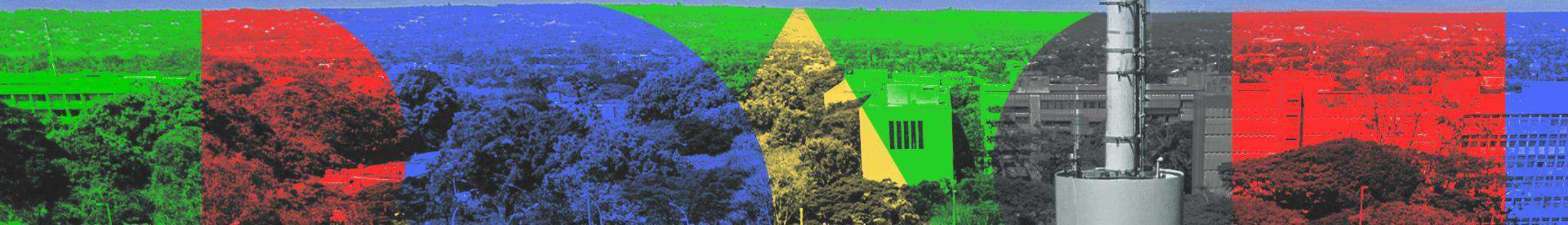
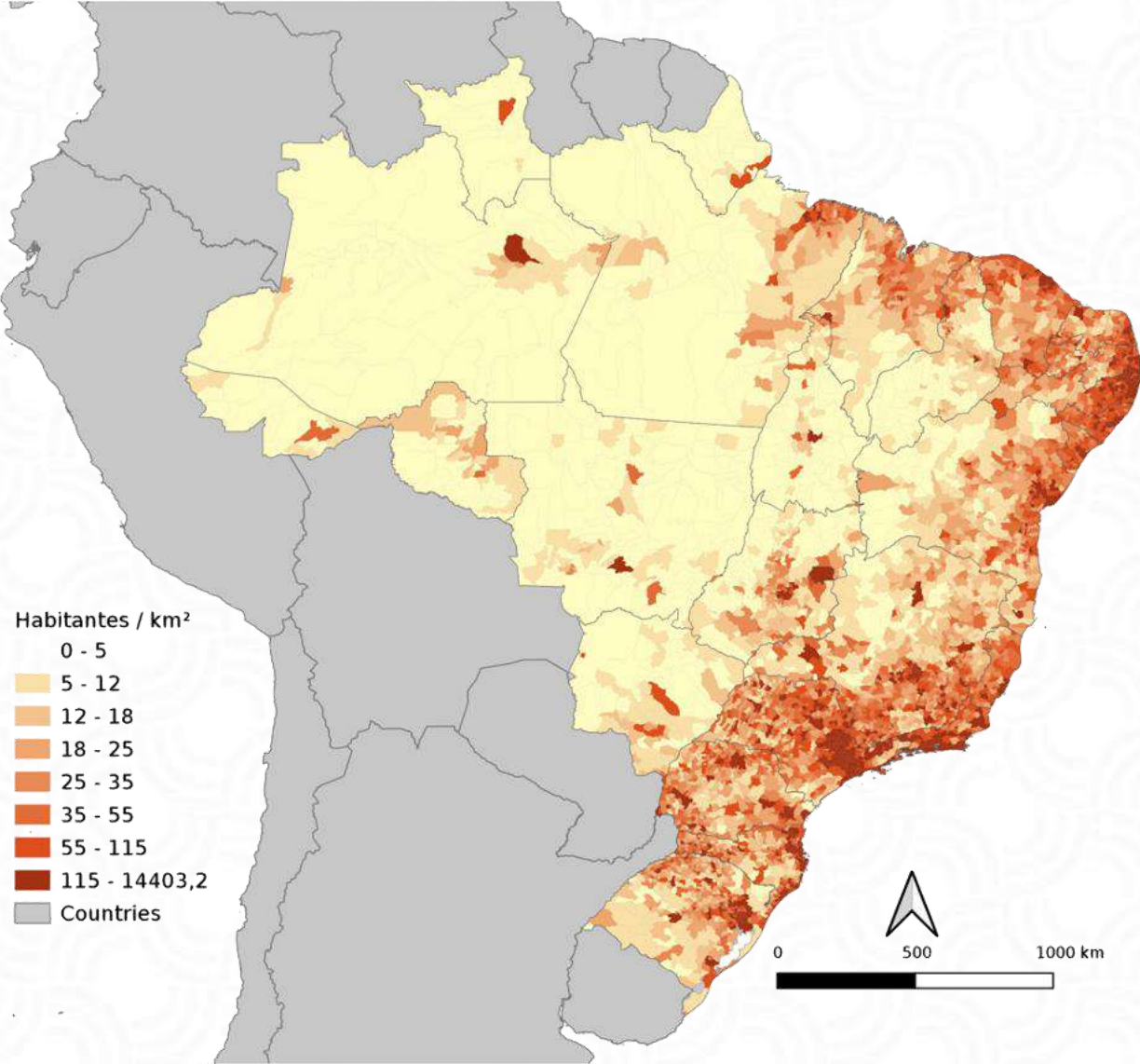


MCOM 



Brazil Factsheet



Population: 210 million

Area: 8,5 million km²

GDP: \$4 trillion USD (PPP; 2022)



Brazil Compared



Population: 50% of South America

Area: 85% of Europe

GDP: 50% of South America



Telecom in Brazil

Fixed Broadband Accesses

 45,6mi

Density (accesses/100 inhab.)

21,4

Mobile Phone Accesses

 251.1mi

Density (accesses/100 inhab.)

98,7

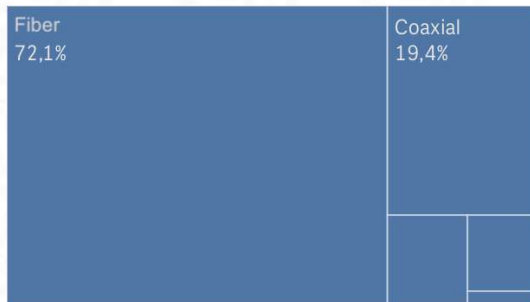
Pay TV Accesses

 13,2mi

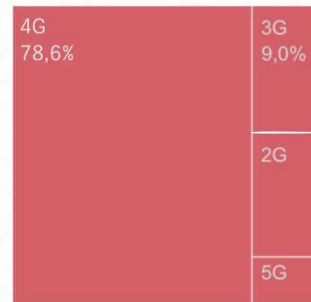
Density (accesses/100 inhab.)

6,2

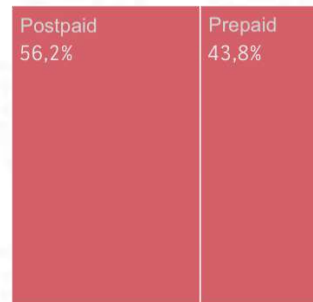
Fixed Broadband Technology



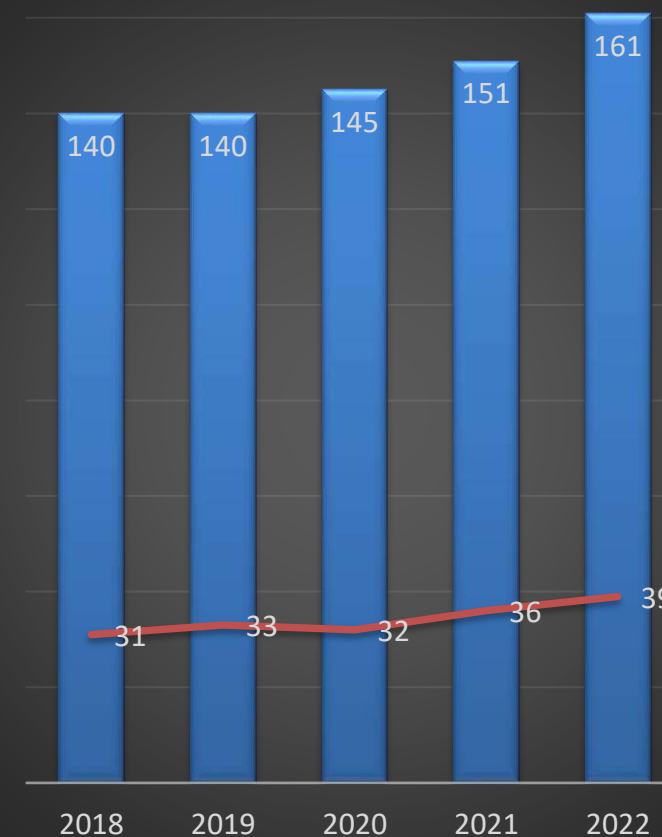
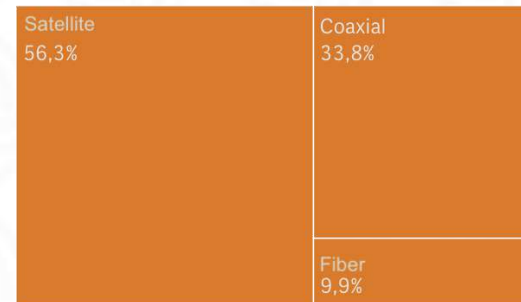
Mobile Phone Technology



Mobile Phone Billing Mode



Pay TV Technology



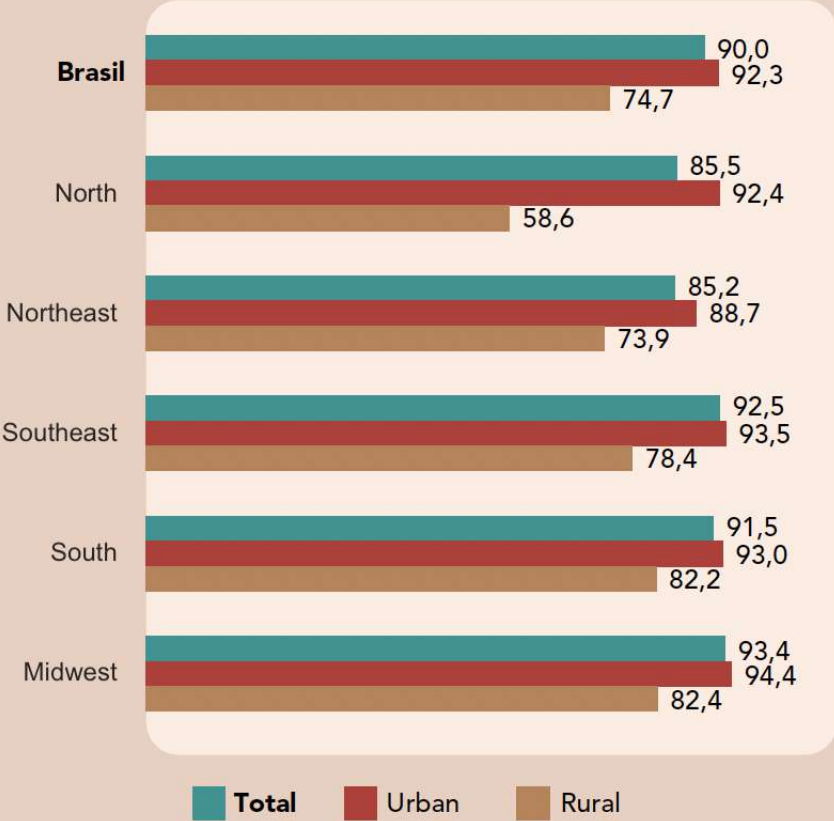
Revenue (R\$ bi) CAPEX (R\$ bi)



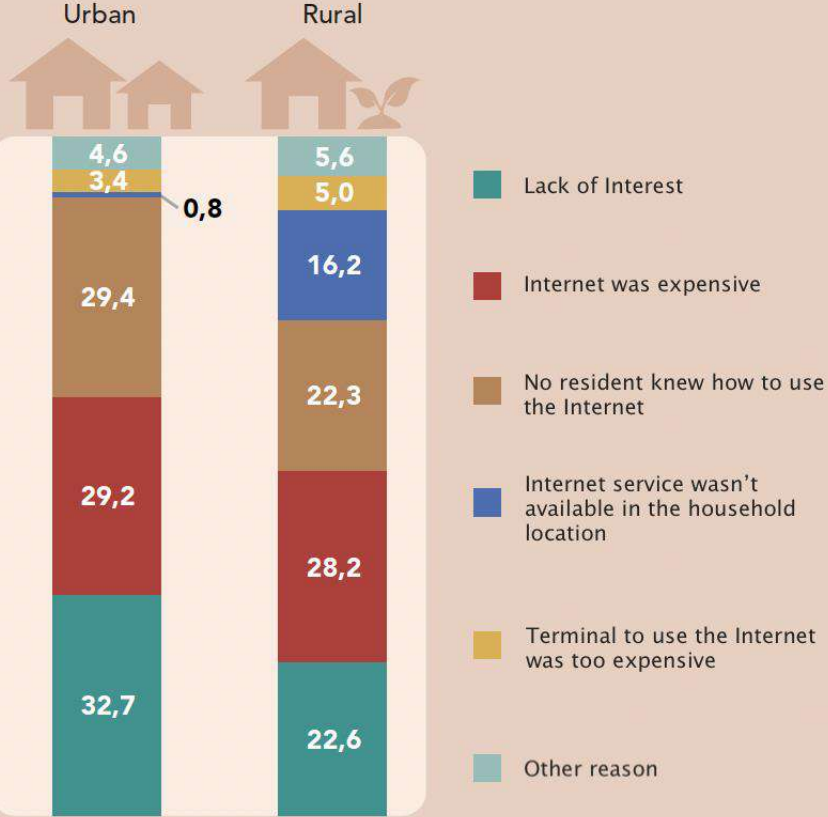
Challenges

Internet Usage by Households

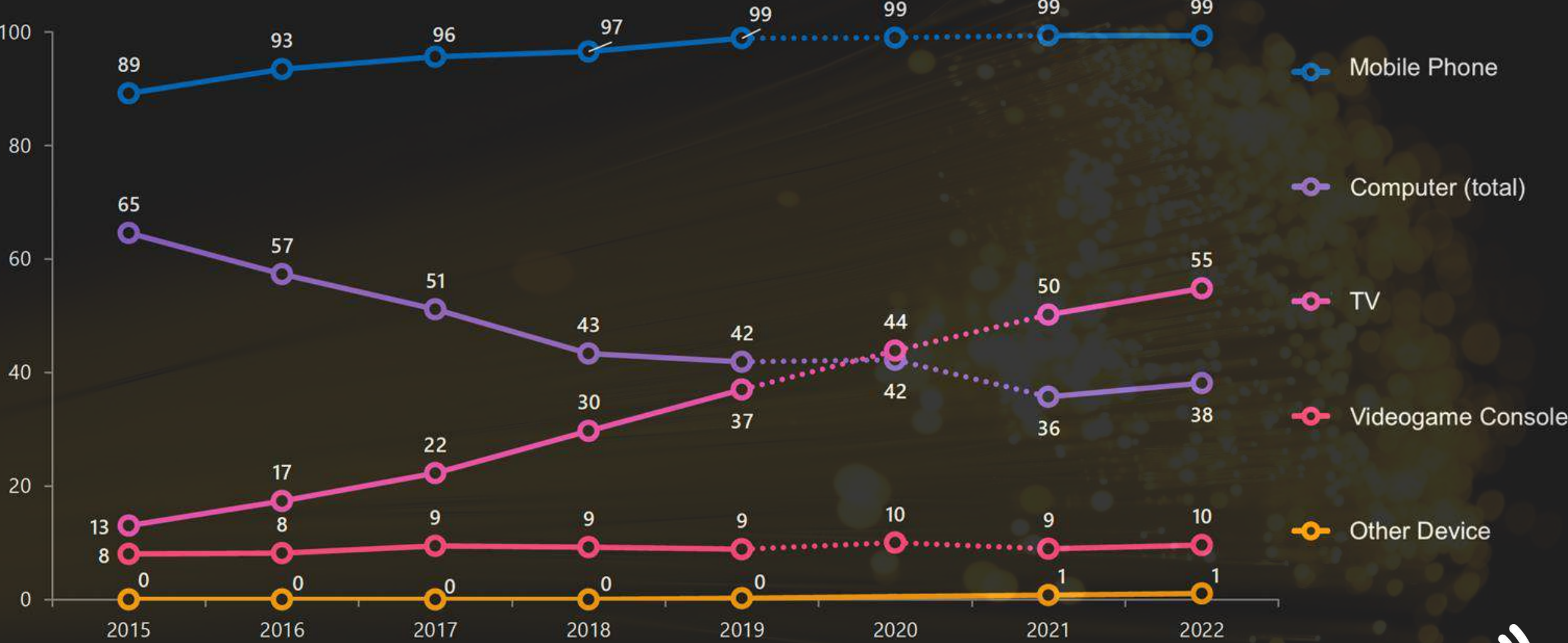
Households with Internet usage (%)



Reasons for not using the Internet (%)



Internet Usage by Device



Health



Meaningful
Connectivity for
58,000 health
units

Education

Meaningful Connectivity for 138,000 schools



A blue background with concentric white circles representing a signal. The text '5G' is centered in white.

5G

in all cities and 1.170 other additional locations

A perspective view of a long, straight road stretching towards the horizon under a cloudy sky.

4G or better in 36.000 km of federal roads and highways

A blue background with white light trails and bokeh effects, suggesting fiber optic technology.

Fiber optics backhaul in 530 cities not covered today

A smartphone is shown on the right, with a world map and various business icons overlaid on the background.

4G or better in 7.430 locations not covered today.



