

secuvera

Cybersicherheit. Nachhaltig.



5G Security

MOB1 Guest Lecture at Goethe University Frankfurt
21.01.2025

Sebastian Fritsch
secuvera GmbH, Gäufelden/Stuttgart

- Agenda
 - **Introduction & Motivation**
 - 5G Overview
 - 5G Security: Regulation and Certification
 - Security Testing in 5G
 - Future Challenges

- whoami
 - Sebastian Fritsch
 - Dipl.-Inform.
 - TU Darmstadt
 - Product Security Evaluator
 - Head of Evaluation Facility (CC Laboratory, ITSEF)
 - Working in ISO and IEC
 - ISO SC 27/WG 3 develops Common Criteria (ISO 15408/18045)
 - IEC TC 65/WG 10 develops IEC 62443

- We are...
 - 40 top security experts
- What we do...
 - IT Security, Cybersecurity, 100%
- We are located in...
 - near Stuttgart, Gäufelden
 - and work remote

- BSI Security Testing Lab (aka ITSEF)
 - **5G Security Testing Lab**
- Penetration testing / web application security
- ISO/IEC 27001 / Security Management
- Training, Consulting,
Research Projects, ...



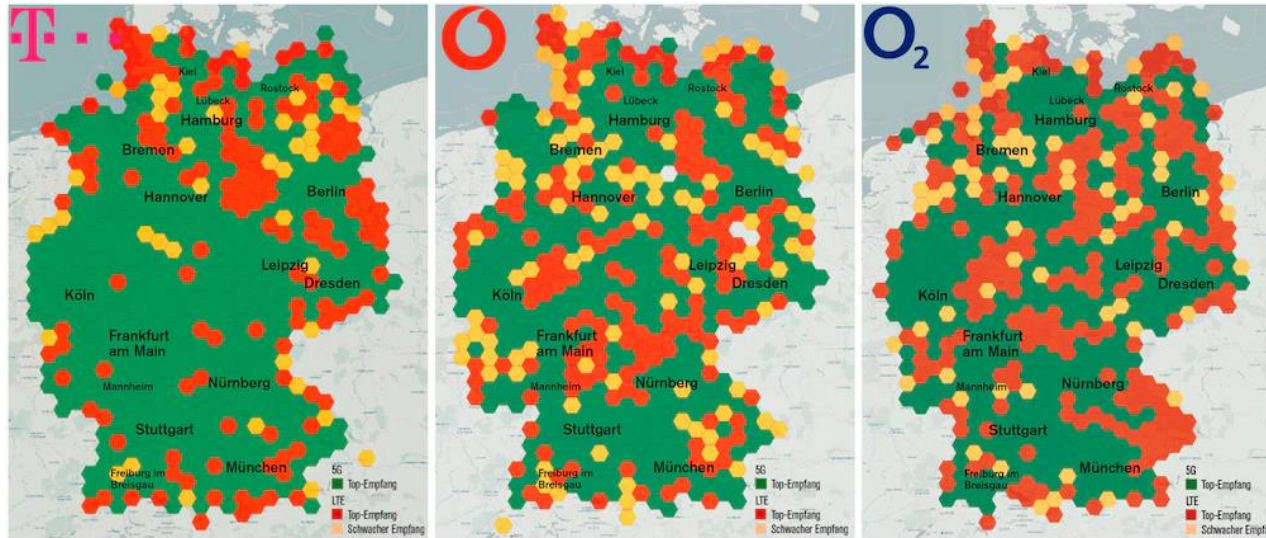
- Agenda
 - Introduction & Motivation
 - **5G Overview**
 - 5G Security: Regulation and Certification
 - Security Testing in 5G
 - Future Challenges

- Who is already using 5G?



Source: www.teltarif.de

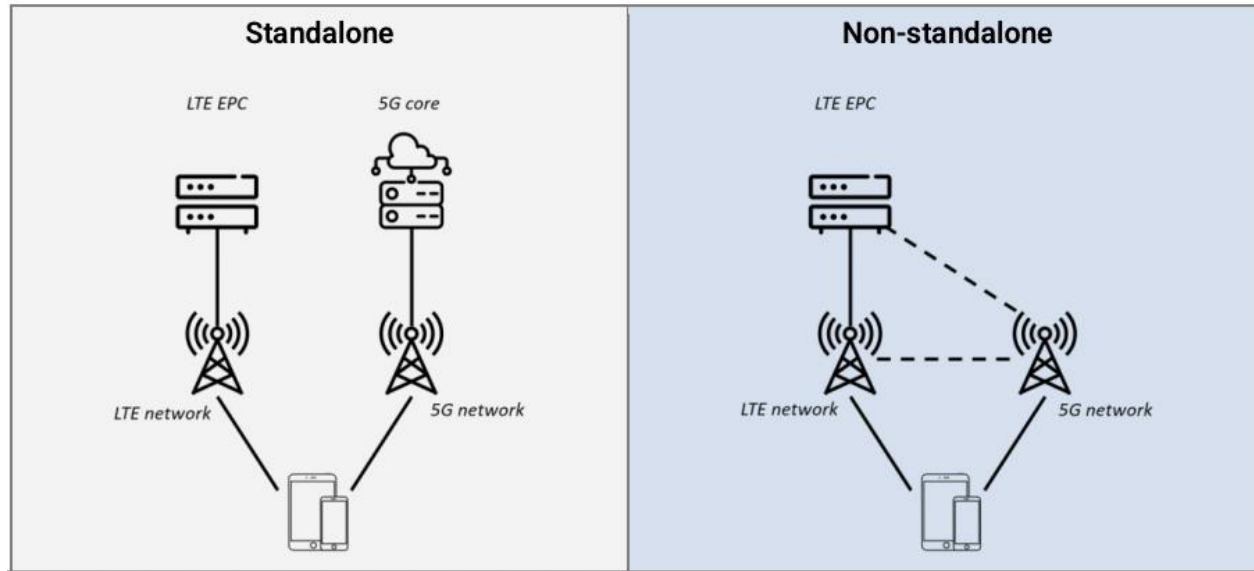
- 5G Availability
 - Germany, October 2022



Source:
<https://www.computerbild.de/artikel/cb-Tests-Handy-Mobilfunk-Netztest-2022-2023-34919053.html>

