



CCI Seminar

5G Technologies Overview: Opportunities and Challenges for Secure Data Exchange Infrastructure

Dr. Yuri Demchenko
CCI Seminar 4 June 2020
University of Amsterdam



Outline

- 5G Technologies Overview
 - Roadmap, use cases and components
 - Architecture and Cloud Native Network Functions
 - Network slicing
 - Security Architecture (as 5G potentially will become dependable critical infrastructure)
- Concerns in 5G roll-out
 - Huawei 5G and security concerns
- Opportunities and Challenges for Secure and Trusted Data Exchange Infrastructure
 - Dedicated E2E network slices for IoT network
 - Potentially easy integration with cloud based applications (5G cloud native network and native cloud applications)

Disclaimer: All images in this presentation are taken from multiple published source.
All right remains at authors of the published sources. All trademarks are acknowledged



5G Technologies Overview

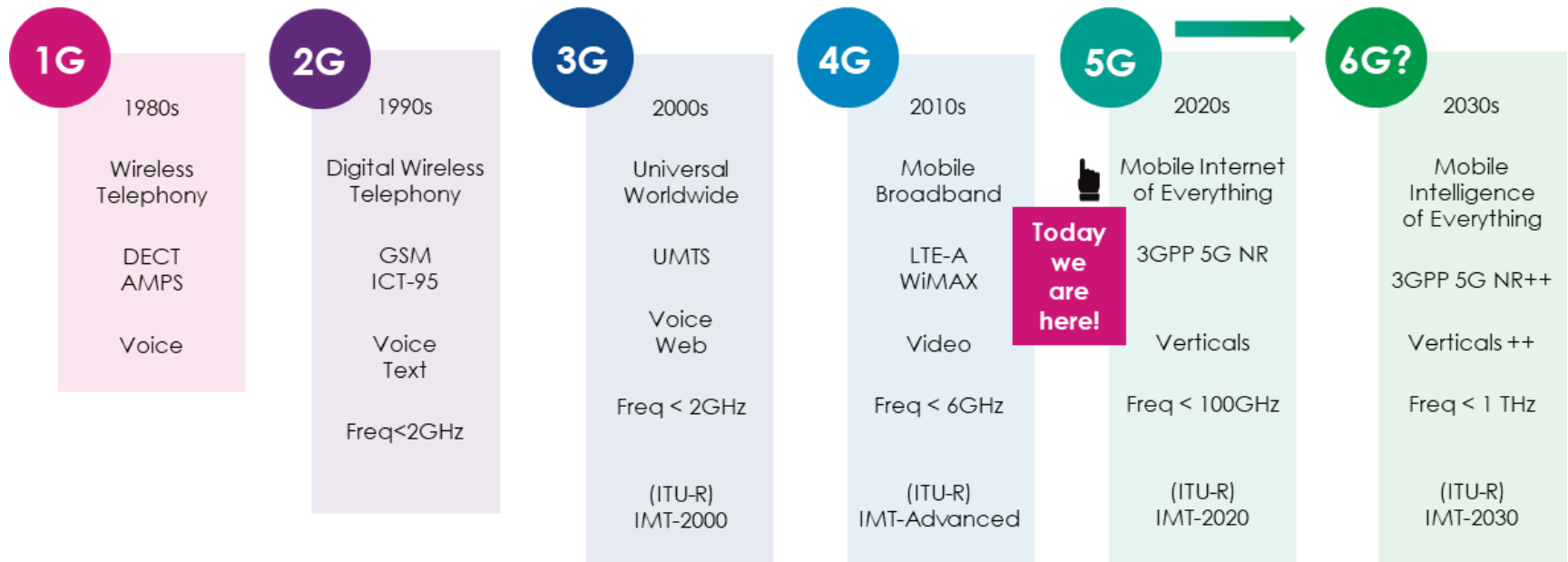
- Timeline and basics
- Use cases
- Architecture components



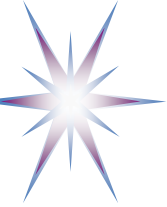
EU and NL involvement into 5G development

- EU and NL actively participate and play leading role in 5G development
- The following frequencies will be used in EU
 - 700 MHz, 3.5 GHz, and 26 GHz.
- Nederland will additionally use 1.4 GHz and 2.1 GHz
 - <https://stralingsbewust.info/2019/10/25/5g-waar-staan-de-zendmasten-voor-test-uitzendingen/>

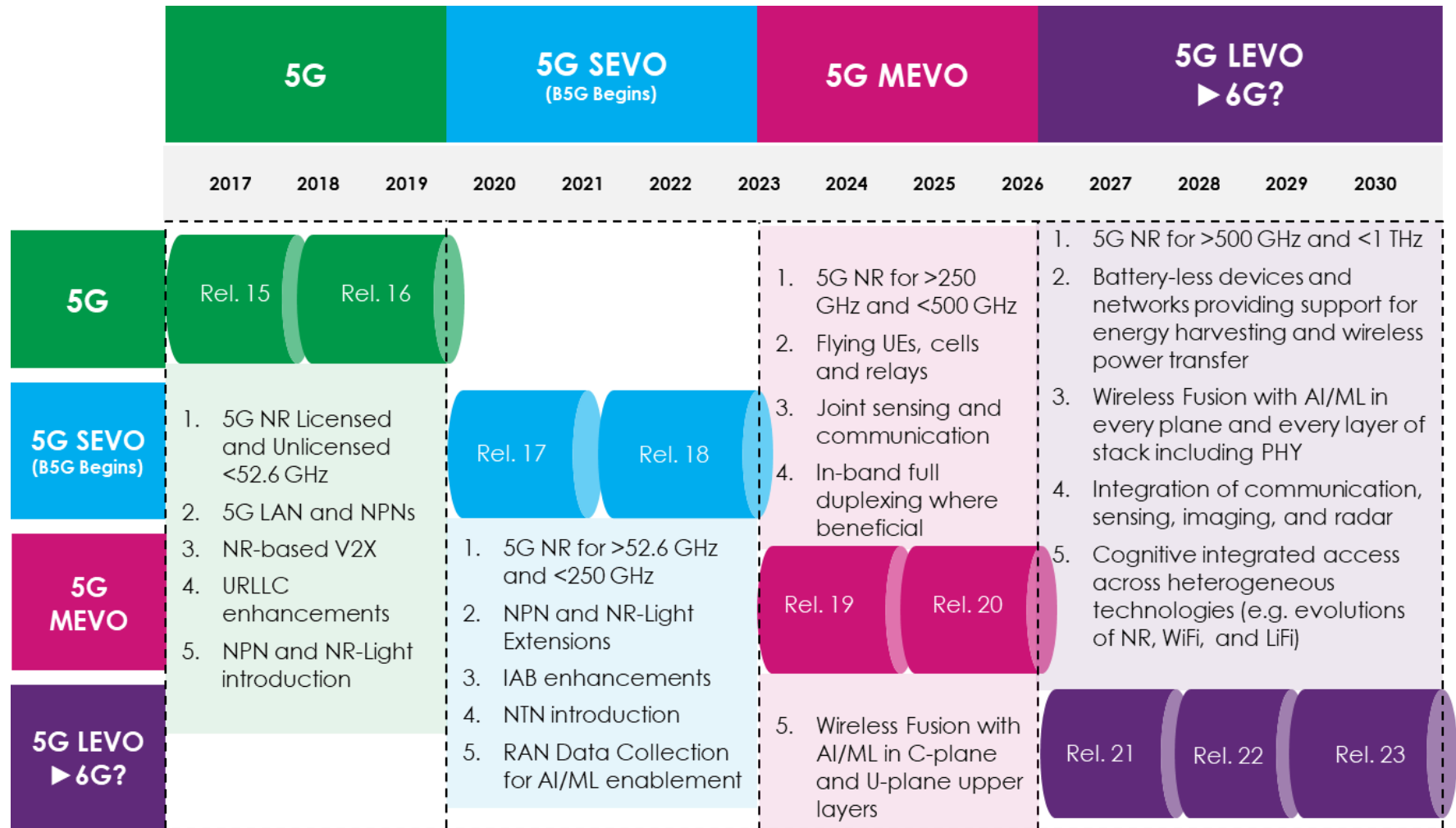
EU Project EMPOWER Roadmap Scope

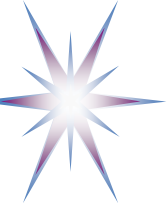


- ***Complete roadmap and related scientific areas*** will be developed in order to embrace the multi-resource composition (***IoT, Wireless, Cloud/HPC, Data/AI***) of the future Internet/digital infrastructures.



