Cybersecurity Management: T7 - 5G and Beyond Networks

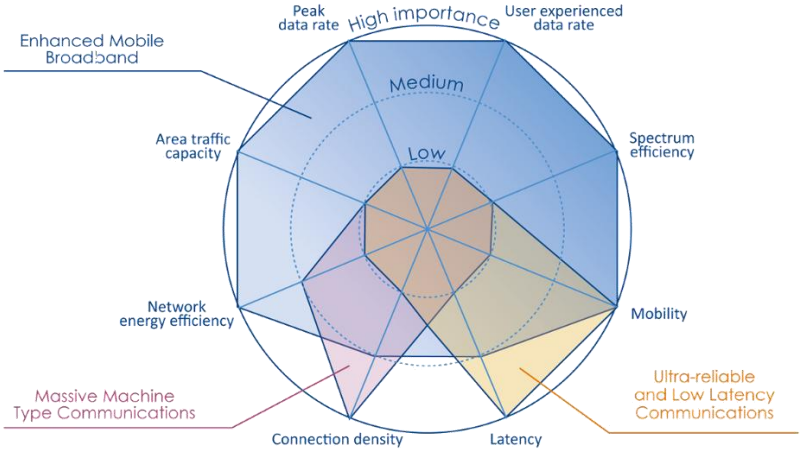
2025-2026

Marc Ruiz (marc.ruiz-ramirez@upc.edu)
Fernando Agraz (fernando.agraz@upc.edu)

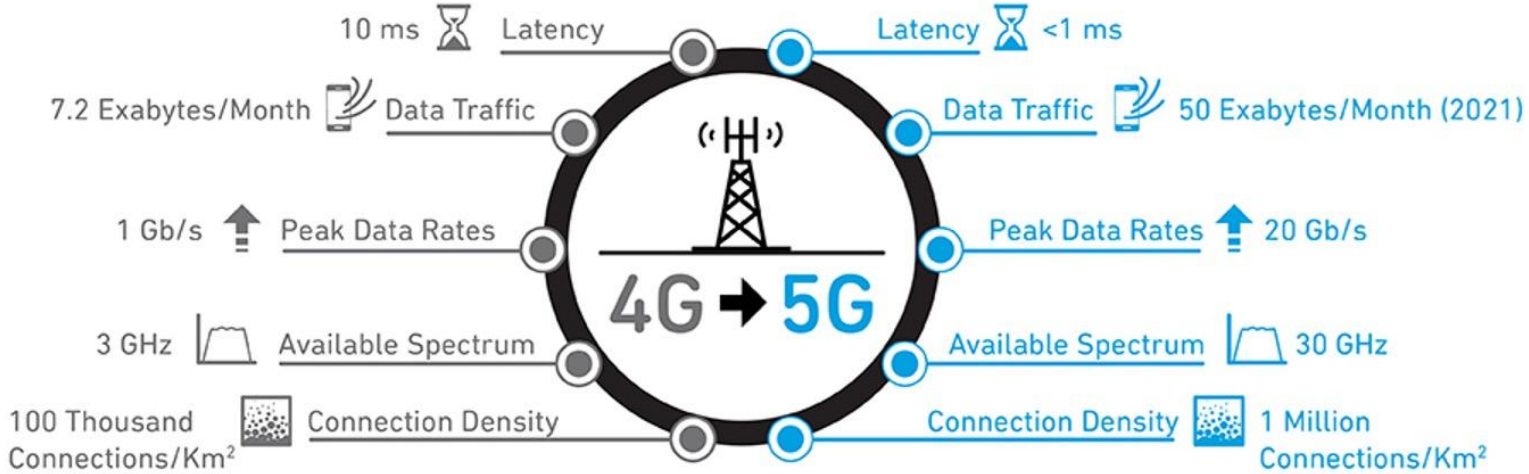
5G Use Cases


Enhanced mobile broadband
Non-SIM devices
Smart phones
Homes, enterprises and venues (mobile/wireless/fixed)
4K/8K, UHD, broadcasting, virtual reality, augmented reality
Massive machine-type communication
Smart building
Logistics, tracking and fleet management
Smart meters
Smart agriculture
Capillary networks
Critical machine-type communcation
Traffic safety and control
Remote manufacturing, training and surgery
Industrial applications and control