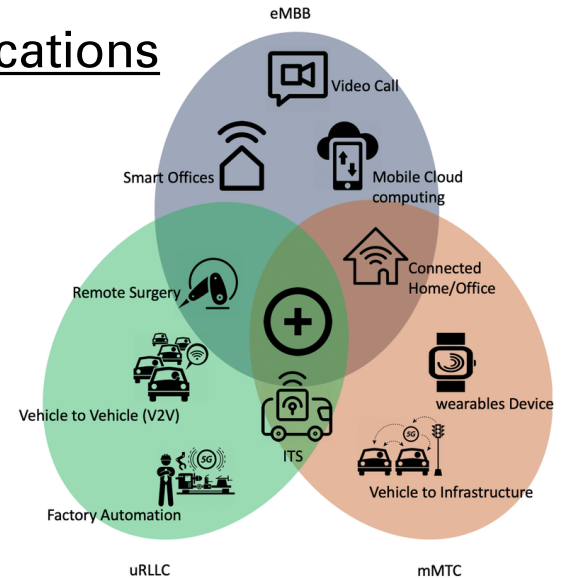
- Two types of 5G networks
 - Public networks
 - Germany: Telekom, Vodafone, Telefonica, 1&1
 - Private networks
 - „5G-Campusnetze“
 - Germany: needs licence from BNetzA (Federal Network Agency)

- 4G (LTE) to 5G migration
 - Non-standalone networks: allow migration path



- 5G technology's impact on B2B landscape
 1. B2B Applications of 5G
 2. B2B Service Model
 3. Network Configuration for B2B
 4. B2B Collaborations in 5G Development

- New use-cases
 - 5G brings new use-cases and new applications for mobile networks → *Verticals*
 - E-Health
 - Smart Energy Grid
 - Smart Factories
 - Media & Entertainment
 - Mobility
 - ...
 - New 5G service categories/profiles
 - Enhanced Mobile Broadband (eMBB)
 - Massive Machine-type Communications (mMTC)
 - Ultra-reliable and Low Latency Communications (URLLC)



Source:
https://www.researchgate.net/figure/5G-three-main-use-cases-with-examples-of-associated-applications-17_fig4_343115757

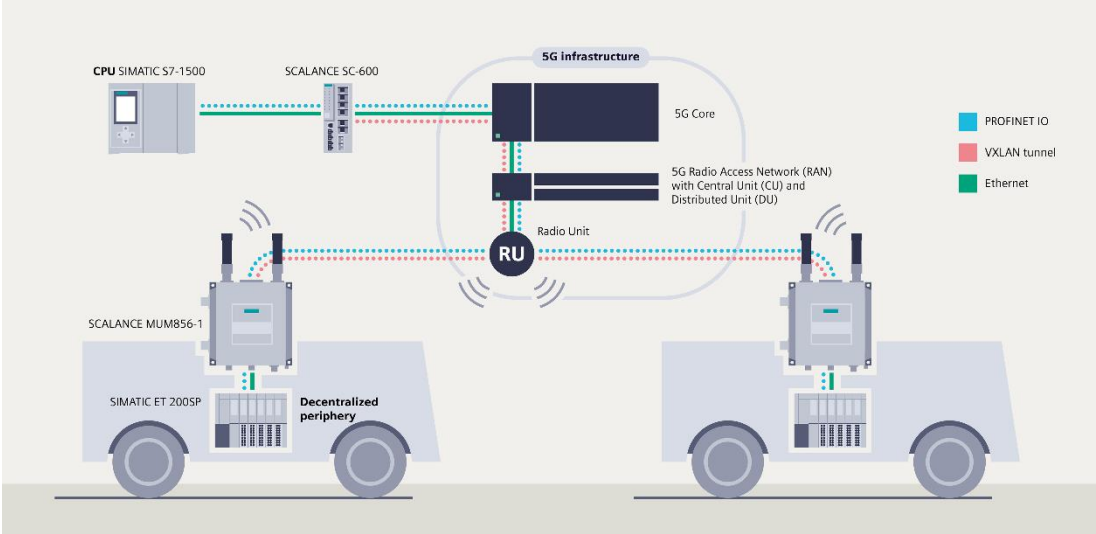
- Alternative for connectivity
 - 5G allows public deployments (mobile operators) or private deployment (private 5G networks)
 - WiFi and 5G will become more competitive standards



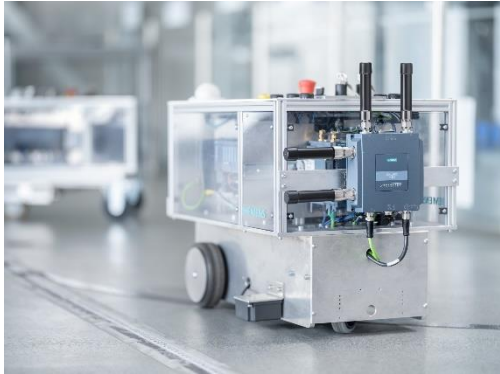
Source: <https://www.mecsware.com/>

form factor comparable to
WiFi access points

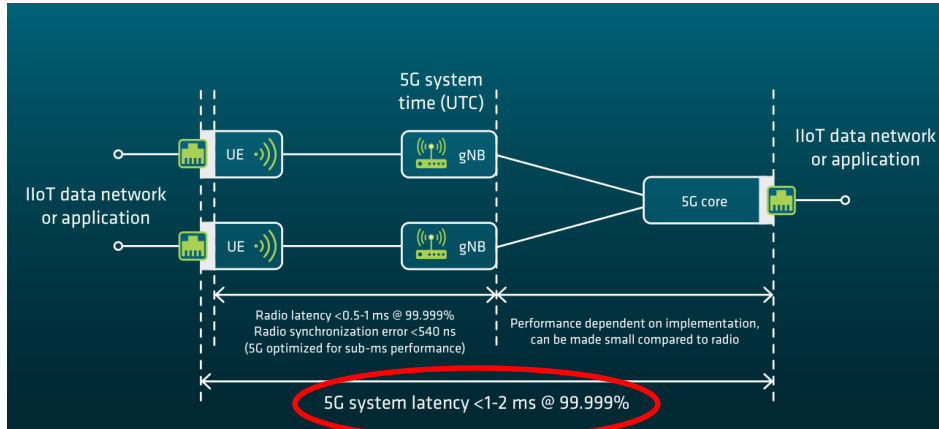
- 5G Use-Case example



Source: Siemens, <https://new.siemens.com/de/de/produkte/automatisierung/industrielle-kommunikation/industrial-5g.html>



- 5G Use-Case example



Source: 5G-ACIA White Paper, 5G for Industrial Internet of Things (IIoT): Capabilities, Features, and Potential

