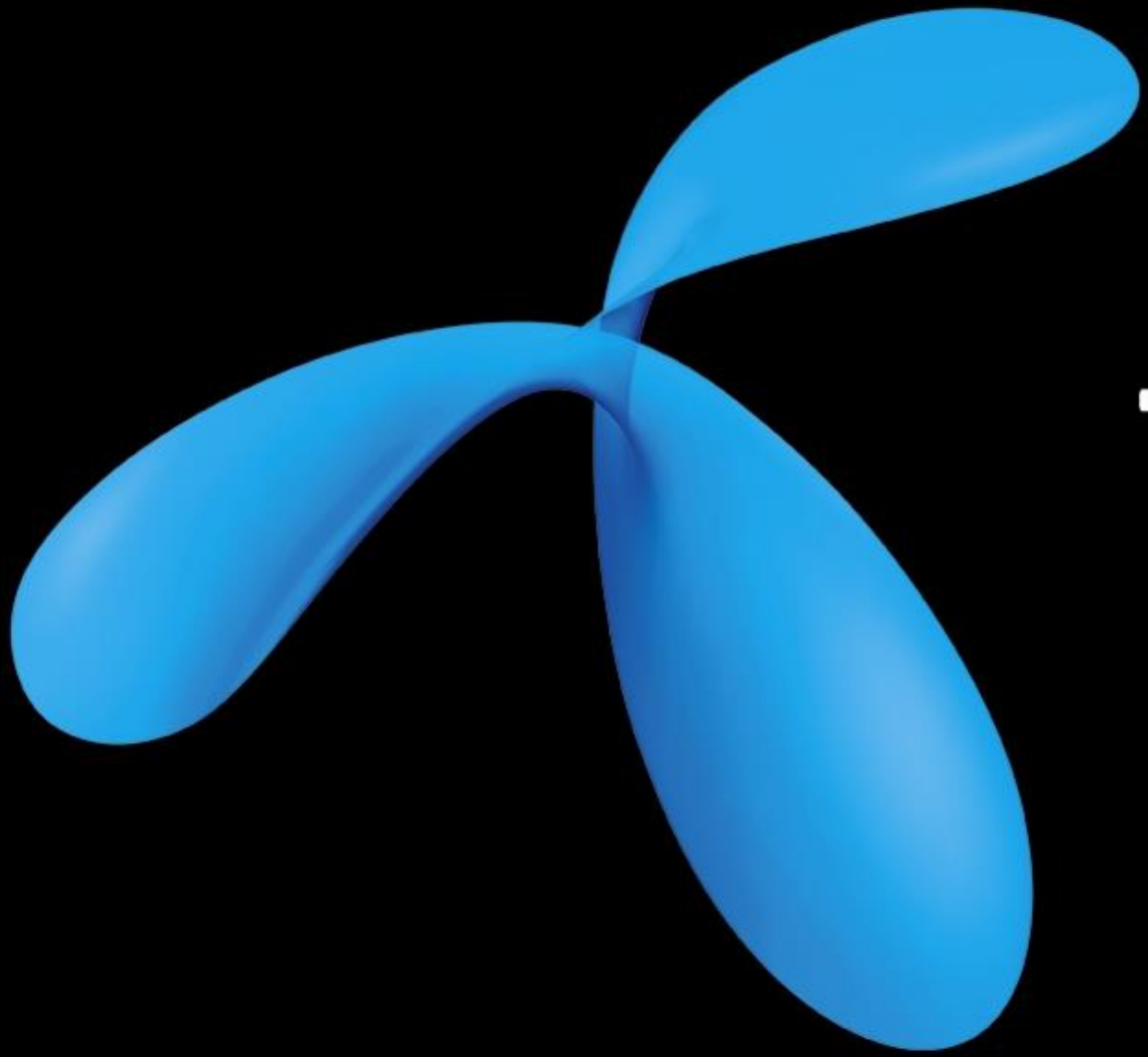


telenor

5G Introduction and Security Perspectives

Rolv R. Hauge
Security, Telenor Norway

Today’s Menu

1. The Promise of 5G
2. 5G Innovations Supporting New Usecases
3. Select Security Improvements in 5G
4. Key Security-Relevant Changes
5. Security Challenges
6. Private Networks and Edge Offering
7. 5G network criticality and robustification
8. 5G deployment plan 2022

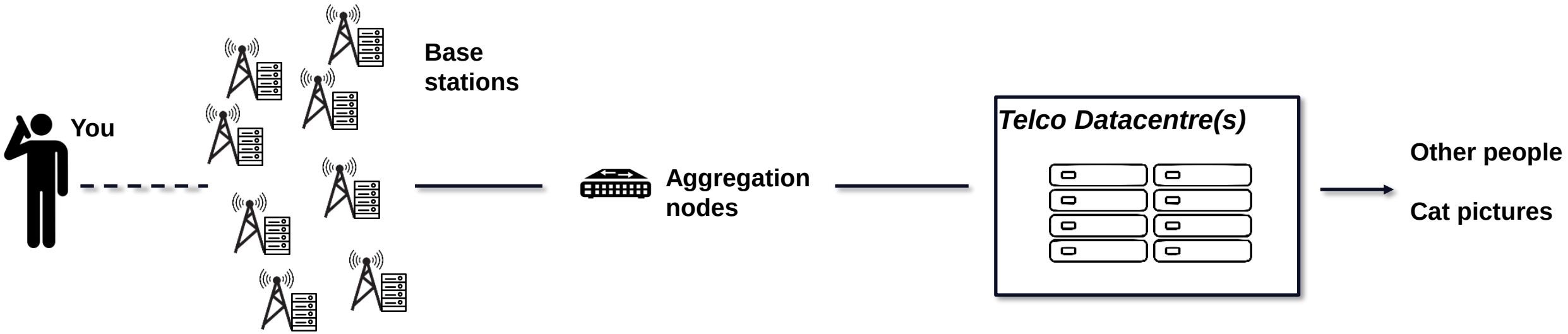
Today's Menu

1. The Promise of 5G
2. 5G Innovations Supporting New Usecases
3. Select Security Improvements in 5G
4. Key Security-Relevant Changes
5. Security Challenges
6. Private Networks and Edge Offering
7. 5G network criticality and robustification
8. 5G deployment plan 2022

***Not* on the Menu Today:**

- **Supply chain risk and attack surface**
  - It's there
  - It's not unique to 5G
  - It's a growing concern
  - It's being addressed
  - It's worth a talk of its own – or more
- **The criticality of available and trustworthy connectivity in the *connected society***
  - You known it, I know it, we all know it
  - Significant part of the reason why '5G security' is high on so many agendas in the first place

Super-duper-over-simplified: A mobile network



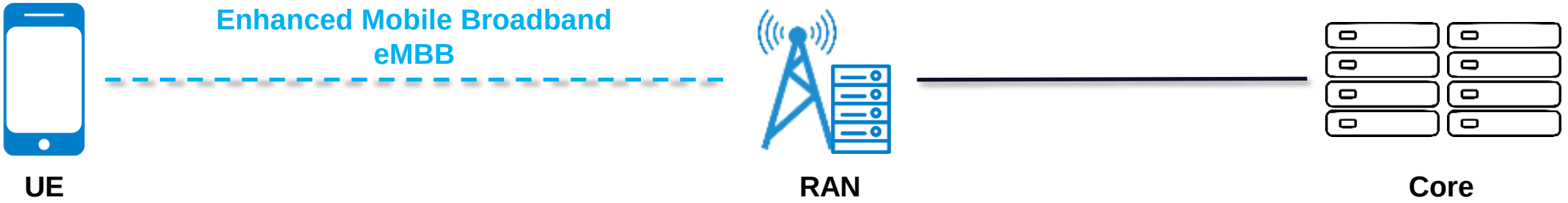
The Promise of 5G

5G vs. LTE – Industry Targets

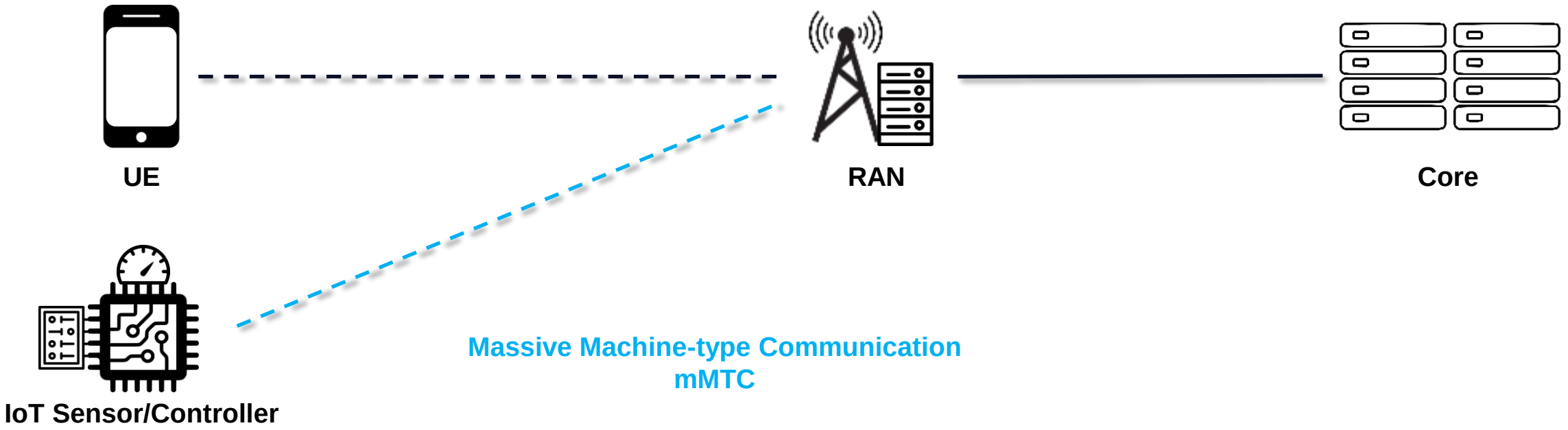
	Latency	Throughput	Connections	Mobility	Network Architecture
5G	**1 ms** E2E Latency	**10Gbps** Per Connection	**1,000K** Connections Per km²	**500km/h** High-speed Railway	**Slicing** Ability Required
Gap	**30~50x**	**100x**	**100x**	**1.5x**	**NFV/SDN**
LTE	30~50ms	100Mbps	10K	350Km/h	Inflexible

5G Innovations Supporting New Usecases

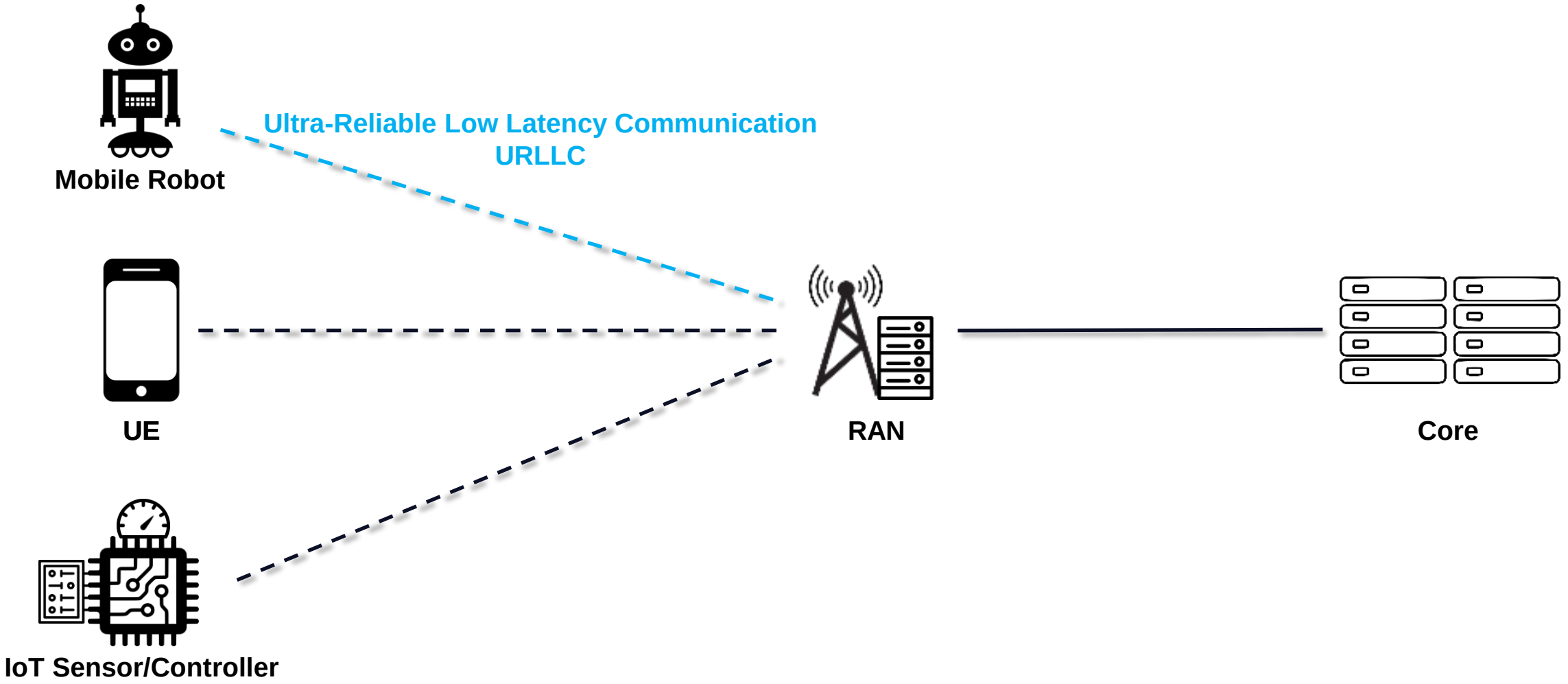
Innovations Enabling New Usecases - **Faster**



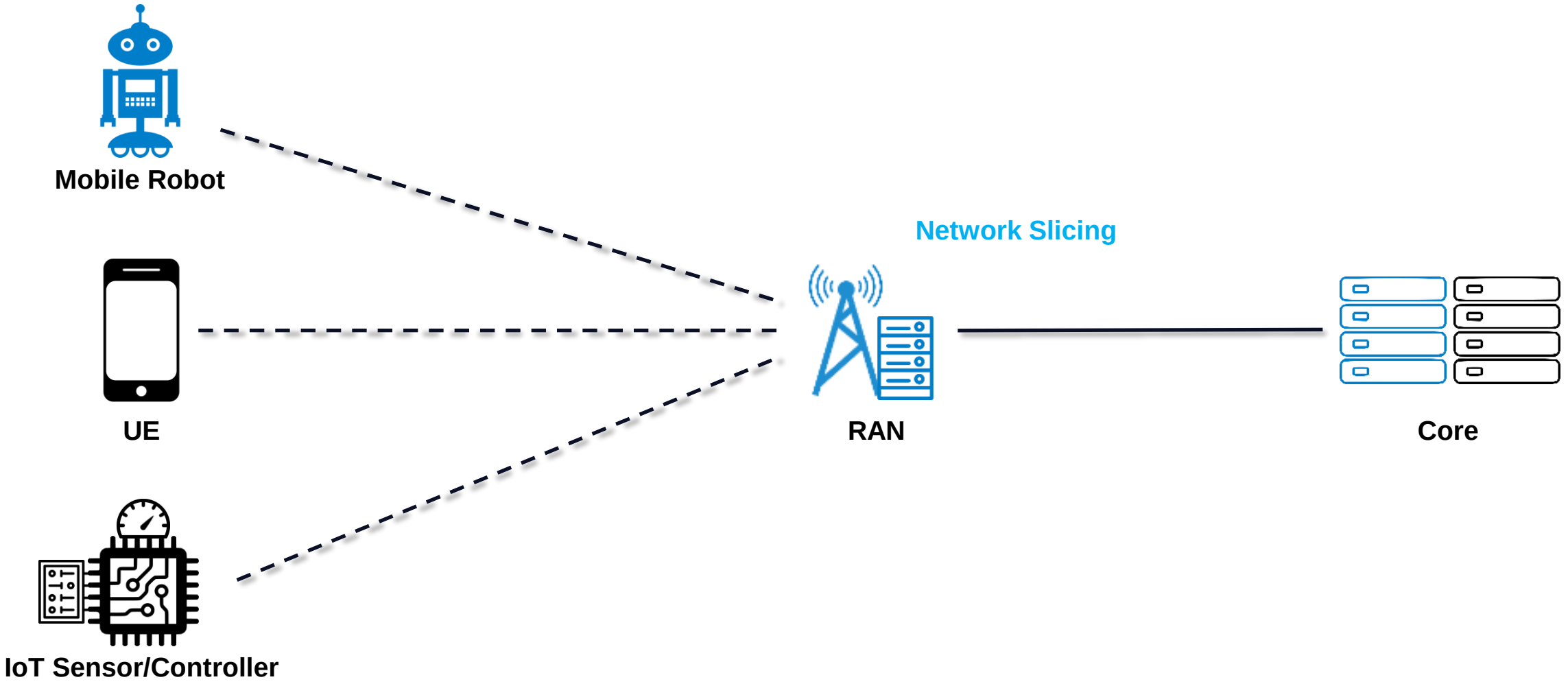
Innovations Enabling New Usecases - **Massive**



