwendungsszenarien. Einige ausgewählte Themen von bekannten Experten der Informationstechnik präsentieren wir Ihnen hier als Überblick und sind gespannt auf Ihre Einschätzung dazu.

Overview of Mission-Critical Networks

- H. DE MEER, University of Passau, Chair of Computer Networks and Computer Communication
- E. GOLLER, University of Passau, Chair of Computer Networks and Computer Communications

The Critical Communications Association (TCCA) defines mission-critical networks as national networks that are primarily meant to enable communications for emergency services like fire brigades, police, rescue and ambulances [27]. As TCCA points out, mission-critical networks play an essential role beyond emergency services and includes other domains, where communication failures could cause severe service degradations. This includes domains like utilities, transportation, critical industries and critical infrastructure [26,27].

Traditionally, the networks used in mission-critical communications have been Land Mobile Radio systems like TETRA or GSM-R, which are typically narrowband networks [29, 31]. However, operators are now integrating or even transitioning to the mission critical services (MCX services) defined by the 3rd Generation Partnership Project (3GPP), which are carried by 5G and LTE [1, 26, 29]. The 3GPP network ecosystem is shown in Figure 1.

This article provides an overview of mission-critical networks and focuses on the MCX platforms provided

via LTE and 5G, since broadband is considered the future of mission-critical networks [26]. First, an overview of domains where mission-critical networks are essential and of the networks used is provided. Second, the MCX services defined by 3GPP alongside their requirements are discussed. Third, some common engineering practices for mission-critical networks are outlined. Lastly, the article highlights two examples of mission-critical networks: TETRA as an example of legacy narrowband networks and 5G as a bearer for MCX services.

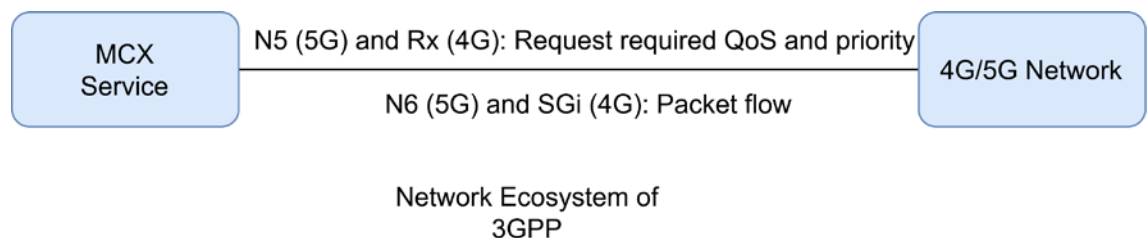


FIGURE 1

Depiction of the 3GPP Network Ecosystem for MCX services based on [31]

Mission Critical Networks

THEMA

08
09

VDE ITG news 10/2026

Where Mission-Critical Communications are Used

Mission-critical communications are relevant in a wide range of domains. *Table 1* provides an overview of some common mission-critical networks. *Table 2* provides an overview of domains where mission-critical communications are used and over which mission-critical networks they are realized.

In Germany BDBOS, the Federal Agency for Public Safety Digital Radio, operates the Public Safety Digital Radio in cooperation with the federal government and the federal states [1, 19]. The network is used in the context of public safety by police, fire brigades, disaster and civil protection authorities [1]. In addition, it is utilized by the Federal Office for the Protection of the Constitution, the Federal Customs Administration and by the German Armed Forces, where it enables communications in search-and-rescue units, medical services and the military police. The Public Safety Digital Radio provides group communications, where

messages are sent to all group members [1]. It further provides emergency calls that have priority over other communications. Additionally, it offers short data services for sending status updates, short messages or GPS data.

In the maritime domain, mission-critical communications are used in the context of navigation and fleet management [36]. The standardized MCX services further mention maritime safety applications [5].

In aviation, the South American Region Digital Network (REDDIG) exists. Participating countries use this network for mission-critical operational aeronautical communications [37]. Moreover, 3GPP mentions the use of MCX services for air-ground-air communication [38]. For example, in rescue, real-time communication with helicopters is required. 3GPP further defines specific requirements for the maximum height and speed up to which communications must be supported.

In railways, the Future Railway Mobile Communication System (FRMCS) enables operational communication between ground users and drivers, while also allowing for emergency communications with higher priority [40].

For smart grids, mission-critical machine-to-machine communication is used [41]. These communications assert strict requirements: for communications in real-time system protection, high requirements for latency and reliability must be met. For smart meter communications, a large number of communication devices must be supported.

Shared requirements for Mission-Critical Services Across Domains

3GPP defines a common functional architecture for MCX services alongside additional specifications for specific mission-critical services: push to talk (MCPTT), video (MCVideo) and data (MCData) [3]. These services have their own set of requirements. In fact, 3GPP defines mission criticality via requirements such as high availability and reliability, low latency for setup and transport as well as the capability to support a large number of users. Furthermore, strong security must be guaranteed, and priority and pre-emption handling must be supported. This shows that best-effort forwarding is insufficient for mission-critical communication: while best-effort forwarding implies that packets may be lost, arrive out of order, be duplicated or experience delays, 3GPP sets specific requirements for mission-critical services that must be fulfilled [3, 4]. In the following, these requirements are discussed: first for normal conditions, then for emergencies.

In non-emergency use, 3GPP requires specific performance indicators to be met [5]. For MCPTT audio calls, 3GPP defines requirements regarding, for example, access time and mouth-to-ear latency [5].

NETWORK	PROPERTIES AND TECHNOLOGIES
TETRA	Terrestrial trunked radio network that supports voice and data transmission, typically narrowband but can be a wideband. [28, 30, 31]
3GPP MCX services over 5G/LTE	Broadband 5G/LTE mobile network for providing 3GPP MCX. The underlying network infrastructure for MCX services can be public or private. [15, 31]
Global System for Mobile Communications – Railway (GSM-R)	Narrowband 2G network designed for railway communications. It supports, for example, text messages and emergency calls for railways. [29, 33, 42]
Future Railway Mobile Communication System (FRMCS)	Uses 5G core and access networks and provides voice/data communication services for railway applications via 3GPP MCX services. [43]
Industrial/private 5G Non-Public Network (NPN)	Private 5G campus or factory networks that can be integrated with a public network or be a non-public network. [17] In Germany, a dedicated spectrum for campus networks is available. [34]
REDDIG	Network used in the South American region for mission-critical communication in aviation. [37] REDDIG III is the current version. [18]
450LTE	Nationwide broadband LTE network for Germany that uses the 450 MHz range. Supports 3GPP MCX services and provides communication for utilities, transport and public institutions. [14]
Power Line Carrier (PLC)	Transmission system operators communicate via a dedicated network, which may employ power line carrier. Transmission happens over high-voltage conductors. [32]
Optical Ground Wire (OPGW)	Optical ground wire is an overhead-line ground wire with integrated optical fibre. It is an alternative to power line carrier communication. [25, 32]

TABLE 1
Overview of common mission-critical networks.

DOMAIN	USE OF MISSION-CRITICAL COMMUNICATIONS	NETWORKS
Public Safety	USERS Police, fire brigades, civil protection, emergency medical and rescue services ^[1] USE Operational voice and incident coordination ^[1]	TETRA ^[1] , 3GPP MCX services over LTE/5G ^[1]
Railway	USERS Train drivers, dispatchers, controllers, shunting teams and railway operations and maintenance staff ^[42] USE Emergency and group communication, train-control data ^[42]	GSM-R ^[42] , FRMCS ^[43]
Maritime	USERS Rescue-control and rescue units ^[44] USE Rescue units on sea communicate with safe organizations on land, navigation and fleet management ^[36,44]	3GPP MCX services over LTE/5G ^[12] , TETRA ^[44]
Aviation	USERS Airport operators, users in helicopter/aircraft and their ground teams in operations, traffic controller operators, air traffic services ^[3, 35, 37] USE Reliable airport operations, real-time air-ground-air communication, coordination for search-and-rescue centers as well as air traffic between operators in neighboring control centers, aeronautical information ^[3, 35, 37]	TETRA ^[35] , 3GPP MCX services over LTE/5G ^[3] , REDDIG ^[37]
Power /Smart Grid	USERS Transmission system operators ^[32] USE Voice, data, relay protection signals, real-time system protection and smart meter communication ^[32, 41]	Network using OPGW or PLC ^[25, 32] , LTE450/450 connect ^[14]
Utilities	USERS Users in utilities like energy and water suppliers ^[14] USE Grid monitoring/control, smart-grid connectivity and resilient operational/crisis voice, control commands in water supply systems, reading meters for wastewater ^[14]	LTE450/450 connect ^[14] , TETRA ^[23]
Industrial Applications	USERS Industrial and commercial users ^[21, 23] USE Closed-loop control, monitoring of processes, maintenance, remote access ^[21]	TETRA ^[23] , 5G Non-Public Network ^[21]
Military	USERS Staff in medical/rescue, search-and-rescue units, military police ^[1] USE Blue-light functions ^[1]	TETRA ^[1, 23]

TABLE 2

Overview of relevant domains where mission-critical communication is used. Some selected examples of users and uses are given.

These requirements also give services a level of predictability. For example, MCVideo requires urgent real-time video to start within 2 s of the request and reach communication partners for non-urgent priority video [12].

But what happens to these targets when the network is congested or resources are sparse while an emergency requires urgent communication?

In case traffic load exceeds 70 % of the capacity of each network node, the performance indicators for MCPTT are no longer a hard requirement [5]. Instead, certain communications must be prioritized. The specifications define ways to protect high-priority users by employing access control, admission control, scheduling control, and pre-emption of lower-priority traffic [3]. A pre-emption hierarchy is created to prioritize communications with pre-emption permissions. Queuing and retention by priority must also be supported. The priority assigned to a communication is determined by attributes associated with a user and the service group.

Beyond congestion, the available resources can also become too sparse when the network is in a degraded state. 3GPP considers the backhaul, which is the link from a base station to the central core, to be in one of four potential states: normal, limited, signaling-only and none [13]. Where a limited backhaul exists, the isolated network must be able to use it for exchanging control plane signaling with the core and can use it for user plane data exchange. For user data, no expectations for QoS are promised.

For emergencies, additional requirements exist: while ordinary group calls must connect within 300 ms on 95 % of attempts, an emergency or imminent-peril group call must reach this target in 99 % of attempts [5]. Additionally, emergency communications have priority over other communication types [3]. For MCVideo, the video must reach the other communication partners in 1 s once the communication has started, compared to 10 s for non-urgent video [12].

Important Characteristics of Mission-Critical Services

Four important characteristics of mission-critical services are availability, reliability, dependability, and resilience. Two of these characteristics are named directly in the 3GPP requirements: high availability and high reliability [3]. In this context, availability means the service is there when the user asks for it [3, 9]. Reliability means the service works until it is no longer needed once it has started [3, 9]. A mission-critical service must also be dependable, where dependability is the »ability to deliver service that can justifiably be trusted« [9]. It must also be resilient. Resilience, defined as »the persistence of dependability when facing changes« [24], implies that a mission-critical network must remain dependable not only under faults, but under change more broadly. These changes can be classified by their prospect, timing and nature [24]. Examples in mission-critical networks include an increasing number of users, a shift toward real-time services and the integration of legacy networks with 5G systems. In the following, engineering principles to ensure that the underlying mission-critical network meets the requirements for availability, reliability, dependability and resilience are discussed.

Engineering Principles of Mission-Critical Networks

Users of mission-critical communications expect that a service is available even during major incidents, extreme weather or other crises [11]. Consequently, commercial networks are insufficient: according to TCCA, commercial mobile networks cannot provide the coverage, capacity, availability and reliability expected for critical operations [26]. According to BDBOS, the Public Safety Digital Radio shows much higher availability than commercial mobile networks [1].

A mission-critical network requires redundancies and should avoid a single point of failure [7]. In addition, fallbacks to ensure communication between key base stations as well as backup power are required. The Public Safety Digital Radio, for example, uses redundant uninterruptible power supplies and redundant emergency generators for the central switching centers [1]. BDBOS further uses mobile base stations that allow users to access the network via satellite links, for which they have two redundant switching centers [19]. In fact, low Earth orbit satellites have been shown to enhance communication resilience when used in addition to terrestrial ICT [39]. They help improve connectivity, end-to-end delays and system reliability. In power grids, low Earth orbit satellites can be used in addition to terrestrial networks for communication between a control center and nodes of the power grid like substations [39]. 3GPP describes satellites to access

MCX services [15]. TCCA describes the broad coverage provide by satellites and emergency communication through direct-to-device technologies as particularly relevant [16]. Using satellite communication as a backup communication path is an example of diversifying communication paths and thereby increasing resilience.

Operating a dedicated network also ensures exclusivity, where only mission-critical users can access and use the network. For example, the Public Safety Digital Radio is used by approximately 300,000 people and achieves availability of 99,98 % [1]. Exclusivity can also be reflected in the use of a dedicated radio spectrum. For example, 450connect uses the 450 MHz frequency band to provide crisis-resistant communication [14]. In 5G, it can also mean isolating MCX services and their traffic from other services [20]: network slicing is the concept of slicing physical networks into isolated logical ones [22]. Users, devices and applications can be placed in a separate slice than other traffic [15]. Each session is tied to one slice and receives dedicated transmission capacity [15]. 3GPP points out that network slicing also entails that transport resources are virtualized [20]. Virtualization can improve network resilience: when failures occur, software-based network functions can be moved from failing nodes to operational ones [10]. These functions can be deployed across geographically dispersed data centers, which helps recovery as a failed virtual instance can be restored from identical images.

Virtualization also introduce challenges, particularly when the infrastructure is hosted on a third-party cloud or when software-related failures occur [10]. A TCCA white paper on cybersecurity identifies several components that must be protected in broadband mission-critical networks [8]. This includes the radio access network, the core, the providers of mission-critical services, applications, devices, device management and SIM cards. In this context, TCCA singles out the supply chain as a potential vulnerability since various components from different vendors are involved. They advise accounting for the risk of supply chain attacks as part of the overall security planning. For government authorities, TCCA advises protecting against jamming and interference and complying with ISO 27001, which describes eavesdropping, interception, masquerading, manipulation, replay and traffic analysis [7]. In addition, TCCA states that infrastructure assets must be secured physically via measure like CCTV and intruder alarms. If the network is used for both mission-critical and non-mission-critical communications, both must be isolated to ensure that staff taking care of the general network cannot access mission-critical communication [7]. In the context of TETRA, TCCA also mentions that cryptographic keys should be changed routinely [6].

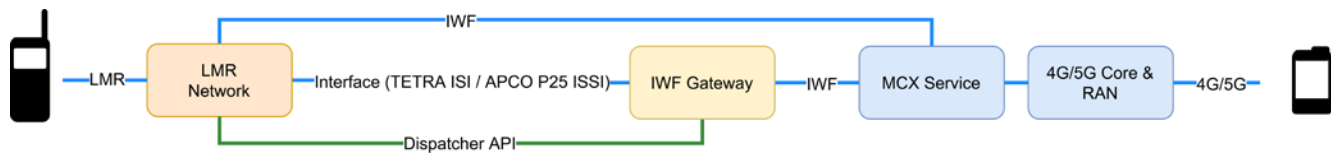


FIGURE 2

Depiction of three possible architectures to integrate LMR with MCX services based on [31]

TETRA - A Land Mobile Radio Network

TETRA, short for Terrestrial Trunked Radio, provides a standardized communications architecture that supports individual, group and broadcast calls, short messages and packet data and has been used for narrowband networks [30, 31]. The standard by the European Telecommunications Standards Institute (ETSI) defines TETRA [30]: TETRA uses a trunked design, which means that radio channels are shared and only assigned when they are needed. Its Medium Access Control layer manages radio-channel access and radio resources. Base stations provide cellular coverage. The TETRA Switching and Management Infrastructure sets up and manages calls, releases them and handles the network side of registration and authentication. It also provides supplementary services such as priority calls.

The Public Safety Digital Radio is one example of a network based on the TETRA standard and is the largest TETRA radio network [1]. The network covers 99.2 % of Germany with 5,000 base stations and it can handle large-scale operations of thousands of devices.

Many operators are now gradually replacing narrowband Land Mobile Radio (LMR) networks with broadband MCX platforms served via 5G and LTE [29]. The transition to MCX services is expected to be a multi-year process, which is why the Interworking Function (IWF) has been defined by 3GPP. It allows both systems to interoperate. Figure 2 illustrates three different architectures the TCCA suggests for the integration of LMR and MCX networks [31]: via native integration that adds support for the Interworking Function directly into the network infrastructure of LMR, via an interface-based architecture where an interface of the LMR network is used to connect to a gateway or by using an API that is offered by the LMR vendor.

Mission-Critical Communication via 5G

The transition from narrowband to broadband is driven by the demand to send high volume data and larger files, which enables new possibilities such as broadcasting live video and sharing maps [26]. 3GPP provides a specification that connects the MCX services to the 5G system and defines a common functional architecture [15]. It distinguishes two planes: the application plane and the signaling control plane. The application plane encompasses the functions responsible for delivering the mission-critical service. The signaling control plane associates users in a session, provides access to services, controls them

and relies on session connectivity provided by the 5G system.

To prioritize emergency calls, the 5G system's support for quality of service (QoS) is utilized. Packets that must be handled identically are grouped as QoS flows and marked with an identifier. This identifier is associated with the allowed delays and error rates for packets of this flow and what priority these packets should receive. 3GPP specifies the identifiers that should be used for mission-critical push to talk, video and data. In addition, the Allocation Retentions Priority defines a priority level that helps decide whether a new QoS flow should be declined in case the network is congested.

Conclusions

Mission-critical networks and services are deployed across a wide range of domains, yet they share common requirements they must adhere to. These include high availability, high reliability, dependability and resilience. Users must be able to rely on them during crises and emergency situations. Hence, engineering mission-critical networks requires its own set of principles. Redundancies, multiple communication paths, security aspects as well as virtualization techniques should be considered. While mission-critical networks have traditionally been narrowband networks, there is a transition toward broadband networks that support 3GPP's MCX services. Hence, new challenges arise, such as the need to withstand potential supply chain attacks. Above all, however, it means new possibilities and the potential for strengthening resilience through the integration of technologies like low Earth orbit satellites. ●

References

- [1] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, »Wir sind die Netzbetreiberin des Bundes,« BDBOS. Accessed: Aug. 8, 2026. [Online]. Available: https://www.bdbos.bund.de/DE/Home/home_node.html
- [2] European Telecommunications Standards Institute, LTE; 5G; Security of the Mission Critical (MC) service (3GPP TS 33.180 version 19.4.0 Release 19), ETSI TS 133 180 V19.4.0, Feb. 2026.
- [3] European Telecommunications Standards Institute, LTE; 5G; Mission Critical Services Common Requirements (MCCoRe); Stage 1, ETSI TS 122 280 V19.7.0, 3GPP TS 22.280 version 19.7.0 Release 19, Jan. 2026.
- [4] J. Babiarz, K. Chan and F. Baker, »Configuration Guidelines for DiffServ Service Classes,« RFC 4594, Aug. 2006, doi: 10.17487/RFC4594. Accessed: Jul. 23, 2026. [Online]. Available: <https://www.rfc-editor.org/info/rfc4594/>
- [5] European Telecommunications Standards Institute, LTE; 5G; Mission Critical Push to Talk (MCPTT); Stage 1 (3GPP TS 22.179 version 19.3.0 Release 19), ETSI TS 122 179 V19.3.0, Jan. 2026.

- [6] TCCA Security and Fraud Prevention Group, Maintaining TETRA Security, TCCA White Paper, Mar. 2020.
- [7] TCCA Critical Communications Broadband Group – Strategic Case Group, Considerations for Government Authorities when they are planning to acquire Mission Critical Mobile Broadband Services, ver. 1.01, TCCA White Paper, Dec. 10, 2015.
- [8] TCCA's Cybersecurity Task Force, Cybersecurity in Critical Communications: An initial overview, TCCA White Paper, Apr. 2026.
- [9] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, »Basic concepts and taxonomy of dependable and secure computing,« in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, Jan.–March 2004, doi: 10.1109/TDSC.2004.2.
- [10] European Telecommunications Standards Institute, Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness, ETSI TR 102 445 V1.2.1, Apr. 2023.
- [11] TCCA Critical Communications Broadband Group, Critical Communications and Mobile Network Operators: Options for new revenue streams and new market segments, TCCA White Paper, May 2018.
- [12] European Telecommunications Standards Institute, LTE; 5G; Mission Critical (MC) video (3GPP TS 22.281 version 19.0.0 Release 19), ETSI TS 122 281 V19.0.0, Oct. 2025.
- [13] European Telecommunications Standards Institute, Universal Mobile Telecommunications System (UMTS); LTE; Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1 (3GPP TS 22.346 version 19.0.0 Release 19), ETSI TS 122 346 V19.0.0, Oct. 2025.
- [14] 450connect GmbH, »Ausfallsichere Kommunikation für kritische Infrastrukturen,« 450connect. Accessed: Aug. 7, 2026. [Online]. Available: <https://www.450connect.de>
- [15] European Telecommunications Standards Institute, 5G; Mission Critical Services over 5G System; Stage 2 (3GPP TS 23.289 version 18.8.0 Release 18), ETSI TS 123 289 V18.8.0, Apr. 2024.
- [16] TCCA Critical Communications Broadband Group, Mission-Critical High Power User Equipment Market Survey Results, TCCA White Paper, Sep. 2024.
- [17] 5G Alliance for Connected Industries and Automation, 5G Non-Public Networks for Industrial Scenarios, 5G-ACIA White Paper, Jul. 2019.
- [18] International Civil Aviation Organization, »A Connected Sky: The concept of REDDIG,« ICAO. Accessed: Aug. 16, 2026. [Online]. Available: <https://www.icao.int/SAM/REDDIG-CONCEPT>
- [19] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, »FAQ Digitalfunk BOS: Fragen und Antworten zum Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben,« BDBOS. Accessed: Aug. 6, 2026. [Online]. Available: <https://www.bdbos.bund.de/SharedDocs/Downloads/DE/Publikationen/faq-broschuere.html>
- [20] European Telecommunications Standards Institute, Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Release 17 Description; Summary of Rel-17 Work Items (3GPP TR 21.917 version 17.0.1 Release 17), ETSI TR 121 917 V17.0.1, Jan. 2023.
- [21] 5G Alliance for Connected Industries and Automation, Integration of Industrial Ethernet Networks with 5G Networks, 5G-ACIA White Paper, Nov. 2019.
- [22] M. Yan, G. Feng, J. Zhou, Y. Sun and Y. -C. Liang, »Intelligent Resource Scheduling for 5G Radio Access Network Slicing,« in IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7691–7703, Aug. 2019, doi: 10.1109/TVT.2019.2922668.
- [23] European Telecommunications Standards Institute, »Technical Committee on TETRA and Critical Communications Evolution (TC TCCE),« ETSI. Accessed: Aug. 8, 2026. [Online]. Available: <https://www.etsi.org/technical-groups/tcce>
- [24] J.-C. Laprie. »From dependability to resilience.« 38th IEEE/IFIP Int. Conf. On dependable systems and networks. 2008.
- [25] L. Cai, T. Han, J. Wang, J. Xue, F. Xu, M. Zhou, and Y. Fan, »Experimental analysis of the strands breaking characteristics of optical fibre composite overhead ground wire due to simulating lightning strike,« IET Generation, Transmission & Distribution, vol. 14, pp. 2922–2929, 2020, doi: 10.1049/iet-gtd.2019.1826.
- [26] The Critical Communications Association, Pocket Guide to Critical Communications, Jun. 2022.
- [27] TCCA Legal and Regulatory Working Group, Definition of Users in Mission Critical Networks, Jun. 2026.
- [28] European Telecommunications Standards Institute, Electro-magnetic compatibility and Radio spectrum Matters (ERM); System reference document (SRdoc); Land Mobile Service; Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems in the UHF frequency range, ETSI TR 102 628 V1.2.1, Sep. 2014.
- [29] 3rd Generation Partnership Project, »Mission Critical standardised interworking,« 3GPP, Jan. 20, 2026. Accessed: Jul. 27, 2026. [Online]. Available: <https://www.3gpp.org/technologies/mc-interworking>
- [30] European Telecommunications Standards Institute, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design, ETSI EN 300 392-1 V1.6.1, Apr. 2020.
- [31] TCCA Interworking Function Working Group, Interworking Function (IWF); Interworking of LMR networks with 3GPP Mission Critical Services, TCCA White Paper, Aug. 2025. Accessed: Jul. 28, 2026. [Online]. Available: <https://tcca.info/documents/Interworking-Function-IWF-Interworking-of-LMR-networks-with-3GPP-Mission-Critical-Services.pdf/>
- [32] A. G. Merkulov, »Electrical Power-transmission Grids: Future of High-voltage Power Line Carrier,« CIGRE Science & Engineering, no. 26, 2022. Accessed: Aug. 6, 2026. [Online]. Available: <https://cse.cigre.org/cse-n026/electrical-power-transmission-grids-future-of-high-voltage-power-line-carrier.html>
- [33] 3rd Generation Partnership Project, »Use of 3GPP Technologies by Railways,« 3GPP, Jul. 8, 2024, updated Apr. 8, 2025. Accessed: Aug. 10, 2026. [Online]. Available: <https://www.3gpp.org/technologies/deep-dive/railways1>
- [34] Bundesnetzagentur, »Regionale und lokale Netze,« Bundesnetzagentur. Accessed: Aug. 6, 2026. [Online]. Available: <https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Frequenzen/OeffentlicheNetze/LokaleNetze/lokalenetze-node.html>
- [35] P3 communications GmbH, Study on the relative merits of TETRA, LTE and other broadband technologies for critical communications markets, ver. 1.1, commissioned by TETRA & TCCA, Feb. 2015.
- [36] Z. Paladin, E. Fountoulakis, Ž. Lukšić, N. Kapidani, D. Ribar and G. Boustras, »Advanced Mission Critical Communication in Maritime Search and Rescue Actions,« 2023 27th International Conference on Information Technology (IT), Zabljak, Montenegro, 2023, pp. 1–6, doi: 10.1109/IT57431.2023.10078557.
- [37] International Civil Aviation Organization, SAM Region Digital Network (REDDIG), Concept Note. Accessed: Jul. 30, 2026. [Online]. Available: <https://www.icao.int/APAC/meetingdocs?fid=38432>
- [38] European Telecommunications Standards Institute, LTE; 5G; Mission Critical Services Common Requirements (MCCoRe); Stage 1, ETSI TS 122 280 V19.7.0, 3GPP TS 22.280 ver. 19.7.0 Release 18, Jan. 2026.
- [39] A. Volkova, J. Rak and H. de Meer, »Toward Hybrid Satellite-Terrestrial Networks for Power Grid Control under Weather Disturbances,« European WIRELESS 2025; 30th European Wireless Conference, Sophia Antipolis, France, 2025, pp. 64–69.
- [40] International Union of Railways, Future Railway Mobile Communication System Functional Requirements Specification, UIC Ref. FU-7120, ver. 2.1.0, Apr. 29, 2025.
- [41] A. Hassebo, A. Rezk and M. A. Ali, »A Hybrid Uplink Scheduling Approach for Supporting Mission-Critical Smart Grid applications in Commercial 4G Cellular Networks,« 2018 9th IEEE Annual Ubiquitous Computing (UEMCON), New York, NY, USA, 2018, pp. 303–308, doi: 10.1109/UEMCON.2018.8796758.
- [42] International Union of Railways, EIRENE System Requirements Specification, ver. 16.1.0, Feb. 2023.
- [43] International Union of Railways, Future Railway Mobile Communication System System Requirements Specification, UIC Ref. AT-7800, ver. 2.1.0, Apr. 30, 2025.
- [44] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, Wellenreiter: Das Magazin für den Digitalfunk BOS, Ausgabe Sommer 2022, ISSN 2568-7883, 2022. Accessed: Aug. 8, 2026. [Online]. Available: https://www.bdbos.bund.de/SharedDocs/Downloads/DE/Publikationen/wr2022-1.pdf?__blob=publicationFile&v=5