Baseline Technology Roadmap from a 3GPP-Release perspective





Usage Scenarios

Usage scenarios of IMT for 2020 and beyond

Enhanced mobile broadband

Gigabytes in a second



3D video, UHD screens



Work and play in the cloud

Smart home/building



Augmented reality



Industry automation



Mission critical application



Self driving car



Voice



Smart city



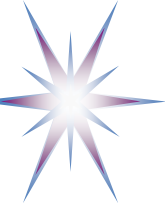
Future IMT



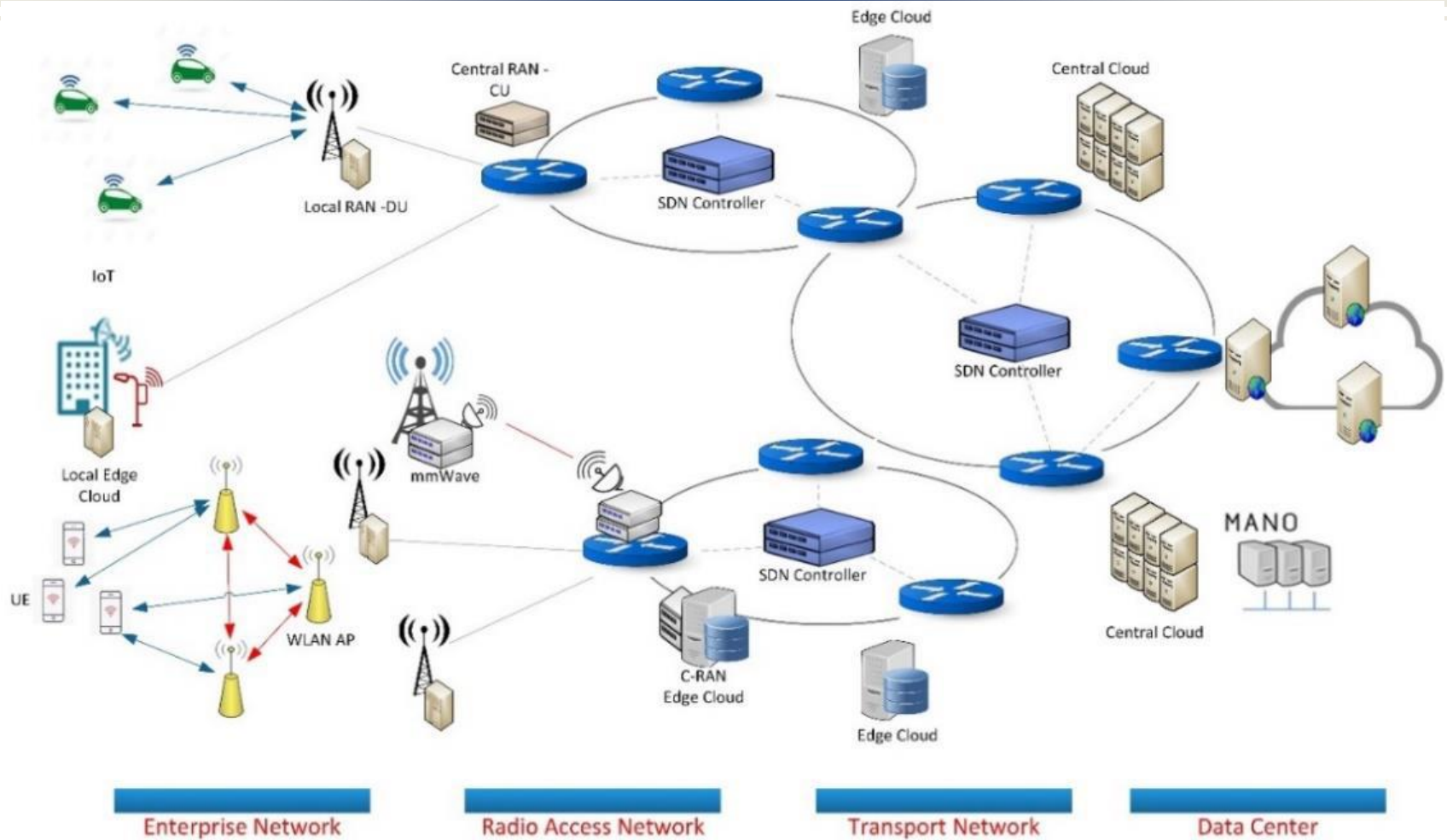
Massive machine type communications

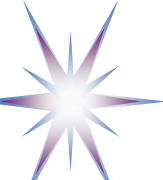
Ultra-reliable and low latency communications

- Enhanced Mobile Broadband (eMBB)
 - Incl new Frequencies
- Massive Machine Type Communications (mMTC)
- Ultra Reliable and Low Latency Communications (URLLC)



Physical Architecture



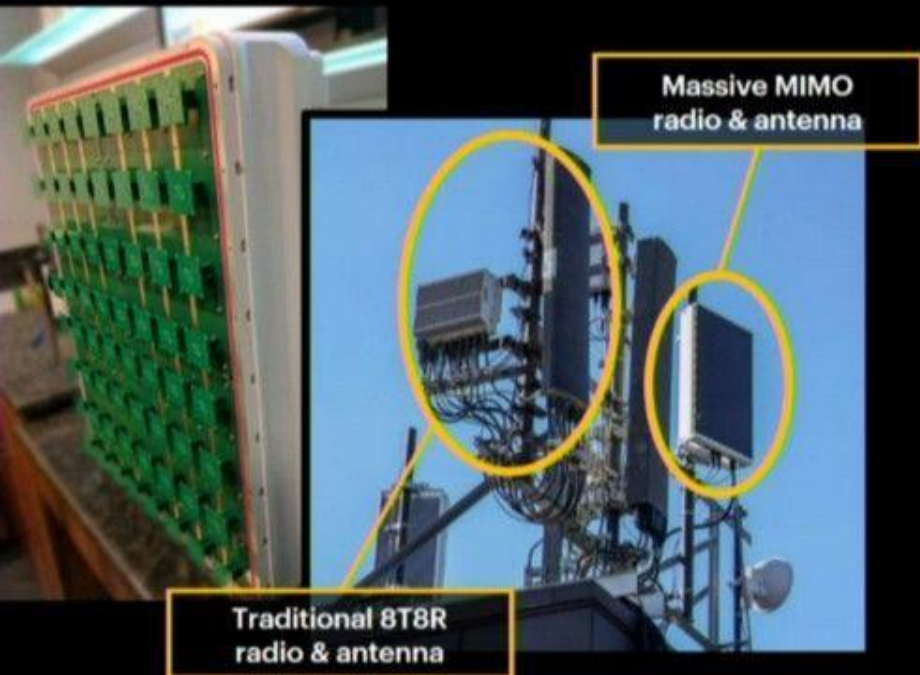


Example: Sprint in US

Sprint is leveraging **Massive MIMO** at 2.5 GHz for LTE Advanced and 5G



64T64R Massive MIMO

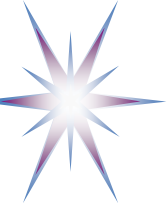


32 LTE Massive MIMO Sites at Super Bowl 53
25TB of data on Super Bowl Sunday – 157% increase from Super Bowl 52



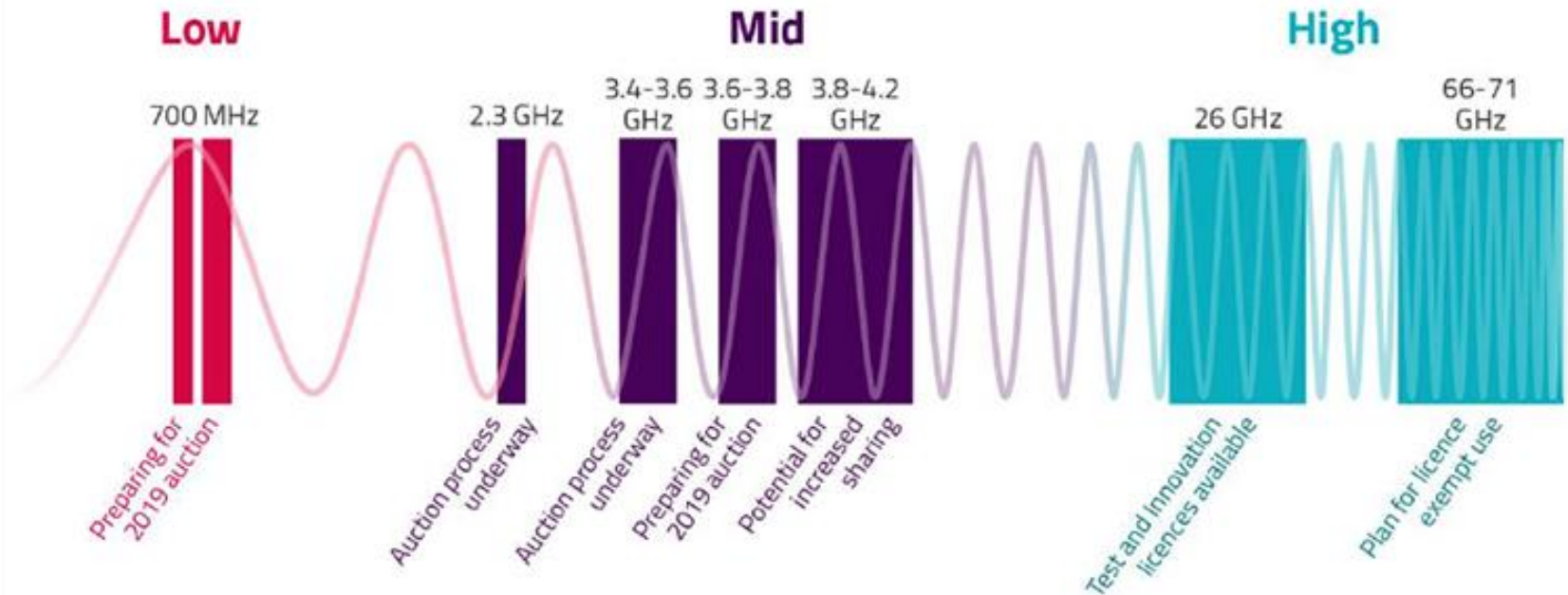
IEEE.tv

©2019 Sprint. This information is subject to Sprint policies regarding use and is the property of Sprint and/or its relevant affiliates and may contain exempted, confidential or privileged materials intended for the sole use of the intended recipient. Any review, use, distribution or disclosure is prohibited without authorization.