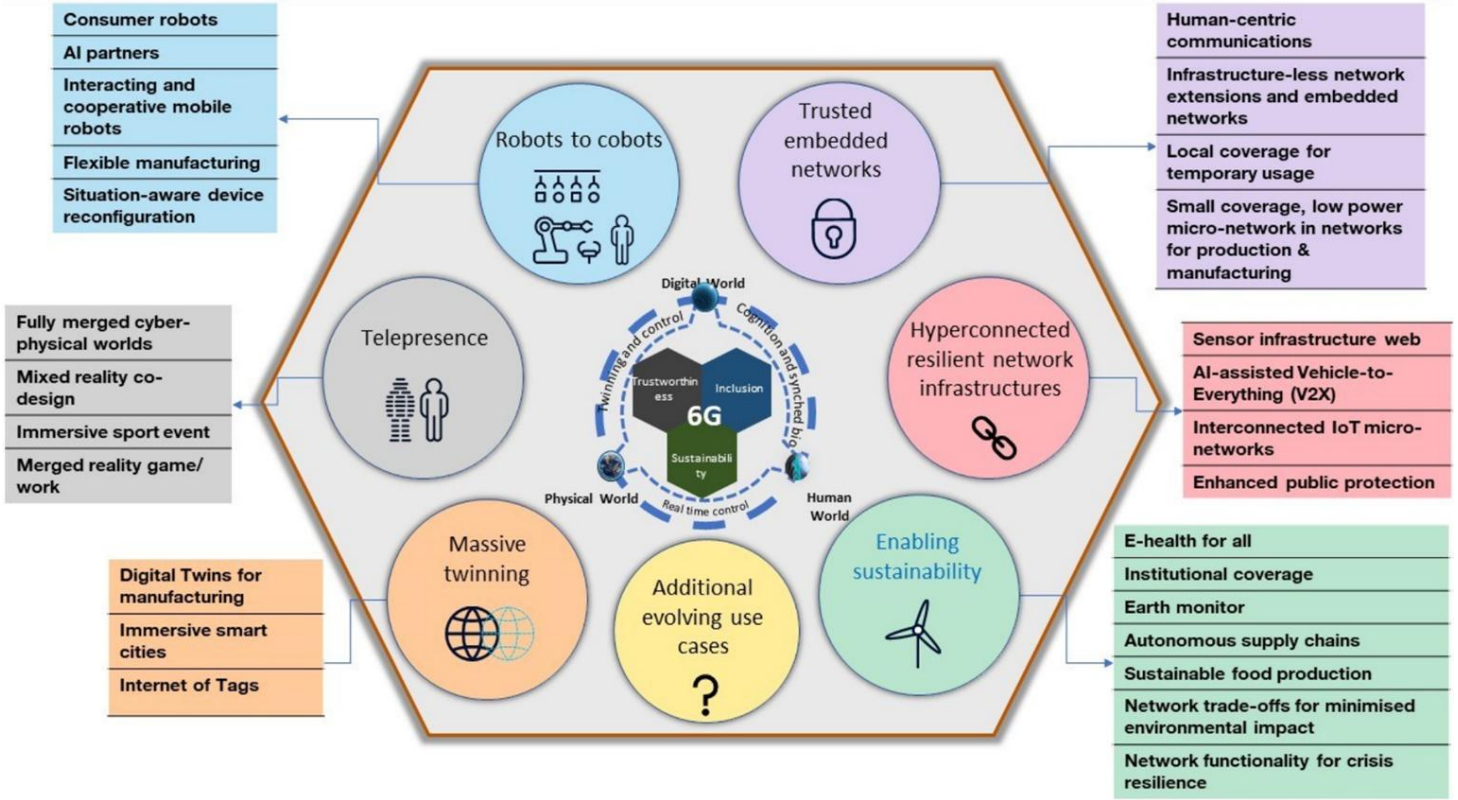
5G Requirements



Comparing 4G and 5G

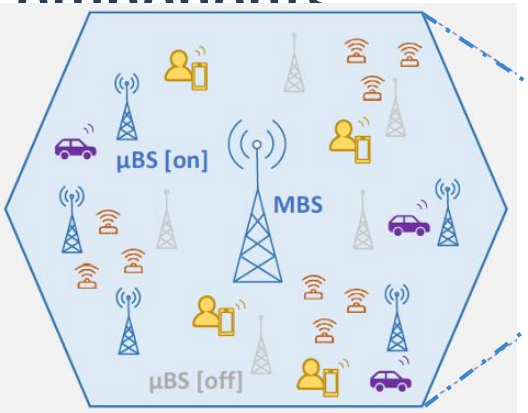


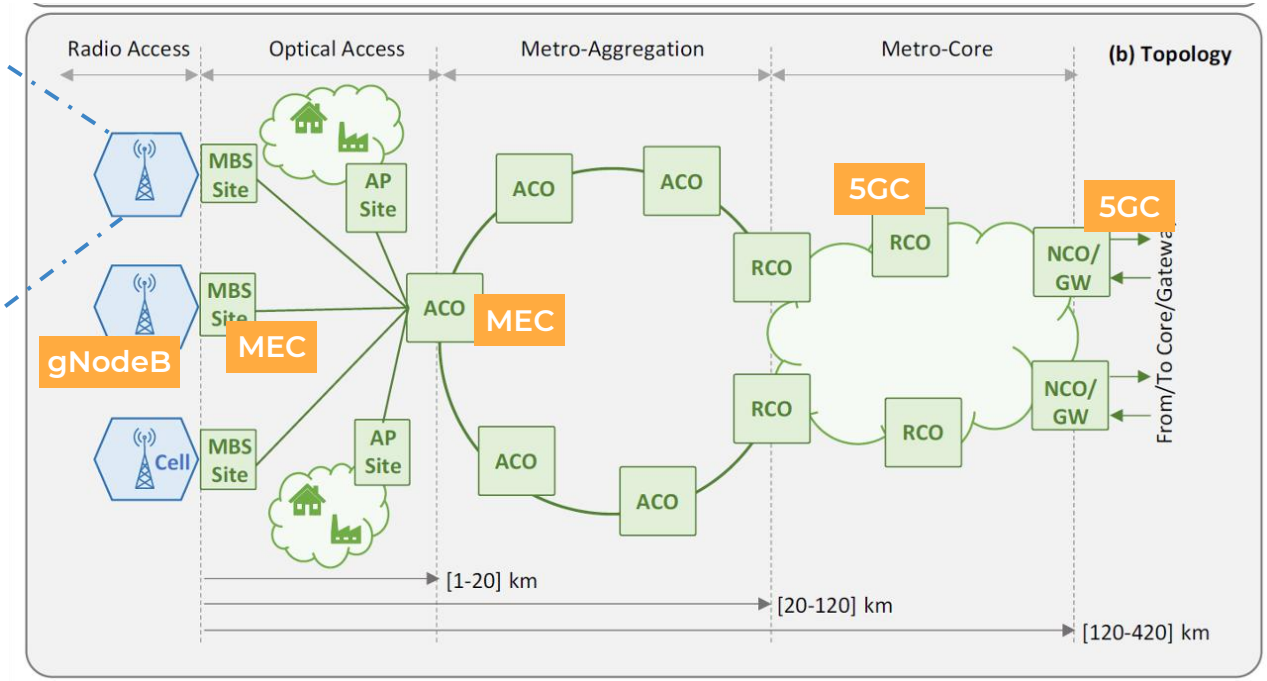
Towards 6G



https://hexa-x.eu/category/use-cases/

The 5G Network Reference Architecture and Key Components



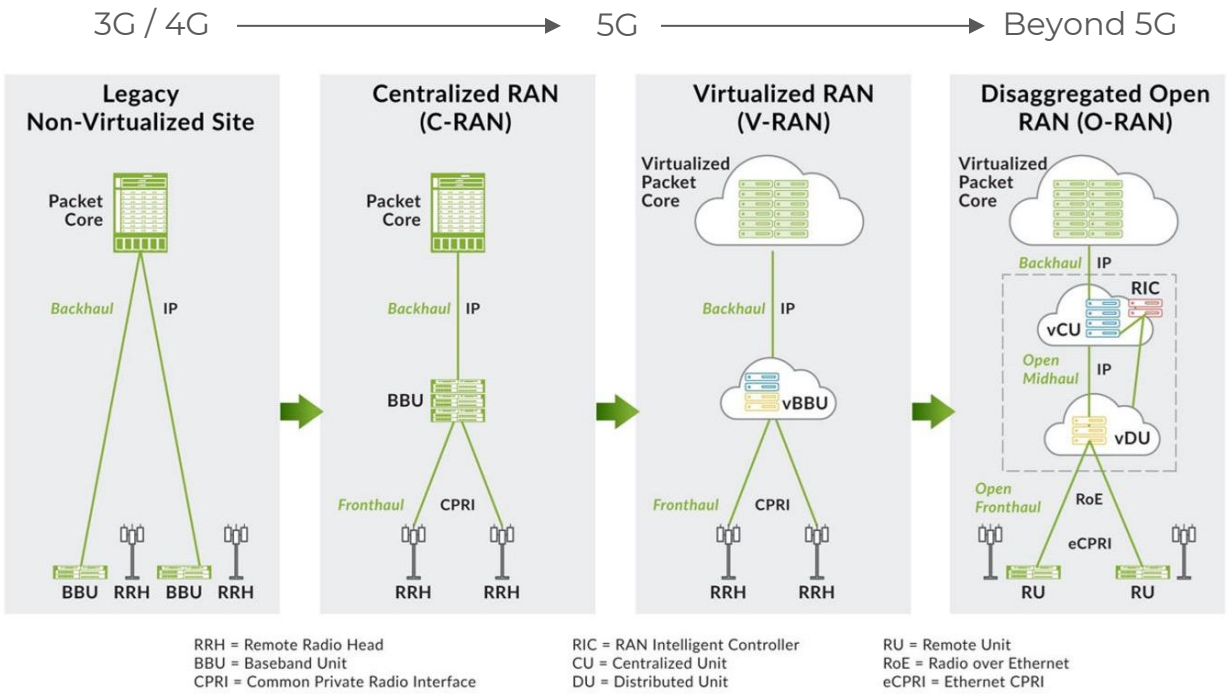


MBS = Macro Base Station
µBS = Micro Base Station
AP = Access Point
ACO = Access Central Office
RCO = Regional Central Office
NCO = National Central Office
GW = Gateway