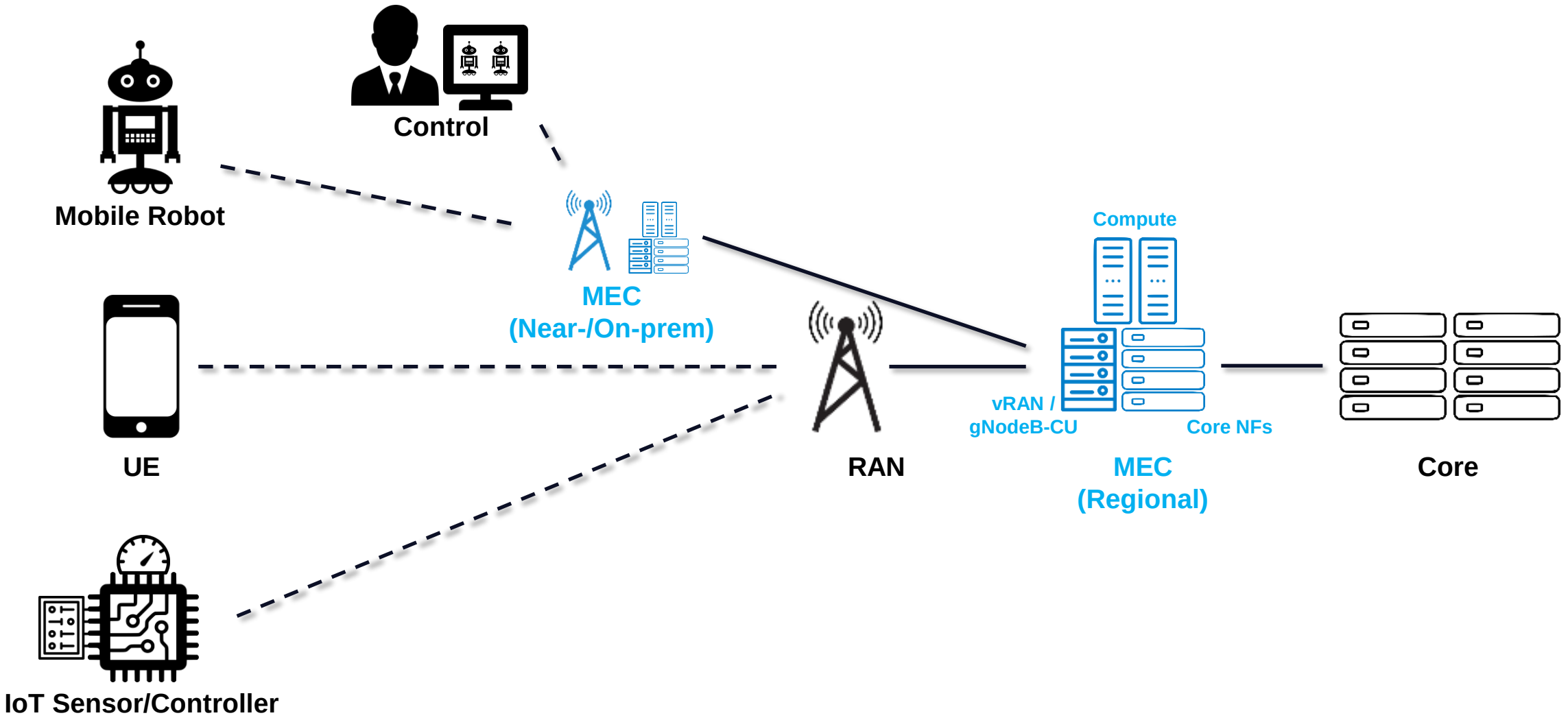
Innovations Enabling New Usecases – **Latency / Reliability**



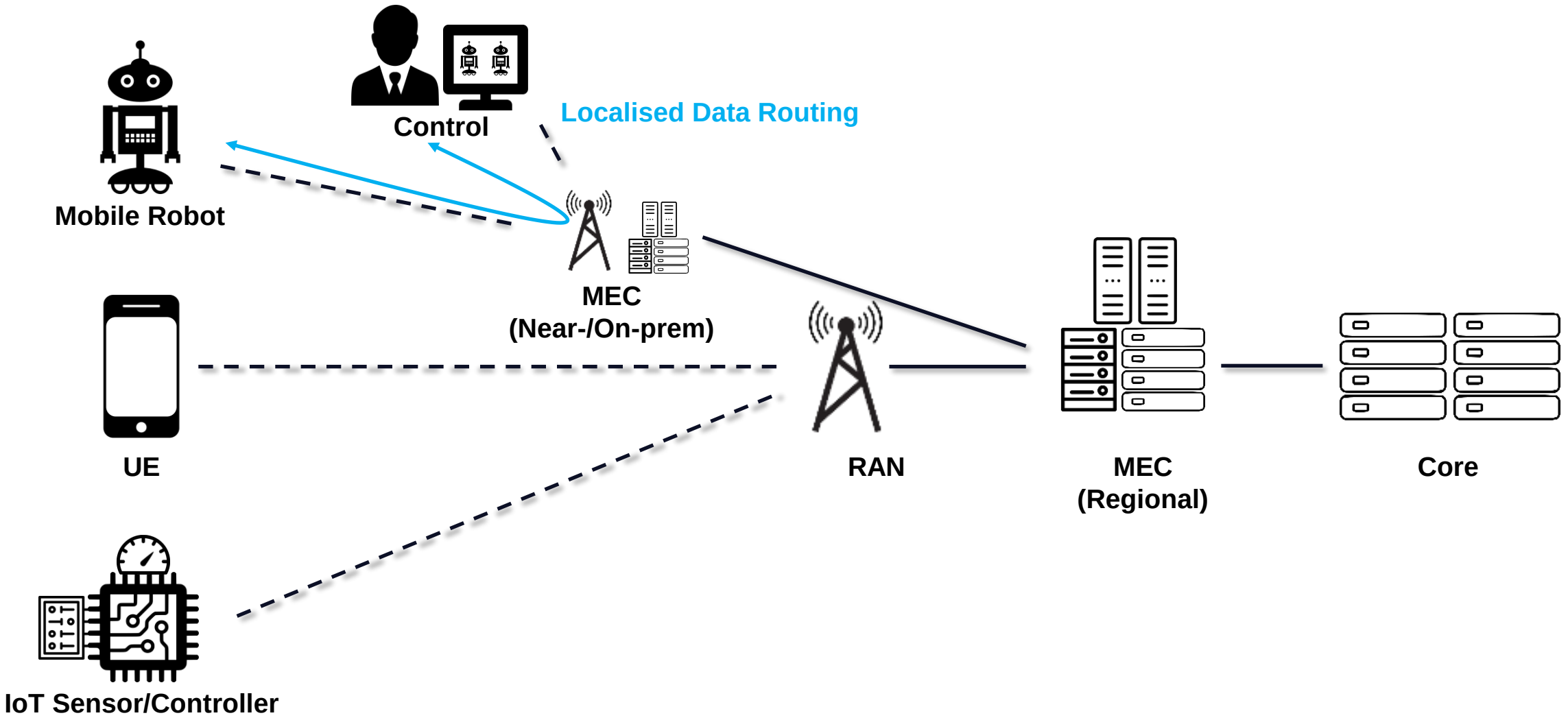
Innovations Enabling New Usecases – **QoS / Slicing**



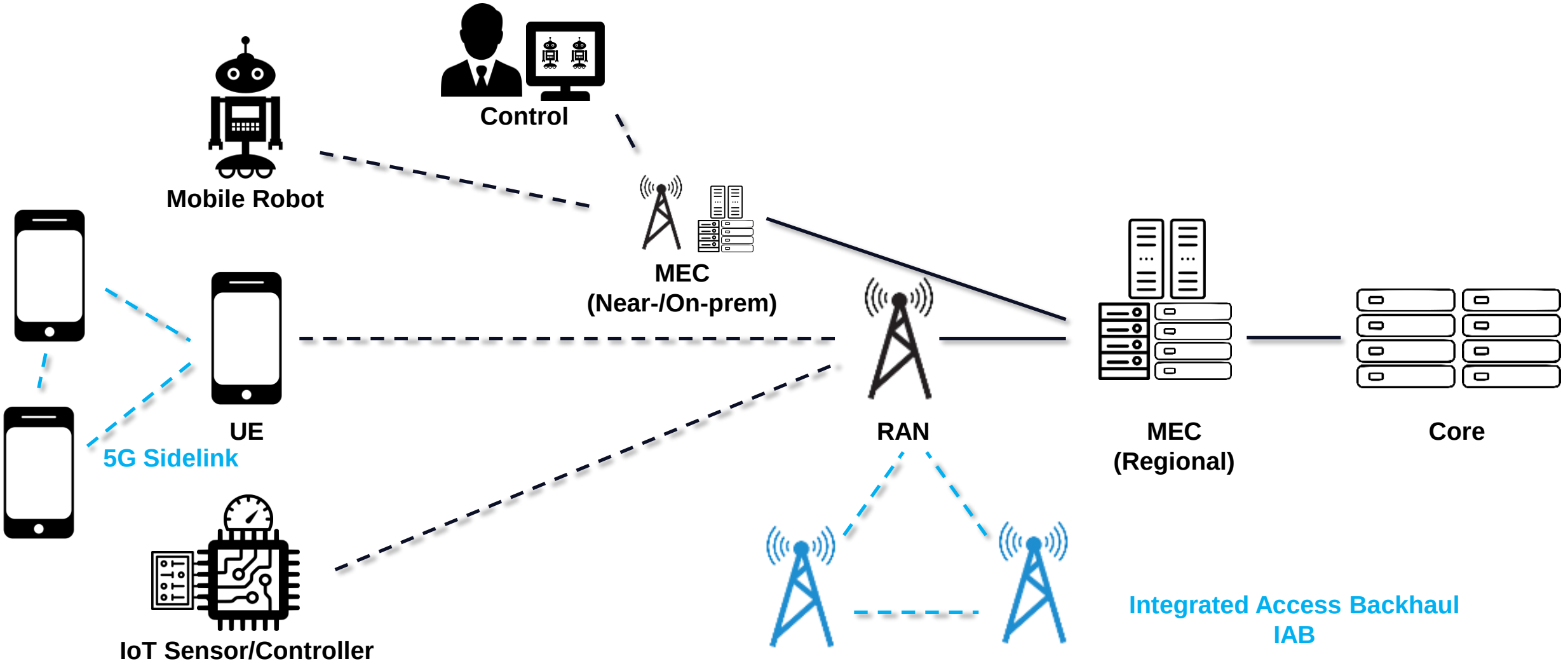
Innovations Enabling New Usecases – **Virtualisation and MEC**



Innovations Enabling New Usecases – **Loalised Data Routing**

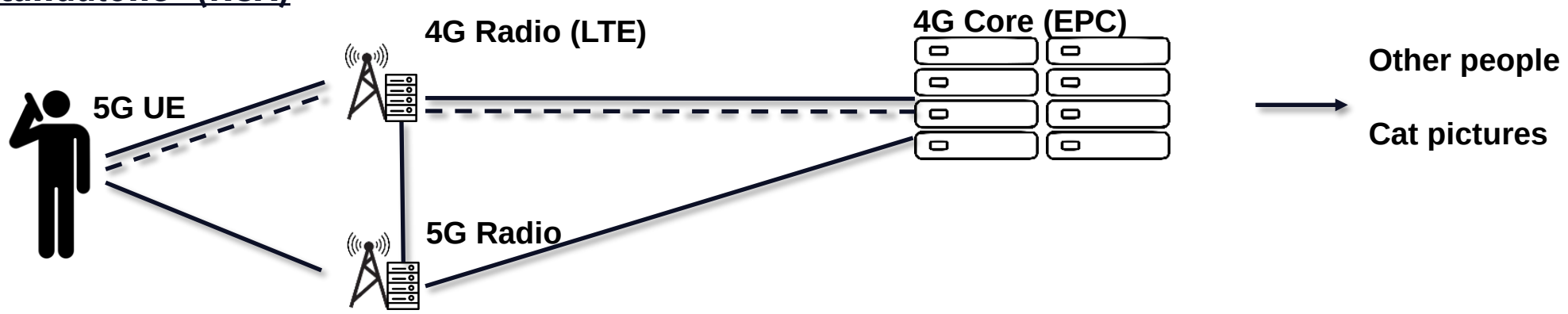


Innovations Enabling New Usecases – **Direct Communications**

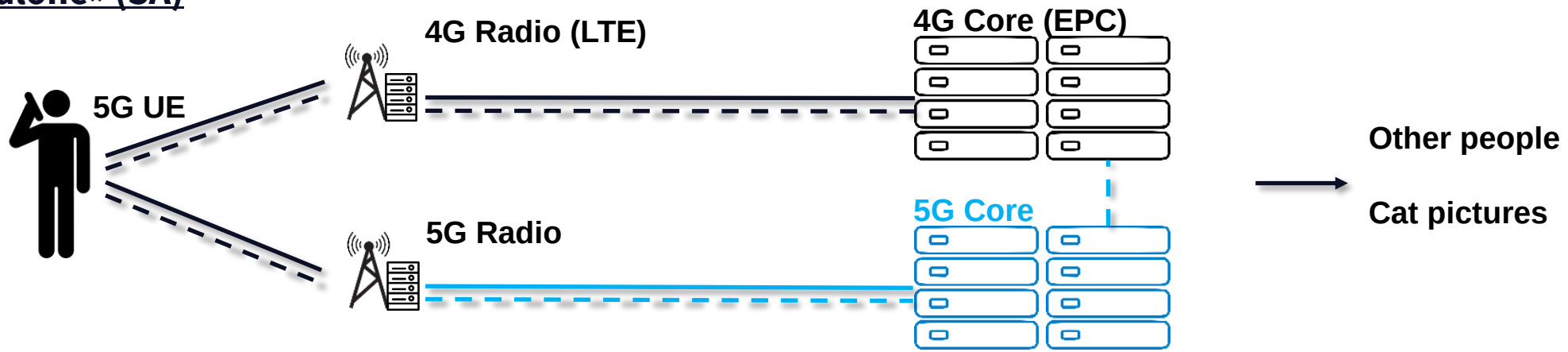


«We’re deploying 5G»

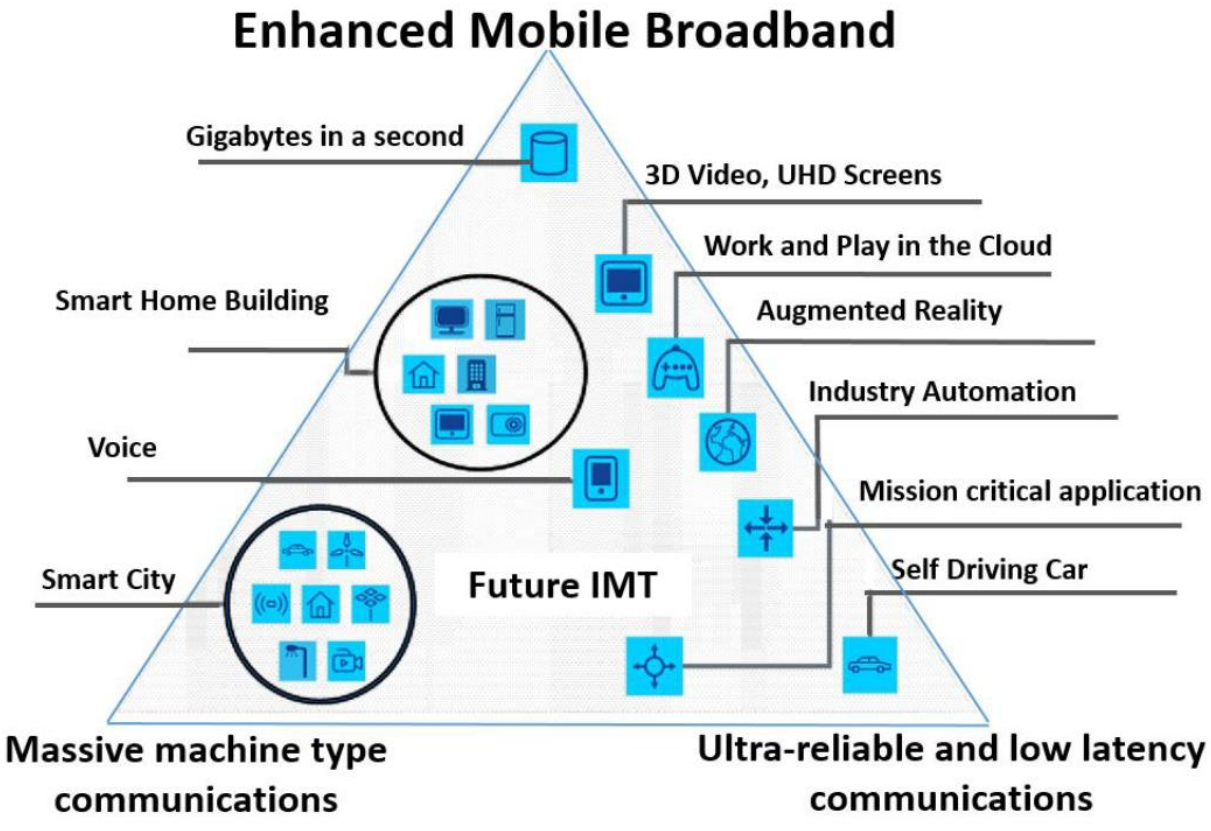
«Non-Standalone» (NSA)