5G Spectrum and Data Speed

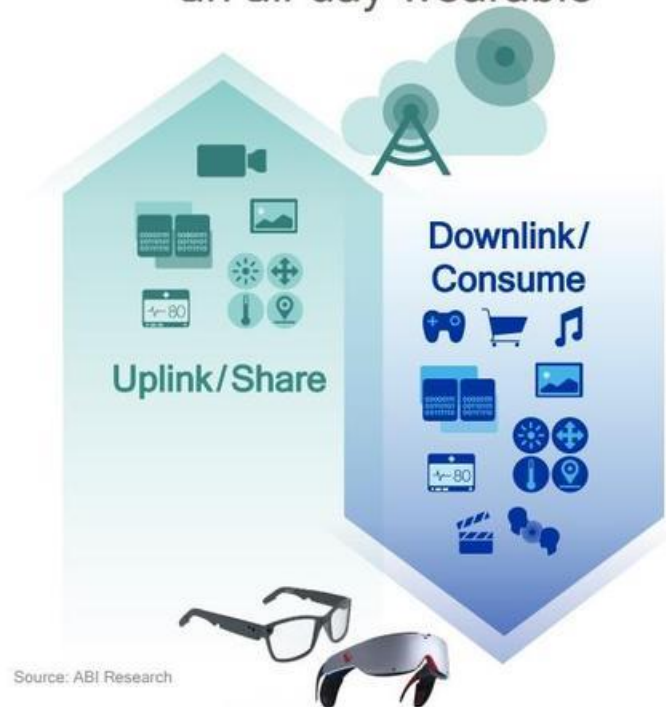
Spectrum pipeline



AV (Automotive Vehicles), VR (Virtual Reality), AR (Augmented Reality)

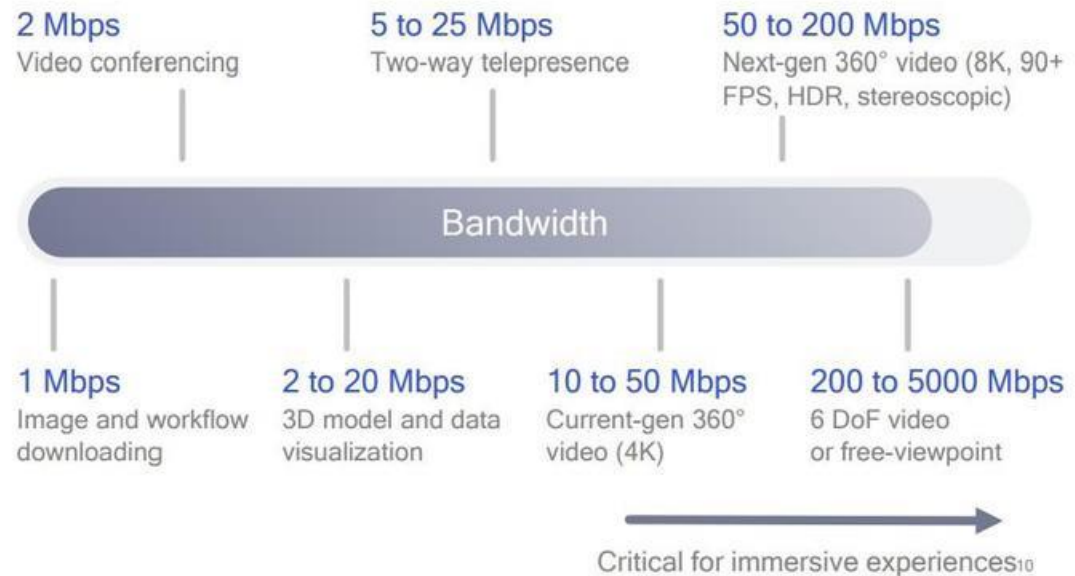
VR and AR require efficient increase in wireless capacity

Constant up/download on an all-day wearable

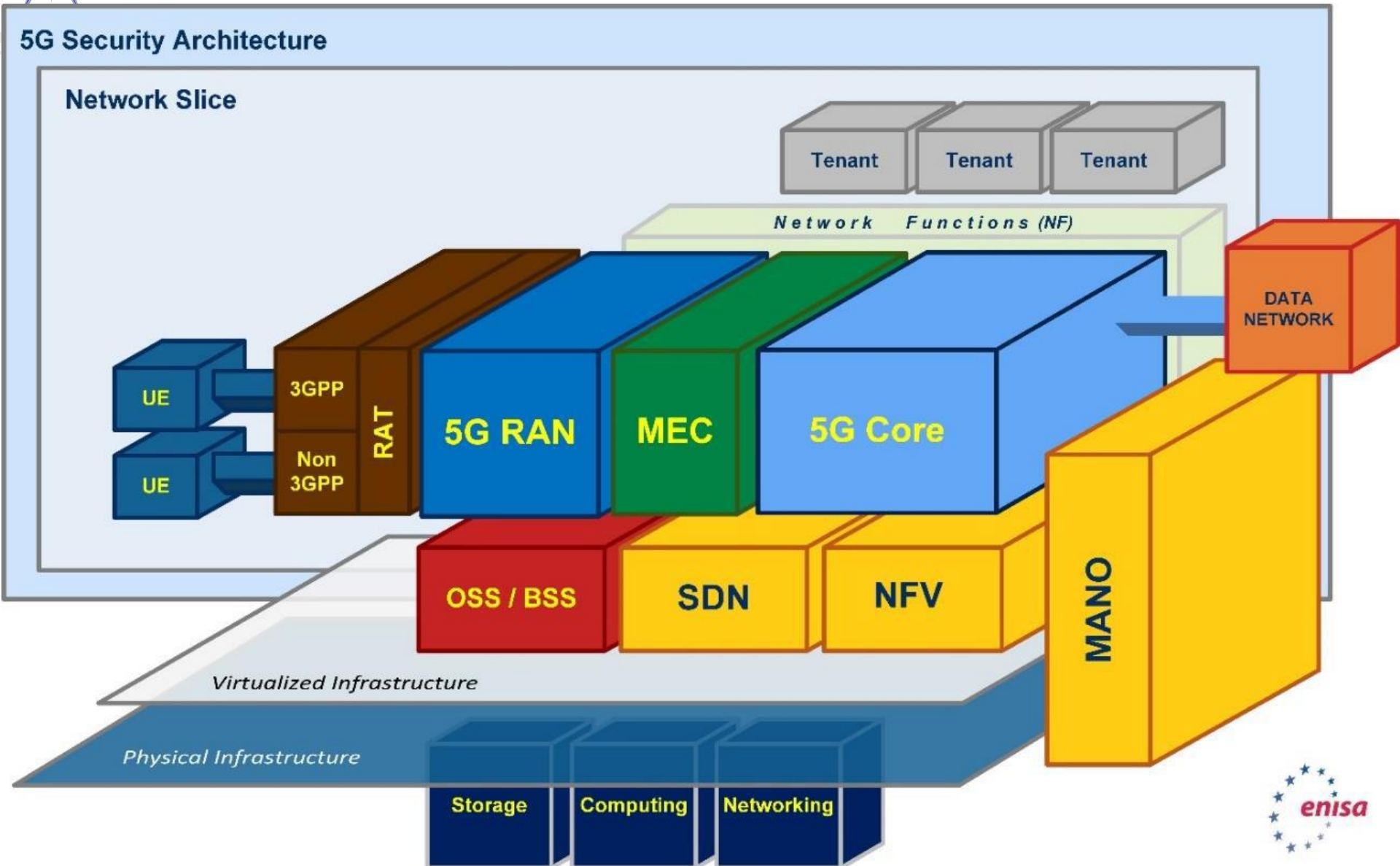


Richer visual content

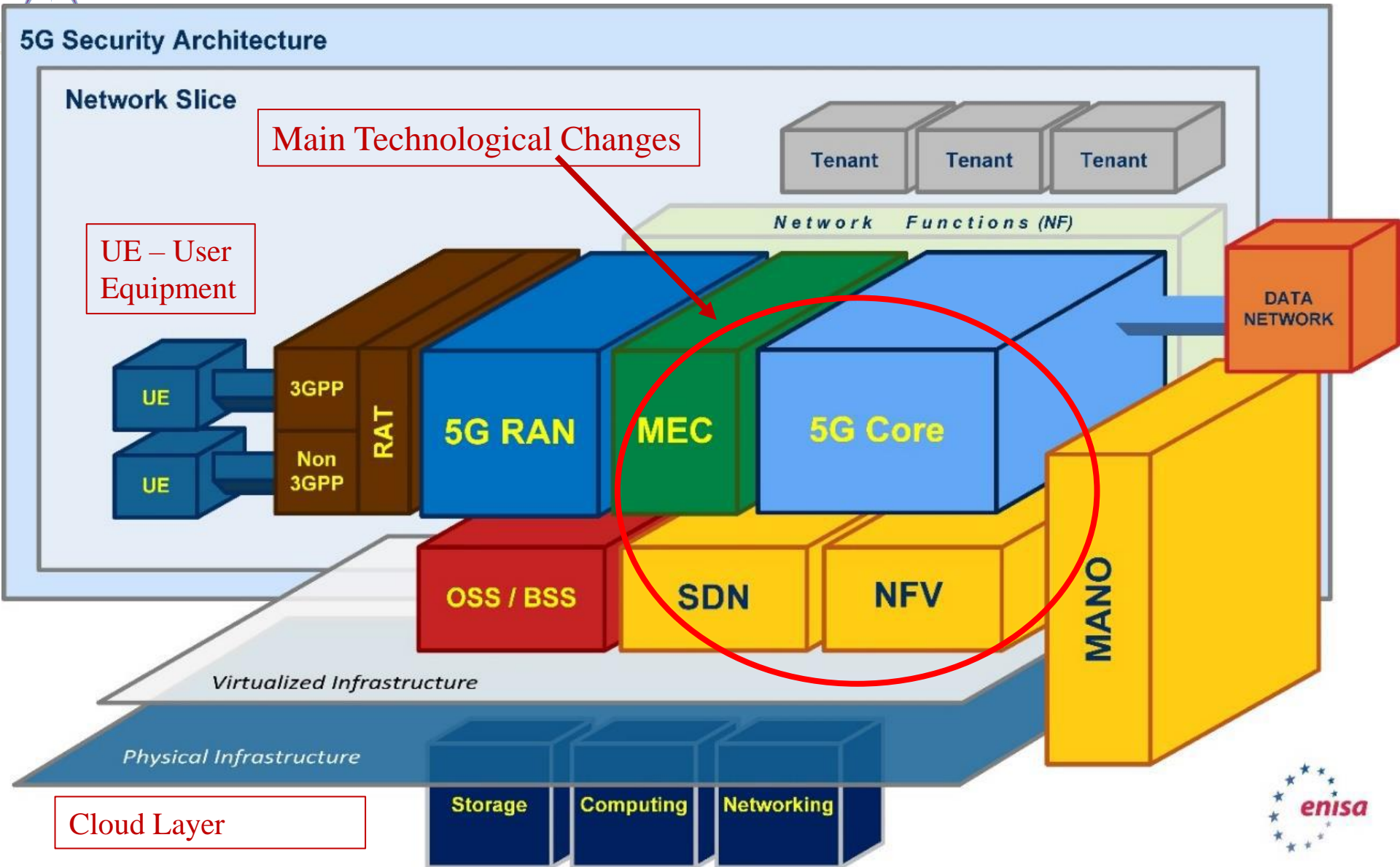
- Higher resolution, higher frame rate
- Stereoscopic, High Dynamic Range (HDR), 360° spherical content, 6 DoF