S. Wang, M. Ruiz and L. Velasco, **"Context-based e2e Autonomous Operation in B5G Networks,"** MDPI Sensors, vol. 24, pp. 1-25, 2024

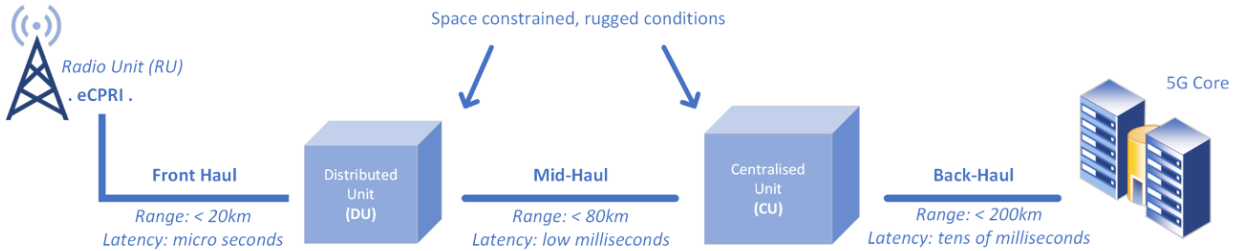
The Radio Access Network (RAN) evolution

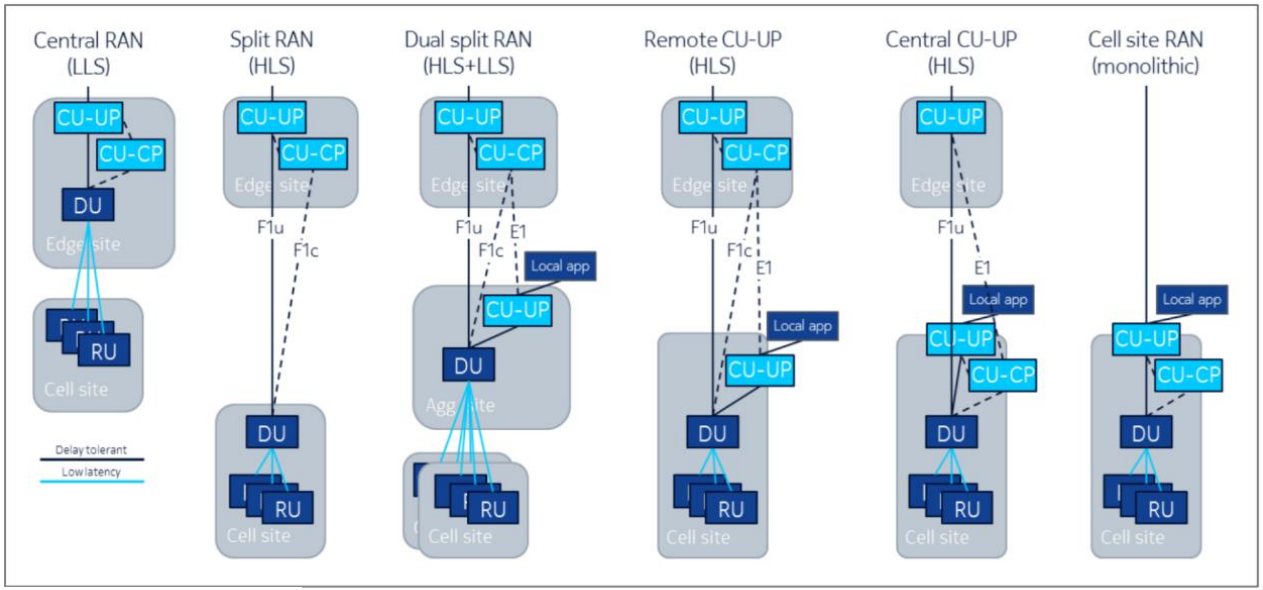
5G networks can be virtualized, software-driven with open, flexible deployment models that leverage cloud technologies and software-defined platforms in which networking functionality is managed through software rather than hardware.



