secuvera

Cybersicherheit. Nachhaltig.

mobile business

5G

5G and security evaluation

MOB1 Guest Lecture at Goethe University Frankfurt

17.01.2023

Sebastian Fritsch

secuvera GmbH, Gäufelden/Stuttgart

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

secuvera

- 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

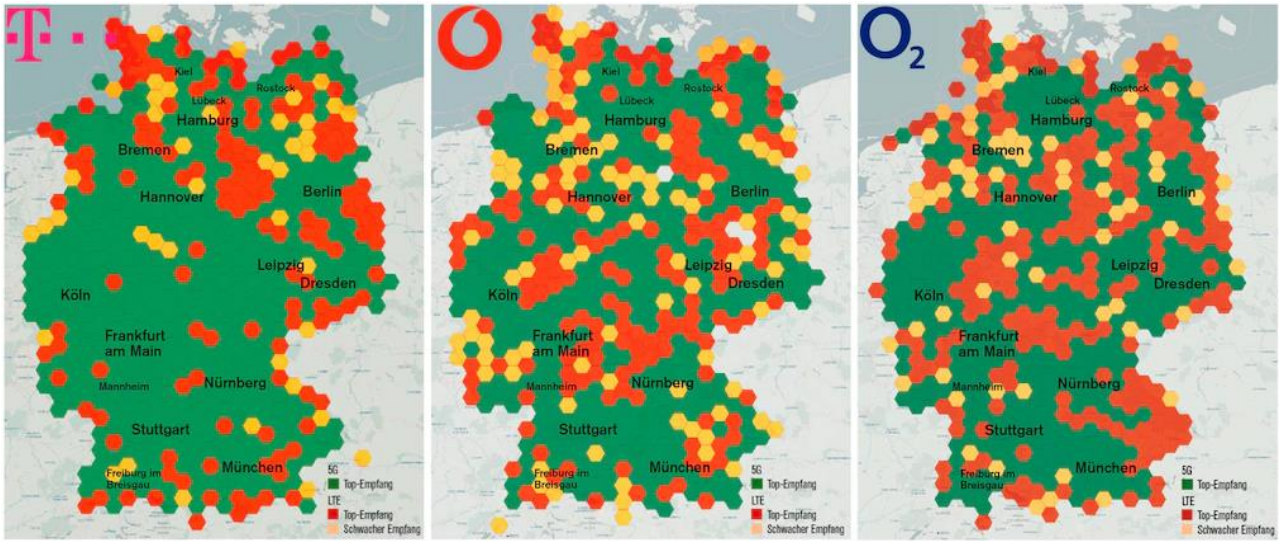
- secuvera GmbH
  - Located in Gäufelden/Stuttgart (STR)
  - Established in 1982
  - Owner-managed company
  - Headcount >30
  - Cyber security since 1988
  - Only focused on cyber security
  - Vendor-independent security consultants and lab (CC ITSEF)

- Three divisions
  - BSI-Prüfstelle für Common Criteria /
    CC Lab (ITSEF) at BSI
  - Penetrationstests/Webanwendungsprüfungen /
    penetration testing / web application security
  - BSI-Grundschutz/ISO 27001 /
    IT baseline protection/native ISO 27001
- BSI-certified/recognized in all areas
  - Annually reviews by BSI
  - Company and staff certified

- Who is already using 5G?

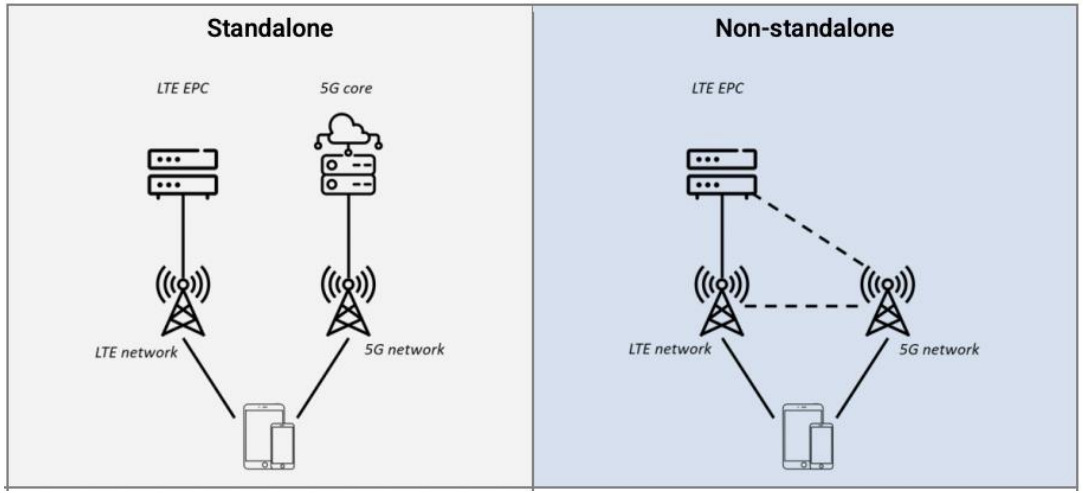
Source: www.teltarif.de

- 5G Availability
  - Germany, October 2022

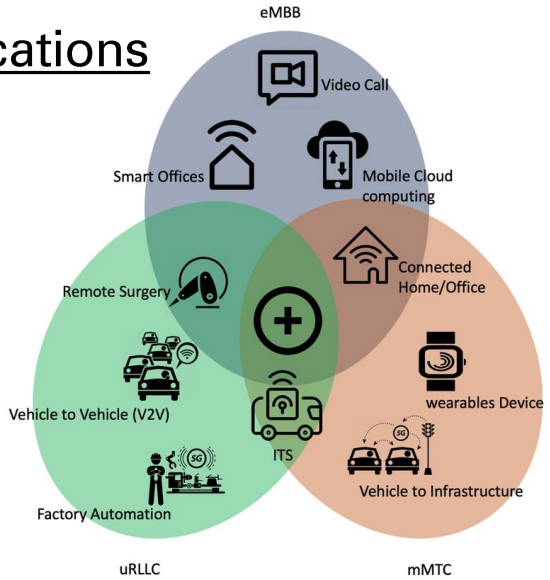


Source: https://www.computerbild.de/artikel/cb-Tests-Handy-Mobilfunk-Netztest-2022-2023-34919053.html

- 4G to 5G migration
  - Non-standalone networks



- Motivation #1
  - 5G brings <u>new use-cases and new applications</u> 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)



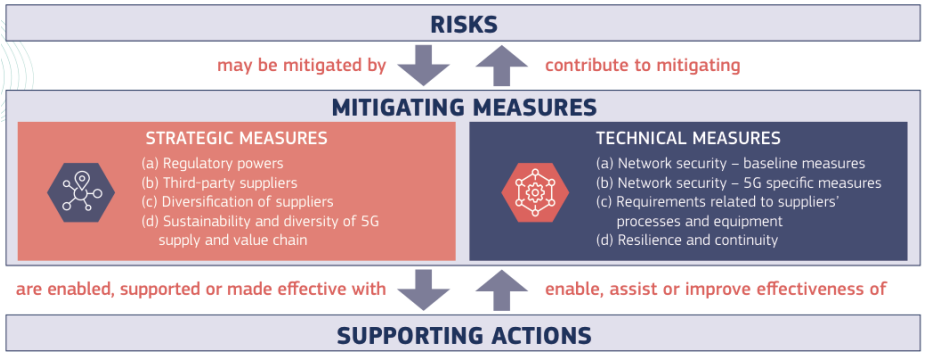
Source: https://www.researchgate.net/figure/5G-three-main-use-cases-with-examples-of-associated-applications-17_fig4_343115757

