Broader Ecosystem : 5G Berlin

ALFONS MITTERMAIER | highstreet technologies

Innovationscluster 5G BERLIN e.V.

@ the i14y LAB Summit 2022

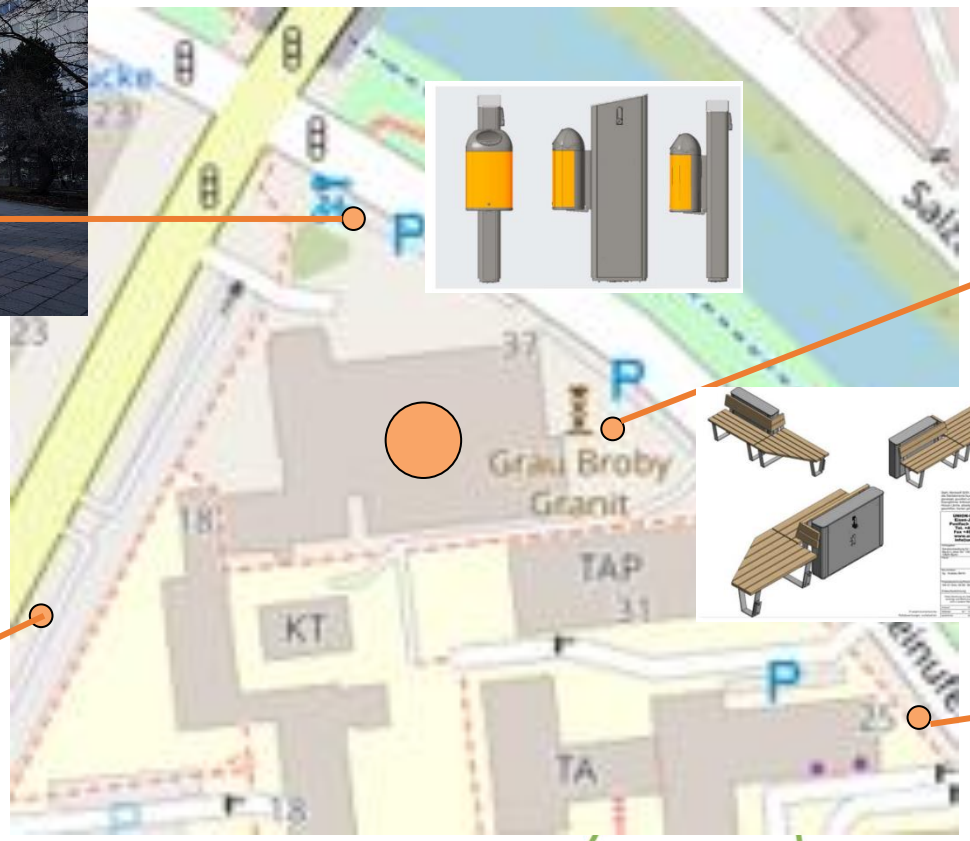
June 9th, 2022

Innovationscluster 5G Berlin e.V.

- Non-profit association acc. to German law
- Founded in 2018
- Operates a 5G test network (3.7 – 3.8 GHz) on the TU Berlin / Fraunhofer HHI campus
- Hosts research projects like BMBF-sponsored OTB-5G+ and BMWK-sponsored CampusOS
- Addresses both public and private 5G networks...
- ... and the interaction between public and private 5G networks.

5G BERLIN

5G Berlin test network being built as part of BMBF-sponsored project OTB-5G+



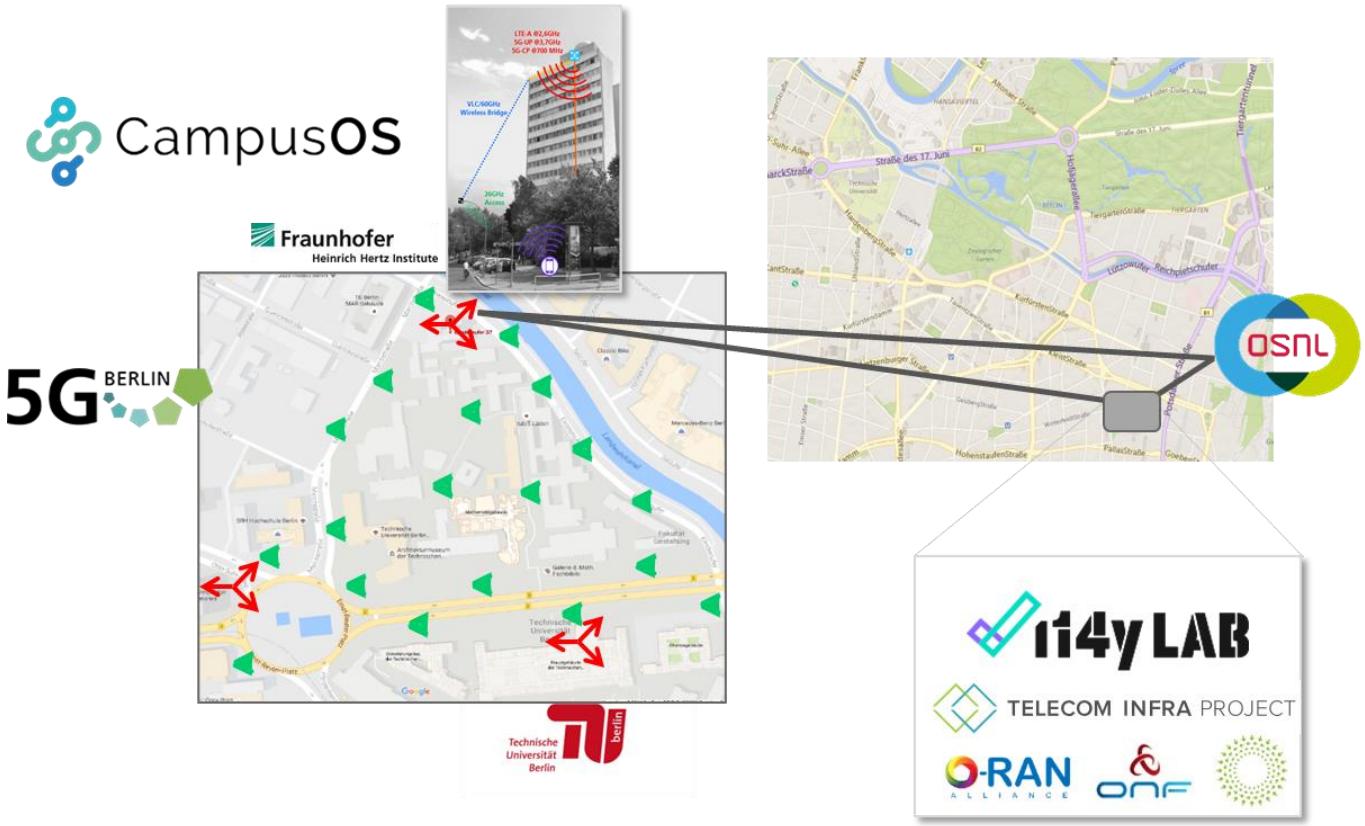
5G BERLIN

OSNL – The Open SDN & NFV Lab

- Loose consortium of primarily small and medium enterprises jointly commercializing research results in the realm of open and programmable networks.
- Test and integration lab in the center of Berlin connected to 5G Berlin test network by dark fibers.

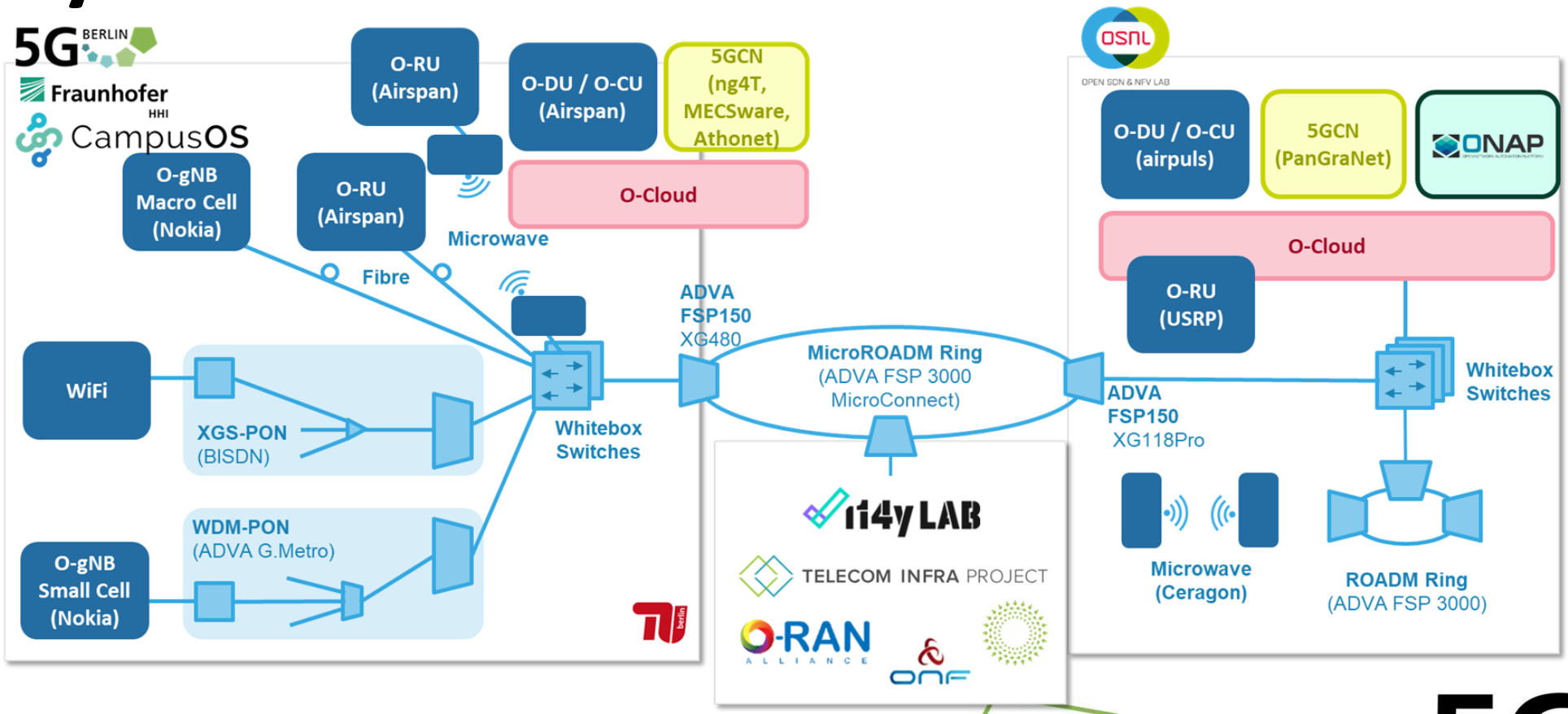
5G BERLIN

Integration of 5G Berlin, CampusOS, i14y LAB and the OSNL



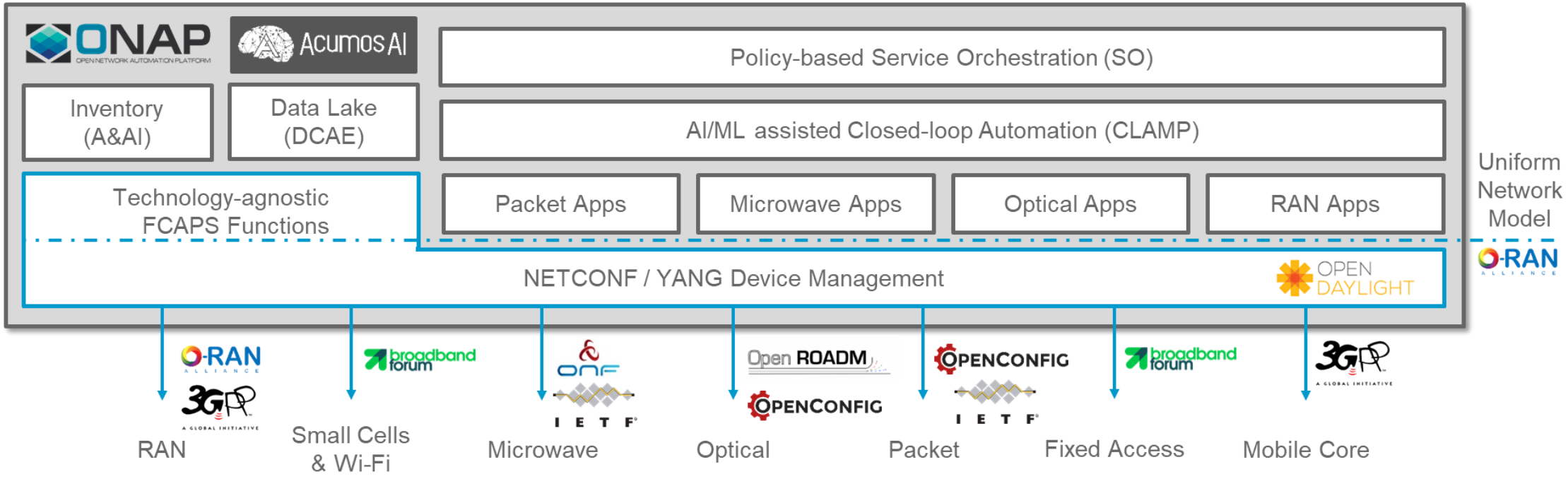
5G BERLIN

Integration of 5G Berlin, CampusOS, i14y LAB and the OSNL



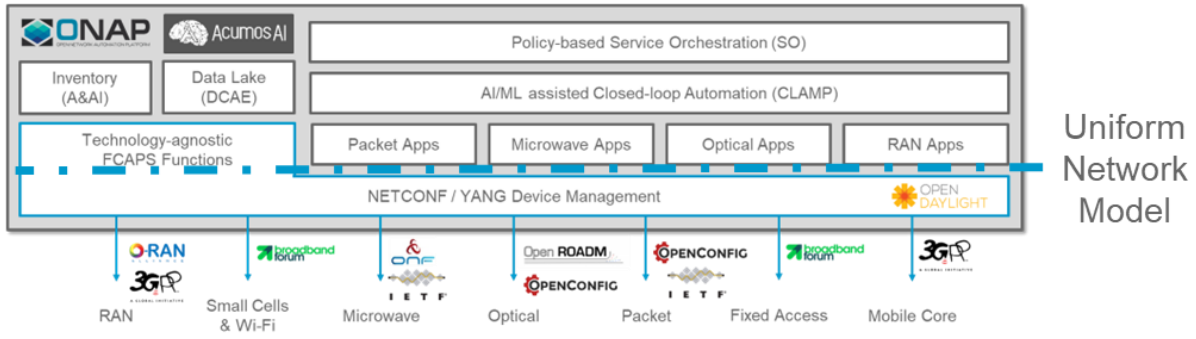
5G BERLIN

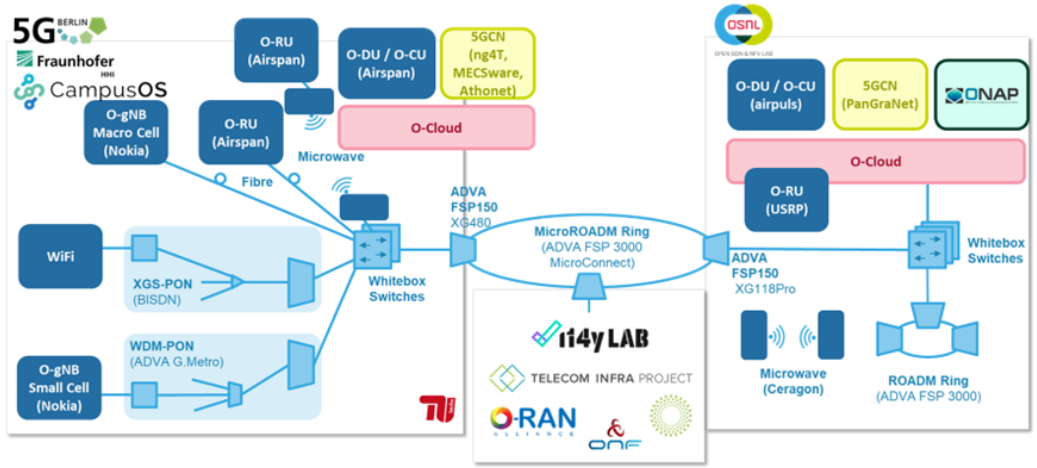
Integration in ONAP



5G BERLIN

Architecture and Roadmap





Standardisation

Q4 2021: Uniform Network Model proposed for discussion in O-RAN Alliance WG 9
Q1 2022: Uniform Network Model concept approved by O-RAN Alliance WG 9
Q2 2022: Uniform Network Model approved by O-RAN Alliance TSC
Q4 2022: Uniform Network Model standardized in O-RAN Alliance WG9

Implementation & integration

Q2 2022: Prototype of Uniform Network Model
Q3 2022: Uniform Network Model implemented for Microwave
Q1 2023: At least one device per technology (Open RAN, 5G Core, Optical, Microwave, Packet, PON, Sync ...) integrated

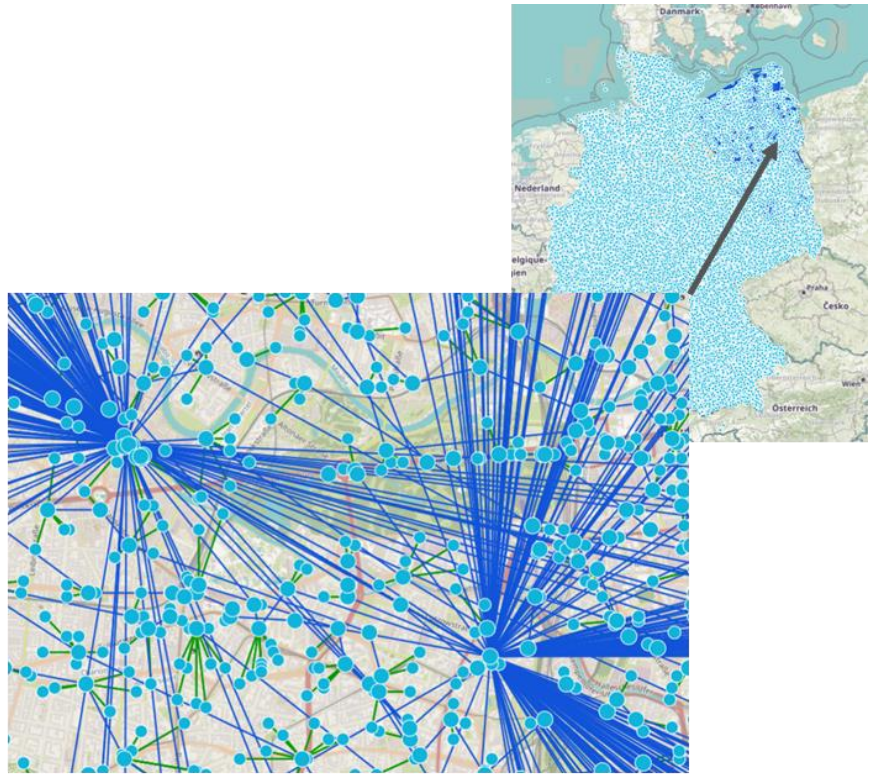
Network infrastructure

Q1 2022: Infrastructure within OSNL up 'n running
Q2 2022: 5G Berlin testbed and OSNL connected
Q3 2022: i14y LAB connected
Q2 2023: All integrated in ONAP

