VDE POSITIONSPAPIER

RESILIENTE NETZE MIT FUNKZUGANG

ITG

VDE

Dieses Positionspapier ist eine Initiative der Fokusgruppe „Mobilkommunikation“ der Informationstechnischen Gesellschaft im VDE (ITG).

Autoren
Prof. Dr. Gerhard P. Fettweis, Technische Universität Dresden
Dr. Norman Franchi, Technische Universität Dresden
Frank Bittner, Universität Bremen
Prof. Dr. Armin Dekorsy, Universität Bremen
Markus Dillinger, 5G AA Vorstandsmitglied, Huawei
Dr. Zoya Dyka, IHP, Leibniz Institut für innovative Mikroelektronik
Hans J. Einsiedler, Deutsche Telekom AG
Prof. Dr. Frank Fitzek, Technische Universität Dresden
Dr. Andreas Frotzscher, Fraunhofer IIS, Institutsteil Entwicklung Adaptiver Systeme EAS
Martin Glänzer, Siemens AG, Corporate Technology
Dr. Tim Hentschel, National Instruments
Dr. Frank Hofmann, Robert Bosch GmbH
Dr. Marco Hoffmann, NOKIA Bell Labs
Dr. Ralf Irmer, Vodafone GmbH
Uwe Janßen, Deutsche Telekom AG
Josef Jiru, Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK
Dr. Volker Jungnickel, Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut, HHI
Prof. Rudi Knorr, Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK
Prof. Rolf Kraemer, IHP, Leibniz Institut für innovative Mikroelektronik
Andreas Kornbichler, Siemens AG, Corporate Technology
Dr. Markus Kückelhaus, DHL Customer Solutions & Innovation
Prof. Dr. Peter Langendörfer, IHP, Leibniz Institut für innovative Mikroelektronik
Georg Menges, NXP Semiconductors Germany GmbH
Peter Merz, NOKIA Bell Labs
Dr. Michael Meyer, Ericsson GmbH
Dr. Maciej Mühleisen, Ericsson GmbH
Dr. Andreas Müller, Robert Bosch GmbH
Dr. Erik Oswald, Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik ESK
Dr. Lutz Rauchhaupt, ifak, Institut für Automation und Kommunikation e.V.
Dr. Simone Redana, NOKIA Bell Labs
Michael Reinartz, Vodafone GmbH
Hon.-Prof. Dr. Klaus Richter, Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF
Dr. Johannes Riedl, Siemens AG, Corporate Technology
Prof. Dr. Hans Schotten, DFKI und Technische Universität Kaiserslautern
Dr. Dirk Schulz, ABB AG, Corporate Research
Dr. Dominic Schupke, Airbus
Prof. Dr. Christoph Thümmler, Edinburgh Napier University
Prof. Dr. Andreas Timm-Giel, Technische Universität Hamburg
Christian Wiebus, NXP Semiconductors Germany GmbH
Sarah Willmann, ifak, Institut für Automation und Kommunikation e.V.
Dr. Gerd Zimmermann, Deutsche Telekom AG

Und unter Mithilfe ungenannter Autoren der Automobil-, Bau- und Gesundheitsindustrie

Empfohlene Zitierweise: VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (2017): VDE-Positionspapier Resiliente Netze mit Funkzugang. Frankfurt am Main.

Inhalt

Impressum

VDE VERBAND DER ELEKTROTECHNIK
ELEKTRONIK INFORMATIONSTECHNIK e.V.

Informationstechnische Gesellschaft im VDE (ITG))
Stresemannallee 15 · 60596 Frankfurt am Main · http://www.vde.com/itg

Bildnachweise ©: VDE e.V., https://openclipart.org/search/?query=robot+arm, https://openclipart.org/search/?query=tracktor, Schaper Kommunikation
Design: www.schaper-kommunikation.de

März 2017

1 Kurzfassung und Mission

Die Digitalisierung der Gesellschaft und Industrie schreitet unaufhörlich voran, und die Bedeutung des Zugangs zu uneingeschränkter mobiler Vernetzung für unser gesellschaftliches und berufliches Leben nimmt somit ebenfalls stetig zu. Mit der Entwicklung der 5G Mobilfunkgeneration, aber auch echtzeitfähiger lokaler Funknetze werden in Zukunft digitale drahtlose Kommunikationsnetze eine Vielzahl neuer industrieller Anwendungen erschließen und dabei technische Anforderungen erfüllen, die bisher nur durch kabelgebundene Netze erfüllt werden konnten. Die stetige Erhöhung der Datenrate, die Minimierung von Ende-zu-Ende Latenzen zur Erfüllung von Echtzeitanforderungen und die Steigerung der Netzzuverlässigkeit sind aktuell zentrale Forschungs- und Entwicklungsziele bei der Optimierung von Netzen mit Funkzugang.

Etliche Ereignisse der letzten Jahre, wie bspw. die Erdbeben in Italien, die Flutkatastrophen in Süd- und Norddeutschland, abschnittsweise tagelange Ausfälle des Internets in deutschen Großstädten infolge von Netzbeschädigungen, bspw. durch Bauarbeiten, oder auch die Cyber-Angriffe auf ein deutsches Telekommunikationsnetz sowie auf vernetzte Automobile haben deutlich aufgezeigt, wie verletzlich unsere heutigen Kommunikationsnetze sind und wie wichtig es in Zukunft sein wird, dass unsere Netze die Fähigkeit haben, auch mit unbekannten und unvorhersehbaren widrigen Störereignissen umzugehen. Als Nutzer von Internetdiensten sind wir es heute gewohnt zu akzeptieren, dass das Netz einmal nicht verfügbar sein kann und versuchen es einfach zu einem späteren Zeitpunkt erneut. In sicherheitskritischen Anwendungen und Szenarien, in denen man auf die Verfügbarkeit des Netzes angewiesen ist, ist dies jedoch nicht akzeptabel.

Unsere zukünftigen Netze müssen daher mit anpassungsfähigen Sicherheitsmechanismen ausgestattet sein, um sich vor Schäden jeder Art, verursacht durch gezielte Störangriffe von Innen oder Außen, Terroranschläge, Naturkatastrophen, Unfälle, Stromschwankungen und -ausfälle oder andere extreme Störereignisse, schützen zu können. In solchen resilienten Systemen führen widrige Ereignisse mit sehr hoher Wahrscheinlichkeit nicht zu einem Ausfall der Netze, sondern allenfalls temporär zu einer reduzierten Servicequalität. In einer digitalisierten hochvernetzen Welt müssen insbesondere die zukünftigen Kommunikationssysteme auch in sehr kritischen Situationen eine Grundversorgung von relevanten Funktionen zuverlässig zur Verfügung stellen können. Der konkrete Handlungsbedarf ist in Abschnitt 2 dieses Papiers erläutert.

Die Forschung zur Resilienz von Kommunikationsnetzen zielt darauf ab, Strategien, Methoden und Technologien zu entwickeln, mit deren Hilfe sichere und robuste Netze mit Funkzugang für zukünftige industrielle wie auch öffentliche Anwendungen realisiert werden können. Dies wird allgemein als Voraussetzung gesehen, um in Zukunft verstärkt u.a. Fahrzeuge, Flugzeuge und andere Transportsysteme, Maschinen, Roboter, Industrieanlagen, Automatisierungssysteme und neue Mensch-Maschine-Schnittstellen sicher und zuverlässig miteinander vernetzen und damit vollkommen neue Anwendungen, Märkte und effizientere Wertschöpfungsketten erschließen zu können.

Auch wenn aus heutiger Sicht gravierende Störereignisse relativ selten aufzutreten scheinen, so sind sie doch faktisch existent und nehmen stetig zu. Gleichwohl nehmen die Risiken für Netzausfälle mit steigender Komplexität, insbesondere der mobilen Infrastruktur, unaufhörlich zu. Gleichzeitig sollen die zukünftigen Netze mit Funkzugang nie zuvor dagewesene Zuverlässigkeit erreichen. Je mehr die Vernetzungstechnologie unverzichtbarer Bestandteil der Anwendungen wird, desto mehr muss sie als Teil einer kritischen Infrastruktur betrachtet und geschützt werden. Netzausfälle in sicherheitskritischen Infrastrukturen können erhöhte ökonomische, persönliche und gesellschaftliche Schäden nach sich ziehen und das Vertrauen der Bevölkerung in die Technik und in Unternehmen beeinträchtigen.

Heutige Kommunikationsnetze können mit unbekannten und unvorhersehbaren netzinternen wie auch netzexternen Störereignissen nur begrenzt und meist unzulänglich umgehen. Um dies zu verbessern, müssen die Kommunikationsnetze mit Funkzugang zukünftig ihren Netzzustand durchgängig und feingranular überwachen, über elastische und prädiktive Reaktionsmechanismen sowie über adaptive Regenerations- und Lernfähigkeiten verfügen. Erzielt wird dies durch ein holistisches Resilienzkonzept nach dem „Resilience-by-Design“-Ansatz für Netze mit Funkzugang, wodurch die genannten Netzfähigkeiten und die zu berücksichtigenden Wechselwirkungen abgebildet werden.

Die Digitalisierung Deutschlands und die damit verbundenen zentralen technologischen, ökonomischen und gesellschaftlichen Herausforderungen und Zielsetzungen der Industrie und Bundesregierung lassen sich ohne resiliente digitale Kommunikationsnetze nicht bewerkstelligen und verwirklichen. Resiliente Netze sind mit ihrem hohen Grad an Verlässlichkeit, Widerstandsfähigkeit und Sicherheit unverzichtbare Grundvoraussetzungen für die vollständige Implementierung des durch die Bundesregierung vorangetriebenen digitalen Wandels hin zur Digitalgesellschaft und der intelligenten Vernetzung.

Resilienz wird zudem maßgeblich die grundlegende Akzeptanz und den erzielbaren gesellschaftlichen Wert von neuen innovativen Vernetzungstechnologien im 21. Jahrhundert beeinflussen und mitbestimmen.

Deutschland nimmt als Innovations- und Technologietreiber eine zentrale Rolle im Bereich der 5G-Forschung sowie der 5G-Anpassung auf die einzelnen Bedürfnisse der verschiedenen industriellen Verwertungszweige, auch „Verticals” genannt, ein. Zudem ist Deutschland führend im Bereich der Zuverlässigkeitsforschung. Deutschland hat demzufolge hervorragende Ausgangsbedingungen, um in dem noch jungen, aber für zukünftige Netze mit Funkzugang entscheidenden Forschungsfeld „Resilienzforschung“ maßgeblich Impulse zu setzen.

Dieses Impulspapier zeigt die Notwendigkeit für die Erforschung und Entwicklung von resilienten Netzen mit Funkzugang auf. Es erläutert und erörtert die dabei relevanten Aspekte. So werden aufbauend auf der einleitenden Kurzfassung und Motivation anschließend in Abschnitt 2 die aus dem Papier abgeleiteten Thesen und Handlungsempfehlungen vorgestellt. Die Bedeutung von Resilienz in allgemeiner Form und ihre grundlegenden Eigenschaften wird anhand von Beispielen in Abschnitt 3 dargelegt. In Abschnitt 4 werden dann die Notwendigkeit für und Anforderungen an resiliente Netze aus der Perspektive von wichtigen zukünftigen Anwendungsfeldern aufgezeigt. Die zu berücksichtigenden Störeinflüsse beim Design von resilienten Netzen werden in Abschnitt 5 beschrieben. Danach wird in Abschnitt 6 Resilienz in Bezug auf Kommunikationsnetze mit Funkzugang definiert und erläutert. Aufbauend darauf werden dann in Abschnitt 7 die Herausforderungen und Ansätze konkret aus unterschiedlichen technologischen Blickwinkeln beleuchtet und zum Abschluss eine anwendungsübergreifende Übersicht zu Netzanforderungen gegeben.

VDE-Positionspapier Resiliente Netze mit Funkzugang
© VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

2 Thesen und Handlungsbedarf

These 1: Die zentralen technologischen, ökonomischen und gesellschaftlichen Herausforderungen und Zielsetzungen der Digitalisierung in Deutschland lassen sich ohne resiliente digitale Kommunikationsnetze nicht lösen und verwirklichen. Resiliente Netze sind mit ihrem hohen Grad an Verlässlichkeit, Widerstandsfähigkeit und Sicherheit unverzichtbare Grundvoraussetzungen für die vollständige Implementierung des durch die Bundesregierung vorangetriebenen Wandels hin zur Digitalgesellschaft und der intelligenten Vernetzung. Partiell resiliente Kommunikationsnetze sind heute nur in Spezialanwendungen realisiert (z.B. Banken, Energie). Dies muss sich ändern.

Handlungsempfehlung: Erforschen, entwickeln, quantifizieren und verstehen von Resilienz als holistisches integratives Designkonzept zur Sicherung von Kommunikationsnetzen mit Funkzugang und den darüber realisierten Anwendungen vor schädigenden Auswirkungen von externen und internen widrigen Störereignissen.

These 2: Resilienz ist eine entscheidende Fähigkeit von sicheren Kommunikationsnetzen, die im 21. Jahrhundert maßgeblich die grundlegende Akzeptanz und den erzielbaren gesellschaftlichen Wert von neuen innovativen Vernetzungstechnologien beeinflussen und bestimmen wird.

Handlungsempfehlung: Die steigende Bedeutung von Kommunikationsnetzen für die industrielle und gesellschaftliche Weiterentwicklung in Deutschland erfordert eine Erweiterung um die Resilienz-Perspektive, welche auf eine sicherheitsbezogene, strategische und nachhaltige Optimierung von Infrastrukturen abzielt.

These 3: Resilienz stellt eine Schlüsselkompetenz für die Umsetzung von sicheren Kommunikationsnetzen mit Funkzugang dar.

Handlungsempfehlung: Kommunikationsbezogene Resilienzforschung bzw. Resilience Engineering sollte für das Design von Kommunikationsnetzen mit Funkzugang als eigenständiges Fachgebiet etabliert werden. Dies betrifft die Forschung, Entwicklung sowie die kommerzielle Planung und Umsetzung von resilienten Infrastrukturen und Geräten.

These 4: Resiliente Netze sind kein vermeintlicher Kostenverursacher, sondern versprechen eine Vielzahl neuer Geschäftsmodelle und Business Cases und schaffen einen langfristigen ökonomischen und gesellschaftlichen Mehrwert.

Handlungsempfehlung: Gesellschaftliche und ökonomische Aspekte müssen untersucht und dabei aufgezeigt werden, welcher quantifizierbare Mehrwert durch die Resilienzforschung in Hinblick auf die Erhöhung der Netzsicherheit und der Nachhaltigkeit geschaffen werden kann. Zudem sollten frühzeitig Finanzierungs- und Förderungsinstrumente geschaffen werden, um innovative Gründungen und Start-Ups mit dem Schwerpunkt Resilience Engineering zu ermutigen und zu unterstützen, damit Deutschland im Bereich Kommunikationsnetze auch in den nächsten Jahren dynamisch und wettbewerbsfähig ist.

VDE-Positionspapier Resiliente Netze mit Funkzugang

These 5: Deutschland verfügt über eine hervorragende Ausgangssituation durch Detailwissen der Anwendungsindustrien für die resiliente Kommunikation eine Grundvoraussetzung für eine erfolgreiche Digitalisierung ist. Zum Erhalt und Ausbau dieser Rolle sowie der Wettbewerbsfähigkeit müssen jedoch Anreize für Unternehmen geschaffen werden, die Resilienzeigenschaften ihrer Netze zu erhöhen.

Handlungsempfehlung: Für die Realisierung von resilienten Netzen mit Funkzugang bedarf es interdisziplinärer und branchenübergreifender Anstrengungen von Industrie und Forschung mit Unterstützung durch Förderprogramme, um die zukünftigen technologischen Herausforderungen zu meistern. Eine nationale Strategie für resiliente öffentliche Netze sollte entwickelt werden.

These 6: Widrige Ereignisse, auch wenn sie häufig lokaler Natur sind, haben Auswirkungen auf die Infrastruktur, die nicht lokal oder national beschränkt sind. Um die Resilienz von Netzen auf internationaler Ebene gewährleisten zu können, sind gemeinsame und verbindliche Begrifflichkeiten und Kennziffern nötig. Standardisierungsgremien und regulatorische Gremien spielen eine wichtige Rolle bei der Sicherstellung von Resilienz in modernen Kommunikationsnetzen. Funkspektrum stellt die knappste und wertvollste Ressource für Funknetze dar und unterliegt der staatlichen Aufsicht.

Handlungsempfehlung: Berücksichtigung von regulatorischen Einflüssen und Auswirkungen auf die Realisierung von resilienten Netzen und ggf. Vorantreiben von erforderlichen regulatorischen Anpassungen.

These 7: Die Modellierung und Evaluation von Resilienz und die entsprechend erzielbare Verfügbarkeit von drahtlosen Kommunikationsnetzen ist essentiell für die Zertifizierung.

Handlungsempfehlung: Industrie, Wissenschaft sowie staatliche, bzw. vom Staat für die Zertifizierung beauftragte Stellen müssen gemeinsam anerkannte Methoden zur Modellierung und Evaluation entwickeln. Diese müssen validiert und ständig verbessert werden.

3 Resilienz im Allgemeinen

Der Begriff Resilienz (von lat. resilire: zurückspringen, abprallen) findet seit vielen Jahren Anwendung in verschiedensten Disziplinen wie der Psychologie, Infrastrukturforschung, Ökologie, Ökonomie sowie den Sozial- und Ingenieurwissenschaften. Er beschreibt die Fähigkeit eines Systems, auf Krisen und Störungen reagieren zu können, sich im Sinne der Selbstregulierung zu erneuern ohne sich grundlegend zu verändern [1].

