Security-Herausforderungen in industriellen Netzen

Dirk Kretzschmar
Member Group Executive Committee TÜV NORD GROUP
CEO TÜViT
Managing Director
TÜV Informationstechnik GmbH

Hannover, September 2nd, 2020

TÜViT®
TÜV NORD GROUP

5G Modell

Mobilfunkbetreiber (MNO)

Nutzer/Infrastruktur Betreiber

Mobilfunkbetreiber

3GPP A GLOBAL INITIATIVE

Nationale/Internationale Netzagentur

Remote Service Providers

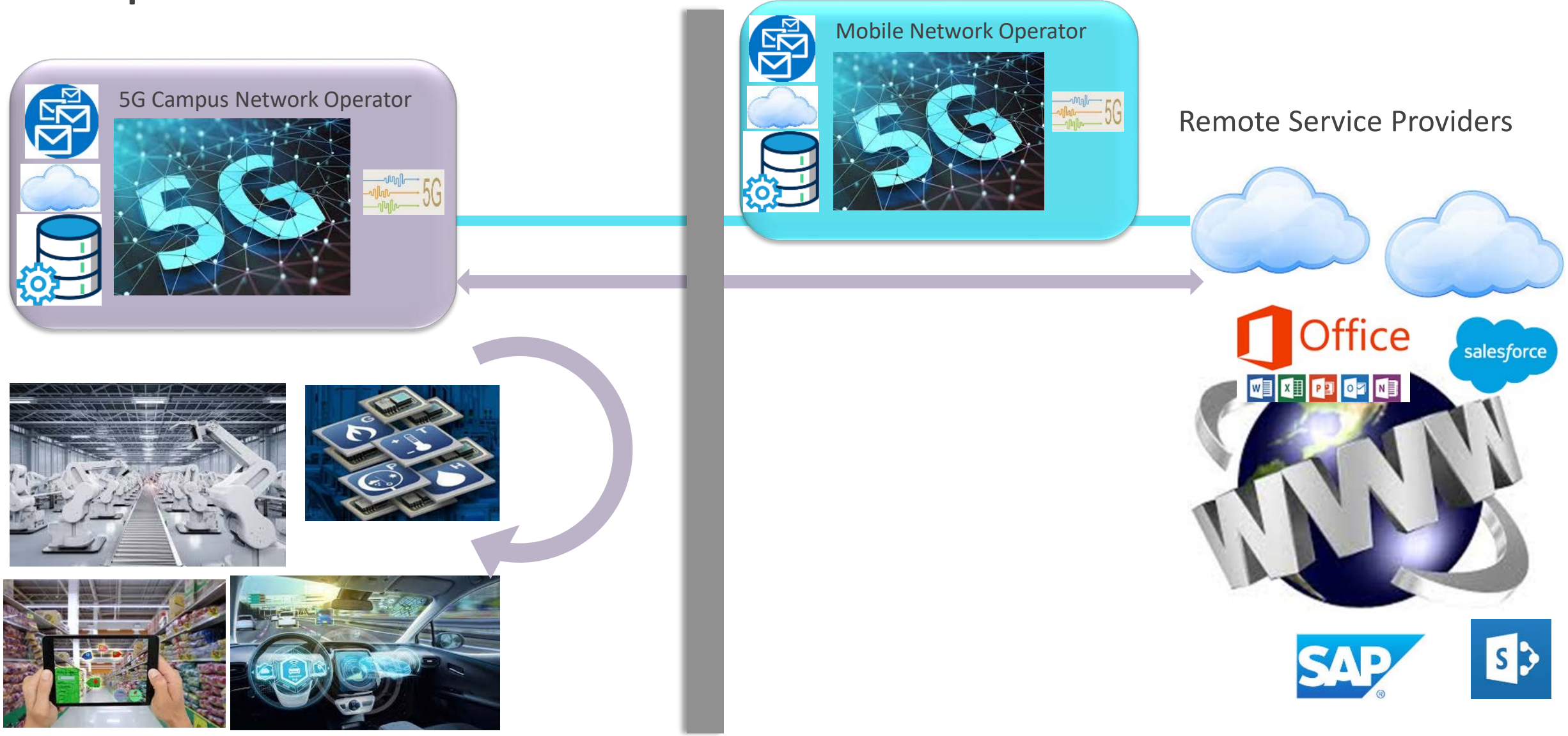
Office

salesforce

SAP

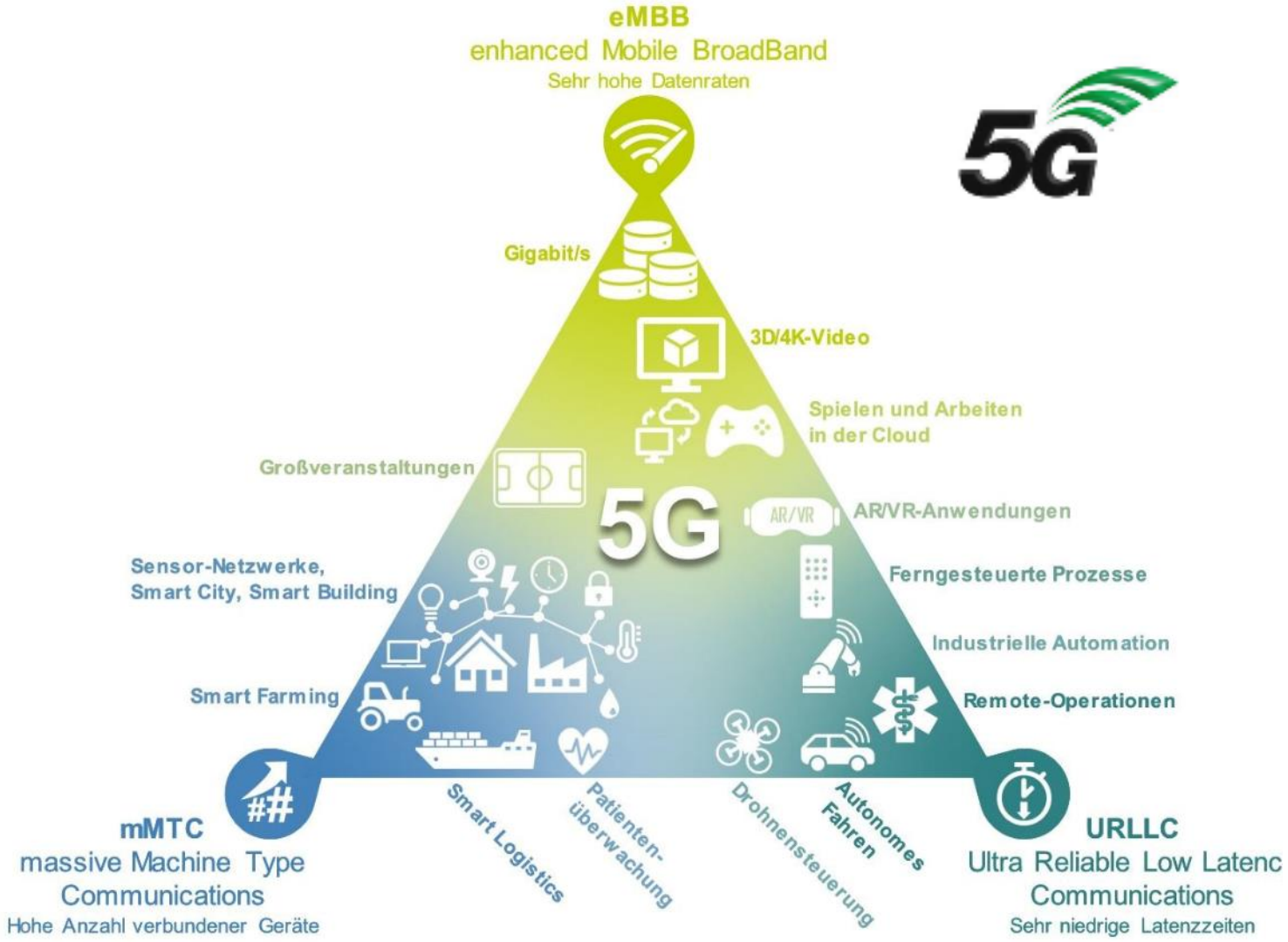
Anwender / Service Provider Policies

5G Campus Modell



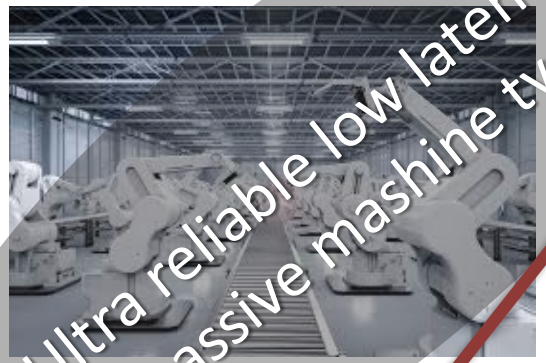
Was ist neu an 5G?