5G BERLIN

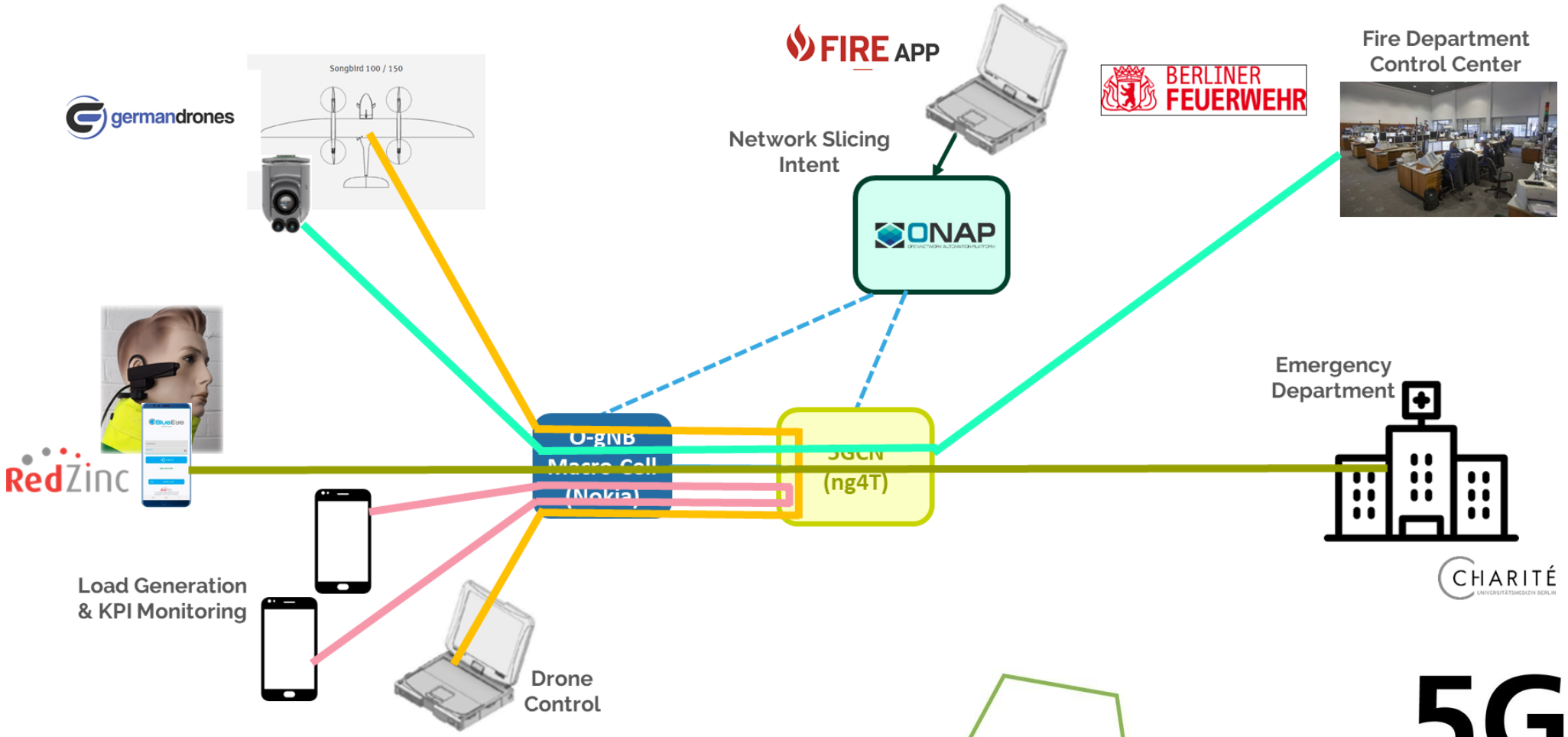
Germany-wide Network

- Simulated network with >90,000 sites
  - Site locations provided by German regulator BNetzA
  - 25% connected by fiber, 75% by microwave
  - Simulated base stations, microwave links and DWDM systems
  - >150,000 simulated devices
- 5G Berlin test network and OSNL
  - Real 5G network with real devices consisting of gNB, Open RAN, 5G Core, microwave, PON, DWDM, IP being built and integrated into ONAP
- Multi-vendor, multi-domain controller
  - FCAPS support of basic feature set
  - Southbound-integration via NETCONF/YANG
  - Northbound-integration via REST-API with Uniform Network Model
- Integration of further devices
  1. VPN connection to vendor and/or operator lab
  2. Devices in i14y LAB
  3. Deployment in operator's lab



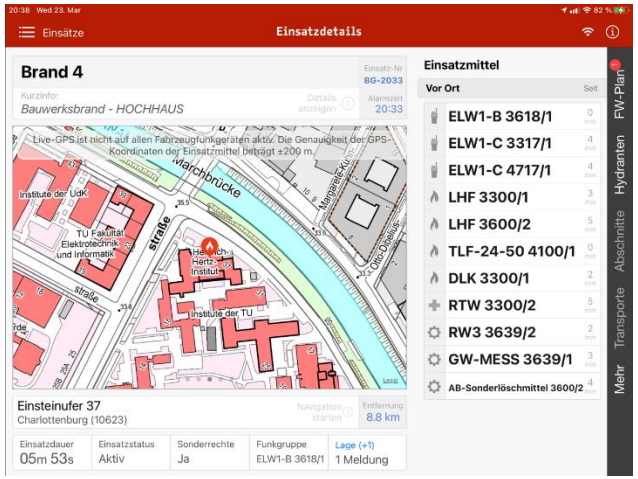
5G BERLIN

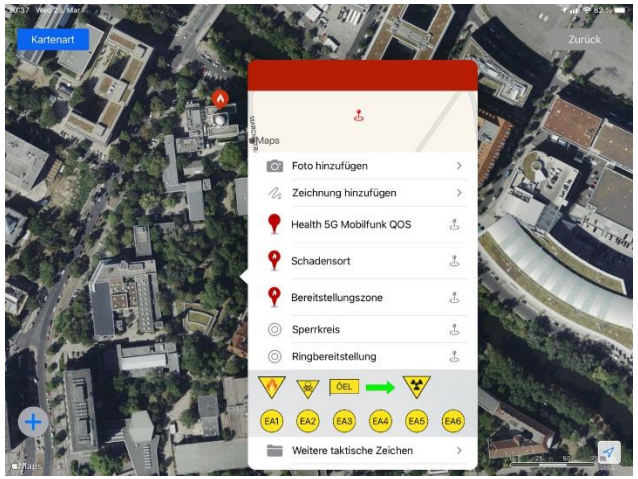
Network Slicing for Emergency Use Cases



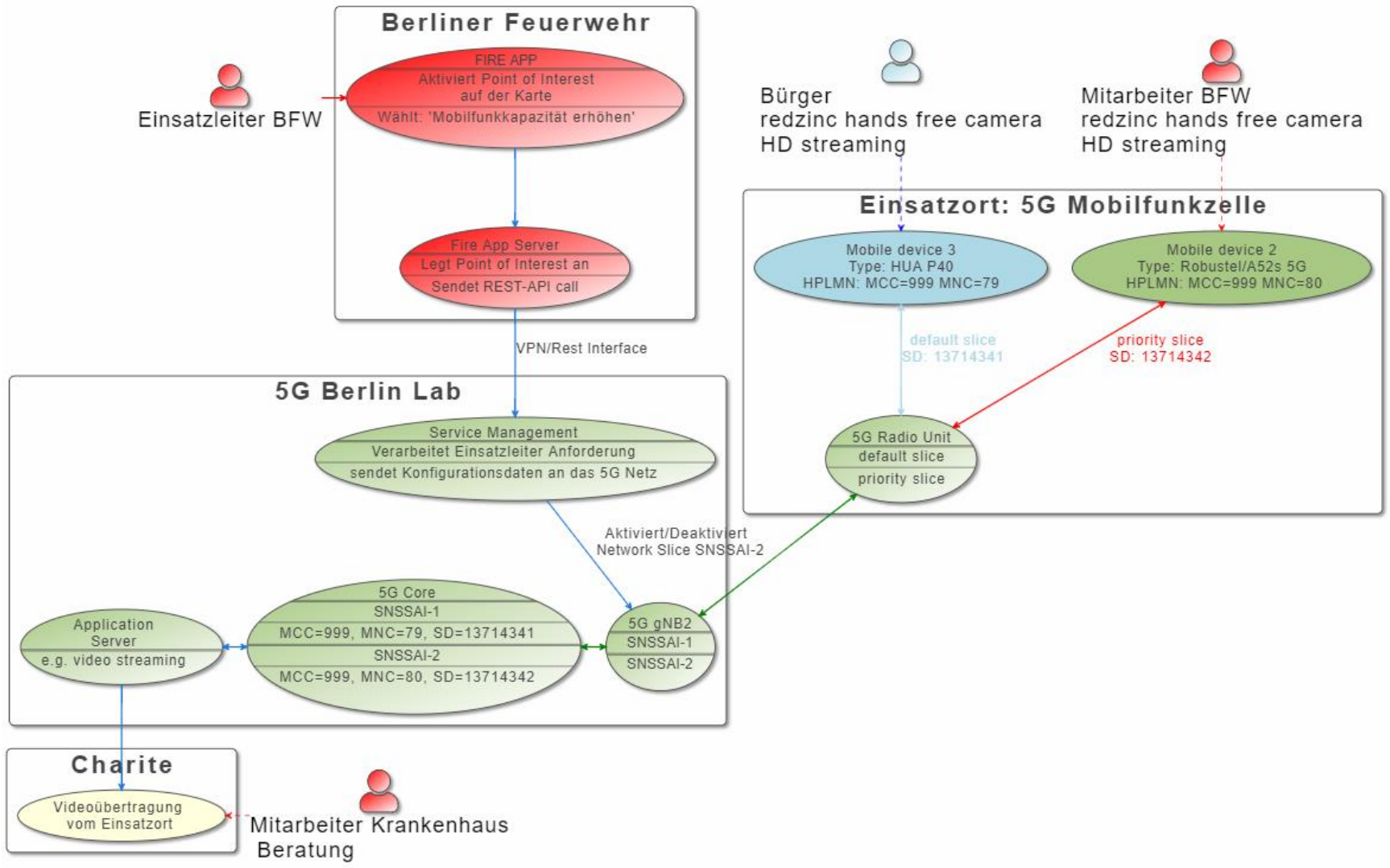
5G BERLIN

Network Slicing – From Intent to QoS





Network Slicing Process



Demo - Overview

‚Einsatzleitung‘ (HHI-Hörsaal)

- **Operator: FireApp**
- **Video-Auswertung**

‚Einsatzort‘ (HHI-Hof)

- ‚Mitarbeiter FW‘ redzinc handsfree camera

Robustel 5G Router

- ‚Bürger‘ mit redzinc handsfree camera

Hua P40pro

POC Integrations Team:

HHI: Konstantin Koslowski, Sven Wittig **ng4T:** Thomas Patzelt

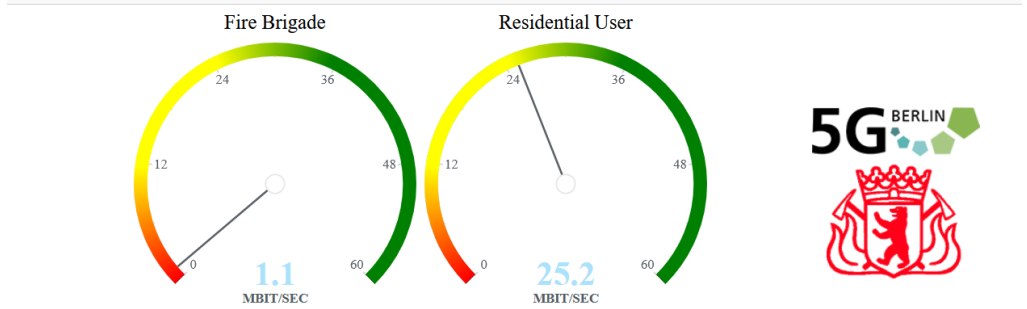
Micronova: Maximilian Heinemann **BananaGlue:** Dr. Jan Winter

highstreet-technologies: Shabnam Sultana, Alexander Dehn

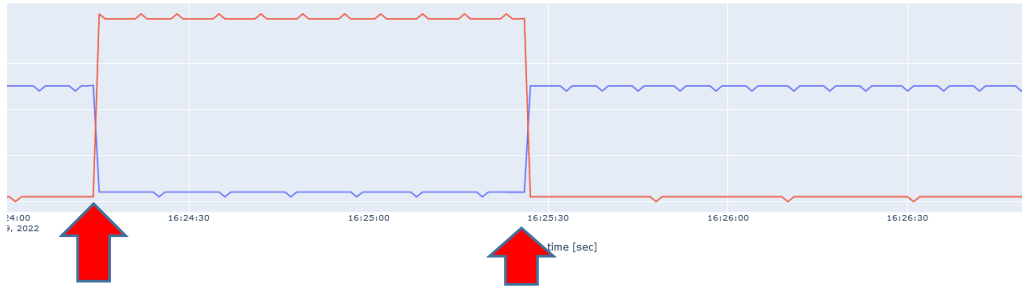
5G BERLIN

Demo – Teil 1

ZIEL: Aktivierung und Deaktivierung eines priorisierten ‚Emergency 5G Netzwerk Slices' über die FireApp.
Nachweis der verfügbaren (Upstream) Bandbreite über Messung von Lastgeneratoren auf den Endgeräten



Bandbreite
Mbit/s

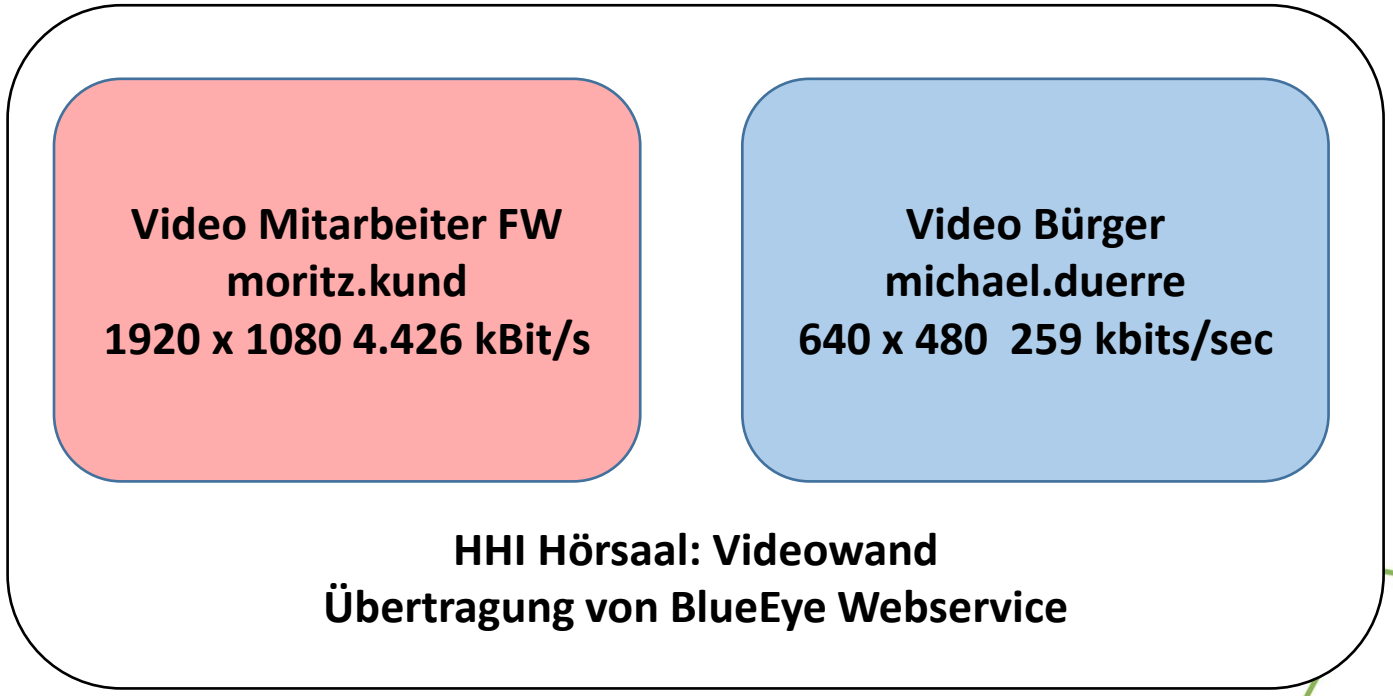


(1) (2) (3) (4) (5)

1) Emergency Slice ist deaktiviert
   Bürger hat hohe Bandbreite
2) FireApp: Bereitstellung QoS
   Emergency Slice aktiviert
3) Hohe Bandbreite für Einsatzkräfte
   Niedrige Bandbreite für Bürger
4) FireApp: QoS Anforderung aufgehoben
5) Emergency Slice deaktiviert
   Bürger erhält wieder hohe Bandbreite

Demo – Teil 2

ZIEL: Bereitstellung eines priorisierten ‚Emergency Slices' über FireApp.
Videoübertragung vom ‚Einsatzort' mit hohem QoS über Emergency Slice
Videoübertragung vom ‚Einsatzort' durch einen Unbeteiligten mit niedrigem QoS über den Standard-Slice



1) Emergency Slice deaktiviert
   Bürger-Video: hohe Auflösung
   FW-Video: Aus
2) FireApp: Bereitstellung QoS
   Emergency Slice aktiviert
3) Bürger-Video: schlechtere Auflösung
   FW-Video: hohe Auflösung

5G BERLIN

Feedback and Next Steps

- Applications
  - Drones
  - Ad-hoc networks (nomadic nodes)
  - ...
- QoS of 5G network slices
  - Data rate (up- / down-link), latency, availability, coverage ...
  - Arbitration of services in situations of scarce resources
  - Do we need a digital twin for knowing in advance what we can get where?
- Interface between emergency organizations and Service Management & Orchestration
  - Fire fighters, first responders, BDBOS ... <-> Mobile Network Operators
- Multi-operator network slices
- Collaboration with other 5G projects

Join us!
5G-BERLIN.org

5G BERLIN

Don´t worry about ORAN security – ETSI has other headaches

JEAN PIERRE SEIFERT | TU Berlin
professor

Don’t worry about ORAN security – ETSI has other headaches

Jean-Pierre Seifert
Einstein Professor
TU Berlin, Berlin (Germany)
jeanpierreseifert@gmail.com

Based on:

Breaking the quadratic barrier: Quantum cryptanalysis of Milenage, telecommunications’ cryptographic backbone

Vincent Ulitzsch
Technische Universität Berlin
Berlin, Germany
vincent@sect.tu-berlin.de

Jean-Pierre Seifert
Technische Universität Berlin
Berlin, Germany
jean-pierre.seifert@tu-berlin.de

Bundesministerium für Bildung und Forschung

6G-RIC Research and Innovation Cluster

9th June 2022

Agenda

- ORAN Security
- Telecommunication Crypto 101
- Quantum Computing $\rightarrow$ Crypto
- Results for Milenage (crypto backbone of TelCo world)
- Implications for 6G

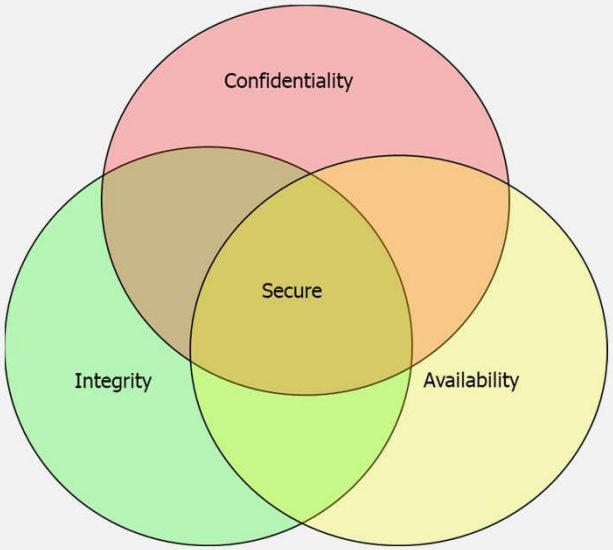
Agenda

- **ORAN Security**
- Telecommunication Crypto 101
- Quantum Computing $\rightarrow$ Crypto
- Results for Milenage (crypto backbone of TelCo world)
- Implications for 6G

Definition: (Computer) Security

- Two views on it:

1. Intersection of …



2. (Computer) Security deals with the prevention and detection of unauthorized actions by users or others of a System.