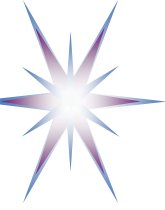


5G High-level Technical Architecture (ENISA)

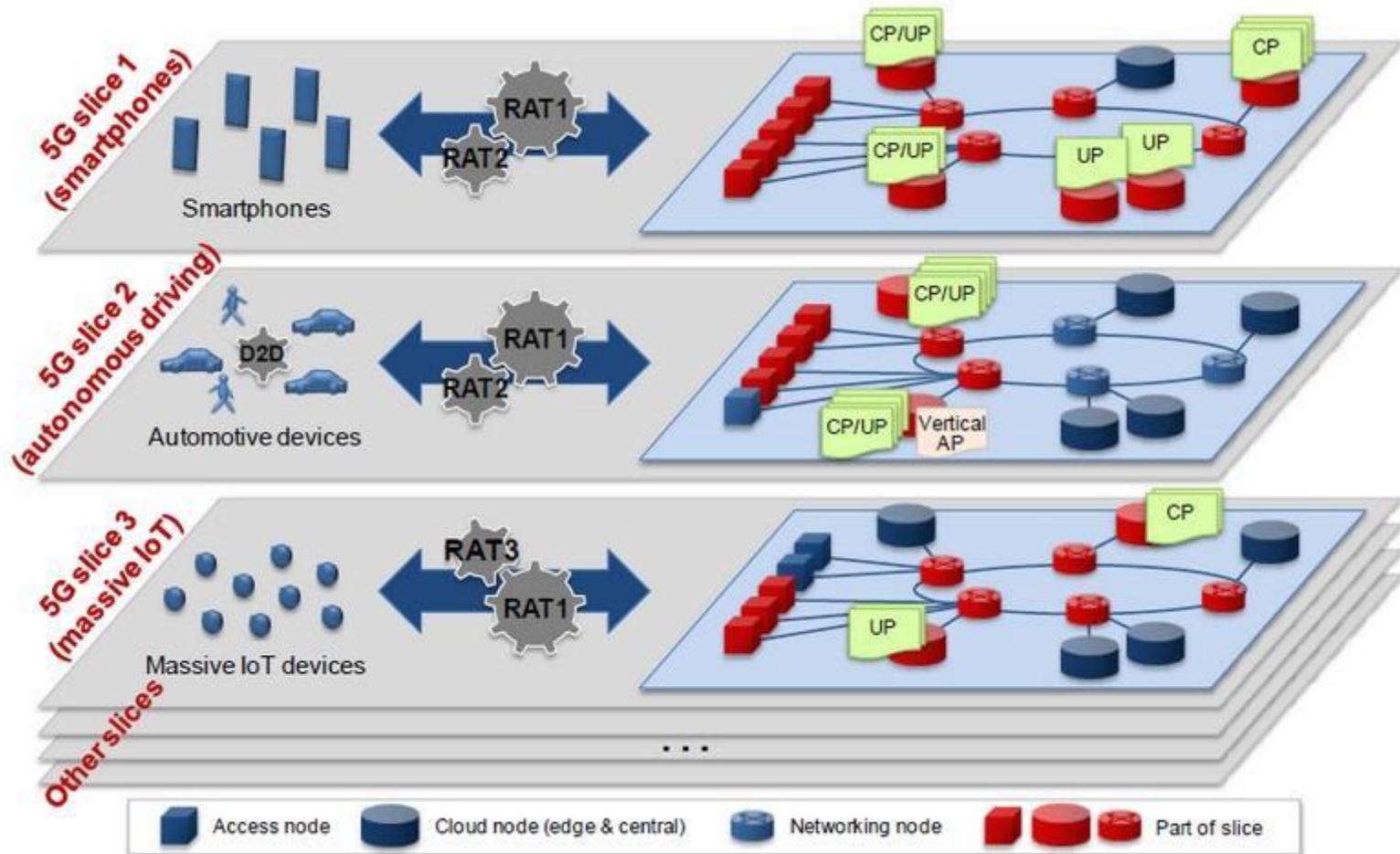


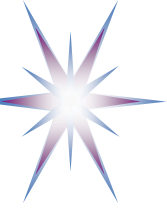
5G High-level Technical Architecture (ENISA)





