5G.NRW
Competence Center

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

5G Infrastruktur-Sicherheit: welche Sicherheitstests sind notwendig und machbar?

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

Dortmund/ZOOM, 28.October.2020

TÜViT®
TÜV NORD GROUP

5G Modell

Mobilfunkbetreiber (MNO)

Nutzer/Infrastruktur Betreiber

Mobilfunkbetreiber

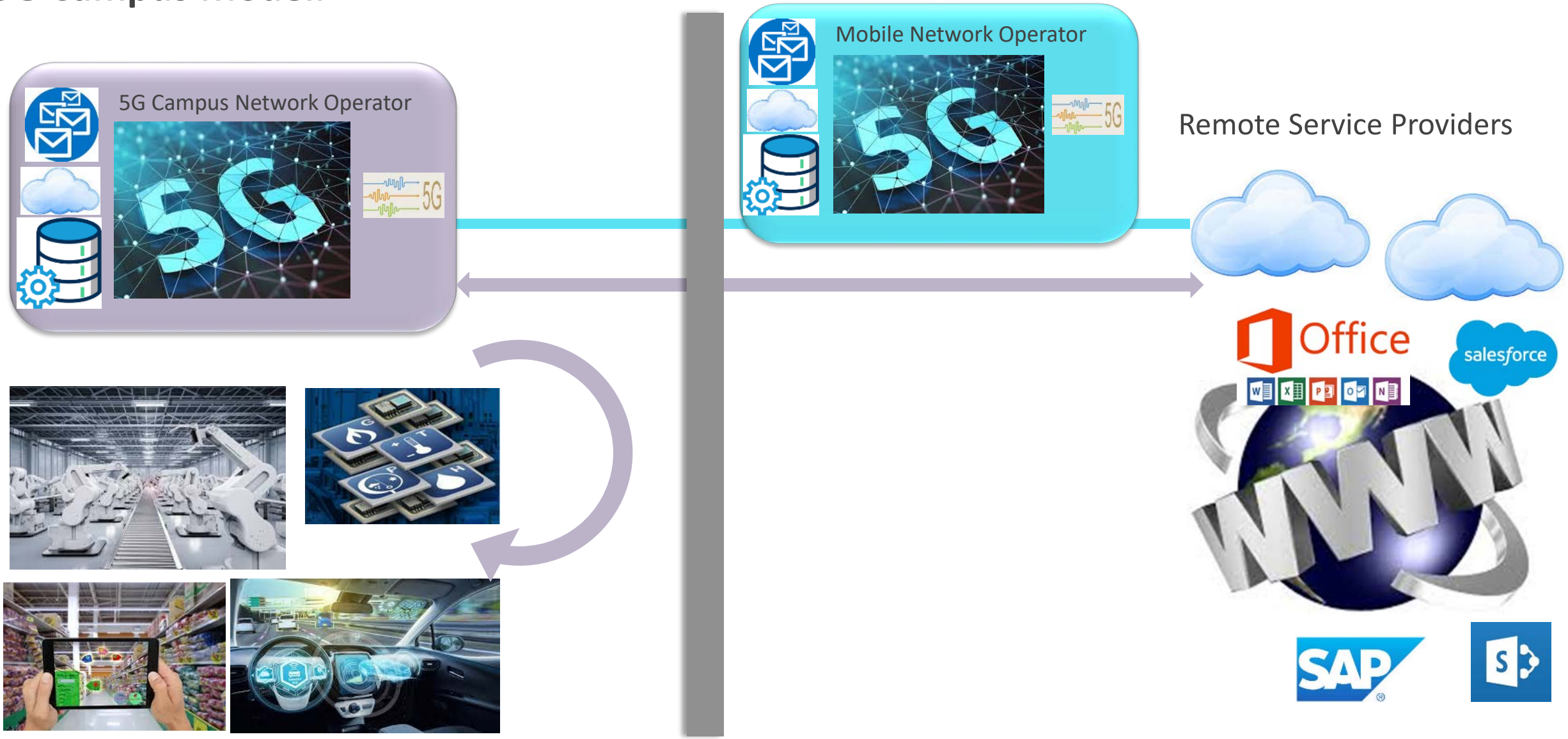