«Standalone» (SA)



Current Non-standalone 5G is addressing eMBB use-cases and FWA

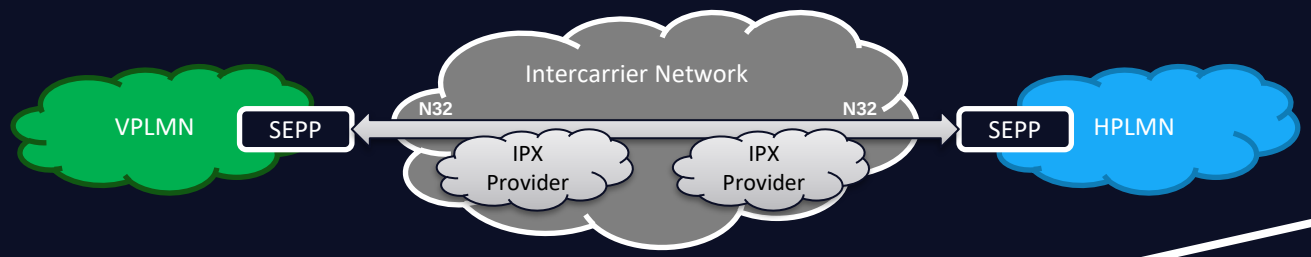


- eMBB/FWA
- 5G Terminals
- Smart Home
- Smart Cities
- Industrial Control/Automation
- Aquaculture Automation
- *… and the list goes on …*

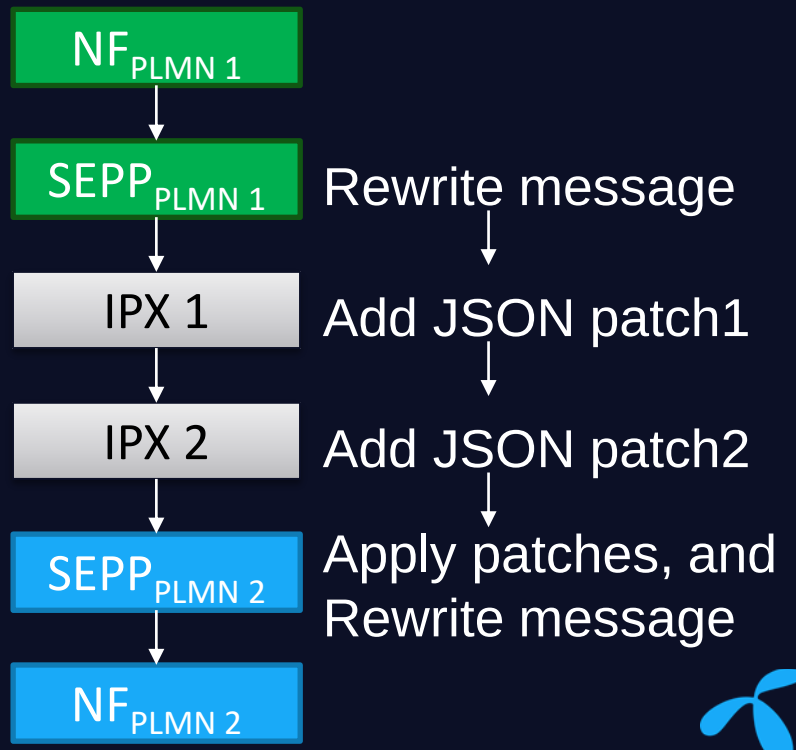
Select Security Improvements in 5G

Improved Home Control and Interconnect Security

- **Improved home control**; verified roaming subscriber presence
  - User Equipment message required to be signed with home network public key



- **Improved Interconnect Security**
  - End-to-end integrity protection
  - Sensitive elements end-to-end confidentiality protected



Improved Subscriber Privacy

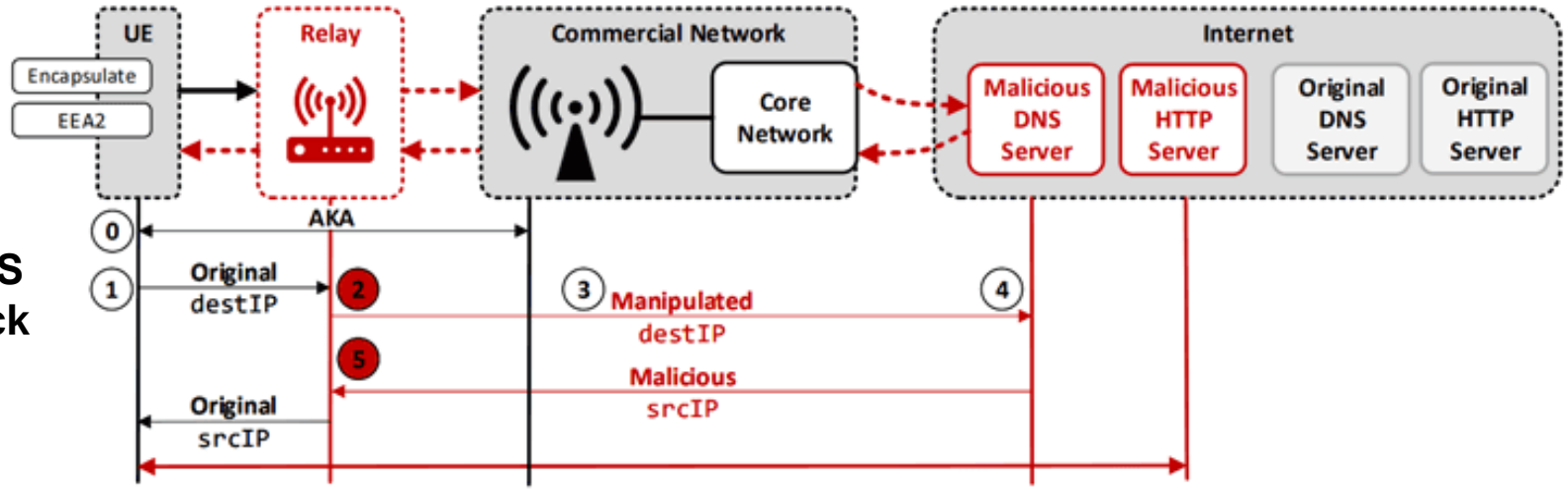
- Previous generations have specified a temporary identifier to be used on the radio interface, but
  - Changing the TMSI - ever – is optional!
  - Simple tricks like provoking ATTACH, makes the terminal transmit its permanent identifier (IMSI) in clear.

- Finally in 5G, we seem to have got it right!
  - The **SU**bscriber **P**ermanent **I**dentity (SUPI) is never transmitted over the air, only the ephemeral **SU**bscriber **C**oncealed **I**dentity (SUCI), and
  - Paging of the UE by SUPI is not allowed.

Integrity protection of *User Plane*

- Researchers have demonstrated how lack of integrity controls on radio *user plane* in previous generations, allows for manipulation of encrypted communications.
- In 5G, *user plane* integrity control is mandatory.

Example:
The "aLTEr" DNS redirection attack



ALTER: Overview of the DNS redirection attack.

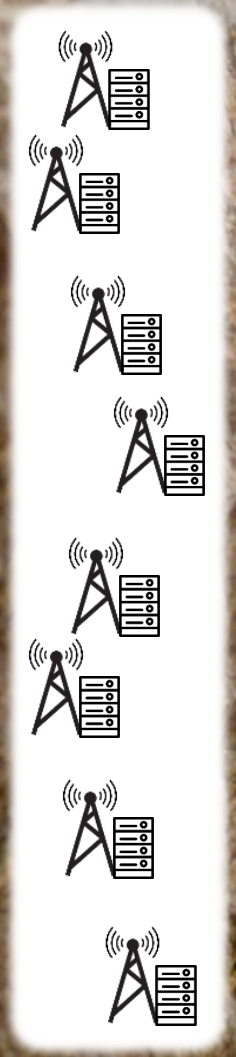
Details at https://alter-attack.net

Authentication

- Updated, unified algorithms
  - 5G-EAP and EAP-AKA
- Access agnostic
  - Both can be applied to 3GPP and non-3GPP access.
- **Optional secondary authentication**
  - **between the mobile device and an external data network.**

Key Security-Relevant Changes

Changes: 1. Edge Compute (MEC)



gNodeB-DU

«midhaul»

Edge Compute Site

gNodeB-CU

Core functions

Customer / 3rd party

«backhaul»

Telco Datacentre

Mobile core

Resource sharing and cross-exposure?

Physical vs. logical security balance?

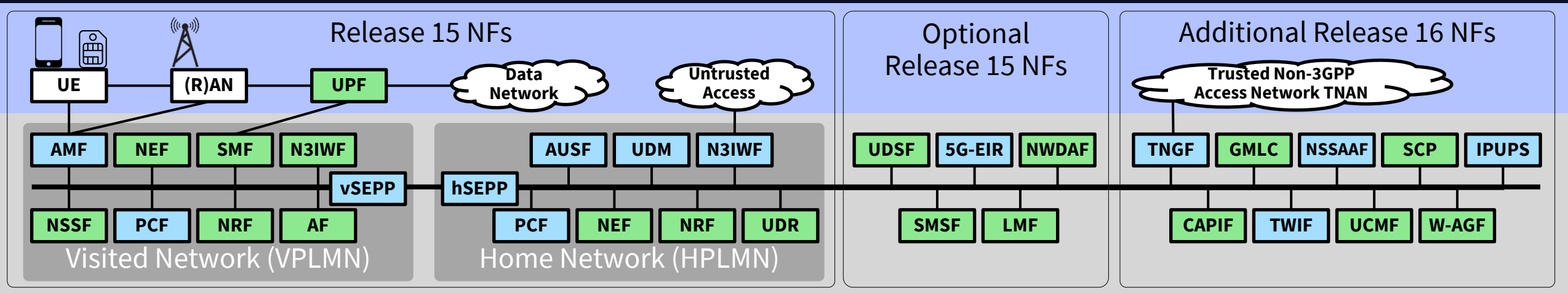
thousands ***more than a few*** ***a few***

Changes: 2. External Exposure of Core

- **Use cases depend on core functions exposure**
- ***NEF* (Network Exposure Function) in the 5G architecture provides API-based exposure of core functions to 3rd parties**
- **A material expansion of the attack surface**
- **Risk relates to vulnerabilities and misconfiguration of the API layer and functions (NEF) or authentication function.**

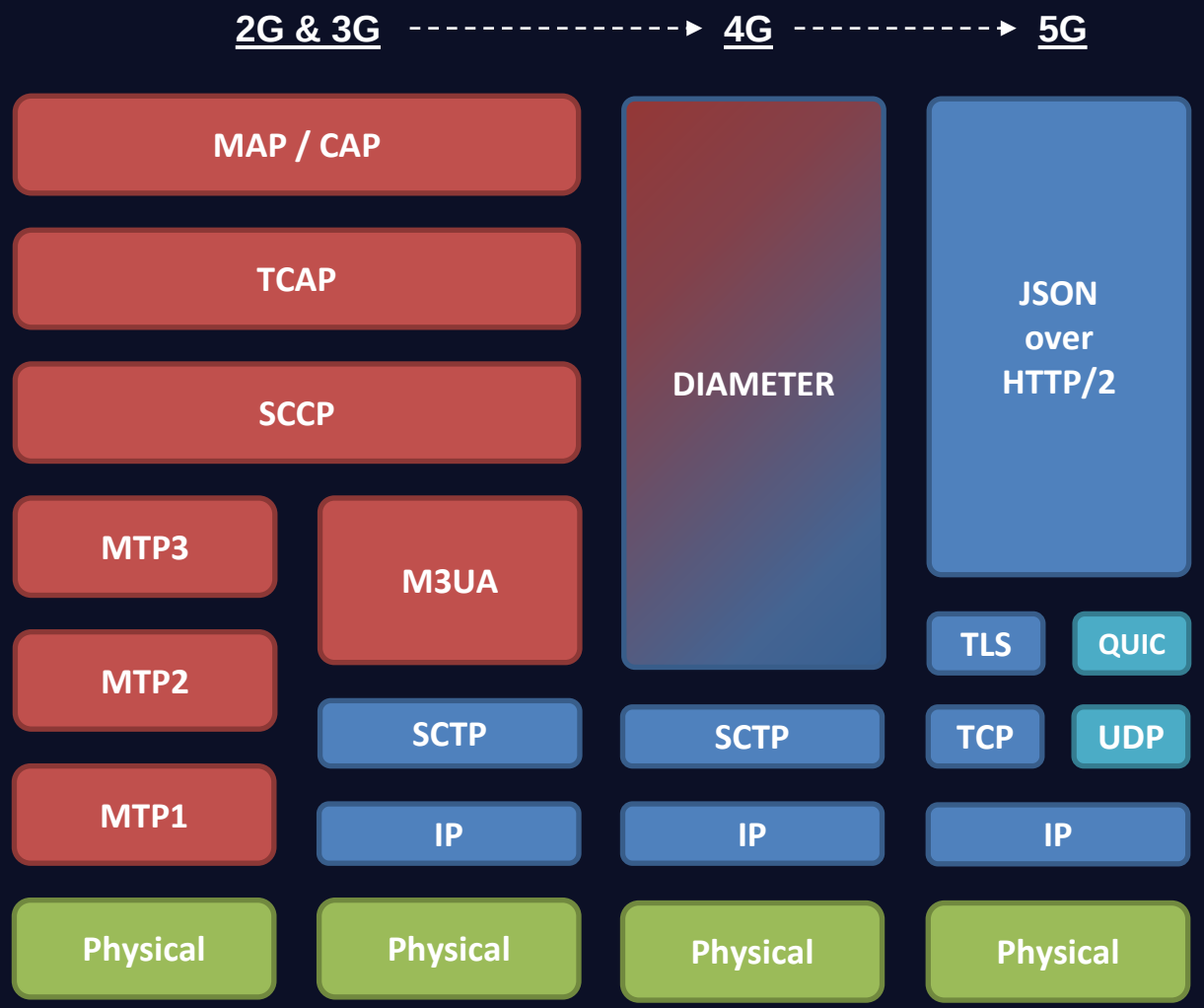
Changes: 3. Service Bus Architecture

- **Design based on “zero-trust” network philosophy;**
  - all functions are available to one another over the service bus, but
  - all access, use and communications are **authenticated** and positively **authorised**.
- **The secured communication between all NFs inside a PLMN is based on TLS** with:
  - **Confidentiality** protection by encryption, **Integrity** protection by hash validation, **Authentication** by certificates.
- **But; does not preclude further connectivity-restricting / network level security measures.**



Changes: 4. New Signalling Stack

- Radical shift to Internet standards and protocols
- Well-maintained and subject to a lot of security research and offensive activity
- Risk:
  - Implementing and operating organisations unfamiliar with securely applying, configuring and operating this stack
  - High availability of offensive research and attack tools
  - Lower-tier attackers more familiar with it

