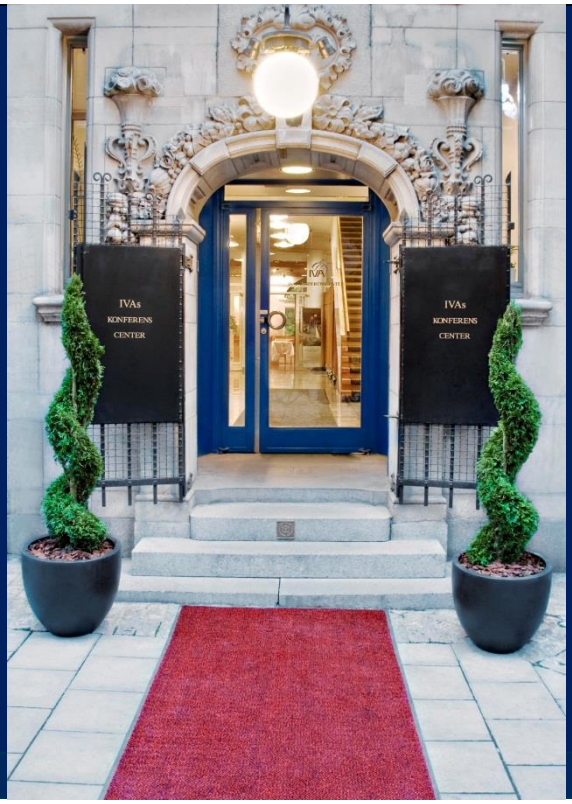
Draft program: PA4

Broadband for all

- a trusted base for the digitalization of our societies



Seminar
June 25-26, 2018
Stockholm

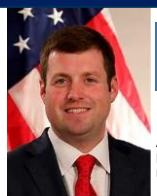
Location
Royal Swedish Academy of Engineering Sciences (IVA)
Grev Turegatan 16
Stockholm

- In a 5G world where industries and societies transform, which new requirements will emerge on spectrum regimes and other regulations?
- Which are the most significant policy actions in the Cyber-security area that national governments need to prioritize? What are the lessons learned to improve the effectiveness of policy implementation?
- What are the perspectives and best practices for successful broadband policies and regulations?
- In 2017, the seminar gathered 80 Government & Regulator representatives from 30 countries on all continents.

With contributions from the following speakers

PTS

Dan Sjöblom
Director-General
PTS, Sweden



NTIA

David Redl
Assistant Secretary, NTIA
Department of Commerce, United States

arcep

Pierre-Jean Benghozi
Board Member
ARCEP, France

National Cyber Security Centre
a part of GCHQ

Ian Levy
Technical Director
NCSC, United Kingdom

ERICSSON

Erik Ekudden
SVP & CTO
Ericsson

Seminar – Morning session

Monday June 25, 2018

08:00 - 08:30 Registration and morning tea - networking

08:30 - 10:00 Welcome and introduction
- Ulf Pehrsson, Vice President Government & Industry Relations, Ericsson

Keynote: Perspectives from United States
- David Redl, Assistant Secretary, NTIA, Department of Commerce, United States

Keynote: Perspectives from France
- Pierre-Jean Benghozi, Board member, ARCEP, France

Keynote: Technology strategies and trends
- Erik Ekudden, Senior Vice President & CTO, Ericsson

10:00 - 10:30 Coffee break - networking

10:30 - 11:00 Keynote: Perspectives on Cyber-security
- Ian Levy, Technical Director, National Cyber Security Center (GCHQ), United Kingdom

11:00 - 12:00 Panel debate: Which are the most significant policy actions in the Cyber-security area that national governments need to prioritize? What are the lessons learned to improve the effectiveness of policy implementation?

Chair: Rene Summer, Director, Government and Industry Relations, Ericsson
- Ian Levy, Technical Director, National Cyber Security Center (GCHQ), United Kingdom
- NN, title, affiliation, Country
- NN, title, affiliation, Country
- NN, title, affiliation, Country

12:00 - 13:30 Lunch - networking

Chatham House Rule

Seminar – Afternoon session

Monday June 25, 2018

13:30 - 15:30

Broadband for all in Sweden
- Dan Sjöblom, Director-General, PTS, Sweden

Broadband for all in Country X
- NN, title, affiliation, Country X

Broadband for all in Country Y
- NN, title, affiliation, Country Y

Implementing the Port of the Future: the digital agenda at the Port of Livorno
- Paolo Pagano, Director of CNIT / Port of Livorno joint laboratory, Italy

15:30 - 16:00

Coffee break - networking

16:00 - 17:00

Panel debate: Can we secure spectrum for the 5G introduction and in the perspective of longer-term?

Chair: Lasse Wieweg, Director, Government & Industry Relations, Ericsson
- Antonio Nicita, Commissioner, AGCOM, Italy
- NN, title, affiliation, Country
- NN, title, affiliation, Country
- NN, title, affiliation, Country

17:00 – 17:10

Concluding remarks
- Ulf Pehrsson, Vice President Government & Industry Relations, Ericsson

17:30 – 21:45

Dinner networking cruise on M/S Blue Charm. Boarding: Strandvägen, Quay 17 at 17:30. Departure 18:00 sharp.

Chatham House Rule

Bilateral meetings

Tuesday June 26, 2018

We are pleased to offer a number of activities that you can select from to match your interests and thereby ensure maximum value of your visit to Stockholm. On request we can also arrange for other meetings to respond to specific needs.

Your individual program will be created based on your choice of activities:

- Bilateral meeting with the **Swedish Regulator PTS**
- Dialogue about the **ITU leading up to the WRC-19**
- 40 min bilateral meetings with **Ericsson experts** in the fields of spectrum, technology and cyber security
- A three hour **Technology Briefing** including technology demonstrations
- A one and a half hour **PTS Seminar** on spectrum
- A two hour **Seminar** on Cyber-security issues in a 5G context

PTS

Valhallavägen 117
Stockholm City

09:00 – 17:00 PTS Headquarter	PTS bilateral meeting – regulations (general) - Dan Sjöblom, Director-General, PTS

Ericsson

Ericsson Studio
Grönlandsgatan 8
Kista, Stockholm

08:00 – 09:00 Room: Operation Center	Dialogue about the ITU study period leading up to the WRC-19 - Håkan Ohlsén, Director, Spectrum and Radio Technology Strategy, Ericsson - Lasse Wieweg, Director, Government & Industry Relations, Ericsson
09:00 – 12:00 Room: Jeanne	PTS bilateral meeting – regulations (spectrum) – 40 min - Jonas Wessel, Director of Spectrum Department, PTS - Bo Andersson, Chief Economist, PTS
09:00 – 12:00 Room: Diana	Bilateral meeting – Meet Ericsson's Cyber-security experts – 40 min - Mikko Karikytö, Head of Ericsson Network Security - Anna Kåhre, Strategic Product Management Radio Access Networks - Patrik Palm, Portfolio Manager Security
09:00 – 17:00 Room: Niklas	Bilateral meeting – Spectrum & technologies – 40 min - Håkan Ohlsén, Director, Spectrum and Radio Technology Strategy, Ericsson - Lasse Wieweg, Director, Government & Industry Relations, Ericsson
12:00 – 13:00	Lunch is served at the Ericsson Studio

Chatham House Rule

5G Technology briefing

Tuesday June 26, 2018

Ericsson
Ericsson Studio
Grönlandsgatan 8
Kista, Stockholm

Room:
Forum

09:00 - 12:00

A digital transformation is taking place in almost every industry. 5G will expand the broadband capability of mobile networks and help consumers and enterprises boost the efficiency of their lives and their business. New business models using distributed cloud services and programmable networks will allow an unprecedented level of information sharing and collaboration among all kinds of industries and sectors in society. The result is an unprecedented capacity for individual empowerment, entrepreneurship and innovation as well as a vehicle for entire industries to transform, that gives rise to a new era - the connected society.

This transformation will put new demands on the networks, with requirements varying radically between different use cases but also between different devices. The imminent 5G mobile network systems – will provide global, wireless, connectivity with superior performance for people and machines, with capabilities to handle very large data rates and data volumes, while being very reliable to allow for critical industrial and societal applications. The 5G systems also need to accommodate for IoT devices with limited capabilities where device cost, power consumption or coverage (range) are among the key properties.

This briefing will address the latest developments in 5G research & network evolution to meet the future requirements on user services and network efficiencies, as well as, offer insights into the EMF area related to the introduction of 5G.

08:30 - 09:00	Registration and morning tea
09:00 - 09:10	Welcome and introduction - Mikael Halén, Director, Government & Industry Relations
09:10 - 09:40	5G and network slicing - Håkan Djuphammar, Technology & Architecture, CTO Office
09:40 - 10:10	5G and radio network efficiency - Magnus Frodigh, Research Director, Ericsson Research
10:10 - 10:30	Coffee break and networking
10:30 - 11:00	5G and EMF - Christer Törnevik, Senior expert, Ericsson Research
11:00 - 12:00	5G Technology demonstrations
12:00 - 13:00	Lunch is served at the Ericsson Studio

Chatham House Rule

PTS Spectrum seminar

Tuesday June 26, 2018

Ericsson
Ericsson Studio
Grönlandsgatan 8
Kista, Stockholm

Room:
Operations Center

13:00 - 14:30

Sweden is one of the leading countries when it comes to progressive spectrum management. The Swedish market is in many regards unique even though it shares many regulatory challenges with the rest of the world. The Radio Spectrum Policy Group (RSPG) is the key EU advisor consisting of the relevant authorities from all 28 EU member states.

5G is one of the key areas of work for European spectrum managers, both nationally, regionally and globally. During this seminar PTS will share the latest news and information on what is happening on EU and national level when it comes to spectrum to enable 5G. There will also be time for a Q&A session.

- The need for harmonization and long term policy on spectrum issues
- Spectrum for 5G on national, regional and global level
- Identification of spectrum related challenges such as spectrum sharing, usage and licensing
- The Swedish large scale 5G test and trial plan

13:00 - 13:30	Jonas Wessel, Director of Spectrum Department, Swedish Post and Telecom Authority, PTS and Chairman, Radio Spectrum Policy Group, RSPG
13:30 - 14:00	Bo Andersson, Chief Economist, Swedish Post and Telecom Authority, PTS Rapporteur RSPG working group on 5G
14:00 - 14:30	Q&A and discussion

Chatham House Rule

Seminar:

Cyber-security in a 5G context

Tuesday June 26, 2018

Ericsson
Ericsson Studio
Grönlandsgatan 8
Kista, Stockholm

Room:
Hiba

13:00 - 15:00

Connected devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy, and the 5G system is designed with these requirements in mind. This seminar provides an overview of the properties that contribute to the trustworthiness of the 5G system: resilience, communication security, identity management, privacy and security assurance. Ericsson believes that these properties of the 5G system contribute toward creating a trustworthy communications platform that is an ideal foundation on which to build large-scale, security-sensitive systems, including those used in industrial settings.

Moderator: Rene Summer, Director, Government & Industry Relations, Ericsson

Introduction: Rene Summer:

Presenter #1: **Network Cyber-security threats**
Mikko Karikytö, Head of Ericsson Network Security (30 min including discussion.
As part of the critical infrastructure, an operator today faces multitude of cyber threats. In today's presentation we will describe the threat landscape from Ericsson Product Security Incident Response Team (PSIRT) point of view. We will also present our analysis on common risks identified in PSIRT investigations.

Presenter #2: **5G Security evolution**
Anna Kåhre, Strategic Product Management Radio Access Networks, Ericsson
(30 min including discussion)

Presenter #3: **Ericsson approach to enhancing cyber resilience in products & solutions**
Patrik Palm, Portfolio Manager Security (30 min including discussion)
In order to meet the continuously growing demands on cyber resilience in the products and solutions in the Ericsson portfolio, we have created the Ericsson Security Reliability Model as our company-wide approach. This model is well aligned with the efforts in 3GPP and GSMA focusing on Security Assurance, and is also aligned with the EU security certification efforts. Vulnerability management from components to solutions is an essential building block in mitigating existing and potential threats.

Conclusions: Rene Summer, Director, Government & Industry Relations, Ericsson

Chatham House Rule

The program is arranged by Ericsson

BEREC perspectives on broadband policy and 5G

Jeremy Godfrey
- BEREC Vice-Chair 2018 & Incoming BEREC Chair 2019
- ComReg (Ireland) Commissioner

Stockholm, 25 June 2018

Body of European Regulators for Electronic Communications

BEREC

Body of European Regulators for Electronic Communications
BEREC

Overview

- **BEREC's role in Broadband for All**
- **BEREC and broadband**
- **BEREC and 5G**
- **BEREC in 2019**

Body of European Regulators
for Electronic Communications
BEREC

BEREC's role in Broadband for All

Body of European Regulators for Electronic Communications
BEREC

BEREC's role

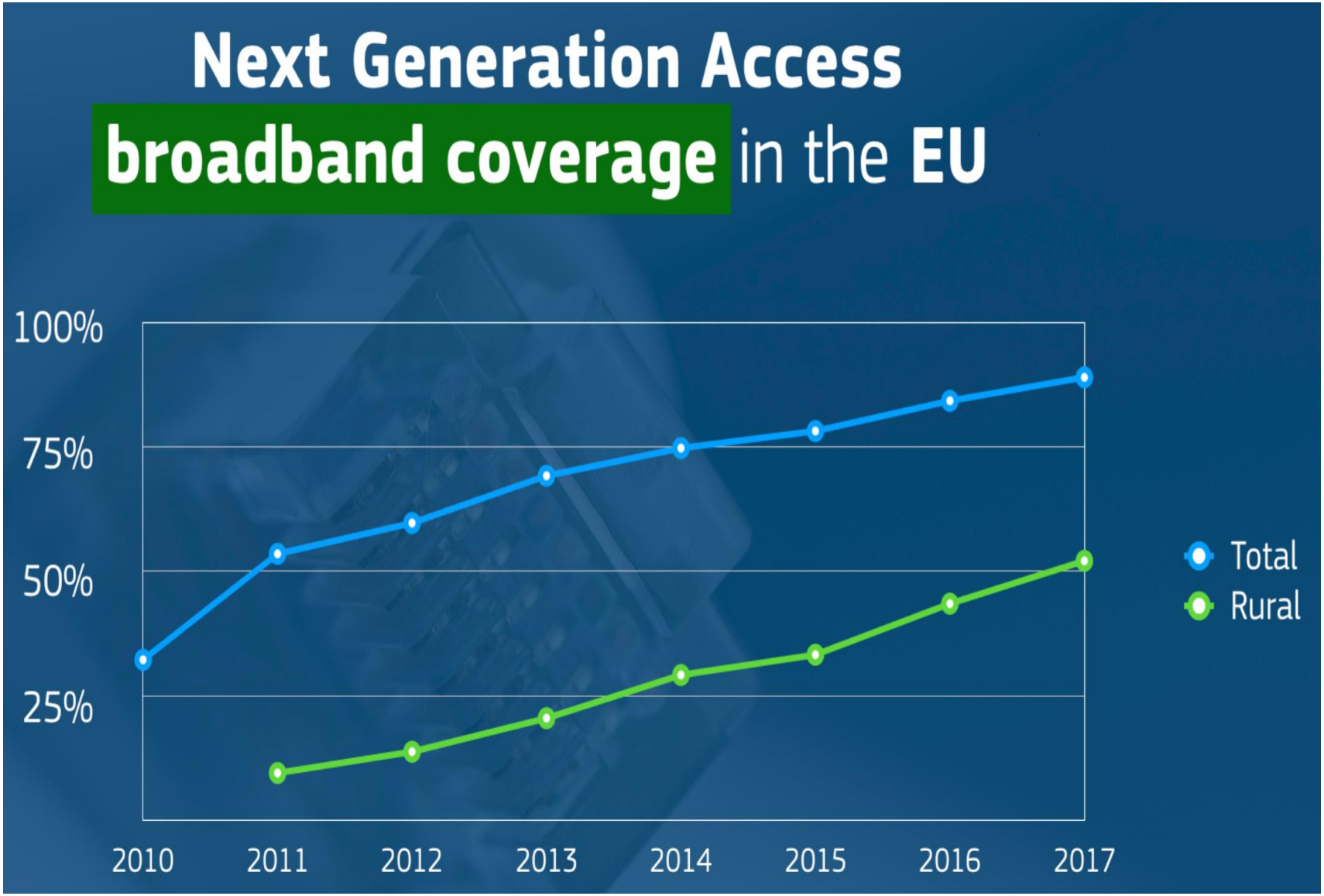
- Coordinate implementation of the European telecom framework
- Guidelines, best practices, benchmarking, reports
- Experts from national regulatory authorities
- Promote competition & investment, internal market, end-user interests
- ***New*** for 2019 - connectivity
- Strategic priorities:
  - High capacity networks
  - Bottlenecks in access to digital services
  - 5G
  - Net neutrality
  - Consumer empowerment
- 5G is particular focus in 2018

Body of European Regulators
for Electronic Communications
BEREC

BEREC perspectives on broadband policy

Body of European Regulators for Electronic Communications
BEREC

Broadband trends in Europe



Body of European Regulators for Electronic Communications
BEREC

BEREC, broadband and the EECC

- Impact of regulation on investment a major theme of discussions on new European code

- BEREC view
  - Geography and history matter
  - Competition drives investment and innovation

- BEREC workstreams in 2018:
  - Pricing for access to infrastructure and civil works (P3)
  - BEREC Report on access to physical infrastructure in market analyses (P4)
  - BEREC Report on geographical market definition (P4)

- Possible work in 2019 and beyond
  - Guidelines on co-investment, “symmetric regulation”, coverage mapping etc
  - Study on dynamics of investment and. Innovation

Body of European Regulators
for Electronic Communications
BEREC

BEREC perspectives on 5G

Body of European Regulators for Electronic Communications
BEREC

BEREC and 5G

"We have many topics to work on, but all designed to identify and eliminate hurdles to fast 5G deployment and if existing practices are adequate for 5G" - Johannes Gungl, BEREC Chair 2018

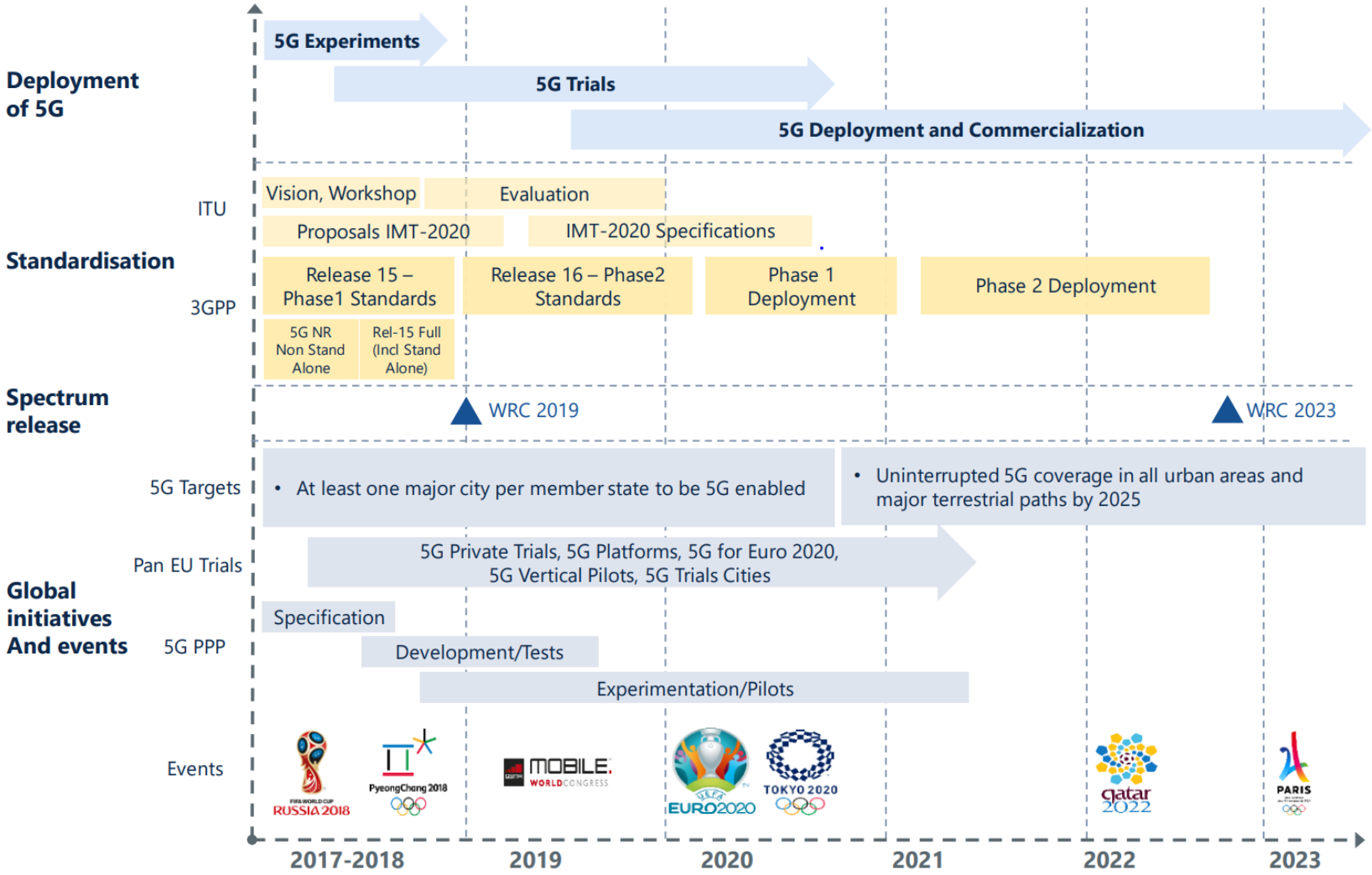
Body of European Regulators for Electronic Communications
BEREC

DotEcon / Axon study

- Interviews with operators, regulators, manufacturers, verticals
- Initial deployment evolutionary not revolutionary - both eMBB and verticals
- But potentially significant changes:
  - Small cells
  - Non-traditional operators focusing on cell densification
  - Network slicing
- Fast rollout requires both spectrum and facilitation of small cells
- A range of other regulatory issues, including
  - Coverage
  - Competition and market structure
  - Backhaul
  - Edge computing
  - Net Neutrality
  - Quality of service

Body of European Regulators for Electronic Communications
BEREC

5G: the next 5 years



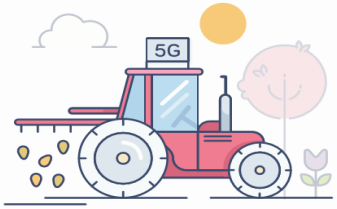
Body of European Regulators for Electronic Communications
BEREC

BEREC and 5G in 2018

BEREC FACILITATES A FAST AND SMOOTH DEPLOYMENT OF 5G IN EUROPE

PREPARE
the 5G landscape

5G is based on small cells, meaning more base stations are needed for it to work properly. To help minimise the cost and boost the speed of 5G deployment, BEREC will gather best practices in infrastructure sharing across Europe. It will publish a **Report on Infrastructure Sharing** and adopt a **Common Position**.



SOW
the seeds of 5G in Europe

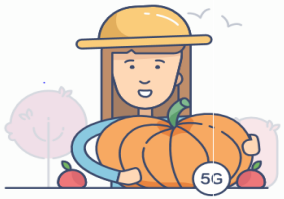
For 5G deployment, spectrum needs to be assigned. Member States may have different spectrum available and use different ways to assign it. To help each country to pick the most suitable procedure for its market, BEREC will publish a **Report on Spectrum Authorisation and Award Procedures**.

HELP
the crop of 5G grow

Citizens and companies should benefit from reliable 5G services. Coverage obligations can help to ensure the wide availability of 5G, especially in challenge areas like rural regions, indoors or along transportation networks. A **Best Practices Report on Coverage Obligations** by BEREC will help Europe to foster a fertile 5G deployment.

MONITOR
the development of 5G

There are clear benefits to achieving a common understanding of how to monitor mobile coverage. A BEREC **Common Position on Monitoring Mobile Coverage** will facilitate a mutual understanding and foster a consistent approach on how this information can be made available and understandable throughout Europe.



HARVEST
the bountiful 5G crop

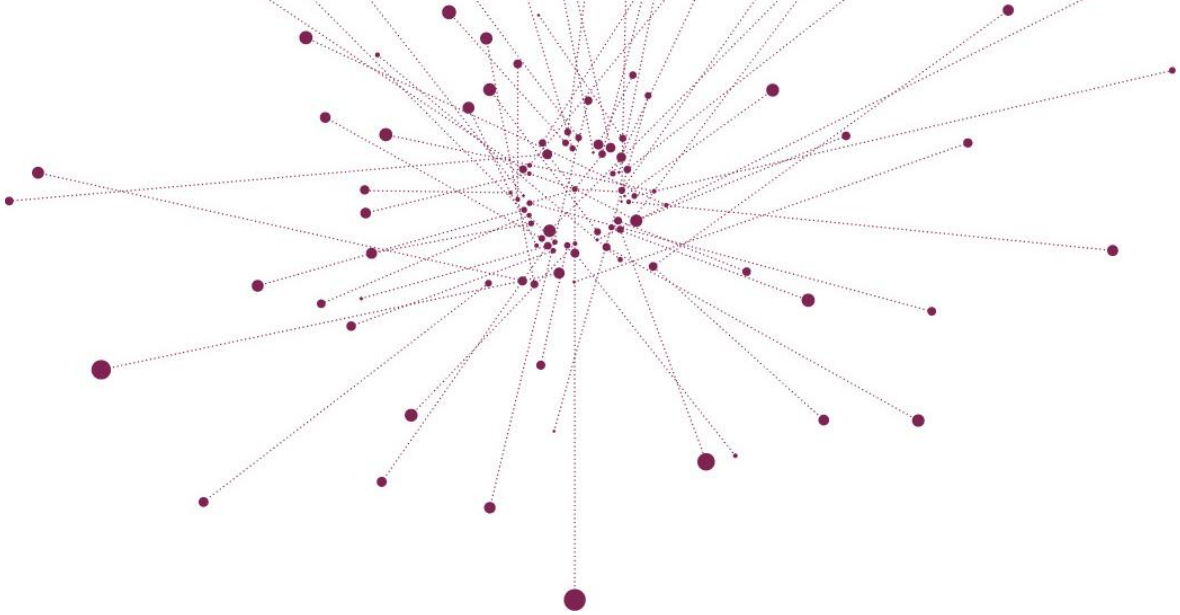
With its work, BEREC will help to prepare a fertile landscape for 5G deployment. The next step is for citizens and operators to harvest the 5G crop, maximising the potential that 5G has to offer. Completely new business models, high speed internet everywhere and smart homes are just the beginning.

Body of European Regulators for Electronic Communications
BEREC

Body of European Regulators for Electronic Communications
BEREC

BEREC in 2019

- 5G will still be to the forefront of BEREC's 2019 work
- 3 potential 5G related reports in 2019 for BEREC:
  - Impact of 5G on regulation and role of regulation in enabling 5G ecosystem
  - Cost of rolling out 5G in EU
  - 5G's impact on definition, measurement and communication of mobile QoS
- Public Consultation & Stakeholder Forum on BEREC Work Programme 2019 in October; to be adopted in December 2018.
- 2019 is an important year for BEREC: the EECC and also BEREC's 10th anniversary.



Thank you!

Body of European Regulators
for Electronic Communications

BEREC

सत्यमेव जयते

Broadband for all : Perspective from India

Presenters:
Mr. Anil Kumar Gupta
Mr. Pramod Kumar Panda

BBNL
ACCESS ACROSS INDIA
भारत ब्रॉडबैंड नेटवर्क लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT BROADBAND NETWORK LIMITED
(A Govt. of India Undertaking)

Administrative Structure of India

29 states and 7 union territories

644 Districts

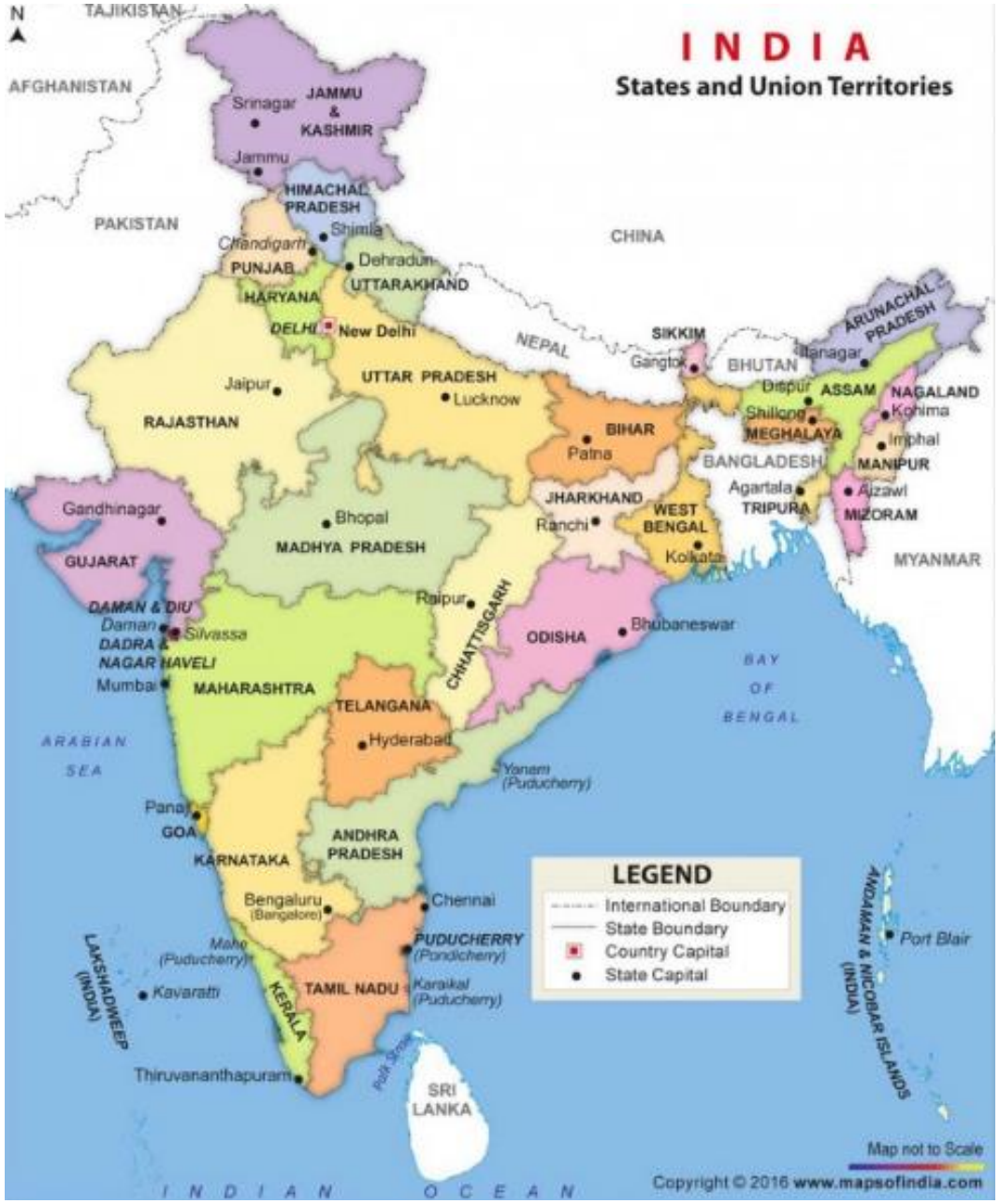
5500 Block(s)

Block is a district sub-division for the purpose of Rural development

2,50,00 Village Panchayat(s)

A Village Panchayat is the local self-government organisation. To implement the development programmes

6,40,867 Villages



Broadband Subscription Data

- India's telecommunication network is the second largest in the world by number of telephone users (both fixed and mobile phone) with 1.206 billion subscribers as on 31 March 2018.
- Wireless telephony constitutes 98.04% (1186.21 million) of all subscriptions whereas share of the landline telephony now stands at only 1.96% (23.75 million) at the end of August, 2017.
- As on 30 March 2018, India has the world's second-largest Internet user-base with 412.60 million internet subscribers in the country.

Particulars	Unit of Measurement	Wireless	Wireline	Total
Broadband Subscribers	**Million**	**266**	**18**	**284**
Telephone Subscribers	**Million**	**1175**	**24**	**1199**
Urban		*675*	*21*	*696*
Rural		*499*	*4*	*503*
Overall Tele-density	**91.90**			
Urban Tele-density	*168.29*			
Rural Tele-density	*56.66*			

Future Plans

- **BharatNet** to Cover over 2.5 Lakh Villages by March 2019.

- **National Digital Communications Policy 2018**, in May, laid out plans to attract investments of $100 billion by 2022, creating 4 million additional jobs and enhance the sector's contribution to 8% of India's GDP from about 6% in 2017.

- The investment target includes the development of a digital ecosystem to be driven by the transition to **5G technology**.

- The **Department of Telecommunications** plans to price spectrum optimally, review levies such as licence fees and spectrum usage charges, ease the exit of companies and take a fresh look at spectrum sharing, leasing and trading guidelines. Thus enabling the industry to grow and contribute towards the growth of the country's GDP.

Broadband for All - Rural

- **2,50,000 Village Panchayats** would be covered under the **BharatNet project**.

- Department of Telecommunications (DoT) is the nodal Department for this project

- Bharat Broadband Network Limited (BBNL) is the executing agency.

BharatNet Project Highlights

- World's largest rural broadband connectivity project through optical fibre
- All 2,50,000 Village Panchayats in India to be connected on optical fibre
- 100 Mbps bandwidth at each Village Panchayat scalable to 1 Gbps
- Non discriminatory Access infrastructure for all Service Providers
- Approx. 6,00,000 Kms of new incremental optical fiber cable to be laid
- High capacity Network Management System and Network Operation Centre

Building a Strong Pulse

- BharatNet project is being implemented in a phased manner for providing Broadband connectivity to all Village Panchayats (approx. 2,50,000) in the country.
- Estimated cost of the project is **6.2 Billion USD.**
- Thus creating a Broadband Highways through the length and breadth of the country.
- Last Mile Connectivity at Railway Stations, Village Choupals and Blocks.
- Installation of Mobile Towers with 2G and 4G compatibility at difficult areas such as North East region and Left Wing Extremism Affected areas.

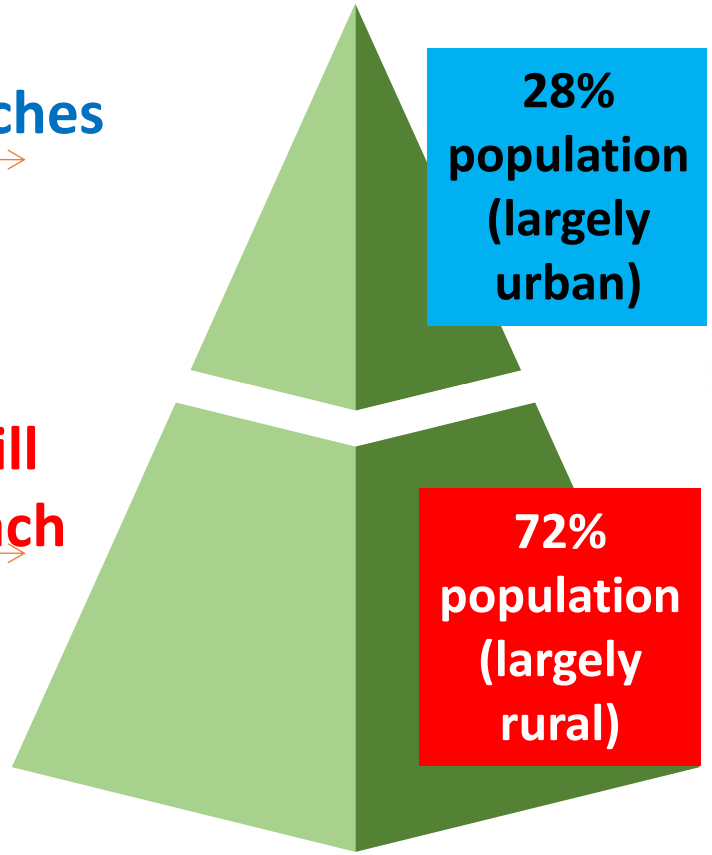
BharatNet aims to reach the bottom of the pyramid

1.2 Million KM existing fiber

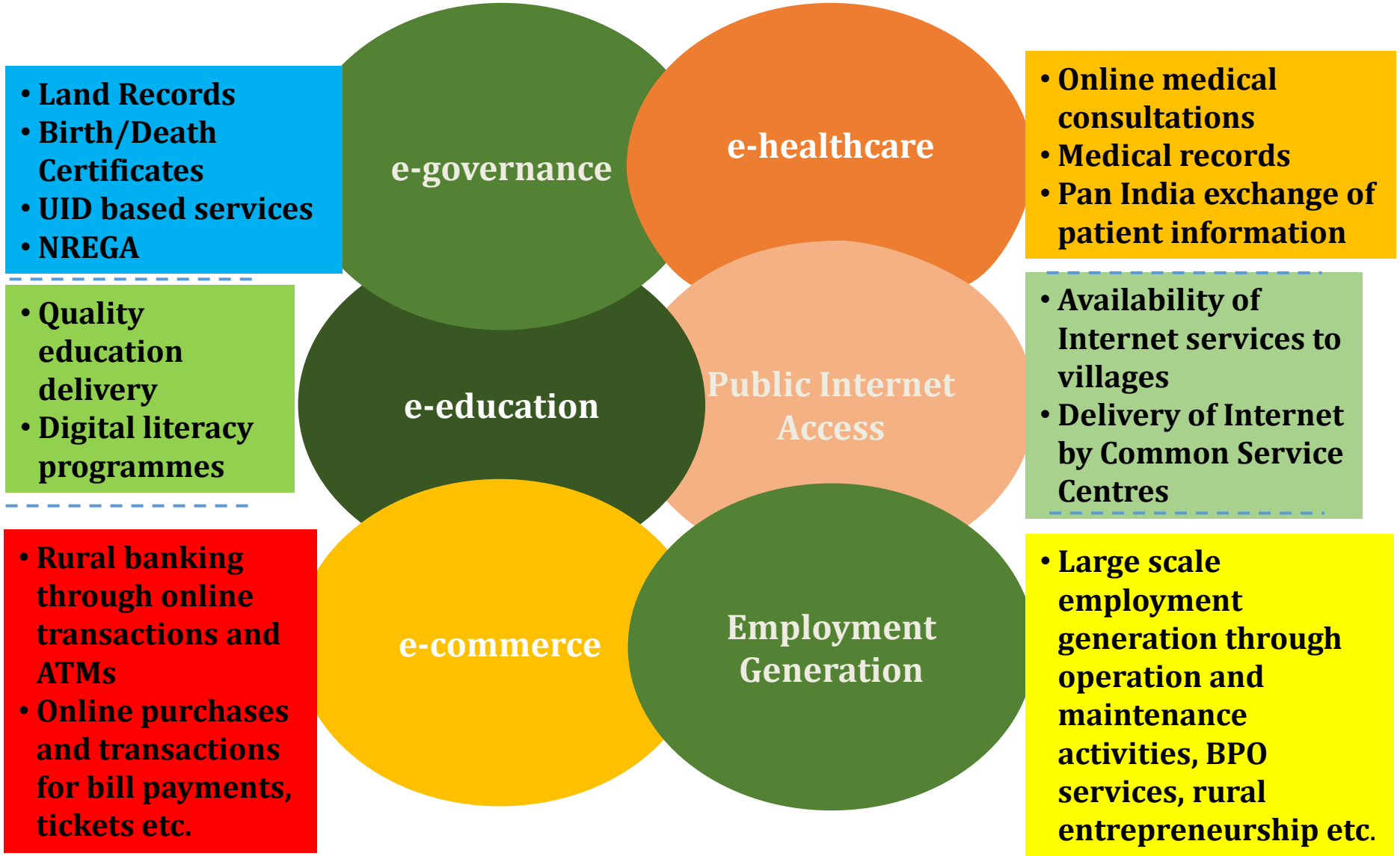
Reaches

0.6 Million KM new fiber under BharatNet

Will Reach



BharatNet – Social Impact



Implementation Strategy of BharatNet

Phase-I

- Project Period: 2014 – 2017
- Broadband has reached in More than 100,000 Village Panchayats
- **Investment of USD 1639 Million**

Phase-II

- Provide broadband connectivity to remaining 150,000 Village Panchayats
- By Optimal Mix of OFC (UG & Aerial), Radio & Satellite by March, 2019
- Last mile architecture (Wi-Fi) to be set up in all the Village Panchayats
- **Overall investment of USD 6.2 Billion**

Phase-III

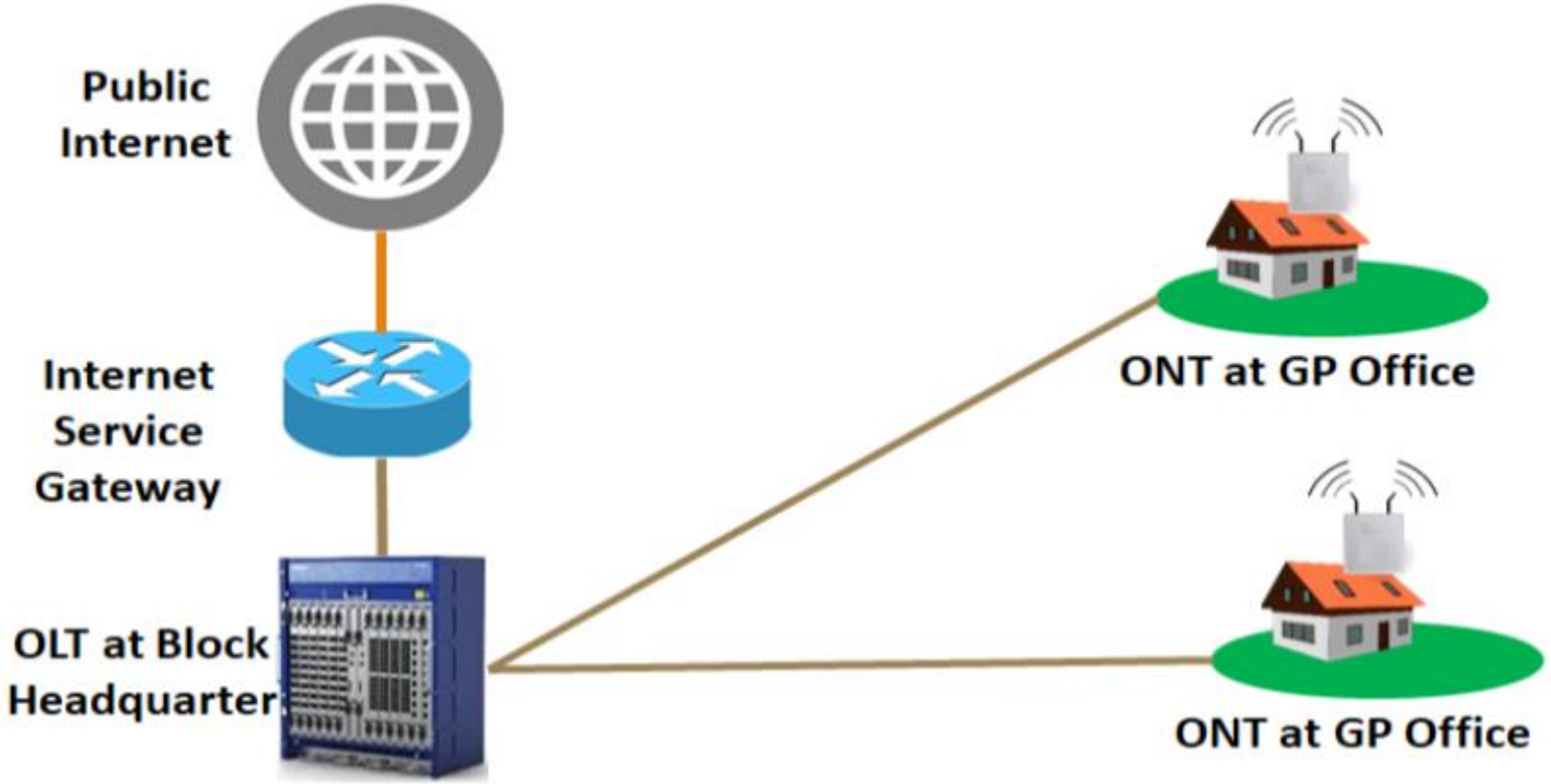
- Project Period : **2018 - 2023**
- Futuristic Network; Ring Topology, Data Center & service delivery infrastructure to meet the infrastructure need of 5G and Internet of Things era.

BBNL

Implementation Complexities

- **Several Implementing Agencies – Varied Implementing Strategies**
  - CPSUs, State PSUs
  - Distribution Companies
  - Private Sector: TSP, ISP, MSO, LCO etc.
- Varied models of implementation of States being integrated and varied requirements of States. Varied Technologies.
- Issues of integration, aggregation, coordination and Management of **vast and distributed network** and virtual assets

Current Status- Phase 1



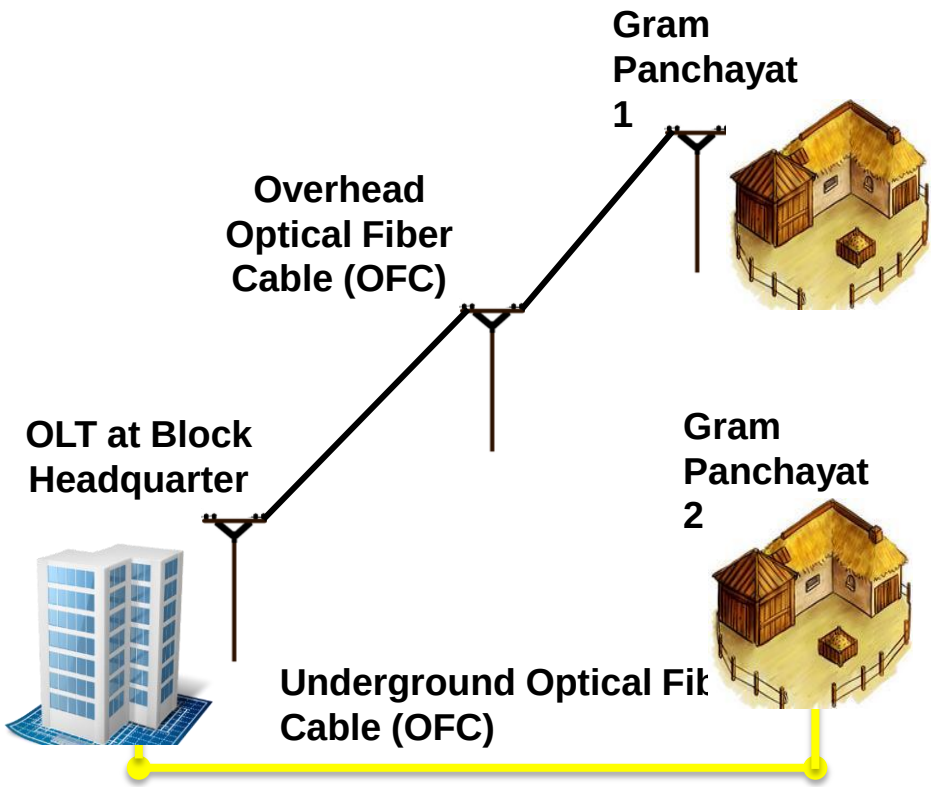
1,11,510 Village Panchayats are Broadband connected

Way Forward – Phase 2

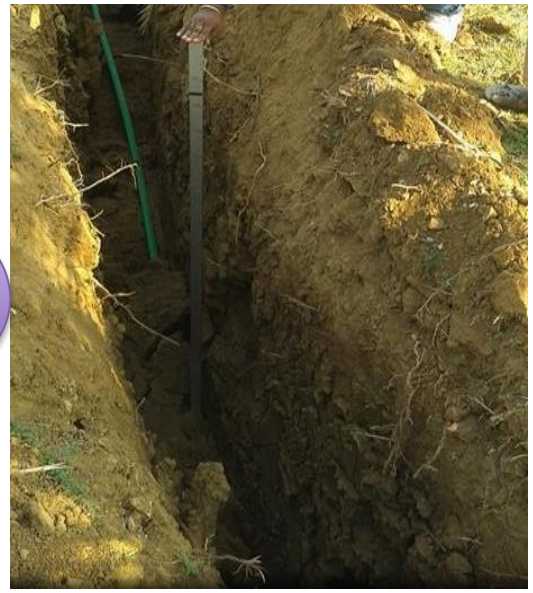
Optimal Mix of Overhead, Underground Fiber, Radio and Satellite Planned

Radio Connectivity Architecture

Fiber Connectivity

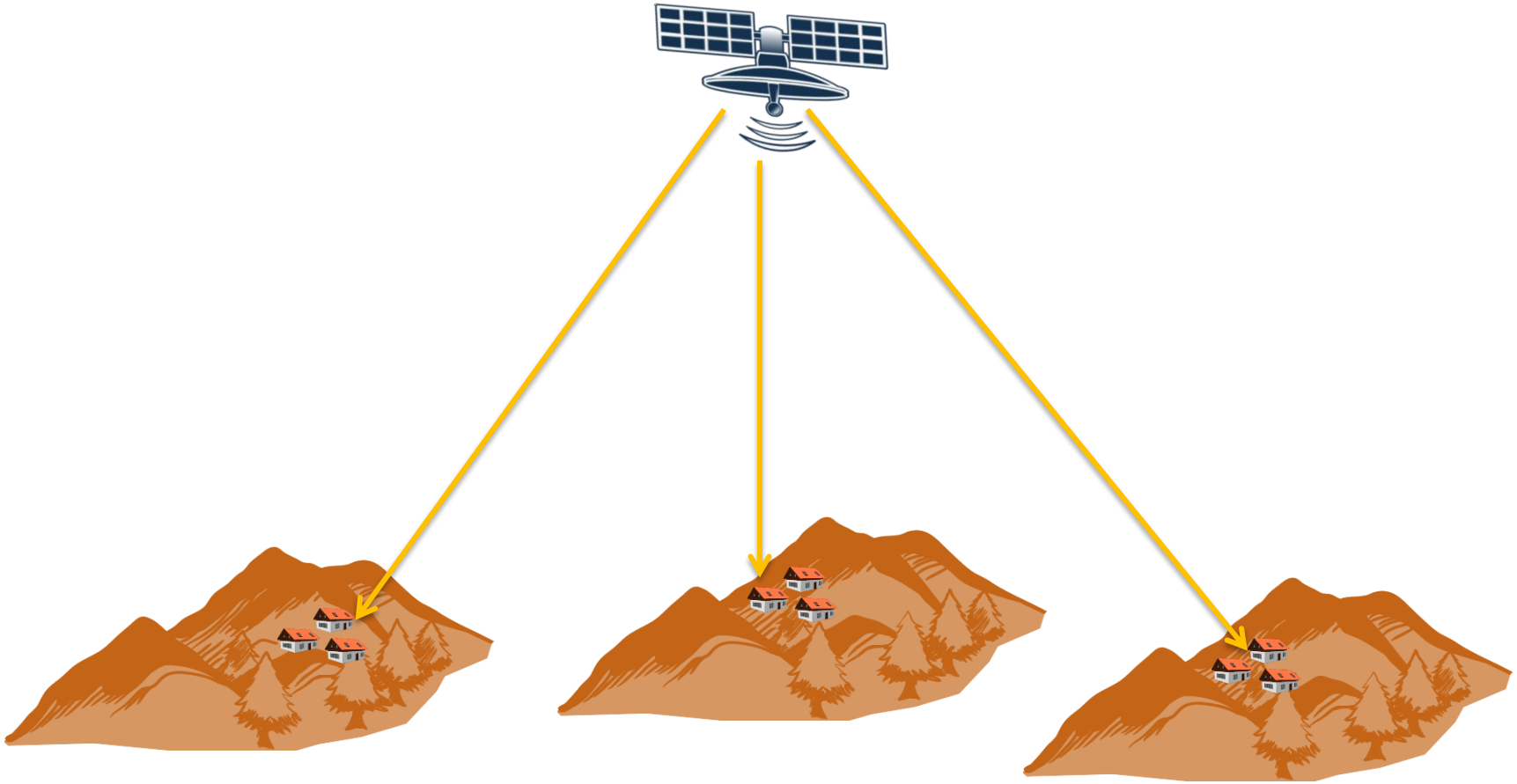


Underground OFC Laying



Aerial OFC Laying

Satellite Connectivity



6407 Village Panchayats to be connected through Satellite media

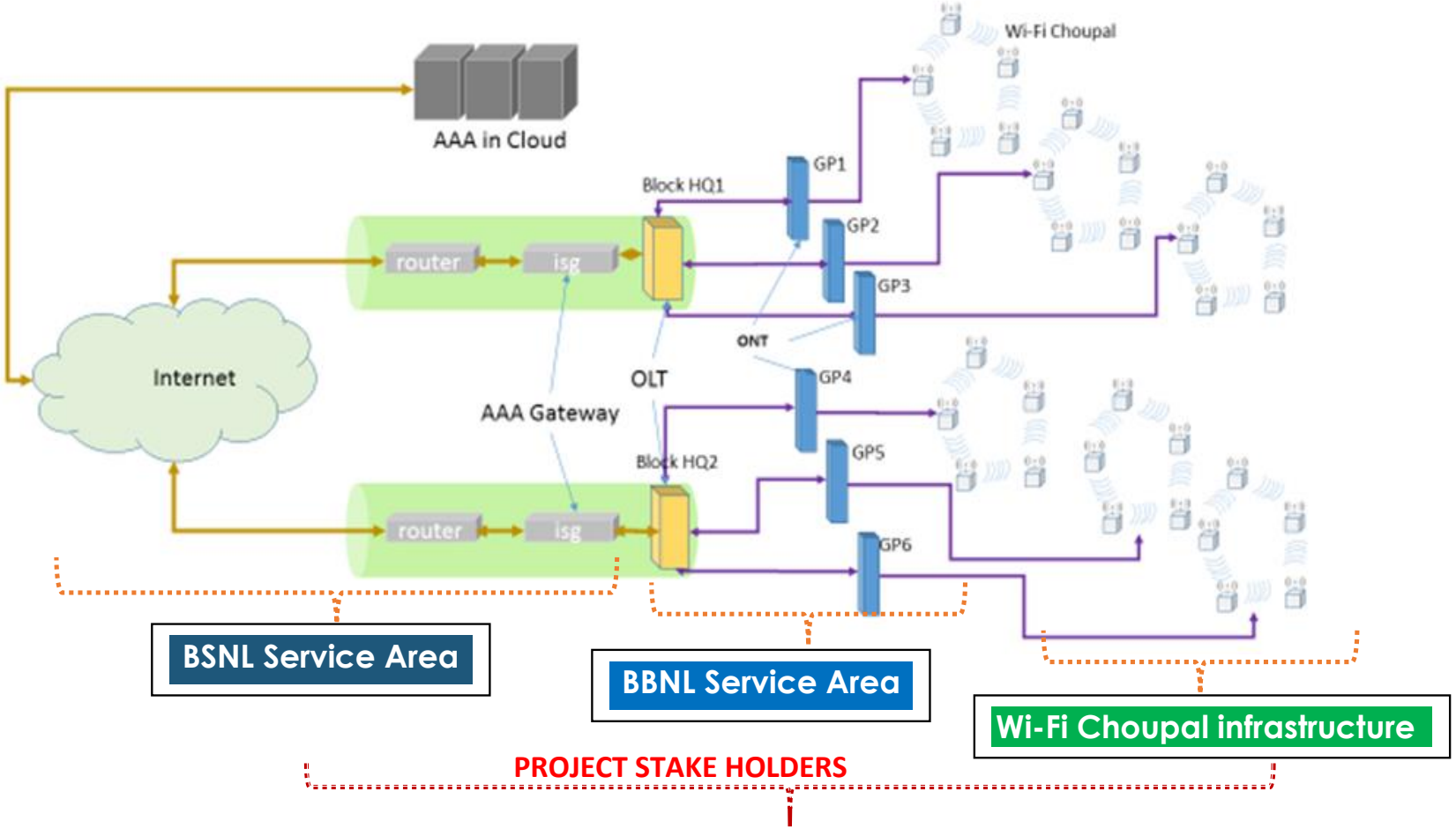
Wi-Fi Hotspots

Wi-Fi Choupal project has been initiated to provide Wi-Fi Internet access in rural India.

