



WHITE PAPER

# 5G Virtualisierung

PADERBORN 2020

| VERSION 1.1

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung



Industrielles  
Internet



Taktiler  
Internet

# Inhalt

01 Einführung.....	4
02 Virtualisierung .....	6
03 Nutzungspotential und begünstigende Randbedingungen.....	11
04 Use Cases.....	14
05 Fazit .....	23
06 Verweise .....	24
07 Glossar .....	25
08 Notizen .....	26
09 Impressum .....	27

## Autoren:

Dr. Simon Oberthür | Universität Paderborn / SICP  
Lukas Sebastian Arendt | Universität Paderborn / SICP  
Michael Kemkes | InnoZent OWL e.V.  
Dr. Lutz Stobbe, Fraunhofer IZM  
Thomas Mager | Fraunhofer IEM

## Hinweis:

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen **16KIS0564K** gefördert.  
Die Inhalte wurden im Rahmen der Fachgruppen der „Informationsplattform für 5G“ und des Forschungsschwerpunktes „5G – Industrielles Internet“ des BMBF-Förderprogramms „IKT 2020 – Forschung für Innovationen“ erörtert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

# 01 Einführung

Industrie 4.0 definiert sich vor allem durch die hochgradige Vernetzung, beispielsweise von Prozessen und Lieferketten. Hieraus ergeben sich neue Anforderungen aber auch neue Chancen für die industrielle Kommunikation. Der neue Mobilfunkstandard 5G hat den Anspruch, Kommunikationsnetzwerke zu realisieren, die diese Anforderungen und Erwartungen in einer hochgradig verknüpften und industriell geprägten Gesellschaft erfüllen (vgl. [4]).

In unserem Whitepaper „5G Lean Industrial Communication“ [1] haben wir die neuen Chancen und Möglichkeiten moderner Kommunikationstechnologien bereits herausgearbeitet. Dabei ist die hochgradige Virtualisierung und Softwareifizierung in 5G Netzen ein elementarer Baustein für eine zukunftssichere industrielle Kommunikation.

Die Ericsson Studie „The Industry Impact of 5G“ [11] hat die Erwartungshaltung wiedergegeben, bei welchen Problemen 5G im industriellen Kontext helfen soll. In der Studie wird deutlich, dass die Befragten nicht nur als Lösungselement auf der Ebene der Netzwerkkommunikation sehen, sondern vermehrt auch auch in anderen Bereichen. Man erhofft sich davon beispielsweise ein vereinfachtes Change Management.

Wie in allen Bereichen steigen auch im industriellen Kontext die Anforderungen an Kommunikationsnetze. Wichtig ist in diesem Kontext der Bedarf höhere Datenmengen zu transportieren, die bedarfsgerechte Verteilung der Netzwerkressourcen und die Echtzeitfähigkeit. Im Kontext 5G werden die folgenden drei anwendungsbezogenen Leistungsanforderungen [2] diskutiert, die auch für verschiedene industrielle Anwendungen von Bedeutung sind:

**eMBB** – „Enhanced Mobile Broadband – wird gekennzeichnet durch hohe Datenraten von 1 Gbps im kommerziellen und endkundenorientierten Mobilfunknetz.“ [2]

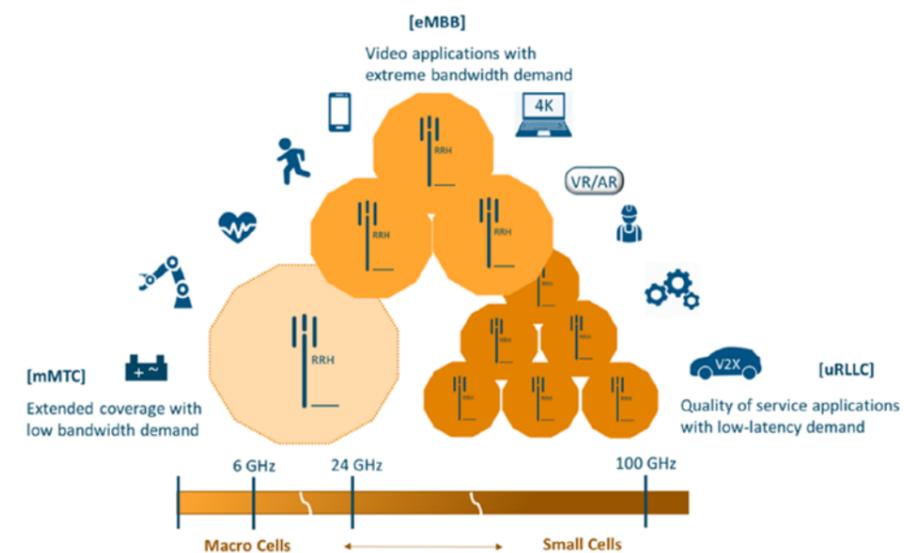
**uRLLC** – „Ultra Reliable Low Latency Communication – wird gekennzeichnet durch Echtzeitkommunikation mit 1 ms Latenz für hoch verfügbare Anwendungen.“ [2]

**mMTC** – „Massive Machine Type Communication – wird gekennzeichnet durch hochenergieeffiziente, skalierbare und flächendeckende Kommunikation mit geringen Datenraten.“ [2]

In diesem Zusammenhang wird häufig die Virtualisierung, eine der zugrundeliegenden Technologien und Enabler der formulierten Anforderungen, vernachlässigt. Die Virtualisierung ist aber ein wesentlicher Bestandteil eines 5G Netzwerkes und ermöglicht die Realisierung neuer Services, Geschäftsmodelle und Anwendungsfälle.

Cloud Computing, das sich zu dem vorrangigen IT-Paradigma entwickelt hat, basiert bereits auf Virtualisierung. Marktführer wie Amazon, Google und Microsoft bieten verschiedene Angebote in ihrem Portfolio an, auf denen beispielsweise prominente Services wie Netflix oder Dropbox realisiert werden. In den letzten Jahren setzt sich dieser Virtualisierungstrend bei den Telekommunikationsanbietern (Telcos) fort und bildet das Herzstück zukünftiger 5G Netze.

Aus diesem Grund möchten wir mit diesem Paper die Virtualisierung und die dadurch ermöglichten Use Cases thematisieren. Ziel ist es, die aktuell relevanten Use Cases für die Industrie zu beschreiben, die Zusammenhänge dieser Use Cases für die 5G Architektur zu erläutern und auf Chancen, die sich aus dieser Technologie ergeben, sowie Herausforderungen, die bei der Nutzung beachtet werden müssen, hinzuweisen. Dabei basiert der hier zusammengefasste Beitrag vorwiegend auf der veröffentlichten Literatur von ETSI und 5GPPP (vgl. [4]–[9]).



**Abb. 1.01**  
5G Leistungsanforderung und Service-Typen laut 3GPP Standardisierung [2]

## 02 Virtualisierung

Viele Whitepapers thematisieren die Virtualisierung, indem sie den Zusammenhang zwischen dieser Technologie und 5G Netzwerken erläutern. Es fehlt jedoch häufig eine generelle und eindeutige Definition des Begriffs „Virtualisierung“. Diese wird entweder als bekannt vorausgesetzt oder bezieht sich auf die zu virtualisierende Ressource. Die Literatur unterscheidet zumeist die folgenden drei zu virtualisierenden Ressourcen [3]:

- Speicherressourcen
- Netzwerkressourcen
- Rechenressourcen

Diese Virtualisierungen verfolgen das gemeinsame Ziel, die Ressourcen in isolierte Ausführungsumgebungen aufzuteilen, um so die Funktionalitäten von der für die Ausführung benötigten Ressource zu entkoppeln (vgl. [4]).