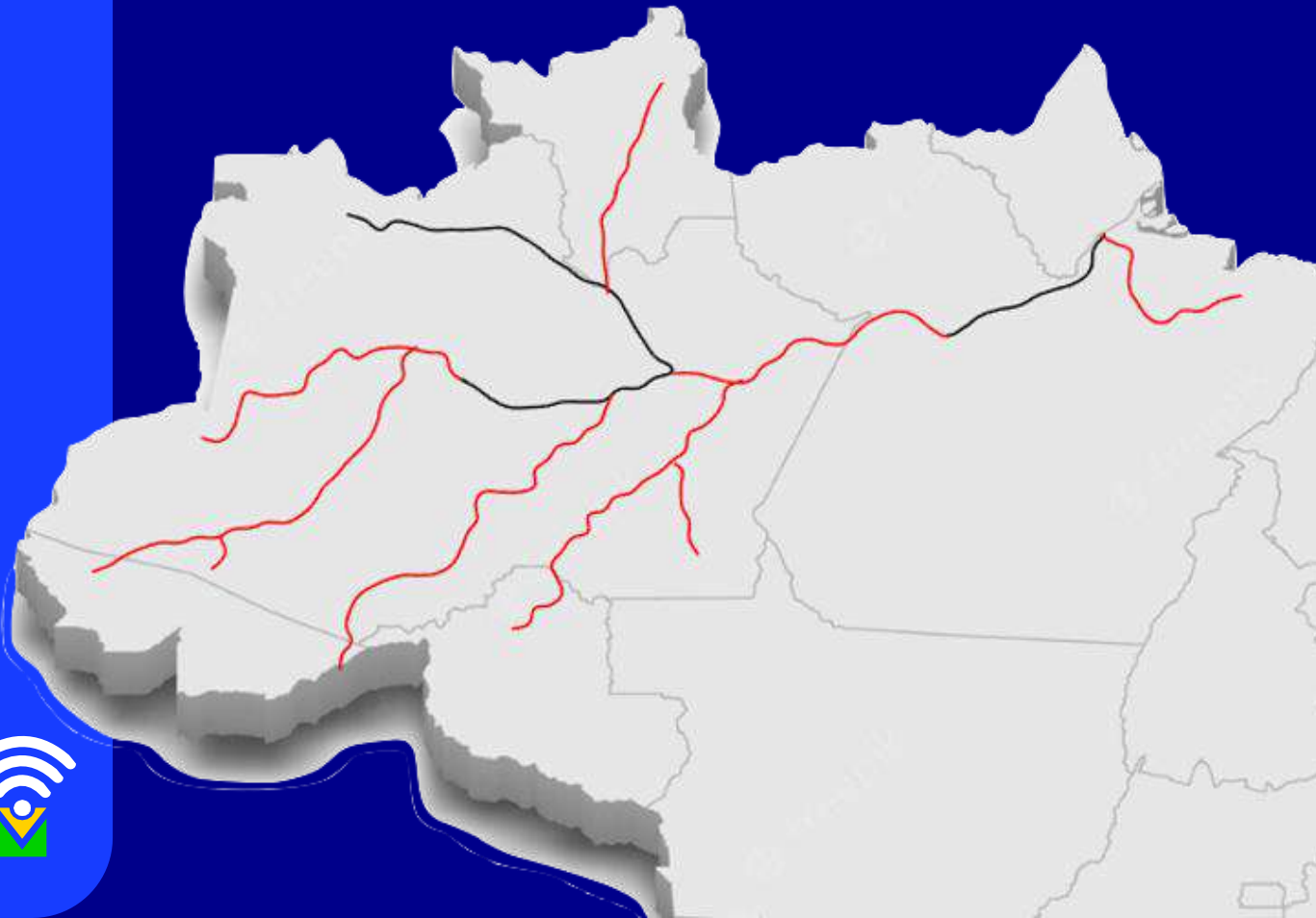
Open RAN

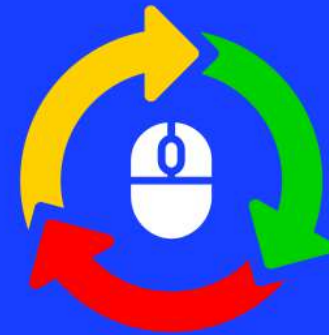


Connected North



12,000 km fiber optics network on the riverbeds of the Amazon forest





**COMPUTADORES
PARA INCLUSÃO**

MCOM 

Final Remarks

Broadband for All
For a better country

Minister Juscelino Filho



MINISTÉRIO DAS
COMUNICAÇÕES

GOVERNO FEDERAL



UNIÃO E RECONSTRUÇÃO

gov.br/**mcom**



mincomunicacoes

Digital Resilience for All

moda

Ning Yeh, Deputy Minister
Ministry of Digital Affairs, Taiwan
@Stockholm, 06/26/2023



Contents

1

Introduction of moda

2

Broadband development



3

Strengthen digital resilience

4

Conclusion



-  Administration for Cyber Security
-  Administration for Digital Industries



Goal

Social
Development

Industrial
Development

Cybersecurity Incident
Response

Application



User

All People and devices in Taiwan

Network



Contents

1

Introduction of moda

2

Broadband development

3

Strengthen digital resilience

4

Conclusion



121%

*Mobile broadband
penetration*

100%

*4G · 5G broadband
usage percentage in phones*

99%

*Mobile broadband
coverage*



5,000 people/dot

Build **fixed broadband network**
in remote areas

Improve **mobile broadband coverage**
rate in remote areas

Enhance **disaster resilience** of digital
infrastructure

Improve communications
in **mountainous areas**



99 Cabin, altitude 2,699M



*Mobile broadband coverage rate
in remote areas*

*Remote areas:
Townships, (Towns, Cities and District) with a population density no more than one-fifth of the average
national population density, or outlying area at least 7.5 km away from the location of the cabinet-level
municipality, county or city government.*

Drive Digital Transformation

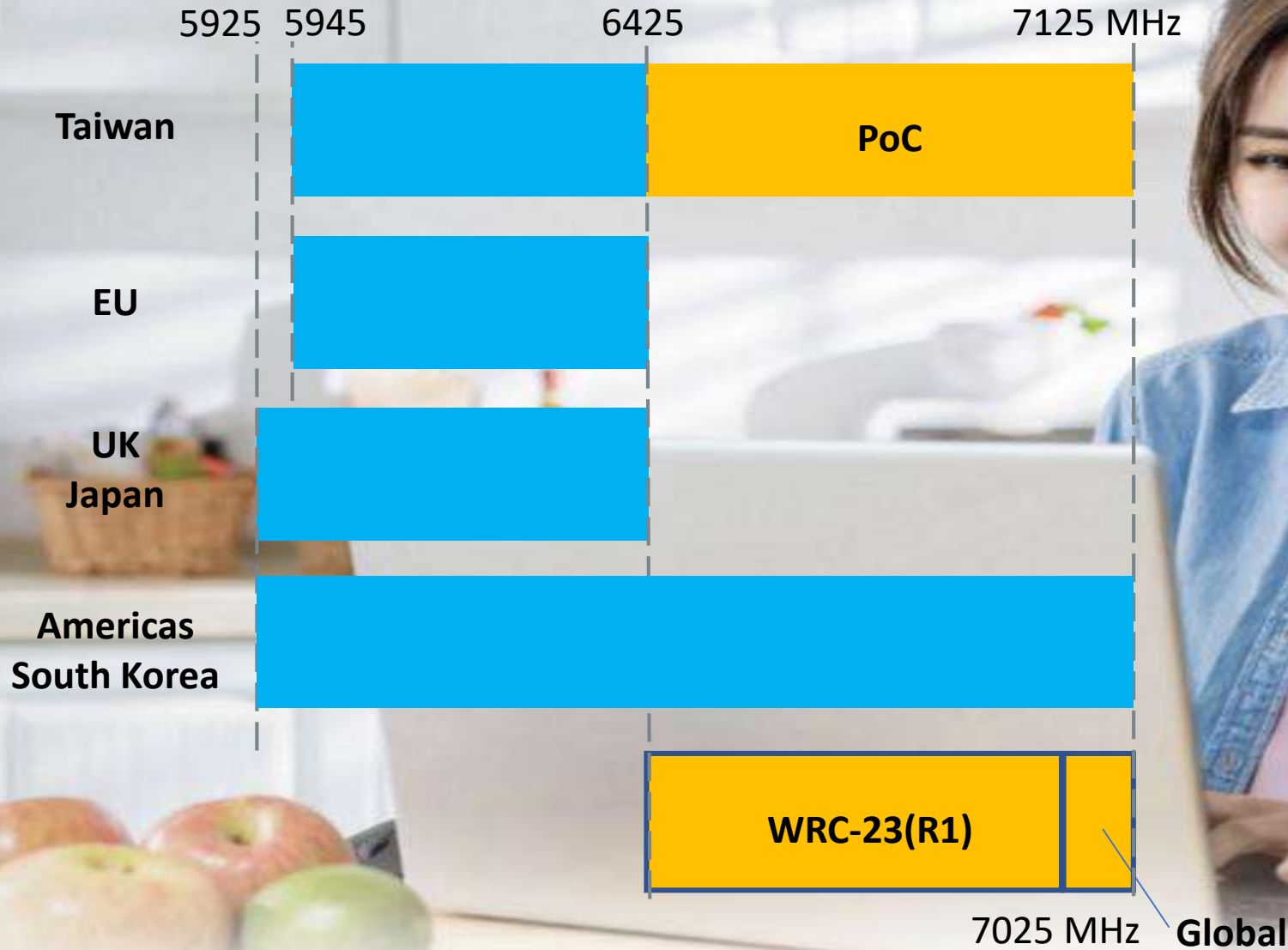
5G private network
4.8-4.9GHz

- Lower cost
- Simplify procedures
- Open up applications





Allocate 5945-6425MHz for Wi-Fi 6E



Contents

1

Introduction of moda

2

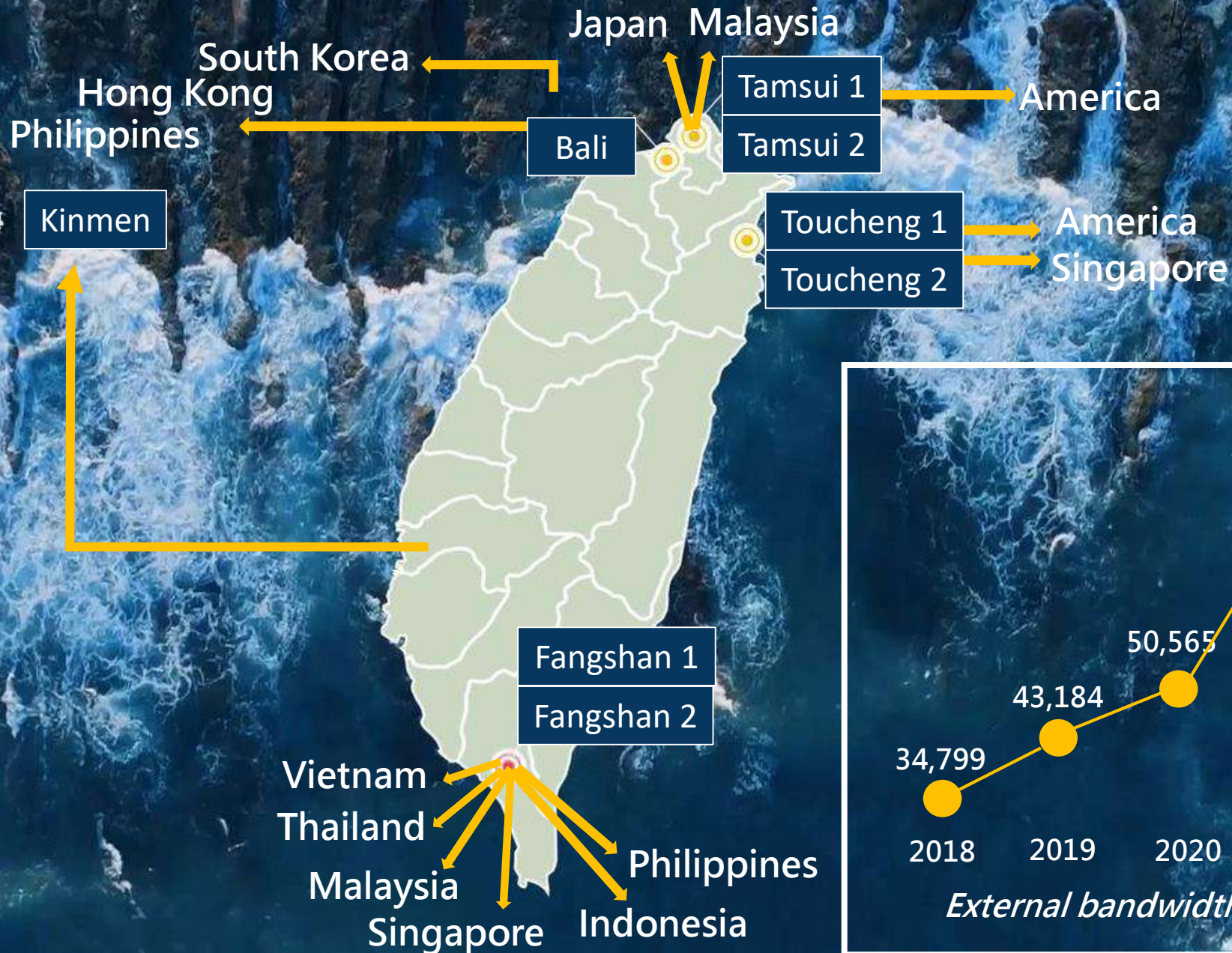
Broadband development

3

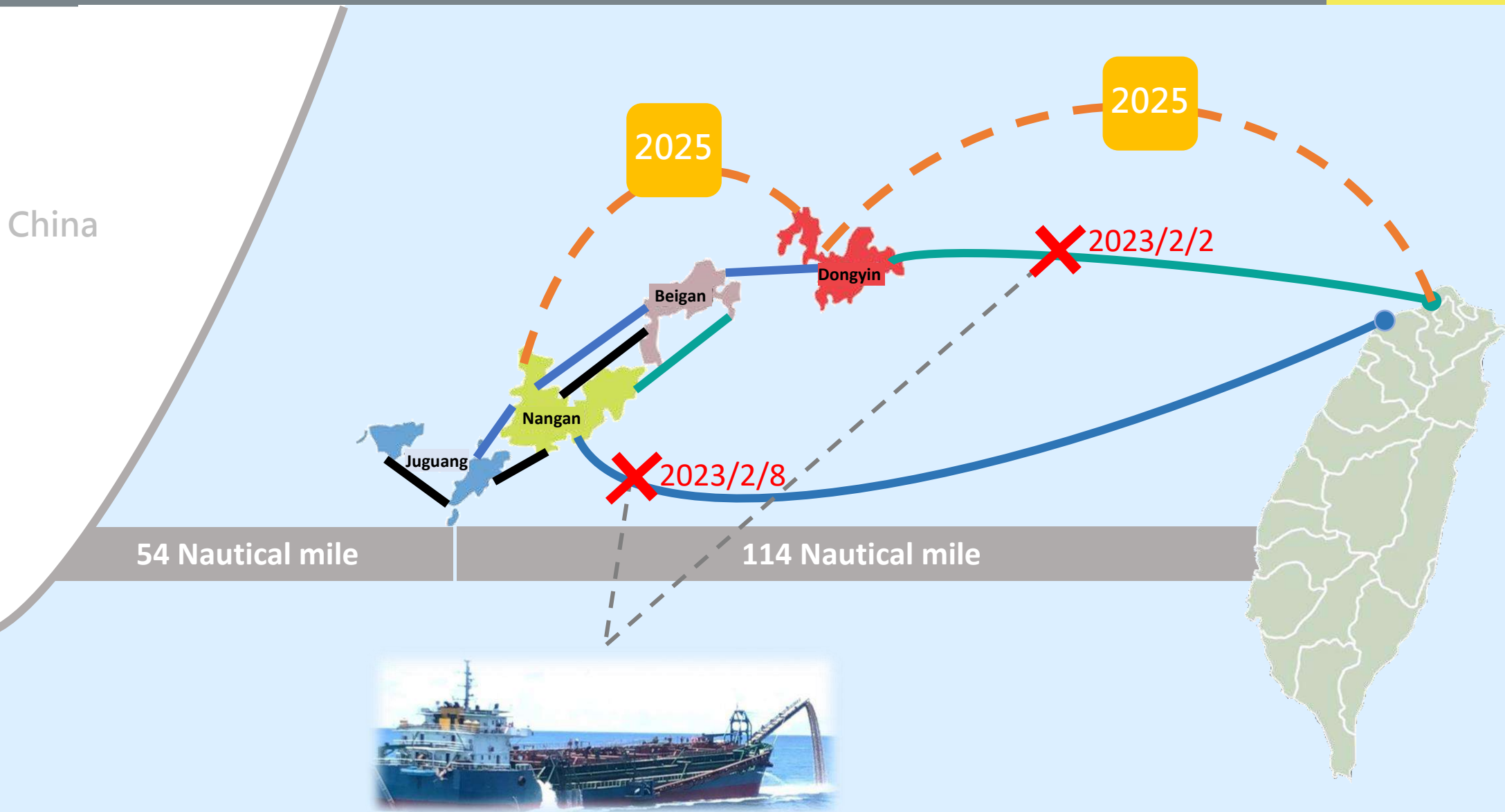
Strengthen digital resilience

4

Conclusion



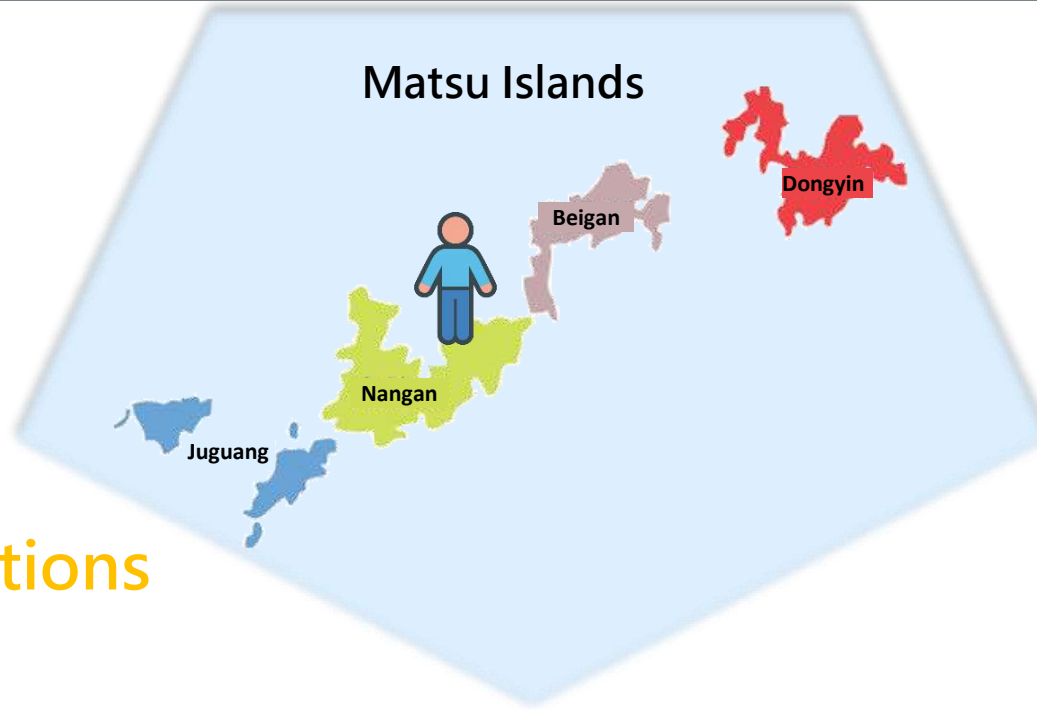
10 Two submarine cables got severed in one week on this Feb 2023