Wi-Fi Choupal essentially facilitates a Service Delivery ecosystem which can be used to deliver the following services:-

1. Hi Speed Internet Access across village
2. Free Wi-Fi calling solution
3. Video Calling between local Smartphones possible without using telecom billing
4. Streaming of Audio/Video Content (entertainment, edutainment and infotainment) over Smartphones and Tablets
5. Mobile Commerce

Wi-Fi Choupal Internet Access Architecture:



Tariff

- Pricing is substantially lower than the market prices.
- Customizable pricing models to meet every customer segment.
- Both Bandwidth and Dark Fibres are available for service provisioning.
- Bandwidth:

  INR 7000 **(USD 102)** for 10 Mbps Bandwidth for 1 year.

  INR 2,00,000 **(USD 2,941)** for 1 Gbps Bandwidth for 1 year
- Dark Fibre:

  INR 2,250 **(USD 33)** / Fiber / Km / Year

Thanks

PTS

Post- och telestyrelsen arbetar för att alla i Sverige ska ha tillgång till bra telefoni, bredband och post.

Broadband for all – the Swedish experience

Dan Sjöblom

Director-General Swedish Post and Telecom Authority

Current trends

- The vertical model is challenged
- Demand for speed and capacity everywhere
- Difficult to distinguish between infrastructure, services and content
- Growth of IoT/connected devices
- Importance of data
- Digitalization, AI and blockchain …

Where we are now …

The development of fixed and mobile broadband access on the Swedish market

77 %

access to >100 Mbps

---

65 %

have bought 100 Mbps

72 %

access to fibre

---

84 %

”homes passed”

54 %

SDUs access to fibre

---

70 %

of SDUs ”homes passed”

31 %

Fibre in rural Areas

< 60 Houses

lack 1 Mbps connection

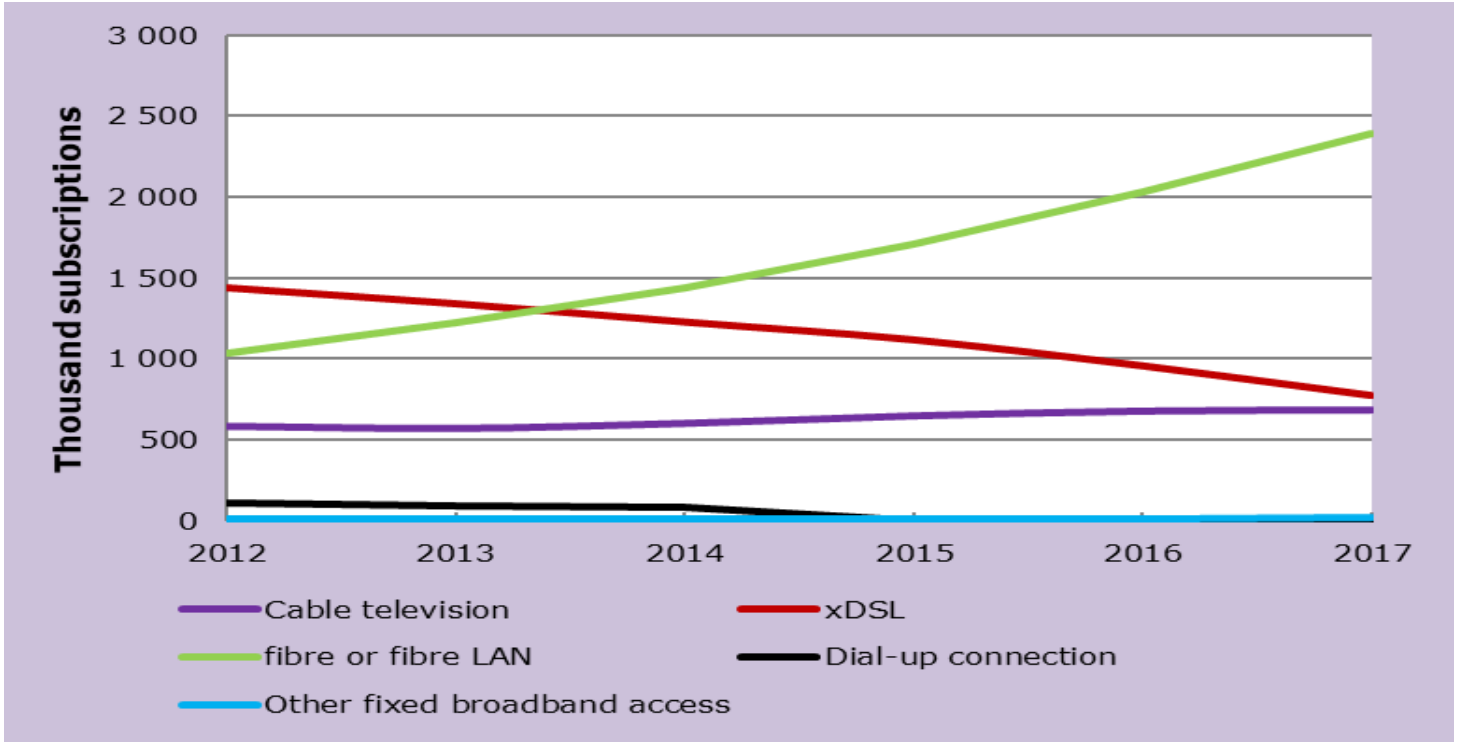
Speed

Fibre

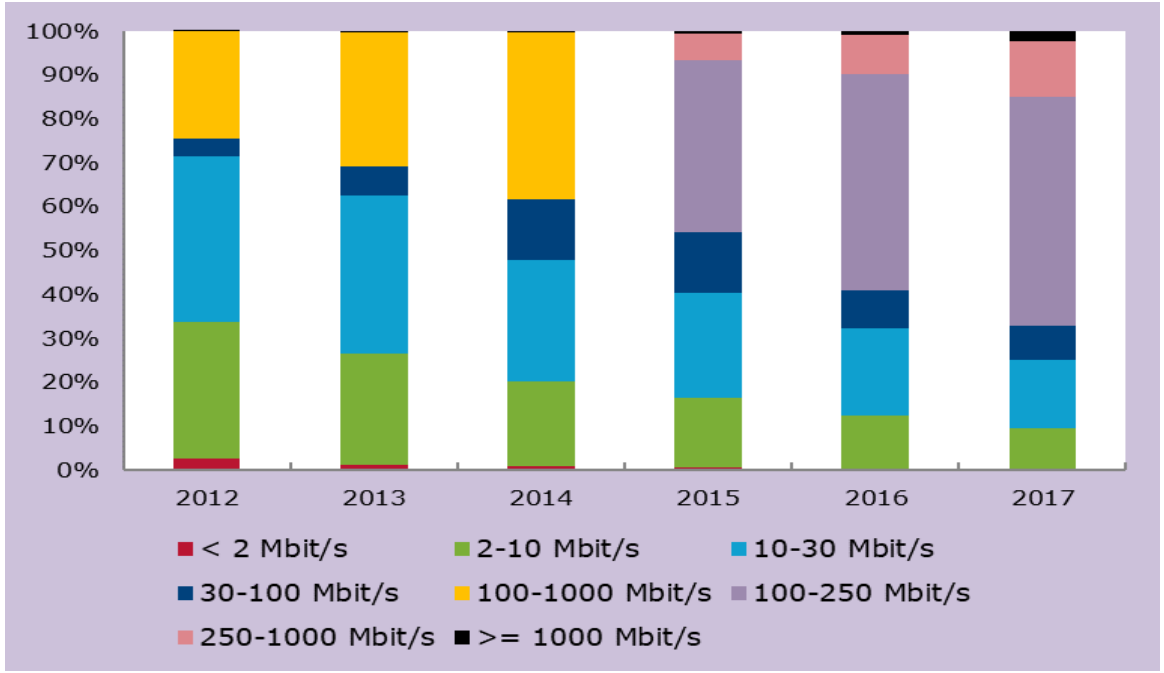
SDUs

Rural

Fixed broadband
Fibre (LAN) continues to grow

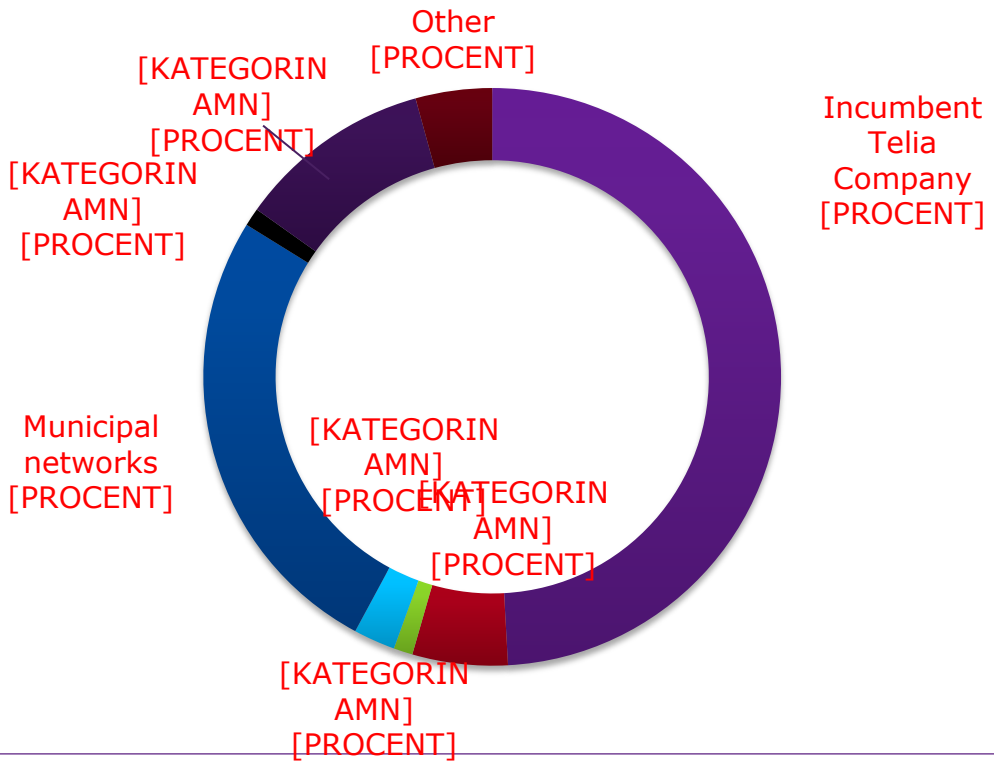


More than half of all fixed subscriptions are +100 Mbit/s



- 51% of all households have active subscriptions of 100 Mbit/s
- The EU goal is that 50 % of all households should have that by 2020

Investments in fixed infrastructure by different market actors



Source: Annual reports

Wireless access in Sweden

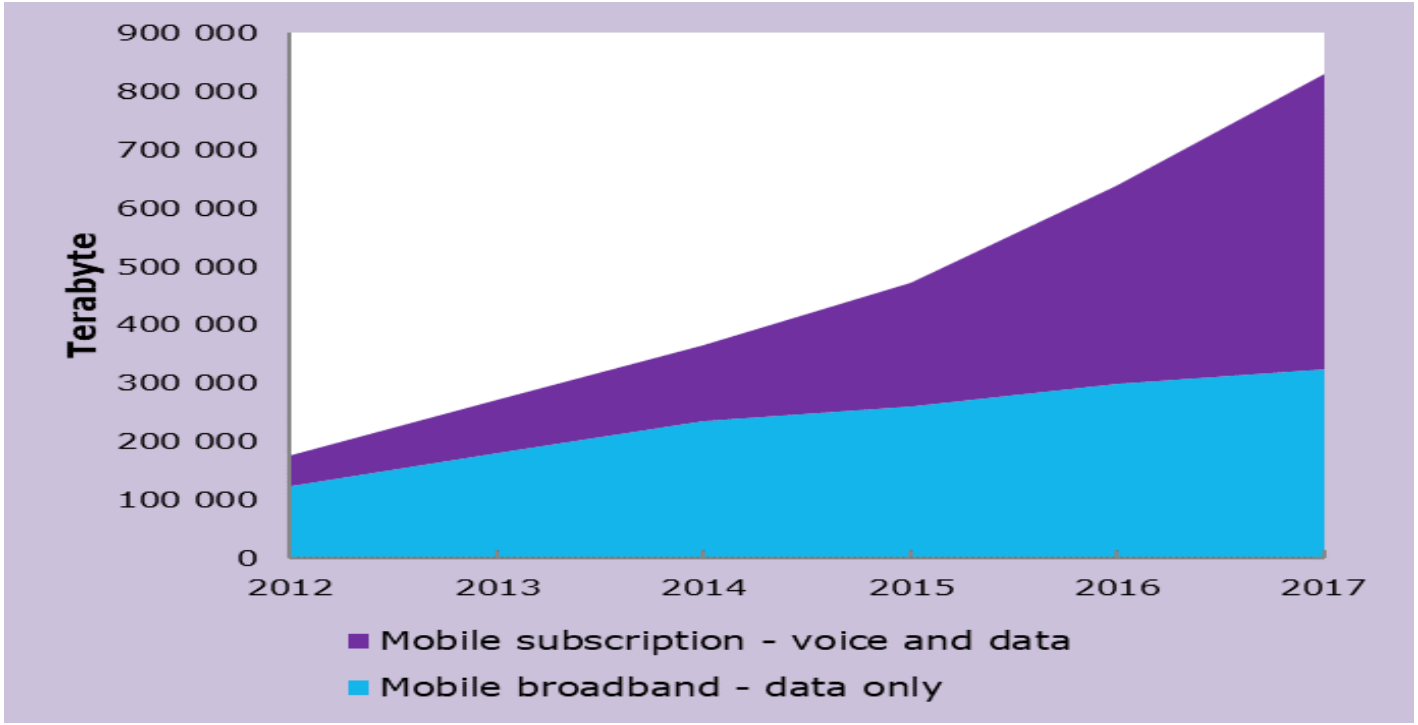
84 % area coverage from wireless services with 10 Mbps or more

99,99 % of households has access to LTE wireless broadband.

95% had access to 30 Mbps – the EU goal is that all households and business should have that access by 2020

PTS

Continued growth in mobile data traffic



Success factor - The Swedish Broadband Forum
Cooperation among actors

Regional and local associations

Market players

Government stakeholders

Still some way to go …

The challenges on the Swedish market

The geographical challenge

MDU 100 % access to fibre

SDU 42 % access to fibre

22 % fibre in rural areas

65 % fibre in urban areas

The rural challenge

Rural Areas

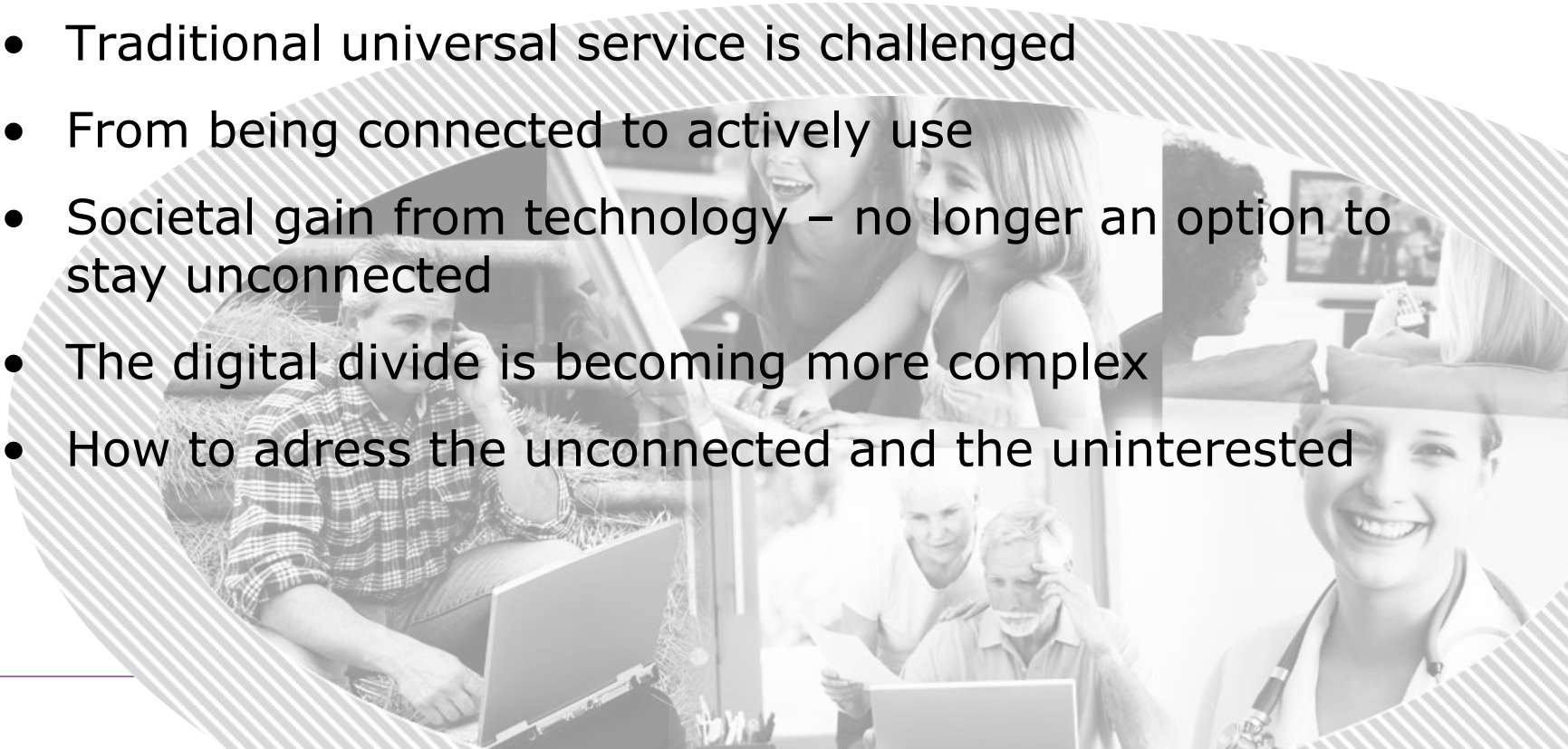
3,5
pers/km^2

Urban Areas

1500
pers/km^2

The digital inclusion challenge

- Traditional universal service is challenged
- From being connected to actively use
- Societal gain from technology – no longer an option to stay unconnected
- The digital divide is becoming more complex
- How to adress the unconnected and the uninterested



Thank you!

Arcep

Broadband for all in France

Ericsson Seminar

Pierre-Jean Benghozi
Arcep Board member

25 June 2018

Stockholm

Summary

Arcep

New deal

5G and Arcep’s action plan

Overview about the Arcep

The Arcep:

- Arcep is an **independent** Administrative Authority created in 1997 to accompany the opening up to competition in the telecommunication sector and to ensure the provision and financing of the universal service for telecommunications
- As a NRA, Arcep ensures, on behalf of the State, and under the control of the Parliament and the judge, the regulation of telecommunications and postal sectors. Arcep is in charge of the **regulation of the telecommunication and the postal sectors**.

Actual priorities and means to achieve Broadband for all :

Create the conditions for a plural and decentralised network organisation

Optical fibre

Encourage investments in and the transition to optical fibre, particularly through the way copper pair access (LLU) is priced.

Connected SMEs

Stimulate the development of a universal fibre network architecture to enable the emergence of a fibre mass market for small and medium enterprises.

Fight against any type of silo that could threaten the freedom of communicate on the networks

Net neutrality

Set up an investigation programme and implement the regular collection of detailed information from operators.

5G Experimentation

Introduce provisions in support of experimentation into the regulatory framework.

Guarante the openness of the market to new players and to all forms of innovation

Ensure the sector's competitiveness through pro-investment competition

arcep

Coverage objective : more and more prominent in spectrum awards

	2001 to 2010	2010	2011	2012	2015	2018 (Future)	
	3G 2.1 GHz (4 awards)	3G 2.1 GHz additional	4G 2,6 GHz FDD	4G 800 MHz	4G 700 MHz	4G 900 , 1800, 2100 MHz	4G 2600 MHz TDD
Monetising the State's intangible assets	Fees fixed *ex ante*	sealed-bid auction	sealed-bid auction	sealed-bid auction	Multi round auction		
Digital development				Coverage: ✓ Nationwide ✓ Priority rollout zone ✓ Departmental area	Coverage: ✓ Same as 800 MHz ✓ on-board coverage of everyday trains	**Achieve ubiquitous high standard mobile coverage by 2020**	Achieve ubiquitous high standard mobile coverage in some stakeholders areas
Competition issues	Room for a 4th entrant with conditions favouring its expected arrival	MVNO access criteria	MVNO access criteria	MVNO access criteria	Multi band spectrum caps		
Innovation			Minimum data rate registered in the licences	Minimum data rate registered in the licences		✓ **fast internet access (>8 Mbit/s) for every citizen** ✓ **2022: superfast access networks (>30 Mbit/s) in every region**	
Other objectives	14 technical and economic criteria, including : network quality, service offering and corresponding price, rollout speed...						Opportunity, for some stakeholders, to operate their own network with a specific coverage and a outstanding quality of service

Technology neutrality

New deal for mobile coverage = new commitments and implementation

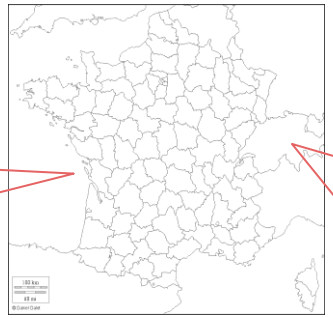
Historic agreement between the Government and mobile operators that aims to ensure the availability of high standard mobile coverage for everyone in France

Context of the mobile coverage : why a “New deal” ?

Context of renewal of the 900, 1800 and 2100 MHz band frequency licences expiring between 2021 and 2024 with a 2018 reassignment procedure conducted by Arcep

- **1. Mobile coverage situation**

Regarding the population, good mobile coverage for 2G,3G and 4G



Regarding the geographical area, unsatisfying mobile coverage expecially for 4G technology

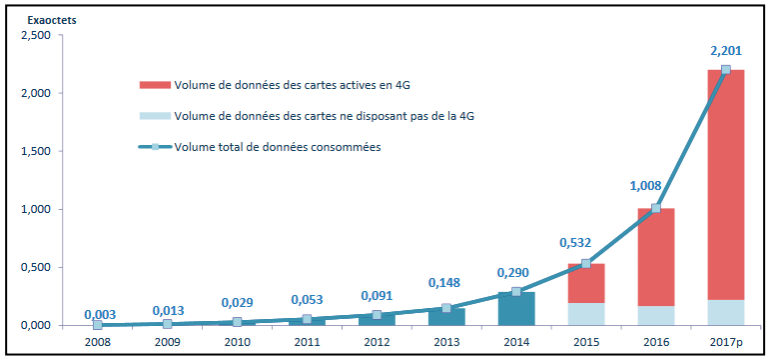
	Population	Area
Orange	92%	65%
SFR	91%	65%
Bouygues	90%	61%
Free	82%	48%

4G Mobile coverage in July 2017

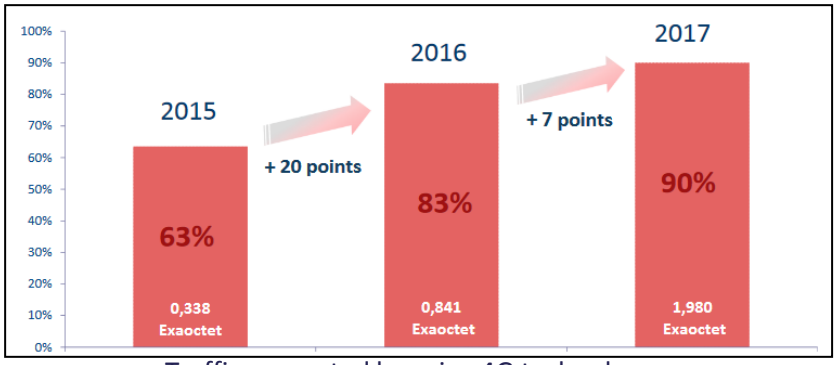
- **2. Mobile traffic explosion**

Data traffic consumption in 2017, in France, has doubled comparing with 2016 (+118,3%)

--> the consumer needs more data everywhere!



Traffic generated by using all the mobile technologies



Traffic generated by usign 4G technology

Implementing 4 new principles to generalize a good quality mobile coverage for all

1. Change of paradigm for the State	For the first time in a frequency allocation, the digital coverage of the territory takes precedence
2. Operators' commitments for a gradual improvement of mobile coverage in the daily life of the people	Generalization of 4G coverage, coverage of major roads, indoor coverage, no more obligation of coverage expressed in terms of a % of the population
3. A solution for challenge areas	Operators will use their own funds where the authorities have identified coverage needs
4. Acceleration of digital coverage throughout the country	The Government will implement measures to simplify deployments under the Housing Bill; other regulatory measures will follow.

Intended new commitments for mobile operators

Accelerating the coverage of transportation means
(major roads and regional railways)

Achieving ubiquitous indoor telephone coverage
(Voice over Wifi and on demand coverage)

Achieving ubiquitous 4G coverage for 2020
(« White areas national Programme » : 75% end 2020, 100% end 2022)

Accelering deployments and **availability** of high standard mobile coverage and Qos for everyone

Improving reception quality across the entire country, and particularly in rural areas
(transparency, high QoS)

Increasing the rhythm of existing national programmes for improving coverage

Dedicated sites
- each operator deploying 5,000 new 4G sites across the country (with some shared sites). NB: 100% private funds

Fixed 4G
- + 1,000 new sites for fixed 4G offers

1,000 new 4G sites in order to provide fixed 4G. Orange (500) and SFR (500)

2,000 new sites RAN-sharing 4G by the 4 operators
Cover the more densely populated areas where no operator currently provides good coverage

list of the locations provided by the Government => **between 600 and 800 a year**, per operator

3,000 locations to cover in 4G by each operator.
It could concern any type of location. Some of these new sites will be shared.

arcep

Coverage priority and new obligations rooted into operators' frequency licences

January 2018 : New Deal agreement

April 2018 : Launch by Arcep of a public consultation on the conditions of reallocation of the frequencies expiring between 2021 and 2024

Now : Modification of the current authorizations of the operators to set from 2018 these new obligations, covering the intermediate period

The inclusion of these obligations in operators' authorizations makes them legally binding and controllable by Arcep

--> i.e. : consistent with Arcep’s data-driven regulation and observatory

5G
and
Arcep’s action plan

5G : a priority subject

An international mobilisation

Ambitious european action plans to contrast USA and Asia plans

5G roll-out in one major city in every European country by 2020 and global coverage (every city, motorway and high-speed railway lines) by 2025

- National initiatives : government action plans, trials and pilots

Objective: 5G commercial rollouts in 2020

5G competition

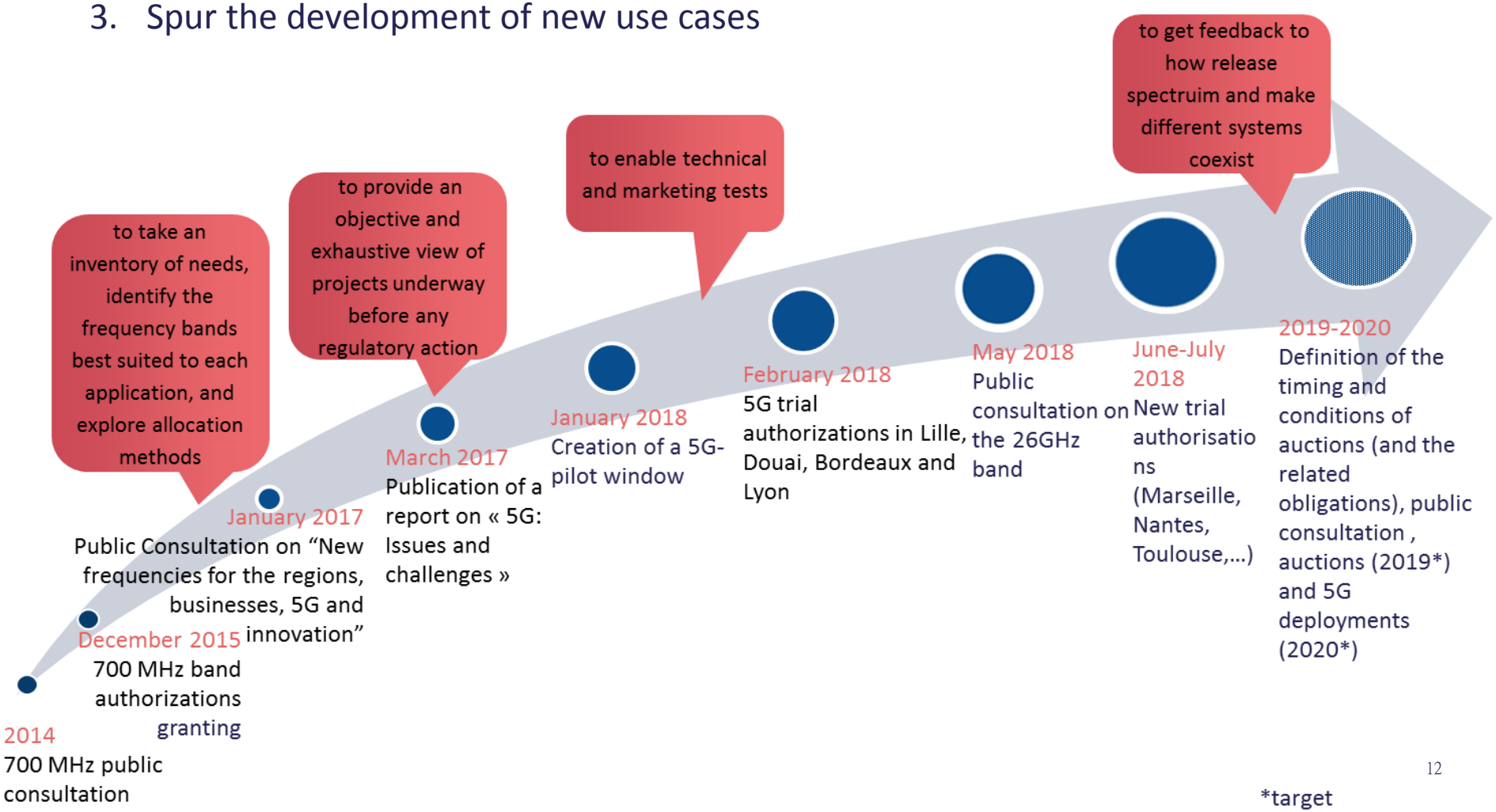
French situation: strong commitment and « on the move » for 5G implementation

- **4** operators
- All committed to the fixed and the mobile rollout
- Important delays in 4G roll out, particularly in rural areas
- Gouvernemental plan for having superfast access networks everywhere
- Active participation to the work of BEREC : Particularly on infrastructure sharing, frequency allocation procedures and coverage obligations
- Frequencies: a global mission
  - **700 MHz band**: already allocated to operators in France and partially on hand, fully available mid-2019!
  - **C band** (3.4 - 3.8 GHz): requires **relocation** of **existing radio relay links** and **wireless local loop networks** to the lowest end of the band
  - **Millimeter-wave band** (26 GHz): **relocation** of **existing radio relay links**, and definition of **coexistence** between 5G mobile and other existing services (FSS: Fixed Satellite Services, Radio-astronomy, etc.)
  - **Other frequencies**: thoughts about the “L band”, the “2,6 GHz TDD” band,..

Arcep's spectrum work on 5G since 2014

Action plan:

1. Release and allocate spectrum
2. Support the improvement and simplifications of the rollout conditions
3. Spur the development of new use cases



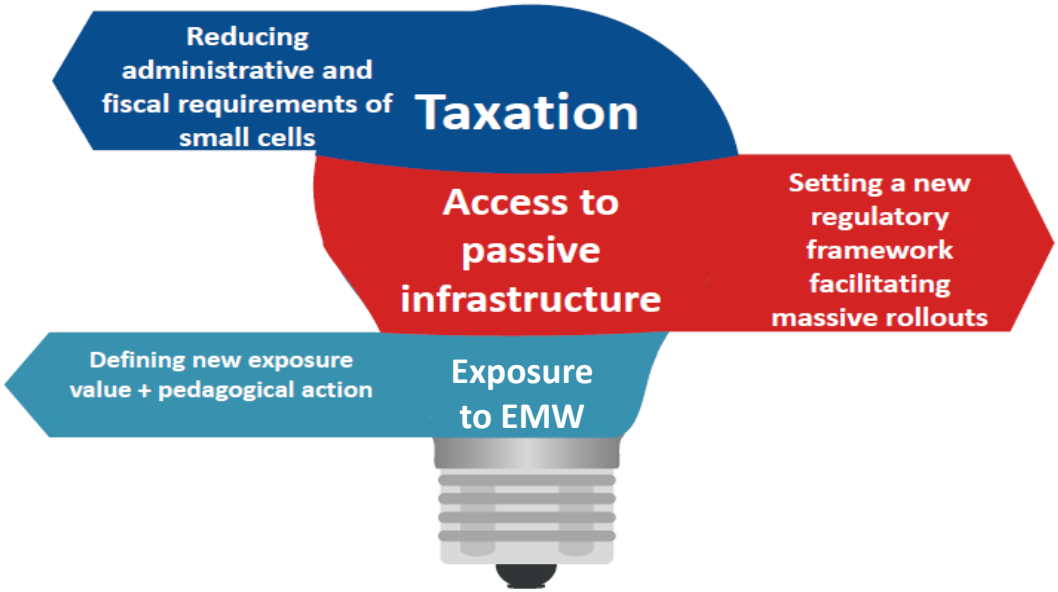
*target

Action#1: Release and allocate spectrum

- May 2018: Public consultation on 26 GHz band
  - How to make the 26 GHz band available to host 5G?
  - What conditions for the coexistence between 5G mobile and other existing services?
- Definition of the **timing and conditions of auctions (and the related obligations)**: for both C band and millimeter-wave band
  - C band **spectrum awards** should take place soon enough to permit 5G dedicated equipment planning and supply for operators;
  - **2019-2020**: first rollouts in C band (3.4 – 3.8 GHz) to meet the objective of **5G commercial launch by 2020**;
  - A specific focus on 2,6Ghz TDD (2575 – 2615 MHz sub band 4G)
    - 40 MHz dedicated to professional mobile radio LTE networks
- Progressive migration of existing systems to other mobile frequency bands

Action #2: Support the improvement and simplifications of the rollout conditions

A **fast 5G rollout** calls for setting a **favorable regulatory environment**, especially with regard to **small cells deployment**, involving contribution of public stakeholders and authorities, and related to:



Action #3: Spur the development of use cases – **5G pilots**

Principle: **granting temporary 5G licenses** for willing operators and vertical industry partners in C band and in 26 GHz band, **in 2018 and 2019**.

9 metropolitan areas already identified (Lyon, Bordeaux, Nantes, Lille, Le Havre, Saint-Étienne, Douai, Montpellier and Grenoble) and ready for 3400-3800 MHz. Other locations available on request, subject to study.

5G temporary licences already given in main cities

Objective: Facilitate technical uses and experiments and implement **5G pilots involving all actors including non-operators (e.g. vertical industries)** allowing to:

- identify actors interested with 5G spectrum;
- deepen understanding of concrete use cases for 5G;
- explore business models and associated challenges for the players of the 5G value chain
- obtain initial feedback that will help shaping 5G frequency allocation, especially regarding cohabitation between actors.

Conclusion

Coverage:

- Arcep, as network **architect**
  - create the conditions for a plural and decentralised network organisation
  - guarantee the openness of the market to new players and to all forms of innovation
  - ensure the sector's competitiveness through pro-investment competition

- Arcep, as network **guardian**
  - enforce the principles essential to guaranteeing users' ability to communicate
  - assist public authorities in expanding digital coverage nationwide
  - protect against possible net neutrality provisions

In a nutshell, "Broadband for all" means:

Broadband for all

- Coverage for all
- Information for all (data-driven regulation)
- Uses for all (SME, stakeholders, G.E.)
- Connectivity and access fo all (Mobile, IoT, IoE, Net neutrality)

Thank you for your attention

Pierre-Jean BENGHOZI

Arcep Board member

pierre-jean.benghozi@arcep.fr

VISION رؤيـــة 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

Mobile Broadband Spectrum In Saudi Arabia

Broadband for All

June 25-26, 2018, Stockholmn

Mohammed Alotaibi
Communications and Information Technology Commission
Kingdom of Saudi Arabia

Scope

1) **More IMT Spectrum**
   - Status 2016
   - Intervention 2017/2018
   - Impact
2) **Longer Term IMT Spectrum Plan**
   - 2020 Target
   - Timeline
   - Increasing Utilization
3) **IMT-2020 Spectrum**
   - Identified and candidate bands
   - 5G Trials

2016

- Three Mobile Operators
- Only a total of 260 MHz assigned

Band	Assigned Bandwidth
900 MHz	2x35 MHz
1800 MHz	2x35 MHz
2100 MHz	2x60 MHz

- Average Download Speed on Mobile Network less than 10 Mbps
- Artificial spectrum scarcity was the main reason
- Quick intervention needed

2017/2018

- Government legacy use, including terrestrial broadcasting, in the 700, 800, 1800 MHz bands
- Inter-governmental task force formed
- Additional 200 MHz made available
- Two spectrum auctions were held in 2017 and 2018, and 160 MHz was assigned

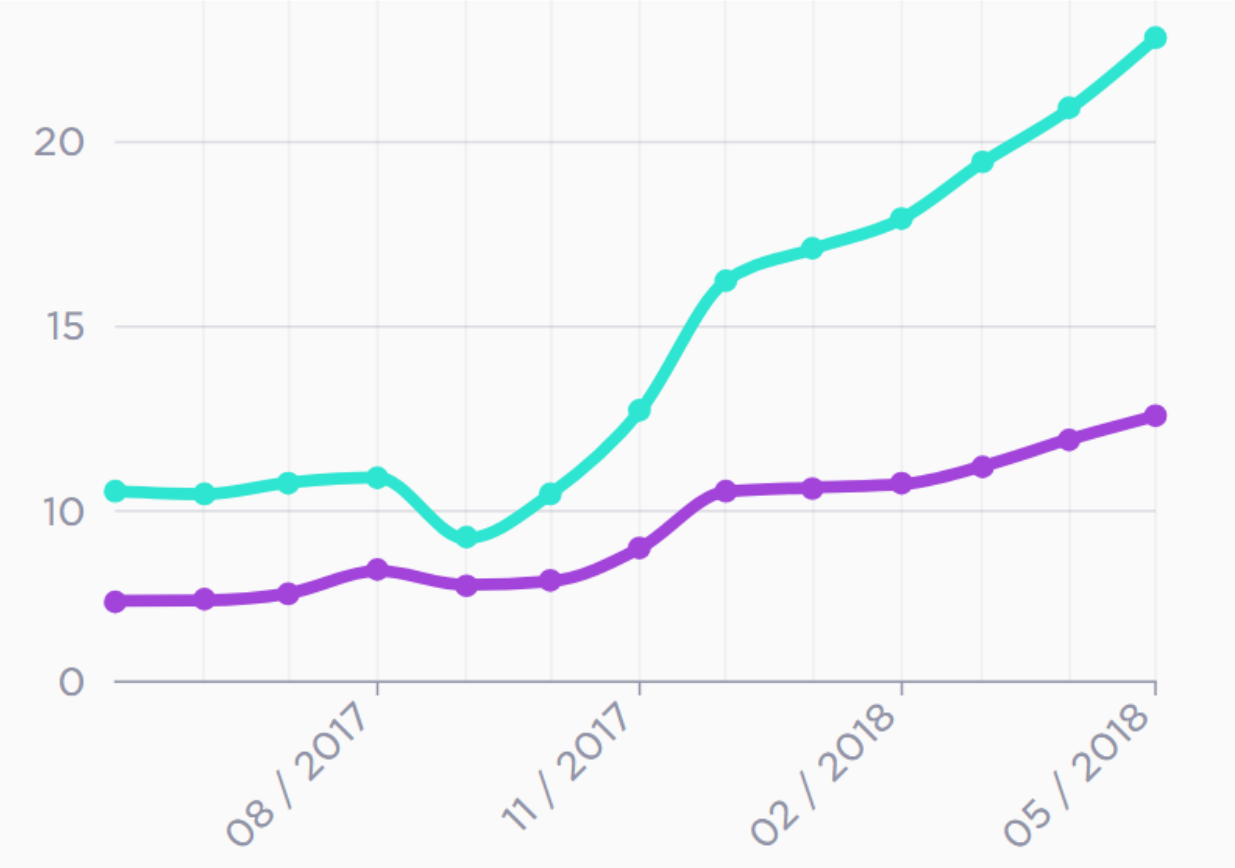
Band (MHz)	**700**	**800**	900	1800	2100
Assigned Bandwidth (MHz)	**2x20**	**2x20**	2x35	**2x75**	2x60

Impact

Speedtest Global Index
May 2018

Download Mbps	Upload Mbps
22.81	12.58

Global Average	Download	Upload
	23.57	9.35



2020 Target

- **National Transformation Program 2020:** Initiative to improve mobile broadband speed
- CITC set **IMT spectrum policy and regulation** to ensure goals achieved
- **Minimum Target:** To make more than 1 GHz available for mobile broadband by 2020

Band (MHz)	700	800	900	1500	1800
Bandwidth (MHz)	60	60	70	70	150

Band (MHz)	2100	2300	2600	3500
Bandwidth (MHz)	180	100	190	200

Timeline

Band (MHz)	Bandwidth (MHz)	Action	Expected Release
2300	100	Clear band from government legacy users	2018
2600	190	Clear band from government legacy users Move FWA providers to other band	2018
3500	200	Move FWA providers to other band	2019/2020
700	20	-	2019
1500	70	-	2019
2100	60	WRC-19 Decision	2019/2020

More Utilization

Band Identified for IMT in RR (MHz)	Frequency Arrangements (MHz)	Unutilized frequencies for IMT (MHz)
698-960	703-733 758-788 791-821 832-862 880-915 925-960	698-703 733-758 (25 MHz) 788-791 821-832 862-880 915-925
1 710-2 025	1710-1785 1805-1880 1920-2010	1785-1805 1880-1920 (40 MHz) 2010-2025

5G Bands

Band	Status	Note
3600-3800 MHz	Identified	To be combined with the IMT band 3500 MHz to create a contiguous 400 MHz of spectrum
3800-4200 MHz	Candidate	To be considered after consultation with other stakeholders (satellite operators)
24.25-27.5 GHz	Candidate	Supported by ASMG
40.5-43.5 GHz	Candidate	Supported by ASMG
614-694 MHz	Candidate	WRC-23 Agenda item

شكراً

Thank you

Port of the Future: the digital agenda at the Port of Livorno

Paolo Pagano

Joint Laboratory of Advanced Sensing Networks & Communication in Sea Ports

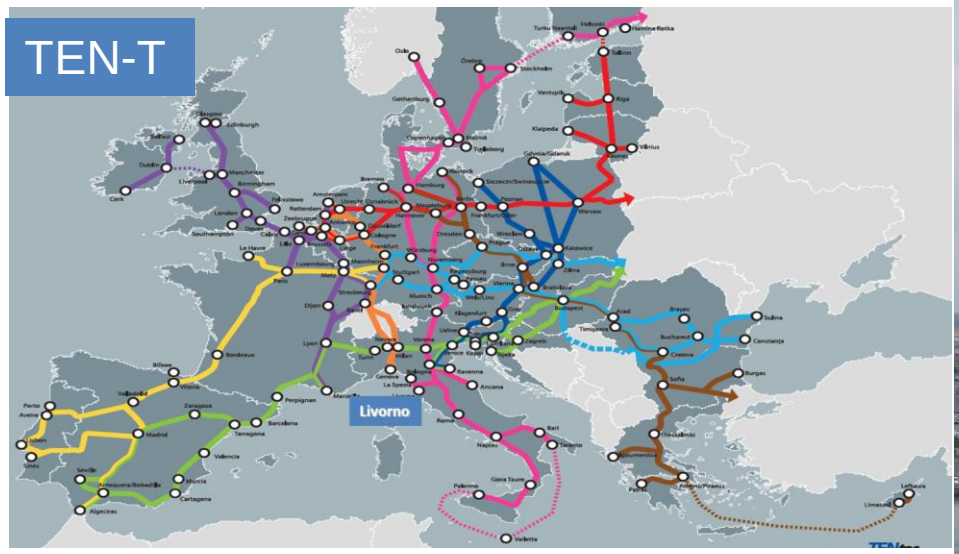
Outline

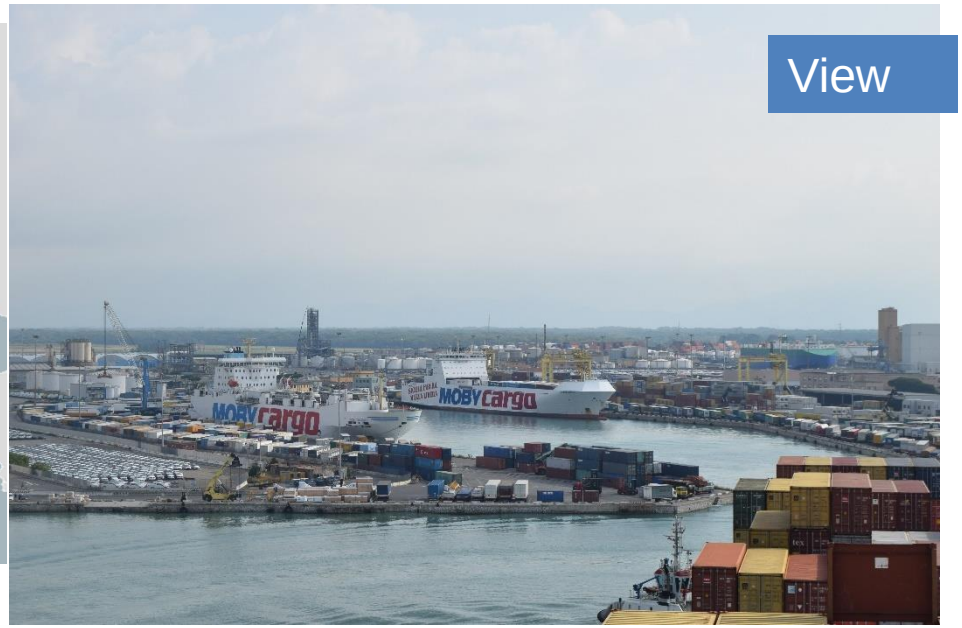
- Profile of the Port Authority (AdSP):
  - Port of Livorno
    - Objectives, digital agenda, international relationships and cross/fertilization
- AdSP innovation technologies and innovation assets
- Final User Services:
  - Connected Vessel
  - e-Freight and Smart Corridors
  - Mobility Services, Urban Nodes
  - Port Monitoring and Security
- Conclusions

Motivations

- The technological development underlying the digital era involves a deep societal transformation:
  - relationships between people and businesses (i.e communities);
  - industry and production cycles (e.g. industry 4.0);
  - professional skills (i.e. specialization).
- Need of industrial transformation in all sectors (including the port) for:
  - maintain competitiveness and employment;
  - respond to new business and citizen needs;
  - sustainable development of the port-city eco-system.
- Governance role for AdSPs:
  - define objectives and priorities, to frame innovation activities according to the indications of the European and Italian digital agendae.

Our eco-system





- The Passenger Port: ferry and cruise terminals (100,000 m^2), ship repair and ship building
- The Commercial Multipurpose Port: 2.5 million m2 (850,000 m^2 customs boundary) 90 berths and 13 km of quays, 3 railways & 60 km of tracks, freight traffic fully separate from the urban one
- The Industrial Area: refinery, oil stock areas, energy power stations, chemical and automotive component industry
- The Freight Village “A. Vespucci”: 2.8 million m^2 , cargo consolidation with multimodal access, distribution centres, packing firms, customs clearance and scanning area, railstation, 3 MWh PV park, etc.
- The Dry port “Il Faldo”: car stocking and distribution area fully automatised , 640,000 m^2, capacity 25,000 cars, road and rail accesses

Cross-fertilization

- The result is a strong and structured collaboration with the main port innovation initiatives in Europe and beyond;
- Collaboration means:
  - being considered;
  - being up to date;
  - import best practices.
- The authority is an active player towards EC and EU most relevant lobbies (ESPO, Corridor Forum, ERTICO).