Die Vielfalt der Anwendungen

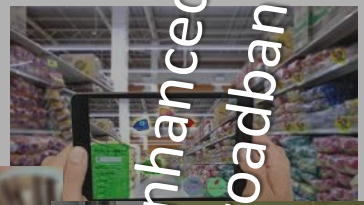


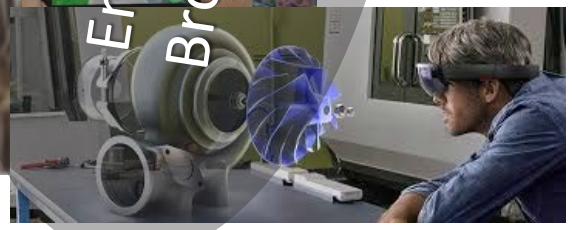
5G Network Slicing

Security



Ultra reliable low latency
+ massive mashine type





Enhanced mobile
Broadband (eMB)

Real time Traffic

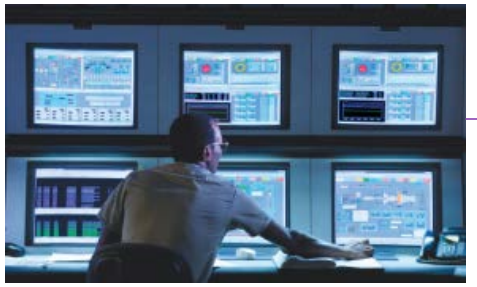
Massive mashine type
Traffic

5G Campus
Anwendungen

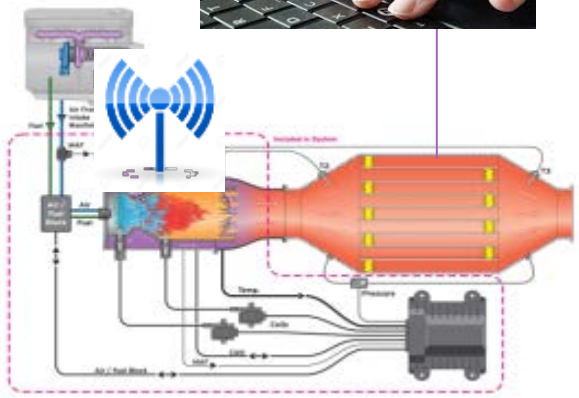
Quelle: BOSCH

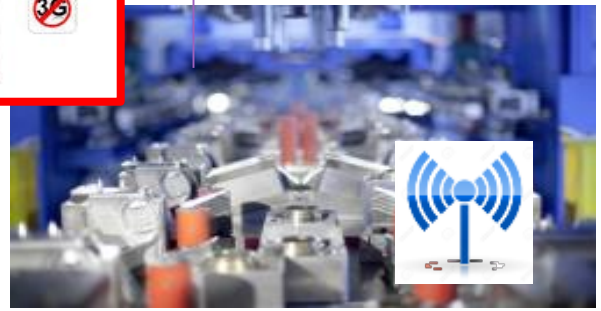
Images: Bosch

Industrial Security



5G Campus Network Operator





Vorteile der Mobilfunktechnologie, insbesondere 5G

Etablierte Massentechnologie (2Mrd Smartphones/Jahr)