ORAN Security

- **Sure, ORAN Security is a wide, complex, and new field!**
- **Openess caused already in Android phones trouble!**
- **But where to start to meet the definition?**

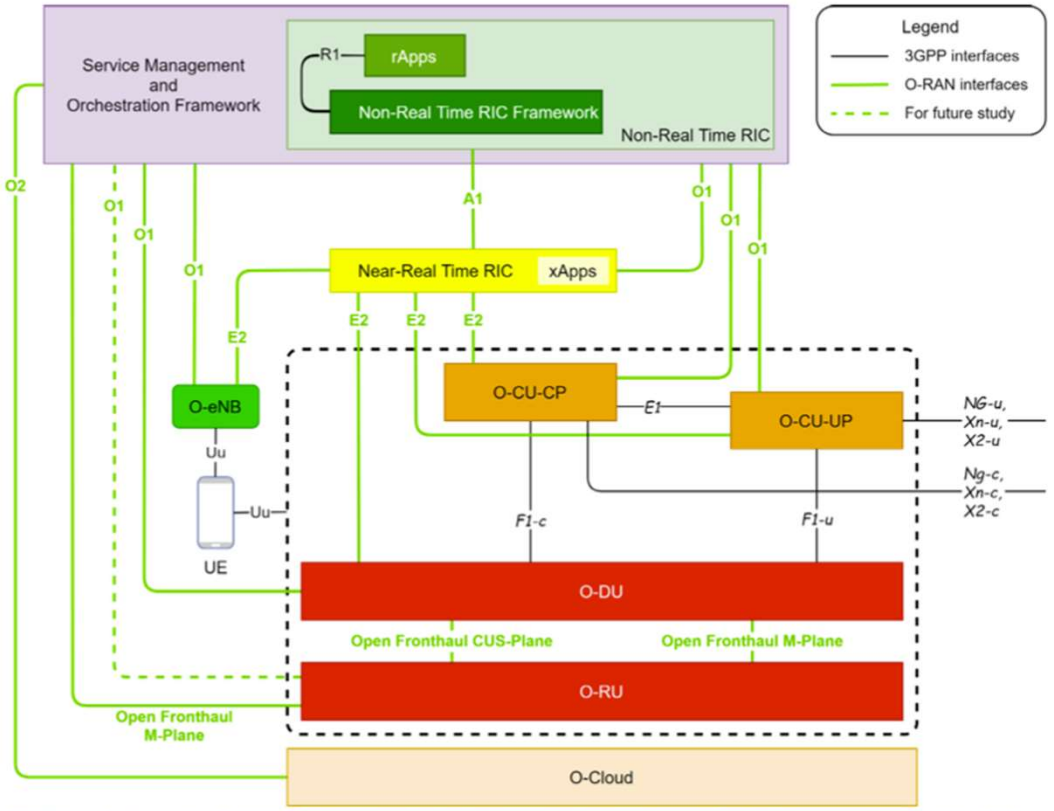


Abbildung 5: Logische O-RAN-Architektur einschließlich Uu-Schnittstelle zu O-RAN-Komponenten und O-eNB [14]

ORAN Security

- **Some initial work did some theoretical & „claimish“ investigation:**

LinkedIn Personen Kashif Shakil

Implementing a secure 5G open RAN

Kashif Shakil
Strategic Product Manager, Cloud RAN
Veröffentlicht: 22. Sept. 2020

+ Folgen

ORAN is enabling exciting new opportunities in radio access networks. It disaggregates hardware from software, virtualizes and breaks down network functions and establishes new open interfaces. ORAN based 5G networks could use components from different HW and SW vendors, promoting vendor diversity and 5G supply chain resiliency.

One important consequence of ORAN is that operators need to rethink network security. Ericsson has recently published a white paper (https://www.ericsson.com/en/blog/2020/9/open-ran-security-5g) highlighting the need for new security considerations in ORAN. In summary, ORAN specifications expand the threat surface of 5G networks. ORAN operator and vendor community need to strengthen security.

In this article, we discuss the new security paradigm that results from the architecture of ORAN vs. traditional RAN. Information security is a big topic. The discussion in this article is constrained to ORAN security architecture. We do not discuss system security topics like securing perimeter, penetration testing etc.

Im Auftrag des:
Bundesamt für Sicherheit in der Informationstechnik

In Zusammenarbeit mit:
secunet

Studie

Open-RAN Risikoanalyse

5GRANR

Version: 1.2.1
Datum: 21. Februar 2022
Autoren: Stefan Köpsell (Barkhausen Institut)
Andrey Ruzhanskiy (Barkhausen Institut)
Andreas Hecker (Advancing Individual Networks GmbH)
Dirk Stachorra (Advancing Individual Networks GmbH)

ORAN Security

- **Some initial work did some theoretical & „claimish“ investigation:**

Adversarial Machine Learning Threat Analysis in Open Radio Access Networks

Ron Bitton, Dan Avraham, Eitan Klevansky, Dudu Mimran, Oleg Brodt
Heiko Lehmann, Yuval Elovici, and Asaf Shabtai

***Abstract*—The Open Radio Access Network (O-RAN) is a new, *open*, *adaptive*, and *intelligent* RAN architecture. Motivated by the success of artificial intelligence in other domains, O-RAN strives to leverage machine learning (ML) to automatically and efficiently manage network resources in diverse use cases such as traffic steering, quality of experience prediction, and anomaly detection. Unfortunately, ML-based systems are not free of vulnerabilities; specifically, they suffer from a special type of logical vulnerabilities that stem from the inherent limitations of the learning algorithms. To exploit these vulnerabilities, an adversary can utilize an attack technique referred to as adversarial machine learning (AML). These special type of attacks has already been demonstrated in recent researches. In this paper, we present a systematic AML threat analysis for the O-RAN. We start by reviewing relevant ML use cases and analyzing the different ML workflow deployment scenarios in O-RAN. Then, we define the threat model, identifying potential adversaries, enumerating their adversarial capabilities, and analyzing their main goals. Finally, we explore the various AML threats in the O-RAN and review a large number of attacks that can be performed to materialize these threats and demonstrate an AML attack on a traffic steering model.**

***Index Terms*—Open radio access networks, adversarial machine learning, security and privacy, threat analysis**

I. Introduction

In recent years, the number of cellular network users has increased dramatically. According to Statista's 2021 report,[1] in 2021 there were 15 billion unique mobile devices, a number which is expected to reach 18.22 billion by 2025. There has also been rapid growth in the number of connected IoT devices, with a projection of 27 billion connected IoT devices in 2025,[2] and thus, the requirements of the cellular network are not limited to just mobile devices. Currently, cellular networks must support a diverse set of use cases [34], including smartphones and smart watches, drones, industrial IoT devices, distributed sensors, and connected cars. New devices, use cases and applications pose new challenges for cellular networks. Such challenges include the need to serve billions of devices, while maintaining low expenses, and the need to offer adaptive bandwidth and latency requirements, in real time, for different application and use cases.

[1]Statista's Forecast: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/
[2]IoT Analytics State of IoT Summer 2021: https://iot-analytics.com/product/state-of-iot-summer-2021/

A. The Open Radio Access Network

In order to support new cellular network requirements, vendors have started investigating new radio access network (RAN) architectures. A promising RAN architecture that has gained worldwide acceptance is the Open Radio Access Network (O-RAN), which was suggested by the O-RAN Alliance [1]. The O-RAN Alliance (founded in February 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange) is a worldwide community of mobile network operators, vendors, and academic institutes. The alliance's vision is to reshape the RAN industry toward the establishment of an *open*, *adaptive*, and *intelligent* RAN.

O-RAN's Vision: key objectives defined by the alliance

Open: All design documents, interfaces, and software must be open. The openness aspect promotes multi-vendor deployments with open interfaces between all decoupled RAN components, enabling a more competitive ecosystem.
Adaptive: RAN components must be able to adapt themselves, in real time, to support different use cases and service requirements. To achieve this goal, the alliance promotes the cloudification of the RAN technology and an overall shift to cloud-native technologies, where network components are virtualized and controlled by software-defined networking. Cloudification facilitates flexible resource provisioning and enables centralization of the RAN infrastructure and a reduction of operational costs [2].
Intelligent: RAN management must not rely on human intensive means. Motivated by the success of artificial intelligence and machine learning (ML) in other domains, the O-RAN strives to leverage ML for efficient automated network resource management. This includes a large set of use cases such as: traffic steering, quality of experience prediction, network traffic prediction, and anomaly detection.

B. Security of the O-RAN

The introduction of new concepts and technologies into the RAN is promising in terms of meeting the new requirements [35]. Unfortunately, when new technologies are introduced, they are accompanied by new cybersecurity threats; as a result, the RAN's attack surface may change dramatically when integrating new technologies. Understanding the new attack surface is crucial for securing the new Open RAN architecture.

Recent studies have provided a throughout security analysis of the new Open RAN architecture, however

Open or not open: Are conventional radio access networks more secure and trustworthy than Open-RAN?

Felix Klement[1], Stefan Katzenbeisser[1], Vincent Ulitzsch[2], Juliane Krämer[3], Slawomir Stanczak[4], Zoran Utkovski[4], Igor Bjelakovic[4], and Gerhard Wunder[5]

[1]Computer Engineering, University of Passau, 94032 Passau, Germany
[2]Security in Telecommunications, TU Berlin, 10587 Berlin, Germany
[3]Data Security and Cryptography, University of Regensburg, 93053 Regensburg, Germany
[4]Fraunhofer Heinrich Hertz Institute, 10587 Berlin, Germany
[5]Cybersecurity and AI Group, FU Berlin, 14195 Berlin, Germany

***Abstract* — The Open-RAN architecture is a highly promising and future-oriented architecture. It is intended to open up the radio access network and enable more innovation and competition in the market. This will lead to RANs for current 5G networks, but especially for future 6G networks, to move away from the current centralised, provider-specific 3G RAN architecture and therefore even better meet the requirements for future RANs. However, the change in design has also created a drastic shift in the attack surface compared to conventional RANs. In the past, this has often led to negative headlines, which in summary have often associated O-RAN with faulty or inadequate security. In this paper, we analyze what components are involved in an Open-RAN deployment, how the current state of security is to be assessed and what measures need to be taken to ensure secure operation.**

***Keywords* — Open-RAN, O-RAN, 5G, 6G, Security**

I. Introduction to Open-RAN

A. Motivation

Modern communication is one of the central pillars of successful digitization. Particularly instrumental is the recently introduced 5G technology and its ongoing evolution towards 6G. In addition to public mobile networks, 5G technology - and in the long term 6G - will also be used for local radio networks (so-called private networks or campus networks).

A 5G mobile network (whether public or private) typically consists of a transport network (e.g., fiber optic network), a core network with central elements for network control, and the radio access network (RAN) that provides connections to mobile terminals. A schematic example of such a 5G mobile radio network can be taken from Figure 1. While there is a plethora of vendors for virtualized core networks, radio access networks are provided by only a handful of major network equipment vendors. Today's RANs are also highly vertically integrated solutions from individual vendors, with little interoperability between products from different vendors. This inevitably leads to barriers to innovation.

A key to more innovation in mobile networks lies in the Open-RAN concept, making use of RAN technologies

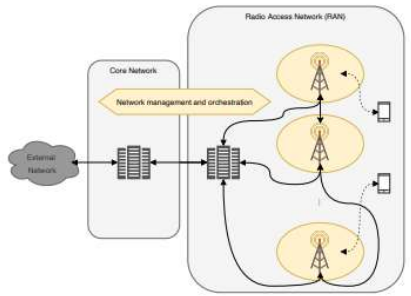


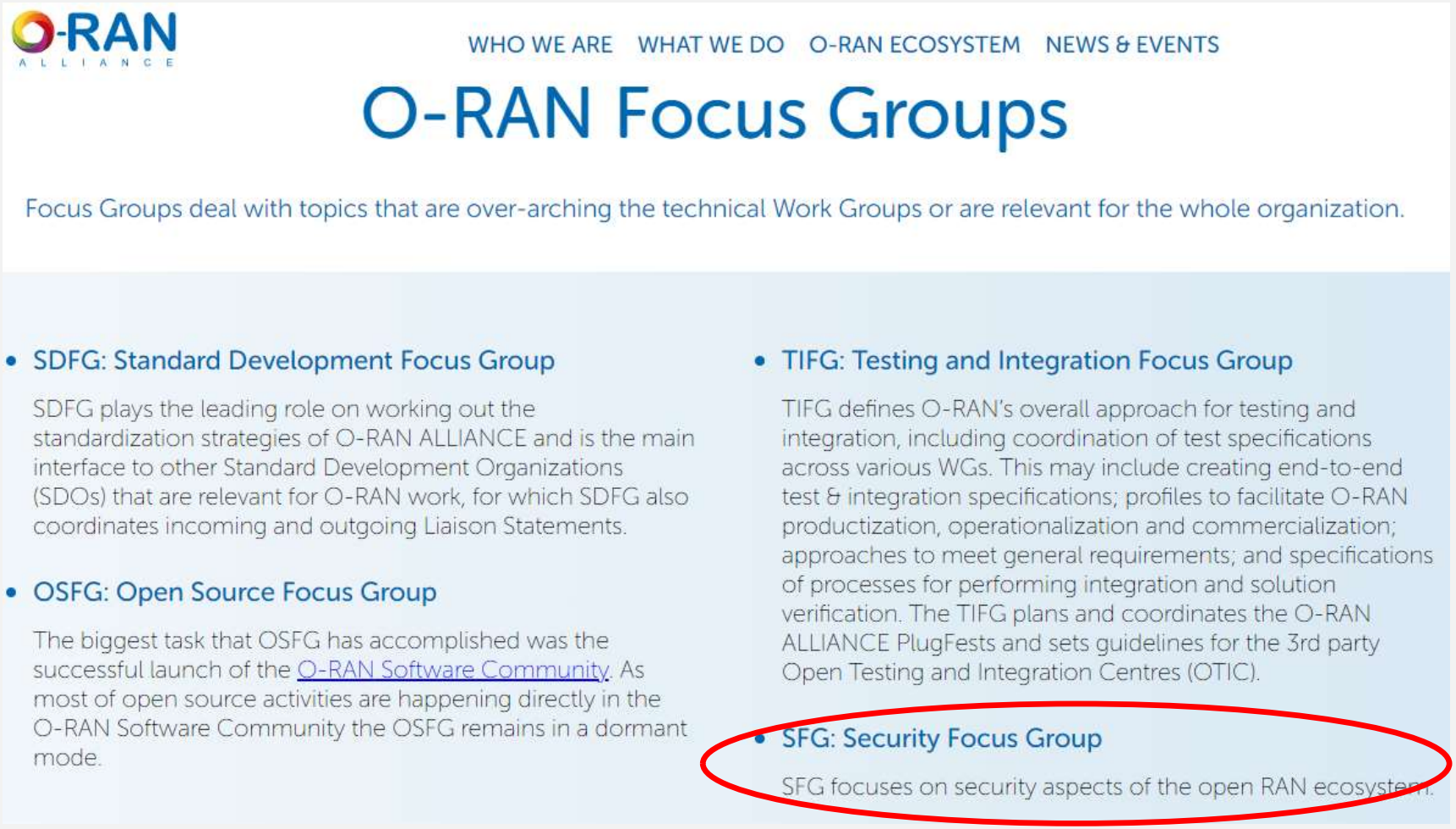
Fig. 1. Mobile Network

based on disaggregation and openness. At the Open-RAN concept is the division of the RAN into several RAN modules that perform different RAN functions. The crucial point here is that the interfaces between the RAN modules are open and guarantee interoperability. The open interfaces are at the same time the basis for more flexibility and the much needed trust in communication technologies. Finally, Open-RAN promises performance enhancements over the current integrated vendor-specific solutions.

In addition to the architectural disaggregation and openness (in the sense of interoperability), the aspects of cloudification and virtualisation [1], network slicing [2], [3] and machine learning [4] also play an important role in the Open-RAN context. Yet, it is important to emphasize that except for disaggregation and openness, the other aspects such as virtualization and machine learning are not an integral part of the Open-RAN concept. For instance, in Massive MIMO systems, it may be much more efficient to implement the

ORAN Security

- **Some real ORAN Security work:**



O-RAN ALLIANCE

WHO WE ARE WHAT WE DO O-RAN ECOSYSTEM NEWS & EVENTS

O-RAN Focus Groups

Focus Groups deal with topics that are over-arching the technical Work Groups or are relevant for the whole organization.

- **SDFG: Standard Development Focus Group**

  SDFG plays the leading role on working out the standardization strategies of O-RAN ALLIANCE and is the main interface to other Standard Development Organizations (SDOs) that are relevant for O-RAN work, for which SDFG also coordinates incoming and outgoing Liaison Statements.

- **OSFG: Open Source Focus Group**

  The biggest task that OSFG has accomplished was the successful launch of the O-RAN Software Community. As most of open source activities are happening directly in the O-RAN Software Community the OSFG remains in a dormant mode.

- **TIFG: Testing and Integration Focus Group**

  TIFG defines O-RAN's overall approach for testing and integration, including coordination of test specifications across various WGs. This may include creating end-to-end test & integration specifications; profiles to facilitate O-RAN productization, operationalization and commercialization; approaches to meet general requirements; and specifications of processes for performing integration and solution verification. The TIFG plans and coordinates the O-RAN ALLIANCE PlugFests and sets guidelines for the 3rd party Open Testing and Integration Centres (OTIC).

- **SFG: Security Focus Group**

  SFG focuses on security aspects of the open RAN ecosystem.

Usually the strongest weapon in (computer) security is for good reasons still:

CRYPTOGRAPHY

CYBER TELECOM — Cybertelecom Federal Internet Law & Policy An Educational Project

Crypto

It is said that the United States traditionally prepares for the last war - meaning that the United States has historically been unprepared for the current war that it confronts. The last "great war" was World War II. Cryptography had everything to do with winning that war. Messages broadcast using early radio technology were out in the open for any covert ears to capture. Cryptography, however, turned public broadcasts into private communications. Conversely, cracking the code turned garbled nonsense into powerful information. In World War II, the allies ability to break the code was crucial.

In The Pond, the Germans communicated with their U Boat submarines during the Great Duck Hunt (the period where the U Boats roamed in wolf packs largely unchallenged, sinking ship after ship carrying supplies to the Britain from the United States) using an odd type writer like mechanism called The Enigma. Alan Turing leading the team at Bletchley Park developed one of the first electronic computing machines, cracked the Enigma Code, and turned the U Boat from the hunter to the hunted.