About us

July 2016

Most innovative Public Body

June 2017

Port and 5G

June 2018

Swedish Ministry of Post & Telco 2018 edt 31 countries, 113 invited delegates

November 2016

EU Connected Vehicle

July 2017

Port of the Future

September 2018

"Port of the future towards automation" @

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Porti di Livorno, Piombino, Capraia Isola, Portoferraio, Rio Marina, Cavo

Offizielles Stadtportal für Hamburg

Conveners:

consorzio nazionale
interuniversitario
per le telecomunicazioni

Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

«Livorno as a Digital Port»

General Objectives

(Continuous) definition of requirements with final users (from various communities)

Normalization of the IT assets (APIs, platforms)

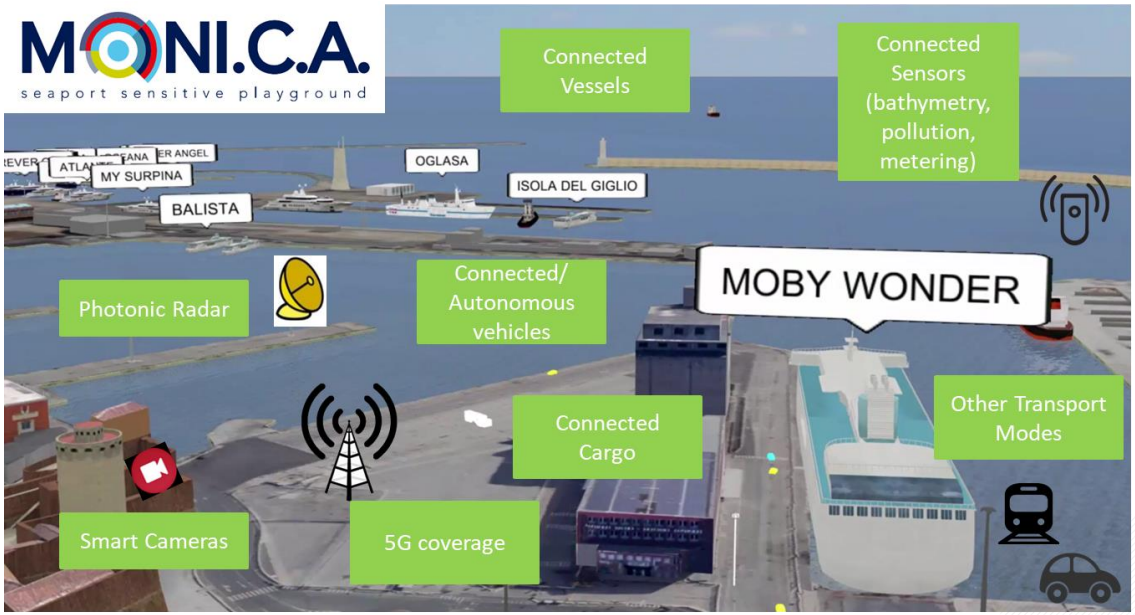
Design of an inovative and standard architecture

R&D ICT stack to prototype functions at every cloud layers

Technological Transfer: roll-out of pilots tailored to port communities

Digital tools of the Port Authority

- Convergence platform for data and services;
- Sharp layer separation:
  - data production;
  - custodial, indexing, retrieval:
    - interaction with other platforms (e.g. Coast Guard, Line Operators, Regional Authorities, City Hall, etc.);
  - data consumption (i.e. final user services and applications).



- Standardization, open-data, interoperability:
  - the Authority can interconnect distributed heterogeneous sensors through a new generation network serving terminals and port infrastructures.

Why standards?

- In seaports digital services rely on the interaction among field equipment (sensors), networks and information appliances (servers and repositories).
- Although proprietary (vertical) systems can effectively respond to the requirements set by the community:
  - they will rapidly get old;
  - they need dedicated maintanance;
  - they are not interoperable with other systems.

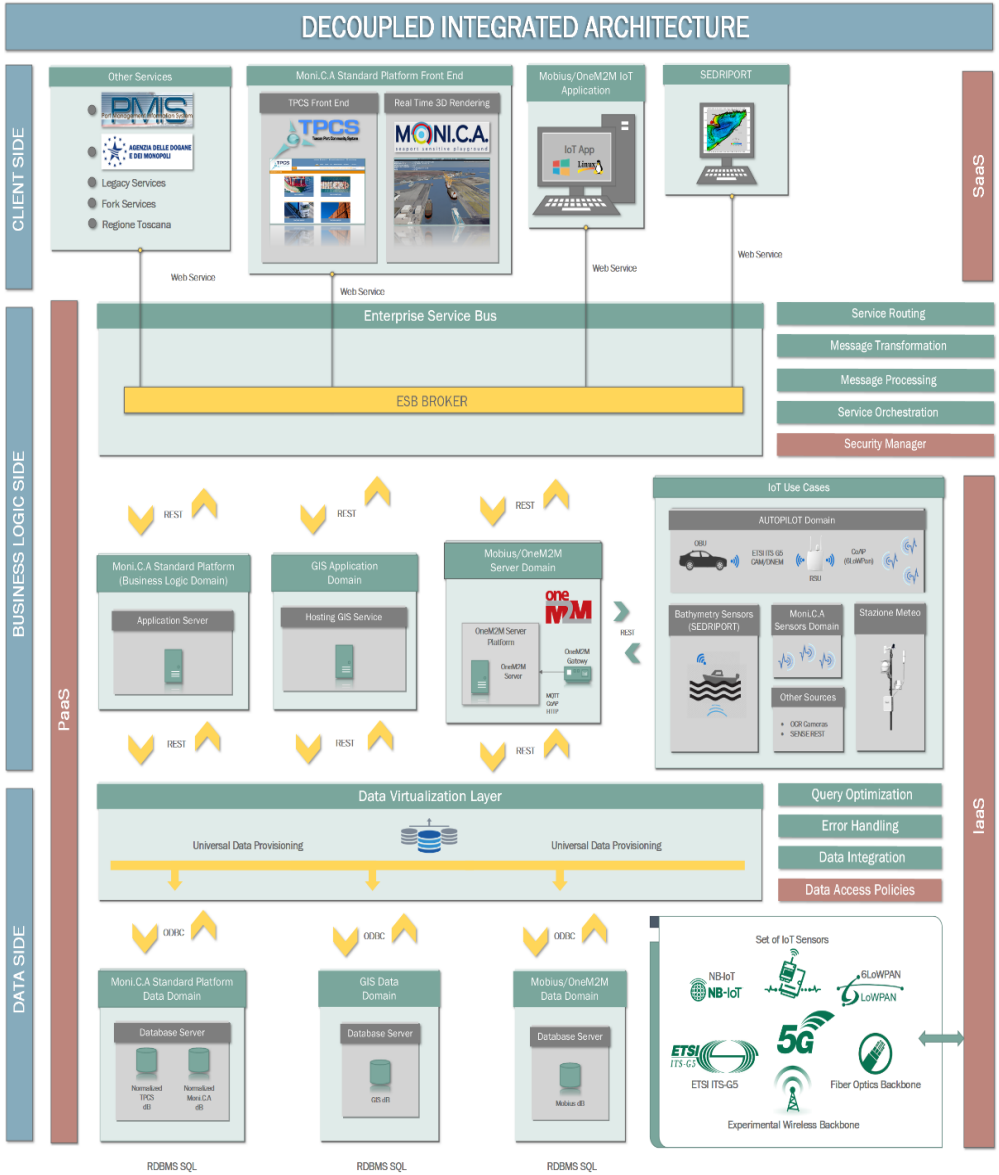
- Therefore open and standard technologies can boost innovation in the industrial sector:
  - adoption of standards are beneficial in the long term for the industrial sector.

Standards & Maritime Trade

- 22/2/2018: «Hapag-Lloyd CEO Rolf Habben Jansen has assured the market it has no plans to follow the terminal-owning strategy employed by the rest of the global container carrier» (Source: IHS Maritime & Trade, US);
- Drewry Maritime Research shows:
  - 11.7 million TEU handled by «THE Alliance» in 2016;
  - other haulers: 58.8 million TEU by 2M, 47.4 million TEU by Ocean Alliance.
- Why?
  - Standardization allows transparent processes independent of industrial control on the logistic node;
  - Outstanding role of port services.

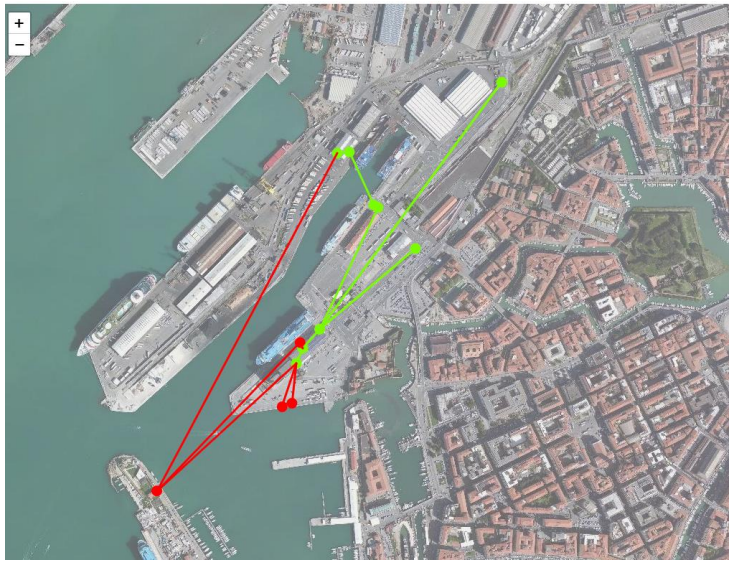
Livorno ICT architecture

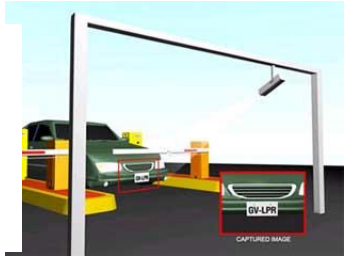
- Various ICT components produced by competing companies on specifications indicated by AdSP starting from international standards (e.g. ETSI, ISO, etc.);
- Towards lightweight app's rather than bulky packages.
- User profiles:
  - public user: calculation of the carbon footprint, modeling of emissions;
  - port community: process monitoring, industrial applications, security.



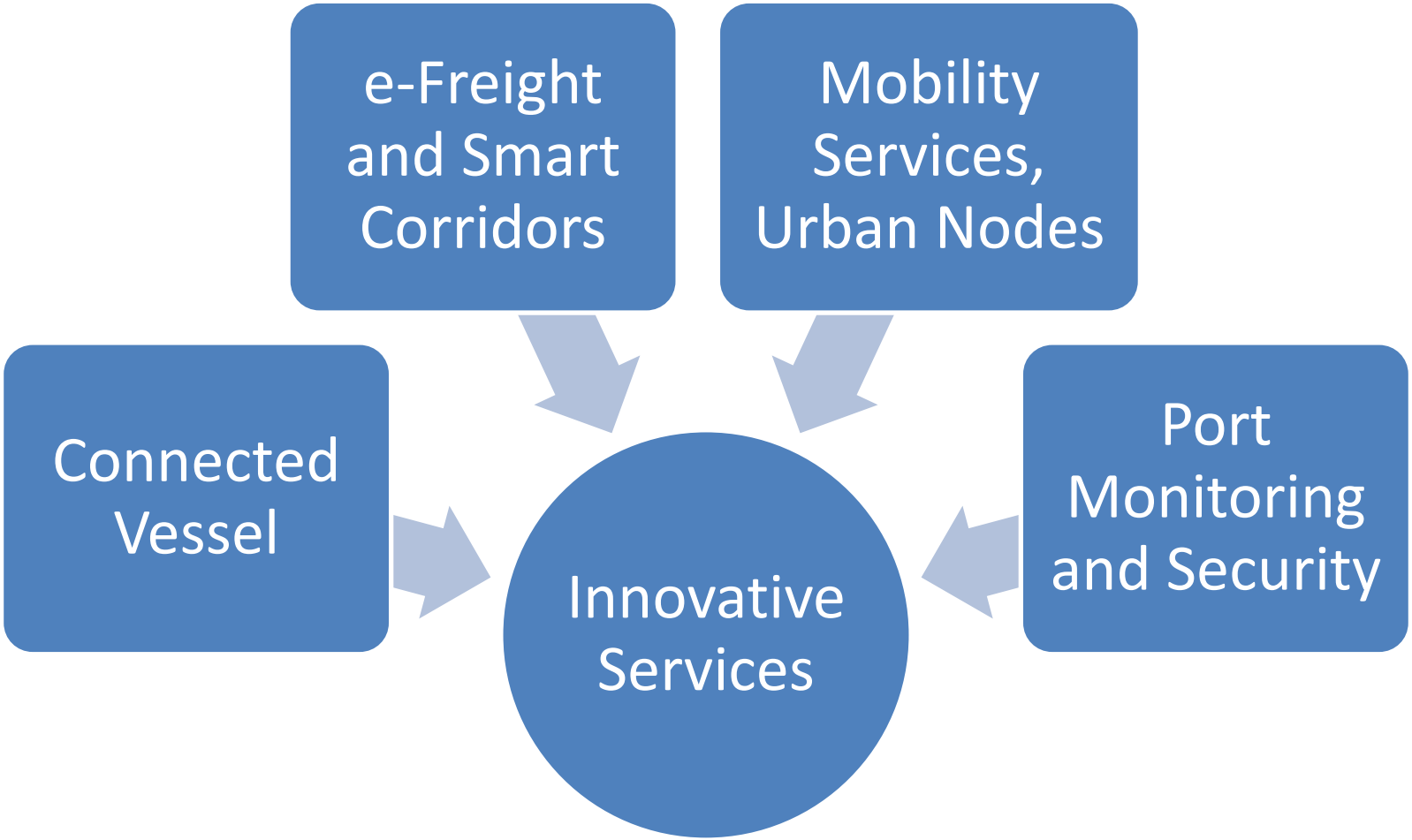
Networks, Sensors, Platforms

- Networks:
  - fiber optic infrastructure;
  - 100 Mbps wireless network around the maritime station;
  - vehicle network complying with the European ETSI-G5 standard (first "smart road" in Italy);
  - NB-IoT commercial network (first port in Italy);
  - 5G prototype installations (from December 2018, first port in Italy).
- Platforms:
  - compliance with OneM2M for the IoT;
  - data abstraction layer (independent of the DBMS technology).
- Integrated sensors:
  - connected vehicles, (soon) autonomous vehicles, (soon) connected ship, (soon) photonic radar, pollution sensors, OCR sensors, weather stations, (soon) LiDAR, (soon) bathymetric sensors





Vertical deployments

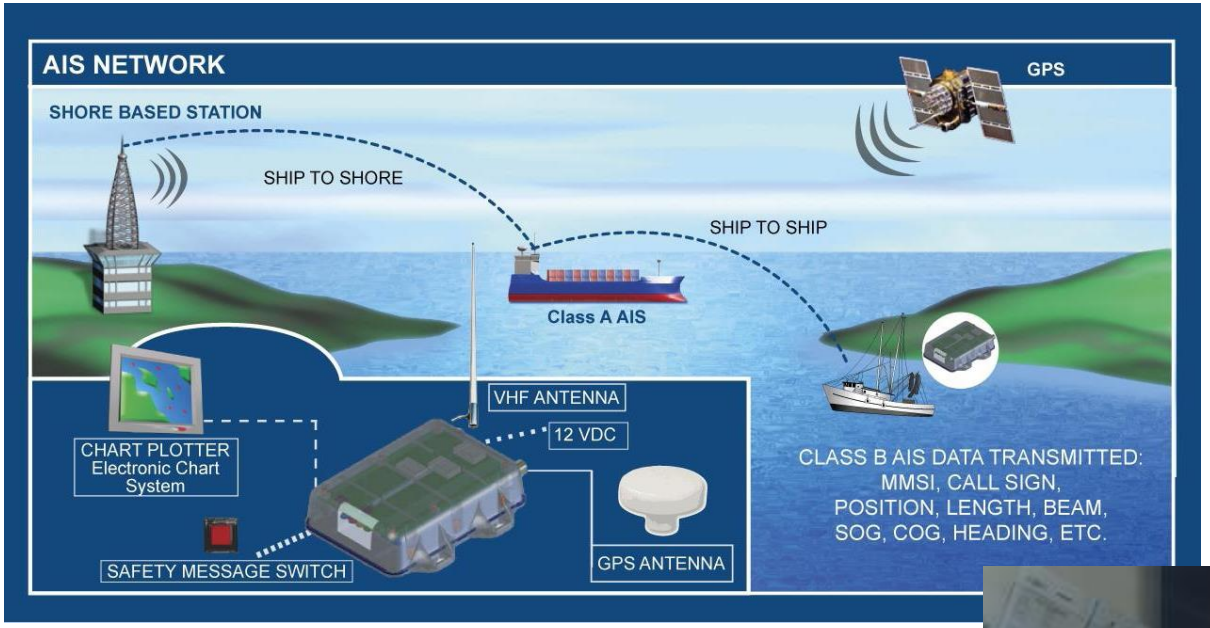


consorzio nazionale
interuniversitario
per le telecomunicazioni

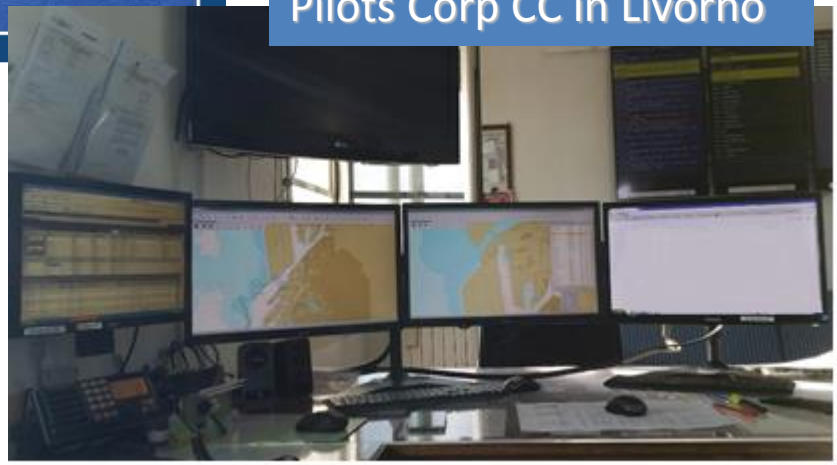
Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

«FOCUS: Connected Vessel»

SoTA equipment: VTS

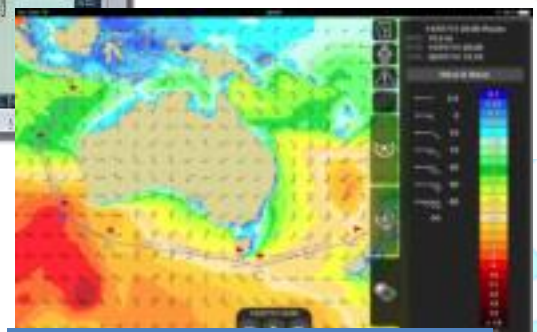


Pilots Corp CC in Livorno



Vessels Traffic Services: Information provided by AIS equipment, such as unique identification, position, course, and speed, can be displayed on a screen or an Electronic Chart Display and Information Systems (ECDIS)

SoTA: On-Board Equipment



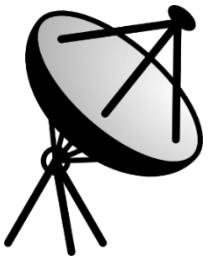
Assist pilots and other marine professionals in their daily routine, helping them to maintain efficient pilotage and other onboard operation

SoTA: Networks (SAT and mobile)

As the vessel enters the communication range of the port it can switch from satellite to terrestrial networks.

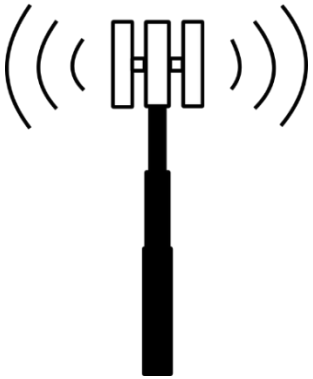
SAT:

- Point-to-Point bidirectional
- Bandwidth:
  - typical 10-20 Mbps,
  - dedicated 150 Mbps.
- Latency: order of 100 ms
- Reliability: High
- Cost: High



LTE:

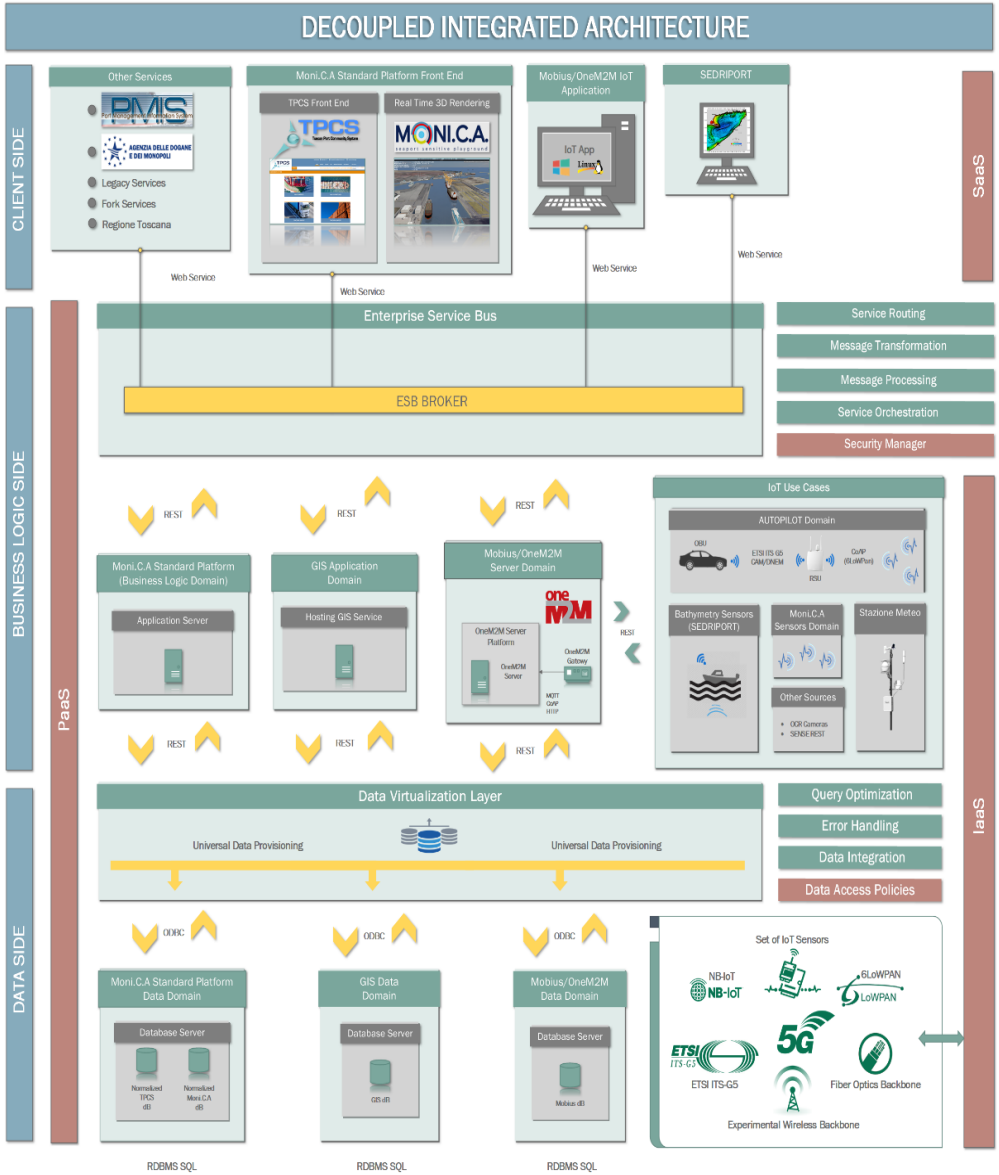
- Mobile Broadband
- Bandwidth: 100/50 Mbps
- Latency: < 10 ms
- Reliability: High
- Cost: Medium



Interesting 5G features

- What features of 5G…
  - Millimiter Waves, Small Cells, Massive MIMO, Beam Forming, Full Duplex, …
- …really matter for the "Connected Vessel"?
  - High Capacity (10 Gbps peak demand):
    - willing to accommodate real-time multimedia streams.
  - Low Latency (< 1 ms):
    - willing to neglect network transmission delays in Vessel Traffic Services.
  - Beam forming:
    - tracking the vessel and delivering data at specialized QoS.

Connected vessel on our stack



Connected Vessel Use Case

Wind Strenght
Congestion at the Port Entrance

Annotated real-time streams

Vessel View
Machinery status
Request of assisted berthing

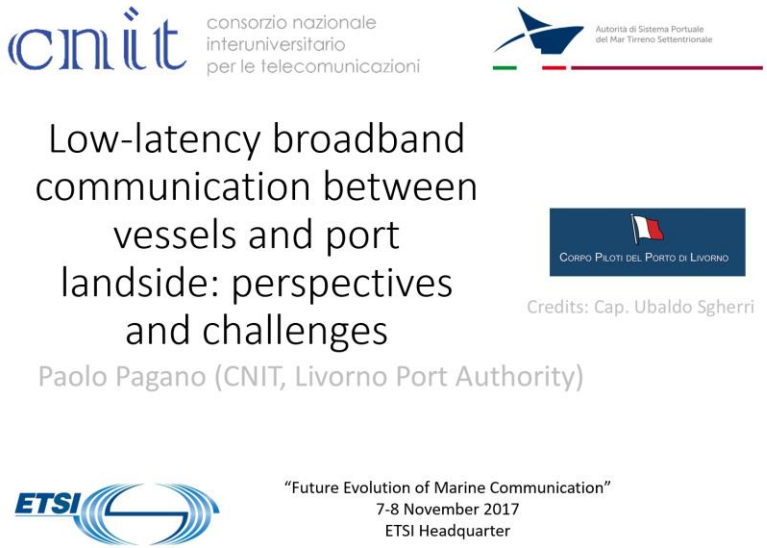
Malfunction logs

Connected vessel:

- managing vessel traffic;
- easing vessel maneuvering task.

Connected Vessel standardization

- IMO Global Maritime Distress and Safety System (GMDSS);
- AIS/VDES and DSC;
- ETSI EN 303 276 (broadband comm. off-shore);
- ITU-R band allocation;
- 3GPP TR 22819 (use of LTE in port areas).



consorzio nazionale
interuniversitario
per le telecomunicazioni

Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

«FOCUS: e-Freight and Smart Docks»

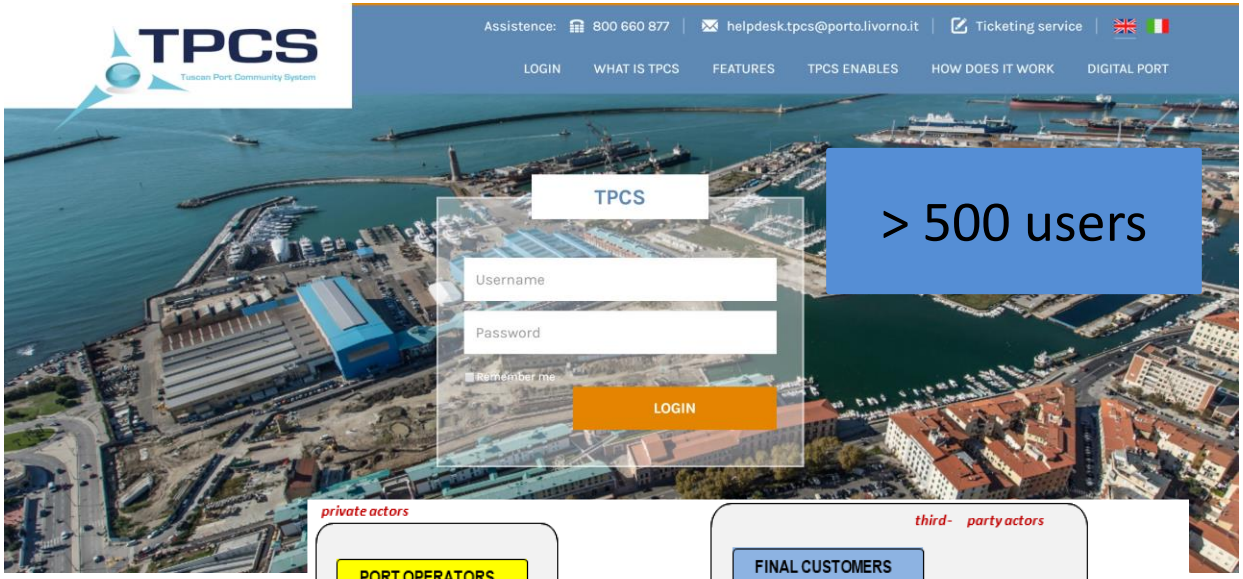
SoTA: PCSs

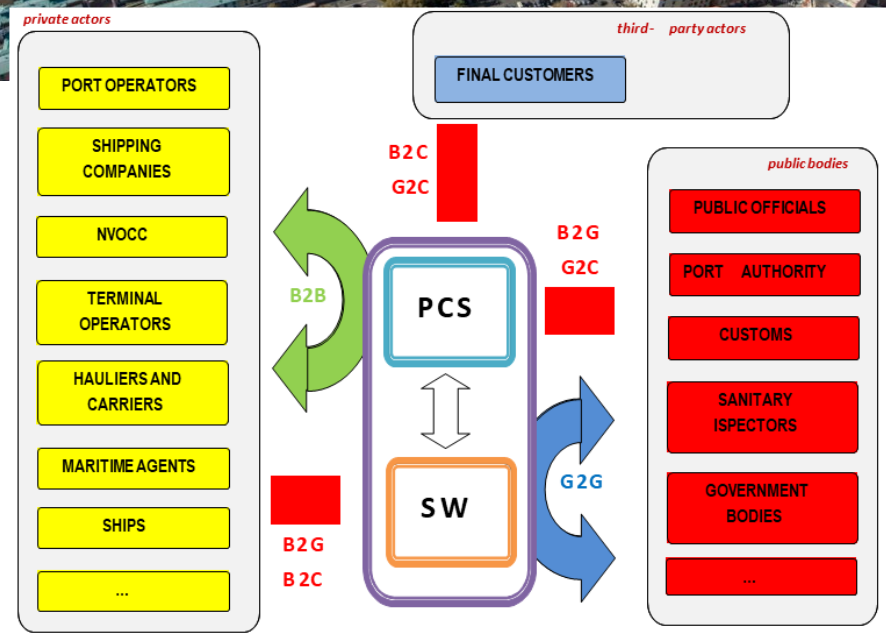
- Port Community System connects to the SPOC established at national level;
- Private and public institutions use PCS to:
  - enable intelligent and secure exchange of information,
  - interoperate with haulers TOS,
  - improve the efficiency and competitive position of the seaports,

  - automate smooth port and logistics processes through a single submission of data and by connecting transport and logistics chains.

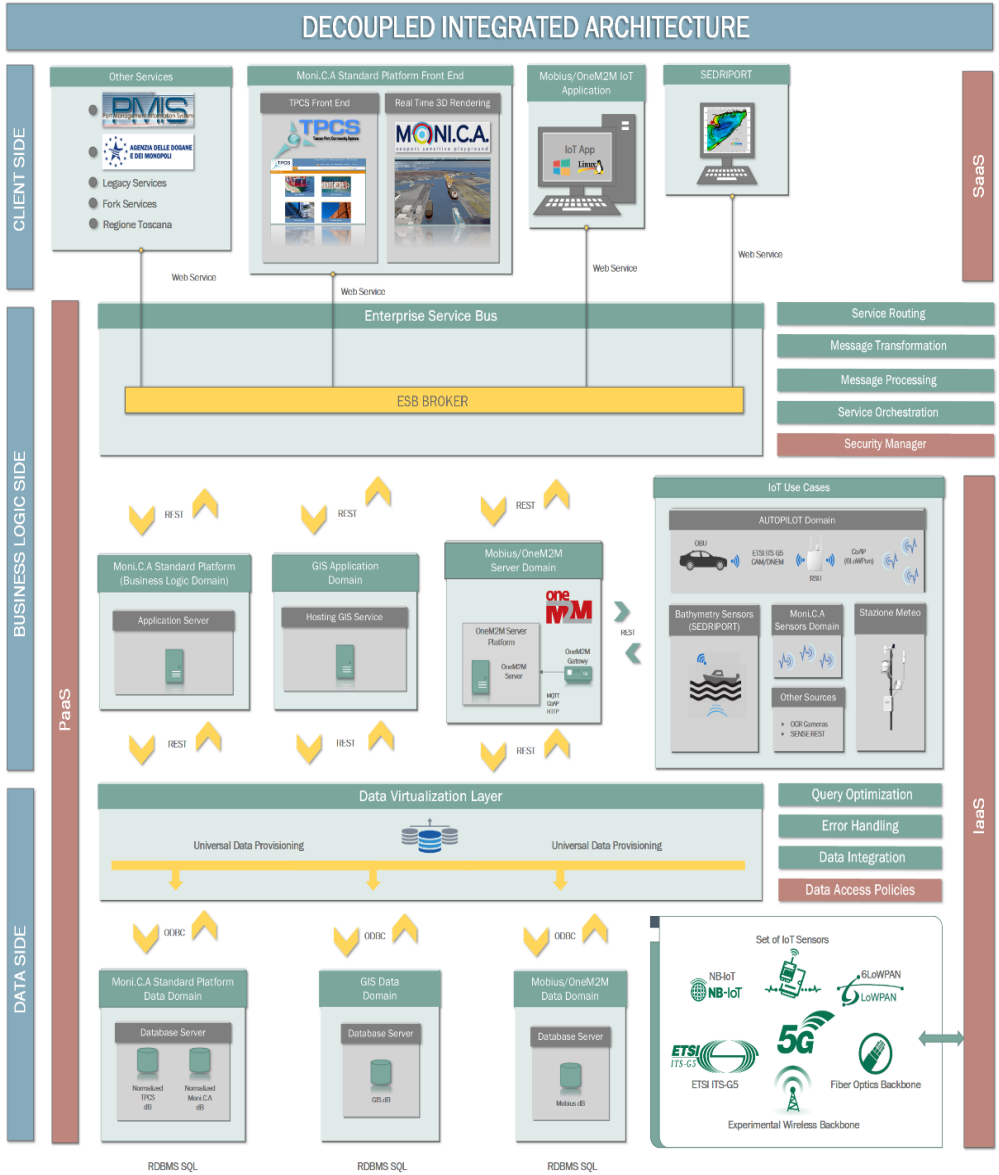
SoTA: Livorno logistics package

- Port Community & Single Window System
  - automate smooth port and logistics processes through a single submission of data and by connecting transport and logistics chains.
- Import
  - Telematics import procedures
  - Document valid for container release (DVRC)
- Export
  - Telematic export procedures
  - Telematic weight data (VGM)
  - Gate-in status
- Tracking
  - Checking ships on arrival/departure
  - Tracking goods in import/export



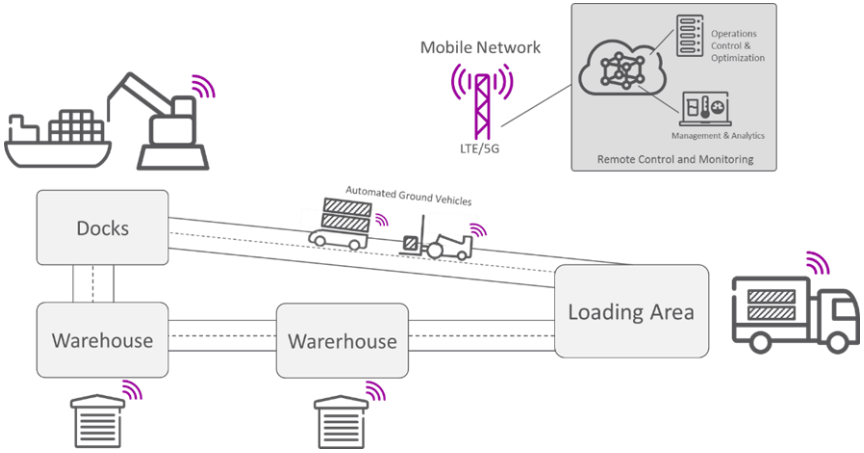


PCS on our stack



5G in Smart Docks

- 5G means low latency, high bandwidth, ad-hoc capabilities;
- Reduction of empty trips in containers terminals:
  - by connecting PCS and mobility services enabled by the digital agenda of the Port Authority in C-ITS:
    - a full logistics end-to-end service chain can be implemented.
  - unbounded data flow among machines (sensors and vehicles), humans, and central systems.



- Enhancement of safety footprint in freight terminals:
  - by interoperating field components (devices integrated in containers, sensors implanted in docks and terminals, pervasive gateways and service points) with information systems in the cloud, new services will be implemented in the real-time monitoring platforms .

consorzio nazionale
interuniversitario
per le telecomunicazioni

Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

«FOCUS: ITS and Mobility»

Intelligent Transportation Systems

- The term **ITS:**
  - (**Wikipedia**): refers to efforts to add ICT to ***transport infrastructure and vehicles*** in an effort to manage factors that typically are ***at odds with each other***, such as vehicles, loads, and routes to improve safety and reduce vehicle wear, transportation times, and fuel consumption.
- Buzzwords:
  - vehicular networks, c-roads / smart roads, Cooperative ITS (C-ITS), Cooperative and Connected Automated Mobility (CCAM).

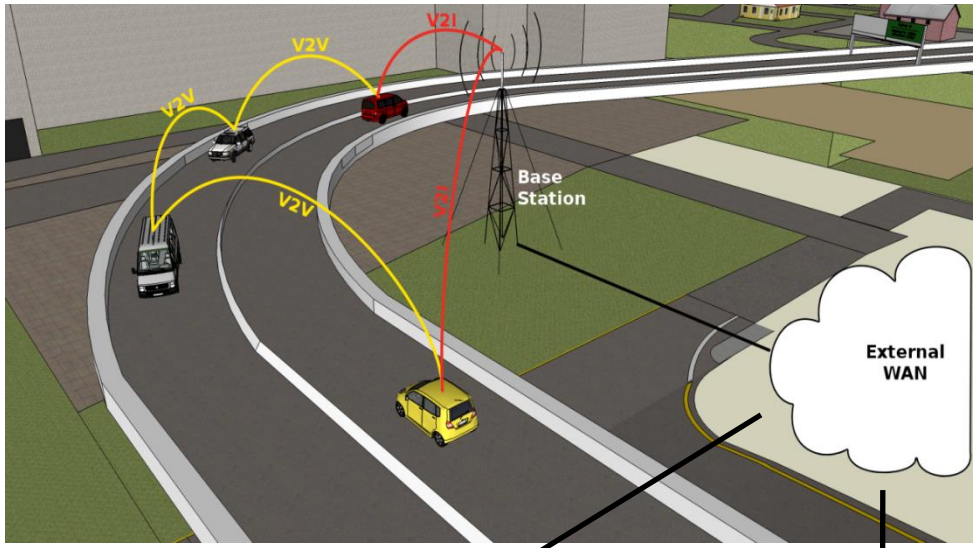
- Motivations:
  - reduction of public costs (e.g. pollution, deseases, deaths, etc.) introduced by undisciplined transportation;
  - improvement of the “transport systems”;
  - ICT innovation for sensing, telecommunication, services.

CCAM: business case

- 2017: European connected and autonomous car market is worth € 16.4 billion
- 2022: European connected and autonomous car market is worth € 48 billion
- Every euro invested in vehicles and e-infrastructure generates estimated benefits of over 3 euros
- Save over € 200 billion in social spending for minor accidents if all vehicles were connected and autonomous Savings of over 50 billion euros for lower fuel consumption if all vehicles were connected and autonomous
- Sector involving new stakeholders: Apple, Google, Samsung, Intel, ...

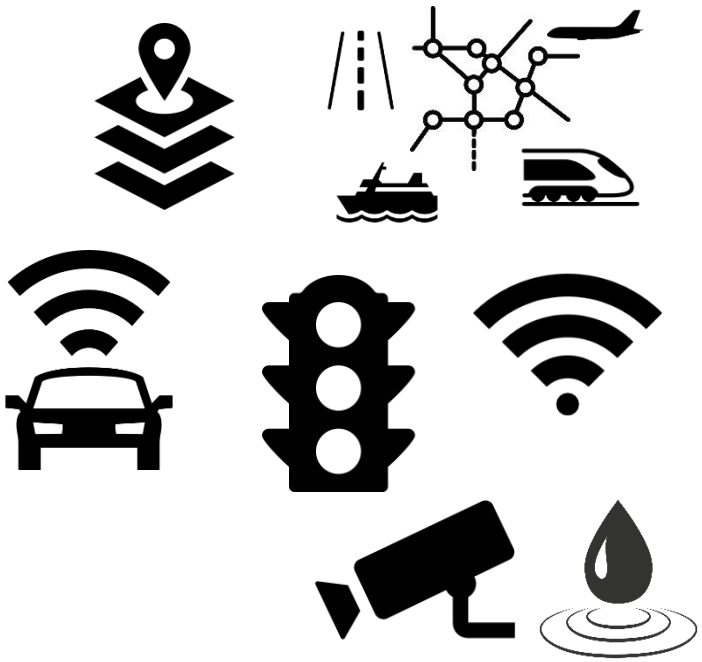
Source: TTS ITALIA

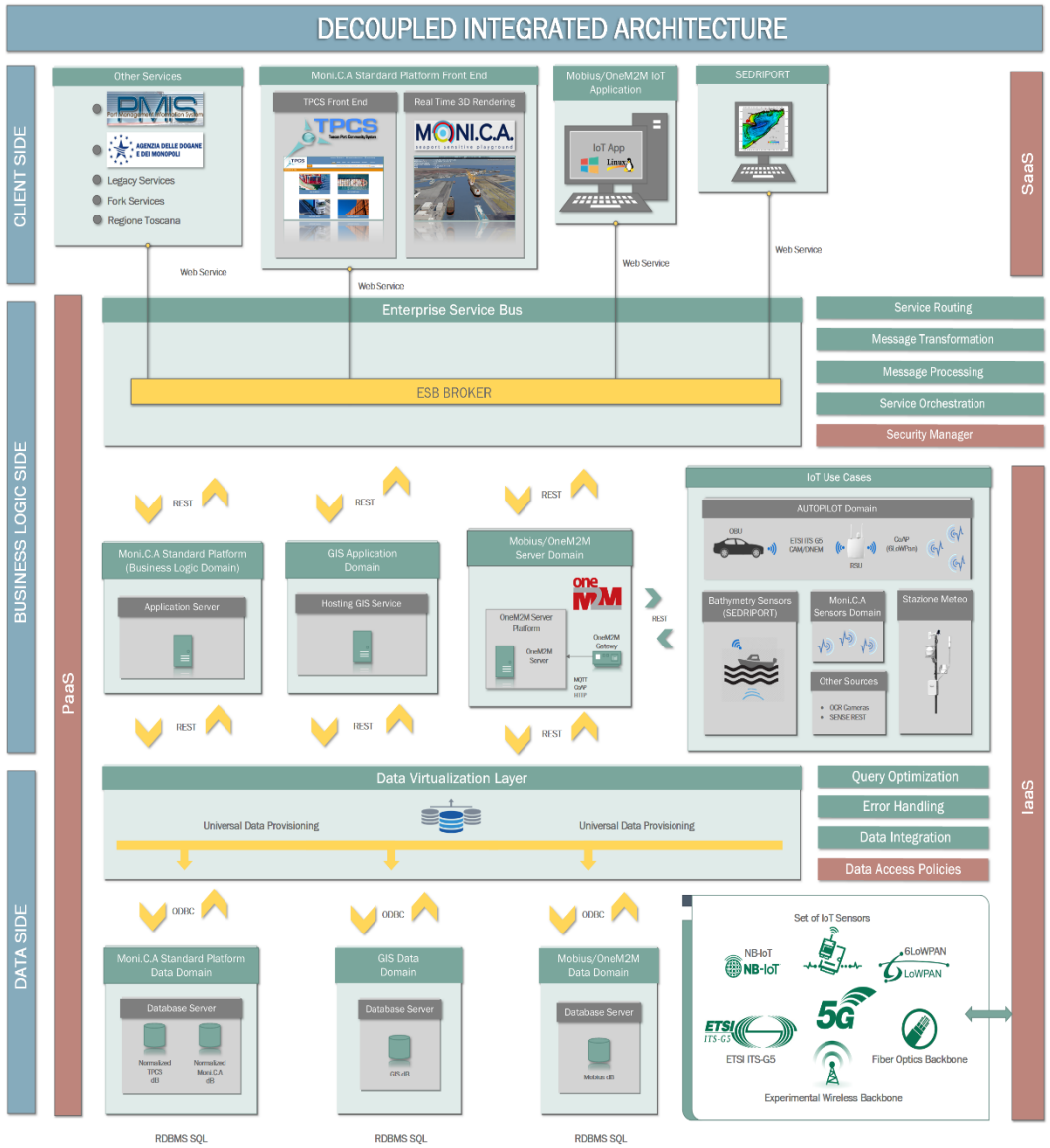
KETs for ITS



- in-vehicle systems
  - embedded systems OEM, new functions (ADAS)
- nomadic systems
  - pervasive devices, (e.g. smartphones)
- infrastructure devices
  - road-side / in-road devices
- cooperative systems
  - interconnecting a vehicle with other devices (notably other vehicles and infrastructure)

CCAM on our stack

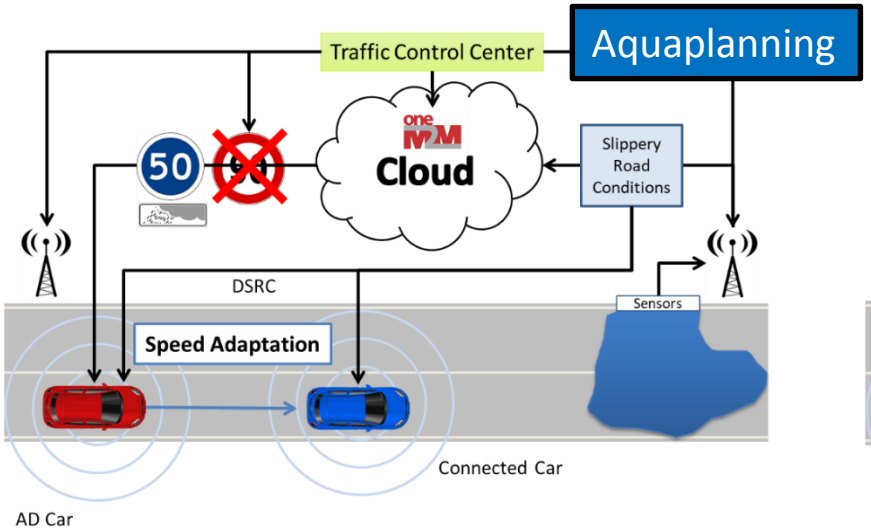


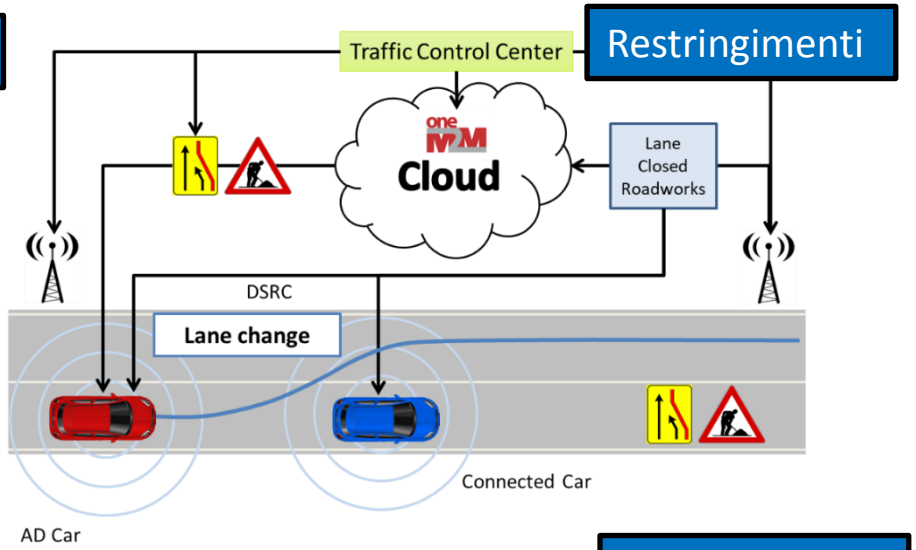


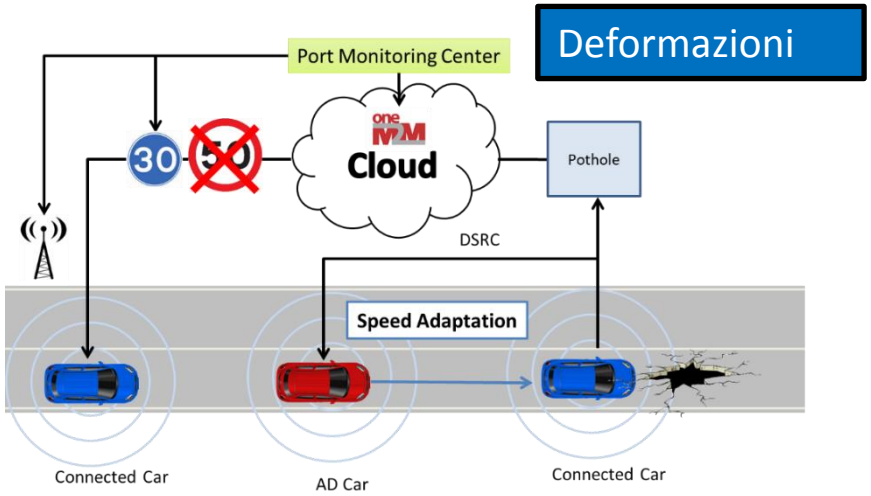
Autonomous Driving

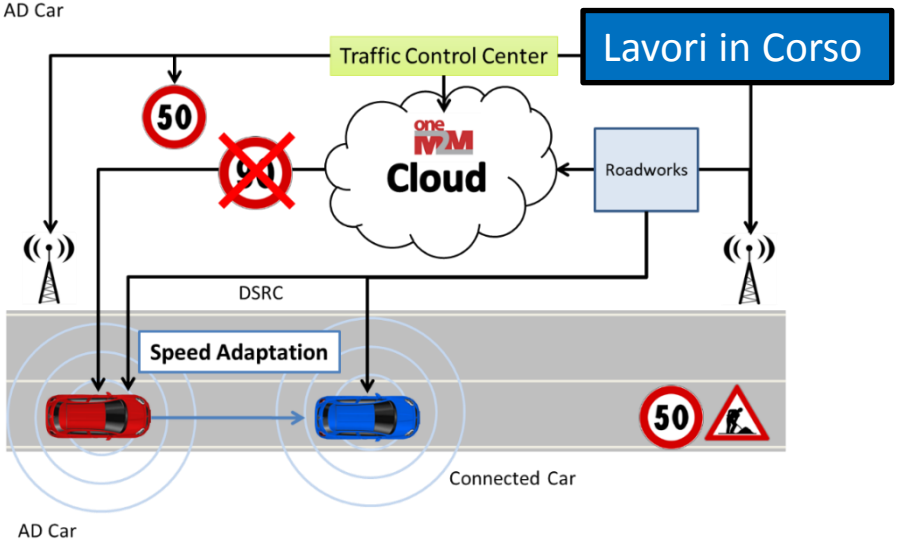
- Autonomous Driving in the IoT:
  - Re-use of the 2016 ITS CMS-5 ETSI/ERTICO Plugtests™ facilities:
    - Florence – Livorno highway and traffic control center (Empoli);
    - road access to the Livorno sea port terminals.
  - First Smart Road in Italy, public demo in Oct. 2018

Use Case Gallery (1/2)