Vom TETRA-basierten BOS-Netz zu breitbandiger 5G-Technik Resiliente Breitband- kommunikation **für Einsatzkräfte**

• P. OELRICHS, Dataport AöR

In Deutschland steht für die Einsatzkräfte der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), also Polizei, Feuerwehr, Rettungsdienste etc., seit vielen Jahren ein eigenbeherrschtes TETRA-basiertes Netz zur Verfügung. Dieses BOS Digitalfunknetz bietet hochverfügbar schmalbandige einsatzkritische Sprachkommunikation auf einer landesweiten, redundant und schwarzfallfest ausgelegten Infrastruktur und wird von der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) in Zusammenarbeit mit den Bundesländern betrieben.

Die Einsatzkräfte benötigen zunehmend breitbandige Datendienste auf Basis der standardisierten Mission Critical Services (MCX-Dienste), die auch in Katastrophenfällen, bei großflächigen Stromausfällen oder bei Sabotage performant zur Verfügung stehen müssen. Heute nutzen Einsatzkräfte für breitbandige Anwendungen die kommerziellen Mobilfunknetze, die die spezifischen Bedarfe jedoch nur teilweise abdecken. Deshalb soll für die BOS ein eigenes 5G-basiertes Netz gemäß 3GPP-Standard errichtet werden. Solange dafür noch keine Frequenzen zugeteilt wurden, bietet sich als Zwischenschritt zu einem eigenbeherrschten Breitbandnetz ein hybrides Netz aus einem BDBOS-eigenen Core-Netz (inkl. National-Roaming-Funktionalität) mit eigenen MCX-Servern, punktuell errichteten 5G-Campusnetzen und der Mitnutzung ausgewählter 5G-Funkstationen der öffentlichen Netzbetreiber an. Technisch basiert diese Kombination auf der Multi-Operator-Core-Network (MOCN)-Funktionalität. Die genutzten Stationen der öffentlichen Netzbetreiber und ihre Anbindung an das BDBOS-Core-Netz müssen dafür gegen Stromausfälle und andere Gefährdungen resilient gemacht werden.

Das von der BDBOS geförderte FuE-Projekt »DTF_MXCp5G« hat diesen Ansatz konzeptionell untersucht, in einem Proof-of-Concept (PoC) in

einem operativ genutzten IT-Verbund validiert und die Ergebnisse in einen praktisch umsetzbaren Vorschlag für eine bundesweite Implementierung überführt. Das Projektkonsortium bestand aus Dataport AöR als Verbundkoordinator, Telefónica Germany GmbH & Co. OHG als öffentlichem Mobilfunknetzbetreiber, sowie Frequentis Deutschland GmbH als Anbieter der MCX-Kommunikationslösung.

Ziel des Vorhabens war, einen Lösungsansatz zu entwickeln und zu validieren, wie für zukünftige breitbandige MCX-Dienste eine robuste, kurzfristig realisierbare und wirtschaftlich tragfähige Übergangslösung bis zu einem späteren bundesweiten eigenbeherrschten BOS-Breitbandnetz geschaffen werden kann.

Untersucht wurde daher, ob und unter welchen technischen, betrieblichen, regulatorischen und wirtschaftlichen Randbedingungen ein gehärtetes privates 5G-Kernnetz mit ausgewählten, gehärteten Funkzugangskomponenten eines öffentlichen Mobilfunknetzes gekoppelt werden kann. Im Mittelpunkt stand die Nutzung der 3GPP-standardisierten MOCN-Funktionalität um auf einer kommerziellen 5G-Funkstation (gNB) gleichzeitig die Netzkennungen des öffentlichen Netzes (PLMN) und eines privaten BOS-Netzes auszustrahlen und damit im Schwarzfall breitbandige MCX-Dienste weiter bereitzustellen.

Dies mit der Maßgabe, sicherheitskritische Merkmale zu ergänzen, um die Krisenfestigkeit zu verbessern:

- (1) Erweiterte Netzabdeckung: Private 5G-Campusnetze werden durch RAN-Sharing (MOCN) mit öffentlichen 5G Mobilfunkstandorten erweitert.
- (2) Nutzung von MCX-Diensten: Kritische Kommunikationsdienste werden integriert.
- (3) Zentrales Management: Ein einheitliches System (Unified Endpoint Management, UEM) verwaltet die Endgeräte.

Der PoC wurde unter Realbedingungen in einem hybriden Verbund aus privatem 5G-Netz, öffentlichem 5G-Mobilfunknetz und zentralen Diensten in einem operativen Umfeld im Landesnetz des Bundeslandes Schleswig-Holstein durchgeführt. Dies führte bewusst zu höheren Anforderungen als in einer Laborumgebung, weil betriebliche Sicherheitsvorgaben, Freigabeprozesse, Interoperabilitätsfragen und Einschränkungen eines operativen Netzbetriebs berücksichtigt werden

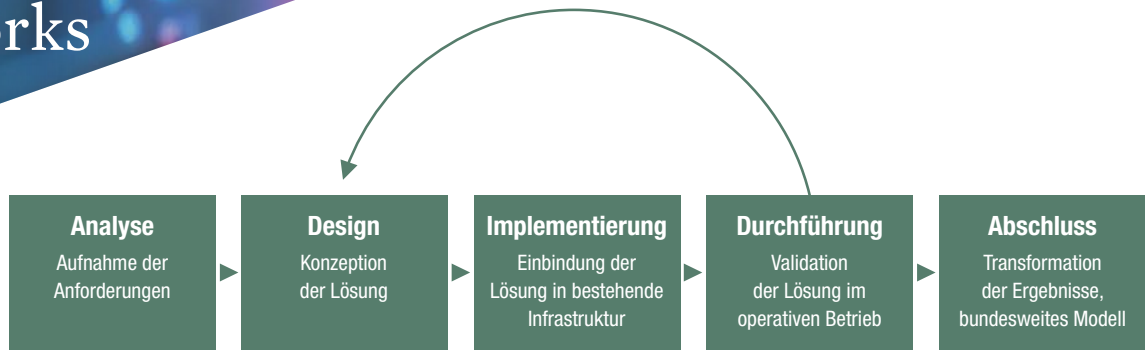


ABBILDUNG 1 Vorgehensmodell

mussten. Eine wesentliche Rahmenbedingung war, dass Beeinträchtigungen des operativen Telefónica-Livenetzes ausgeschlossen werden mussten. Ebenso waren die Vorgaben zum sicheren Betrieb, zur Verkehrstrennung, zur physischen Sicherung der Infrastruktur und zur realistischen Simulation des Schwarzfalls zu beachten.

Hinzu kam, dass das Vorhaben in zwei Ebenen gedacht wurde: erstens als PoC mit konkreter Infrastruktur in Schleswig-Holstein und zweitens als methodische Vorstufe für eine spätere Übertragbarkeit auf eine bundesweit nutzbare BOS-Breitbandlösung. Diese Zweiteilung prägte praktisch alle Arbeitspakete und insbesondere die Arbeiten in den Bereichen IT-Sicherheit, Endgerätemanagement, Dienstverfügbarkeit, Funknetzdesign, Frequenzwahl, MOCN-Konfiguration, Integrationsdesign und Schwarzfallvalidierung.

Das Vorhaben folgte dabei einem klassischen Phasenmodell mit den Abschnitten Analyse, Design, Implementierung, Durchführung und Abschluss.

Zur Aufnahme der Anforderungen wurden exemplarisch drei Anwendungsszenarien aus Nutzersicht beschrieben:

- › Erstens ein wetterbedingtes Katastrophenereignis an der schleswig-holsteinischen Westküste mit Deichbruch und Stromausfall, bei dem breitbandige MCX-Dienste für Lagebeurteilung, Einsatzkoordination und Datenzugriff über ein gehärtetes privates 5G-Netz und integrierte öffentliche 5G-gNBs mit automatischer Notstromversorgung bereitgestellt werden müssen.
- › Zweitens eine planbare Vorbereitung auf einen möglichen Großschadensfall bei einer öffentlichen Großveranstaltung, dem Wacken Open Air Festival, bei dem private temporär aufgestellte 5G-Funkstationen und ausgewählte öffentliche 5G-gNBs mit manueller Aktivierung und Notstromversorgung zur Unterstützung der BOS-Kommunikation eingesetzt werden.
- › Drittens ein technischer Ausfall von gNBs im privaten 5G-Netz des Hafens Husum, bei dem öffentliche 5G-Stationen als redundante, gehärtete Backup-Lösung mit automatischer Notstromversorgung temporär einspringen.

In allen Szenarien sind unterbrechungsfreie Umschaltung der Endgeräte zwischen privaten und öffentlichen 5G-Zellen, automatisierte Teilnehmer-

verwaltung sowie die Unterstützung aller MCX-Dienste mit mindestens vergleichbarer Performance gefordert. Die generelle Leitlinie lautet »Technik folgt Taktik«, um die taktischen Anforderungen der BOS bestmöglich zu unterstützen.

Technisch müssen die öffentlichen gNBs, die den MOCN-Betrieb unterstützen, so konfiguriert sein, dass eine unterbrechungsfreie Umschaltung im Schwarzfall ohne manuelle Änderungen möglich ist, und über eine mindestens 72-stündige Notstromversorgung verfügen. Die Anbindung an das gehärtete Transportnetz erfolgt möglichst direkt über das Netz des Landes Schleswig-Holstein, das ebenfalls eine 72-stündige Überbrückungszeit gewährleisten muss. Die MCX-Dienste sind gemäß 3GPP-Standards mit priorisierter Datenübertragung, niedriger Latenz und hoher Verfügbarkeit zu realisieren und als virtuelle Maschinen auf geeigneten Virtualisierungsplattformen in einem BSI-zertifizierten Rechenzentrum bereitzustellen.

Gegenüber der ursprünglichen Planung zeigte sich, dass die Realbedingungen des operativen Netzbetriebs zusätzliche Iterationen in Design und Freigabe erforderlich machten. Zudem wurde deutlich, dass eine verzugsfreie Service-Kontinuität nur erreichbar ist, wenn die für den Schwarzfall vorgesehenen MOCN-gNBs bereits im Normalbetrieb permanent in der Zielkonfiguration betrieben werden. Diese Erkenntnis führte zu einer fachlich wichtigen Schärfung des Konzepts, bedeutete aber zugleich mehr Abstimmungsaufwand in Architektur, Betrieb und Sicherheit.

Das Vorhaben baut auf dem Stand der 3GPP-konformen 5G-SA-Technik, der MCX-Dienste, des RAN-Sharing mittels MOCN, der Nutzung gehärteter souverän betriebener privater 5G-Campusnetze sowie der etablierten Betriebs- und Sicherheitsprozesse öffentlicher und behördlicher Netze auf. Ausgangspunkt war die Annahme, dass ein späteres BOS-Breitbandnetz auf einem eigenen Core und auf eine Kombination aus eigenem privaten 5G-RAN und ergänzend mitgenutzten RAN-Komponenten öffentlicher Netze angewiesen sein könnte.

In der unteren Hälfte von *Abbildung 2* ist das 5G-Netz des kommerziellen Mobilfunknetzbetreibers (MNO) mit seinem 5G-Funknetz (RAN), dem Transportnetz und dem Core samt Applikationsservern und Netzbetriebszentrum dargestellt. Die Nicht-BOS-Nutzer des öffentlichen Mobilfunknetzes samt ihren

ABBILDUNG 2

Einfaches Modell einer bundesweiten einsatzkritischen Breitbandlösung aus privaten 5G-Netzen und öffentlichen gNBs im Normalbetrieb

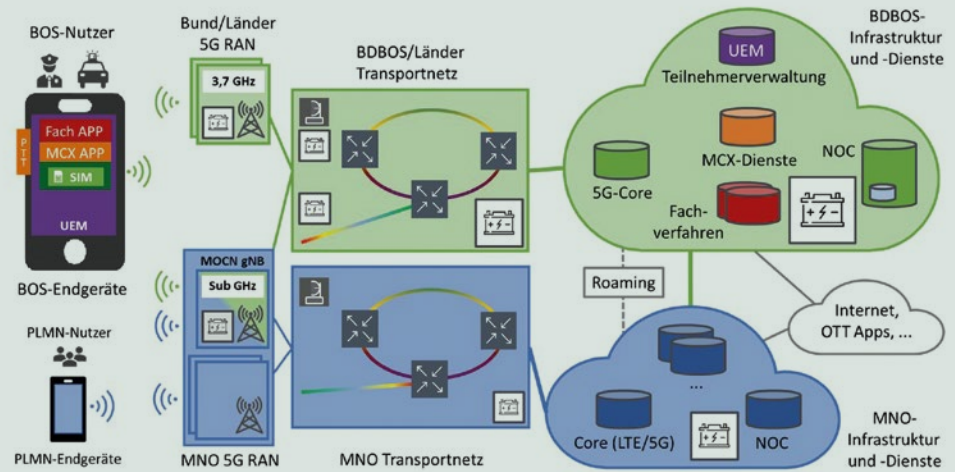
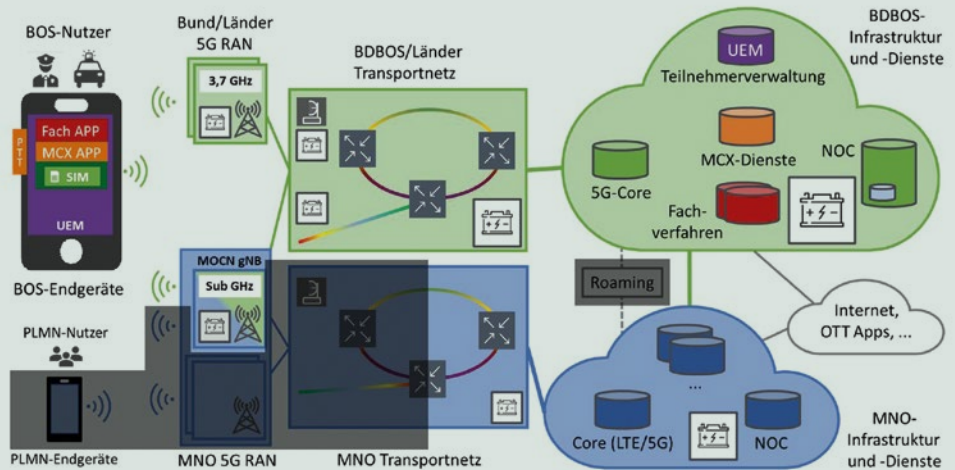


ABBILDUNG 3

Einfaches Modell einer bundesweiten einsatzkritischen Breitbandlösung aus privaten 5G-Netzen und öffentlichen gNBs im Schwarzfall



Endgeräten sind der Vollständigkeit halber links unten in der Abbildung gezeigt.

In der oberen rechten Hälfte des Bildes befinden sich die zentralen Komponenten der BDBOS (eigener 5G-Core, MCX-Server, Server für Fachverfahren, die zentrale Teilnehmerverwaltung sowie das zugehörige Netzbetriebszentrum (NOC)).

Oben links ist ein Endgerät der BOS-Nutzer dargestellt. Es handelt sich um ein für die BOS-Nutzung geeignetes 3GPP-konformes 5G-Endgerät, bestückt mit einer BOS-Netz-spezifischen SIM-Karte, die zur Authentifikation gegenüber dem BDBOS-Core dient. Die MCX-Dienste und die zugänglichen Fachverfahren werden über jeweils zugehörige Applikationen im Zusammenspiel mit den zentralen Servern bereitgestellt. Das Management der Endgeräte samt z.B. Berechtigungsverwaltung erfolgt über eine Endgeräte-Management-Applikation, die auf den zentralen Teilnehmerverwaltungs-Server zugreift.

Der Funkteil des Endgeräts wird über einen 5G-Funkkanal im 3,7 GHz-Band mit eigenen Campuszellen privater 5G-Radionetze von Bund bzw. Ländern verbunden. Diese Funkzellen sind über bundes- bzw. ländereigene Transportnetze (i. W. Glasfaserleitungen, Richtfunkverbindungen, Router) an das zentrale Corenetz der BDBOS angebunden, wie in der linken Mitte und der Mitte in der oberen Hälfte der Abbildung dargestellt.

Mit dieser Netzkonfiguration werden eigenbeherrschte, schwarzfallfeste Breitbanddienste (MCX, Fachverfahren) digital souverän für die BOS im

begrenzten Abdeckungsbereich der privaten 5G-Campuszellen bereitgestellt. Für alle im Verantwortungsbereich von Bund bzw. Ländern betriebenen Netzelemente wird dazu eine schwarzfallfeste Stromversorgung unterstellt.

Solange der BDBOS keine eigenen Frequenzen im Sub-GHz-Bereich zur Verfügung stehen, ist daher eine ergänzende Nutzung kommerzieller Mobilfunknetze zwingend. Gemäß Strategie der BDBOS ist geplant, die BOS-Nutzer mittels Roaming aus dem BDBOS-Core über den Core des MNO, sein Transportnetz und sein 5G-Funknetz anzubinden. Den BOS-Nutzern steht damit der gesamte vom MNO versorgte Funkabdeckungsbereich zur Verfügung. Da die Radionetze und die Transportnetze der öffentlichen Netzbetreiber nur punktuell schwarzfallfest ausgeführt sind, sind die auf diesem Weg bereitgestellten Breitbanddienste weder eigenbeherrscht noch schwarzfallfest.

Zwischen den 5G-Campusnetzen und dem flächendeckenden 5G-Radionetz des MNO sind die MOCN-Zellen dargestellt. Sie sind integrale Bestandteile des Radionetzes des MNO und zugleich des 5G-Netzes der BDBOS, sind über schwarzfallfeste Transportverbindungen an die Transportnetze von Bund bzw. Ländern angebunden, erhalten dedizierte Ersatzstromversorgungen und stellen dadurch schwarzfallfest dieselben Breitbanddienste für die BOS bereit, die diesen durch den oben beschriebenen 5G-Netzverbund im Bereich der Campuszellen zur Verfügung steht.

Im Normalbetrieb, also ohne Stromausfall, werden sich die BOS-Endgeräte über die MOCN-Zellen direkt mit dem 5G-Core der BDBOS verbinden und Nicht-BOS-Endgeräte verbinden sich mit dem MNO-Core.

Im Schwarzfall in *Abbildung 3* bleibt dieser Zustand unverändert, wobei durch den Ausfall der nicht notstromversorgten Transportnetzverbindungen zum Core des Mobilfunknetzbetreibers die Nicht-BOS-Nutzer keine Konnektivität mehr bekommen und damit den BOS prinzipiell die volle Kapazität der MOCN-Zellen zur Verfügung gestellt werden kann, ähnlich wie dies bei eigenbeherrschten Funknetzen mit eigenem Frequenzband der Fall ist.

Bezüglich Netzbetrieb ist es erforderlich, dass im Network Operation Center (NOC) der BDBOS eine Instanz des RAN-Netzwerkmanagementsystems des PLMN vorgehalten wird, die den Zugriff auf die MOCN-Stationen für eingeschränkte Funktionen (i. W. Betriebsüberwachung und Fehlerbeseitigung) erlaubt.

Bei der Netzplanung für das hybride Netz mit MOCN-Stationen bedürfen besonderer Sorgfalt

- › die Auswahl der MOCN-Zellen nach operativ-taktischen Erfordernissen (Funkabdeckung für die BOS durch Nutzung von Zellen mit Sub-GHz-Frequenzen und weitreichender Coverage) und technischer Realisierbarkeit (Härtung und Transportnetz-Anbindung an den 5G-Core der BDBOS)
- › die Trennung der Verkehrsströme und die Aufteilung der Zellkapazität auf BOS-Nutzer und Nicht-BOS-Nutzer (ideal so, dass im Schwarzfall die volle Kapazität der MOCN-Zellen im Sub-GHz-Layer den BOS zur Verfügung steht)
- › die sicherheitstechnisch geeignete Auslegung der Anbindung der MOCN-Zellen an das Corenetz des MNO und zugleich an das 5G-Corenetz der BDBOS (unter Berücksichtigung der Schnittstellen und Spezifikationen der eingesetzten gNB)
- › die funktechnisch sorgfältige Implementierung des entstehenden hybriden Netzes mit Festlegung der Nachbarschafts- und Handover-Parameter der Zellen der Campusnetze und der MOCN-Zellen
- › die Vermeidung von möglicher Zell-Überlast der MOCN-gNB im Schwarzfall durch erfolglose Verbindungsversuche von Nicht-BOS-Nutzern
- › die standortindividuelle Härtung der MOCN-gNB (gegen Stromausfälle sowie bezüglich Materieller Sicherheit).