### Exkurs: Cloud Computing

Cloud Computing ermöglicht es, eine Vielzahl an unterschiedlichen Anwendungen auf einer gemeinsamen Infrastruktur zu unterstützen, sodass Dienstleister ihren Kunden On-Demand-Services anbieten können. Dabei ist die Virtualisierung der Enabler für Cloud Computing. Nach der NIST Definition wird Cloud Computing durch die folgenden 5 Merkmale charakterisiert [10]:

1. On-demand self-service: Dieses Merkmal bedeutet, dass ein Verbraucher von sich aus automatisch Rechenfunktionen anfordern kann.
2. Broad network access: Mithilfe der broad network accesses sind alle Funktionen über das Netzwerk durch standardisierte Schnittstellen ortsunabhängig verfügbar.
3. Ressource pooling: Die benötigten physischen und virtuellen Ressourcen für die Bereitstellung eines Dienstes werden gebündelt, um diese dynamisch der Verbrauchernachfrage zuzuordnen.
4. Rapid elasticity: Da sich benötigte Funktionen elastisch bereitstellen lassen, können Dienstanbieter die Nachfrage des Verbrauchers skalieren.
5. Measured service: Um Transparenz sowohl für den Verbraucher als auch Anbieter zu schaffen und die Ressourcenverteilung zu optimieren, muss der angebotene Service kontrolliert und überwacht werden. Das gilt typischerweise als Basis für Pay-per-use Abrechnungsmodelle.

Die Bereitstellung von IT-Ressourcen auf Basis von Cloudtechnologie ist mittlerweile zum Standard geworden und spiegelt sich in dem Term „Cloud first“ wider. Die Vorteile sind hierbei vielfältig: Aus der Nutzung von IT-Ressourcen als externe Cloud-Dienstleistung ergibt sich beispielsweise die Möglichkeit der Verschiebung von Investitionsausgaben (CAPEX) in den operativen Betrieb (OPEX). Dank der flexiblen, bedarfsgerechten on-demand Nutzung entstehen neue Möglichkeiten, die unter anderem die Skalierung oder das kostengünstige Erproben neuer Technologien im Kontext der Digitalisierung erlauben. Gleichzeitig resultieren aus der Entkopplung von Software und Hardware neue Chancen. Software kann somit flexibler platziert werden und es können verschiedene Anforderungen auf der gleichen Infrastruktur bedient werden, wie z. B. eine kostengünstige Umsetzung oder Echtzeitfähigkeit. Ein Beispiel hierfür ist Cloud-Robotik. Hier wird der Ausführungsort der SW vom Roboter selbst in EDGE-Cloudkomponenten ausgelagert, wodurch der eigentliche Roboter günstiger angeboten werden kann. Ein anderes Beispiel ist das Industrial IoT, bei dem günstige Sensoren Maschinen- und Umweltdaten erheben können, die dann in der Cloud verarbeitet werden.

Die bisherigen Netzwerke sind durch eine große Vielfalt an proprietärer Hardware charakterisiert. Dies bedeutet, dass Funktionen und Dienste der bestehenden Netzwerke unmittelbar mit der eingesetzten proprietären Hardware verbunden sind. Muss diese wegen beispielsweise neuer Entwicklungen ausgetauscht werden, so ist dies oft sehr kostspielig.

Um dieses Problem zu lösen und mehrere dedizierte logische Netzwerke aufzubauen, wird eine Netzwerkvirtualisierungstechnologie verwendet. Diese eliminiert die Abhängigkeit zwischen den Netzwerkfunktionen (NF) und der Hardware.

Dieses Ziel realisiert die Network Functions Virtualisation (NFV), die die Netzwerkfunktionen von der Hardware, auf der sie läuft, trennt und in der Software realisiert (vgl. [3], [7]). Damit Netzbetreiber virtualisierte Netzwerkfunktionen (VNF) ausführen können, ist eine spezielle Architektur der Infrastruktur nötig, die sogenannte Network Functions Virtualisation Infrastructure (NFVI). Dabei sind diese Technologien keine Neuentwicklungen, sondern kommen bereits erfolgreich in modernen Rechenzentren zum Einsatz. NFV setzt somit die zuvor beschriebene Virtualisierung im Netzwerkkontext um.

## 2.1 Die zehn NFV Schlüsselmerkmale für 5G (10 Key Features for NFV)

Um die in Kapitel 4 beschriebenen Use Cases zu realisieren, sind nach ETSI 10 Schlüsselmerkmale relevant (vgl. [6]). Diese Merkmale werden nun beschrieben und um die Bedeutung für die industrielle Kommunikation ergänzt:

### 1. Network Slicing

Network Slicing beschreibt ein serviceorientiertes Netzwerkkonstrukt, das als „Network as a Service Paradigma“ bezeichnet wird. Ein Netzwerk Slice setzt sich aus Netzwerkfunktionen, -anwendungen und der zugrundeliegenden Cloud-Infrastruktur (physische, virtuelle oder emulierte Ressourcen) zusammen. Diese werden gebündelt, um die Anforderungen eines bestimmten Anwendungsfalls und Geschäftszwecks zu erfüllen. Das bedeutet, dass verschiedene Dienste mit unterschiedlichen Anforderungen auf derselben Netzwerkinfrastruktur laufen und Dienstleister On-Demand-Netzwerke anbieten können. Für den industriellen Einsatz können folglich verschiedene Netze konsolidiert und über eine Infrastruktur abgewickelt werden.

### 2. Cloud-native Network Functions

Aufbauend auf generischen Cloud-Techniken, die über klassische Virtualisierungsprinzipien hinausgehen, verfolgen Cloud-native Netzwerkfunktionen (NF) das Ziel, die Effizienz durch eine bedarfsgerechte Skalierung der verwendeten Ressourcen zu maximieren. Dienstleister müssen VNFs implementieren, die die Cloud-native Design Prinzipien dann umsetzen. Für den industriellen Einsatz ergibt sich hier die Möglichkeit, auf universelle Bausteine aufsetzen zu können und für den eigenen Anwendungsfall zusammenzustellen.

### 3. End-to-End Service Management

Das End-to-End Prinzip ermöglicht es, zwei beliebige Endgeräte durch eine Kommunikationsverbindung miteinander zu verbinden, sodass ein beliebiger Dienst von einem Endgerät direkt für ein anderes Endgerät erbracht werden kann.

Dieses Prinzip ist ein zentrales Schlüsselkonzept für 5G, um verschiedene Services unterschiedlichen Kunden anzubieten. Dabei soll der Kunde die benötigten Ressourcen für die von ihm gewünschten Services selbst auswählen können. Aus diesem Grund stellt die Verteilung und Zuweisung dieser Ressourcen durch das Management- und Orchestrierungsframework eine zentrale Herausforderung dar. Auf diese Weise können für den industriellen Einsatz verschiedene Komponenten und Prozesse miteinander verknüpft werden.

### 4. Edge Computing

Eines der Ziele von 5G ist es, Dienste mit extrem niedrigen Latenzanforderungen zu unterstützen. Dafür müssen Dienstleister Systeme einsetzen, bei denen die Dienste, die am empfindlichsten auf Latenz reagieren, auf Servern ausgeführt werden, die möglichst nah an den Endgeräten sind. Edge Computing kann im industriellen Kontext besonders dazu dienen, Cloud Computing unter Einhaltung von Echtzeitfähigkeit vor Ort zu nutzen.

### 5. RAN Cloudification

Die Radio Access Network Technologie beschreibt das Verbindungsverfahren für ein funkbasiertes Kommunikationsnetzwerk. Mithilfe von RAN ist es möglich, ein Signal an verschiedene drahtlose Endpunkte in einem Netzwerk zu senden. Dafür muss das Signal von der Antenne des verwendeten Endgeräts zu einem nahegelegenen Funkmast weitergeleitet werden, wo das Endgerät authentifiziert und identifiziert wird. Diese beschriebene Technologie lässt sich in 5G Netzwerken virtualisieren.

Die Virtualisierung ermöglicht, das universelle 5G Netz im industriellen Kontext an verschiedene Anwendungsfälle anzupassen und entsprechend zu optimieren. Sind sehr kleine Latenzen für die Echtzeitkommunikation nötig, muss die RAN Technologie schnell reagieren und wird nah an den Endgeräten in der EDGE-Cloud platziert. Bedarf es dagegen keiner kleinen Latenz, kann die Funktionalität kostengünstiger in entfernten Rechenzentren realisiert werden.

### 6. Multi-site Services

Es müssen verschiedene administrative Bereiche automatisiert zusammenarbeiten, um ein lauffähiges 5G Netzwerk zu garantieren. Das bedeutet, dass die Zusammensetzung verschiedener Services, u. a. IaaS, NFVaaS und NS, die für den Aufbau eines 5G Netzwerkes essenziell sind, durch administrative Bereiche unterstützt werden.

Hier wird ein hoher Grad an Automatisierung angestrebt, was im Kontext der industriellen Kommunikation die automatisierte Nutzung und Konfiguration der Netzwerkinfrastruktur sowie der darauf ausgeführten Dienste und vernetzten Komponenten ermöglicht.