Extrem hohes Qualitätsniveau in Standardisierung, Prozessen, Interoperabilität

Spektrum ist international standardisiert

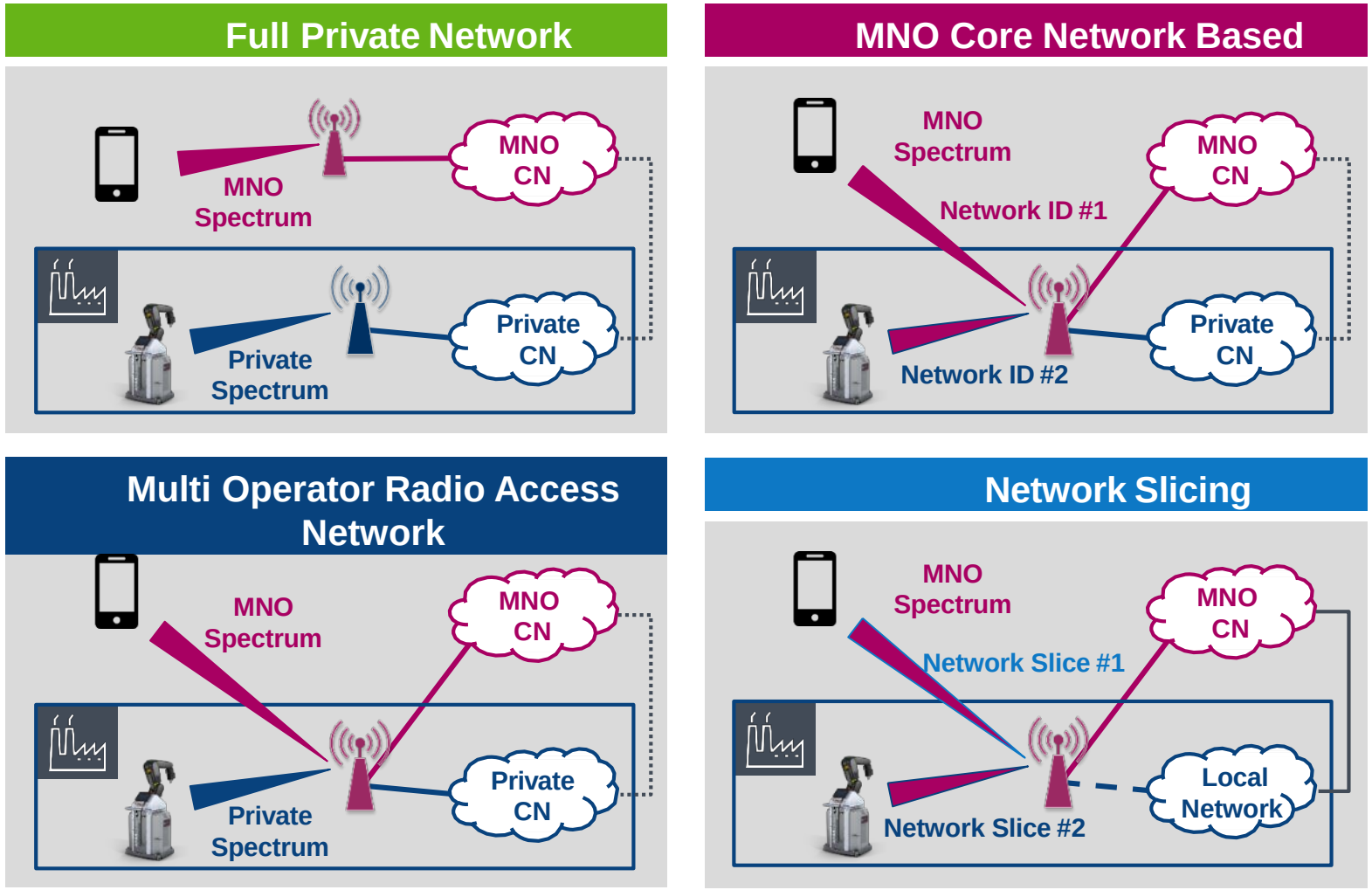
durchgängiges Sicherheitskonzept

Endgerätemanagement (Authentisierung, Autorisierung, (Accounting)

Netzgesteuerter Handover

Dienstgütemanagement

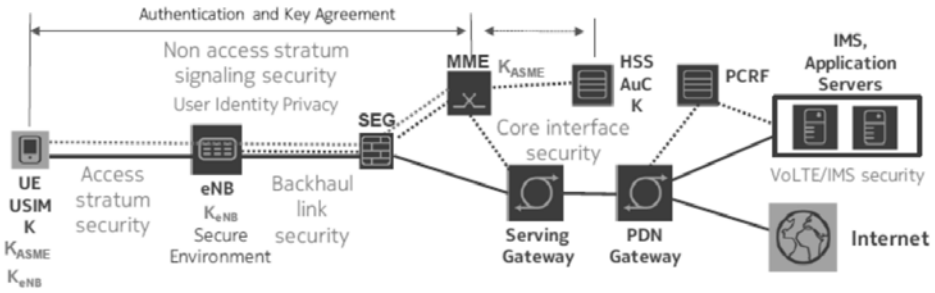
Verschiedene Optionen für Private 5G Campus Netze (Beispiele)



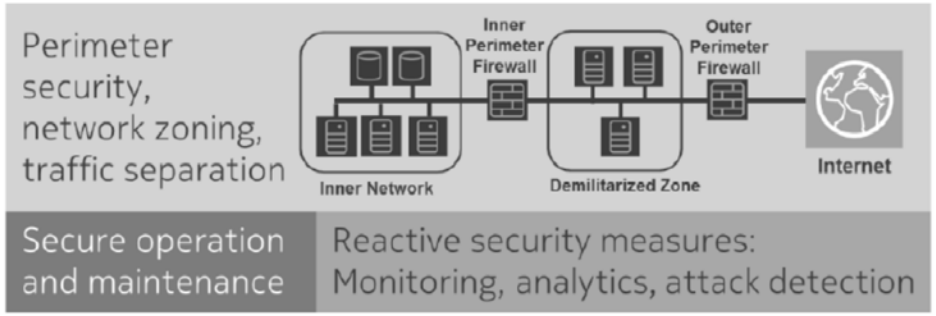
Mobilfunknetz Security heute

Beispiel LTE (4G)

