# Risks in initial 5G deployments

**3rd Telecom & Digital Infrastructure Security Forum**
Lisboa
24.05.2023

Pedro Simão
pedro.simao@umlaut.com

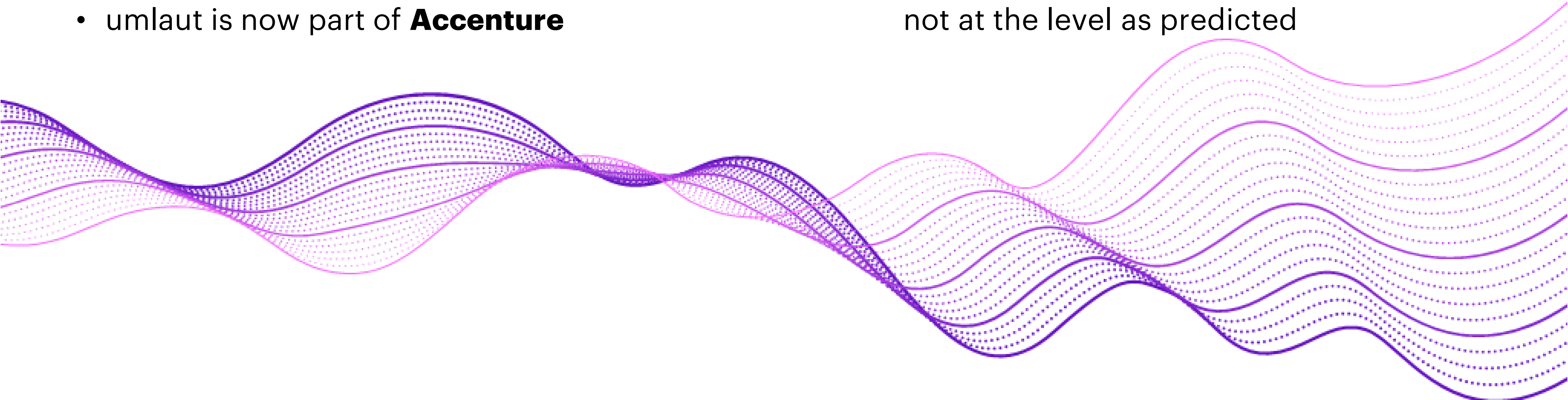
# Introduction

## umlaut

- umlaut is a technical consulting and testing company with 15+ years of experience in telecom security
- umlaut is now part of **Accenture**

