Zero Trust

Defense in Depth

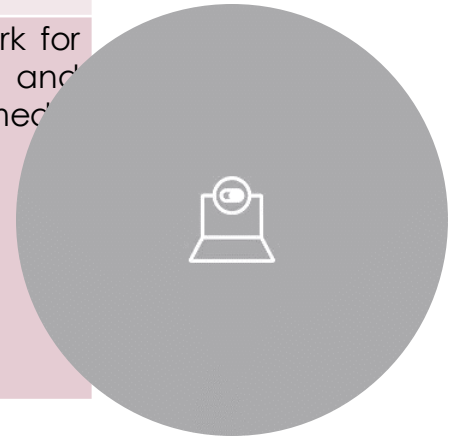
UKNOF51
April 3 – 4, 2023
Manchester, UK

5G Security

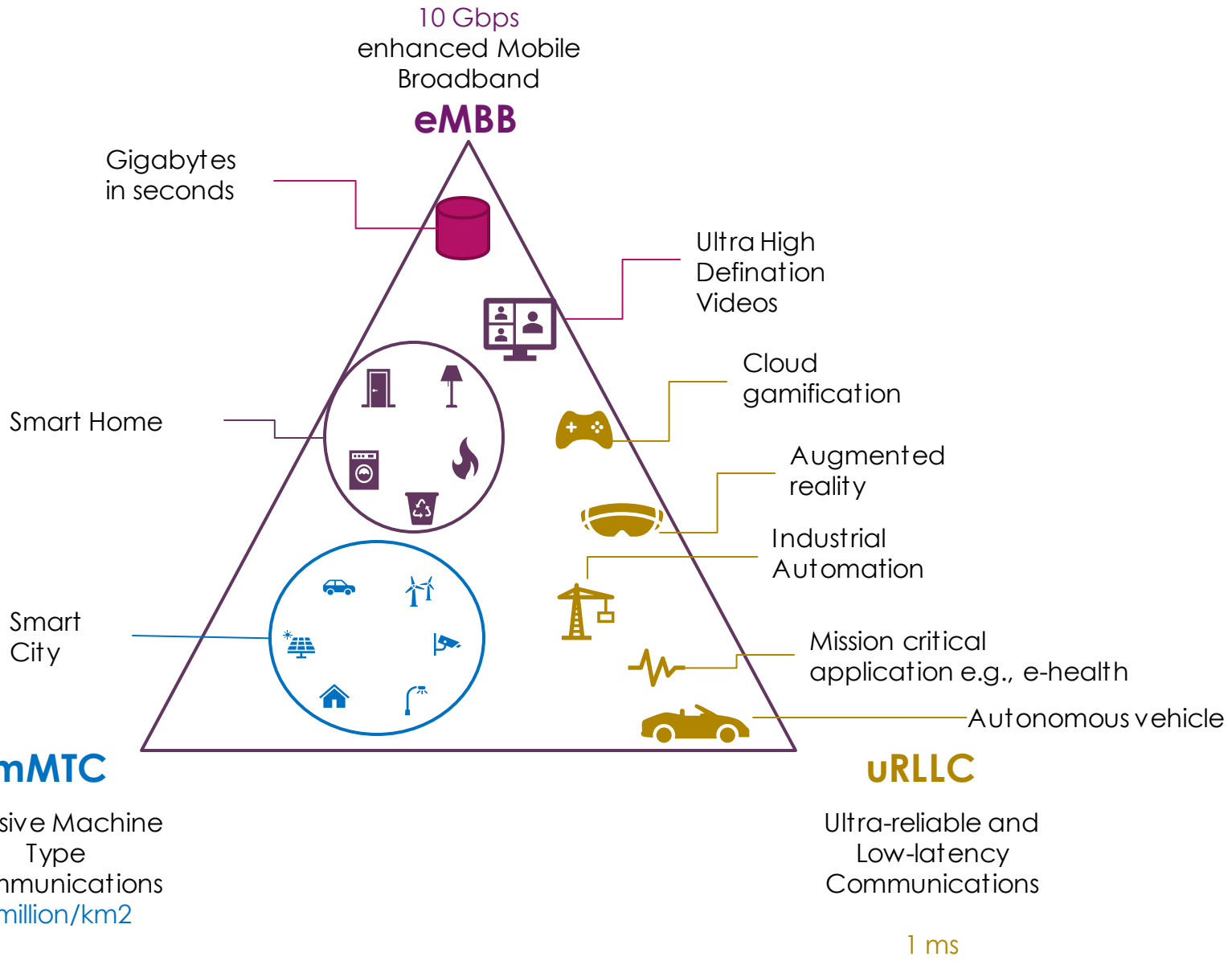
Rohit Saxena, Telecom, Cloud, and Cyber Security Architect
Kamal Singh, Cloud, Network, and Cyber Security Architect