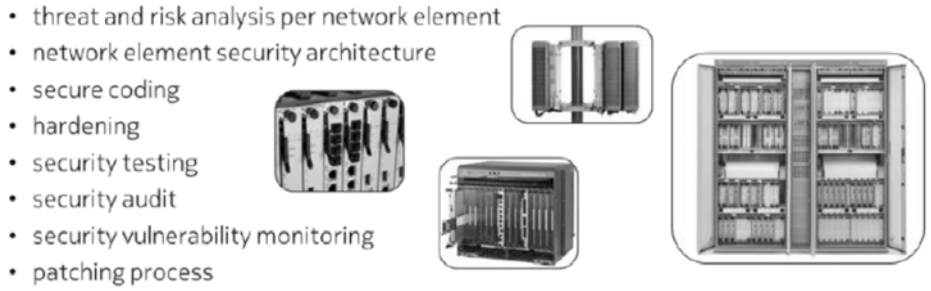
3GPP-specified security architecture



Network security not specified by 3GPP



Network element security measures

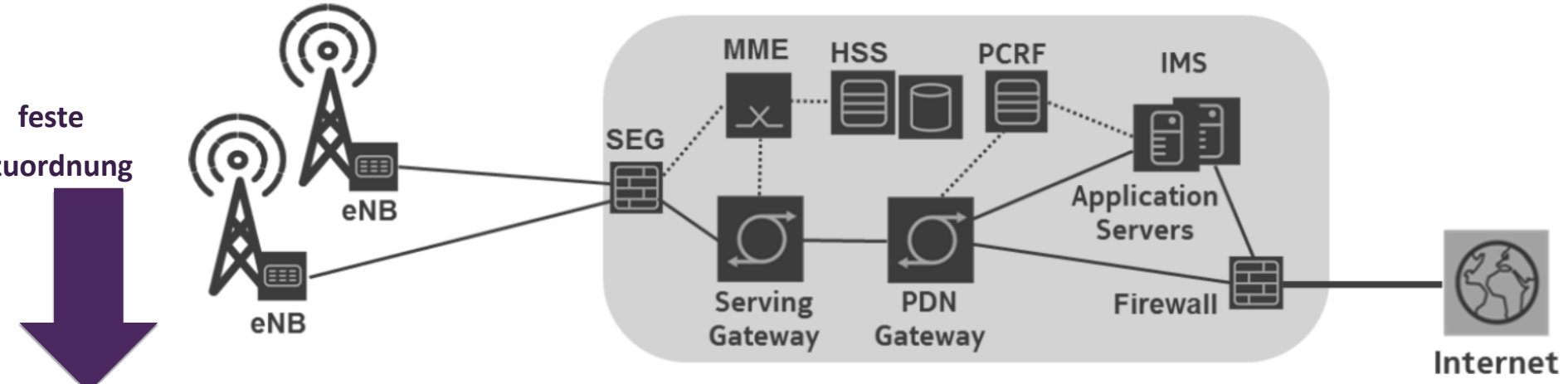


Source: Nokia

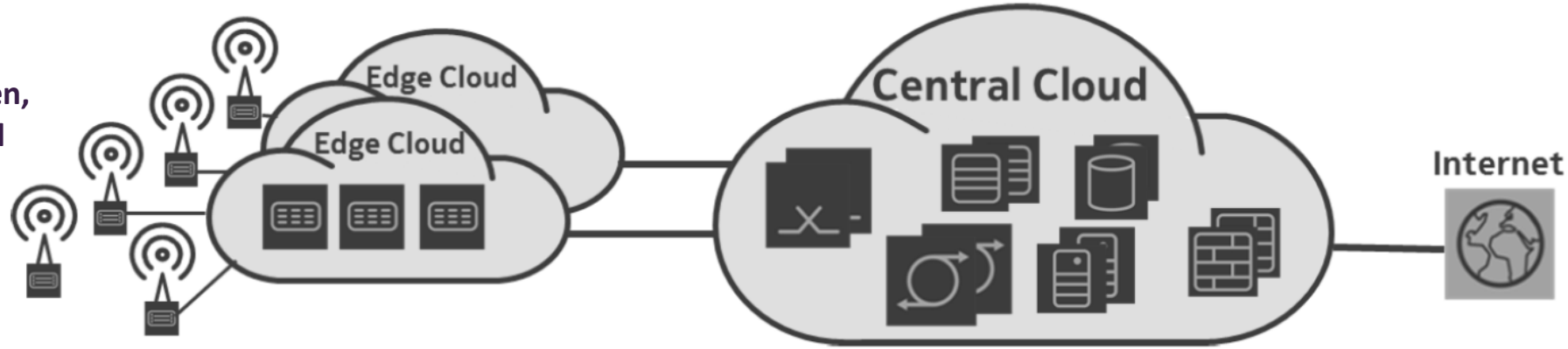
Von LTE (4G) zu 5G

Einführung der Virtualisierung

LTE feste Funktionszuordnung

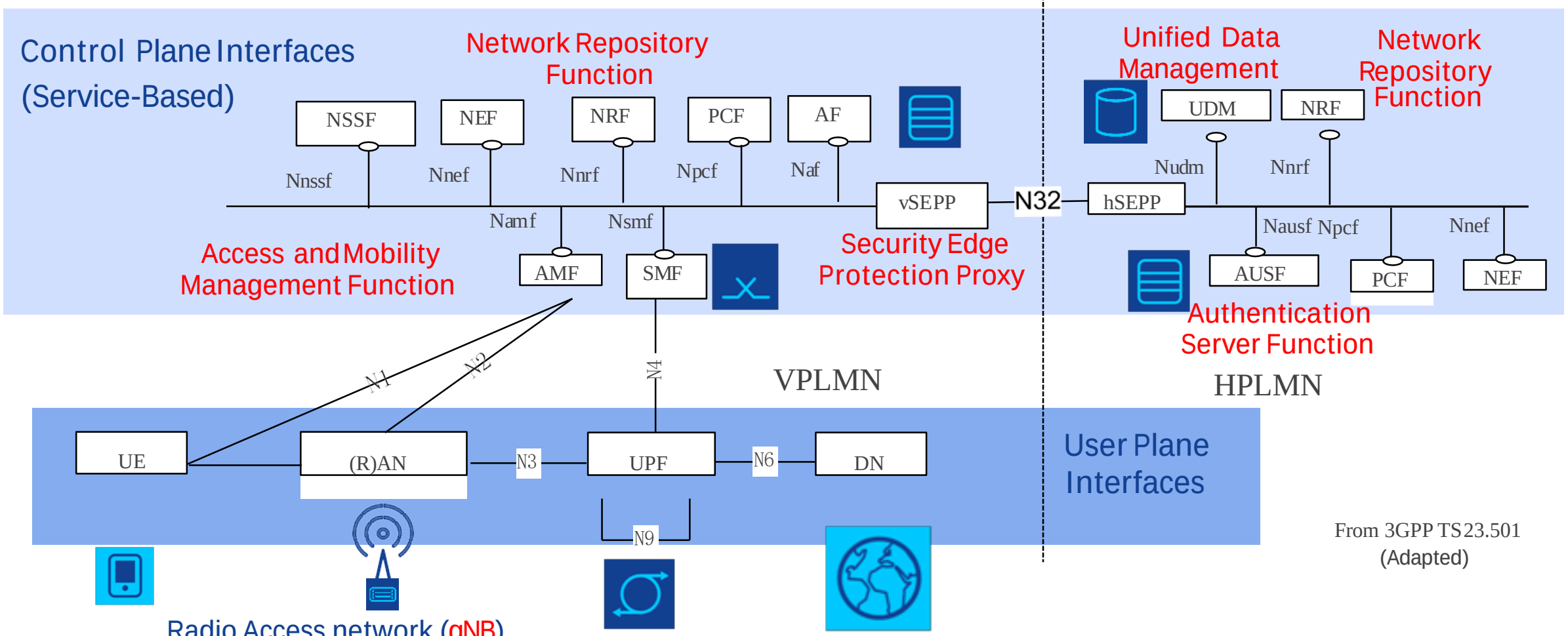


5G virtuelle Funktionen, Software Defined Networking



Source: Nokia

Kritische Security Funktionen entsprechend 3GPP in 5G Systemen



From 3GPP TS23.501 (Adapted)

Red: Functions crucial for the security architecture

Quelle

5G

01.09.2020 14:30

Telefónica verlegt sein 5G-Kernnetz in die Cloud

Telefónica arbeitet mit Amazon und Ericsson zusammen, um sein 5G-Kernnetz in die Cloud zu verlegen. Wir berichten darüber, welche Vorteile diese Lösung mit sich bringt.