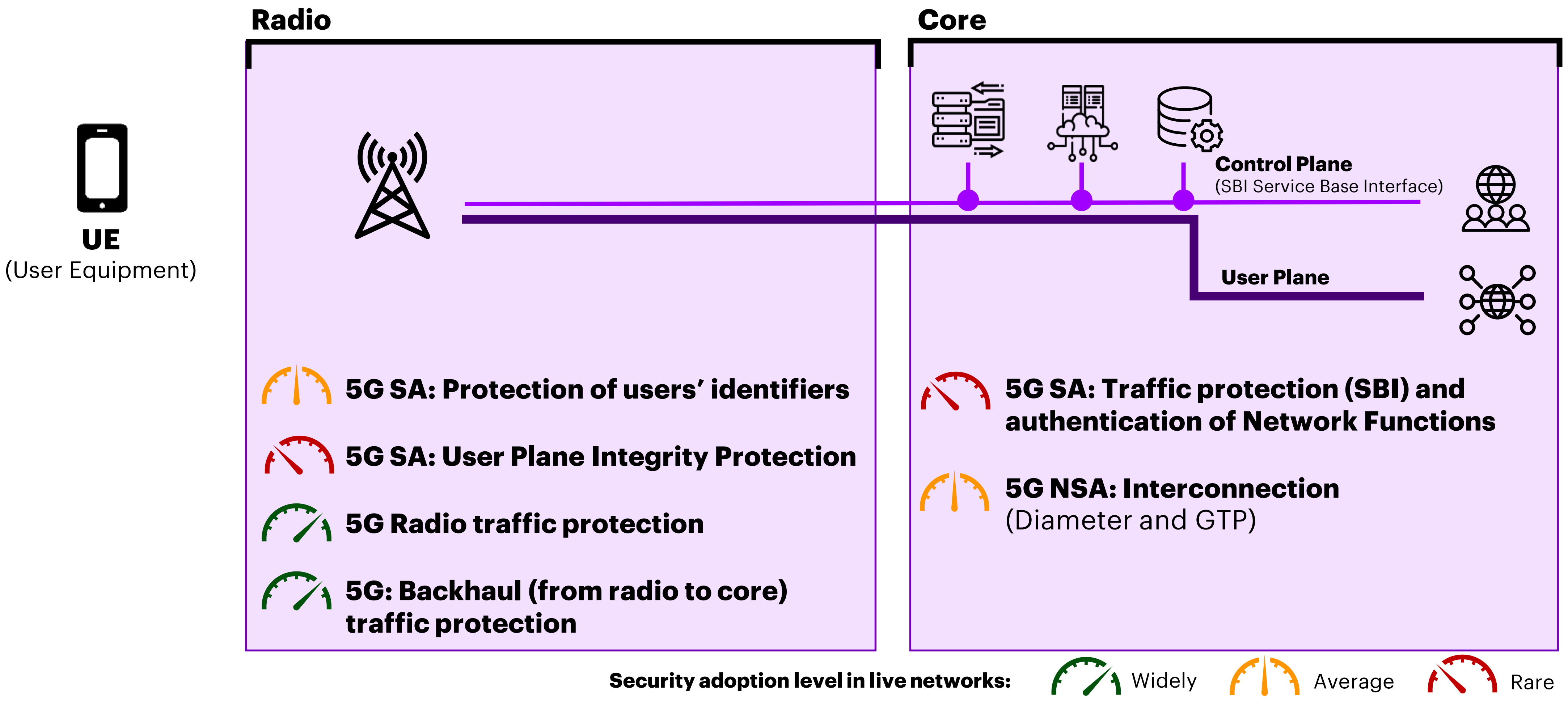
## 5G

- 3GPP improved the security specifications to mitigate known attacks
- The speed of 5G Stand-Alone deployment is not at the level as predicted