What has changed in 5G

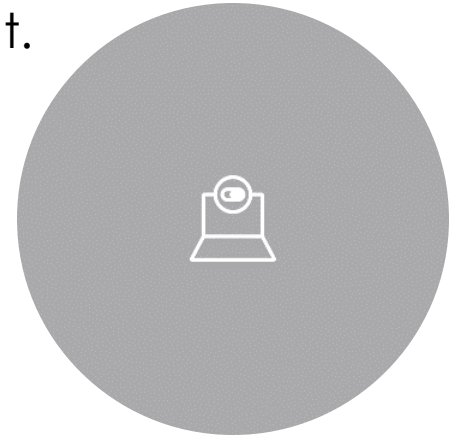
'G'eneration	Speed	Air Interface technology	Key features
1G **Where it all began**		AMPS	Analogue switching voice only
2G/2.5G/2.7G **The Cultural Revolution**	14.4 to 171.2 kbps	TDMA, CDMA, GPRS	Voice, data, web mobile Internet, Low Speed streaming and Email services
3G / 3.5G **The 'Packet-Switching' Revolution**	3.1 Mbps to 14.4 Mbps	EDGE & HSPA	Voice, data, Multimedia, smart phone applications, enhanced speed & fast web browsing
4G **The Streaming Era**	600 Mbps to 1 Gbps	LTE	High-speed, High-quality Voice over IP, multimedia streaming, gaming On Virtulized platform Latency 50 ms to 10 ms IOT Density 10k/ km^2 to 100k / km^2
5G **The Internet of Things Era**	10 Gbps	NR	Super-fast mobile internet, Low latency network for mission critical applications, IoT, Security and surveillance smart healthcare apps, HD multimedia streaming .. etc. Cloud native Micro services based Latency 1 ms IOT Density 1 million / km^2



5G – Service Scope



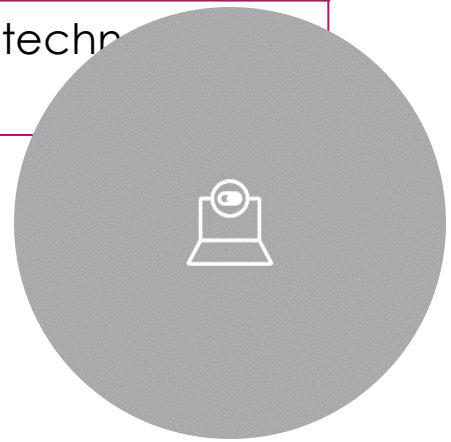
5G network is no longer a technology for making calls and data browsing over the phone alone; rather, it has become an enabler for a connected world with advanced use cases for almost every industry, such as manufacturing, public safety, healthcare, public transport, energy, and utility, automotive, media, and entertainment.