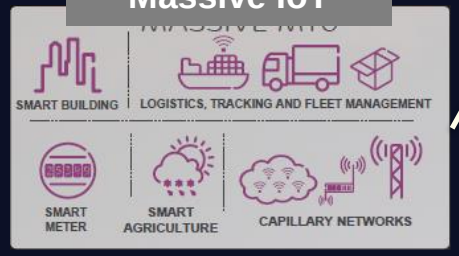


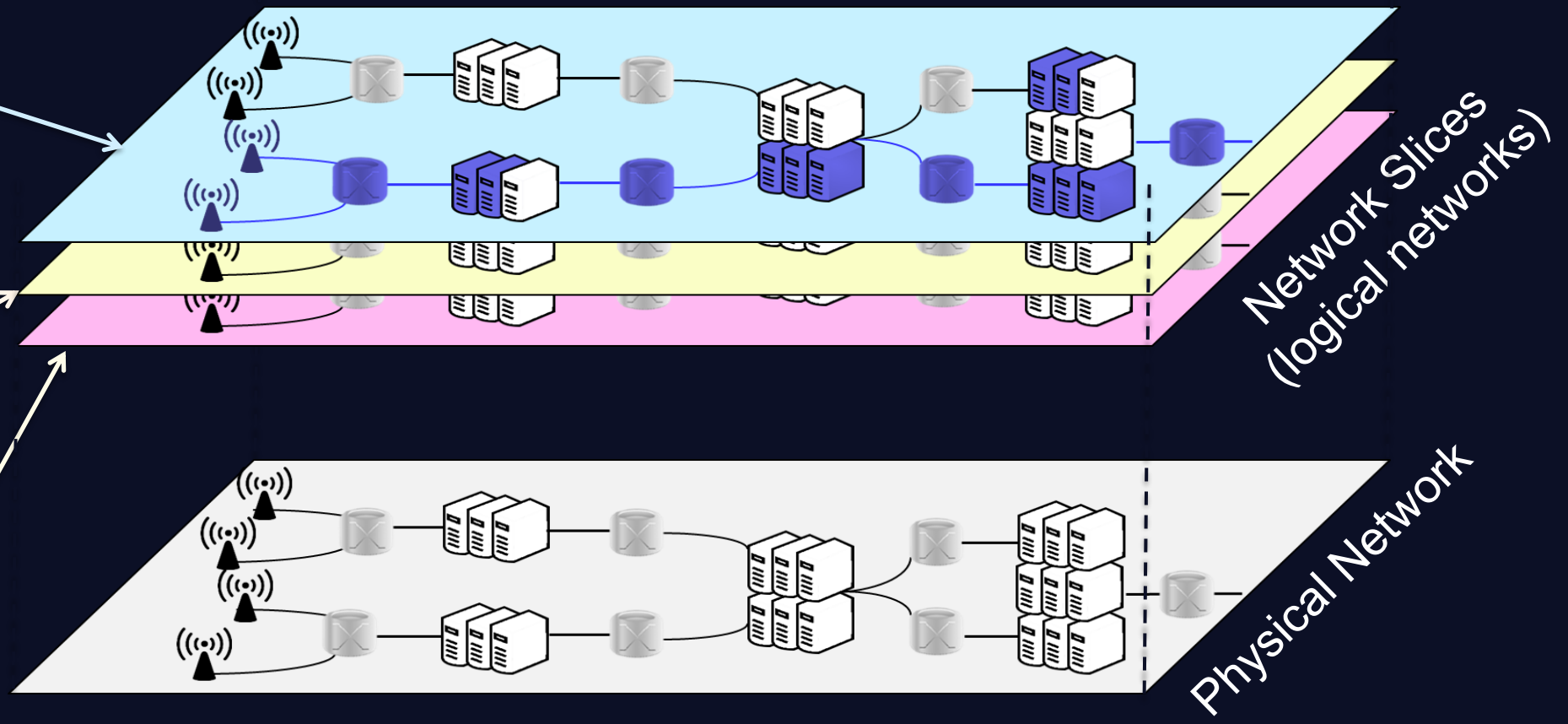
Changes: 5. Slicing

Enhanced Mobile Broadband

Ultra-reliable

Massive IoT





Security Challenges

Backwards Compatibility and Interoperation with Legacy

- **Older terminals, roaming and interconnect requires legacy support and backwards compatibility**
  - UEs may be susceptible to downgrade attacks (radio)
  - Old interconnect signalling protocols (e.g. SS7 and Diameter) still need to be supported

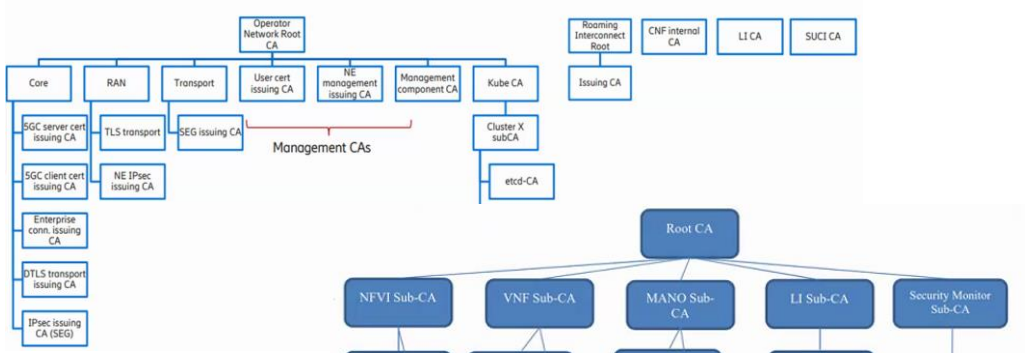
- **Internal interoperability with 4G core**
  - Even 5G “Stand Alone”, has interconnections with the 4G core.

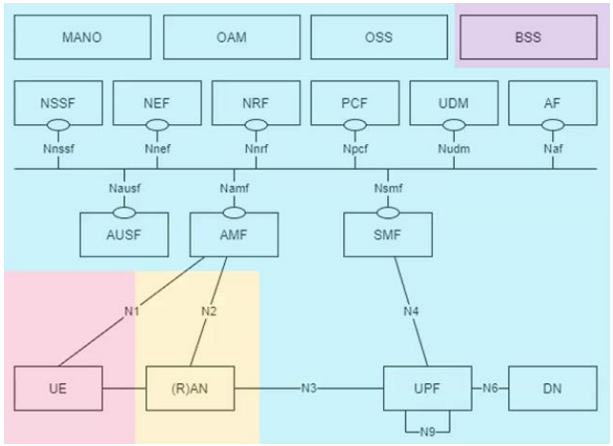
Significantly Different Use

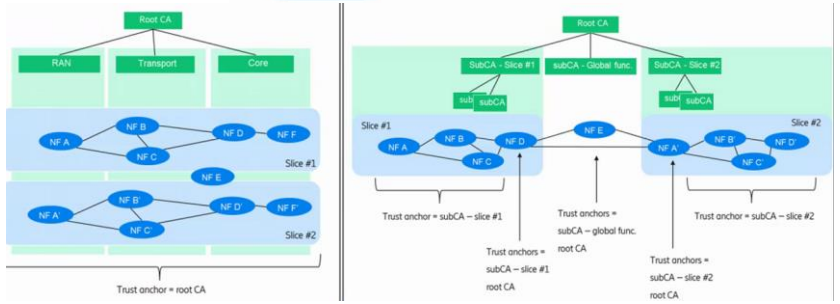
- Security methods designed for networks with mostly human use phone devices, may no longer be suitable
- 5G supports a plethora of diverse use cases and terminals
- Slicing allows for differentiation of security mechanisms, priorities, policies and approaches.

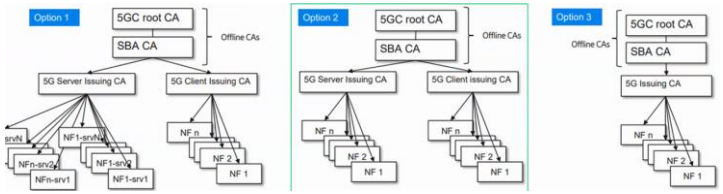
Got PKI(s)?

- Cryptographically rooted security permeates all aspects of 5G.
- Defining the PKI domain scopes and hierarchies is a design challenge.
- Needed <u>everywhere</u>, e.g.:
  - **RAN**
    - UE
    - Network
  - **Core Service Bus (VNFs/CNFs)**
    - Slicing
  - **Roaming/interconnect**
  - **Network Function Virtualisation Infrastructure**
    - Compute
    - Management
  - **Special domains, e.g. lawful interception**
  - **Services / Service platforms**
  - **Business Applications (BSS)**



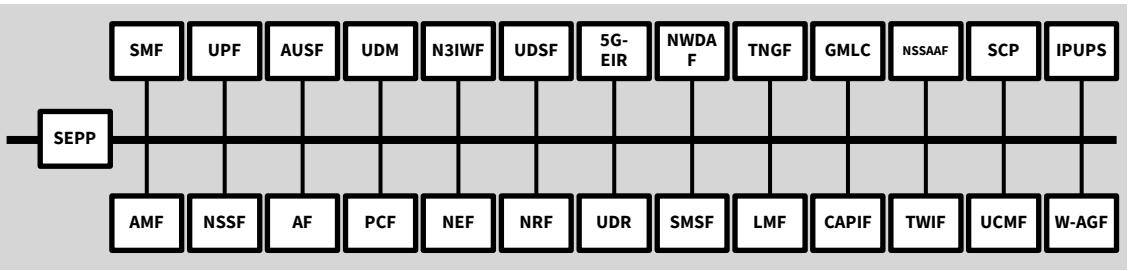




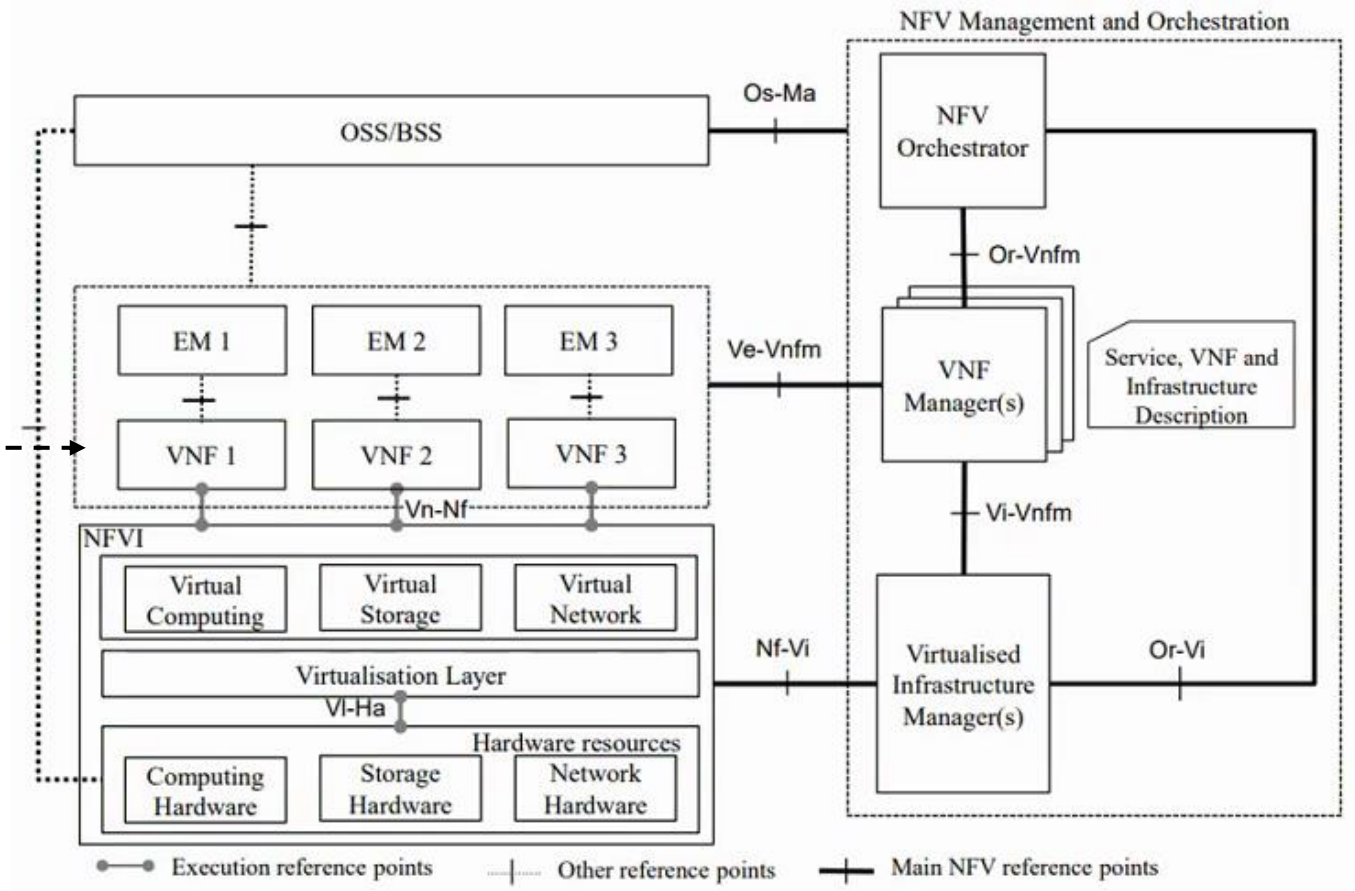


The Shift to Fully Virtualised

3GPP 5G Core (virtualised) Functions



Virtualisation Infrastructure Architecture



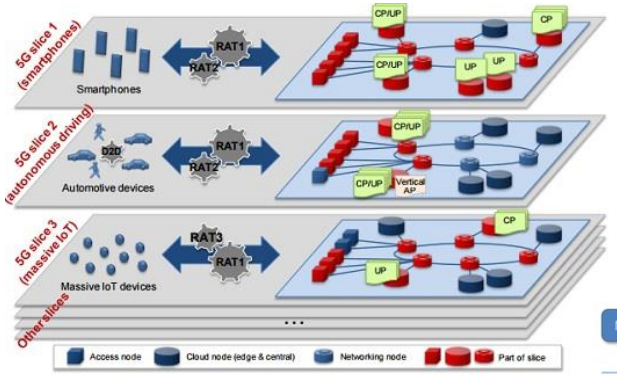
The Shift to Fully Virtualised

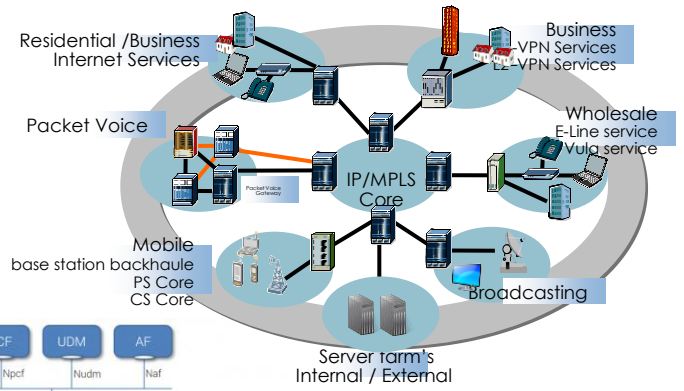
- **Disparate trust levels may share compute resources**
- **Vulnerabilities in assumed segregation**
  - hardware (e.g. x86, mem.) vulnerabilities,
  - hypervisor escapes,
  - VM escapes,
  - container escapes and
  - application-level vulnerabilities,
- **Somewhat immature** security tools and practices
- **Advanced adversaries exploit shared resources** to pivot

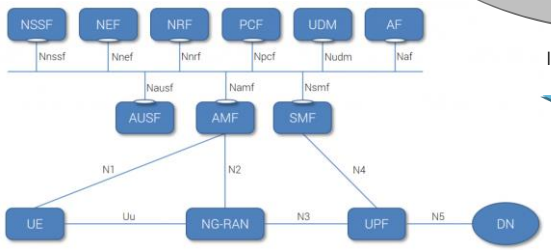
Hence, we

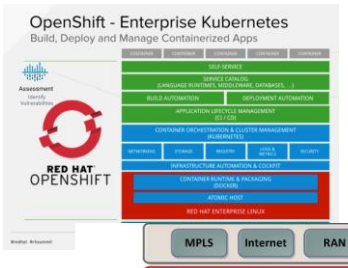
- Apply some **physical segregation**
- Mandate granular logical **micro-segmentation**
- Design to **minimise cross-exposure** through shared resources
- Continuously **identify and apply further security tools and techniques**
- Instrument for in-depth **security monitoring**
  - Pervasive log collection from “everything”
  - Granular IP traffic metadata collection
  - Various host measures as technically applicable
  - Traffic capture and analysis capabilities

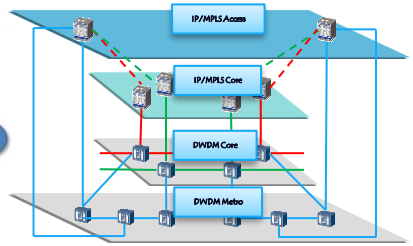
The Increasing Complexity

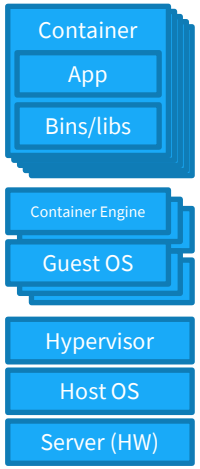


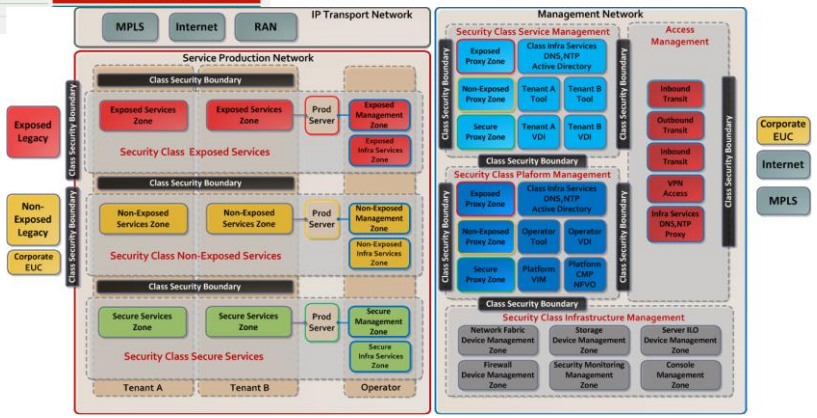












- Significant complexity increase!
- Requires integrated orchestration across domains, layers and technologies.
- Requires robust automation for operation and security.