Source: https://www.juniper.net/us/en/research-topics/what-is-open-ran.html

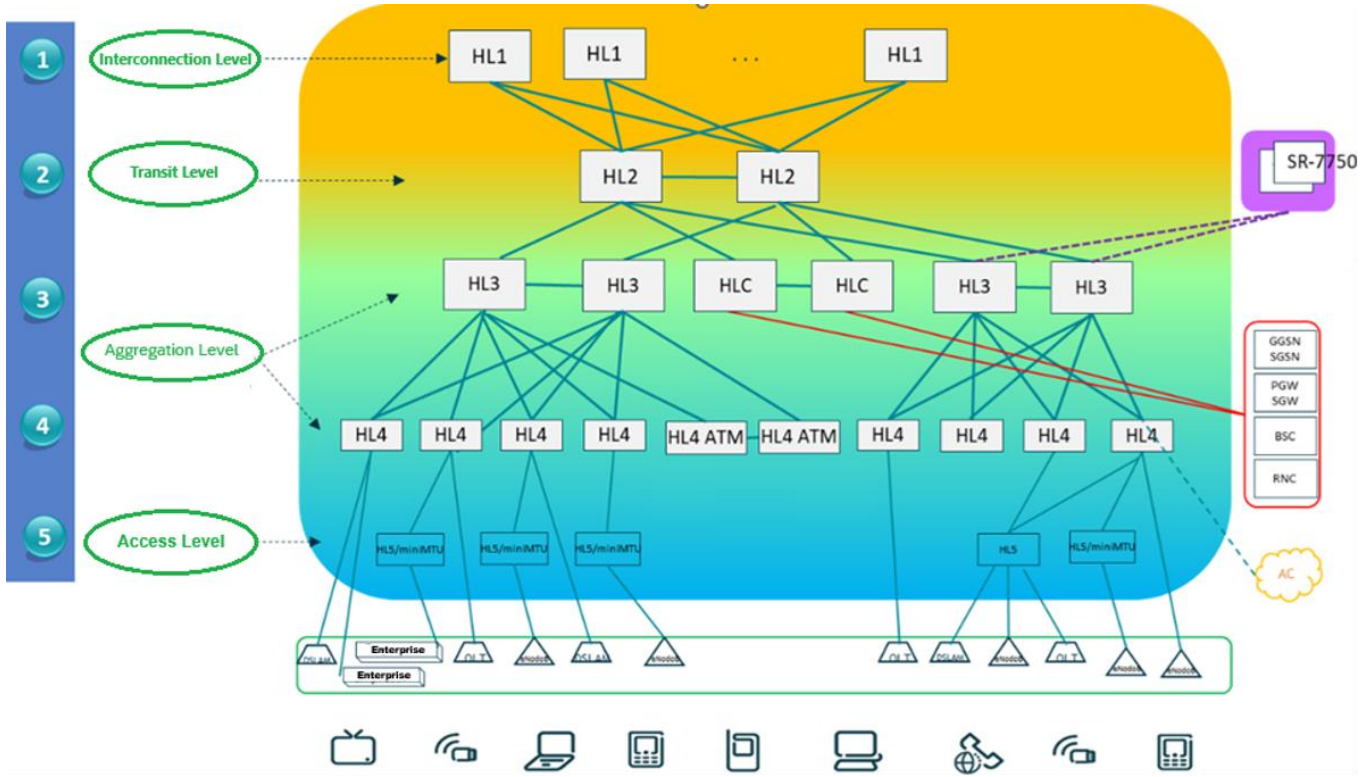
RAN Functional Splits

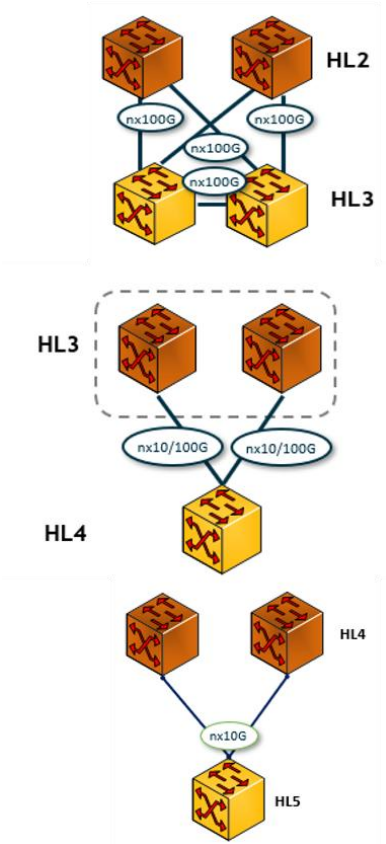




Source: NGMN, 2018

The (fixed) Transport Network Hierarchical Model



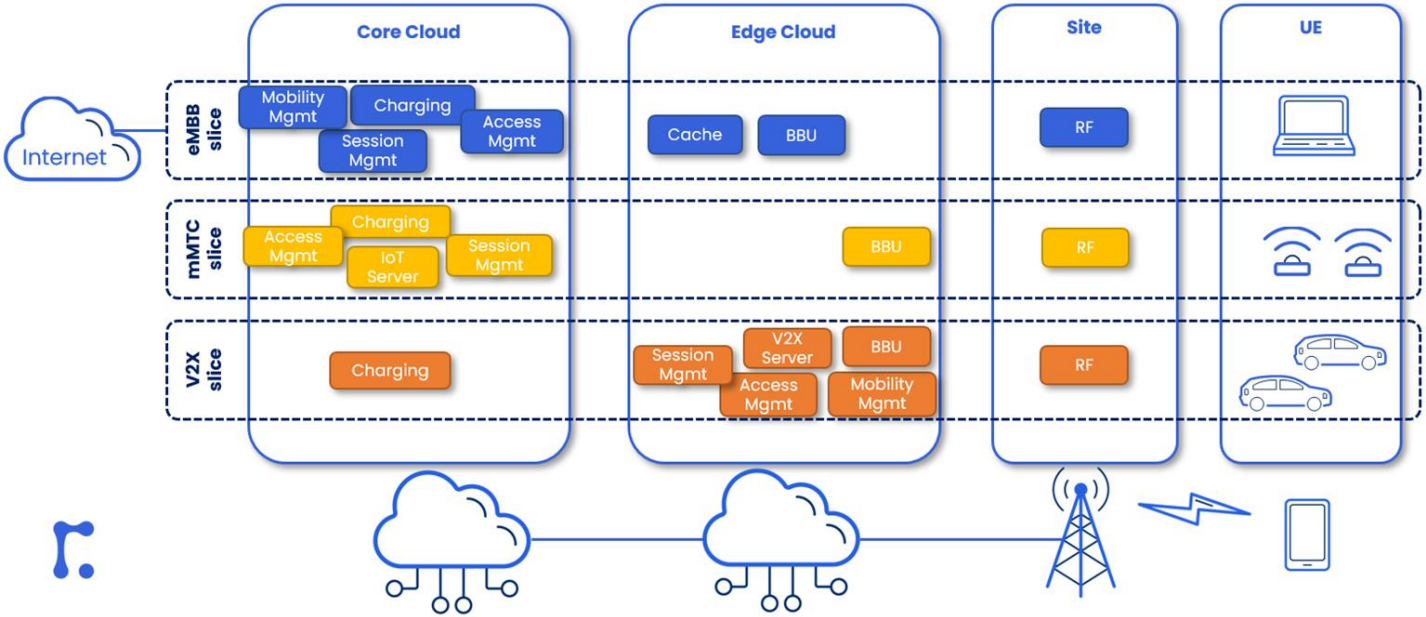


D2.3: Techno-economic Analysis and Dataset Definition, DESIRE-6G project deliverable, 2025
https://doi.org/10.5281/zenodo.15799684

Network Slicing

5G networks can create software-defined subnetwork constructs known as **network slices**, which enables operators to create **isolated end-to-end networks** consisting of both virtualized and physical components, that is, including their own radio resources, core network functions, and management layer **tailored to service-specific requirements** (e.g., latency, capacity, security).

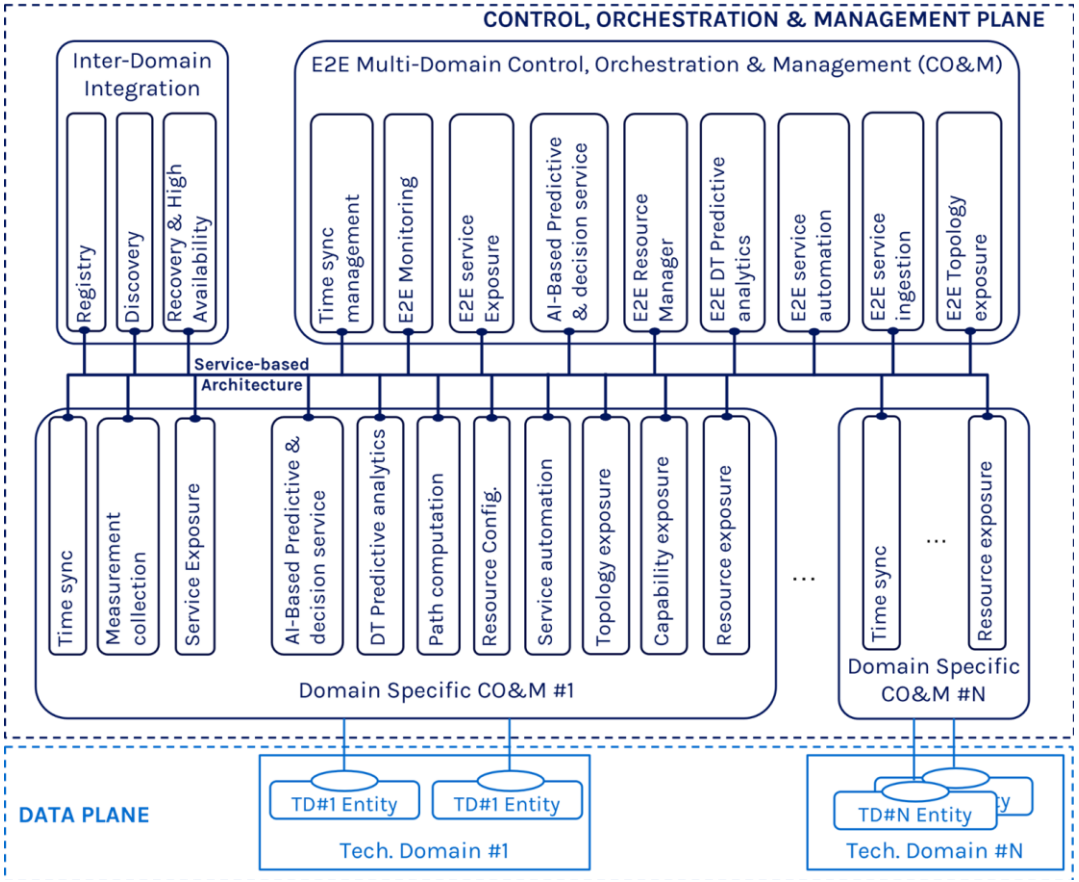
Network slices can be tailored using **automated provisioning and proactive management** of traffic and services to fulfill diverse service level QoS and security requirements requested for a particular application or customer.