***Source : ITU-R WP5D**

Security Challenges in 5G

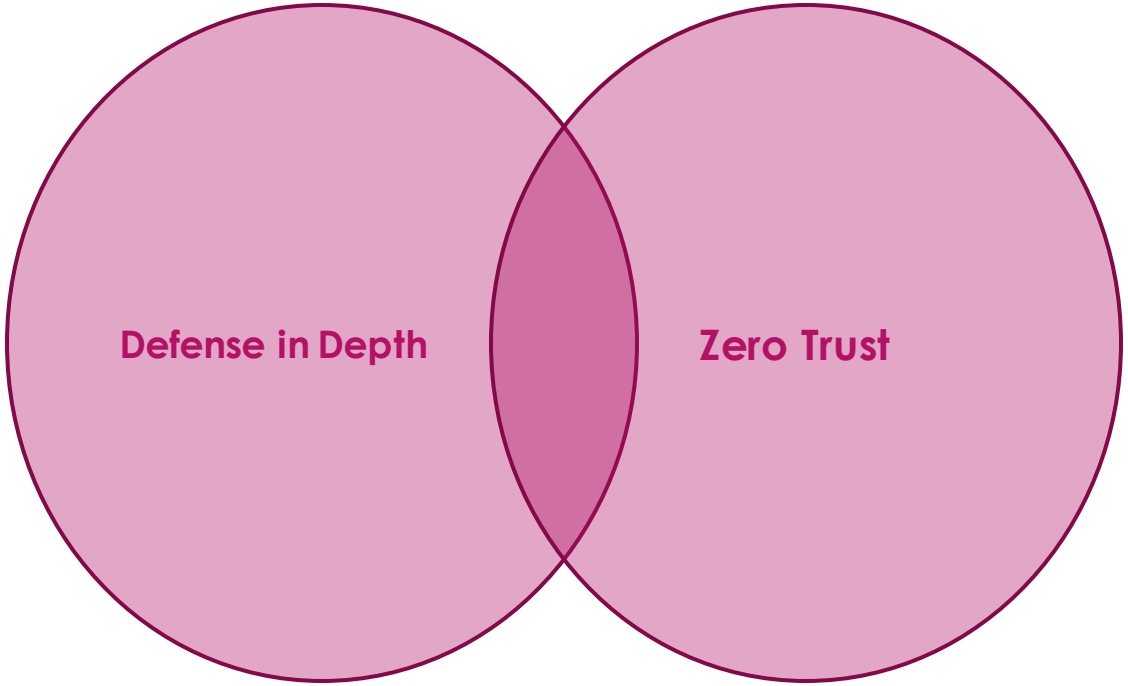
Distributed Architecture	Increased threat vectors due to distributed architecture, data centers, edge computing, Network slicing etc.
Virtualization	Increased cyber susceptibility in securing cloud native architectures
IOT devices & M2M	Tens of billions of IoT Devices with weak inbuilt security provides a vulnerability, especially when there are low-end devices from a variety of manufacturers throughout the world
High bandwidth	With high number of logs existing security monitoring will be overwhelmed
Use of open standards & open sources software	Use if open standards and open-source software introduces new risks due to issues in the supply chain, insufficient testing, poorly written code, and built-in backdoors.
New and Legacy Technologies	Multiple Technology convergence, threat migration between techn… like 4G, 5G, 3G, makes it complex



Security Principles

"uses multiple layers of security for holistic protection"

Series of defensive mechanisms are layered in order to protect valuable data and assets. If one mechanism fails, another steps up immediately to thwart an attack.

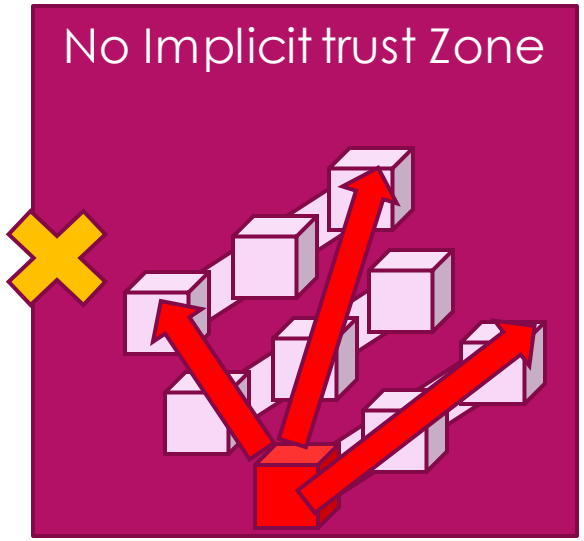


"Never Trust, Always verify"

Zero Trust requires continuous verification of users and devices. Supported by Least privilege and need to know principles.