Die detaillierte Planung muss unter Berücksichtigung der Spezifika der eingesetzten Netzelemente mit ihren Hardware- und Software-Ständen durchgeführt werden.

Fazit

Das Vorhaben konnte die technische Machbarkeit eines hybriden 5G-Verbunds aus privatem Kernnetz und ausgewählten, gehärteten kommerziellen Funkzugangskomponenten in einem operativen IT-Verbund erfolgreich nachweisen. Die MCX-Dienste MCPTT, MCVideo und MCDATA wurden sowohl im öffentlichen Telefónica-Netz als auch im MOCN-Betrieb und im simulierten Schwarzfall funktional validiert. Im Schwarzfall verbanden sich die über ein das zentrale UEM provisionierte BOS-Endgeräte erfolgreich über die gehärtete MOCN-Basisstation mit dem privaten 5G-Core; die Dienste liefen stabil weiter.

Die Arbeiten führten ferner zu belastbaren Empfehlungen für einen späteren bundesweiten Ausbau. Dazu zählen die permanente MOCN-Konfiguration im Normalbetrieb, die Nutzung von Sub-GHz-Spektrum – im PoC insbesondere 700 MHz –, die konsequente Trennung und Härtung der Transportpfade, eingeschränkte aber notwendige Management-zugriffe auf MOCN-Stationen sowie die Notwendigkeit, Betriebs- und Verantwortungsgrenzen zwischen BOS-seitigem Netzbetrieb und MNO-Betrieb frühzeitig zu definieren.

Zusammenfassend können nachstehende Ergebnisse konstatiert werden:

- › Hybrider 5G-Netzverbund mit privatem Core, gehärteter MOCN-gNB und zentralen MCX-Diensten im operativen IT-Verbund erfolgreich demonstriert
- › MCX-Dienste für Sprache, Video und Daten im Regel- und Schwarzfall validiert; alle definierten Testfälle bestanden
- › Netzmodell und Vorgehensansatz für eine bundesweit skalierbare MOCN-Lösung zur Resilienzerhöhung abgeleitet
- › UEM-gestütztes Endgeräte- und Teilnehmermanagement im 5G-Netzverbund erprobt
- › Rechtliche, regulatorische, betriebliche und wirtschaftliche Handlungsfelder für die Weiterentwicklung aufgezeigt.

Die Ergebnisse sind für die BDBOS und die Bundesländer von hohem Nutzen, weil sie einen realistischen und technisch fundierten Entwicklungspfad zwischen heutiger Nutzung öffentlicher Breitbandnetze und einem späteren eigenbeherrschten BOS-Breitbandnetz beschreiben. Das Vorhaben zeigt, wie sich die Krisenresilienz breitbandiger BOS-Kommunikation kurzfristiger steigern lässt, ohne den vollständigen Neubau eines bundesweiten Netzes abzuwarten zu müssen.

Der konzipierte Lösungsansatz kann als ein integraler Baustein auf dem Weg zur Breitbandnetz-Autonomie der BDBOS dienen und die Resilienz der aktuell verfügbaren Breitbanddienste der BOS signifikant und unmittelbar erhöhen. Dies trägt dem Gedanken des Förderprogramms insoweit Rechnung, dass unmittelbar Mehrwerte für die BOS durch die Möglichkeit einer zeitnahen Umsetzung geniert werden können. ●



Resilient networks for critical communication in **electrical power grids**

• J. TUSCH, Dr. Tusch Consulting

Abstract

Energy transition will lead us into a carbon free future electrical energy system but it does not come for free. Substantial investments have to be made in replacing traditional power plants with renewables, enhancing and digitizing grid infrastructure as well as coping with the energy storage challenge. In addition, grid control systems make sure that all components of the energy system are well coordinated thus enabling high availability of supply. All these subsystems require reliable and resilient communication to operate securely and properly. In this paper we give an overview on the typical communications use cases in a power grid, the communication requirements and possible network architectures.

Energy transition and the importance of reliable communications

Renewable energy sources open the way to the desired reduction of carbon emissions leading to sustainable energy systems. At the same time, a reliable integration of renewables requires that the energy system has to be monitored and controlled in a much greater detail than today. The main objective here is to reduce the carbon footprint without sacrificing the high availability of supply.

The benefit of a zero-carbon footprint comes with the drawback of a fluctuating generation profile of renewables. There can be strong variations in power generation dependent on the amount of wind or sun available. At noon there is lots of sun radiation available leading to high photo voltaic (PV) power output. Similarly, the output of wind turbines is strongly dependent on the strength of wind in a specific region. If there is an extended power balance mismatch in the power grid the control mechanisms are no longer able to keep the system stable and the consequence is a system crash or black-out. One of the recent

examples of such a situation is the black-out in Spain in April 2025. In order to keep the required balance between generation and consumption in the power grid, an active control of renewable sources is mandatory and critical to system stability. Consequently, communications to control renewables is system critical, and the networks providing the communication connections have to be highly reliable and highly resilient.

Observability and control in modern power systems mean more than just the reliable integration of renewable power generation devices. Today medium and low voltage layers are almost invisible to grid control engineers. Digitizing these parts of the power grid brings a huge benefit for stable operation in a renewable generation environment and in addition to integrate new services. This includes smart meters offering flexible tariffs to cope with the increased dynamics of power flow in the grid. Also, the digitization of secondary substations helps to keep up with the demand in the low voltage grid. Increasing PV installations, heat pumps and electric vehicles can bring traditional low voltage grids to their limits. The first step is to gain transparency of this part of the grid by measurements. A second step can be the active control of low voltage grids where ever necessary. Finally, there is an increasing requirement for storage and switchable loads in the power grid. All these measures require reliable communications to function properly.

Another field is reliable voice communication for grid technicians in order to communicate with the grid control center to perform remote switching. In the case of disasters switching actions by technicians in the field may sometimes be the last option to restore power. Generally, communication is key to effectively manage and recover from disasters. Voice communication services for utilities can also be made available to other parties involved in disaster recovery like crisis coordination centers of municipalities.

Communications network architecture for a reliable power grid operation

Figure 1 shows a typical diagram of an electrical power grid. The highest voltage layer (extra high voltage) is operated by the transmission system operators (TSO). The lower layers are managed by distribution system operators (DSO) including high voltage layer, medium voltage layer and low voltage layer. Typically, utilities operate their own fiber communication networks. This holds true for transmission system operators with a fiber network providing a power resiliency of 72 hours. The aim is to be able to restart the power system after a complete black-out in a country. In addition to data communication also voice communication is required to recover the energy system from a black-out. Larger distribution system operators run their own fiber networks in parts of the high voltage layer typically also with a power resiliency of 72 hours in the core part of the network. Things change in the medium and low voltage part of the grid. Typically, there has been almost no utility operating own communications infrastructure with power resiliency. All communication in this part of the grid typically is not black-out resilient and thus not prepared for blackout recovery.

To put things into perspective: we have to investigate the connection points of renewable energy sources to the power grid. In the past, power stations were connected to extra high voltage and high voltage layers.

In today's power grids renewables feed their power into all voltage layers of the power grid, specifically into medium and low voltage layers. The example of Germany shows that roughly two thirds of the renewable power is fed into medium and low voltage whereas only one third is fed into the high and extra high voltage layers of the grid. Bearing in mind the system stability criteria it is obvious that reliable communications to control renewables is mandatory at least in medium voltage and also desirable in low voltage layers.

From the above it can be concluded that the communications networks of the transmission system in the extra high voltage layer and in the high voltage layer of the distribution system generally are well prepared for the extended communication requirements of energy transition. The big communications gap typically exists in the medium and low voltage layers of the power grid. For these layers, a cost-effective communications technology is required, since there are hundreds of thousands or even millions of devices (e.g. PV systems, heat pumps, EV charging stations) in these voltage layers which are widely spread over a country. The best technical option would be to run optical fiber to all devices but this approach would be cost prohibitive. Radio technology seems to be a good approach provided that strict performance, reliability and resilience requirements are met. These requirements include traffic engineering with end-to-end real-time priorities and guaranteed packet delivery.

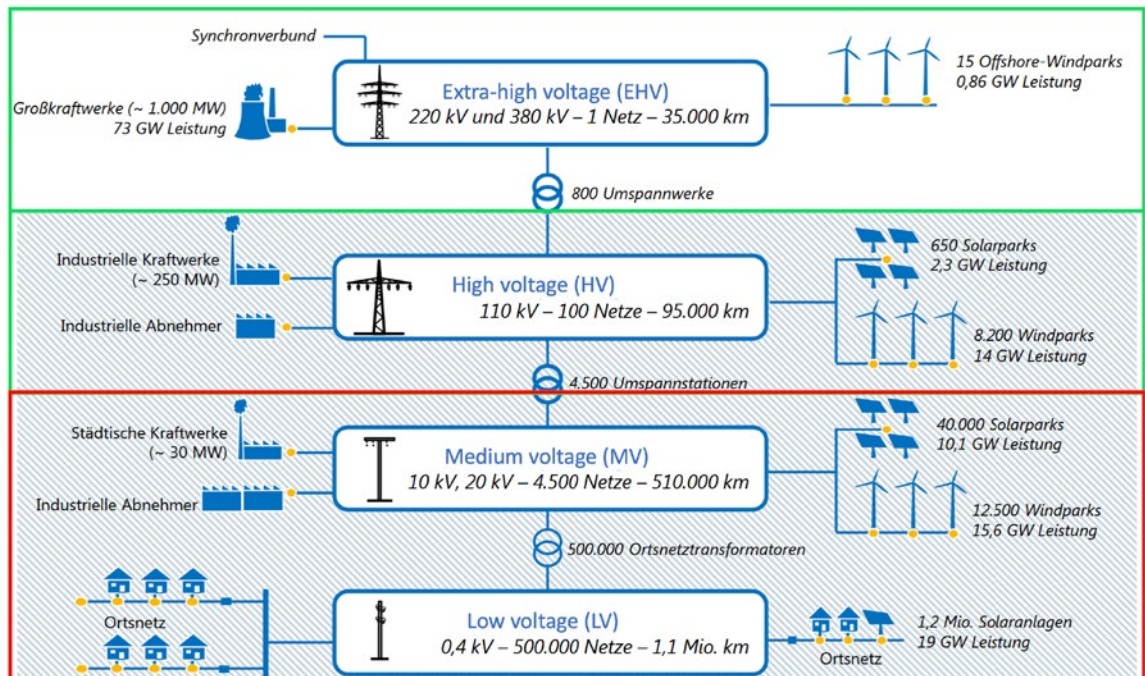


FIGURE 1

Power grid architecture in Germany and renewable power input

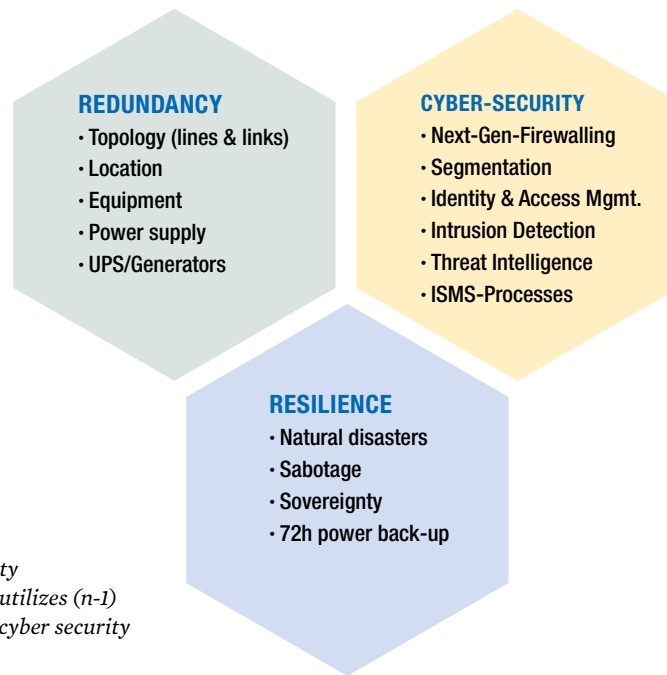


FIGURE 2

A secure and highly resilient utility process communication network utilizes (n-1) redundancy as well as top-notch cyber security and provides effective resilience.

In addition to that, redundancy concepts for communication links as well as for critical system components have to be implemented to achieve high availability. *Figure 2* gives some examples of required resilience and security measures. These networks should withstand natural disasters as well as cyber-attacks to deliver a high level of resilience. Finally, there is the requirement of black-out resiliency in order to enable a system restart after a black-out. This requires battery back-up or generators at each location with active components to achieve a power resiliency of 72h. Typically, commercial communication carrier networks do not fulfil these requirements. Consequently, dedicated private mobile radio networks are built on a dedicated frequency (e. g. 450 MHz) with a country wide coverage to support critical infrastructure providers like utilities, water companies or gas grid operators. Lower frequency bands in the 400 MHz range offer the advantages of good regional coverage which means less radio towers per region and a better in-building coverage. One of the major benefits of using radio technology is the provision of black-out resilient mobile voice services through the network to support grid operation in crisis scenarios and disaster recovery.

Due to the current geopolitical situation, sovereignty in critical communication networks is even more important for the security of a country. It has to be made sure that the only instance which can control the critical communications network is its own network control center and nobody else. To achieve this goal several requirements have to be met. First of all, a careful selection of the equipment suppliers for the communications network has to be made. In addition to that the operational principals and processes have to be clearly defined and executed by the network operations team. Secondly top-notch cyber security measures have to be integrated in the operation

nal processes starting with next generation firewalls, protocol monitoring (e. g. IEC 104 or IEC 61850), threat intelligence, identity and access management with public key infrastructures, firewall management systems and finally effective ISMS (Information Security Management System) processes. After all a SIEM (Security Information and Event Management) is required to effectively keep track of the state of the critical communications infrastructure and to be able to react (automatically or by operator intervention) properly if required. The SIEM may be AI supported as well.

A lot of progress has been made in terms of the standardization of mobile radio networks. 5G standards are available for 450 MHz mobile networks and offer the advantage of vendor selection and interoperability. Also new functions like new radio side-link can be of good value to utilities when it comes down to voice communication within buildings like stations with poor in-building network coverage where side-link offers the opportunity to relay from device to device without routing through the base station.

Summary

In summary, reliable communication is key for the successful and secure operation of modern electrical power grids. Typically, in higher voltage layers there is already a good foundation available whereas in the lower voltage layers of the grid, reliable communications is missing. The integration of renewables in the course of the energy transition requires additional reliable communications in the lower voltage layers of the power grid. In these parts of the grid, practical experience has shown that dedicated mobile radio networks offer a cost-effective solution to cover grid requirements. In addition, they offer mobile voice services for utility grid operation in crisis situations as well as the integration of external parties which are crucial for disaster recovery. ●

Industrial 5G

Private Campus Networks as Enablers of Industrial Automation

• D. MAI, Director Industrial Wireless Communication at Siemens

The industrial landscape is undergoing profound change. Digitalization, flexible manufacturing, and increasing automation are placing new demands on the communication infrastructure in production environments. Wired networks reach their limits wherever mobility, flexibility, and the connection of a growing number of devices are required. The 5G mobile communications standard – and private 5G campus networks in particular – offers a promising approach in this regard but will only be accepted and adopted by industry if it delivers a clear, measurable advantage over existing solutions.

Industrial Requirements: More Than Just Bandwidth

When industrial companies consider deploying a new communications network, bandwidth is rarely the top priority. What matters most are three core requirements that differ fundamentally from those of the consumer market: determinism, availability, and data sovereignty.

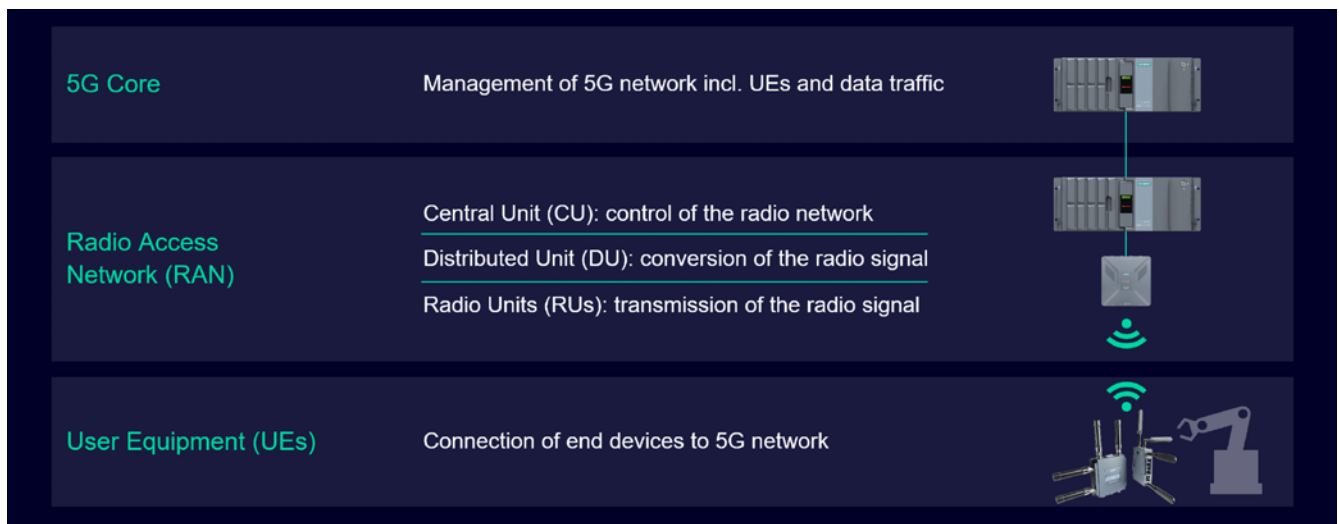
Industrial communication is based on protocols such as PROFINET, EtherNet/IP, or OPC UA, which impose strict requirements on the temporal predictability of data transmission. In automation technology, it is not only the average latency that matters, but its consistency – that is, the guarantee that a control command will reliably arrive within a defined time window. Variations in transmission delay, technically referred to as jitter, must be minimized, as even minor timing irregularities in synchronized control sequences can lead to plant shutdowns.

This principle of determinism is the fundamental prerequisite for the safe operation of machines and systems. Fluctuating transmission times, as can occur in public mobile networks, are simply not tolerable in a production environment. Private 5G networks address this requirement through dedicated network resources and tailored configurations in which critical communication paths are prioritized over less time-sensitive data streams.

Closely linked to determinism is the requirement for network availability. In industrial manufacturing, a communication failure can, in the worst case, result

in a production standstill – with direct economic consequences that, depending on the industry and plant capacity, can generate significant costs within minutes. For production plant operators, a network availability of 99.999% – the so-called »five nines« availability – is therefore not a wishful aspiration but an operational necessity. Private 5G campus networks offer a decisive advantage over public networks in this regard: since the network is entirely under the user's control, redundancy concepts, maintenance windows, and failure scenarios can be specifically planned and implemented without dependence on the availability of an external network operator. In addition, private 5G networks use licensed private 5G spectrum which, unlike other radio technologies, is interference-free and therefore enables practically uninterrupted operation.

The third core requirement concerns the protection of data and intellectual property. Production data – whether machine condition data, process parameters, or quality measurements – is highly sensitive. It reveals manufacturing processes, production capacities, and technological innovations that represent a company's core assets. In a private 5G campus network, all data remains within the company premises. There is no transmission to public infrastructure, no dependency on third-party cloud services, and no uncontrolled data paths to the outside world. This aspect of data sovereignty is a decisive factor for many industrial companies when choosing a private 5G network over a public or hybrid approach.



Architecture of a private Industrial 5G network

Concrete Use Cases:

Where Private 5G Networks Prove Their Value Today

Industry is well known for adopting new technologies broadly only once their benefits are clearly demonstrated. That proof is currently being established in a large number of projects. Several application areas are emerging in which private 5G networks can showcase their strengths effectively.

A particularly compelling example is automated guided vehicles (AGVs) and monorail systems in intralogistics. These vehicles must coordinate in real time with central control systems, avoid collisions, dynamically adjust routes, and continuously transmit position and status data. Wired solutions are naturally out of the question for mobile units, and older Wi-Fi technologies frequently reach their limits in terms of the required latency and reliability values due to interference. Private 5G networks provide the necessary combination of low latency and stable connectivity even while moving through different radio cells – a decisive advantage in large production or warehouse facilities where seamless handover between radio units is essential.

Another application area with significant potential is the automation and remote control of cranes. In steel plants, ports, or large production halls, cranes are traditionally operated by on-site personnel or from cabins in proximity. Relocating this control function to central control rooms – known as remote operation – makes it possible to keep operators out of hazardous environments, coordinate multiple cranes from a single location, and increase operational efficiency. However, such applications require extremely low and stable latency: the operator must receive camera images from the cranes in real time and transmit control commands without any perceptible delay. Public networks are generally unable to meet these requirements reliably; a dedicated private 5G network with guaranteed transmission parameters, on the other hand, can.

A third, increasingly significant application area is the use of artificial intelligence in industrial production. AI systems – whether for predictive maintenance, real-time quality assurance, or the optimization of production processes – are directly dependent in their performance on the quality and availability

of the data fed to them. The more sensors, machines, and systems continuously supply data, the more precisely and responsively AI models can operate. This is where network infrastructure becomes the decisive factor: to transmit the volumes of data generated from a large number of distributed sources reliably, with low latency, and in real time, high-performance communication networks are indispensable – and this explicitly includes wireless networks. Private 5G campus networks create the conditions for AI in industry to reach its full potential not only in the laboratory, but in live production operations.

Closely related to this is the question of brownfield digitalization – that is, the retrofitting of existing production plants with digital capabilities. While greenfield projects – built from scratch – can be planned with modern network infrastructure from the outset, connecting legacy plants that have grown over time presents a considerable practical challenge. Retrofitting cables in existing production halls is not only costly, but in many cases technically barely feasible – whether due to structural constraints, ongoing production, or certification requirements. Private 5G networks offer a decisive advantage here: machines and systems that previously had no network connection can be wirelessly integrated into the digital infrastructure via 5G-capable gateways or directly embedded radio modules – without extensive construction work and without production interruptions. This significantly lowers the barrier to digitalization in existing facilities and makes 5G an important tool on the path to the connected factory, even where the industrial history stretches back decades. New, modern applications can thus be implemented very easily and cost-effectively.

Technological Foundations and Regulatory Framework

Private 5G campus networks – also referred to as local 5G networks – are 5G infrastructures confined to a defined company site, production area, or individual buildings. Companies deploy them locally at their sites and tailor them specifically to their particular requirements and applications. The 5G infrastructure typically comprises a 5G core, a 5G RAN (Radio Access Network), and radio units, as well as the necessary end devices. Private 5G networks are frequently complemented by edge computing solutions, which enable data

Mission Critical Networks

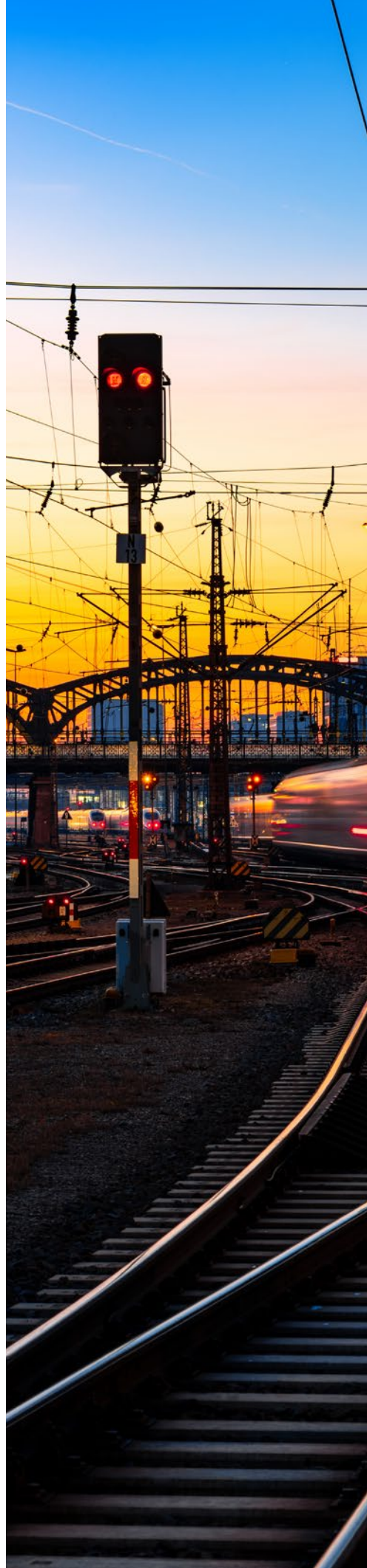
processing directly on-site – close to the data source. This further reduces latency and allows fast, auto-nomous decisions to be made without routing data through external data centers.