Grundlegend zeichnen sich resiliente Systeme durch Eigenschaften aus, welche sich auch sehr gut anhand der Eigenschaften eines Baumes bei zeitweisen Stürmen veranschaulichen lässt (siehe Abbildung 1):

- Widerstandsfähigkeit durch Elastizität/Anpassungsfähigkeit ermöglicht dynamische Reaktion auf Störung und Sicherstellung funktionaler Minimalanforderungen
- Regenerationsfähigkeit durch weiche Rückführung in den stabilen Normalzustand bei Abklingen der Störung, sowie Überführung von Funktionen in andere Systemteile bei irreparable Beschädigungen einzelner Systemteile
- Fortlaufende, langfristige Stärkung des Systems aus den Erfahrungen aller Ereignisse durch Lernfähigkeit (Reifung)

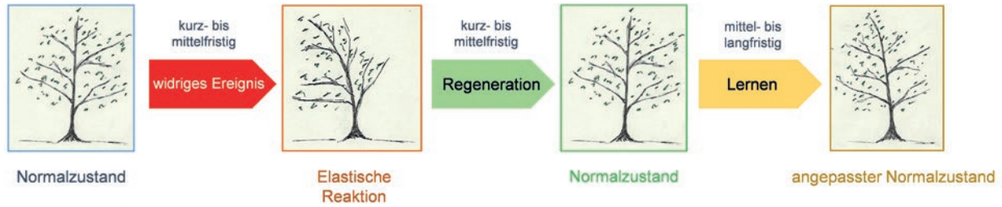

Abbildung 1: Beispiel zur Veranschaulichung grundlegender Resilienzeigenschaften

Um die Rolle technologischer Lösungen im Zusammenhang von Resilienz weiter zu verdeutlichen, wird in Abbildung 2 ein zweites Beispiel, der Hochwasserschutz, veranschaulicht. Ob in den Flüssen oder an der Küste unterliegt der Wasserstand einer stetigen Veränderung. Den typischen bekannten Schwankungen und typischen Störungen wird beispielsweise über statische Vorkehrungen, wie eine überhöhte Kaimauer und Deichen, begegnet. Durch widrige Einflüsse, wie Orkane, starken Regen, Schmelzwasser oder Erdbeben, treten besondere Situationen auf, die ohne zusätzliche Gegenmaßnahmen verheerende Auswirkungen haben können. Ein frühes Erkennen von widrigen Ereignissen und eine vorausschauende Abschätzung der Auswirkungen (Prädiktion), also die Kenntnis über den erwarteten erhöhten Wasserstand, ermöglicht ein rechtzeitiges Einleiten von nachgeschalteten Maßnahmen, wie beispielsweise das Sperren des Hafengebiets, Aufhäufen von Sandsäcken (Fall A in Abbildung 2) oder gegebenenfalls das Aufstellen von temporären Schutzwänden (Fall B) sowie der Evakuierung von Wohngebieten (Widerstandsfähigkeit). Mit dauerhaftem Abklingen der Flut können die eingeleiteten Maßnahmen nach und nach aufgehoben und mit der Beseitigung der Auswirkungen begonnen werden (Regeneration). Im

Abschluss können die konkreten Erfahrungen der Hochwassersituation genutzt werden, um langfristig Maßnahmenprozesse inklusiv der Prädiktion zu verbessern (Lernfähigkeit). Darüber hinaus werden Deichverläufe optimiert, zusätzliche Absperrmöglichkeiten vorbereitet, und verstärkt Ausgleichsflächen in Flussverläufen geschaffen. Im Sinne der Resilienz muss möglichst gewährleistet werden, dass ein einsetzendes Hochwasser nicht zu einer Katastrophe führt.

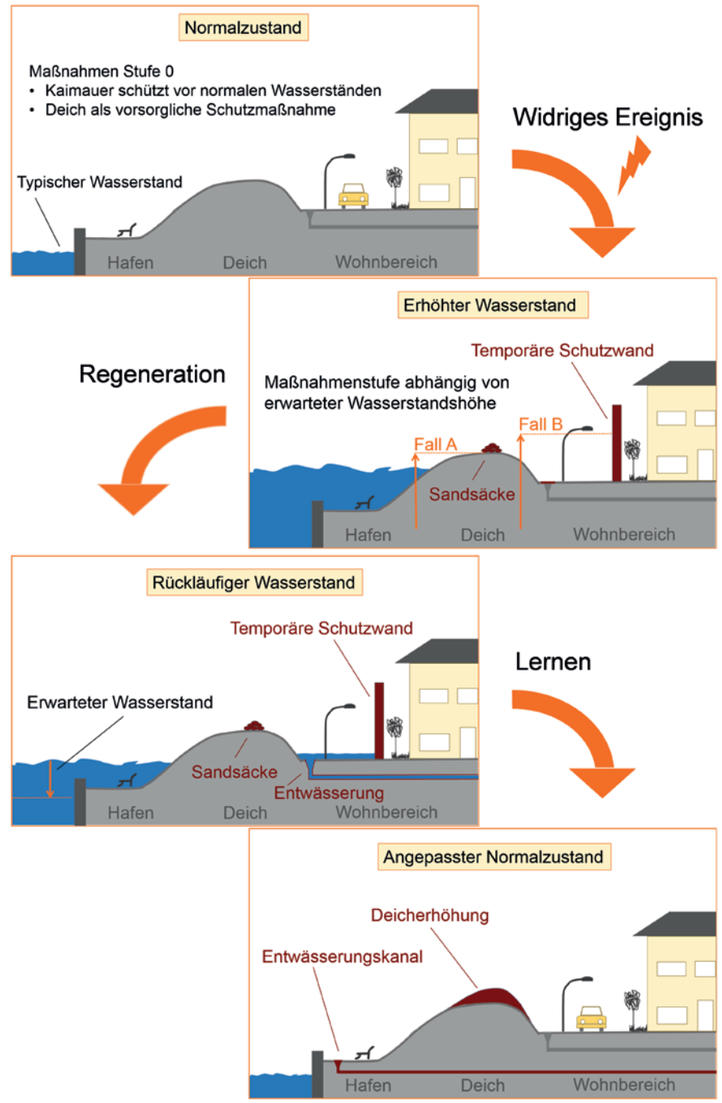

Abbildung 2: Veranschaulichung der Notwendigkeit von Resilienz und dem Zusammenspiel von Resilienzmaßnahmen

4 Anwendungsperspektiven: Bedarf und Anforderungen

Nachfolgend werden die Anforderungen an zukünftige Kommunikationsnetze und damit auch die Bedeutung von resilienten Netzen mit Funkzugang aus Sicht von wichtigen Anwendungsfeldern aufgezeigt.

4.1 Automotive

Der Individualverkehr steht vor einem fundamentalen Umbruch. Selbstfahrende vernetzte Autos werden unsere Lebensbedingungen verändern. Für die Automobilbranche, aber auch für andere Sektoren wie Logistik, Versicherungen, Serviceunternehmen und Stadtplanung bedeutet dies einen großen Wandel. Kommunikationstechnik spielt für die Umsetzung des vernetzten Fahrzeuges eine zentrale Rolle. Das vernetzte selbstfahrende Fahrzeug erfordert die Kooperation der verschiedenen Sektoren, wie Mobilfunkbetreiber, Auto- und Telekommunikationshersteller. Deshalb wurden zu dem bereits seit 2007 existierenden Car2Car Communication Consortium (C2C-CC) im September 2016 die 5G Automotive Association e.V. (5GAA) sowie die European Automotive Telecom Alliance (EATA) gegründet um Anforderungen und Lösungen gemeinsam zu entwickeln.

Bereits heute verfügbare Dienste zeigen das Potential der Fahrzeugvernetzung auf. Neben Entertainmentangeboten für den Fahrer- und Passagierkomfort lässt sich durch Funktionen wie eCall die Sicherheit der Insassen erhöhen. Da die fahrzeugeigene Sensorik nur den Nahbereich des Fahrzeugs überwachen kann, ist die drahtlose Kommunikation zur Erweiterung der „Sichtweite“ ein wesentlicher Bestandteil des hochautomatisierten Fahrens. Einerseits können sich Verkehrsteilnehmer damit gegenseitig vor kurzfristigen Gefahrensituationen warnen, den Spritverbrauch senken und die Verkehrseffizienz steigern. Wird weiterhin die Kommunikation zwischen Verkehrsinfrastruktur und Fahrzeugen eingebunden, so spricht man von C-ITS (Cooperative Intelligent Transport Systems).

Für die Transformation von Autos in vernetzte automatisierte Fahrzeuge, welche auch komplexeste Straßen- und Umfeldsituationen meistern können, sind weitere technologische Stufen zu erklimmen. Aber auch widrige Wetterbedingungen schränken die Leistungsfähigkeit der Sensoren ein. Beim Elektrofahrzeug ergeben sich auch weitere Einschränkungen in der Reichweite, weil eventuelles Oberflächeneis auf den Sensoren durch die Heizsysteme entfernt werden muss. Der Energieverbrauch dieser Heizsysteme (ca. 60 Watt pro Sensor) verringert damit die Fahrzeugreichweite. Über kooperative Perzeption können Fahrzeuge Sensordaten, wie bspw. durch Radar oder Video detektierte Objektinformationen, austauschen. Dabei ist aber auch die Herausforderung zu berücksichtigen, dass bspw. widrige Wetterbedingungen die Leistungsfähigkeit der Sensoren beeinträchtigen können. Die kooperative Manöverplanung erlaubt eine Abstimmung der Fahrtrajektorien zwischen Autos mittels Funk, wie dies zum Beispiel beim „Einfädeln“ notwendig ist. Mit diesen Fähigkeiten lassen sich Funktionen wie Kolonnenfahrt mit sehr geringen Abständen zwischen den Fahrzeugen realisieren, wodurch der Treibstoffverbrauch deutlich gesenkt werden kann.

Die Herausforderungen für die dargestellten Funktionen sind vielfältig und umfassen sehr hohe Anforderungen bezüglich Resilienz, Latenz und Zuverlässigkeit der Funkkommunikation, eine durchgehende Netzabdeckung sowie Aspekte zu Security und Privacy. Die Verbindungsqualität muss laufend überwacht und prädiziert werden, bei Bedarf ist eine schnelle Anpassung nötig, z.B. durch eine Anpassung des QoS-Grades (Quality-of-Service) oder einen Wechsel der Kommuni-

kationstechnologie. Über das Netz können Fahrzeugen zudem aktuelle Zustandsinformationen des Netzes (z.B. temporäre Funklöcher an Straßenbereichen, Zellüberlastsituationen etc.) geliefert werden, die für präventive Maßnahmen genutzt werden können. Durch die steigende Kritikalität der Anforderungen bekommt die Resilienz des Kommunikationsnetzes und vor allem des Funkzugangs eine entscheidende Bedeutung. Dabei ist die Vernetzung des Fahrzeuges mit anderen Fahrzeugen (V2V), mit Motorrädern (V2M), mit Infrastrukturkomponenten wie z.B. Ampeln (V2I), mit dem Internet oder Backend-Servern (V2N) sowie zwischen nichtmotorisierten Verkehrsteilnehmern (V2P) zu berücksichtigen. Die hohe Sicherheit, die präzise Zuverlässigkeit und die kurzen Latenzen in der Vernetzung sind zur erfolgreichen Einführung des vernetzten hochautomatisierten Fahrens zwingend notwendig.

Folgende Fähigkeiten für die Resilienz des Kommunikationsnetzes sind hier von besonderer Relevanz:

- Widerstandfähigkeit gegenüber widrigen Störereignissen im Funkzugang, wie bspw. umgebungsbedingte, unvermeidbare, gegenseitige Störung zwischen Funkteilnehmern, aber vor allem auch gezielte Funkstörung von außen (Jamming): Eine permanente Überwachung der Funksituationen kombiniert mit den Fähigkeiten zur Prädiktion und Adaption durch Nutzung unterschiedlicher Kommunikationstechnologien (z.B. zellulare und direkte Funkverbindungen zwischen Verkehrsteilnehmern) ist hierfür ein Ansatz.
- Vermeidung von Single Points of Failure (SPoF): Maßnahmen sind hier z.B. Redundanzelemente an wichtigen Stellen im Netz und im Fahrzeug vorzusehen.
- Ermöglichung von Rückfallgarantien im Netz: Gewährleistung von Basisfunktionalitäten im Störungsfall, z.B. durch garantierte Datenraten, um die wichtigsten Fahrfunktionen weiterhin ausführen zu können.
- Bereitstellung von Fail-Safe Mechanismen: Kompensation oder zumindest Minderung der Auswirkungen von Fehlern im Netz, indem z.B. bereits in der Entwicklung von Fahrfunktionen mögliche Netzfehler berücksichtigt werden, aber auch die Netze und Fahrzeuge im Falle extremer Störungen in anwendungsabhängigen Reaktionszeiten in sichere Modi übergehen.
- Schnelle Regenerationsfähigkeit des Netzes: Eigenschaften des Netzes, um Ausfallzeiten gering zu halten und Gegenmaßnahmen einzuläuten, um die ursprüngliche Netzleistung wieder herstellen zu können.

Die erforderlichen Maßnahmen umfassen die kombinierte Betrachtung von Fahrer, Fahrzeug und Netz, was neue Lösungsansätze notwendig macht, und damit Forschungsbedarf in Industrie und Wissenschaft erfordert. Die bisherige Forschung konzentriert sich stark auf QoS- und Security-Aspekte, wobei das Thema Resilienz nicht genauer betrachtet wurde, die für das vernetzte automatisierte Fahren und die Realisierung von sicherheitskritischen Anwendungen jedoch eine wichtige Rolle spielt.

4.2 Industrie 4.0 (Produktion und Automation)

Derzeit wird die industrielle Vernetzung von drahtgebundenen Technologien (z.B. Industrial Ethernet, Feldbusse) dominiert. Funksysteme fristen immer noch ein Nischendasein. Sie werden hauptsächlich zur Datenanbindung unkritischer mobiler oder beweglicher Subsysteme (z.B. mobile Bedienpanels, Elektrohängebahn, Rundtaktmaschinen), für Monitoring-Aufgaben oder den Fernzugriff auf Anlagen eingesetzt. Diese Anwendungen stellen vergleichsweise geringe Anforderungen an die Verfügbarkeit, Zuverlässigkeit und Echtzeitfähigkeit der eingesetzten Funksysteme.

Auch in Anlagen der Prozessindustrie mit großer Flächenausdehnung werden fast ausschließlich drahtgebundene Netze eingesetzt. Die Kosten für die Installation neuer Sensoren werden hauptsächlich von der Verkabelung bestimmt [2]. Big-Data-Anwendungen, die von zusätzlicher Sensorik stark profitieren würden, sind damit wirtschaftlich oft unattraktiv.

Eine wesentliche Grundlage für die vierte industrielle Revolution ist generell die enge Verzahnung der klassischen Produktions- und Automatisierungswelt mit modernen IKT-Technologien. Auf diese Weise werden cyber-physische Produktionssysteme geschaffen, die sich durch einen noch nie dagewesenen Grad an Flexibilität, Wandelbarkeit, Effizienz und Produktivität auszeichnen. Dies kann aber nur erreicht werden, wenn zukünftig auch verstärkt drahtlose Zugangstechnologien zum Einsatz kommen. Dies gilt beispielsweise für die Vernetzung mobiler Roboter, fahrerloser Transportsysteme, für die Anbindung von mobilen Human-Machine-Interfaces (HMI), wie z.B. Augmented-Reality (AR) Brillen, oder für die Etablierung hochmodularer und Plug-&-Play-fähiger Produktionsmodule, die flexibel und ohne großen Aufwand miteinander kombiniert werden können.

Drahtlose Zugangstechnologien sind dabei verschiedenen widrigen Umständen (z.B. schlechter Funkempfang, elektromagnetische Interferenzen durch Produktionsprozesse oder der Ausfall einzelner Vernetzungskomponenten), aber auch bewusst herbeigeführten Störungen (z.B. Jamming oder IT-Angriffe) ausgesetzt. In den lizenzfreien Frequenzbändern können sich zudem benachbarte Funksysteme wechselseitig beeinflussen und so genannte Koexistenzprobleme verursachen [3]. Diese Störungen können die Zuverlässigkeit der Funkübertragungen erheblich beeinträchtigen und schlimmstenfalls zu Verbindungsabbrüchen führen. In Abhängigkeit der Dauer der Störung und der Widerstandsfähigkeit der Anwendung können einzelne Systeme oder Produktionsanlagen ausfallen und somit die übergeordneten Produktionsabläufe empfindlich stören oder gar ungeplante Produktionsausfälle mit erheblichen finanziellen Schäden verursachen.

Daher ist eine hohe Resilienz der zugrundeliegenden Netze eine wichtige Voraussetzung, um in flexiblen, effizienten und wandelbaren Produktionssystemen ein hohes Maß an Verfügbarkeit, Zuverlässigkeit und funktionaler Sicherheit gewährleisten zu können. Störungen müssen frühzeitig detektiert werden, um geeignete Gegenmaßnahmen schnell ergreifen und mögliche Schäden (z.B. Produktionsausfälle) abwenden zu können.

In einer offenen Industrie 4.0 Systemarchitektur sind folgende Aspekte und Fähigkeiten für die Resilienz industrieller Netze besonders relevant:

- Permanente Überwachung des Netzzustands (inkl. relevanter QoS-Parameter) und der Koexistenzsituation zwischen benachbarten Funknetzen zur frühzeitigen Detektion von möglichen Problemen, aber auch zur Rückverfolgbarkeit von Störungen
- Widerstandsfähigkeit gegenüber widrigen Umständen sowie bewusst herbeigeführten Störungen
- Schnelle und automatisierte Regenerationsfähigkeit zur Minimierung von Stillstandzeiten
- Antizipation von möglichen Problemen und adaptive, an die jeweilige Situation angepasste Reaktion der Anwendungen bei bestehenden oder absehbaren Beeinträchtigungen im Netz („Graceful Degradation“)
- Möglichkeit zum räumlichen begrenzten, autarken Betrieb von Funksystemen (z.B. in einer Fabrik), ohne unkontrollierte Interferenzen. Dies könnte insbesondere durch ein dezidiertes (eigenes) Frequenzband ermöglicht werden, alternativ ggf. aber auch mittels neuer, flexiblerer Spektrumsnutzungskonzepte.
- Schnittstellen zur Verhandlung der zugesicherten Dienstgüten mit den Anwendungen und deren Kontrolle
- Selbstmanagement der Vernetzungsinfrastruktur inkl. Funkschnittstelle zur schnelleren Reaktionsfähigkeit und zur Erhöhung der Benutzerfreundlichkeit
- Schnittstellen zum Koexistenz- und Interferenzmanagement zwischen verschiedenen Funksystemen

Bei allen Punkten besteht Forschungs- und Normierungsbedarf in Industrie und Wissenschaft.

VDE-Positionspapier Resiliente Netze mit Funkzugang
© VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

4.3 Gesundheitswesen, Pharmazeutische Industrie und eHealth

Gesundheitssysteme sind soziale Sicherungssysteme, die weltweit als kritische Infrastrukturen verstanden werden. Funktionierende “Kritische Infrastrukturen” sind für die Aufrechterhaltung geordneter Abläufe im gesellschaftlichen Tagesgeschäft unerlässlich und als besonders schützenswert einzuordnen. Aufgrund gesetzlicher Bestimmungen sind zudem die relevanten Daten als besonders schutzwürdig eingestuft. Daraus ergeben sich besondere Anforderungen an die Resilienz der Netze im Gesundheitswesen, die nicht nur gesetzlich, sondern auch durch internationale Standardisierung definiert sind (z.B. ISO 80001, ISO 27000, IEEE 302.15.6). Die Bundesregierung hat mit Blick auf die Stärkung der Zukunftsfähigkeit der Digitalisierung des Gesundheitswesens deshalb kürzlich das „Gesetz für sichere Digitale Kommunikation und Anwendungen im Gesundheitswesen sowie Änderungen weiterer Gesetze“ beschlossen und das SGB V entsprechend geändert [4]. Der radikale Umbruch der Versorgungskonzepte von einem zentralistischen, systemorientierten Ansatz hin zu einem verteilten, patientenzentrierten Modell soll das Subsidiaritätsprinzip und die Selbstbestimmungsrechte der Menschen stärken und die Wertschöpfung aus dem „Sozialen Kapital“ unterstützen. Dezentralisierte, dynamische Versorgungskonzepte, die sich Industrie 4.0 Prinzipien bedienen, sind jedoch in einem hohen Maß auf Echtzeitkommunikation angewiesen und erfordern widerstands- und leistungsfähige Kommunikationssysteme [5].