Enigma Machine

On the other side of the globe, US intelligence broke Japanese Code leading to multiple turning points in the War. Unsure of the destination of the massed Japanese fleet, the U.S. sent a low priority, unsecured transmission that Midway Island was facing a water shortage. When the Japanese sent a coded message that their target faced a water shortage, the Americans knew the Japanese battle plan and the famous Battle of the Midway was initiated. In another epic moment, the Americans intercepted a Japanese encoded message giving the specific flight itinerary of the famous Admiral Yamamoto. The United States sent a squadron to meet the notoriously punctual Japanese and deprived the Japanese Navy of the further service one of its great commanders.

It is in this context (and of course that of the Cold War) that the United States has become particularly anxious about cryptography. In the eyes of the United States government, cryptography is not just a cute mathematical algorithm produced by a bunch of software. Cryptography is a weapon. And you do not get to export weapons outside of the United States without the oversight and consent of an anxious government.

Of course this creates a bit of a problem. Cryptography is more than a weapon. It is also a vehicle for e-commerce. It is a vehicle for secure communications and transactions, including financial services and commercial transactions. Consumer faith in the ability to purchase widgets online will not be high where the cryptography used to protect the financial instruments, in other words the credit cards, can be easily broken by off the shelf code. For American companies to sell their software products and provide their services abroad, they need to be able to utilize strong encryption. But US export regulation, for a while, forbade it, and US products suffered a competitive disadvantage.

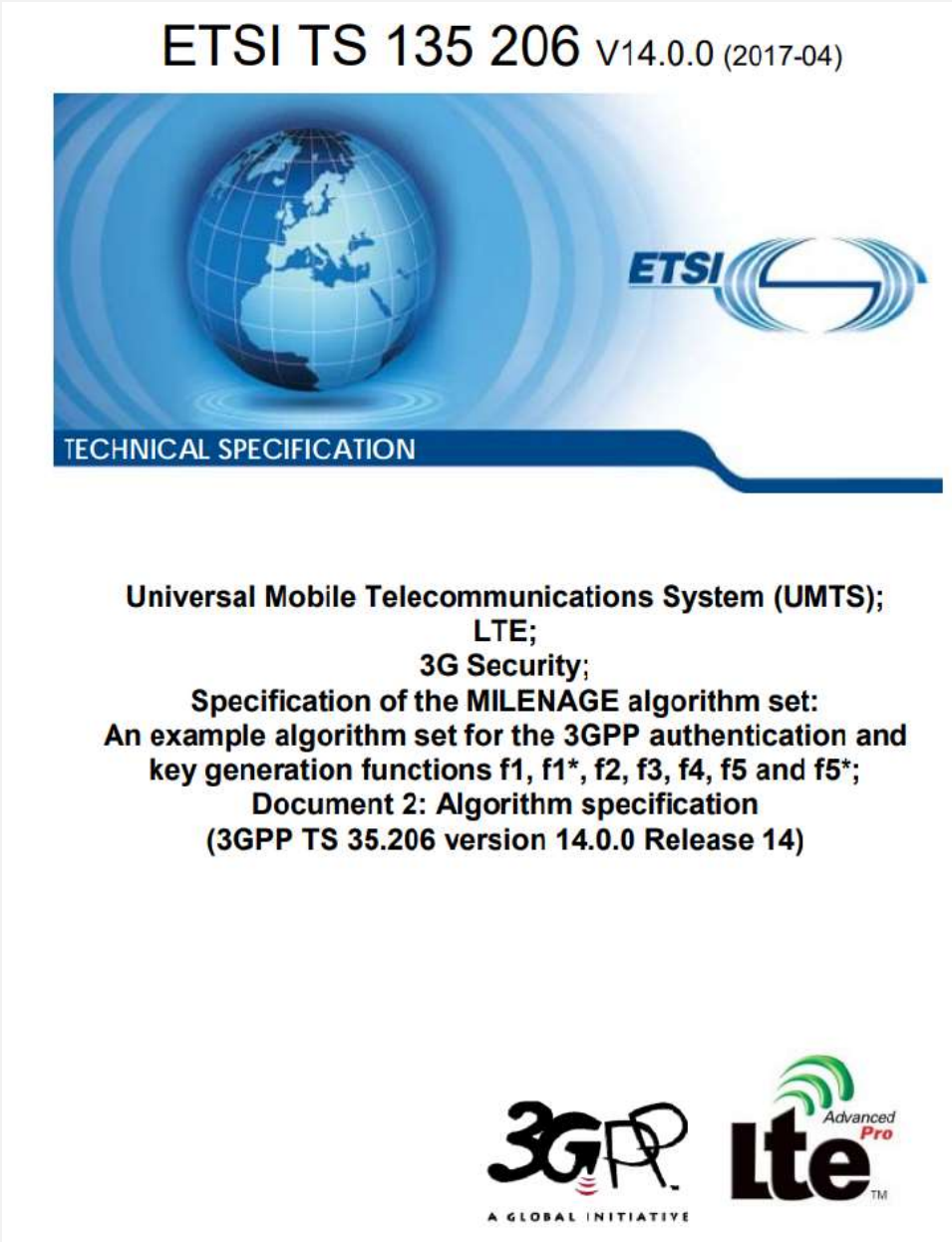
The debate of cryptography reached strange heights. Export of the cryptography violated US law. But discussion of the algorithm was arguably protected by the First Amendment. Thus, in order to get the code out of the country, instead of trying to move it as software, cryptography might print the code in a book and carry the book out. The government indicated that the code in the form of a book did not need an export license whereas the same code "in machine readable form" on a computer disc would. This ultimately led to T-Shirts with Phil Zimmerman's PGP code printed on them (including bar codes that made the shirts machine readable). The shirts were available to US citizens from a US address and the rest of the world from a UK address. The speaker proclaimed

> Along with the sale pitch ("Now you, too, can become an international arms dealer for the price of a T-shirt") come warnings that if a non-U.S. citizen sees you wearing the shirt you may be classified as a criminal. (If you wear it inside-out, is it a concealed weapon?) If you are arrested, the promoters will refund the purchase price of the shirt.

Agenda

- ORAN Security
- **Telecommunication Crypto 101**
- Quantum Computing → Crypto
- Results for Milenage (crypto backbone of TelCo world)
- Implications for 6G

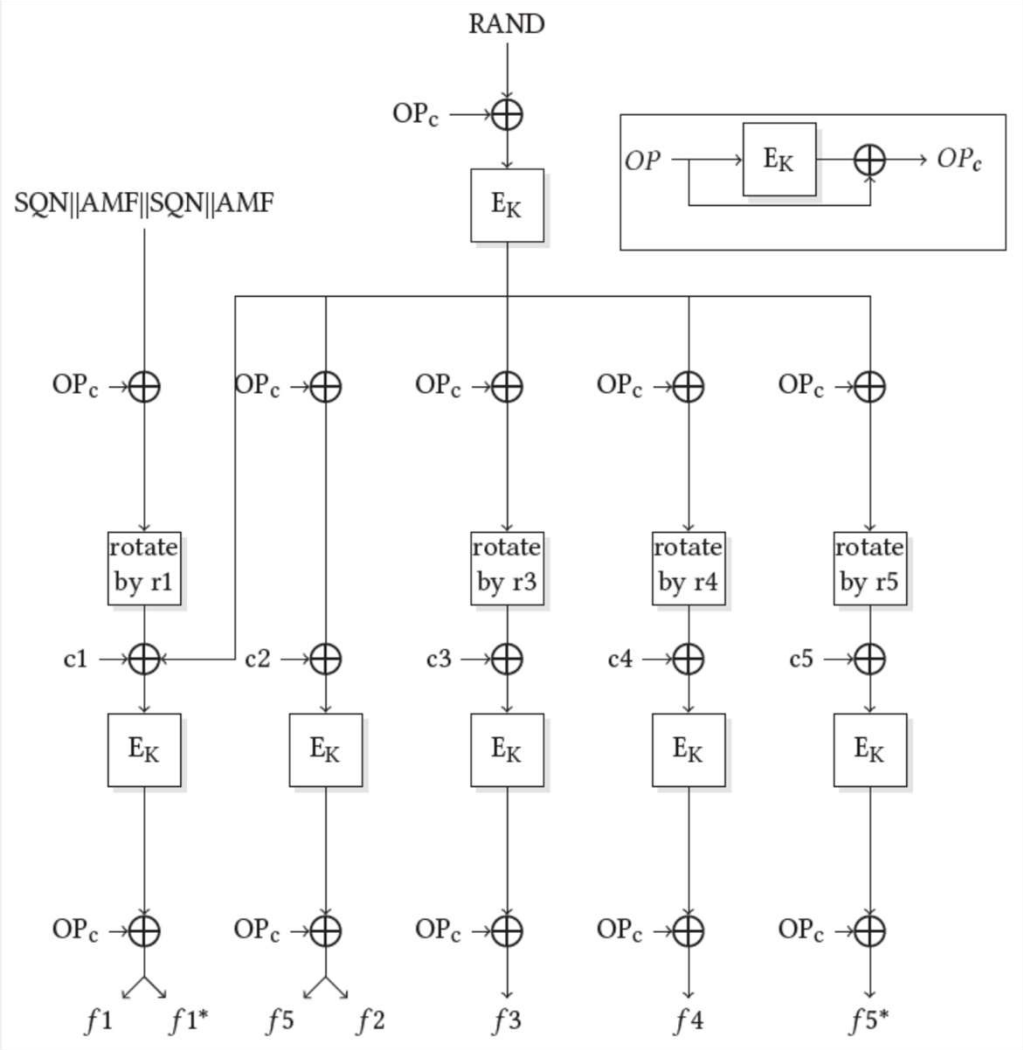
Crypto of cellular world is defined by ETSI and 3GPP standardization bodies:



The entire cryptography of contemporary cellular networks is centered around seven secret-key algorithms

$$f_1, \ldots, f_5, f_1^*, f_5^*,$$

aggregated into a single "Authentication and Key Agreement" known as AKA algorithm set.



<u>Known result:</u> The algorithms $f_1, \ldots, f_5, f_1^*, f_5^*$, of the AKA set are provably secure by all means in the classical (i.e., non-quantum) world, …

BUT it is envisioned that 6G

„… cannot be broken even by quantum computers of arbitrary complexity.”

6G Technology | DOI:10.1145/3512996

On 6G and Trustworthiness

BY GERHARD P. FETTWEIS AND HOLGER BOCHE

THE FIRST TWO generations of cellular—1G/2G—enabled ubiquitous voice connectivity. 3G/4G enabled broadband Internet. Even generations introduced services for business customers, and odd generations democratized them for consumers. 5G is enabling network-controlled robotics and XR, the Tactile Internet for business verticals,[1] and 5G will democratize this for consumers. One main avenue for achieving this is cost reduction.[6] Another avenue is radio access with joint communications and sensing.[7] New services are envisioned, such as low-altitude air traffic control, detecting, for example, bird migration and adapting drone services accordingly.

Not only data but physical and virtual objects will be controlled with 6G. This requires addressing *trustworthiness* of the system and its services at an unprecedented level. Indeed, trustworthiness must be understood in a new context, as we envision:

- Localization of unheard precision,
- Sensing—not only radio and camera sensing, and
- Gesture recognition—also emotions.

How can we provide these new qualities without compromising legal and societal requirements, for example, General Data Protection Regulation (GDPR)? Every opportunity of improving sensing is an opportunity for *spying*. Trustworthiness for 6G is key. It comprises:

- Privacy
- Security
- Integrity
- Resilience
- Reliability
- Availability
- Accountability
- Authenticity
- Device independence

Every opportunity of improving sensing is an opportunity for spying. Trustworthiness for 6G is key.

The trustworthiness of 6G technology has crucial implication. The University of Oulu in Finland recently acquired a self-driving car from Toyota to be used as a piece of research equipment where researchers can install their own instruments for testing.

Mathematical Frameworks

For communication tasks beyond Shannon's theory for message transmission, like event-driven-communication, transmission of status states, and joint communication and sensing, we must develop a Post-Shannon information theory. Several Post-Shannon transmission and storage schemes achieve exponential gains compared to the Shannon and Turing approaches.[7,8] Besides, initial Post-Shannon transmission methods allow a secure transmission of information, which cannot be broken even by quantum computers of arbitrary complexity. One important feature of 6G is resilience by design. This is particularly interesting since the successful execution of jamming attacks by an attacker cannot be detected by Turing machines.[9]

However, we must not only design systems that are robust against attacks from the outside, but also from within. Many cryptographic tasks have emerged in the last decade. Important examples are oblivious transfer, secure computing, bit commitment, and information masking. These tasks involve two or more untrusted parties with different types of behavior.[5] Some of the parties may be dishonest or even jam the communication system. It is well known that oblivious transfer is the most

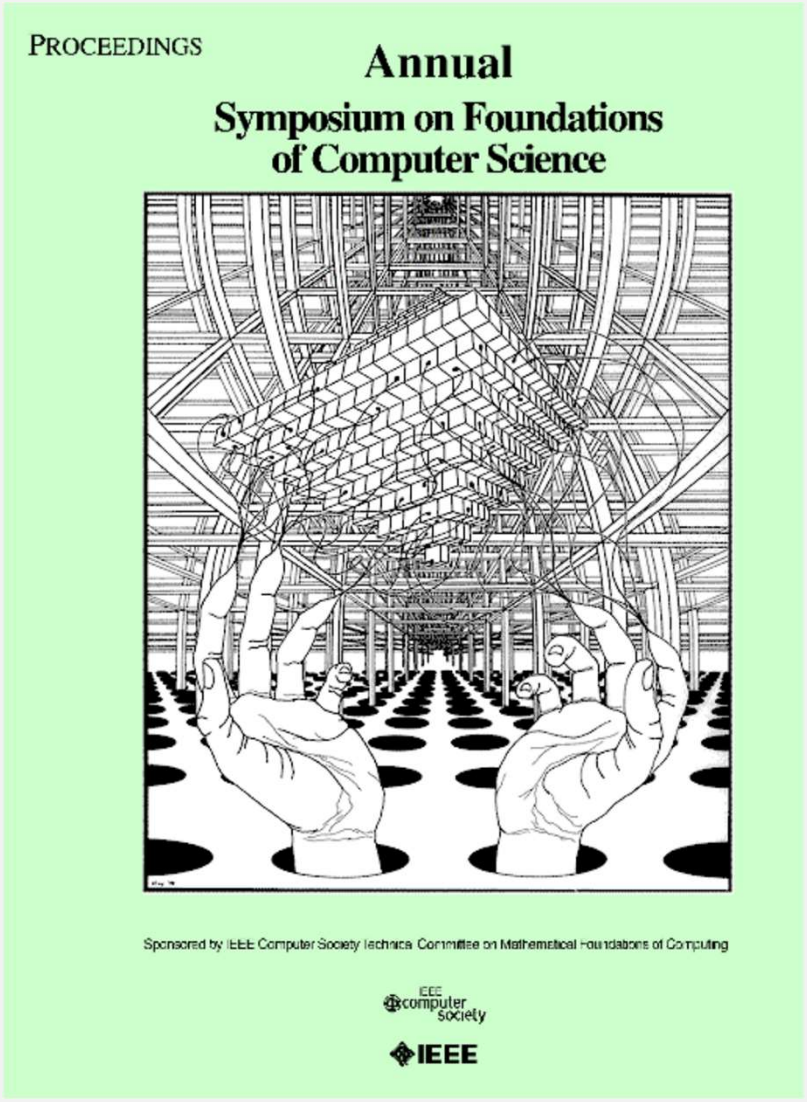
48 COMMUNICATIONS OF THE ACM | APRIL 2022 VOL. 65 | NO. 4

Agenda

- ORAN Security
- Telecommunication Crypto 101
- **Quantum Computing $\rightarrow$ Crypto**
- Results for Milenage (crypto backbone of TelCo world)
- Implications for 6G

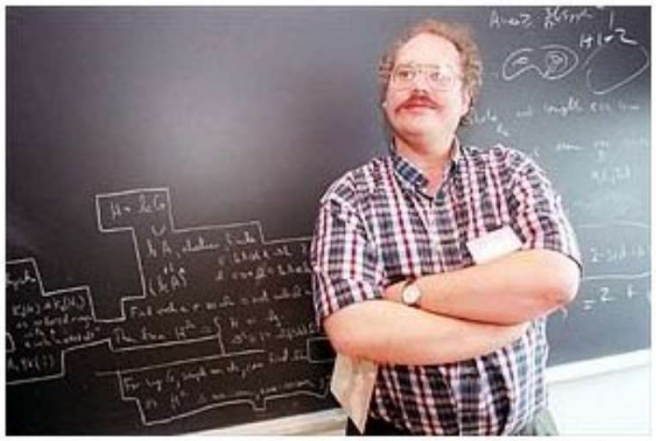
Why Quantum Computing → Crypto ???

1994: Shor´s factorization algorithm



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

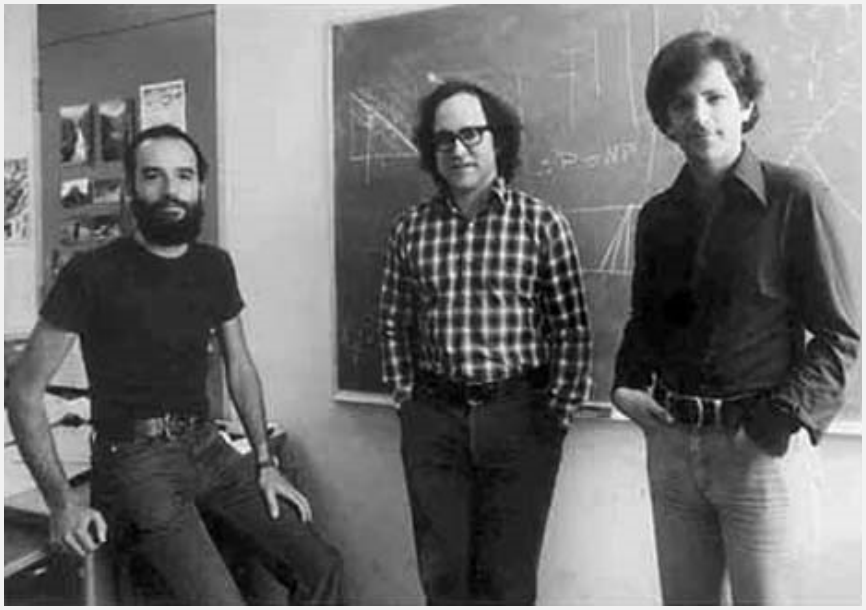
Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

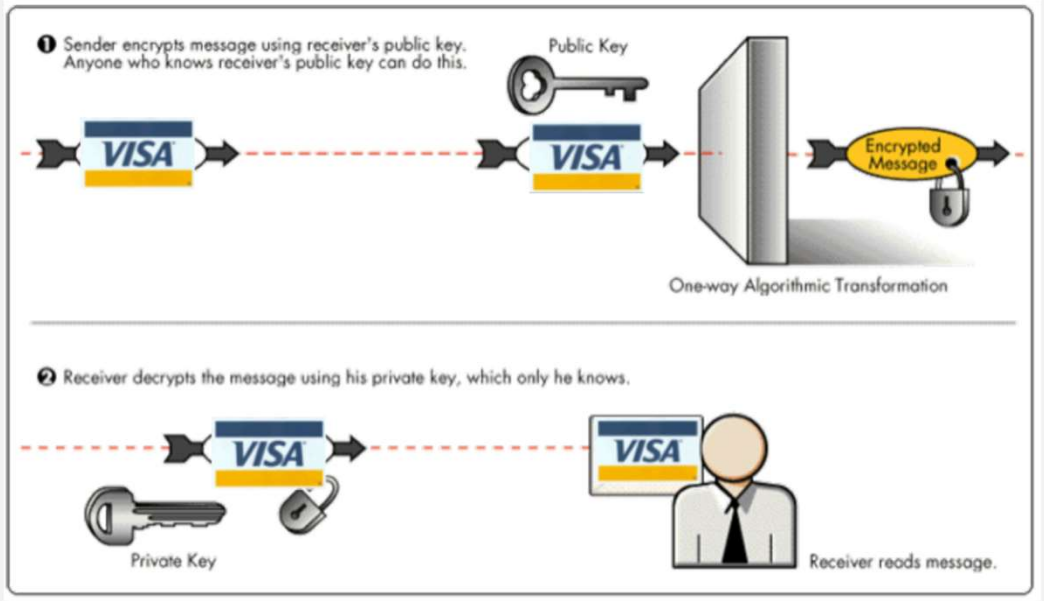


Susan Spann for The New York Times

Dr. Peter Shor, a researcher with AT&T and a pioneer in quantum computing, sees the field's potential in areas like cracking codes.