11 Internet disconnection in Matsu islands



 B&B operators deal with online reservations



 E commerce



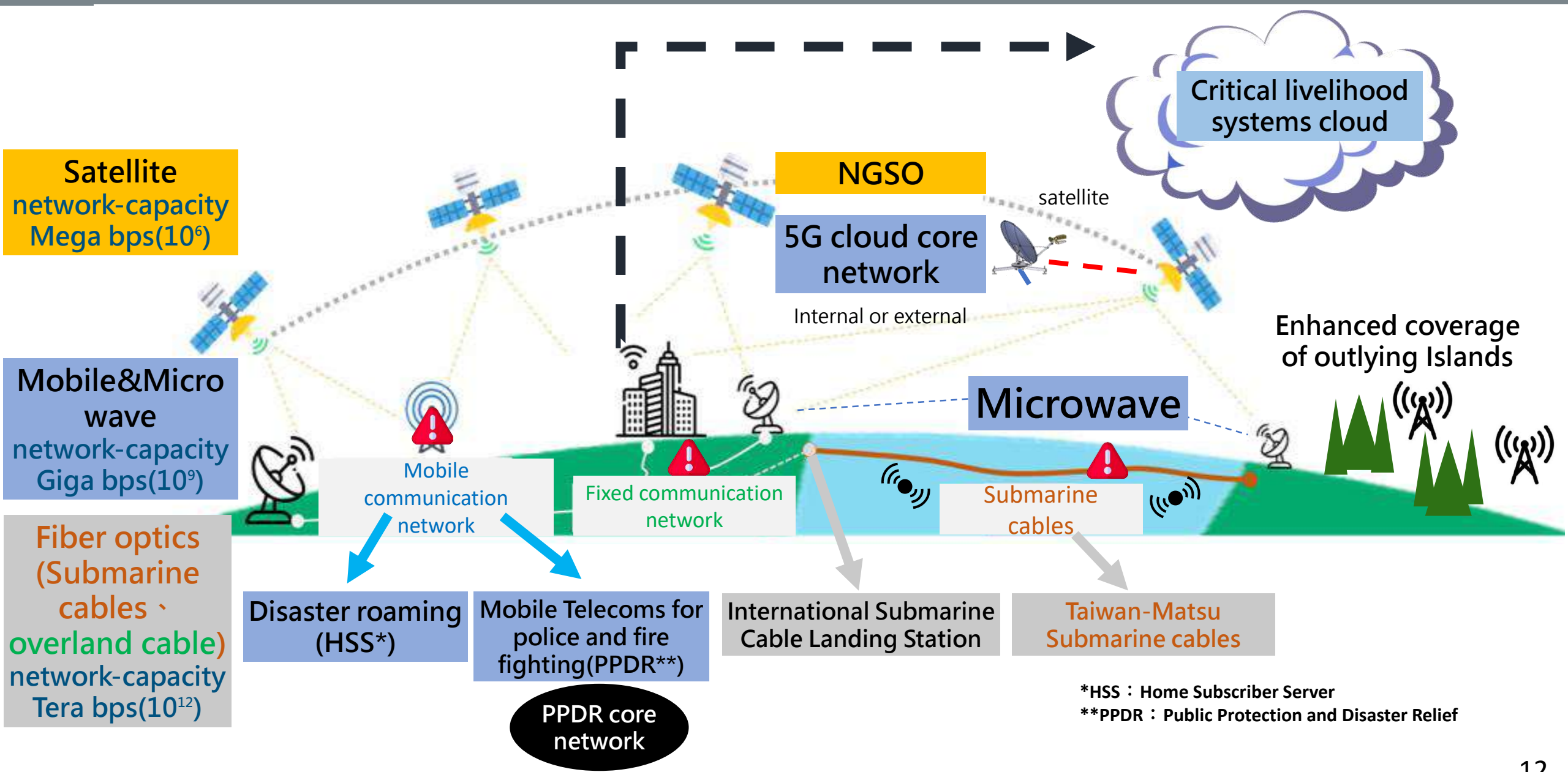
 Social media



 Online Map



 News and Information

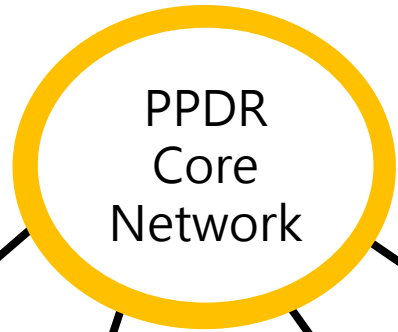


PLAN

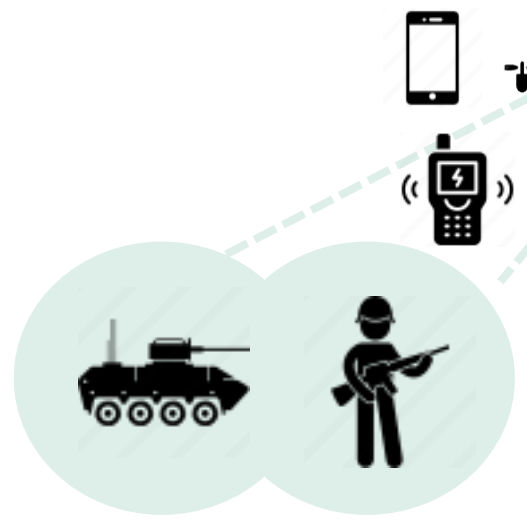
1. At least 700 domestic LEO terminals (hotspot)
2. At least 3 overseas LEO terminals (hotspot)
3. 70 mobile telecommunications base station (Backhaul)



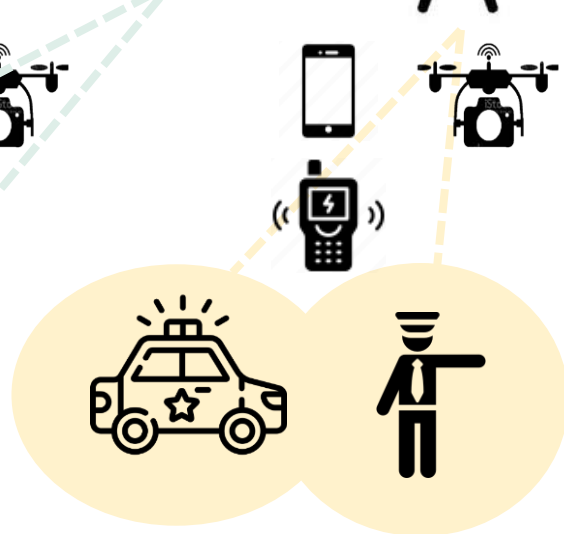
Incidents



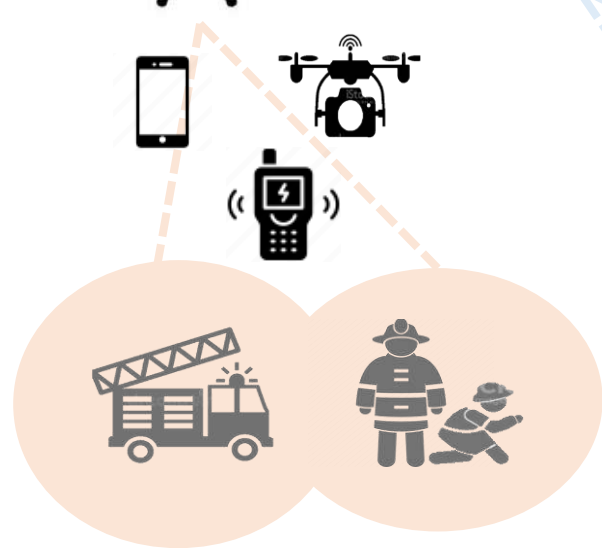
Use drones and other smart devices :
1. Transmit live videos and images
2. Transmit physiological monitoring data



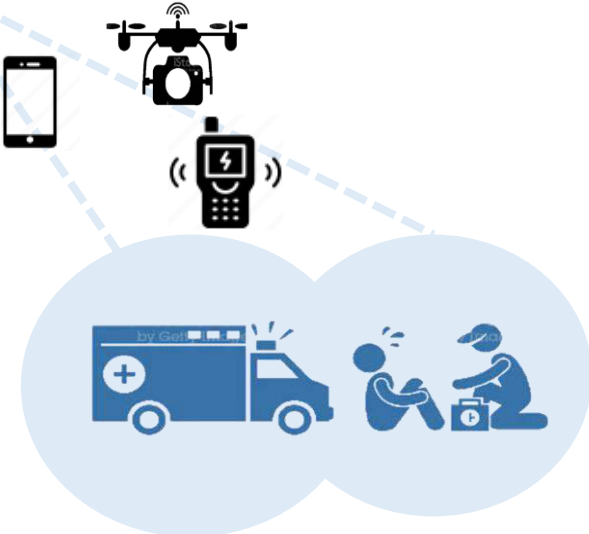
Military



Police

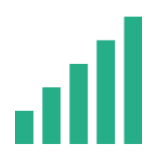


Fire Department



First Aid Unit

Disaster



Users roam between MNO operators

Chunghwa Telecom

Far EasTone Telecom

Taiwan Mobile Telecom



Cyber Security Management Act



Critical Infrastructure:

That refers to asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities, which shall be re-examined and promulgated by the competent authority regularly

Contents

1

Introduction of moda

2

Broadband development

3

Strengthen digital resilience

4

Conclusion

Building an accessible, universal digital infrastructure

Utilizing the digital environment to assist various industries

Building multiple heterogeneous network to provide alternatives

Thank you for your listening

m o d a

數位發展部

Ministry of Digital Affairs



Broadband for All

Eric Dagenais, Senior Assistant

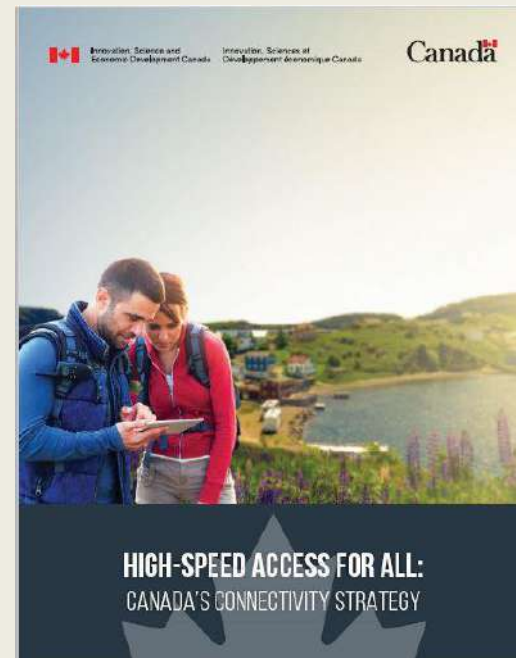
Deputy Minister, Spectrum and

Telecommunications Sector

(June 2023)

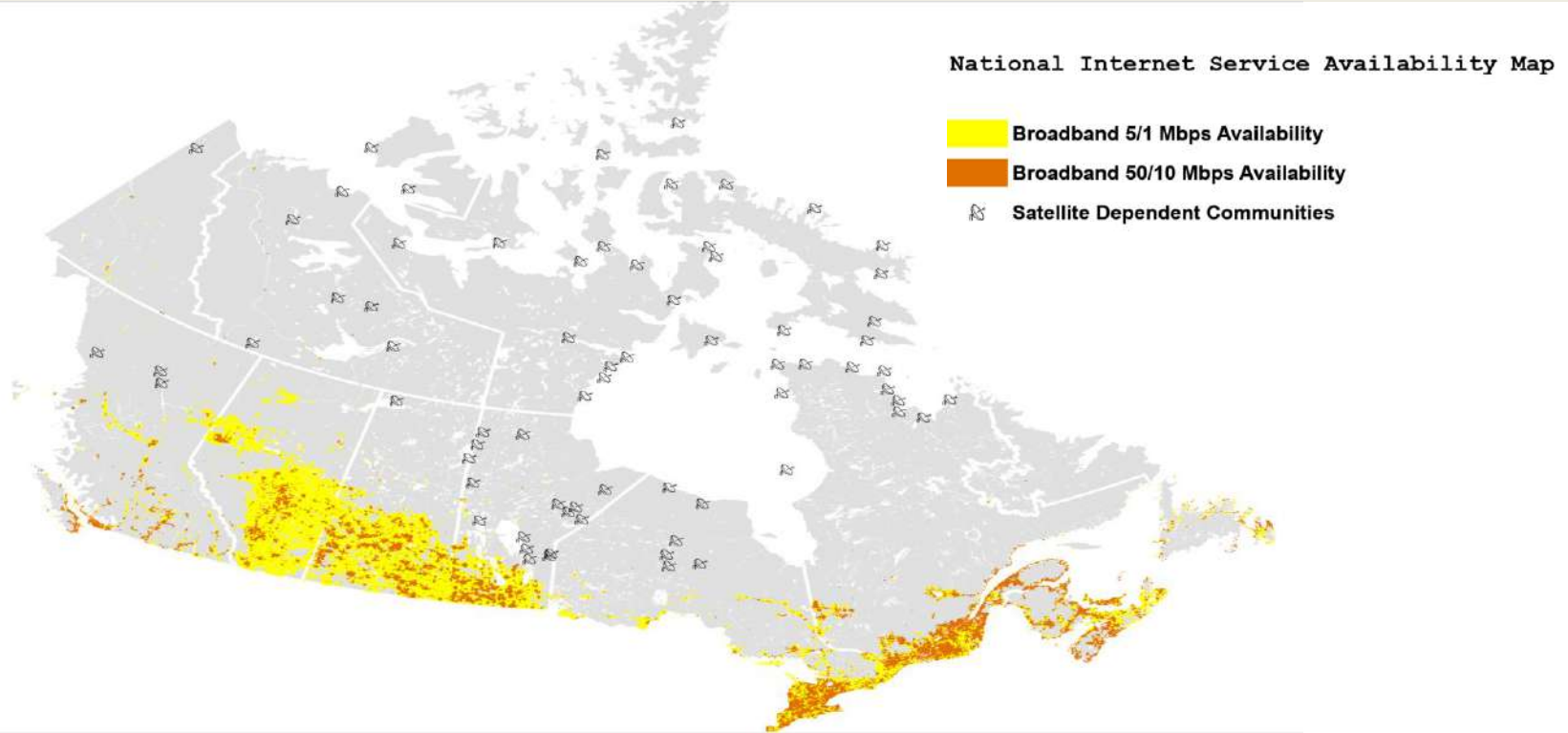
Canada's Connectivity Strategy

- **Canada's Connectivity Strategy**, released in 2019, sets the policy frame and aims to connect every Canadian to high-speed Internet no matter where they live, and to improve mobile cellular access from coast to coast.
- This Strategy includes a universal target of a minimum of **50/10 Mbps (download/upload) by 2030** and expanded mobile wireless.



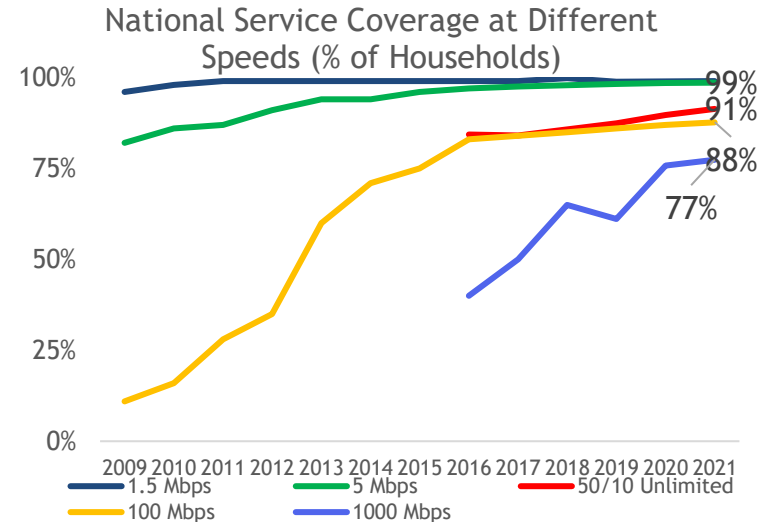
Canada is a large country

- A mix of technologies is required to meet our 100% connectivity goal

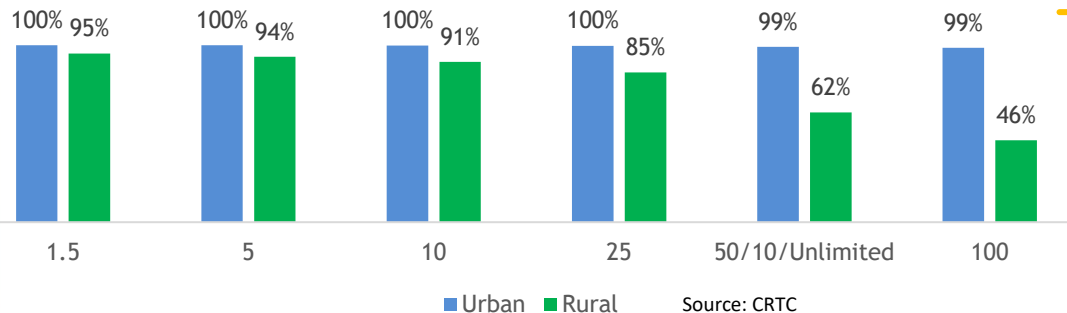


Broadband coverage is strong nationally, but substantial rural gap

- The private sector invests heavily where it is economic to do so, but areas with a lack of business case are underserved
- Some further progress outside urban areas but in general there is a pronounced divide



Download Speed Availability, Urban vs Rural (% of Homes), 2021



Source: CRTC

Source: CRTC

Broadband Programs

- **Universal Broadband Fund (UBF)**
 - \$3.225 billion for high-speed Internet access and mobile expansion
- **Low Earth Orbit (LEO) technology will play an important role in connecting the hardest to reach homes in Canada.**
 - The government has invested \$1.44B in Canadian company Telesat's LEO project, Telesat Lightspeed.
- The CRTC and the Canadian Infrastructure Bank are also making close to \$4B available to ISPs in loans and grants.

Progress to Date

Where we started

- There are **15.4M** households in Canada.
- In Jan. 2021, **1.54M** households were without 50/10 Mbps.

Year	Target	Actual/Projected	Status
2021	90%	91.6%	EXCEEDED
2026	98%	98.7%	ON TRACK
2030	100%	100%	ON TRACK

What we've accomplished

- As of March 2023, **517K** underserved households now have service, another **750K** will be serviced from approved projects, and only **200K households** remain.
- The \$2.6B approved under the UBF has leveraged over \$5B from P/Ts and the private sector.
- Large ISPs (\$1.2B - 185 UBF projects) and smaller players (\$1B - 240 UBF projects) including municipalities and Indigenous groups have each received 50% of the UBF funding to date.