Source: https://www.juniper.net/us/en/research-topics/what-is-open-ran.html

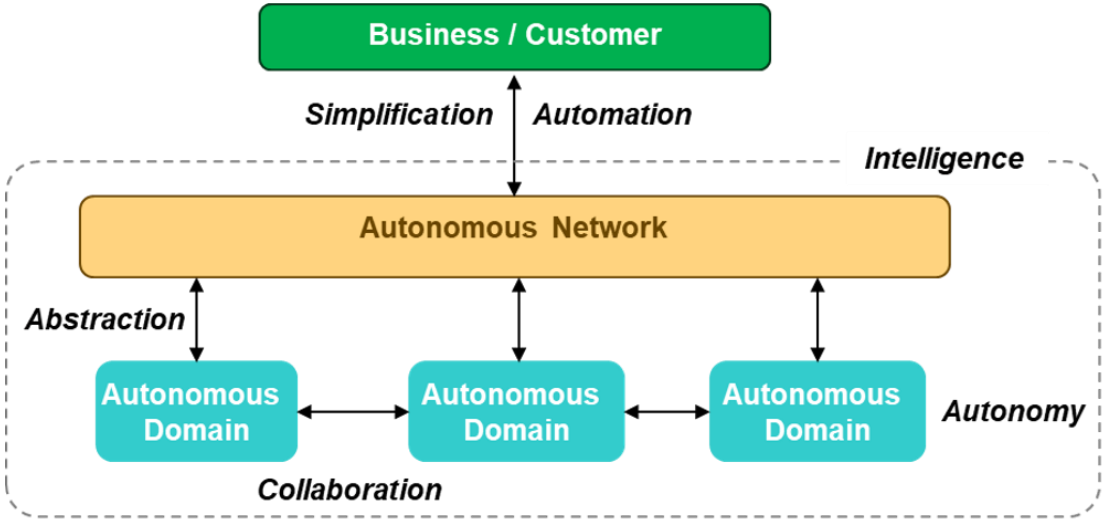
Network Automation

- The main enabler of network automation is the **control, orchestration and management system**, which implements a set of functions aimed to provide **connectivity services configuration** and **maintenance**.
- Some features of the CO&M:
  - Highly softwarized → Resides in the cloud
  - Service-based architecture → Internal APIs
  - It is distributed and multi-layer → External APIs
  - Can use AI mechanisms for enhanced automation



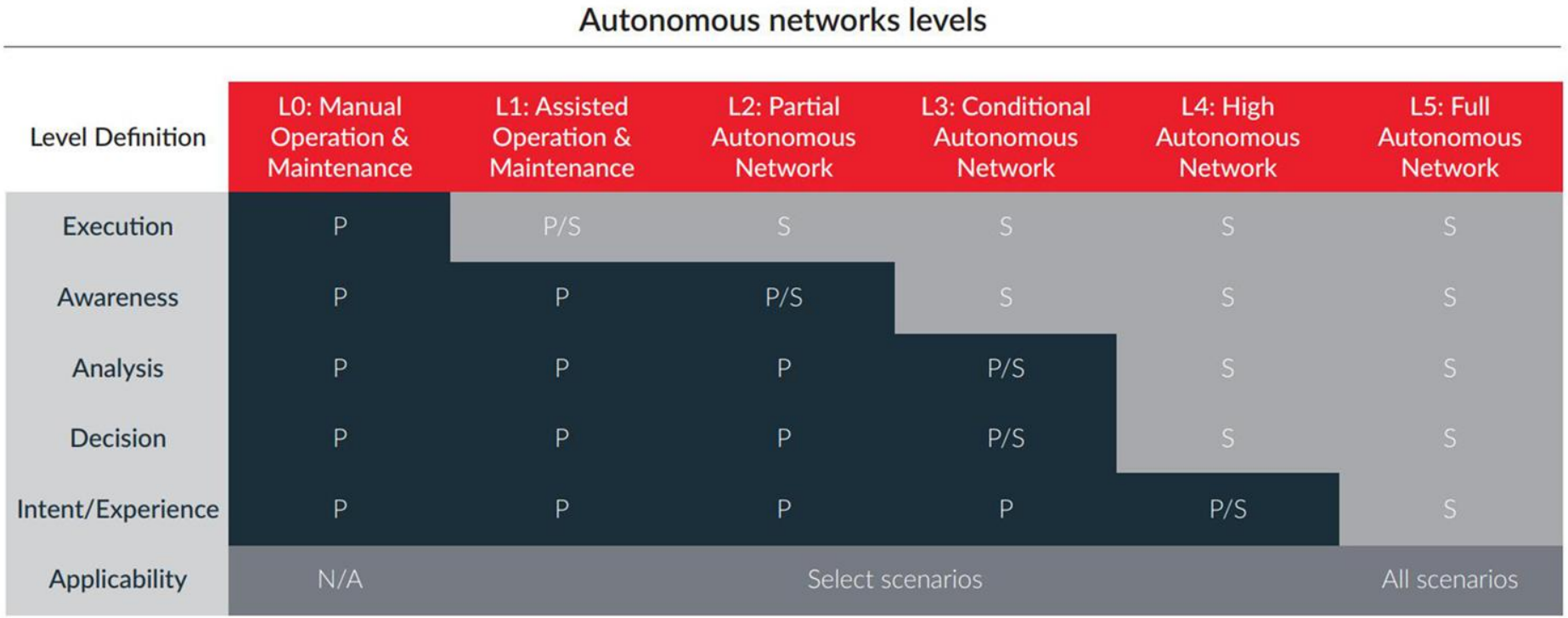
Autonomous Networking Paradigm

- Autonomous Networking targets at providing a wide variety of autonomous "Network/ICT" services, infrastructure and capabilities with "Zero-X" (zero wait, zero touch, zero trouble) experience based on **fully automated lifecycle operations** of "Self-X" (self-serving, self-fulfilling, self-assuring) to dynamically accommodate and adapt to customer needs and available resources.
- An Autonomous Network consists of a simplified network architecture, virtualized components, automating agents, intelligent decision engines which present self-dynamic capabilities with the goal to create intelligent business and network operations based on the concept of **closed-loop** controls.



Autonomous Networks, supporting tomorrow's ICT business, ETSI White Paper, n° 40, 2020

Towards High and Full Autonomous Networks



P: Personnel, **S:** Systems

"Autonomous Networks: Empowering Digital Transformation for the Telecoms Industry," TM Forum White Paper

Towards High and Full Autonomous Networks (cont.)