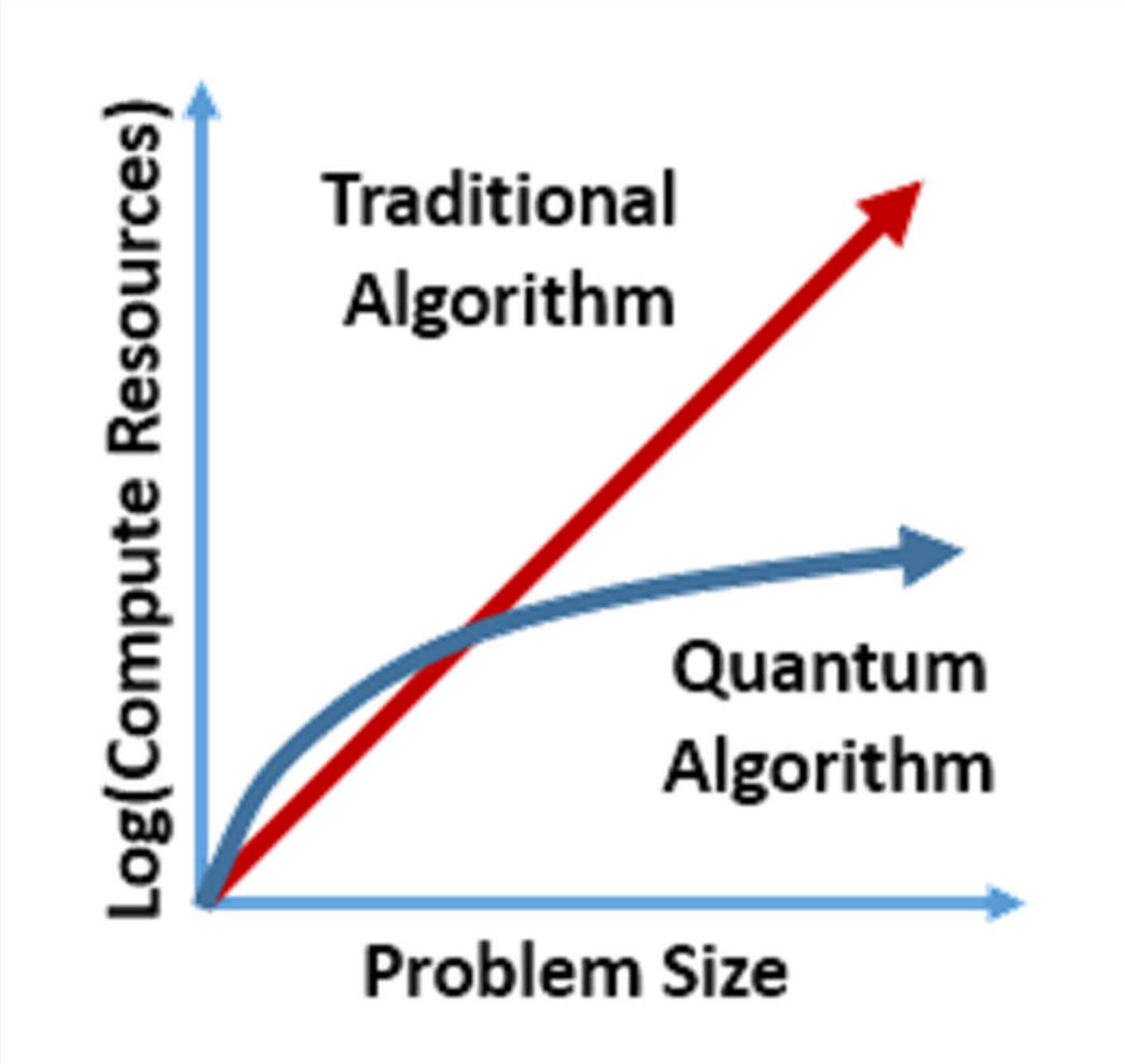
Rivest, Shamir, Adleman – The RSA PK Encryption/Signature system





- **The RSA scheme (due to Rivest, Shamir and Adleman) is the current de-facto standard (ANSI X9.62, etc.) for Public Key Encryption and protects almost all of our *entire digital life* in various forms & govt. secrets.**

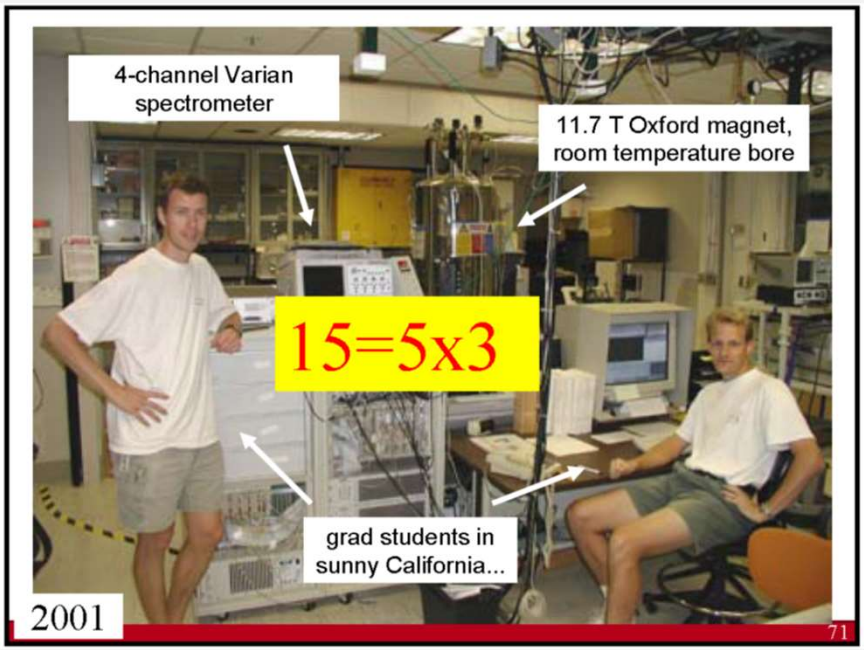
Summary of Shor´s paper wrt. security of RSA



Anticipated timeline of QCs

Michele Mosca
[Oxford 1996]:

"20 qubits in 20 years"



NIST
[NIST April 2015, ISACA September 2015]:

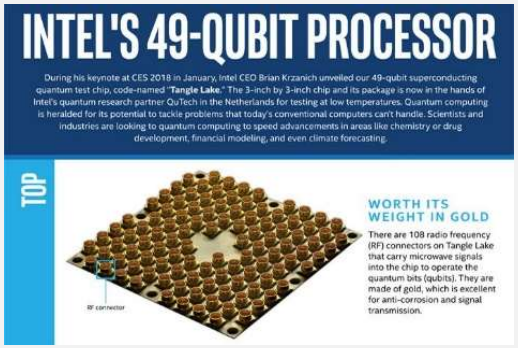
"1/7 chance of breaking RSA-2048 by 2026,
½ chance by 2031"

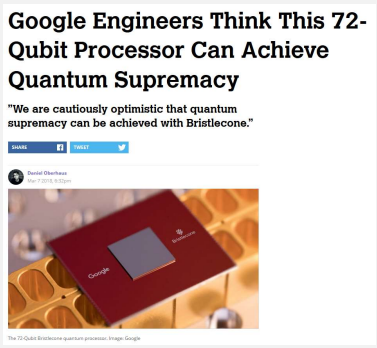
Implications for ETSI = MILENAGE = AKA?

Remember:?

The entire cryptography of contemporary cellular networks is centered on secret-key algorithms = AKA set and not at all solvable by Shor's QC algorithm.

Is ETSI lucky?





Hard research question:

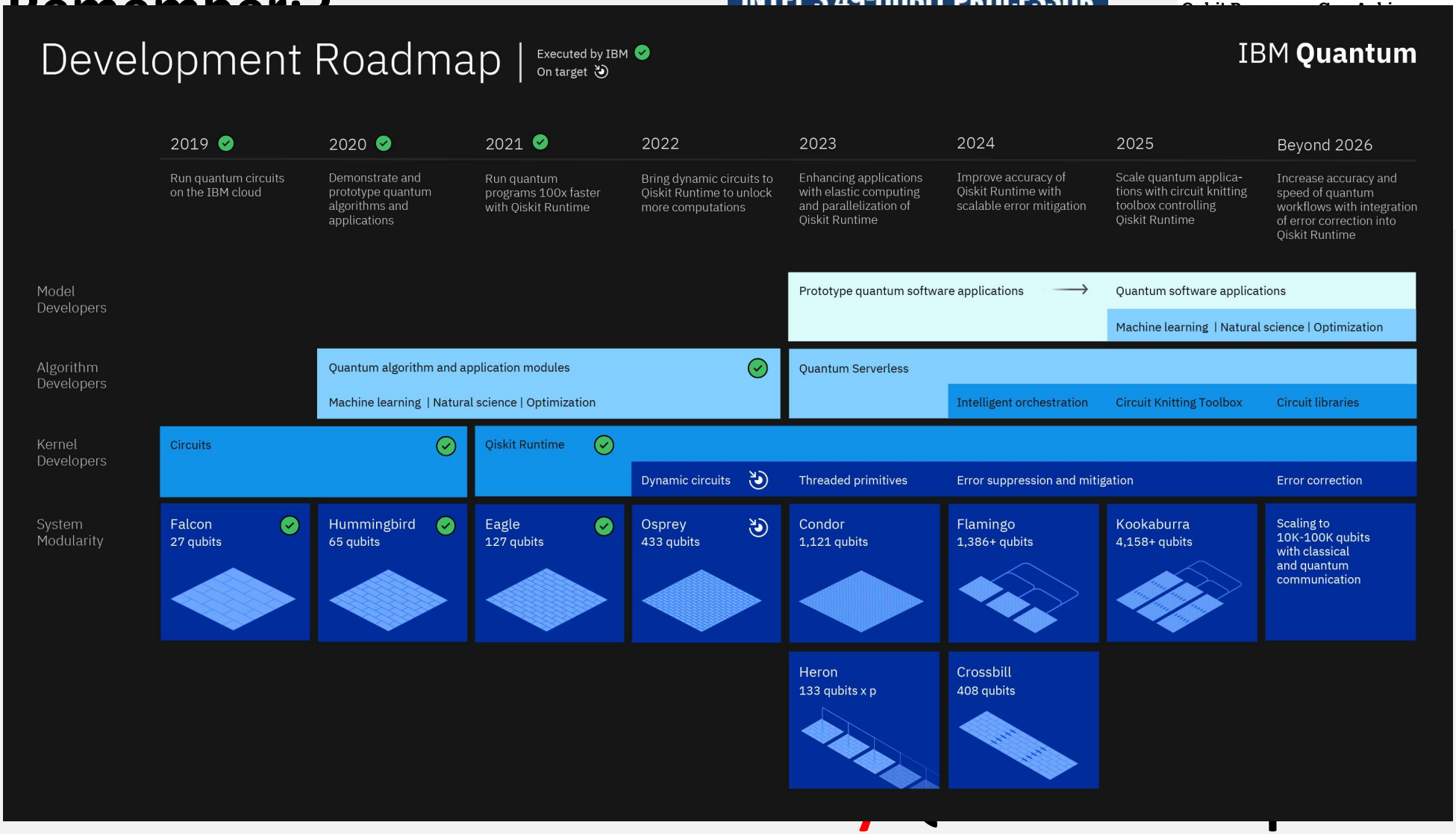
- Are existing, but small & noisy Quantum Computers a threat for ETSI?

Implications for ETSI = MILENAGE = AKA?

Remember?

INTEL'S 49-QUBIT PROCESSOR

Google Engineers Think This 72-



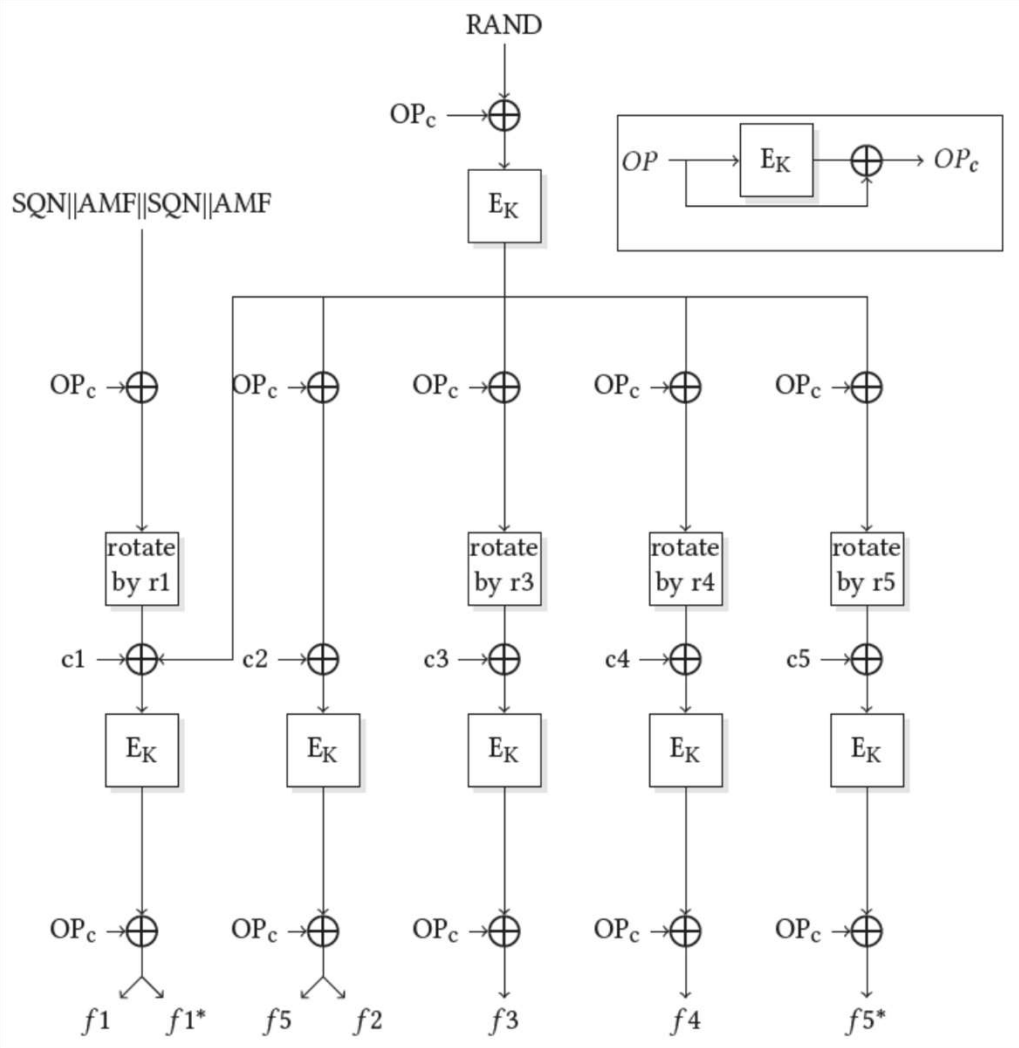
Is ETSI lucky?

a threat for ETSI?

Agenda

- ORAN Security
- Telecommunication Crypto 101
- Quantum Computing → Crypto
- **Results for Milenage (crypto backbone of TelCo world)**
- Implications for 6G

Quantum Cryptanalysis of Milenage = $f_1, \ldots, f_5, f_1^*, f_5^*,$



E_K = AES,

AES = Advanced Encryption Standard

Results of our Quantum Cryptanalysis of Milenage

Breaking the quadratic barrier:
Quantum cryptanalysis of Milenage,
telecommunications' cryptographic backbone

Attack	Model	Classical Queries	Quantum Queries	Complexity	OP Known?	Best Known Classical Attack	Description
Grover's attack for key recovery, OP known	Q_1	$O(1)$	0	$O\left(2^{\lvert K\rvert/2}\right)$	Yes	$O\left(2^{\lvert K\rvert}\right)$	Sec. 4.1
Grover's attack for key recovery, OP unknown	Q_1	$O(1)$	0	$O\left(2^{(\lvert K\rvert+\lvert OP_c\rvert)/2}\right)$	No	$O\left(2^{\lvert K\rvert+\lvert OP_c\rvert}\right)$	Sec. 4.1
Key Recovery f_2, OP unknown	Q_2	0	$O(\lvert M\rvert)$	$O\left(\lvert M\rvert^3 \cdot 2^{\lvert K\rvert/2}\right)$	No	$O\left(2^{\lvert K\rvert+\lvert OP_c\rvert}\right)$	Sec. 4.2
Offline Key Recovery f_2, OP unknown	Q_1	$O\left(2^{\lvert M\rvert}\right)$	0	$O^*\left(2^{\lvert M\rvert} + 2^{\lvert K\rvert/2}\right)$	No	$O\left(2^{\lvert K\rvert+\lvert OP_c\rvert}\right)$	Sec. 4.2
Existential Forgery f_1	Q_2	$O(1)$	$O(\lvert M\rvert)$	$O\left(\lvert M\rvert^3\right)$	No	$O\left(2^{\lvert M\rvert/2}\right)$	Sec. 4.3
Related Key Attack $f_1, \ldots, f_5$	Q_2	0	$O(\lvert K\rvert)$	$O\left(\lvert K\rvert^3\right)$	No	$O\left(2^{\frac{\lvert K\rvert+\lvert OP_c\rvert}{2}}\right)$	Sec. 4.4
Offline Related Key Attack $f_1, \ldots, f_5$	Q_1	$O\left(2^{\lvert K\rvert/3}\right)$	0	$O^*\left(2^{\lvert K\rvert/3}\right)$	No	$O\left(2^{\frac{\lvert K\rvert+\lvert OP_c\rvert}{2}}\right)$	Sec. 4.4

Table 1: Summary of the results. $|K|$ is the length of the message authentication key, $|OP_C|$ is the length of the OP_c bitstring and $|M|$ is the block length of the underlying block cipher. In the case of Milenage, $|K| = |OP_C| = |M| = 128$. For all complexity estimates, the big-O notation hides only a very small multiplicative constant.

Agenda

- ORAN Security
- Telecommunication Crypto 101
- Quantum Computing $\rightarrow$ Crypto
- Results for Milenage (crypto backbone of TelCo world)
- **Implications for 6G**

Summary

- Our attacks require only a very small number of qubits (256 + ε) contrary to algorithms breaking RSA, highlighting the imminent danger of the quantum threat towards Milenage.
- The security of symmetric key cryptography against quantum adversaries is not ensured by doubling the key size, contrary to popular belief.
- We gave strong evidence against choosing Milenage as the cryptographic cipher underpinning the security of quantum resistant telecommunication networks.
- What security guarantees suffice and what kind of quantum adversary models should be used in quantum security considerations for cellular 6G networks?