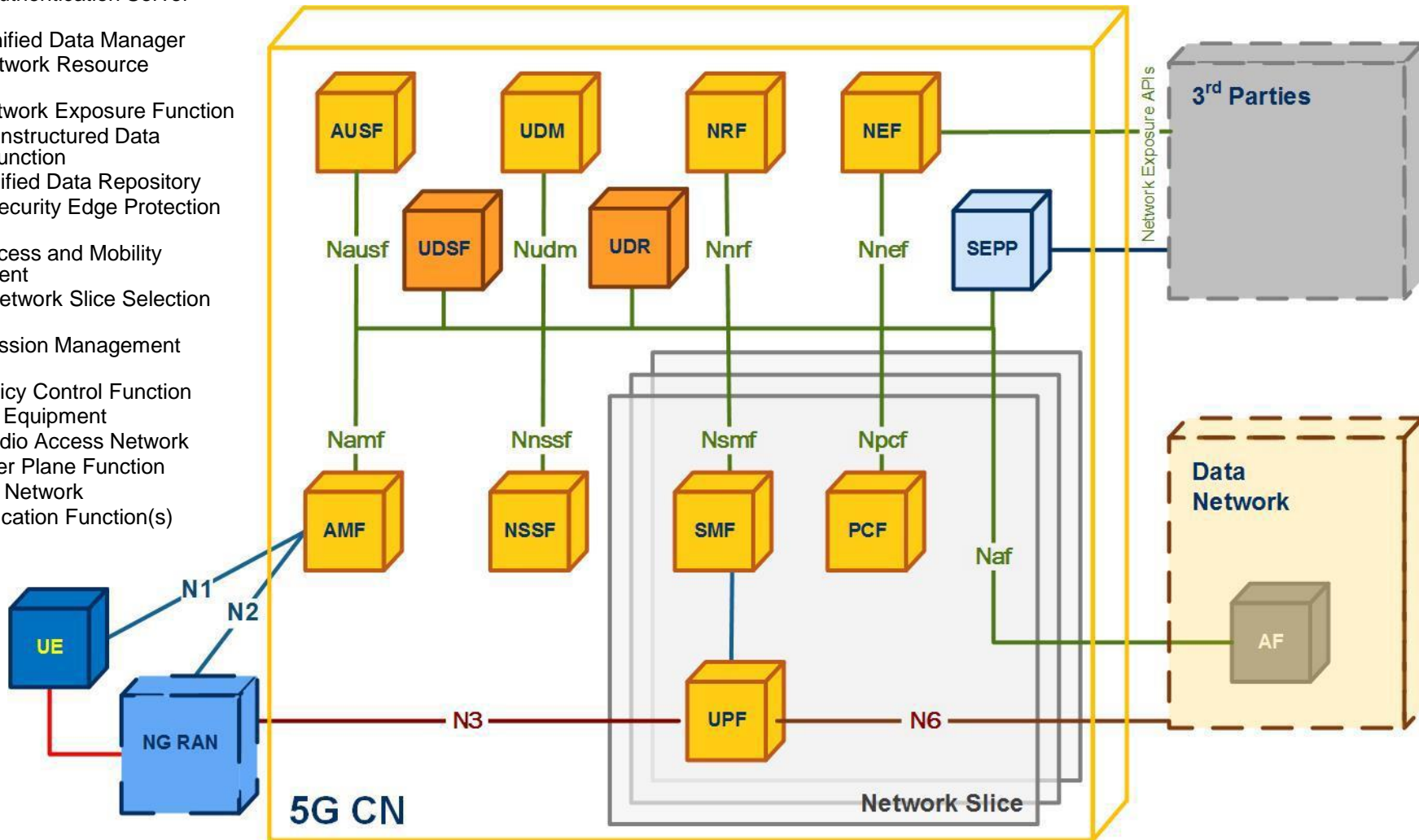
5G Core Network Slicing



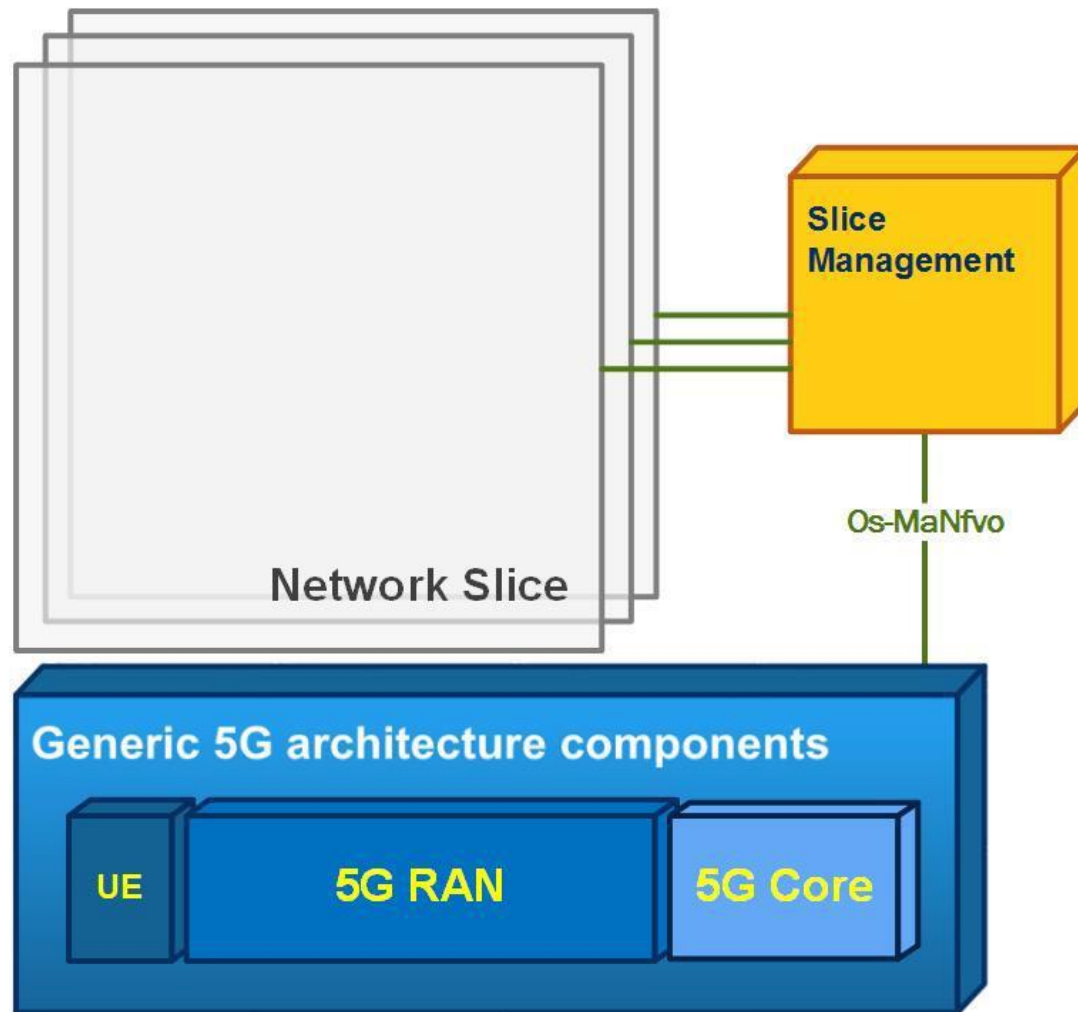


Core network architecture and slicing zoom-in

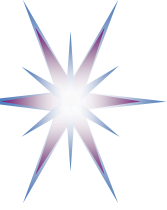
- AUSF – Authentication Server Function
- UDM – Unified Data Manager
- NRF – Network Resource Function
- NEF – Network Exposure Function
- UDSF – Unstructured Data Storage Function
- UDR – Unified Data Repository
- SEPP – Security Edge Protection Function
- AMF – Access and Mobility Management
- NSSF – Network Slice Selection Function
- SMF – Session Management Function
- PCF – Policy Control Function
- UE - User Equipment
- RAN – Radio Access Network
- UPF – User Plane Function
- DN - Data Network
- AF – Application Function(s)



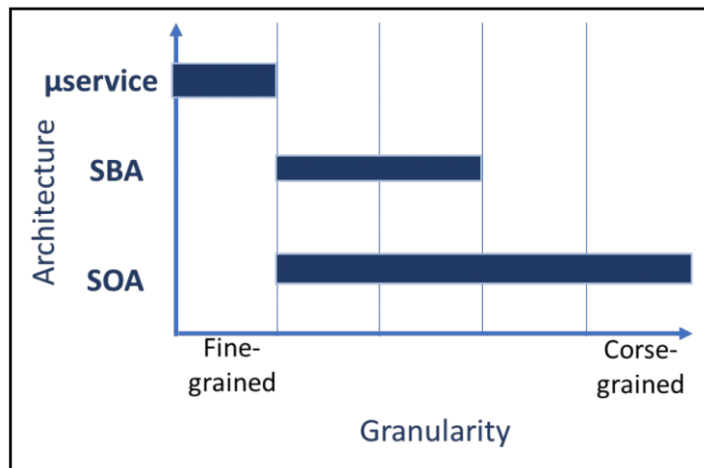
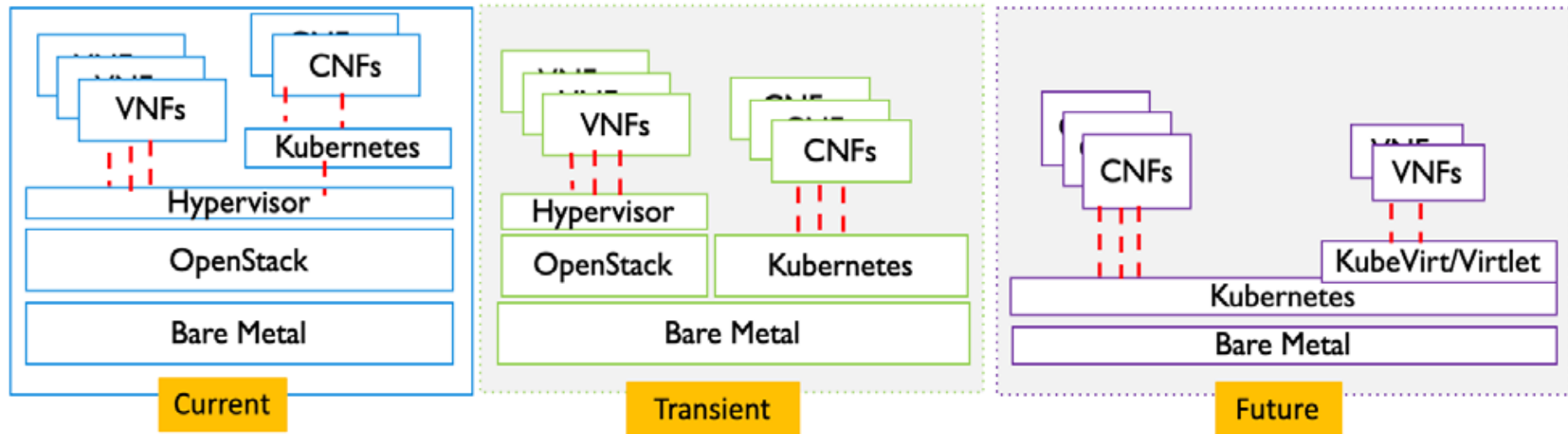
Dependencies of slices with the generic 5G architecture components



[ref] ENISA Threats Landscape for 5 G Networks, Nov 2019

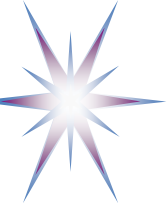


Evolution to Cloud Native Ecosystem



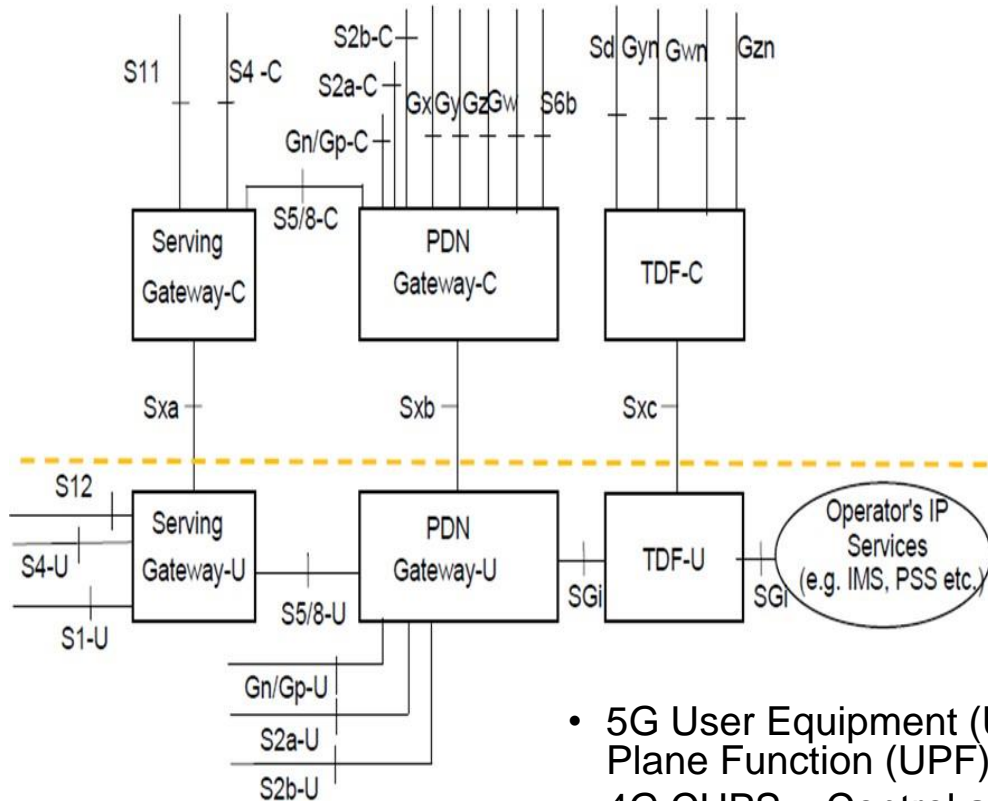
- Cloud Native: SBA vs SOA
 - Focus on microservices
 - RESTful interface
- SBA - Service Based Architecture
- SOA – Service Oriented Architecture
- Kubernetes platform still to advance on network virtualization and isolation

[ref] A 5G Americas White Paper. 5G and the Cloud, Dec 2019

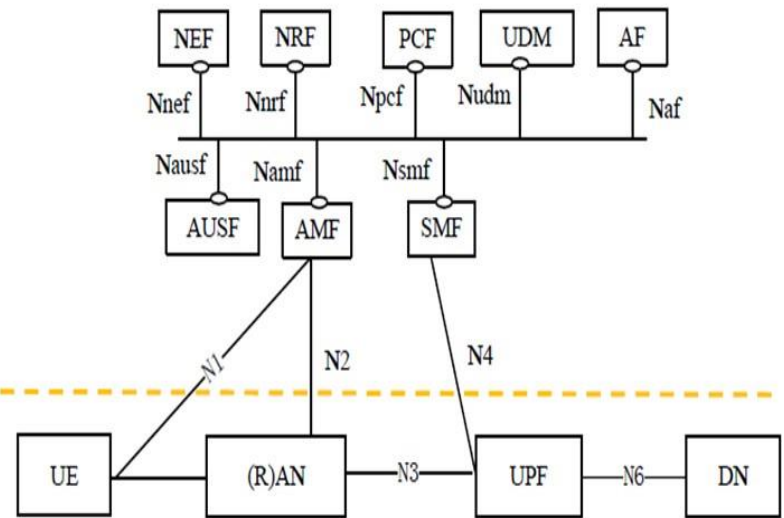


Comparison 4G and 5G SBA Model: Transforming vertical NFV stack into composable SBA services

4G Core Using "CUPS"