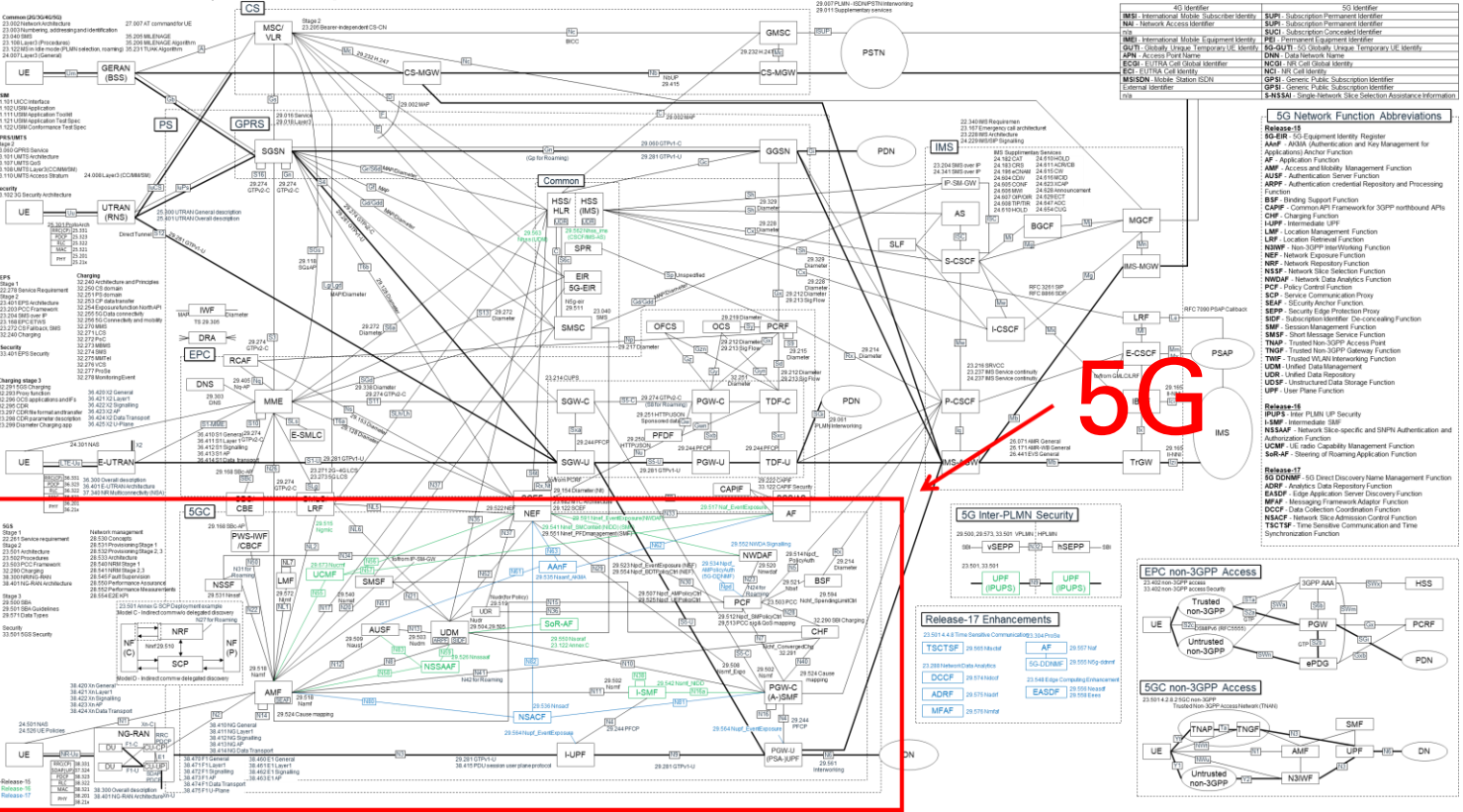
Classical fieldbuses for automation systems (wired connections)

ORGANIZATION	RESPONSE TIME (for 100 axes)	JITTER	DATA RATE
Ethernet/IP CIPSync ODVA	1ms	<math>< 1 \text{ ms}</math>	100Mbit/s
Ethernet Powerlink EPSPG	<math>< 1 \text{ ms}</math>	<math>< 1 \text{ ms}</math>	100Mbit/s
PROFINET-IRT PNO	<math>< 1 \text{ ms}</math>	<math>< 1 \text{ ms}</math>	100Mbit/s
SERCOS-III IGS	<math>< 0.5 \text{ ms}</math>	<math>< 0.1 \text{ ms}</math>	100Mbit/s
EtherCAT ETG	0.1ms	<math>< 0.1 \text{ ms}</math>	100Mbit/s

Real-time comparison of the various real-time methods (Source: IEbmedia)