Supply Chain
Disruptions



Indigenous
Connectivity



Satellite-dependent
communities



Inflation



Natural Disasters



Labour Shortages

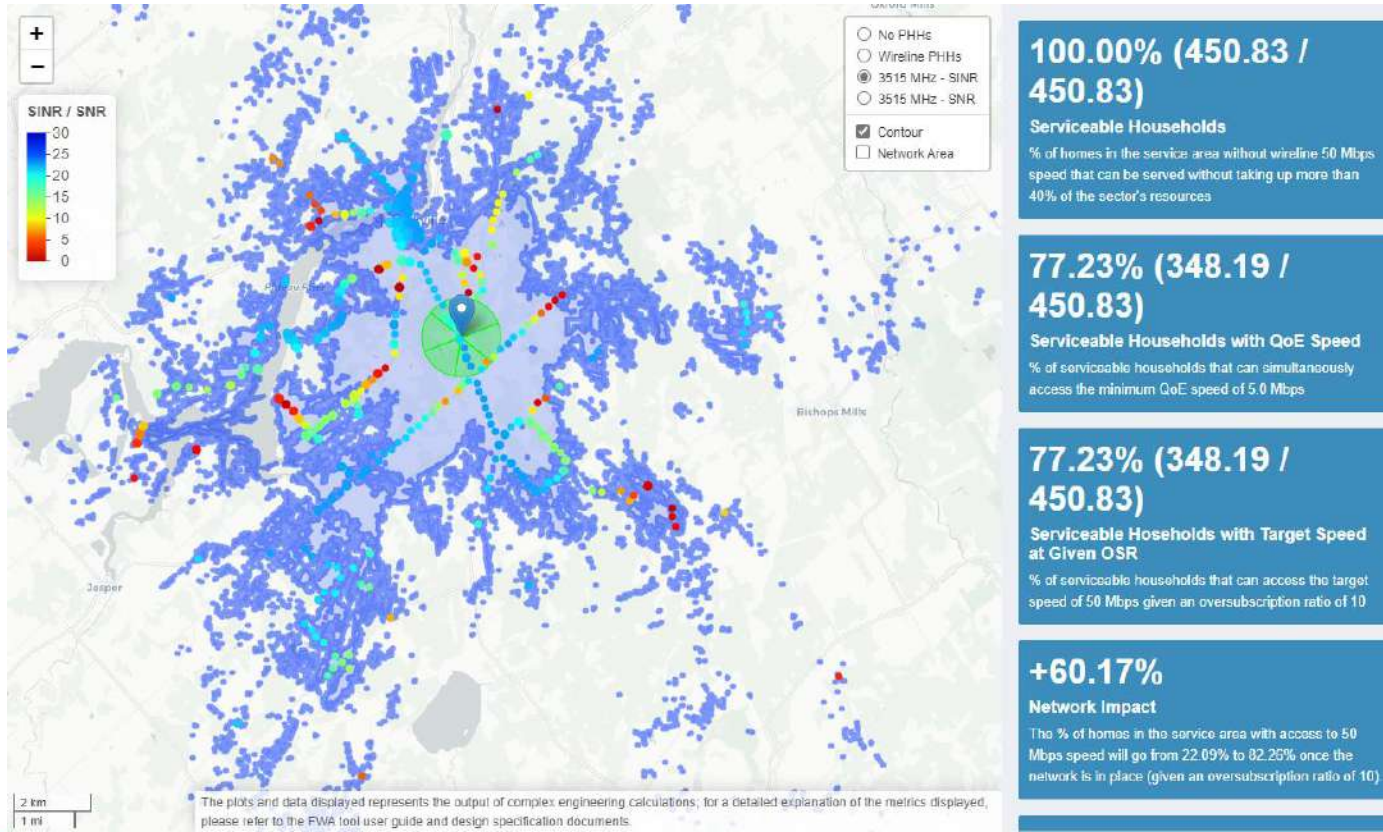
Challenges

Fixed Wireless is Part of the Solution

- 2020 was the first year ISPs reported reaching speeds of 50/10 Mbps but Canadians were not always confirming these reports.
- ISED developed an assessment tool to assess fixed wireless coverage for both UBF applications and the National Broadband Availability Map.
- A variety of technical and environmental factors are used in the assessment: **radio transmission power, radio spectrum, equipment capability, distance from the tower and local demographics.**
- The ratio of available capacity to the number of subscribers (called the ‘oversubscription ratio’) is particularly important - fewer users means better service.
- Given specific parameters, the results of this analysis gives parameters for:
 - The maximum number of customers at 50/10 Mbps that could subscribe per tower.
 - Those towers with sufficient capacity to support all serviceable subscribers at 50/10 Mbps.



Example of Fixed Wireless Assessment Tool Result



Satellite Technology will be Key to Reach 100%

- Innovations in space-based technologies and their service delivery are further enabling broadband access. Canada recently modernized its satellite licensing regime to further encourage innovation; and is considering the implications of the emergence of combined satellite-terrestrial mobile networks
- In Canada, both LEO and GSO satellite networks enable connectivity in rural communities where gaps in traditional broadband infrastructure exist.
- Telesat, SES and Hughes are among the GSO operators providing broadband capacity in Canada to community hubs
- SpaceX and OneWeb LEO networks are now providing high capacity, low latency broadband capacity which can offer good coverage in Canada's North
 - SpaceX's has deployed direct to consumer broadband capacity while OneWeb offers its broadband capacity through a community hub model
- While not yet realized, some Industry analysts note the use of multi-orbit strategies where LEO will provide the global coverage and the low latency, and GSO adds on top of that the ability to bring capacity in higher-density populated places



The Role of Spectrum in achieving Canada's Connectivity Goals

Canada's Spectrum Outlook: 2023-2027

- We recently consulted on our 5-year plan that sets out the key themes that will influence our spectrum decisions:
 - Spectrum as an economic driver and enabler of Industry 4.0
 - Rural connectivity in the wake of COVID-19
 - Indigenous connectivity
 - Competition and wireless affordability
- It also provides our assessment of demand and spectrum needs for various services/applications and our spectrum release plan going forward

Canada's Non-Competitive Local Licensing Framework

- ISED recently published a decision on a non-competitive licensing framework to facilitate simple localised access to shared 5G spectrum
- This framework will offer automated local licences on a first-come, first-served basis to new and smaller users including industry verticals, Indigenous communities, and rural broadband providers
- License areas will be user-defined, with holding and area limits to keep licences from being foreclosed to smaller users
- The automated system is expected to be launched in 2024 for licensing 3900 MHz

Other Canadian initiatives to support connectivity

Spectrum for 5G and rural

- 3800 MHz auction scheduled for October 2023
- mmWave decision later this year, with auction to follow next year

Making more licence-exempt spectrum available

- 6 GHz band / TV whitespace / mmWave band / 5.9 GHz

Improving rural spectrum use

- Increasing use of smaller licence areas and targeted deployment requirements
- Developing a new access licensing regime to license unused spectrum in rural areas
- Stronger Cellular and PCS licence conditions

Canada's Plan to promote secure and resilient networks

Trusted industry-government forums for security and resilience

- ISED has established the [Canadian Security Telecommunications Advisory Committee \(CSTAC\)](#) and the [Canadian Forum for Digital Infrastructure Resilience \(CFDIR\)](#) to advance common priorities and share information.

Declaration on securing Canada's telecommunications system

- [Policy Statement in May 2022](#) announced intention to ban Huawei and ZTE products and services from 4G and 5G networks, subject to consultation

Proposed legislation on cyber security

- [Bill C-26](#) Provides authority to take action to promote the security of telecommunications system and critical cyber systems underpinning the finance, energy, transportation and telecommunications sectors

Resilience goes beyond cyber security

- Networks must be reliable and resilient not just in the face of cyber attacks but also natural disasters and human error that might cause network disruptions.
- In July 2022, an outage at one of Canada's largest telecommunications companies lasted 15 hours and affected millions of subscribers.
- Since then, telecommunications companies have implemented agreements on emergency roaming, mutual assistance, and improving public awareness around telecommunications emergencies and network outages.
- The Government is now examining further recommendations from industry on strengthening resilience.

Broadband for All

Midsummer Conference June 26-27, 2023: Stockholm

Keynote: *Perspectives from India*

by Meenakshi Gupta,

Member, Telecom Regulatory Authority of India

26 June 2023

Significance of 'Broadband for All'

- ❑ In the last two decades, knowledge-driven globalized world has realised telecommunications as a key driver of economic and social development, in which broadband plays a critical role contributing significantly to the digital economy of a country.
- ❑ Broadband, a luxury long ago is one of the essentials for improving the socioeconomic development, job creation, civic engagement, global competitiveness, and a better quality of life – fundamental element of an inclusive and sustainable world under Sustainable Development Goals 2030
- ❑ Demand for high speed and reliable broadband has been growing over the past 5-6 years. Still over 3 billion people remain offline!

Universal Broadband *Manifesto**
“leaving no one behind means leaving no one offline”

10 percentage point increase in fixed-broadband penetration
→ increase in growth of GDP/capita
• 1.21 percentage points (high-income countries)
• 1.38 percentage points (low- and middle-income countries)

World Bank (2009)
120 countries
1980-2006 annual data

One-time effect in the year fixed-broadband was introduced → increase in growth of GDP/capita
• 3.06 per cent
Thereafter 10 per cent increase in fixed-broadband → annual increase in growth of GDP/capita
• 0.01 percentage points

Candelaria (2015)
35 developed and developing countries
1981-2013 annual data

10 per cent increase in fixed-broadband penetration
→ increase in GDP
• 0.8 per cent
10 per cent increase in mobile-broadband penetration
→ increase in GDP
• 1.5 per cent

ITU (2018)
Full sample of 139 developed and developing countries
2010-2017 quarterly data

10 per cent increase in fixed-broadband penetration
→ increase in GDP/capita
• 2.0 to 2.3 per cent
10 per cent increase in mobile-broadband penetration
→ increase in GDP/capita
• 2.5 to 2.8 per cent

ITU (2019)
47 (fixed broadband) and 62 (mobile broadband) LDCs, LLDCs and SIDS
2000-2017 annual data

* The ITU/UNESCO Broadband Commission for Sustainable Development

Telecom Sector in India – Snapshot



Enormous Size

- **Approximately 1.4 billion people; 65% <= 35 years**
- **Country divided in to 22 licence service areas.**
- **Total 1,170 Million connections.**
- **Tele-density around 85**

Internet Penetration

- **Broadband Subs: 846.57 Million; 33.94 M wired**
- **Internet Subscribers per 100 : Urban 107.11 Rural: 40**
- **Smartphones : Appx 650 Million**

Very competitive Pricing

- **Tariffs one of the lowest in the world- unlimited data for ~US \$ 3 / month**
- **Average per GB data costs : US \$ 0.12**

Barriers in growth & adaptation

High Device cost (> US \$ 50 is a barrier)

Low Fiberization of sites (40%)

villages without telephone

Limited online Content in local languages

Low Incomes

Wireless Penetration

- **Wireless subscribers: 1,144 Million**
- **Teledensity Urban: 130; Rural: 57.8 (65% population rural)**
- **Handles >36 Bn minutes of talk-time every day**

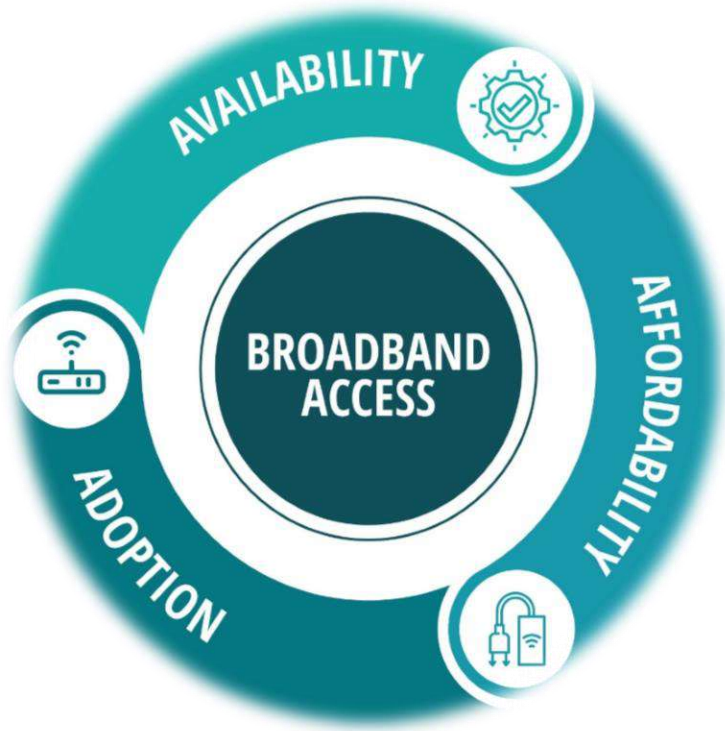
Data Usage of Mobile Users

- **Mobile data users : 850 Million**
- **Monthly overall data usage : 14985 Peta Bytes**
- **Data Usage per subscriber per month: 18.05 GB**

Telecom Financial Data

- **Gross Revenue during a quarter: USD 11 Billion**
- **ARPU (Wireless): USD 2.0 per month**

Challenges in Broadband proliferation



Availability, Affordability and Adoption (Accessibility)

- Lack of infrastructure
- Spectrum related issues for mobile broadband
- Affordability of fixed-line services
- Lack of affordable devices, Rural-Urban Digital divide
- Adoption - Local Content, Awareness, Security concerns, Cultural-divides & Perceived utility

Infrastructural Challenges

- Right of Way Rules, delayed permissions-excess fees, cost over-runs
- Need for high upfront Investments / Return on Investment uncertain due to high capex-opex & poor revenue stream
- In-Building access, access to public places etc.
- Cross-sectoral collaborations for infra sharing

Sharing of passive and active infrastructure

National Digital Communication Policy

- **To prepare the country and its citizens for future**
- **Collaborative approach among all the stakeholders**

Objectives:

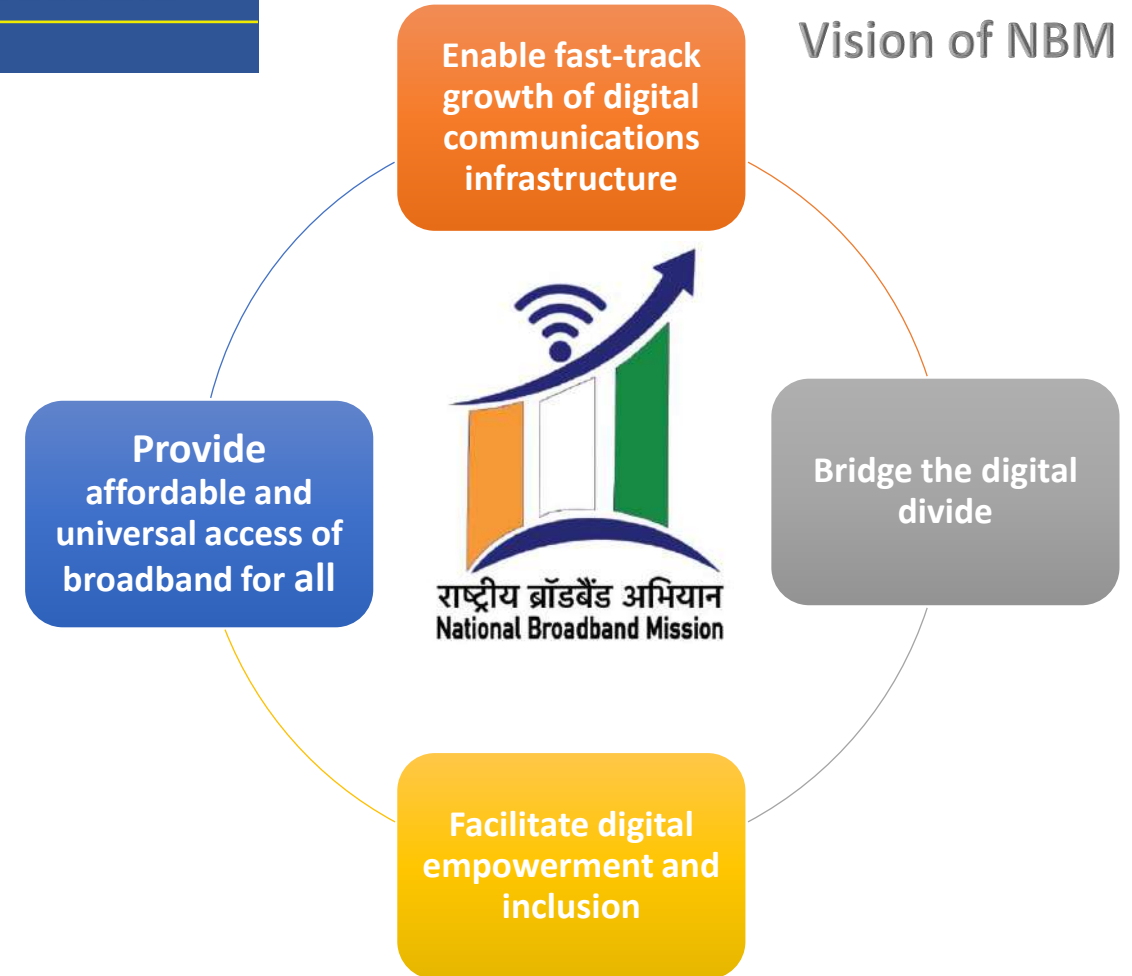
- **Provisioning of Broadband for all**
- **Creation of 4 m additional jobs in Digital Communication Sector**
- **Enhancing contribution of Digital Communication Sector to 8% of GDP**
- **Propelling India to Top 50 in ICT Development Index of ITU**
- **Enhancing India's contribution to global value chains**

National Broadband Mission

Enabling Public Private Partnership for Universal Broadband

- ❑ **National Broadband Mission** under National Digital Communications Policy 2018, is required to design and implement the strategy to be adopted by all stakeholders to achieve the goal of 'Broadband for All'.
- ❑ Based on three pillars
 - ❑ **Universality:** Ubiquitous availability of broadband services to bridge digital divide
 - ❑ **Affordability:** Availability of affordable broadband services to every citizen of India to bridge the socio-economic divide
 - ❑ **Quality:** Availability of high speed and highly reliable broadband access to all
- ❑ **Infrastructure Funding model (including USOF support)**

Infrastructure Component	Investment (In billion USD)
Investment of establishing Telecom Towers	35
Investment in Optical Fiber Infrastructure	30
Investment in other resources like spectrum, R&D and other network resources	35
Total	100



BharatNet Project *connecting all the villages of India...*

Approach towards universal access

Fiber to village

Mobile towers

Fiber to the Home

Wi-Fi Access Points

Unto the last mile



Technologies involved →

For transmission: OFC(Underground, Aerial), OPGW, RF, Satcom, Submarine

For Access : 4G-LTE, FTTx, Public Wi-Fi, VSAT

01

One of the **biggest rural telecom projects of the world**, to connect all the uncovered villages of India with broadband

02

To create the **“Digital Highway”** of the nation to meet the requirements and aspirations of the rural masses

03

Initially envisaged to connect 0.25 million villages. Scope has ben increased to **connect 0.64 million villages**

04

Over **0.63 million Kms of Optical Fibre cables (OFC)** laid till date

05

About **0.2 million** Gram Panchayats provided with broadband connectivity till date

06

Over **0.1 million villages provided with Wi-Fi access points** and **nearly 0.5 million** Fiber-to-the-home broadband connections (FTTH) provided

Provisioning of mobile towers across all the uncovered and remote areas of India

- Infrastructure augmentation in progress after surveying about 33,436 villages where 16,014 towers are proposed to be installed to cover all uncovered villages under different projects.
- About 24,680 villages lack access & 6,279 villages have access to 2G/ 3G based telephony.