Access to suitable radio spectrum is a fundamental prerequisite for the widespread adoption of private 5G networks in industry. Many countries worldwide have already reserved dedicated frequency bands for this purpose. The European Union has designated the frequency range from 3.8 to 4.2 GHz for private 5G networks, thereby establishing a uniform framework that significantly simplifies the planning and deployment of campus networks. An EU-wide harmonized frequency band benefits both end users and device manufacturers alike: the ecosystem of 5G-capable industrial devices – from sensors and controllers to mobile terminals – can develop more rapidly, which in turn will have a positive impact on acceptance and implementation across industry.

Outlook: 5G as an Enabler of Industrial Transformation

The economic significance of 5G for industry is substantial. Analyses by ABI Research with industry stakeholders show that the implementation of private 5G networks in factories leads to a productivity increase of up to 30 %. Concurrently, work-related injuries decrease by up to 40 %. This effect is not created by the technology itself, but by the applications it enables: autonomous transport systems, connected robotics, predictive maintenance, and the seamless integration of production systems across all levels of the value chain.

A clear principle applies in industry: new technologies are only introduced when they deliver tangible added value – in the form of efficiency gains, cost reductions, or the development of new business models. Private 5G networks are well on their way to providing that proof. Characteristic of industrial adoption is a step-by-step approach: companies typically start with a single, clearly defined application – such as the connection of automated guided vehicles. Only when this first application is running reliably and its added value is internally verified, other applications will be successively migrated to the 5G network or new applications will be developed on it. This iterative approach reduces investment risk, builds internal expertise, and allows the network to scale organically with the company's growing requirements. The technology has moved beyond the phase of pure pilot projects and is being concretely implemented in an increasing number of companies. As the ecosystem matures, infrastructure costs decline, and the range of 5G-capable industrial devices grows, private campus networks will become an integral component of modern production environments – serving as a reliable, secure, and deterministic communication foundation for the factory of the future. ●



How to prepare the railway communications network for FRMCS, end to end

→ K. OBERLE, Railway Business Development Lead Europe, Nokia

When FRMCS gets introduced — and in many countries will replace GSM-R, especially across European railways — the changeover won't be a simple radio upgrade. Instead, it requires a transformation of the entire communications architecture, so planning should begin now. Here's what rail operators need to address, layer by layer.

The Future Railway Mobile Communication System (FRMCS) is the next-generation standard for railway communications. It provides a foundation for enhanced capabilities and enables an array of operating benefits. Yet many rail operators don't realize it's time to begin key preparations for implementing this new standard.

The meticulous FRMCS standardization process is progressing through the International Union of Railways (UIC) — and the European Railway Agency (ERA) is not expected to release the final Technical Specifications for Interoperability (TSI) until approximately 2028.

The migration to FRMCS is a complex endeavor. It first requires the transformation of a railway infrastructure manager's entire mission-critical communication architecture, touching every layer of the network stack. Consequently, the lead times for FRMCS

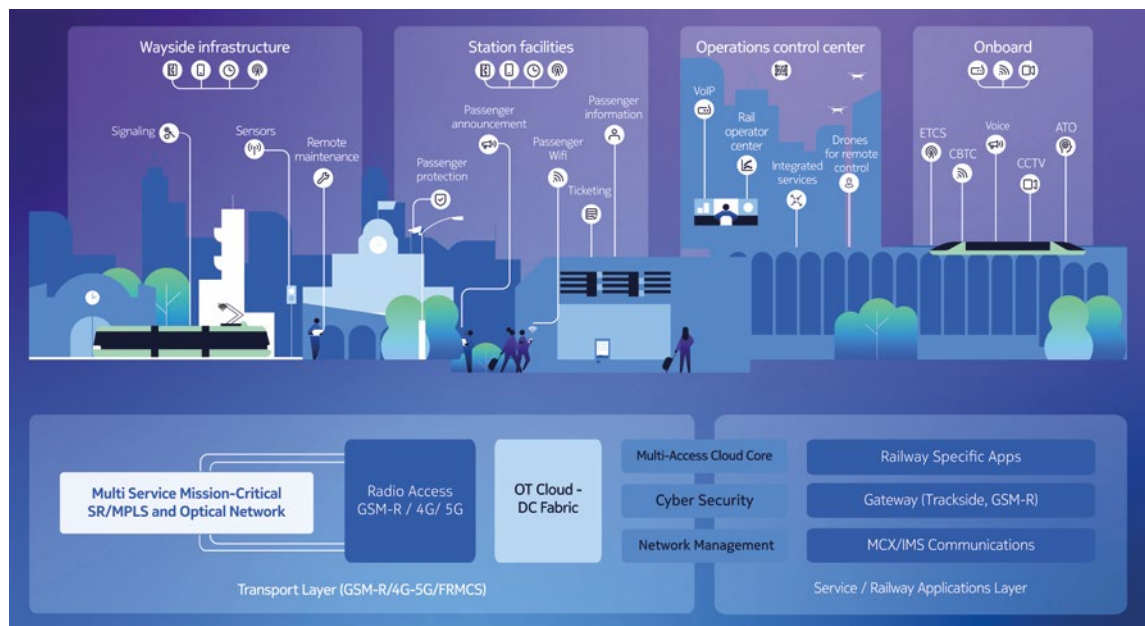
readiness are substantial. And crucial steps should be addressed as quickly as possible.

Here's one approach to making necessary changes:

Focus first on the transmission backbone

This fixed IP and optical network provides the foundation for everything else that will be built, and it must be fully ready before any further steps are taken. Readiness includes:

- › Establishing IP/MPLS connectivity at every base station
- › Ensuring that routers support 5G's synchronization demands
- › Making changes to the IP network's physical topology, where needed; for instance, ring sizes must match strict 5G synchronization requirements.



Nokia solutions for railways



Consider what's needed for the RAN

The first step in radio access network (RAN) planning is to determine what will actually run through the network, because those requirements will help create a proper network design, including the number of radio sites that will be needed.

Initially, FRMCS planning assumed far more radio sites would be needed, when moving from GSM-R's 900 MHz band to FRMCS at 1900 MHz (n101). In fact, that's not always correct. If railway operators are first focusing on basic ETCS signaling and mission-critical voice — and the GSM-R network has already been designed to serve ETCS — the same cell sizes for GSM-R should work for FRMCS. This is due to the fact that cell sizes are mainly dominated by the available bandwidth at the cell edge, in contrast to GSM-R where coverage level was the main planning parameter to be obeyed.

However, there are times when additional sites may be needed. This can occur when operators want to run higher-throughput use cases on top, such as automated train operation (ATO) with a higher grade of automation that includes video. So keep in mind that goals like this can require a denser network.

BBU architecture options are the next essential consideration for the RAN. Operators can choose a distributed architecture — where each site has its own baseband units (BBUs) — or a hotel architecture, where resources are pooled across multiple sites. The distributed architecture is more costly, while the hotel architecture offers significant savings. But if a pooled BBU fails, every connected site goes down. By providing a second BBU at a separate location as backup in case of failure, the hotel architecture can offer a balance of cost and resilience.

Understand the potential of a 5G core

The transformative capabilities of FRMCS rely on a resilient 5G core designed to meet the specific demands of railway operations. That means it can deliver high throughput and low latency for safety-critical services, while enabling high availability, resilience, and reliable operations.

Because this 5G core is cloud-native — unlike the GSM-R core network — it can provide other crucial advantages as well, such as running on an on-premises cloud platform. Or enabling more flexible operations, because software functions run in containers with spare capacity built into the platform. In addition, updates, security fixes, capacity

changes, automation, and new applications can be managed as part of normal lifecycle operations, because the 5G core is modular, software-defined and standards-based.

Be aware of mission-critical communications (MCX) advances

Using a standardized MCX framework, FRMCS provides interoperable voice, data, and video capabilities for railway operations. These offerings incorporate the resilience and prioritization required for safety-critical use, along with the functionality defined in 3GPP mission-critical domains. For example, this includes mission-critical push-to-talk (MCPTT), the 5G evolution of group voice communications that is central to railway operations. MCPTT delivers higher quality audio, faster push-to-talk setup and group management, along with advanced features such as dynamic group management and user prioritization.

MCData enables secure, reliable exchange of operational information, including ETCS train control data and critical messaging. MCVideo adds real-time video to and from moving trains, supporting applications such as HD CCTV, incident management and future automated train operations.

Strengthen security measures

This step is highly important, because moving to a 5G IP-based network expands the possibility of cyber attacks. That's because the foundation of GSM-R's time division multiplexing (TDM) provided a degree of natural protection, but a change to FRMCS extends the »attack surface.« As a result, operators need to take more deliberate security steps.

The first step is to recognize the Third Generation Partnership Project (3GPP) requirements for IPsec encryption from radio to core. In addition, European regulations are beginning to establish policies that consider secure rail communication a matter of national infrastructure protection.

However, compliance alone is not enough, and a more robust »zero-trust« approach is needed. This means limiting the ability of attackers to enter the network, while simultaneously using zoning to contain any potential damage if they do intrude. The goal, in other words, is to restrict what any attack can reach. Every network element should play a role in this approach, rather than relying on a single security measure, such as a firewall.

Resilient Satellite Communications **for Defence**

X. BERTRAN, SES. S.A., Luxembourg

Resilient Satellite Communications Needs

Modern defence operations are critically dependent on assured access to satellite-enabled communications. Command and Control (C2), intelligence dissemination, sensor-to-shooter connectivity, logistics, and multinational coordination all require uninterrupted information exchange across strategic, operational and tactical levels.

Recent conflicts have demonstrated that satellite communications (SATCOM) are no longer merely enabling capabilities but have become essential components of military operations and are therefore priority targets for electronic warfare, cyber operations, kinetic attacks and other counter-space activities.

The U.S. Space Force (USSF) Commercial Space Strategy and German Space Safety and Security Strategy both conclude that future military effectiveness depends on building resilient, diversified and hybrid space architectures rather than relying on a limited number of highly capable but vulnerable systems [1,2].

Resilience in satellite communications is the ability to maintain mission-critical connectivity despite deliberate attacks, technical failures or environmental disruptions. This extends beyond satellite survivability to include resilience across the complete communication chain: the space segment, the radio links, ground infrastructure, networks and user equipment. Modern resilience is achieved through architectural diversity rather than redundancy alone.

Hybrid constellations combining military, Allied and commercial capabilities, supported by multiple operators and multiple orbital regimes, significantly complicate

an adversary's ability to disrupt communications while allowing rapid reconfiguration when assets are degraded. The USSF therefore advocates hybrid architectures that integrate government-owned, Allied and commercial systems while avoiding dependence on any single provider or technology.

Particular emphasis is placed on interoperability, cyber resilience, diversified supply chains and the integration of proliferated commercial constellations into military communications architectures. A resilient SATCOM architecture spans several interconnected domains.

The German Space Safety and Security Strategy further emphasises that resilient satellite communications must support not only military forces but also government agencies, emergency services and critical national infrastructure [2]. Satellite communications are indispensable when terrestrial infrastructure has been degraded by natural disasters, cyber-attacks or armed conflict. At the same time, future users must be capable of continuing operations even when certain space services are unavailable, requiring resilient operational concepts, alternative communication paths and comprehensive mission planning. Germany therefore highlights the importance of combining national, European and commercial capabilities, strengthening European initiatives such as IRIS² and GOVSATCOM, while simultaneously developing sovereign capabilities and reducing critical dependencies [4, 6, 7].

Encompassing above are of course availability of budget, public value for money and other economic

considerations, to which the solution often lies in commercial partnerships as emphasised by the USSF strategy [1], as well as government to government to commercial players partnerships enabled through a strong employment of standards, typically driven by existing associations such as for example 3rd Generation Partnership Project (3GPP) or GSM Association (GSMA) or the NATO Standardization Office, all with the aim of ensuring interoperability of systems and operations.

In conclusion, resilient satellite communications can no longer be viewed as a single protected or proprietary closed satellite system but rather as an adaptive, distributed and hybrid ecosystem. Resilience is achieved through diversity across orbital regimes, service providers, communication links, network architectures and intelligent small form factor user terminals. Such an approach ensures that defence forces can preserve command and control, maintain operational speed and continue multi-domain operations even under sustained attack, thereby strengthening deterrence and increasing the overall effectiveness of modern military operations.

Domains of a resilient satellite communications architecture

A satellite communications system is typically segmented into:

1. Space domain,
2. Ground domain,
3. Link domain,
4. Network domain, and
5. User terminal domain.

The space domain is typically characterised by the orbit in which satellites are placed which includes GEO, MEO and LEO orbits. Multi-orbit diversity improves availability and survivability of resilient satellite-based communication systems and can and does extend the resiliency of terrestrial communication systems already today.

Large, proliferated LEO constellations provide redundancy through the sheer number of satellites, while GEO systems continue to deliver wide-area coverage and high-capacity strategic communications. MEO provides redundancy and resilience through orbit diversity, view diversity and enables, just as GEO, ground sites diversity. While GEO comes with a noticeable latency disadvantage, LEO and MEO system operate in latency ranges of existing terrestrial network systems (40 to 120 ms).

The ground domain encompasses gateway stations, network operation centres, mission control facilities and cloud-based network management systems, all of which must be geographically distributed and protected against cyber and physical attacks. They are also reliant on terrestrial or/and space based networks for interconnectivity, in most cases fibre networks on land or at sea. In defence applications, access to secure sites with redundancy may be a geographical challenge and one reason for additional requirements for the space domain to provide inter-satellites links or larger geographical satellite field of view.

The link domain comprises radio-frequency and optical communication links that require anti-jamming

techniques, adaptive modulation, beam steering, frequency agility, encryption and low-probability-of-intercept/low-probability-of-detection (LPI/LPD), and Effective Isotropic Radiated Power (EIRP) characteristics.

The network domain integrates routing, orchestration and service management across heterogeneous satellite operators and terrestrial networks, enabling seamless traffic migration during disruptions.

The USSF explicitly identifies the need for system-agnostic, multi-band, multi-orbit and machine-to-machine automated networking to support future hybrid military architectures.

And finally, user terminal domain represents the operational use of resilient SATCOM and are increasingly recognised as the most decisive elements of mission assurance and usability characterised by increasingly small form factors, enhanced mobility, low power consumption and simple ease of use.

It all starts with what the user needs and touches

Future defence terminals for resilient communications must support multi-band and multi-orbit operation, enabling automatic switching at least between MEO and LEO networks without interrupting ongoing communications. Whilst high performance services levels must be attained at least by using LEO and MEO orbits space domain, software-defined radios, electronically steered antennas and open standards enable rapid adaptation to evolving operational requirements and simplify integration with allied and commercial systems.

Terminals must also incorporate strong cybersecurity, secure key management, anti-jamming capabilities, resilient positioning and timing, and autonomous network selection based on real-time link quality.

For deployed forces, portability, low power consumption, rapid deployment and interoperability across coalition networks are equally important.

Rather than acting as fixed endpoints, future user terminals will become intelligent network nodes capable of dynamically selecting the optimal communication path while maintaining secure connectivity in contested electromagnetic environments.

As the use cases for user terminals in defence applications proliferate by small form factors (<50 cm x 50 cm) and high service levels (>250 Mbps throughput), emphasis must also be put on scalability of production of user terminals, access to high-grade, high-volume components, supply chain availability and security in case of crisis.

Implications on the Space and Link domain

The implications of these strategies create profound drivers towards the space domain system topology. For low latency up to near real time communications with an uneven user terminal density requirement often characterised by the need for dynamic and temporal concentration over regions, means that the space domain must deliver to ground domain constraints, a large variation of user terminal density typically centred around a country's geographic location or other areas of interest. To achieve this, a multi-orbit, multi-band space domain architecture spanning across LEO, MEO and

even GEO is the only way for an efficient programmatic, technical and economic implementation.

This is driven largely by the following considerations:

1. Ability to provide optimised interference, jamming, resistant user terminal density, volumes and minimum service levels for a global coverage,
2. Efficiency of the space domain in operations in terms of maximum value adding utilisation, typically ranging from 5 – 15 % for LEOs, up to 60 % for MEOs and near 100 % for GEOs,
3. Effect of inter-satellite links on latency whilst ensuring network redundancy and dealing with ground sites availability/connectivity,
4. Network redundancy to both physical and cybersecurity attacks,
5. Transportation to space considerations, fast deployment time,
6. Upgrade, maintenance and replenishment considerations,
7. Fiscal budget availability.

A multi-orbit, multi-band, low latency space domain is architecturally the way to go for resilient satellite-based communications.

Implications on the Ground, Network and User Terminal domain

There is no doubt that low latency is the key to connectivity experience and in any case inevitable for near real-time applications. Physics is in play and therefore distance of the communications path is key for improvement, but not the only factor, implying an optimisation between the use of different orbits. This applies very much so to the space to user terminal, space to gateway and the network (user to space to space/ground to ground) and the network topology of star or/and mesh which directly drives how data flows are organised. In order to avoid single points of failure, typically mesh topologies provide greater resilience subject to their implementation.

Important considerations are also:

1. User terminal management and additional functions (obfuscation, identity, authorisation),
2. Use of interoperable standards/modulations which allow the network domain to operate across heterogeneous systems, here 5G based networks are a strong consideration,
3. Ground sites diversity, geographic availability and network redundancy (ground/space) optimised for latency,
4. Network redundancy to both physical and cybersecurity attacks,
5. Upgrade and maintenance considerations,
6. Fiscal budget availability.

Proliferated LEOs have paved the way to extensive use of 3GPP standards in satellite communications, starting with 4G and there is no doubt that this path will continue into 5G and 6G technologies into the

future where the use of terrestrial technologies adapted for space will be key to build a truly resilient and interoperable communications system of systems and connect both satellites with terrestrial networks [5].

Ultimately in the long future beyond 2035, a seamless merge between terrestrial and non-terrestrial networks can be envisioned, the steps towards seamless worldwide access are being taken now.

How SES with meoSphere addresses these needs

The SES announced and developed meoSphere system is a new approach to space based resilient communications in a future hybrid multi-orbit, multi-band, low latency communications requirement [3]. It is built as a primary system to provide end users with services at the same time as it acts as a backbone fibre-like optical data relay network within a multi-orbit, multi-band, low latency hybrid and heterogeneous system of systems architecture and in addition a multi-mission platform by enabling a hosted payload capability (see figure 1).

It provides low latency, high-throughput services on small form factor user terminals using multi-band user links in Ka and Ka military reserved frequencies enabled through a 5G mesh network connectivity system. The design drivers for the payload accomplish also resistant to jamming, interference with digital beam forming, transparent mode, adding to its resilience characteristics.

The user terminal is defined in two form factors 25 cm x 25 cm and 50 cm x 50 cm with up to 1 Gbps throughput and even higher with the use of 1.3 m parabolic antennas for very high throughput use cases of multi Gbps services (see figure 2).

The 5G network allows for a segregation of a sovereign ground, user and ultimately the sovereign network whilst providing the capability for a secure use of a shared and individual segregated space domain simultaneously operated, reaching a new level of interoperability in a hybrid architecture requirement. Core to this ability is the use of 5G technologies and features and the implementation of a regenerative digital payload with optical inter-satellite links and encryption technologies.

The new approach is also characterised by a verticalized development and implementation model, which is based on a continuous and iterative deployment and upgrade roadmap and a de-risking of the iterative development phase with pathfinder missions in 2026, 2027 and 2028 with a target for the global coverage system in 2030. In accordance with service market demand the plan is to deploy every year additional satellites and ground systems, allowing also for upgrades to functionality, in order to dynamically meet demand and scale to volume effects, whilst maintaining versatility, multi-mission capability and other resilience characteristics important for defence applications (see figure 3).

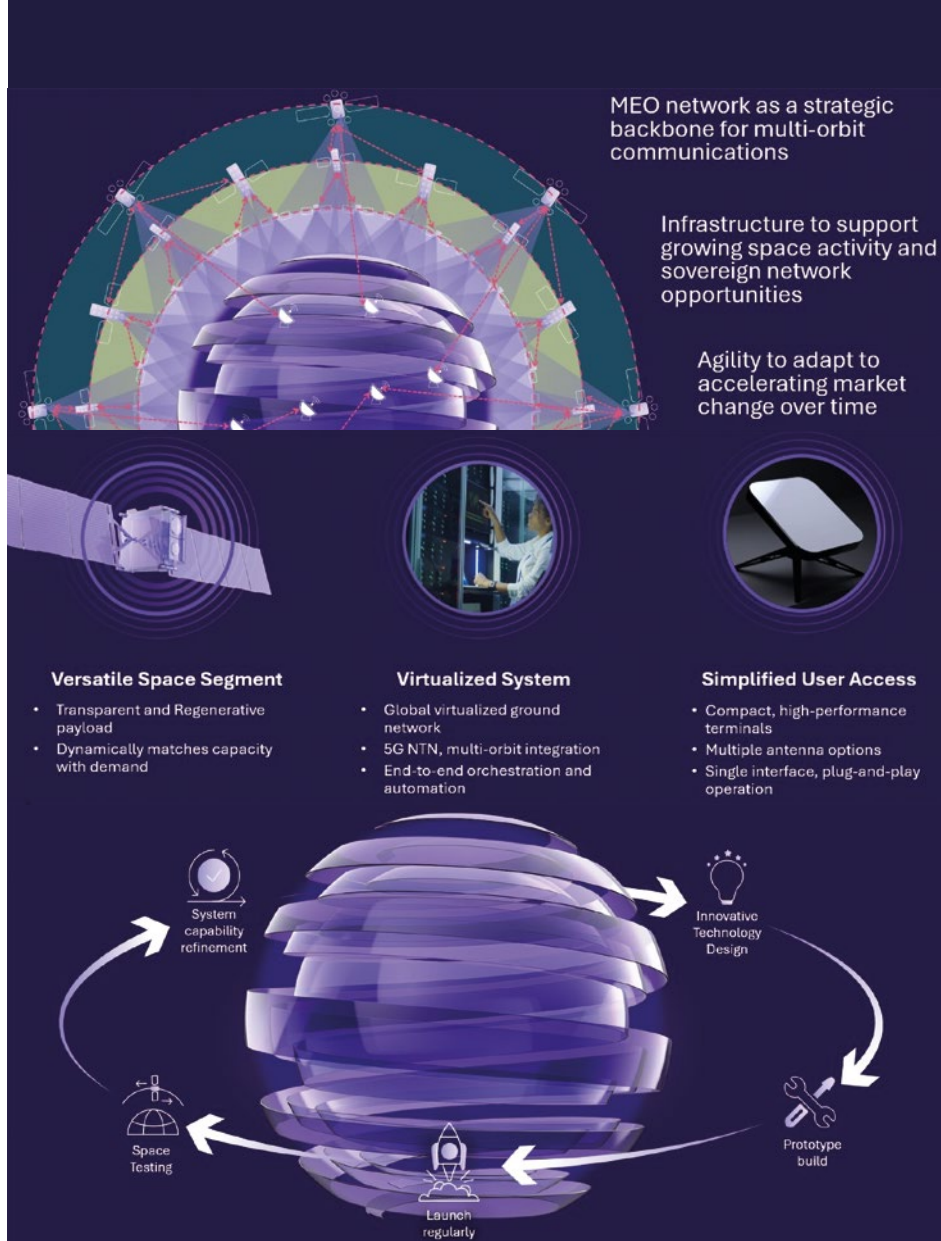


FIGURE 1
MEO as the Backbone of a Resilient Multi-Orbit Communications Architecture

FIGURE 2
Iterative Development Approach for meoSphere

FIGURE 3
Key Elements of the meoSphere Communications Architecture

As such therefore meoSphere enables with multi-mission, either:

1. further communications services in UHF, or
2. through data relay LEO based Direct-to-Device,
3. can also support enhanced Positioning, Navigation and Timing (PNT),
4. as well as Space Situational Awareness (SSA) and Surveillance, Reconnaissance & Tracking (SRT), as a data relay or through hosted payload missions,
5. act as a network and operational backbone for LEO constellations,
6. and provide for more defence specific sensor capability through its hosted payload capability.