- Motivation #2
  - 5G allows public deployments (mobile operators) or private deployment (private 5G networks)
  - WiFi and 5G will become more competitive standards

form factor comparable to
WiFi access points

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

- Motivation #3
  - 5G Security is already a strategic goal in the EU: EU Toolbox for 5G Security

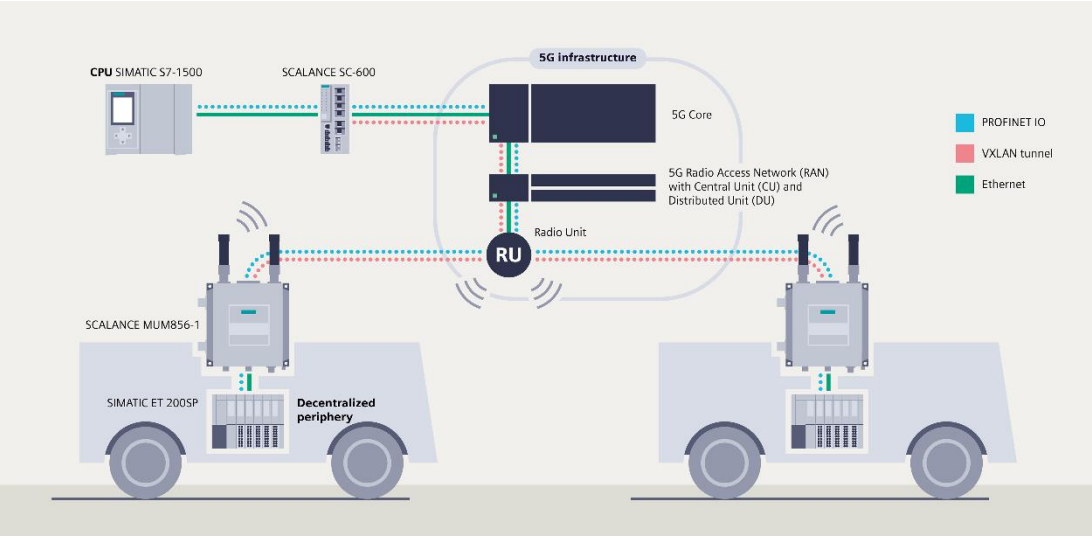


Source: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

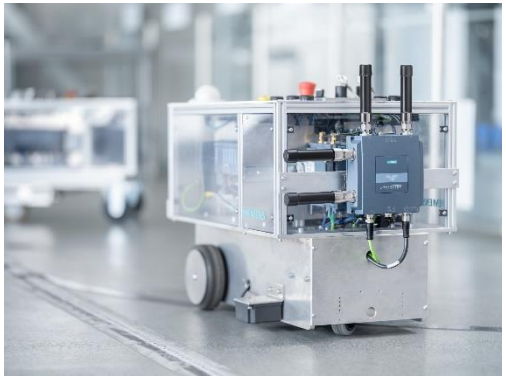
  - German 5G regulation: Starting from 2026 all critical components must be certified before installation
    - Note: Only EU member state which has implemented mandatory certification.

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

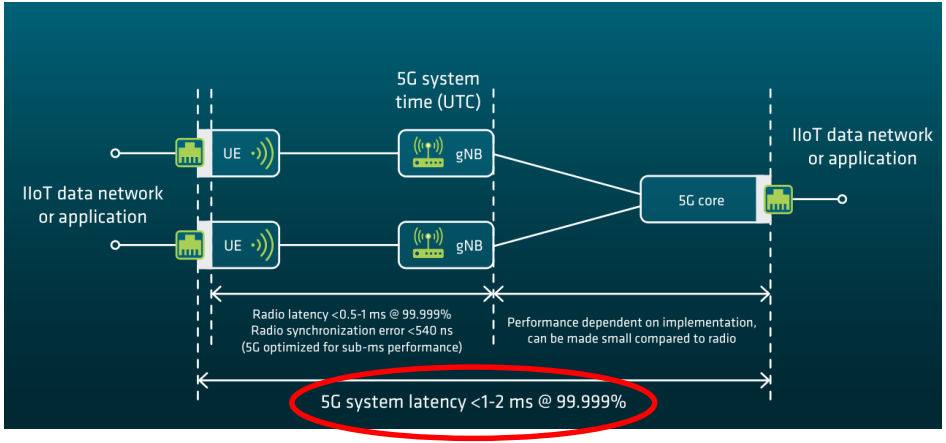
5G Use-Case example



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



5G Use-Case example



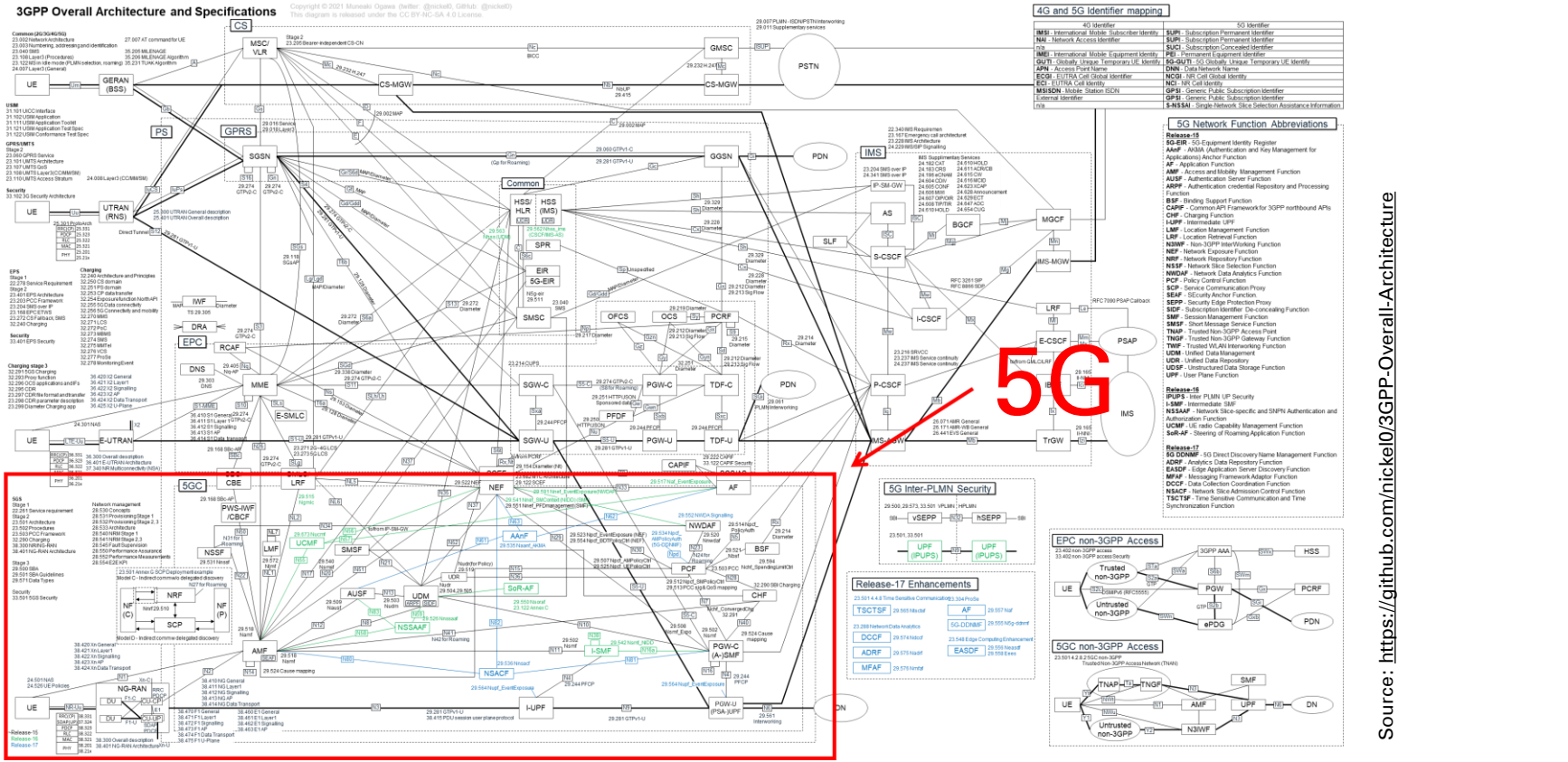
Source: 5G-ACIA White Paper, 5G for Industrial Internet of Things (IIoT): Capabilities, Features, and Potential