Eine interessante Entwicklung ist die Tatsache, dass relevante europäische Regularien, basierend auf Direktiven und den Empfehlungen der multinationalen BEREC Kommission klar herausstellen, dass die Priorisierung von Gesundheitsdaten ungeachtet der bestehenden Regelungen zur Netzneutralität ausdrücklich gestattet ist [6, 7]. Das bedeutet, dass die Servicequalität (QoS) in anderen Netzsegmenten abgesenkt werden darf, um Gesundheitsdienste zu stabilisieren.

Somit ist es von großer Bedeutung, dass definierte Parameter bei der Signalübertragung gezielt gesteuert und sichergestellt werden können. Dies ist insbesondere relevant für Szenarien, in denen die reale Welt in Echtzeit dynamisch mit einer virtuellen, computerbasierten Realität zur Prozessoptimierung verknüpft werden soll (Cyber-Physical Systems, CPS).

- Interessante Trends und zukünftig Anwendungsbeispiele von herausragender sozioökonomischer Bedeutung sind hierbei u.a.

- der wachsende Dienstleistungssektor der pharmazeutischen Industrie (z.B. Echtzeitanalyse von Daten von netzfähigen Asthma-Inhalarien und Insulin-Pens, Feedback über Mobiltelefone, Bereitstellung externer Dienste) [9]

- die Vernetzung Deutscher Kliniken durch das Innovationsprogramm „Medizininformatik“ der Bundesregierung zu Forschungszwecken und zur Optimierung der Versorgungsqualität [5]

- „Krankenhaus zu Hause“, die Vernetzung mobiler medizinischer Geräte und die Integration von Diensten (Dialyseapparate, Infusionspumpen, Insulinpumpen, Informationsintegration durch Algorithmen)

- Anti-Counterfeiting (Anwendung von Blockchain-Technologie zur Authentisierung von Medikamenten und hochwertigen Gütern)

- Medizinische und soziale Robotik [10]

Resilienz spielt für die sichere Digitalisierung von Gesundheitsleistungen und für die Nachhaltigkeit neuer Geschäftsmodelle eine herausragende Rolle. Die Erfassung, Speicherung und intelligente Auswertung von großen Datenmengen wird in den kommenden Jahren eine entscheidende Rolle in der Weiterentwicklung der Medizin spielen. „Big Data“ wird auch das Gesundheits-

wesen grundlegend verändern und entscheidende Fortschritte in den Bereichen Bildverarbeitung und Genomanalyse hin zur personalisierten Medizinversorgung erlauben. All diese Entwicklungen setzen allerdings die Verfügbarkeit sicherer, robuster, zuverlässiger und schneller Netzinfrastruktur voraus. Algorithmen, die bspw. eine drohende, akute Zustandsverschlechterung bei Asthmatikern oder Diabetespatienten erkennen und somit das Risiko einer Krankenhauseinweisung oder einer Exazerbation senken sollen, sind auf einen kontinuierlichen Fluss zuverlässiger, authentischer Daten angewiesen. Netze müssen in der Lage sein, die notwendige Servicequalität jederzeit und an jedem Ort auch unter widrigsten Umständen zur Verfügung stellen zu können. Patienten und Angehörige können im „Krankenhaus zu Hause“ nur Aufgaben übernehmen, wenn die Unterstützung durch digitale Dienste immer, also unabhängig vom aktuellen Netzzustand, uneingeschränkt zur Verfügung steht. Die ständige Netzverfügbarkeit bei gleichzeitiger Performancegarantie sind hierbei unter Umständen lebenswichtige Voraussetzungen. Patienten oder deren Beauftragte sollen außerdem in der Lage sein im Einklang mit der bestehenden Gesetzgebung die Nutzung ihrer persönlichen Daten zu kontrollieren. Ähnliches gilt für Körperschaften des öffentlichen Rechts, die gesetzlich geregelte Aufgaben der Selbstverwaltung wahrnehmen (z.B. Gematik). Neue Netzstrategien sollen außerdem die Sicherheit der Patienten im Zusammenhang mit Online-Bestellungen von Diensten und medizinischen Produkten erhöhen. Das Marktvolumen gefälschter Medikamente wird weltweit derzeit auf etwa 200 Milliarden US Dollar pro Jahr geschätzt. Blockchain-Technologien sind geeignet ähnlich wie bei elektronischen Währungen (Bitcoin) die Authentizität von Medikamenten oder hochwertigen Gütern an jedem beliebigen Punkt in der Wertschöpfungskette zu belegen. Langfristig wird sich global der Trend zur künstlichen Intelligenz (AI) und Robotik, vor allem im häuslichen Pflegesektor, verstärken. Diese Maschinen müssen aus ethischen und sicherheitstechnischen Überlegungen heraus einer zentralen Echtzeitüberwachung (Pflege, Wartung, Management) unterliegen. Mit Blick auf die Sicherung der Netze ist es außerdem von großer Bedeutung, dass mobile Endgeräte und Sensoren nicht durch Hackerangriffe (z.B. DDoS-Attacken) als „Waffen“ gegen Netze und Plattformen gerichtet werden können. Aber auch bei der Vernetzung von bildgebenden, diagnostischen oder therapeutischen medizinischen Geräten ist der Schutz vor Manipulation oder Missbrauch von entscheidender Bedeutung. Die Widerstandsfähigkeit der Netze und deren Komponenten muss dazu deutlich verbessert und es müssen gemeinsame Standards angestrebt werden. Die Zusicherung von funktionaler Sicherheit, auch unter widrigen Störeinflüssen, ist eine zentrale Anforderung an zukünftige Kommunikationsnetze.

Heutige Netze und die bisherige Netzabdeckung sind aus Sicht des Gesundheitswesens nicht ausreichend geeignet, um in Zukunft die Anforderungen der Digitalisierung in diesem Bereich erfüllen zu können. Zeit- und aufgabenkritische Anwendungen, sog. Mission-Critical Applications, erfordern verbindlich zugesicherte Servicequalitäten und dies auch oder ggf. erst recht unter widrigen Störeinflüssen des Netzes. „Best Effort“ Strategien können die erforderlichen Garantien nicht liefern. Die Fernsteuerung von kritischen Prozessen, wie z.B. die Korrektur der Förderrate einer Insulinpumpe oder die Justierung eines Hirnschrittmachers oder Interventionen (bspw. die ferngesteuerte assistierende robotische Intervention), sind somit -obgleich medizinisch möglich- nicht risikofrei zur Anwendung zu bringen. Auch fehlt es bisher an geeigneten Methoden, um diese in Zukunft erforderlichen Servicequalitäten zu jedem erforderlichen Zeitpunkt, an jedem Ort und unter widrigsten Umständen zuverlässig feststellen zu können. Robuste, widerstandsfähige Netztechnologien mit geeigneten und messbaren Spezifikationen sind eine grundlegende Voraussetzung für die erfolgreiche Digitalisierung des (Deutschen) Gesundheitswesens. Netze müssen in der Lage sein durch Priorisierung von Diensten, dynamischem Routing, Rückfallstrategien und das frühzeitige Erkennen von Anomalien und Angriffen eine ausreichende Servicequalität sicher zu stellen. Spezifische Anforderungen für digitale, zukunftsfähige Netze im Gesundheitswesen wurden eingehend analysiert und bereits in mehreren Veröffentlichungen detailliert beschrieben [11, 12, 13]. Resilienz und möglichst hochwertige Servicequalitäten wurden hierbei klar als Schlüsselanforderungen herausgestellt.

VDE-Positionspapier Resiliente Netze mit Funkzugang
© VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

4.4 Logistik 4.0

Logistik 4.0 versteht sich als Integrator für alle industriellen Anwendungsgebiete in der Gigabit-Gesellschaft und umfasst - ähnlich zu Industrie 4.0 - digitalisierte Prozesse und Systeme, die auf einem kontinuierlichen Datenaustausch zwischen den Mitarbeitern, der Fracht und den Betriebsmitteln beruhen. In Logistik 4.0 werden für unterschiedliche Supply-Chain-Umgebungsbedingungen und Modalitäten wie die Intralogistik im produzierenden Unternehmen, den Logistik-Hubs, dem Straßen-, Land- und Lufttransport sowie der „letzten Meile“ in Städten unterschiedliche Anforderungen an die IT-Infrastruktur und damit im besonderen Maße auch an die drahtlose Kommunikation gestellt [37].

Frachtstücke und Ladungsträger sind international unterwegs und benötigen die Konnektivität regionen- und grenzübergreifend. Lückenlose Konnektivität bedeutet auch Konnektivität auf dem Verkehrsmittel, ob nun bspw. LKW, Flugzeug oder Schiff, die derzeitig auf Grund internationaler Regularien und teilweise fehlender Infrastrukturen nicht durchgängig gewährleistet werden kann. Die Logistik benötigt daher eine durchgängige, kontinuierliche und sichere Konnektivität, wenn auch mit geringen Datenraten, um lückenlos über die gesamte (weltweite) Logistikkette, beginnend an der Montagelinie des produzierenden Unternehmens bis hin zum privaten Endkunden bspw. im ländlichen Raum, kommunizieren zu können. Es werden hohe Anforderungen an die energiesparsame Anbindung an Weitverkehrsnetze, hinsichtlich geringer Investitions- und Kommunikationskosten, an hohe Lebensdauern und an die flächendeckende Verfügbarkeit gestellt.

Für die Logistik der Zukunft werden Telekommunikationsdienste benötigt, die über gemeinsame Serviceplattformen und sich gegenseitig ergänzende, konvergente Netzstrukturen [35] bedarfsgerecht und ohne feste Grenzen den Kommunikationszugang für das logistische Objekt (auf allen Hierarchieebenen vom Packstück bis zum Container), das Betriebsmittel oder den Mitarbeiter bereitstellen.

Breitbandige Kommunikationsverbindungen kommen bereits bei örtlich abgesetzten Röntgenkontrollen, in der videobasierten Situationsanalyse im Logistikhub oder beim privaten Endkunden zum Einsatz und werden zukünftig aber auch für Robotik-Lösungen stärker notwendig. In speziellen Szenarien werden materialflusstechnische Anlagen analog zu Industrie 4.0-Szenarien ferngesteuert. Störungen in der Datenübertragung können zu einem Stillstand des logistischen Prozesses führen, der aber robust wiederaufgenommen wird, wenn z. B. die Frachtstücke automatisch identifizierbar sind. Der Erfolg von sicheren Roboterlösungen im öffentlichen Raum wird von der Konnektivität vergleichbar zur V2X-Kommunikation abhängen. [38]

Internationale Logistik bedeutet auch die Einhaltung internationaler Regelwerke zur zivilen Sicherheit entlang der gesamten Transportkette. Netzneutralität darf diesen Forderungen nicht entgegenwirken. Zollorganen und Sicherheitsbehörden muss ein effizienter Zugriff auf Daten zur Fracht und zum Versender/Empfänger ermöglicht werden, um die logistischen Prozesse nicht zu behindern. Die Regularien müssen ein Roaming zwischen unterschiedlichen Netzanbietern diskriminierungsfrei ermöglichen. Netze und TK-Angebote müssen entsprechend der Kurzfristigkeit in der Kontraktlogistik dynamisch anpassbar sein und eine Logistik-Konnektivität bis an die Montagelinie in der Fabrikhalle anbieten.

Resilienz im logistischen Sinn bezeichnet die Fähigkeit einer Verkehrsinfrastruktur, ihre Funktionalität trotz störender widriger Ereignisse zu wahren, indem sie das Ausmaß, den Einfluss und/oder die Dauer störender Ereignisse zu vermindern vermag [36]. Der Ausfall der Kommunikationssysteme in einer sicherheitskritischen

Logistikinfrastruktur, die Grundlage für das Monitoring und die Steuerung logistischer Prozesse sind, würde große Auswirkungen auf die gesamte Wirtschaft eines Strukturraumes haben. Somit ist die Resilienz der Logistik im besonderen Maße abhängig von der Resilienz der Kommunikationsnetze in ihrer räumlichen, zeitlichen und aufgabenbezogenen Diversität. Forschungsbedarf besteht insbesondere in der Entwicklung weltweit funktionierender Ecosysteme für resiliente Kommunikationsdienste in der Logistik auf Basis standardisierter LPWAN-Lösungen mit diskriminierungsfreien Roaming-Verfahren unter Einbeziehung von Lösungen in lizenzfreien Bändern. Die neue 5G-Mobilfunkgeneration sollte anforderungsgerecht Quality-of-Service-Level in der Ende-zu-Ende-Kommunikation anbieten, um den unterschiedlichen Anforderungen Intelligenter Logistikräume hinsichtlich der Konnektivität zu genügen. Logistisch motivierte Raumkategorien werden dabei die Akteure aus Logistik und Telekommunikation unterstützen, gemeinsam Kommunikationsservices zu spezifizieren, zu standardisieren und sowohl regional als auch weltweit für neue, resiliente Logistik 4.0 Geschäftsmodelle anzubieten.

4.5 Luft- und Raumfahrt

Es liegt in der Natur von Luft- und Raumfahrt, dass drahtlose Kommunikationsnetze seit Jahrzehnten für sicherheitskritische Anwendungen verwendet werden. Die Industrie sucht fortlaufend Möglichkeiten, um Treibstoff und Emissionen einzusparen sowie die Produktivität und den Durchsatz zu erhöhen. Darunter ist der weiterreichende Einsatz funkbasierter Netze in letzter Zeit in den Fokus gerückt, der Gewichtseinsparungen und Re-/Konfigurationsvereinfachungen durch Vermeidung von Kabeln und Kabelbäumen erlaubt. Weiterhin werden vermehrt Commercial Off-The-Shelf (COTS) Komponenten und Systeme sowie Standards aus anderen Industriesektoren mit idealerweise minimalen Modifikationen für die On-Board-Kommunikation sowie für die Kommunikation zwischen Boden-, Luft- und Raumfahrtentitäten verwendet. Bei der drahtgebundenen Kommunikation innerhalb von Flugzeugen wurde der Trend zu COTS bereits vollzogen durch die Verwendung von Avionics Full-Duplex Switched Ethernet (AFDX), das ein für sicherheitskritische Anwendungen modifiziertes IP/Ethernet darstellt. Für die sicherheitskritische Kommunikation mit der Flugverkehrsleitung kommen heute kurze digitale Textnachrichten zum Einsatz. Bei modern ausgestatteten Flugzeugen können diese auch über IP-Dienste, beispielsweise per Satellitenkommunikation, verschickt werden. Dabei können Latenzen von über einer Minute toleriert werden aufgrund von Abständen von über 100 km, die in entsprechend kontrollierten Lufträumen gefordert werden. Die Latenz muss somit strikt eingehalten werden, weil sonst Zusammenstöße drohen [14].

Der Trend hin zu Netzen, die generischer Natur sind und mehrere Dienste, auch sicherheitskritische, anbieten können, setzt sich weiter fort. Das derzeit erforschte Digital Aeronautical Communication System (LDACS) [15] soll im L-Band die Flugverkehrsleitung durch Positionsbestimmung zur Navigation und zur Flugüberwachung sowie durch Kommunikation unterstützen. Auch können zukünftig Netze, die nicht für sicherheitskritische Anwendungen geschaffen wurden, als Teil des Redundanzkonzepts betrachtet werden. Dazu kann neben Ka-/Ku-Band-Satelliten auch das LTE-basierte European Aviation Network (EAN) [16] gehören.

In der Raumfahrt werden vielfältige Ansätze verfolgt, u.a. Klein- und Kleinstsatelliten, Großkonstellationen (z.B. SpaceX mit 4425 LEO Satelliten) und Satelliten mit erhöhter Funktionalität und Kapazität (z.B. Tbit/s-Durchsatz). Dienstseitig kann dadurch z.B. ein weltweiter Internetzugang ermöglicht werden, wobei das Endgerät den Satellitenlink direkt oder als Backhaul-Link über Boden-Basisstationen via 4G/5G/WiFi nutzt. Satellitendienste können insbesondere Backup- und Offload-Links für resiliente Netze bereitstellen.

An Bord von Flugzeugen beginnt die Transformation hin zu drahtloser Kommunikation für sicherheitskritische Anwendungen. Bei der World Radio Conference (WRC) 2015 wurde ein 200 MHz breites Spektrum von 4,2 bis 4,4 GHz weltweit für eine Sekundärnutzung durch Sensornetze, sogenannte Wireless Avionics Intra- Communications (WAIC), im Flugzeug freigegeben [17]. Im Sinne eines Cognitive Radio müssen die Systeme den störungsfreien Betrieb des Primärnutzers, eines analogen Luft-Boden-Radars, sowie anderer gleichartiger Systeme in anderen Flugzeugen, insbesondere auf dem Flughafen, sicherstellen. Ist dies gewährleistet, können über WAIC auch sicherheitskritische Anwendungen betrieben werden.

Abseits der klassischen Passagier- und Frachtluftfahrt ergibt sich im stark wachsenden Bereich der Unmanned Aerial Vehicles (UAV) ein weiterer Markt [18]. Eine verlässliche Kommunikation ist nicht nur zur UAV-Steuerung insbesondere bei kritischen Situationen, sondern auch für viele Missionen und Anwendungsgebiete nötig, z.B. autonome Lufttaxis (wie „CityAirbus“) oder „Low Orbit“ Anwendungen (wie Drohnen für Logistikzwecke) im Smart City Kontext.

In der Luftfahrt ist schon lange das Verständnis dafür vorhanden, dass verschiedene Akteure zusammenwirken müssen, um Sicherheit zu gewährleisten. Dies sind beispielsweise Piloten und Flugverkehrsleitung, die sich gleichzeitig auch auf das Kommunikationsnetz verlassen müssen. Vorrausetzung dafür sind höchste Sicherheitsstandards bei Entwicklung und Zulassung der Netze. Flugzeuge folgen dabei dem Paradigma klassischer Zuverlässigkeit, bei dem möglichst automatisch andere Komponenten die Ausfälle kompensieren (Redundanzkonzepte). Es liegt dabei in der Natur der Luftfahrt, dass ein „Safe-State“ im Störfall oft nur durch eine Landung herbeigeführt werden kann und dabei innerhalb von Sekunden die richtigen Entscheidungen getroffen werden müssen.

Zukünftige Kommunikationsnetze in Flugzeugen können ganz neue Sicherheitskonzepte im Sinne von Resilienz ermöglichen. Wo heute noch in der Regel zwei oder sogar drei redundante Datenbusse eingesetzt werden, könnten zukünftige Flugzeuge auf ein robustes, vermaschtes Funknetz zurückgreifen. Intelligente resiliente Netze für die Luftfahrt der Zukunft sollten in der Lage sein, jedes im Flugzeug verbaute Kommunikationssystem verwenden zu können, um im Notfall zuverlässig, im Normalfall aber günstig zu kommunizieren. So könnten sogar katastrophale Ausfälle verhindert werden, die bei der Entwicklung von Flugzeugen vielleicht noch gar nicht vorhergesehen wurden. Dafür bedarf es aber zum einen der Entwicklung zuverlässiger Protokolle und Systeme, die zur Zertifizierung auch entsprechend modelliert und evaluiert werden können. Die korrekte Evaluation hoher Zuverlässigkeit und Resilienz ist wegen der Seltenheit der antizipierten Störereignisse eine eigene Herausforderung und bedarf weiterer F&E-Aktivitäten für entsprechende Methoden, z.B. für die Validierung.