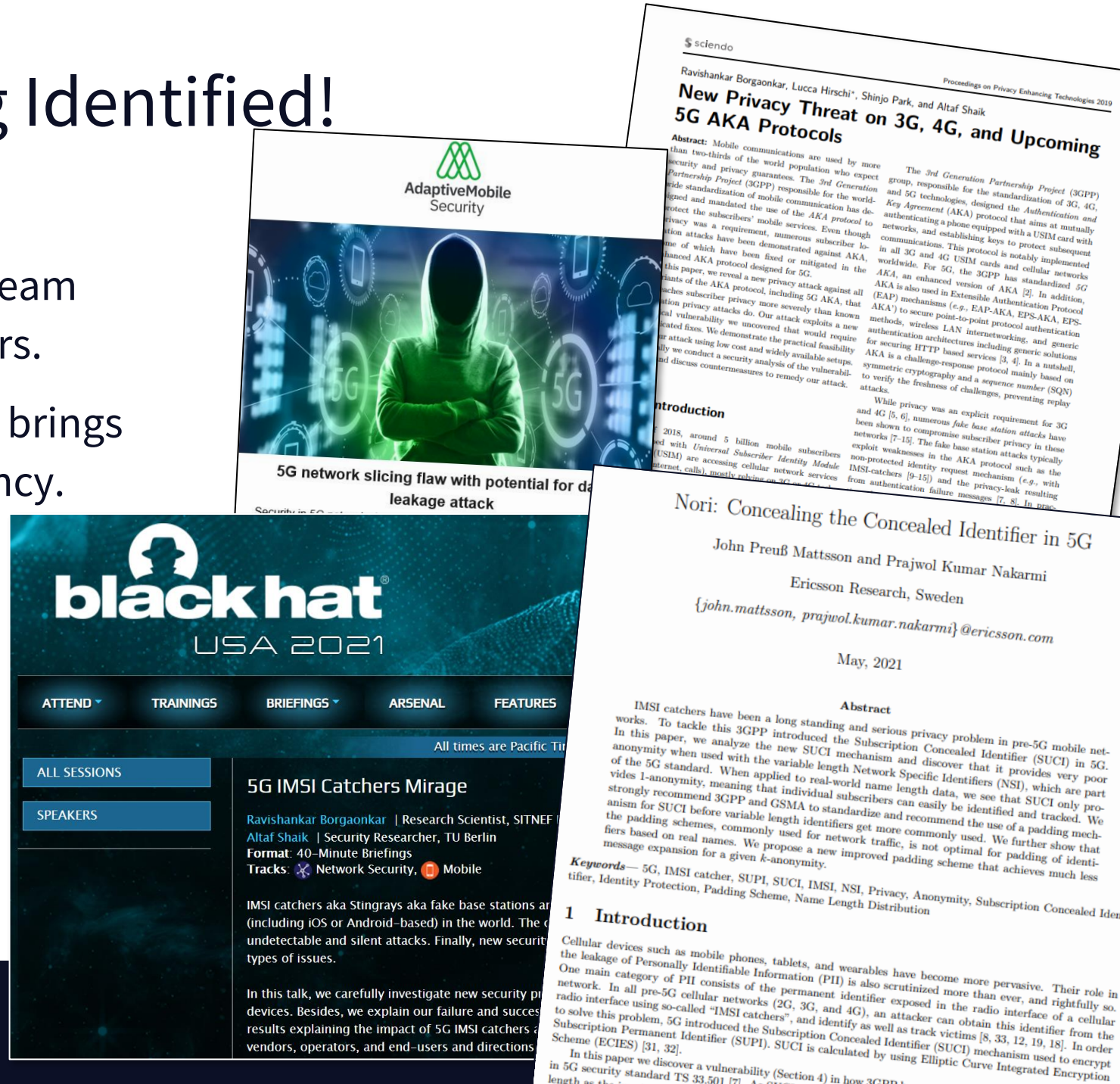
Vulnerabilities Are Being Identified!

- **And that is a very good thing!**
- Telco has gone from niche to mainstream among all kinds of security researchers.
- Telco adoption of «commodity» tech, brings more vulnerabilities into telco relevancy.

Hax0rs, please report findings to the *GSMA's Coordinated Vulnerability Disclosure Programme*!

https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

security@gsma.com

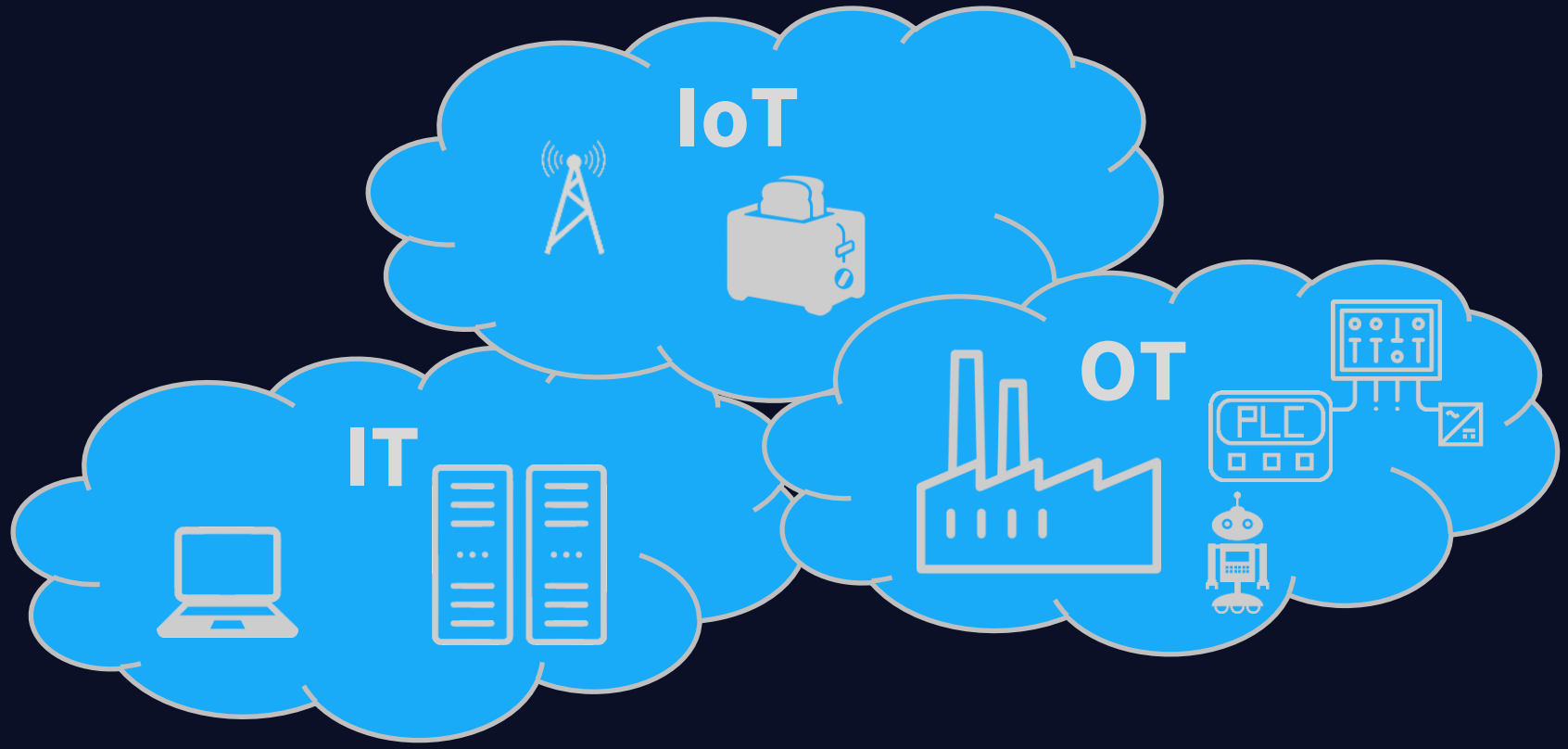


6

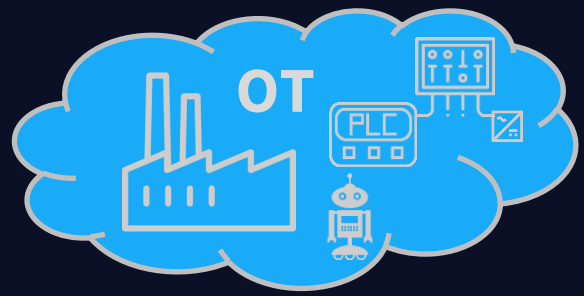
Private Networks and Edge Offering

5G technology supports digitalisation

With digitalisation and IT-OT interconnection, comes an increase in attack surface



IT vs OT



- Security focus on full CIA triad, often emphasis on *confidentiality* and *integrity*
- High rate of change, agile, devops. Frequent change-windows, if at all structured into windows.
- Tolerant of minor outages, failures, and need for fixes.
- Used to being exposed and interconnected.
  High cybersecurity focus.
- Need for keeping all HW and SW in-support and security patched well understood.
- Staff often separate from, culturally different from and mistrusting of the OT staff.

- Security focus traditionally highly centered on *availability*
- Low rate of change. Highly tested for functionality and stability. Very infrequent change-windows.
- Outages can have devastating, even catastrophic consequences.
- Used to being on a closed network.
  Limited cybersecurity focus and competence.
- Huge «technological debt», from a cybersecurity perspective. Lots of legacy.
- Staff often separate from, cuturally different from and mistrusting of the IT staff.

- We see an increase in digitalisation, OT exposure, IT-OT interconnection and IIoT rollout initiatives with inadequte consideration for the cybesecurity implications.
- When what was formerly on isolated networks is interconnected or exposed, security *must* be considered. For many integrated IIoT solutions and legacy OT infrastructures, security must be built underneath, around and in-between.

Private cellular networks
are dedicated cellular networks , established to support business-critical processes.

Edge Computing
moves (cloud) compute closer to where data is being created and consumed, primarily motivated by low-latency use-cases.

The perfect storm

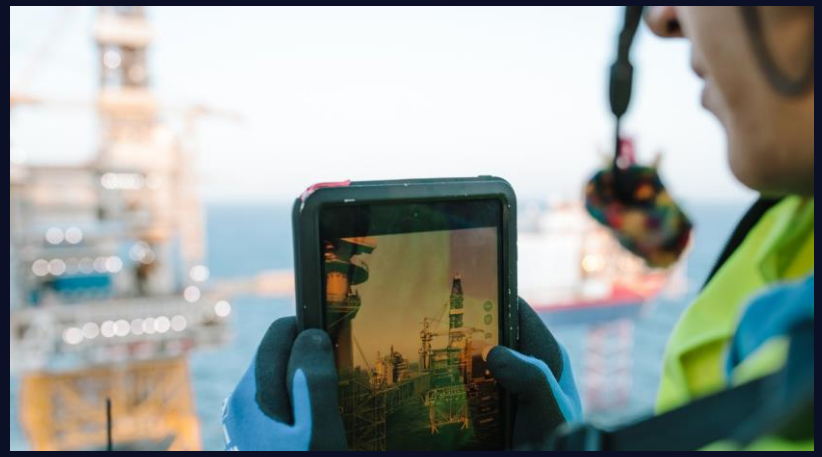
Key industries harvesting benefits from digitalisation supported by the 5G-enablement

Industrial / manufacturing

Health

Defense / security

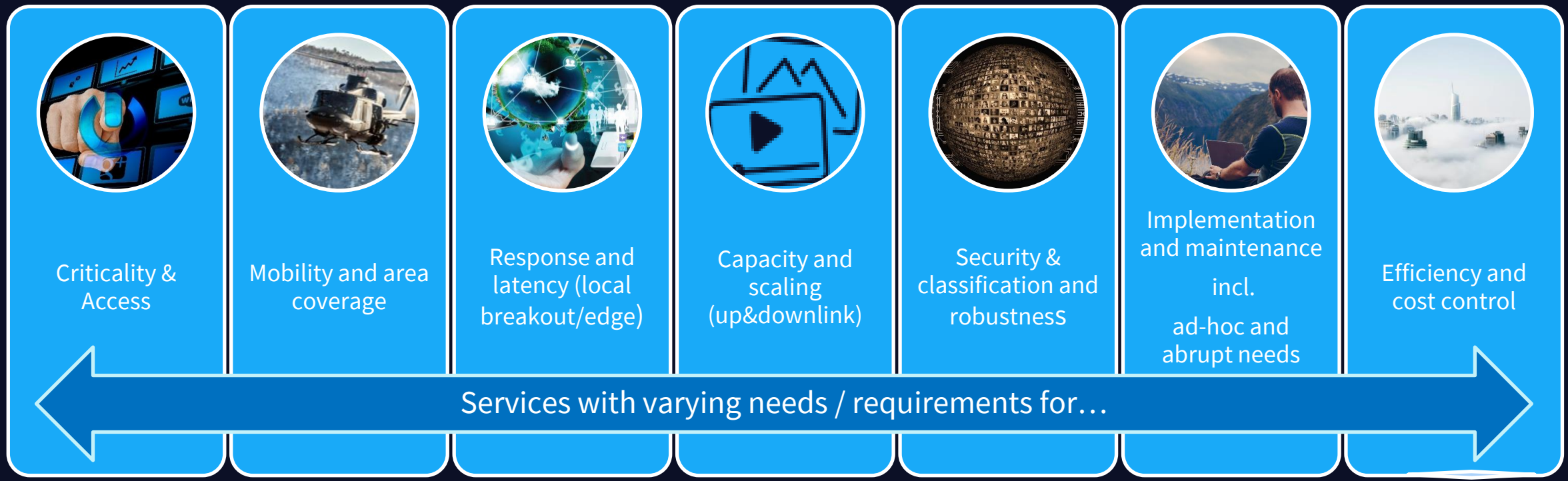
Transport

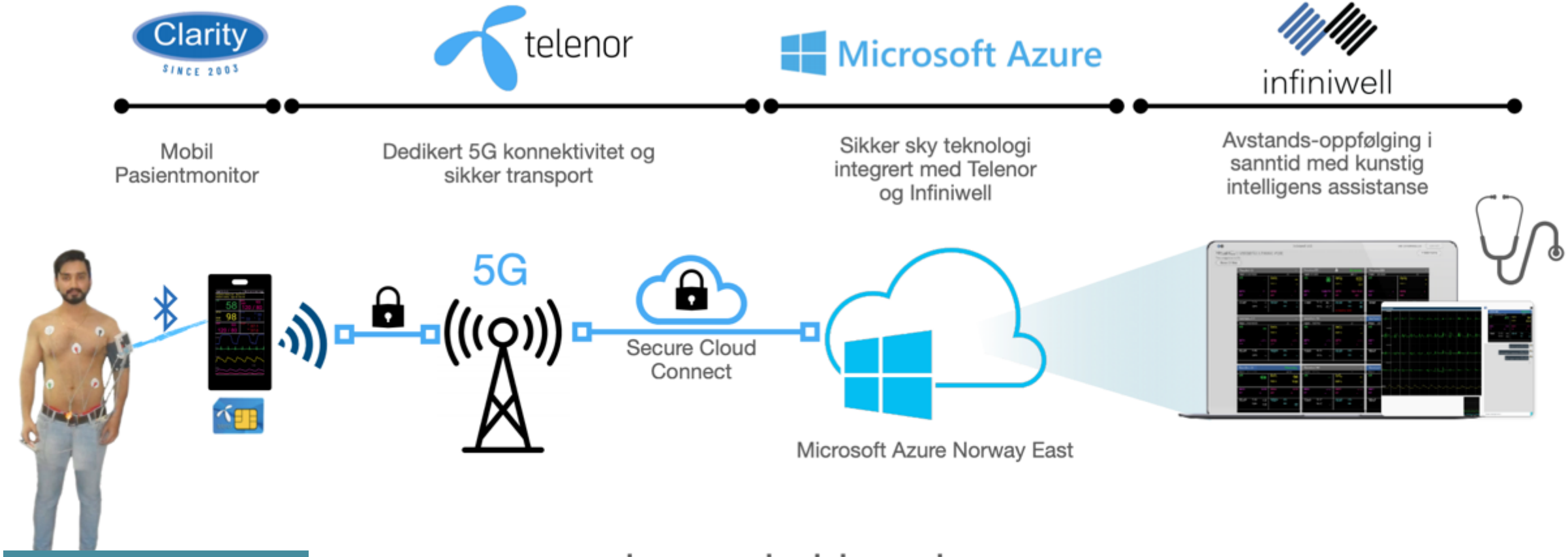


Energy, oil and gas

Key drivers & needs

Though low latency is often a prerequisite, there is a range of other major use cases and customer needs for Edge