3GPP A GLOBAL INITIATIVE

Remote Service Providers

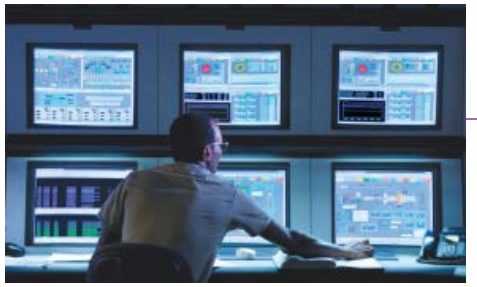
Nationale/Internationale Netzagentur

Anwender / Service Provider Policies

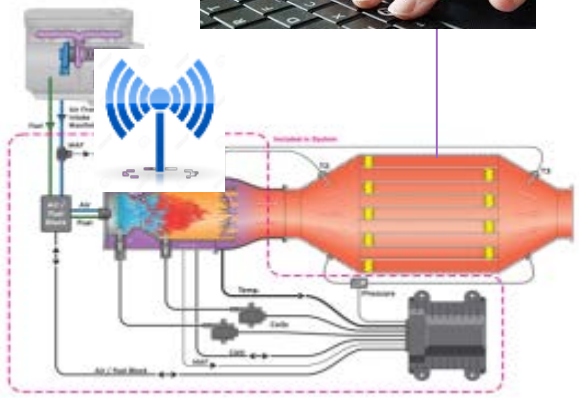
5G Campus Modell

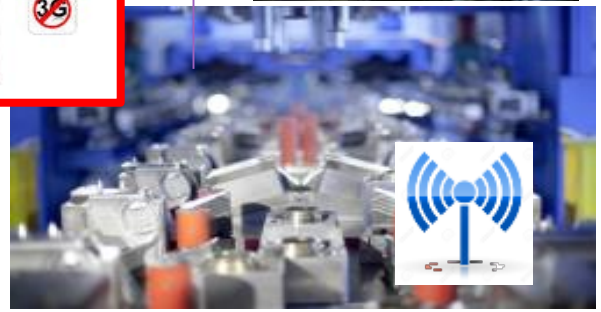


Industrial Security



5G Campus Network Operator

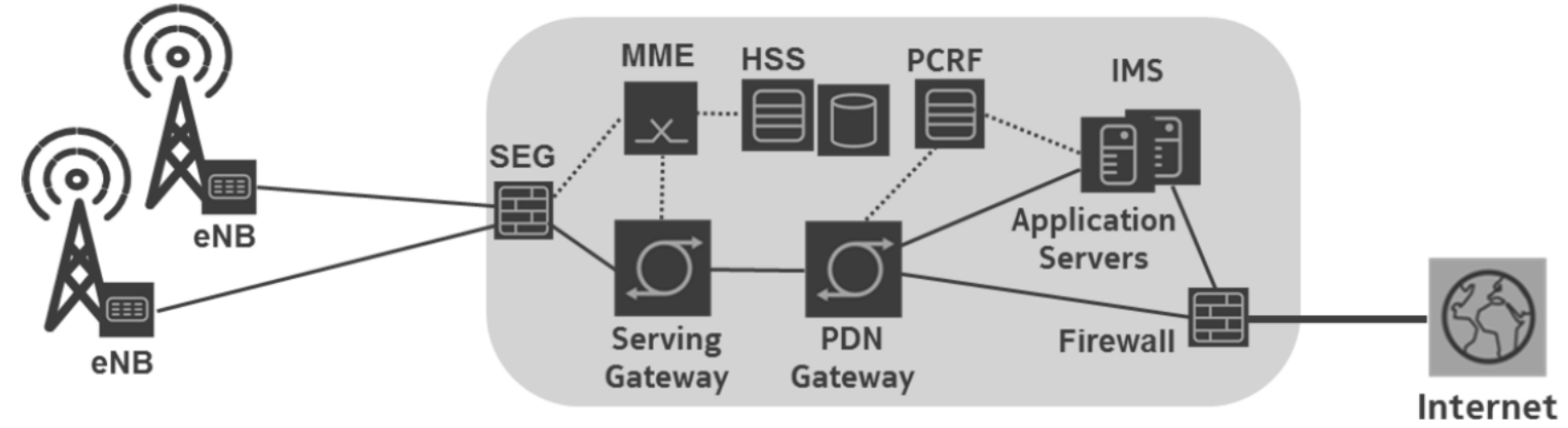




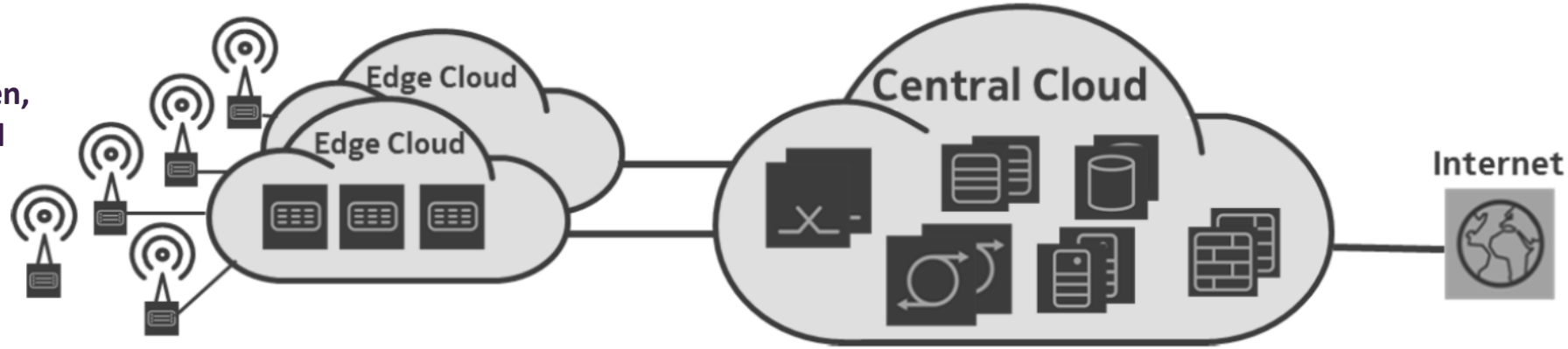