Future challenges that TRAI is addressing to promote broadband penetration



Recommended 'Roadmap to promote Broadband Connectivity and Enhanced Broadband Speed' & 'Proliferation of Broadband through public Wi-Fi Networks'



Recommendations regarding allocation of 5G Spectrum, 4G spectrum for Metro-routes; reduction in Spectrum Usage-charges (SUC)



Encouraging Infrastructure Sharing through cross collaboration across sectors including telecom & power grids, State-level distribution companies



Enabling access through Street furniture and In-building solutions for Smart City connectivity & shared infrastructure under National Highways, Railways, Metro



Liberalisation of Satellite Communications inc. enabling setting up of Earth station Gateway & cost-reductions



Recommending Central Right of Way (RoW) web-portal paving way for concurrent laying of OFC & installation of telecom towers with participation of States



Recommendations on high altitude-connectivity in Himalayan region, Ladakh & Himachal Pradesh



Recommendations on amending the rules under the Cable Television Networks (Regulation) Act to enable telecom broadband services through Local CA TV



Bharat 6G Vision



- **“ Design, develop and deploy 6G network technologies that provide ubiquitous, intelligent and secure connectivity for high quality living experience for the world”**
- **Affordable**
- **Sustainable**
- **Ubiquitous**



6 Pillars of Bharat 6 G Vision

- **Multiplatform next generation network**
- **Standardization**
- **R&D Finance**
- **Ecosystem for devices and systems**
- **Innovative Solutions**
- **Identification of Spectrum**



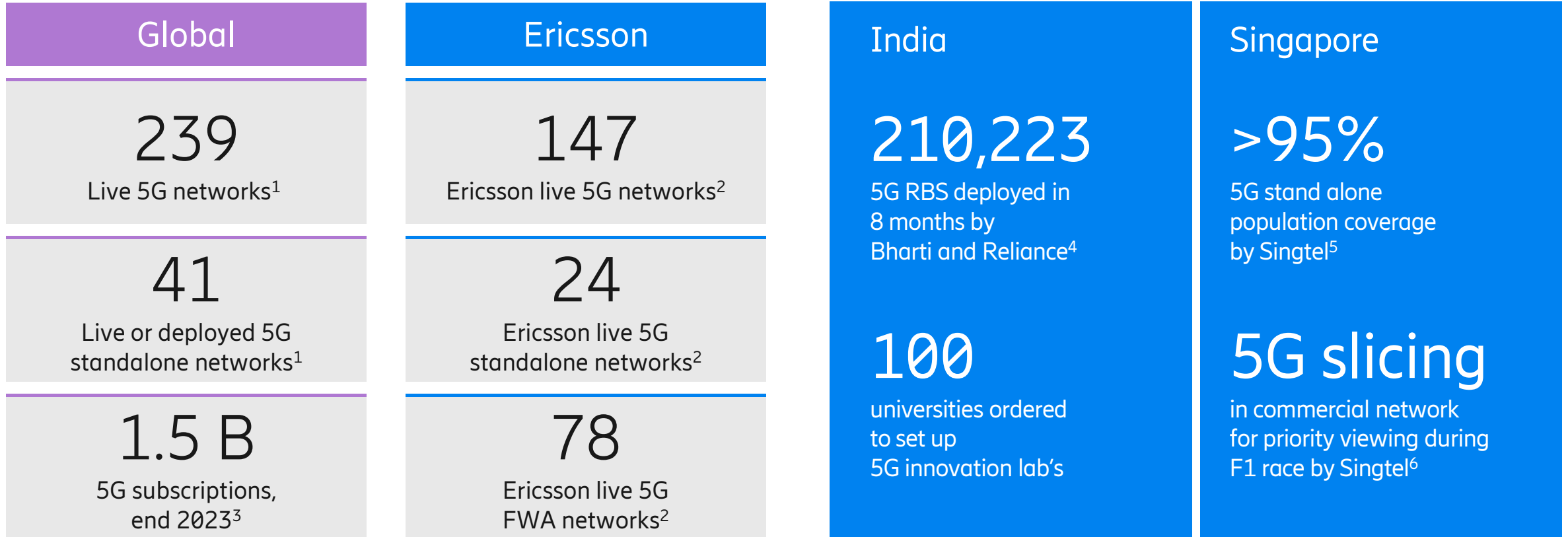
Thank you, tack!

Technology perspectives

Erik Ekudden
CTO Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Fast pick-up of 5G

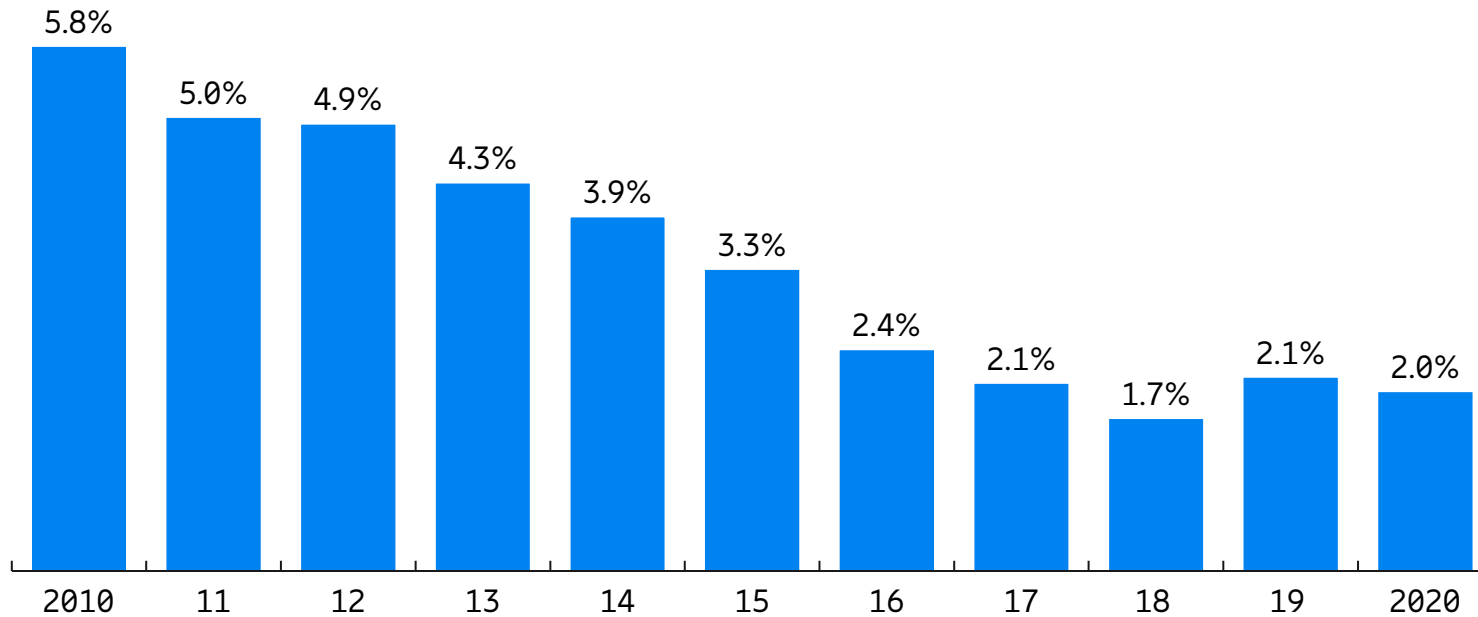


Leading nations have high performing networks, latest technology and strong innovation on 5G

It has become increasingly difficult for CSPs to generate a positive return on capital

Poor capital efficiency (ROIC) has been industry wide concern for more than a decade

CSP ROIC Including Goodwill - WACC¹(%)

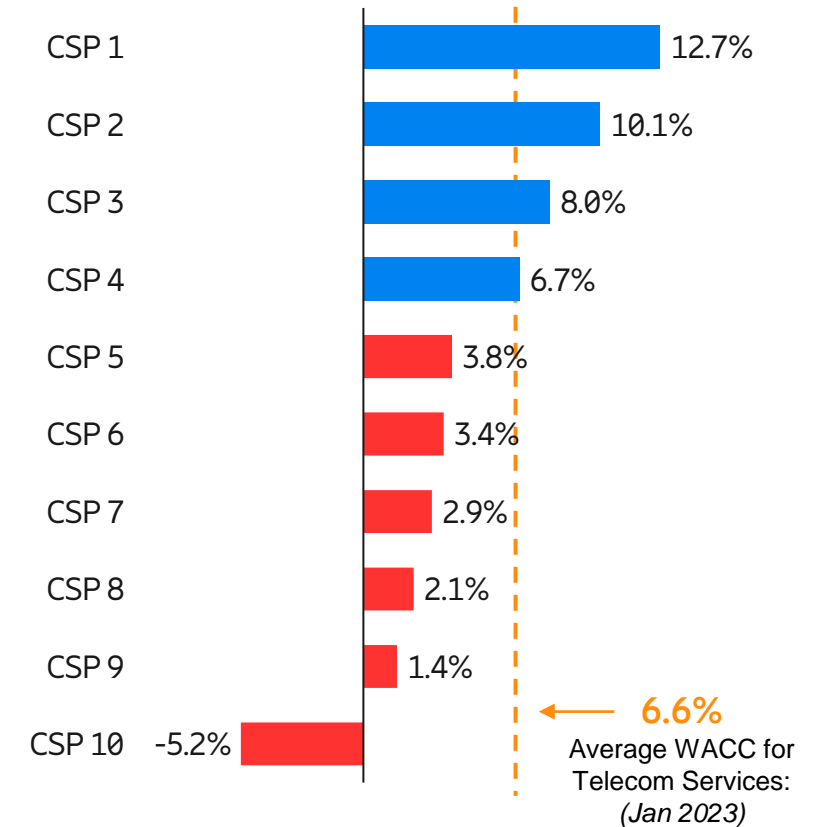


1. Top 24 global operators by revenue, excluding private companies. Top 24 global Telcos include: AT&T, Verizon, DT, China Mobile, NTT, China Telecom, Softbank, Vodafone, AMX, Orange, Telefonica, China Unicom, KDDI, BT, Telecom Italia, KT, Telstra, BCE, STC, SK Telecom, Bharti Airtel, Telenor, Telus

Source: Omdia, Analysys Mason, McKinsey Corporate Performance Analytics

Little evidence of a changing pattern in 2022

2022 snapshot: ROIC & WACC²



2. Based on 10 leading global CSPs

Source: S&P Capital IQ, Stern, Ericsson analysis

New services, new demands



XR introduction in phases

VR to AR → XR takes lead → All day XR
Near term Mid term Long term

Head-Up-Display,
blended information

Surrounding based,
geo-specific

Fully
immersive

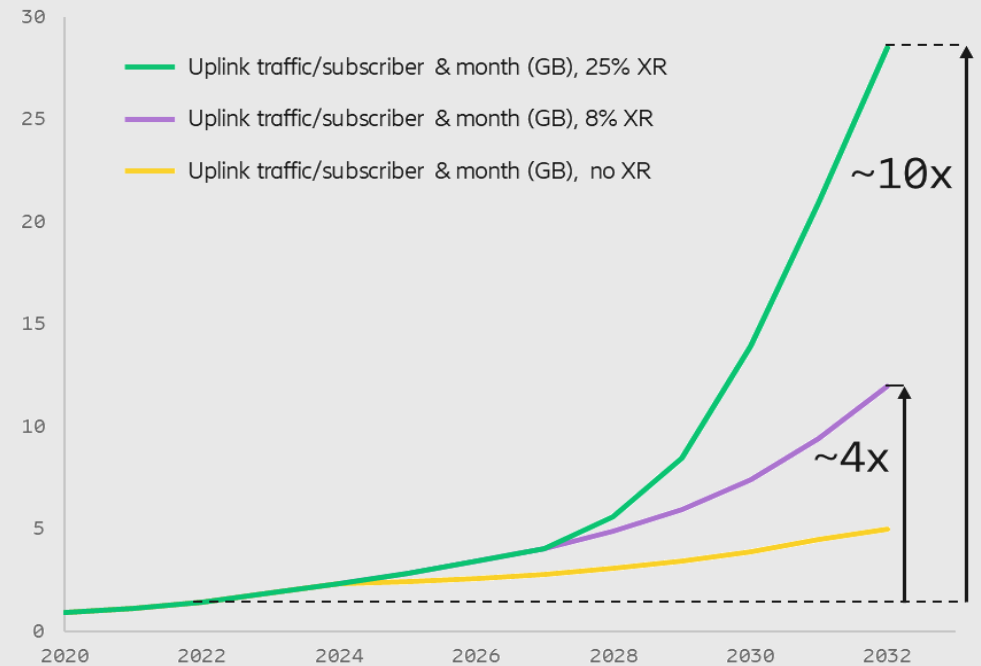


Network
implications

⚠ Uplink,
bounded latency

⚠ Uplink
capacity

10-year *uplink* traffic estimate



XR services drives service differentiation demands for consumer and enterprise

Connected vehicles, new 5G opportunities



Vay

- Car rental service with car delivery and pick-up
- Teledriving, remote-operator driving
- High vehicle utilization

Regulation

- Differentiated services are needed to support consumer and enterprise services in constrained radio-pipe
- Incentivize road-side coverage, consistent network quality needed throughout

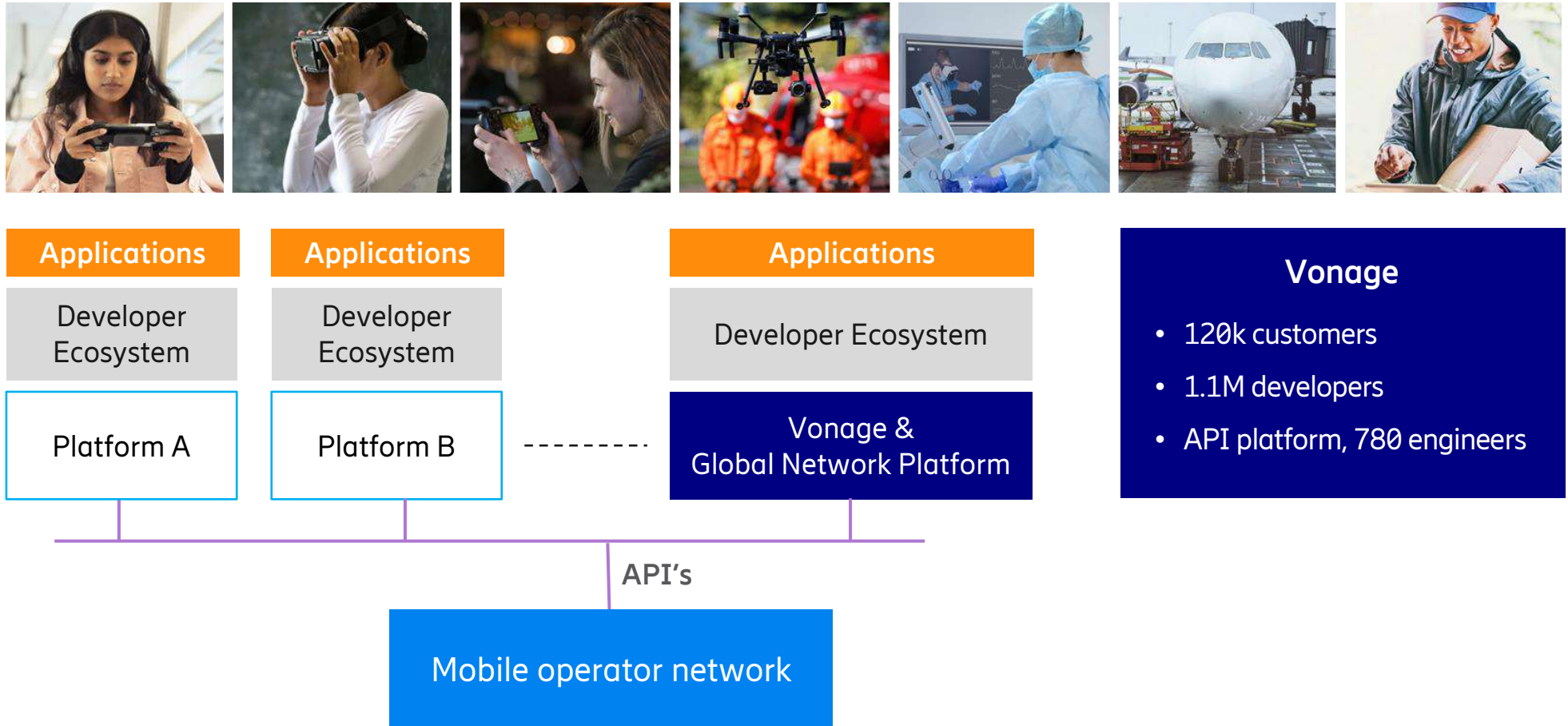


Einride

- Driverless trucks
- Remote assistance
- Higher load capability

Source: Vay & Einride

Network exposure API's to drive global innovation



Ericsson will drive the definition of API's for global industry adoption

Competitive regulation, driving innovation on 5G



Embracing &
Enabling

Incentivize investments
by private investors

Gain national advantage—unlock private innovation and investments with supporting regulation

Spectrum as an enabler to drive 5G adoption



More spectrum allocations for IMT

- More demanding devices
- More applications
- Lack of spectrum is a national disadvantage

Technology free allocations for IMT

- Encourage fast re-farming
- Encourage aggregation
- Avoid allocations related to one generation

Wide BW allocations for high performance

- Boost cell-edge speeds with wider allocations—new demanding services
- Avoid fragmentation with narrow local allocations

Clean spectrum allocations

- Avoid power back-off
- Avoid multiple systems in same allocations
- Network performance is a competitive advantage

Encourage large eco-system

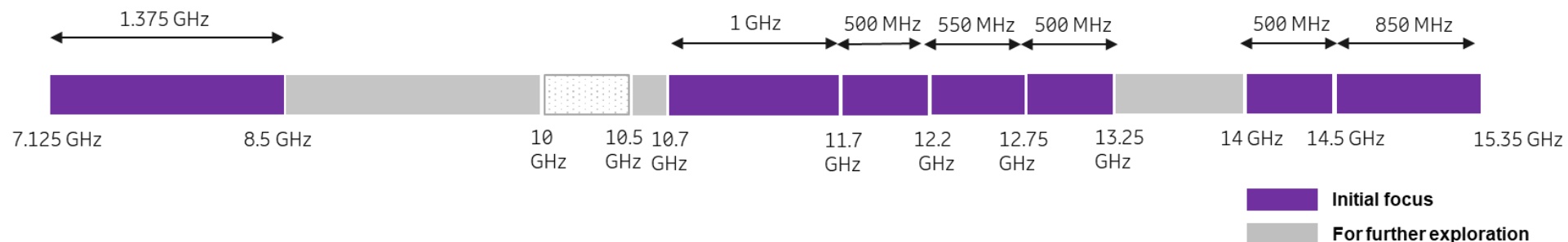
- Seek global or regional allocations
- Allocate wide-area licenses for wide-area subscriptions



WRC-23/WRC-27

Key opportunities for additional mobile spectrum

- WRC-23
 - Geographical expansion of existing IMT frequency bands (low and mid-band)
600 MHz, 3300 – 3400 MHz, 3600 – 3800 MHz, 4800 – 4990 MHz
 - Critical mid-band expansion: 6425 – 7125 MHz, primarily Region 1 but preferably additional countries
- WRC-27 (Agenda Item from WRC-23)
 - Deployment of 6G/IMT-2030 expected around 2030, implies need for decision at WRC-27
 - Essential frequency range 7 – 15 GHz, sub-THz possible as complimentary spectrum
 - Figure suggests band to be studied for WRC-27, variations expected for different countries/regions



A complete 2030 network for all use cases

Multiple spectrum layers, aggregation potential



Sub-Terahertz (90...300 GHz)

Extreme performance

mmWave (24...47 GHz)

High-speed, very low latency

Centimetric (7...15GHz)