Non-invasive | mobilitet

i samarbeid med

ST. OLAVS HOSPITAL
TRONDHEIM UNIVERSITY HOSPITAL

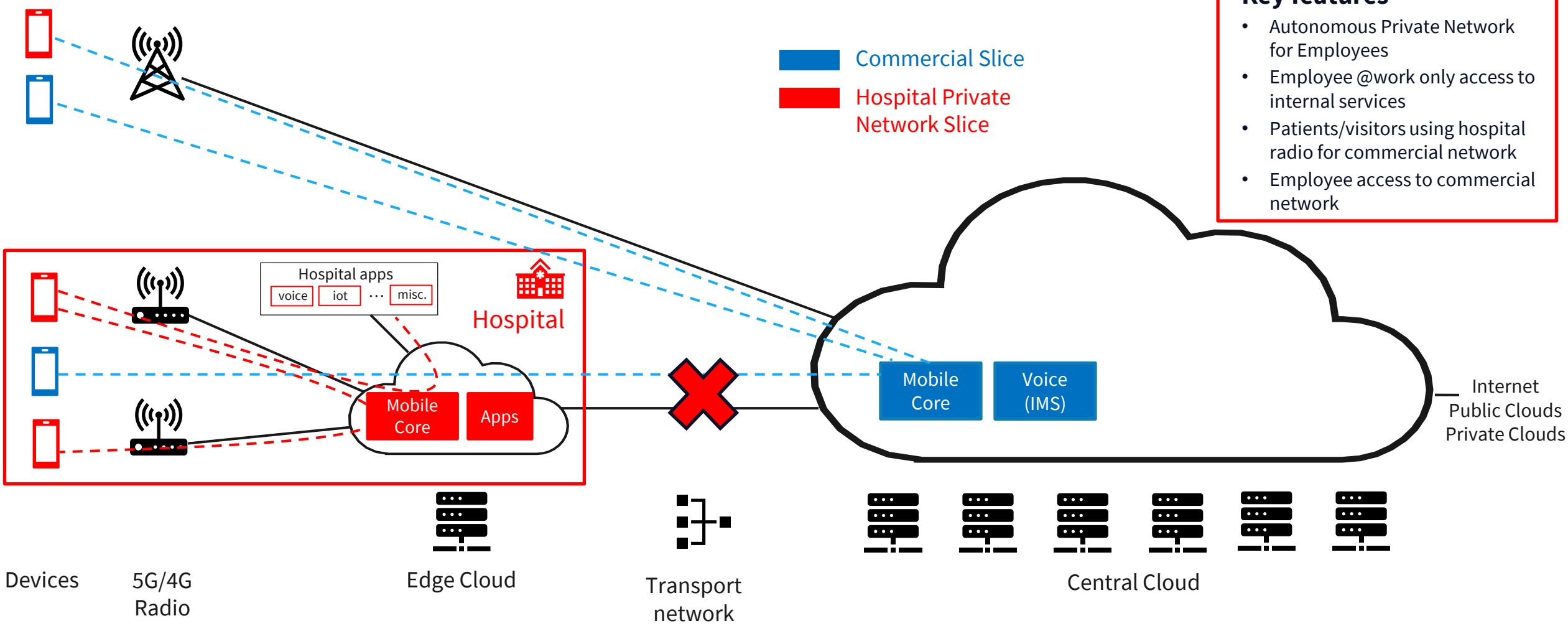
Operating Room of the Future

HELSE MIDT-NORGE IT

Økt bruk av MTU i medisinsk avstandsoppfølging stiller nye krav til mobilnett
MTU plattformer flyttes over til globale skyleverandører
Utvikling av edge computing og 5G, muliggjør lokal prosessering og lagring av data med optimal responstid nye usecases


Oslo
universitetssykehus
Foto: OUS

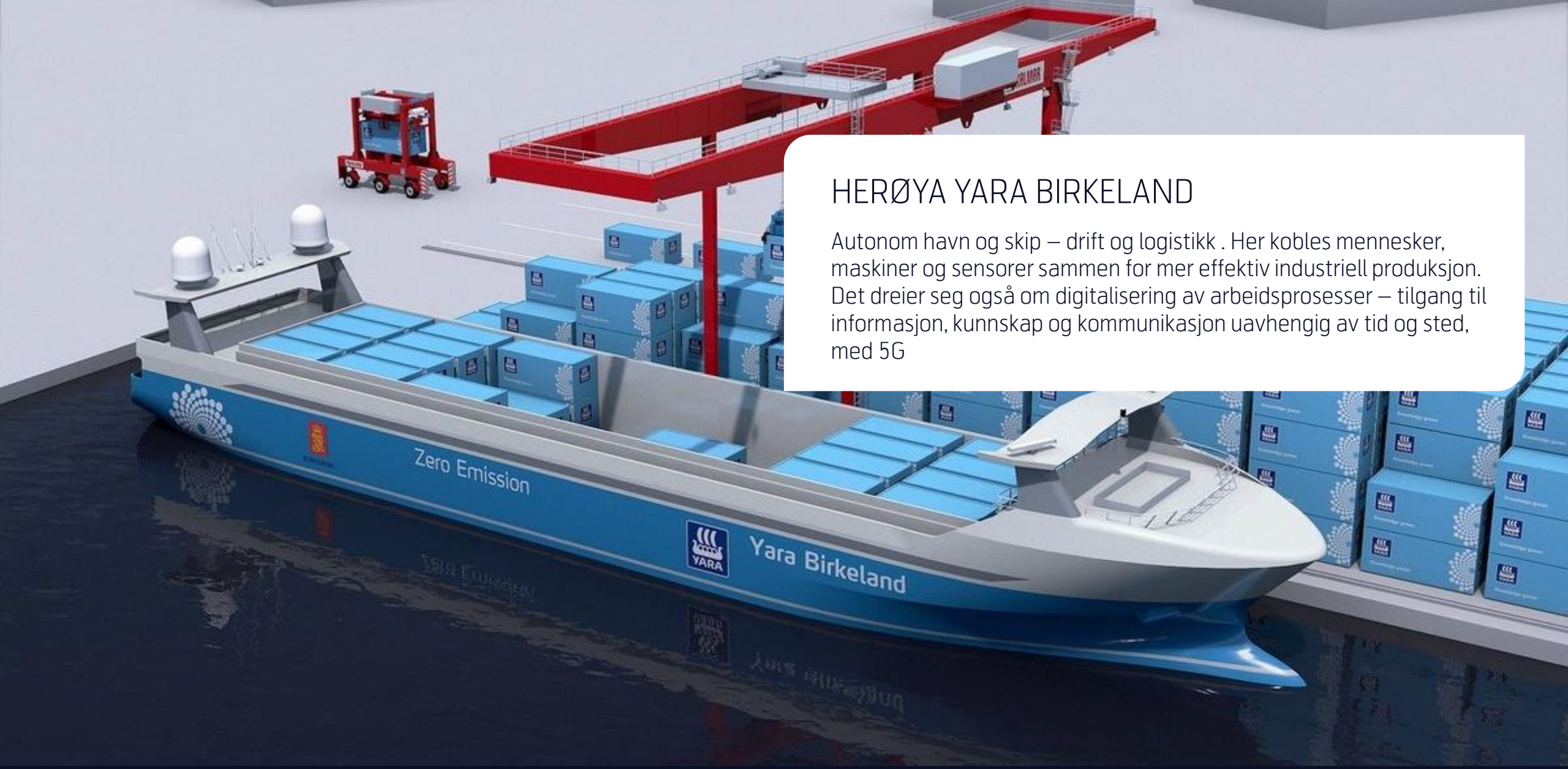
Implementation of a Private Network with Helse SørØst



Key features

- Autonomous Private Network for Employees
- Employee @work only access to internal services
- Patients/visitors using hospital radio for commercial network
- Employee access to commercial network


VARD
MARIN TEKNIKK
Yara Birkeland
Zero Emission



HERØYA YARA BIRKELAND

Autonom havn og skip – drift og logistikk . Her kobles mennesker, maskiner og sensorer sammen for mer effektiv industriell produksjon. Det dreier seg også om digitalisering av arbeidsprosesser – tilgang til informasjon, kunnskap og kommunikasjon uavhengig av tid og sted, med 5G

Private Networks

- Private networks as such is not new, but use of 3GPP technology in private networks is.
- Closely related to edge computing.
- Part of a continuum of connectivity and computing – from extreme edge to public cloud.

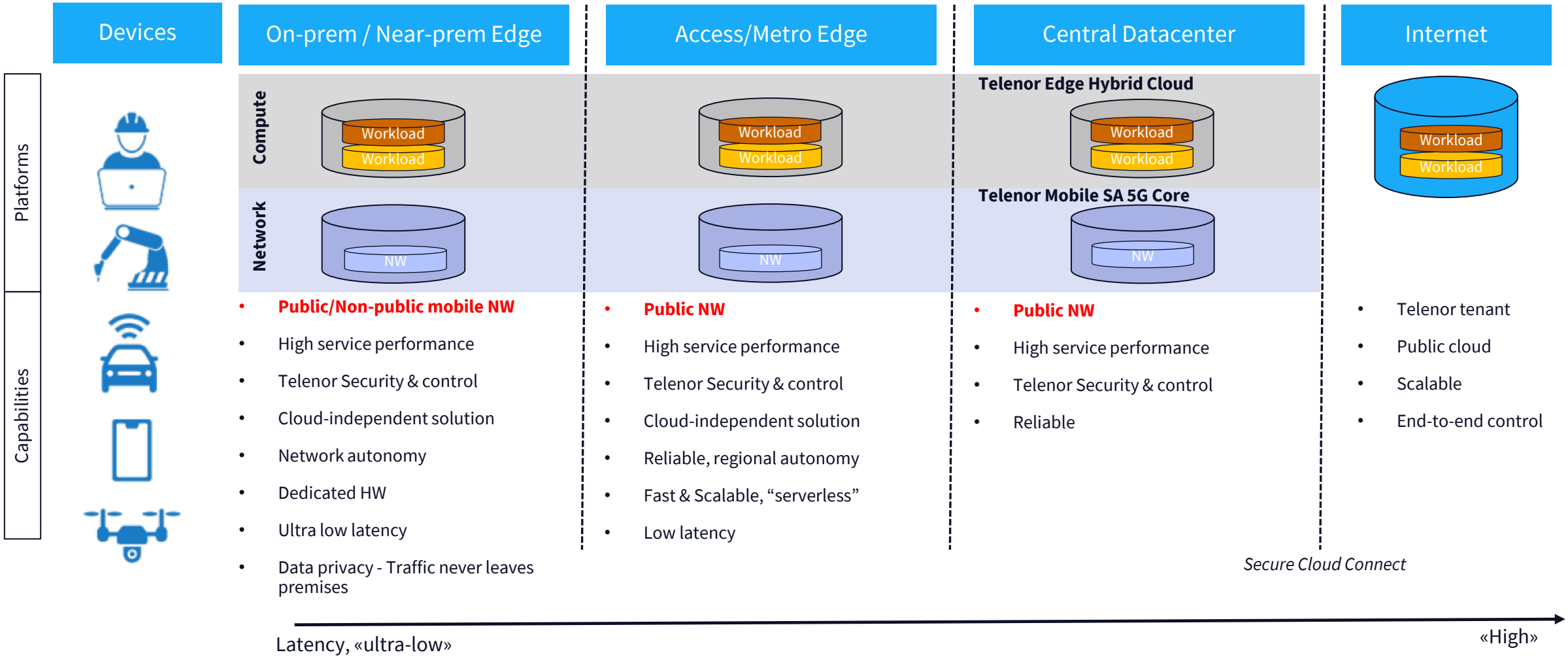
Indoor or outdoor Radio units

Pre-packaged Core Network

- No cloud solution included. Can be added locally or connect to regional cloud

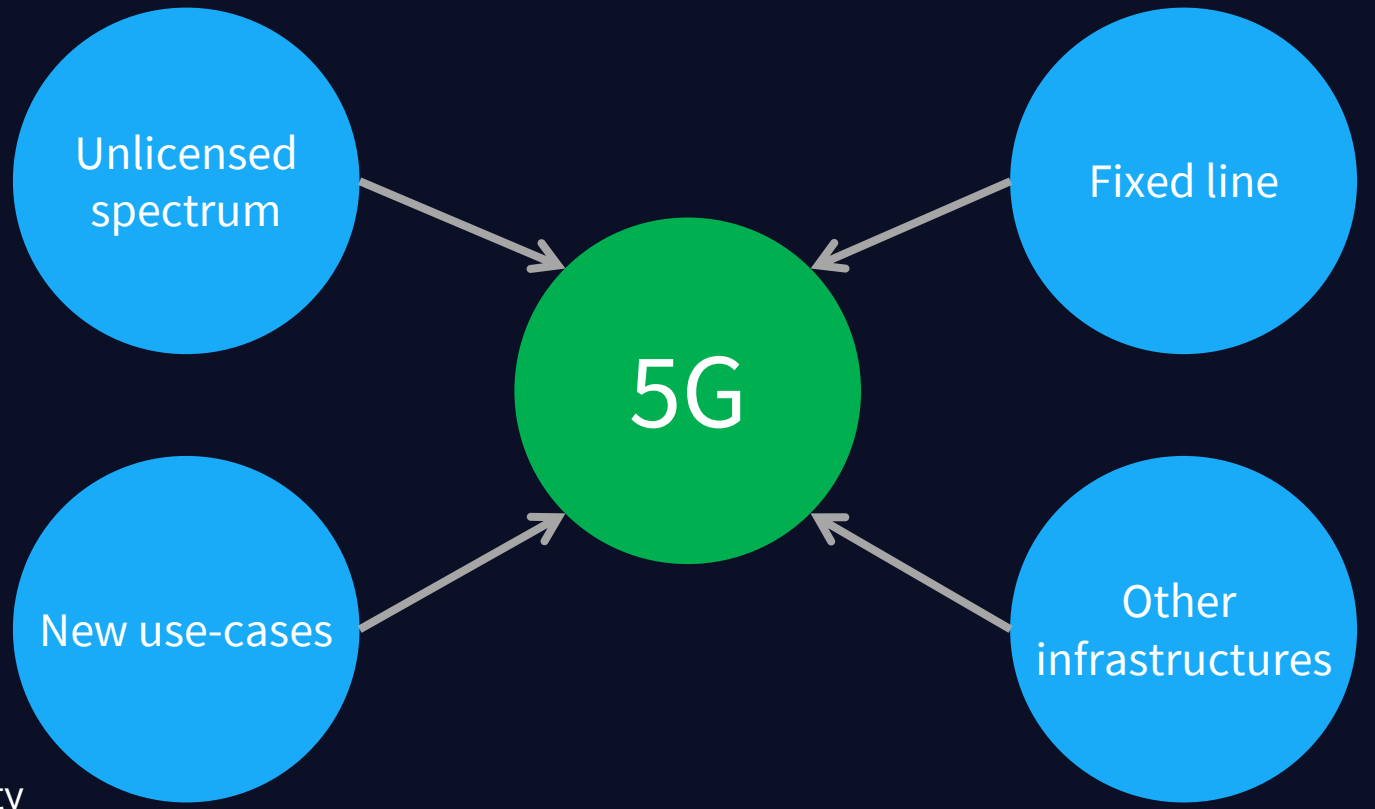
- Includes local cloud environment.
- Alternative is to connect to regional cloud

Edge Offering: Compute and Network, from Edge to Public Cloud



A robust network is required to support the increasing criticality

Consolidation onto 5G – as a techology and as a network – significantly increases criticality



- Wi-Fi
- LoRa/Sigfox

- Copper-based services (xDSL)

- Industrial
- AR/VR
- Gaming
- Digitalisation and connectivity for *everything*

- *Nødnett*
- Defense
- GSM-R
- Industrial networks

Telenor har mål om å bygge verdens mest hardføre nett – innføring av doble linjeføringer (dual-homing)

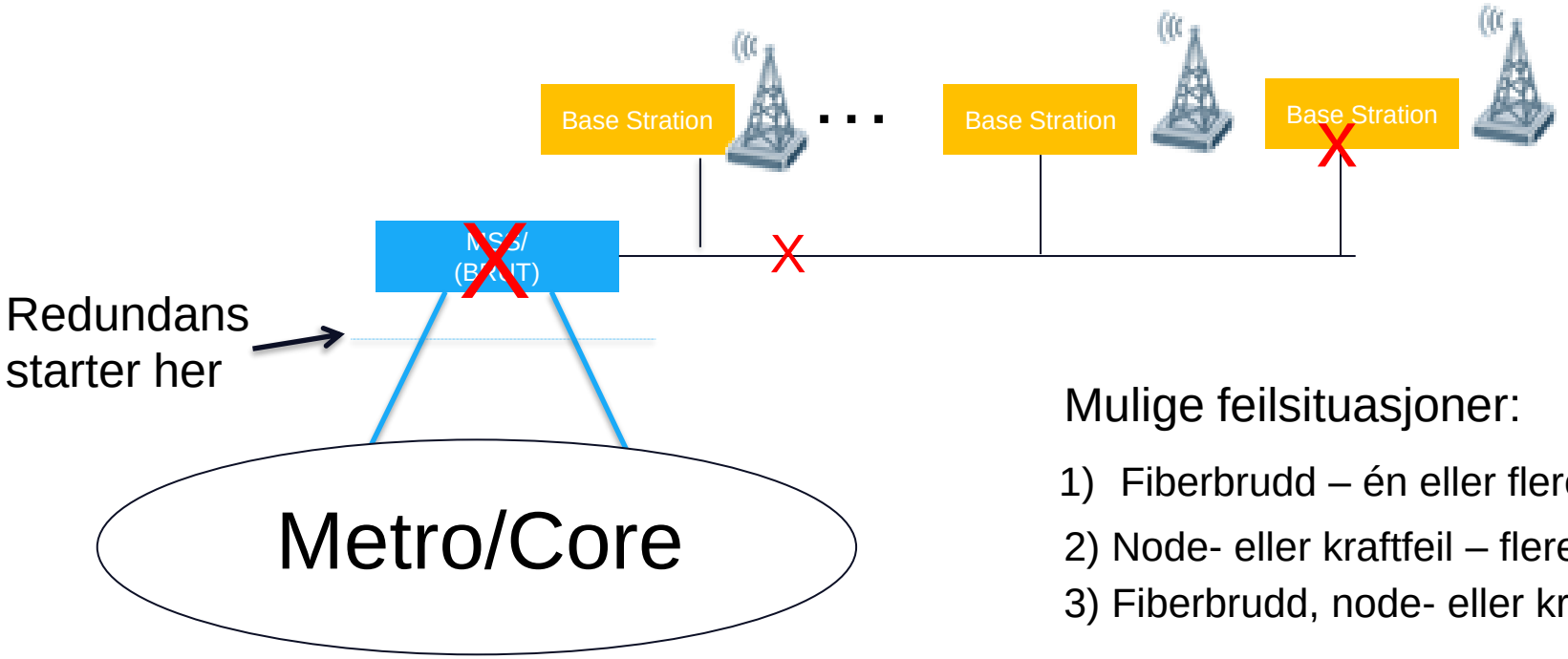
Telenor-5G på Elverum

Foto: Martin Phillip Fjellanger

Utfordringen: Økt krav om høy mobil oppetid

- Økt samfunnsmessig avhengighet av kommunikasjonsløsninger, spesielt mobil
- Utfasing av kobbernettet
- Nye og kritiske anvendelser på 5G – særlig i det offentlige og i næringslivet
- Økende grad av ekstremvær med tilhørende feilsituasjoner