4.6 Baustelle 4.0

Heutige Bauprojekte geraten derzeit häufiger in die öffentliche Kritik, da Kostenüberschreitungen und Fertigstellungsverzögerungen eintreten, die vermeidbar erscheinen. Hierbei werden aufgetretene Probleme und vorhandene Optimierungspotentiale in der Planung, Ausführung und Absicherung der Qualität der Projekte nachträglich ersichtlich, d.h. es bestehen ungenutzte, insbesondere auch technologische Potentiale, die eine effizientere und planungskonforme Realisierung von Bauprojekten erlauben würden.

Planung, Ausführung und qualitative Absicherung von komplexen Prozessfolgen auf einer Baustelle werden jedoch zukünftig möglich durch

- die Teil- oder Vollautomatisierung von mobilen Baumaschinen (Arbeitsmaschinen)
- die Vernetzung verschiedenster Maschinen, um Teil- und Gesamtprozesse abzubilden
- die interaktive Einbindung der Maschinen in die umgebende Infrastruktur
- die kontinuierliche Überwachung und Kontrolle der Teil- und Gesamtprozesse über Baustellenleitstände.

Durch die Kopplung einer zunehmend digitalisierten Planung von Bauprojekten (BIM, Bauplanung, Logistik, etc.) mit der Digitalisierung der Bauprozesse selbst und der zur Ausführung dieser Prozesse eingesetzten intelligenten Baumaschinen, werden Effizienzsteigerungen und damit Kostenreduktionen möglich, wobei durch die Einhaltung von zunehmend restriktiven Umweltgesetzgebungen (z.B. Restriktionen bzgl. Emissionen und Immissionen) gleichzeitig Beiträge zur Nachhaltigkeit der Baumaßnahmen geleistet werden.

Effizienzsteigerungen in der Baurealisierung resultieren u.a. aus einer optimierten Ablaufplanung (z.B. Vermeidung von Stillstandzeiten, Wartezeiten etc.), der prozessbezogenen und richtigen Wahl der Arbeitsmaschinen (Größe, Leistungsvermögen, Konfiguration), der Prozessoptimierung und der Nutzung möglicher Prozessintegrationen. Die Digitalisierung von Bauprozessen und Baumaschinen ermöglicht darüber hinaus Qualitätssteigerungen, da der Einfluss individueller Fehler durch ausführende Personen (z.B. Maschinenbediener) verringert wird.

Die genannten Potenziale können genutzt werden, wenn leistungsfähige und zuverlässige Technologien, Verfahren und Standards für die

- Machine-to-Infrastructure (M2I) Kommunikation
- Machine-to-Machine (M2M) Kommunikation
- Kollisionsvermeidung, d.h. durch stetige und ausreichend dynamische Kommunikation

entwickelt sowie bereit- und sichergestellt werden. Eine zentrale Rolle kommt damit den Kommunikationsnetzen mit Funkzugang zu. Heutige Technologien stoßen hierbei an Grenzen, da sie den steigenden Anforderungen (Informationsdichte/-geschwindigkeit, Verfügbarkeit, Zuverlässigkeit, Resilienz, etc.) nicht genügen.

In den sog. „Off-Road“ Anwendungen sind Infrastrukturanbindungen nicht immer gegeben oder nur bedingt zuverlässig verfügbar. Darüber hinaus gelten für Kommunikationssysteme in Baumaschinen aufgrund der harten Betriebs- und Umgebungsbedingungen besondere Anforderungen. Elektrik, Elektronik, Sensorik und Aktuatorik der eingesetzten Maschinen und Systeme können prozessbedingt mechanischen Schockbelastungen (bis zur 10-fachen Erdbeschleunigung, 10g), extremen Temperaturwechseln, hoher Feuchtigkeit, extremer Staubbelastungen, elektromagnetischen Feldern etc. ausgesetzt sein. In allen Fällen sind die Sicherheit der Maschinen und deren Funktionen seitens der Hersteller (OEM) zu gewährleisten. Nur dann

können auch die Prozesssicherheit der Baustelle und die Sicherheit der Mitarbeiter stets gewährleistet werden. Jegliche Kommunikationstechnologie, die zur Steuerung von Maschinen, von komplexen Prozessen und/oder ganzen Prozessketten eingesetzt werden soll, muss den genannten Ansprüchen höchst verlässlich genügen.

Die Gesamtheit der Anforderungen, die sich für eine sichere Realisierung einer „Baustelle 4.0“ ergeben, beinhalten die Anforderungen, die an die Systemarchitektur und deren resiliente Auslegung aus Sicht von „Industrie 4.0“ und an die Kommunikationsnetze für vernetztes Fahren unter „Automotive“ gestellt werden.

In Erweiterung dazu bestehen die spezifischen Herausforderungen „Baustelle 4.0“ in der Beherrschung

- sich verändernder harscher Umgebungsparameter und Konfigurationen (wie z.B. Gelände, Bauten und Baufortschritt, Maschinenpopulation, Maschinenpositionen)

- der Heterogenität der eingesetzten Maschinentypen (z.B. Hochbaukrane, Mobile Krane, LKWs, Radlader, Raupen, Bagger, Spezialtiefbaumaschinen) und Maschinengenerationen

- der Einschränkungen für drahtlose, funkbasierte Kommunikation (reflektierende Hindernisse)

- fehlender Standardisierungen von Schnittstellen.

Um Ausfallrisiken der Kommunikationsnetze mit Funkzugang zu beherrschen, die direkt mit der Größe und Komplexität des Bauprojektes, der Größe und Anzahl der vernetzten Maschinen, der Anzahl beteiligter Personen und der möglichen Folgen für die Umwelt korrelieren, müssen Technologien entwickelt werden, die einen Ausfall ausschließen (z.B. durch redundante Systeme) und/oder die möglichen Folgen eines Ausfalls auf ein tolerables Maß (z.B. vertretbare wirtschaftliche Folgen durch gezielten, temporären Stillstand einer Baustelle) einschränken.

Da es heute weder eine ganzheitliche Systemarchitektur „Baustelle 4.0“ noch für alle unterschiedlichen Baustellentypen geeignete und resiliente Kommunikationsnetze gibt, die den genannten Anforderungen vollumfänglich entsprechen, besteht Forschungsbedarf hinsichtlich der resilienten Auslegung von Kommunikationsnetzen (Infrastruktur) sowie Baumaschinen und eingesetzter Endgeräte.

4.7 Weitere Anwendungsfelder

Resiliente Netze mit Funkzugang sind für eine Vielzahl weiterer Anwendungsfelder von hoher Relevanz. Dabei sind die Anforderungen zum Teil ähnlich zu den bereits diskutierten Anwendungsfeldern, sind aber z.T. auch spezifisch.

Hierzu zählen u.a. folgende Bereiche:

- Energieversorgung und Umweltüberwachung
  - Intelligente Zähler (Smart Meter) und automatisches Last- und Ressourcenmanagement von Netzen (Smart Grid) können durch Funknetze realisiert werden. Es gibt dazu politische Vorgaben und gesetzliche Rahmenbedingungen auf EU- und Landesebene. Weiterhin müssen Anlagen nach dem „Erneuerbare Energie-Gesetz“ (EEG) ab einer bestimmen Größe über intelligente Messsysteme angebunden werden.
  - Anforderungen zu Datensicherheit und Datenschutz sind bei derartigen Systemen besonders wichtig und werden vom BSI spezifiziert. Das Thema Resilienz ist besonders für Smart Grid wichtig, da Ausfälle bei Steuerungssystemen von Energieanlagen erhebliche Auswirkungen auch auf andere Infrastrukturen haben können. Zur Steuerung von Energieanlagen werden zunehmend auch garantierte Latenzen wichtig.

- Wasser- und Abwasserversorgung

- Kommunikationsnetze für Behörden und Organisationen mit Sicherheitsaufgaben (BOS / Public Safety) [19, 20, 21].
  - In Deutschland gibt es ca. 650.000 Nutzer der BOS-Netze (Polizei des Bundes und der Länder, Hilfsdienste, THW etc.). Diese Netze sind derzeit auf Sprachdienste ausgerichtet aber nur in geringem Maße datenfähig und nicht breitbandfähig. Für ein Land ist ein resilientes Funkkommunikationsnetz der BOS essentiell im „Normalbetrieb“, damit die Behörden effizient ihnen Aufgaben nachgehen können. Die Wichtigkeit der resilienten Kommunikation innerhalb und zwischen den Behörden (wie z.B. Polizei) ist aber insbesondere auch im Krisenfall gegeben, z.B. bei Stromausfall, Überflutungen, Terrorattacken, Cyberangriffen etc. Diese Krisenfälle können regional begrenzt sein oder auch ganze Bundesländer oder das gesamte Land betreffen.
  - Verfügbarkeit, sowohl über die gesamte Zeit, flächendeckeckend in einem Land, außerhalb und innerhalb von Gebäuden ist eines der wichtigsten Kriterien für BOS-Netze Zunehmend wichtig sind auch entsprechende Datenraten für Breitbanddienste wie Messenger, Videoapplikationen, Bodycams etc.), Sicherheit, Abhörsicherheit. Weiterhin muss ein Netz für Großeinsätze skalierbar sein. Eine weitere Anforderung ist der Weiterbetrieb, wenn andere Infrastrukturen, wie z.B. das Stromnetz ausgefallen sind.

- Strom, Gas, Wasser, Fernwärmeversorgung und Umweltüberwachung.

4.8 Anwendungsübergreifende Anforderungen

Die Ausführungen in den Abschnitten zuvor zeigen, dass zahlreiche industrielle Anwendungen spezielle Anforderungen an die Kommunikationsnetze haben. Die Anforderung der Resilienz dieser Netze spielt dabei in unterschiedlichen Ausprägungen eine wichtige, an manchen Stellen sogar eine entscheidende Rolle. Die Forderung nach allumfassender Resilienz erfordert eine Interaktion zwischen den Resilienzkomponenten der Netze und denen der Anwendung. Folgende drei Resilienz-bezogene Anforderungskategorien lassen sich unterscheiden:

Industrie-taugliche Servicequalitäten: Für die beschriebenen Anwendungen ist nicht nur das Erreichen einer bestimmten Datenrate erforderlich. Daneben sind weitere Netzeigenschaften ganz wesentlich. Dazu zählen insbesondere die Verfügbarkeit der Netzdienste, die Wiederherstellung des Dienstes innerhalb einer tolerierbaren Zeitspanne oder sogar gänzliche Vermeidung von Informationsverlust im Fehlerfall. Weiterhin bestehen oftmals hohe Anforderungen an die Übertragungslatenz sowie deren Jitter (Latenzvariation).

Netzbetrieb: Trotz bzw. gerade wegen der hohen Anforderungen an zukünftige Kommunikationsnetze muss die einfache Nutzbarkeit eine wesentliche Eigenschaft solcher Netze sein. Dazu zählt auch das Vorhandensein von entsprechenden Nutzerschnittstellen, mittels derer der Benutzer bzw. die benutzende Applikation Netzdienste geeignet anfordern, ändern und überwachen kann. Für den Zweck der Überwachung der Netzdienste ist ein ausgeprägtes Service Level Agreement (SLA) Tooling sowohl für Nutzer als auch Provider vonnöten, welches jederzeit Informationen über den aktuellen Netzzustand bereitstellt, um im Problemfall schnell und zielgerichtet agieren zu können.

VDE-Positionspapier Resiliente Netze mit Funkzugang

Nicht-technische Anforderungen: Hierzu zählen insbesondere Skalierbarkeitsanforderungen bzgl. Ausdehnung und Knotenanzahl, langfristige Technologieverfügbarkeit und Sicherstellung eines übergreifend akzeptierten Verständnisses von grundlegenden Qualitätseigenschaften für Konnektivitätsservices. Letzteres ist entscheidend, um ohne großen Aufwand auch Ende-zu-Ende Dienstgüten über Netzübergänge verschiedener Provider hinweg realisieren zu können.

Die Erfüllung all diese Anforderungen muss dabei in geeigneter Art und Weise garantiert werden und das nicht nur unter Normalbedingungen, sondern unter den im industriellen Umfeld oft anzutreffenden widrigen Umständen oder Störeinflüssen (eine Abschnitt 5). Einige der industriellen Anwendungen sind dahingehend sehr kritisch, dass ein zeitweises Nichterfüllen der Anforderungen zu enormen Schäden führen kann (Gefährdung von Menschenleben, physikalische Beschädigung von ganzen Fertigungsanlagen, etc.). In diesen Fällen ist die Erfüllung der o.g. Anforderungen „im Mittel“ nicht ausreichend, sondern es müssen Garantien für bestimmte Parameter (minimale Bandbreiten, maximale Latenz, maximale Ausfallzeit, etc.) gegeben werden können. Dies ist ein grundlegendes Unterscheidungsmerkmal zu sogenannten „Best Effort“-Netzen.

Eine vollständige Auflistung der aus Sicht der Kommunikationsnetze mit Funkzugang zu berücksichtigenden Eigenschaften in diesen Kategorien findet sich in Abschnitt 7.5.

5 Widrige Störereignisse in Netzen

Viele Störungen in Kommunikationsnetzen lösen sich mit der Zeit selbständig wieder auf, da sie rein temporärer Natur sind. Daher sind hier heutzutage in der Regel keine speziellen Netzfähigkeiten zur Regeneration oder Selbstheilung erforderlich. Zu solchen Störungen zählen beispielweise überhöhtes Verkehrsaufkommen in allen Netzsegmenten oder Einbrüche der Signalstärke (Schwundeffekte) im Funkzugang, die durch Abschattungen hervorgerufen werden. Die hohen Anforderungen der zukünftigen industriellen Anwendungen an die Sicherheit, Verfügbarkeit, Zuverlässigkeit und Echtzeitfähigkeit der Netze erfordern jedoch, dass diese Störungen rechtzeitig erkannt und im Sinne der erforderlichen Dienstgüte ausgeregelt werden können.

Beim Design von resilienten Netzen muss grundlegend unterschieden werden, ob die Störereignisse innerhalb des Netzes auftreten oder von außerhalb die Netzeigenschaften beeinflussen.

Störereignisse, die innerhalb des Kommunikationsnetzes auftreten sind bspw.

- Kapazitätsengpässe aufgrund zu hohen Datenverkehrs (Netzlasterhöhungen)
- menschliche Fehler, wie Bedienfehler oder fehlerhafte Konfigurationen
- Softwarefehler (z.B. Designfehler, Laufzeitfehler, logische Fehler)
- Hardwarefehler (z.B. defekte Netzknoten und Leitungen)
- ungenügende Netzmanagement- und Network-Slicing-Fähigkeiten bei der Zuordnung von Funk- und Netzressourcen bei konkurrierenden Kommunikationsdiensten unterschiedlicher Prioritäten.

Störereignisse, die von außerhalb auf das Netz wirken sind bspw.

- Naturkatastrophen (Hochwasser, Erdbeben, Hurrikane, Tornados etc.), Explosionen und Brände
- Terroranschläge und gezielte Angriffe auf die physikalische Infrastruktur
- Elektromagnetische Interferenzen (EMI) auf Stecker, Leitungen und Funkgeräte
- prozessbedingte erschwerte Bedingungen für die Komponenten (z.B. durch mechanische Schockbelastungen, extreme Temperaturänderungen, Feuchtigkeit, Staub etc.)
- gezielte Jamming-Attacken zur Störung der Funkkommunikation
- gezielte Denial-of Service (DoS) und Distributed Denial-of-Service (DDoS) Attacken
- gezielte IT-Angriffe, z.B. Viren, Botnets, Malware, Phishing etc.

- unbeabsichtigte Kommunikationsstörung in lizenzfreien Frequenzbändern durch benachbarte Funknetze
- Kommunikationsstörungen durch bewegte Objekte und dynamisch wechselnde Umgebungsbedingungen
- Stromausfälle.

Eine ganz wesentliche Klassifikation von Störereignissen, die bei der Auslegung von resilienten Netzen wichtig ist, erfolgt jedoch durch die Unterscheidung aus Sicht des Kommunikationsnetzes zwischen bekannten, unbekannten, vorhersehbaren und unvorhersehbaren Störereignissen. Zudem muss unterschieden werden, ob sie zufällig, systematisch, sporadisch, periodisch, unbewusst oder bewusst auftreten.

Bekannte Störungen sind im Vorfeld definierbar und demzufolge dem Kommunikationsnetz grundsätzlich bekannt, d.h. es weiß, dass solche Fehler auftreten können, welche Ursachen sie haben und wie das Netz im Falle des Eintretens darauf zu reagieren hat. Sie verursachen somit Störereignisse, von denen im Vorfeld bekannt ist, dass sie während des Netzbetriebs irgendwann und mit definierbaren Intensitäten bzw. Eigenschaften auftreten können und welche Schäden und Folgen sie verursachen können. Exemplarisch hierfür sind temporäre lokale Netzlasterhöhungen zu nennen. Man kann somit für die Kompensation oder Minderung der Störungen im Netz auf ein definiertes Vorwissen zurückgreifen.

Unbekannte Störungen sind im Vorfeld bei der Entwicklung eines Kommunikationsnetzes nicht genau definierbar, was ebenfalls für die möglichen daraus resultierenden Schäden und Folgen gilt. Sie beschreiben Störungen, deren Auftrittszeitpunkte und -muster, Intensitäten, die davon betroffenen Netzteile und -funktionen und auch die resultierenden Schäden im Vorfeld nicht bekannt sind. Hierzu zählen u.a. gezielte Jamming-Attacken durch einfache Breitbandstörer bis hin zu intelligenten Funk-Jammern, die bspw. Funkkommunikationsszenarien und -teilnehmer analysieren und zu gezielten Zeitpunkten die Kommunikation präzise stören und dabei ihre Bandbreite, Sendeleistung, Sendedauer und Funkausrichtungen flexibel einstellen können, um im Idealfall unentdeckt zu bleiben. Dies ermöglicht exemplarisch die gezielte Störung von Trainingssequenzen, die für die Synchronisation von Funksender und -empfänger wichtig ist, wodurch die Kommunikation verhindert wird, ohne dass dauerhafte Störsignale ausgesendet werden müssen, was die Ortung des Störsenders erheblich erschwert.

Vorhersehbare Störungen können sowohl bekannte als auch unbekannte Störungen sein. Je nachdem, über welche Monitoring- und Prädiktionsfähigkeiten ein Kommunikationsnetz verfügt, desto früher können potentielle Netzstörungen und Verschlechterungen von Servicequalitäten identifiziert und abgeschätzt werden und in der Folge eine Netzoptimierung vorgenommen werden. Hierzu zählen bspw. Abschattungseffekte, fehlerhafte Netzkomponenten.

Unvorhersehbare Störereignisse können ebenfalls bekannte wie auch unbekannte Störungen sein, die jedoch meist erst nach Eintreten erkannt werden können und in der Regel abrupt auftreten, wie bspw. gezielte Anschläge auf die physikalische Infrastruktur oder IT-Hackerangriffe.