### 7. NFV License Management

Die Anbieter von NFV Software Komponenten nutzen proprietäre Lizenzen, um die Rechte an beispielsweise der Wiederverwendung oder Änderungen der Software durch den Kunden einzuschränken. Je nach Anbieter können diese Lizenzbedingungen und die daraus resultierenden Bestimmungen zur Nutzung der Software variieren. Für den Kunden bedeutet dies, dass er nicht mehrere NFV Software Komponenten von unterschiedlichen Anbietern kombinieren kann, wenn die Lizenzbedingungen eines Anbieters verletzt werden. Daraus folgt, dass sowohl die Implementierung von VNFs als auch die Realisierung der Virtualisierung erschwert werden. Aus diesem Grund sind einheitlich geltende Standards zu definieren. Dies ist im Kontext der industriellen Kommunikation von hoher Bedeutung, um Interoperabilität zu gewährleisten.

### 8. Security

Da Netzwerkkommunikation viele Bereiche im privaten und öffentlichen Leben erfasst, ist der Sicherheitsaspekt ein besonders wichtiger und kritischer Punkt. Deshalb sind die klassischen Sicherheitsaspekte (Identitätsmanagement, Authentifizierungsmanagement, Rechtemanagement, Verschlüsselungslösungen) auch im Virtualisierungskontext zu beachten. Dies kann beispielsweise mithilfe des „Security-by-design“ Ansatzes gelingen. Bei diesem Ansatz werden die benötigten Sicherheitsanforderungen an die Software und Hardware bereits bei der Entwicklung berücksichtigt. Jedoch stellen einige Sicherheitsanforderungen an 5G Netzwerke immer noch eine große Herausforderung dar. Es fehlt z. B. das tiefere Verständnis, wie ein umfassendes

Identitätsmanagement aufgebaut werden kann, das sowohl die stationären und mobilen Endbenutzer als auch Methoden der Identifizierung von Hardware- und Softwarekomponenten beachtet. Da im industriellen Kontext Maschinendaten oftmals Betriebsgeheimnisse beinhalten, ist dieser Aspekt von hoher Bedeutung.

### 9. Realibility

Die Zuverlässigkeit, die die Verfügbarkeit der Netze beschreibt, stellt ein weiteres zu berücksichtigendes Schlüsselmerkmal dar. Zu der NFV Zuverlässigkeit zählen folgende Aspekte [6]:

- (i) robuste Designarchitekturen
- (ii) Bewertung der Widerstandsfähigkeit von End-zu-End-Netzdiensten
- (iii) Auswirkungen auf die Verfügbarkeit von Softwareänderungen
- (iv) aktive Überwachung zur Erkennung von Anomalien
- (v) NFV-Resilienzmetriken
- (vi) Rollen und Verantwortlichkeiten, die zu Abgrenzungspunkten in einem Rahmen für Qualitätsverantwortung führen.

Da zuverlässige Kommunikation einen elementaren Bestandteil von Industrie 4.0 bildet, ist dieser Aspekt essenziell für den Einsatz dieser Technologien im industriellen Kontext.

### 10. Scalability

Die Grundidee von 5G ist es, dass jeder Kunde von einem beliebigen Standort aus verschiedene Anwendungen starten kann, um individuelle Serviceleistungen zu erhalten. Dafür ist eine Architektur nötig, die höchst skalierbar ist und durch die Virtualisierung eine bedarfsgerechte Skalierung der vom Kunden benötigten (Netzwerk-)Ressourcen ermöglicht.

Im industriellen Kontext gewinnt dieser Aspekt immer mehr an Bedeutung. Anwendungsfälle wie Predictive Maintenance können sehr dynamische Anforderungen an die Infrastruktur stellen. Der flexible Einsatz von IKT-Ressourcen und der bessere Zugang zu relevanten Daten ist hier ein essenzieller Baustein.

Diese zehn NFV-Schlüsselmerkmale für 5G zeigen, dass die NFV viele unterschiedliche Gestaltungsbereiche einer Netzwerkinfrastruktur erfasst und eine hohe Bedeutung für den industriellen Einsatz hat. Dazu zählen beispielsweise Aspekte wie das Netzwerkdesign, Hardware, Cloud Computing, Speichertechnologien sowie Management und Orchestrierung. Jeder dieser Aspekte verwendet unterschiedliche Techniken, Ressourcen sowie Technologien, die auf verschiedenen Spezifikationen und zugrundeliegenden Terminologien basieren. Da 5G die genannten Bereiche integriert, muss eine einheitliche Sprache entwickelt werden, sodass die Grundbegriffe und Prinzipien für alle Industrien kompatibel sind. Aus diesem Grund müssen Standards definiert werden, um ein einheitliches Grundverständnis der Begriffe und Zusammenhänge der Bereiche zu schaffen (vgl. [5]).

# Nutzungspotential und begünstigende Randbedingungen 03

## 3.1 Chancen

Das aus den 5G Netzwerken resultierende und bisher ungenutzte Potential basiert auf dem Virtualisierungsparadigma, Hardware und Software voneinander zu trennen. Dieses ermöglicht es, Management und Orchestrierung der Netzwerke zu verbessern, um neuartige Netzwerkdienste für den Kunden einfacher umzusetzen. Die neuartigen Netzwerkdienste resultieren aus den drei beschriebenen anwendungsbezogenen Leistungsanforderungen von 5G (vgl. Kapitel 1).

Für Dienstleister ist es essentiell, von der Flexibilität der 5G Netzwerke zu profitieren, um mehrere logische und unabhängige End-to-End Netzwerke auf einer gemeinsamen physischen Infrastrukturplattform anzubieten. Dadurch können Netzwerk Slices effizient skaliert werden, sodass Dienstleister On-Demand Services definieren und diese Services gezielt auf die Kundenbedürfnisse anpassen können (vgl. [4]). Außerdem können Dienstleister neue und effizientere Test- und Integrationsmöglichkeiten realisieren, weil sich auch Test Cases auf einer gemeinsamen Infrastruktur ausführen lassen. Erwartet wird, dass dies die Markteinführungszeit neuer Produkte und Services minimiert und anfallende Kosten, wie z. B. für Geräte, Strom oder Entwicklung, senkt (vgl. [7]). Voraussetzung für die beschriebene Flexibilität ist, dass die zugrundeliegende Infrastruktur in eine physikalische und virtuelle zerteilt werden kann.

Die erwähnten Chancen zeigen, dass 5G die Betriebseffizienz verbessert und Netzwerkkonfigurationen optimiert, sodass Dienstleister neue Services und Use Cases (u. a. auch Echtzeitangebote) entwickeln können.

## 3.2 Herausforderungen

Um den Erfolg der 5G Technologie zu gewährleisten, müssen neue Methoden zur wirtschaftlichen Analyse der Virtualisierung, neue Geschäftsmodelle sowie kommerzielle Ökosysteme und Marktstrukturen entwickelt werden. Dafür müssen Dienstleister, wie Telcos bzw. Netzwerkanbieter, die beschriebenen Use Cases und Services (vgl. Kapitel 4) erfolgreich realisieren und sich am bestehenden Markt mit ihrem neuen Serviceangebot etablieren (vgl. [5]).

Eine weitere wichtige Herausforderung ist die Sicherheit (Security and Safety). Dieser Aspekt berücksichtigt sowohl die Datensicherheit als auch die Managementkonzepte, die das Ziel verfolgen, das gesamte 5G Netzwerk und deren einzelne Komponenten vor inneren und äußeren Bedrohungen zu schützen. Während es bei inneren Bedrohungen um unbeabsichtigte Fehler innerhalb des Netzwerks geht, die z. B. zu Netzwerkausfällen führen, sind mit äußeren Bedrohungen gezielte Angriffe (beispielsweise Cyberattacken) auf das Netzwerk gemeint. Die neu entwickelten Sicherheitsmaßnahmen müssen zum einen Regeln definieren, die beschreiben, wie VNFs zu kontrollieren und visualisieren sind. Zum anderen müssen sie für jeden einzelnen Use Case getestet werden, um sicherzustellen, dass diese ihren Zweck erfüllen (vgl. [5]).