Classical fieldbuses for automation systems (wired connections)

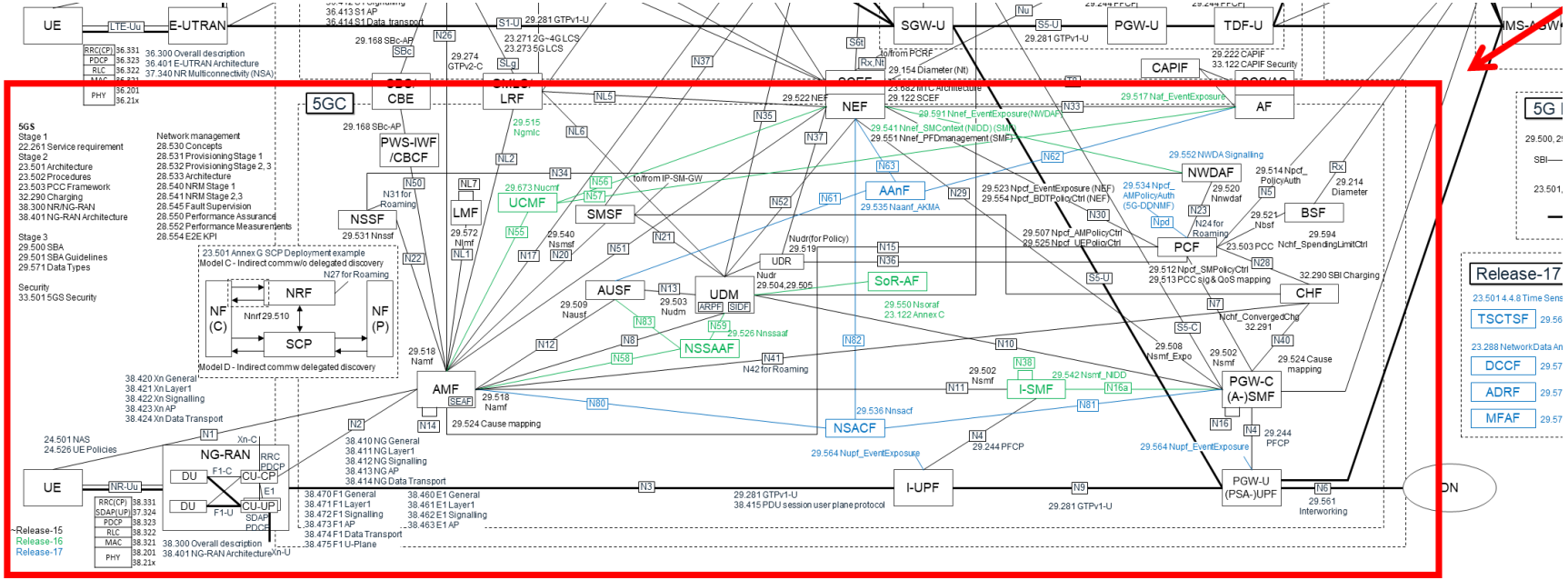
ORGANIZATION	RESPONSE TIME (for 100 axles)	JITTER	DATA RATE
Ethernet/IP CIPSync ODVA	1ms	<1ms	100Mbit/s
Ethernet Powerlink EPSG	<1ms	<1ms	100Mbit/s
PROFINET-IRT PNO	<1ms	<1ms	100Mbit/s
SERCOS-III IGS	<0.5ms	<0.1ms	100Mbit/s
EtherCAT ETG	0.1ms	<0.1ms	100Mbit/s