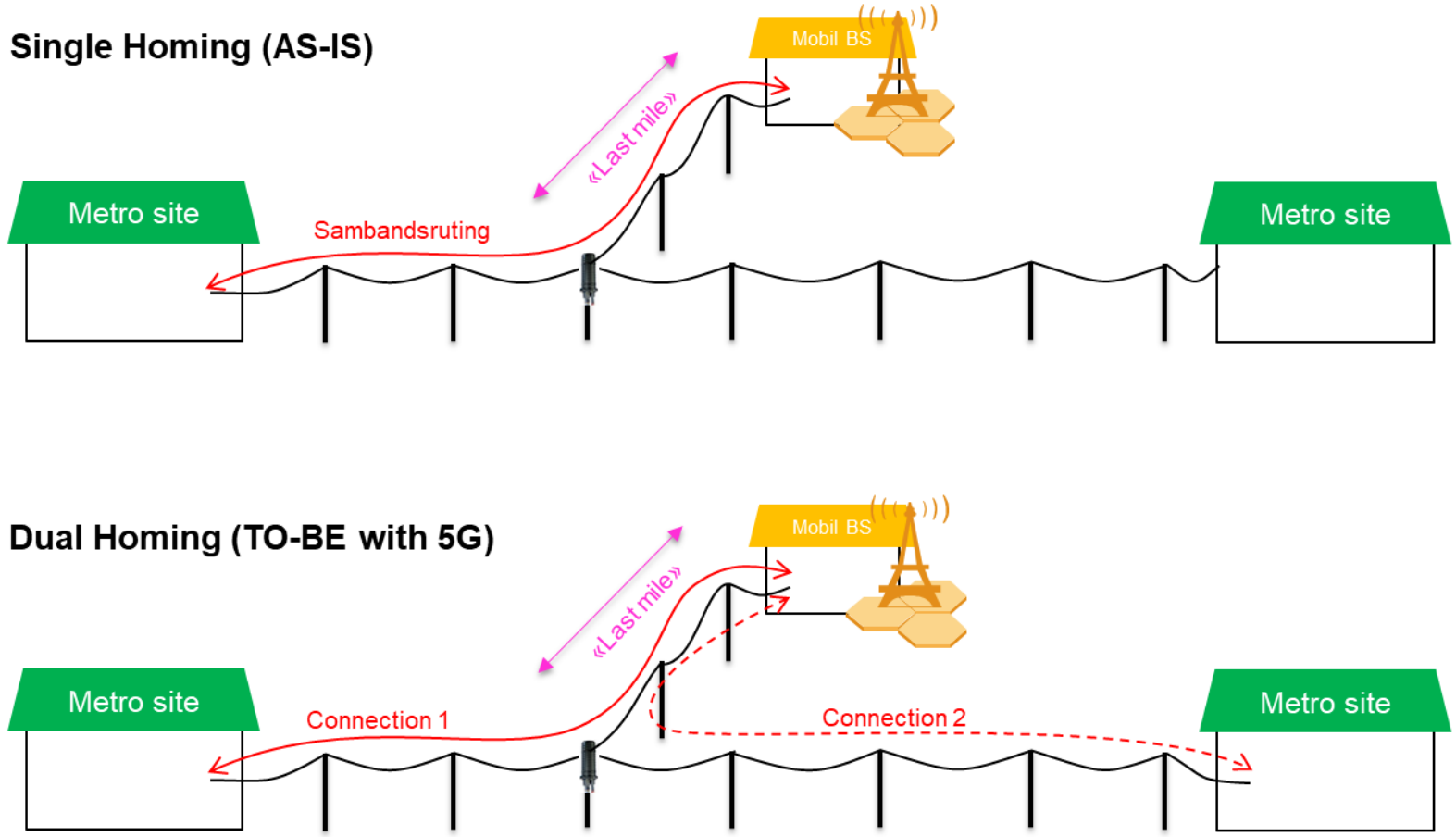
Eksempler på feilsituasjoner med enkel linjeføring



Mulige feilsituasjoner:

1) Fiberbrudd – én eller flere basestasjoner nede
2) Node- eller kraftfeil – flere basestasjoner nede
3) Fiberbrudd, node- eller kraftfeil på basestasjon – 1 nede

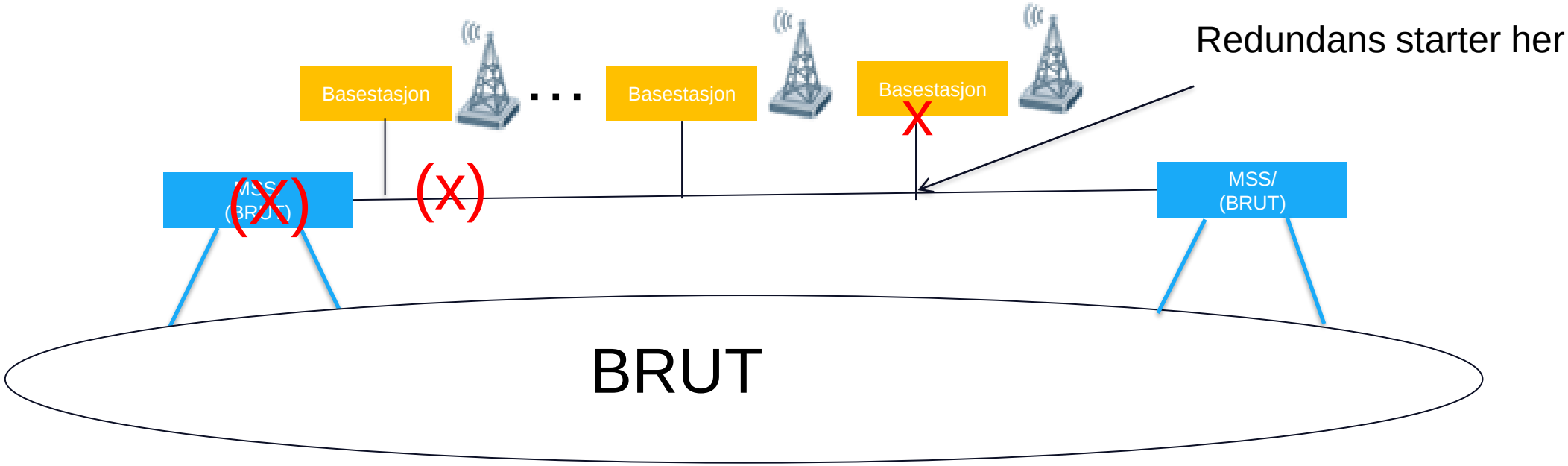
Dobbel linjeføring (dual homing) gir forbedret redundans til basestasionene



To hovedløsninger:

1) Bruk av mørk fiber
2) Bruk av passiv WDM

Eksempler på feilsituasjoner med dobbel linjeføring



Mulige feilsituasjoner

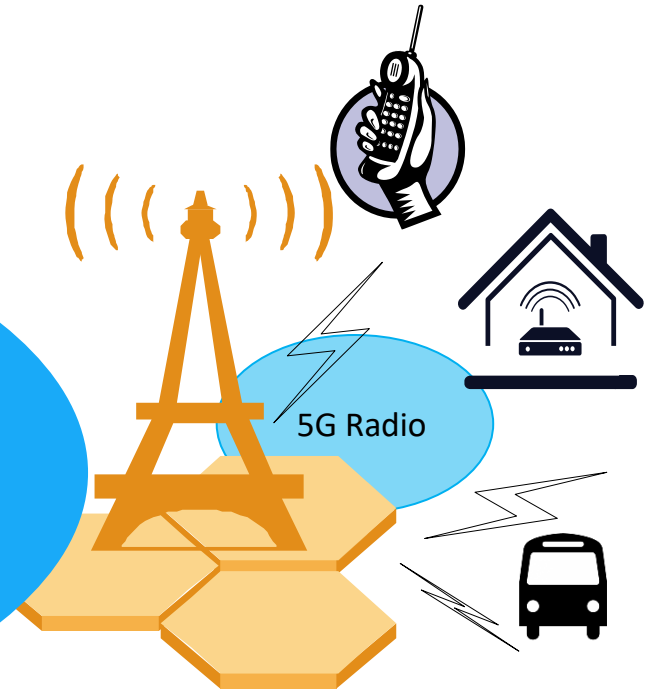
1) Fiberbrudd – ingen kundekonsekvens
2) Node- eller kraftfeil – ingen kundekonsekvens
3) Fiberbrudd, node- eller kraftfeil på basestasjon – 1 nede

5G-utbyggingen: Telenor bygger et modernisert og mer redundant transportnett

Mobilt kjernenett

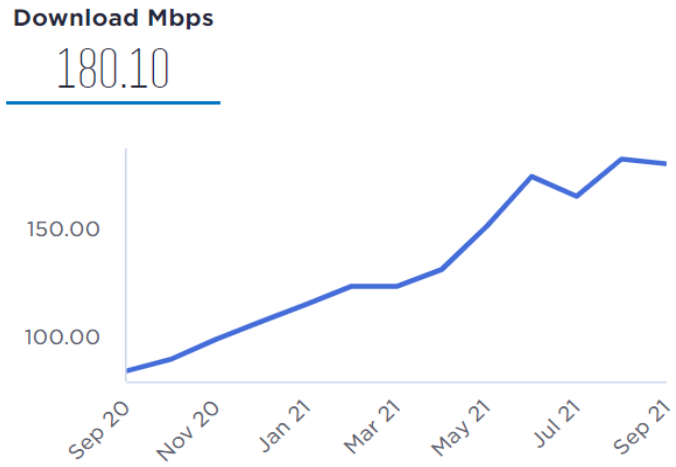
Hovedelementer:

- Økt redundans til basestasjon – Dual Homing
- Høy kapasitet i Metro og Kjerne – 100 Gbit/s
- Høy kapasitet til basestasjon - 10 Gbit/s
- Synkronisering PTP (fase/frekvens – 8275.1)
- Skivedeling mm.

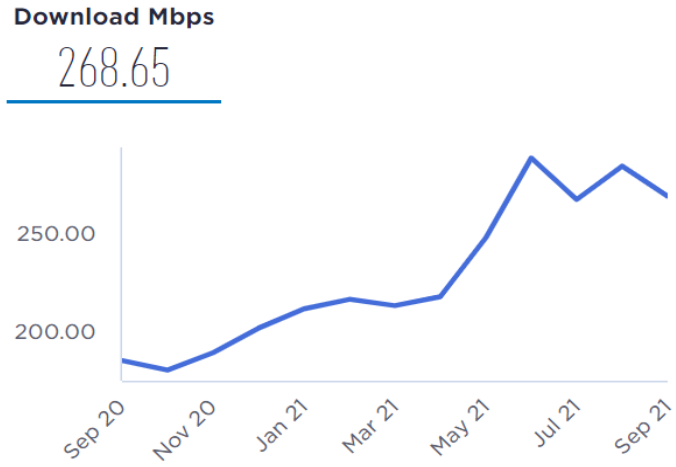


5G Deployment plan 2022

På ett år er brukeropplevelsen i Telenors mobilnett blitt mer enn dobbelt så god



4G/5G 2020 til 2021



4G/5G 2020 til 2021
med 5G-telefon

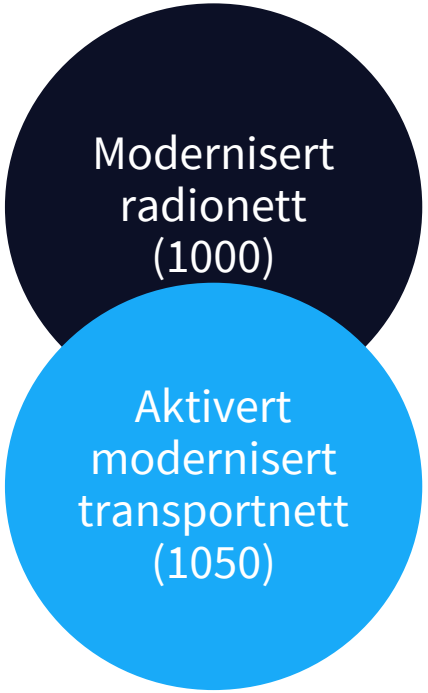
Telenor OPEN

Alle tall hentet fra resultater basert på målinger av brukere av Ookla Speedtest app.

Telenor har modernisert 1000 basestasjoner så langt i 2021

Telenors 5G-utbygging i 2021 er i rute: *Kongsberg, Trondheim, Elverum, Bodø, Fornebu, Kvitfjell, Mausund, Svalbard, Oslo, Askvoll/Flokeneset, Bergen, Stavanger, Ålesund, Tromsø, Kristiansand, Fredrikstad og Drammen.*

For å gi kundene våre 5G må vi oppgradere radionettet og aktivere et nytt transportnett:

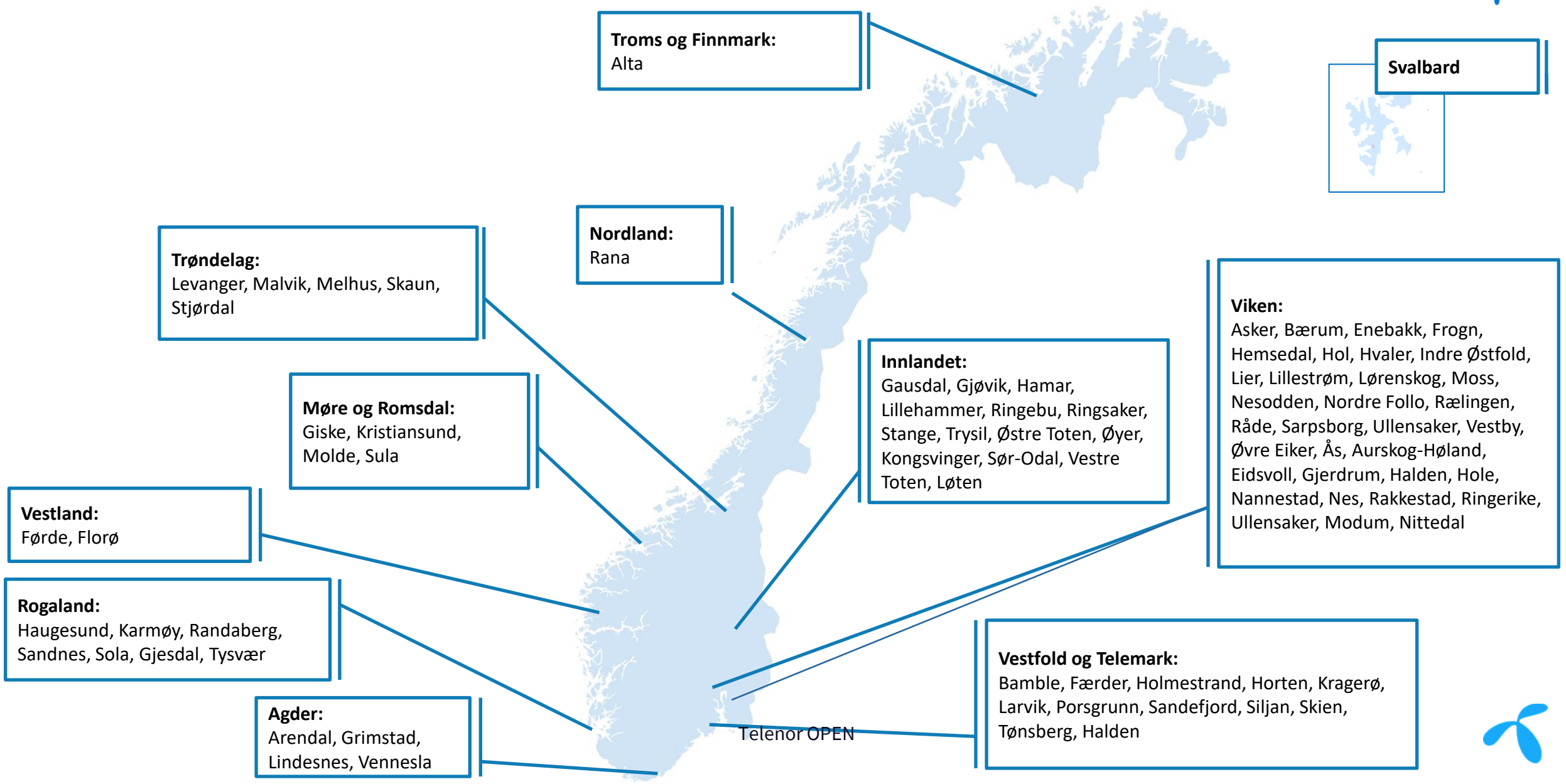


Modernisert radionett gir 5G radioteknologi, men det er ikke nok.