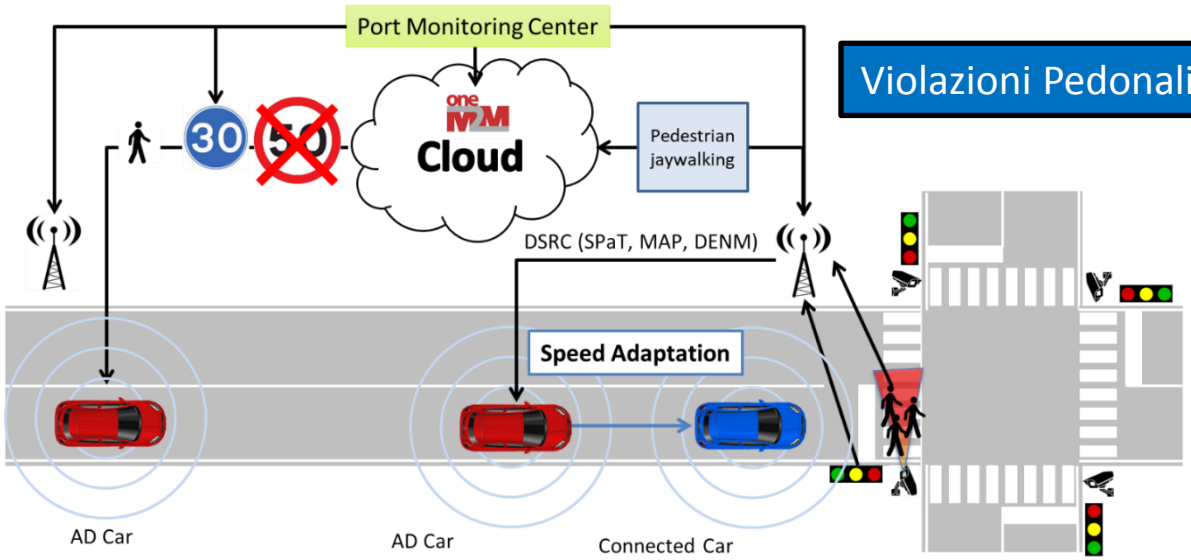




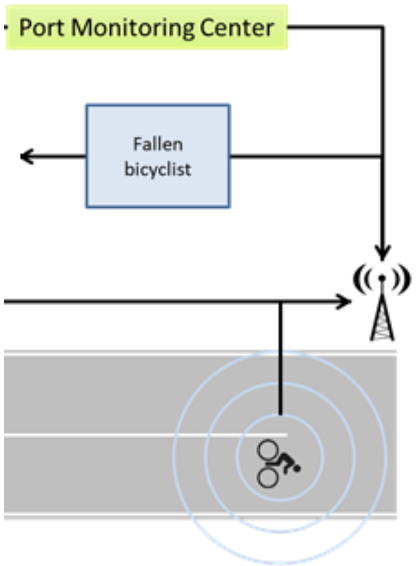




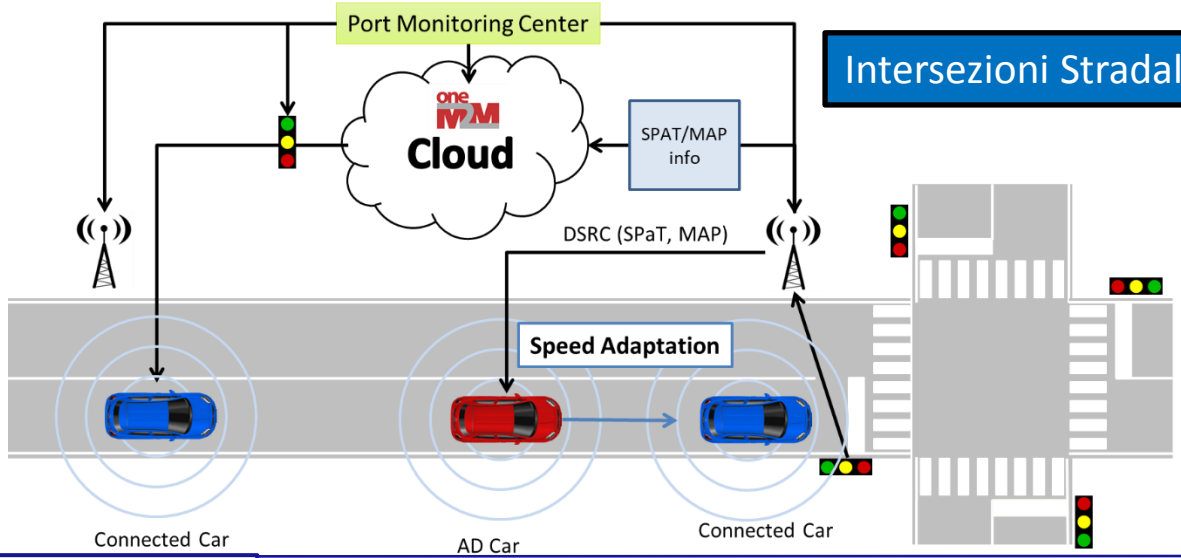
Use Case Gallery (2/2)



Violazioni Pedonali



Ciclisti Incidentati

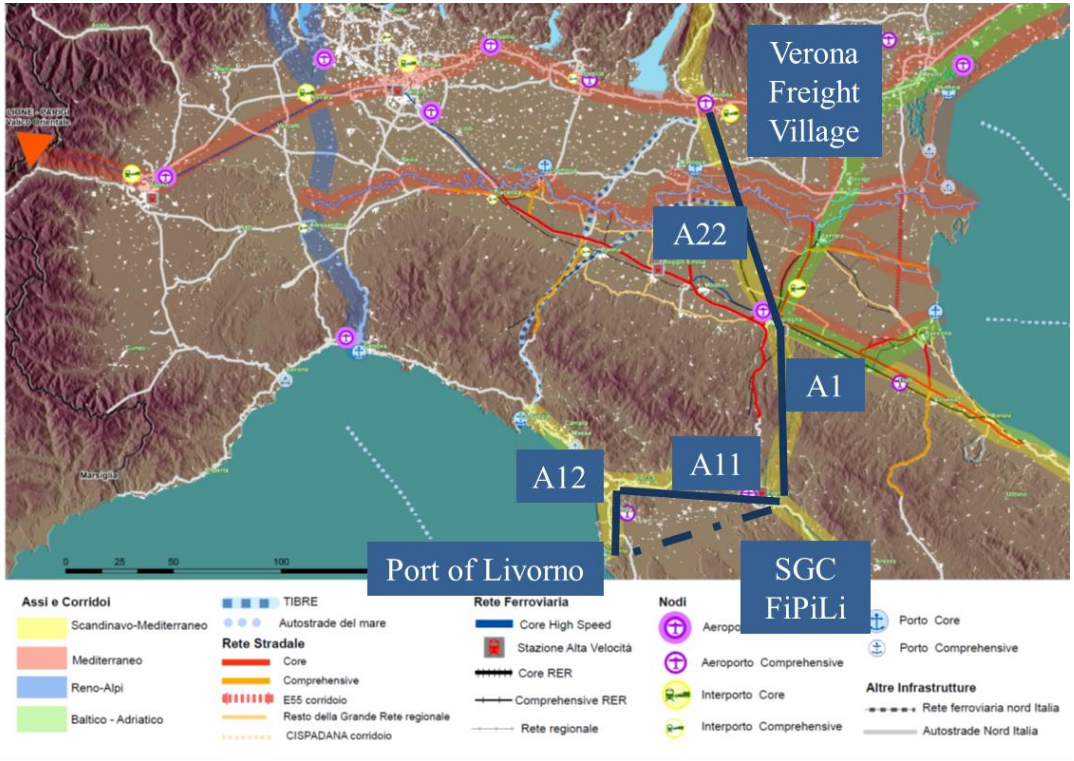


Intersezioni Stradali

C-ITS at corridor level

URSA MAJOR neo · instituto de telecomunicações · cnit consorzio nazionale interuniversitario per le telecomunicazioni

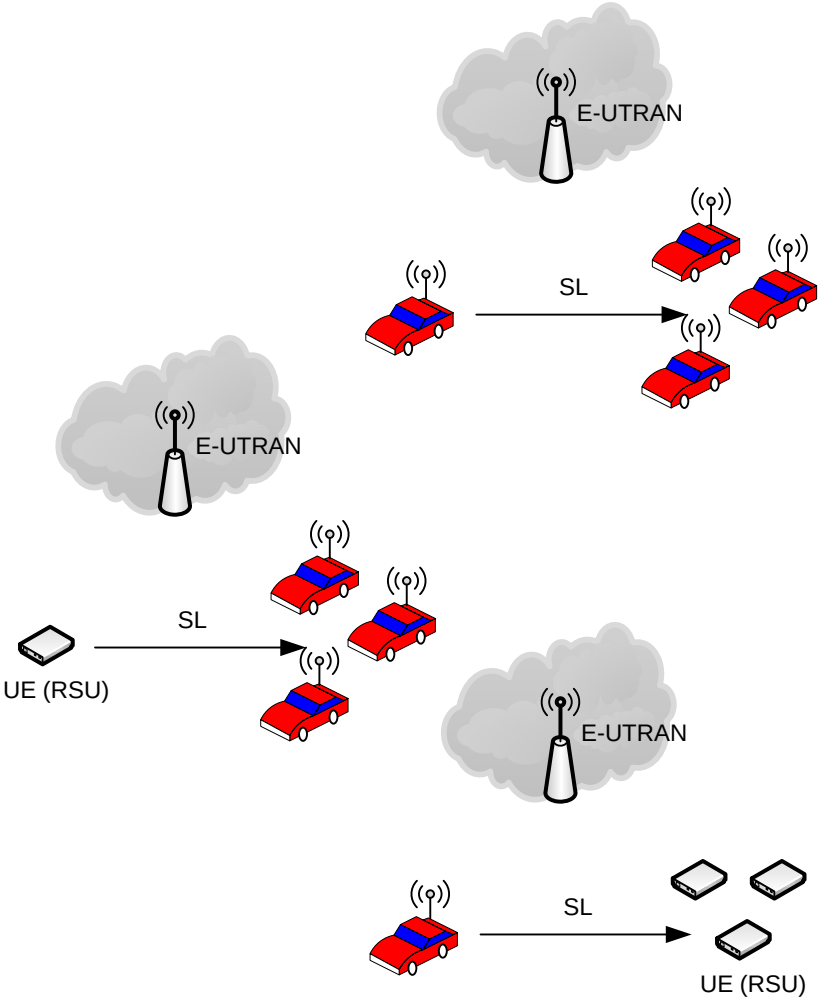
- Turning R&D in C-ITS into services to freight carriers;
- Cooperation with Verona Freight Village.



- C-ITS for Pan-European Corridor 5:
  - Bottleneck removal service: Real-time information and early notification about potential congestion;
  - Safety information services: Real-time information about hazards detected along the route;
  - Smart Truck Parking: Drivers will be suggested temporary parkings and specific time slot (truck appointments) to enter the port premises based on terminal handling capabilities at the port of Livorno.

Connected vehicles towards 5G

- In 3GPP:
  - Release 14:
    - LTE-based V2X Services;
    - Support for V2V services based on LTE sidelink.
  - Towards Release 15 (pre-5G release).
- In ETSI:
  - NWIs (GeoNet and BTP) approved in October '17
  - Call for Plugtests in Q2 2018 (ITS(17)026037)
  - 3GPP vs 11p ongoing performance assessment
- From EC:
  - Technology neutrality of 5.9 GHz



consorzio nazionale
interuniversitario
per le telecomunicazioni

Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

«FOCUS: Port Monitoring and Security»

What's happening on the IoT?

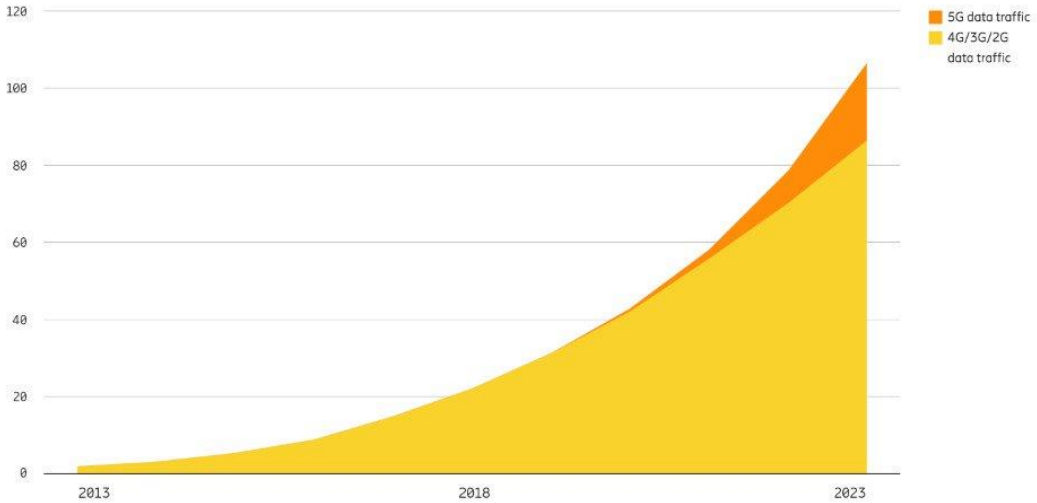
Connected devices (billion)

IoT	2017	2023	CAGR
Wide-area IoT	0.8	4.1	30%
Cellular IoT[1]	0.7	3.5	30%
Short-range IoT	6.2	15.7	17%
Other devices			
PC/laptop/tablet	1.6	1.7	0%
Mobile phones	7.5	8.6	2%
Fixed phones	1.4	1.3	0%
Total connected devices	**17.5**	**31.4**	**11%**

[1] These figures are also included in the figures for wide-area IoT

Ericsson Mobility Report June 2018

Global mobile data traffic (exabytes per month)

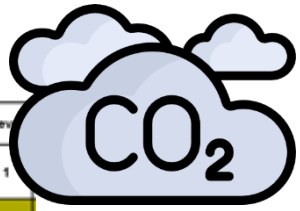


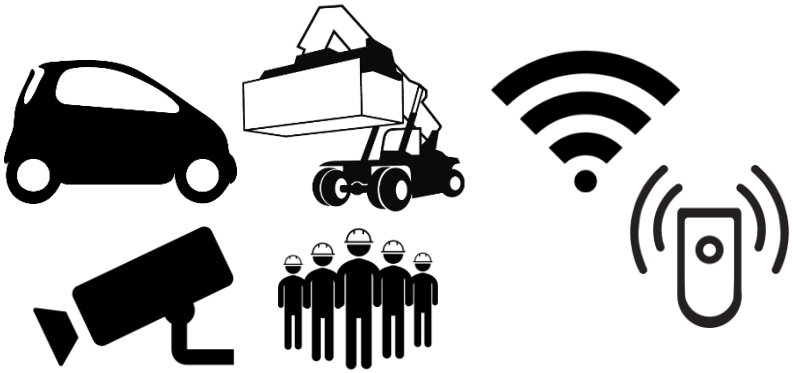
Ericsson Mobility Report June 2018

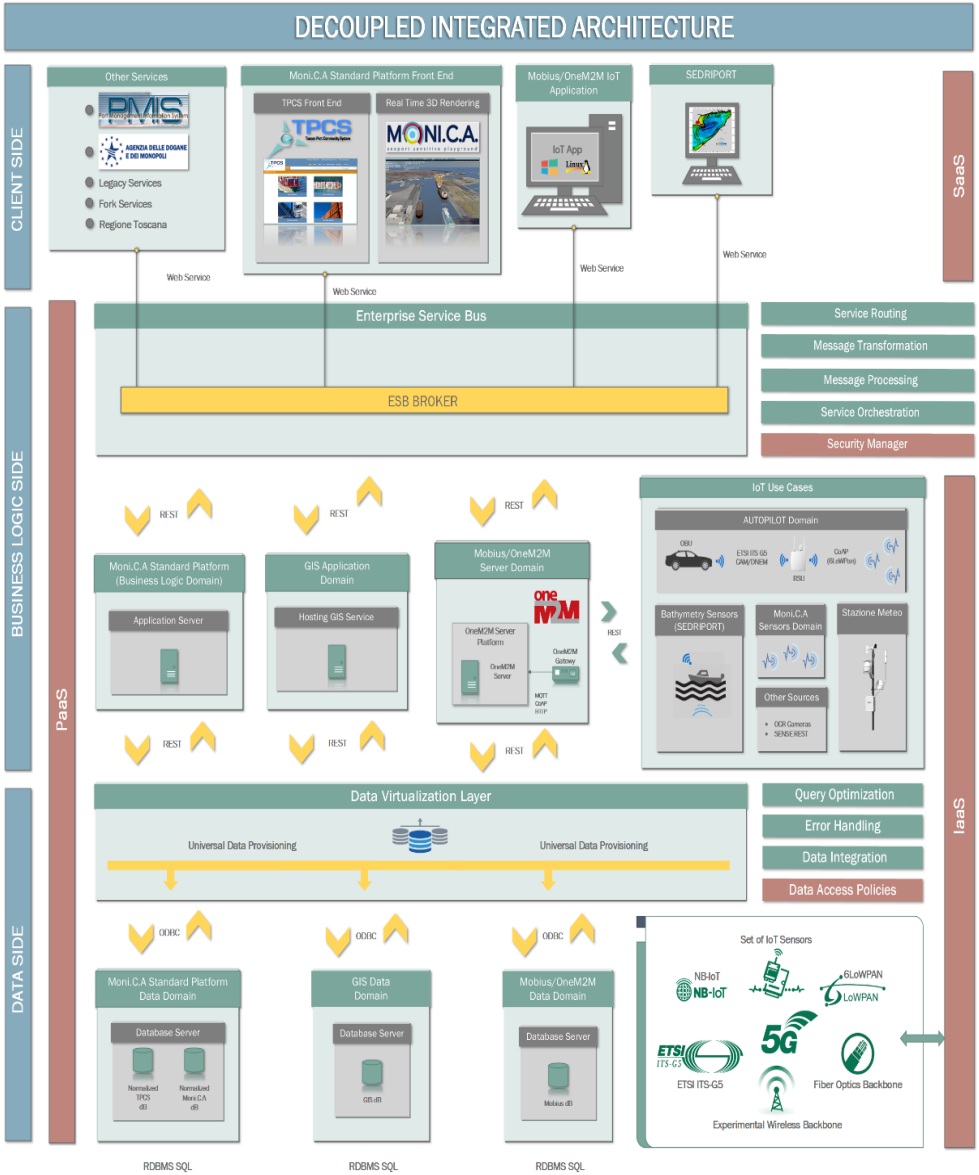
- Many M2M devices are being connected to information systems (e.g. gas and liquid pipelines, critical infrastructures, power plants)
  - (data) fetch and forward in low rate access networks
  - simple on-board logic
  - simple interaction model (REST)
- To safely accommodate more streams of M2M data:
  - (IP-compliant) secure communication for the IoT

Security on our ICT stack

Risk	Harm caused	Lev
Negligible	Minimal injury requiring no/minimal intervention or treatment	1
Minor	Minor injury or illness, requiring minor intervention	2
Moderate	Moderate injury requiring professional intervention	3
Major	Major injury leading to long-term incapacity/disability	4
Catastrophic	Incident leading to death or an event which impacts on a large number of patients	5







Cyber-security and 5G

- Relying on standards for cyber-security (for components, modules, units, systems):
  - "Security Test and Assessment" (NIST SP 800-115);
  - "Guide for Conducting Risk Assessment" (NIST SP 800-30);
  - "Guide to Computer Security Log Management" (NIST SP 800-92)
    - it can be seen as a best practice endorsing «Security by Design»;
    - log management in distributed systems is risky by definition.
- In 5G:
  - convergence of access and metro networks;
  - outstanding role of NFV (and towards MEC);
  - «security by design» is not an option but mandatory.

consorzio nazionale
interuniversitario
per le telecomunicazioni

Autorità di Sistema Portuale
del Mar Tirreno Settentrionale

Conclusions

Conclusions

- The Port Authority (supported by CNIT):
  - has a digital agenda oriented towards the sustainable growth of the area of competence;
  - has an unquestionable recognition in the international field;
  - has enabled a digital infrastructure capable of delivering innovative services;
  - focuses on standardization and interoperability in collaboration with major European ports and industrial partners;
  - wants the full involvement of the port communities in the development, prototyping and production of services.
- We have presented some examples:
  - in the domain of navigation services and the connected ship;
  - for integration along the regional, national, and trans-European logistics corridor;
  - for passenger (inter-modal) transport, for public transport and for access management and transit authorizations;
  - for cybersecurity and risk management in the port area.

Courtesy of: Corpo Piloti del Porto di Livorno

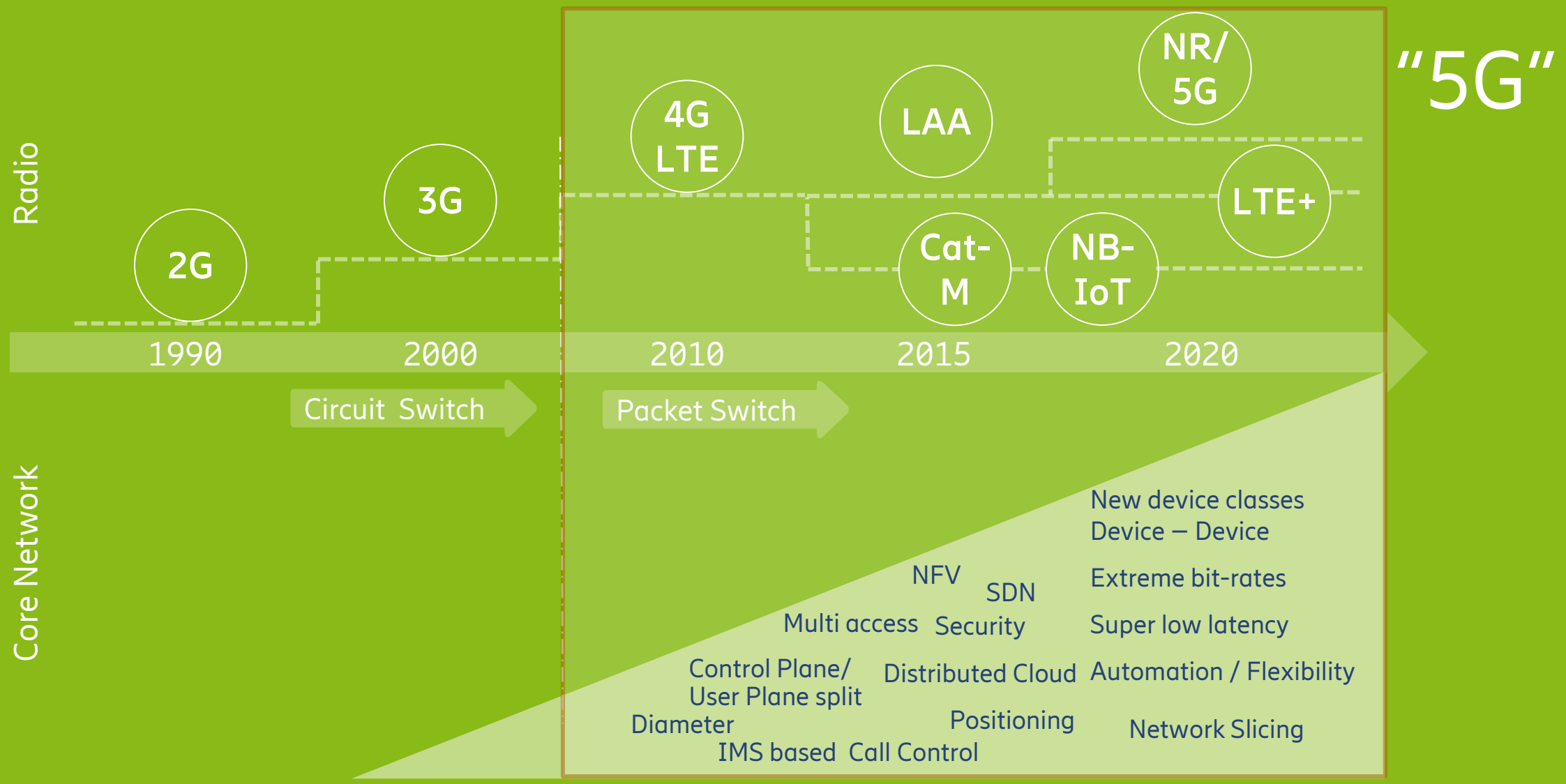
5G and Network Slicing

Håkan Djuphammar

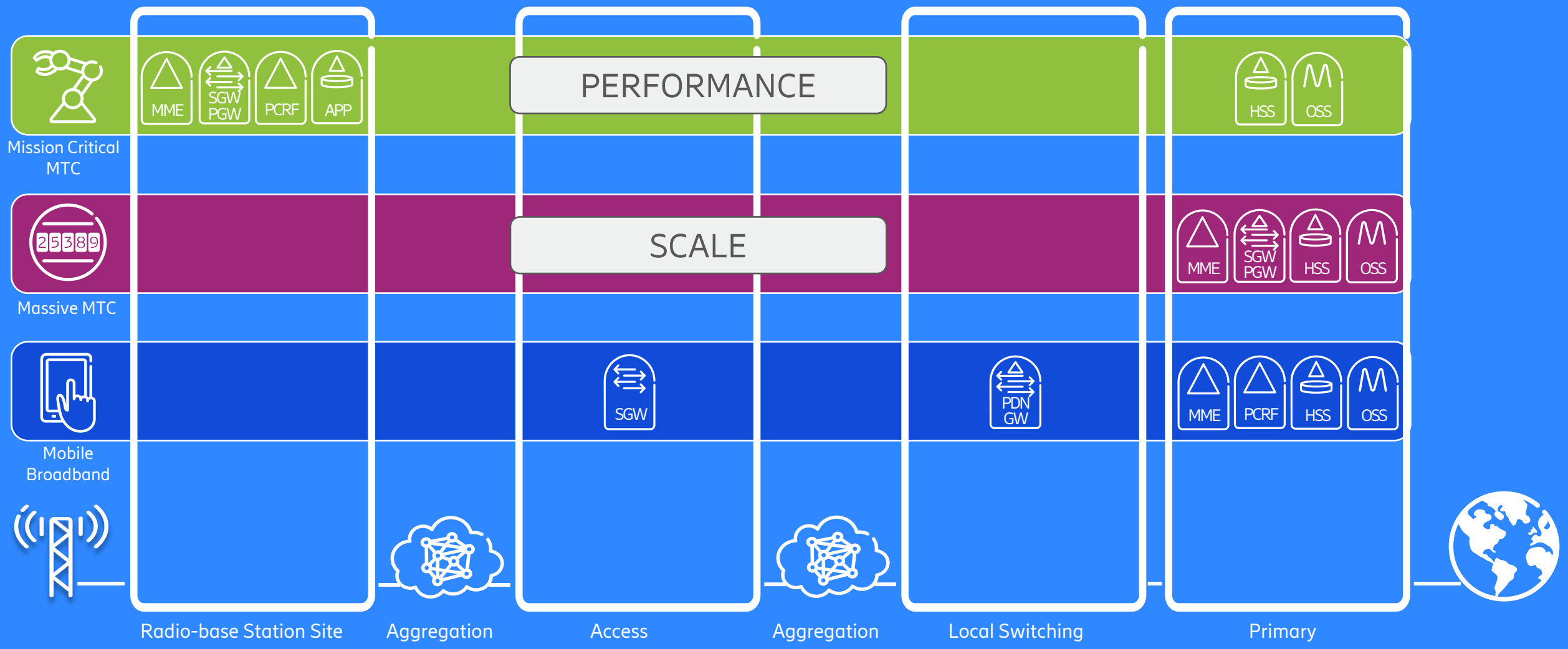
Ericsson CTO Office

2018-06-26

The evolution towards 5G



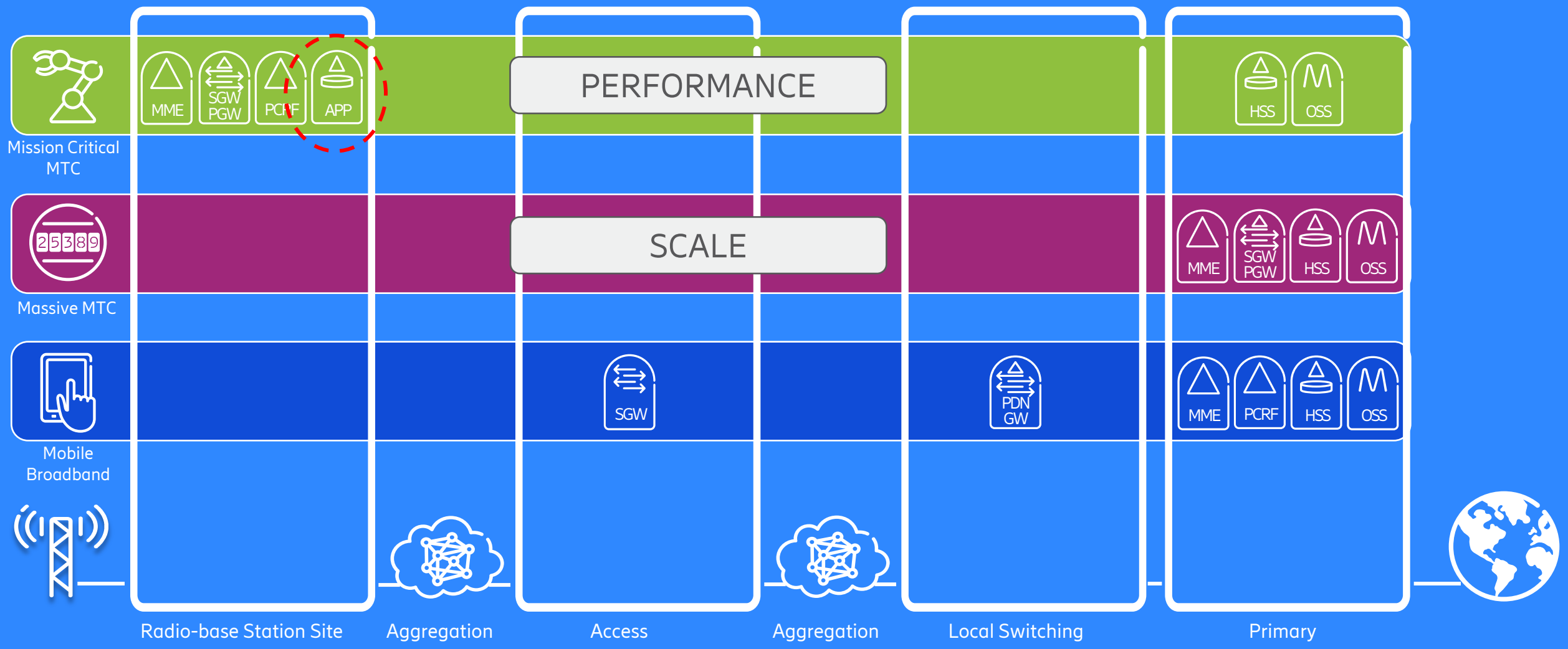
NETWORK SLICING



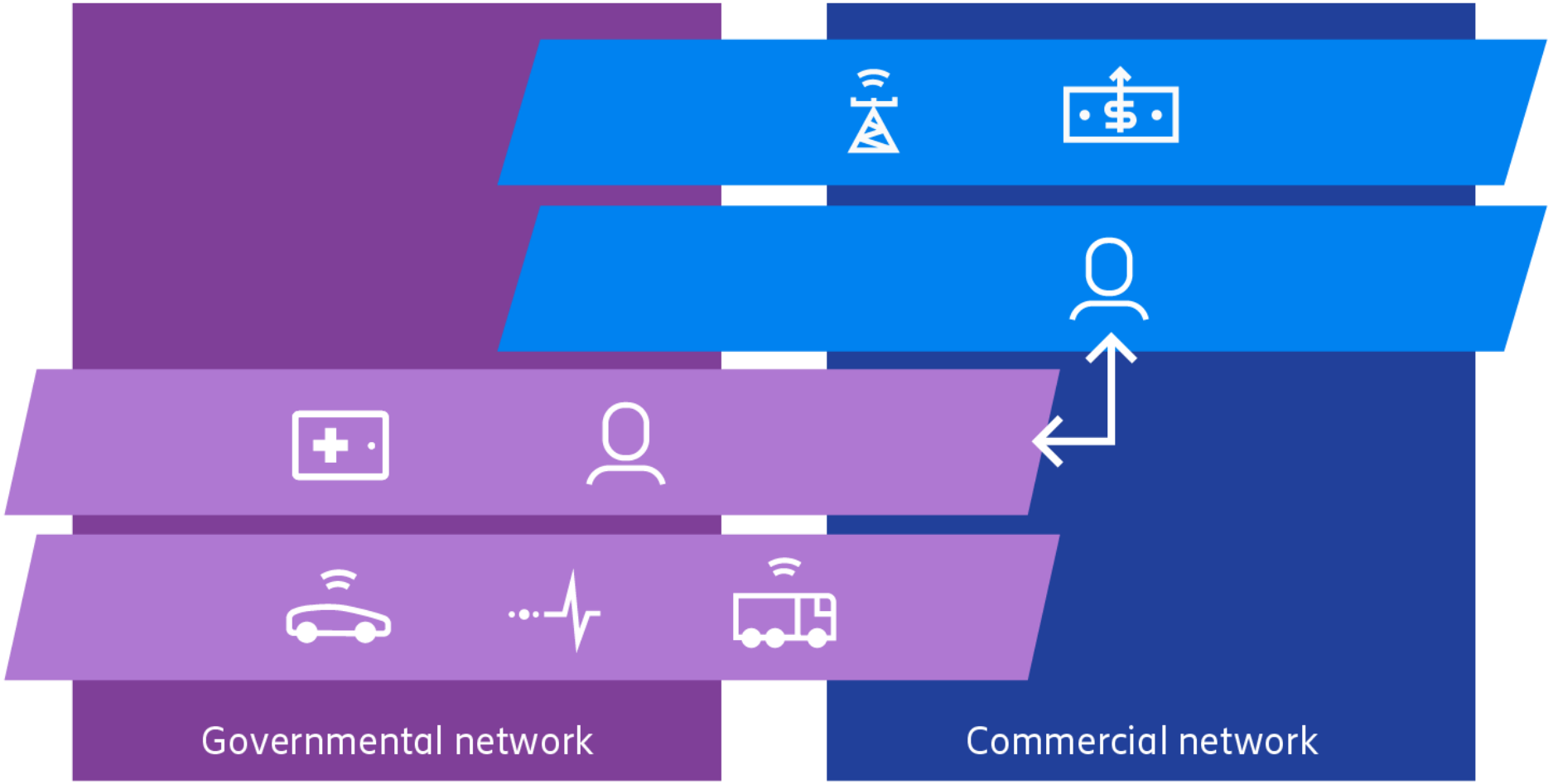
Federation

- Interconnect
- Roaming

NETWORK SLICING



National Secure Symbiotic Network

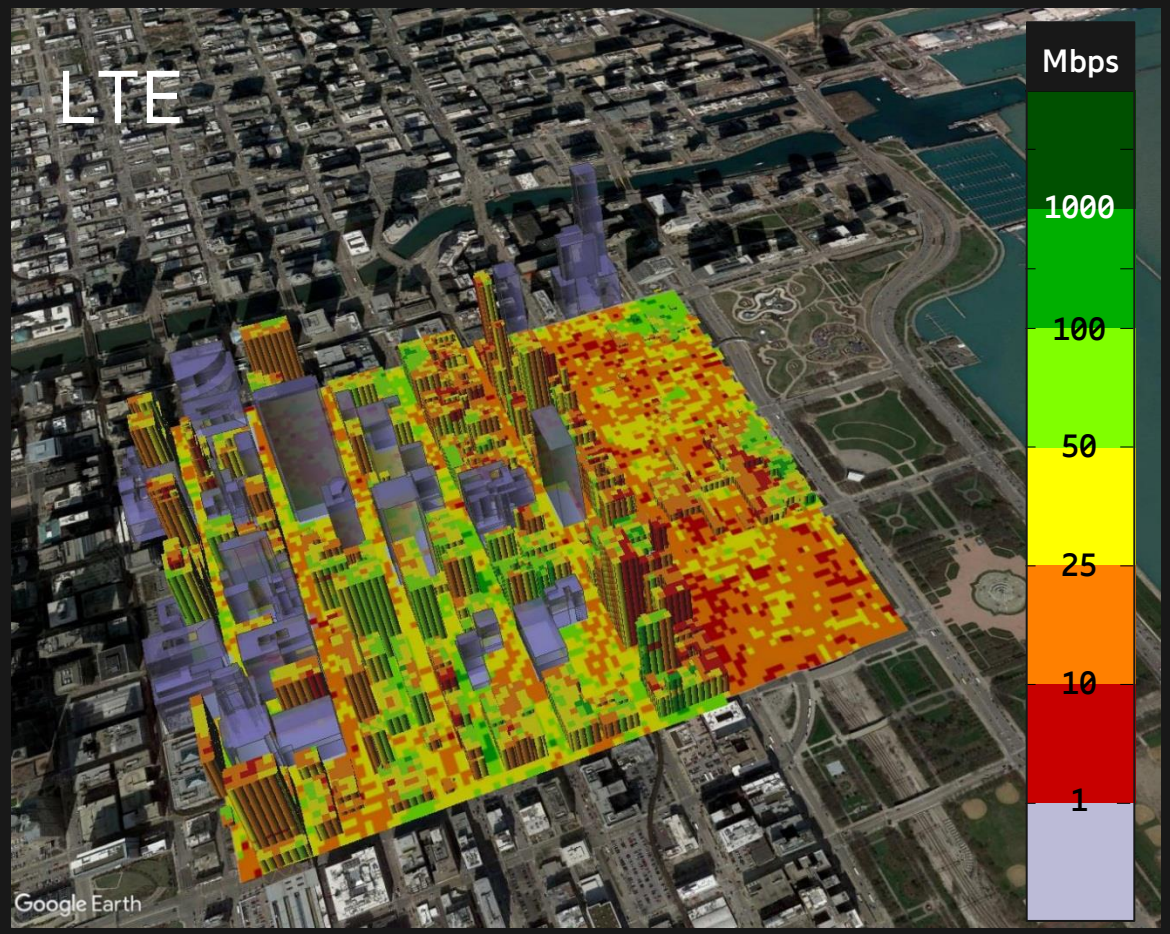


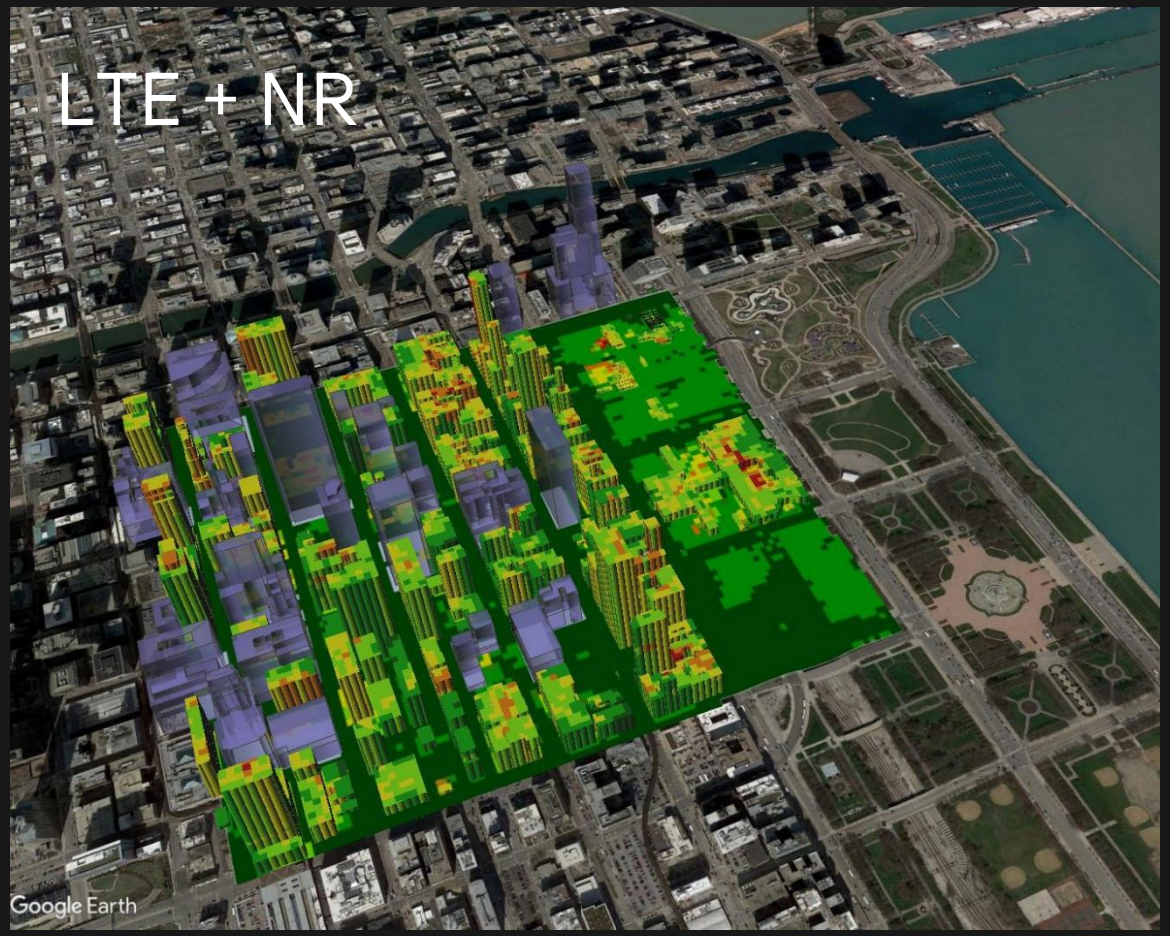
5G radio network efficiency

Magnus Frodigh, Ph. D.
Acting head of Ericsson Research

Chicago – 28 GHz coverage

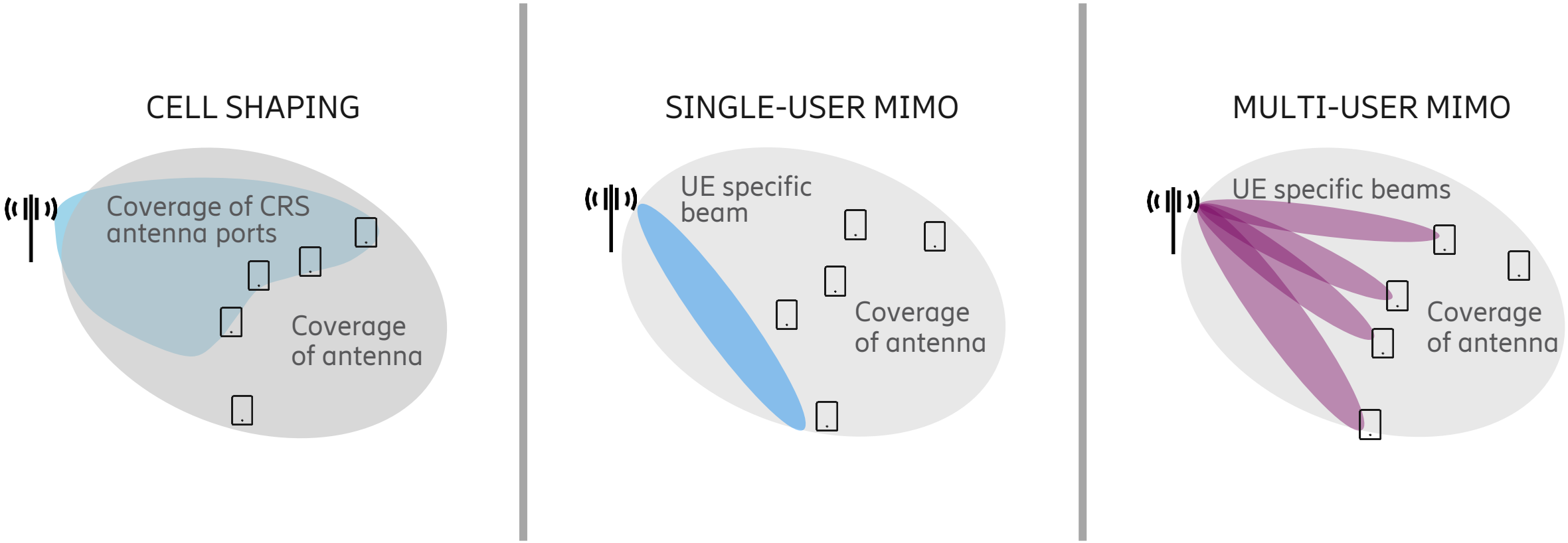
NR on 200m ISD street-cell layer





Key technology components

Massive MIMO



Example antenna gains for high rise and low rise dense urban

Asian high-rise dense urban scenario

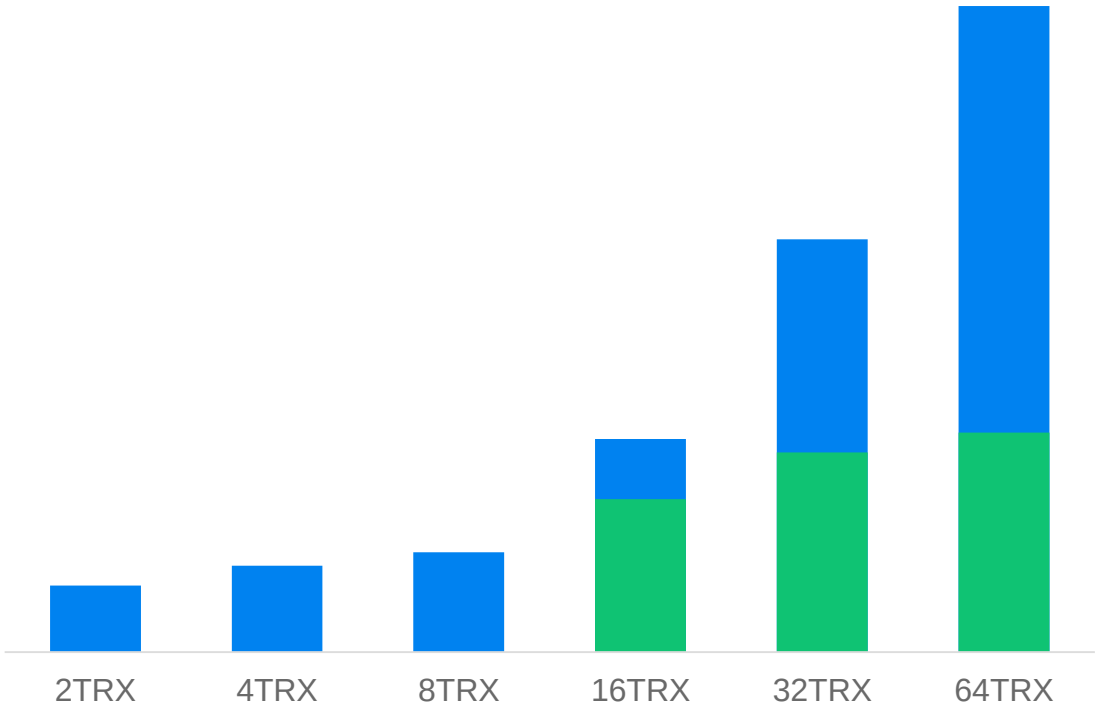
200m inter-site distance, 80% indoor traffic

Very substantial gains up to 64 TRX

European low-rise urban scenario

500m inter-site distance, 50% indoor traffic

Significant gains up to 32 TRX



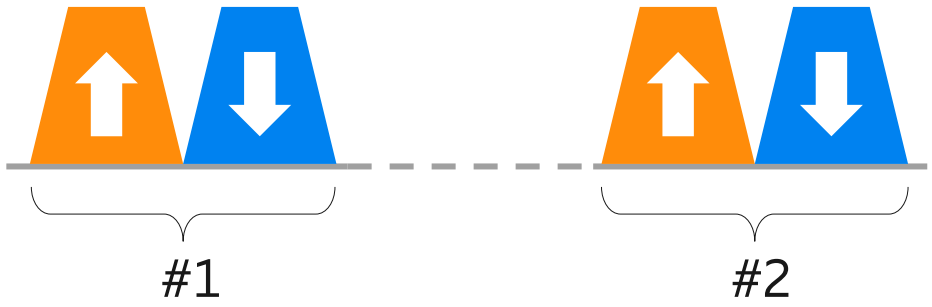
Carrier aggregation and supplementary uplink

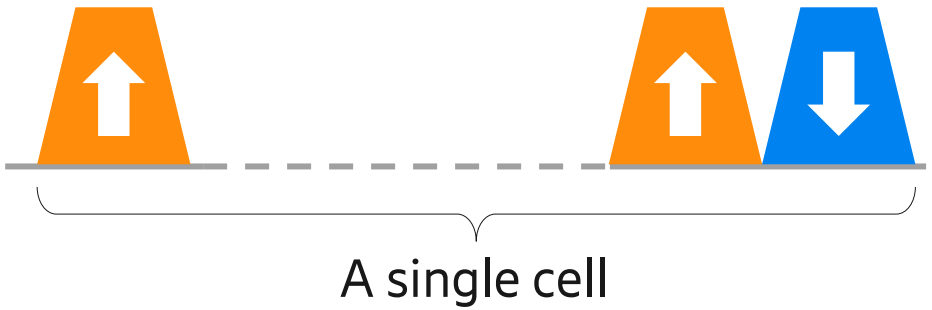
Carrier aggregation (up to 16 carriers)

— main use case: bandwidth extension

Supplementary uplink

— main use case: uplink coverage

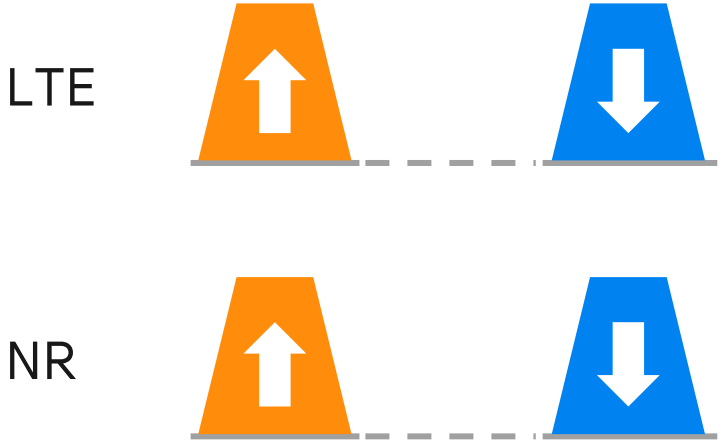




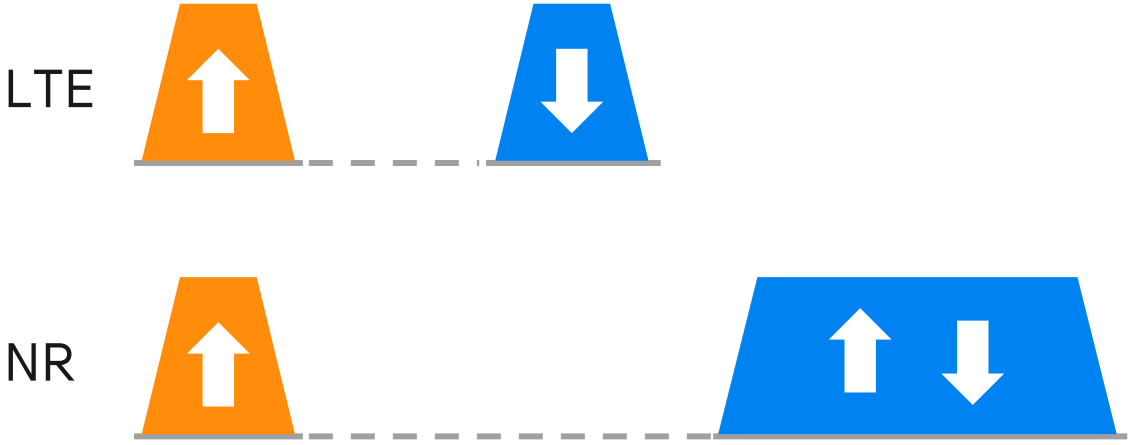
Spectrum coexistence NR and LTE

NR can coexist with LTE on the same carrier

— example: NB-IoT or eMTC for MTC on same carrier as NR



Downlink and uplink co-existence

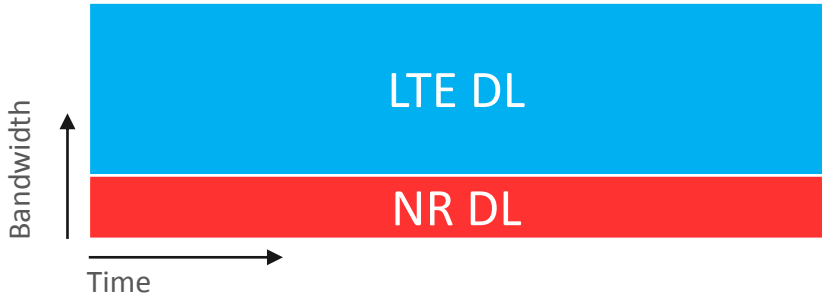


Uplink-only co-existence

Spectrum sharing between NR and LTE

Static spectrum allocation

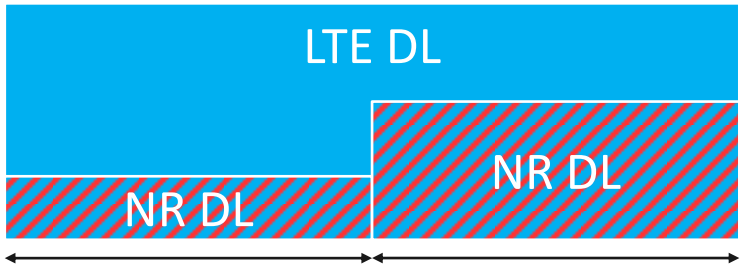
Same, constrained, NR experience everywhere