SES today provides a multitude of multi-orbit and multi-band network services, either using GEO-MEO, for example in mobile, fixed and government markets as well as GEO-LEO. Through meoSphere the real power of a multi-orbit approach will become reality in a MEO-LEO service, that will allow through 5G to deploy most modern quality of services functionality to users, further increasing the effective utilisation of the system.

meoSphere will hence support maritime, terrestrial, aeronautical and space mission of armed forces with global, resilient and interoperable connectivity – pole to pole.

Encouraged by space strategies published by governmental actors, resilience in satellite-based communications with the adoption of terrestrial technologies will allow to implement resilient, diversified and hybrid space architectures called for in the strategies, not only for commercial companies but also for governments with sovereign and interoperable solutions which so far have been elusive. ●

Sources

- [1] U.S. Space Force Commercial Space Strategy, Department of Air Force, April 2024
- [2] Space Safety and Security Strategy, German Government, 2025
- [3] SES S.A. Webpage
- [4] Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027
- [5] 3GPP NTN Architecture, <https://www.3gpp.org/technologies/ntn-overview>
- [6] IRIS2 - Infrastructure for Resilience, Interconnectivity and Security by Satellite: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en
- [7] GOVSATCOM: EU GOVSATCOM is the satellite communications component of the European Union's Space programme: https://defence-industry-space.ec.europa.eu/eu-space/govsatcom-satellite-communications_en

VDE-Gremienarbeit im KI-Zeitalter

KOLUMNE

ZUM NACHDENKEN & MITREDEN

Reicht gesichertes Fachwissen noch?



→ **J. VIEBRANZ** Vice CMO, Brand,
Marketing & Communication, VDE Gruppe

Fragen Sie einen Chatbot, der auf einem großen Sprachmodell beruht, nach der Position eines Normungsgremiums zu einer technischen Sicherheitsfrage. Was zurückkommt, sieht aus wie eine Stellungnahme, mit Normverweisen, Tabellen und sauberer Gliederung. Beim Prüfen zeigt sich, dass Grenzwerte vermischt und Schutzmechanismen falsch zugeordnet sind. Auffallen kann das vor allem jemandem, der das Thema ohnehin kennt.

Hier stoßen zwei Arbeitsweisen aufeinander. Gremienarbeit ist langsam und zurechenbar. Sie lebt von Konsens, von Dokumentation und davon, dass am Ende benannte Fachleute für ein Ergebnis geradestehen. Die Öffentlichkeit, in der diese Ergebnisse ankommen sollen, folgt anderen Regeln. Dort entscheidet Aufmerksamkeit über Verbreitung, und zunehmend antworten Maschinen, bevor jemand die zuständige Fachgesellschaft überhaupt fragt.

Die ITG hat dazu bereits eine Kurzinformation veröffentlicht. »Mechanismen sozialer Netzwerke im öffentlichen Meinungsbild« beschreibt, wie Vorschlagsmechanismen und Bot-Netzwerke die Meinungsbildung verschieben. Dieser Blick geht nach außen, auf die Plattformen. Mich interessiert die Gegenrichtung, also das, was in unseren Gremien und Fachbereichen passiert, bevor die Verteilung überhaupt beginnt.

Ich schreibe das als jemand, dessen Beruf Sichtbarkeit ist. Der naheliegende Rat aus meiner Zunft lautet, zuzuspitzen und den Kanal zu bedienen, wie er gebaut ist. Dieser Rat ist nicht falsch. Er ist teuer.

Während Fachleute mit Normen, Berechnungen und Erfahrungswerten argumentieren, setzt sich draußen oft ein einziges Wort durch. Sobald eine Rahmung sitzt, werden neue Informationen einsortiert statt geprüft. Selbst der offenste Gremienbericht gilt dann als Lobbyarbeit, weil der Rahmen schon steht.

Darauf reagieren wir in den Fachgesellschaften mit zwei Reflexen. Wir werden genauer und schreiben das nächste Faktenpapier, in der Hoffnung, dass es diesmal wirkt. Oder wir gehen dorthin, wo die anderen sind, und machen es so, wie die anderen es machen. Verständlicher zu werden kostet uns nichts und ist überfällig. Der Preis liegt in der Zuspitzung, und das sind zwei verschiedene Dinge.

Vertrauen hat drei Stufen. Prüfbarkeit sagt, wo etwas steht, und das kann inzwischen jedes Modell. Herkunft heißt, dass ein benennbarer Mensch geradesteht. Haftung heißt, dass jemand mit seinem Namen etwas riskiert. Normung ist genau das, diese drei Stufen in einem geordneten Verfahren. Wer den Weg zur Aussage wegschneidet, gibt die beiden oberen Stufen ab.

Nur zeigen wir diesen Weg fast nie. In einer öffentlichen Einspruchsberatung bei der DKE wurden über 750 Stellungnahmen einzeln beantwortet, von Fachleuten aus Industrie, Forschung und Verbraucherschutz, über Monate. Außerhalb des Sitzungsraums hat davon praktisch niemand erfahren. Dabei ist genau das der Teil, den kein Modell erzeugen kann.

Wer dafür zuständig ist, ist in den meisten Organisationen ungeklärt. Der Fachbereich sagt, das sei Sache der Kommunikation. Die Kommunikation sagt, das sei fachlich. In dieser Lücke entstehen die Wörter, mit denen später Gesetze begründet werden.

Deshalb drei Fragen an Sie. Was würde es kosten, von Ihrer Arbeit auch den Weg dorthin zu zeigen, und was gewännen Sie dafür? Wenn die Vokabulare für maschinenlesbare Herkunft seit über einem Jahrzehnt bereitliegen und niemand sie abrufen, wer müsste das lösen? Und ist unsere Zurückhaltung im lauten Raum Haltung oder Gewohnheit?

Reichweite lässt sich kaufen. Vertrauen nicht. •



Federated Learning: A human-centered perspective

• R. GLITZA • L. BECKER • R. MARTIN, Institute of Communication Acoustics, Ruhr-Universität Bochum
 • V. LANGHOLF • U. WILKENS, Institute of Work Science, Ruhr-Universität Bochum
 • D. KOLOSSA, Electronic Systems of Medical Engineering, Technische Universität Berlin

Abstract

Federated learning (FL) enables distributed clients to collaboratively train machine-learning models without centralizing raw data, making it attractive for privacy-sensitive and heterogeneous application domains. However, successful deployment requires more than selecting an aggregation algorithm. Organizations must manage non-IID data, personalization of clients, privacy and security threats, as well as changing human roles. After introducing the basic FL workflow and clustered FL as a response to client heterogeneity, we discuss privacy and security risks. Beyond algorithmic aspects, we also emphasize the human-centered aspects of federated learning, including issues of explainability, fairness, and the involvement of human experts. Thus, we provide insights into the responsible and effective deployment of federated learning in organizations, with particular attention to privacy-preserving design and heterogeneous data handling.

1. Introduction

Recently, artificial intelligence (AI) gained tremendous significance in research, product development, and societal interest. As a consequence, AI-based solutions have become ubiquitous companions in our daily lives. Using vast amounts of data, it has been possible to develop generative AI algorithms that change the way we work. Machine learning (ML) algorithms for text generation, code-writing, autonomous driving, diagnostics for healthcare, and many more bring unprecedented possibilities, accelerate productivity, and enhance the quality of products and services. These ML models are often trained and deployed on massive commercial server platforms. To compute model output predictions, one has to upload raw data to the server platform over the Internet. In some cases, sending sensitive data over the Internet is not feasible due to privacy or security concerns. Regulations like the European Union General Data Protection Regulation (EU GDPR) [1] call for privacy-enhancing methods, such as data minimization and privacy-by-design in the development and deployment of ML algorithms. To mitigate these concerns, both data acquisition and model inference could be performed locally on the client device — for example, a smartphone, a car, or a server within a local network. This development, often referred to as Edge AI, has been enabled by the rapid increase in computational power and efficiency of mobile microprocessor and neural processing units. Edge AI brings the advantages of not just increasing privacy, but also reducing latency and bitrates on networks, which are all crucial in safety-critical

applications such as autonomous driving or fault detection. Furthermore, it is possible to significantly enhance the performance of ML models by incorporating data of individual users into the training process. However, due to regulations like the EU GDPR and user concerns with respect to sharing private data, collecting the data in a single data center is often not possible. While it would be desirable to fine-tune the model with local data, updating a model in isolation from other edge devices may lead to degraded models in comparison to a pre-trained global model [2].

Federated Learning (FL) [3] introduces innovative methods to address several challenges inherent in traditional centralized machine learning and data privacy. As shown in Figure 1, FL trains a centralized model with input from multiple edge devices, known as clients, each of which uses its own locally available data. Instead of sharing raw data, each client computes updates to the model parameters based on its local data, and these weight updates are then sent to a central server. The central server aggregates these updates, typically by averaging them, to refine the global model [4].

Thus, FL allows data owners to benefit from collective model training without exposing sensitive information. This characteristic makes FL an appealing solution for applications that handle user-sensitive data, such as in healthcare and finance, where privacy and data security are critical. However, when privacy is no issue and it is possible to transmit raw data, a centralized training may perform better than FL [5].

Yet, FL comes with its own set of challenges, such as model performance or communication overhead in heterogeneous data environments [6], [7] and model safety [8]. Therefore, the objective of this article is to shed light on these issues and place them in the context of socio-technical AI systems, including implications for human role development in organizations.

II. Fundamentals of Federated Learning

Federated Learning (FL) aims to overcome challenges related to data privacy and data availability by allowing multiple clients, such as mobile devices or edge nodes, to collaboratively train a model without sharing their raw data. Instead of centralizing data in a single server, FL keeps the data on each device and aggregates only the model updates to improve the global model. This enables the use of decentralized data while maintaining privacy, as sensitive information never leaves the local devices.

A. BASIC FEDERATED LEARNING ALGORITHM

In its standard implementation, FL operates as a synchronous three-step iterative procedure, where each iteration constitutes a communication round with index τ , in which M clients update their local model θ using gradient descent learning. In each communication round, the following steps are conducted:

- 1) The communication round τ starts with M clients $i \in 1, \dots, M$ downloading the global model $\theta^{\tau-1}$ from the previous round from the central server to synchronize their local ML models.

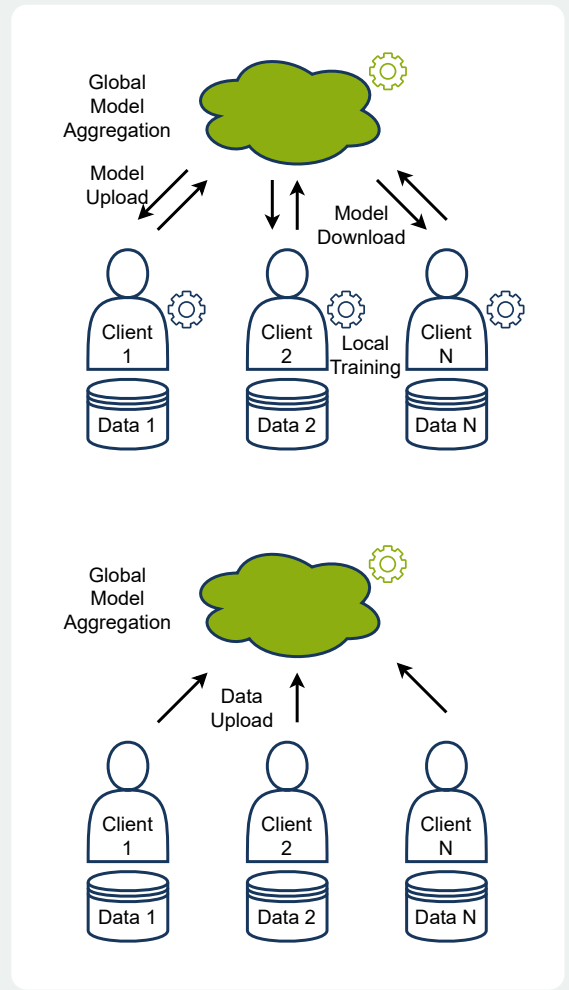
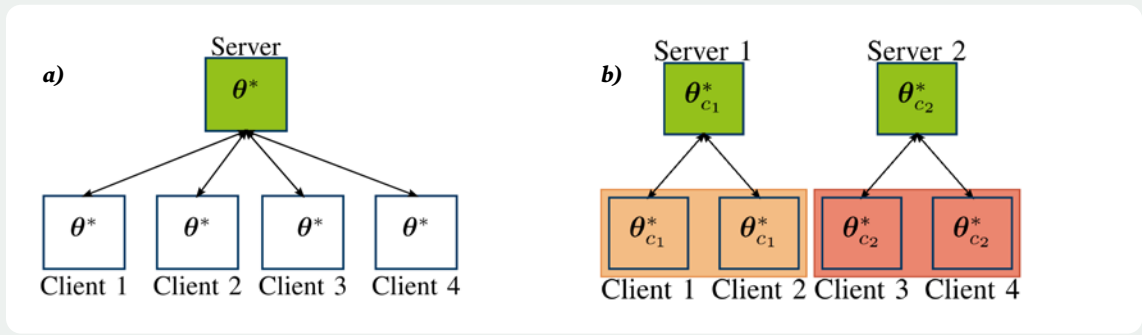


FIGURE 1

Federated (top) versus centralized learning (bottom)

- 2) Clients $i \in 1, \dots, M$ train and improve this model locally on their respective local data D_i for a specified number of training steps. The weight update vectors $\Delta\theta_i^\tau$ are determined by computing the changes of the model weights between the global and the new local model, $\Delta\theta_i^\tau = \text{SGD}(\theta^{\tau-1}, D_i) - \theta^{\tau-1}$, (1) where $\theta^{\tau-1}$ represents the global model of the previous communication round $\tau-1$ and SGD denotes a stochastic gradient descent optimizer.
- 3) In the last step all clients (or a randomly selected subset of the clients) upload their weight update vectors $\Delta\theta_i^\tau$ to the server, which then aggregates them using a weighted sum to form the new global model $\theta^\tau = \theta^{\tau-1} + \sum_{i=1}^M \sigma_i \Delta\theta_i^\tau$, (2) where θ^τ is the global weight vector for the current communication round τ , and σ_i is the impact factor of client i . The impact factors specifies the contribution of each client to the global model. This impact factor may weigh the relative amount of data each client trained on, the relative number of local training steps, or the results of local validation loss computations [5].

**FIGURE 2**

FL and clustered FL scenarios with four partially incongruent clients. Each client holds a neural model θ^* . a) Basic FL scenario with one server. b) Clustered FL scenario. Congruent clients are grouped together in clusters c_1 and c_2 , and synchronize with their specific server models.

The above steps are repeated until a maximum number of communication rounds $\tau_{\max}$ or another termination criterion is reached.

B. CLUSTERED FEDERATED LEARNING

Clustered federated learning (CFL) is an extension of the standard FL framework that aims to address the issue of statistical heterogeneity among clients. In real-world scenarios, data distributions across different clients can be highly non-IID (not independent and identically distributed), which can significantly degrade the performance of a single global model. CFL, as proposed by Sattler et al. [9], addresses this by aggregating clients into groups based on the similarity of their data distributions, allowing the training of specialized models for each cluster on the central server.

The CFL process begins with an initial training phase, where all clients participate in training of a preliminary global model. After this initial phase, clients are clustered according to certain criteria, such as similarities of model weight updates [10] or other statistical properties of their local data [11]. These clusters c are then used to train specialized models for the clients in each cluster, resulting in better model approximations of the data characteristics of each client. This clustering mechanism ensures that the differences in data distributions are properly accounted for, thus enhancing both the efficiency and the accuracy of federated training, especially in scenarios with significant diversity in data [12]. Moreover, CFL can help reduce negative transfer, a phenomenon where training a single global model leads to suboptimal performance due to conflicting data distributions.

C. DATA PRIVACY IN FEDERATED LEARNING

Although the FL training paradigm ensures that data samples remain on edge devices, it does not inherently prevent data reconstruction or, more directly, the inference of meta-data. These privacy attacks are based on accumulated weight updates and are a result of dishonest but non-intrusive behavior by the server, a dishonest client, or a combination of both. Such attacks range from GAN (generative adversarial network) attacks which generate virtual samples of the same distribution as a targeted client [13] to completely

reconstructing training data and labels from a single intercepted gradient or weight update using a gradient descent scheme [14], [15].

In contrast to passive attacks, which aim to infer sensitive information without disrupting the learning process, active attacks involve adversaries who intentionally interfere with the FL workflow to degrade model performance or introduce hidden behaviors. These attacks can be launched by malicious clients or even a compromised server and pose a serious threat to model integrity and trustworthiness. A common form is the data poisoning attack, where adversaries inject carefully crafted data or manipulate labels in their local dataset. This malicious input leads to degraded model behavior, even though the attacker contributes only a small fraction of the data [8]. Additionally, the adversary can attempt to design its own weight updates so that a designated target client may leak confidential information after being indirectly influenced by these weight updates (backdoor attacks) [16]. These attacks can be further reinforced when combined with sybil attacks: by masquerading as multiple clients, a single adversary can appear as many genuine clients and thus, increase its influence on the FL scheme [17]. A visual outline of the passive and active attacks against FL is depicted in Figures 3 and 4, respectively. Consequently, measures should be taken which render the system robust against adversaries.

A reliable privacy-preserving technique is using a homomorphic encryption (HE) system such as Paillier [18]. The key advantage of homomorphic encryption is that arithmetic operations, such as weight averaging, can be performed on the encrypted representations. Using HE, clients locally encrypt their weight updates. Then, the server treats these updates as in conventional FL and computes an average weight update. This average (encrypted) weight update is broadcasted to all clients that decrypt the global weight update and apply it locally as in standard FL. While HE is a strong method for privacy preservation, its computational cost scales with ciphertext size, making HE impractical in some settings [18].

Alternatively, clients can add carefully tailored noise to their weight updates (differential privacy). This procedure is easy and cost-efficient to implement while reducing privacy leakage under passive attacks.

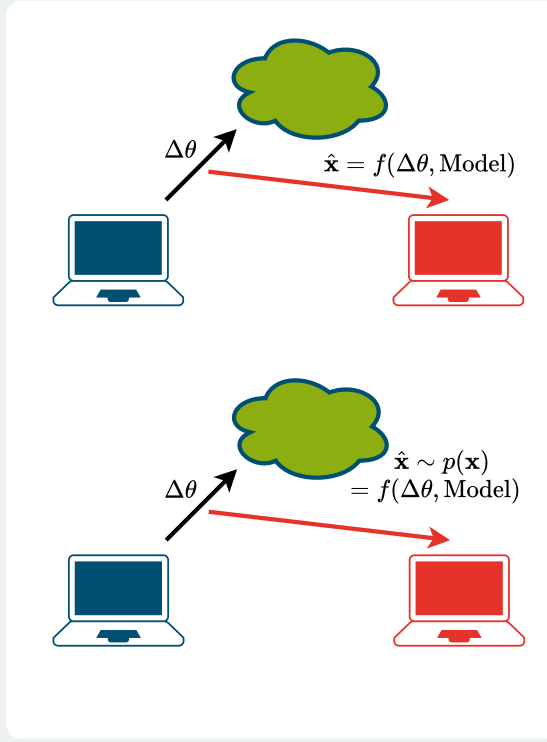


FIGURE 3 Passive attacks against FL

- (a) Model inversion attack: based on intercepted weight updates $\Delta\theta$, the attacker leverages information about the model to reconstruct the training data $\hat{x}$ which led to $\Delta\theta$ [14], [15].
- (b) GAN-based attack: based on intercepted weight updates $\Delta\theta$, the attacker leverages information about the model to estimate the victim client's data generating distribution $p(x)$ from which the training data $\hat{x}$ can be sampled [13].

However, since noise also affects the training of the system, slight losses in performance are to be expected for the global model [19], [20].

To counteract active attacks, AUROR^[21], a statistical mechanism, identifies malicious clients by clustering the updates of participants and eliminating outliers. Based on the principle that honest clients' updates show a consistent distribution, the method isolates and removes contributions from clusters exhibiting anomalous behavior, preserving model integrity against adversarial updates. Other detection methods focus on recognizing and removing backdoors by analyzing the model's activation statistics and latent representations. These algorithms detect discrepancies between the representations of clean and backdoor-enabled inputs, isolating and neutralizing the adversarial influence [22]. While some sophisticated attackers may attempt to obscure backdoors, detection techniques provide a vital line of defense, ensuring model security even in complex FL environments.

In conclusion, while FL offers substantial advantages for data privacy by keeping data on local devices, it is still vulnerable to various privacy and security threats, including passive and active adversarial attacks. Therefore, ensuring privacy and security in FL, however, remains a balancing act between robust protections and practical feasibility, and will require monitoring model performance during deployment.

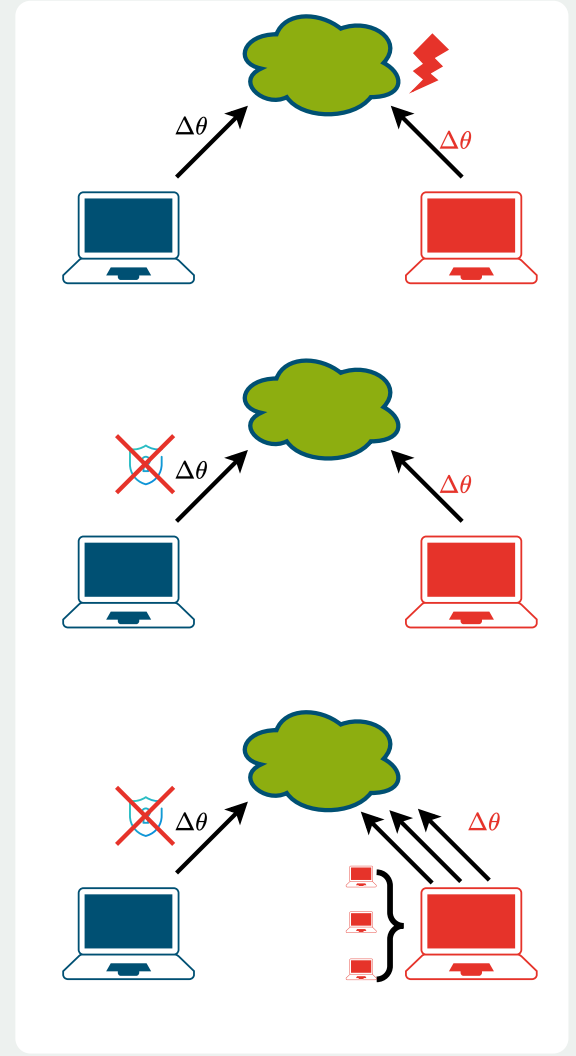


FIGURE 4 Active attacks against FL

- (a) Poisoning attack: the attacker injects malicious weight updates $\Delta\theta$ to sabotage the whole FL process for all clients (e.g., the process does not converge) [8].
- (b) Backdoor attack: the attacker injects malicious weight updates $\Delta\theta$ leading to victim clients unintentionally exposing sensitive information [16].
- (c) Sybil attack: the attacker amplifies the impact of its own weight updates $\Delta\theta$ by pretending to be a set of clients. Can be combined with poisoning attacks [17].

III. Implementation challenges and solutions

A. NON-IID DATA DISTRIBUTIONS

In FL, clients typically operate on private data generated in unique contexts, leading to non-IID data across the federation. This statistical heterogeneity reflects the natural diversity of user behavior, device capabilities, and environmental conditions. Common forms of non-IIDness include label distribution skew – where clients see only a subset of classes – and feature distribution skew, resulting from differences in sensors or data domains. Additionally, quantity skew (variable dataset sizes) and temporal drift (shifting data distributions over time) are prevalent. These deviations from the IID assumption are typical in real-world federated learning scenarios – whether in cross-device FL, where data originates from many individual users (e.g., smartphones), or in cross-silo FL, where data is distributed across institutions (e.g., hospitals). In both cases, heterogeneity is the norm rather than the exception [23].