Im weiteren Verlauf soll die Summe an möglichen Störeinflüssen aufgrund ihrer widrigen Charaktereigenschaften auch als „widrige Umstände bzw. Störereignisse“ bezeichnet werden. Widrige Störereignisse sind dabei technisch, menschlich oder natürlich verursachte Einflüsse bis hin zu Katastrophen, die in Kommunikationsnetzen Veränderungsprozesse hervorrufen, welche anwendungsseitig gravierende Folgen und Schäden verursachen können, wenn sie nicht rechtzeitig erkannt oder abgeschätzt und im Sinne der Anwendungen ausgeregelt werden können.

Eine generelle Kategorisierung widriger Umstände ist kaum möglich. Als Beispiel sei ein (Elbe-)Hochwasser angenommen. Dieses Ereignis ist bekannt und dass es auftreten kann, ist vorhersehbar, aber der Zeitpunkt und das Ausmaß des Auftretens sind zufällig. Das Ereignis wird unbewusst ausgelöst und wirkt in der Region des Hochwassers von außen auf das lokale Kommunikationssystem ein. Ein anderes Beispiel sind konkurrierende Kommunikationsdienste. Sie können zufällig oder systematisch, innerhalb oder außerhalb eines Kommunikationssystems, bewusst oder unbewusst auftreten. So sind für jeden Fall alle oben genannten Kategorien zu betrachten.

Trotz der vielleicht aus heutiger Sicht teilweise geringen Wahrscheinlichkeiten für das Eintreten von gravierenden widrigen Störereignissen treten diese jedoch in der Realität faktisch auf. Unter Berücksichtigung der zunehmenden Cyberkriminalität rücken insbesondere die Attacken auf industrielle und öffentliche Netze und die Schäden, die damit verursacht werden können, mehr und mehr in den Fokus der Betrachtungen.

Die Summe der möglichen Störeinflüsse und insbesondere die Tatsache, dass unvorhersehbare Störereignisse mit enormen Schadenspotentialen auftreten können, birgt große Herausforderungen beim Design von Netzen mit Funkzugang und erfordert die Erforschung und Entwicklung von Resilienzstrategien, um die in den Abschnitten 4.1 bis 4.8 aufgezeigten Anforderungen der industriellen und öffentlichen Anwendungsfälle an zukünftige Kommunikationsnetze umfänglich erfüllen zu können.

6 Resilienz für Kommunikationsnetze: Definition und Einordnung

Prof. Dr. Erik Hollnagel ist für seine Untersuchungen im Bereich der Resilienzforschung bekannt und er definiert resiliente Systeme allgemein wie folgt [22]:

> *"A system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions."*

Die Herausforderung besteht nun darin, die aufgezeigten erforderlichen Eigenschaften von resilienten Systemen für die relevanten zukünftigen Anwendungsfelder (siehe Abschnitt 4) sowie die Erkenntnisse aus den bisherigen Untersuchungen von Forschern auf diesem Gebiet, wie Prof. Dr. Hollnagel oder David D. Woods [23], auf die heutigen und insbesondere zukünftigen Kommunikationsnetze mit Funkzugang zu übertragen, eine Strategie und Methoden für resiliente Netze in Abhängigkeit der möglichen widrigen Störeinflüsse (siehe Abschnitt 5) zu entwickeln und diese im Sinne der zukünftigen Anwendungen und deren Anforderungen (siehe Abschnitt 4) zu optimieren.

Resilienz im Kontext von Kommunikationsnetzen mit Funkzugang wird wie folgt definiert:

Ein resilientes Kommunikationsnetz mit Funkzugang garantiert definierte Netzdienste auch unter widrigen Umständen durch Anpassbarkeit seiner Funktionalität vor, während und auch nach auftretenden Störereignissen und zeichnet sich dadurch aus, dass es in Summe folgende Fähigkeiten besitzt:

a) Sensitivität: Es ist sensitiv gegenüber bekannten und vorher-/absehbaren, aber vor allem auch unbekannten und unvorhersehbaren/unerwarteten internen wie auch externen widrigen Störereignissen. Das Kommunikationsnetz besitzt demnach die Fähigkeit zum kontinuierlichen Netz-Monitoring, wodurch es seinen Netzzustand stets kennt.

b) Antizipationsfähigkeit: Es kann einen Großteil der Störereignisse antizipieren, wodurch diese bereits im Vorfeld verhindert, kompensiert oder zumindest deren Auswirkung gemildert werden können (Fail Safe Modus bzw. Ersatzzustand).

c) Widerstandsfähigkeit: Es kann auf unvorhersehbare Störereignisse elastisch/adaptiv und rasch bzw. in angemessener Zeit reagieren und Maßnahmen zur Wahrung der erforderlichen QoS und zum Schutz des Netzes einleiten.

d) Regenerationsfähigkeit: Es kann sich im Falle von Netzausfällen und/oder Schädigungen infolge von Störereignissen nach (a) rasch bzw. in angemessener Zeit erholen bzw. selbst heilen und die ursprünglichen Netzfunktionen vollständig oder zumindest in Teilen wiederherstellen.

e) Lernfähigkeit: Es hat kognitive Fähigkeiten, um die gesammelten Erfahrungen in die Optimierung der Fähigkeiten (a) bis (d) einfließen zu lassen.

Folgen von widrigen Störereignissen sind die Verletzung, der durch eine Spezifikation eines Kommunikationsnetzes angenommenen Grenzwerte relevanter Einflussgrößen (siehe [24]). Das können anwendungsbezogene Einflussgrößen (z. B. Sendezeitintervall), umgebungsbezogene Einflussgrößen (z. B. bewegliche Hindernisse) oder geräte- und systembezogene Einflussgrößen (z. B. Sendeleistung) sein. Für die Ableitung von Maßnahmen gegen widrige Umstände ist die Festlegung eines Betrachtungsraumes erforderlich, da sich Einflüsse unterschiedlich auf eine logische Verbindung, ein Kommunikationsgerät oder ein Kommunikationssystem auswirken. Widrige Umstände stellen eine Bedrohung dar, die zum Ausfall des Kommunikationsnetzes führen können, wenn sie zu lange auf das System wirken. Ein resilientes Kommunikationsnetz reagiert auf solche widrigen Umstände. Die Tatsache das widrige Umstände auftreten können ist in den meisten Fällen vorhersehbar, allerdings nicht der Zeitpunkt und das Ausmaß. Das resiliente Kommunikationsnetz führt unter den aktuell gegebenen Bedingungen Maßnahmen durch und kann somit einen Ausfall verhindern.

Basis hierfür ist die Entwicklung eines ganzheitlichen Resilienzkonzepts für Kommunikationsnetze mit Funkzugang (siehe Abbildung 3), welches die Abbildung der Fähigkeiten (a) bis (e) und die Minimierung von Ausfallwahrscheinlichkeiten ressourceneffizient ermöglicht.

Resilience-by-Design: das besondere an resilienten Systemen ist, dass sie ihre Funktionsfähigkeit –zumindest bis zu einem gewissen Grad– auch unter unvorhergesehenen Umständen erhalten können. Dazu ist es notwendig, dass diese Systeme ihren aktuellen Zustand möglichst genau kennen. Das gilt sowohl für das Wissen über den individuellen Zustand der einzelnen Netzknoten als auch für das Wissen über einen geeigneten Nachbarschaftsbereich. Diese Informationen spannen quasi einen Lösungsraum auf, innerhalb dessen das System eine Lösung zum Erhalt seiner Funktionsfähigkeit finden sollte. Zur Auswahl einer geeigneten Lösung muss das System die Wechselwirkungen der individuellen Parameter kennen und berücksichtigen können. Dazu müssen diese Wechselwirkungen beim Design der Systeme entsprechend modelliert werden. So ist Redundanz ein bekanntes Mittel, um Zuverlässigkeit bereitzustellen. Redundanz kann aber auch helfen, Angriffe abzuwehren oder zumindest abzuschwächen.

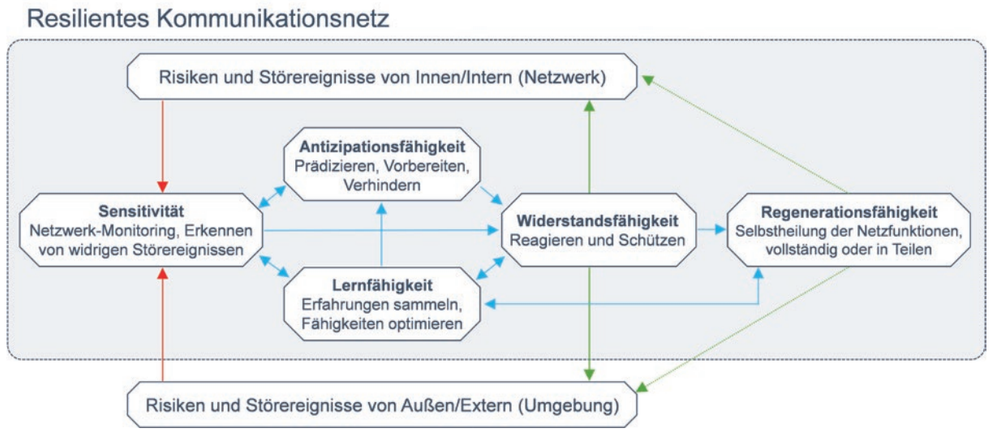

Abbildung 3: Gesamtheitliches Resilienzkonzept „Resilience-by-Design": Fähigkeiten resilienter Kommunikationsnetze mit Funkzugang

Die erforderlichen Netzdienste werden dabei aus Sicht der relevanten Anwendungen (siehe Abschnitt 4) definiert, sie sehen in der Regel in ihren Anforderungen Abstufungen vor und erlauben in Fällen funktionaler Sicherheit (Functional Safety) in der Regel auch die Option, mit einer vordefinierten Vorwarnzeit in einen sicheren Rückfallmodus umzuschalten. Auch das aktuell verfolgte Konzept des „Network Slicing“ [27] enthält eine implizite Definition eines Netzdienstes, der dem Anwender garantiert werden muss.

Ein Wesensmerkmal resilienter Netze ist es dafür zu sorgen, dass störende Ereignisse nicht zum Verlust der Funktionsfähigkeit führen. Deshalb ist die Definition der Funktionsfähigkeit dahingehend zu erweitern, dass eine Abstufung erfolgen kann. Neben den derzeitig verwendeten Zuständen „Funktionsfähig“ (Optimaler Betrieb) und „Nicht-Funktionsfähig“ sind zusätzliche Zustände beispielsweise „Störstufe x“ festzulegen. Anzahl und Kenngrößen zur Bewertung dieser Störstufen sind anwendungsorientiert zu definieren. Diese Spezifikationen stellen den Handlungsspielraum für die Erforschung von Methoden und Algorithmen resilienter Netze dar.

Abbildung 4 veranschaulicht die grundlegende Funktionsweise von resilienten Netzen mit Funkzugang, die über die Fähigkeiten (a) bis (e) verfügen.

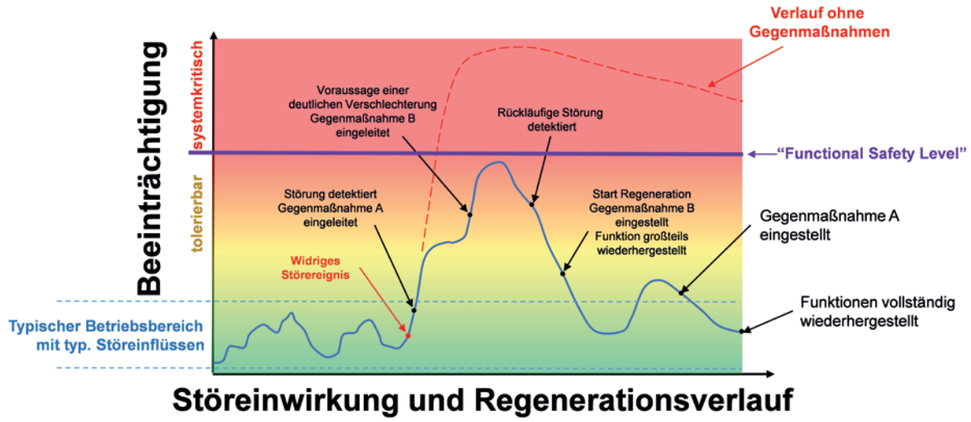

Abbildung 4: Grundlegende Funktionsweise von resilienten Kommunikationsnetzen mit unterschiedlichen Störstufen

Eine wesentliche Eigenschaft zukünftiger industrieller Netze ist, dass die über sie kommunizierenden Anwendungen unterschiedlichen Anforderungen an Zeitverhalten und Zuverlässigkeit unterliegen. Hinzu kommt, dass sich diese unterschiedlichen Prioritäten während des Betriebes verschieben können. Diesem Umstand müssen die Methoden resilienter Netze Rechnung tragen.

Potenzielle Methoden zur Erreichung der Resilienz in Netzen mit Funkzugang:

- Partielle Redundanz (adaptive, teilweise gemeinsame Nutzung mehrerer Übertragungswege)
- Partielle Diversität (adaptive, teilweise gemeinsame Nutzung verschiedener Frequenzbänder)
- Aktivierung temporär/spatial autonomer Funktionen (z.B. selbständiger Kanalzugriff im Falle eines Scheduler-Ausfalls)

- Temporäre und spatiale Funktionsrelokation zum Erhalt der kritischen Steuerfunktionen
- Aktivierung temporär verringerter zugesicherter Werte für Zeit- und Zuverlässigkeitskenngrößen (verminderter Produktionsausstoß)
- Vorhersagen durch Beobachtung der Netzkommunikation zur rechtzeitigen Aktivierung von Maßnahmen
- Schnittstelle zwischen Kommunikationsnetz und Anwendung zur Spezifikation von Abstufungen der Funktionsfähigkeit
- Wiederherstellung der Funktionsfähigkeit oder Steuerung des Übergangs in eine bessere Stufe der Funktionsfähigkeit (Notfallplan)
- Optimierung der Entscheidungsfindung bei der Auswahl einer Methode durch Lernen kritischer Zustände und des Erfolges angewendeter Algorithmen

Eine Grundvoraussetzung für resiliente Netze ist die Herstellung einer „Self-Awareness“ durch permanente Beobachtung ihres Zustandes, möglichst durch quantifizierbare Eigenschaften. Die Begriffe QoS und QoE (Quality of Experience) werden häufig verwendet, um die Güte von Datenkommunikation zu beschreiben. QoS beschreibt dabei verschiedene, zumeist einfach messbare technische Dienstgüteparameter, wie Latenz, Paketverlust und Durchsatz. Diese können pro Punkt-zu-Punkt-Verbindung, Netzsegment oder Ende-zu-Ende gemessen werden. Sie sind beispielsweise im ITU-T Standard E.800 [25] definiert, auf den auch der IEC Standard 60050-192 [26] zur Definition der Begrifflichkeiten zu Zuverlässigkeit und Verfügbarkeit verweist. QoE hingegen beschreibt die wahrgenommene Güte der Anwendung, die über die Datenkommunikation realisiert wird. Diese ist zwar meist eng verwandt mit der durch QoS bestimmten technischen Dienstgüteparametern, doch ist der Zusammenhang oft komplex und hängt bei Anwendungen wie Audio und Video auch von der subjektiven Wahrnehmung des Betrachters ab. Für viele sicherheitskritische Anwendungen muss der Zusammenhang zwischen QoS und QoE noch erforscht werden. Da bei QoE-Eigenschaften insbesondere die dem Nutzer nicht sichtbare Netzredundanz eine Rolle spielt, muss durch aktives Redundanzmanagement dafür gesorgt werden, dass bei Störungen nur die Redundanz, aber nicht die Service-Qualität leidet. Die Informationen des Redundanzmanagements können für die Auswertung der „Self-Awareness“ sowie zur Indikation von möglichen zukünftigen Service-Störungen der Anwendung signalisiert werden. Dazu gehören bspw. das Fernsteuern von Robotern und Fahrzeugen, aber auch Anwendungen ohne menschliche Beteiligung wie Regelschleifen für Fahrzeug-Platoons. Resiliente Netze der Zukunft müssen somit entweder aus punktuell verfügbaren QoS-Messungen auf die QoE der Anwendung schließen und diese dafür sehr genau kennen oder Ende-zu-Ende-QoE-Messungen vornehmen, bei denen ggf. auch der Mensch als Nutzer Rückmeldung geben muss.

7 Technologische Aspekte: Herausforderungen und Ansätze

7.1 Blickwinkel: Netzinfrastrukturentwicklung

Die nachfolgende Abbildung zeigt eine vereinfachte Darstellung der Netzinfrastruktur, wie sie sich in den nächsten Jahren auf Basis der laufenden 5G-Aktivitäten voraussichtlich entwickeln wird (siehe NGMN [27] und 5G PPP [28]), ergänzt um Elemente für die Berücksichtigung von lokalen und Ad-Hoc Netze Funkzugangsnetzen.

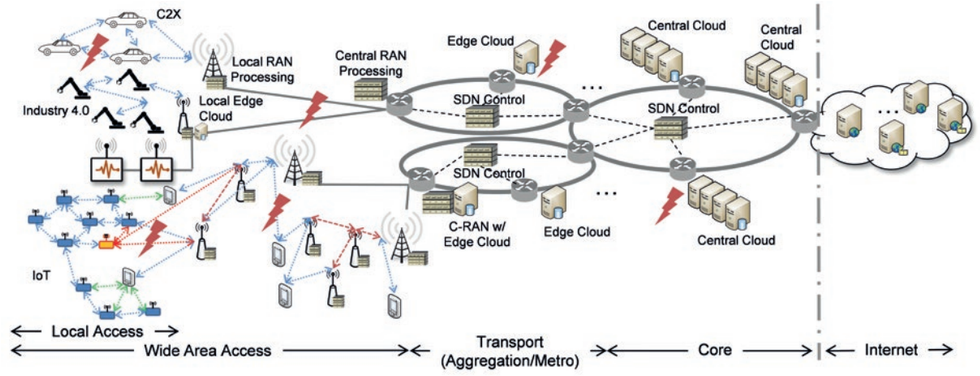

Abbildung 5: 5G-basierte Netzarchitektur[1] mit Anbindungsmöglichkeit von lokalen und Ad-Hoc Netze Funkzugangsnetzen

Die zukünftige Netzinfrastruktur wird neben den eigentlichen Kommunikationsverbindungen auch verstärkt Computingleistungen und Speicherkapazität bieten, wodurch mehr Intelligenz in das Netz verlagert werden kann. Die Umsetzung erfolgt dabei durch technische Konzepte wie Software Defined Radio (SDR), Software Defined Networking (SDN) und Network Function Virtualisation (NFV) [29], die zu einer stärkeren Flexibilisierung und Programmierbarkeit der Netzkomponenten mit Hilfe von größtenteils virtualisierbaren (vor allem im Kernnetz) und damit je nach Anwendungsfall flexibel platzierbaren Netzfunktionen (NFs) führen [30]. Ein Beispiel hierfür ist die Orchestrierung von Processing- und Applikationsfunktionen möglichst nahe an Antennenstandorten unter Verwendung von sogenannten Edge Clouds [33], um hierdurch z.B. niedrige Servicelatenzen gewährleisten zu können (auch in Verbindung mit Cloud RANs (Radio Access Network), die zur Zentralisierung bestimmter funkzugangsbezogener NFs dienen [28]). Edge Clouds und Cloud RANs können Teil des Zugangsnetzes sein, aber auch Teil einer lokalen, netzbetreiberunabhängigen Infrastruktur (z.B. in der Industrie), die wiederum in ein größeres Weitverkehrsnetz integriert werden kann.