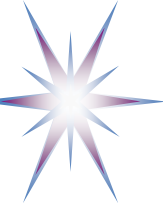


5G Core Using Service-based Architecture

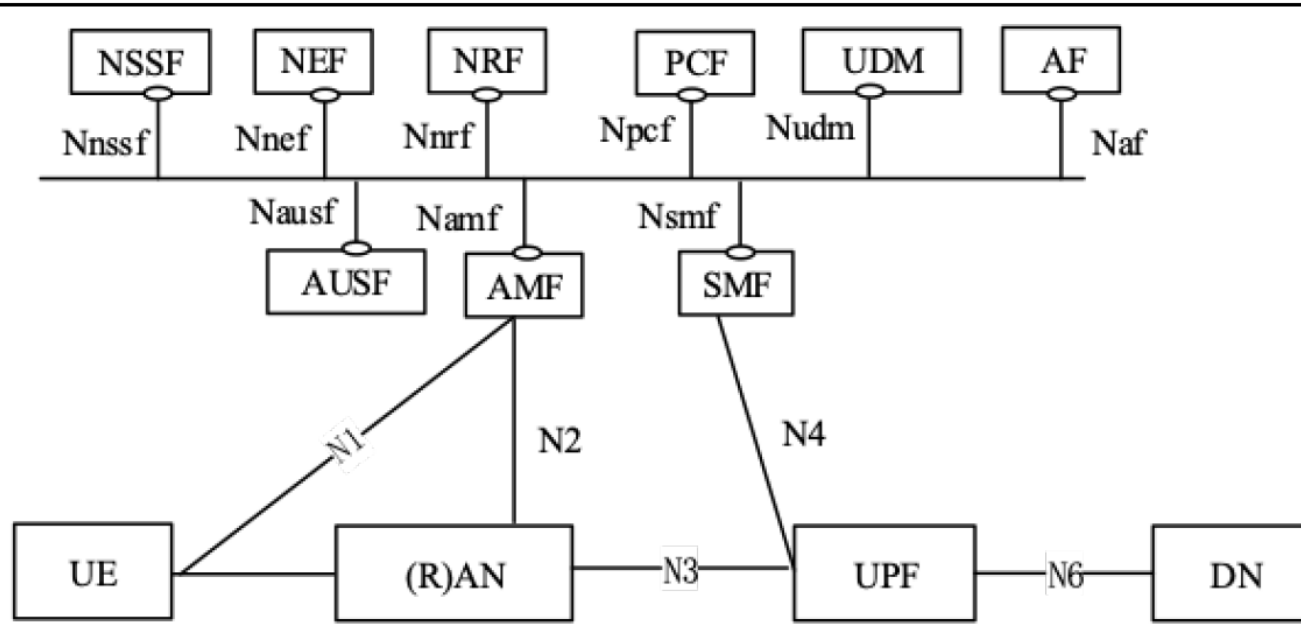


- 5G User Equipment (UE) – (Radio) Access Network (RAN) – User Plane Function (UPF) – Data Network (DN)
- 4G CUPS – Control and User Plane Separation
- **4G vertical stack vs 5G cloud native layering model**

[ref] Service Based Architecture for 5G Core Network, Heavy Reading White Paper, Sponsored by Huawei, 2017



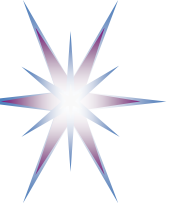
5G-3GPP Architecture based on SBA Functions



- User Equipment (UE)
 - (Radio) Access Network (RAN)
 - User Plane Function (UPF)
 - Data Network (DN)
- AUSF – Authentication Server Function
- AMF – Access and Mobility Management
- SMF – Session Management Function

- NSSF – Network Slice Selection Function
 - This module is responsible for selecting the 5G network slice instance serving User Equipment (UE) and which AMF, or list of AMFs, can be used by a device (UE)
- NEF – Network Exposure Function
- NRF – Network Resource Function
- PCF – Policy Control Function
- UDM – Unified Data Manager
- AF – Application Function(s)

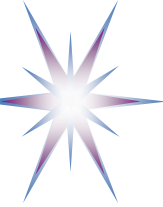
[ref] A 5G Americas White Paper. 5G and the Cloud, Dec 2019



VMs vs Containers: Test by Cloud Native Computing Foundation (CNCF, 2020)

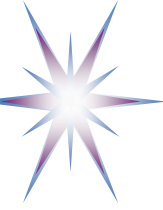
	OpenStack	Kubernetes
Infra deploy time	~65 minutes	16 minutes*
NF deploy time	3 minutes, 39 seconds	< 30 seconds
Idle state RAM	17.8%	5.7%
Idle state CPU	7.2%	0.1%
Runtime NF RAM	17.9%	10.7%
Runtime NF CPU	28.8%	39.1%
Snake case PPS	3.97 million PPS	4.93 million PPS
Snake case latency	~2.1 milliseconds	~2.1 milliseconds
Pipeline case PPS	N/A	7.04 million PPS

https://docs.google.com/presentation/d/1nsPINvxQwZZR_7E4mAzc-50eFCBhbCHsmik6DI_yFA0/edit#slide=id.g5036f143e9_3_672

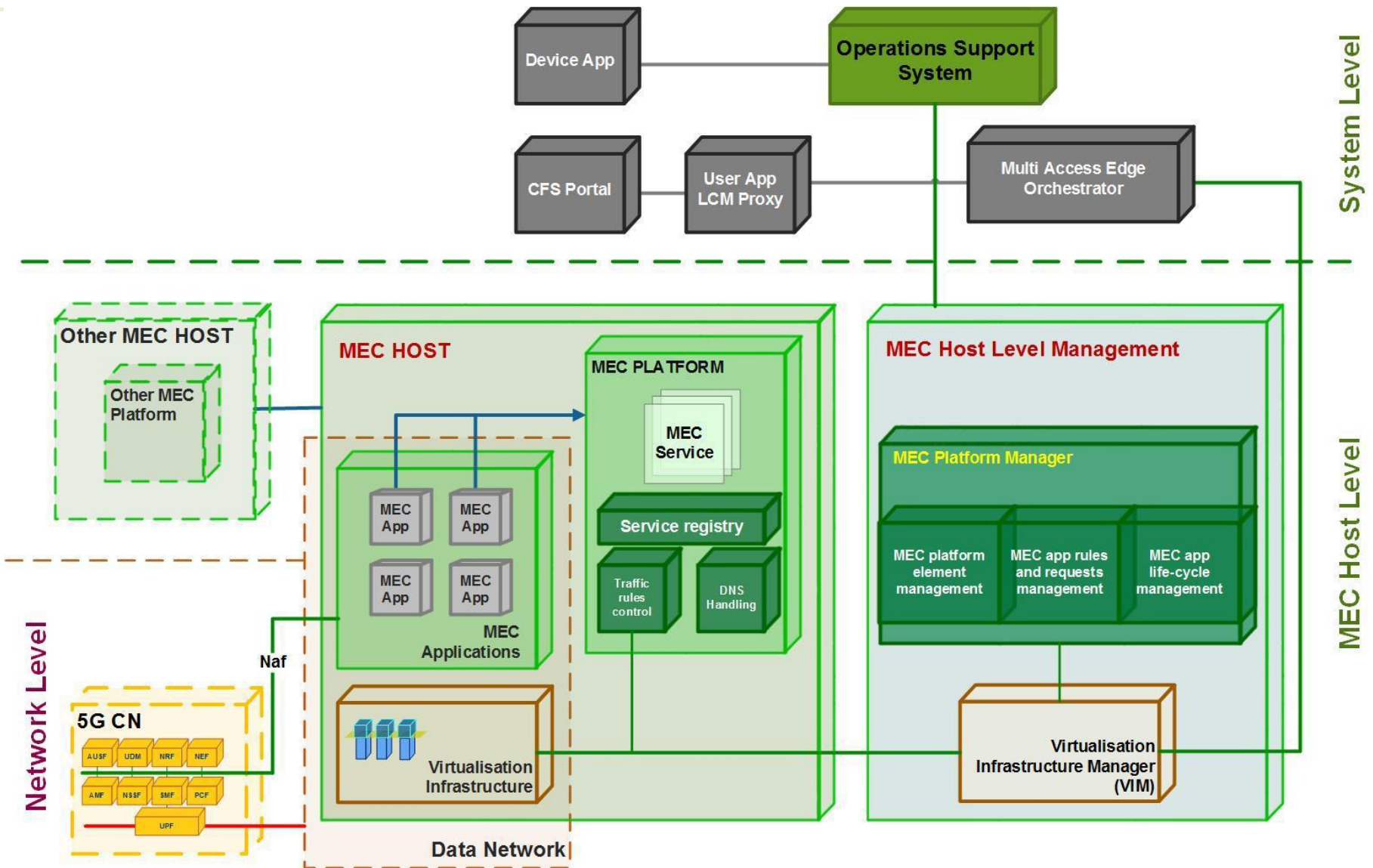


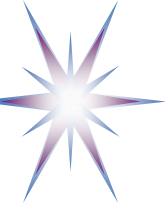
Benefits Cloud Native Approach: Re-usable/Composable Network Components

- Service Based Architecture
 - Vs Service Oriented Architecture
- Cloud Native approach and tools
 - Including DevOps
- VMs vs Containers
 - Noisy neighbor factor is known in Kubernetes
 - But network infrastructure has known type of workload