Eine Auflistung aller Herausforderungen für die Netzwerkvirtualisierung (NFV) nach ETSI (vgl. [7]) ist im Folgenden dargestellt:

• **Portability/Interoperability**

Ziel ist es, eine einheitliche Schnittstelle zu definieren, die die Softwareinstanzen eindeutig von der Hardware trennt, sodass es möglich ist, verschiedene virtuelle Anwendungen auf einer gemeinsamen Infrastruktur auszuführen.

• **Performance Trade-off**

Die Dienstleister müssen moderne Softwaretechnologien verwenden, um die wahrscheinliche Leistungsabnahme – verursacht durch den Verzicht auf Hardware (wie Coprozessoren für Hardwarebeschleunigung) – zu kompensieren.

• **Migration and co-existence of legacy & compatibility with existing platforms**

Die eingesetzten VNFs müssen mit den bereits vorhandenen Infrastrukturen, Netzwerkgeräten und eingesetzten physikalischen NFs der Netzwerkbetreiber kompatibel sein, weil der Übergang von physischen zu offeneren standardbasierten virtuellen Netzwerken und anwendungs-basierten Lösungen ein kontinuierlicher Prozess ist.

• **Management and Orchestration**

Mithilfe einer konsistenten Management- und Orchestrierungsarchitektur ist es möglich, die benötigten Ressourcen für einen gewünschten Kundendienst zu verwalten. Die Herausforderung besteht darin, zu entscheiden, welche der verfügbaren physischen und virtuellen Netzwerkressourcen verwendet werden, um diesen Dienst bereitzustellen. Je mehr Kunden eine Dienstleistung auf einer Netzwerkinfrastruktur anfordern, desto komplexer wird die Kontrolle und die Zuordnung dieser Netzwerkressourcen zu den jeweiligen Kunden.

• **Automation**

Ziel ist es, die für einen Dienst benötigten Netzwerkressourcen automatisiert zuzuordnen, sodass die schnelle Skalierung der Netzwerkfunktionen möglich ist.

• **Security and Resilience**

Der Einsatz von VNFs in den Netzwerken der Betreiber darf die Verfügbarkeit und Sicherheit des bestehenden Netzwerks nicht beeinträchtigen. Die Betreiber müssen garantieren, dass alle getroffenen Sicherheitsmaßnahmen ordnungsgemäß funktionieren.

• **Network Stability**

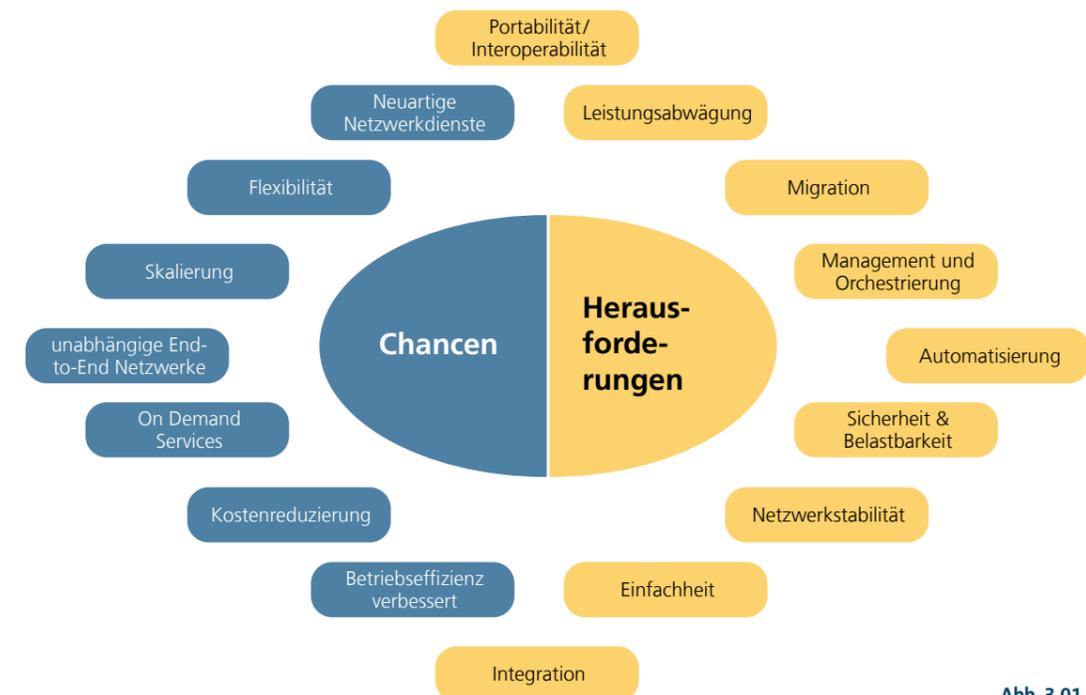
Die Stabilität des Netzwerks sollte zu jedem Zeitpunkt gewährleistet sein, was eine Herausforderung darstellt, die es zu meistern gilt, schließlich muss eine große Anzahl an virtuellen Anwendungen zwischen verschiedenen Hardwareanbietern verwaltet und orchestriert werden.

• **Simplicity**

Die Herausforderung besteht darin, eine verständliche und einfach zu bedienende Netzwerkplattform bereitzustellen.

• **Integration**

Bei der nahtlosen Integration von virtuellen Anwendungen auf unterschiedlicher, heterogener Virtualisierungshardware kann es zu Kompatibilitätsproblemen führen. Validierung und deren Toolunterstützung spielen hierbei eine zentrale Rolle.



**Abb. 3.01**  
Chancen und Herausforderungen der Netzwerkvirtualisierung

## 04 Use Cases

Dieses Kapitel erläutert die relevanten Use Cases bezüglich der Netzwerkvirtualisierung für Industrie, Netzanbieter sowie Telcos und beschreibt, wie diese mit der 5G Architektur zusammenhängen. Hierfür werden die Use Cases in unterschiedliche Anwendungsgebiete gegliedert, die sich an der 5G Architektur orientieren. Dabei ist zu berücksichtigen, dass es sich um keine vollständige Liste aller Use Cases handelt, sondern lediglich die wichtigsten in der Literatur (vgl. [4], [7], [8], [9]) beschriebenen Anwendungsfälle thematisiert werden.

### 4.1 Use Cases

Die identifizierten Use Cases sind in verschiedene Anwendungsgebiete einzuteilen. Diese unterscheiden sich, weil die Autoren ein unterschiedliches Verständnis hinsichtlich der definierten Use Cases und deren Anwendung besitzen.

Während 5GPPP die folgenden 6 Anwendungsgebiete definiert (vgl. [4]):

- Dense urban
- Broadband everywhere
- Connected Vehicles
- Future smart offices
- Low bandwidth IoT
- and Tactile Internet, differenziert ETSI die Use Cases auf der Netzwerkvirtualisierungsebene (vgl. [7]):
- Switching elements
- Mobile network nodes
- Functions contained in home routers and set top boxes to create virtualised home environments
- Tunnelling gateway elements
- Traffic analysis
- Service assurance
- NGN signalling
- Converged and network wide functions
- Application-level optimisation
- Security functions

Da die hier beschriebenen Use Cases auf den Informationen von ETSI basieren und sie nicht bestimmten Anwendungsgebieten zugeordnet sind, wird eine eigene Gliederung für die Use Cases verwendet. Diese orientiert sich an der 5G Architektur (vgl. Abb. 4.01) und dem Aufbau von 5G Netzwerken.

Folgende Anwendungsgebiete lassen sich aus der 5G Architektur ableiten:

### 1. Kernnetzwerkvirtualisierung

Kernnetzwerktechnologien, u. a. die grundlegende Infrastruktur und Hardware (z. B. RAN Knoten, Mobilfunkmasten etc.), sind für jedes Netzwerk essenziell, da Netzbetreiber ohne diese Technologien kein Netzwerk realisieren können. Die Use Cases in dieser Gruppe virtualisieren einzelne Komponenten dieser Kernnetzwerktechnologien, sodass die Virtualisierungskonzepte auf der Kernnetzwerkebene anzuwenden sind.

### 2. Services für die Bereitstellung des Netzwerks

Diese Gruppe definiert alle Anwendungsfälle, bei denen Dienstanbieter Services für einen Kunden bereitstellen, die für die Aufrechterhaltung oder Realisierung eines eigenen 5G Netzwerks benötigt werden. Zu diesen angebotenen Services zählen die Plattform, die zugrundeliegende Infrastruktur, die benötigten VNFs sowie die Verschlüsselungs- und Sicherheitsleistungen. All diese potentiellen Serviceangebote müssen die Herausforderung meistern, dass Kunden Services dauerhaft und mit minimalen Ausfallzeiten verwenden können.