Von LTE (4G) zu 5G

Einführung der Virtualisierung

LTE feste Funktionszuordnung



5G virtuelle Funktionen, Software Defined Networking



Source: Nokia

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 nicht 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

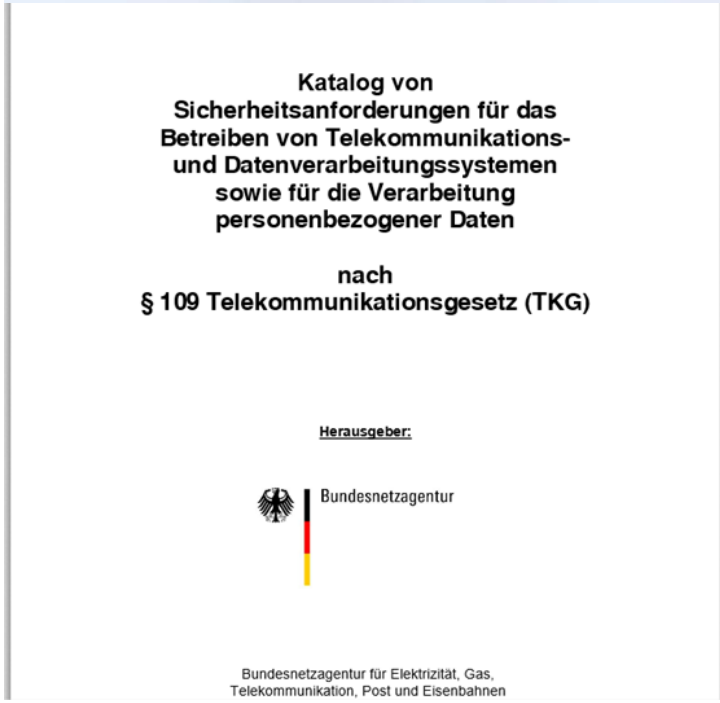
Bundesnetzagentur aktualisiert den Katalog von Sicherheitsanforderungen nach TKG §109