Von Markus Weidner

Kommentare (7) A A A Teilen (7)

5G-Kernnetz von o2 wandert in die Cloud
Foto: iStock / Getty Images / B4LLS via Telefónica

Telefónica hat als einziger der drei bereits aktiven deutschen Mobilfunk-Netzbetreiber sein 5G-Netz für Endverbraucher noch nicht gestartet. Als Vodafone und Telekom im Sommer 2019 ersten Endkunden den neuen Netzstandard schmackhaft machen wollten, setzte der Münchner Konzern zunächst auf 5G-Lösungen für die Industrie.

Jetzt hat Telefónica angekündigt, als erster deutscher Netzbetreiber das 5G-Kernnetz sowie grundlegende Funktionen des neuen Netzstandards für Industrielösungen in die Cloud zu verlegen. Dadurch sei es nicht nur möglich, Projekte für Firmen schneller zu entwickeln. Zudem könnten Produktions- und Logistikprozesse stärker automatisiert und Anwendungen in Echtzeit realisiert werden.

Der Münchner Mobilfunk-Netzbetreiber will für die Virtualisierung seines 5G-Kernnetzes auf die Cloud-Infrastruktur von Amazon Web Services zurückgreifen. Zudem setzt der Konzern auf 5G-Netzkomponenten und -funktionen des schwedischen Telekommunikationsausrüsters Ericsson. Noch im September soll die Virtualisierung des 5G-Kernnetzes starten. Dazu startet o2 mit der Implementierung von 5G-Netzfunktionen für erste ausgewählte Partner in der Industrie.

Markus Haas: "Fundament für die digitale Transformation der Wirtschaft"

"Mit der Virtualisierung unseres 5G-Kernnetzes legen wir das Fundament für die digitale Transformation der deutschen Wirtschaft. Die Kooperation mit Amazon Web Services ist ein wichtiger Teil unserer Strategie für den Aufbau industrieller 5G-Netze", sagt Markus Haas, CEO von Telefónica Deutschland.

Netzab

Übersicl
Telekon
Vodafon
o2 (Tele

Messer

Nichts verp
Messenger
Kommunik
Übersicl
WhatsA
Skype
Faceboo
Threem
Telegra
Übersicl

Werbur

Pressemitteilung vom 01.09.2020

Kooperation mit Amazon Web Services und Ericsson ermöglicht neue 5G-Industrielösungen

Telefónica Deutschland/O2 bringt 5G-Kernnetz in die Cloud (FOTO)

Düsseldorf (ots) - Als erster deutscher Netzbetreiber wird Telefónica Deutschland / O2 das 5G-Kernnetz sowie grundlegende 5G-Netzfunktionen für neue Industrielösungen in die Cloud bringen. Über das cloudbasierte 5G Kernnetz lassen sich neue Industrielösungen schneller entwickeln, Produktions- und Logistikprozesse noch stärker automatisieren und Anwendungen in Echtzeit (Edge Computing) realisieren. Für die Virtualisierung seines 5G-Kernnetzes wird Telefónica Deutschland / O2 die Cloud-Infrastruktur von Amazon Web Services (AWS) nutzen. Zudem setzt das Unternehmen auf 5G-Netzkomponenten und -funktionen des schwedischen Telekommunikationsausrüsters Ericsson.

"Mit der Virtualisierung unseres 5G-Kernnetzes legen wir das Fundament für die digitale Transformation der deutschen Wirtschaft. Die Kooperation mit Amazon Web Services ist ein wichtiger Teil unserer Strategie für den Aufbau industrieller 5G-Netze", sagt Markus Haas, CEO von Telefónica Deutschland / O2.

Layer der Mobilfunknetz Security in einem 3GPP 5G System

3GPP-spezifizierte Security Architektur	Neues Framework für die zugangs-agnostische Authentifizierung Erweiterter Schutz der Privatsphäre der Nutzer EAP-basierte "sekundäre Authentifizierung" Sicherheit für service based Schnittstellen Verbesserungen für die Verbindungssicherheit
Network Security <u>nicht</u> durch 3GPP spezifiziert	Perimeter-Sicherheit und Verkehrsfilterung durch virtuelle Firewalls Logisch oder sogar physisch getrennte Sicherheitszonen Verkehrsseparierung durch VLANs und Wide Area VPNs Ganzheitliches, automatisiertes Sicherheitsmanagement Automatisierte, adaptive, intelligente Sicherheitssteuerung
Virtual Network Function (VNF) Security Telco Cloud Security	Solide, robuste Implementierungen der Virtualisierungsschicht (z.B. Hypervisor) und der gesamten Cloud-Plattform-Software Solide, robuste Implementierung der VNFs Integritätsschutz sowohl für Plattform und VNFs

Quelle NOKIA Bell Labs

TÜVIT®

Elements of the 5G Security Architecture (3GPP)

Authentication/authorization, key agreement

- Security negotiation, key hierarchy
- Enhanced control plane robustness
- Enhanced subscription privacy

Edge Cloud

NFV (network function virtualization)
SDN (software defined network) security

Security assurance for NFV environments

Security management and orchestration

Network slicing security

Self-adaptive, intelligent security controls

Central Cloud

- Subscriber/device
- identifiers/credentials
- Secure Hardware

- Crypto algorithms
- Physical layer Security
- Jamming protection

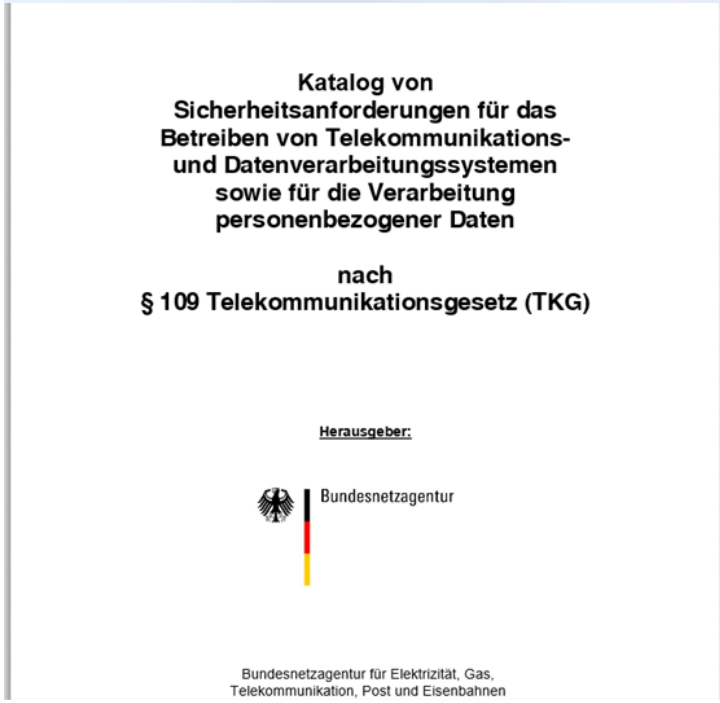
Bundesnetzagentur aktualisiert den Katalog von Sicherheitsanforderungen nach TKG §109