Die zukünftige Netzinfrastruktur unterstützt insbesondere das Konzept der sogenannten Network Slices, d.h. von dedizierten logischen Netzen, die mittels spezifischer NFs die für bestimmte Geschäfts- bzw. Privatkundensegmente geforderten Dienste- und Netzfunktionalitäten auf einer gemeinsamen Infrastruktur realisieren (s.a. [31]). Network Slices sind besonders interessant, um die Anforderungen vertikaler Industriezweige und anderer Anwendungsfelder (wie bspw. eGovernment, eHealth etc.), die sich stark

1 Das Architekturbild enthält aus Vereinfachungsgründen nur eine einzige Infrastrukturdomäne. Slices, z.B. für kontinentale oder globale Anwendungen, können sich über mehrere Domänen erstrecken, erfordern daher eine Art hierarchisches Modell für das Zusammenspiel zwischen dem Slice-Anbieter und den Infrastrukturdomäneneignern [28].

von denen des klassischen Telekommunikationsmarktes unterscheiden können [32], zeitnah, flexibel und ressourcenschonend auf der Netzinfrastruktur umzusetzen. Ende-zu-Ende Slices (von Endgerät zu Endgerät) können sowohl regional/global unter Einbeziehung von einer oder mehreren Netzbetreiberdomänen und dem Internet aufgesetzt sein, aber auch rein lokal funktionieren – zum Beispiel auf Basis von Ad-Hoc Netze-Netzen. Zudem können sie auch etablierte, domänenspezifische Kommunikationstechnologien mit einbeziehen (z.B. Industrial Ethernet-Lösungen in der Industrie). Typische Anwendungsbeispiele hierfür sind die Umsetzung einer verteilten Steuerungsarchitektur in der Fertigungsautomatisierung oder die lokale Vernetzung von Landwirtschafts- und Baumaschinen.

Die in Abschnitt 6 genannten Resilienz-Aspekte wie Sensitivität, Antizipationsfähigkeit, Widerstandsfähigkeit, Regenerationsfähigkeit und Lernfähigkeit müssen auch in der zukünftigen Netzinfrastruktur stärkere Berücksichtigung finden. Resilienz-Aspekte sind meistens eng mit der Physik verbunden, betreffen mit Nutzung der SDR/SDN/NFV-Konzepte aber in zunehmendem Maße auch die rein software-basierten Layer und deren Abbildung auf die Infrastruktur (z.B. durch Verwendung von Hypervisors) [29].

In Abbildung 5 sind die kritischsten Punkte hervorgehoben (siehe rote Pfeile), betreffend u.a.:

- Ausfallsicherheit von Funkverbindungen (unter Berücksichtigung der Netzsicht, des Übertragungsmediums und möglichen Störern, gewollt oder ungewollt) und Gewährleistung von Dienstgütevorgaben, vor allem für mobile Endgeräte

- Gesicherte Anbindung von Funkknoten an das Transportnetz

- Ausfallsicherheit von Netzfunktionen speziell in Zusammenhang mit Cloudifizierung (Berücksichtigung von Wiederherstellungszeiten, u.a.)

- Sichere Trennung von Netzfunktionen und Datenströmen unterschiedlicher Slices bei Verwendung einer gemeinsamen Infrastruktur (Transport, Verarbeitung, Speicherung)

- Angreifbarkeit von Infrastrukturknoten aufgrund verstärkten Software-Einsatzes

- Prädiktives Netzmanagement.

Nähere Einzelheiten zu den sich ergebenden Herausforderungen in den einzelnen Netzpartitionen, d.h. Funkzugangs-, Transport- und Kernnetz bzw. Cloud, und zu möglichen Maßnahmen, deren Umsetzung den Weg zu resilienten Netzen ebnen kann, sind in den nachfolgenden Abschnitten beschrieben.

7.2 Blickwinkel: Transportnetze

Das Transportnetz kann man grob in das nationale Kernnetz (Core in Abb. 5), regionale Metronetze (Aggregation/Metro in Abb. 5) und die lokalen Zugangsnetze (Access in Abb. 5) unterteilen. Kern- und Metronetze basieren auf optischer Übertragung über Einmoden-Glasfasern, wobei bis zu 100 Wellenlängen parallel genutzt werden (Dense Wavelength-Division Multiplex, DWDM). Beide sind heute schon mithilfe einer sogenannten Ringarchitektur teilredundant ausgelegt, die es ermöglicht, dass ein Netzausfall an einer Stelle kurzfristig überbrückt werden kann. Wenn ein Signal z.B. in Uhrzeigerrichtung von

einem Knoten zu einem anderen gesendet wird, und die Verbindung plötzlich unterbrochen wird, kann das Signal den Empfänger auch in entgegengesetzter Uhrzeigerrichtung erreichen.

Kern- und Metronetze sind für solche Fälle mit einer Basissensitivität ausgestattet, um z.B. einen Faserbruch schnell zu erkennen. Sie weisen durch aktive Elemente in den Netzknoten, z.B. sog. optischer Add-/Drop Multiplexer (OADM), und die grundlegende Ringarchitektur Basisfunktionen zur Widerstandsfähigkeit auf, d.h. man kann beispielsweise die Signallaufrichtung umkehren und so die Betriebsfähigkeit wiederherstellen. Die Überwachung des Netzes und die eventuelle Einleitung von Gegenmaßnahmen sind die Aufgabe des sog. Operation, Admininstration and Maintenance (OAM) Systems, auf das zukünftig immer mehr Aufgaben zukommen. Im Zuge der stetig ansteigenden Ausnutzung der vorhandenen Glasfaserkapazität ist anzunehmen, dass die Kapazitätsgrenzen der vorhandenen Infrastruktur in Spitzenlastzeiten immer häufiger erreicht bzw. überschritten werden. Solche Ereignisse sind vorhersagbar, weil sie sich in Tageszyklen wiederholen. Das zukünftige OAM sollte demnach eine stärkere Antizipationsfähigkeit aufweisen, d.h. mögliche Störungen durch Überlast im Vorfeld erkennen und beseitigen können. Anhand der Kenntnis der vorhandenen Infrastruktur und der aktuellen Verkehrslasten sollte das OAM System eine bessere Regenerationsfähigkeit aufweisen, d.h. jederzeit in der Lage sein, zeitlich variierende Verkehrslasten zu erkennen, sie vorausschauend umzuleiten und den im Fall einer Überlastsituationen auftretenden zeitweiligen Netzausfall auf diese Weise zu vermeiden. Das OAM muss dafür auch über eine zunehmende Lernfähigkeit verfügen, d.h. Methoden besitzen, um den Istzustand der Infrastruktur zu erkennen und auf möglichen Änderungen durch Inbetriebnahme neuer bzw. Abschaltung alter Infrastrukturen sofort reagieren zu können. Dafür müssen lastkritischen Pfade identifiziert und ihre Verkehrslast gezielt überwacht werden können, um im Überlastfall an diesen Stellen schnell reagieren zu können. Langfristiger muss der Netzbetreiber an solchen Brennpunkten durch zusätzliche Infrastruktur für eine nachhaltige Entlastung sorgen.

Insgesamt sind OAM Systeme und die erforderliche Ringarchitektur im Kern- und Metronetz bereits weit verbreitet, d.h. hier sind Redundanzen als Basis für Resilienz netzseitig bereits vorgesehen, weshalb in aktuellen Netzen große Störungen in kompletten Netzsegmenten mit verheerenden Folgen nur noch vergleichsweise selten auftreten. Das ist jedoch im Zugangsnetz u.a. aufgrund der hier vielfach verwendeten Baumstruktur (siehe Abb. 5 im sog. „Access“ Bereich Mitte links) noch nicht der Fall. Typische Zugangsnetz-Technologien sind passive optische Netzwerke (PON) und aktives Ethernet. Beide realisieren eine Baumstruktur.

5G wird derzeit als ein konvergentes Netz entworfen, d.h. als holistischer Entwurf bei dem drahtgebundene und drahtlose Netze ineinandergreifen und sich wechselseitig unterstützen.[2] Ein wesentlicher Grund für die zunehmende Heterogenität der Zugangsnetze ist die hierdurch mögliche weitere Kosteneinsparung. Nicht nur die Funktechnologie ist heterogen und nutzt beispielsweise verschiedene Frequenzen, sondern auch das dahinterliegende feste Zugangsnetz kann verschiedene Medien verwenden. Für mehr Resilienz im Zugangsnetz müssen zunächst in der physikalischen Infrastruktur Möglichkeiten geschaffen werden, um die bisherige Baumstruktur zu überwinden und das Netz auf diese Weise ebenfalls redundant auszulegen. Eine naheliegende Architektur ist wiederum ein Ring, was aber bedeutet, dass jeder Zugangspunkt, vom nächstliegenden Metroknoten aus gesehen, auf zwei voneinander unabhängigen Wegen erreichbar sein muss.

2 z.B. lässt sich das sog. Slicing im Festnetz sehr einfach mithilfe der o.g. logischen Metro Ethernet Profile umsetzen. Jedoch ist es bislang noch nicht möglich, den Slices bestimmte, sich zeitlich ändernde Bandbreiten zuzuweisen. Hierfür werden derzeit Ansätze vorgeschlagen, die auf einer gemeinsamen Steuerschicht für Festnetz und Mobilfunk beruhen.

In privaten Zugangsnetzen, z.B. in einer Industriehalle, würde man ein resilientes Netz immer redundant auslegen. So ist es bereits in der privaten IT Glasfaserinfrastruktur üblich, Ringnetze zu verlegen, wie sie z.B. auch für Feuermelder genutzt werden. Im Hinblick auf steigende Resilienzanforderungen für zukünftigen 5G-Dienste ist es zunehmend wichtig, auch die heutigen Netzausbaukonzepte im öffentlichen Zugangsnetz kritisch zu hinterfragen und das Potential einer konvergenten IT-, Telekom- und Kabelinfrastruktur im Zugangsbereich umfassend auszuloten, da an vielen Orten verschiedene Medien bereits heute redundant ausgebaut sind. In einem heterogenen Zugangsnetz könnte die gewünschte Resilienz durch eine variable Konfiguration der Zugangs- und Aggregationsknoten gewährleistet werden. Hierzu müssen zukünftig stärker auch die im Kern- und Metronetz bereits üblichen OAM Methoden zur Resilienz auf das OAM im Zugangsnetz ausgedehnt werden. Man muss dabei allerdings beachten, dass die Verkehrslast im Zugangsnetz noch sehr viel dynamischer ist als im Metro- und Kernnetz, wo die Verkehrslasten aggregiert und „ausgemittelt“ sind, so dass es in der Regel ausreicht, vergleichsweise inflexible optische Technologien einsetzen, um z.B. neue Wellenlängen zu benutzen oder die Signalrichtung zu ändern. Im Zugangsnetz werden vorzugsweise elektronische Technologien eingesetzt, um die Ressourcen im Netz an die einzelnen Nutzer zuzuweisen. Erst dadurch wird das sog. statistische Multiplexing realisiert, welches die Mittelung der aggregierten Rate in Richtung höherer Aggregationsschichten bewirkt.

In den öffentlichen Zugangsnetzen wäre Resilienz technisch prinzipiell dadurch möglich, indem man die in vielen Hausanschlüssen, zumindest in den Städten, mehrfach vorhandene Netzanbindung, mittels DSL, Glasfaser, Koaxialkabel und Mobilfunk, zukünftig parallel nutzt und dadurch für die benötigte Redundanz sorgt. Beide Infrastrukturen müssen unabhängig voneinander an das Metronetz angeschlossen werden. Der Verkehr im Zugangsnetz sollte über mehrere Medien aggregiert und dem Nutzer über einen gebündelten Anschluss übergeben werden. Die zu entwickelnde Lösung muss auch der hohen Dynamik und dem statistischen Multiplex Rechnung tragen. Eine derartige Anschlussverdopplung würde jedoch auch zu höheren Kosten führen. Auch wenn die erzielbaren Datenraten durch Kanalaggregation steigen, was ein Wettbewerbsvorteil sein kann, sind die höheren Kosten sicherlich nicht immer für normale Endnutzer-Anwendungen gerechtfertigt. Für Industriekunden könnte dieser einfache Ansatz jedoch bereits ein wichtiger Schritt hin zu besserer Resilienz sein. Parallel dazu sollte sich die Bereitschaft der Netzbetreiber zum sog. Infrastructure Sharing erhöhen. Beispielsweise stellen Industrie- und Fahrzeugkommunikation neue Anforderungen an die Resilienz der öffentlichen Netze, die auch als neue Schlüsselmerkmale bekannt sind (Key Performance Indicators, KPIs). Man könnte den techno-ökonomischen Nutzen quantifizieren, der durch Resilienz der Netze entsteht, und die Schlussfolgerungen an die Netzbetreiber und die Politik herantragen.

Zur Resilienz gehören auch grundlegende Arbeiten zu flexibleren Routing- und Aggregationsprotokollen. Zukünftig werden universelle, standardisierte Lösungen benötigt, welche in der Breite verfügbar und kostengünstig einsetzbar sind. Redundante Verbindungen, wie zuvor beschrieben, schützen z.B. nur bedingt vor Überlast durch zu hohen Verkehr. Eine gewisse Entlastung ist durch Kanalbündelung möglich. In der Theorie existieren seit vielen Jahren Traffic Engineering Methoden, um sicherzustellen, dass die über eine Verbindung geleiteten Datenströme in der Summe nicht die Leitungskapazität übersteigen (z.B. Flow Control). In der Praxis hat man es auf der Ebene der Netzverbindungen schon lange mit Virtualisierung auf allen möglichen Netzschichten zu tun. Logische Topologien können auf verschiedenste Arten entstehen. Auf der Schicht 3 (Internet Protocol, IP) kommen oft globale virtuelle private Netze (VPN) zum Einsatz, die die Verkehrsströme und ihre Routen maßgeblich beeinflussen. Auch das für die Routenwahl in heutigen Netzen zuständige IP-Protokoll bekommt oftmals von den darunterliegenden Schichten eine virtuelle Topologie „vorgegaukelt“. Diese kann sich durch Umkonfiguration dynamisch

ändern, beispielsweise durch Ändern von Wellenlängen in optischen Netzen oder auch mittels der eher lokal eingesetzten VPN auf Schicht 2.

Dank Software Defined Networking (SDN), wie es derzeit in den Netzen implementiert wird, bekommt man die Möglichkeit bei zentralen Controllern einen Überblick über den Zustand des Netzes zu bekommen und gezielt Maßnahmen, sowohl bei Überlast, als auch bei physischer Beschädigung, zu ergreifen. Bei Zweitem ist es wichtig, schichtübergreifend konsistent zu sein, wenn eine Ersatzroute aufgebaut wird. In den heutigen Netzen beginnt das IP-Protokoll neue Routen zu suchen, während gleichzeitig und dazu asynchron tiefere Schichten versuchen eine neue logische Topologie zu erzeugen, die den Ausfall gegenüber darüber liegenden Schichten wieder verbergen.

Während es bei physikalischer Beschädigung ausreicht, den Zustand „Leitung ist vorhanden“ zu beobachten, ist es bei Überlast komplizierter. Heutige Netze erfassen bestenfalls im Abstand vieler Sekunden oder Minuten die kumulierte Datenmenge über eine Leitung bzw. ihre Auslastung. Dies ist noch weit entfernt von dem Wunsch, für jede einzelne Anwendung Auskunft zu haben, welche Datenmenge sie aktuell erzeugt, um abzuschätzen, welche Datenströme ggf. durch den Controller umgeleitet werden sollen, wenn Überlast droht. Prädiktive Algorithmen erfordern ggf. hohe zeitliche Auflösung in einem gewissen Beobachtungszeitfenster, um drohende Überlast frühzeitig zu erkennen. Dabei müssen die Daten über die Auslastung der Leitungen zum Controller gesendet werden, was wiederum Datenverkehr erzeugt. Hier gilt es Methoden zu erforschen, um lokal zumindest Zwischenergebnisse aus den Messergebnissen zu generieren. Ein weiteres in heutigen Netzen ungelöstes Problem ist die konsistente Änderung von Routen. Entscheidet ein Controller, dass Datenströme aufgrund zu hoher Auslastung eine andere Route wählen sollen, so muss diese Entscheidung synchron an allen betroffenen Routern umgesetzt werden. Dies ist heute mangels Zeitsynchronisation nicht möglich.

Aufgrund von Network Function Virtualization (NFV), auch als Cloudifizierung bezeichnet und in Abschnitt 7.4 näher beschrieben, können schlagartig enorme Änderungen bei den Datenströmen auftreten, wenn ein Server mit hohem Datendurchsatz plötzlich an einer anderen Stelle im Netz auftaucht. Dies geschieht häufig aufgrund von Resilienz-Mechanismen in der Cloud. Diese müssen zukünftig enger mit den Mechanismen des darunterliegenden Transportnetzes verzahnt werden und die Entscheidungen müssen unter Beachtung aller verfügbaren Informationen aus allen Ebenen, von der Datenleitung bis hoch zur Applikation (Funktion) getroffen werden.

Mit SDN wird zukünftig zwar die Möglichkeit geschaffen Verkehrsströme umzuleiten, allerdings kommen beim Zugriff auf die Leitung meist einfachste First-in-First-Out-Buffer zum Einsatz. Auch wenn Priorisierungen bereits möglich sind, so ist die Zahl der Auswahlkriterien dafür meist gering. Insbesondere darf man dem Endbenutzer in der Regel nicht die Entscheidung über die Priorität seiner Daten überlassen, denn dann ist Missbrauch zu befürchten. Die in Flugzeugen verwendeten AFDX Netze (siehe Abschnitt 4.5) basieren auf IP und Ethernet und erlauben an jedem Switch jeden einzelnen Verkehrsstrom zu beobachten und ihm nur eine definierte Bandbreite zuzuweisen. Derzeit laufen Standardisierungsbemühungen, um sowohl Ethernet als auch das darüber laufende IP Protokoll zuverlässiger zu machen. Beide Protokolle waren ursprünglich nur für Best-Effort-Dienste gedacht. Für Ethernet wird eine als „Time-Sensitive Networking“ (TSN) bezeichnete Erweiterung entwickelt, die darüber liegende Protokolle mit „Deterministic Networking“ ausnutzen. Als Grundvoraussetzung dafür unterstützen die Protokolle die Zeitsynchronisation aller Netzknoten.