### 3. Management, Orchestrierung & Ressourcenzuweisung

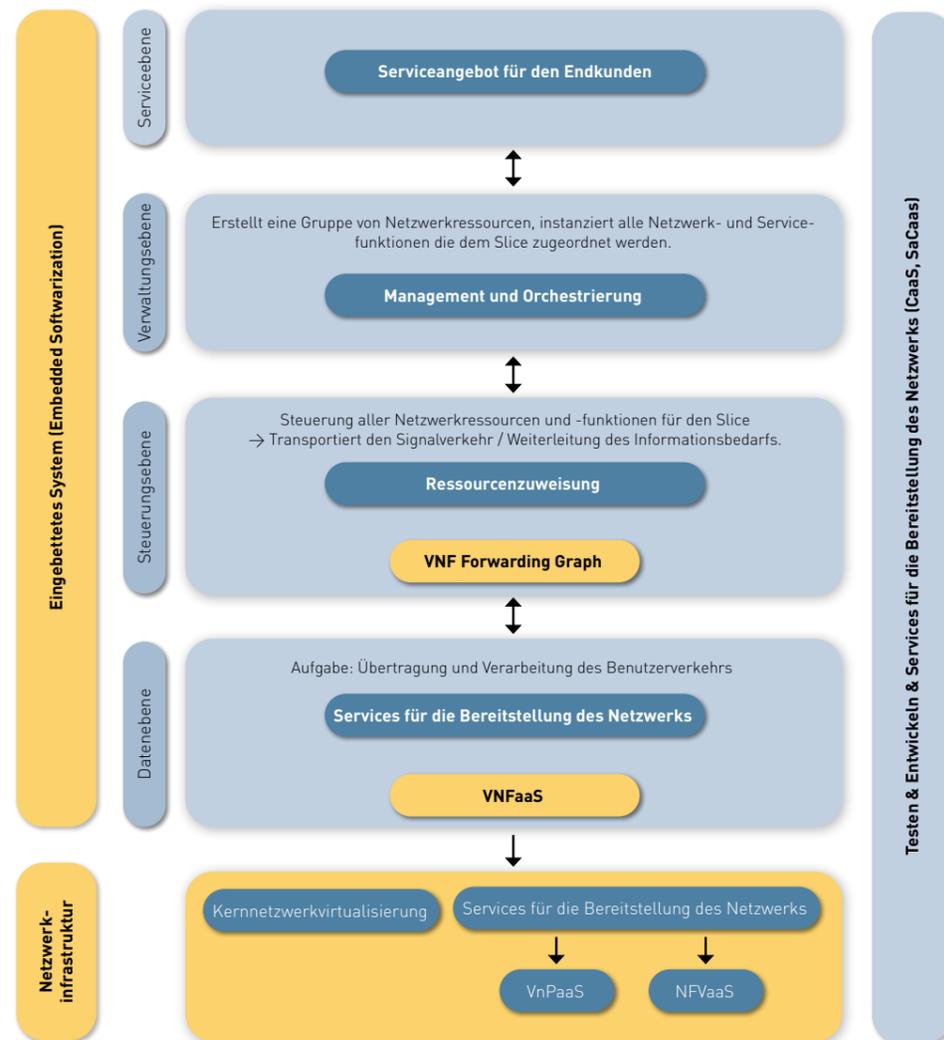
Wenn dem Kunden an einem physischen Standort nicht genügend Ressourcen zugeordnet werden können, ist der gewünschte Service für den Kunden nur eingeschränkt oder gar nicht verfügbar. Aus diesem Grund sind die benötigten Ressourcen erfolgreich zu managen und zu orchestrieren, sodass die Ressourcenzuteilung für den genannten Service jederzeit ausreichend ist.

### 4. Testen und Entwickeln

Da die Entwicklung und Instandhaltung von 5G Netzwerken kein statischer, sondern ein dynamischer, agiler und iterativer Prozess ist, müssen alle Use Cases sowie angebotene Services auf Richtigkeit und Funktionsfähigkeit kontrolliert werden. Die Mechanismen und Prinzipien, die prüfen, ob die Unternehmensziele der Telcos zu erreichen sind, lassen sich virtualisieren.

### 5. Serviceangebot für den Endkunden

Die oben beschriebenen Use Case Gruppen bilden die Grundlage für erfolgreiche 5G Netzwerke. Besonders die Industrie muss die obigen Use Cases verstehen und diese Anwendungsfälle in ihre bestehenden Konzepte integrieren, um von 5G zu profitieren und ein eigenes Serviceangebot basierend auf 5G Technologien zu entwickeln. Dafür ist es erforderlich, dass Industrien die zugrundeliegenden Mechanismen und die Architektur von 5G sowie deren Möglichkeiten und Risiken begreifen, sodass die Anwendung dieses Wissens einen Mehrwert für das Unternehmen schafft. Dies ist essenziell, weil sich der normale Endkunde weder mit 5G Netzwerken noch mit den Zusammenhängen verschiedener Netzwerkkomponenten auskennt. In der Regel möchte er einen funktionierenden Service von einem Dienstanbieter kaufen oder von neuartigen Innovationen wie IoT profitieren. Demnach ist es die Aufgabe der Industrie, Forschung zu betreiben und neuartige Technologien zu entwickeln und integrieren, um Kundenbedürfnisse zu befriedigen.



**Abb. 4.01**  
Detailliertere Darstellung  
der Use Cases im Kontext  
der 5G Architektur

Die beschriebenen Use Case Gruppen lassen sich in die Architektur von 5G Netzwerken einordnen (siehe Abb. 4.01). Dabei handelt es sich um eine vereinfachte Darstellung der Architektur, um die Zusammenhänge der verschiedenen Use Cases zu erläutern.

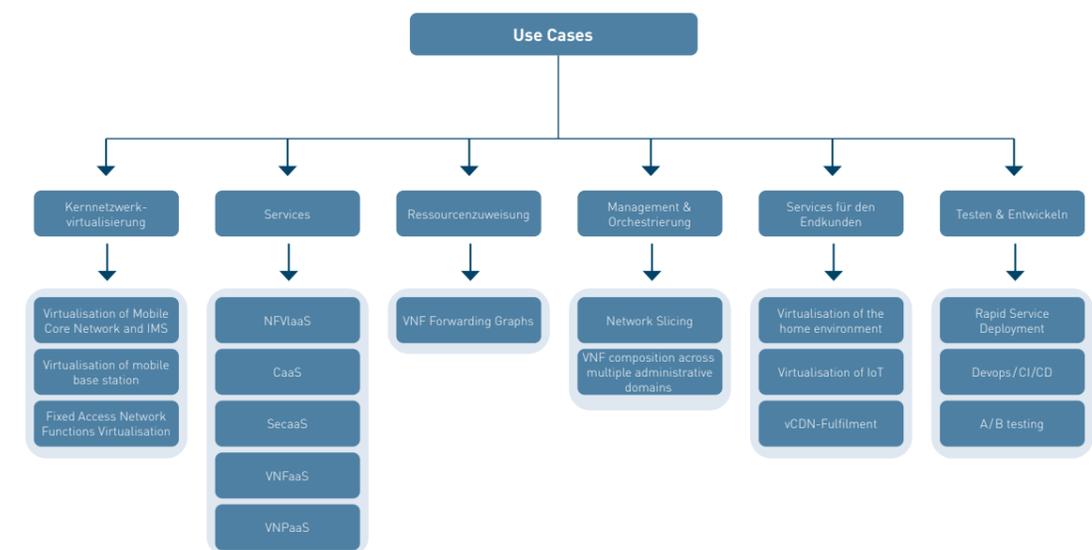
Die dargestellte Architektur lässt sich in zwei zentrale Bereiche unterteilen: Netzwerkinfrastrukturebenen und das darin eingebettete virtuelle System. Während die Netzwerkinfrastruktur die technische Grundlage und die benötigten Ressourcen für 5G Netzwerke bereitstellt, beschreibt das virtuell eingebettete System, wie die Kommunikation innerhalb des Netzwerks funktioniert. Somit definiert das virtuell eingebettete System die Aufgaben und Funktionen, die nötig sind, um dem Kunden einen Service anzubieten.