1 Kritische Funktionen und Komponenten

Kritisch sind Funktionen insbesondere dann, wenn eine technische Kompromittierung zu

- erheblichen Datenschutzverletzungen,
- systematischer Ausforschung des Fernmeldeverkehrs oder
- beträchtlichen Sicherheitsverletzungen nach § 109 Abs. 5 TKG

führt oder führen kann. Die Kritikalität einer Komponente ist dabei jeweils durch diejenigen ihrer Funktionen oder Teilfunktion begründet, die das Potential besitzen, bei Versagen oder nicht sachgerechter Realisierung, eine technische Kompromittierung herbeizuführen. Ist die Realisierung einer solchen Funktion auf mehrere Komponenten verteilt, so ist von der Kritikalität aller dieser Komponenten auszugehen. Dabei ist es grundsätzlich unerheblich, ob Funktionen durch Hard- und/oder Software realisiert werden.


Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten

nach
§ 109 Telekommunikationsgesetz (TKG)

Herausgeber:

Bundesnetzagentur

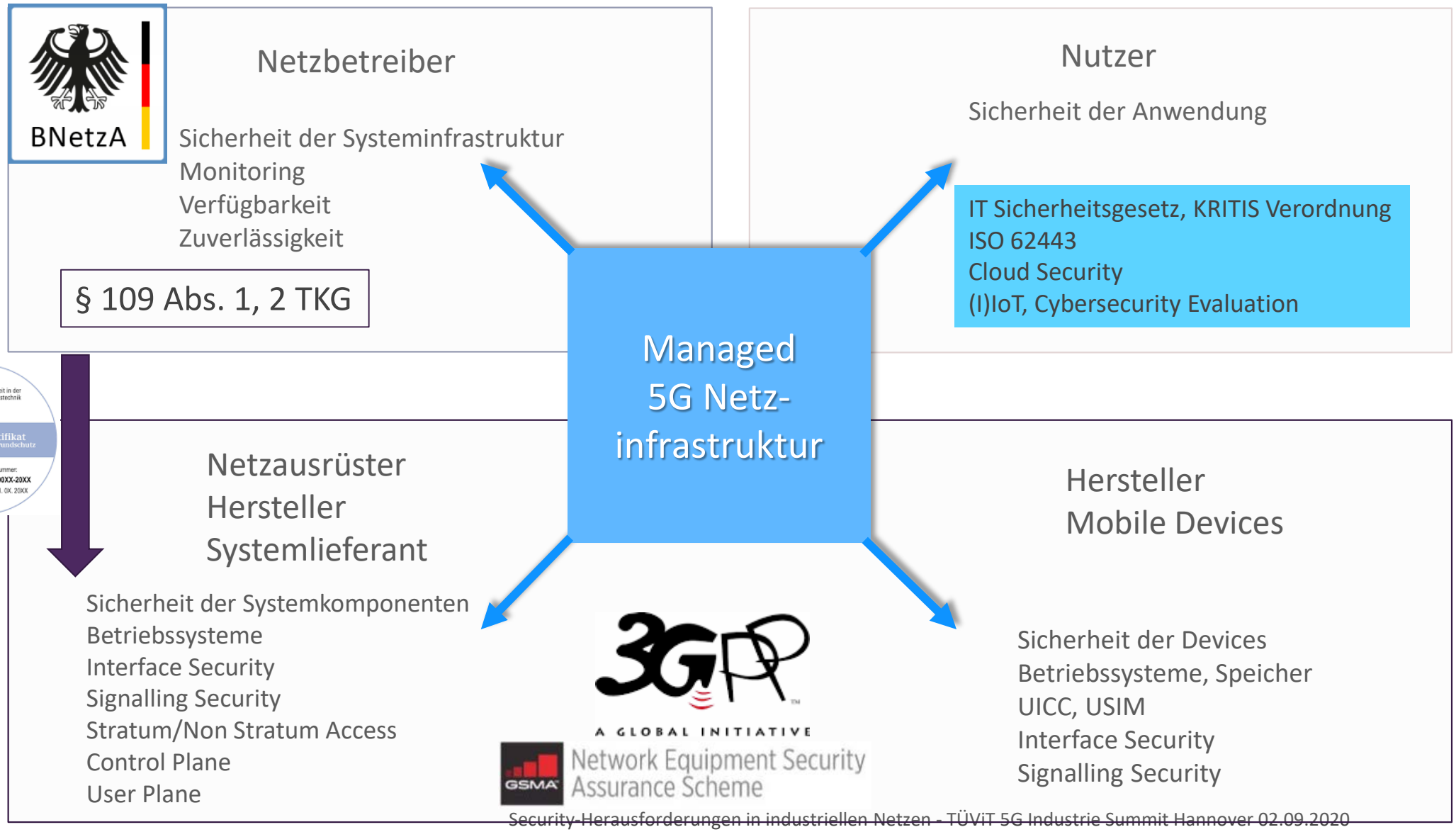
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bundesnetzagentur aktualisiert den Katalog von Sicherheitsanforderungen

§109 TKG (Telekommunikationsgesetz)