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

5G Protocols → 3GPP

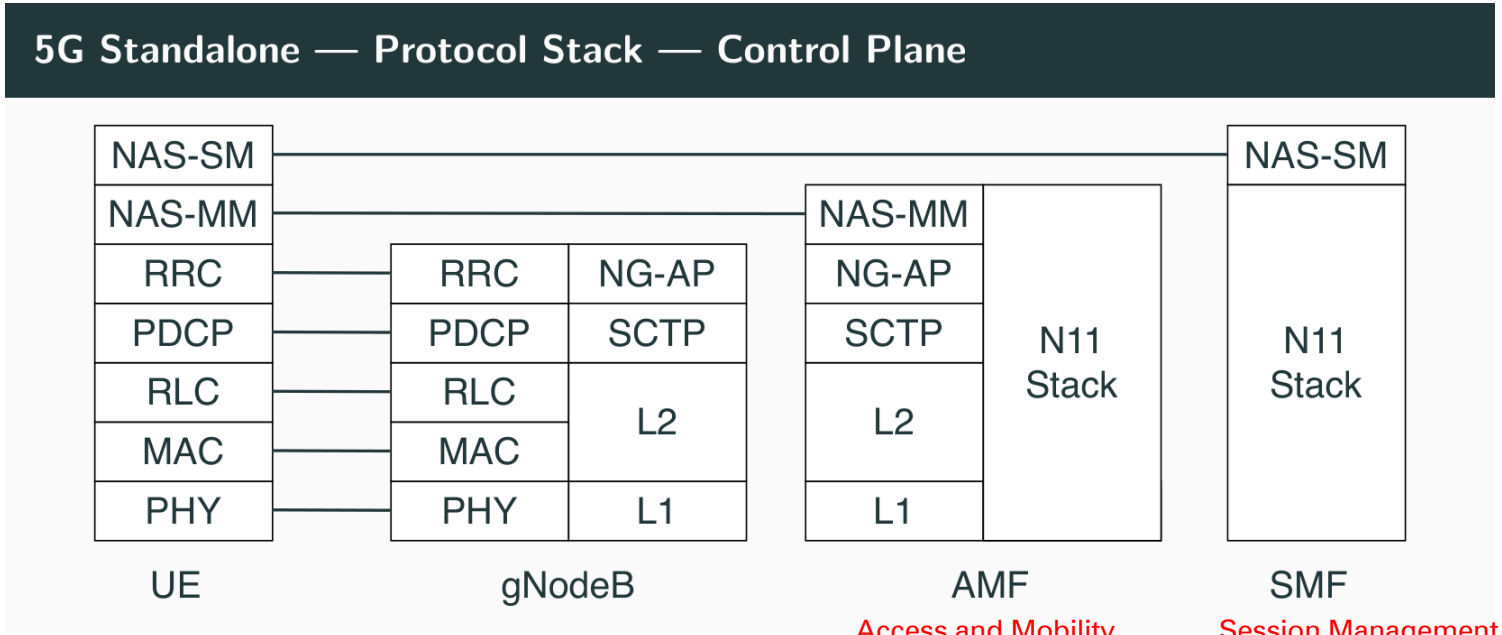


- 5G Protocols → 3GPP → 5G



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

5G Internals: Protocol Stack



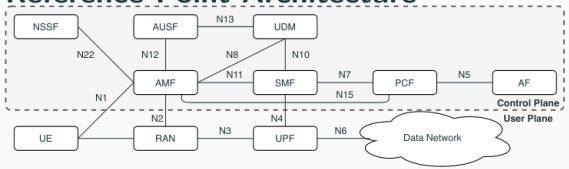
Source: David Rupprecht, Radix Security, 5G Security: Attacks & Architecture

- 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)
  - AUSF: Authentication Server Function
    - Authentication Server
    - Stores Session keys for other NF (Network Functions)
  - …more Network Functions

5G Internals: Protocol Stack

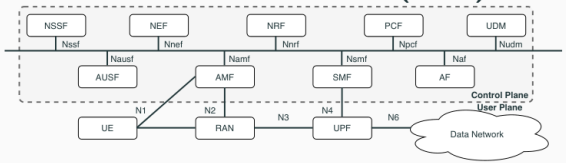
5G Core Architecture - Two Perspectives

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

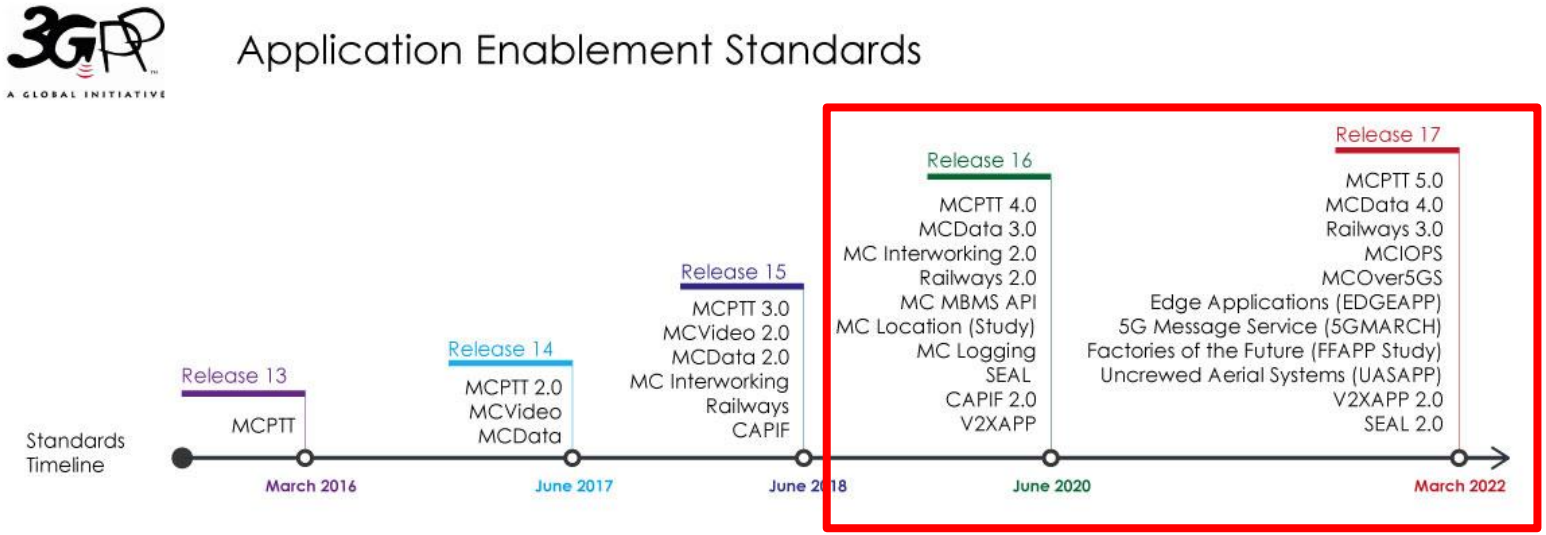
Source: David Rupprecht, Radix Security, 5G Security: Architecture & Security Features

- 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

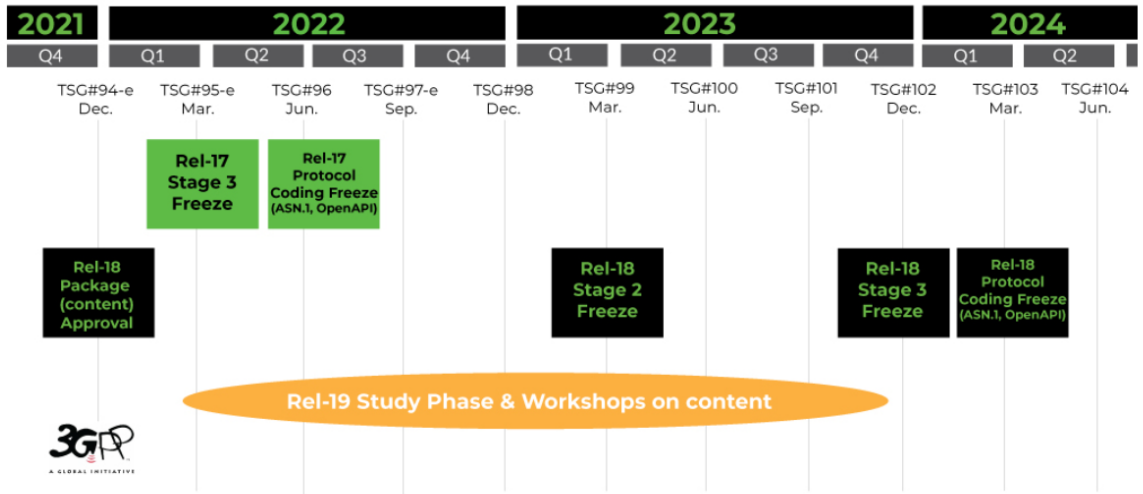


Source: https://www.3gpp.org/news-events/3gpp-news/sa6-app-enable

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

- Threats & Risks in 5G Networks
  - Risks for mobile operators
    - Integrity: correct charging service protects mobile operators revenue, protect from fraud attacks
    - Software & Hardware integrity: run known software, components might become stepping stones for more advances attacks on more internal hosts
    - Availability of the network: critical infrastructure, emergency use-cases
    - …
  - and risks for end users of mobile networks