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

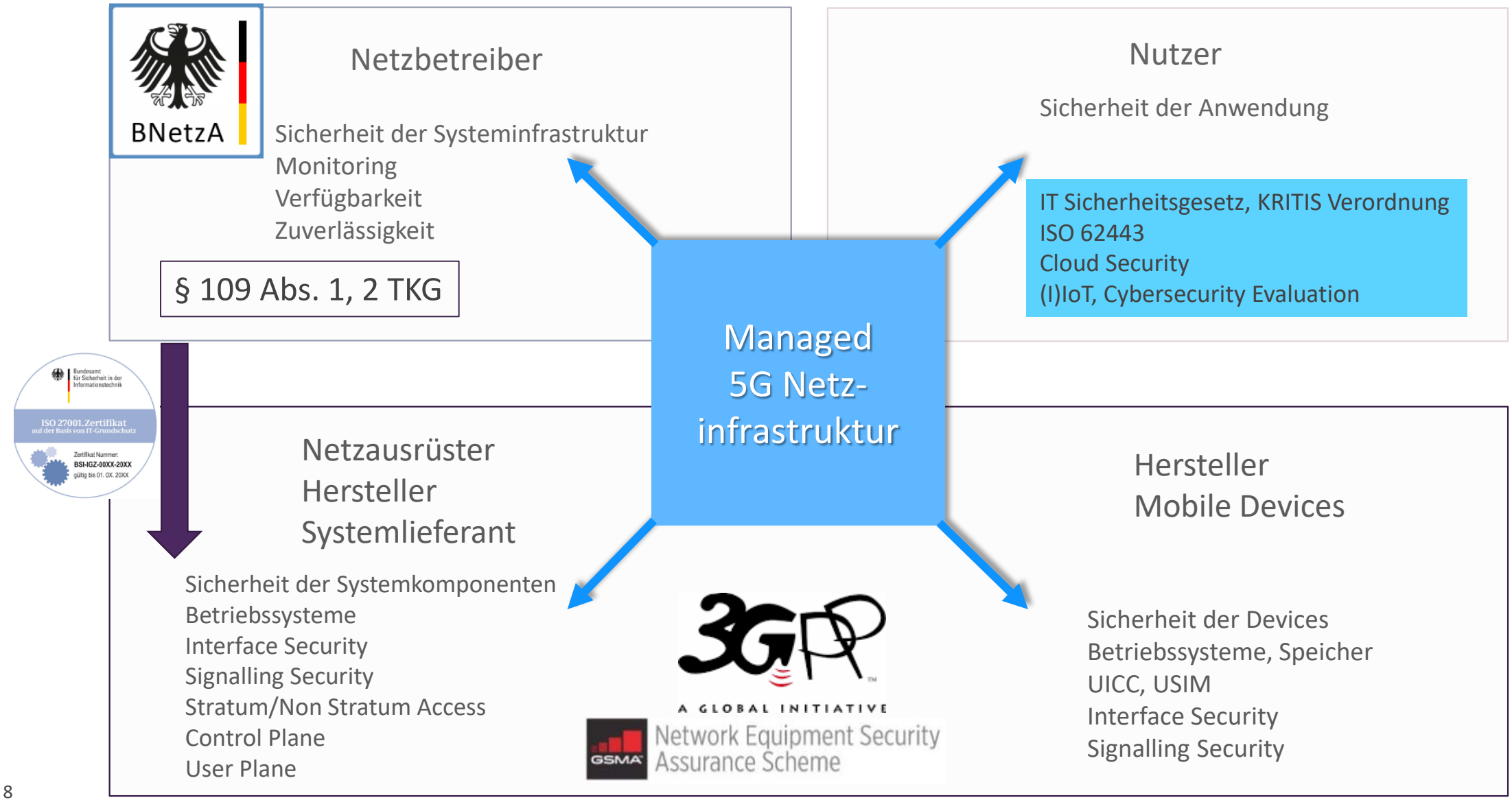
nach
§ 109 Telekommunikationsgesetz (TKG)