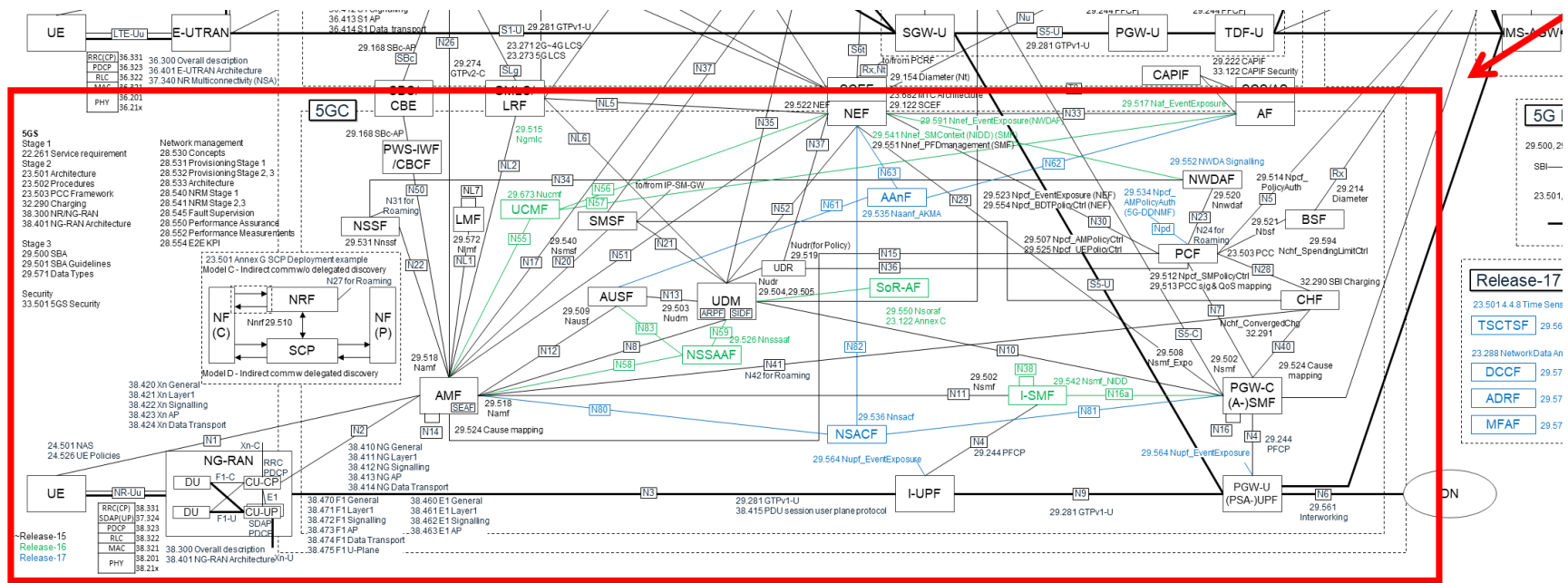
• 5G Protocols → 3GPP

3GPP Overall Architecture and Specifications



Source: <https://github.com/nicke10/3GPP-Overall-Architecture>

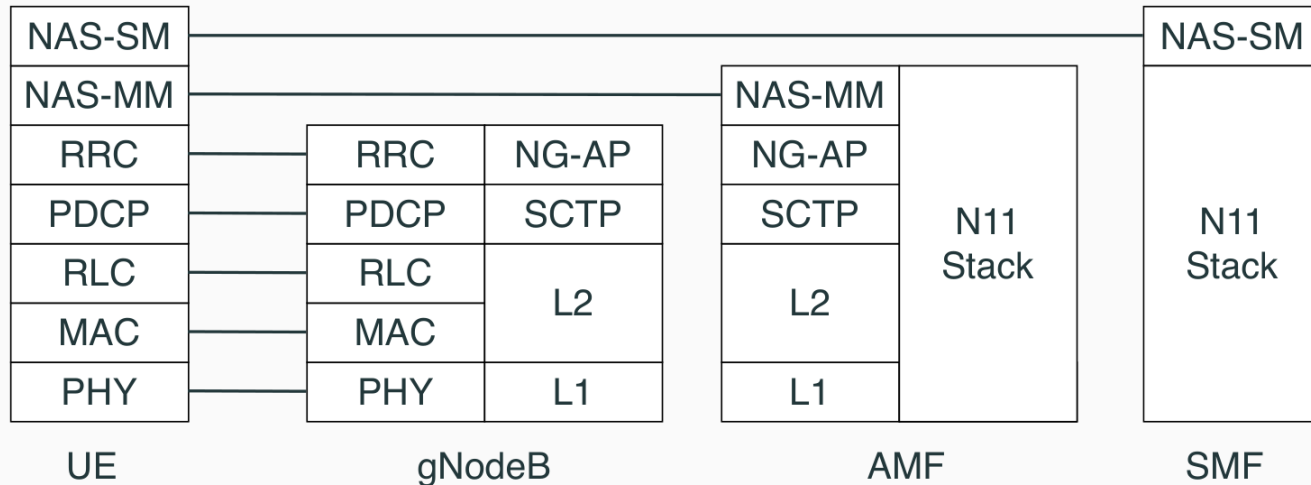
• 5G Protocols → 3GPP → 5G



Source: <https://github.com/nickel0/3GPP-Overall-Architecture>

- 5G Internals: Protocol Stack

5G Standalone — Protocol Stack — Control Plane



Access and Mobility
management Function

Session Management
Function

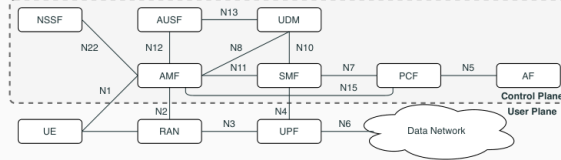
Source: David Rupprecht, Radix Security, 5G Security: Attacks & Architecture

- 5G Internals
 - AMF: Access and Mobility Management Function
 - Mobility & Registration & Connection Management
 - User Authentication & Core Network Security Anchor
 - SMF: Session Management Function
 - Session (User Plane Data) management
 - Session Establishment / Modification/ Release
 - Controlling QoS Parameter (Quality of Service)
 - Configuration of the UPF (User Plane Function)
 - ...much more other Network Functions

- 5G Internals: Protocol Stack

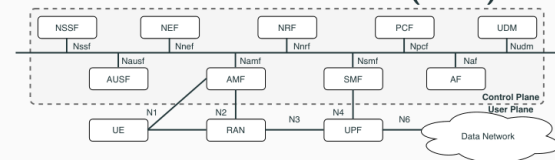
5G Core Architecture - Two Perspectives

Reference Point Architecture



- Elements Network Functions
- Interaction between NFs represented by point-to-point reference point
- Software based simplified Network Functions

Service Based Architecture (SBA)



- Service based interfaces
- Web based RESTful APIs
- Set of definitions acting as interface between different software applications enabling communication

Source: David Rupprecht, Radix Security, 5G Security: Architecture & Security Features

- Do you remember?

5G evolution works like this:

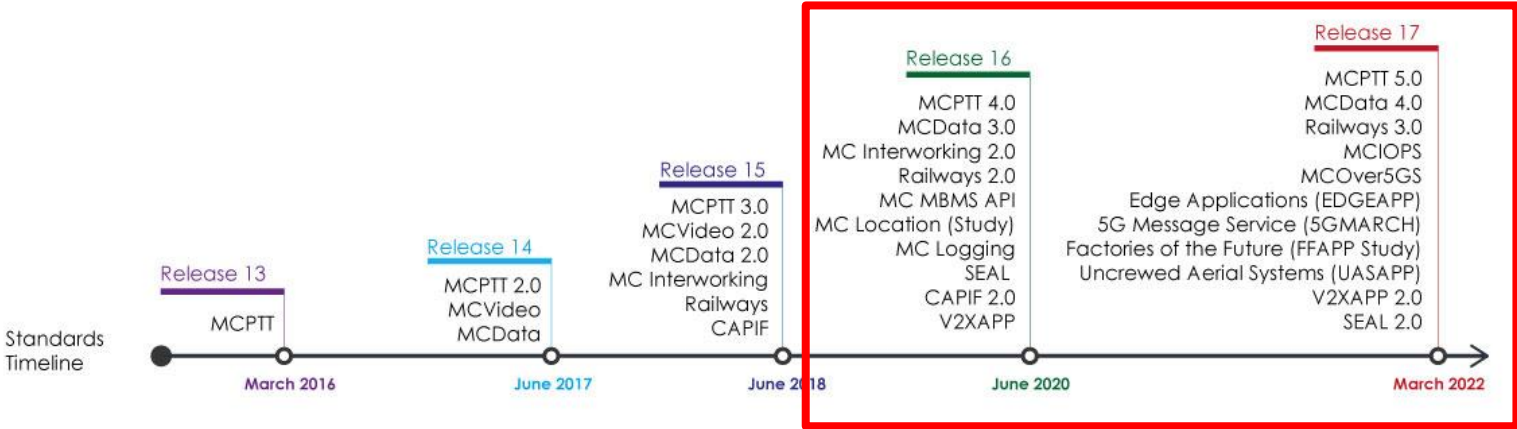
- 5G Non-Standalone (NSA)
 - uses existing 4G RAN and 4G Core Network
- 5G Standalone (SA)
 - greenfield network