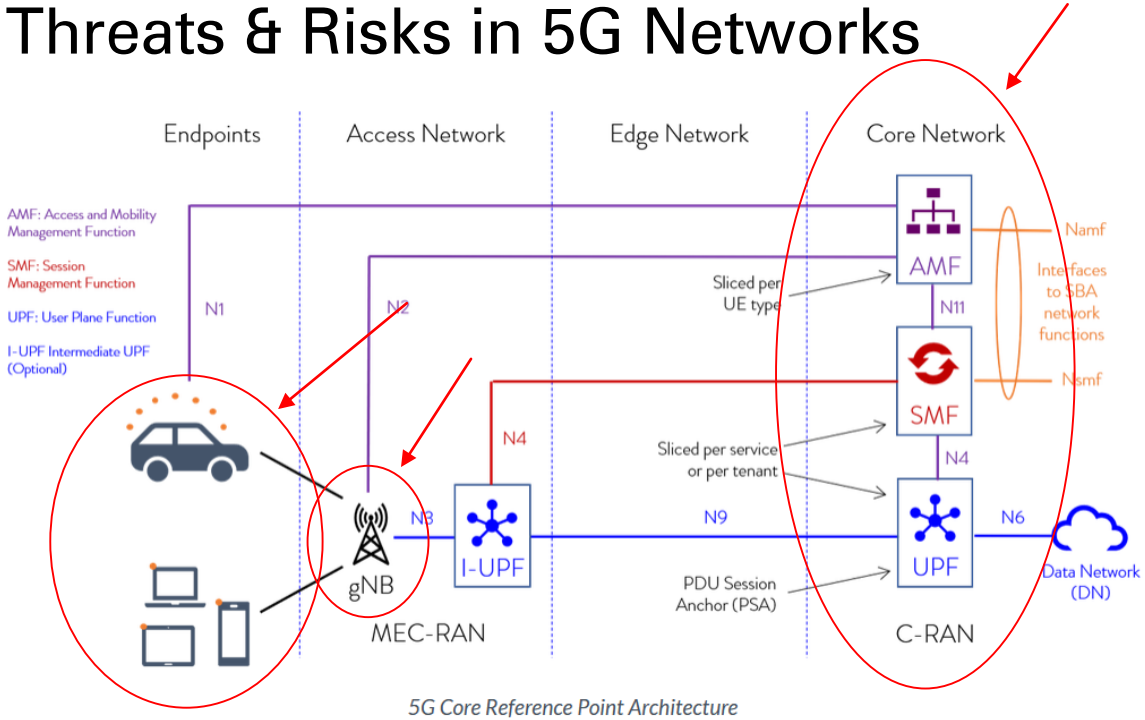
Overview of Attack Aims in 5G Networks

Attack Aims

Security Category	Mobile Network Aims	Attack Aims
Confidentiality	Confidentiality of User Data Traffic	Interception of Internet traffic
	Confidentiality of Voice/Video Calls	Eavesdropping Phone Calls
	Confidentiality of text messages (SMS) / RCS	Interception of text messages / RCS
Privacy	Location Privacy	User tracking
	Identity Privacy	User identification
		User localization
Integrity	Correct Charging Service	Fraud attacks
	Traffic Integrity	Modification of traffic
	Mutual Authentication	Impersonation attack
	Software and Hardware Integrity	Malware and Hardware Trojan
Availability	Undistributed Service	Downgrade Attacks (stepping stone attack)
		DoS of target subscribers
		DoS of infrastructure (ransom)

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

Threats & Risks in 5G Networks



5G Core Reference Point Architecture

Source: https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-session-management-function-smf

Which are the relevant 5G attack vectors?

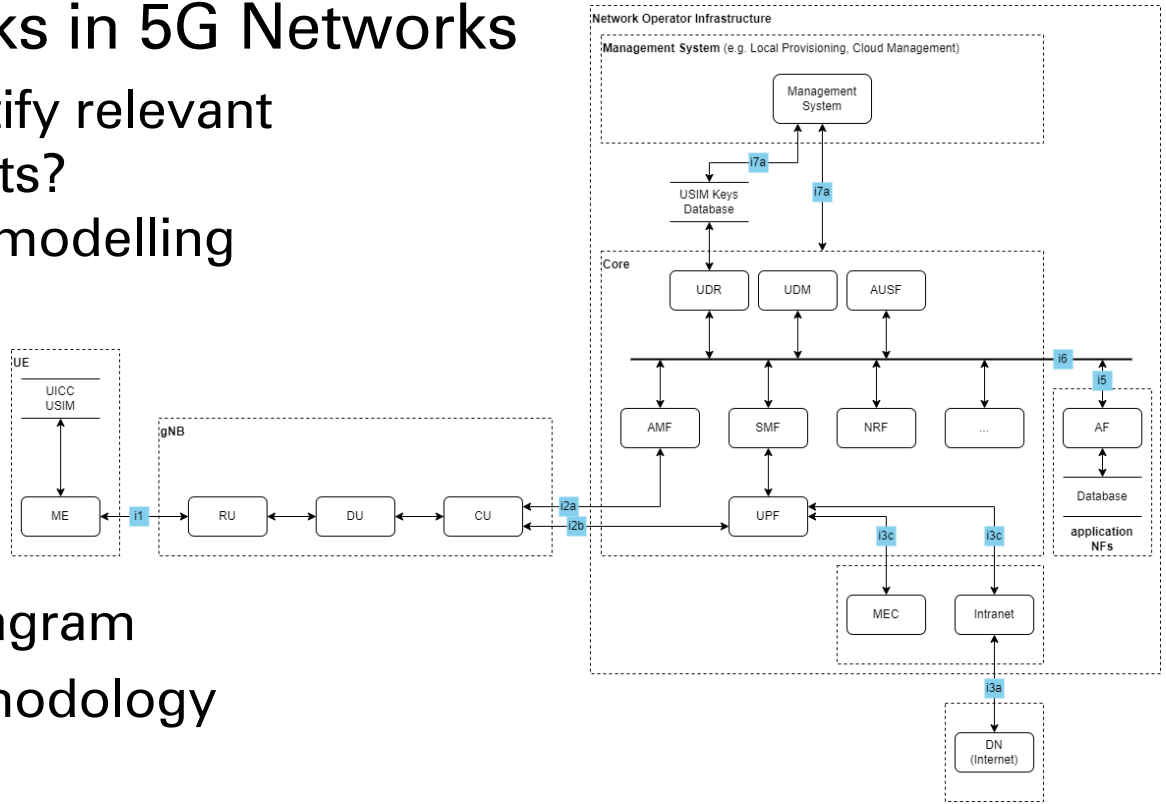
Focus on the devices (user equipment), or on the network (Radio Access Network/RAN, and Core Network)?