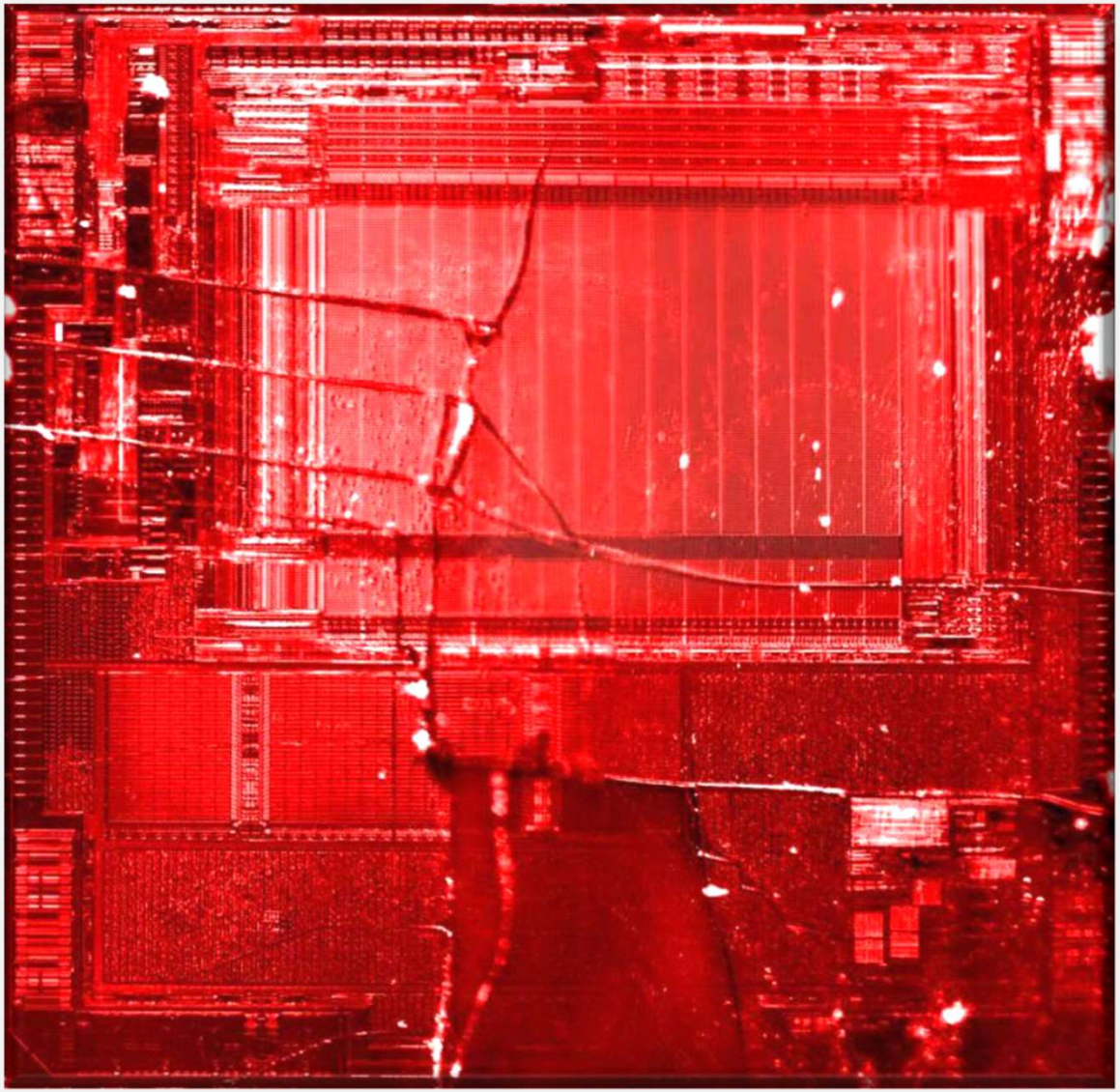
Thank you for your attention!

This work has been supported by:

DFG Deutsche Forschungsgemeinschaft

EINSTEIN Foundation.de

Questions?



EINSTEIN Foundation.de

Backup

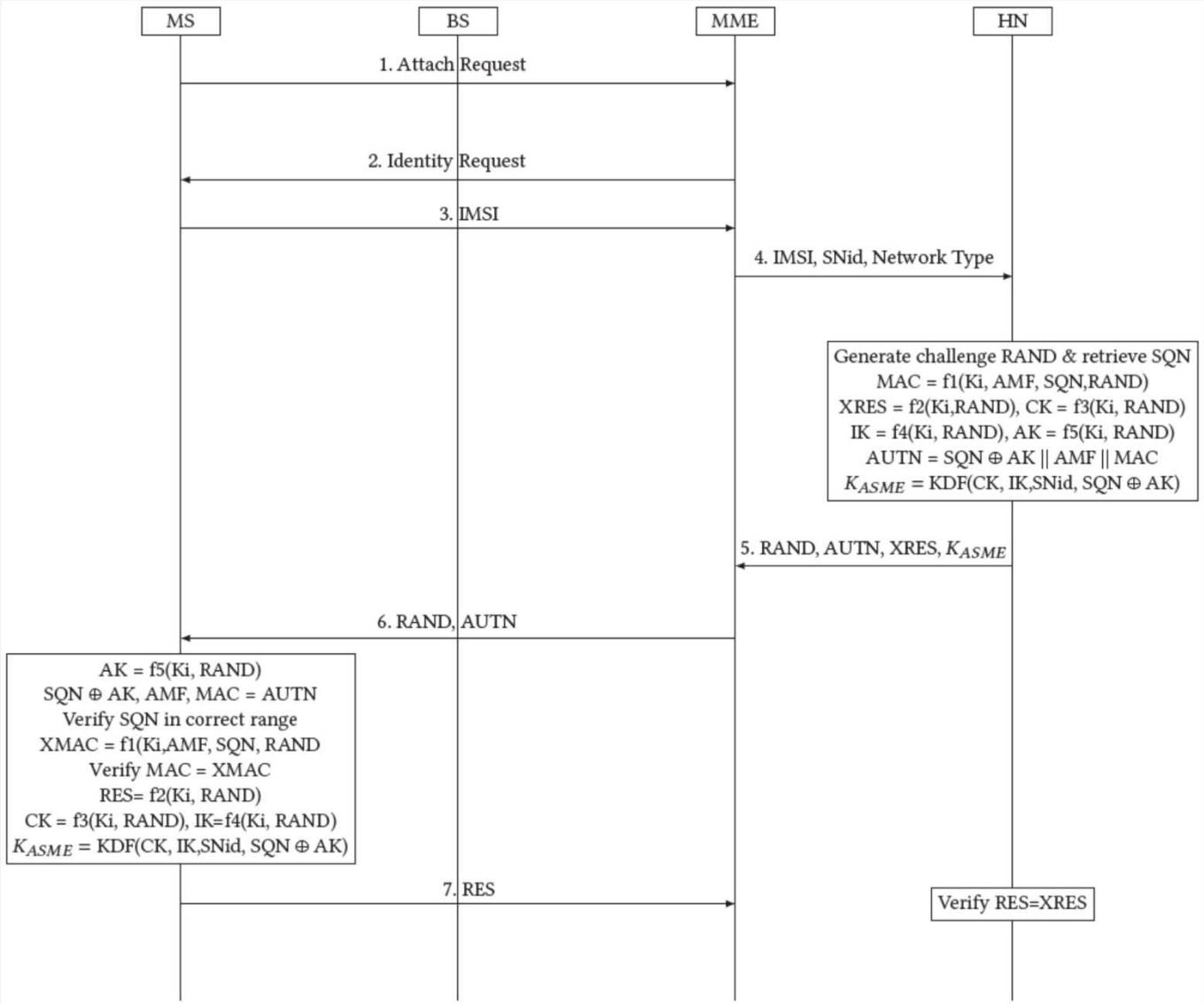


Figure 3: The AKA protocol as used in Long-Term Evolution (LTE). The user's device, referred to as Mobile Station (MS), communicates with the Base Station (BS) to authenticate towards the network. The BS forwards the request to the Mobility Management Entity (MME), which in turn forwards it to the Home Network (HN). The home network uses the function $f1, \ldots, f5$ to calculate session information and secret key material and forwards the necessary information back to the MME.

Disaggregation & Digital Twinning

HEIKO LEHMANN | Deutsche Telekom
Senior Expert Machine Learning

Disaggregate Networks & Digital Twinning

i14y summit | H. Lehmann | Berlin | June 9th, 2022

LIFE IS FOR SHARING.

Agenda

The promise of
Digital Twins.

What may we ask the
Digital Twin?

What do we need to do for
it to answer sensibly?

In Disaggregate Network
context, which building
blocks can we start with?

... the solution to (nearly)
all the problems of design
& development in complex
settings,

or,

... a trendy, ill-defined
term which is prone to
create illusions.

Digital Twin – Definitory Problems

Wikipedia says: A **digital twin** is a virtual representation that serves as the real-time digital counterpart of a physical object or process.

- But, virtual representation of what?

- shape → 3D model
- dynamical properties (short time scale) → mass density, material, joints, heat transport, molecular structure
- dynamical properties (long time scale) → aging, material fatigue, chemical reactions, inhomogeneity forming

Conclusion: true virtual twinning is an illusion. It takes clean scoping to devise useful tools.

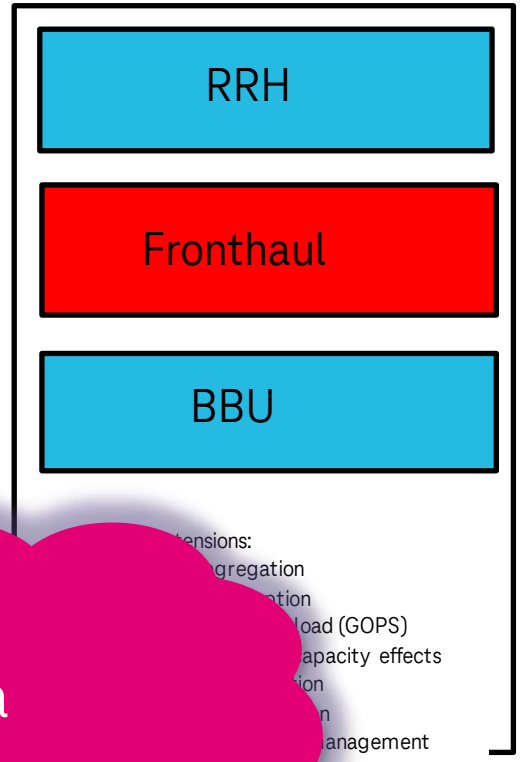
Digital Twin in Telco - System Scale Evaluation

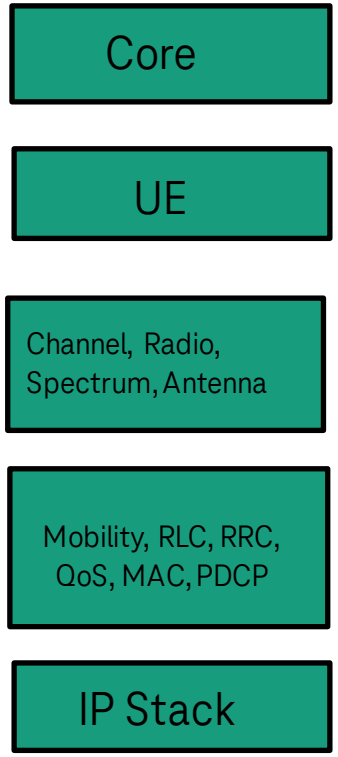
i14y LAB

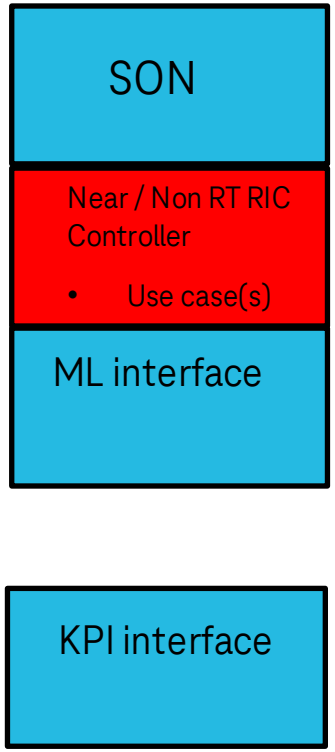
Interoperability: Functional testing in a lab set-up.

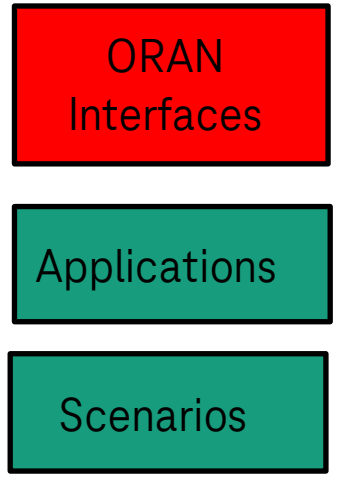
Digital Twin to complementally evaluate sys

But is it really a Digital Twin?









Already there (green), extension required (blue), not there (red)

Scope Discussion

abstraction

	physics, topology		architecture
modelling need	· electromagnetic wave propagation for different channels · fine-grained topology modelling (surfaces, scattering etc.)	Basic Question: What is the Network Twin basically for?	· ORAN interfaces · disaggregation specifics · binding in of RIC / SMO and SW residing there (apps)
data need	· 3D digital maps · antenna / radio specifics		· ORAN specs · x/rApps IO · cell-wise KPIs
questions	· customer-centric planning tool · optimal positioning and configuration of radio resources		· optimal ORAN configuration · systemic App behaviour · virtualization effects · overall efficiency (e.g. energy consumption)

Scope Discussion

map vs. model

	static	dynamic
modelling need	· use DTw as true representation of the real world (meaning as true as feasibly possible)	· „equations of motion“: capture as precisely as possible the dynamics drivers in ORAN-flavoured campus networks · abstraction conventions
data need	· DTw as „HD“ snapshot of the real world: capture as much detail as possible · which will be a nuisance	· abstracted (according to convention) state data
questions	· data capture · data logistics	· with state of system at t_0 given, what is the system state at $t_0 + \Delta t$?

Basic Question: Do we want an indefinitely zoomable map of the real world as it is at a given time, or, do we want a simulation engine? If we want both, how do we combine the requirements?

Scope Discussion

capturing the dynamics

model

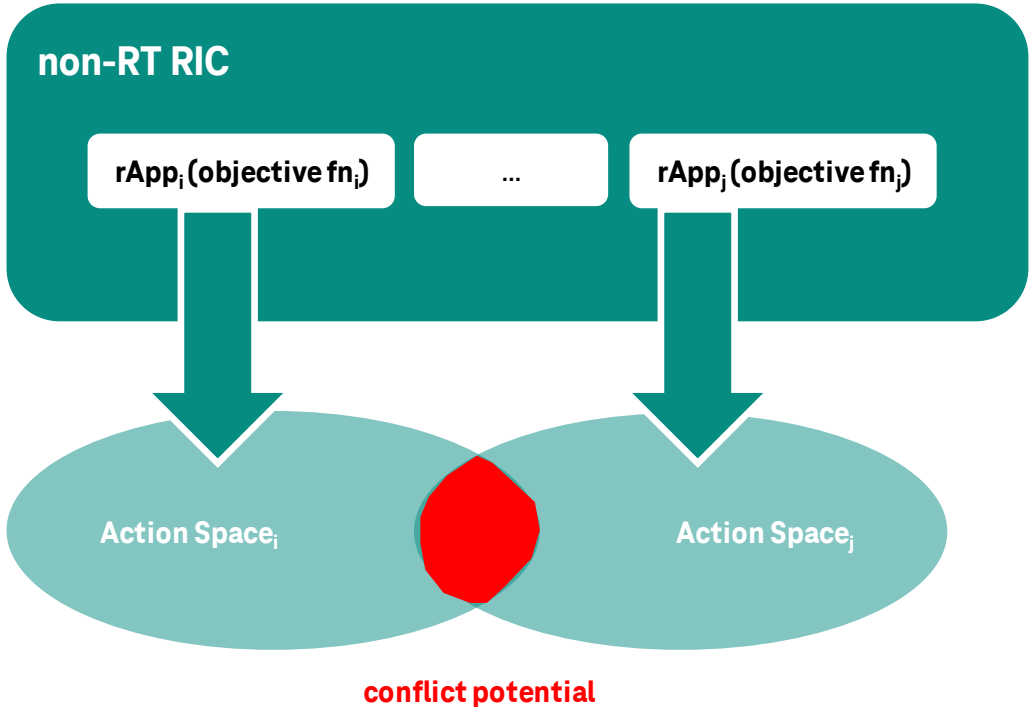
- “An exact formula is equivalent to an infinite amount of computing time.” N.H. March

Basic Dilemma: models may be bad, learning never exceeds the experience set.

learn

- mapping of sets which are always limited.