security impact: legacy support and more interfaces

- 5G Releases



Application Enablement Standards

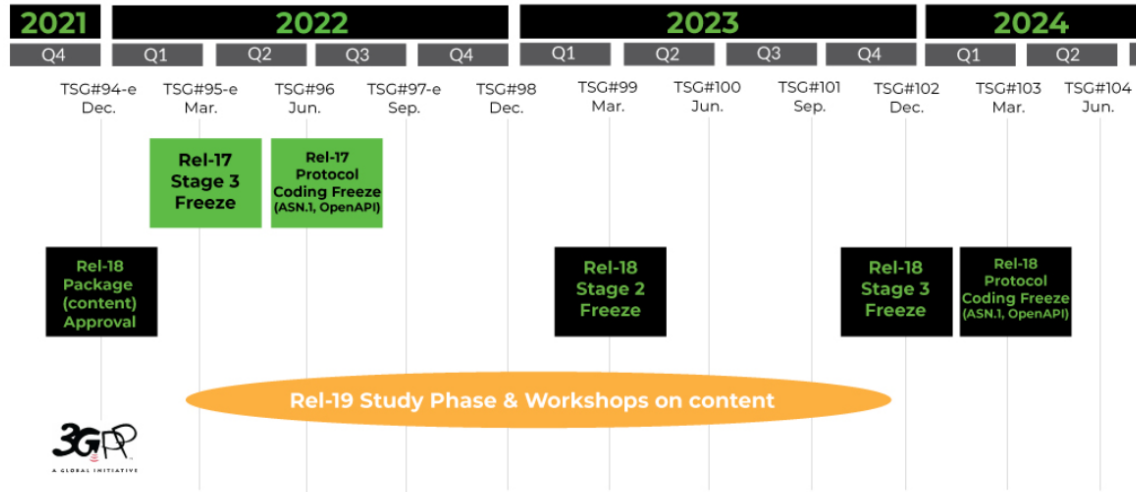


Source: <https://www.3gpp.org/news-events/3gpp-news/sa6-app-enable>

- 5G Release Roadmap

High frequency of new releases
 → challenge for security evaluation

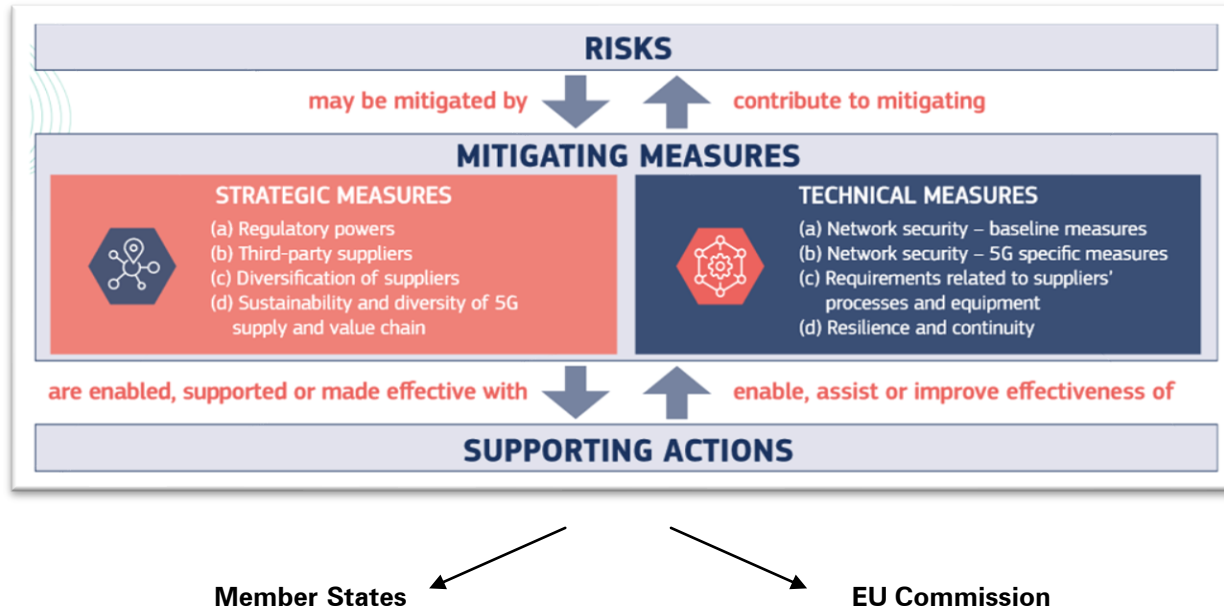
Release timelines:



Source: <https://www.3gpp.org/specifications-technologies/releases>

- Agenda
 - Introduction & Motivation
 - 5G Overview
 - **5G Security: Regulation and Certification**
 - Security Testing in 5G
 - Future Challenges