SERVICE PROVISIONING	L4: High Autonomous Network	L5: Full Autonomous Network
	Services take hours to provision.	Services take minutes to provision.
	Services and changes to those services are fully expressed in intent by the customer through a Service catalogue	Intent is provided by the customer interacting through Service catalogue APIs and infrastructure is fully intent driven.
	Services are assigned and designed automatically from intent specifications in the catalogue Resources are dynamically created on demand.	Auto-generated set of workflow steps based on the intent expressed in the catalogue.
	Intent is translated into automatic network activation, but some aspects remain static with some manual work required (for network physical infrastructure).	Service is automatically provisioned and assured. Network is primarily composed of virtualized infrastructure

CLOSED-LOOP CONTROL	L4: High Autonomous Network	L5: Full Autonomous Network
	Services take seconds to restore	Services never fail
	Automated closed loop end2end Large parts of the autonomous network are fully automated with closed loop control happening based on real-time views of telemetry Fully programmable interfaces allow software control of the autonomous network. DevOps fully implemented.	Self-optimised, Self-healing network Fully zero touch management The network is fully Autonomous and control systems work in closed loop permanently, with real-time views of the network available.
	Real-time insights on network performance are automatically created and provided to operations – DevOps.	Information is analysed in real-time by AI expert systems and changes happen in split seconds automatically. No manual intervention is required except in extreme circumstances.

Why 5G Security Matters?

With over **2.4 billion* connections** worldwide as of 2025 (Q1), the 5G network technology powers critical sectors including healthcare systems, financial services and industrial automation.

The massive data throughput and exponential device density inherent to 5G, plus its technological innovations, dramatically **expand potential attack surfaces**. Every connected device, virtualized network function, and data stream represents a potential vulnerability that could be exploited.

As 5G increasingly underpins **critical infrastructure and services**, robust security frameworks become not just important but absolutely essential for societal stability.

2.4B

Global 5G Connections

Active connections as of 2025

100X

Data Speed Increase

Compared to 4G networks

1M

Devices per Km^2

Maximum connection density

*billion = 10^9

From 4G to 5G: Security Enhancements

- **Subscriber authentication:** authentication using 5G Authentication and Key Agreement (5G-AKA), Extensible Authentication Protocol Authentication and Key Agreement Prime (EAP-AKA'), and Extensible Authentication Protocol – Transport Layer Security (EAP-TLS), Home Control of authentication for roaming devices, and non-SIM card-based authentication for IoT devices.
- **Subscriber privacy:** Stronger False Base Station (FBS) protection and Subscription Permanent Identifier/Subscription Concealed Identifier (SUPI/SUCI) for encrypted long-term subscriber identifiers. CSRIC VII recommends that the SUCI feature is mandatory for U.S. deployments, except when the UE is requesting emergency services.
- **Secure service-based architecture:** TLS and OAuth 2.0 on all mandatory functions.
- **Secure roaming interconnects:** Introduction of the Security Edge Protection Proxy (SEPP) at the application layer.
- **Network Slice Specific Authentication and Authorization (NSSAA):** Provides separate authentication and authorization per network slice.
- **Non-Public Networks (NPN):** 5G Private networks to provide security and privacy on dedicated resources that are independently managed.
- **Use case specific security enhancements** for cellular IoT and URLLC services.

5G Security: Challenges

- **Massive IoT Proliferation:** Millions of connected devices with **limited processing power, basic security features and infrequent updates**. This creates an **enormous attack surface** for coordinated breaches (e.g., massive DDoS). Compromised devices can also be used as entry points to the network.
- **Supply Chain Threats:** Compromised hardware and software **components from untrusted vendors** can introduce backdoors and vulnerabilities.
- **Virtualization Vulnerabilities:** The core network's shift to a virtualized cloud environment opens the door to risks related to **cloud security** and **API security**. For example, a vulnerability in a virtualized network function (VNF) could affect multiple services.
- **Network Slicing Risks:** Misconfigurations in virtual network partitions can inadvertently **expose entire network segments** to unauthorized access, potentially compromising multiple tenants simultaneously.
- **Edge Computing Risks:** Distributed computing at the network edge challenges traditional **perimeter-based security**. In a broader view, the 5G deployment may require placing equipment in more publicly accessible locations (e.g., streetlights, rooftops), thus challenging **physical security**.

5G Security: Network Level

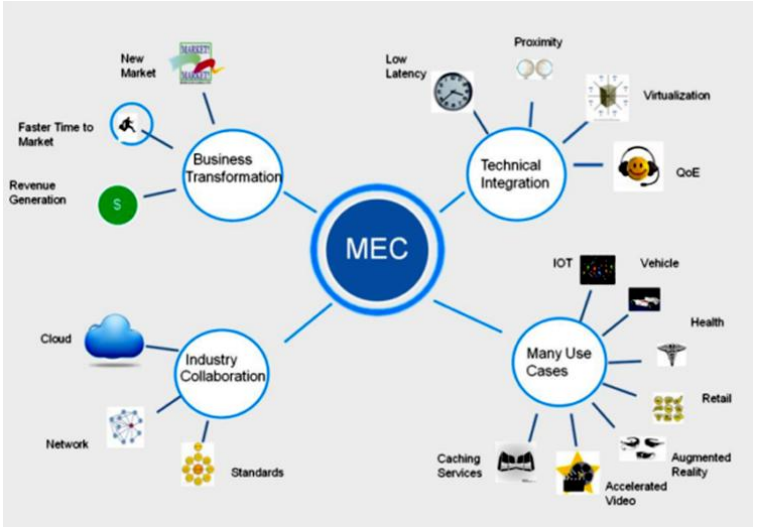
- Fronthaul: Lightweight security to prioritize low-latency (<100µs).
  - MACsec: L2 security mechanism to secure user and control plane traffic.
  - Physical isolation
- Midhaul: Layered security.
  - L2/L3 security for encryption and integrity: MACsec and/or IPsec.
  - Slice isolation through tunneling and QoS policies.
- Backhaul / Core: Network and Transport level security + Application level protection.
  - L3/L4 security based on IPsec VPNs and TLS
  - 5G-AKA for the initial connection between the UE and the 5GC.
    - Identity protection: Encrypts the SUPI to create a temporary identifier (SUCI) to prevent IMSI-catcher attacks

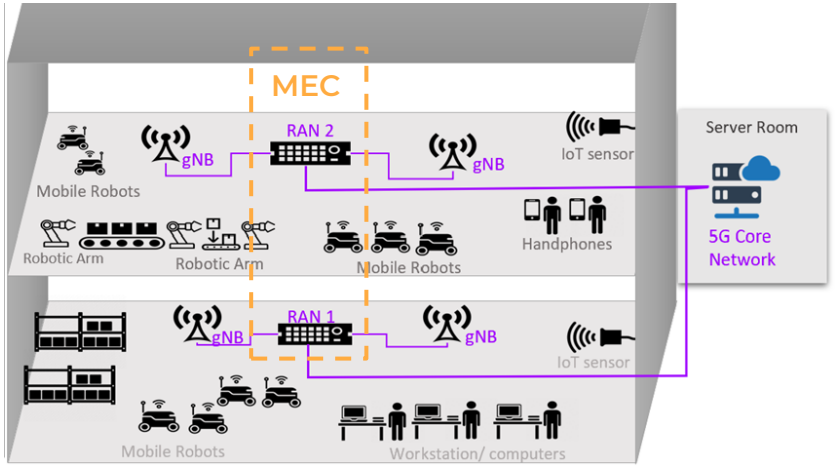
5G Security: RAN Cloudification

- 5G is the first cellular technology designed for the cloud → Service-based Architecture (SBA)
- The cloudification of the 5G RAN and Core leverages **cloud security** best practices to protect networks, applications, and data, while also introducing new security risks associated with the cloud that must be considered for 5G deployments.
- Cloud deployments of RAN and Core should be built upon a foundation of **zero-trust** with a strong security posture based on industry best practices and standards for cloud security, Cloud-Native Function (CNF) security, and secure use of open-source software.
- 5G RAN and Core can be deployed using the **NIST cloud deployment** models (IaaS, PaaS, SaaS)
- Cloud Security ↔ 5G Security
- Virtualized cloud native deployment of 5G network functions such as 5GC and 5G RAN allows flexibility and scalability in deployment, but **introduces new vulnerabilities**.
- Increased network perimeter