Good coverage and capacity trade-off

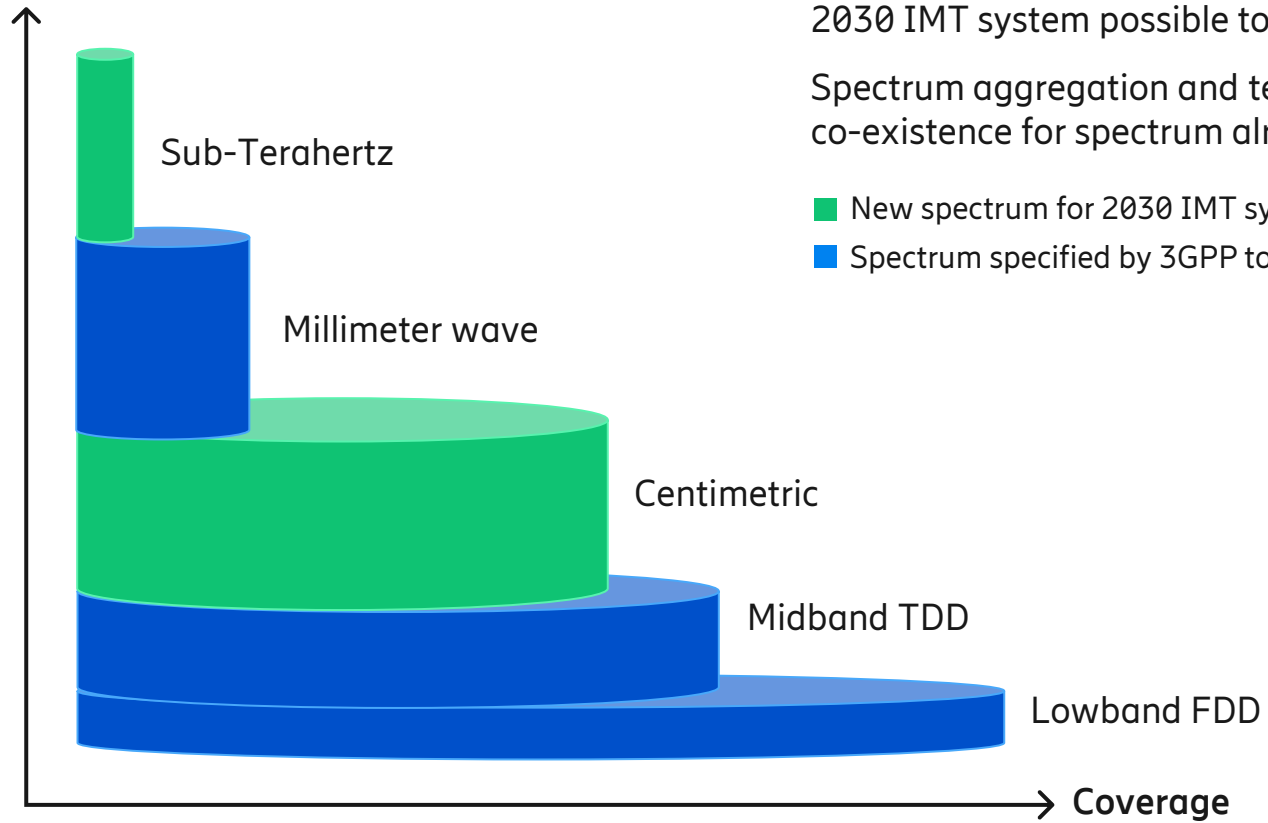
Midband TDD (2.3...<7 GHz)

Wide-area coverage and good capacity

Lowband FDD (<2.6 GHz)

Nationwide coverage and deep indoor penetration

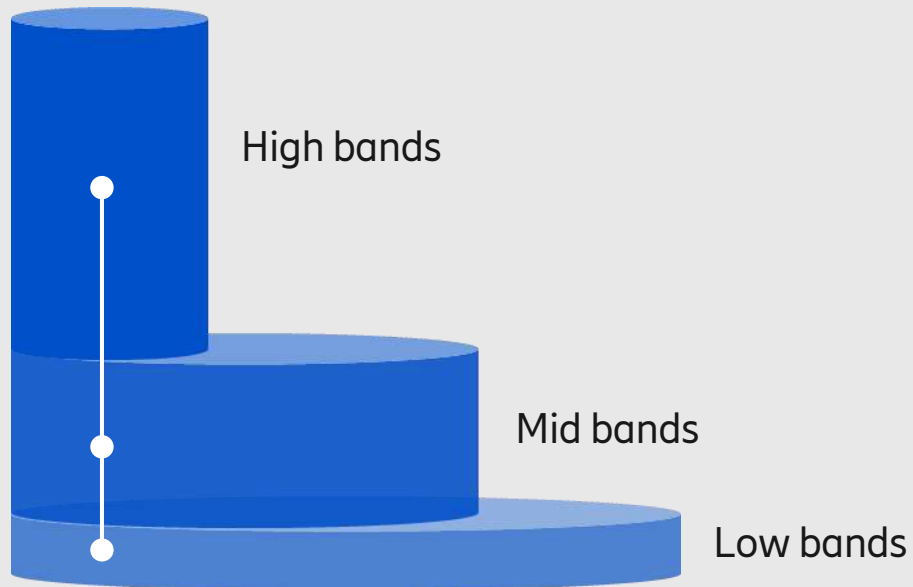
Bandwidth



Aggregate bands, optimize performance



Higher throughput, higher reach, system and user level

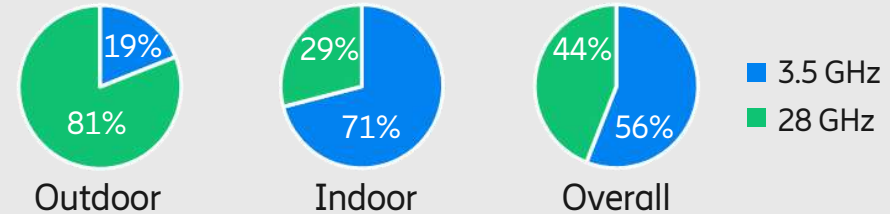


System simulation, 3.5 & 28 GHz, real NW data

150 m site-to-site distance,
21 m antenna height
3.5 & 28 GHz on all macro sites

100 MHz BW @ 3.5 GHz
800 MHz BW @ 28 GHz
70% of traffic indoors

Traffic distribution per band



Outdoor median speed

3.5 GHz only: 0.7 Gbps
3.5+28 GHz: 4.3 Gbps

Indoor speed @ 60%-tile

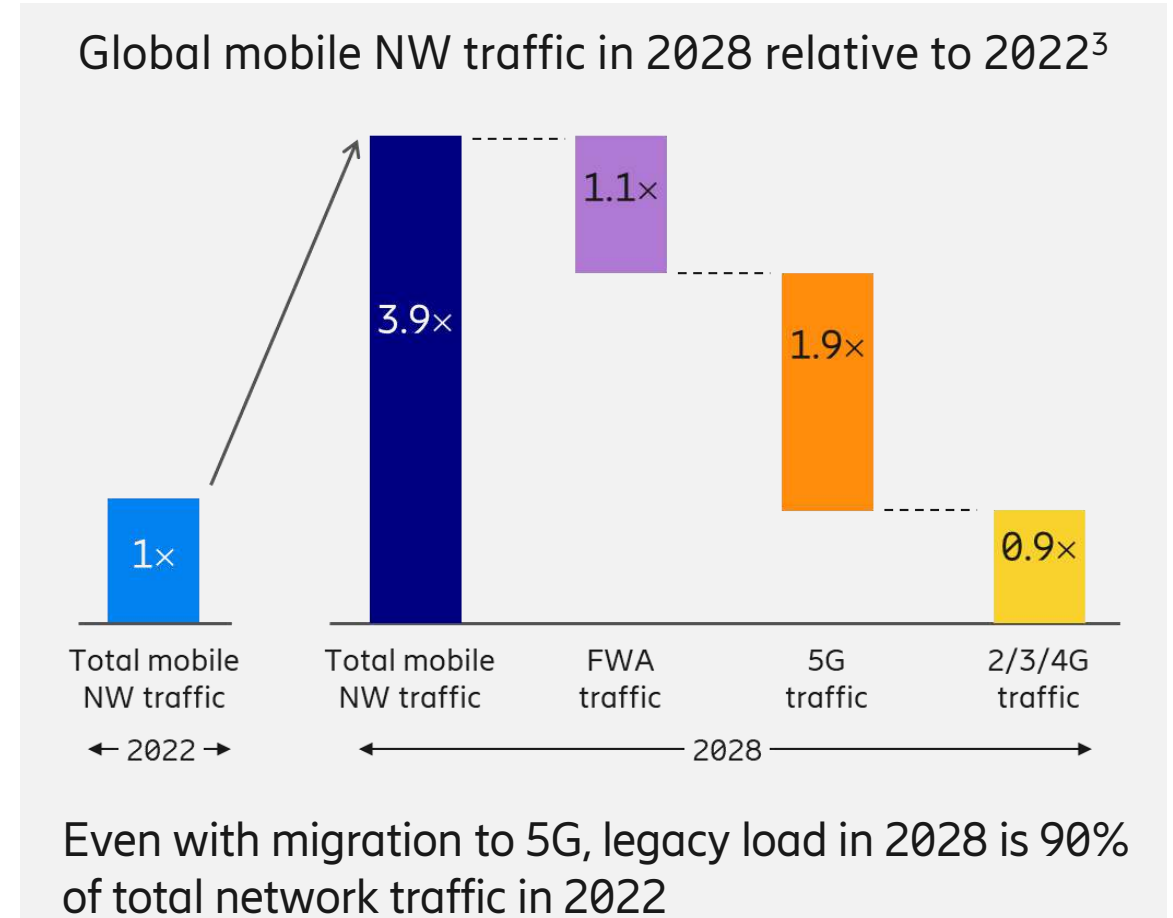
3.5 GHz only: 0.6 Gbps
3.5+28 GHz: 1.2 Gbps

High bands add significant throughput & capacity to 5G

Summary



- 5G innovation for total society is progressing
- Leading nations have
 - Best performing networks
 - Most advanced networks in the field
 - Leading services being introduced
- Regulation must support
 - 5G momentum
 - Differentiated 5G services
 - Private investments and return
- Future IMT focus and support needed in WRC and local regulations

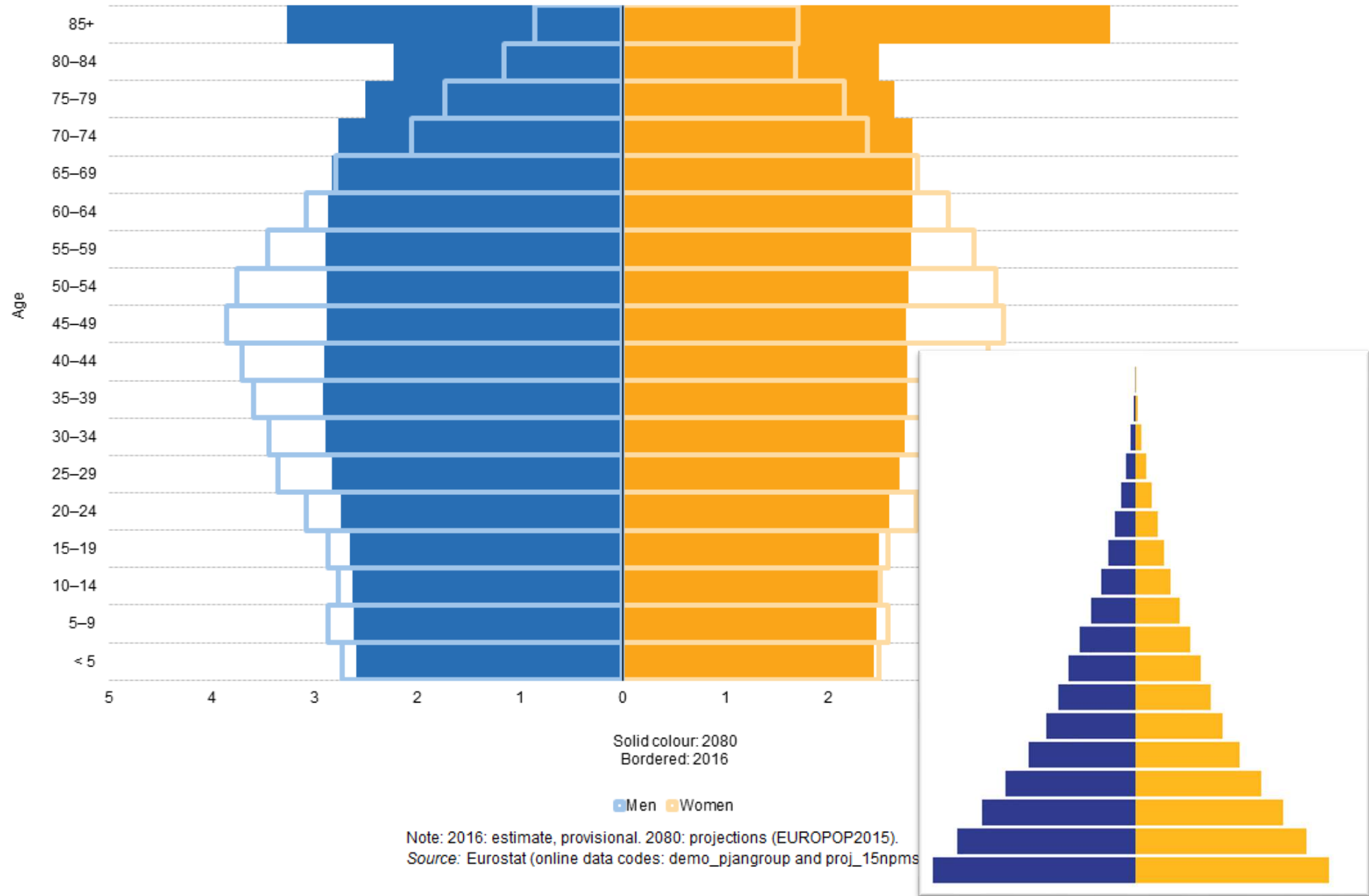




State of the nation

The need to connect everyone and everything!

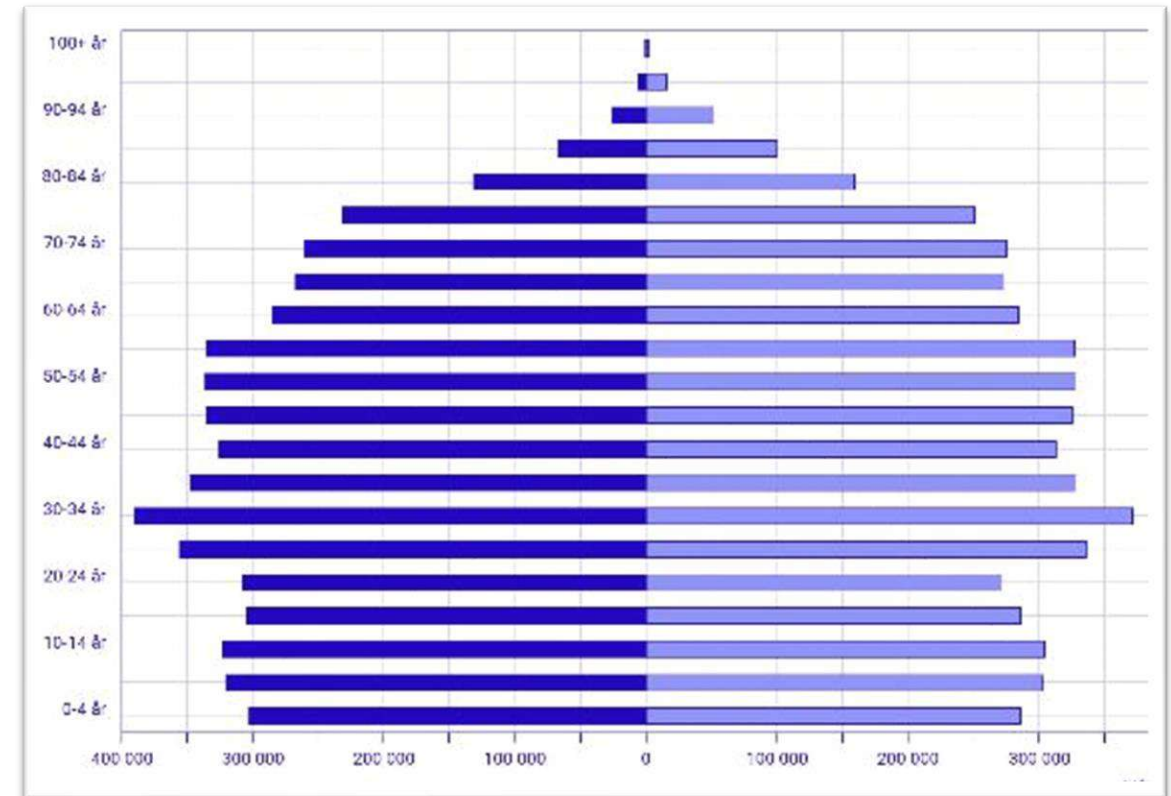
EU 27



Sweden at a glance

The 2% & 8% challenge

- Growing digitalisation of Public Sector
- Connectivity as of Oct 2022
 - Fibre: 98% Homes passed and 93% Homes connected
 - 98% of mobile coverage (population), 57% 5G coverage (population)
- Payments
 - Digital payments dominating
 - Difficult to pay your invoices/bills with cash. (ClearOn cancels service)
 - 500€ in cash per capita available
Note: Swedish Civil Contingencies Agency
- Mail/Letter volumes rapidly decreasing but small packets increasing in volumes



The development of the future

- We need to drive digitalisation even harder and faster
- Innovation is key to accelerate the digital evolution
 - The use of AI and sharing data
- Resilience/Robustness/Security

The need for connecting everything and everyone

- We need to evolve from offering connectivity to secure connectivity to everything and everyone
- It is not a choice it is an obligation

Informal interagency security dialogue 16:00-17:00 (4:00 PM – 5:00 PM)

Pre-registration required, please contact PTS Ola Bergström



CONNECTED SOCIETY

The Malaysia Approach

Broadband for All
Stockholm, Sweden

26 June 2023



Malaysians are highly connected and primarily mobile-first users



48.6%

Fixed-broadband
Penetration Rate



132%

Mobile-broadband
Penetration Rate



147.5%

Cellular Penetration Rate



Total Area: 330,803 km²
Population: 32.7 million
Urbanisation rate: 75.1%
Households: 8.2 million

The pandemic triggered an urgency to address the ‘new norm’ and cater for future demands

Internet traffic increased by 30% - 70%



Internet usage moved to residential areas by 50%-70%



Complaints on internet speed, new coverage areas and indoor have increased from 40%-70%