2019

Dynamic spectrum sharing

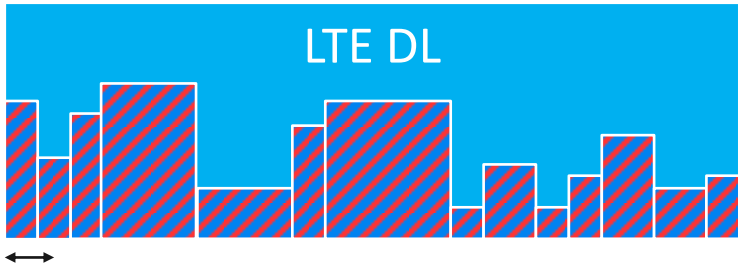
Using spectrum for NR as needed without wasting LTE capacity (useful for spotty NR penetration and demand), while preserving LTE and NR peak rates (but not simultaneously)



2019

Instant spectrum sharing

Balance LTE and NR load dynamically in mid-high load situations



2020

5G deployments – what performance to expect

London example

26 GHz
200 MHz TDD
16x16 base station antenna array

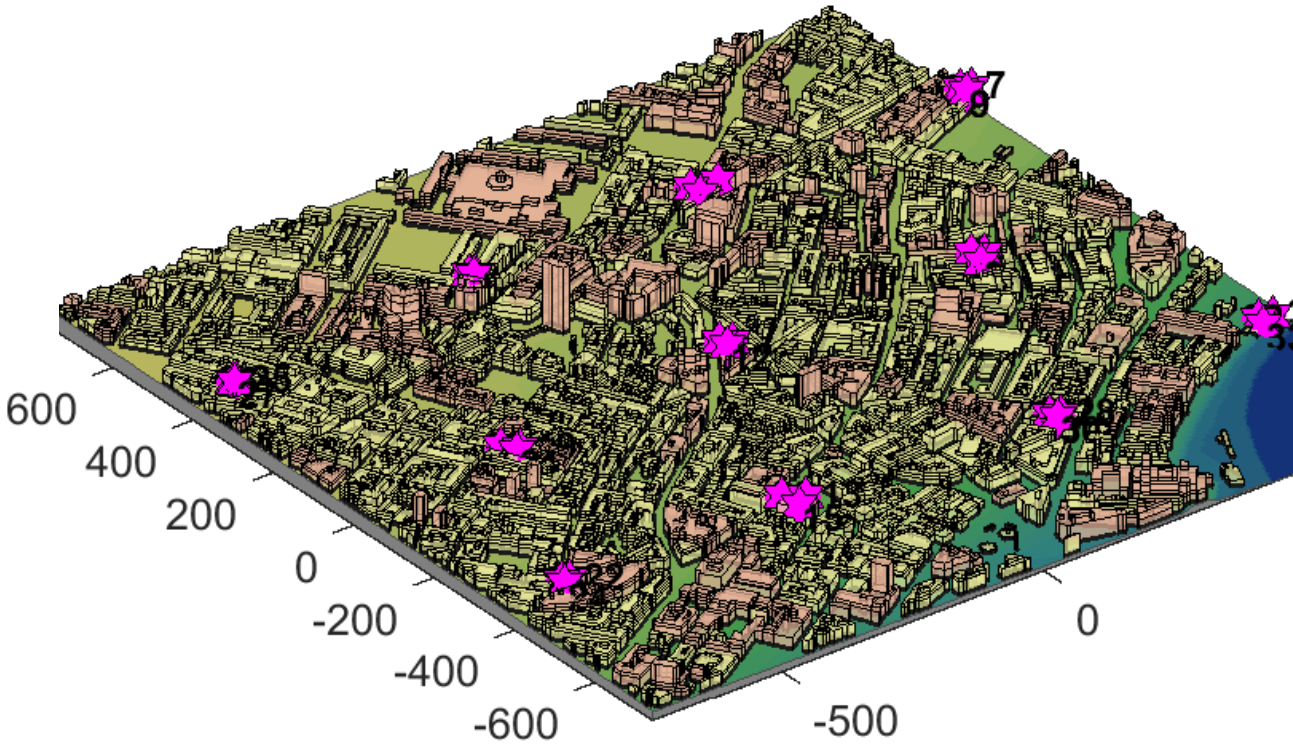
3.5 GHz
100 MHz TDD, DL:UL 3:1
8x8 base station antenna array

NR

800/2600 MHz
10/40 MHz FDD
2T/2R base station antenna

LTE

Macro network in London
- ~400 m inter-site distance
- digital 3D map
- raytracing propagation model



Site-specific 3D propagation model

Ericsson state-of-the-art 3D channel model

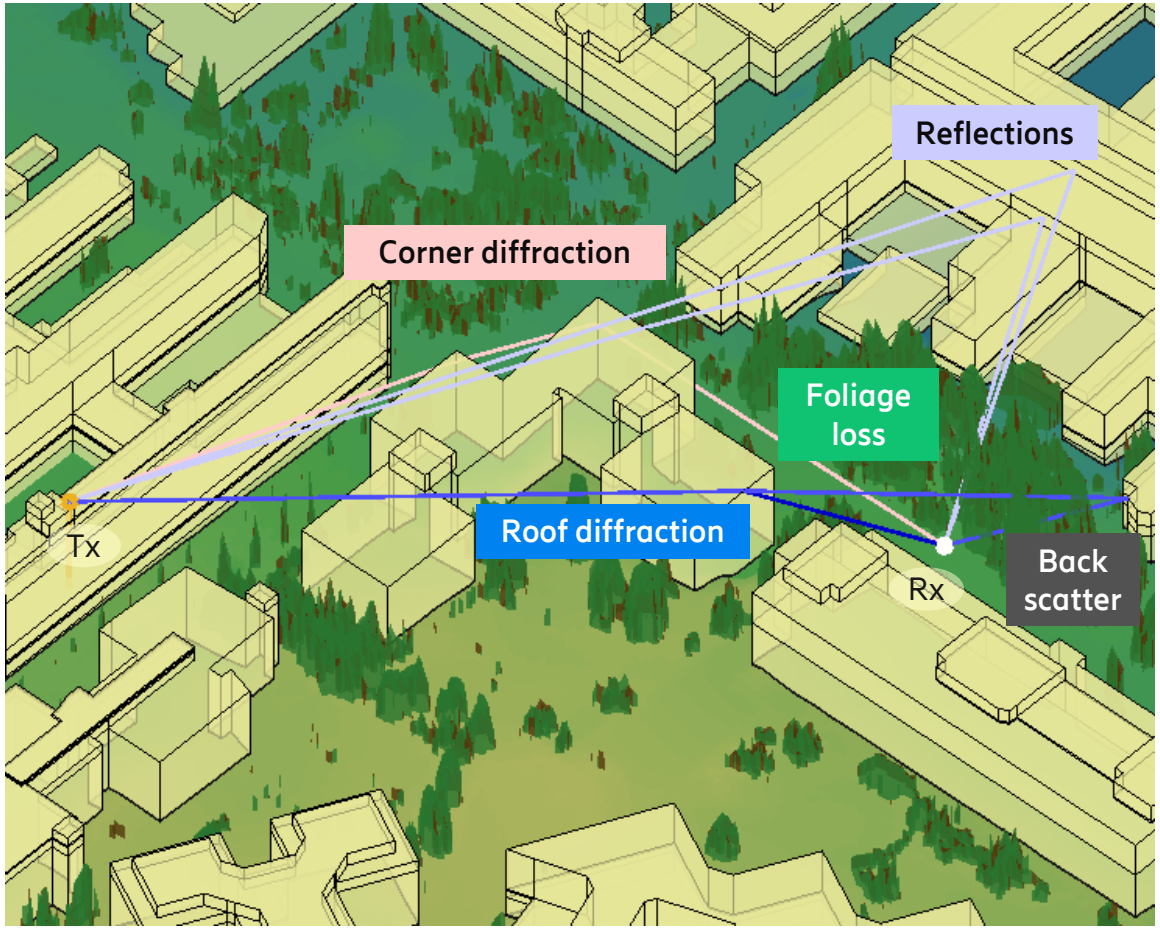
- based on many years of experience in site specific path-loss modeling, with a blend of geometric and stochastic modelling
- frequency support 1 GHz up to and including mmW
- truly site-specific – good accuracy also un-tuned

Ray tracing that captures

- propagation above building rooftop
- propagation around building corners
- specular reflections on building walls

Reciprocal outdoor ←→ indoor

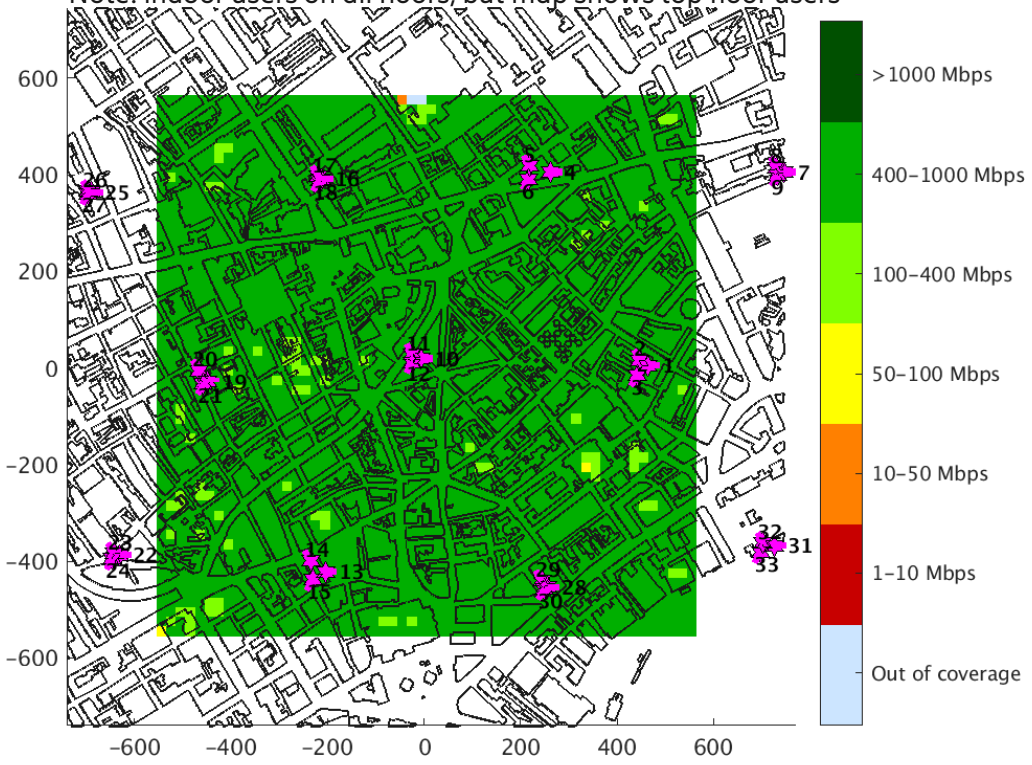
- frequency dependent wall loss



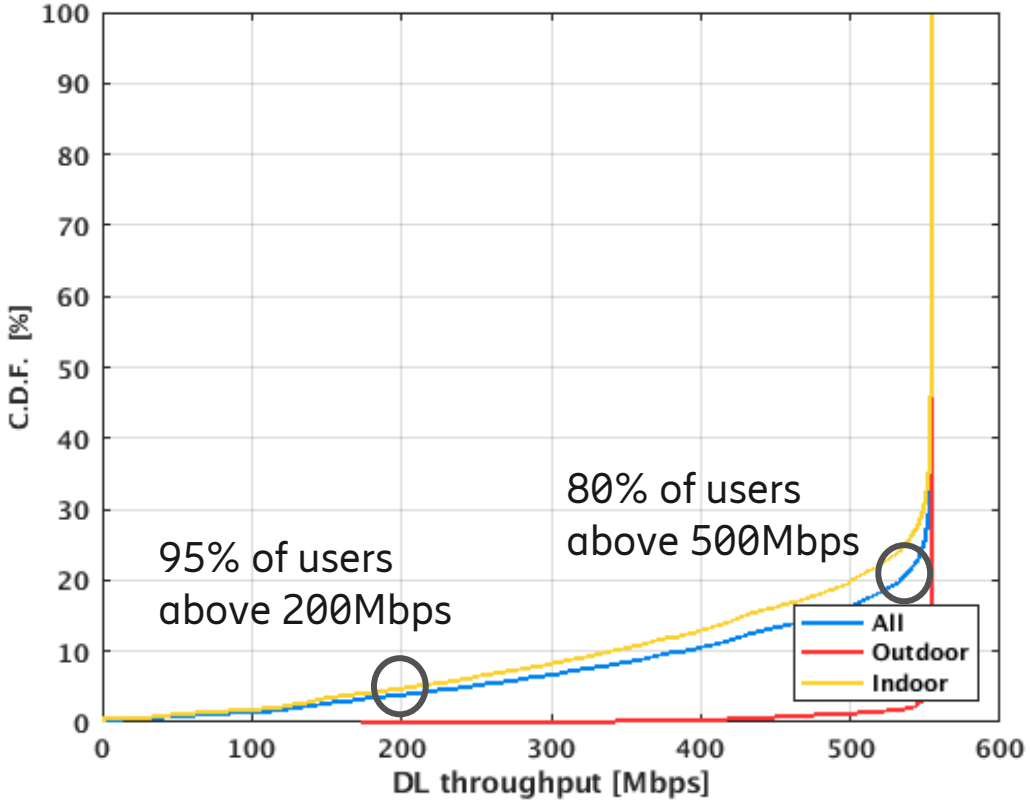
London 3.5GHz coverage
Downlink

- Majority of users above 400Mbps
- Good indoor coverage, exceptions in large buildings at cell-edge

Note: indoor users on all floors, but map shows top floor users



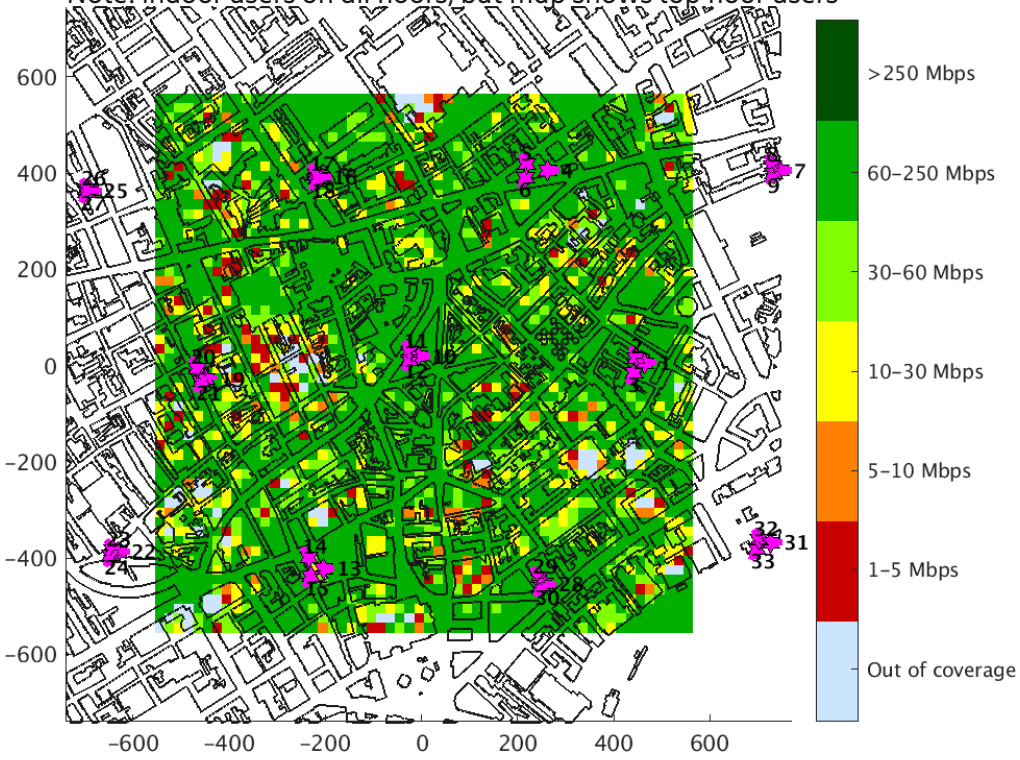
- Many users near peak datarates



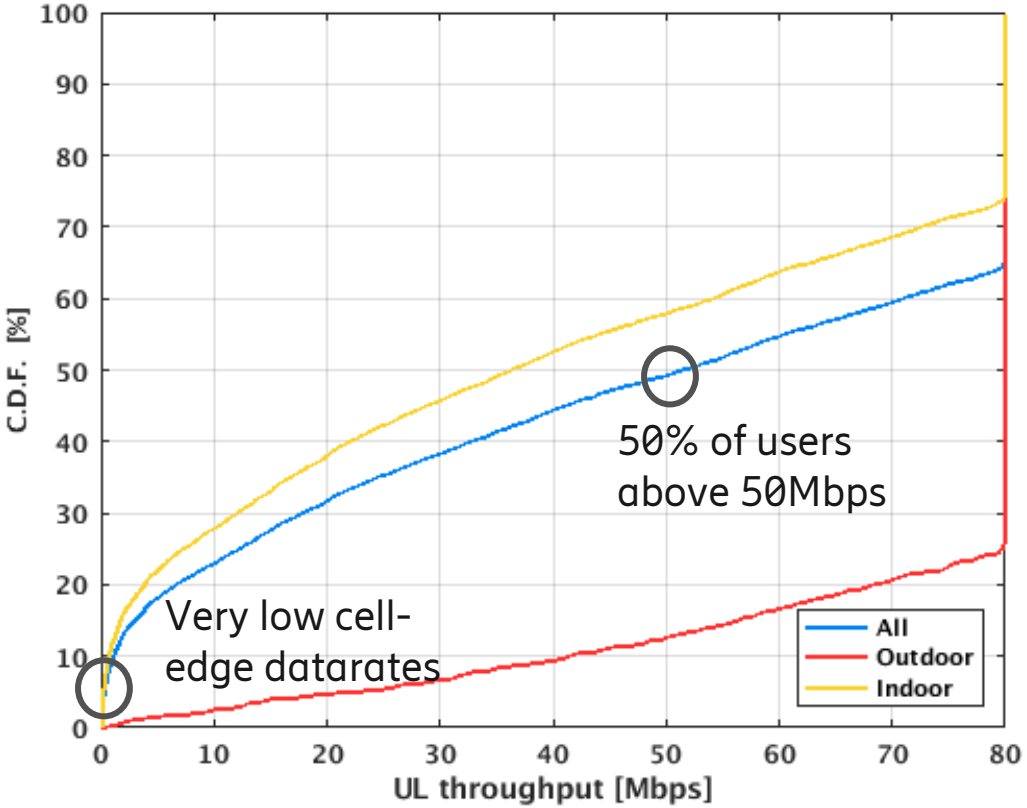
London 3.5GHz coverage
Uplink

- Many users above 60Mbps
- Coverage holes common indoors

Note: indoor users on all floors, but map shows top floor users



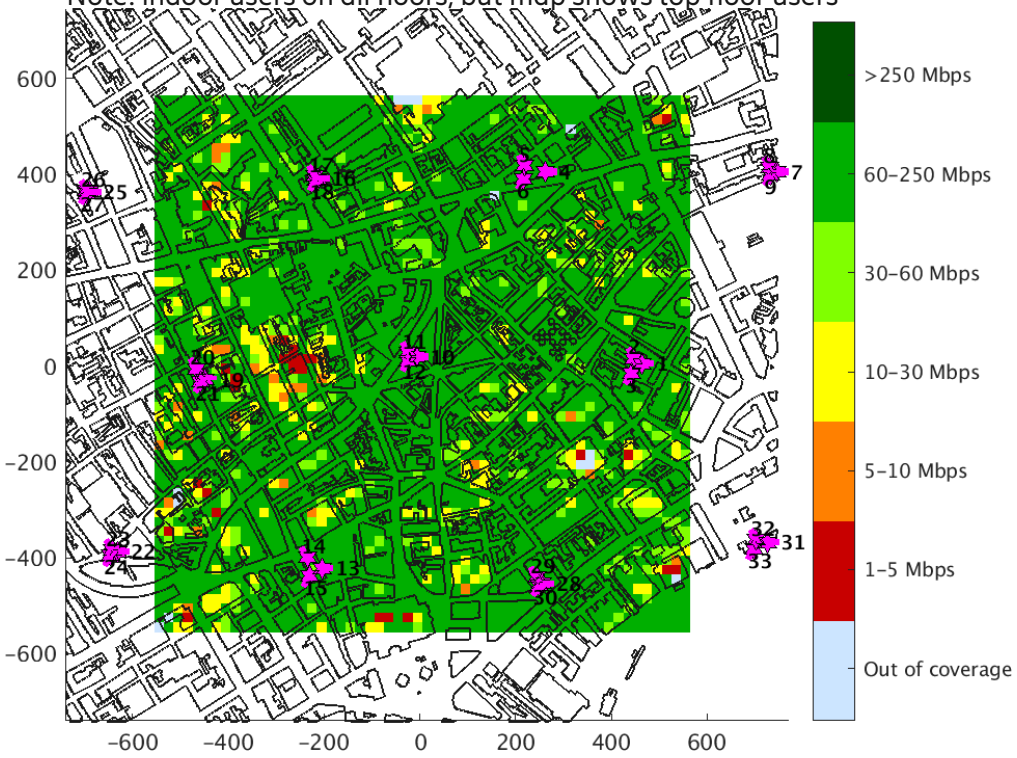
- Very low cell-edge datarates
- Interworking with low-band needed
- Still 98% Control channel coverage



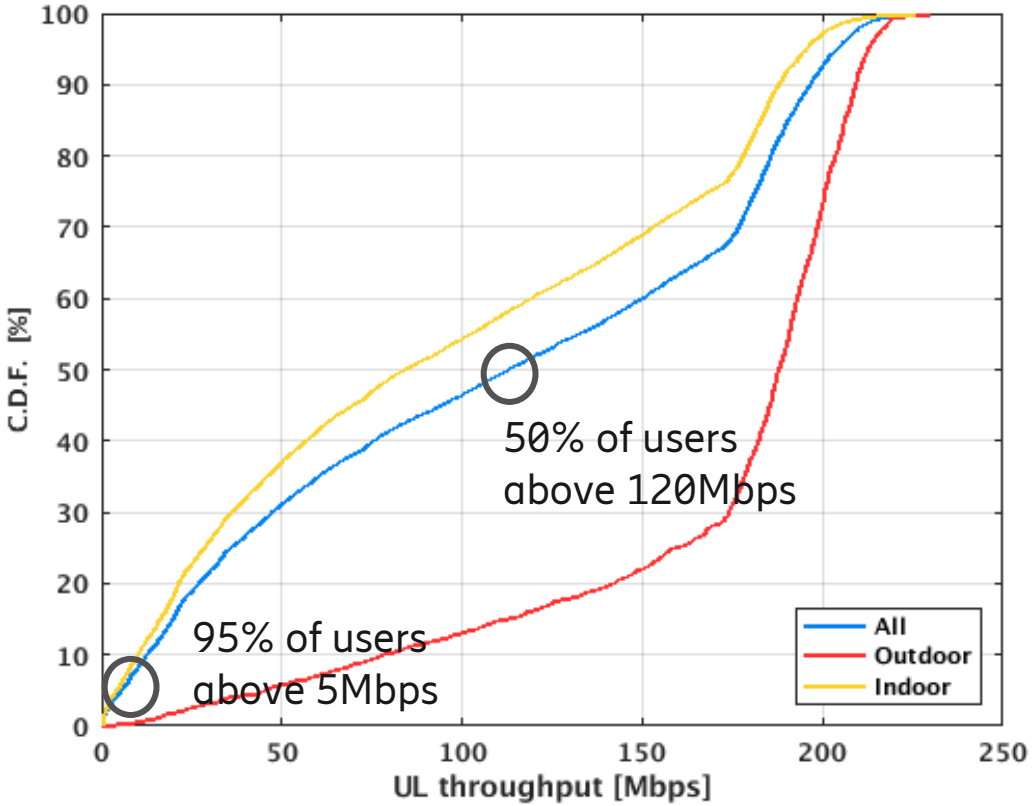
London 0.8, 2.6, 3.5GHz interworking coverage
Uplink

- Many users above 60Mbps
- Coverage holes addressed by low band

Note: indoor users on all floors, but map shows top floor users



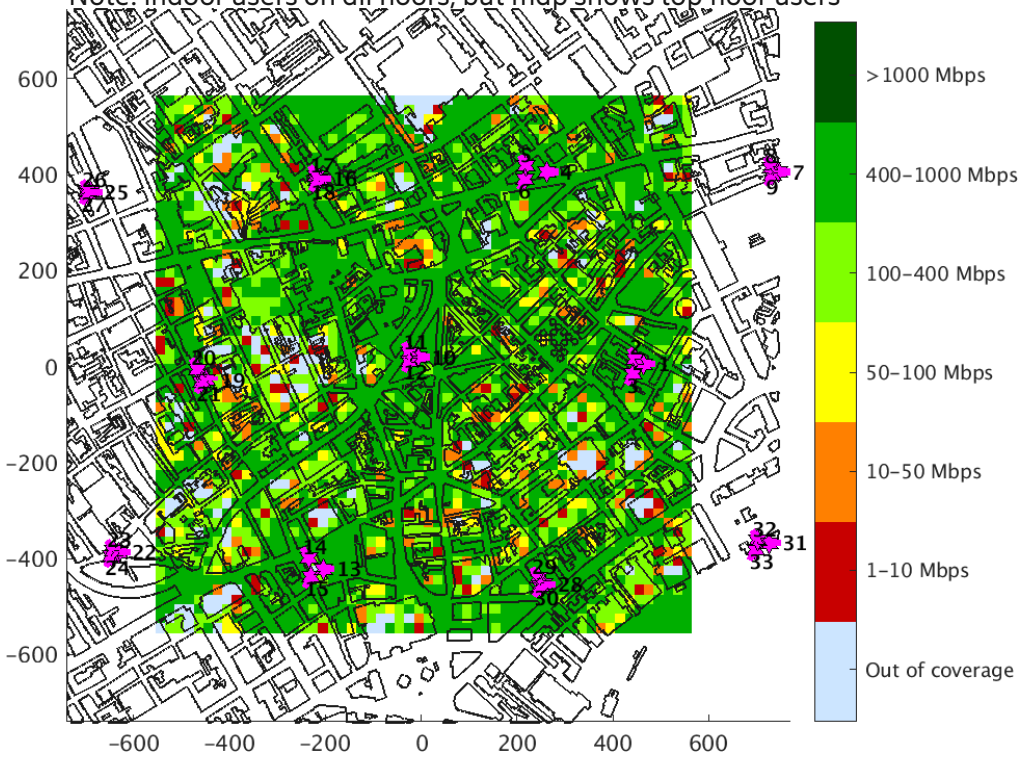
- Interworking improves cell-edge datarates and makes overall system useable



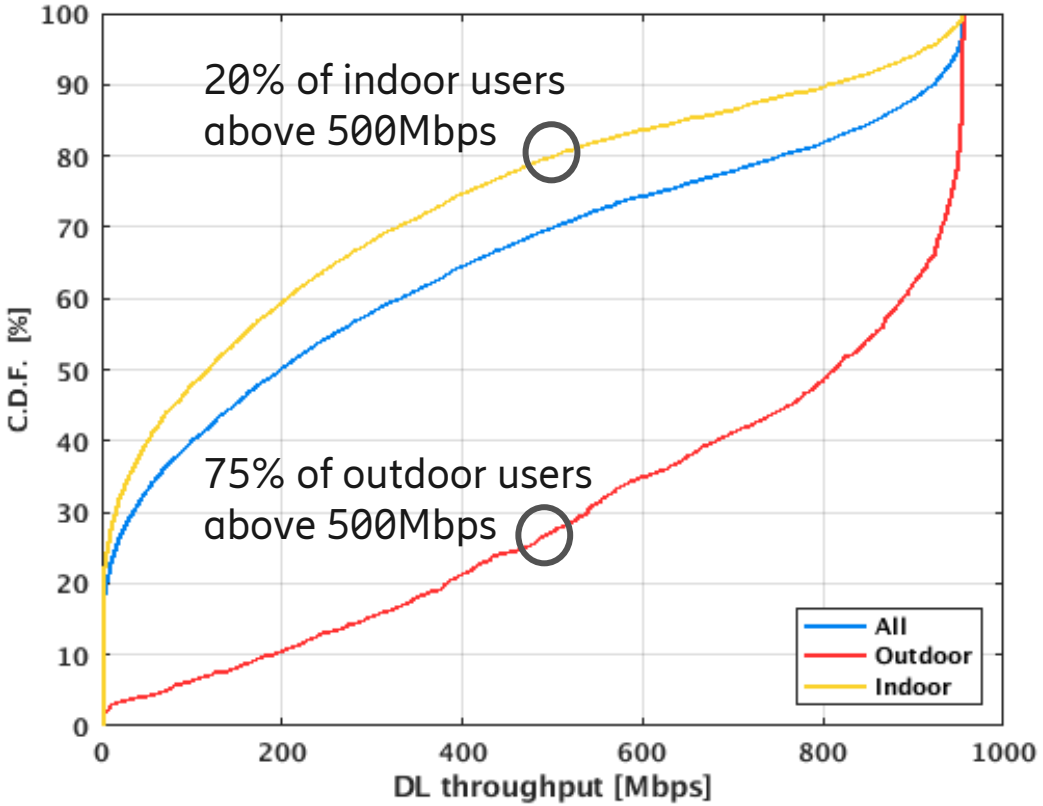
London 26GHz coverage
Downlink

- Many major streets and squares above 400Mbps

Note: indoor users on all floors, but map shows top floor users



- Very good outdoor coverage
- Indoor coverage in low-loss buildings near sites



London – capacity

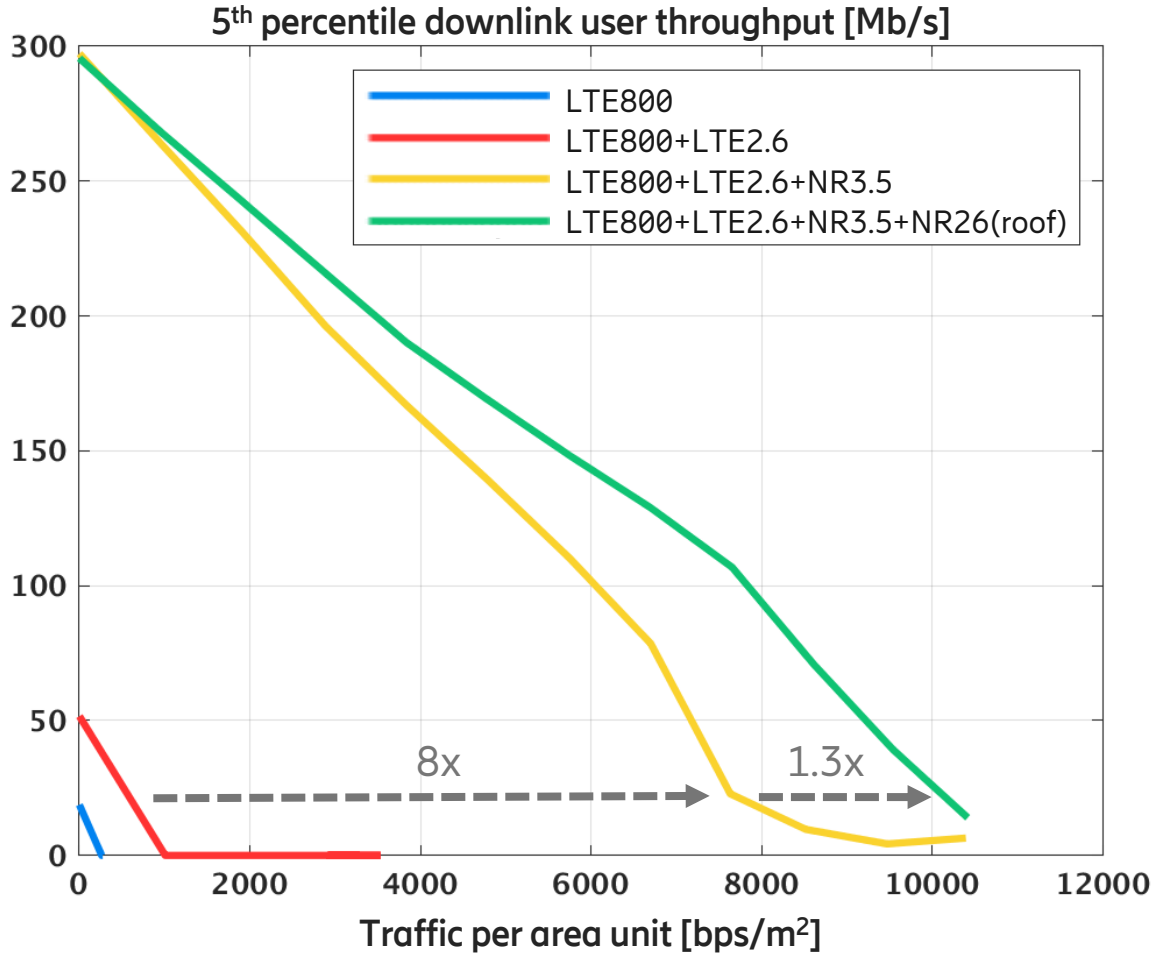
NR 3.5 GHz provides 8x capacity gain over LTE at 800-2600 MHz

- NR allocated 1.5x more DL spectrum
  ⇒ 5x more efficient

NR at 26 GHz further improves capacity by ~30%

How large buckets?

- 8 000Mbps/km² and 10 000 subs/km²
  ⇒ 0.8Mbps/subscriber during busy hour
  ~133GB/month (with 8% of daily traffic during busy hour)

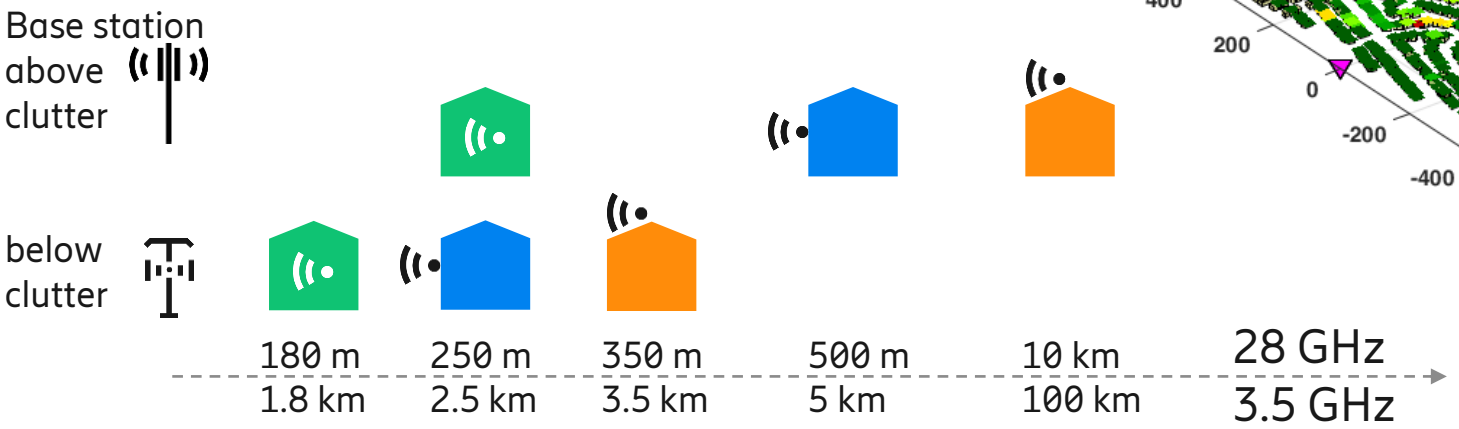


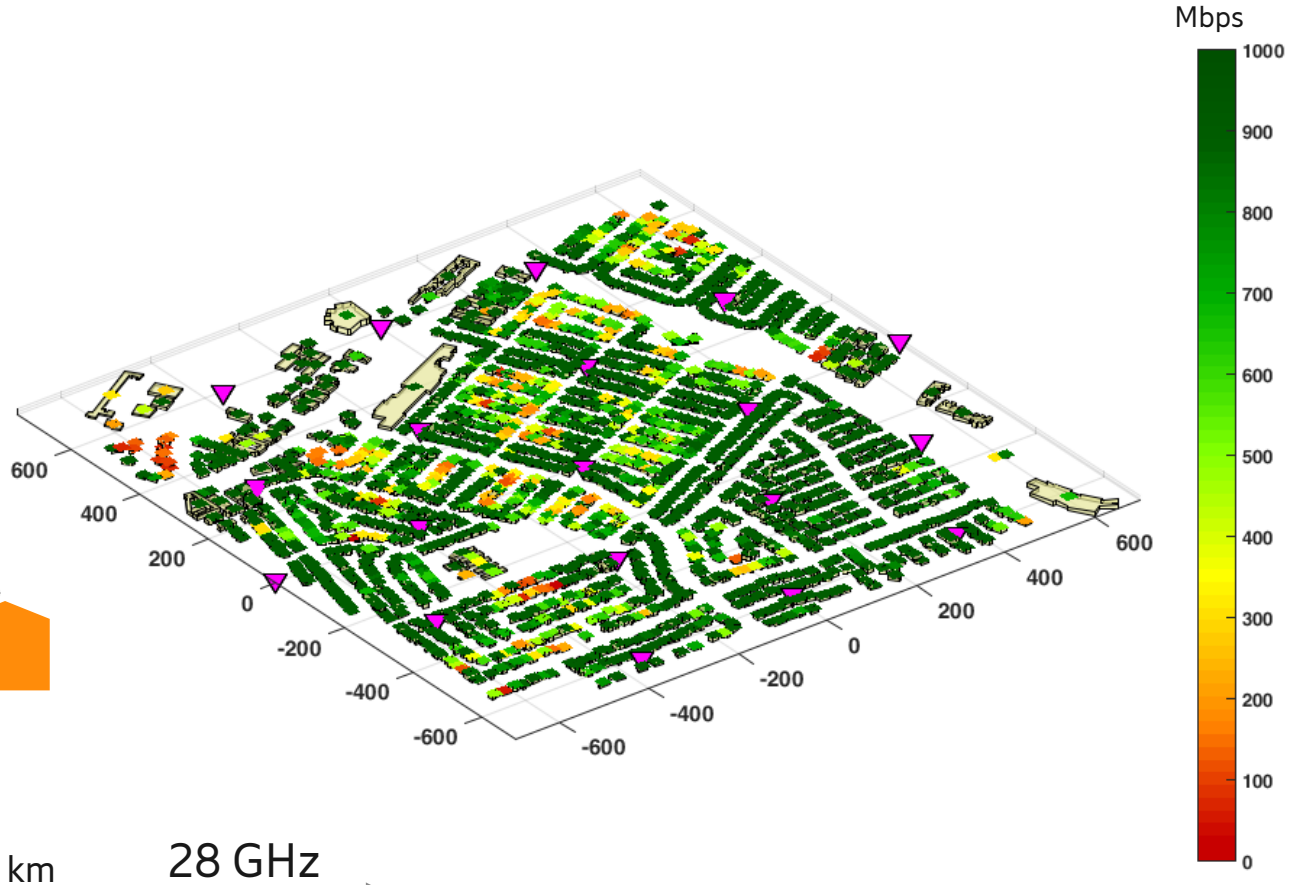
Suburban fixed wireless – 28 GHz

Very high cell capacities

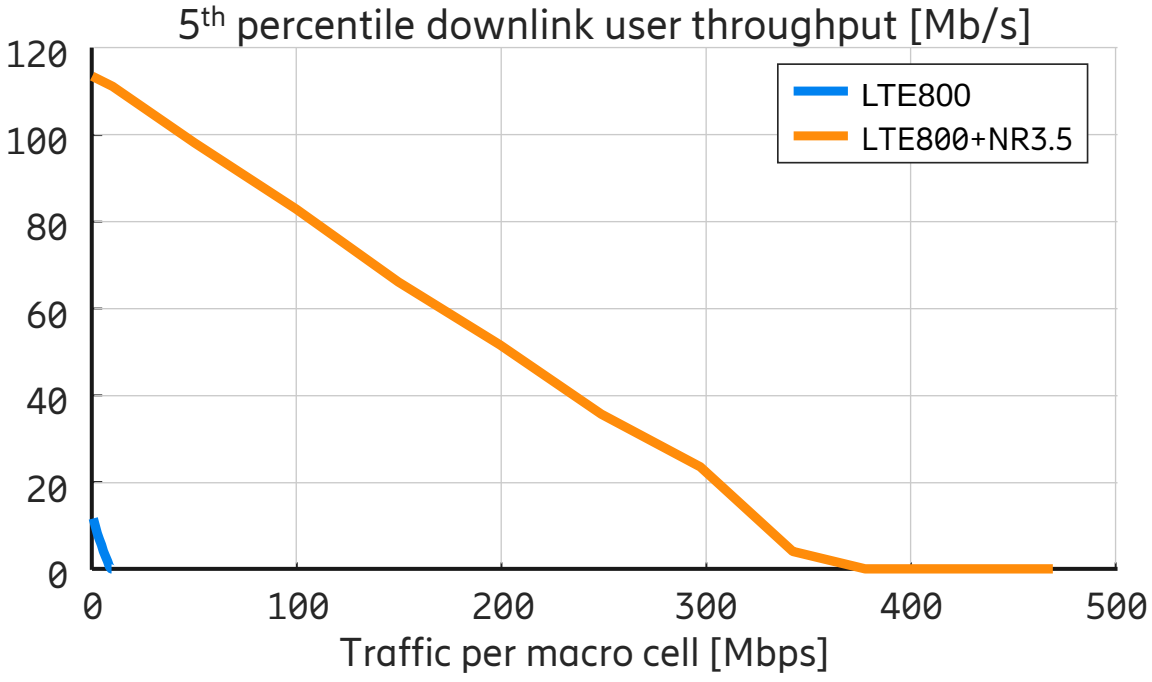
NR on 28 GHz (or 3.5 GHz)

- sites on utility poles
- 8x12 array at base station
- fixed wireless CPEs outdoor or indoor
- 350m ISD, targeting 50 Mb/s downlink
- CPE location: indoor, outdoor, or rooftop





Rural coverage and capacity



3GPP/ITU rural scenario
- 50% indoor in low-loss buildings, 50% in cars
- statistical propagation models
- inter-site distance 4 500m ~ GSM coverage at 900 MHz

Deploying
NR at 3.5 GHz (100 MHz TDD) with
LTE at 800 MHz (2x10 MHz FDD)

- Very large gains in user throughput and capacity
- Same base station grid as typical rural GSM 900 deployment
- 95% of users get >100 Mb/s DL

3GPP and ITU evaluations of NR

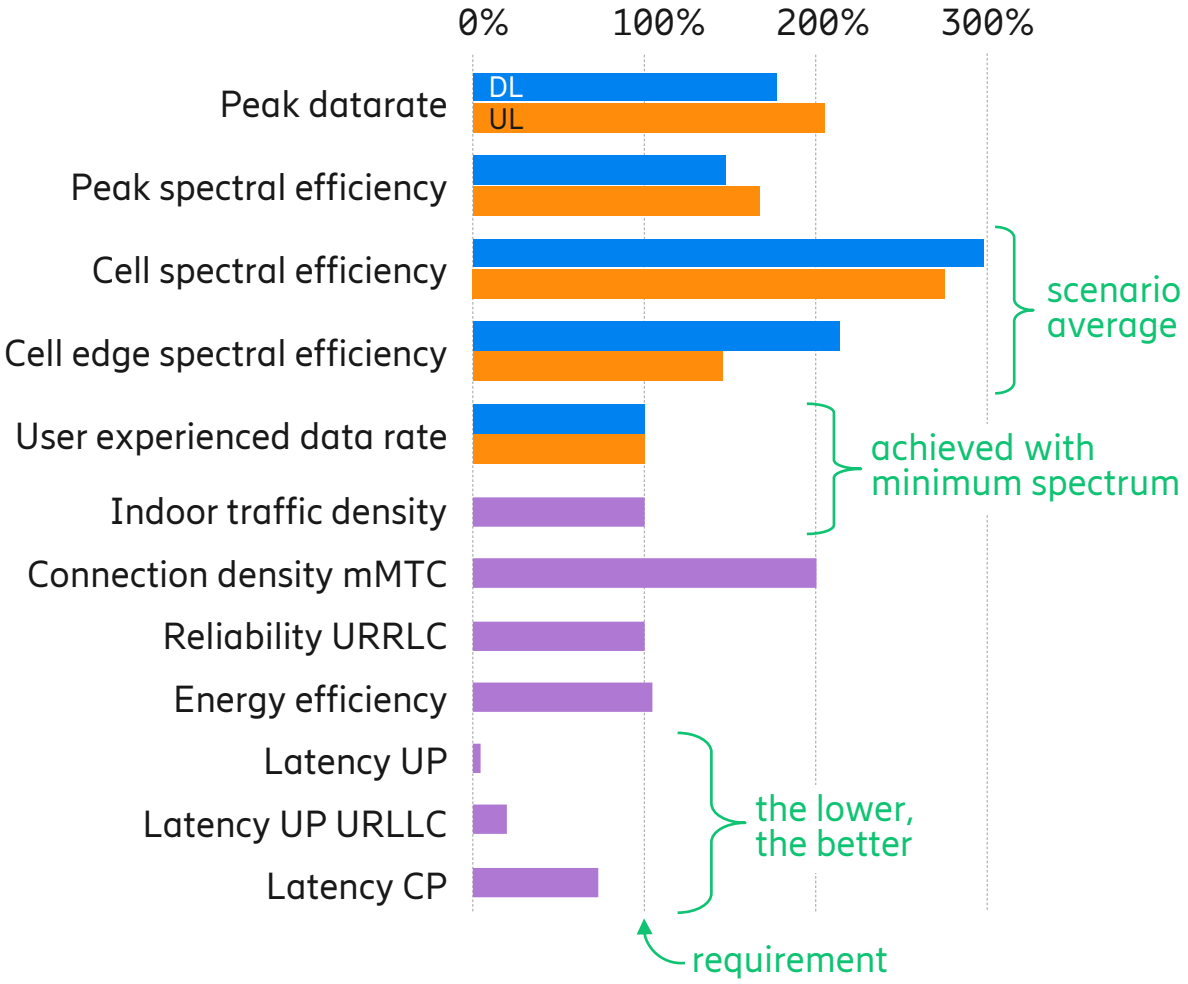
NR can realize the IMT-2020 vision

— All requirements reachable

— Extreme MBB, URLLC, M-MTC...

— Ericsson results from April 3GPP RAN WG meeting

— Similar results from other sources



Summary

Key radio technologies

— Antenna beam-forming and beam-tracking
— MU-MIMO
— Flexible spectrum compositions

5G NR fulfills ITU requirements

— often with flying colors
— enables massive capacity increase

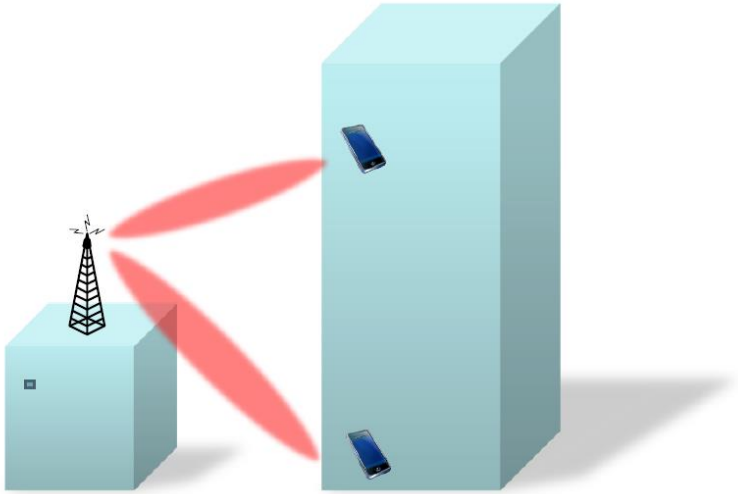
Flexible, supportive spectrum allocations unleashes 5G capabilities and helps NR migration

5G and EMF

Christer Törnevik
Senior Expert, EMF and Health
Ericsson Research

5G and EMF
Introduction

- Like current mobile networks, 5G will use radio waves, or electromagnetic fields (EMF), for communication between base stations and connected devices.
- 5G will use new spectrum, also above 6 GHz, which is already covered by current EMF safety standards and limits.
- 5G will use advanced beamforming antennas (massive MIMO) that can steer the radio signals to optimize the communication with connected devices – this will improve performance and keep average power and environmental EMF exposure levels low.
- The higher frequencies (mmW) and the beam steering may cause public concern that needs to be addressed by proper information.



Information about 5G and EMF

ERICSSON

RADIO WAVES AND HEALTH: 5G

Over the past 140 years, Ericsson has been at the forefront of communications technology. Today, we are committed to maximizing customer value by continuously evolving our business portfolio and leading the Information and Communication Technology industry. In fact, 40% of the world's mobile traffic is carried over Ericsson networks.

Communication is a basic human need and modern communication technologies are an essential part of a sustainable future. We consider your safety a key priority when using these technologies.

5G is the next step in the evolution of mobile communication. Its capabilities will extend far beyond previous generations, but it will be based on similar radio technologies. 5G devices will be designed and tested to comply with established radio wave exposure limits, and base stations will be installed so that the exposure in homes and public areas is well below the limits.

Since 1996, Ericsson has co-sponsored over 100 studies related to radio waves and health. Independent expert groups and public health authorities, including the World Health Organization, have reviewed the available research and have consistently concluded that there is no evidence of any health effects associated with radio wave exposure from either mobile phones or radio base stations.

Ericsson fact sheet:
www.ericsson.com/health

GSMA

5G, the Internet of Things (IoT) and Wearable Devices

What do the new uses of wireless technologies mean for radio frequency exposure?