5G Security: MEC

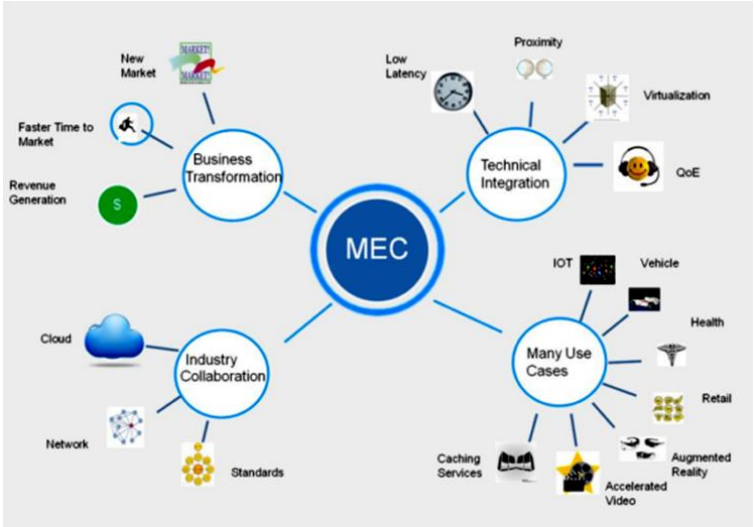
- Multi-access Edge Computing (MEC) is one of the key pillars for meeting the low latency demands of 5G use cases.
- Data is processed and stored at the network edge to bring technology resources closer to the user.
- The 3rd party MEC applications deployed at the edge require **API integration** with the MEC application server and possibly other 5GC network functions.
- An API that is not deployed following industry best practices can introduce attack vectors related to insecure API security risks such as user and function-level authorization, excessive data exposure, and broken object level that are more prominent in 5G MEC deployments.

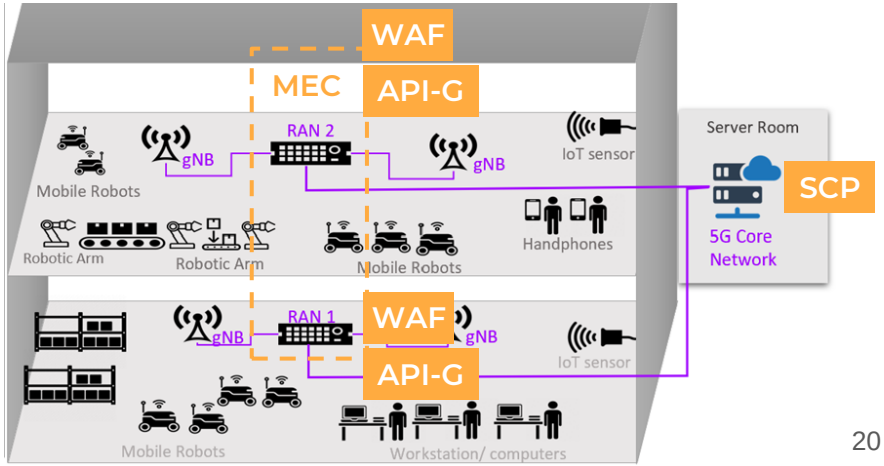




5G Security: MEC and APIs

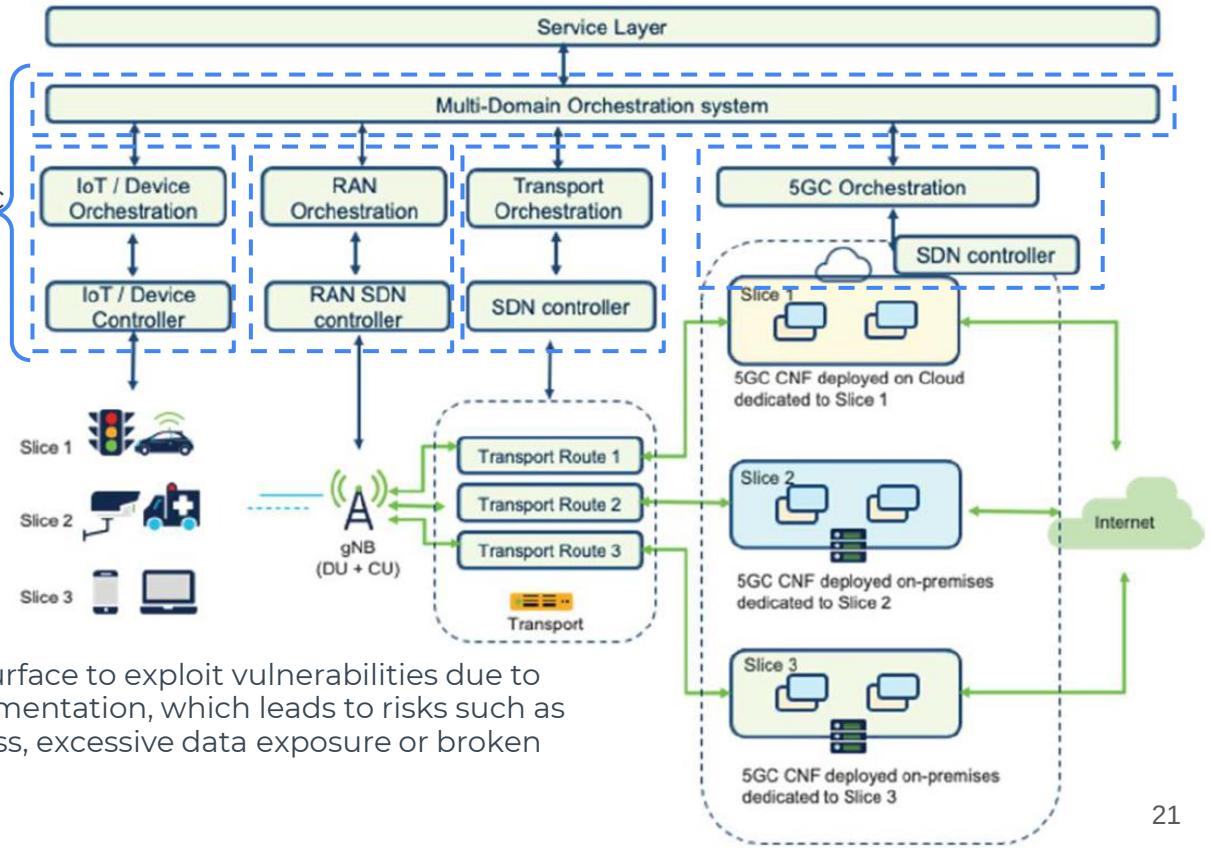
- Securing the APIs in a SBA:
  - Secure APIs access using mechanisms like token-based authorization. Secure APIs communications using IPsec and/or TLS.
  - Service Communication Proxy (SCP):
    - TLS for encryption and token-based authorization
      - Mutual TLS (mTLS) for CNF to CNF communication
      - Token validation for consumer CNFs
    - Topology hiding and service brokerage (hide NFs internal IP addresses, centralized discovery).
    - Overload and attack mitigation through the monitoring and control of the signaling traffic flow (throttling, load-balancing, message filtering and access lists based on content)
  - The API Gateway acts as single entry point for API traffic destined for MEC applications
    - Centralized Authentication and Authorization: Checks client credentials before the request reaches the MEC application.
    - Rate limiting and throttling to prevent DoS and brute force attacks.
    - Protocol mediation and validation to ensure the API requests follow the expected format.
    - Logging and monitoring to be fed to a SIEM.
  - The Web Application Firewall (WAF) provides inspection of the HTTP/HTTPS traffic to block web-based attacks
    - Application layer attack mitigation: Protects against known vulnerabilities (e.g., OWASP) → SQLi, Cross-Site Scripting (XSS), XML External Entity (XXE).
    - Input validation by examining request parameters, headers and payload.