Utility Discussion: Logical Inconsistency



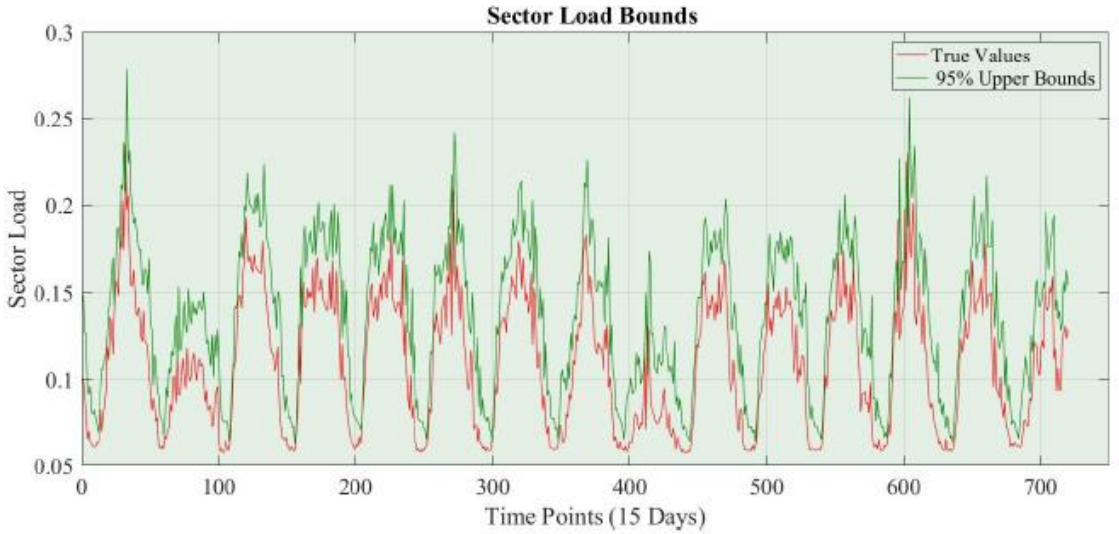
- Sometimes, the apparent simplicity of cleanly decoupled apps is misleading.
- Our approach:
- A system-scale Network Simulator and cutting edge ML to quantitatively evaluate conflicts,
- and suggest mediation strategies.
- Formula: ORAN specs + Causality Modelling + ns3

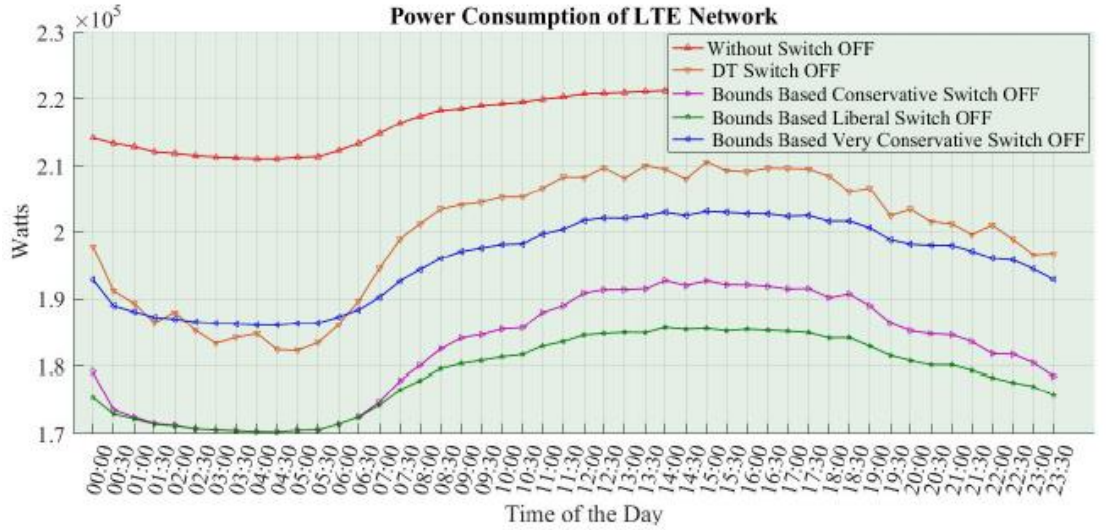
TELECOM INFRA PROJECT

i4y LAB

Utility Discussion: Optimization

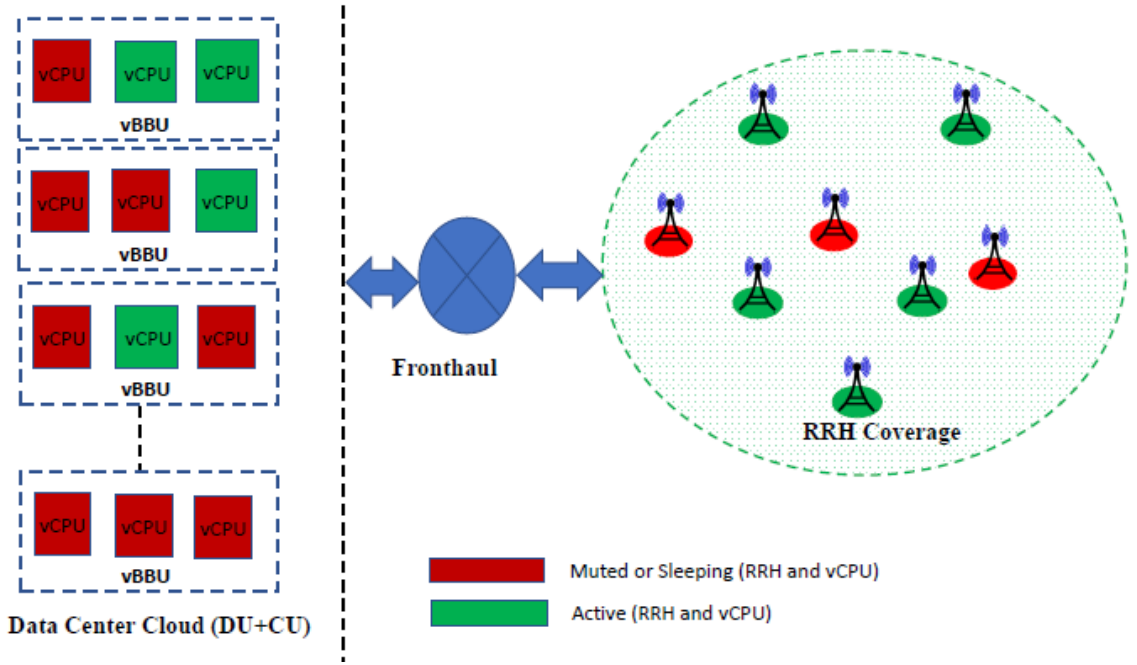
- Load-Adaptive Mode in RAN: We predict 'robust' upper bounds on cell-load in the network.
- **Statistical guarantees**: Optimization based on these upper bounds is unlikely to result in violation of network QoS.
- **Global Optimization**: Switch OFF cells that
  1. show low expected cell-load locally (existing method),
  2. minimize global network power consumption (our extension).
- **Robustness**: Ensure QoS –
  1. switch ON cells if there is a sudden increase in network load (existing method),
  2. keep such oscillations to a minimum (our method).





Utility Discussion: Optimization

- While the *ms* time scale is the one where stable and robust operation is secured,
- the non-RT scale is where network efficiency and systemic optimisation are decided:
  - non-local effects for overarching optimisation (as seen in the power save case)
  - proactive control (forecasts are non-locality in time)
  - possibly, an instance for conflict mediation (to be addressed in nonRT RIC / SMO conext)



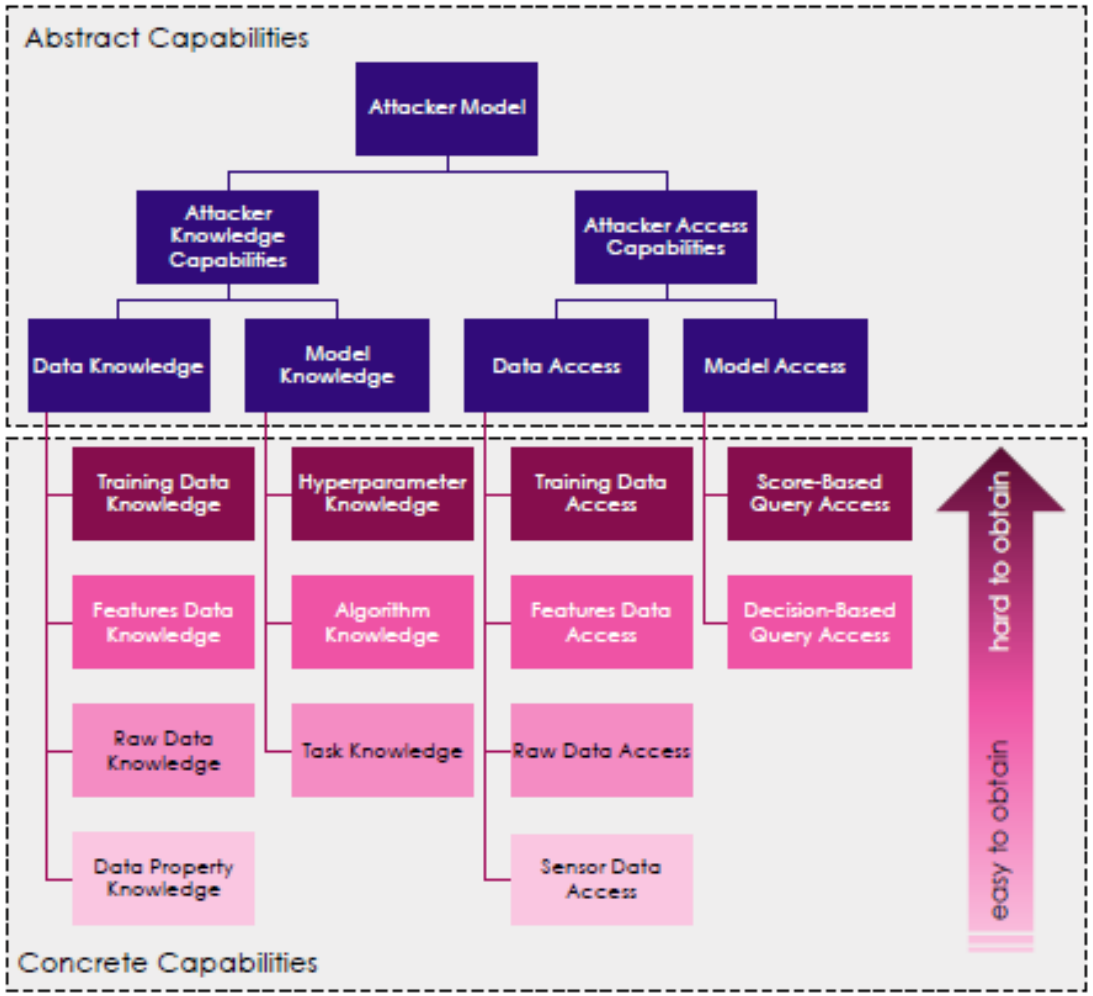
$$P(\rho(x)) \rightarrow P_{RRH}(x_{traffic}) + P_{BBU}(x_{cloud})$$

single RAN, locally optimizable

spatial distribution of actual traffic

distribution of compute activity

Utility Discussion: Security



Threat Actor	Compromised Component	DC	Attacker Capabilities			
			Data Knowledge	Model Knowledge	Data Access	Model Access
O-RAN Software Application Developer	Data Collection	All	Raw Data		Raw Data	
	Data Host		Features Data		Features Data	
	Training Host		Training Data	Hyperparameter	Training Data	
	Serving Host		Features Data	Hyperparameter	Features Data	Score
	ML APP			Task		Score
O-RAN Software Infrastructure Developer	Non Real Time RIC	1	Training Data	Hyperparameter	Training Data	Score
		2	Training Data	Hyperparameter	Training Data	
		3				
		4	Training Data	Hyperparameter	Training Data	
		5				
	Near Real Time RIC	1	Features Data		Features Data	Score
		2	Features Data	Hyperparameter	Features Data	Score
		3	Training Data	Hyperparameter	Training Data	Score
		4				
		5				
	O-CU O-DU	1	Raw Data		Raw Data	
		2	Raw Data		Raw Data	
		3	Raw Data		Raw Data	
		4	Features Data	Hyperparameter	Features Data	Score
		5	Training Data	Hyperparameter	Training Data	Score
Containerization Software Infrastructure Provider	All	All	Training Data	Hyperparameter	Training Data	Score
Hardware Infrastructure Provider	All	All	Training Data	Hyperparameter	Training Data	Score
User Equipment	All	All	Raw Data	Task	Sensor Data	Decision

Utility Discussion: Security

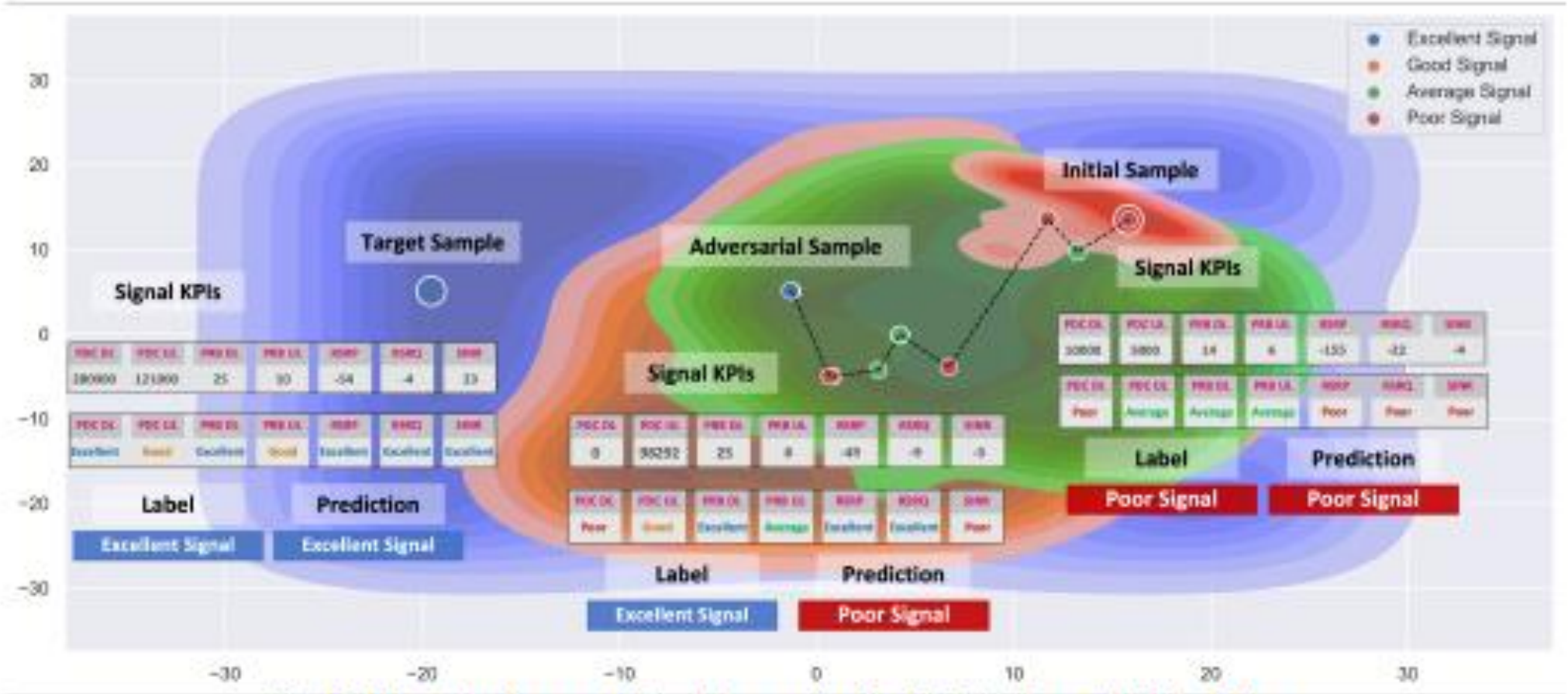


Fig. 14: Demonstrating an attack strategy using the HopSkipJump attack technique.

Digital Twin in CampusOS – Preliminary Conclusions

CampusOS Digital Twin (Suite)

Strive for a tool that helps to illustrate & configure customer offers:

- component catalogue reference
- reference architecture acknowledgment (real-world boundary conditions)
- configure to actual needs (nontrivial interplay of “map vs. model” and abstraction levels)
- selected problems of topology configuration and radio coverage
- avoid non-scalable tailor-made solutions
- …

Strive for a tool that has dynamic power:

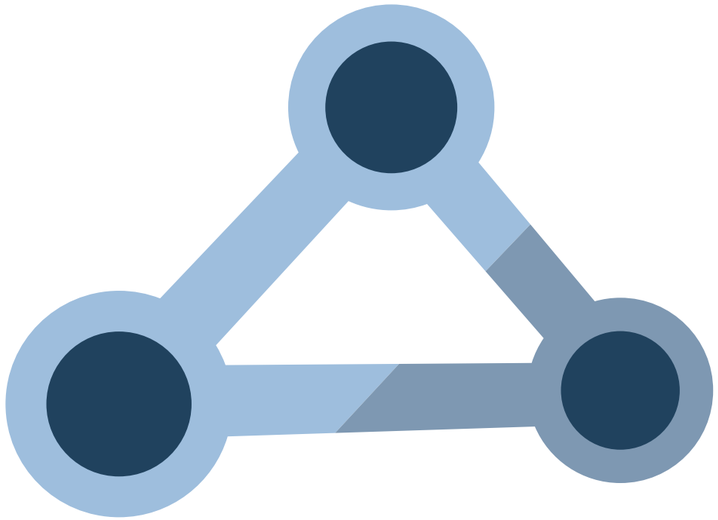
- scenario analysis for possible but unlikely load situations (virtual benchmarking)
- scenario analyses e.g. for energy optimization (configuration-wise and mode-wise, i.e. “static vs. dynamic”)
- interaction modelling “given world” ←→ campus network components
- catalogue of most relevant planning questions leads to modelling and mapping requirements
- …

- If and when we have done all this in a rigid way, we will have:
  - defined modelling depth
  - defined interfaces, splits, abstractions
  - defined coarse-graining levels of topology modelling

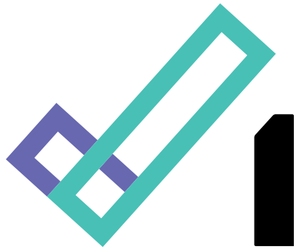
thx

Automated network configuration with gitlab-ci in the i14y Lab

JAN KLARE | BISDN



BISDN



i4y LAB

Network config with GitLab CI/CD

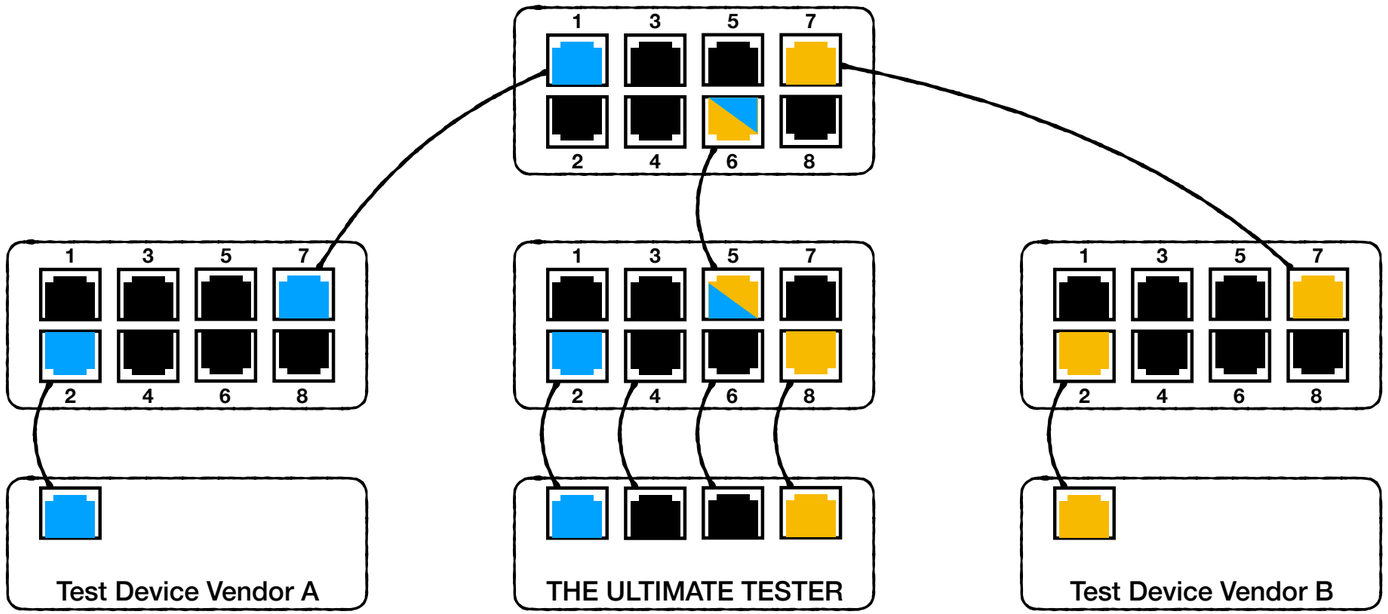
The next 25 minutes

- some network config
- the idea behind configuration as code
- how we combine those in the i14y-lab