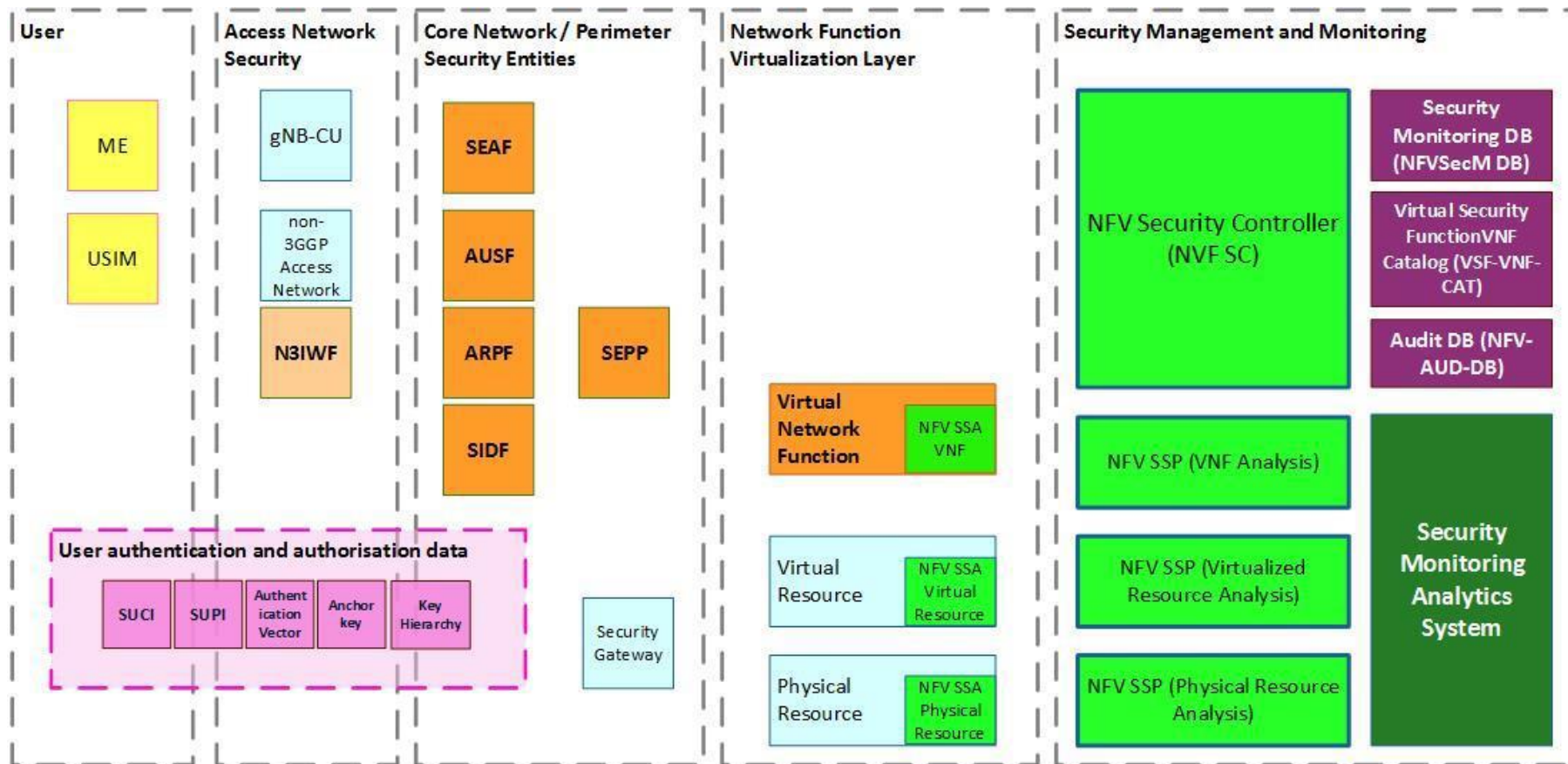


MEC (Mobile Edge Computing) Architecture

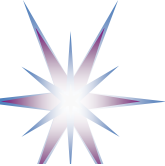




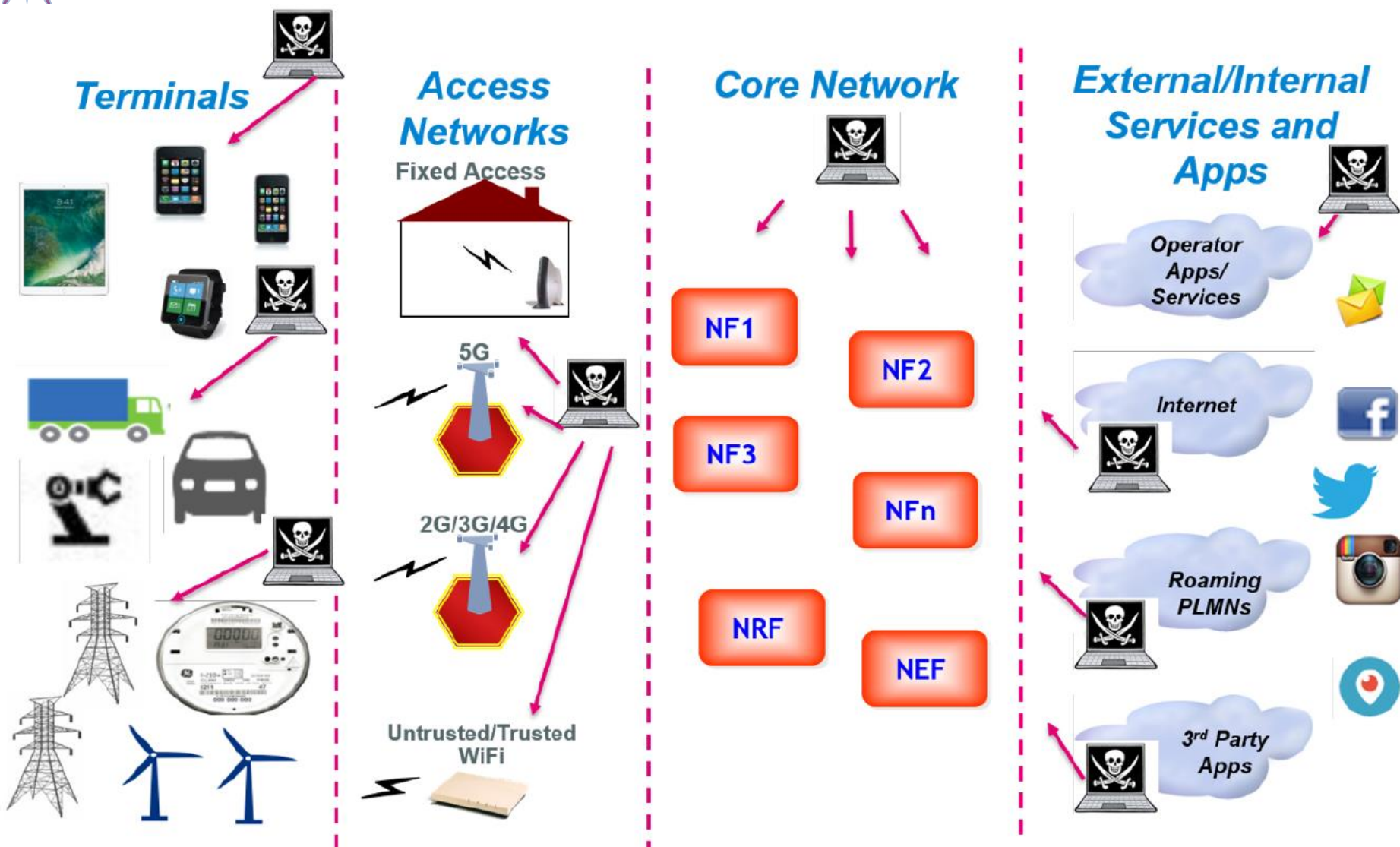
5G Security Architecture



[ref] ENISA Threats Landscape for 5 G Networks, Nov 2019



5G Threats Landscape

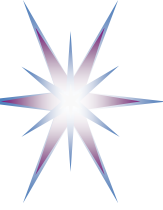


[ref] A 5G Americas White Paper. The Evolution of Security in 5G: A ‘Slice’ of Mobile Threats, July 2019

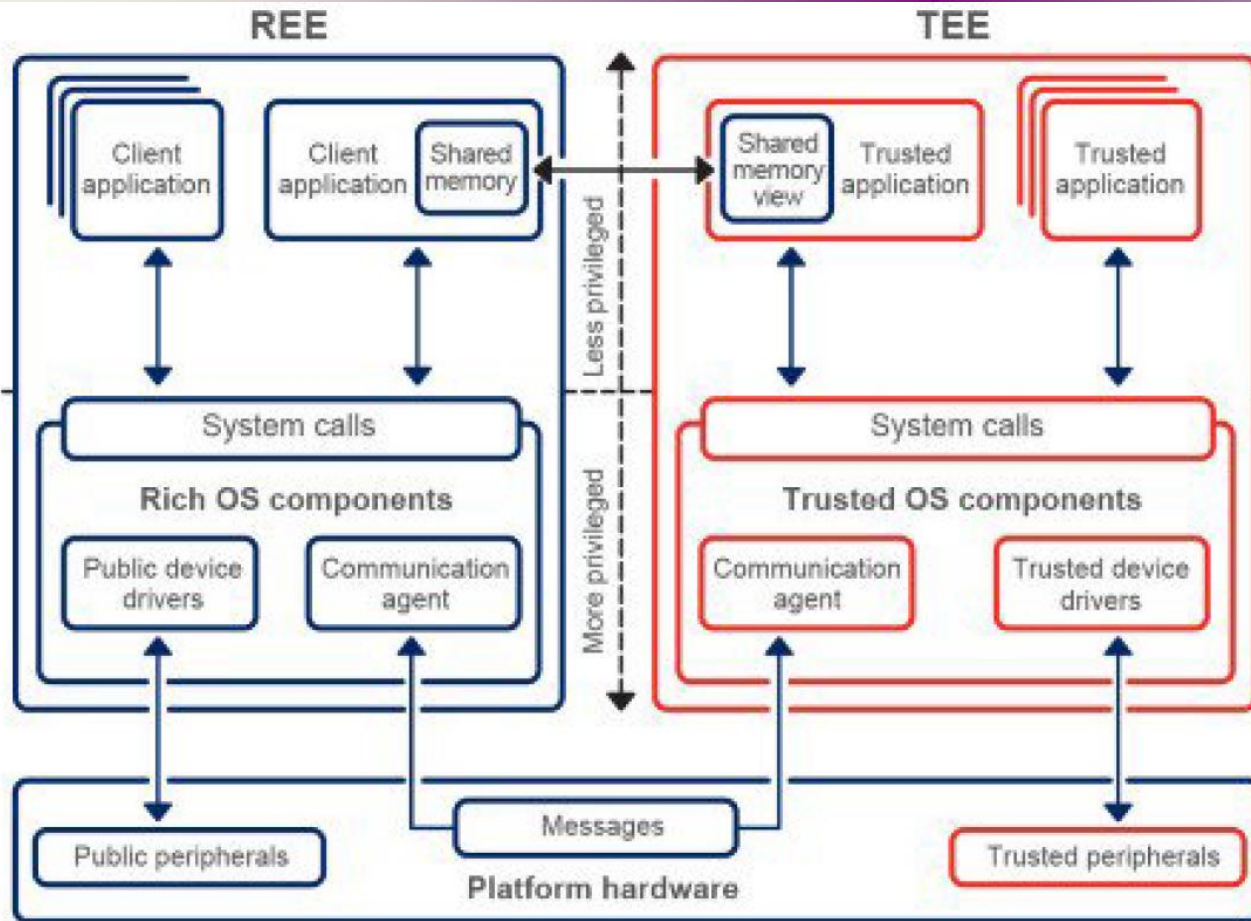


Building Secure and Trusted E2E Env for IoT and Edge with the Trusted Execution Environment (TEE)

- **Trusted Execution Environment (TEE)** is a secure area of a main processor that guarantees code and data loaded inside to be protected with respect to confidentiality and integrity.
 - TEE as an isolated execution environment provides security features such as isolated execution, integrity of applications executing with the TEE, along with confidentiality of their assets
- TEE is a standard which creates an isolated environment that runs in parallel with the operating system, providing security for the rich environment.
 - Only trusted applications running in a TEE have access to the full power of a device's main processor, peripherals and memory, while hardware isolation protects these from user installed apps running in a main operating system.
 - **Proposed and implemented by ARM as ARM TrustZone firmware utilising both hardware and software to protect data on terminal devices**
 - TEE is a derivation of the Trusted Computing Group (TCG) Architecture
- "Hardware root of trust" is used in TEE to prevent simulation of hardware with user-controlled software.
 - Technically this is a set of private keys (so-called "endorsement keys" or "provisioned secrets") which are embedded directly into the chip during manufacturing.