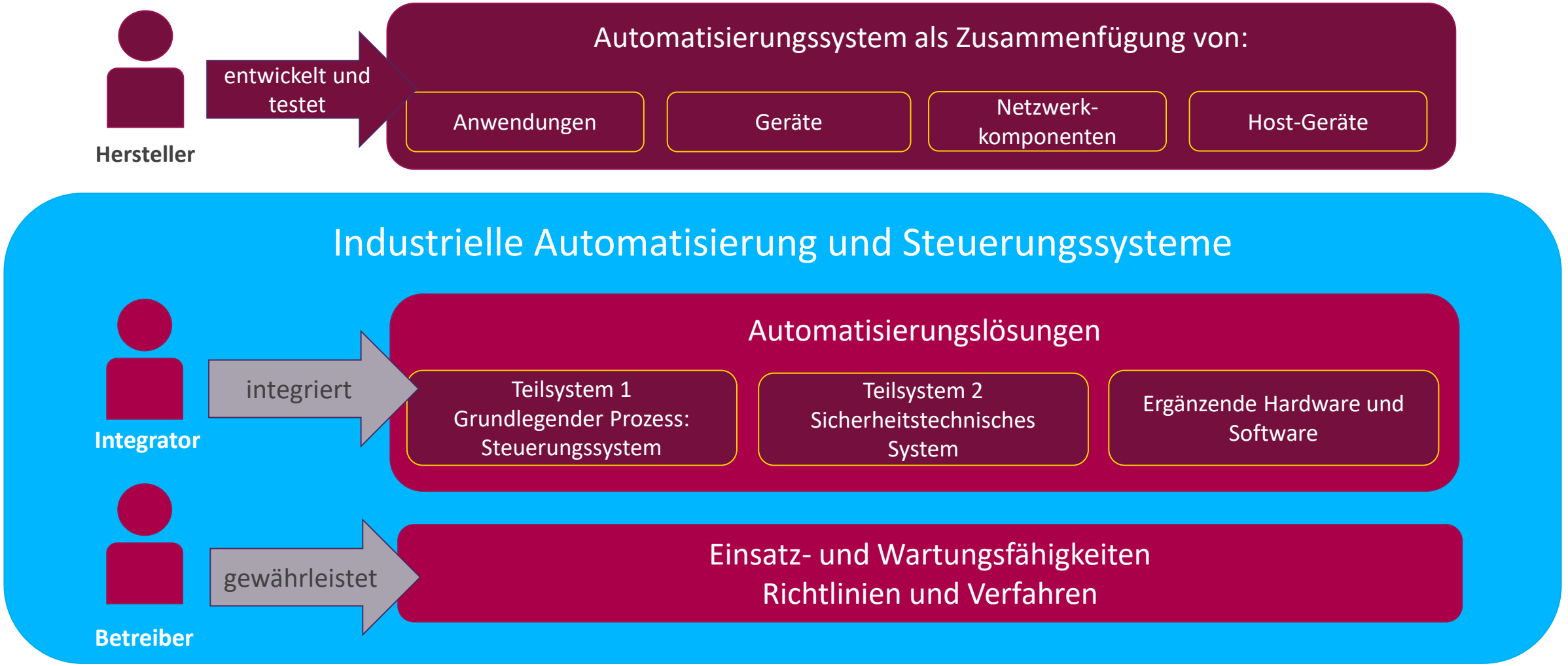
- Beobachtung des Netzverkehrs und geeignete Maßnahmen zum Schutz ergreifen
- Ausschließlich Einsatz sicherheitsrelevanter Netz- und Systemkomponenten (kritische Kernkomponenten) die vom BSI zertifiziert wurden
- Notwendigkeit des Einsatzes von Fachpersonal mit Systemkenntnissen
  Personal ist in ausreichendem Umfang vorzuhalten
- Nachweis des Einsatzes geprüfter HW und Quellcodes am Ende der Lieferkette
- Sicherstellen des Einsatzes von Netz- und Systemkomponenten unterschiedlicher Hersteller
- Vorhalten ausreichender Redundanzen für kritische Kernkomponenten

Complex 5g Security Targets ecosystem



IEC 62443 für 5G Campus Netze?

Definierte Rollen



Übersicht IEC 62443

IEC 62443 Normreihe

Allgemein	Management System	Industrielle IT Sicherheit (IACS)	Eingebettete Sicherheitskomponenten
Dieser Bereich definiert die Begriffe, Definitionen, Glossare und Konzepte, die in der Reihe IEC 62443 verwendet werden.	Dieser Bereich definiert die Anforderungen für die sichere Umsetzung des Managementprozesses und den sicheren Integrationsprozess einer Lösung in der Prozessindustrie.	Dieser Bereich definiert die Anforderungen an die Sicherheit von industriellen Systemen oder Lösungen, z.B. SCADA-Systemen.	Dieser Bereich definiert die Anforderungen an die Sicherheit von industriellen Komponenten, z.B. Firewalls

IEC 62443 für 5G Campus Netze?

Übersicht IEC 62443

IEC 62443 Normreihe

Allgemein	Management System	Industrielle IT Sicherheit (IACS)	Eingebettete Sicherheitskomponenten
1-1 Terminologie, Konzepte & Modelle	2-1 Einrichtung eines IACS-Sicherheitsprogramms	3-1 Sicherheits-technologien für IACS	4-1 Anforderungen an die Produktentwicklung
1-2 Glossar der Begriffe und Abkürzungen	2-2 Betrieb eines IACS-Sicherheitsprogramms	3-2 Sicherheitsrisiko-bewertung und Systementwurf	4-2 Technische Sicherheits-anforderungen für IACS-Komponenten
1-3 Metriken zur Einhaltung der Systemsicherheit	2-3 Patch Management in der IACS-Umgebung	3-3 Systemsicherheits-anforderungen und Sicherheitsstufen	
	2-4 Anforderungen für Anbieter von IACS-Lösungen		

Legende

- Noch nicht veröffentlicht und zertifizierbar
- Veröffentlicht, noch nicht zertifizierbar
- Veröffentlicht und zertifizierbar

MATURITY LEVEL UND SECURITY LEVEL

Maturity Level

- basieren auf dem Modell der Capability Maturity Model Integration (CMMI)
- zeigen die Optimierung von Prozessen
- Mittel zur Verbesserung des Prozesses

Security Level

- Messen der Wirksamkeit von Gegenmaßnahmen und den Sicherheitseigenschaften der Vorrichtungen und Systeme
- basierend auf der Risikobewertung für die Zone