Folgende Bereiche lassen sich bei dem virtuell eingebetteten System unterscheiden:

- 1. Datenebene:** Dieser Teil des Netzwerks dient der Verarbeitung und dem Transport des Datennutzerverkehrs. Dies bedeutet, dass mithilfe der ausgewählten VNFs ein Datentransfer vom Client oder zum Client ermöglicht wird.
- 2. Steuerungsebene:** Diese Ebene steuert alle Netzwerkressourcen und -funktionen für den benötigten Slice. Ziel ist es, die benötigten Informationen an die ausgewählten VNFs auf der Datenebene weiterzuleiten.
- 3. Verwaltungsebene:** Es ist essenziell, eine Gruppe von Netzwerkressourcen zu erstellen, um dem Kunden seinen gewünschten Dienst anzubieten. Aus diesem Grund muss der Dienstleister identifizieren, welche Ressourcen verfügbar und verwendbar sind, sodass diese Ressourcen auf der Steuerungsebene dem Dienst zugewiesen werden können. Daraus ergibt sich, dass der Dienstleister die Ressourcen auf dieser Ebene managen und orchestrieren muss.
- 4. Serviceebene:** Diese Ebene beschreibt die angebotene Dienstleistung für den Kunden.

Um die Stabilität und Zuverlässigkeit des Netzwerks zu gewährleisten, sollte die Sicherheit auf allen Ebenen der 5G Infrastruktur garantiert werden. Aus diesem Grund ist ein kontinuierliches Testen und die Verwendung von Sicherheits- und Verschlüsselungskonzepten auf allen Ebenen wichtig.

Im Folgenden sind alle Use Cases und deren Zuordnung zu den Anwendungsgebieten nochmals grafisch dargestellt (vgl. Abb. 4.02):



**Abb. 4.02**  
Zuordnung der Use Cases  
zu den einzelnen Use Case  
Anwendungsgebieten

GLIEDERUNG	USE CASE	BESCHREIBUNG	VIRTUALISIERUNGSZIEL	HERAUSFORDERUNG(EN)
<b>Kernnetzwerk-virtualisierung:</b>	Virtualisation of Mobile Core Network and IMS (IP Multimedia Subsystem)	Zur Zeit sind die Mobilfunknetze mit einer Vielzahl an proprietärer Hardware ausgestattet, sodass mithilfe von VNFs die Komplexität des Netzwerks reduziert werden soll. Durch die Virtualisierung des Kernnetzwerks oder lediglich einzelner Komponenten des Kernnetzwerks (virtualisierte und nicht virtualisierte Komponenten können koexistieren) sollen beispielsweise die Serviceverfügbarkeit sowie die Effizienz der Ressourcenzuweisung erhöht werden.	Dieser Anwendungsfall beschreibt die Virtualisierung eines Mobilfunknetzes, das die Kundenanfragen und die damit verbundenen Kapazitätsanforderungen für das Netzwerk erfüllt.	Die Virtualisierung des Kernnetzwerks hat beispielsweise folgende zu lösende Herausforderungen: Ressourcenskalerung Ressourcenzuweisung Virtualisierungstransparenz für Netzwerkkontrolle Wartung Überwachung, Diagnose etc.
	Virtualisation of Mobile base station	Durch die Zunahme mobiler und vernetzter Geräte steigen die Netzwerk-anfragen und der Datenverkehr in Mobilfunknetzen. Aus diesem Grund nehmen die Kosten für die Betreibung solcher Netzwerke weiter zu. Ein Großteil dieser Kosten wird durch die RAN Knoten verursacht. Indem die mobilen Basisstationen virtualisiert werden, kann ein Teil der RAN Knoten auf Standard-IT-Servern, -Speicher und -Switches realisiert werden. Dadurch kann die Kapazität der Ressourcenteilung erhöht werden und es gelingt, Kundenanforderungen besser zu erfüllen.	Während für traditionelle RAN Knoten (z. B. eNodeB) die Basisband-funkinheit, MAC oder RRC, mögliche Virtualisierungsziele darstellt, können hingegen für C-RAN Knoten die BBU oder Schaltfunktionen virtualisiert werden.	Um diesen Use Case zu realisieren, müssen verschiedene technische Herausforderungen erfüllt werden. Dazu zählen die Echtzeitbetriebssystemvirtualisierung, die Virtualisierung der Basisbandfunkprozesse oder die Verbindungen innerhalb eines virtualisierten BBU-Pools.
	Fixed Access Network Functions Virtualisation	Um Systeme mit hohem Bandbreitenzugang zu ermöglichen, müssen elektronische Systeme in entfernten Knotenpunkten (z. B. in Gebäuden) eingesetzt werden. Mit diesen Knotenpunkten können sich dann Modems verbinden. Durch die Netzwerkvirtualisierung lässt sich das Remote Equipment vereinfachen und es können Kosten eingespart und Mehrfachvermietungen der Zugang-netzwerk-ausrüstung gewährleistet werden.	Die Fixed Access Technologie soll virtualisiert werden.	Zur Zeit existieren noch keine Standards bezüglich der Virtualisierung der Fixed Access Technologie. Des Weiteren muss der Virtualisierungsmechanismus für den Zugang und die Verwaltung des Netzwerks und der API spezifiziert werden.

GLIEDERUNG	USE CASE	BESCHREIBUNG	VIRTUALISIERUNGSZIEL	HERAUSFORDERUNG(EN)
<b>Services (für die Bereitstellung eines Netzwerks):</b>	Network Function Virtualisation Infrastructure as a Service (NFVlaaS)	Die meisten Serviceanbieter benötigen für die Bereitstellung von VNFs physikalische Rechen-, Netzwerk- und Speicherressourcen, um die Nachfrage der Kunden nach globalen Services zu befriedigen. Da viele dieser Serviceanbieter nicht selbst über die benötigten Ressourcen verfügen, stellt der Anwendungsfall NFVlaaS eine potentielle Lösung für dieses Problem dar. NFVlaaS bedeutet, dass ein anderer Dienstleister als der Serviceanbieter seine Infrastruktur bereitstellt, sodass die virtualisierenden NFs innerhalb der bereitgestellten NFV Infrastruktur ausgeführt werden können, ohne dabei die zugrundeliegende NFV Infrastruktur zu kontrollieren. Da VNFs von verschiedenen Serviceanbietern auf der gleichen Infrastruktur koexistieren können, stellt die Möglichkeit, die NFV-Infrastruktur bereitzustellen, ein zusätzliches kommerzielles Serviceangebot dar.	Das zugrundeliegende Virtualisierungsziel ist die Bereitstellung der NFV Infrastruktur als eine Ausführungsumgebung. Indem Serviceanbieter dieses Angebot nutzen, kann das Kundenerlebnis durch Reduzierung der Latenzzeiten verbessert werden und die Ausfallzeiten verringern sich.	Damit die NFV Infrastruktur angeboten werden kann, müssen Orchestrierungs- und Managementmechanismen implementiert werden. Dazu zählen u. a. Zugriffsbeschränkungen und Authentifizierungsmechanismen, sodass nur autorisierte VNFs auf der Infrastruktur ausgeführt werden können. Zusätzlich müssen die SLA (Service-Level Agreement) Anforderungen, wie z. B. Fehlermeldungen und Diagnoseberichte, unterstützt werden.
	Crypto as a Service (CaaS)	Es ist notwendig, den kryptographischen Schlüsselbetrieb sowie die zentrale Schlüsselverwaltung für VNFs, die sich mit dem verschlüsselten Verkehr beschäftigen, zu entlasten. Dabei existieren zwei Möglichkeiten: Erstens kann der Anwendungsfall CaaS auf einer dedizierten Plattform laufen und gemeinsam Ressourcen im Netzwerk teilen. Somit teilen sich mehrere Mandanten dieselbe CaaS Plattform. Zweitens kann der CaaS Server als VNF auf derselben Plattform implementiert werden und sich im gleichen Rechenzentrum befinden.	VNF Dienstleister können für andere Dienstleister Services, die Netzwerkfunktionen und Anwendungen unter Berücksichtigung des verschlüsselten Datenverkehrs thematisieren, bereitstellen.	Um die Funktionalitäten der VNFs zu nutzen, muss der verschlüsselte Datenverkehr zuerst entschlüsselt werden, damit die benötigten Daten bereitgestellt werden können.
	Security as a Service (SecaaS)	Aufgrund der zunehmenden Vernetzung und Internetabhängigkeit der Geräte wird sich die Situation von Cyberangriffen verschärfen, sodass die Sicherheit der Services und Daten gewährleistet werden muss. Eine Möglichkeit hierfür ist, Sicherheit als Service anzubieten, indem ein auf NFV Orchestrierung basierender Dienst bereitgestellt wird.	Jeder potentielle Sicherheitsanspruch stellt eine Möglichkeit zur Virtualisierung dar: <ul style="list-style-type: none"> <li>- Zutrittskontrolle</li> <li>- Anti-Malware</li> <li>- Datenschutz</li> <li>- Auditor</li> <li>- Netzwerküberwachung</li> <li>- Gesetze</li> </ul>	Zum einen kann die Leistungs-isolation zwischen Kunden ein Problem darstellen. Zum anderen ist es möglich, dass der Service nicht verfügbar ist, wenn dem Kunden an einem physischen Standort nicht genügend Ressourcen zugeordnet werden.