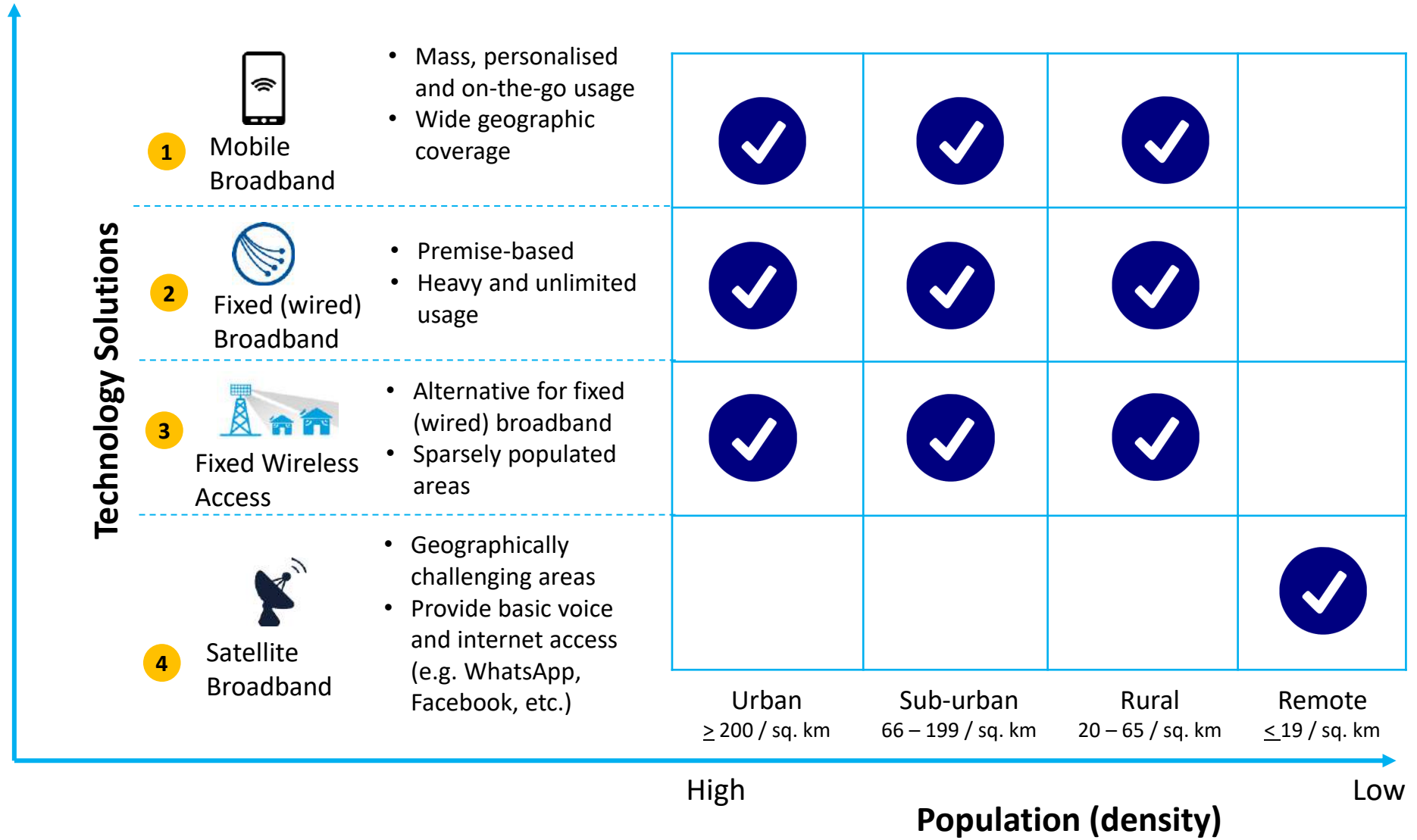
Internet speed reduced by 30%-40%



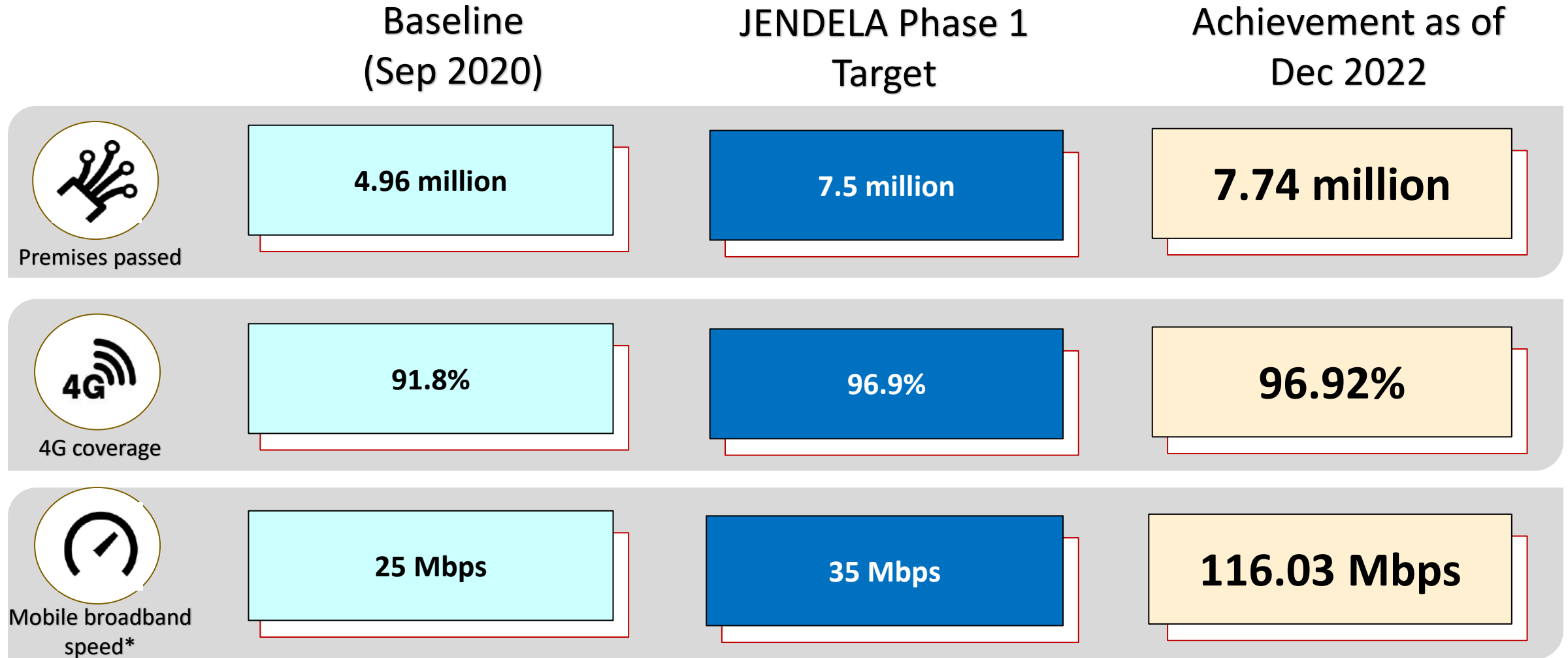
Plans that were already in place to improve coverage and quality for broadband and digital services had to be **accelerated**

National Digital Network (JENDELA) Action Plan

Fit-for-purpose solutions to be deployed in different areas to maximise coverage and connectivity



JENDELA Phase 1 progress (Sep 2020 - Dec 2022)



All targets exceeded

* Mean Mobile Broadband Speed based on Ookla's report

Recognition for JENDELA

World Summit on the Information Society (WSIS) Prizes 2023 for JENDELA is a recognition of MCMC's continuous effort in improving Malaysia's connectivity

The WSIS 2023 Award Ceremony was hosted by ITU in conjunction with the 2023 WSIS Forum at the ITU United Nations (UN) in Geneva, Switzerland on the 14th March 2023



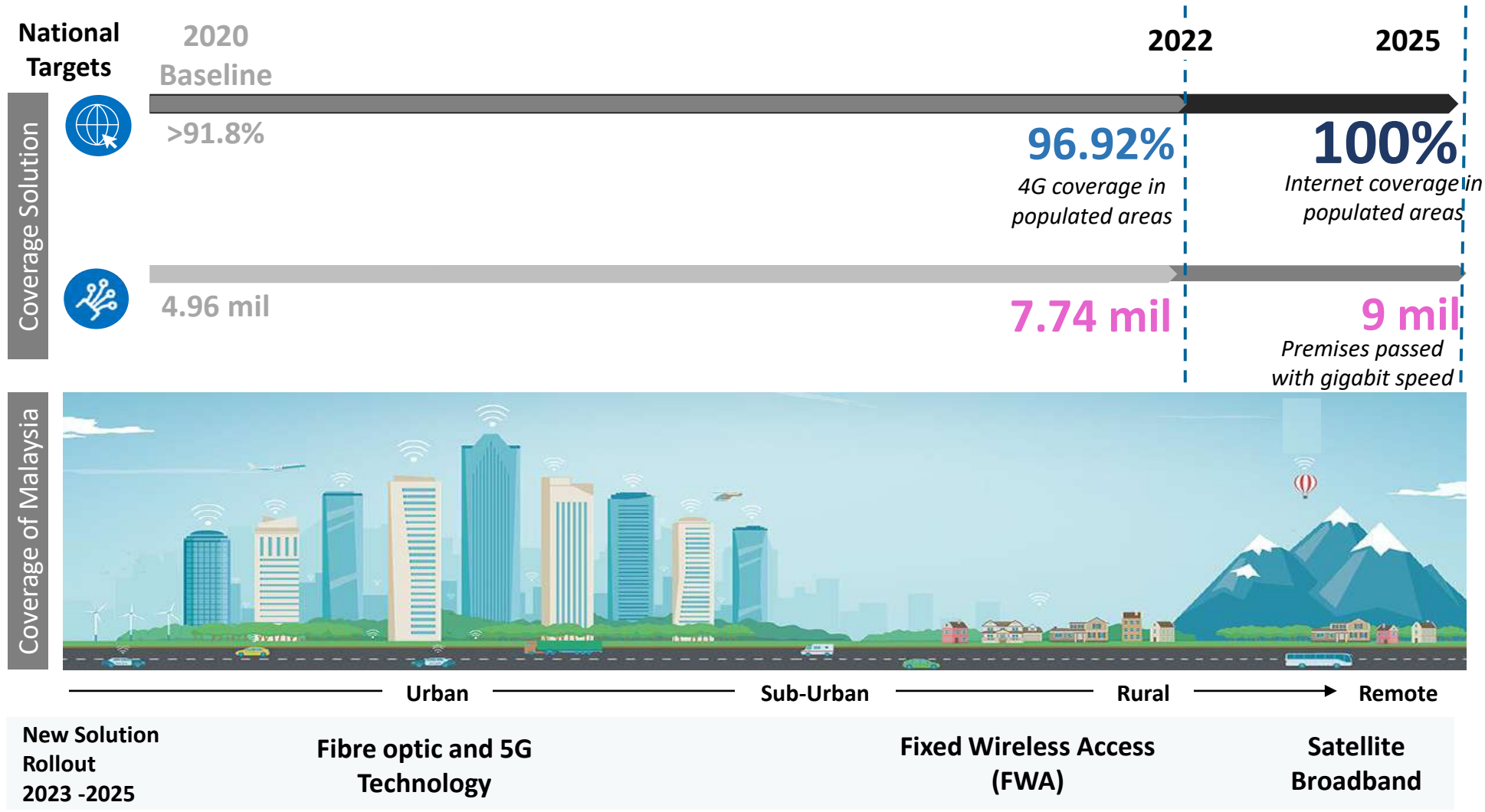
Winner of
WSIS PRIZES 2023

For

Information and communication
infrastructure



JENDELA continues into Phase 2 to connect all Malaysians





Connecting the unconnected remains a challenge especially for Malaysia's rural communities



Scattered and sparse population

Extensively high deployment cost

Varying legislative setting

Lack of other infrastructure including power

Nomadic living

Lack of ICT literacy

Challenging Terrains

Moving forward, several action plans have been implemented and identified to ensure all Malaysians are connected

01

Concerted effort by all

The Government, agencies and the industry working together to provide connectivity to people, especially in remote areas. Government has classified communications as 3rd utility

02

Strengthening regulatory framework

Required to ensure the service providers always provide quality that is up to mark based on the needs of the people

03

Infrastructure Sharing

Promote further infrastructure sharing, particularly active sharing such as MOCN, to minimize cost in rolling out infrastructure particularly in rural and remote areas

04

Use fit-for-purpose technology

Fit-for-purpose technology is preferable to address challenges especially on high deployment cost, time to deploy and pervasiveness of the coverage

05

Establish a platform for ICT and entrepreneurship

Important to address gap in ICT literacy as well as providing knowledge sharing platform to improve socio-economic level of the community in rural and remote areas

Leveraging 5G to improve connectivity

Quick snapshot on Malaysia's 5G:

62.1%

5G coverage in populated areas

735TB

Average daily traffic

1.03 mil

Active subscribers

345 Mbps

Average download speed



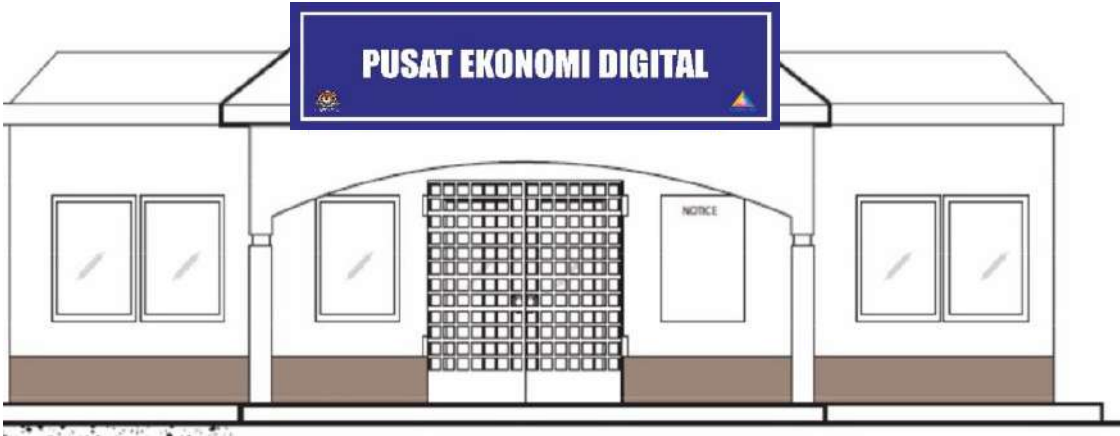
- Single Wholesale Network (SWN) approach has proven to expedite 5G rollout, covering more than half the population in less than 18 months, and continues to expand
- Shift from SWN will take place to provide infrastructure diversity in the long run, on top of a strong foundation
- MCMC's focus is in increasing 5G adoption. To encourage enterprises toward digitalisation, and consumers toward better user experience as well as new services
- Exploring 5G for fixed wireless access to allow faster broadband access rollout where fixed infrastructure is a challenge

Digital Economy Centre (PEDi)

Empowering the Community Towards Digital Economy

OBJECTIVE

- An MCMC project under the Universal Service Provision (USP) initiative;
- Collective internet access in rural areas and for low-income residences;
- To uplift the socio-economic status and human capital development for the rural communities;
- Training based on ICT, entrepreneurship, multimedia & STEM; and
- To close the digital gap between the rural and urban communities



PEDi Users Training by PEDi

<p>Using facilities in PEDi</p> <h1>1.3 Mil</h1>	<p>More than</p> <h1>3.3 Mil</h1> <p>Participations in all categories</p>
--	---

PEDi Entrepreneurs

 <h1>26,448</h1> <p>PEDi active entrepreneurs</p>	<h1>22,113</h1> <p>Participant in Pupuk@Shopee</p>
--	--

<h1>22,598</h1> <p>Business activities conducted on at least 1 online platform</p>	<h1>RM39.7Mil</h1> <p>Sales generated through Pupuk@Shopee</p>
--	--

As of March 2023

From June 2021 - Dec 2022



THANK YOU

Broadband for all in Japan

Yoko Nakata

26 June 2023

Ministry of Internal Affairs and Communications (MIC), JAPAN

Table of Contents

1. Digital Garden City Nation

(1) Abstract

(2) Fixed Broadband, Wireless and IoT Infrastructure

(3) Development of Data Center/Submarine Cable,
Non-terrestrial network (NTN)

(4) Beyond 5G (6G)

2. Secure and Trusted Network

3. International Cooperation

1. Digital Garden City Nation

■ Digital implementation to solve local issues

Local 5G implementation

Proof of Concept for the realization of problem-solving local 5G, etc (FY2020~FY2022).

- ✓ Contribution to the revitalization of local communities through digital implementation based on the each local community's needs.
- ✓ Conducting Proof of Concept to develop technical standards for operation and local 5G solutions.

■ Development of Digital Infrastructure

Universalization of optical fiber service

Project to promote the development of an advanced wireless environment

- ✓ Collaboration with local governments and telecommunications carriers in deployment of optical fibers
- ✓ Subsidies for the construction of optical fibers to the entrance of radio stations in disadvantaged areas.
- * Other efforts include extending the duration of 5G tax incentives (FY2022 tax reform)

■ Efforts to ensure that no one is left behind

Support to encourage digital utilization

Project to promote the digital utilization

- ✓ Roll out of workshops for those who are unfamiliar with digital technology, such as the elderly, to give advice and consultation for how to use governmental online services in order to mitigate their anxiety about such services.

5 pillars of the Plan

- ① Fixed broadband (e.g., optical fiber)
- ② Wireless and IoT infrastructure (e.g., 5G)
- ③ Development of data centers/submarine cables and other related infrastructure
- ④ Non-terrestrial network (NTN)
- ⑤ Beyond 5G (6G)

Development policy

- 1) Aiming for a **household coverage rate of 99.9%*** by the end of FY2027.
Pursuing further advancement. *At the end of FY2021: 99.7%
- 2) Aiming to **establish a communication environment conducive to the GIGA School Concept by the end of FY2023** (targets: 97 schools with inadequate communication environments).
- 3) Promoting the early and smooth **transition of public facilities to private facilities** based on the local government's requests.

Specific Measures

- 1) **Elimination of underserved areas**
 - **Subsidized support**
 - Promoting **the establishment of a 5G environment in FY2023 for schools that will not be equipped with optical fiber until FY2024 or later.**
- 2) **Transition of public facilities to private facilities**
 - Promotion through **subsidies and universal service grant system**
 - Consideration of **measures to relocate public facilities, including broadcasting facilities, to private facilities**
 - Incorporating **examples of initiatives** transitioning to private facilities in guidelines for local governments
- 3) **Regional council meetings**
 - Promoting **the matching of digital implementation and infrastructure development** among stakeholders.

② Wireless and IoT infrastructure (e.g., 5G)

Development policy

Note: The numerical targets are achieved through the combined efforts of the four parties.

*Major revisions are in red.