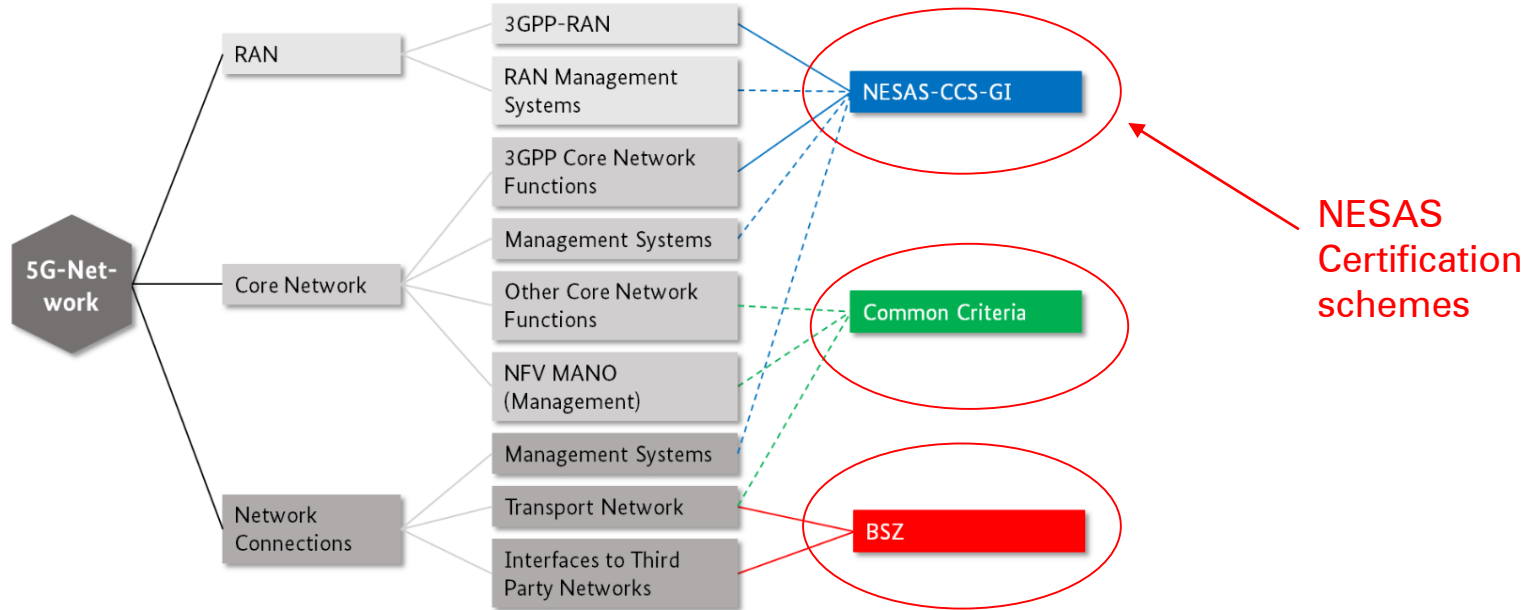
- 5G Regulation in Europe



Source: EU Commission

- German 5G Certification Strategy
 - Article 165(4) of the Telecommunications Act (TKG)
 - operators of public telecommunications networks with increased risk potential may use critical components [...] only if they have been checked and certified by an approved certification body prior to their first use.
 - SiKa (Sicherheitskatalog)
 - Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data pursuant to § 109 of the Telecommunications Act (TKG), Version 2.0
 - BSI TR-03161: Security in Telecommunications Infrastructure

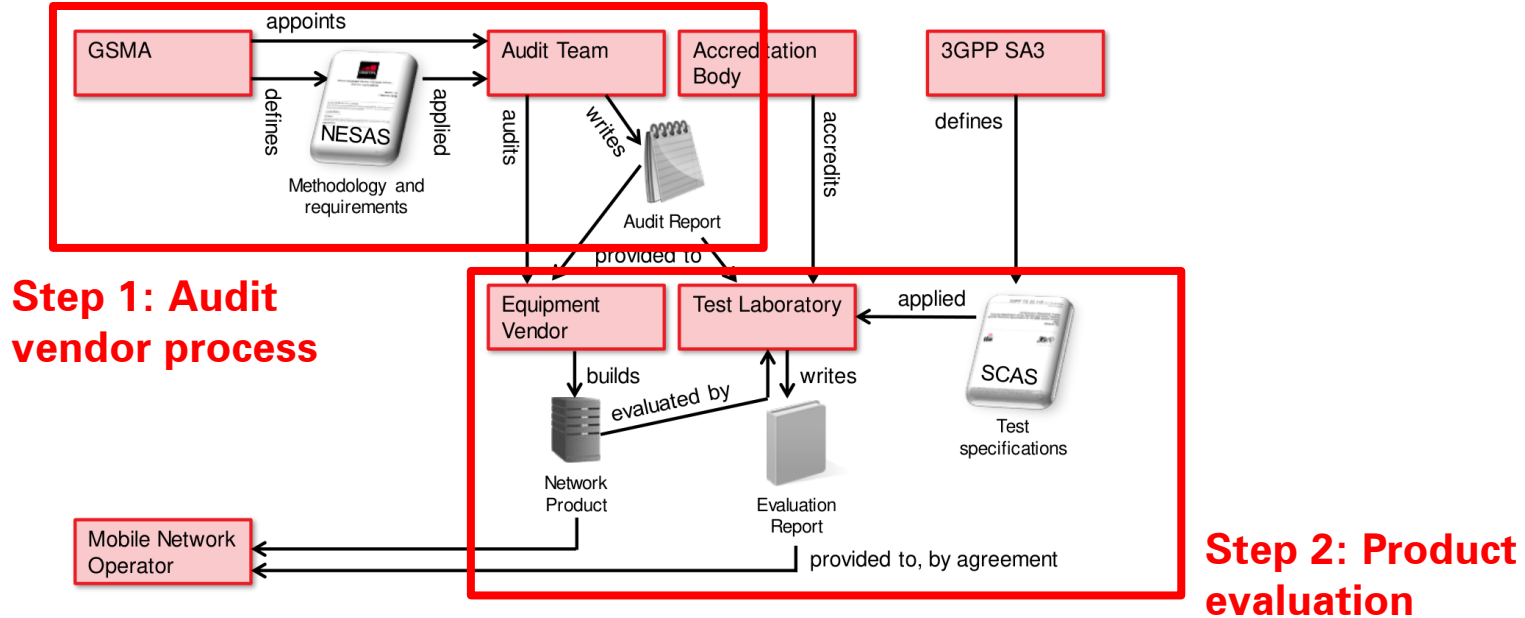
- German 5G Certification Strategy (TR-03163)



Source: BSI, TR-03163: Security in Telecommunications Infrastructure, Annex A, Version 1.2

- **GSMA's security initiatives/schemes**
 - GSMA Security Accreditation Scheme (SAS) for assessment of the security of UICC and eUICC suppliers, and their subscription management service providers
 - **GSMA Network Equipment Security Assurance Scheme (NESAS)**
 - <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>
 - allows mobile operators to audit and test network equipment vendors, and their products, against a security baseline
 - in general: specification-based approach

- Two assurance pillars in NESAS



Source: GSMA, Document FS.13 – NESAS Overview v.2.2

- Step 1: Audit Security Development Lifecycle (SDL)
NESAS Development process requirements
 - [REQ-DES-01] Security by Design
 - [REQ-IMP-01] Source Code Review
 - [REQ-BUI-01] Automated Build Process
 - [REQ-TES-01] Security Testing
 - [REQ-REL-01] Software Integrity Protection
 - [REQ-OPE-01] Security Point of Contact
 - [REQ-GEN-01] Version Control System

- **Step 2: Product evaluation (Network component)**
 - Need for testing requirements
 - **SCAS documents from 3GPP**
 - TS 33.117 Catalogue of general security assurance requirements
 - TS 33.116 Security Assurance Specification (SCAS) for the MME network product class
 - TS 33.216 Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
 - TS 33.250 Security assurance specification for the PGW network product class
 - TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product
 - TS 33.512 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
 - ...
 - **Set of SCAS documents refers to 3GPP-Release**
 - Available for 3GPP release 16, 17 and 18

- SCAS Test cases
 - SCAS document example
 - Example from *TS 33.117 Catalogue of general security assurance requirements*
 - Security functional requirements and related test cases
 - Basic vulnerability testing requirements
 - Tests are specified in 3GPP working groups

4.2.3.5.2 Protecting sessions – Inactivity timeout

Requirement Name: Protecting sessions – inactivity timeout

Requirement Description: An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.

NOTE: The kind of activity required to reset the timeout timer depends on the type of user session.

Test Name: TC_PROTECTING_SESSION_INAC TIMEOUT

Purpose:
To ensure an OAM user interactive session shall be terminated at inactivity timeout.

Procedure and execution steps:

Pre-Conditions:

- The tester has privileges to create an OAM user interactive session.
- The tester has privileges to configure the inactivity time-out period for user interactive session.
- Session log should be enabled.