Herausgeber:

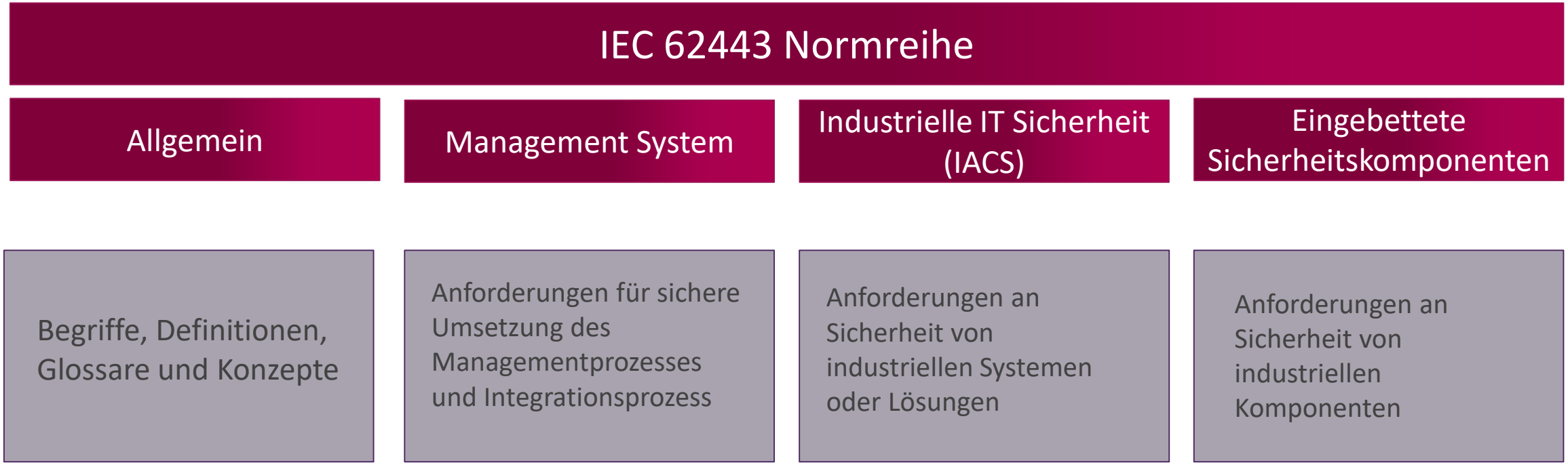
Bundesnetzagentur

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

5G Security Targets „Ecosystem“



Übersicht IEC 62443



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

Critical infrastructure

IT-Grundschutz

Common Criteria

ISO 27001

Web Application Security

DataPrivacy

IT Security

Cyber Security

Security Lab

Smart Grid

Biometrics

Data Center Security

Penetration Testing

ISO 22301

Network Security

FIPS-140-2

Security4Safety

Mobile Security

Automotive Security