- Threats & Risks in Mobile Networks

  Current research and state-of-the-art (industry)

  – *On Security Research Towards Future Mobile Network Generations*, Rupprecht, David and Dabrowski, Adrian and Holz, Thorsten and Weippl, Edgar and Pöpper, Christina, 2017
    - includes threats on 4G and before
  – GSMA Mobile Security Research Acknowledgements
    - https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/
  – SCAS Documents
    - known threats and derived test cases
    - https://www.3gpp.org/dynareport?code=33-series.htm

- Threats & Risks in 5G Networks
  - How to identify relevant or new threats?
    → do threat modelling
  - Data flow diagram
  - STRIDE Methodology



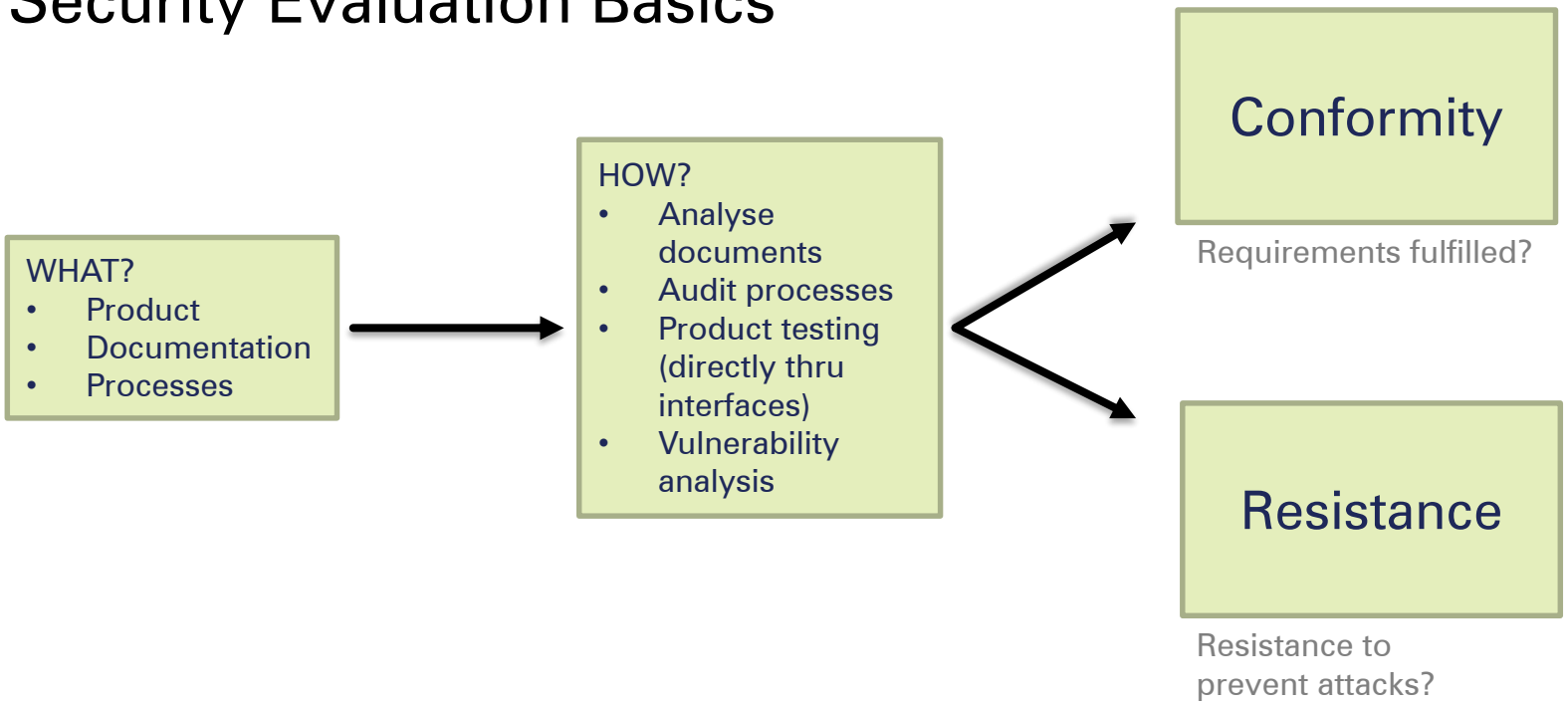
- Agenda
  - Introduction & Motivation
  - 5G Use-Cases & Internals
  - Threats & Risks in 5G Networks
  - → **Security Evaluation of 5G Components**
  - Future Challenges

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

- Safety vs. Security
  - Safety
    - condition of being protected against harmful conditions or events, or the control of hazards to reduce risk
  - (IT) Security
    - protection from attacks by malicious actors
- **What to “test” or evaluate these?**
  - Safety
    - Physical circumstances, measurement results, empirical values, …
    - *we already know the behaviour of something*
  - (IT) Security
    - implementation, configuration, interfaces, (continuous) state of the art, …
    - *we don’t know the full behaviour yet, new knowledge arises*

- Security Evaluation: two approaches (two cultures)
  - 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
  - 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



- 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) → vulnerability analysis → might lead to exploitable vulnerability in product interface

- Requirements for Testers/Evaluation Teams
  - Basic technical skills
    - Computer science, Communications engineering, …, MINT
  - Knowledge of the technology

    for example
    - Network product → TCP/IP, WAN technologies, WiFi, Bluetooth
    - Industrial components → Industrial real-time protocols, requirements in the industrial domain (functional and security)
  - Loves to learn new things (in a short timeframe)
    - and/or loves to learn the deep-insides of a specific technology
  - Team player: sharing knowledge and experience is key to run commercial evaluation projects

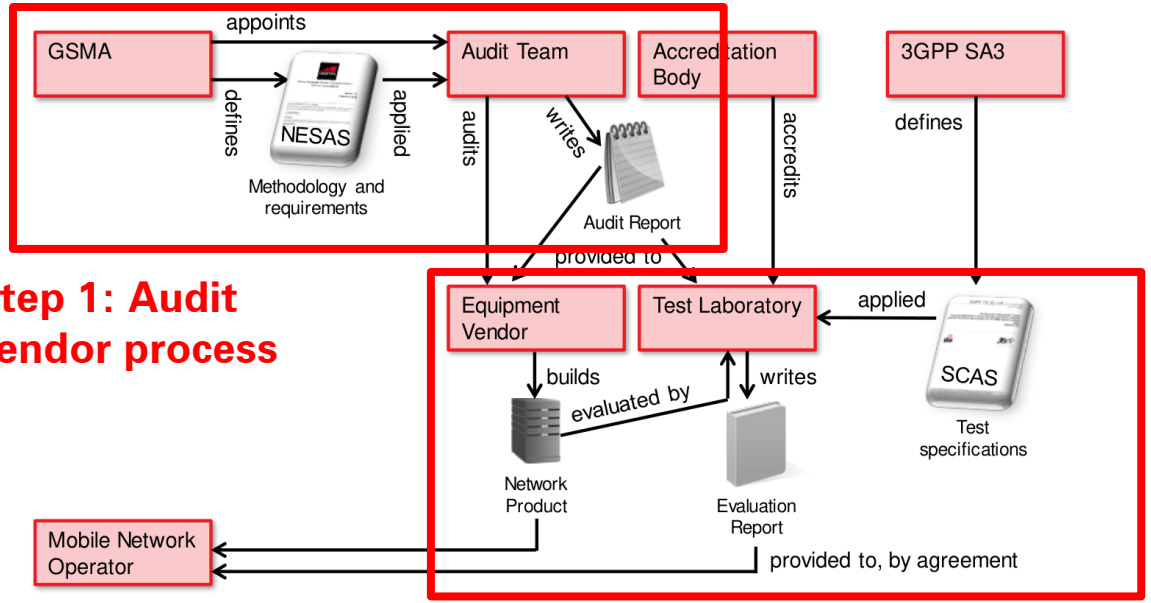
- Requirements for 5G Testers/Evaluation Teams
  - Knowledge of 3GPP terminology and concepts
    - major barrier to entry!
  - Basic protocols like HTTP, REST, TLS, OAUTH, …
  - Communication flows within 5G (physical/radio layer, different logical layers)
  - Deployment strategies: OpenRAN, Network Core Virtualization, Private 5G Scenarios/Devices
  - Knowledge how to read and analyse traffic captures (Wireshark) and tool results (different 5G testing tools are under development, e.g. Radix Security Tool)