Resilienz und Security: Das Netz ist das Rückgrat aller betrachteten Anwendungen und muss deshalb Resilienz in besonderem Masse bereitstellen. Um überhaupt auf erwartete und unerwartete Fehler und Abweichungen vom geplanten Netzverhalten reagieren zu können, muss das Netz zu jedem Zeitpunkt seinen Zustand möglichst genau kennen. Dazu muss das Netz sich selbst überwachen und die dabei erhobenen Sensordaten zwischen den Netzknoten austauschen und evaluieren. Aus IT-Sicherheitssicht müssen deshalb folgende Aspekte betrachtet und sichergestellt werden: für die Sensordaten, die den Netzzustand beschreiben, müssen Integrität und Authentizität sichergestellt werden können. Dies bedeutet, dass darüber hinaus Fehlerzustände erkannt und korrekt klassifiziert werden können, um geeignete Wiederherstellungsmaßnahmen einleiten zu können. Die Herausforderung liegt hier in der korrekten Bestimmung der Fehlerursachen. So lange ausschließlich Angriffe von externen Quellen betrachtet werden müssen, können Datenintegrität und -authentizität mit Hilfe von digitalen Unterschriften gewährleistet werden. Hier gilt es allerdings offene Fragen zum Thema Effizienz zu beantworten. Dazu sind Betrachtungen notwendig, die sowohl die Latenz von kryptografischen Berechnungen angehen als auch den erzeugten Datenoverhead bei diesen Berechnungen. Tatsächlich extrem herausfordernd wird die Sicherstellung korrekter Informationen zum Netzzustand, wenn Insider-Angriffe betrachtet werden müssen. Letzteres wird mit an Sicherheit grenzender Wahrscheinlichkeit notwendig sein, da drahtlose Netzknoten von potentiellen Angreifern direkt kontaktiert und kompromittiert werden können. Das heißt letzten Endes, dass sich diese Knoten autonom gegen alle möglichen Angriffe schützen müssen, was angesichts der beschränkten Ressourcen dieser Geräte eine unmögliche Aufgabe ist. Nachdem also ein Knoten kompromittiert wurde, kann dieser Sensordaten zum Netzzustand mit korrekter, digitaler Signatur in das Netz senden und so den tatsächlichen Netzzustand verschleiern. Die Frage der Erkennung kompromittierter Knoten wird also eine der zentralen Fragen für die Bereitstellung resilienter Netze sein. Denkbare Ansätze sind das Monitoren aller Nachbarknoten um Fehlverhalten entdecken zu können, die statistische Bewertung der Sensordaten zur Erkennung von Manipulationen durch Insider und/oder die periodische Durchführung von Codeattestation. Allerdings sind diese Maßnahmen noch keineswegs etabliert und bedürfen also einer weiteren Untersuchung. Hinzukommen Fragen der Skalierbarkeit der Ansätze, also ihres Einflusses auf die Netzverfügbarkeit damit nicht evtl. die Durchführung von Codeattestation gerade den Leistungseinbruch, auf den das Netz reagieren müsste, verursacht hat. Denkbar wäre auch die mehrschichtige Authentifizierung eines Knotens, um zweifelhafte Identitäten zu erkennen bzw. die Manipulation zu verhindern. Ebenso müssen geeignete Gegenmaßnahmen ergriffen werden, um die kompromittierten Knoten aus dem Netz ausschließen zu können. Letzteres kann durch Verteilung neuer Schlüssel an die nicht kompromittierten Knoten oder durch Verteilung von Blacklists geschehen, wobei auch hier Fragen der Skalierbarkeit betrachtet werden müssen. Die Anzahl der nicht kompromittierten Knoten bestimmt die Fähigkeit des Netzes zu „Graceful Degradation“ bzw. zur Wiederherstellung der Funktionalität, dabei ist insbesondere der Anteil der nicht kompromittierten Knoten an der Gesamtzahl der Knoten in einem bestimmten Gebiet ausschlaggebend. Letztere Relation wird insbesondere durch den Konnektivitätsgraphen des Netzes bzw. der Teilnetze bestimmt.

7.3 Blickwinkel: Funkzugang

Immer mehr Personen, Geräte und Maschinen werden drahtlos miteinander vernetzt. Die Funkschnittstelle ermöglicht dabei den Zugang zum Netz und damit zu den Diensten, die dort bereitgestellt werden. Der Funknetzzugang stellt somit den Eintritt in die vernetzte Welt und deren Mehrwert durch Informati-

onsaustausch und dadurch -zugewinn dar. Die resiliente Auslegung des Funkzugangs ist folglich von zentraler Bedeutung für die Schaffung von resilienten Kommunikationsnetzen. Alle zuvor für das Transportnetz genannten Herausforderungen bezüglich Zuverlässigkeit gelten auch hier. Hinzu kommen weitere, die für das Funkzugangsnetz charakteristisch sind.

Drahtlose Verbindungen können aus „natürlichen“ Ursachen zeitweilig ausfallen oder z.B. von einem Angreifer bewusst gestört werden (Jamming). Wenn der Angreifer undifferenziert stört, ist eine Erkennung des Jamming relativ einfach und lokal möglich. Bei einem selektiven Jammer, der z.B. nur ausgewählte Pakete stört, ist eine kooperative Erkennung notwendig, damit der „Fehler“ überhaupt erkannt werden kann. Im nächsten Schritt muss eine Lokalisierung des Jammers durchgeführt werden, um geeignete Heilungsmaßnahmen (wie Entfernen des Jammers) durchführen zu können. Obwohl dies aktuell ungelöste Probleme sind, ist die Sicherstellung unverfälschter Sensordaten, die den Netzzustand korrekt widerspiegeln, ungleich komplexer. Hierbei sei noch zu erwähnen, dass ein absichtliches Jamming in der Regel einen Gesetzesverstoß darstellt, der mit empfindlichen Strafen sanktioniert wird. Schon heute ist sicherheitskritische Kommunikation, beispielsweise der Behördenfunk und die Leitstelle der Bahn, latent dieser Gefahr ausgesetzt, ohne dass sie tatsächlich zu bekanntgewordenen Störungen führt.

In der Forschung werden aktuell verschiedene technologische Ansätze forciert, um die Zuverlässigkeit und die Verfügbarkeit des Funkzugangs zu verbessern. Zur Realisierung von resilienten Kommunikationsnetzen mit Funkzugang müssen diese Technologien hinterfragt und weiterentwickelt werden. Dabei ist die Auslegung der Netze und der zugrundeliegenden Netzarchitektur in Hinblick auf die erforderlichen anwendungs- und dienstspezifischen Resilienzeigenschaften von besonderer Bedeutung.

Konkret müssen die jeweiligen Technologien bzgl. der Nutzung zur Detektion von widrigen Ereignissen und ihrer Eigenschaften zu elastischen Gegenmaßnahmen unter Berücksichtigung des technischen und zeitlichen Aufwands sowie der erreichbaren Wirkung untersucht werden. Je nach Anwendung oder Dienst können Aspekte wie Latenz, Verfügbarkeit, Datendurchsatz oder Fehlerrate unterschiedlich priorisiert werden. Es gilt die Technologien anhand dieser Kriterien zu bewerten.

Folgende Technologien sind dabei im Kontext resilienter drahtloser Netze in Hinblick auf die in Abschnitt 6 definierten erforderlichen Netzfähigkeiten erweitert zu untersuchen:

- Spektrums- und Koexistenzanalyse sowie -management bei Operation in lizenzfreien Frequenzbändern: u.a. zur Detektion und ggf. Klassifikation von Funkstörern/Jammern, Störmustern, sich verändernden Umgebungsbedingungen sowie zur Überwachung des Netzzustandes; Ermittlung aktueller Freiheitsgrade. Für Bänder, die einer Anwendung vorbehalten sind, z. B. V2X im 5,9 GHz Band oder Kommunikation innerhalb von Flugzeugen bei 4,2 GHz, aber kein bestimmtes Funkprotokoll vorschreiben, ergeben sich weitere Herausforderungen. Diese Konstellation ist bei modernen Systemen derzeit noch selten und entsprechend wenig erforscht und erprobt. Lösungen für technologieunabhängige Koexistenzmechanismen müssen gefunden werden, die gleichzeitig die Einhaltung der Dienstgüte, insbesondere bezüglich der Latenz, garantieren. Einen möglichen Lösungsansatz bieten sog. Cross-Technology-Communication Verfahren [39]. Sie ermöglichen eine schmalbandige Datenübertragung zwischen Funksystemen unterschiedlicher Technologien ohne zusätzliche Funkschnittstellen oder Infrastruktur zu benötigen.

- Multi-Konnektivität mit heterogenen Funkzugangstechnologien (Multi-RAT): Redundanz im Funkzugang durch parallele Nutzung verschiedener Funkzugangstechnologien (z.B. 5G NR, LTE, 802.11) und somit dynamische Anpassung der Datenübertragung. Hohe Wirkungsmöglichkeit der Anpassung bzgl. Datendurchsatz bei verfügbaren Technologien.

- Multi-Band-Kommunikation: Redundanz im Funkzugang durch Nutzung von Frequenz-Diversität bspw. LTE-Frequenzbandumschaltung, Parallelbetrieb, technisch aufwendiger, geht über verschiedene Layer, hohe Wirkung

- Multi-Link- und Coordinated-Multi-Point-Kommunikation: Redundanz im Funkzugang durch parallele/simultane Nutzung von mehreren Links von einem mobilen Teilnehmer zu mehreren Zugangspunkten zur Erhöhung der Übertragungsrobustheit (Verringerung von Fehlerraten bzw. Verfügbarkeitsausfällen) gegenüber Störungen im Funkspektrum. Fähigkeit zur dynamischen Anpassung der erforderlichen Anzahl von Übertragungs-Links als auch der genutzten Übertragungsbandbreiten und Modulations- & Codierungsschemata in Abhängigkeit von zeitveränderlichen Übertragungsbedingungen. Erfordert netzseitige Koordination und Prädiktionsfähigkeiten. Resiliente Auslegung betrifft mehrere Netzentitäten und -Layer und ist für latenzkritische Dienste zu optimieren.

- Mehrantennensysteme und Massive MIMO: mehrere Sende- und Empfangsantennen, Diversität (Space-Time Codes) und/oder Multiplexing, Datenratenerhöhung und/oder Fehlerrate bzw. Outage, PHY-Layer, erlaubt schnellere Reaktion, Anpassung, Latenz vs. Qualität

- Selbstorganisierender Funkzugang mit dynamischem Radioressourcenmanagement

- Überdimensionierung von Funk-Infrastruktur

- AI RAN: Künstliche Intelligenz zur Optimierung und situationsbedingten Adaptierung des Funkzugangs infolge unbekannter und unerwarteter Störereignisse im Funkkanal

- Control Plane: In der Vergangenheit wurde bei diversen Standards großer Aufwand betrieben, um Latenzen zu minimieren und Paketverluste möglichst vollständig zu eliminieren. Der Fokus lag dabei sinnigerweise auf den Nutzdaten (User Plane), weil die dort verwendeten Protokolle, insbesondere der Medienzugriff, die Leistung maßgeblich bestimmen. Steuermechanismen (Control Plane) machen in der Regel nur einen vergleichsweise geringen Anteil des Datenverkehrs aus und wurden somit oft nur nachrangig betrachtet. Strebt man aber Verfügbarkeiten im Bereich 99,999 % an, so muss auch sichergestellt werden, dass seltene Steuerereignisse zuverlässig und schnell ablaufen. Bei Funknetzen beinhaltet das insbesondere:
  - Netzsuche und Synchronisation, deren Dauer und Erfolgswahrscheinlichkeit davon abhängen, wie häufig die dafür benötigten Informationen (z.B. Beacons) versendet werden. Einige Protokolle beherrschen aktive Verfahren, bei denen Knoten Pakete aussenden und die entsprechenden Informationen anfragen.
  - Initialer Netzzugriff, der meist über nicht-deterministischen Zufallszugriff realisiert wird. Hierbei ist entscheidend, wie viele Knoten um den Zugriff konkurrieren und wie häufig der Zufallszugriff möglich ist.
  - Handover, wobei für hochverfügbare Netze unbedingt durchgehende Datenverbindung gewährleistet sein muss (Make-before-break). Hierarchische und hybride Netze, bei denen eine Anbindung über mehrere Verbindungen die Regel statt Ausnahme ist, können hier deutliche Abhilfe schaffen.
  - Energiesparmechanismen und zugehörige Aufwachprozeduren resultieren oft in Verzögerungen ähnlich denen der Netzsuche und Synchronisation

Beim Entwurf und der Leistungsbewertung drahtloser resilienter Netze der Zukunft müssen unbedingt alle benötigten Steuermechanismen mit betrachtet werden. Hierbei muss zunächst für jede Anwendung und jedes Szenario abgeschätzt werden, wie häufig sie aktiv werden. Anschließend müssen sie gemäß ihrem Gesamtbeitrag zur Ende-zu-Ende Dienstgüte optimiert werden, so dass sie nicht zum Leistungsengpass werden. Die Lösung für jeden Einzelfall liegt irgendwo zwischen den zwei Extremen eines verteilt gesteuerten Netzes, bei dem alle Knoten gleichberechtigt sind und ständig um Funkressourcen konkurrieren und einem statischen, zentral koordinierten Netz (oder sogar mehreren Netzen), bei dem für jeden potentiell vorhandenen Knoten Ressourcen strikt reserviert sind.

In resilienten Netzen kann der Funkzugang über zellulare Mobilfunknetze und über lokale Netze (z.B. WLAN, Ad-Hoc Netze Netze) realisiert werden. Der untere linke Teil der Referenzarchitektur in Abbildung 5 zeigt verschiedene Funkzugangsoptionen. Neben dem klassischen Ansatz, wo ein Teilnehmer immer genau von einem Zugangspunkt versorgt wird oder mit gleichartigen Teilnehmern ein Ad-Hoc Netz bildet, ist auch Mehrfachkonnektivität dargestellt. Redundante Funkverbindungen können auf verschiedenste Arten realisiert werden. Charakteristisch ist dabei, an welcher Stelle im Protokollstapel die Daten dupliziert und mehrfach versendet werden bzw. wo sie wieder zusammengeführt werden. Neben reinem Duplizieren können auch Kodierverfahren, beispielsweise Network Coding eingesetzt werden, um unterschiedliche Daten pro Strom zu versenden. So sind beispielsweise in der Abbildung Mobilfunkteilnehmer zu sehen, die von mehreren Stationen versorgt werden. Im Extremfall (im Sinne des tiefstmöglichen Punktes im Protokollstapel) passiert das auf analoger Ebene, wo beide Stationen exakt das gleiche elektromagnetische Signal aussenden. Denkbar ist aber auch, dass die Stationen auf verschiedenen Frequenzbändern arbeiten oder sogar verschiedenen Technologiestandards angehören (z. B. LTE und WLAN). Diese können demselben Betreiber gehören, wodurch der Verkehr irgendwo zwischen Access und Core getrennt und zusammengeführt wird. Sie können aber auch völlig unabhängig voneinander sein und der Datenstrom könnte (fast) auf der gesamten Strecke getrennte Pfade nehmen.

Während der zellulare Mobilfunk auf lizensierte Frequenzbänder zurückgreifen kann, nutzen die lokalen Netze zumeist lizenzfreie Frequenzbänder (z.B. 433 MHz, 868 MHz, 2.4 GHz, 5 GHz, 60 GHz). Die lizenzfreien Frequenzbänder können bei Einhaltung gewisser regulatorischer Vorgaben kostenfrei genutzt werden, jedoch ohne ein exklusives Nutzungsrecht. Zur Vermeidung von wechselseitigen Störungen (sog. Koexistenzprobleme), sollten benachbarte Funknetze hinsichtlich ihrer Nutzung der Funkressourcen möglichst koordiniert werden. Um dies zuverlässig zu erreichen, können neue Funknetze oder Störer in dem Frequenzband z.B. mithilfe von virtuellen oder realen Sensing-Knoten erkannt werden. Bei virtuellen Sensing Knoten wird die Sensing-Funktionalität in die schon existierenden Knoten als Element der Control- oder der Management-Plane eingefügt.

Redundante Anbindung auf verschiedenen Ebenen ist für die jeweilige Realisierungsoption gut erforscht und im Markt etabliert. Die Forschungsfrage, wie man aus all diesen Optionen adaptiv und im Sinne bestmöglicher Ende-zu-Ende-Dienstgüte die beste auswählt, ist noch offen. Der Fokus sollte abgelenkt werden von einer reinen Bandbreitenerhöhung durch Nutzung mehrerer Verbindungen und stattdessen gerichtet werden auf Erhöhung der Zuverlässigkeit, was insbesondere die Frage aufwirft, welche Daten über welche Verbindung verschickt werden sollen. Neben technischen Fragen müssen aufgrund verschiedener Zuständigkeiten und Betreibermodelle auch organisatorische und rechtliche Fragen geklärt werden. Letzteres umfasst insbesondere die Haftung im Störfall.

7.4 Blickwinkel: Cloud

Im Sinne einer ganzheitlichen Optimierung des Gesamtsystems beschränken sich die Anforderungen hinsichtlich einer hohen Resilienz in vielen Anwendungsdomänen nicht nur auf die reine Kommunikationsinfrastruktur (insb. Funkzugangsnetz und Transportnetz), sondern erfordern zunehmend auch die Berücksichtigung von (mehrstufigen) Cloud-Infrastrukturen mit Computing- und Storage-Ressourcen sowie der eigentlichen Anwendungen. Beide Aspekte können zudem zu einer deutlichen Verbesserung der Resilienz eines Gesamtsystems beitragen.

Klassischerweise wurden in vielen Domänen Anwendungen zumeist lokal ausgeführt – sei es im Fahrzeug, in der Fabrik oder in der Luftfahrt. Dank des Erfolgs des Cloud-Computing in der IT-Welt dringen entsprechende Ansätze aber nun verstärkt auch in diese Anwendungsbereiche mit hinein. Aufgrund oftmals hoher Anforderungen an die Echtzeitfähigkeit von Prozessen (bspw. in der Fabrikautomatisierung) sowie aufgrund von Sicherheits- und Datenschutzgründen (z.B. im Medizinbereich) ist eine Verlagerung von Anwendungen in klassische Cloud-Data-Center oftmals aber nicht möglich oder gewünscht. Neue Konzepte wie Edge Computing wirken diesen Herausforderungen entgegen, indem flexibel nutzbare Rechen- und Speicherressourcen in die Nähe der Anwendungen gebracht werden. Dadurch lässt sich gleichzeitig auch die Ausfallsicherheit und Verfügbarkeit des Systems erhöhen, da selbst bei Beeinträchtigungen des Backbone-Netzes zumindest der in der Edge Cloud laufende Teil einer Anwendung aufrechterhalten werden kann. Prinzipiell gehen die Entwicklungen aber sogar weiter hin zu Multi-Tier-Cloud-Architekturen, mit gebündelten Rechen- und Speicher-Ressourcen auf verschiedenen Ebenen. So sind im Bereich der Industrie zukünftig beispielsweise Mini-Clouds auf Shopfloor-Ebene vorstellbar, die dynamisch mit fabrikweiten Factory-Clouds, unternehmensweiten Enterprise-Clouds und schließlich den klassischen, global verteilten Datenzentren interagieren. Optimierte Anwendungen können dann dynamisch und flexibel – abhängig von der Verfügbarkeit und Leistungsfähigkeit der zugrundeliegenden Vernetzungs-, Rechen- und Speicher-Infrastruktur – auf die verschiedenen Cloud-Ebenen verteilt werden. Fällt eine Ebene aus oder ist beeinträchtigt (bspw. aufgrund von Problemen mit der Vernetzungsinfrastruktur oder aufgrund eines Systemabsturzes), wird der dort laufende Anwendungsteil einfach auf eine andere Cloud-Ebene verschoben, idealerweise ohne dass die Gesamtanwendung dadurch beeinträchtigt wird. Darüber hinaus sind auch redundante Ansätze vorstellbar, wobei beispielsweise eine Anwendungskomponente gleichzeitig auf mehreren unterschiedlichen Clouds bzw. Cloud-Instanzen ausgeführt wird bzw. Daten redundant abgespeichert werden, wobei u.a. Ansätze wie eine Netzwerkcodierung sinnvoll zum Einsatz kommen können. Die unterschiedlichen Clouds bzw. Cloud-Instanzen sind dann idealerweise auch noch über disjunkte Verbindungspfade angeschlossen, wodurch sich die Resilienz ebenfalls deutlich verbessern lässt.