Non-IID data introduces several critical challenges to FL. First, it significantly hampers convergence and stability. Clients trained on disparate data may produce conflicting updates, causing the global model to oscillate or converge slowly. This phenomenon, known as client drift, has been shown to degrade both the convergence rate and the quality of the final model [24]. Second, accuracy degradation is a consistent empirical finding: Zhao et al. [25] showed that in scenarios where clients possess only single-class data, classification accuracy can drop by more than 50% compared to the IID case. Third, fairness becomes a pressing concern, as a single global model may systematically underperform for clients with rare or unique data patterns, exacerbating bias and potentially leading to inequitable outcomes [26]. Finally, the non-IID setting complicates the balance between global generalization and local specialization, prompting the need for models that can adapt effectively to individual clients while leveraging the collective knowledge of the federation.

Several strategies have been proposed to mitigate the impact of non-IID data in FL. One prominent direction involves modifying the optimization algorithm to account for heterogeneity. FedProx [27] introduces a proximal term to local objectives, discouraging local models from deviating too far from the global model. SCAFFOLD [24] further improves convergence by using control variates to correct for client drift. Another line of work focuses on data sharing and augmentation; Zhao et al. [25] demonstrated that incorporating even a small globally shared dataset can significantly align model updates and improve performance. In addition, clustered federated learning methods, such as those proposed by Sattler et al. in [9], partition clients into groups with similar data distributions, enabling more specialized model training within each cluster. Additionally, knowledge distillation approaches like FedDF [28] enable clients to share knowledge through soft labels rather than model weights, facilitating aggregation even in highly heterogeneous environments. These strategies aim to reduce the impact of divergent data distributions while preserving privacy and communication efficiency.

B. PERSONALIZATION

Personalization has emerged as a compelling solution to the non-IID challenge, offering each client a tailored model that better reflects its local data. The simplest technique is local fine-tuning that adapts the global model using each client's local data. While effective, this approach risks overfitting when data is scarce. More advanced methods include personalization layers, such as in FedPer [29], which retain global base layers but allow clients to train private output layers. Meta-learning strategies like Per-FedAvg [30] take this further by learning an initialization that enables rapid client-specific adaptation with few local updates. Multi-task learning formulations, such as MOCHA [31], treat each client's task as related but distinct, optimizing both shared and client-specific components. Lastly, hybrid approaches like Ditto [32] and pFedMARRL [33] train global and personalized models in parallel, regularizing the latter to stay close to the former. These personalization strategies offer a principled way to reconcile global collaboration with local specialization, yielding robust performance even in highly heterogeneous federations.

IV. The human factor in Federated Learning

FL introduces a decentralized approach to machine learning that inherently relies on client data and as such on the participation of individual users or institutions. While this architecture offers substantial privacy advantages and scalability, it also foregrounds the importance of the human factor in the life cycle of federated systems. Human decisions influence everything from data collection and sharing preferences to model performance and ethical considerations. Therefore, FL must not only be seen as a technical system but also as a socio-technical construct in which users, developers, and stakeholders interact with and shape the learning process [34].

A. DATA LABELING, EXPLAINABILITY, RESPONSIBILITY, AND FAIRNESS

A critical component of any machine learning system is data labeling, and this becomes particularly complex in FL. In decentralized environments, labels may be inconsistent, sparse, or subject to user interpretation, especially in domains such as healthcare, image analysis, or speech and audio processing. The lack of centralized oversight makes it difficult to enforce labeling standards or perform quality checks, which can lead to heterogeneous and noisy annotations. Crowd-sourced or local labeling processes also carry cultural, contextual, or subjective biases that may not generalize well across other clients. Ensuring high-quality, consistent labeling thus becomes a human-centric challenge that significantly impacts the model's generalizability and fairness.

Explainability is another major concern in human-centered FL systems. Users or domain experts interacting with model predictions, such as clinicians in medical FL, need to understand how a model arrived at its conclusions. However, explainability becomes more difficult when data is distributed and models are personalized. Techniques for federated explainability must account for client-specific behavior without revealing sensitive information. Striking a balance

between transparency and privacy is not only a technical challenge but also a human-centered requirement that determines trust and acceptance [35].

Responsibility and accountability in FL are diffused across various actors. When a model fails or produces harmful predictions, it is often unclear who should be held responsible: the model developer, the data contributor, the platform provider, or the system integrator? Unlike centralized systems, FL lacks a clear locus of control, which complicates traditional accountability structures. Moreover, participants may not fully understand the implications of their involvement, particularly in cross-silo FL where contributions might have legal or ethical ramifications. Human-centered FL design must therefore consider mechanisms for informed consent, liability management, and stakeholder education [36].

Finally, discrimination and fairness pose critical challenges in FL settings. Non-IID data distributions, where users contribute data that reflect their unique environments, can lead to biased models that work well for some groups but poorly for others. These disparities may go unnoticed if underrepresented groups are not adequately included in the federated network. Moreover, decentralized training reduces the visibility of demographic imbalances, making it harder to audit for fairness. It is essential to incorporate human-centered fairness metrics and participatory evaluation strategies to detect and mitigate discriminatory behavior in federated models [37].

B. IMPLICATIONS FOR HUMAN ROLE DEVELOPMENT

While the organizational integration of AI-based workflows and their proper application is a challenge in its own right, a number of additional issues arise when AI models make use of FL, as outlined in the previous sections.

When FL is involved in training a centralized model, the integration and interactions of clients and a centralized server move into the center of interest. While human experts are still involved in the specification and design stage of the client-server system, they are not much involved in the actual data collection and annotation process. As a result, data heterogeneity becomes a major challenge. Furthermore, ensuring explainable results might require in-depth analysis of model updates and their long-term effect on model performance.

Therefore, developers now have to focus on the supervision of the data collection process and are responsible for defining and monitoring appropriate application-related evaluation criteria. Thus, the human role shifts from the curation of raw data towards monitoring model updates and the performance of the AI model, including the detection of adversarial attacks. This could also entail running a multitude of models which were trained on different client data sets and additional backup models on predefined test data in order to detect deviation from the expected behavior early on. This process becomes even more challenging when FL is used in combination with a personalization of clients and real-time user feedback. Obviously, the development and deployment of large-scale FL methods will require the expertise

of multiple disciplines ranging from application domain developers to communication systems and IT security experts.

The shift of human roles when applying FL calls for organizational efforts to reduce potential pitfalls and support meaningful work through continuous development of skills and work characteristics. Research on human-centered job design suggests that AI could increase or decrease the meaningfulness of work, depending on whether it amplifies, replaces, or redirects human capabilities toward controlling and operating AI systems [38]. Therefore, the following human-centered measures can help to support the introduction and maintenance of FL-based system design:

Job crafting and participatory job design:

Focusing on monitoring and testing AI systems can negatively impact the perception of autonomy and the importance of one's work. This can be counteracted through individual and organizational measures. Individual approaches consist of proactively modifying and developing one's organizational identity and are often referred to as job or identity crafting [39]. Organizational approaches include company role development measures that clarify and update work roles by clarifying expectations and differentiating human-AI roles, thereby counteracting the risk of loss of meaning, deskilling, and reduced autonomy [40].

Change process aimed at work redesign:

Research on AI-driven transformation shows that it is most successful when the focus is not solely on implementing an AI-based system but on redesigning work. This includes clear objectives, consistent training, transparent rules, genuine participation, and a management team that views AI as a long-term organizational transformation [41].

Competence development: The changing role of human experts is also accompanied by shifting competency requirements. This can apply both to the shift in the roles of software engineers – from processing raw data to monitoring the performance of AI models – as described above, and to people at the client level. The new requirements are therefore highly context-dependent. Consequently, the respective change process should take into account whether the competency requirements primarily concern AI/FL competencies or subject-matter and methodological competencies.

In summary, conscious role development practices are needed to ensure the successful introduction and operation of FL-based AI systems, as well as to mitigate intrinsic risks in a proactive fashion.

V. Conclusion

This paper provides a brief introduction to federated learning (FL), its advantages and challenges, and highlights measures for integrating human responsibilities and role development in this process. We position FL not merely as an algorithmic alternative to centralized learning but as a socio-technical innovation that, when properly deployed, can reconcile data-driven value creation with standards for privacy, fairness, and workforce participation. Properly deployed, FL will help organizations to remain agile and shorten the path to AI systems based on large-scale data.

Acknowledgement

This work has been funded by the German Federal Ministry of Research, Technology and Space (BMFTR) within the Innovations for Tomorrow's Production, Services, and Work program (HUMAINE, funding number 02L19C200).

References

- [1] "General Data Protection Regulation," May 2016. [Online]. Available: <http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng>
- [2] J. Ding, E. Tramel, A. K. Sahu, S. Wu, S. Avestimehr, and T. Zhang, "Federated Learning Challenges and Opportunities: An Outlook," in ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), May 2022, pp. 8752–8756.
- [3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. PMLR, Apr. 2017, pp. 1273–1282.
- [4] Q. Wu, K. He, and X. Chen, "Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge Based Framework," IEEE Open Journal of the Computer Society, vol. 1, pp. 35–44, Jan. 2020.
- [5] R. Glitza, L. Becker, and R. Martin, "Unsupervised Anomalous Sound Detection Using Loss-Weighted Clustered Federated Pre-Training," in 2024 IEEE 34th International Workshop on Machine Learning for Signal Processing (MLSP), Sep. 2024, pp. 1–6.
- [6] —, "Global vs. Local Federated Learning in Heterogeneous Acoustic Environments," in Speech Communication; 15th ITG Conference, Sep. 2023, pp. 171–175.
- [7] W. Yu, J. Freiwald, S. Tewes, F. Huennemeyer, and D. Kolossa, "Federated learning in ASR: Not as easy as you think," in Speech Communication; 14th ITG Conference. VDE, 2021, pp. 1–5.
- [8] A. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing Federated Learning through an Adversarial Lens," International Conference on Machine Learning, 2018.
- [9] F. Sattler, K.-R. Müller, and W. Samek, "Clustered Federated Learning: Model-Agnostic Distributed Multitask Optimization Under Privacy Constraints," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 8, pp. 3710–3722, Aug. 2021.
- [10] A. Nelus, R. Glitza, and R. Martin, "Unsupervised Clustered Federated Learning in Complex Multi-source Acoustic Environments," in 29th European Signal Processing Conference, Aug. 2021, pp. 1115–1119.
- [11] F.-E. Yang, C.-Y. Wang, and Y.-C. F. Wang, "Efficient model personalization in federated learning via client-specific prompt generation," in 2023 IEEE/CVF International Conference on Computer Vision (ICCV), 2023, pp. 19 102–19 111.
- [12] C. Briggs, Z. Fan, and P. Andras, "Federated learning with hierarchical clustering of local updates to improve training on non-IID data," IEEE International Joint Conference on Neural Network, pp. 1–9, 2020.
- [13] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning," arXiv: Cryptography and Security, Feb. 2017.
- [14] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in Advances in Neural Information Processing Systems, H. Wallach et al., Ed., vol. 32. Curran Associates, Inc., 2019.
- [15] B. Zhao, K. R. Mopuri, and H. Bilen, "iDLG: Improved deep leakage from gradients," 2020. [Online]. Available: <https://arxiv.org/abs/2001.02610>
- [16] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, and V. Shmatikov, "How To Backdoor Federated Learning," International Conference on Artificial Intelligence and Statistics, pp. 2938–2948, Jul. 2018.
- [17] C. Fung, C. J. M. Yoon, and I. Beschastnikh, "The limitations of federated learning in sybil settings," in 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). San Sebastian: USENIX Association, Oct. 2020, pp. 301–316.
- [18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," International Conference on the Theory and Application of Cryptographic Techniques, vol. 1592, pp. 223–238, May 1999.
- [19] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," Theory of Cryptography Conference, vol. 3876, pp. 265–284, Mar. 2006.
- [20] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," Foundations and Trends® in Theoretical Computer Science, Aug. 2014.
- [21] S. Shen, S. Tople, and P. Saxena, "Auror: Defending Against Poisoning Attacks in Collaborative Deep Learning Systems," in Proc. 32nd Annual Conference on Computer Security Applications, pp. 508–519, Dec. 2016.
- [22] B. Wang, Y. Yao, S. Shan, H. Li, B. Viswanath, H. Zheng, and B. Y. Zhao, "Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks," IEEE Symposium on Security and Privacy, pp. 707–723, May 2019.
- [23] P. Kairouz, B. H. McMahan, and B. Avent et al., "Advances and Open Problems in Federated Learning," Found. Trends Mach. Learn., vol. 14, pp. 1–210, Mar. 2021.
- [24] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, "SCAFFOLD: Stochastic controlled averaging for federated learning," in Proceedings of the 37th International Conference on Machine Learning, vol. 119. PMLR, 13–18 Jul 2020, pp. 5132–5143.
- [25] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated Learning with Non-IID Data," 2018. Available: <https://arxiv.org/abs/1806.00582>
- [26] M. Mohri, G. Sivek, and A. T. Suresh, "Agnostic federated learning," in Proceedings of the 36th International Conference on Machine Learning, vol. 97. PMLR, 09–15 Jun 2019, pp. 4615–4625.
- [27] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated Optimization in Heterogeneous Networks," Conference on Machine Learning and Systems, vol. 2, pp. 429–450, Mar. 2020.
- [28] T. Lin, L. Kong, S. U. Stich, and M. Jaggi, "Ensemble Distillation for Robust Model Fusion in Federated Learning," in 34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada, Jun. 2020.
- [29] M. G. Arivazhagan, V. Aggarwal, A. K. Singh, and S. Choudhary, "Federated learning with personalization layers," 2019. Available: <https://arxiv.org/abs/1912.00818>
- [30] A. Fallah, A. Mokhtari, and A. Ozdaglar, "Personalized Federated Learning with Theoretical Guarantees: A Model-Agnostic Meta-Learning Approach," Neural Information Processing Systems, vol. 33, pp. 3557–3568, 2020.
- [31] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated Multi-Task Learning," in Advances in Neural Information Processing Systems, vol. 30. Curran Associates, Inc., 2017.
- [32] T. Li, S. Hu, A. Beirami, and V. Smith, "Ditto: Fair and Robust Federated Learning Through Personalization," in Proceedings of the 38th International Conference on Machine Learning, PMLR 139, 2021.
- [33] R. Glitza, L. Becker, and R. Martin, "Cooperative multi-agent reinforcement learning for adaptive aggregation in semi-supervised federated learning with non-iid data," in 2026 IEEE International Conference on Acoustics, Speech and Signal Processing, 2026, pp. 1151–1155.
- [34] O. Aouedi, A. Sacco, L. U. Khan, D. C. Nguyen, and M. Guizani, "Federated Learning for Human Activity Recognition: Overview, Advances, and Challenges," IEEE Open Journal of the Communications Society, vol. 5, pp. 7341–7367, 2024.
- [35] J. L. C. B'arcena, M. Daole, P. Ducange, F. Marcelloni, A. Renda, F. Ruffini, and A. Schiavo, "Fed-XAI: Federated Learning of Explainable Artificial Intelligence Models," Proceedings of the 3rd Italian Workshop on Explainable Artificial Intelligence, pp. 104–117, 2022.
- [36] N. Baracaldo, A. Anwar, M. Purcell, A. Rawat, M. Sinn, B. Altakrouri, D. Balta, M. Sellami, P. Kuhn, U. Schopp, and M. Buchinger, "Towards an Accountable and Reproducible Federated Learning: A FactSheets Approach," arXiv.org, 2022.
- [37] T. Salazar, H. Araujo, A. Alberto Cano, and P. H. Abreu, "A Survey on Group Fairness in Federated Learning: Challenges, Taxonomy of Solutions and Directions for Future Research," Artificial Intelligence Review, vol. 59, no. 81, 2026.
- [38] S. Banks and P. Formosa, "The ethical implications of artificial intelligence (AI) for meaningful work," Journal of Business Ethics, vol. 185, no. 4, p. 725–740, Feb. 2023.
- [39] R. Zhao, L. Niu, S. Wang, and Z. Chen, "Who am I with AI? Occupational identity crafting in human-AI workplaces," International Journal of Information Management, vol. 86, p. 102990, Feb. 2026.
- [40] V. Langholf and U. Wilkens, "Pathway to work with AI: Testing the clAIr role development method in an industrial work environment," Zeitschrift für Arbeitswissenschaft, vol. 78, no. 3, p. 377–386, Sep. 2024.
- [41] T. Tavantzis, S. Lambiasi, D. Russo, and R. Feldt, "From challenge to change: Design principles for AI transformations," 2025. Available: <https://arxiv.org/abs/2512.0553>



VDE ITG Fachausschuss 7.3. Mikrowellentechnik Klausurtagung 2026

- **G. HAMBERGER**, Rohde & Schwarz GmbH & Co. KG
- **M. EBERSPÄCHER**, Technische Hochschule Würzburg-Schweinfurt / Balluff GmbH

Der VDE ITG-Fachausschuss 7.3 Mikrowellentechnik traf sich am 22. und 23. Juli 2026 zu seiner diesjährigen Klausurtagung bei Rohde & Schwarz in München. 14 Mitglieder aus Wissenschaft und Industrie kamen zusammen, um aktuelle fachliche Themen zu diskutieren und die zukünftige Ausrichtung des Fachausschusses weiterzuentwickeln.

Zum Auftakt wurden die Teilnehmer von Christina Gessner, bei Rohde & Schwarz verantwortlich für den Bereich Messtechnik, herzlich begrüßt. Im Mittelpunkt der anschließenden Fachausschusssitzung standen insbesondere die Modernisierung der Aktivitäten und der Außendarstellung des Gremiums. Neben einer Überarbeitung des Internetauftritts wurde die Einführung einer neuen jährlichen Veranstaltungsreihe zum Thema »Radar für industrielle Anwendungen« und deren aktuelle Planung diskutiert. Ziel ist es, die heute verfügbare Radartechnik und ihre vielfältigen Einsatzmöglichkeiten einem breiteren, insbesondere nicht-akademischen Publikum vorzustellen und den direkten Austausch zwischen Technologieanbietern, Forschung und potenziellen industriellen Anwendern zu fördern.

Ein weiterer Programmpunkt war die Aufnahme neuer Mitglieder. Wir freuen uns, dass Prof. Stefan Zorn (Rohde & Schwarz / Technische Hochschule Deggendorf) einstimmig als neues Mitglied in den Fachausschuss aufgenommen wurde.

Im Verlauf der Tagung bot Rohde & Schwarz in mehreren Beiträgen aktuelle Einblicke, unter anderem zu Personenscannern und zur Mikrowellenbildgebung für die zerstörungsfreie Prüfung, zur High-End-Netzwerkanalyse, zur Hochfrequenz-Leistungsmessung und ihrer Rückführbarkeit sowie zu Themen der 6G-Forschung. Am zweiten Tag rundeten eine Diskussionsrunde zu Messtechnikgeräten und aktuellen Forschungsthemen sowie Demo-Touren durch die Mikrowellenfertigung und das Umweltlabor das Programm ab.

Die Klausurtagung bot damit nicht nur Raum für die strategische Weiterentwicklung des Fachausschusses, sondern auch für einen intensiven Austausch zwischen seinen Mitgliedern und den Fachkolleginnen und Fachkollegen von Rohde & Schwarz.

Der ITG-Fachausschuss 7.3 bedankt sich herzlich bei Rohde & Schwarz für die Gastfreundschaft, die fachlichen Beiträge und die hervorragende Organisation der beiden Tage. Die nächste Ausschusssitzung wird im Rahmen der GeMiC 2027 in Hamburg stattfinden. •

Veranstaltungen

4. QUARTAL 2026 / 1. QUARTAL 2027

1. OKTOBER 2026, BREMEN

FACHTAGUNG

»Satellitenkommunikation der Zukunft:
D2D, D2C und NTN/TN Integration«

VDE ITG FACHAUSSCHUSS HF2 FUNKSYSTEME

★ www.vde.com/itg-satkom

24. NOVEMBER 2026, BERLIN

VDE ITG Mitgliederversammlung 2026

VDE ITG

★ www.vde.com/de/itg/veranstaltungen

24. NOVEMBER 2026, BERLIN

VDE Hauptstadtforum 2026

VDE ITG

★ www.vde.com/hauptstadtforum

25. NOVEMBER 2026, BERLIN

**1st ITG Future Forum on AI-powered
Networks and Networking for AI**

VDE ITG

★ www.vde.com/de/itg/veranstaltungen

25.– 29. JANUAR 2027, MÜNCHEN

SYMPOSIUM

**7th IEEE International Symposium
on Joint Communications & Sensing**

IEE, VDE ITG

★ <https://jcms-symposium.org>

21.– 23. FEBRUAR 2027, HAMBURG

FACHTAGUNG / KONFERENZ

**39. ITG/GMM/GI-Workshop
Testmethoden und Zuverlässigkeit von
Schaltungen und Systemen – TuZ 2027**

VDE ITG, GMM, GI

★ <https://tuz2027.rp.es.tuhh.de>

2.– 3. MÄRZ 2027, PADERBORN

WORKSHOP

**MBMV 2027 – 30. RSS Workshop
Methoden und Beschreibungssprachen
zur Modellierung und Verifikation
von Schaltungen und Systemen**

VDE ITG

★ www.vde.com/de/itg/veranstaltungen

15. – 18. MÄRZ 2027, BREMEN

FACHTAGUNG / KONFERENZ

**15th International ITG Conference on Systems,
Communications and Coding (SCC)**

VDE ITG

★ <https://scc2027.uni-bremen.de>

15.– 17. MÄRZ 2027, HAMBURG

FACHTAGUNG / KONFERENZ

**18th German Microwave Conference
(GeMiC) 2027**

VDE ITG

★ <https://gemic2027.org>



SAFE THE DATE

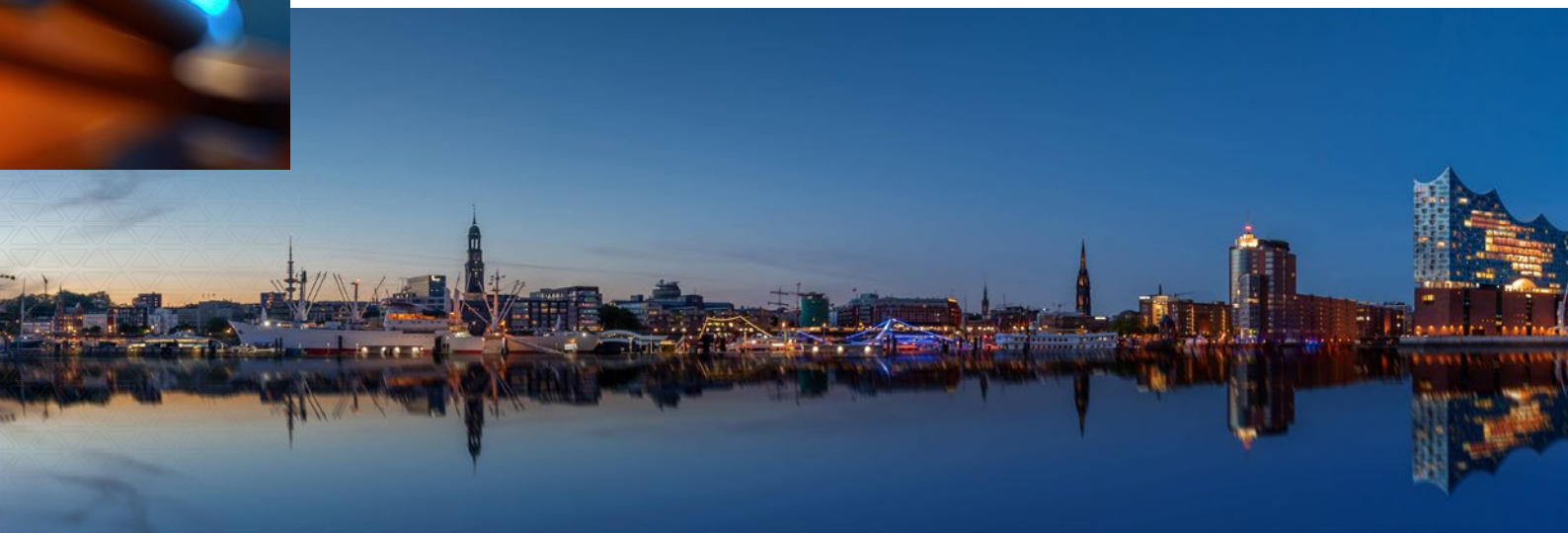
20.– 23.6.2027, HAMBURG, GERMANY

VTC2027 Spring – IEEE 105th Vehicular Technology Conference

The 2027 IEEE 105th Vehicular Technology Conference: VTC2027 Spring will be held in Hamburg, Germany on 20-23 June 2027. This semi-annual flagship conference of IEEE Vehicular Technology Society will bring together individuals from academia, government, and industry to discuss and exchange ideas in the fields of wireless, mobile, and vehicular technology. IEEE VTC2027-Spring will feature world-class plenary speakers, tutorials, technical as well as application sessions, and an innovative Industry Track, which will feature panels and presentations with industry leaders sharing their perspectives on the latest technologies.