# Technology

# 3GPP security features are often not adopted.



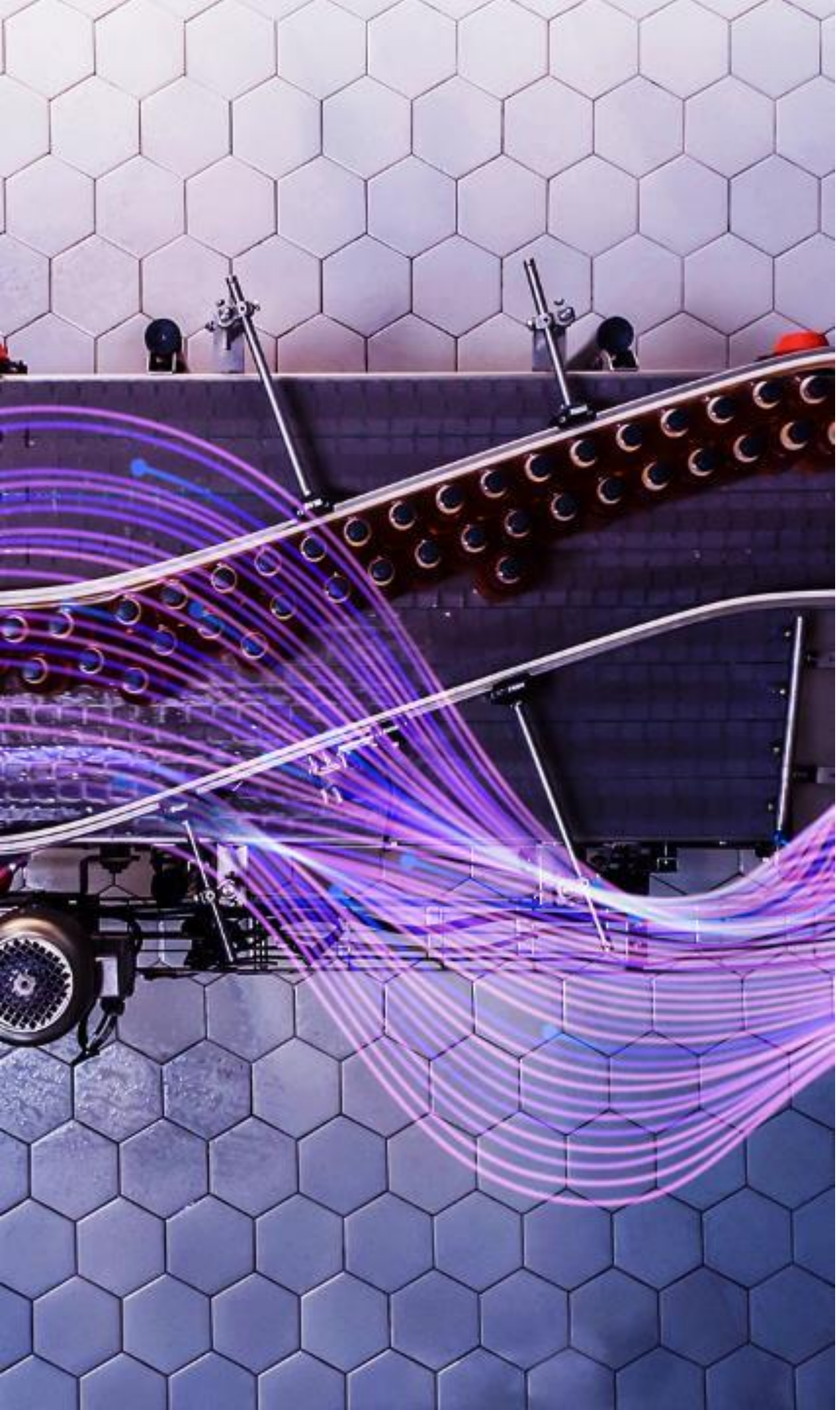
**Radio**

- 🟧 **5G SA: Protection of users' identifiers**
- 🟥 **5G SA: User Plane Integrity Protection**
- 🟩 **5G Radio traffic protection**
- 🟩 **5G: Backhaul (from radio to core) traffic protection**

**Core**

- 🟥 **5G SA: Traffic protection (SBI) and authentication of Network Functions**
- 🟧 **5G NSA: Interconnection** (Diameter and GTP)

**Security adoption level in live networks:** 🟩 Widely 🟧 Average 🟥 Rare



# Telecom environment technologies are bringing value and security risks

## Cloud infrastructure

- Test containers and features enabled by default and not used once in production
- Lack of resources isolation between network functions (eg, memory, network)
- Lack of APIs / interfaces protection (eg, traffic protection, authentication)

## Open RAN

- Lack of security features in early product versions
- Solutions deployed with security vulnerabilities due to lack of security testing
- Lack of hardening and patching of services used

## OSS (Operations Support Systems)

- Centralized management services are not integrated with identity management
- Vulnerabilities in the infrastructure might allow hijack of the full network
- Often security features are not part of consistency checks across all assets

## eSIM

- Level of security in GSMA specs for key exchange and provisioning is high
- Online vouchers / QR code (eg, via self-care portal) generators lack for strong authentication of users. eSIM swap attacks might be possible fully remotely.

# Security Operations

# Security Processes Challenges

## Supply Chain of software components

- Software assets provided by vendors are often not **minimized** (including APIs)**, not patched** and **with security features enabled**
- Mobile operators **do not inspect all software packages**
- Lack of isolation for remote support of assets
- Vendors **TLS self-signed certificates** left at the running environment

## Vulnerability Management

- **Vulnerability and hardening** management on network elements is not widely supported in telecom (including native cloud services)
- Operators struggle to automate the security processes and integrate into IT processes
- **Time to fix is long** in the telecom environment
- Responsibility of mitigation is not clear in some organizations

## Monitoring of network functions and cloud

- Mobile operators rarely deploy monitoring use cases from **external and infrastructure attacks**. Current coverage is limited to identity and access
- Level of **awareness** of telecom attacks and incident response in SOC (Security Operations Center) is low
- Business model from SOC / SIEM solutions limit usage at scale in telecom

*“One of the biggest barriers to cyber resilience in many organizations is time.*

*Business leaders broadly understand they need to become more cyber resilient, but they can’t snap their fingers to make it happen.*

*They know there is a journey to travel to make their organizations cyber resilient, but time is not on their side.”*

**Jacky Fox,**
**Europe Security Lead, Accenture**

# Thank You

**Pedro Simão**

pedro.simao@umlaut.com