Bei der eigentlichen Anwendung besteht zudem in vielen Domänen noch enormes Potenzial in Hinblick auf eine gemeinsame Optimierung der Anwendung selbst sowie der zugrundeliegenden Vernetzungsinfrastruktur. So wird die bestmögliche Gesamtperformance vermutlich nicht erreicht, in dem man auf Anwendungsseite eine perfekte Vernetzungsinfrastruktur annimmt und diese so weit wie möglich optimiert, sondern wenn man die unvermeidbaren Einschränkungen in praktischen Systemen hinsichtlich Restfehlerwahrscheinlichkeiten, Ausfallwahrscheinlichkeiten, usw. auch in der Anwendungsentwicklung selbst bereits geeignet berücksichtigt. Ein konkretes Beispiel hierfür aus der Industrie sind fehlertolerante Regelungsalgorithmen, die zu einem gewissen Grad Totzeiten, Jitter, Übertragungsfehler u.ä. tolerieren können.

Im Bereich virtualisierter Komponenten und Virtualisierungssysteme, wie sie beim Cloud-Computing zum Einsatz kommen, ist für ein resilientes Verhalten die sichere Erkennung von Störfällen durch geeignete Sensoren nötig. Diese sollten in der Lage sein, vor allem Kernfunktionen (wie z.B. Hypervisor und wesentliche Kommunikationskanäle sowie das Systemmanagement), aber auch Systemfunktionen (Service) zu überwachen und möglichst frühzeitig deren Ausfall oder Beeinträchtigung melden bzw. vorhersagen können. Bei Störfällen müssen zunächst die Funktionen erhalten bleiben, die eine Erkennung und geeignete Reaktionen auf einen Störfall ermöglichen, etwa im Bereich der Hardware (Plattformen, physikalische Netzkomponenten), des System- und Sicherheitsmanagements, sowie der Controllerfunktionen (SDN) für die Verwaltung der Verkehrsverbindungen (z.B. Fernwartung und Administration). Solche Komponenten/Funktionen könnten redundant und lokal verteilt (im Falle von Katastrophen oder Unfällen) ausgelegt, bzw. durch spezielle Schutzmaßnahmen (IT-Sicherheit, Schutz vor physikalischem Zugriff) und Härtung vor Angriffen geschützt werden.

In einem verteilten, Cloud-basierten Service müssen Maßnahmen bereitgestellt werden, um gefährdete Systemkomponenten und Ressourcen im Bedarfsfalle wiederherstellen zu können. Neben virtualisierten Komponenten (die z.B. aus den ‚Images' oder Snapshots erzeugt werden können) ist auch der Systemzustand (Daten, Backups) wesentlich, um möglichst nahtlos und ohne Verlust relevanter Daten neue Aufsetzpunkte für den gesamten Service zu schaffen. Dies gilt für spezielle Formen von Angriffen auf IT-Ebene (Sabotage, Ransomware, DoS etc.) genauso wie für natürliche Ursachen (Erdbeben, Gewitter, Hochwasser etc.) und für zufällige oder provozierte Einwirkungen (Unfälle, zerstörende Angriffe). In einigen (Standard-) Fällen kann eine Schutzwirkung gegen bestimmte, vorhersagbare oder erwartete Bedrohungen auch präventiv erzielt werden, etwa kann ein durch Hochwasser, Stromausfall (Notstrombetrieb), Gewitter, o.ä. Ursachen bedrohtes Daten-/ Rechenzentrum lokal verlagert oder erweitert werden („Elasticity"). Dies ist im Wesentlichen eine Frage der Ressourcen-Bereitstellung und -Reservierung, organisatorisch wie wirtschaftlich.

Automatisierung der Managementaufgaben ist ein wesentlicher Bestandteil der Störfallerkennung sowie des Krisen- und Präventionsmanagements. Manuelle Eingriffe sind wo möglich auf ein Mindestmaß zu beschränken, unter Umständen aber nicht komplett verzichtbar.

7.5 Anforderungsübersicht

Wie bereits unter Abschnitt 4.8 erläutert, zeigt eine Analyse der unterschiedlichen Anwendungsfelder, dass zukünftige Kommunikationsnetze die unterschiedlichsten Anforderungen erfüllen müssen. Tabelle 1 fasst domänenspezifisch wichtige Parameter, die in allen Betriebssituationen zu berücksichtigen sind, zusammen.

Die Schwierigkeit liegt dabei darin, diese Anforderungen in resilienter Art und Weise zu erfüllen. Das bedeutet, dass die in jeder einzelnen Zeile genannten Anforderungen (z.B. Latenz, Jitter, max. tolerierbare Ausfallzeit, etc.) nicht nur unter Normalbedingungen zu erfüllen sind, sondern eben auch in kritischen Situationen und schwierigen Umfeldern. Und wenn aufgrund eines unvorhersehbaren Ergebnisses (s. Abschnitt 5) eine dieser Anforderungen nur noch eingeschränkt erfüllt werden kann, muss das Kommunikationssystem selbstständig dafür sorgen, dass innerhalb kürzester Zeit wieder ein Zustand erreicht wird, in dem die Anforderungen entsprechend erfüllt sind.

Beispielsweise müssen die aufgeführten Latenzanforderungen auch dann erfüllt werden, wenn eine Störung in der Entstehung bzw. schon aufgetreten ist. Dafür sind insbesondere die in Abschnitt 6 aufgeführten Fähigkeiten resilienter Kommunikationsnetze entscheidend: Sensitivität sorgt dafür, z.B. durch kontinuierliche Testmessungen frühzeitig zu erkennen, wenn die Einhaltung der maximalen Latenzzeiten gefährdet ist; Antizipationsfähigkeit ermöglicht ein frühzeitiges Gegensteuern, wie z.B. die Vorbereitung und ggfs. Nutzung alternativer Kommunikationswege mit stabileren Latenzeigenschaften; Widerstandsfähigkeit stellt sicher, dass es Mechanismen für die Latenzreduzierung gibt, die auch in unvorhergesehenen Situationen entsprechend wirksam sind; Regenerationsfähigkeit gewährleistet nach einem Schadensfall, der nicht abgewendet werden konnte, dass unmittelbar nach der Wiederherstellung des Kommunikationsnetzes auch die Latenzvorgaben wieder nachhaltig erfüllt werden und dies auch entsprechend verifiziert wird; Lernfähigkeit stellt sicher, dass Verletzungshäufigkeit und -dauer des Latenzverhaltens langfristig deutlich reduziert werden können.

Category	Requirement	Consolidated requirements from verticals - Siemens view	Smart City	Smart Mobility / Rail	Smart Process Automation	Smart Manufacturing	Smart Energy			Smart Building
							Low Voltage	Medium Voltage	High Voltage	
Indstry-grade Service Quality	Realtime capabilty - Latency	1 ms (local) 5 ms (long distance)	-	1ms (local) 10 ms (long distance)	20ms (local) 1s (long distance)	1ms (local) 20ms (long distance)	-	25ms	5ms (long distance)	100ms
	Realtime capabilty - Jitter	1us (local)	-	20ms (long distance)	20ms	1us (local)	-	25ms	1ms	-
	Range (distance between communication neighbors, local ... long distance):	0,1 m ... 200 km	10 km	1 m ... 10 km	0,1m ... 10 km	0,1 m ... 100 m	10 km	20 km	200 km	100m
	Bandwidth	kbps ... 10Gbps	kbps (sensors) ... Mbps (video supervision) ... 10 Gbps (data centers)	10 Mbps ... 1 Gbps	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)	1 kbps per subscriber	5 Mbps per secondary substation	1Gbps along power lines	100 kbit/s (automaton stream) ... 100 Mbps (remote access, video supervision)
	Time period of information loss during failures	none (seamless failover)	1s	100 ms	100 ms	none (seamless failover)	minutes	25ms	none (seamless failover)	100 ms
	Availability/coverage	ubiquituous	city-level	ubiquituous	Industrial plant areas	Industrial plant areas	ubiquituous	ubiquituous	ubiquituous	city-level
	Reliability (minimum uptime per year [%])	99,9999%	99,9%	99,9999%	99,9999%	99,9999%	98%	99,9%	99,9999%	99,9%
	Mobility	500km/h	100km/h	500km/h	50km/h	50km/h	5km/h	-	-	5km/h
	Outdoor terminal location accuracy	0,1 m	1 m	0,1 m	0,1 m	0,1 m	10 m	10 m	-	0,1 m
	Mutli-tenant support	yes								
	Resilience	yes								
Operation and maintenance	Non-standard operating conditions	- battery powered devices with >10years lifetime - harsh environments (weather, vibrations, heat, dust, hazardous gases, etc.)								
	Ease of use	- Communication services approach - Plug and play device (sensor, actuator, controller) integration								
	SLA Tooling	Service Level Agreement (SLA) monitoring and management tools for provider and consumer								
	Service deployment time (time between service request and service realization)	hours								
	private 5G infrastructures	yes	-	yes	yes	yes	-	optional	yes	optional
Non-technical	Scalability: Number of devices per km^2	10^5	10^5	10^4	10^5 (high density of devices)	10^5 (high density of devices)	10^4	10^3	10^3	10^5
	Globally harmonized definition of Service Qualities	yes	-	yes	yes (for long distance)	yes (for long distance)	-	yes	yes	-
	Technology availability	>30 years								
	Globally simplified certification of ICT components	Yes								
Assured Guarantees		mandatory	relaxed	mandatory	mandatory	mandatory	relaxed	mandatory	mandatory	relaxed

Abbila Tabelle 1: Anforderungen industrieller Domänen an resiliente Kommunikationsnetze (nach [34])

8 Anhang

8.1 Referenzen

[1] Newman, Resilient Cities: Responding to Peak Oil and Climate Change, Washington, 2009, .S.6

[2] IEC, „Internet of Things: Wireless Sensor Networks“, White Paper
http://www.iec.ch/whitepaper/internetofthings/

[3] Plattform Industrie 4.0, „Netzkommunikation für Industrie 4.0“, Diskussionspapier, April 2016

[4] „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze“, Bundesgesetzblatt Jahrgang 2015 Teil I Nr.54, ausgegeben zu Bonn am 28. Dezember 2015

[5] Thuemmler C, “The Case for Health 4.0”, in Thuemmler C, Bai C (2017) (Hrsg) Health 4.0, Springer

[6] Regulation (EU) 2015/2120 Of the European Parliament and the Council of 25 November 2015

[7] Body of European Regulators for Electronic Communications [BEREC] (2016), BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127

[8] Bundesministerium für Bildung und Forschung (2015) Förderkonzept Medizininformatik, http://www.gesundheitsforschung-bmbf.de/_media/BMBF_040_Medizininformatik_BARRIEREFREI.pdf

[9] Bender BG, Chrystyn H, Bernard Vrijens (2017), „Smart Pharmaceuticals“, in Thuemmler C, Bai C (2017) Health 4.0 (Editors), Springer Verlag

[10] Schlenk CT (2015) Mobilfunk 5G, Die Ferngesteuerte Welt, Handelsblatt, 09.04.2015, http://www.handelsblatt.com/technik/hannovermesse/mobilfunk-5g-die-ferngesteuerte-welt/11615084.html

[11] 5G Infrastructure Association (2015), 5G PPP White Paper on eHealth vertical sector, https://5g-ppp.eu/wp-content/uploads/2016/02/5G-PPP-White-Paper-on-eHealth-Vertical-Sector.pdf

[12] WWRF (2016) Outlook No 17, A New Generation of e-Health Systems Powered by 5G, http://www.wwrf.ch/files/wwrf/content/files/publications/outlook/Outlook17.pdf

[13] Thuemmler C, Paulin A, Jell T, Keow Lim A (2017) Information Technology – Next Generation: The Impact of 5G on the Evolution of Health and Care Services, ITNG 2017, conference proceedings, Springer (accepted)

[14] Global Operational Data Link Document (GOLD), Second Edition, April 2013 https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/link2000/gold_2nd_edition_26-apr-13.pdf

[15] LDACS: Future Aeronautical Communications for Air-Traffic Management

[16] Deutsche Telekom, Inmarsat, Thales, “The European Aviation Network – Powering Europe’s aviation connectivity”, White Paper, 2016

[17] World Radiocommunication Conference 2015 (WRC-15) Agenda and Relevant Resolutions

[18] Y. Zeng, R. Zhang and T. J. Lim, “Wireless communications with unmanned aerial vehicles: opportunities and challenges,” in IEEE Communications Magazine, vol. 54, no. 5, pp. 36-42, May 2016

[19] J.-S. Bedo, B. Barani and, A. Kemos, “Making 5G a real booster for vertical markets”, https://5g-ppp.eu/wp-content/uploads/2015/12/5GandVerticalSectorsEUCNCpaper.pdf

[20] 5G Ensure Project, “New Mission Critical Communications Alliance aims to improve Public Safety”, http://5gensure.eu/news/new-mission-critical-communications-alliance-aims-improve-public-safety

[21] FirstNet, “FirstNet Commends FCC on Taking Critical Steps in Planning for the Nationwide Public Safety Broadband Network”, http://www.firstnet.gov/news/firstnet-commends-fcc-taking-critical-steps-planning-nationwide-public-safety-broadband-network

[22] Erik Hollnagel, „The Resilience Engineering understanding of ‘resilience’“, 2016, Online: http://erikhollnagel.com/ideas/resilience-engineering.html

[23] Hollnagel, E., Woods, D. D. & Leveson, N. C., “Resilience engineering: Concepts and precepts”, Aldershot, 2016, UK: Ashgate.

[24] L. Rauchhaupt, E. Hintze, A. Gnad, „Über die Bewertung der Zuverlässigkeit industrieller Funklösungen - Die theoretischen Grundlagen.“, In: atp, Heft 3, 49 (2007), S. 38-47, Oldenbourg Industrieverlag

[25] ITU-T Recommendation E.800, Online: http://www.itu.int/rec/T-REC-E.800-200809-I

[26] IEC 60050-192 International Standard, Online: https://webstore.iec.ch/publication/21886

[27] Next Generation Mobile Networks Alliance (NGMN): “5G White Paper”, März 2015.

[28] 5G PPP, Architecture Working Group, White Paper „View on 5G Architecture”, Version 1.0, Juli 2016.

[29] ETSI Industrial Specification Group (ISG) Network Function Virtualisation (NFV), http://www.etsi.org/technologies-clusters/technologies/nfv

[30] ETSI ISG NFV, GS NFV-MAN 001, “Network Functions Virtualisation (NFV); Management and Orchestration”, V1.1.1, December 2014.

[31] 3GPP, TR 22.891 “Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)”, V14.2.0, September 2016.

[32] 5G PPP, White Paper “5G empowering vertical industries”, März 2016.

[33] ETSI Industrial Specification Group (ISG) Mobile Edge Computing (MEC), http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing

[34] Siemens Position Paper, “5G communication networks: Vertical industry requirements”, 2016

[35] Konvergente Netze als Infrastruktur für die Gigabit-Gesellschaft. Strategiepapier der | Projektgruppe „Konvergente Netze als Infrastruktur für die Gigabit-Gesellschaft“ Herausgeber: Nationaler IT-Gipfel Saarbrücken 2016 http://plattform-digitale-netze.de/app/uploads/2016/11/PF1_Gigabit_Konvergente_Netze_web_20161111.pdf

[36] DIN SPEC 91282:2012-11: Terminologie für das Securitymanagement von Verkehrsinfrastrukturen

[37] Schenk, M.; Richter, K.: Echtzeitdaten für die Logistik. Digitale Netze und Logistik, 27. Oktober 2015. Herausgeber: Nationaler IT-Gipfel Berlin 2015 Plattform „Digitale Netze und Mobilität“. http://plattform-digitale-netze.de/app/uploads/2016/06/151110_PF1_007_FG1_Digitale_Netze_und_Logistik.pdf

[38] Trend Report ROBOTICS IN LOGISTICS: A DPDHL perspective on implications and use cases for the logistics industry. DHL Customer Solutions & Innovation, March 2016. http://www.dhl.com/content/dam/downloads/g0/about_us/logistics_insights/dhl_trendreport_robotics.pdf

[39] A. Bereza et al., „Cross-Technology Communication between BLE and Wi-Fi using Commodity Hardware“, International Conference on Embedded Wireless Systems and Networks, EWSN ’15, Uppsala, Sweden, 2017

8.2 Abkürzungsverzeichnis

4G	Vierte (Mobilfunk) Generation
5G	Fünfte (Mobilfunk) Generation
5GAA	5G Automotive Association
5G NR	5G New Radio
5G PPP	5G Private Public Partnership
AFDX	Avionics Full-Duplex Switched Ethernet
AI	Artificial Intelligence
AR	Augmented-Reality
BEREC	Body of European Regulators for Electronic Communications
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BS	Base Station
C2C-CC	Car 2 Car - Communication Consortium
C-ITS	Cooperative ITS
CMF	Common Mode Failures
COTS	Commercial Off-The-Shelf
CP	Control Plane
CPS	Cyber-Physical Systems
DDoS	Distributed-Denial-of-Service
DIN	Deutsches Institut für Normung
DoS	Denial of Service
DSL	Digital Subscriber Line
DWDM	Dense Wavelength-Division Multiplex
EAN	European Aviation Network
EATA	European Automotive Telecom Alliance

EEG	Erneuerbare-Energie-Gesetz
EMI	Elektromagnetische Interferenz
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnik
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information und Telekommunikation
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LDACS	L-Band Digital Aeronautical Communication System
LEO	Low Earth Orbit
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
M2I	Machine-to-Infrastructure
M2M	Machine-to-Machine
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MS	Mobile Station
NF	Network Function
NFV	Network Functions Virtualization
NGMN	Next Generation Mobile Networks Alliance
OAM	Operation, Admininstration and Maintenance
OEM	Original Equipment Manufacturer
PHY	Physical Layer
PON	Passive Optical Network
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SDN	Software-Defined Networks
SDR	Software-Defined Radio
SLA	Service Level Agreement
SPoF	Single Point of Failure
TCP	Transmission Control Protocol
TK	Telekommunikation
TSN	Time Sensitive Networking
UAV	Unmanned Aerial Vehicles
UP	User Plane
V2I	Vehicle-to-Infrastructure
V2M	Vehicle-to-Motorcycle
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-X
VPN	Virtual Private Network

VDE-Positionspapier Resiliente Netze mit Funkzugang

WAIC	Wireless Avionics Intra- Communications
WLAN	Wireless Local Area Network
WRC	World Radio Conference

© VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

Notizen

VDE VERBAND DER ELEKTROTECHNIK
ELEKTRONIK INFORMATIONSTECHNIK e.V.

Stresemannallee 15
60596 Frankfurt am Main
Telefon: 069 6308-0
service@vde.com
www.vde.com