EARLY BIRD REGISTRATION ENDS 9 MAY 2027

★ <https://events.vtsociety.org/vtc2027-spring/>



VDE Netzwerk Medizintechnik & LifeScience Electronic:

Vorträge zu Gesundheitsdaten und über Halbleiter für die Medizintechnik

Alle Vorträge finden vor Ort in München statt, werden aber auch im Livestream übertragen. Beginn ist jeweils um 18.15 Uhr, die Teilnahme ist kostenlos. Weitere Infos und Anmeldung unter:

★ <https://www.vde-bayern.de/de/veranstaltungen>

6. OKTOBER 2026

Dipl.-Ing. Markus Zimmik von Texas Instruments Deutschland informiert über aktuelle Trends bei Halbleitern für die Medizintechnik. In seinem Vortrag **»Technologie heilt mit – Wie Halbleiter die Zukunft der Medizintechnik prägen«** beleuchtet er den Einfluss der Halbleiterentwicklung auf medizinische Anwendungen und bietet einen fundierten Ausblick auf kommende Technologietrends, darunter intelligente Sensorik, KI-gestützte Systeme und personalisierte Medizin.

27. OKTOBER 2026

Das VDE Netzwerk Medizintechnik & LifeScience Electronic« begrüßt in diesem Herbst einen besonderen Gastreferenten aus Skandinavien: **Prof. Dr. Josef Noll** von der University of Oslo wird in seinem Vortrag **»Von Afrika lernen - Chancen digitaler Gesundheitsinformation«** die unterschiedlichen Auffassungen bezüglich der Verwaltung und Bereitstellung von Patientendaten in Norwegen und Deutschland aufzeigen. Außerdem wird er erörtern, ob sich Deutschland in diesem Bereich nicht vielleicht sogar ein Beispiel an einigen afrikanischen Ländern nehmen könnte.

24. NOVEMBER 2026

Bei **Dr. Michael Kraus** vom Universitätsklinikum Freiburg geht es ebenfalls um Gesundheitsdaten mit Fokus auf den digitalen Workflow und die innerklinische IT-Infrastruktur. Kraus ist Leiter des Zentrums für Digitalisierung und Informationstechnik am Klinikum und hat dort die grundlegende Neuausrichtung in der Verwaltung und Verarbeitung von Gesundheitsdaten maßgeblich mitgestaltet. Der Titel seines Vortrags lautet **»Daten treiben Medizin – Gesundheitsdateninfrastruktur im Wandel«**.

Call for Papers

25.–29.1.2027
MUNICH, GERMANY

7th IEEE International Symposium on Joint Communications & Sensing

The IEEE International Symposium on Joint Communications & Sensing (JC&S) will bring together leading experts from academia and industry at Airbus in Ottobrunn (near Munich), Germany, from 27–29 January 2027. As an international forum, the symposium fosters the exchange of the latest research results, technological challenges, and emerging applications in the field of Joint Communications & Sensing (JC&S). The technical program features scientific presentations, paper sessions, demonstrations, and tutorials, while also providing numerous opportunities for networking and knowledge transfer between academia and industry.

CALL FOR TUTORIALS/WORKSHOPS

Deadline October 9, 2026

CALL FOR PAPERS

Technical Paper Submission: Manuscripts not exceeding 6 pages must be submitted through EDAS not later than 11.10.2026

Demo Paper Submission: Manuscripts not exceeding 2 pages must be submitted not later than 25.10.2026

★ <https://jcns-symposium.org/>

15.–18.3.2027

BREMEN, GERMANY

15th International ITG Conference on Systems, Communications and Coding (SCC)

SCC is a biannual conference and organized by the Information Technology Society (ITG) of the Association for Electrical, Electronic and Information Technologies (VDE). The conference aims at bridging the gap between theory and applications as well as different communities working on communications. The 15th SCC will take place in Bremen, Germany, from March 15th to 18th, 2027. We encourage contributions from both academia and industry presenting original work in various fields of communications like:

- wireless communications (cellular, satellite, vehicular)
- optical communications
- sensor networks, Internet-of-Things (IoT) communications
- industrial radio, low-latency & ultra-reliable communications
- massive communications
- cloud and fog-based RANs
- distributed (storage) systems
- communications and control

Topics of interest include, but are not limited to:

- information and coding theory
- source and channel coding, semantic communications
- communication theory, detection, and estimation
- cryptography, privacy, and security
- cooperative communications and network coding
- machine learning and artificial intelligence for communications
- energy efficient and sustainable communications
- resource management and interference handling
- localization and navigation, integrated sensing and communications
- smart antennas and intelligent reflecting surfaces in communications
- quantum information processing and quantum communications
- molecular communications and biology-inspired data storage

PAPER SUBMISSION

Deadline October 16, 2026

NOTIFICATION OF ACCEPTANCE

January 8, 2027

FINAL MANUSCRIPT AND AUTHOR REGISTRATION

February 5, 2027

★ <https://scc2027.uni-bremen.de/>

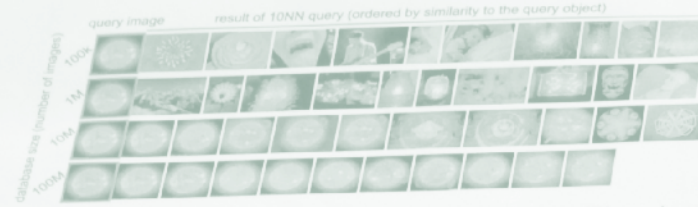


Figure 1: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.



Figure 2: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

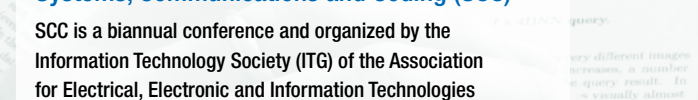


Figure 3: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

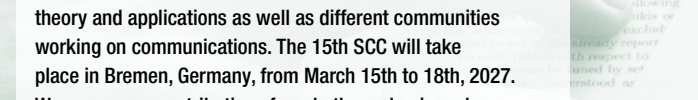


Figure 4: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

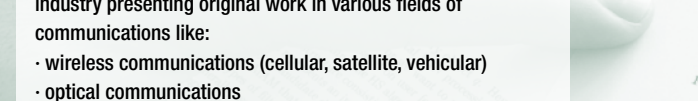


Figure 5: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

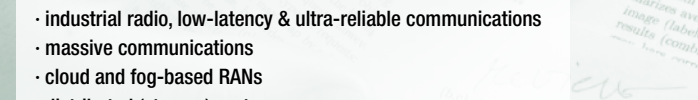


Figure 6: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

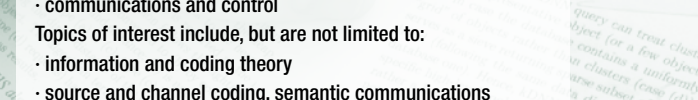


Figure 7: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

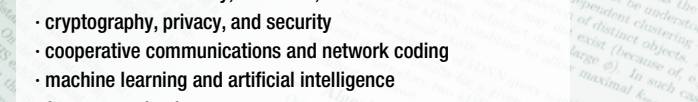


Figure 8: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.



Figure 9: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

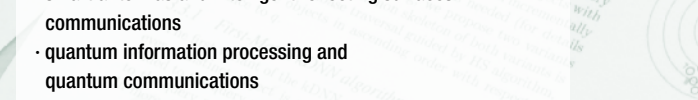


Figure 10: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.



Figure 11: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.



Figure 12: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

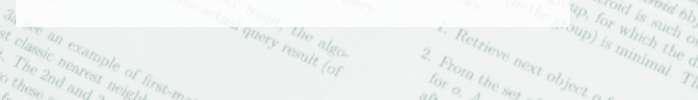


Figure 13: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

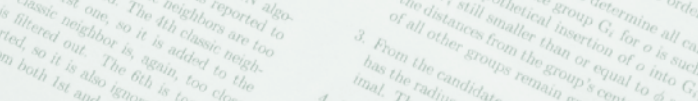


Figure 14: Limited power of classic kNN in very large databases. Results of the same 10NN query in a small, medium, large and very large database.

21.– 23.2.2027
HAMBURG, GERMANY

39. ITG / GMM / GI - Workshop Testmethoden und Zuverlässigkeit von Schaltungen und Systemen – TuZ 2027

The workshop »Test Methods and Reliability of Circuits and Systems« is the most important german forum for discussing trends, results and current problems in the field of testing, diagnostics and reliability of digital, analog, mixed-signal and RF circuits. The world-wide exchange of ideas is an important concern of the workshop. International contributions from both industrial practice and research institutions are welcome. We welcome highly practice-related experience reports and results as well as contributions on theoretical topics from the following areas, among others:

- hardware-oriented test and hardware-oriented security
- fault tolerance, resilience, robust and radiation-hard systems
- dependability and functional safety
- adaptive systems (e.g. self-repair, self-healing, self-awareness)
- statistical and AI-learning for test and reliability
- automatic test-equipment, test automation, test programs and test modeling
- defect- and fault models
- diagnosis of failure causes
- test and simulation of mixed-Signal, HF- and analog-circuit-test
- test generation, fault simulation, self-test and online-test
- test-oriented design, DfT methods
- test costs and quality
- test standards, e.g. IEEE 1149.x, IEEE 1687.x, IEEE 1838

SUBMISSION OF TITLE & ABSTRACT:

Deadline November 1st 2026

SUBMISSION OF FULL PAPER:

Deadline November 9th 2026

AUTHOR NOTIFICATION:

December 22nd 2026

CAMERA-READY PAPER

January 18th 2027

★ www.tuz2027.rp.es.tuHH.de

15.– 17.3.2027
HAMBURG, GERMANY

18th German Microwave Conference (GeMiC) 2027

The 18th German Microwave Conference will be hosted by Hamburg University of Technology on March 15-17, 2026 in cooperation with IMA e.V. and VDE/ITG. GeMiC 2027 provides a unique platform of exchange with experts, and a great opportunity to meet with colleagues from industry, research institutes, and universities. Topics include but are not limited to:

- Systems and Sensors
- Passives, EM, and Antennas
- Electronics and Active Circuits

SUBMISSION

Deadline: November 2, 2026 (abstracts 2–4 pages A4)

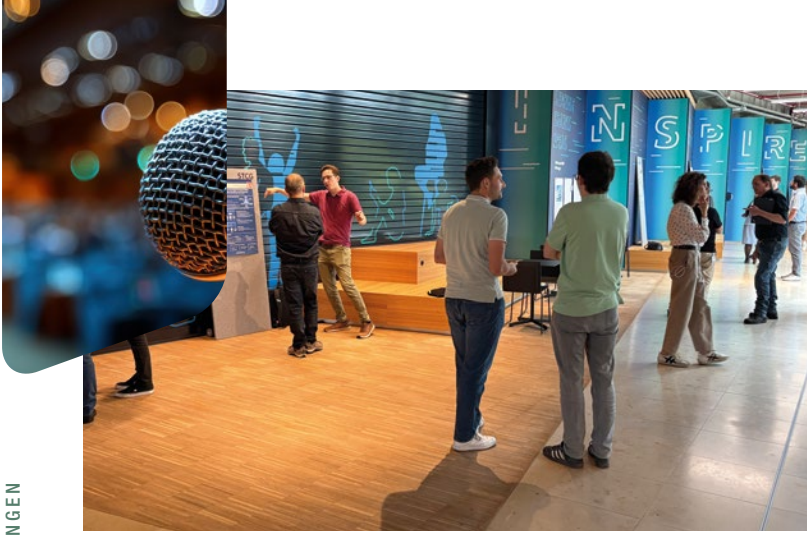
NOTIFICATION OF ACCEPTANCE:

January 8, 2027

FINAL PAPER SUBMISSION:

January 31, 2027

★ <https://gemic2027.org/>



NACHBERICHT

MueWoWAS 2026 Communication networks in vertical industries

- J. RIEDL, Siemens AG
- T. HOSSFELD, Universität Würzburg
- W. KELLERER, TU München
- J. SACHS, Ericsson

The 2nd MueWoWAS Workshop on »Communication networks in vertical industries« took place on June 17, 2026, in Garching (close to Munich), Germany. The event, hosted by the Siemens Technology Center and organized by Siemens AG, TU Munich, University of Würzburg and Ericsson, and supported by the VDE ITG technical committee KT2, provided the opportunity for industry and academia to exchange on the role of wired and wireless communication networks in vertical industries like factory automation, process automation, transport systems, energy automation, building automation. The workshop was moderated by Johannes Riedl (Siemens AG). It brought together around 40 participants from 18 organizations.

The program started with five keynote talks to provide different perspectives: Daniel Mai (Siemens AG) provided an overview on communication network requirements for selected industrial use cases clearly explaining the differences to the requirements know from telecommunication use cases. Joachim Sachs (Ericsson) continued with an overview on differentiated connectivity services for enterprises and industries which could be provided soon from a technical perspective but the concrete offerings of which obviously depend on business aspects as well. Nicola Michailow (Rivada Space Networks) has shown his experiences to develop a model for the communication demands of all European wind parks as a case study, while heavily using AI-based tools but avoiding a deep-dive into the specific communication flows to and from wind parks. Dominic Schupke (Airbus) pointed out the importance of 5G/6G/Non-Terrestrial Networks for the aerospace industry and explained from an aerospace perspective the most important technical expectations on 6G and related use cases for them. Finally, Meik Kottkamp (Rohde & Schwarz) explained the relevance of test systems for wireless services and show cased an app-based approach to track and analyse along the own movement path the quality of wireless connectivity.

In the second part of the program, the workshop

participants had the opportunity to present their posters on their academic and industrial research in the context of the workshop. Nine posters have been presented from seven different organizations. These posters addressed 5G/6G research, deterministic networking based on TSN approaches, energy-efficient communication, network management aspects, Network Digital Twins and more. Extensive discussions happened in the community along all the presented posters.

Afterwards a demo session has been organized in which all participants had the chance to visit three different demos at the Siemens Technology Center which are the results of selected research activities on Siemens side. These demos focused on Non-Terrestrial Networks and their use in vertical industries, Seamless Failover between (virtual) Programmable Logic Controllers controlling a robot using programmable networks, as well as a novel approach for successfully controlling a robot over a 5G-TSN infrastructure. At all demo locations a lot of interaction and discussions have happened.

Finally, a panel session with the keynote speakers closed the technical part of the meeting. In this panel the participants deepened on the relevance of requirements from vertical side on 6G, the most important research areas of 6G and the gaps we still see on 5G side. In this panel session also the audience played an active role and asked many questions.

All in all the event was a full success, highly relevant topics have been addressed and people networks could be substantially extended. The organizers would like to thank all speakers, contributors, and participants for their valuable contributions. ●





NACHBERICHT

30. ITG-Fachtagung Mobilkommunikation 2026 Technologien und Anwendungen

- G. HÜDEPOHL,
Hochschule Osnabrück (University of Applied Sciences)
- R. TÖNJES,
Hochschule Osnabrück (University of Applied Sciences)

Am 12. und 13. Mai 2026 fand zum 30. Jubiläum die ITG-Fachtagung Mobilkommunikation an der Hochschule Osnabrück statt. In den vergangenen drei Jahrzehnten hat die Einführung des digitalen Mobilfunks die Kommunikation grundlegend verändert und ermöglichte eine Vernetzung, die heute selbstverständlich ist – von den ersten digitalen Mobiltelefonen bis zu leistungsstarken Smartphones, die permanente Interaktionen über soziale Medien ermöglichen. Über 50 Forscher, Entwickler und Anwender aus Industrie, Hochschulen und Forschungsinstituten präsentierten und diskutierten an zwei Tagen ihre aktuellen Forschungsergebnisse und Erfahrungen u.a. zu den KI gestützten Interaktionsmöglichkeiten oder das Mobile Cloud Computing im Kontext des 6G Mobilfunks.

Tagungsleiter Prof. Tönjes eröffnete die Veranstaltung mit einem Rückblick auf die Historie der Jubiläumstagung. 1996 organisierte Prof. Pehl die erste Fachtagung »Mobilfunk«, die sich damals ausschließlich mit GSM-Netzen befasste. Heute stehen die 5G Erweiterungen und Ausblicke auf die sechste Mobilfunkgeneration im Fokus. Neben 18 Fachvorträgen gab es vier Key-Notes, einen invited Talk und eine Poster-Session, die das zweitägige Programm abrundeten. In der ersten Key Note stellte Herr Heyn vom Fraunhofer-Institut für Integrierte Schaltungen (IIS) neue Konzepte für nicht-terrestrische Netzwerke in 5G/6G vor. Im invited Talk entwickelte Herr Kunzmann von Nokia ausgehend von 5G ein intelligentes IT-Sicherheitskonzept für 6G basierend auf agentic AI. Die Konferenz bestand aus insgesamt sechs Sitzungen, mit jeweils drei Vorträgen. In der ersten Sitzung wurden die Themen »Cell Free and Non-Terrestrial Networks« behandelt. Eine Machbarkeitsstudie untersuchte Optimierungen für den Mehrbenutzer-Zugang in zellfreien Massive-MIMO-Systemen. Ein zweiter Vortrag stellte eine dynamische Clusterbildung für nutzerzentrierte, zellfreie MIMO Netzwerke vor. Ein dritter Beitrag zeigte, wie die Verbindungsqualität für die Direct

to Device-LEO-Kommunikation mittels Deep Learning vorhergesagt werden kann. In einer zweiten Key Note analysierte Herr Bahr (Siemens) die Trends der drahtlosen Kommunikation für industrielle Anwendungen und deren Anforderungen. Nach der Poster-Session zu speziellen Lösungen und neuen Ansätzen adressierte die folgende Sitzung »Campus Network Performance«. Ein Beitrag zeigte, dass für Regelkreise in der Industrieautomatisierung nicht nur die Verteilung sondern auch die Korrelation der Paketverzögerungen unbedingt berücksichtigt werden muss. Anschließend wurden Messungen unter realen Bedingungen in industriellen Robotik-Anwendungen präsentiert. Die Sitzung schloss mit einem Vortrag über experimentelle Ergebnisse zu saisonalen und umweltbedingten Einflussfaktoren. In der dritten und letzten Sitzung des ersten Tages stand das Thema »5G Network Configuration and Digital Twins« im Vordergrund. Zunächst wurde ein automatisiertes Konfigurations-Framework für private Netzwerke vorgestellt. Anschließend präsentierten die Referenten Untersuchungen zur Auswirkung der Modemauswahl auf die 5G-NR-Uplink-Leistung sowie ein Konzept für einen digitalen Zwilling für die Überwachung von 5G/6G-Netzen.

Der zweite Konferenztag begann mit einer Key Note von Herrn Sezgin (Universität Bochum) über rekonfigurierbare intelligente Oberflächen in 6G. Die vierte Sitzung widmete sich den Fortschritten bei 6G. Es wurde ein Blick auf 6G aus der Perspektive von Standardisierung, Forschung, Netzbetreibern und Anbietern geworfen. Danach ging es um die Nachhaltigkeit in Informations- und Kommunikationstechniksystemen. Der dritte Vortrag dieser Sitzung präsentierte experimentelle Erkenntnisse über intelligente reflektierende Oberflächen für 6G-Signale. Thema der fünften Sitzung waren IoT Netzwerke. Zunächst wurde eine performante ereignisgesteuerte Kommunikation für Signale mit variabler Bandbreite vorgestellt. Anschließend wurde ein System zur Evaluation von Mobilitätseinflüssen in verschiedenen zellularen IoT Szenarien präsentiert. Die Sitzung endete mit einem Überblick über die Herausforderungen bei der Integration von Time Sensitive Networking (TSN) und 5G. Herr Benze (Deutsche Telekom) gab in der vierten Key Note einen Ausblick auf Europas souveräne Multi-Provider-Cloud-Edge-Infrastruktur. Die abschließende Sitzung der Tagung befasste sich mit Sicherheit und Cloud-Infrastruktur für 6G-Anwendungen. Zunächst zeigte ein Referent eine sichere Authentifizierung im drahtlosen Internet der Dinge (IoT). Ein Mobilfunkbetreiber stellte einen Ansatz für eine sichere und cloud-fähige 5G-Infrastruktur vor. Die Tagung wurde mit einem Leitfaden zur Auswahl von Funktechnologien für medizinische Anwendungen abgeschlossen.

Begleitend zur Tagung wurden mehrere Demonstratoren aus Kooperationsprojekten zwischen Hochschulen und Industrie präsentiert. Diese Demos und die interessanten Präsentationen der Tagung lösten zahlreiche Fachgespräche aus. Eine Abendveranstaltung in einer Osnabrücker Hausbrauerei mit Jazz-Musik rundete das erfolgreiche Programm ab. Die Teilnehmer lobten die hohe fachliche Qualität der Beiträge sowie das ausgewogene Verhältnis von Vorträgen aus Hochschulen und Industrie. Der Tagungsband mit den Beiträgen ist im VDE-Verlag erschienen.

Die Präsentationen können unter www.mobilkomtagung.de eingesehen werden. Die nächste ITG Fachtagung Mobilkommunikation ist schon für den 12. und 13. Mai 2027 an der Hochschule Osnabrück geplant. •



NACHBERICHT

11. ITG/VDE Summer School on Video Coding and Processing Experten-Treffen zu Video- kommunikation und -verarbeitung

• M. WIEN, RWTH Aachen

An der Brandenburgische Technische Universität Cottbus-Senftenberg (BTU) fand vom 28. bis 30. Juni 2026 die 11. Ausgabe der ITG/VDE Summer School on Video Coding and Processing statt. Organisiert wurde die Veranstaltung vom ITG Fachausschuss MT 2 »Bildkommunikation und Bildverarbeitung«. Die Summer School richtet sich an nationale und internationale Forschende auf den Gebieten der Videocodierung, Bildverarbeitung und Multimediakommunikation. Sie bietet im jährlichen Turnus die Möglichkeit zu Austausch und Diskussionen über aktuelle Entwicklungen und Themen mit zahlreichen Experten auf dem Gebiet.

Die diesjährige SVCP hatte 35 Teilnehmende aus Deutschland, Frankreich und Großbritannien. Das Programm umfasste zwei Keynotes, elf Fachvorträge und zehn Posterpräsentationen. Die Anreise erfolgte für die meisten Teilnehmenden am Sonntag, einem außergewöhnlich heißen Tag mit Hitzerekord in der Lausitz. Beim gemeinsamen Abendessen klang der Anreisetag in gemütlicher Atmosphäre aus; einige Teilnehmende trafen aufgrund der angespannten Verkehrssituation erst später in Cottbus ein.

Die Veranstaltung wurde von Stellv. Prof. Herglotz von der BTU und seinem Team exzellent organisiert.

Eröffnet wurde die Summer School durch den BTU-Vizepräsidenten Prof. Dr. Wolfram Berger. Die erste Keynote hielt am Montag Dr. Mahdi Taheri von der BTU unter dem Titel »Don't Trust Every Pixel«. Der Vortrag gab spannende Einblicke in die Authentizität von Bild- und Videosignalen. Es folgten drei Vortragssessions zu den Themen »Enhanced Compression«, »Cinema & XR« sowie »Deep Learning for Image Processing«. Die Postersession »Image and Video Processing I« bildete den fachlichen Ausklang des ersten Tages. Nach der Mittagspause boten Führungen und Demonstrationen der BTU, insbesondere durch die Modellfabrik und das Videoproduktionsstudio, interessante Einblicke in die Forschung und Infrastruktur der Universität. Am Abend fand das Social Event statt, das mit einem Spaziergang durch die Parkanlagen des Fürsten Pückler und einem gemeinsamen Abendessen im Cavalierhaus Branitz einen gelungenen Rahmen bot.