Zero Trust

Micro segmentation
"No trust Zones"



Identity & Access Management

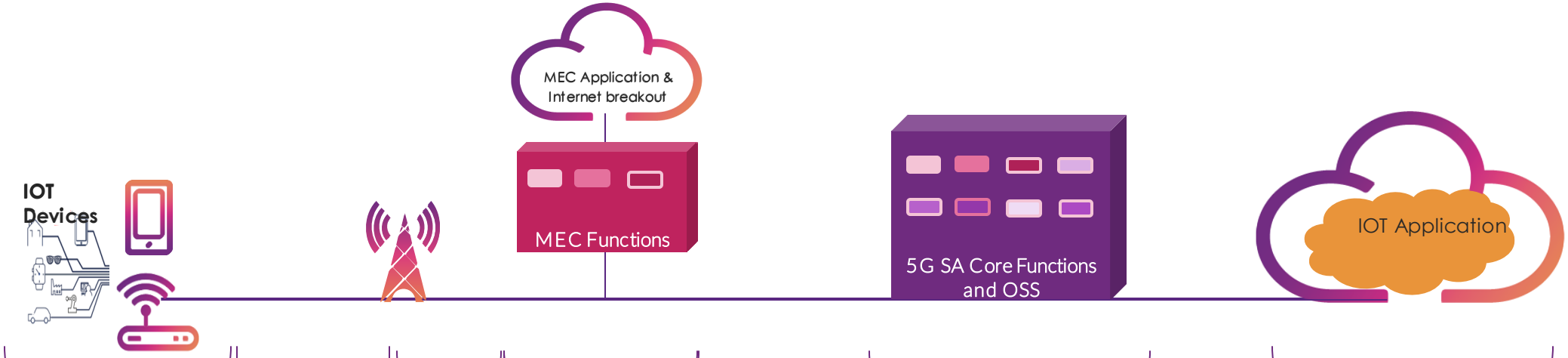
"Who are you ?"

Use of secrets, ephemeral certificates, MFA, mTLS

Authorization

"Can you do it ?"

Understanding 5G domains and threat landscape



End Point (IOT Device / Mobile)

- Malware
- BOT network DDoS
- DOS
- Device tampering
- MitM
- Firmware based attacks

Air Interface

- MitM
- Jamming

Radio Base Station

- Rouge Nodes
- Insecure interfaces
- Improper user access

MEC Edge Computing

- DDoS attack
- Insecure interfaces
- Control plane manipulation
- Virtualization vulnerabilities
- LI vulnerabilities
- Improper user access