- Security Evaluation Take-aways
  - Most evaluations/testing is done outside of labs (ITSEFs)
    - e.g. penetration testing, university research
  - (Certification) Evaluations require a lot of documentation
    - Common Criteria-style, standard used for 25+ years in high-security / governmental environments
  - Alternatively, black-box methodologies are available
    - European FIT-CEM approach (fixed-time evaluation)
  - Industry is interested in specification-based approaches
    - uncertainties of security testing is a risk for product availability

- 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: 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

NESAS, FS.16 – NESAS Development and Lifecycle Security Requirements v.2.0

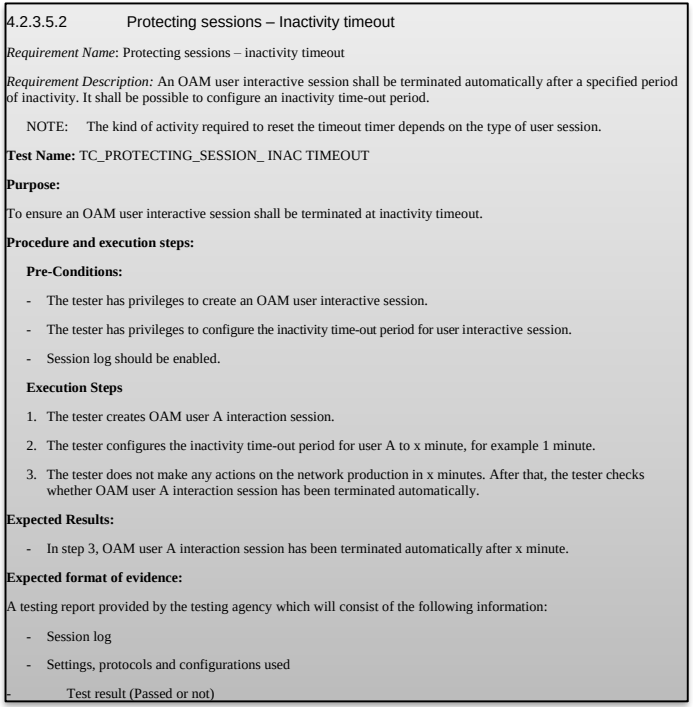
- Step 2: Evaluation network component
  - Need for testing requirements
  - SCAS documents from 3GPP

TS 33.116 Security Assurance Specification (SCAS) for the MME network product class
TS 33.117 Catalogue of general security assurance requirements
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 class
TS 33.512 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
…

  - Set of SCAS documents refers to 3GPP-Release
    - current 3GPP-Release 16

- Evaluation network component
  - makes use of 3GPP **Security Assurance Specifications (SCAS)**
  - Two categories:
    - one document for common vulnerabilities / IT Interfaces
      - 33.117 Catalogue of general security assurance requirements
    - one set of documents for each 5G network function (NF) / 3GPP functionality
      - 33.116 Security Assurance Specification (SCAS) for the MME network product class
      - 33.216 SCAS for the evolved Node B (eNB) network product class
      - ...

- NESAS Schema
  - 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



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:

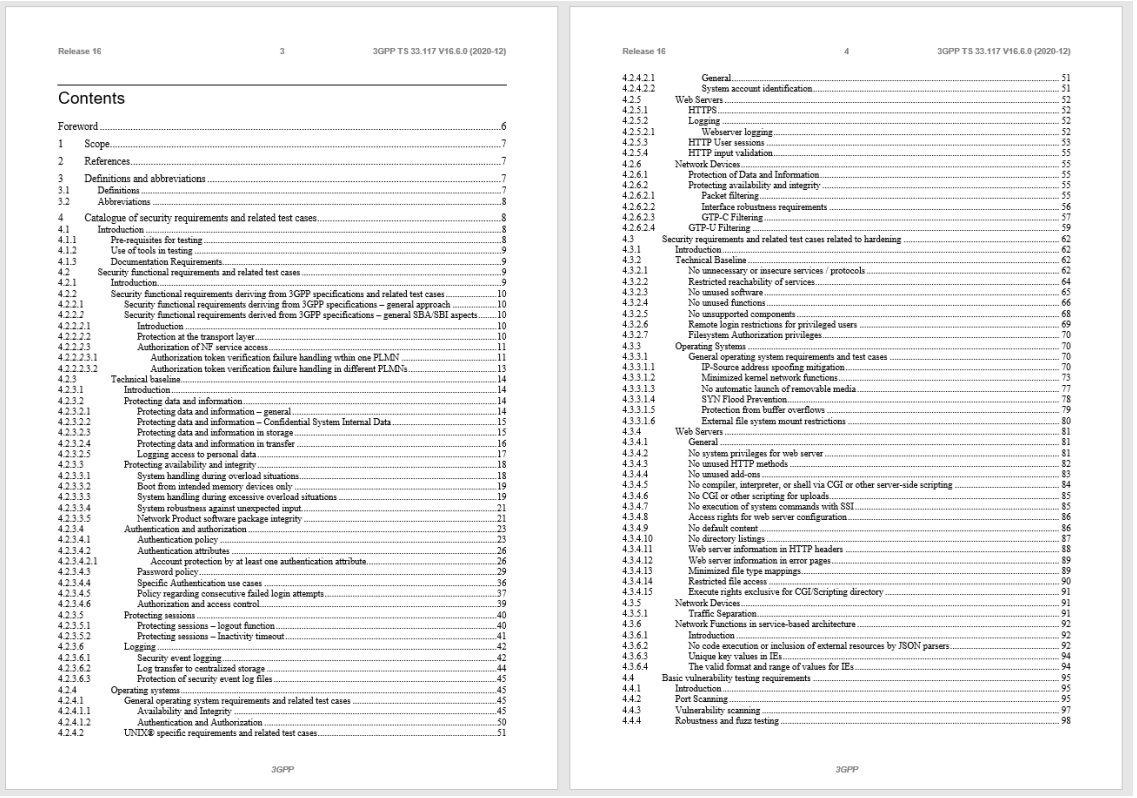
- In step 3, OAM user A interaction session has been terminated automatically after x minute.