TEE Root of Trust: As used in 5G Security Architecture



- TEE – Trusted Execution Environment
 - Protected by hardware secrets
- REE – Rich Execution Environment (OS)
 - Endorsed by TEE
 - Ensures Confidentiality and Integrity of application data



Huawei 5G and security concerns

- Facts and studies
- Huawei firmware analysis by Finite State



Huawei 5G security

- Controversial security reports about Huawei 5G security
 - <https://www.ft.com/content/8b48f460-50af-11e9-9c76-bf4a0ce37d49>
 - Not only Huawei play role in network/infra security
- 1. Data: It is almost impossible for encrypted communications to be read by anyone who does not have the encryption keys.
 - But in the way wireless telecoms networks are currently structured, much data passes through the network in unencrypted form.
 - Some experts have argued that the risk from Huawei's equipment could be minimised by only using the vendor in the "edge" or "access" networks — the periphery of the network, which includes the base stations (or masts) that broadcast mobile signal, and not the "core" network.
- 2. Attacks on individuals: Base stations can send false emergency alerts, or not pass on real emergency alerts. Base stations can also launch "man in the middle attacks".
- 3. Attacking the whole network Base stations relay signals between the phone and the core network, but can also be used to send malicious signals into the core.
 - DoS attacks that jam part or all of the network
 - Mr Clancy said that keeping Huawei out of one country's network would not significantly reduce Huawei's offensive capabilities. "With their market share, they can take down the global Internet whenever they want," he said.



Huawei security: Half its kit has 'at least one potential backdoor'

<https://www.zdnet.com/article/huawei-security-half-its-kit-has-at-least-one-potential-backdoor/>

- Recent facts that [suspected Chinese state-sponsored hackers](#) broke [into telecom giants through IBM and HPE](#), researchers have revealed that over half the equipment from China's telecoms giant, Huawei, has "at least one potential backdoor".
- Huawei equipment assessment by the UK's National Cyber Security Centre (NCSC) over concerns its 5G gear could be used by China to spy on the country:
 - Huawei security was ["objectively worse" and "shoddy" compared with that of rivals](#), which include Ericsson, Nokia, and Cisco.
- Finite State analyzed 1.5 million files within about 10,000 firmware images that are used across 558 Huawei enterprise networking products.
 - More than 55 percent of firmware images have at least one potential backdoor
 - The flaws include hard-coded credentials that could be used as a backdoor, unsafe use of cryptographic keys, and indications of poor software development practices.
 - Finite State nonetheless found that on average there are 102 known vulnerabilities in each Huawei firmware image, along with evidence of numerous zero-day vulnerabilities.
- One of the key problems Finite State found lies in Huawei's use of and failure to update open-source software components, in particular OpenSSL,
 - It found that the average age of third-party open-source software components in Huawei firmware is 5.36 years and says there are "thousands of instances of components that are more than 10 years old".
 - The oldest version of OpenSSL contained in Huawei firmware was released by the open-source project in 1999. The company said it found 389 binaries on Huawei firmware that were vulnerable to [Heartbleed](#), the critical bug [disclosed in 2014](#) that allows an attacker to steal email and other communications that would normally be protected by the Transport Layer Security protocol.



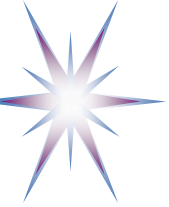
Discussion

- 5G technologies for Secure Cyberinfrastructure and Data exchange
- E2E infrastructure from IoT – Edge – Data Center - Data Analytics
- Bring cloud experience to 5G core network
- Bring computationally enforceable policies via CNF cloud native provisioning



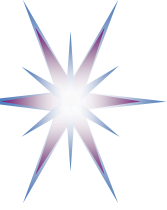
Additional: Mobile devices and smartphone security

- Mobile devices security
- Baseband processor architecture



Mobile devices security

- See overview and comparison of the security of mobile platforms: IOS, Android, Windows
<http://meseec.ce.rit.edu/551-projects/fall2015/3-2.pdf>
<https://crypto.stanford.edu/cs155old/cs155-spring15/lectures/17-mobile-platforms.pdf>
- Every smartphone or other device with mobile communications capability (e.g. 3G/4G or LTE) has **two processors and runs two operating systems by design**
 - Application Processor/OS (Android, iOS, Windows)
 - Broadband Processor and **proprietary** RTOS that manages everything related to radio, e.g. Qualcomm's Infineon and chip
http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone
 - Implements std protocols GSM, UMTS, HSDPA, etc
 - Runs Hayes commands for controlling modem function
 - Existing bug allows multiple attacks
<https://www.infoworld.com/article/2625180/smartphones/coming-soon--a-new-way-to-hack-into-smartphones.html>



Baseband processor architecture

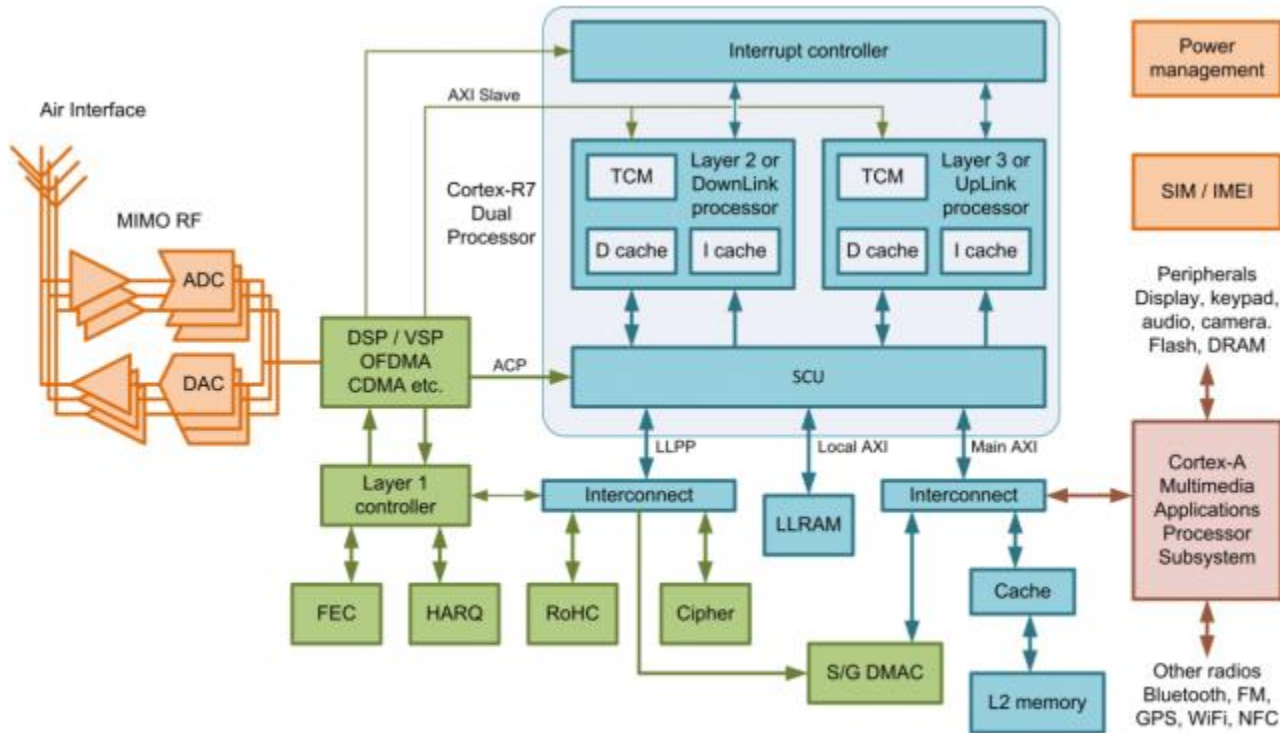


Figure 3: Illustrative baseband architecture

- Baseband processor is the digital system for transmitting and receiving data over the radio. Baseband processor is divided in two parts - <https://www.androidauthority.com/smartphones-have-a-second-os-317800/>
 - Modem to modulate and demodulate the radio signal
 - Protocol stack processor which manages the communication between base station and mobile terminal by establishing connections, managing radio resources, handling errors and packetizing incoming and outgoing data
- Patent <https://encrypted.google.com/patents/US9191823>



References

- ENISA Threats Landscape for 5 G Networks, Nov 2019
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport
- A 5G Americas White Paper. 5G and the Cloud, Dec 2019
<https://www.5gamericas.org/5g-and-the-cloud/>
- A 5G Americas White Paper. The Evolution of Security in 5G: A ‘Slice’ of Mobile Threats, July 2019
https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf
- CNCF Cloud Native Interactive Landscape <https://landscape.cncf.io/>
- Service Based Architecture for 5G Core Network, Heavy Reading White Paper, Sponsored by Huawei, 2017