Modernisert transportnett er nødvendig for en god 5G-opplevelse

Mange vil få 5G-dekning utover året på stedene Telenor er i gang med modernisering

Utbyggingsplan 2022: Nye kommuner i alle fylker vil få 5G fra Telenor i 2022



Troms og Finnmark:
Alta

Svalbard

Nordland:
Rana

Trøndelag:
Levanger, Malvik, Melhus, Skaun, Stjørdal

Møre og Romsdal:
Giske, Kristiansund, Molde, Sula

Innlandet:
Gausdal, Gjøvik, Hamar, Lillehammer, Ringebu, Ringsaker, Stange, Trysil, Østre Toten, Øyer, Kongsvinger, Sør-Odal, Vestre Toten, Løten

Viken:
Asker, Bærum, Enebakk, Frogn, Hemsedal, Hol, Hvaler, Indre Østfold, Lier, Lillestrøm, Lørenskog, Moss, Nesodden, Nordre Follo, Rælingen, Råde, Sarpsborg, Ullensaker, Vestby, Øvre Eiker, Ås, Aurskog-Høland, Eidsvoll, Gjerdrum, Halden, Hole, Nannestad, Nes, Rakkestad, Ringerike, Ullensaker, Modum, Nittedal

Vestland:
Førde, Florø

Rogaland:
Haugesund, Karmøy, Randaberg, Sandnes, Sola, Gjesdal, Tysvær

Agder:
Arendal, Grimstad, Lindesnes, Vennesla

Telenor OPEN

Vestfold og Telemark:
Bamble, Færder, Holmestrand, Horten, Kragerø, Larvik, Porsgrunn, Sandefjord, Siljan, Skien, Tønsberg, Halden

Telenor OPEN

Viktig for 2022 er å bygge 5G-dekning på populære ferie- og fritidssteder

Klar før sommeren 2022

Sarpsborg
Arendal
Kragerø
Færder (Nøtterøy/Tjøme)
Larvik
Moss
Sandefjord
Tønsberg
Bamble
Frogn
Hvaler
Råde

Klar for vinteren 2022/2023

Gausdal (Skeikampen)
Hemsedal
Hol (Geilo)
Ringebu (Kvitfjell)
Ringsaker (Sjusjøen)
Trysil
Øyer (Hafjell)
Lillehammer

Innlandet:
Gausdal, Lillehammer, Ringebu, Ringsaker, Trysil, Øyer

Viken:
Frogn, Hemsedal, Hol, Hvaler, Moss, Råde, Sarpsborg, Vestby, Halden

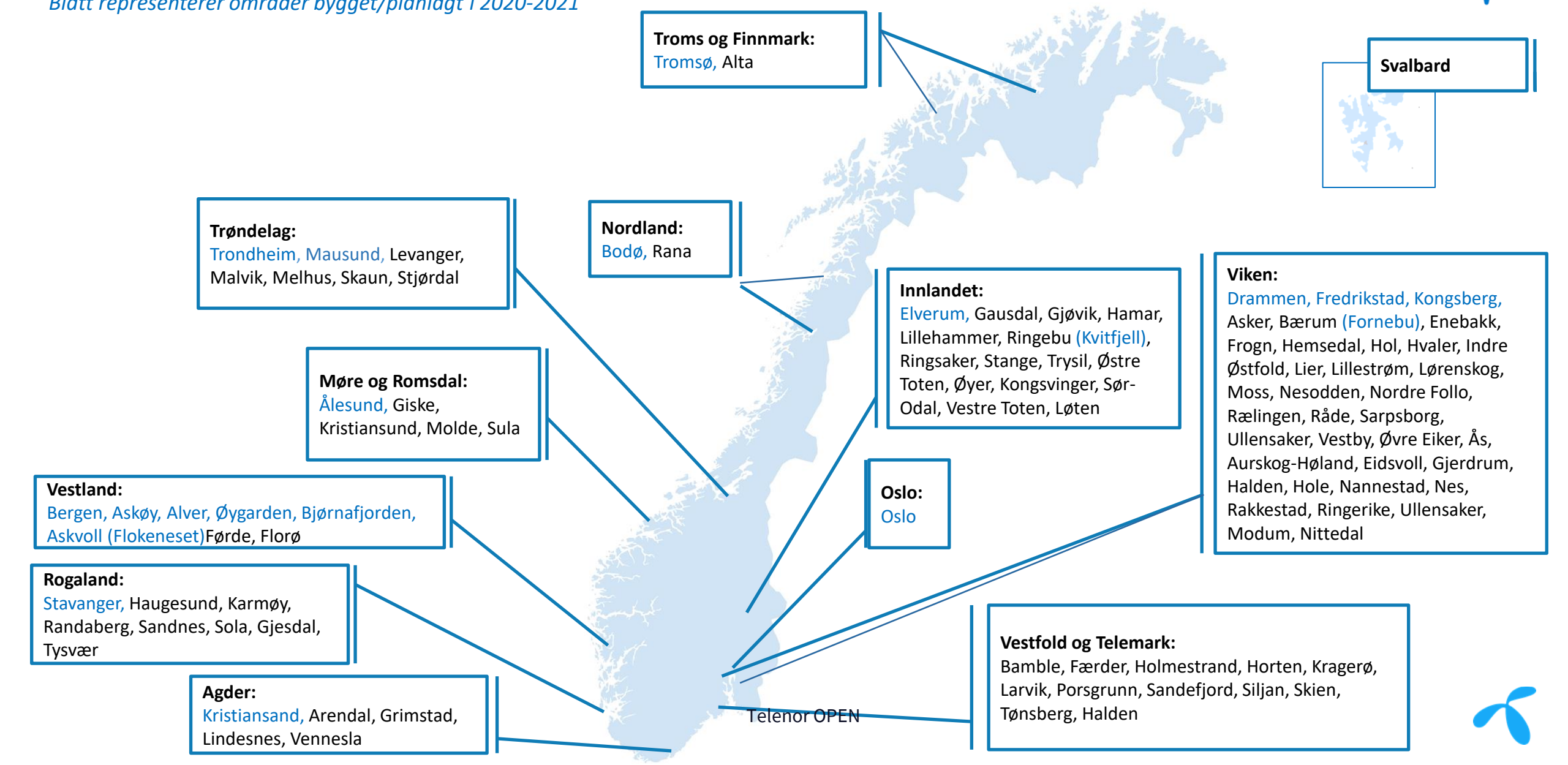
Agder:
Arendal, Grimstad, Lindesnes

Vestfold og Telemark:
Bamble, Færder, Kragerø, Larvik, Sandefjord, Tønsberg, (Skien, Holmestrand, Porsgrunn)

Telenor OPEN

I løpet av 2022 vil disse kommunene ha 5G-dekning fra Telenor

Blått representerer områder bygget/planlagt i 2020-2021



Troms og Finnmark:
Tromsø, Alta

Svalbard

Trøndelag:
Trondheim, Mausund, Levanger, Malvik, Melhus, Skaun, Stjørdal

Nordland:
Bodø, Rana

Innlandet:
Elverum, Gausdal, Gjøvik, Hamar, Lillehammer, Ringebu (Kvitfjell), Ringsaker, Stange, Trysil, Østre Toten, Øyer, Kongsvinger, Sør-Odal, Vestre Toten, Løten

Viken:
Drammen, Fredrikstad, Kongsberg, Asker, Bærum (Fornebu), Enebakk, Frogn, Hemsedal, Hol, Hvaler, Indre Østfold, Lier, Lillestrøm, Lørenskog, Moss, Nesodden, Nordre Follo, Rælingen, Råde, Sarpsborg, Ullensaker, Vestby, Øvre Eiker, Ås, Aurskog-Høland, Eidsvoll, Gjerdrum, Halden, Hole, Nannestad, Nes, Rakkestad, Ringerike, Ullensaker, Modum, Nittedal

Møre og Romsdal:
Ålesund, Giske, Kristiansund, Molde, Sula

Oslo:
Oslo

Vestland:
Bergen, Askøy, Alver, Øygarden, Bjørnafjorden, Askvoll (Flokeneset)Førde, Florø

Rogaland:
Stavanger, Haugesund, Karmøy, Randaberg, Sandnes, Sola, Gjesdal, Tysvær

Vestfold og Telemark:
Bamble, Færder, Holmestrand, Horten, Kragerø, Larvik, Porsgrunn, Sandefjord, Siljan, Skien, Tønsberg, Halden

Agder:
Kristiansand, Arendal, Grimstad, Lindesnes, Vennesla

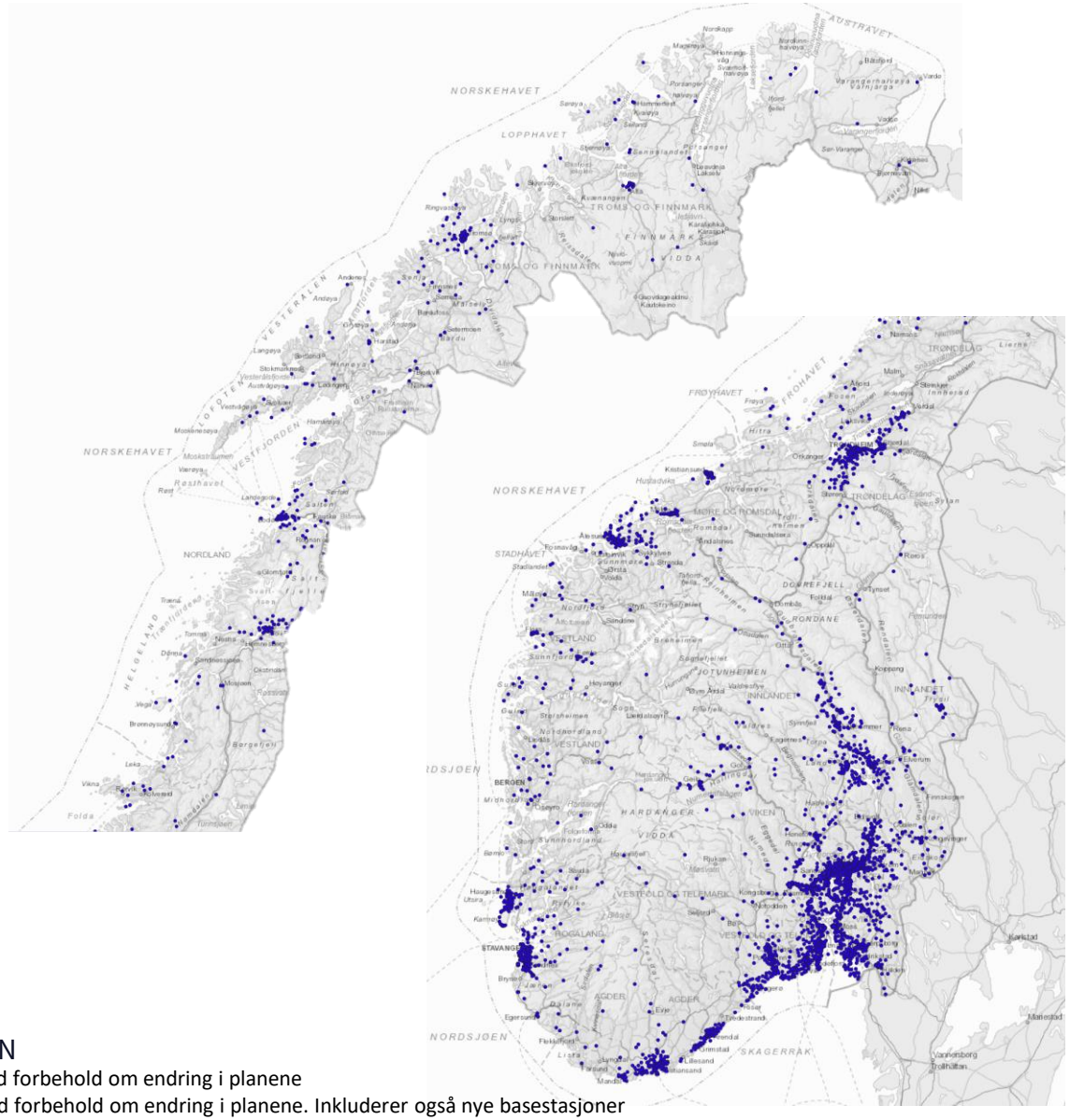
Telenor OPEN

Flere steder vil bli modernisert med 4G og de fleste får 5G – gir et godt bredbåndstilbud til kundene

*I tillegg til utbygging beskrevet i overnevnte slider foreligger plan om oppstart på utrulling av moderniserte basestasjon i inntil 150 kommuner***

ALSTAHAUG	FRØYA	KÅFJORD	OS (INNLANDET)	SØR-AURDAL
ALVDAL	GAMVIK	LESJA	OSTERØY	SØRFOLD
ANDØY	GJERDRUM	LILLESAND	PORSANGER	SØR-FRON
AREMARK	GOL	LOM	RANDABERG	SØRREISA
ASKVOLL	GRAN	LOPPA	RENNEBU	SØR-VARANGER
AUKRA	GRATANGEN	LUND	RISØR	TANA
AURE	GRONG	LUNNER	ROLLAG	TIME
AURLAND	GULEN	LUSTER	RØROS	TVEDESTRAND
AUSTEVOLL	HADSEL	LYNGEN	SALTDAL	TYNSET
AUSTRHEIM	HAMMERFEST	LÆRDAL	SAMNANGER	TYSVÆR
BALSFJORD	HAREID	MARKER	SAUDA	ULLENSVANG
BARDU	HARSTAD	MASFJORDEN	SEL	ULSTEIN
BEIARN	HATTFJELLDAL	MIDTRE GAULDAL	SELJORD	VADSØ
BINDAL	HITRA	MIDT-TELEMARK	SENJA	VARDØ
BIRKENES	HJELMELAND	MODALEN	SIGDAL	VEFSN
BRØNNØY	HOLE	MODUM	SILJAN	VEGA
BØMLO	HURDAL	MOSKENES	SIRDAL	VENNESLA
DOVRE	HUSTADVIKA	MÅLSELV	SKIPTVET	VERDAL
DØNNA	HYLLESTAD	NAMSOS	SKJERVØY	VESTRE SLIDRE
EIDFJORD	HØYANGER	NAMSSKOGAN	SKJÅK	VESTVÅGØY
EIDSKOG	HØYLANDET	NANNESTAD	SOKNDAL	VINJE
EIGERSUND	HÅ	NARVIK	STAD	VOSS
ENGERDAL	IVELAND	NESBYEN	STEIGEN	VÅGAN
EVJE OG HORNNES	JEVNAKER	NOME	STEINKJER	VÅGÅ
FARSUND	KARASJOK	NORD-FRON	STORFJORD	VÅLER (VIKEN)
FAUSKE	KARLSØY	NORD-ODAL	STRAND	ØKSNES
FJORD	KLEPP	NORDRE LAND	STRANDA	ØRLAND
FLATANGER	KRØDSHERAD	NORE OG UVDAL	STRYN	ØYSTRE SLIDRE
FLEKKEFJORD	KVAM	NOTODDEN	SULDAL	ÅFJORD
FLESBERG	KVINESDAL	OPPDAL	SYKKYLVEN	ÅL
FLÅ	KVINNHERAD	ORKLAND	SØNDRE LAND	ÅMOT
FROSTAD	KVÆNANGEN			ÅSNES

Kartet under viser total utbyggingsplan 2020 – 2022*



Telenor OPEN

* Med forbehold om endring i planene

* Med forbehold om endring i planene. Inkluderer også nye basestasjoner

Telenor-5G i hele Norge

5G i hele nettet i løpet av første halvår 2024

Går fra 8400 basestasjoner til 9000

So…


Is it safe?

5G Security – Bottom Line

- **5G (3GPP) is by far the most secure cellular technology specification we have ever had!**
  - Specified with security in mind from the ground up
  - Built on proven constructs and concepts
  - The entire industry is more security-aware, -conscious and –competent than ever
  - The ability to provide security suited to support the *connected society* is an imperative
- **5G is by far the most challenging generation of mobile infrastructure to secure!**
  - Complexity
  - Layered virtualisation
  - Integrations and exposures
  - Distributed functions
  - Rate of change
  - Agility and vulnerability management
  - Prevalence and volume of machine-type terminals
  - Variety of use cases
- **Pervasive digitalisation and interconnectedness enabled by 5G, brings new dependencies, increases criticality and expands the attack surface.**

Embrace 5G! **Seek a competent partner!**

telenor

telenor

Rolv R. Hauge

Head of Advisory and Architecture, Security, Telenor Norway, Business div.

+47 91138287

rolv.hauge@telenor.no