Execution Steps

1. The tester creates OAM user A interaction session.
2. The tester configures the inactivity time-out period for user A to x minute, for example 1 minute.
3. The tester does not make any actions on the network production in x minutes. After that, the tester checks whether OAM user A interaction session has been terminated automatically.

Expected Results:

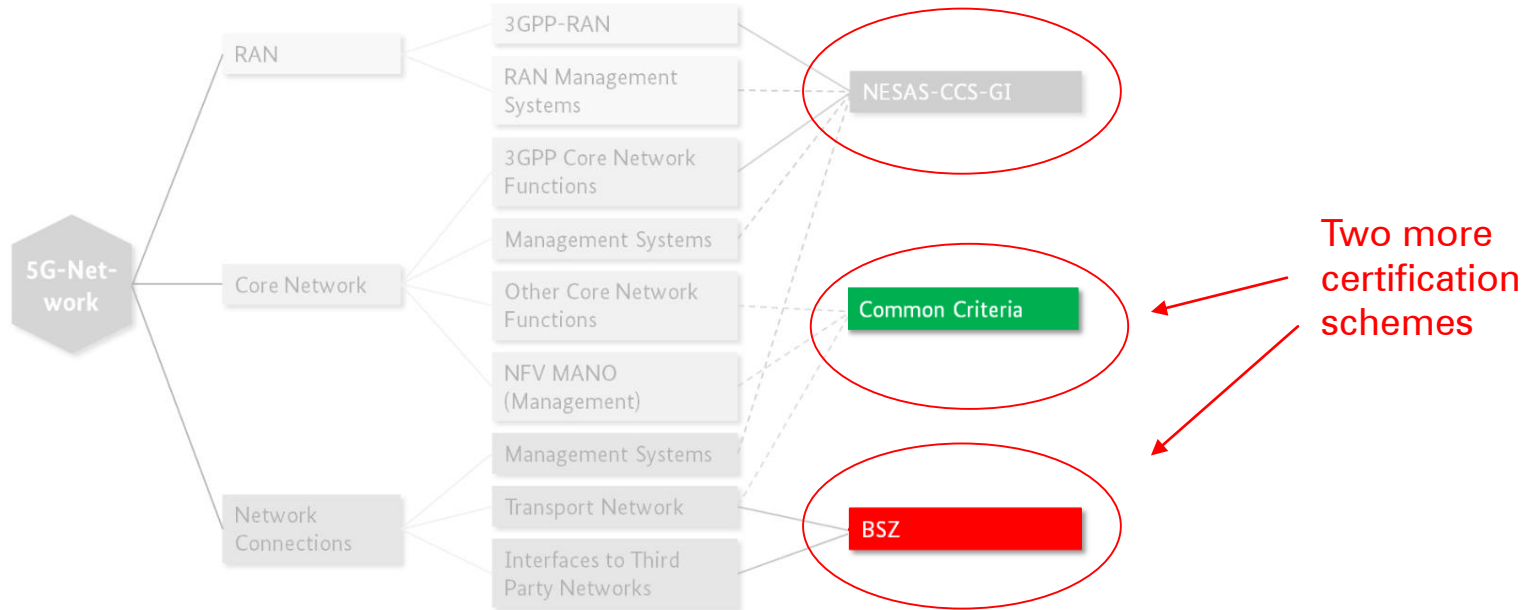
- In step 3, OAM user A interaction session has been terminated automatically after x minute.

Expected format of evidence:
A testing report provided by the testing agency which will consist of the following information:

- Session log
- Settings, protocols and configurations used

Test result (Passed or not)

- German 5G Certification Strategy (TR-03163)



Source: BSI, TR-03163: Security in Telecommunications Infrastructure, Annex A, Version 1.2

- Agenda
 - Introduction & Motivation
 - 5G Overview
 - 5G Security: Regulation and Certification
 - **Security Testing in 5G**
 - Future Challenges

- Security ...in general
 - Security is about CIA
 - Confidentiality, Integrity, Availability
 - and Privacy
 - and Safety, Quality... (sometimes called essential functions)
 - What is the security scope?
 - Security functionality
 - Security of products
 - Security of systems

- Security Certification
 - Security Evaluation
 - Evaluate/Analyse Products (includes Design) and Processes
 - Security Testing
 - Test product directly
 - Vulnerability analysis
 - Complexity of Security Testing
 - specification, implementation, configuration, interfaces, (continuous) state of the art, ...
 - *we never know the complete behaviour, new knowledge arises*

- Security Evaluation: two approaches (two cultures)
 1. Specification-based approach
 - (exactly) define required security functionality
 - develop and maintain test cases
 - pro/con:
 - + predictable evaluation execution time
 - does not find problems outside the scope

- Security Evaluation: two approaches (two cultures)
 2. Attack-based approach
 - allows evaluation team to be investigative and attack focused
 - need for test engineering (in case of new products, new technologies) as part of the evaluation project
 - pro/con:
 - + allows state-of-the-art evaluation results (high quality)
 - uncertainties for vendors regarding test cases and competition

- Security Evaluation Basics

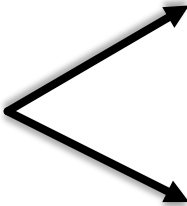
WHAT?

- Product
- Documentation
- Processes



HOW?

- Analyse documents
- Audit processes
- Product testing (directly thru interfaces)
- Vulnerability analysis



Conformity

Requirements fulfilled?

Resistance

Resistance to prevent attacks?

- Security Evaluation Example
 - Example 1:
Test authentication functionality → testing → develop test cases (derived from security functional requirements) → allows pass/fail tests
 - Example 2:
Search for vulnerabilities in used 3rd party software libraries (reading SBOM, or use root shell, or ...) → vulnerability analysis → might lead to exploitable vulnerability in product interface

- Basic Requirements for Testers
 - Basic technical skills
 - Computer science, Communications engineering, ..., MINT
 - Knowledge of the technology
 - for example
 - Network products → TCP/IP, WAN technologies, WiFi, ...
 - Loves to learn new things (in a short timeframe)
 - deep-dive into specific technologies
 - Team player
 - sharing knowledge and experience is key to run commercial evaluation projects

- 5G-specific Requirements for Testers
 - Knowledge of 3GPP terminology and concepts
 - major barrier to entry!
 - Basic protocols like HTTP, REST, TLS, OAUTH, ...
 - Communication flows within 5G (physical/radio layer, different logical layers)
 - Deployment strategies: OpenRAN, Network Core Virtualization, Private 5G Scenarios/Devices
 - ...