GLIEDERUNG	USE CASE	BESCHREIBUNG	VIRTUALISIERUNGSZIEL	HERAUSFORDERUNG(EN)
	Virtual Network Function as a Service (VNaaS)	Der Anbieter kann VNF Funktionalitäten für den Verbraucher bereitstellen, womit dieses Konzept dem Cloud Computing Konzept von Software as a Service ähnelt. Dabei ist zu berücksichtigen, dass die Verbraucher weder die VNF noch die NFVI kontrollieren.	Ziel ist es, eine Vielzahl an NF innerhalb des Enterprise Networks zu virtualisieren (z. B. Access Router, Provider Edge Router, Firewall etc.).	Um die virtualisierten Geräte zu managen, werden viele Ressourcen, die die NFVI bereitstellt, benötigt. Zudem muss sichergestellt sein, dass während eines Ausfalls der Netzwerkverbindung die Dienstkontinuität im Unternehmen gewährleistet ist.
	Virtual Network Platform as a Service (VNPaaS)	Der Dienstanbieter stellt eine Reihe von Infrastrukturen und Anwendungen zur Verfügung, auf der das Unternehmen seine Netzwerkanwendungen anbietet. Im Gegensatz zum VNaaS ist dieser Anwendungsfall umfangreicher, da nicht nur einzelne Funktionen, sondern ein virtuelles Netzwerk offeriert wird.	Mögliche Virtualisierungsziele sind alle Netzwerkfunktionen, die gemeinsam mit einem Drittanbieter genutzt werden.	Zum einen muss der Zugang zu den API Aufrufen durch autorisierte Benutzer realisiert werden. Zum anderen müssen die Infrastrukturressourcen Mechanismen bereitstellen, damit die Arbeitsauslastung zwischen verschiedenen Anbietern getrennt werden kann.
	VNF Forwarding Graphs	Der VNF Forwarding Graph definiert die Reihenfolge der NFs, in der Pakete versendet werden und stellt somit die logischen Verbindungen zwischen den virtuellen Anwendungen (VNFs) zur Verfügung. Die versendeten Pakete können entweder ein bestimmtes (z. B. Serverfunktionen) oder kein bestimmtes (z. B. Internet) Ziel verfolgen. Basiert der VNF Forwarding Graph auf bereits existierenden und verfügbaren Ressourcen, wird ein neuer VNF Forwarding Graph durch die Konfiguration eines neuen Satzes an Kapazitäten definiert. Andernfalls müssen neue Ressourcen, die einen spezifischen Lebenszyklusprozess durchlaufen, realisiert werden.	Der Netzwerkdienstleister muss die Zuordnung der benötigten PNF und VNF auf der zugrundeliegenden NFVI für den VNF Forwarding Graph bestimmen, um diese NF für den spezifischen Service zu konfigurieren und mithilfe der SDN Methoden zu steuern.	Um diesen Use Case zu verwirklichen, müssen die Serviceanbieter die Attribute und Eigenschaften von VNF Forwarding Graphs spezifizieren, sodass die gewünschten Kapazitäts- und Performanceanforderungen erfüllt werden. Hierfür ist die optimale Zuweisung der Ressourcen unerlässlich, die aus einem breiten Spektrum ausgewählt werden können, wodurch es möglich wird, eine Vielzahl an Netzwerkalternativen für die VNF Forwarding Graphs zu verwenden.
<b>Management &amp; Orchestrierung:</b>	Network Slicing	Dieser Use Case wurde bereits in Kapitel XX beschrieben.	Ziel ist es, mehrere logische Netzwerke auf einer gemeinsamen physischen Infrastruktur zu betreiben. Dafür können Netzwerkfunktionen, die den Netzwerk Slice bilden, oder das Netzwerk Slice Management und Orchestrierungseinheiten virtualisiert werden.	Es werden keine Herausforderungen explizit erwähnt.

GLIEDERUNG	USE CASE	BESCHREIBUNG	VIRTUALISIERUNGSZIEL	HERAUSFORDERUNG(EN)
	VNF composition across multiple administrative domains	Um die Kundenanforderungen zu erfüllen, müssen die VNFs in verschiedenen administrativen Bereichen orchestriert werden. Dafür muss der Anbieter unterschiedliche Zugriffs-, Steuerungs- und Managementfunktionen zusammenstellen (bzw. von anderen Anbietern mieten), um den End-to-End Service zu gewährleisten.	Jede Funktion, die der Kunde für die Bereitstellung von Diensten benötigen könnte, kann virtualisiert werden.	Einige potentielle Herausforderungen sind: - Es existieren fehlende Schnittstellen, um Aktionen an die gemieteten VNFs weiterzuleiten. - Der Lebenszyklus von VNFs und anderen Ressourcen aus getrennten Verwaltungsbereichen muss koordiniert und gemanagt werden.
<b>Services für den Endkunden:</b>	Virtualisation of the Home Environment	Um Heimdienste zu verwirklichen, stellen Netzwerkbetreiber Backend-Systeme und Customer Premises Equipment (CPE) Geräte bereit. Diese CPE Geräte beinhalten eine Residential Gateway (RGW) für beispielsweise Internetdienste sowie eine Setup-Box (STB) für Mediendienste, die virtualisiert werden können. Vorteilhaft daran wäre, dass die neu eingeführten Dienste unabhängig von den physischen CPEs wären und dass die Installation neuer Geräte vermieden wird.	Es werden die RGW und STB virtualisiert. Dieses Virtualisierungsziel ermöglicht viele neue Anwendungen und Bereitstellungskombinationen. Hierbei ist zu berücksichtigen, dass virtualisierte und nicht virtualisierte Heimgeräte koexistieren müssen.	Problematisch könnte beispielsweise sein, dass eine erhebliche Rechenleistung der NFV-Infrastruktur benötigt wird, um Mediendienste zu virtualisieren, oder dass gestreamte Inhalte zu Hause verschlüsselt werden müssen.
	Virtualisation of Internet of Things (IoT)	Das Internet der Dinge ermöglicht es, physische und virtuelle Geräte miteinander zu vernetzen, sodass diese miteinander kommunizieren können (vgl. Massive Machine Type Communication). Dadurch entsteht eine Vielzahl an neuen Anwendungsfällen, wie Smart Cities/Homes sowie Smart Wearables oder ehealth etc.. Jede dieser Anwendungsfälle erfordert eine andere Kombination von Netzwerkreisourcen und Funktionen.	Alle traditionellen Netzwerkfunktionen (Authentifizierung, Speicher, Konnektivität etc.), die benötigt werden, um IoT zu ermöglichen, können virtualisiert werden. Die Zugangs- und Kontrollinterfaces der IoT- Geräte eignen sich besonders gut für die Virtualisierung.	Zum einem müssen die Vorschriften zur Datenkontrolle und Verarbeitung eingehalten werden, zum anderen können verschiedene Nutzer zeitgleich auf Ressourcen zugreifen.
	Virtual Content Delivery Network (vCDN)- Fulfillment	Durch Streaming Dienste, Live Videos etc. nimmt der Datenverkehr mit hoher Bandbreite weiter zu. Aus diesem Grund werden Content Delivery Networks (CDNs) in die Betreiber-netzwerke integriert. Dies bedeutet, dass Inhaltströme von Speicherknoten in der geografischen Nähe des Endkunden bereitgestellt werden sollen. Somit stellen die CDN Knoten in der aktuellen Implementierung dedizierte physische Geräte oder Software mit spezifischen Anforderungen dar. Durch die Virtualisierung dieser CDN Knoten sollen die Ressourcen effizienter genutzt und Flexibilität ermöglicht werden.	Als Reaktion auf eine Kundenanfrage soll ein virtualisiertes CDN eingerichtet werden. Dazu zählt auch der CDN Controller.	Es gilt zu berücksichtigen, dass die benötigten Ressourcen verschiedenen Arten von VNFs zugeordnet werden und die Gesamtkapazität auf mehrere VNFs verteilt wird. Daraus ergibt sich, dass die Zuweisung der Ressourcen für verschiedene Parteien harmonisiert und gemanagt werden muss.