Am Dienstag hielt Thomas Maugey von INRIA Rennes, Frankreich, die zweite Keynote mit dem Titel »Accuracy, Efficiency, Sufficiency: Three Pillars for the Sustainability of Video Streaming«. Im Mittelpunkt standen Fragen der Nachhaltigkeit in der Videocodierung, -übertragung und -ausspielung. Anschließend folgten weitere Beiträge in der Session »Energy Efficient and Hardware-Friendly Video Communications« sowie die Postersession »Image and Video Processing II«.

Zum Abschluss der Veranstaltung wurden der »Best Presentation Award« an Marina Ritthaler, der »Best Poster Award« an Teresa Stürzenhofacker sowie zum ersten Mal der »Best SVCP Buddy Award« an Marc Windsheimer (alle Friedrich-Alexander-Universität Erlangen-Nürnberg, FAU) verliehen. Zudem konnte in diesem Jahr der Joint Research Incubator Award des Fachausschusses vergeben werden. Ausgezeichnet wurde ein gemeinsames Paper von Fraunhofer IIS und der FAU: Mahadev Prasad Panda, Purnachandra Rao Makkena, Srivatsa Prativadibhayankaram, Siegfried Föfel und André Kaup, »TreeNet: A Light Weight Model for Low Bitrate Image Compression«, Picture Coding Symposium 2025, IEEE, Dec. 2025.

Für den Joint Research Incubator Award können Arbeiten eingereicht werden, die seit der letzten SVCP gemeinsam von Mitarbeitenden mindestens zweier beteiligter Organisationen verfasst und für eine Konferenz oder ein Journal angenommen wurden. Bewertet werden insbesondere Neuheitswert, Klarheit der Darstellung und der gemeinsame Team-Beitrag. Der Award soll auch im Jahr 2027 wieder vergeben werden.

Insgesamt war die Summer School ein großer Erfolg und erhielt von den Teilnehmenden durchweg positives Feedback. Ein besonderer Dank gilt Stellv. Prof. Herglotz und seinem Team für die hervorragende Organisation. Die nächste Summer School findet Ende Juni 2027 in Hannover statt. •

Festival der Elektronik 2026 in Dresden war

Save the Date: Freitag, 11. Juni 27

hot

Wir sehen
uns 2027
im E-Werk Erlangen!

• D. DUDEK, VDE ITG

Es war wunderbar erfrischend, so viele Menschen zu sehen, die sich voller guter Musikstimmung der Elektronik hingeben und das bei fast 40°C im Dresdner Stromwerk. Am Freitag, 19. Juni 2026 hatten wir, der VDE e.V. gemeinsam mit der TU Dresden, zum bits, bonding, bassline dem Festival der Elektronik 2026 geladen. Ja, es waren mehr als 700 Personen vorort, die zur Livemusik von drei Bands getanz und gefeiert haben, aber vor allem sich mit den Firmen und Instituten aus der Elektronik verkabeln konnten.

Die nächste Station des Festivals der Elektronik 2027 wird das E-Werk in Erlangen sein. Wer diese Bühne betreten wird, das verkünden wird schon bald. Fest steht, dass wir dieses Mal als ITG gemeinsam mit der FAU und der TU Dresden noch mehr Firmen und Partystimmung auffahren werden. Ob wir das Sternchen der deutschen Charts zum bits, bonding, bassline 2027 gewinnen, da bin ich sehr zuversichtlich. Dafür benötigen wir jedoch helfende Hände und die Unterstützung von zahlreichen Firmen der Elektronik als Sponsoren.

Die Fotos aus diesem Jahr
überzeugen doch, oder?



**bits,
bonding,
bassline
festival
der elektronik'27**

Business & Music
für Young Professionals
und Industrie.

**Erlangen
E-Werk
11. Juni '27**

**Eintritt
frei!**

**SAVE
THE
DATE!**



**QUANTUM OPTICS
JENA**

Warum für langfristige Datenvertraulichkeit **QKD und PQC** zusammengehören

→ B. JOUR, Quantum Optics Jena

Die Migration auf Post-Quanten-Kryptografie (PQC) ist in vollem Gange – und greift dennoch zu kurz, wenn Vertraulichkeit über viele Jahre sicher gewährleistet sein muss. Das BSI und die EU empfehlen, die Umstellung auf quantensichere Kryptografie kritikalitätsangepasst zwischen 2030 und spätestens 2035 abzuschließen. Parallel treibt die »Harvest now, decrypt later«-Bedrohung die Dringlichkeit: Heute abgegriffene, klassisch verschlüsselte Daten lassen sich später entschlüsseln, sobald ein kryptografisch relevanter Quantencomputer verfügbar ist. Für langlebige Geheimnisse ist das Zeitfenster bereits heute kritisch.



*ELVIS QKD-System
von Quantum Optics Jena*

Die neue Bedrohung: KI-gestützte Kryptoanalyse

Ein Ereignis aus dem Sommer 2026 zeigt jedoch, dass auch die PQC-Verfahren keine Gewissheit für langfristige Sicherheit bieten. Am 28. Juli 2026 veröffentlichte Anthropic, dass das KI-Modell Claude Mythos Preview eine bis dahin unbekannte strukturelle Schwäche im PQC-Standardisierungs-Kandidaten HAWK fand. Claude Mythos benötigte dafür lediglich rund 60 Stunden weitgehend autonomer Arbeit, während HAWK zuvor zwei Runden menschlicher Experten-Begutachtung über zwei Jahre überstanden hatte. Die Folgen waren unmittelbar: HAWK wird nicht standardisiert.

Für die Praxis ist ein zweiter Punkt mindestens ebenso wichtig. KI-Modelle finden Schwächen nicht nur in der Mathematik eines Verfahrens, sondern auch in dessen Implementierung. So wurden mit Claude auch Fehler in weit verbreiteten Kryptobibliotheken wie OpenSSL und wolfSSL aufgedeckt – also im Code, mit dem korrekte Algorithmen umgesetzt werden. Das deckt sich mit dem bekannten Muster: Nicht der Algorithmus, sondern seine Umsetzung ist oft das schwächste Glied.

Die Lehre daraus ist struktureller Natur: Der bisher begrenzende Faktor der Kryptoanalyse, die knappe und teure Zeit menschlicher Spezialisten, verliert seine bremsende Wirkung.

Die sichere Lösung: PQC und QKD kombinieren

Aus dieser Unsicherheit folgt kein Argument gegen PQC, sondern eines für Verteidigung in der Tiefe. Post-Quanten-Kryptografie ist über beliebige Verbindungen einsetzbar, beruht aber auf mathematischer Härte – und kann durch künftige Kryptoanalyse oder Rechenfortschritte geschwächt werden, wie HAWK zeigt. Quantenschlüsselverteilung (QKD) gründet ihre Sicherheit hingegen auf physikalischen Gesetzen: Jeder Abhörversuch stört die Photonen und wird sofort erkannt; einmal erzeugte Schlüssel können später nicht nachträglich berechnet werden. Beide Verfahren adressieren unterschiedliche Angriffsvektoren. Verrechnet ein Schlüsselkombinierer einen PQC- mit einem QKD-Schlüssel zu einem hybriden

AES-256-Schlüssel, bleibt die Verbindung selbst dann sicher, wenn eine der beiden Methoden später fällt – die eigentliche Immunität gegen »Harvest now, decrypt later«.

Geprüfte Sicherheit und einfache Integration

Die ELVIS QKD-Systeme von Quantum Optics Jena (QOJ), einem Fraunhofer-IOF-Spin-off aus der Optikstadt Jena, sind für den Einsatz im Rechenzentrum ausgelegt und überzeugen durch hohe Zuverlässigkeit, einfache Verwaltbarkeit und definierte Service-Level-Agreements. Über standardisierte Schnittstellen lassen sich die QKD-generierten Schlüssel herstellerübergreifend einbinden und mit PQC zu hybriden AES-256-Schlüsseln für alle Netzebenen kombinieren – von der Layer-1-Verschlüsselung zwischen Standorten über MACsec/IPsec auf Layer 2–3 bis zu Anwendungen.

Auch die Sicherheit der Implementierung hat QOJ unabhängig prüfen lassen: Im August 2026 bestätigte die TÜV Informationstechnik (TÜViT) in einer auf vielfältigen Angriffsversuchen basierten Bewertung nach ISO/IEC 23837, dass ELVIS gezielten Angriffen auf Hardware-Seitenkanäle standhielt.

Das Fazit: Rein klassische Verschlüsselung genügt für langlebige Daten nicht mehr, und selbst PQC bietet – wie HAWK zeigt – keine Gewissheit für Langzeitsicherheit. Ein hybrider Ansatz aus QKD und PQC ist die risikoangemessene mehrschichtige Verteidigung für alles, was langfristig vertraulich bleiben muss.

★ www.qo-jena.com



Burkhard Jour ist Nachrichtentechnik-Ingenieur und hat zahlreiche Schulungen sowie Fachartikel zur Quantensicherheit verfasst. Er arbeitet als Director Business Development and Sales bei Quantum Optics Jena.



LINKS

3D gedruckte Demo eines
Quantum Key Distribution
Networks

RECHTS

Fabian Seidl, Neil-Jocelyn Schark,
Malte Bauch, André Sterba,
Johanna Henrich und Martin
Stiernerling (von links nach rechts)



Verschlüsselung die mitwachsen kann

→ M. BAUCH, Co-Founder qonduit GmbH

In vielen Unternehmen sind kryptografische Verfahren und Protokolle tief in deren IT-Landschaften verwoben, sodass eine nachträgliche Anpassung oder gar ein Austausch einzelner Verfahren oft nur mit erheblichem Aufwand möglich ist. Das Darmstädter Start-up qonduit entwickelt daher eine zentrale Plattform qonflux, die kryptografische Verfahren austauschbar und kombinierbar macht.

Das eigentliche Problem: fehlende Krypto-Agilität

Ein Großteil heutiger digitaler Kommunikation stützt sich auf kryptografische Verfahren, die fest in Anwendungen, Protokollen und Hardware verankert sind. Das wird zum Problem, sobald sich ein Verfahren als unsicher erweist: Ein Austausch bedeutet in gewachsenen IT-Landschaften selten eine einfache Konfigurationsänderung, sondern eine aufwendige, mehrjährige Migration.

Die aktuell drängendste Ausprägung dieses generellen Problems sind Quantencomputer, die die mathematischen Probleme hinter der heute verbreiteten asymmetrischen Kryptografie effizient lösen könnten. Es genügt bereits, verschlüsselten Datenverkehr schon heute aufzuzeichnen und ihn erst später zu entschlüsseln (»Store Now, Decrypt Later«) – ein reales Risiko für Daten mit langer Schutzdauer wie Gesundheitsdaten oder Finanztransaktionen. Zuständige Behörden wie das deutsche BSI, die französische ANSSI und weitere nationale Stellen geben deshalb Fristen zur PQC-

Migration zwischen 2026 und 2035 vor. Wer dabei nur auf ein neues, quantensicheres Verfahren umstellt, löst jedoch nur das aktuelle Symptom – ohne Krypto-Agilität ist die nächste Migration nur eine Frage der Zeit.

Eine Plattform für austauschbare und kombinierbare Verfahren

Genau hier setzt qonduit mit qonflux an: Das Unternehmen hat eine zentrale Kryptografie-Plattform entwickelt, die Organisationen einen Überblick verschafft, welches System welchen Schlüssel über welches Verfahren bezieht, und die es erlaubt, einzelne Verfahren auszutauschen oder zu ergänzen, ohne die gesamte Infrastruktur zu ersetzen. Statt auf einen einzigen Algorithmus festgelegt zu sein, verwaltet die Plattform klassische Kryptografie, PQC und Quantum Key Distribution (QKD) gleichzeitig und herstellerunabhängig – neue Verfahren oder Hardware lassen sich nachrüsten, sobald sie nötig werden.



Ein Schwerpunkt ist dabei die hybride Kombination aus PQC und QKD, die auf unterschiedlichen Sicherheitsgrundlagen beruhen: PQC gilt als rechnerisch sicher, es schützt gegen den heute bekannten Angriffsweg über Quantencomputer, bietet aber keine Garantie gegen einen künftigen mathematischen Durchbruch. QKD beruht dagegen auf physikalischen Eigenschaften des Lichts und gilt als informationstheoretisch sicher, unabhängig von künftigen Rechen- oder Analysefortschritten. Erst die hybride Kombination beider Verfahren liefert nach heutigem Kenntnisstand den vollständigen, dauerhaften Schutz gegen Store-Now-Decrypt-Later.

Um QKD praktisch nutzbar zu machen, muss eine Plattform zudem nativ mit QKD-Modulen unterschiedlicher Hersteller sprechen und Schlüssel über mehrere, nicht direkt verbundene Netzknoten weiterleiten können, eine sogenannte QKD-Netzwerk-Anbindung (QKDN). Diese native QKDN-Fähigkeit unterscheidet conduit von reinen PQC-Plattformen ohne QKD-Anbindung ebenso wie von Hardware-Herstellern, deren Software vor allem auf den Betrieb der eigenen Geräte ausgelegt ist.

Europäisch, herstellerunabhängig, nachvollziehbar

Für Banken, Behörden sowie Telekommunikationsanbieter und Rechenzentren zählen neben der Technik auch Herkunft und Nachvollziehbarkeit der Software. conduit positioniert sich als europäisches Unternehmen und stellt den Quellcode der Plattform einsehbar zur Verfügung (source-available), ein Kriterium, das bei europäischer Beschaffung, zunehmend an Bedeutung gewinnt.

Von der Forschung zum Unternehmen

Die Ursprünge von conduit liegen an der Hochschule Darmstadt (h_da), wo das spätere Gründungsteam im Forschungsprojekt DemoQuandT praktische Erfahrung mit dem Aufbau und Betrieb von QKD-Netzwerken sammelte. Aus der Arbeit an Controller- und Key-Management-Systemen entstand die Idee zu einer herstellerunabhängigen, agilen Kryptografie-Plattform für QKD-Hardware verschiedener Anbieter und moderner PQC-Verfahren. Gefördert durch ein EXIST-Gründerstipendium, gründeten die sechs Gründer:innen – Neil-Jocelyn Schark, André Sterba (inzwischen ausgeschieden), Fabian Seidl, Johanna Henrich, Martin Stiernerling und Malte Bauch – im Februar 2026 die conduit GmbH mit Sitz in Darmstadt. ●



RUHESTAND

Prof. Dr.-Ing. Ralph Urbansky

- T. HOSSFELD, Fachausschuss KT2
- W. KELLERER, TU München
- J. SACHS, Ericsson

Der Vorstand der Informationstechnischen Gesellschaft im VDE (ITG) sowie der Fachausschuss KT2 danken Prof. Dr.-Ing. Ralph Urbansky herzlich für sein langjähriges und außerordentliches ehrenamtliches Engagement.

Mit seinen wissenschaftlichen Arbeiten auf den Gebieten der Nachrichtentechnik und der Kommunikationsnetze sowie seinem langjährigen Wirken in Forschung und Lehre hat Prof. Urbansky die Entwicklung des Fachgebiets nachhaltig geprägt. Als Hochschullehrer hat er zahlreiche Studierende sowie Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftler begleitet und damit einen wichtigen Beitrag zur Weiterentwicklung der Informationstechnik geleistet.

Als langjähriges Mitglied des Fachausschusses KT2 hat Prof. Urbansky die Arbeit der VDE ITG mit seiner wissenschaftlichen Expertise, seiner Erfahrung aus Forschung, Lehre und Industrie sowie seinem persönlichen Engagement nachhaltig bereichert. Sein Wirken war von hoher fachlicher Kompetenz, Verlässlichkeit und Kollegialität geprägt und hat den fachlichen Austausch innerhalb der ITG über viele Jahre hinweg maßgeblich unterstützt.

Der Vorstand der VDE ITG und der Fachausschuss KT2 danken Prof. Urbansky für sein herausragendes Wirken in Wissenschaft, Lehre und der ITG sowie für sein langjähriges ehrenamtliches Engagement. Sie wünschen Prof. Urbansky für seinen Ruhestand alles Gute sowie weiterhin Freude und Erfüllung bei seinen künftigen Vorhaben und freuen sich darauf, ihn auch künftig bei den Veranstaltungen der VDE ITG begrüßen zu dürfen. ●

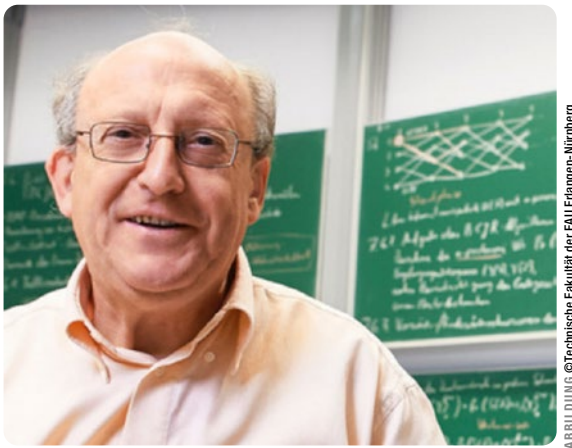


ABBILDUNG © Technische Fakultät der FAU Erlangen-Nürnberg

GEBURTSTAG

Prof. Dr.-Ing. Dr. h.c. Johannes Huber

• R. FISCHER • A. LAMPE • L. LAMPE • R. SCHÖBER

Im August feierte Professor Dr.-Ing. Dr. h.c. Johannes Huber seinen 75. Geburtstag. Wir möchten diese Gelegenheit nutzen, um auf das Wirken dieses herausragenden Wissenschaftlers und angesehenen akademischen Lehrers zurückzublicken.

Professor Huber studierte Elektrotechnik an der Technischen Universität München und schloss das Studium im Jahr 1977 als Dipl.-Ing. ab. Er promovierte 1982 an der Universität der Bundeswehr München mit der Dissertation »Codierung für gedächtnisbehaftete Kanäle« zum Dr.-Ing. Im Jahr 1991 habilitierte er sich mit einer Arbeit über trelliscodierte Modulation. Anschließend war er Gastwissenschaftler in der Gruppe von Dr. Ungerböck am IBM-Forschungslabor in Zürich, Schweiz.

Im Herbst 1991 erhielt er einen Ruf auf eine Professur am Lehrstuhl für Nachrichtentechnik an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Von 1997 bis zu seinem Eintritt in den Ruhestand 2017 leitete er als Ordinarius an derselben Universität den Lehrstuhl für Informationsübertragung.

Johannes Huber hat sich in der Forschung mit einer großen Bandbreite an Themen beschäftigt, darunter digitale Übertragung, Informations- und Codierungstheorie, sowie Entzerrungs- und Detektionsverfahren, um nur die wichtigsten zu nennen. Mit seinem feinen Gespür für zukunftsweisende Themen, seinem enorm breiten und fundierten Wissen und seinen mathematischen Fähigkeiten hat er die stürmische Innovationphase der Nachrichtentechnik um die Jahrtausendwende, die etwa DSL, Mobilfunk, WLAN, und DAB hervorbrachte, an vorderster Front mitgeprägt.

Die wissenschaftlichen Beiträge von Johannes Huber wurden mit zahlreichen renommierten Preisen gewürdigt, darunter der Preis der Informationstechnischen Gesellschaft im VDE (ITG) sowie der Innovationspreis der Vodafone-Stiftung für Forschung in der Mobilkommunikation.

Als führender Experte auf dem Gebiet der Codierungs- und Kommunikationstheorie genießt Professor Huber in der nationalen und internationalen Fach-Community einen ausgezeichneten Ruf und brachte sich dort in vielfältiger Weise ein. So war er unter anderem Mitglied und zeitweise Vorsitzender im Fachausschusses 5.1 (System- und Informationstheorie) der ITG sowie Mitglied im »Board of Governors« der IEEE Information Theory Society. Er war viele Jahre Editor-in-Chief des »International Journal on Electronics and Communications« (AEÜ) und Associate Editor der »IEEE Transactions on Communications«.

Im Jahr 2006 wurde er für seine »Beiträge zur codierten Modulation und zum Entwurf digitaler Teilnehmeranschlüsse« zum IEEE Fellow gewählt. Er ist ebenso Fellow des Fraunhofer IIS, wurde im Jahr 2008 zum korrespondierenden Mitglied der Royal Society of Edinburgh ernannt und ist seit 2009 ordentliches Mitglied der Bayerischen Akademie der Wissenschaften. Im Jahr 2017 erhielt er die Ehrendoktorwürde der Universität Klagenfurt, an der er viele Jahre eine Gastvorlesung zur Informationstheorie hielt. Im gleichen Jahr wurde er aufgrund seiner »hervorragenden wissenschaftlichen Leistungen auf dem Gebiet der Informationstechnik« zum ITG-Fellow ernannt.

Professor Huber engagierte sich auch sehr aktiv in diversen Gremien und Ausschüssen seiner Universität. Insbesondere war er von 1994 bis 1996 Studiendekan der Technischen Fakultät der Universität Erlangen-Nürnberg, von 2001 bis 2003 Sprecher des Departments Elektrotechnik-Elektronik-Informationstechnik und von Oktober 2007 bis September 2009 Dekan der Technischen Fakultät.

Ganz besonders hervorheben möchten wir, dass Johannes Huber ein hoch angesehener, extrem engagierter Dozent und ein herausragender akademischer Lehrer ist. Seine Vorlesungen zu grundlegenden und fortgeschrittenen Themen der Nachrichtentechnik und Informationstheorie haben viele Generationen von Studierenden begeistert, uns eingeschlossen. Er hat immer den direkten Kontakt zu den Studierenden gesucht, aber auch zu talentierten Schülerinnen und Schülern, denen er auf Augenhöhe begegnete. Eine ganz besondere Leidenschaft waren für ihn die Ferienakademie im Sarntal (Südtirol) und das »Coding and Skiing«, bei denen wir das Glück hatten, ihn hautnah zu erleben; tagsüber bei Wanderungen und Skitouren in den Bergen, abends im anregenden wissenschaftlichen Austausch, oft bis spät in die Nacht. Immer wieder hat er viel Zeit und Mühe darauf verwendet, Schülerinnen und Schüler für das Studium der Elektrotechnik zu begeistern und begabte Studierende zu fördern. Wir erinnern uns gerne daran, wie viel Freude ihm das bereitete.

Seine außerordentliche Qualität als akademischer Lehrer kam aber insbesondere uns, seinen Studierenden und Promovierenden zugute. Professor Huber kann mit mehr als 50 »Dokortöchtern- und söhnen« auf eine herausragende Bilanz als »Doktorvater« zurückblicken – fast ein Dutzend davon haben inzwischen selbst eine Professur inne. Wir alle hatten die Ehre und das Glück, mit ihm zu arbeiten und von ihm gefördert zu werden.

Im Namen aller Kolleginnen und Kollegen, Doktorantinnen und Doktoranden und Studierenden, die von ihm lernen durften, möchten wir anlässlich seines 75. Geburtstags ihm unsere herzlichsten Glückwünsche senden. Wir wünschen ihm alles Gute und viel Zeit und Freude mit seiner Familie, allen voran seiner Frau, seinen Kindern und den zahlreichen Enkeln sowie für seine zahlreichen Hobbys, wie Posaune- und Cello-Spielen, Wandern und Rad fahren!

Herzlichen Glückwunsch, Johannes! •



ITGnews

Impressum

HERAUSGEBER

Informationstechnische Gesellschaft
(ITG) im VDE e.V.
Merianstraße 28
63069 Offenbach am Main
069 6308 360
itg@vde.com
www.vde.com/itg

REDAKTION

Dr.-Ing. Damian Dudek
Franziska Bienek

GESTALTUNG UND REALISATION

Lindner & Steffen GmbH
www.lindner-steffen.de

Nachdruck – auch auszugsweise –
nur mit Genehmigung des Herausgebers.

Offenbach am Main, Oktober 2026

BILDNACHWEIS

Sofern nicht auf der Seite angegeben:
AdobeStock: ardanzi KI (Umschlag, 06–28),
Iawei (40–44), ManuPadilla (48–50)

VDE





www.vde.com/itg

VDE