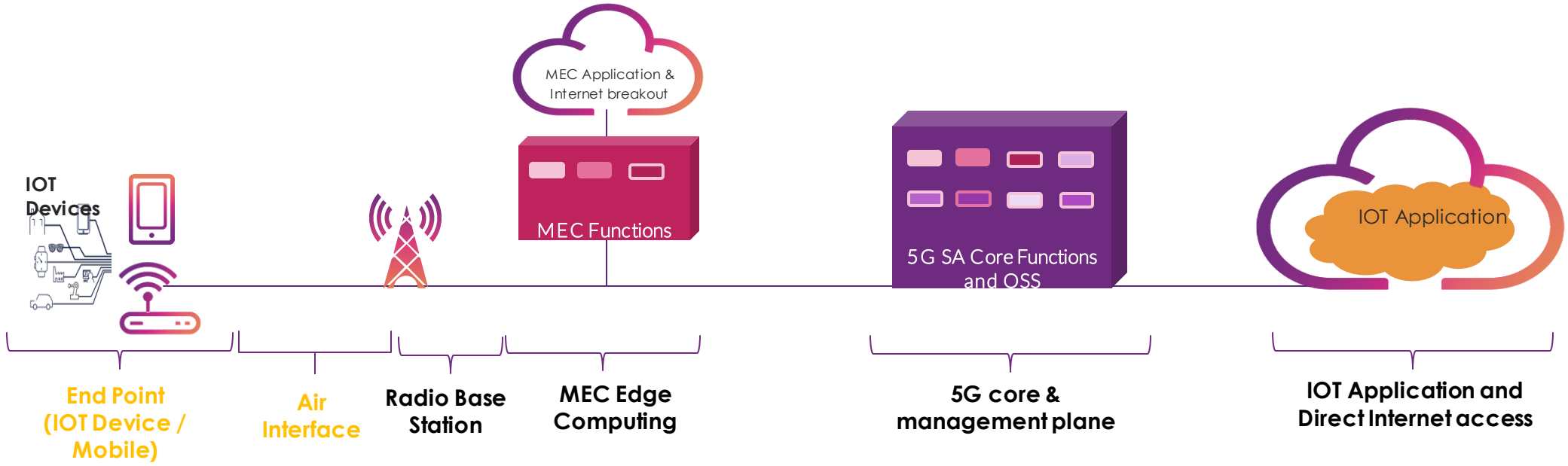
5G core & management plane

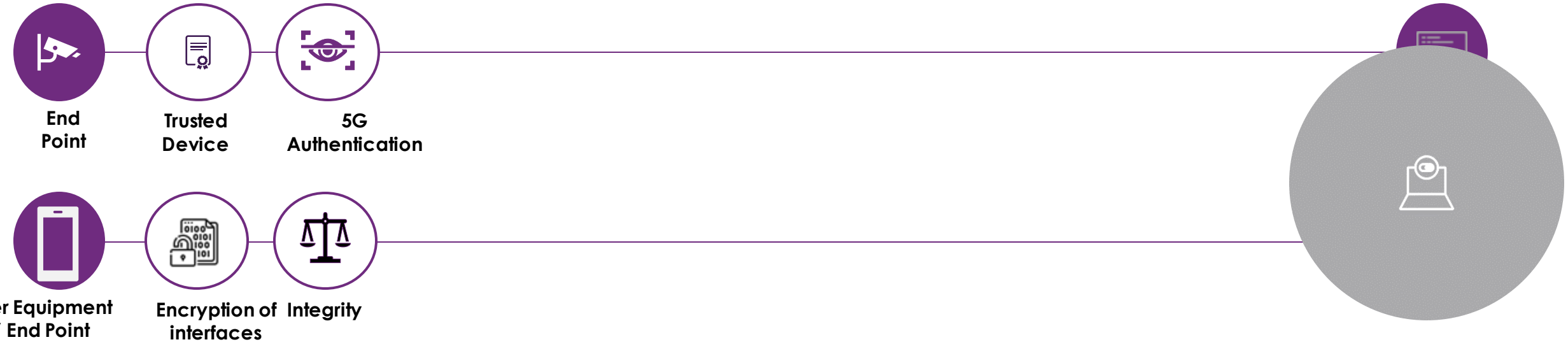
- Insecure interfaces
- Control plane manipulation
- Virtualization vulnerabilities
- LI vulnerabilities
- API Vulnerabilities
- Network functions vulnerabilities
- Supply chain vulnerabilities
- NEF vulnerabilities
- Roaming interconnects
- DDoS & DoS attacks
- Improper user access

IOT Application and Direct Internet access

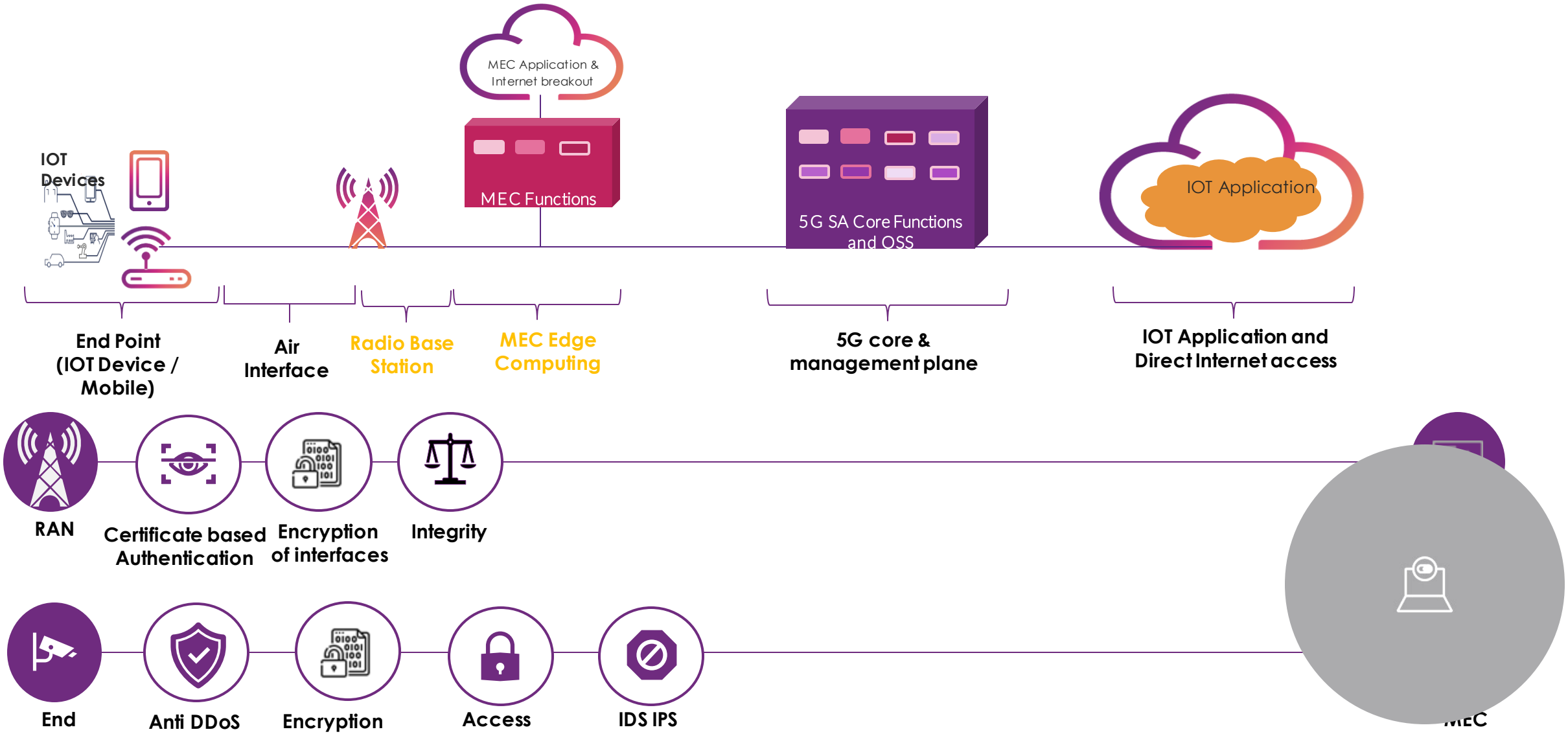
- IoT core integrations
- Application vulnerabilities
- API vulnerabilities
- Improper user access