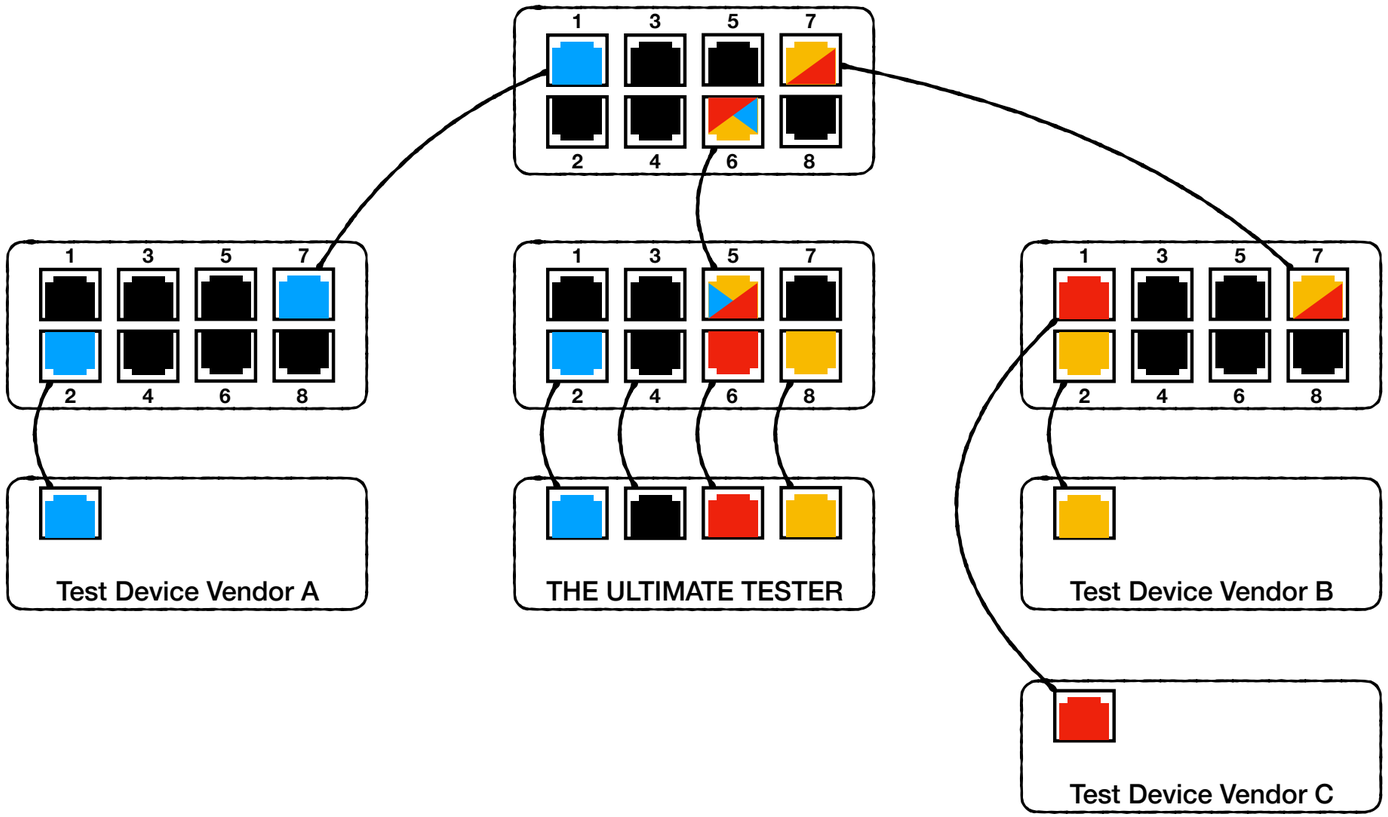
Which kind of config are we talking about?

- information which can't be:
  - calculated
  - learned
  - discovered

A simple example from the testing lab

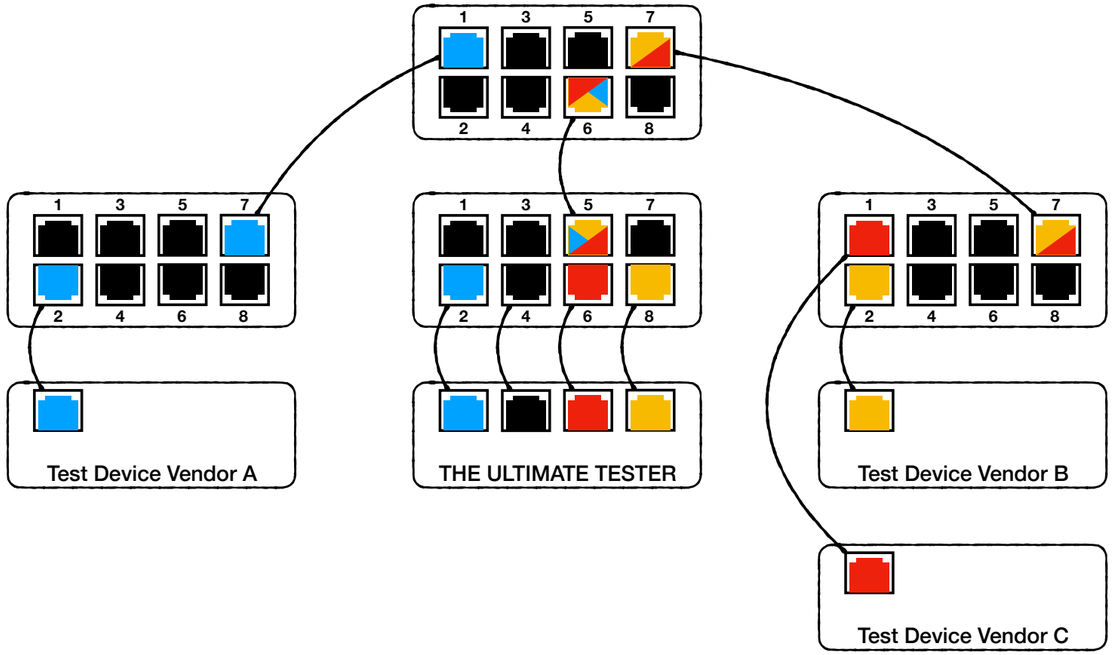


And then: PLUGFEST!



What's so difficult about that?

- one device added
- config changes on
  - 3 switches
  - 6 ports



"Nach dem Plugfest ist vor dem Plugfest"

— freely adapted from Sepp Herberger

But didn't SDN and THE CLOUD solve that?

- some config is always needed
- the tooling changed
- network world opened up a bit

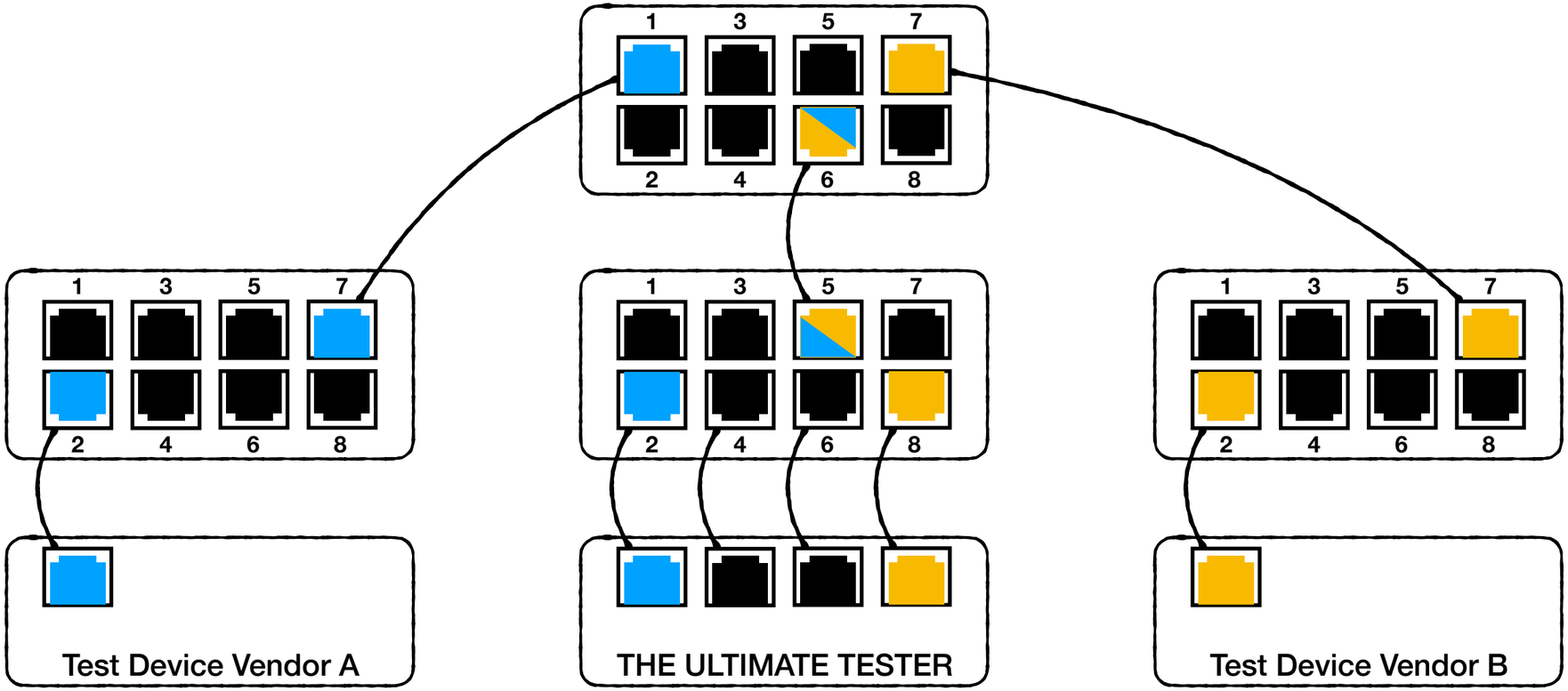
What is configuration as code?

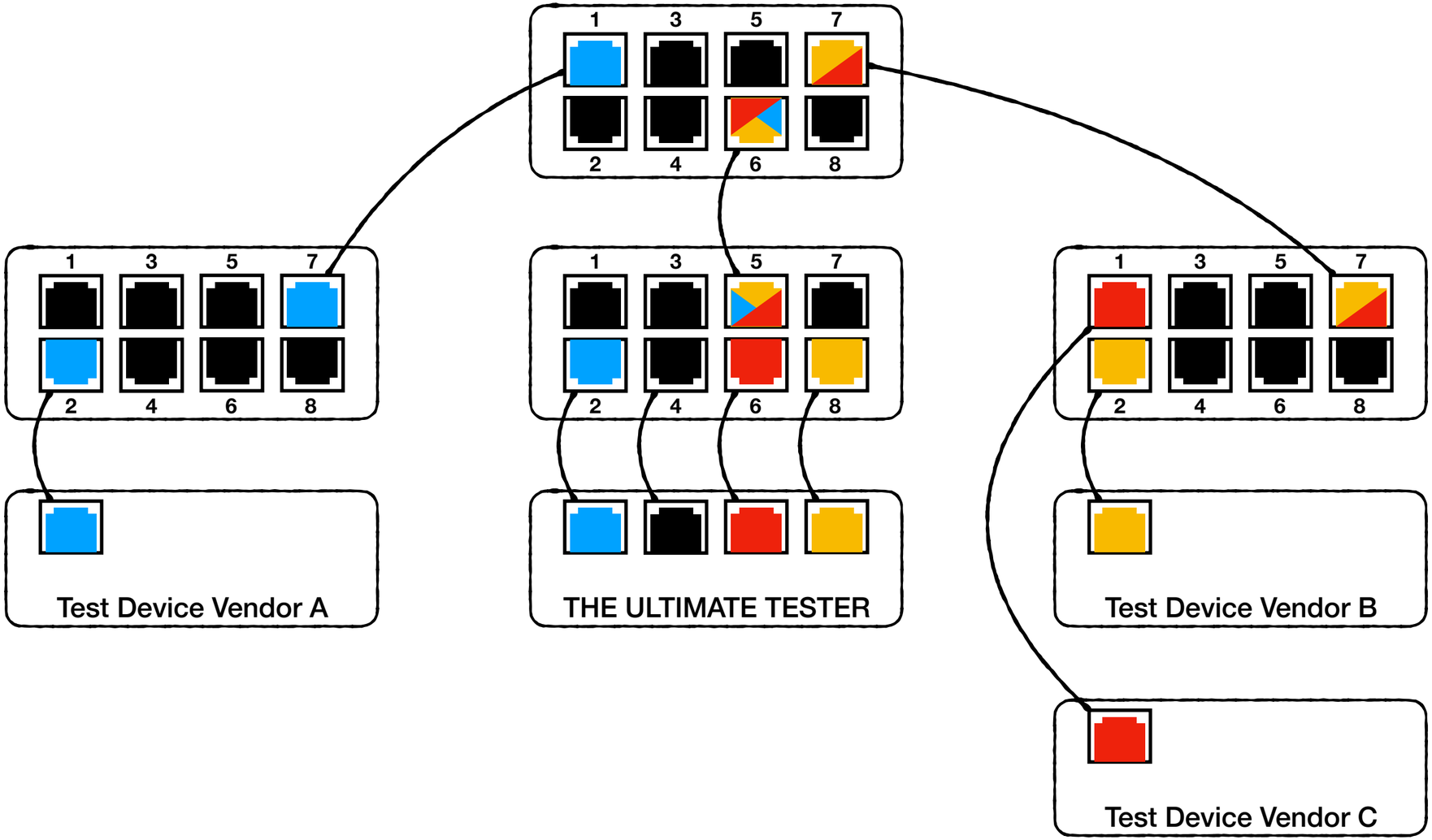
- config handled like source code
  - version controlled
  - reviewed and merged
  - automatically tested and deployed

How does this apply for networking?

- network config should:
  - allow for a rollback
  - always be reviewed before set
  - be tested and automatically applied

Back to our example


1 3 5 7
2 4 6 8
Test Device Vendor A
THE ULTIMATE TESTER
Test Device Vendor B

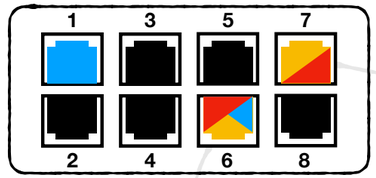

1 3 5 7
2 4 6 8
Test Device Vendor A
THE ULTIMATE TESTER
Test Device Vendor B
Test Device Vendor C

Config change 1

```
port1.network
   VLAN=blue

port6.network
    VLAN=yellow
    VLAN=blue
+   VLAN=red

port7.network
    VLAN=yellow
+   VLAN=red
```



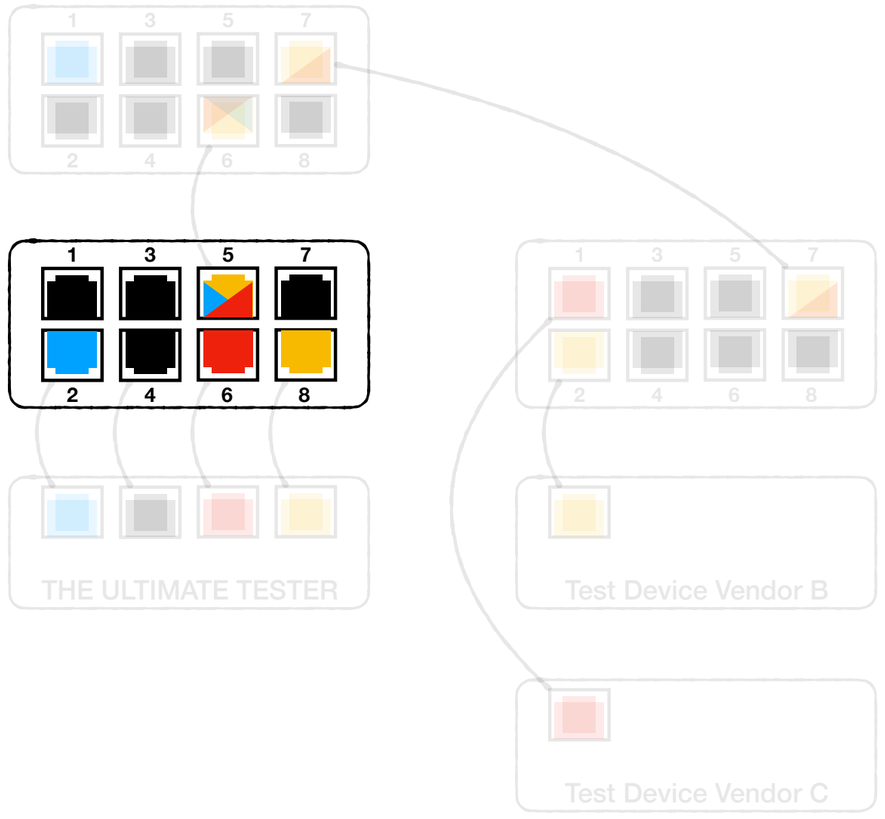
Config change 2

port2.network
VLAN=blue

port5.network
VLAN=yellow
VLAN=blue
+ VLAN=red

port6.network
+ VLAN=red

port7.network
VLAN=yellow

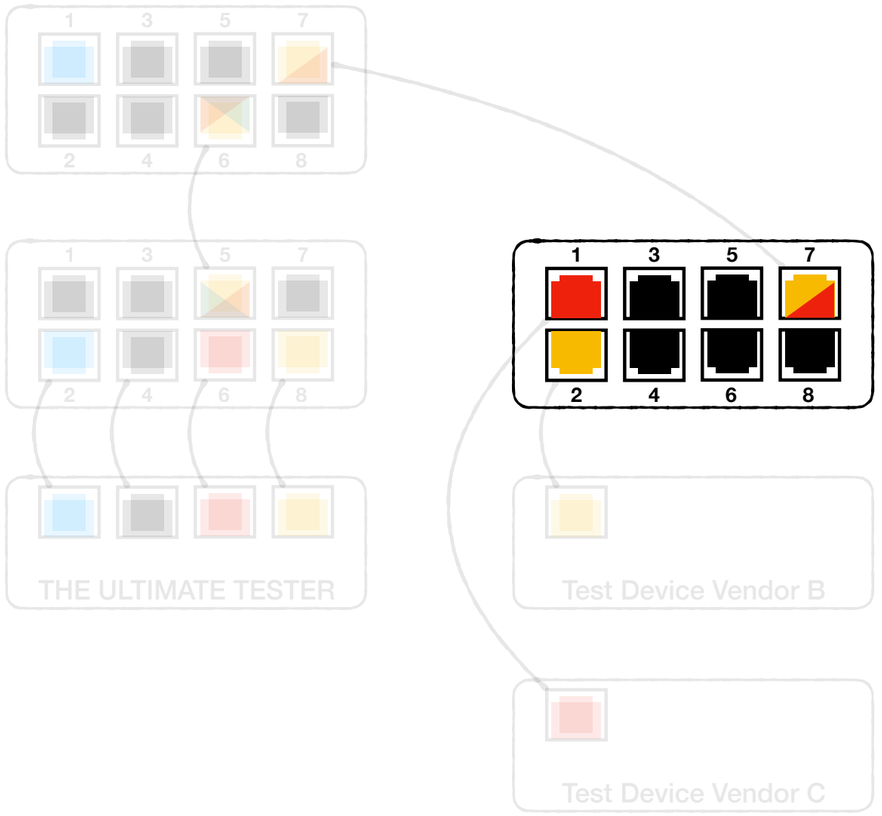


Config change 3

port1.network
+ VLAN=red

port2.network
VLAN=yellow

port7.network
VLAN=yellow
+ VLAN=red



How does this look in real life ?

- updated docs at netbox.i14y-lab.com
- new merge request in gitlab.i14y-lab.com
- automatic GitLab CI/CD pipeline to deploy

Summary

- some config is always needed
- configuration as code allows to version, review and test it
- GitLab CI/CD is a simple tool to automate the deployment

Onwards

- change the "blast radius"
- use some more sophisticated SDN
- onboard more resources

Questions ?

Thank You!