- 5G Security Evaluation
 - performed by ITSEF (IT Security Evaluation Facility)
 - or lab, works according to ISO/IEC 17025 (laboratory standard)
 - evaluation team
 - evaluation test setup

- Challenges in 5G Security Testing
 - 3GPP standards focus on functionality and interoperability
 - but no (additional) test interfaces yet
 - consideration of deployment aspects
 - use of vendor facilities, tools or resources
 - rapid turnaround times → major challenge for actual security certification models
 - fast 3GPP release cycle

- Do you remember? TR-03163 certification

- NESAS

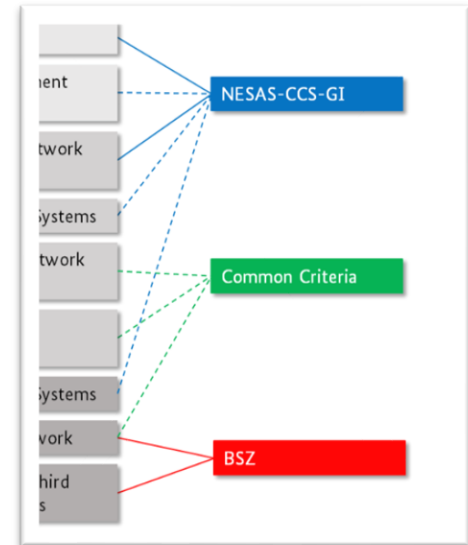
- Allows for automated testing
 - *Specification-based*

- Common Criteria (CC)

- Classical security certification model
 - Compliance to protection profiles
 - *Attack-based (in Europe)*

- BSZ

- Fixed-time product penetration test
 - *Attack-based*



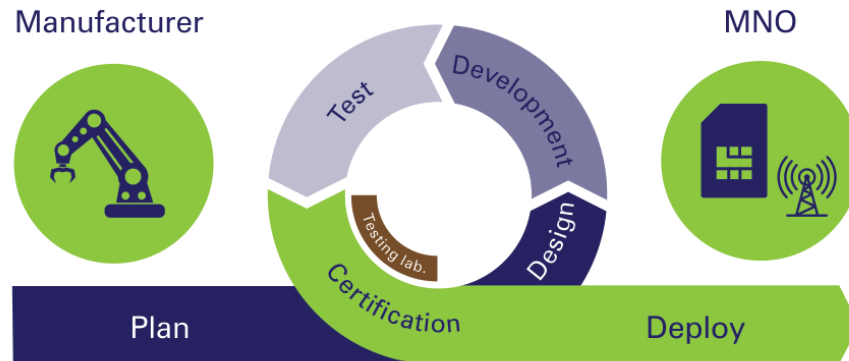
- Agenda
 - Introduction & Motivation
 - 5G Use-Cases & Internals
 - Threats & Risks in 5G Networks
 - Security Evaluation of 5G Components
 - **Future Challenges**

- Complexity of 5G and legacy aspects
 - 5G must be configured and operated
 - Private 5G network
 - Do operators have security experts?
 - New opportunity to operate components from different vendors
 - more open connections
 - Backward compatibility
 - especially in non-standalone networks
 - behaviour of network components could be different

- **Certification of 5G networks**
 - Goal: operators (public or private) have the obligation to run secure networks
 - Configuration is typically a challenge in lab test setups
 - How to setup the full complexity?
 - Misconfiguration is often the root cause of undetected, exploitable vulnerabilities
 - Network scenarios are getting more diverse/complex, e.g. multi vendor strategy
 - **Open question:**
Can we attest the security status of the whole 5G network?

- Agile evaluation/certification process
 - Industry complains: security evaluation limits innovation in products
 - Evaluation requires support/resources from vendors
 - **Open question:**
Can we certify more agile?
Certification as part of the development pipeline?

- Agile evaluation/certification process
 - Shift left optimization



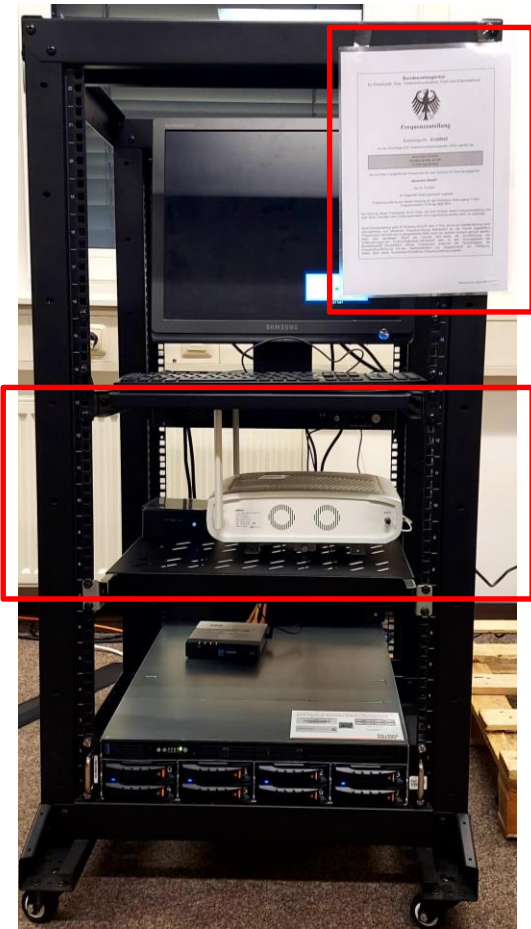
Source: OPNESAS Project

- Global security regulation
 - 5G Regulation in Germany
 - Cyber Resilience Act (CRA) in Europe
 - Regulation in North America, Asia (India, China), ... ?
 - **Open question for manufactures:
How to avoid repetition of tests for different schemes and markets?**
 - **And how to show compliance efficiently?**

Source: OPNESAS Project

- Are you interested in an 5G security internship?
 - **OPNESAS**
 - project partners: secuvera, Radix Security & Ruhr Uni Bochum
 - 24 month, between 01/2023 and 06/2025
 - direct contact: sfritsch@secuvera.de
 - visit: <https://www.secuvera.de/unternehmen/karriere/>

- secuvera
5G laboratory



Licence
(BNetzA)

Technology
(Core and Radio)

- What are our motivations?
 - ...security hygiene for complex products
 - ...identify weaknesses and errors before product is globally available
 - ...have more secure products for own usage
 - ...support the evolution of testing/evaluation criteria for future projects (not only for our team, standardization)

- We are looking for?
 - (Junior) Product Testers
 - (Junior) Consultants for Security Certification
 - (Junior) Industrial Security Consultants
- Details...
 - <https://www.secuvera.de/unternehmen/karriere/>

- Last but not least, since 5 years we are a...



- Why? Please have a look...

- <https://www.secuvera.de/unternehmen/karriere/secuvera-als-arbeitgeber/>

secuvera

Cybersicherheit. Nachhaltig.

mobile
business 

Vielen Dank!
Thank you!



Sebastian Fritsch
sfritsch@secuvera.de
+49-7032/9758-24

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart
Germany