Defense in Depth and Zero Trust approach

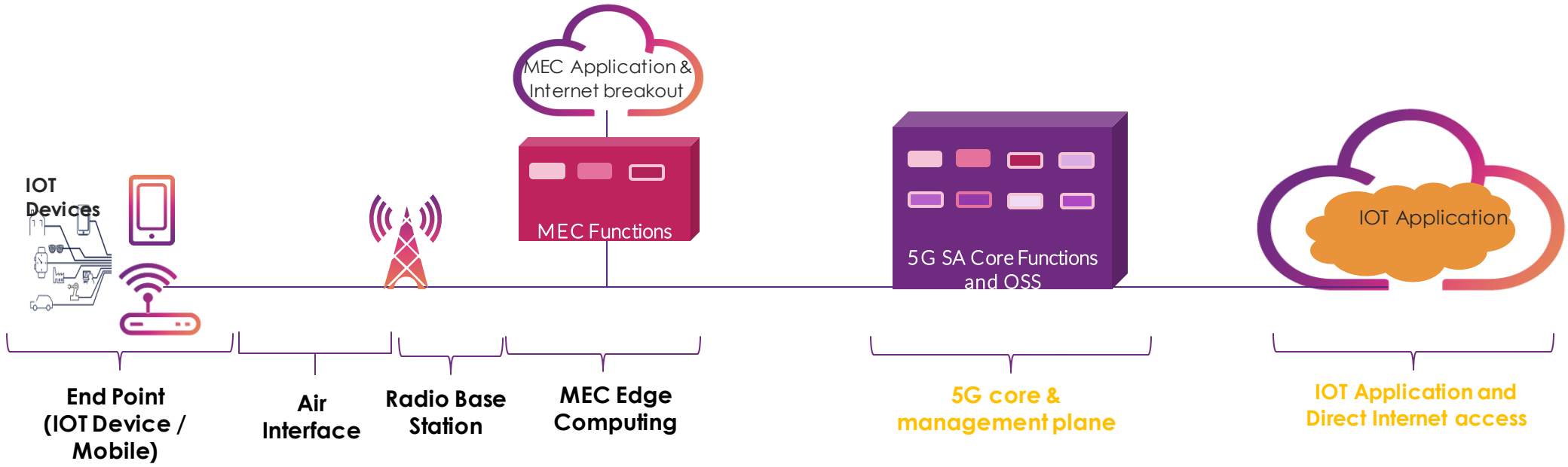




Defense in Depth and Zero Trust approach



Defense in Depth and Zero Trust approach



Questions