September 2017

GSMA Brochure :
www.gsma.com

EMF Explained Series

March 2018

5G and EMF Explained

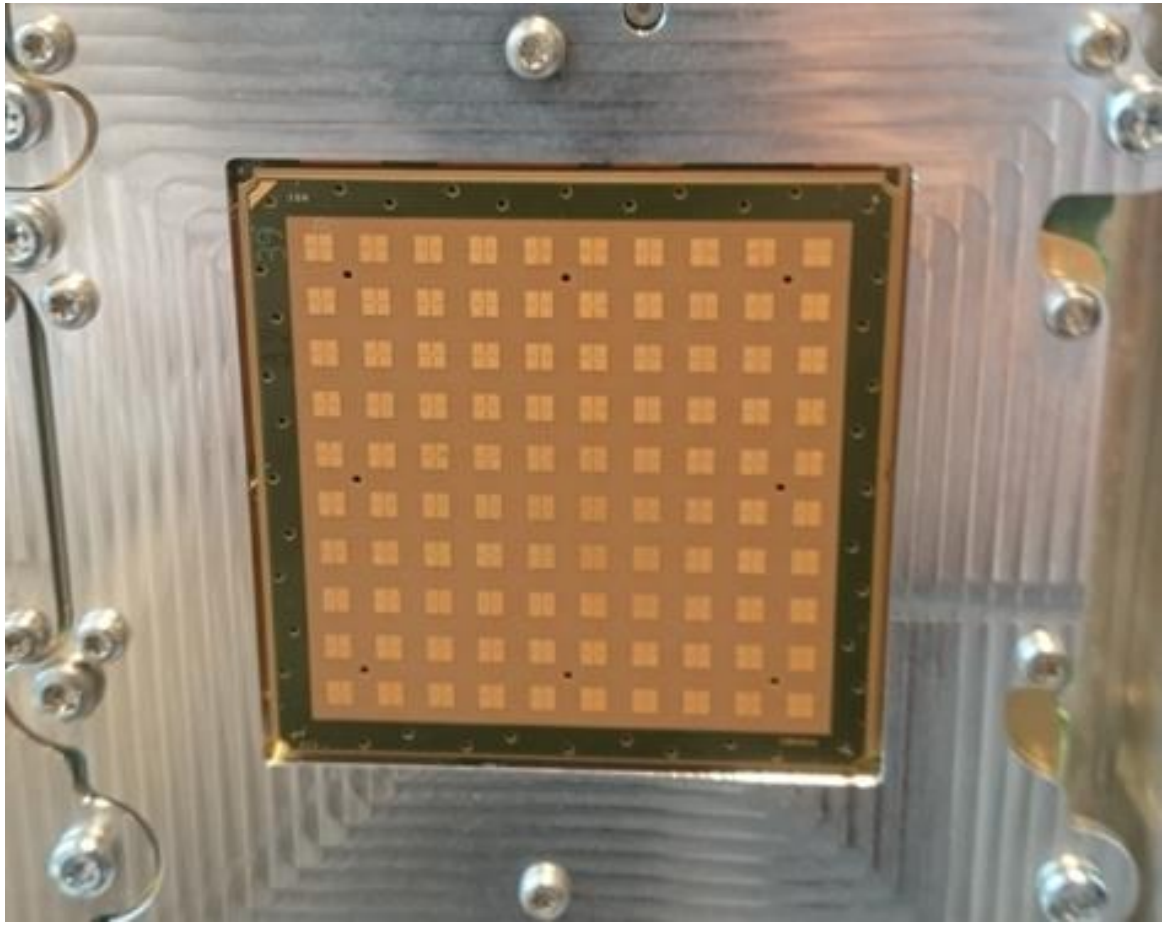
5G

www.emfexplained.info

EMF Explained Information:
www.emfexplained.info

EMF challenges for 5G
Beam forming and beam steering (massive MIMO)

- Large variability of transmitted signals in time and space
- Higher instantaneous EIRP than for current antennas and potentially larger EMF safety zones (if no time-averaging)
- More complex EMF compliance assessments
- Site design of increasing importance (co-siting), since many existing sites already have small margins to EMF limits
- Site compliance very difficult in countries having EMF limits below international guidelines (ICNIRP)



International EMF exposure limits

Same limits for 2G, 3G, 4G and 5G

ICNIRP reference levels, 2 GHz – 300 GHz

Power density	
General public	Workers
10 W/m^2	50 W/m^2

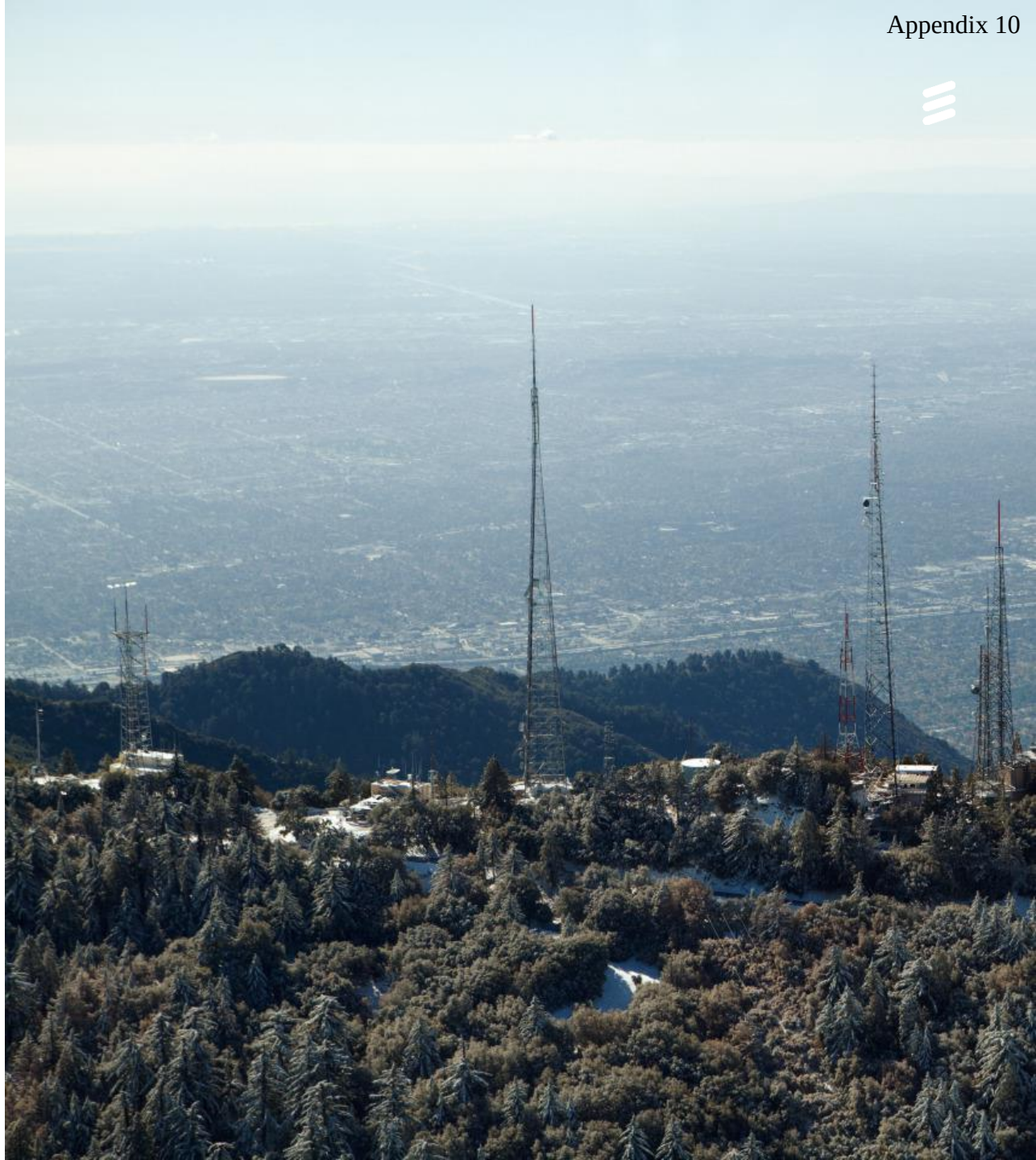
Averaging time: 6 minutes up to 10 GHz, 2 minutes at 30 GHz

WHO view on EMF limits

"The main conclusion from the WHO reviews is that EMF exposures below the limits recommended in the ICNIRP international guidelines do not appear to have any known consequence on health"

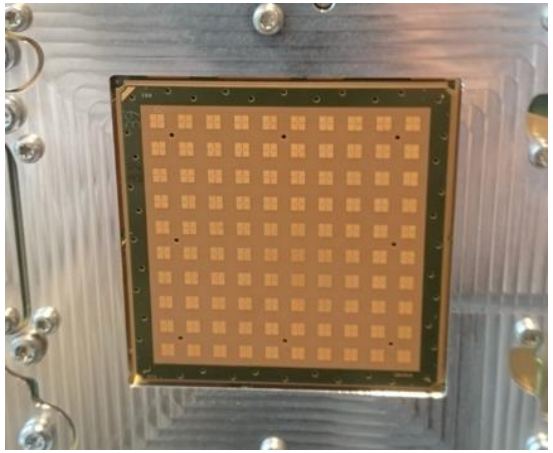
[www.who.int/peh-emf/standards]

World Health Organization

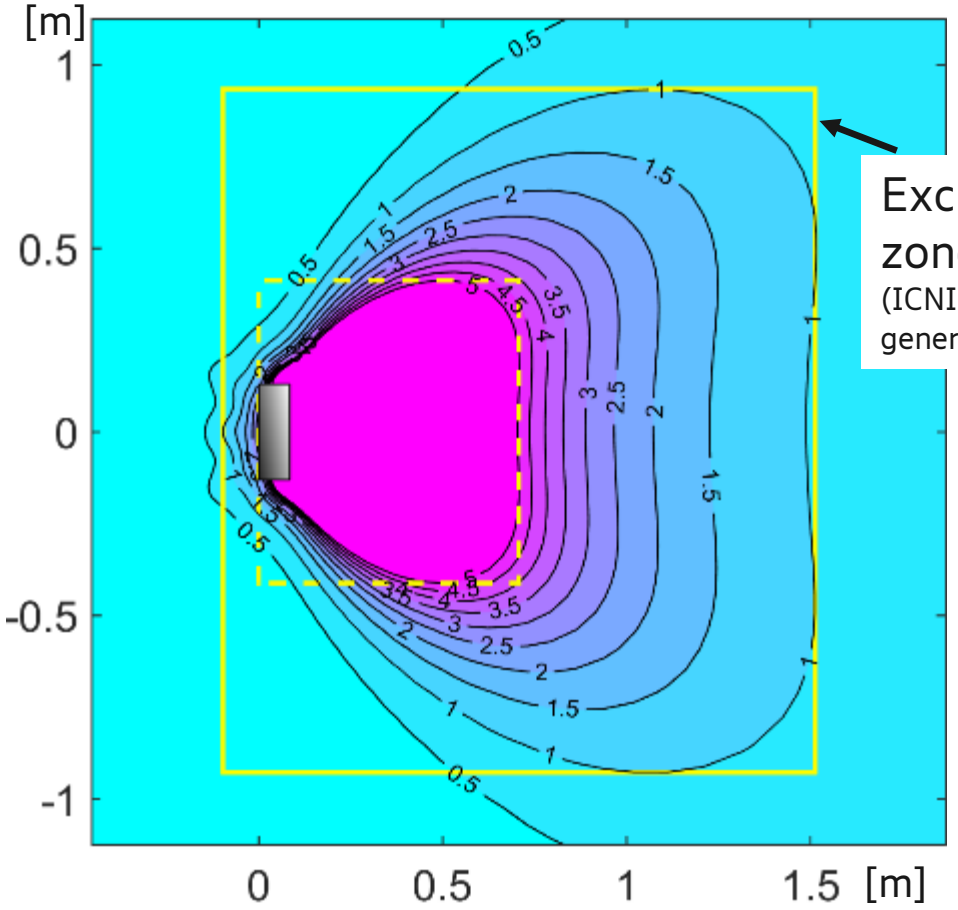


28 GHz massive MIMO 5G base station (low-power)

Ericsson AIR 5121
- 28 GHz
- 512 antenna elements
- 8 beams
- Total output power: ~ 1 W
- Gain: ~ 24 dBi
- Beam steering:
  ± 60° (h)
  ± 15° (v)



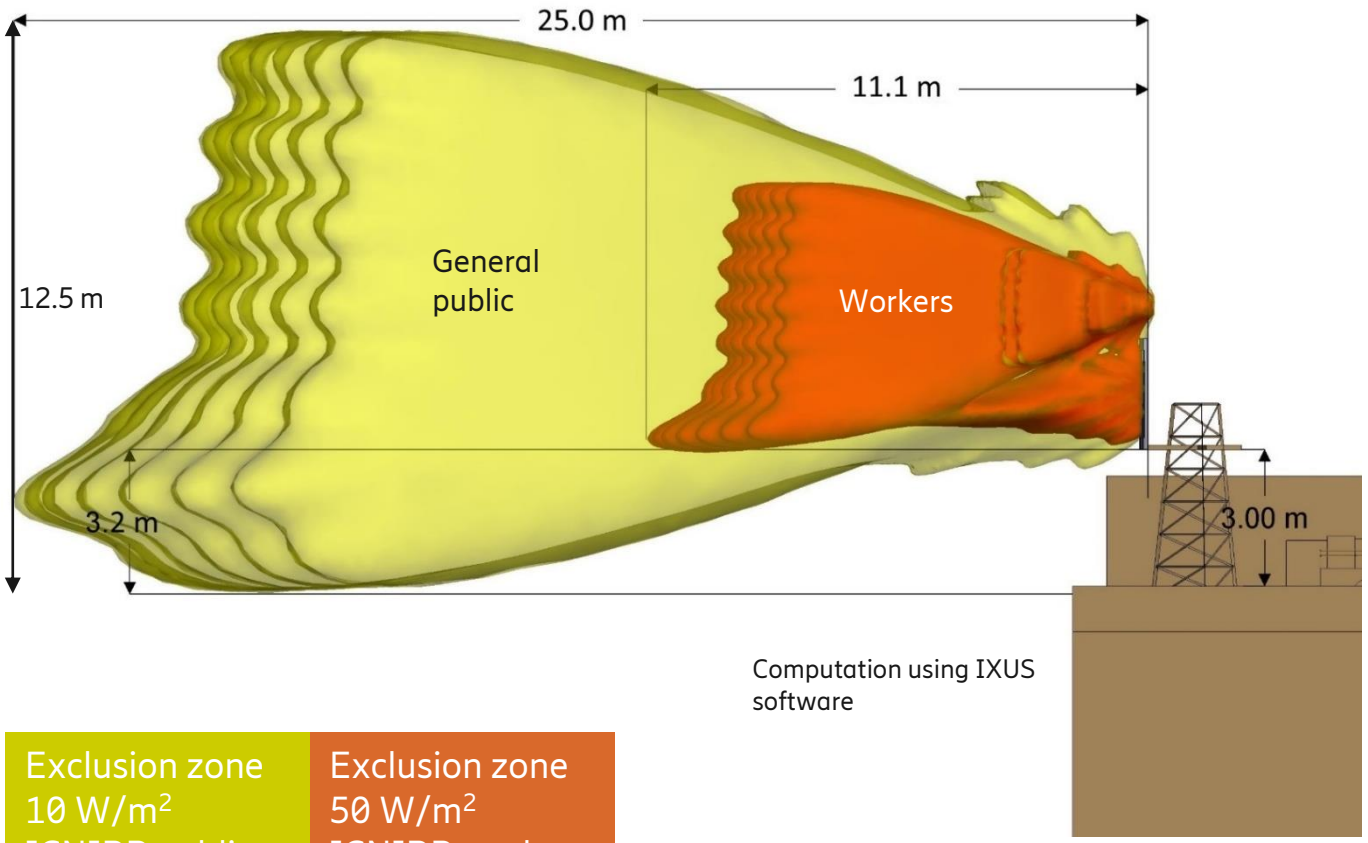
AIR 5121
dimensions 600x300x90 mm



Exclusion zone, 10 W/m^2
(ICNIRP limit for the general public)

Assuming maximum power in all beam directions, EMF compliance is not an issue for normal installations

3.5 GHz massive MIMO 5G site (macro)



Computation using IXUS software

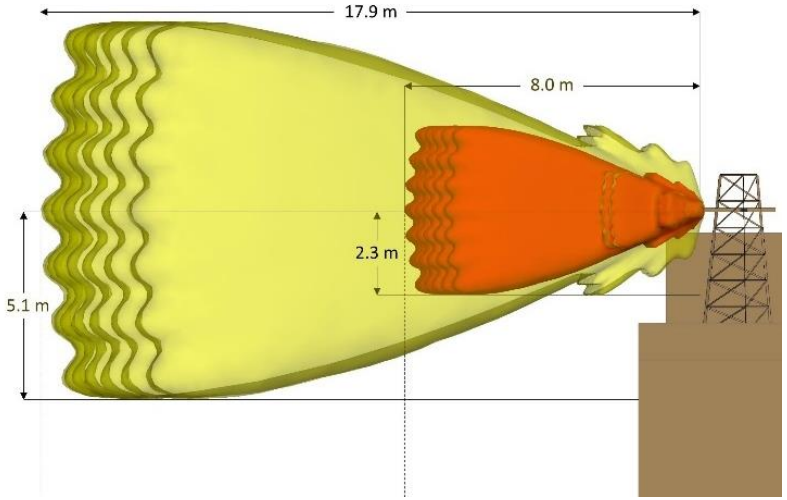
Exclusion zone 10 W/m² ICNIRP public EMF limit	Exclusion zone 50 W/m² ICNIRP worker EMF limit

Very large exclusion zone due to unrealistic power assumption – may lead to substantial 5G deployment challenges

IEC 62232 and ITU K.100 standards open up for use of actual maximum output power (95th percentile)

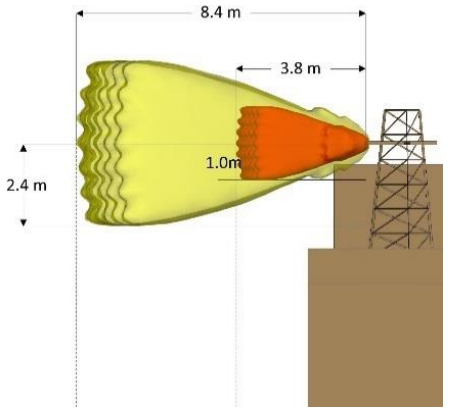
- 3.5 GHz, 200 W (Ericsson AIR 6488)
- Massive MIMO (64 Tx)
- Maximum EIRP of about 76 dBm
- Model of installation on existing site with 2G, 3G and 4G antennas
- Theoretical maximum power (100% traffic load) assumed for all antennas (typical regulatory requirement)

Rationale for actual maximum power use



3.5 GHz 5G base station compliance boundary determined using **theoretical maximum** transmitted power (200 W)

- Not all power will be focused in the same direction for several minutes
- TDD will limit transmit time
- Traffic load less than 100%

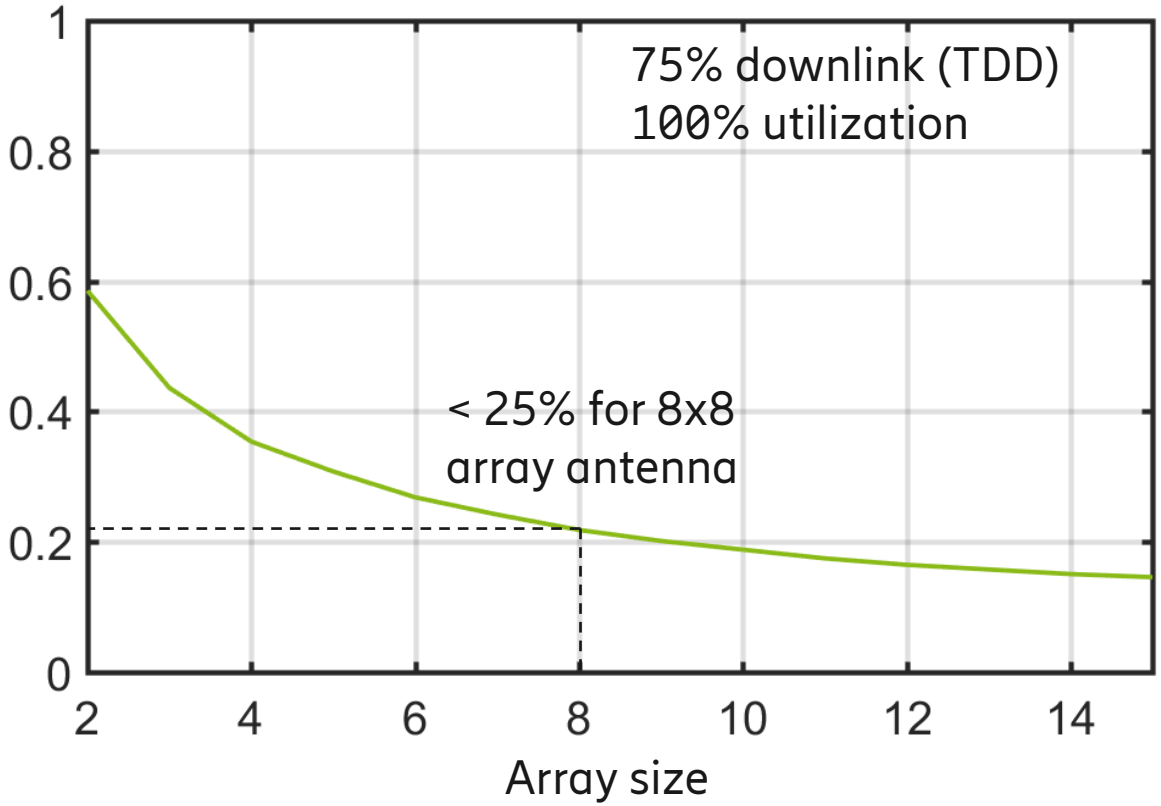


3.5 GHz 5G base station compliance boundary determined using **actual maximum** transmitted power (50 W)

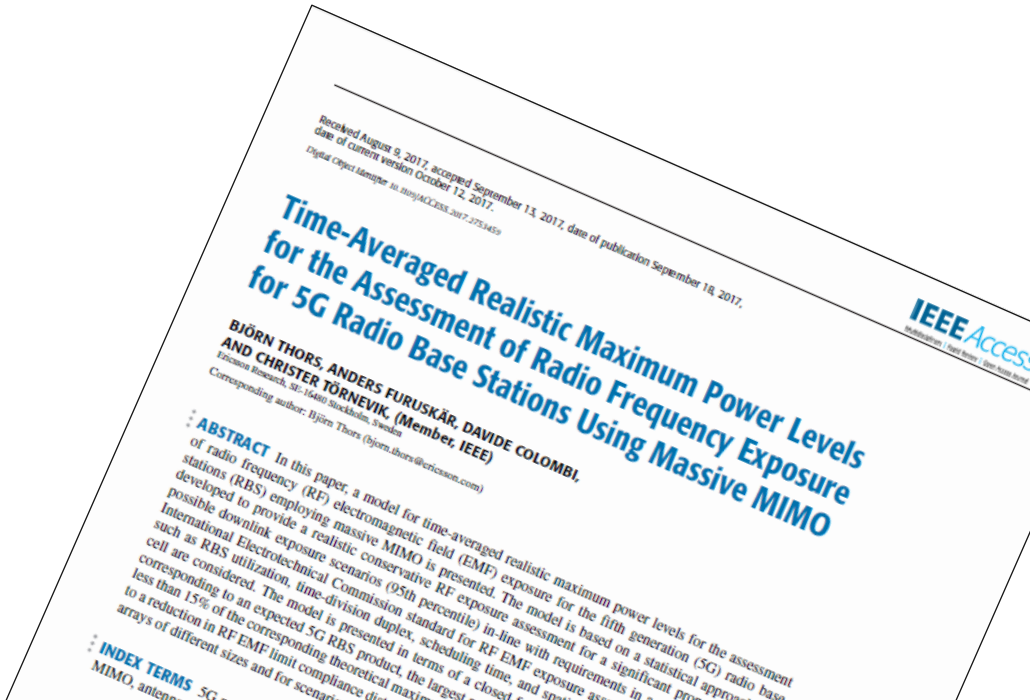
For successful 5G network roll-out it is important that ICNIRP time-averaging and IEC/ITU actual maximum power approach are supported in national EMF regulations

Actual maximum power of massive MIMO

Fraction of total power contributing to the EMF exposure as function of antenna array size (95th percentile)



Statistical model developed that takes into account base station utilization, scheduling time, distribution of user equipment, and time-division duplexing to determine actual maximum power



Received August 9, 2017, accepted September 13, 2017, date of publication September 18, 2017, date of current version October 12, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2753455

Time-Averaged Realistic Maximum Power Levels for the Assessment of Radio Frequency Exposure for 5G Radio Base Stations Using Massive MIMO

BJÖRN THORS, ANDERS FURUSKÄR, DAVIDE COLOMBI, AND CHRISTER TÖRNEVIK, (Member, IEEE)

Ericsson Research, SE-16480 Stockholm, Sweden

Corresponding author: Björn Thors (bjorn.thors@ericsson.com)

ABSTRACT In this paper, a model for time-averaged realistic maximum power levels for the assessment of radio frequency (RF) electromagnetic field (EMF) exposure for the fifth generation (5G) radio base stations (RBS) employing massive MIMO is presented. The model is based on a statistical approach developed to provide a realistic conservative RF exposure assessment for a significant proportion of possible downlink exposure scenarios (95th percentile) in-line with requirements in the International Electrotechnical Commission standard for RF EMF exposure assessment. Factors such as RBS utilization, time-division duplex, scheduling time, and spatial distribution of user equipment in a cell are considered. The model is presented in terms of a closed form expression for the corresponding to an expected 5G RBS product, the largest [illegible] less than 15% of the corresponding theoretical maximum [illegible] to a reduction in RF EMF limit compliance distances [illegible] arrays of different sizes and for scenarios [illegible]

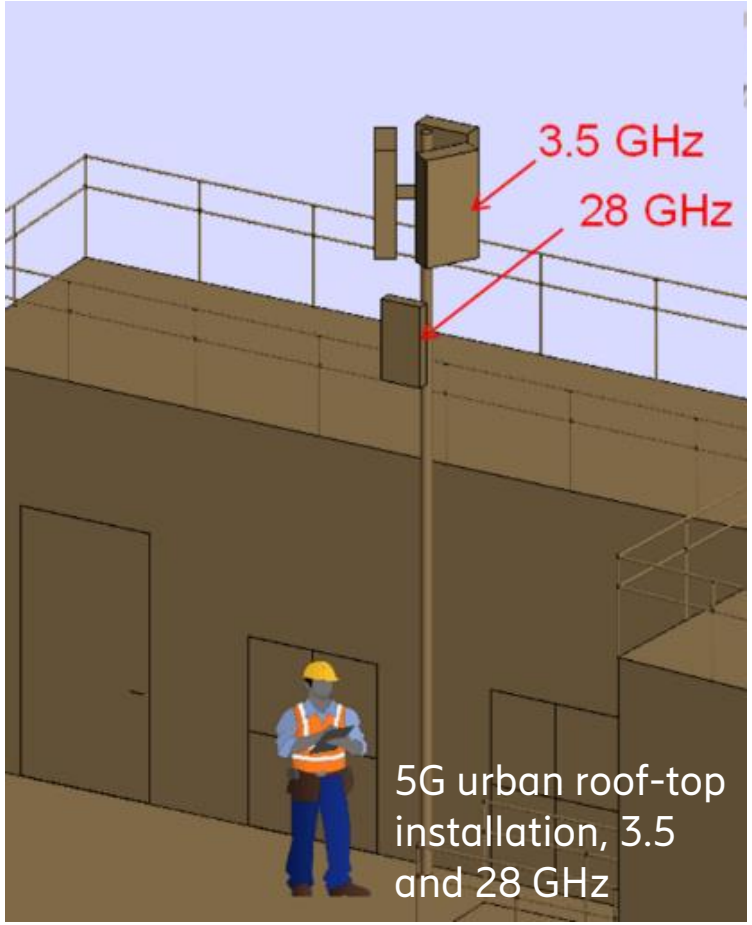
INDEX TERMS 5G [illegible] MIMO, antenna [illegible]

5G and EMF standardization activities

- Technical Report IEC TR 62669 to be published in the end of 2018
- Specifies general principles for massive MIMO statistical methods
- Includes case studies on EMF compliance assessments of 5G base stations and sites
- Regulators involved in the work

- ITU-T to complete a technical report on 5G EMF compliance (massive MIMO) in 2018
- ITU-T recently published the report "The impact of RF-EMF exposure limits stricter than the ICNIRP or IEEE guidelines on 4G and 5G mobile network deployment"

IEC TR 62669 – 5G site case study

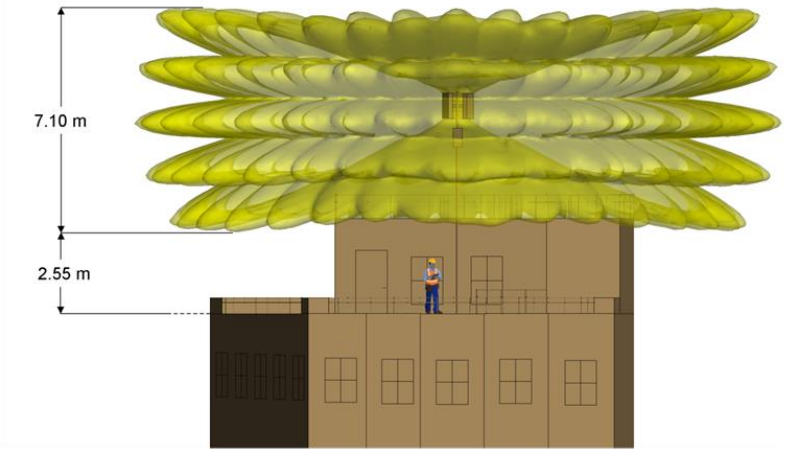


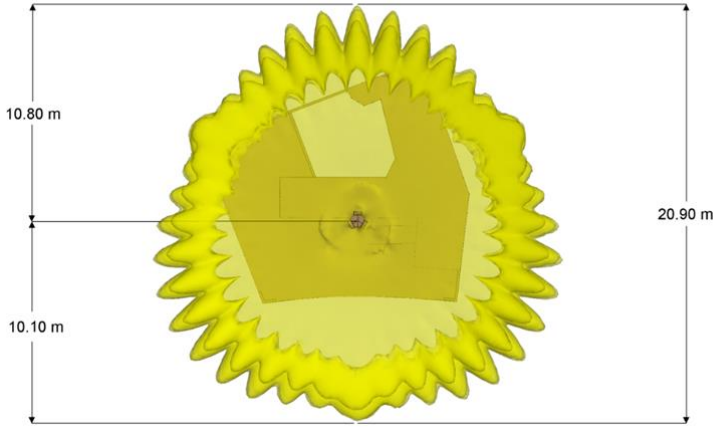
5G urban roof-top installation, 3.5 and 28 GHz

Actual maximum power 25% of the theoretical maximum

RF EMF exposure below ICNIRP limits in public areas

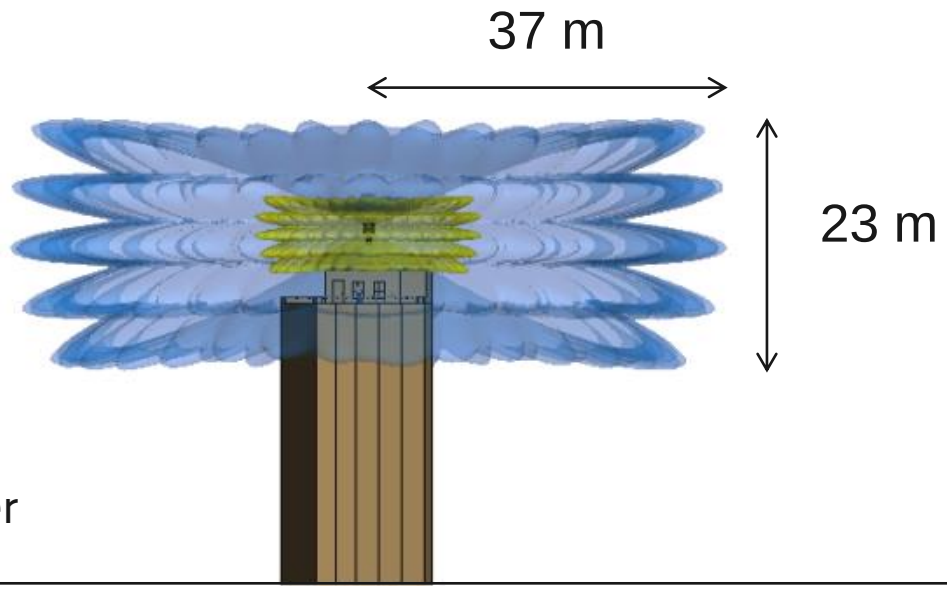
Case study included in IEC TR 62669 – available end of 2018





Exclusion zone 10 W/m^2
ICNIRP general public limit

Impact of lower national EMF limits
1/10 of ICNIRP limit (e.g. India)



5G site
3.5 GHz, three sectors
28 GHz, one sector
Actual maximum power

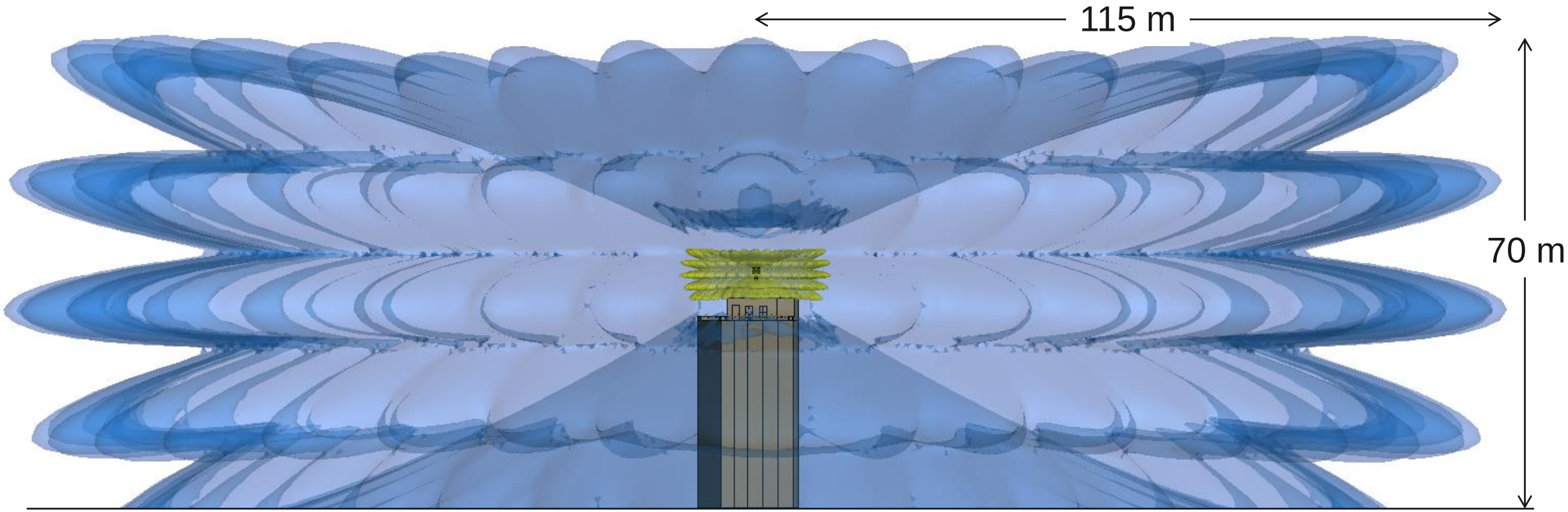
Size of exclusion zone makes 5G network roll-out very challenging

Exclusion zone
10 W/m²
ICNIRP limit

Exclusion zone
1 W/m² (19 V/m)
1/10 of ICNIRP limit

Impact of lower national EMF limits

1/100 of ICNIRP limit (e.g. Poland, Italy, Russia, Switzerland)

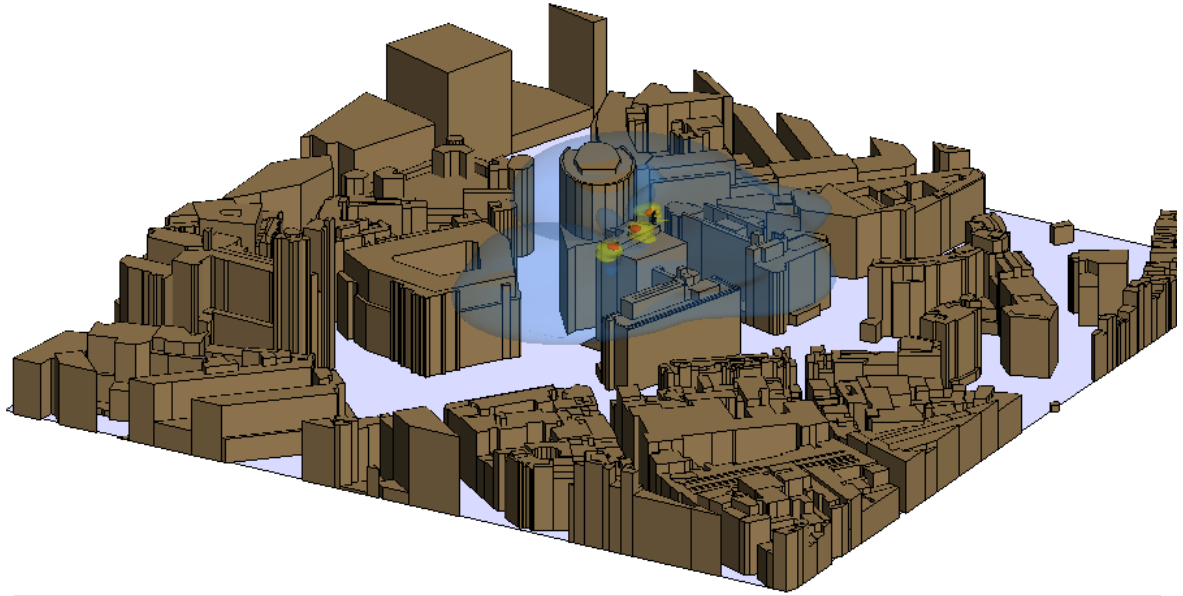


Size of exclusion zone makes 5G network roll-out very difficult or impossible

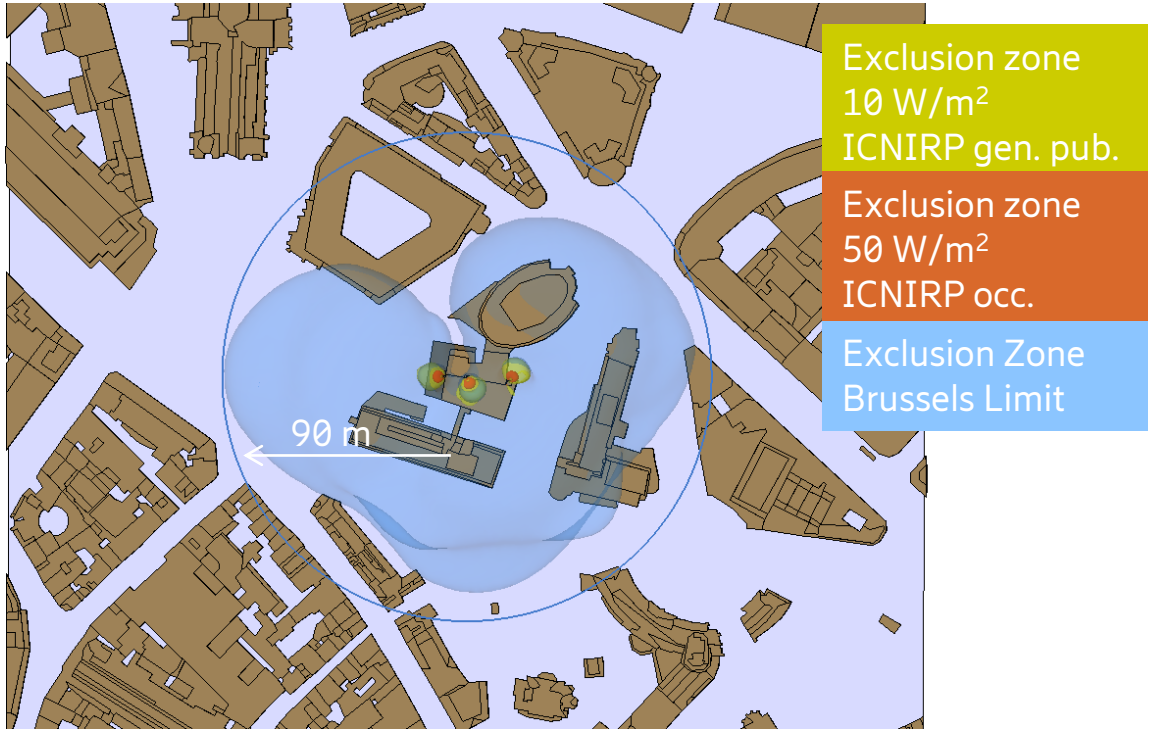
Exclusion zone
10 W/m²
ICNIRP limit

Exclusion zone
0.1 W/m² (6 V/m)
1/100 of ICNIRP limit

5G in regions with very restrictive EMF limits



5G BS (3.5 GHz) on existing 2G/3G/4G rooftop site
Actual maximum power for mMIMO
Brussels limit (6 V/m, 2% of ICNIRP limit)

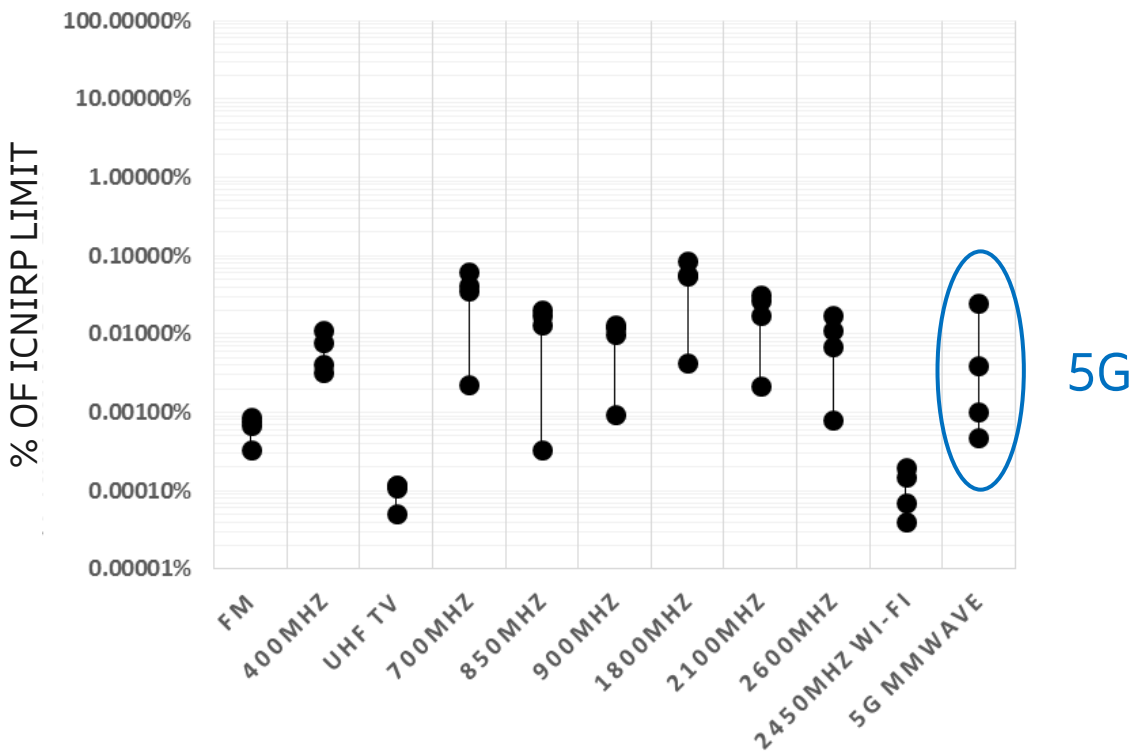


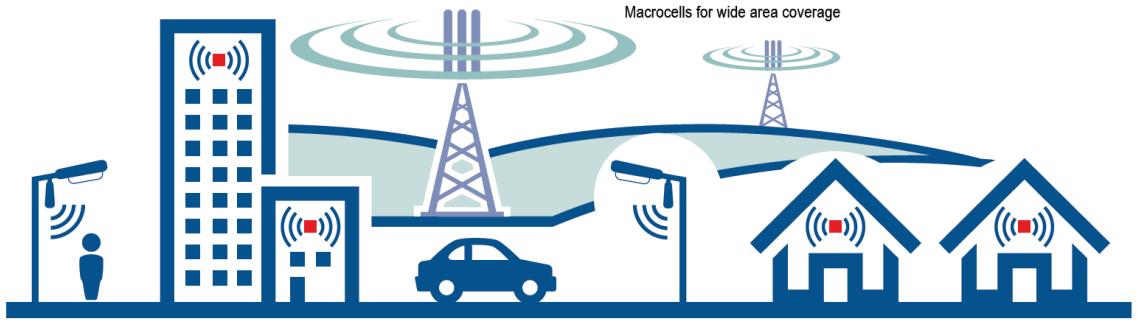
Will be very difficult to rollout 5G on existing sites in countries/regions/cities with EMF limits significantly below ICNIRP guidelines (e.g. Brussels, Paris, Italy, Switzerland, Poland)

Will 5G increase environmental EMF?

- Locally near new 5G transmitters the EMF exposure levels may increase
- The more efficient 5G technology will provide increased capacity with similar EMF levels as for 3G and 4G
- 5G will over time replace existing mobile technologies
- The total EMF exposure will remain low compared to international EMF limits

OUTDOOR MEASUREMENTS IN 27 GHZ 5G TEST NETWORK IN AUSTRALIA (TELSTRA)





Source: GSMA

Conclusions

EMF compliance may be a challenge for 5G if regulations require applying theoretical maximum power for massive MIMO base station sites

International standards from IEC and ITU open up for use of actual maximum power to perform realistic EMF compliance assessments

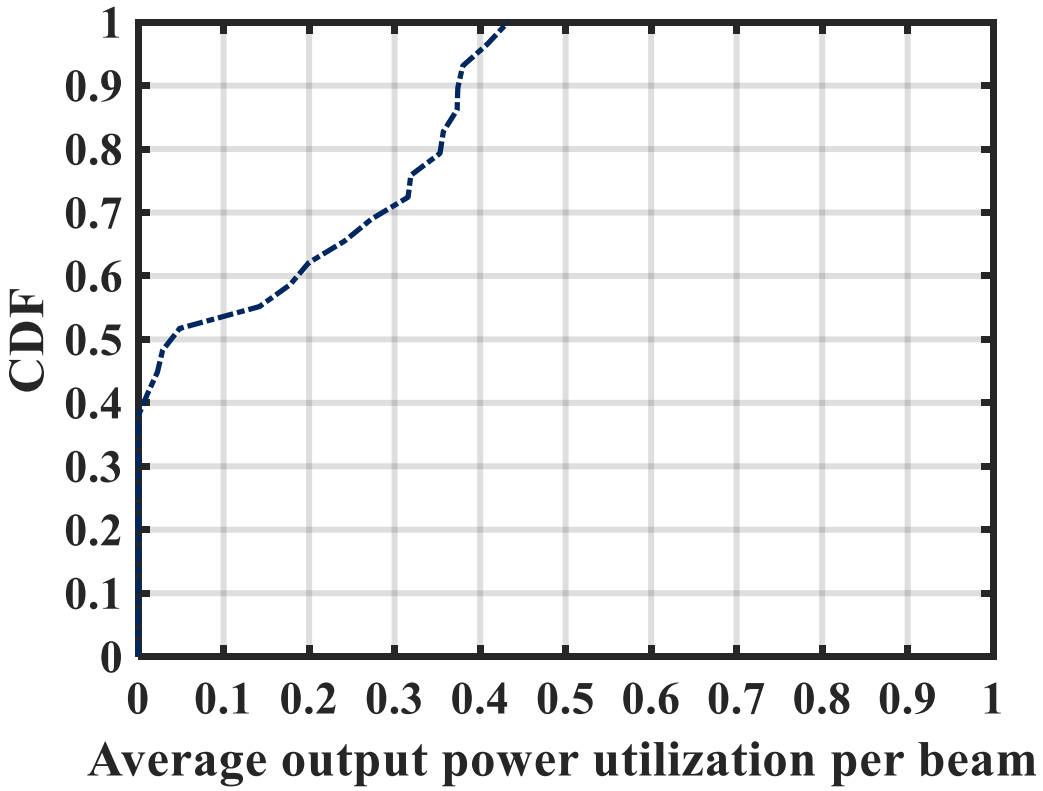
Statistical model to determine actual maximum power of 5G massive MIMO antennas has been developed - found to be around 25% of theoretical maximum power for typical 8x8 array antennas

In countries with EMF limits significantly below the international science-based ICNIRP limits the roll-out of 5G networks will be a major problem – harmonization with international EMF limits and standards needs to be considered

www.ericsson.com/health

Validation of massive MIMO realistic power

Example from first test measurement (not real traffic)



- Using OSS-RC counters
- Possibility to determine time-averaged total and per beam power utilization
- Initially power data will be collected together with customers using AIR 6468 (LTE) and later with AIR 6488 (NR)
- Measurements started in June 2018

National Cyber Security Centre
a part of GCHQ

Some UK Cybersecurity Thoughts

Dr Ian Levy
Technical Director
National Cyber Security Centre

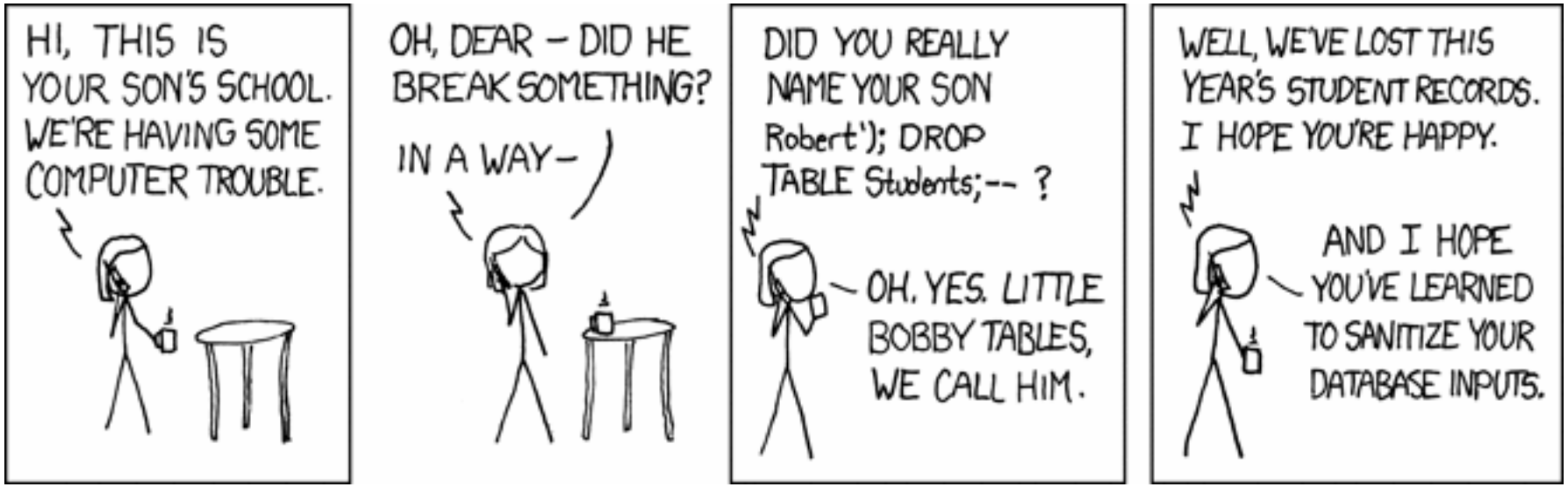
National Cyber Security Centre
a part of GCHQ

Advanced Persistent Threat

National Cyber Security Centre
a part of GCHQ

TalkTalk

National Cyber Security Centre
a part of GCHQ



www.xkcd.com

National Cyber Security Centre
a part of GCHQ

Awesome Advice

Don’t open attachments or click links unless you trust them

National Cyber Security Centre
a part of GCHQ

Awesome Advice

Have a different, complex password for each service and change them often.

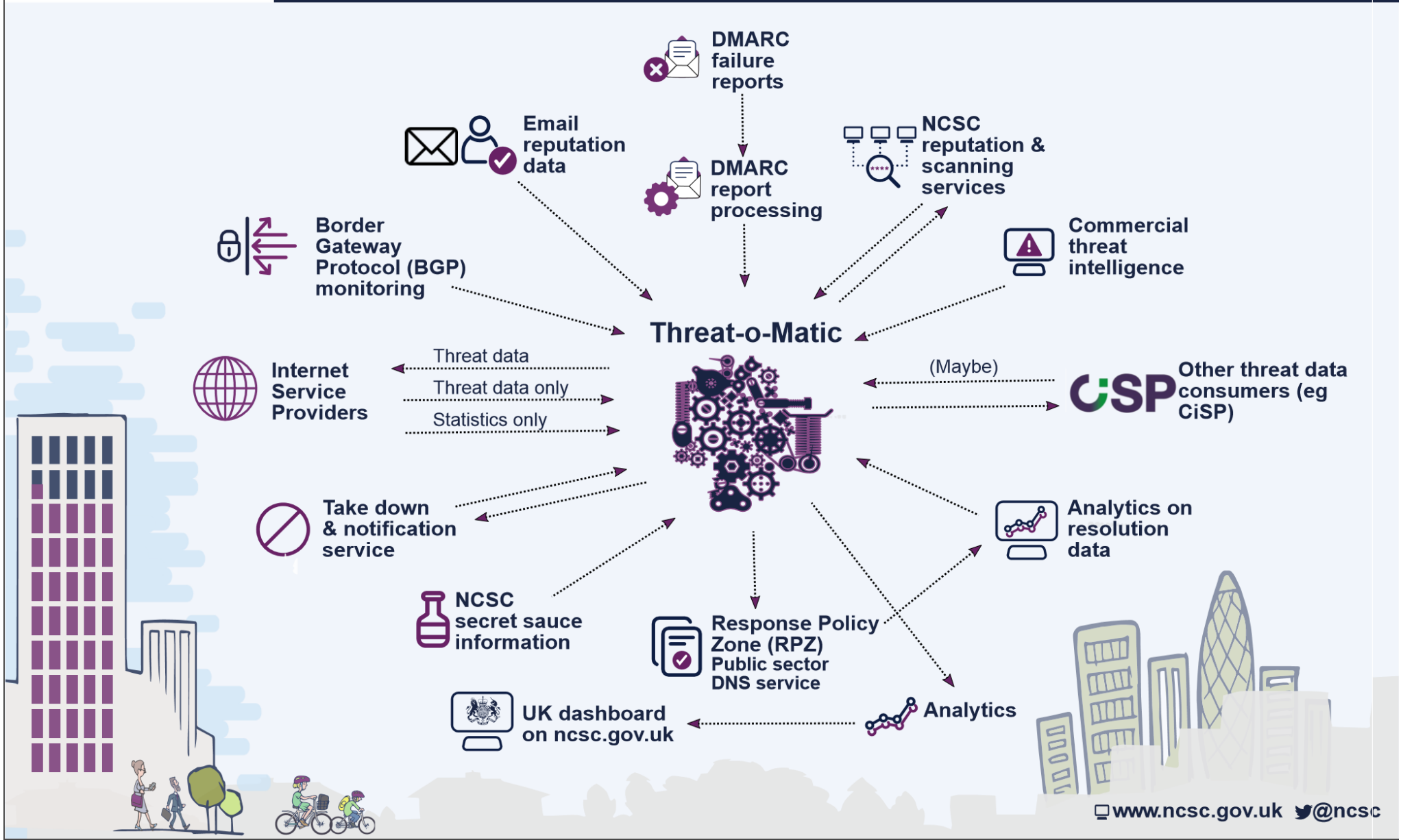
National Cyber Security Centre
a part of GCHQ

https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

National Cyber Security Centre

Active Cyber Defence

The Active Cyber Defence (ACD) Programme outlines how the NCSC intends to tackle - in a relatively automated way - many of the cyber attacks that hit the UK. The diagram below is **not** an architecture, so not all these initiatives will be in place at day one.