Messbarkeit und Güte der Prozesse bzw. Maßnahmen

MATURITY LEVEL & SECURITY LEVEL ROLLEN

Maturity Level

- Hersteller
- Integrator
- Betreiber

Security Level

- Hersteller
- Integrator

Maturity Level & Security Level

Gegenüberstellung

Maturity Level

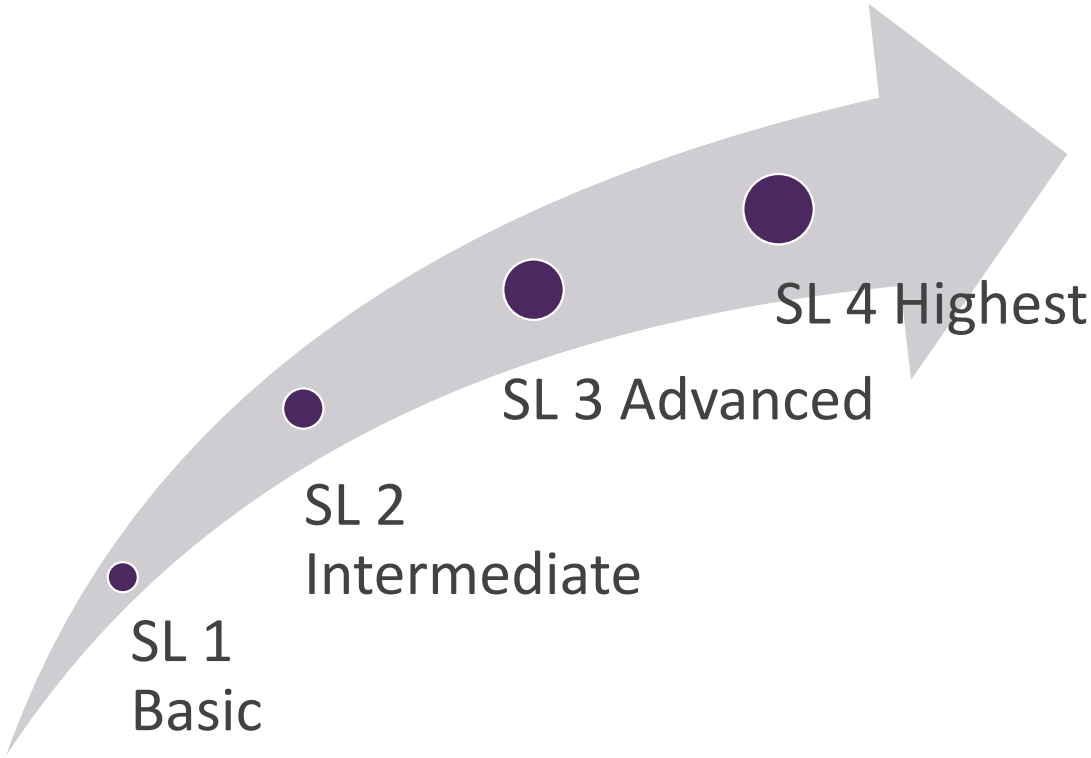
- bezieht sich auf Prozesse
- besteht aus 4 Level
- Die Level bauen sich aufeinander auf
- die Level zeigen die Optimierung von Prozessen

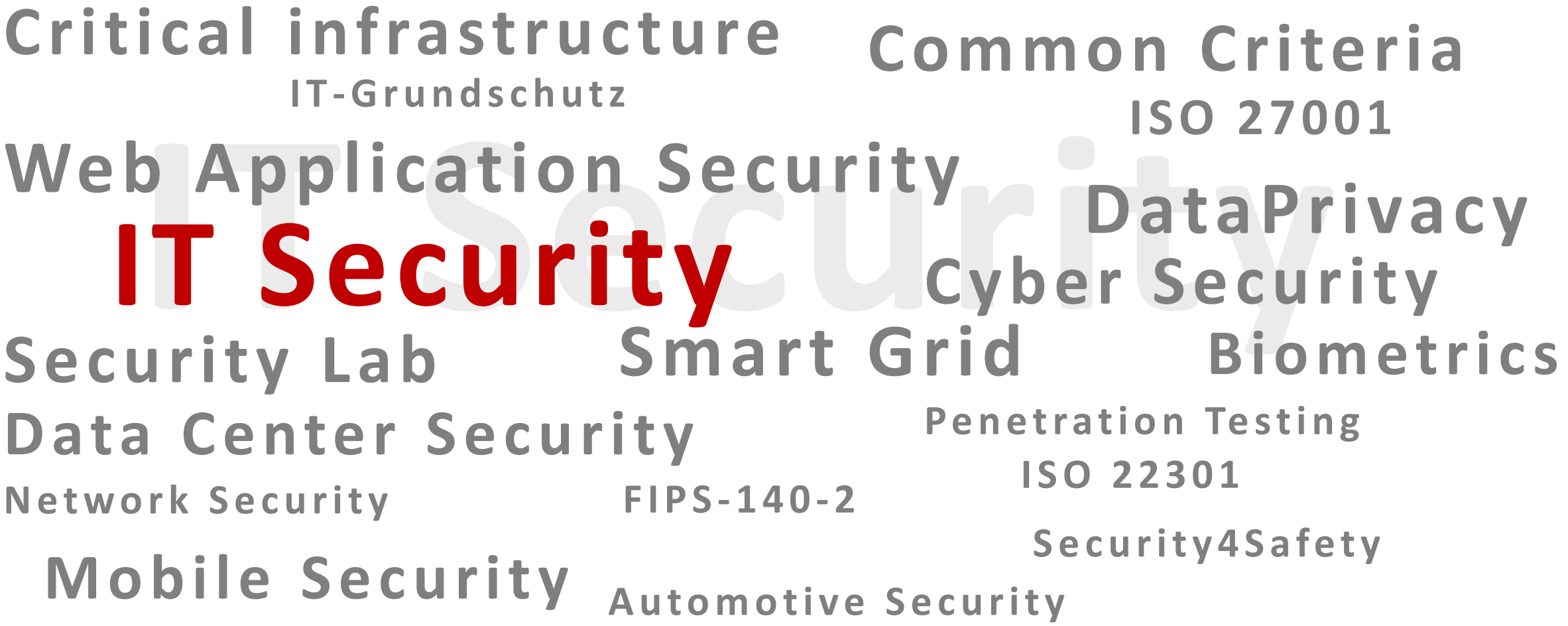
Security Level

- bezieht sich auf das jeweilige System oder die jeweilige Komponente
- besteht aus 4 Level
- Die Level bauen sich aufeinander auf
- die Level zeigen das Niveau der Gegenmaßnahmen und Sicherheitseigenschaften

security Levels für IEC 62443-3-3 und 62443-4-2

Security Level	Beschreibung
SL 1	Schutz vor zufälligen Attacken
SL 2	Schutz vor Attacken mit geringen Ressourcen und Wissen
SL 3	Schutz vor Attacken mit durchschnittlichen Ressourcen und Wissen
SL 4	Schutz vor Attacken mit ausgebauten Ressourcen und Wissen




Critical infrastructure
IT-Grundschutz
Common Criteria
ISO 27001
Web Application Security
IT Security
DataPrivacy
Cyber Security
Security Lab
Smart Grid
Biometrics
Data Center Security
Penetration Testing
ISO 22301
Network Security
FIPS-140-2
Security4Safety
Mobile Security
Automotive Security