GLIEDERUNG	USE CASE	BESCHREIBUNG	VIRTUALISIERUNGSZIEL	HERAUSFORDERUNG(EN)
<b>Testen &amp; Entwickeln:</b>	Rapid Service Deployment	Dieser Anwendungsfall thematisiert die übergeordneten NFV-Ziele. Durch die softwarebasierte Bereitstellung und Operationalisierung von Netzwerkfunktionen und Endgeräten werden schnelle Service Innovationen ermöglicht.	Das Virtualisierungsziel ist Service abhängig.	Es muss eine Methode entwickelt werden, die erkennt, dass eine neue Dienstinstanz betriebsbereit ist.
	Devops/CI/CD	Dieser Use Case beschreibt einen Mechanismus, um zu prüfen, ob die vorgeschlagenen Systeme die Ziele auf Unternehmensebene erfüllen. Hierfür ist es hilfreich, Software mit einer agilen Methodik zu entwickeln.	Dieser Prozess gilt für mehrere Virtualisierungsziele.	Es wird ein Verfahren benötigt, das Softwarefehler identifiziert und an die nächsthöhere Instanz weitergeben kann.
	A/B testing	Mithilfe von A/B testing kann die Leistung zweier Alternativen bestimmt werden, sodass die bessere Alternative hinsichtlich vordefinierter Kriterien identifiziert wird.	Das Virtualisierungsziel ist Service abhängig.	Das Leistungsziel sollte für die beiden Services, die miteinander verglichen werden, gleich sein. Diese Leistungsziele können entweder kundenorientiert oder operationalisiert sein.

## Fazit 05

5G ist mit einer neuen Architektur und der konsequenten Umsetzung von Virtualisierung mehr als nur ein Performance-Update vorheriger Mobilfunkstandards. Mit 5G wird das Netz zur universell programmierbaren Infrastruktur, die neben Kommunikation auch Speicher- und Rechenressourcen dynamisch zur Verfügung stellt. Die Vorteile des Cloud Computing werden somit nicht nur im Rechenzentrum, sondern entlang des gesamten Netzes nutzbar. 5G ist damit nicht nur eine Zugangstechnologie.

Die erforderlichen Standardisierungsprozesse laufen bereits. Nach erfolgreichem Abschluss hat 5G das Potential, eine verstärkte Nutzung einer solchen Infrastruktur, ähnlich wie beim klassischen Cloud Data Center, zu bewirken und einen Innovationsschub bei der Umsetzung neuer digitaler Geschäftsmodelle, wie beispielsweise Pay-per-Use Modelle für Roboter, auszulösen. Die automatisierte Orchestrierung als ein zentrales Merkmal eines modernen 5G Netzwerks bietet darüber hinaus die Chance, in Zukunft zu einer erhöhten Flexibilität auch auf der Anwendungsebene in Bezug auf die schnelle Implementierung von neuen Anwendungen zu führen. Die hochautomatisierte Bereitstellung und der Betrieb von Diensten ermöglicht in der Softwareentwicklung, Software in Form kleiner, abgeschlossener Dienste (Microservices) zu gestalten, um komplexere Anforderungen mit Hilfe einer Komposition aus diesen Diensten zu erfüllen.

5G gestattet eine Realisierung dieses Ansatzes auch im industriellen Kontext. Zwingende Voraussetzung hierfür ist allerdings, dass sich die Hersteller auf gemeinsame Standards über alle Dienstbereiche hinweg einigen und nicht auf proprietäre Schnittstellen setzen. Zusätzlich ist ein einfacher Zugang mittels offenerer Schnittstellen über SDKs nötig, die das Potential der gesamten 5G Infrastruktur für die Anwendungsebene nutzbar machen. Unter diesen Voraussetzungen ist ein ähnlicher Siegeszug wie beim Industrie-PC möglich.

- [1] White Paper 5G Lean Industrial Communication, Version 1.1, Michael Kemkes, Thomas Mager, Dr. Simon Oberthür, Dr. Gunnar Schomaker, Dr. Lutz Stobbe, <https://www.ip45g.de/white-paper/>
- [2] White Paper 5G Charakterisierung, Version 1.1, Dr. Lutz Stobbe, Michael Kemkes, Thomas Mager, Dr. Simon Oberthür, Dr. Gunnar Schomaker, <https://www.ip45g.de/white-paper/>
- [3] Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV, ETSI GS NFV 003 V1.4.1
- [4] 5G Architecture White Paper, Version 2.0, 5GPPP Architecture Working Group
- [5] Network Functions Virtualisation (NFV); Infrastructure Overview; ETSI GS NFV-INF 001 V.1.1.1
- [6] Network Functions Virtualisation – White Paper on NFV priorities for 5G; ETSI NFV ISG; [http://portal.etsi.org/NFV/NFV\\_White\\_Paper\\_5G.pdf](http://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf)
- [7] Network Functions Virtualisation – Introductory White Paper; ETSI [http://portal.etsi.org/NFV/NFV\\_White\\_Paper.pdf](http://portal.etsi.org/NFV/NFV_White_Paper.pdf)
- [8] Network Functions Virtualisation (NFV); Use Cases; ETSI GR NFV 001, Version 1.2.1
- [9] Network Functions Virtualisation (NFV); Use Cases; ETSI GS NFV 001, Version 1.1.1
- [10] NIST SP-800-145 (September 2011): »The NIST Definition of Cloud Computing«, Peter Mell and Timothy Grance, US National Institute of Standards and Technology.
- [11] The Industry Impact of 5G – Insights from 10 sectors into the role of 5G, Ericsson, 2018.

<b>[API]</b>	Application Programming Interface
<b>[BBU]</b>	Base Band Unit
<b>[CaaS]</b>	Crypto as a Service
<b>[CD]</b>	Continuous Deployment
<b>[CDN]</b>	Content Delivery Network
<b>[CI]</b>	Continuous Integration
<b>[CPE]</b>	Customer Premises Equipment
<b>[C-RAN]</b>	Cloud Radio Access Network
<b>[eNodeB]</b>	Evolved Node B
<b>[eMBB]</b>	Enhanced Mobile Broadband
<b>[ETSI]</b>	European Telecommunications Standards Institute
<b>[IaaS]</b>	Infrastructure as a Service
<b>[IMS]</b>	IP Multimedia Subsystem
<b>[IIoT]</b>	Industrial Internet of Things
<b>[MAC]</b>	Media Access Control
<b>[mMTC]</b>	Massive Machine Type Communication
<b>[NF]</b>	Network Function
<b>[NFVI]</b>	Network Functions Virtualisation Infrastructure
<b>[NFVaaS]</b>	Network Functions Virtualisation Infrastructure as a Service
<b>[NGN]</b>	Next Generation Network
<b>[NS]</b>	Network Service
<b>[PNF]</b>	Physical Network Function
<b>[RAN]</b>	Radio Access Network
<b>[RGW]</b>	Residential Gateway
<b>[RRC]</b>	Radio Resource Control
<b>[SecaaS]</b>	Security as a Service
<b>[SDN]</b>	Software Defined Networks
<b>[SLA]</b>	Service Level Agreement
<b>[STB]</b>	Set-top-Box
<b>[Telcos]</b>	Telekommunikationsanbieter
<b>[uRLLC]</b>	Ultra Reliable Low Latency
<b>[VNF]</b>	Virtual Network Function
<b>[VNFaaS]</b>	Virtual Network Function as a Service
<b>[VNPaaS]</b>	Virtual Network Platform as a Service