Blog post

Active Cyber Defence - one year on

Created: 05 Feb 2018
Updated: 05 Feb 2018
Author: Ian Levy
Part of: Cyber strategy, The NCSC

In November 2016, just after the NCSC formally came into existence, and as the National Cyber Security Strategy was launched, I blogged about our ideas for our Active Cyber Defence programme. I described it as an automated set of interventions intended to tackle a range of commodity attacks.

Some people said it sounded great. Some people said I was talking rubbish (many were not quite so polite!).

Well, we said from the start that the NCSC was going to be transparent and open, and we intend to keep that promise. So today, we're publishing a paper that describes the first year of the ACD programme - both the successes and the things that aren't exactly as we'd want. It's a big paper and there's a lot in it. We've tried to draw out the high-level benefits in the Executive Summary, but the rest of it is worth a read if you've got a technical or scientific bent (or have trouble sleeping).

This is only a start and there's lots more to do. But the paper demonstrates that we've already achieved some cool stuff. I think we can summarise by saying that people in the UK are objectively safer in cyberspace because of the ACD programme.

We've got some great plans for the next year, but in the meantime if you want to find out how much malware was sent in the name of government, how many vulnerabilities we found in

Blogs by Topic

Sociotechnical security (29)
Identity and passwords (18)
The NCSC (18)
Cyber strategy (16)
End user technology (15)
End user device (14)
New talent (14)
Cyber attacks (10)
Skills and training (10)
Vulnerabilities (10)
Partnerships (9)
Sectoral engagement (9)
Cyber threats (7)
IT infrastructure (7)
Research (5)
Digital services (5)
Cloud security (5)
Assurance (5)
Government strategy (4)
Secure by default (4)
Operational security (4)
Design and configuration (4)
Secure communications (3)
Technology at OFFICIAL (3)
Risk management (3)
Network security (2)

National Cyber Security Centre
a part of GCHQ

Harm Reduction By Asking Nicely

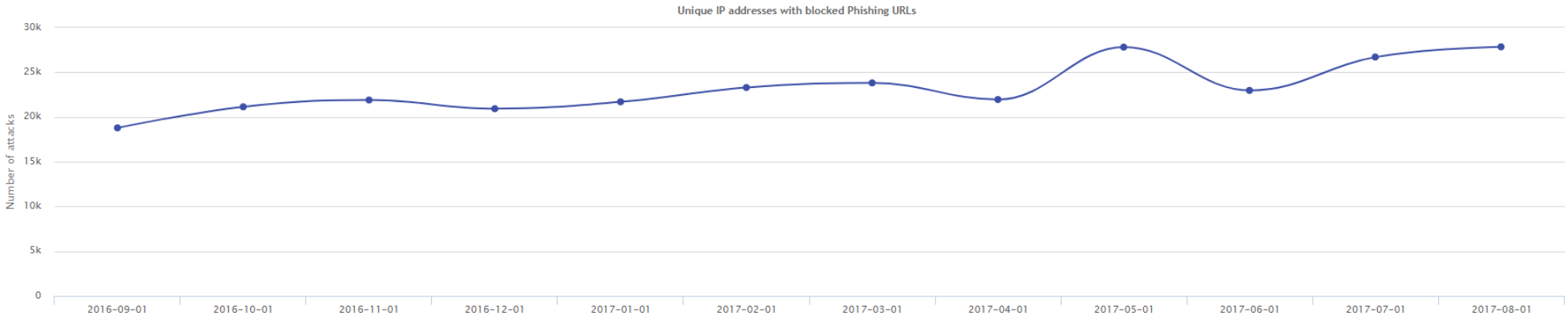
Type	Availability Before (average 1st March 2016 – 31st May 2016)	Availability 31st December 2017
Phishing in UK AS	27 hours (47.4% down in 24 hours)	3 hours (76.8% down in 24 hours)
Webinject in UK AS	525 hours (9.9% down in 24 hours)	39 hours (40.3% down in 24 hours)
UK Gov brand phishing anywhere	45 hours (39% down in 24 hours)	10 hours (65.8% down in 24 hours)

Availability is median time the site is available, until final takedown (yes, we get the tail problem).

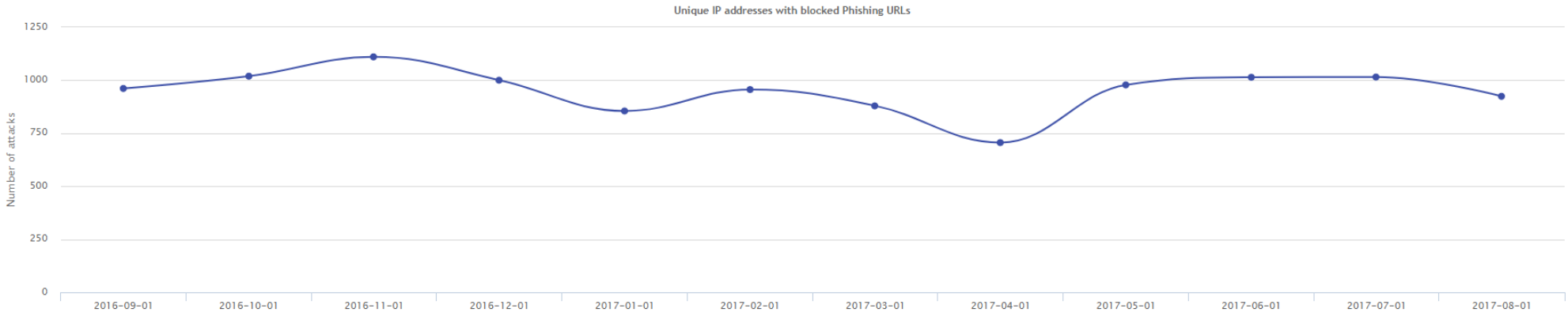
National Cyber Security Centre
a part of GCHQ

It’s all getting worse!!! (Except it’s not)

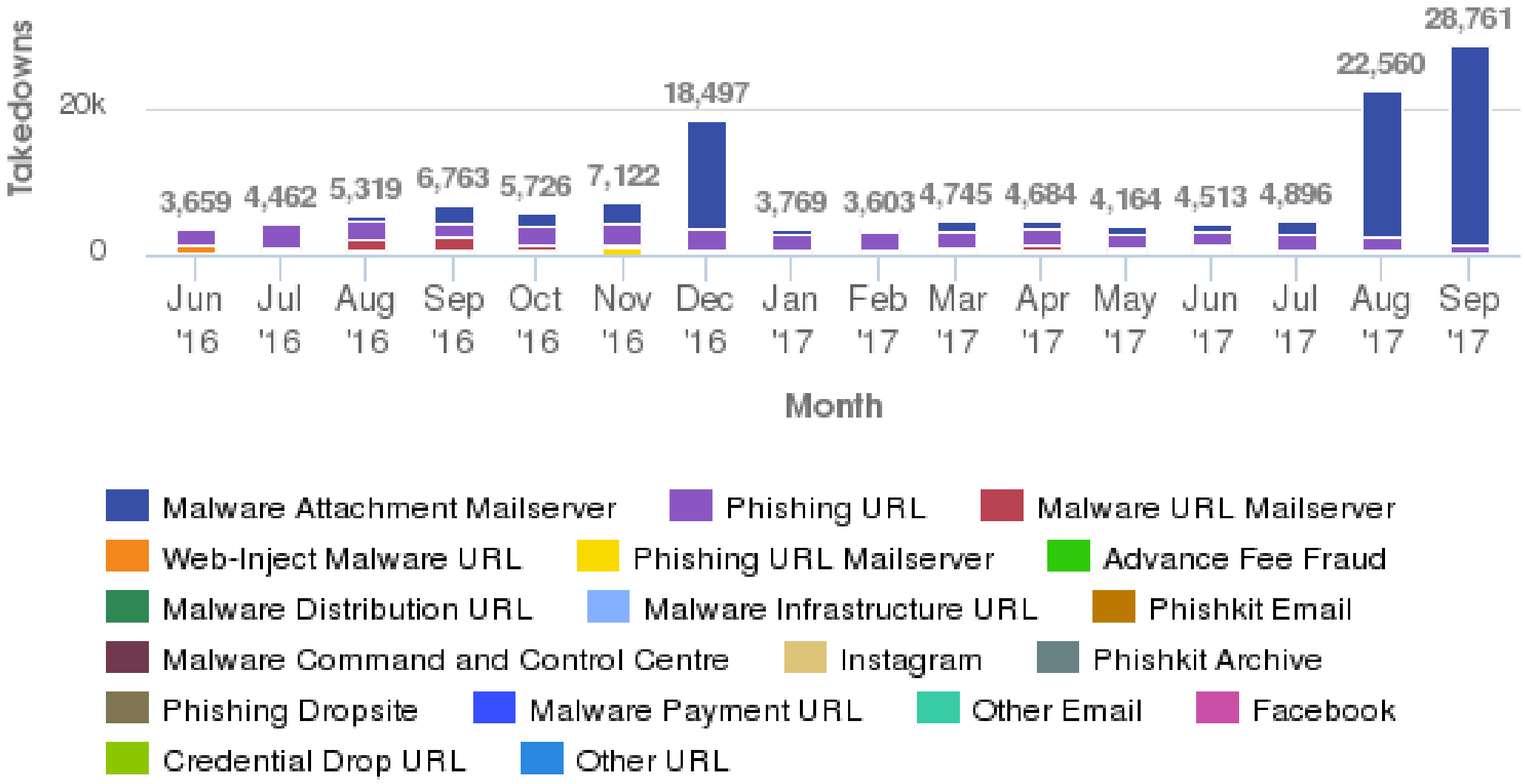
Globally, phishing up 47%



UK share down from 5.1% to 3.3%



National Cyber Security Centre
a part of GCHQ

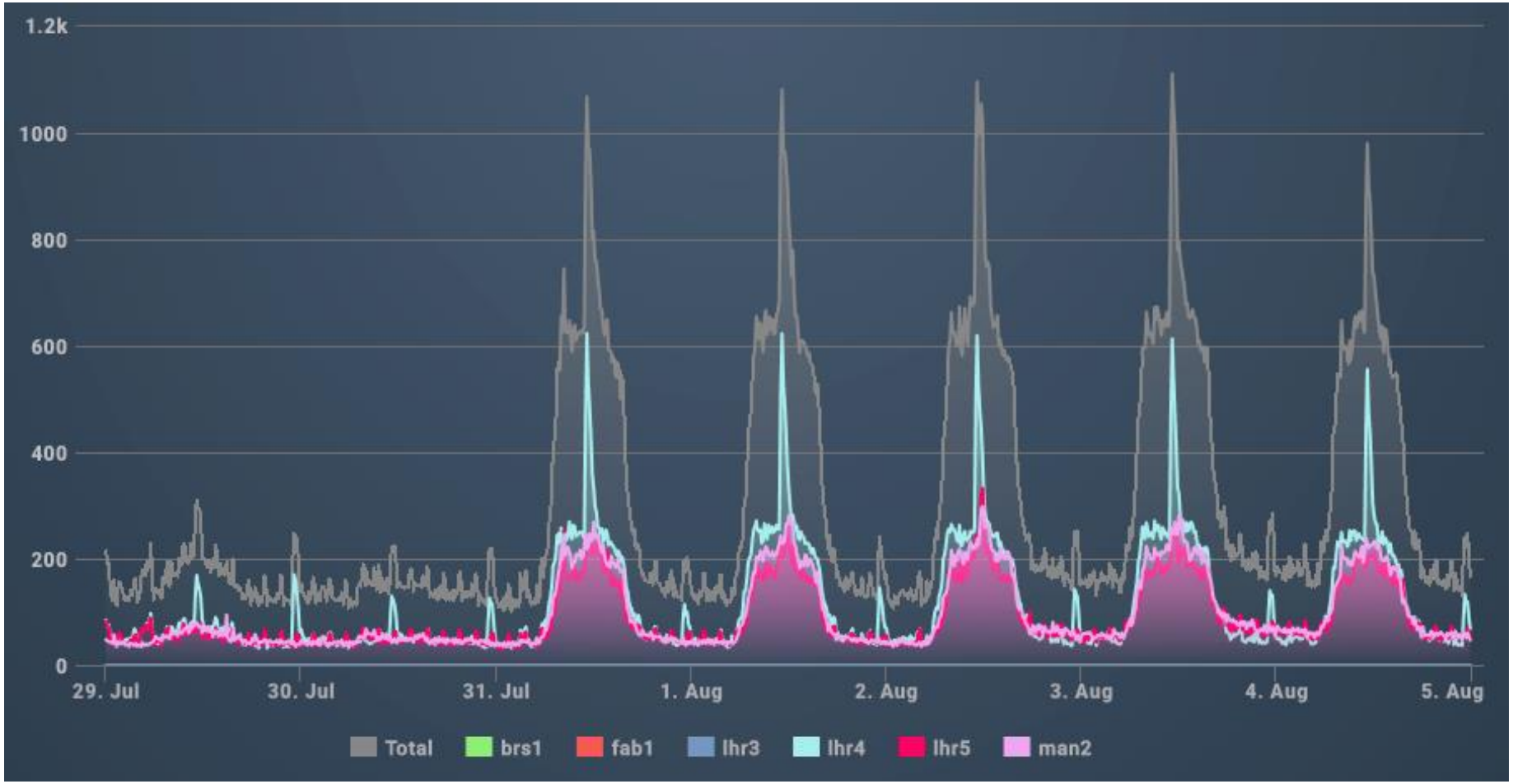


National Cyber Security Centre
a part of GCHQ

+	Date Found	Site	IP	CC	ReverseDNS	ForwardDNS	NetblockOwner	Review Category
+	Since							Filter
+	2017-09-20	income-tax-gov-uk.cf	104.18.52.168	US		cloudflare.com	Cloudflare, Inc.	Suspicious
+	2017-09-13	authorizesecured-hmrc.co.uk				demys.com		Suspicious
+	2017-09-13	government-gateway-servic…	51.15.170.129	FR	te-dns.net	verisign-grs.com	Dedicated Servers and cloud assignment, abuse reports : http:	Suspicious
+	2017-09-11	tax-refunds-hmrc.co.uk	89.36.217.207	DE		tax-refunds-hmrc.co.uk	Cloud Services DC05	Suspicious
+	2017-09-07	hmrc-login.co.uk	198.57.151.195	US	unifiedlayer.com	gator3106.hostgator.com	Unified Layer	Suspicious
+	2017-09-07	loucollgov.uk	94.126.40.154	UK	ai270.net	lcn.com	QUANTUM WEB HOSTING	Suspicious
+	2017-09-06	hmrc-taxrefund.org.uk	134.213.221.69	UK	rackspace.com	demys.com	Cloud Servers UK IP Space	Suspicious

National Cyber Security Centre
a part of GCHQ

DNS is my friend



National Cyber Security Centre
a part of GCHQ

175 = ~ 300,000

National Cyber Security Centre
a part of GCHQ

Markov is DNS's friend

- o2ao4zir7gzgpzfn4dz2jsi7.oo2p9b1nsm1.com
- -n2tdg97d-7speqzsa.iymmvab9gkm1hnx15sx.com
- xf8p0y3fjx6g97gq.-uubwv2gdylsajnypj.com
- iaahgut2gsd.4hmrntzxjhc9r08yo-q476dj7m.com
- z41f23odtjm4c8sz4ivxra0vat.9mo82ft2j1douy.com
- no6hcsvi0ufnasymgpech7i.40v6fp61vdo.com
- g6n6f5mykk6bnmibcgab1wt-.j4ap092agcnyydb.com
- jmvvb4we.7b8sdfinoprtho3ljq4s.com
- zd739c8s8.q8ax0thnqwf7-wbn1gifyfdhj6.com
- p70dgcrd5z8vtpmictdnn6o.v1f-6hdtftl4dyzcwz-0khanp.com
- bomhk02el0in5djqhxs0l.3slfc56wws5f8.com
- fruatgc0d50lys49vtn-.wg48elxnauio6qs8o.com
- v634egrw4l5udvnn45hsehcyi.dwi0tp2aivh0xd.com

National Cyber Security Centre
a part of GCHQ

SS7 and smishing

National Cyber Security Centre
a part of GCHQ

BGP, hijacks and DDOS

National Cyber Security Centre
a part of GCHQ

Dr Ian Levy
Technical Director
NCSC
Hubble Road
Cheltenham, Gloucestershire
GL51 0EX

Tel: 07468 839268
E-mail: ian@ncsc.gov.uk

NCSC Reference:
Date: 02 May 2017

To ISPA Members
via email

Dear ISPA members,

I am writing following the constructive meeting hosted by ISPA on 3rd March which allowed us to discuss the NCSC's Active Cyber Defence programme (ACD) with some ISPA members. The ACD programme is discussed in the National Cyber Security Strategy, available on gov.uk (https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021) and a (slightly) more technical description of the overall programme is in my blog on the NCSC website (https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk). The new strategy seeks to objectively make the UK the safest place in the world to operate online and the ISP community is key to helping us make that a reality. We believe that widespread adoption of relatively simple, industry-standard practices and protocols will have a measurable effect on the harm caused by cyber attack against the UK. For everything we're asking industry to do, we will implement it first across government (where applicable) to prove benefit and help us work out any systemic issues. We will also be open-sourcing the code and infrastructure we build to implement these defences to help wider adoption.

DMARC

We intend to make email mean something again, providing end users with high quality information to help them make good security decisions. While certainly not a panacea, we want to see DMARC implemented widely across the UK to stop simple spoofs being delivered to end users. We will work to ensure that major brands, which generally speaking have high public trust, are protected, but more widespread implementation is important. We are proving the value of DMARC on government domains and have published our implementation guidance on the NCSC website (https://www.ncsc.gov.uk/blog-post/making-email-mean-something-again) and open-sourced the first version of the code for our DMARC report processing service on GitHub (https://www.ncsc.gov.uk/blog-post/open-sourcing-mailcheck). We will be publishing data to show the value of this intervention soon.

We would like all ISPs in the UK to :

1) Implement DMARC on their own domains, moving to p=reject quickly
2) Help us ensure that DMARC records are correctly processed by all receiving MTAs in UK ISPs
3) Help us ensure that all UK ISPs' mail services can correctly support DKIM signing on outbound mail and that neither sending or receiving mail

infrastructure actively breaks SPF or DKIM (for example, by rewriting headers incorrectly)

4) Help your customers implement DMARC on their domains, including providing report processing services where appropriate

Infrastructure Protocols

We are working with the Network Security Information Exchange (NSIE) on better implementation standards for BGP and SS7, to help ensure that the majority of the common attacks using these protocols are much harder against UK ISPs. We are also looking to build a community BGP monitoring solution to enable ISPs to be notified if there are attempts to hijack their prefix ranges. This work is ongoing, and we would welcome participation from any ISP willing to help.

In the interim, we would ask all ISPs to consider the following:

1) If you participate in the SS7 network, implement the SS7 filtering standard available from GSMA and NSIE[1]. We'd strongly encourage you to implement home routing and to ignore messages from your own Global Title that originate from outside your network as an absolute minimum. We intend to secure some SMS TPOAs in the future to make smishing harder and this is greatly enhanced by home routing (among other benefits).
2) To help reduce the effectiveness of UK infrastructure when used as part of a DDoS, we would ask all ISPs to – as a minimum – implement BCP38-like prefix ingress filtering. This will help us reduce the incidence of source IP spoofing on UK networks, making certain types of DDoS harder from UK infrastructure. This will also reduce the value of UK-based infrastructure to attackers in the short term. This is a first, but valuable, step.
3) Catalogue and understand peering and transit relationships and the consequent BGP relationships. The work we will be asking the community to do on BGP hijack prevention will need a good understanding of the intended peering and transit relationships in order to better manage the effect of malicious updates. We do not expect to use RPKI or other cryptographic measures to manage this problem, but instead better manage the update process.

Management protocols

We have seen several attacks using end user equipment and even CPEs to generate malicious traffic. The reality is that we will have to live with vulnerable devices for the foreseeable future, but we should take action to minimize by default the harm those vulnerable devices can cause. Most of those attacks have relied on management-related protocols being available from the WAN side by default. We would ask all ISPs to consider restricting protocols such as telnet, SSH, UPNP and SNMP inbound to consumer endpoints by default. Obviously, customers requiring these should be able to re-enable them – and it is likely those that need these protocols understand how to secure them.

Furthermore, we have seen TR-064/TR-069/CWMP-based attacks against CPEs. Since very few CPEs in the UK seem to correctly implement management security, we would ask all ISPs to block CPE management protocols from being routed from

[1] Please contact us if you require access to these documents and do not already have a way of obtaining them from the relevant bodies.

outside their network. There seems to be no valid use case for allowing CPE management from outside the network, but we would welcome a discussion if ISPs disagree.

Finally, we would ask ISPs to be vigilant in ensuring their own management plane is not accessible from the Internet. We routinely see artefacts that suggest this is not the case. Tools such as Shodan may help an ISP ensure they have not inadvertently allowed access to their management plane.

Protecting customers

We are building a public sector DNS service that will help protect all of public sector against commodity cyber attack. We intend to publish data from this service showing the actual impact and harm reduction. We believe that ISPs should consider protecting their residential and SME customers by default from known cyber attacks. We appreciate that this could be an emotive subject and so we would like to work with industry representatives to develop a taxonomy of 'bad' that explains what we will and will not block. We are working on an early draft for discussion, but our intention is to be transparent with the public on what our data set contains and what we recommend ISPs block. We will not try to mandate ISPs to provide customer protection or mandate the technical implementation or data used to implement it. However, we believe that, if the majority of ISPs choose to protect their customers by default from objectively harmful sites, the UK will be significantly better off in terms of reduction of the harm caused by cyber attack. We will provide the data we use for protection of the public sector and access to our infrastructure if that would help drive adoption.

Working together

I hope the ISP community will come together and work with us, starting with the technical work described above. While we are very happy to work bilaterally, I believe that a community approach is more sustainable and likely to provide benefit to all. To that end, I would like to suggest that we create a group on our CiSP platform (https://www.ncsc.gov.uk/cisp) to enable the community to come together in a safe and secure place to discuss these measures and others as our collective understanding evolves.

We look forward to working together with the ISP community to make the UK a measurably safer place to live and work online. We would welcome a community response through ISPA but equally I am happy to talk bilaterally with any ISP with concerns or suggestions.

Yours Sincerely,

Dr Ian Levy
Technical Director, NCSC

National Cyber Security Centre
a part of GCHQ

Reducing Impact of Cyber Attacks

National Cyber Security Centre
a part of GCHQ

TBEST

National Cyber Security Centre
a part of GCHQ

1000

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight | Pre

Home > News Archive

News

Advice on managing enterprise security published after major cyber campaign detected

Created: 03 Apr 2017
Updated: 03 Apr 2017

- **Third parties who manage large organisations' IT services attacked**
- **NCSC leading investigation in partnership with Cyber Incident Response partners**
- **Advice urges enterprise security teams to discuss risk with Managed Service Providers**

TARGETED expert advice aimed at Managed Service Providers and their customers has been published after a global cyber attack was uncovered by a multi-organisation collaboration led by the National Cyber Security Centre (NCSC).

The attacks are against global Managed Service Providers (MSPs), which are third parties who help to manage large organisations' IT infrastructure and services. MSPs are particularly attractive to attackers because they have privileged access to other organisations' systems and data.

Due to the incident affecting mainly larger organisations, the NCSC believes the risk of direct financial theft from individuals is unlikely.

The attacks provide a reminder about the importance of organisations choosing and monitoring their outsourcing partners carefully, so the NCSC has posted a range of advice on their website about what people should be done to mitigate against risks.

Ciaran Martin, CEO of the government's National Cyber Security Centre Said:

National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight | Press & Media | Topics

Home

UK Internet Edge Router Devices: Advisory

Created: 11 Aug 2017
Updated: 11 Aug 2017

You should read this advice if you are an internet service provider, or an enterprise that manages your own customer edge (CE) devices.

Summary

- This advice builds on existing technical guidance on the NCSC website.
- The NCSC is aware of a number of router compromises in telecommunications companies and Internet Service Providers, where a hostile actor has extracted configuration files from internet facing network devices. The configuration files can contain administrative credentials which may then be used to compromise all traffic passing through the router, and allow the actor to target other devices on the network. They have also gained interactive engineer access to some routers.
- In some cases where routers have been successfully compromised, the NCSC is aware that the hostile actor has created Generic Routing Encapsulation (GRE) tunnels to extract traffic traversing the router. They do this by using an Access Control List which they control on the compromised router, and exfiltrate the traffic they are interested in to infrastructure which they control, which is often outside the victim's country. In these cases where the NCSC is aware, we have already contacted the impacted organisations.
- The incident is still under investigation, and the NCSC is working with ISPs to make affected entities aware, and support remediation.
- This advisory note details mitigation strategies to secure networks against these attacks.

Most Popular | Most Shared

1. What does the NCSC think of password managers?
2. Three random words or #thinkrandom
3. 10 Steps to Cyber Security
4. Cyber Security Information Sharing Partnership (CiSP)
5. Password Guidance: Simplifying Your Approach

National Cyber Security Centre
a part of GCHQ

Economic disincentives

National Cyber Security Centre
a part of GCHQ

Why will 5G networks be better?

National Cyber Security Centre
a part of GCHQ

Questions?

5G Security Evolution

Security measures needed in the underlaying 5G communication infrastructure to meet today's and tomorrow's cyber-attacks

Anna Kåhre,
Strategic Product Manager, RAN Security

Security challenges for Mobile Operators

Ever evolving security threats

Critical infrastructure and increased business risks

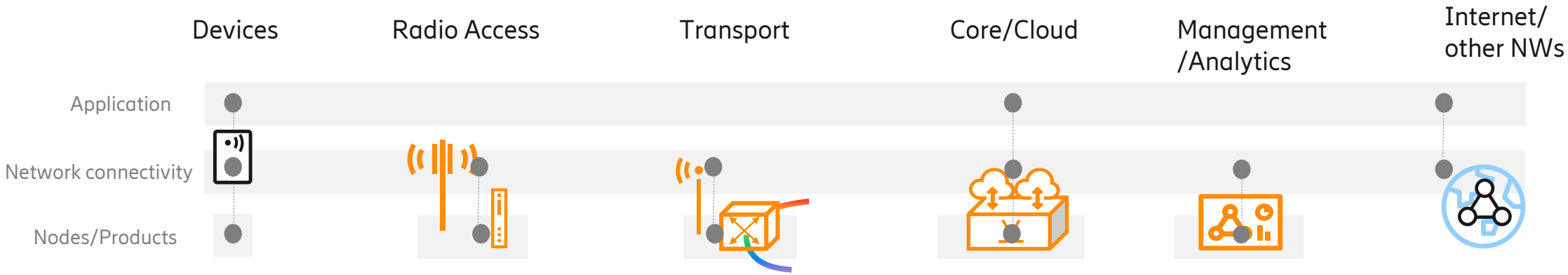
Increasing regulatory requirements (e.g. GDPR)

Rising amount of vulnerabilities (Vulnerability watch)

Billions of new devices

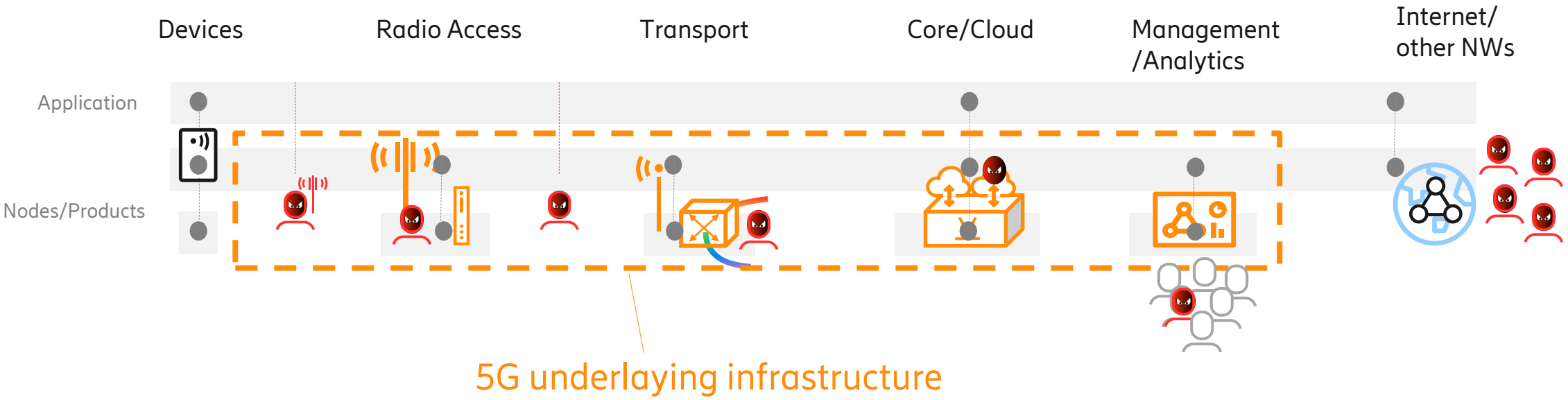
Cloud-specific challenges

5G infrastructure

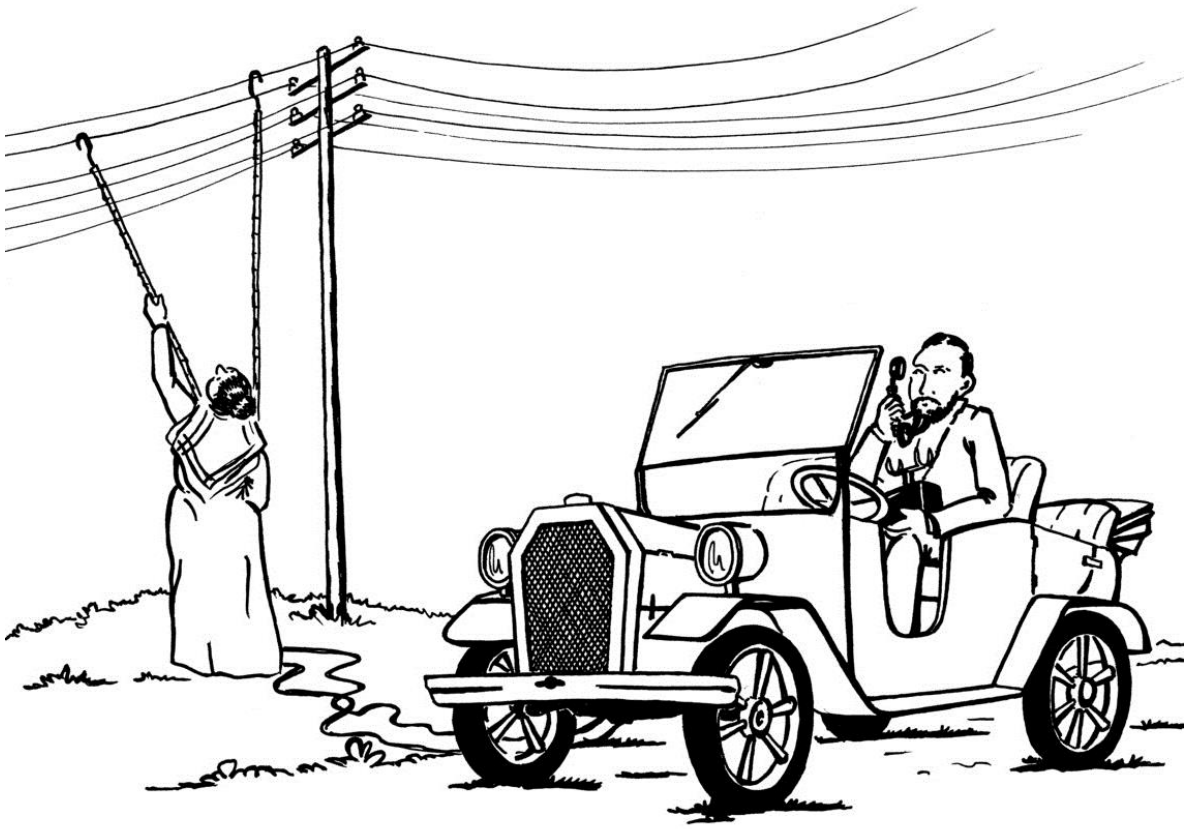


5G infrastructure

- Attack vectors on all levels, external as internal



Threats to the connected society



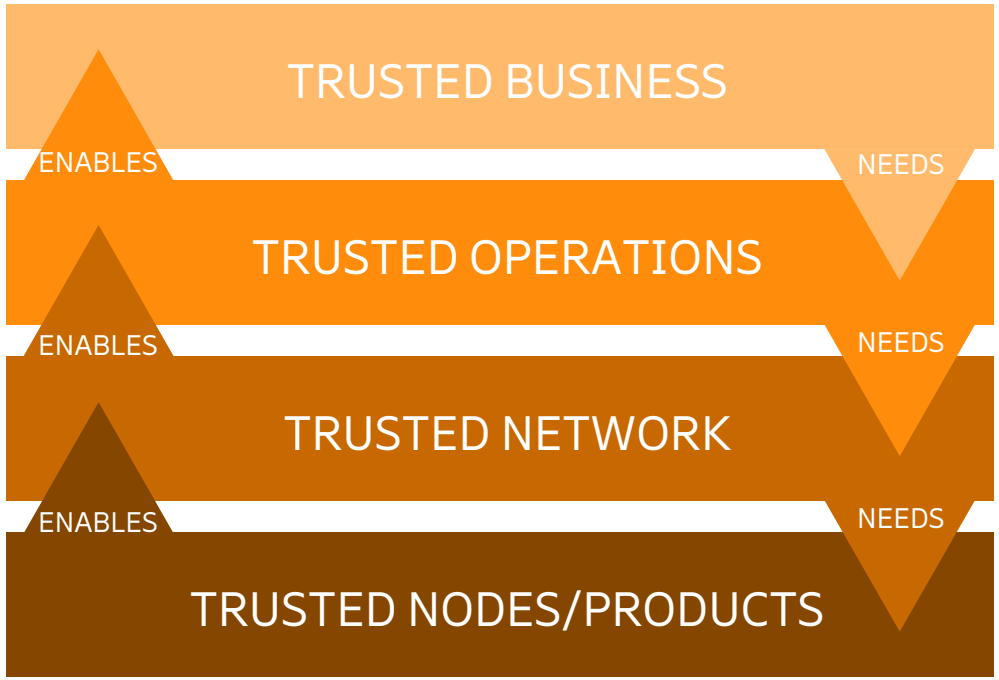
- A number of threat actors exist:
  - Organized Cyber criminals
  - Nation states
  - Hacktivists, e.g. “Anonymous”
  - Terrorists
  - Insiders

Networks Secure by Design

Built in from the start

— Ericsson's holistic approach across technology and services ensures security

The trust stack

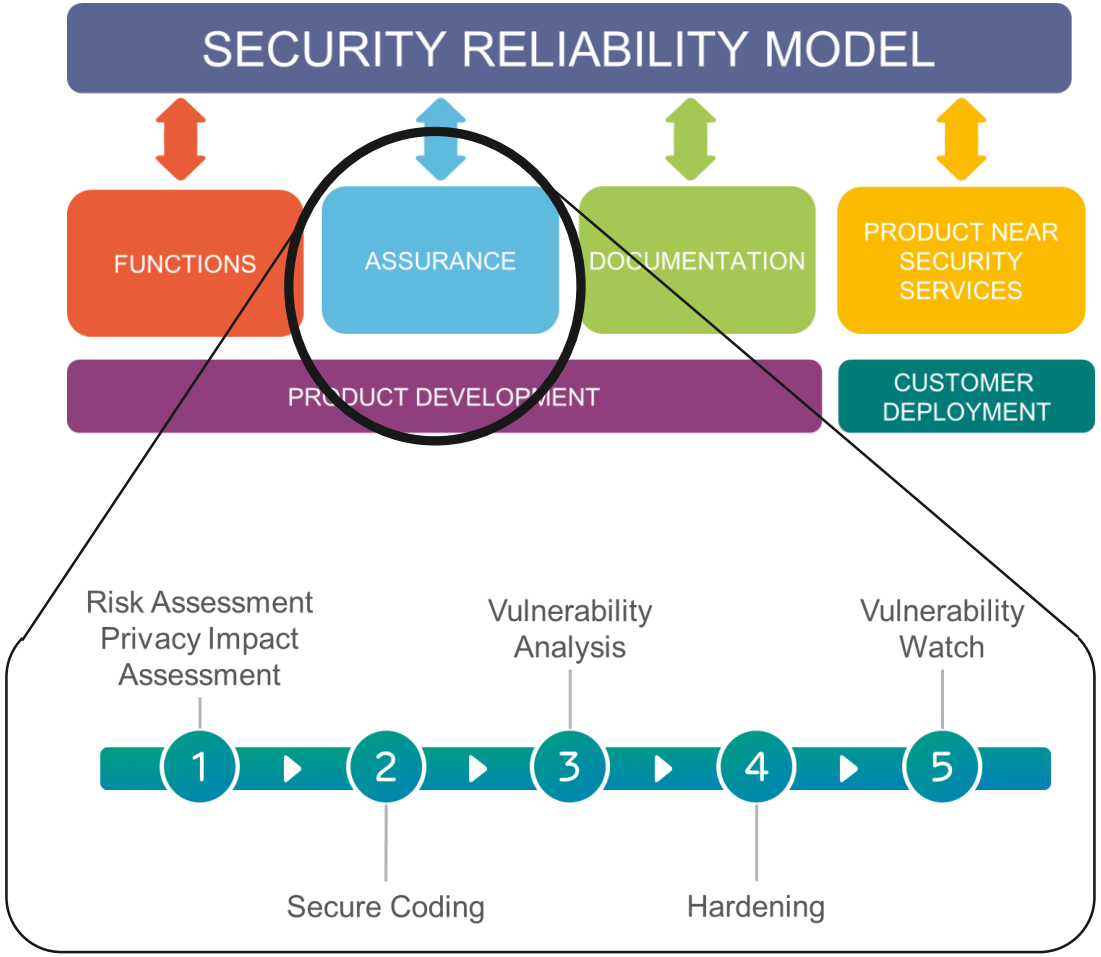


- Business decisions to accept residual risks and manage unacceptable risks
- Appropriate procedures for handling secure operations
  - User handling, security analytics & policy compliances, privacy
- Sound, manageable security architecture
  - Identity management, communication security, resilience, resilience, slicing, privacy
- Nodes/products without exploitable vulnerabilities
  - Security Assurance, node security, cloud security , privacy

Security assurance

- Security reliability model - Ericsson framework related to security
  - Ericsson performs.....
    - Risk Assessment
    - Privacy Impact report
    - Secure Coding
    - Vulnerability Analysis
    - Hardening guideline

      .....for every release
- Ericsson PSIRT keeps track of new vulnerabilities



Node security

- Node hardening
  - Service ports
  - Secure protocols
  - Limit access to file system
  - Access Control Lists (filtering traffic)
  - Etc

→ Limits attack surface towards the node

- Root of Trust
  - Secure Storage

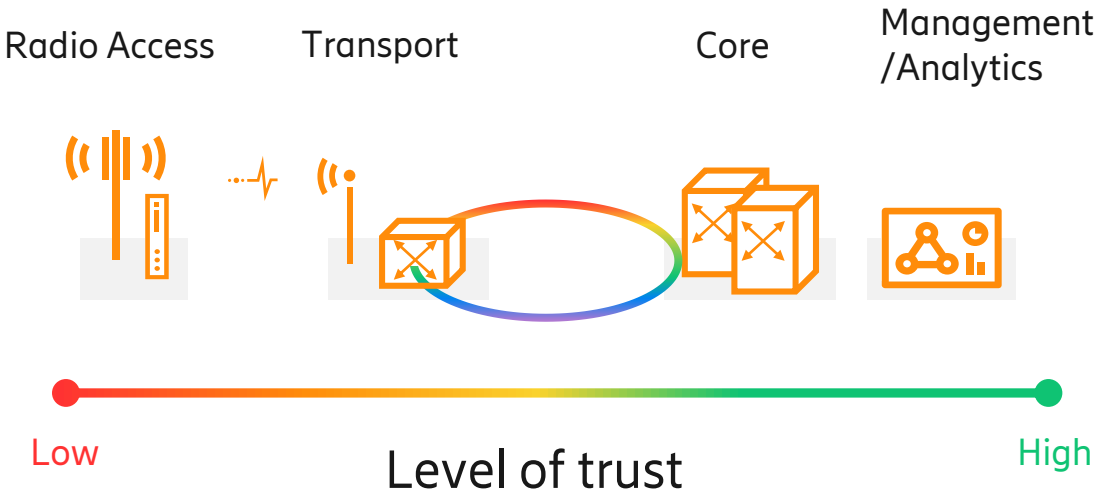
→ Area that keeps secrets e.g. keys in a safe place

- Trust anchors
  - HW-rooted Secure Boot
  - Signed Software
  - Validation of SW

→ Prevents loading of unauthorized SW e.g. malware

- Access rights (& Encryption) of data at rest
  - Sensitive data stored in nodes
  - Security logs/ Audit trail logs

→ Prevents unauthorized users to get hold of sensitive data



Node security

- Node hardening
  - Service ports
  - Secure protocols
  - Limit access to file system
  - Access Control Lists (filtering traffic)
  - Etc

→ Limits attack surface towards the node

- Root of Trust
  - Secure Storage

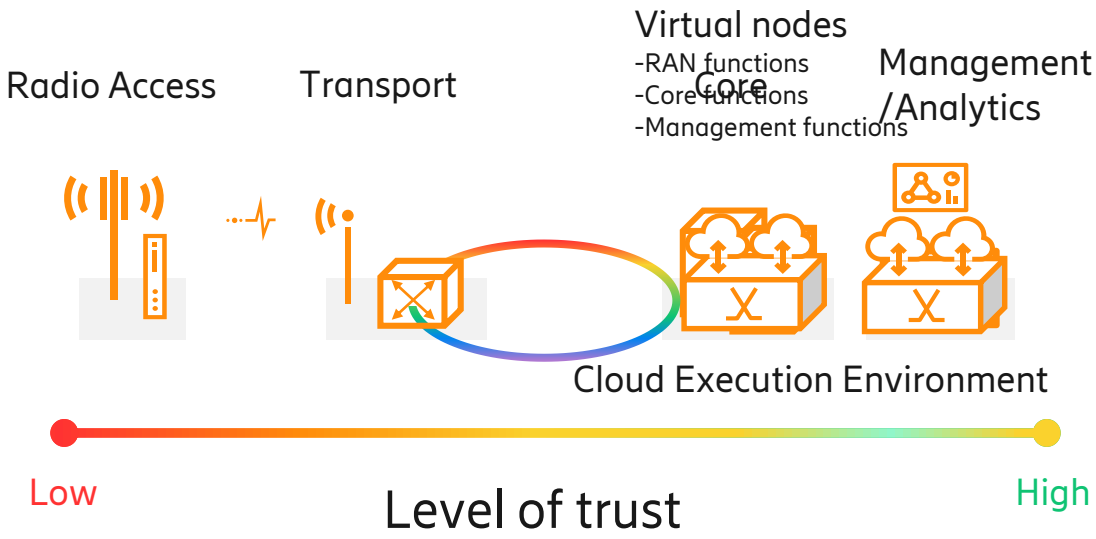
→ Area that keeps secrets e.g. keys in a safe place

- Trust anchors
  - HW-rooted Secure Boot
  - Signed Software
  - Validation of SW

→ Prevents loading of unauthorized SW e.g. malware

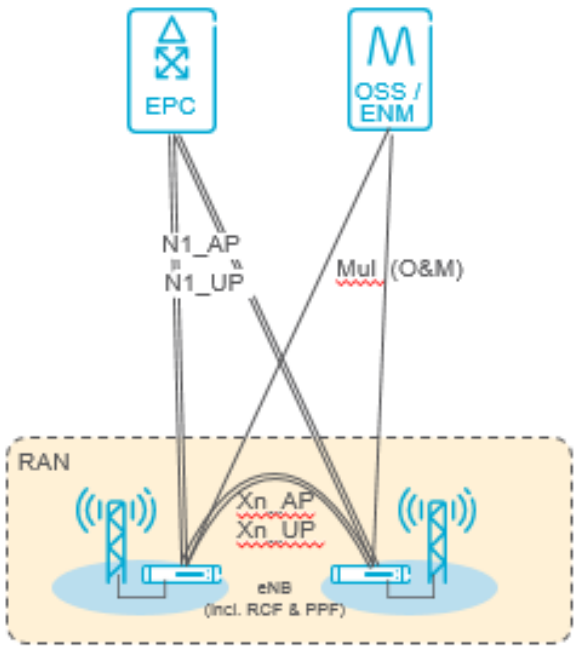
- Access rights (& Encryption) of data at rest
  - Sensitive data stored in nodes
  - Security logs/ Audit trail logs

→ Prevents unauthorized users to get hold of sensitive data

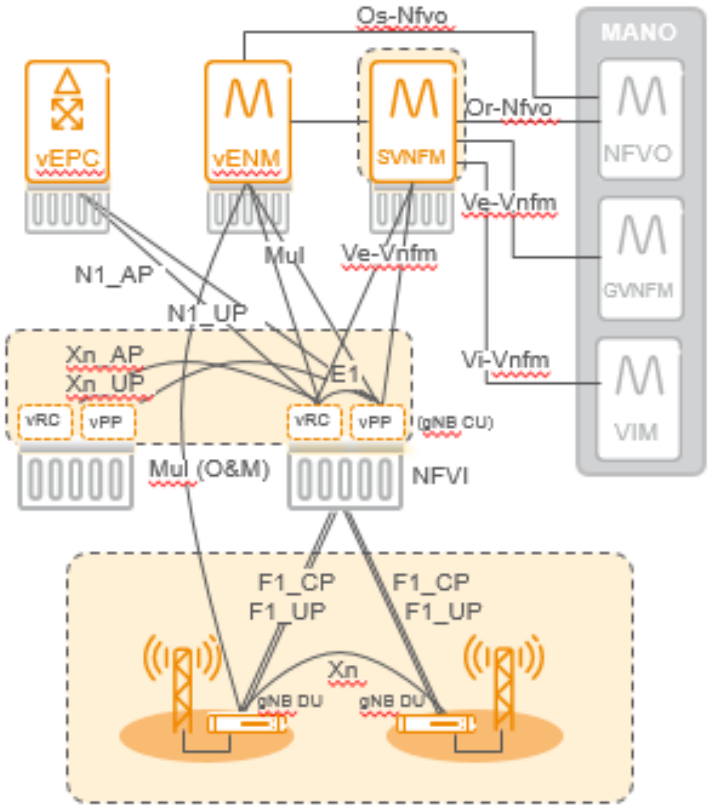


RAN ARCHITECTURE

DRAN
(Distributed RAN)



VRAN
(Virtualized RAN)



Mobile Operator
Mobile Operator (Tenant)
Cloud infrastructure

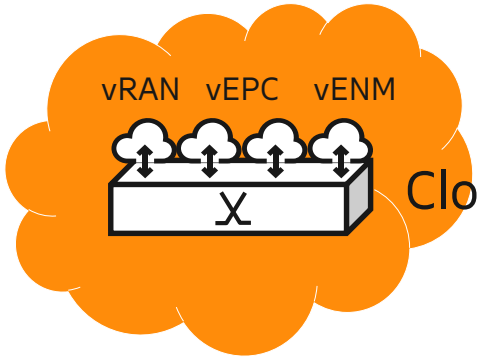
MANO – Management and Orchestration
NFVO - NFV (Network Function Virtualization) Orchestration
GVNFM – Generic VNF (Virtualized Network Function) Manager
SVNFM – Specific VNF Manager
VIM - Virtualized Infrastructure Manager
NFVI – NFV Infrastructure
ENM – Ericsson Network Manager
vRC – virtual Radio Control
vPP – virtual Packet Processing
BPF – Baseband Processing Function

Virtualization & cloud security

- New attack vectors and trust relations requires additional security
  - SW decoupled from dedicated HW
  - Other organization is managing the infrastructure
  - Yet another organization may share the same HW

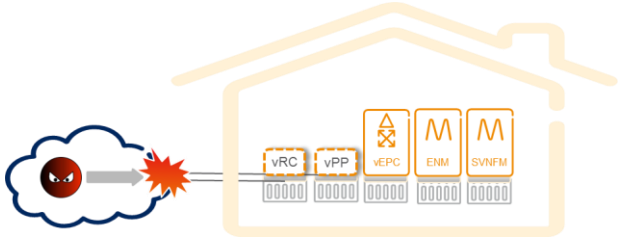
Virtual nodes

-RAN functions
-Core functions
-Management functions

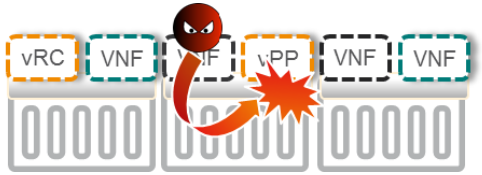


Cloud infrastructure

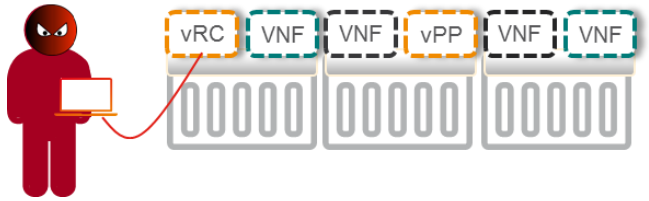
› External attack/intrusion
  – Protection of traffic and access



› Cross VNF attacks
  + Environment correctly set-up
  + Protection of keys and SW



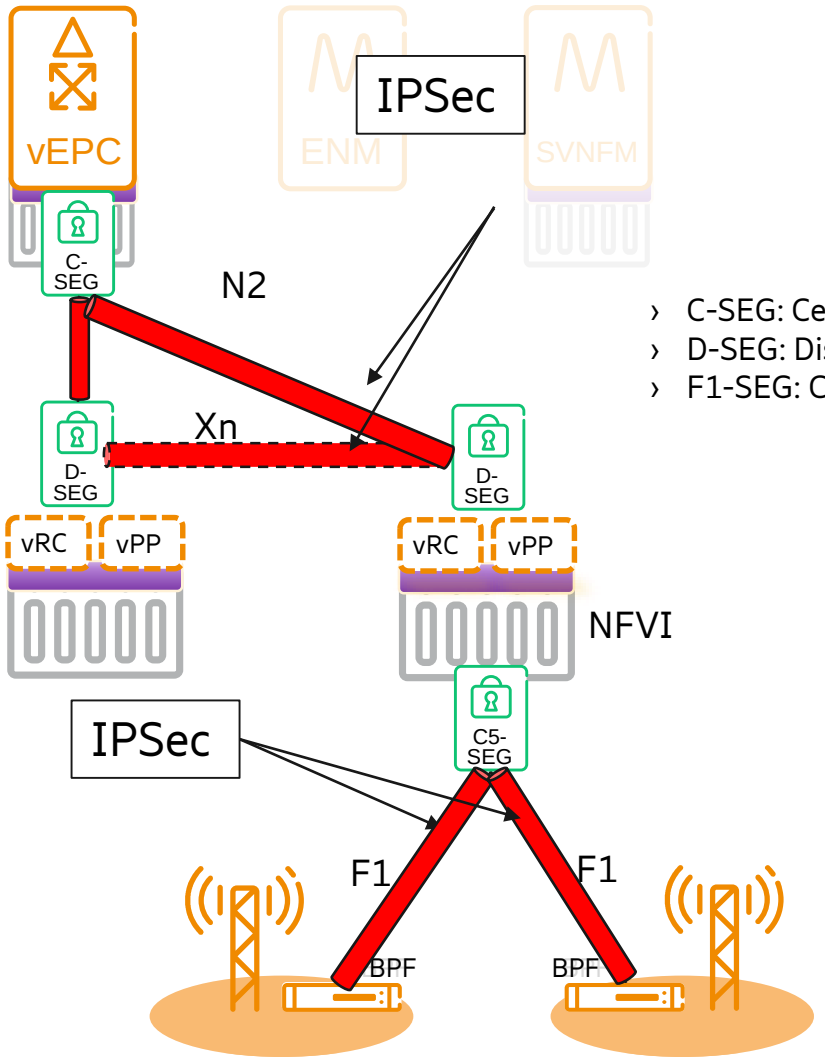
› Insider attack/intrusion
  + Additional authentication and different levels of authorization
  + Trust required