Expected format of evidence:

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

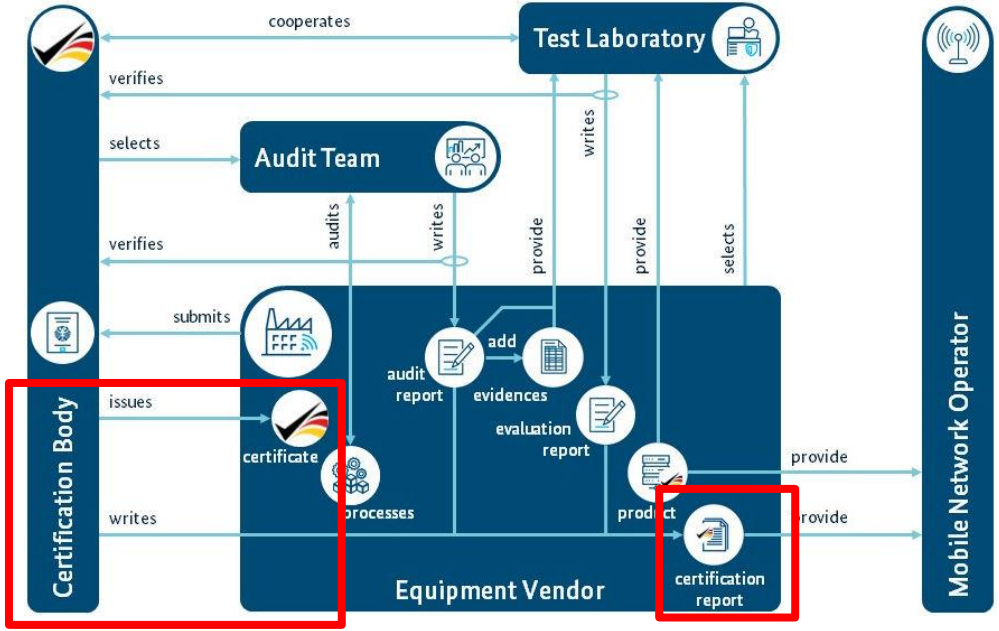
- Session log
- Settings, protocols and configurations used
- Test result (Passed or not)

- 3GPP TS 33.117 Catalogue of general security assurance requirements



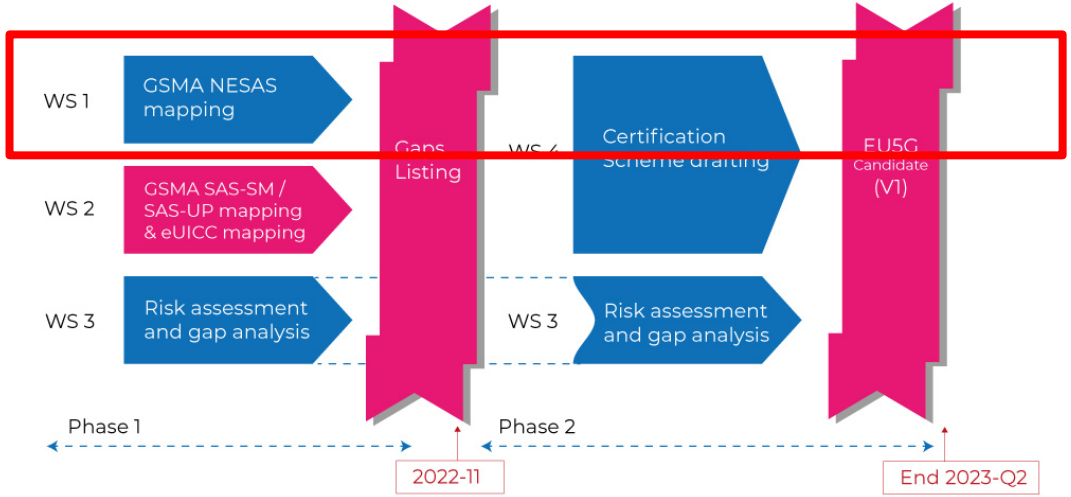
Contents

- NESAS accepted as baseline for German Scheme



Source: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/Ablauf_Verfahren/Ueberblick_node.html

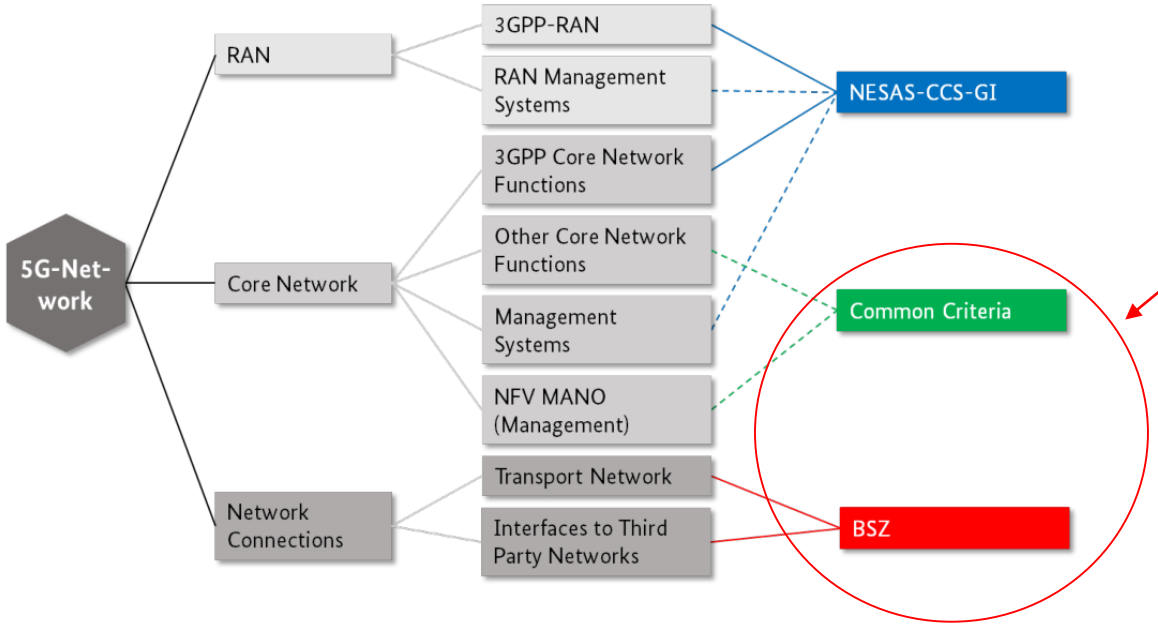
- NESAS accepted for EU approach
  - preparation of European Scheme work in progress



EU5G AHWG Milestones

Source: ENISA — 3GPP/SA3 2022-11-15 & https://www.3gpp.org/news-events/3gpp-news/sa3-enisa

BSI 5G Certification Strategy



additional, generic Certification schemes

Source: BSI, TR-03163: Security in Telecommunications Infrastructure, Annex A, Version 1.1

- 5G Security Evaluation
  - performed by ITSEF (IT Security Evaluation Facility)
    - or lab, works according to ISO/IEC 17025
  - 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
  - fast 3GPP release cycle

- 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

- 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 model 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 5G network?** Tool-based, automatically?

- Agile evaluation/certification process
  - Industry complains security evaluation limits innovation in products
  - Evaluation requires support/resources from vendors
    - Support of ITSEF (ship release, support testers, respond to feedback, …)
    - Need of additional release after ITSEF feedback
  - **Open question: Can we incorporate evaluation activities in CI/CD pipelines? e.g. make evaluation an automatic task**

- 5G Testing Tool Development
  - NESAS and SCAS already defined a set of test cases
  - Currently tools are developed to automatically run these test cases
  - Currently, the test execution need massive configuration and adaption efforts, product are not ready for testing
  - **Open question: Can we develop an ecosystem of test tools and standardized test interfaces?** Needs for implementation in 5G components.

secuvera

Cybersicherheit. Nachhaltig.

Vielen Dank!
Thank you!

...and more slide!

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

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart
Germany

- Are you interested in an 5G security internship, part-time or full-time job?
  - secuvera recently started a 5G research project and needs support!
  - our project:
    - **OP-NESAS**
    - project partners: secuvera, Radix Security & Campus Genius
    - 24 month, between 01/2022 and 12/2023
    - project website coming soon
  - direct contact: sfritsch@secuvera.de
  - visit: https://www.secuvera.de/unternehmen/karriere/