5G Security: Network Automation

Control, Orchestration and Management layers enable dynamic creation and operation of network slices.



This also introduces an expanded attack surface to exploit vulnerabilities due to improper isolation and insecure API implementation, which leads to risks such as unauthorized user and function-level access, excessive data exposure or broken object level authorization.

5G Security: Network Automation

- Potential risks are data exfiltration, data hoarding and sniffing, unauthorized user access, and DoS/DDoS attacks on the control and orchestration layers, which attack network availability by degrading service creation and maintenance capabilities.
- Several steps can be taken to mitigate these risks, including:
    - Implementation of RBAC to authorize access to the different layers of the network automation system.
    - Scan all software images before execution to enforce policy checking and validate execution permissions, preventing the deployment of untrusted and vulnerable images.
    - Monitoring to detect behavioral anomalies, helping to mitigate security breaches.
    - API Security

5G Security: Zero-Trust Architecture (ZTA)

- Zero-trust is a security model built on the principle that no user or NF can be trusted, whether internal or external to the network.
- Zero-trust shifts the focus away from network perimeter security. Instead it restricts access to internal and external users, and software components through the use of strong authentication and least privilege authorization.
- As defined by NIST, the ZTA focuses on protecting resources, including assets, services, workflows, and accounts instead of protecting network segments. It minimizes access to resources to only those subjects and assets identified as needing access.

5G Security: Zero-Trust Architecture (ZTA)

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T1. All data sources and computing services are considered resources.	All 5G network assets and functions, including devices, computing resources, and services, are considered untrusted.	The end-to-end 5G network, including UEs, RAN, Transport, Core, Applications, and Services are assets and data sources. In the 5G SBA, NFs are identified as consumers and producers. UEs are identified using: • International Mobile Equipment Identifier (IMEI) • International Mobile Subscriber Identity (IMSI) or Subscription Permanent Identifier (SUPI)
T2. All communication is secured regardless of network location.	All communications must meet the same security requirements as third parties.	Service Communication Proxy (SCP) helps operators to efficiently secure and manage their 5G network by providing routing control, resiliency, and observability to the core network. Secure communication in 5G includes: • TLS to provide confidentiality and integrity protection across the SBI. • IPsec and DTLS to protect control messaging and user data in transport. • Subscriber identity privacy is provided with the Subscription Concealed Identifier (SUCI). • Full-rate User Plane Integrity protection • Stronger False Base Station (FBS) protection

5G Security: Zero-Trust Architecture (ZTA)

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T3. Access to individual resources is granted on a per-session basis.		UE access is granted using Shared Symmetric Key - Authentication and Key Agreement using 5G-AKA or EAP-AKA', or Public Key Certificate using EAP-TLS. Authentication and authorization between NFs over SBI in the 5GC is provided with certificate-based mutual authentication using TLS. Home Control of authentication is provided for roaming devices. RAN Slicing supports slice-specific mutual authentication for devices using the NSSAA.
T4. Access to resources is determined by dynamic policy	Trigger decisions on granting access based on various factors such as credentials, software version/patches, location, etc	The PCF feeds the AMF with access and mobility policies that affect UE authorization to access 5G network resources. Unified 5G policy allows for creating security policies for security use cases and user plane security enforcement within the session management and established security policies.

5G Security: Zero-Trust Architecture (ZTA)

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T5. The operator monitors and measures the integrity and security posture of all owned and associated assets.	The security state of all resources is monitored continuously in real-time.	5G is redefining Security Monitoring from physical probes and cables to software and virtual links. New software-based solutions include monitoring of East/West and North/South directions. Deliver analytics functions in the network for automation, maintaining security analytics and reporting. NWDAF defined in 3GPP TS 29.520 incorporates standard interfaces from the service-based architecture to collect data and evaluate systems in terms of compliance with security policy rules.
T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Least Privilege: Any access, if granted, should be authorized with the least privileges. The access is only granted for a specific resource (depending on the sensitivity of the resource) and is not valid for a different resource.	The SBA uses OAuth 2.0 token-based authorization for any NF that wants to communicate with another NF. Mutual authentication enables the device to authenticate the network using the AUTH (Authentication Token) returned by the network and the Shared Key using Security Anchor Function (SEAF) and AUthentication Security Function (AUSF).

5G Security: Zero-Trust Architecture (ZTA)

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T7. The operator collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	The security posture of devices, and behavioral patterns of resources are crucial to capture security baseline and maintain it. Trust evaluation and risk assessment is conducted for everything in 5G.	For the MNO, application of this tenet can be considered from two perspectives: 1. The MNO should leverage solutions that align with the continuous diagnostic and mitigation (CDM) systems as defined by NIST in Special Publication 800-207. 2. The MNO should have a mature supply chain risk management (SCRM) which should require the 5G network functions to be compliant with GSMA NESAS. NESAS includes security assessments of vendor development and product lifecycle processes and Security Assurance Specifications. In 5G, the assessment is carried out at the beginning to ensure products/solutions are evaluated against known risks. However, this will need to be automated once the products/solutions are also implemented in the network. The following could serve good reference to 'risk-assess' elements in 5G: • 3GPP Security Assurance Specification (SCAS) • GSMA - Network Equipment Security Assurance Scheme (NESAS)

5G Security: Wrap-up

- 5G holds the promise of elevating society as business, public services, and citizens increasingly rely on such technology for critical infrastructures, mission critical applications, public safety, smart manufacturing, connected vehicles, and other real-time, low-latency use cases.
- This results in greater impact from a cyberattack over the 5G network, thus decreasing our risk tolerance. The combination of greater risk with reduced risk tolerance requires a zero-trust approach.
- Trust in 5G can be enhanced by using a ZTA, which makes no implicit assumptions about trust based upon an asset's network location, geographic location, or ownership.
- 5G provides digital identities, mutual authentication between all functions, and strong cipher suites for confidentiality and integrity protection in the control and user planes.
- 5G is also the first cellular technology to be cloud-native. The cloudification of the 5G RAN and Core can leverage cloud security best practices to protect networks, applications, and data, but it also introduces new risks due to the expanded threat surface.
- Virtualization, disaggregation, automation and intelligence, can become a complementary part of 5G's broader progression to greater security as industry initiatives address Open RAN's security risks.
- Given the complexity of 5G, automated monitoring and detection is essential. Machine learning and AI techniques can be used to identify abnormal traffic within slices or detect compromised edge nodes.

5G Security: Additional References

- https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/telecoms/5g
- https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security
- https://www.5gamericas.org/security-for-5g/
- https://www.cisa.gov/topics/risk-management/5g-security-and-resilience