IPSEC IN VRAN

- N2/Xn IPsec
  - Optional, for encryption and integrity
  - The same as non V-RAN architecture
  - Termination between vEPC and vPP/vRC
  - Direct X2 IPsec is not critical, can go over C-SEG
- F1 IPsec
  - Optional, for hiding V-RAN topology
  - Termination between vPP/vRC and BPF
  - Multi-multi vPP/vRC BPF IPsec tunnels
  - Zero touch provisioning among C5-SEG and BPF

5G transport	C5	S1
Throughput	2-10G	10-40G
Latency (one way)	<5ms	<15-30ms

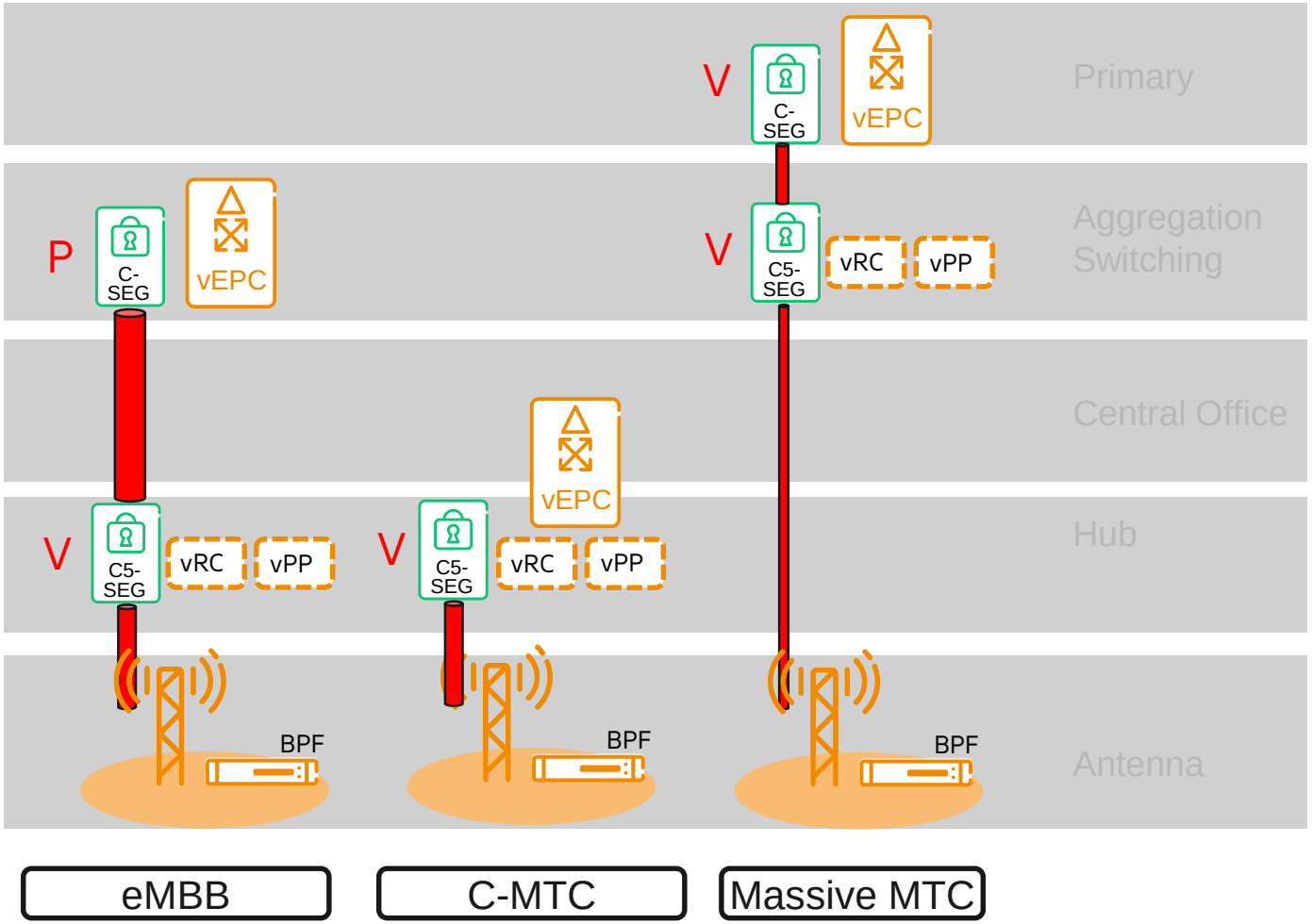


- C-SEG: Central Security Gateway
- D-SEG: Distributed Security Gateway
- F1-SEG: C5 Security Gateway

DEPLOYMENT OPTIONS

- Virtualized or physical SEG
  - Virtualized SEG with flexibility
  - Physical SEG with capacity
- Virtualized SEG
  - Separate VNF in separate HW
  - Separate VNF in the same HW that hosts other VNFs
  - Accelerations possible with dedicated HW
- Example use cases
  - eMBB, IPsec for S1/X2 and C5, high capacity C-SEG
  - C-MTC, IPsec for C5 only
  - Massive MTC, IPsec for S1/X2 and C5, moderate capacity C-SEG

Pysical
Virtual



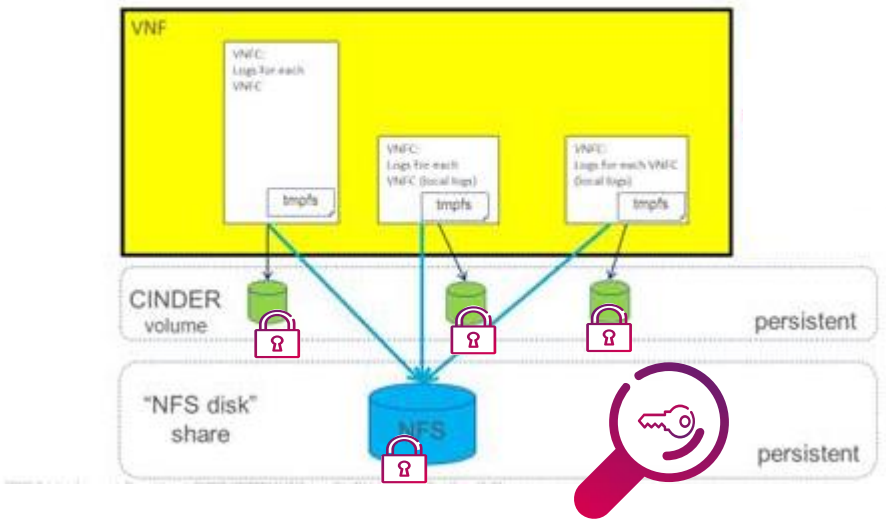
Data at Rest

Application based encryption of

- Configuration data
- Sensitive data (keys and credentials)
- Some of the log files e.g. AuditTrailLog and SecurityLog

Virtualized RAN

FILE SYSTEM/STORAGE FOR VNF/VNFC:S



Protection of secrets

vTPM

- vTPM exposes an API that gives applications the same facilities as the physical TPM
- Security wise maintains the properties of physical TPM (pTPM)
- vTPM requires an anchor in a pTPM

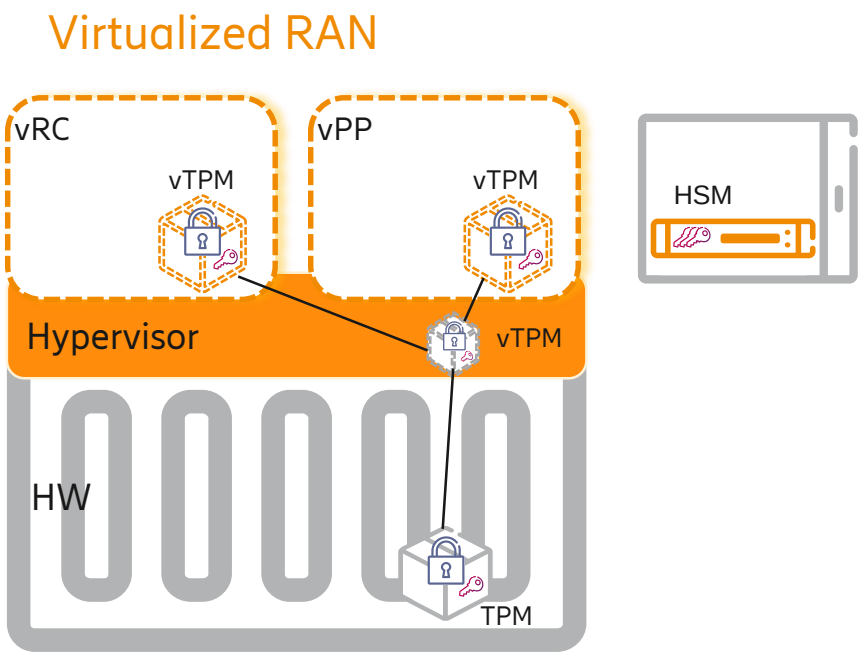
sTPM

Acts from the VNFs point of view as a HW-based TPM.

- When no TPM or vTPM availabile in cloud infrastructure
- Not as secure as vTPM with an anchor in a pTPM
- Obfuscation and white-box crypto to increase security

HSM

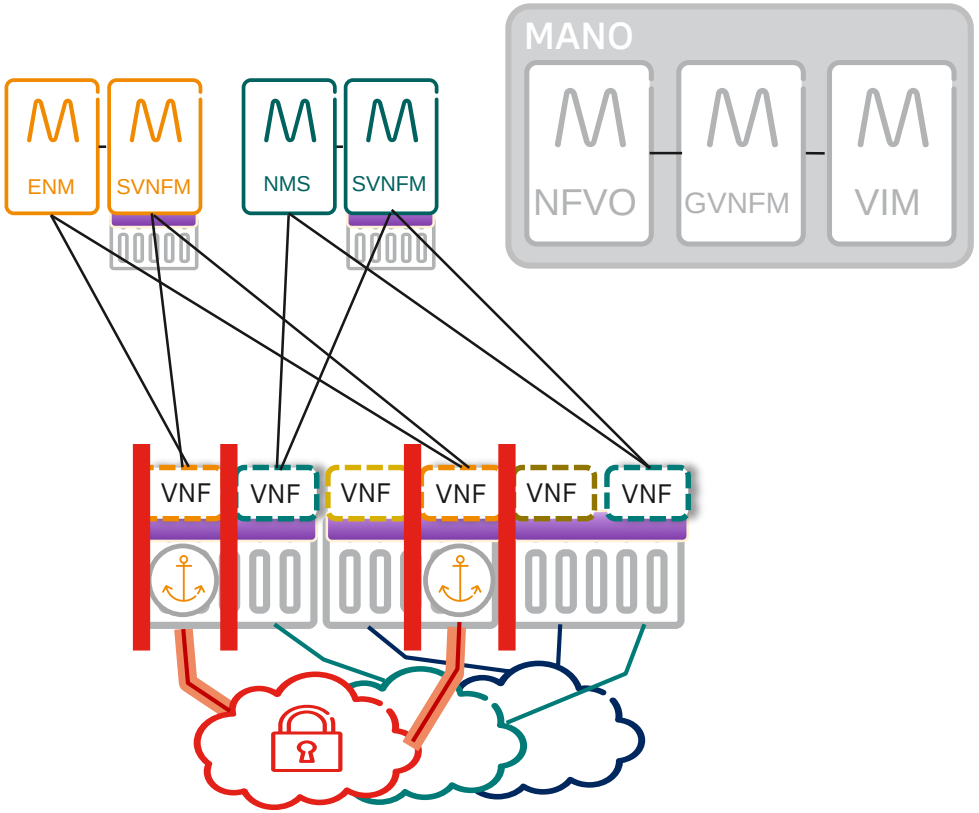
- HW Security Module planned to be supported as an alternative solution
- Requires separate HW



Cloud node security

Infrastructure

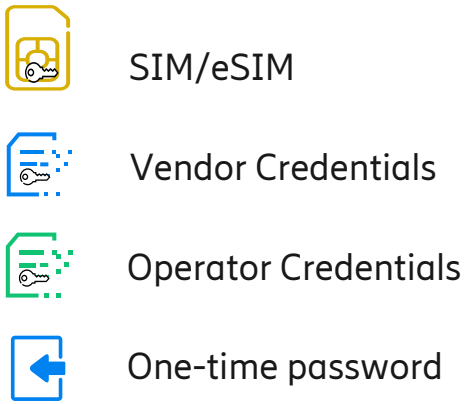
- Hardening (e.g. close unused ports and interfaces)
- Secure framework in place (e.g. login cred. on Ethernet ports)
- Physical root of trust and entropy sources for tenants
- Segmentation and separation between Tenants (e.g. VxLAN), unauthorized VMs to be blocked
- SW check for validation of tenants images

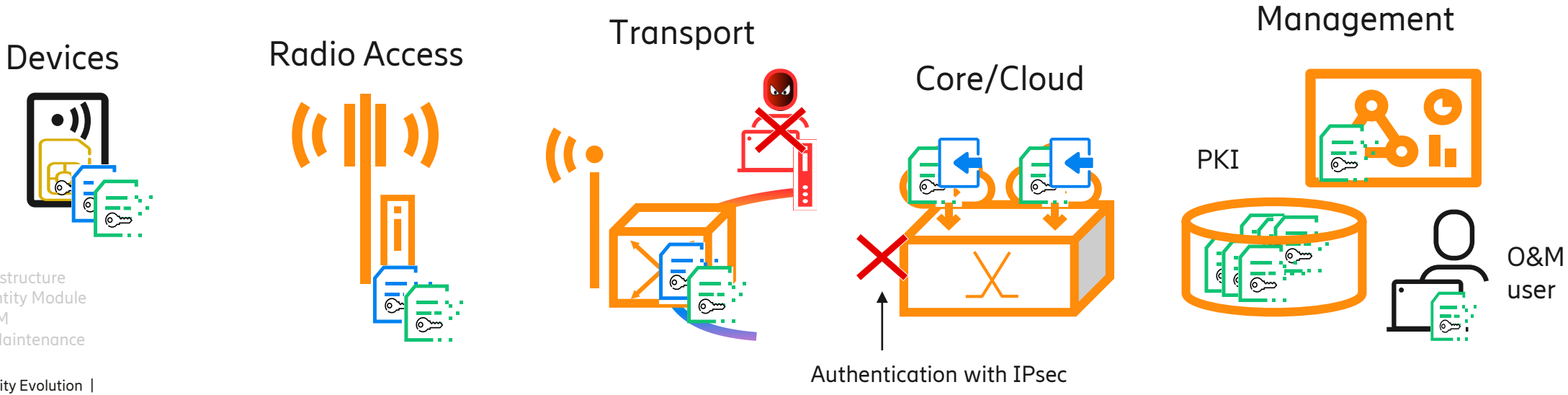


Identity management

- Identity for authentication of nodes
  - Devices
    - Authentication based on SIM or eSIM based on traditional AKA or certificates
  - Nodes
    - Certificates with asymmetric keys
      - Auto Integration
      - IPsec
      - O&M
    - SW nodes uses one-time password

Prevents unauthorized nodes/devices to be connected to the network

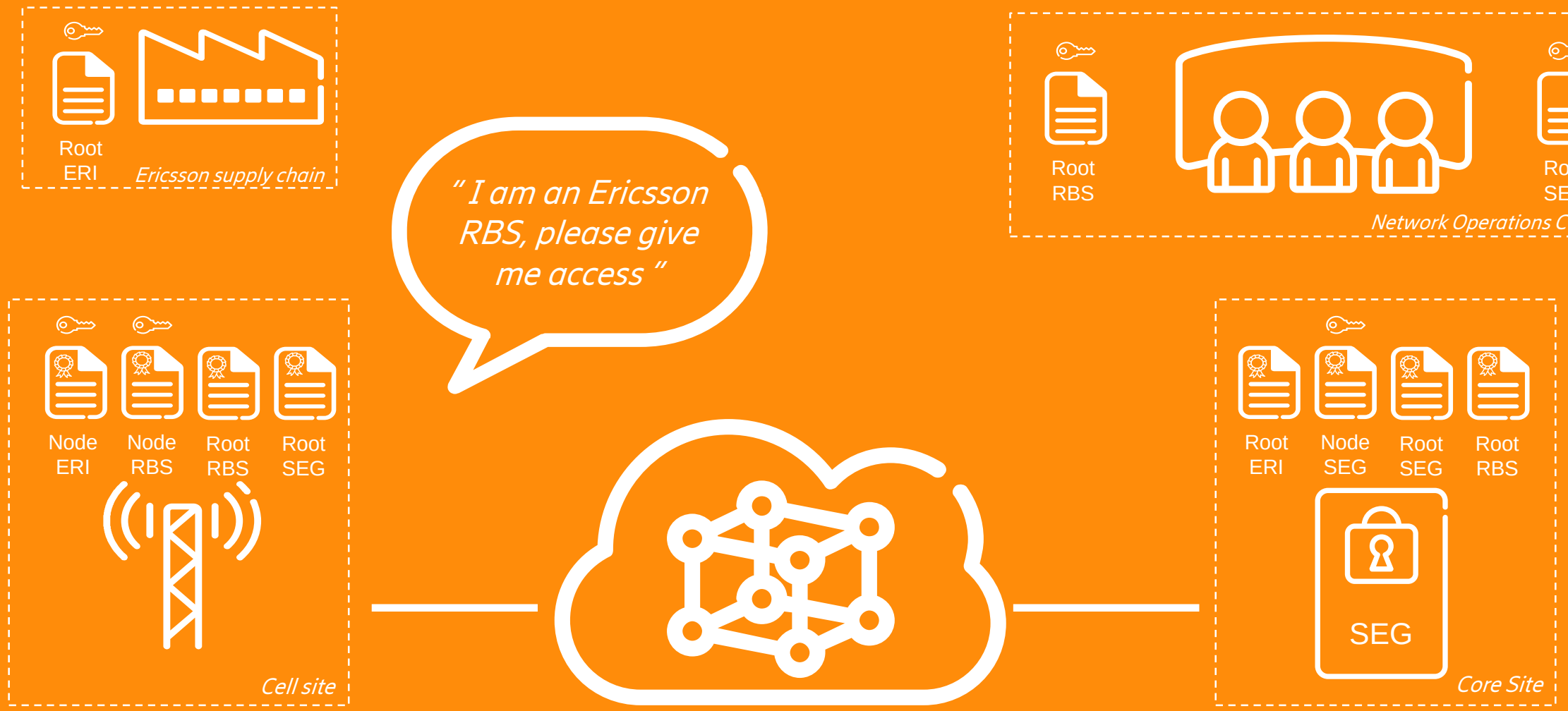




PKI =Public Key Infrastructure
SIM = Subscriber Identity Module
eSIM = embedded SIM
O&M = Operation & Maintenance

Certificate Management

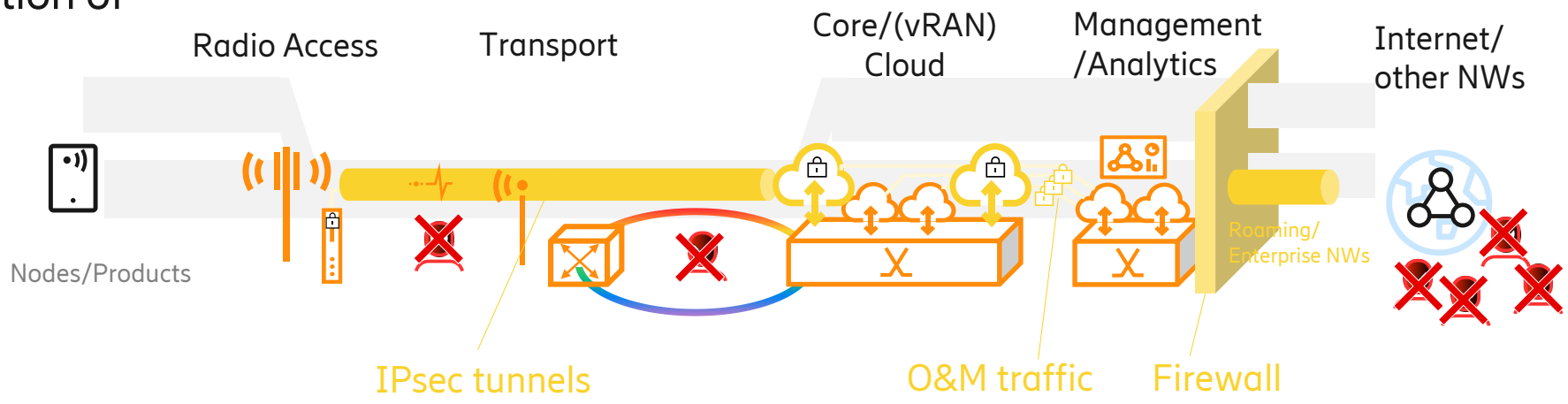
IPsec: Trust relationships



Communication security

- IPsec - authentication, integrity and encryption of user and control traffic (optional)
- Firewalls – allows right type of traffic to enter/exit the NW (optional)
- Secure O&M traffic - authentication, integrity protection and encryption of Management traffic

- Prevents access to gNBs, Core and management systems through the transport NW
- Prevents eavesdropping at gNB and through the transport NW
- Prevents manipulation of traffic along the tunnel
- Protects the network from outside attacks



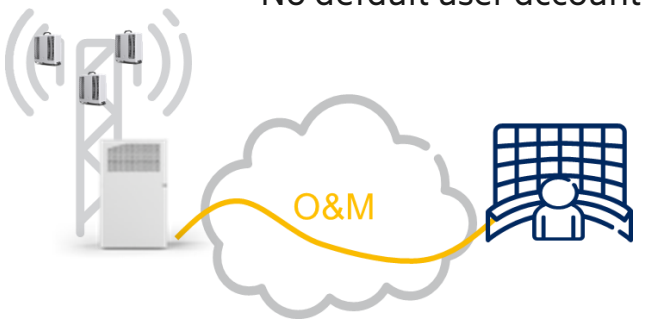
O&M Security

RBS 6000 & Evo Controllers (DU-family, mRBS, RNC/BSC)

- Security level 1 by default
  - FTP/SFTP (File transfer and PM)
  - Corba/IIOP (Configuration Management) wo user authentication
  - Telnet, SSH or seriell interface (terminal connections/commands)
  - Node credentials (same credentials for all users and all nodes)
  - One authorization level for all
- Security level 2
  - Corba/SSLIOP (encryption and integrity added)
- Security level 3
  - SFTP only
  - Corba/SSLIOP
  - SSH or Serial interface

Ericsson Radio System (BB-family, pRBS & mRBS)

- Only secure protocols supported
  - File transfer & PM
    - SFTP only – FTPES in road-map
  - Configuration Management
    - Netconf/TLS
  - Terminal connections/commands
    - CLI/SSH or CLI/TLS
  - User specific password/certificates
  - User specific access rights (LDAPS)
  - No default user account

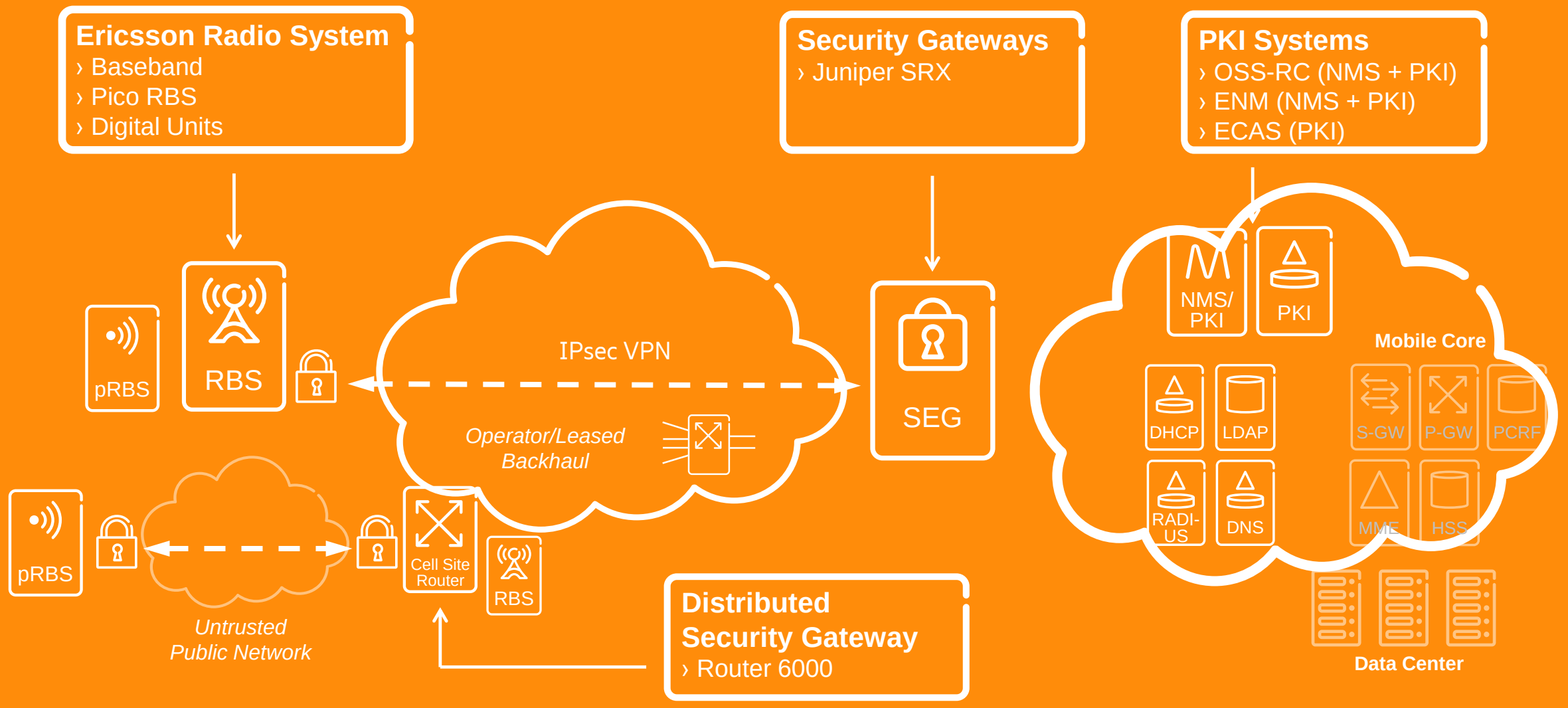


LDAPS - Lightweight Directory Access Protocol over SSL
CLI – Command-Line Interface
CORBA - Common Object Request Broker Architecture
FTP – File Transfer Protocol (unprotected)t
IIOP – Internet InterORB Protocol (unprotected)
PM – Performance Management
SFTP – SSH File Transfer Protocol (protected)
SSH – Secure Shell (protected)
SSL – Secure Sockets Layer
SSLIOP - Internet Inter-ORB Protocol (IIOP) over SSL
TLS - Transport Layer Security

Note: BSC and TCU/SIU supports SFTP, Telnet or SSH, user specific username & password and user specific access rights

RAN Security Solution

Network elements



3GPP Air protection – 5G

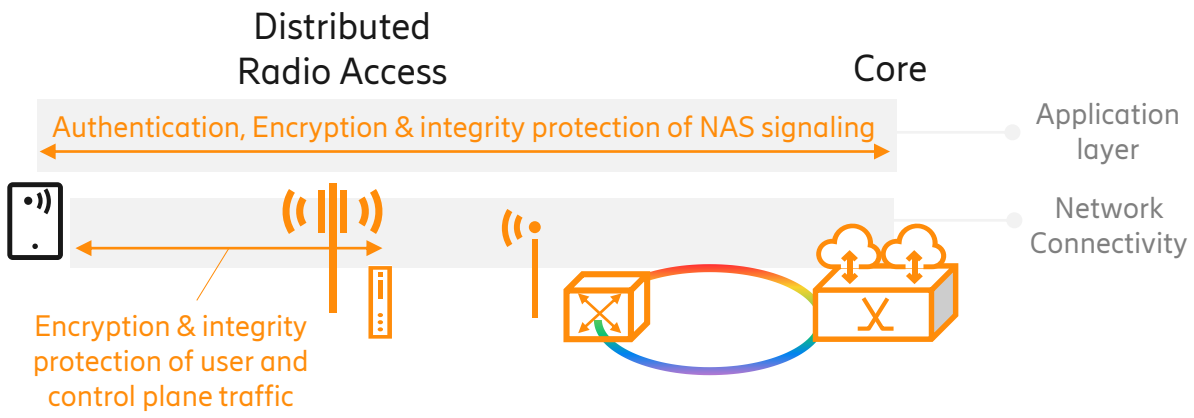
New with 5G

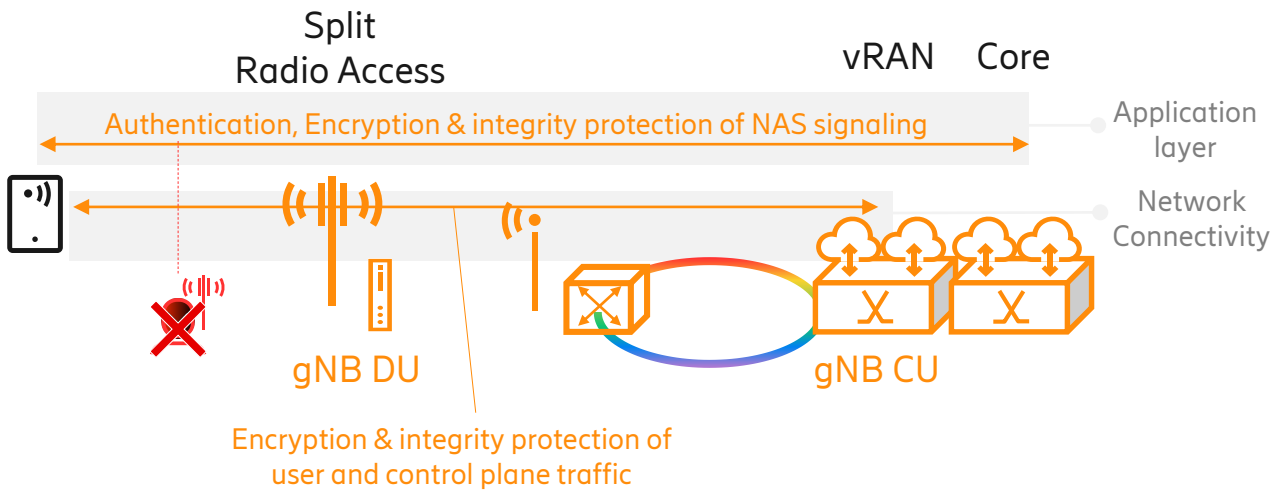
- Integrity protection of UP traffic
- Encryption of IMSI
- Additional smaller enhancements

5G summary

- The air interface is protected by encryption and integrity protection
- Authentication of devices is done by the Core network

- Prevents eavesdropping over the air
- Prevents from manipulation of traffic over the air
- Prevents traceability of subscribers and reduces attack vectors from fake RBSs





Packet Core
DoS and malicious traffic protection

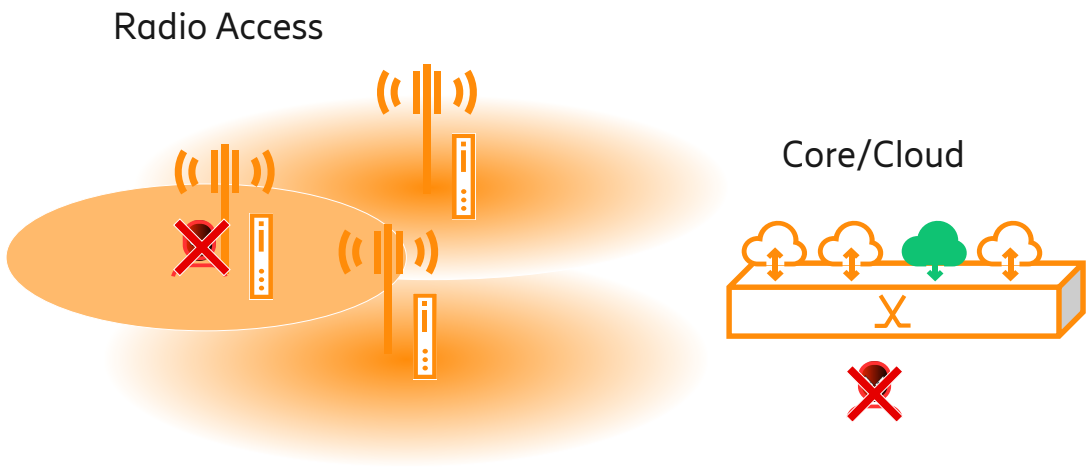
- Denial of Service protection
  - UE signaling control
  - ICMP rate limiting
  - Throttling of bearer requests

- Malicious traffic protection
  - IP, UDP, and TCP short header attacks.
  - Malformed IP header
  - TCP Flags attack
  - TCP SYN Flood attack

Resilience

Example

- Core
  - Physical/geographical node redundancy or resilience of network functions in a cloud
- Transport
  - Physical redundancy, meshed solution, resilience (e.g. BFD, DPD)
- Radio
  - Overlapping radio cells and radio technologies

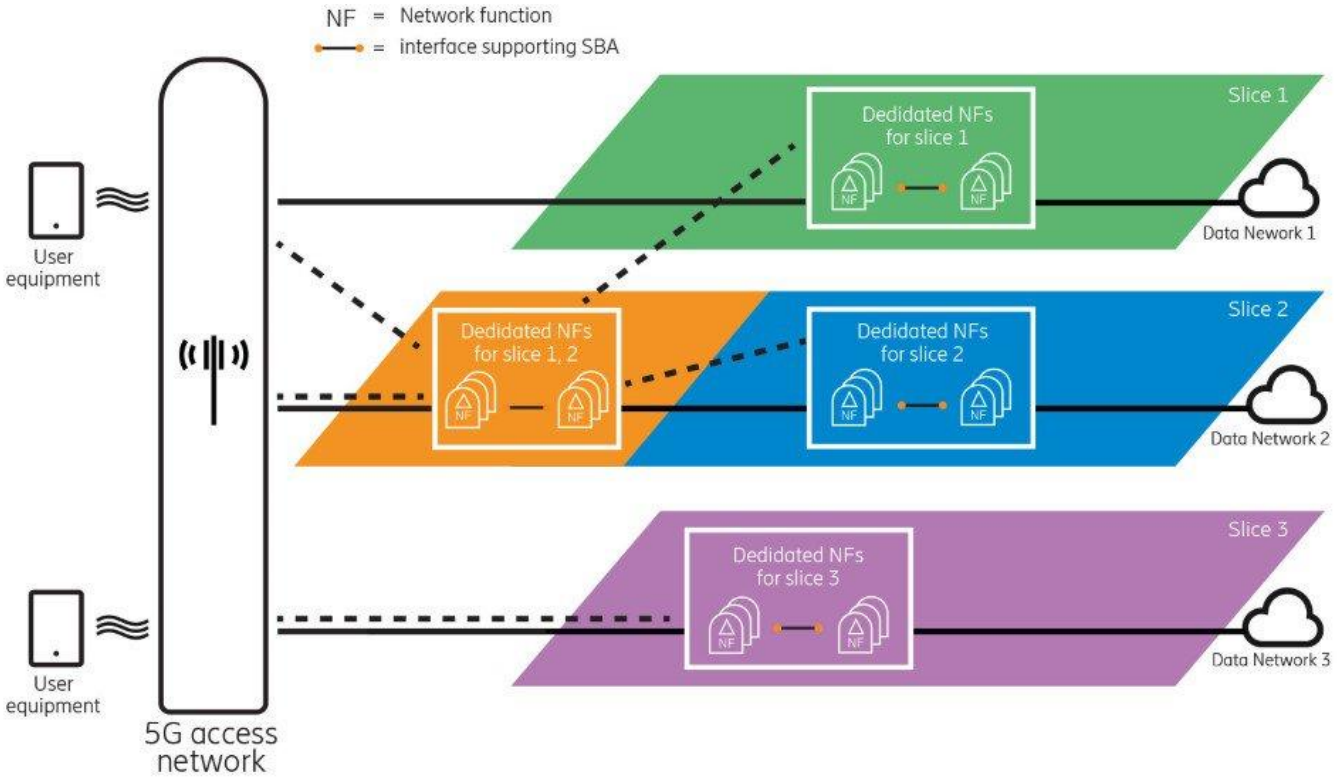


Increased robustness making the network less vulnerable to an attack

5G network slicing

- Separates services/users/devices to belong to a slice of the network
- Logical networks that are customized to meet the needs of each application

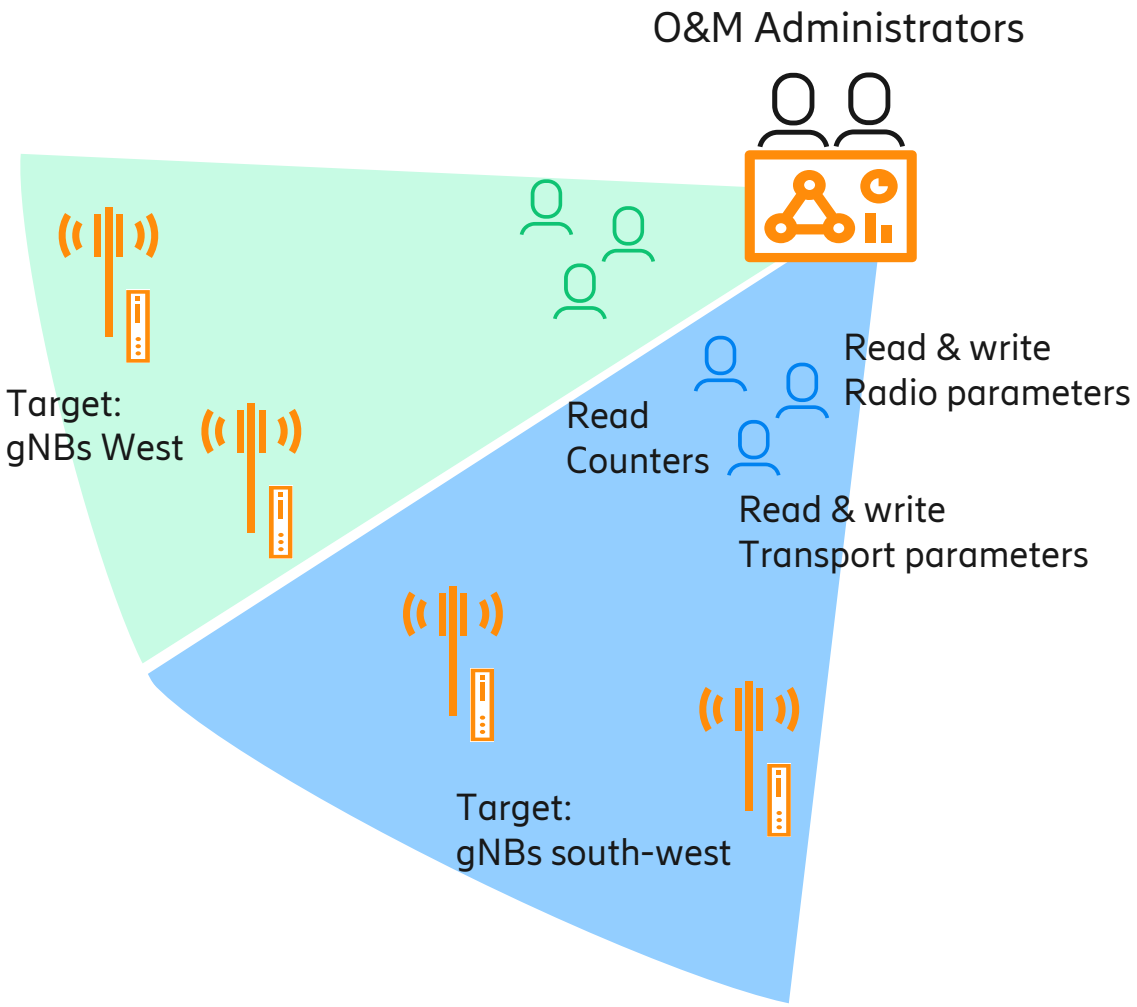
Isolates a potential attack to one slice. Remaining slices are not impacted



Operational security

- Authentication of O&M users
  - Username & password (user specific)
  - Certificate based credentials (user specific)
- Role & Target based access control
  - User specific rights (Pre-defined or tailored)

Isolates the potential harm of an insider attack and provides traces to the user



Security management & orchestration

Sec. Policies

- CIS Benchmark
- ISO 27001
- ISO 27017
- NIST
- Vendor hardening guidelines
- Corporate security instructions
- Other

Ericsson Security Manager

Configuration

- Disable inactive users
- Password change frequency
- Set security zones
- Disable telnet
- Enable logs
- Others

Compliance

- Is default access enabled?
- Are tenants isolated?
- Vulnerabilities patched?
- Others

Analytics

- Events
- Logs
- Notifications
- Subscriber info
- Others

Configuration

FW | IAM
IDS | Other

Assets

GRC

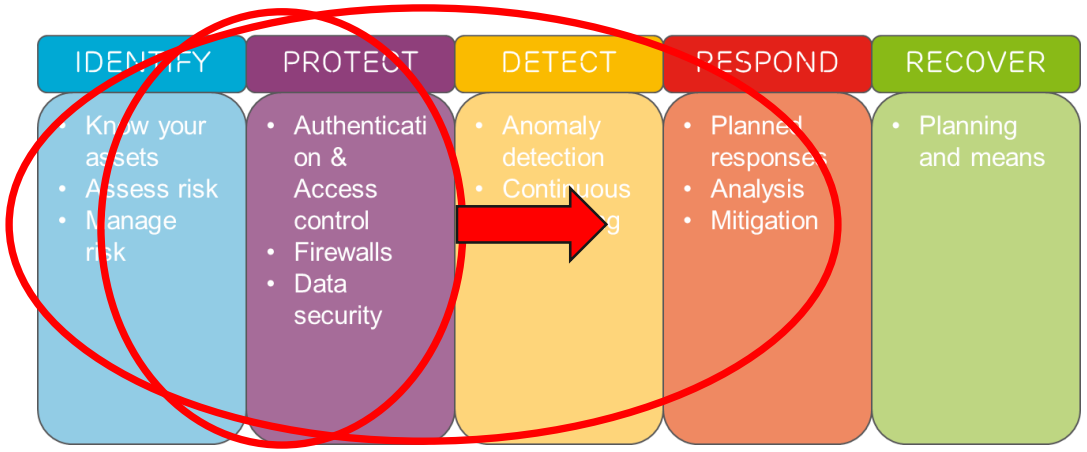
Secured Context

- E2E view & control
- Automatic configuration
- Automatic compliance verification
- Real-time policy breach & unknown threat detection
- Vulnerability mgmt
- Integrity mgmt

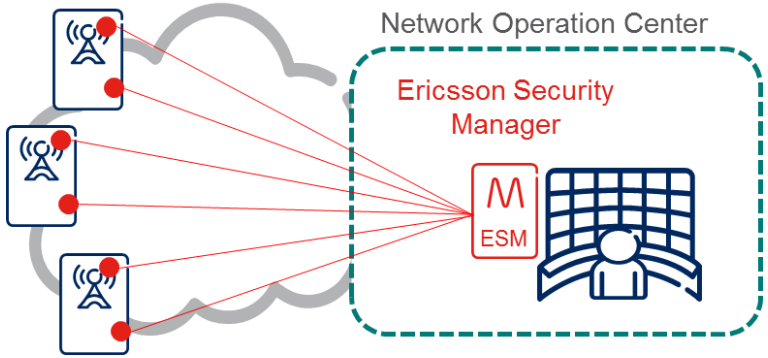
Direction for future RAN enhancements

PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER SECURITY ATTACKS

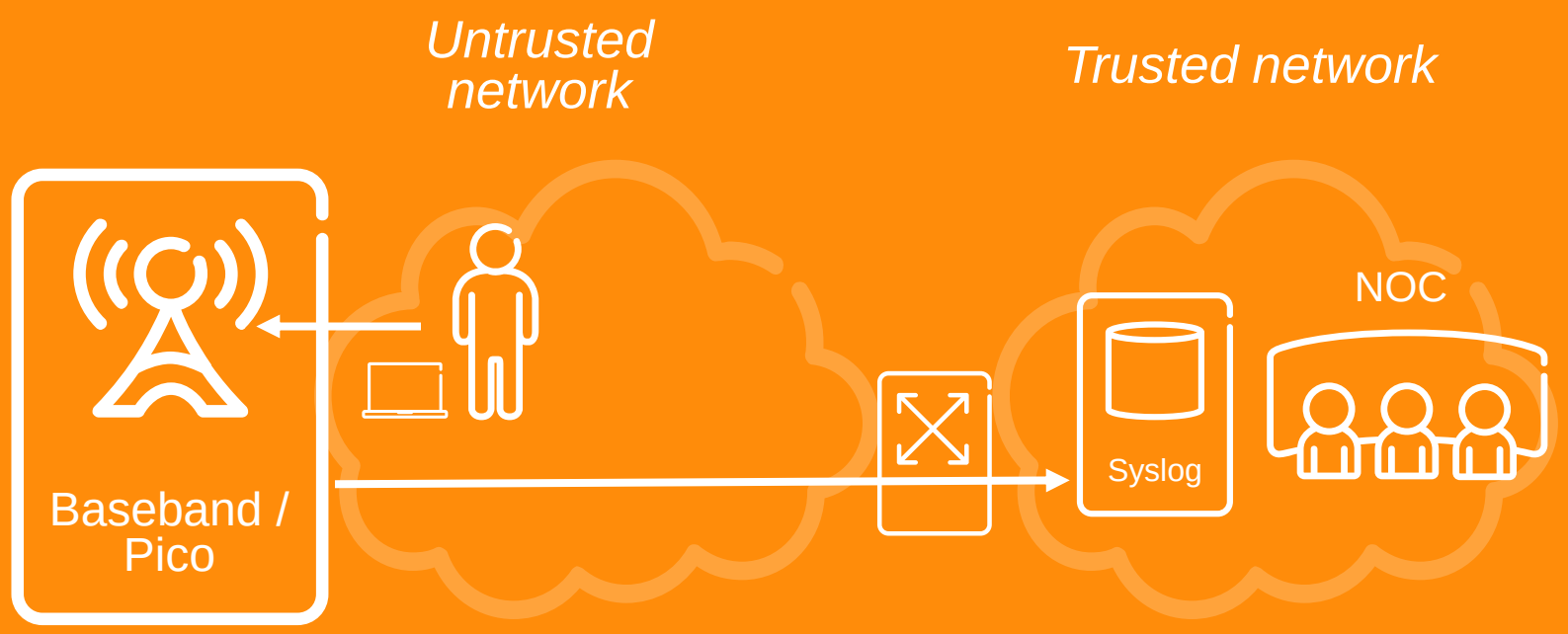
NIST Cybersecurity Framework



- Future development
  - Detection of intrusion
    - Logs (already exist, but may be extended)
    - Events
    - Counters
    - Anomaly in traffic patterns
  - Mitigation
    - tbd



RAN Security
Real-Time Security Event Logging



Cyber Kill Chain VS. RTSEL

- Port scanning, flooding
  - ACL_PACKET_DROPPED (69)
- Brute force / probing remote access
  - USER_LOGIN_FAILURE (2)
  - SECURE_CORBA_SSL_HANDSHAKE_FAILURE (47)
  - SECURE_CORBA_SSL_KEY_FAILURE (48)
  - SECURE_CORBA_SSL_PEER_UNVERIFIED_FAILURE (49)
  - SECURE_CORBA_PROTOCOL_FAILURE (50)
  - SSH_SERVER_CONNECTION_DROPPED (43)
- Physical / probing local access
  - USER_LOGIN_FAILURE (2)
  - LMT_ETHERNETLINK_ENABLED (67)
  - LMT_SERIALPORT_ENABLED (68)

- Getting access
  - USER_LOGIN_SUCCESS (1)
  - SSH_SERVER_LOGIN (42)
  - CORBA_CONNECTION_OPENED (44)
  - SECURE_CORBA_SESSION_CREATED (46)
- Hacking privileged accounts and node passwords
  - LOCAL_AA_DB_UPDATE* (10, 11)
  - LOCAL_AA_DB_FAULT_INFO (63)
  - USER_DEF_PROFILES_UPDATE* (14, 15)
  - VALIDATION_DB_UPDATED (16)
  - NODE_PASSWORD_FILE_MISSING (25)
  - NODE_PASSWORD_CHANGED (26)
  - NODE_PASSWORD_CHANGE_FAILURE (27)

- Degrading node security posture
  - NODE_SECURITY_DEACTIVATED (24)
  - SECURITY_LEVEL_*_* (5, 6)
  - NODE_RESTART (34)
- Poking around
  - COLI_CMD (28)
  - FILE_ACCESS (29)
  - IDL_ACCESS (30)
  - SQLC_ACCESS (31)
- Modifying configuration DB
  - MANAGED_OBJECT_* (35 – 38)

- Playing with certificates
  - TRUSTED_CERTIFICATE_* (12, 13, 58)
  - CERT*.* (59, 60, 70, 71)
  - CRL_DOWNLOAD_FAILURE (61)
  - CRL_LOCAL_STORAGE_CLEANUP (62)
- Compromising IPsec – moving to other nodes
  - IPSEC_TRUSTED_CERTIFICATE_FAULT_INFO (64)
  - IPSEC_PEER_CERTIFICATE_FAULT_INFO (65)
  - IPSEC_CERT_VALID_WO_REVOCATION_CHECK (66)

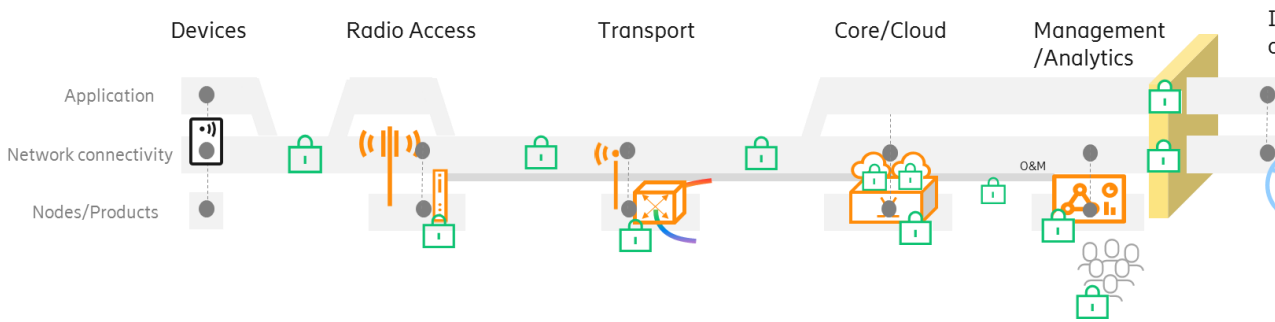
- Change AA servers
  - AA_SERVER_* (7 – 9)
- Looting data
  - SFTP_CLIENT_* (39 – 41)
- Setting scripts
  - DCG_SIGN_VALIDATION_FAILURE (70)

- Manipulating logs
  - REAL_TIME_SECURITY_EVENTS_LOST (55)
  - REAL_TIME_SECURITY_EVENTS_ACTIVATED (56)
  - NTP_SET_CLOCK (32)
  - NTP_CONFIGURATION_CHANGED (33)

Recon Enumeration → Foothold Initial compromise → Exploitation Privilege escalation → Pivoting Lateral → Persistence Exfiltration → Erasing trails Wrecking havoc

Conclusion

- Increased focus on security in 5G due to
  - Evolving threat landscape
  - Critical infrastructure that will carry massive amount of devices
  - Network evolution (Cloud/containers/ONAP/several actors etc)



- Security needed on all levels – Defense in depth
  - Nodes/products with inbuilt defense, without exploitable vulnerabilities
  - Sound security architecture, protecting traffic in transit and providing perimeter protection
  - Appropriate procedures for handling secure operations and act quickly on an incident
  - Business decisions to accept residual risks and manage unacceptable risks