Phase 1:
Deployment of
infrastructure

Phase 2:
Regional
expansion

1) 4G availability in all residential areas

(Population outside 4G area: 0.6 million at the end of FY2021 → 0 at the end of FY2023)

2) Nationwide deployment of parent stations, which will serve as the foundation for 5G deployment, in almost all areas where needs exist (enabling immediate response to need) (5G infrastructure deployment rate: 43.7% at the end of FY2021 to 98% at the end of FY2023)

3) 5G population coverage

[End of FY2023] **Nationwide 95%** (93.2% at the end of FY2021)

Deploying 5G base stations in **all cities, wards, towns, and villages** (Total of 280,000 stations)

[End of FY2025] **Nationwide 97%, with more than 90% in each prefecture** (Total of 300,000 stations)

[End of FY2030] **99% Nationwide and in each prefecture** (Total of 600,000 stations)

4) Road coverage (expressways and national highways)

***Added from the perspective of improving convenience for the public and ensuring safety and security.**

[End of FY2030] **99%** (Actual result at the end of FY2021: Approx. 95%), **100% for highways.**

- Promotion of Open RAN in Japan and abroad
- Realization of inter-carrier roaming in emergencies such as natural disasters and telecommunications facility accident
- Promoting integrated development and utilization of local 5G and other regional digital infrastructures

Specific Measures

1) Securing new 5G frequencies

2) Institutional development (5G relay stations, etc.), support measures (subsidies, taxation), and **functional enhancement of Japan OTIC**

3) **Promoting infrastructure sharing** (preferential subsidy requirements and creation of a database of facilities where base stations can be installed)

4) **Promoting alignment between digital implementation and infrastructure development through the convening of regional councils**

5) **Linkage with projects utilizing automated driving and drones**, which are expected to be implemented in society at an early stage

Two-stage strategy of 5G Implementation

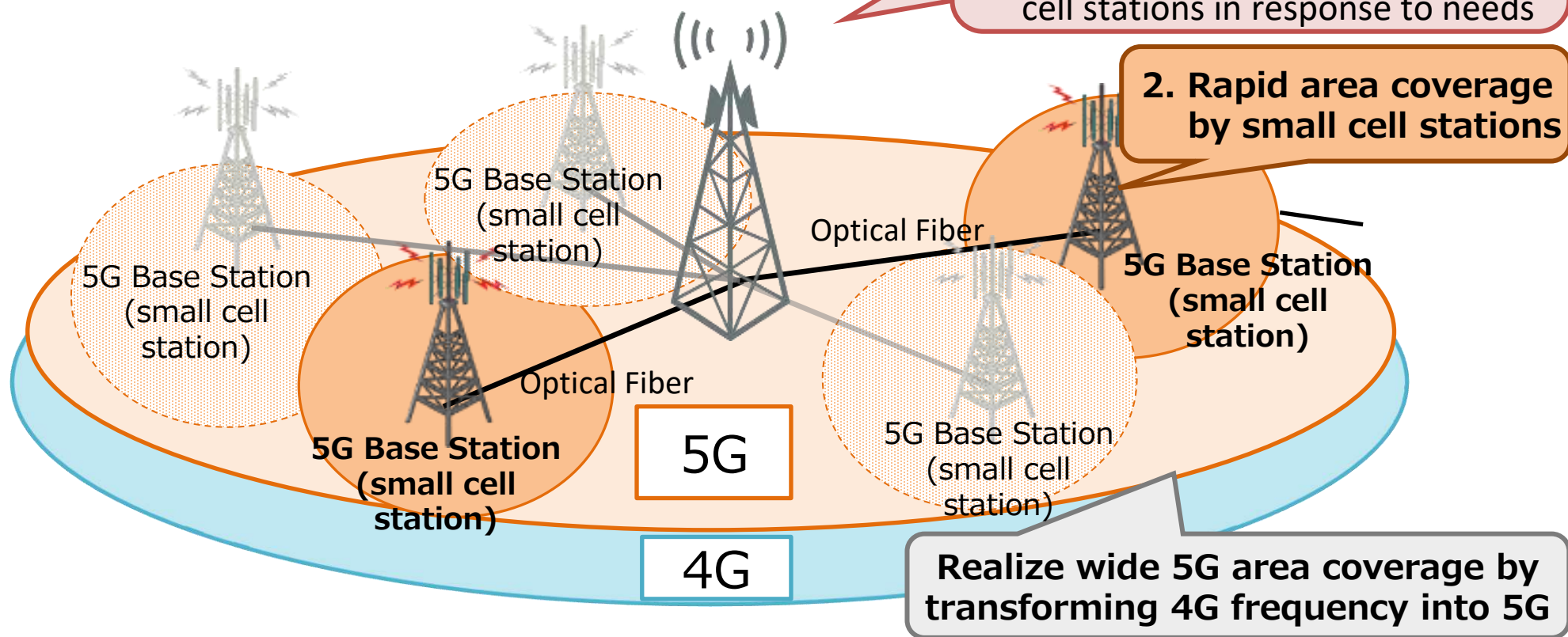
Aim to realize **the world highest level 5G environment** by **the two-stage strategy**:

1. Nationwide deployment of 5G foundation (**4G base stations** and **5G master stations**)
2. **Enhance** nationwide **area coverage** by local development of **small cell stations**

* Target 5G Population Coverage: 95% nation-wide (FY 2023)

5G High-level Specific Station (Node Base Station)

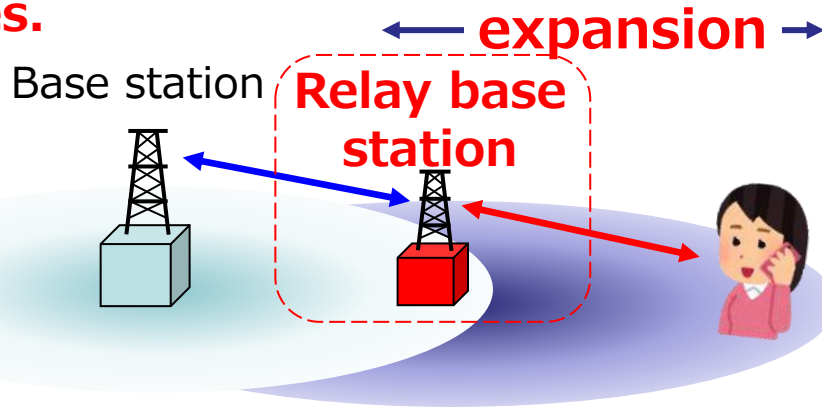
1. Deploy base stations in all areas with business potential
→ Make it possible to deploy small cell stations in response to needs



- Discussing ①5G relay base station, ② Femtocell base station/ Low power repeater ③ Development of system for high output mobile phone, in order to mobile communications area, and concluding the policy of development of system and take necessary actions in 2023.

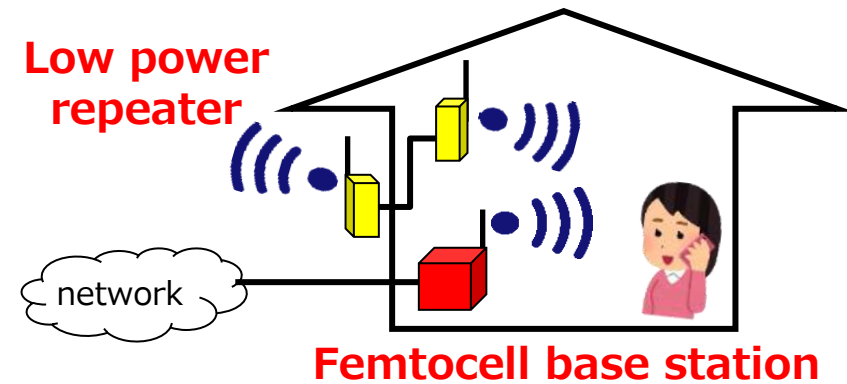
1 5G relay base station

Expanding 5G areas into blind zones.



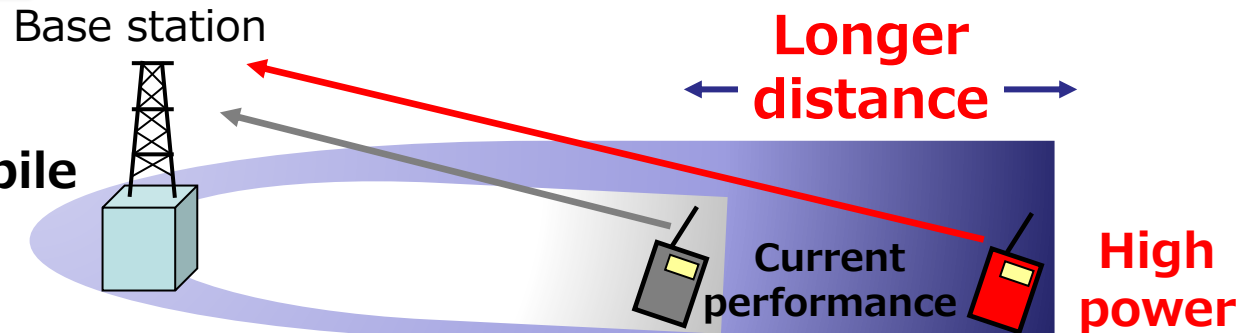
2 Femtocell base station/ Low power repeater

Make home inside as a 5G area



3 High power mobile phone

By advancement of mobile phone with high output, distance and quality of mobile phone is increased.

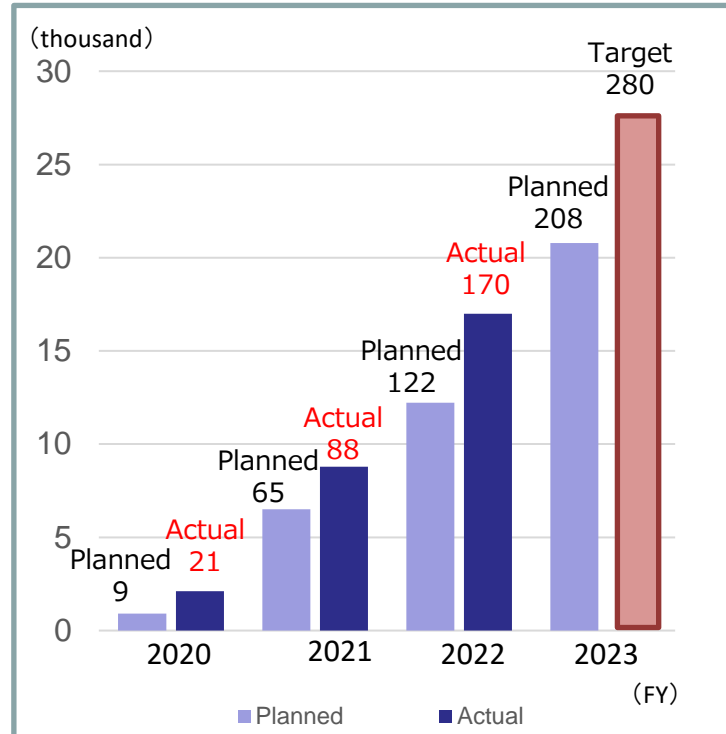
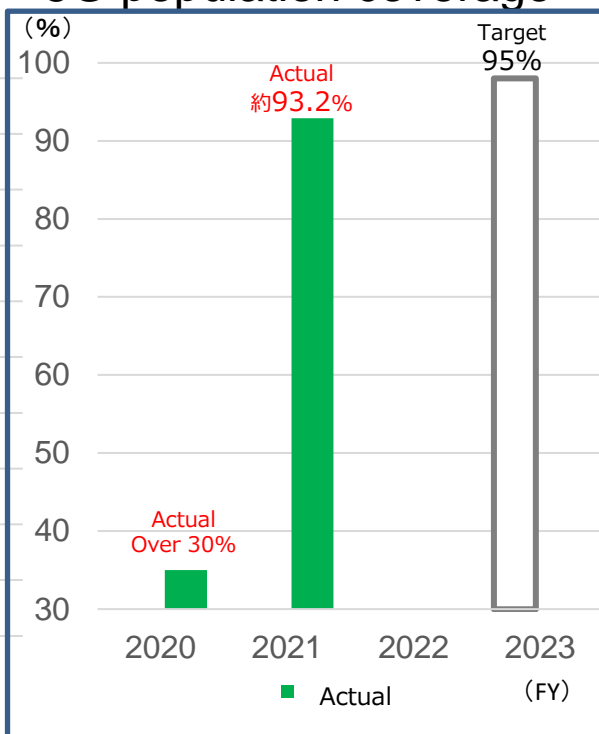
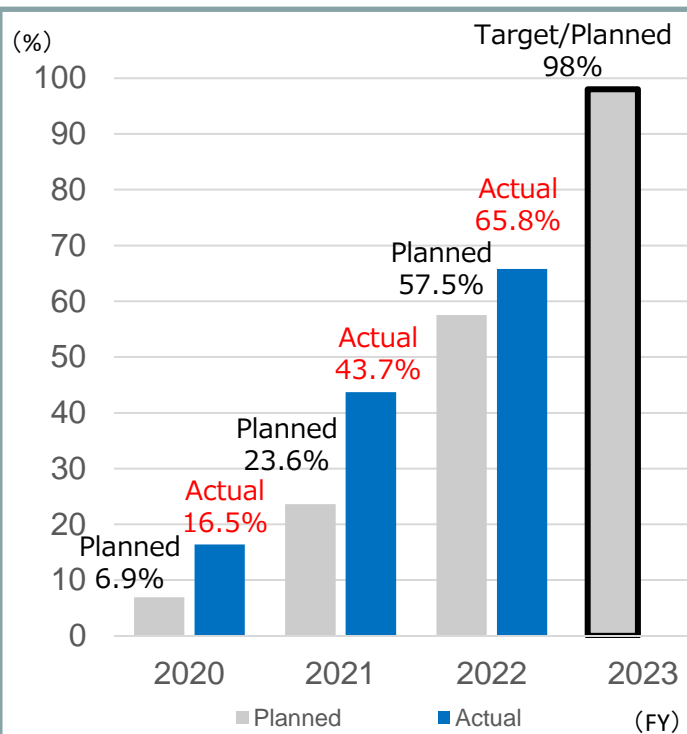


Deployment situation of 5G base stations

- In the “Vision for a Digital Garden City Nation” initiatives in Japan, 98% for the rate of 5G base stations’ deployment and 280,000 of 5G base stations are targeted by the end of March 2024.
- 5G infrastructure deployment rate as of March 2023 is **65.8%**.
(cf. the planned rate: 57.5%)
- 5G population coverage as of March 2022 is **93.2%**
(5G population coverage as of March 2023 is under investigating)
- Total number of 5G base stations as of March 2023 is approx. **170,000**.
(cf. the planned number: 122,000)

5G population coverage

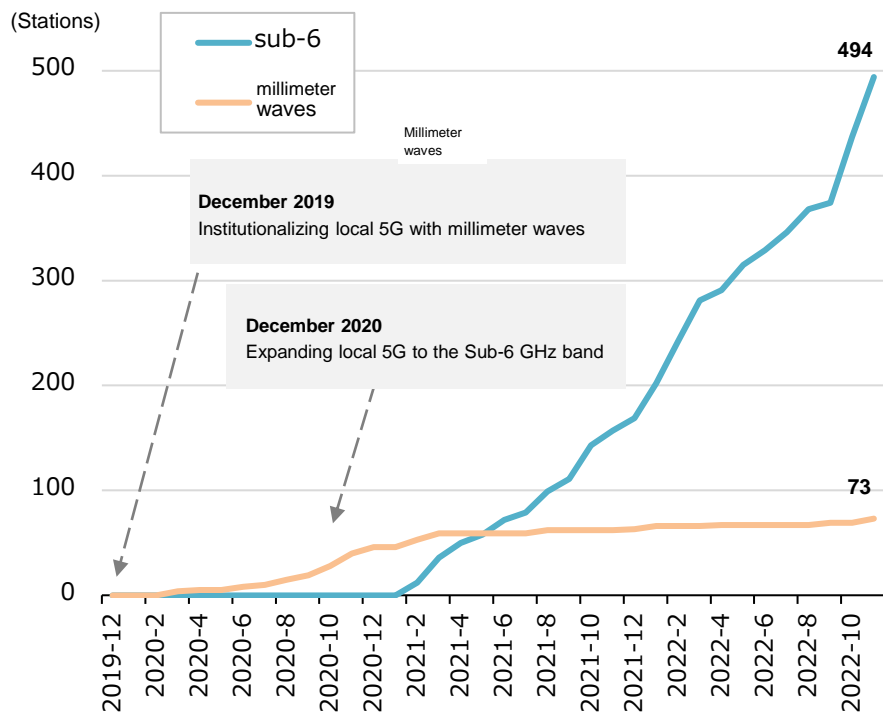
Total number of 5G base stations



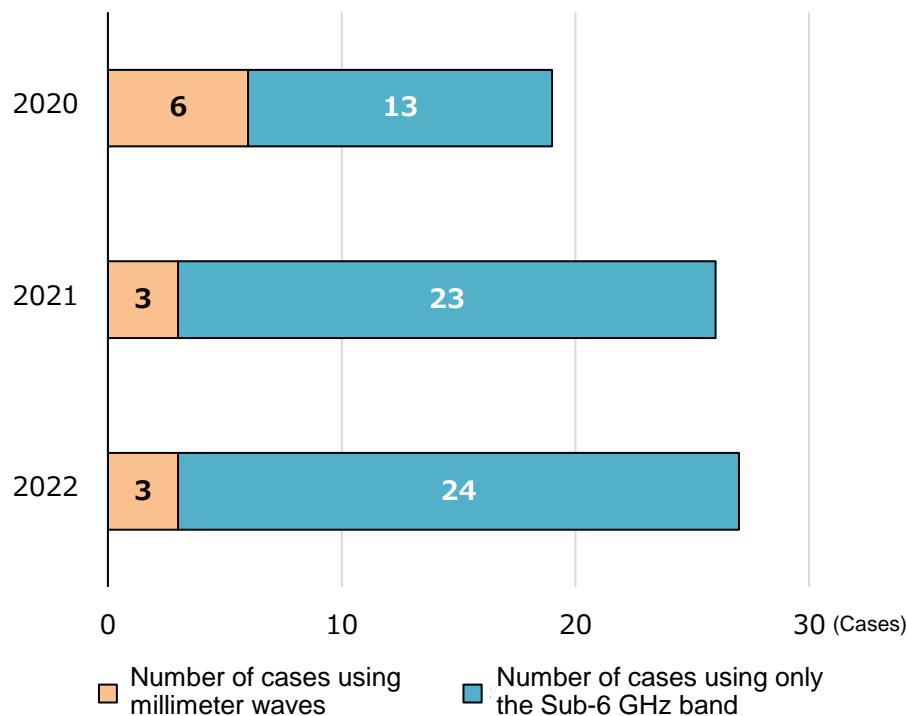
Local 5G

- As for local 5G radio stations, 108 operators have obtained licenses for the Sub-6 GHz band and 31 for the millimeter wave band (as of November 30, 2022).
After expanding the scope for licensing, the number of licenses for millimeter waves remained stagnant. At the same time, there was a significant increase in the number of licenses for the Sub-6 GHz band.
- Currently, use cases are being demonstrated in various fields, such as construction, medical care, entertainment, etc., focusing on the Sub-6 GHz band.

Number of local 5G licenses



Number of local 5G development demonstrations by bandwidth

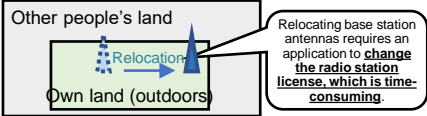
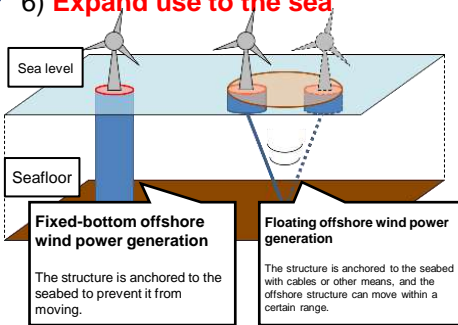


(Source) MIC: The Radio Use Web Site page

(Source) MIC: Based on the development and demonstration of the realization of problem-solving-type local 5G, etc., FY 2020 - FY 2022)

- Since December 24, 2021, the following issues have been studied under the New-generation Mobile Communications System Subcommittee to promote local 5G further.
- Based on a partial report from the Information and Communications Council on January 24, 2023, MIC plans to develop the necessary related regulations in the future.
 - *Maritime use will continue to be studied by the local 5G study working group in the next fiscal year and beyond after examining interference with public business radio stations.

Major issues and considerations for flexibility

(1) Wide-area use	(2) Simplification of licensing procedures and inspections	(3) Expansion of use to the sea*
<ul style="list-style-type: none"> • If someone wants to use local 5G more extensively beyond their own property, the landowners of the extended area have priority, even if they show interest later. ➡ 1) Introduction of Joint Use (tentative name) • <u>Operating mobile stations on someone else's property</u> is not allowed, even without concern about interference. ➡ 2) Relaxation of movement restrictions on other people's land • There is a misleading statement in the guidelines that <u>other parties' land is required to adjust interference unconditionally</u>. ➡ 3) Clarification of the method for adjusting interference between land use by others and land use by oneself 	<ul style="list-style-type: none"> • Even if there is no increase in radio wave strength, "notification only" is not allowed for outdoor use; a change application, such as for area alteration, is required. ➡ 4) Simplification of licensing  <ul style="list-style-type: none"> • If periodic inspections of local 5G are omitted, <u>monitoring and control with the same maintenance and operation system (24 hours a day, 365 days a year) as national 5G</u> is required. ➡ 5) Simplification of periodic inspections 	<ul style="list-style-type: none"> • <u>There is a need to utilize local 5G in offshore locations such as offshore wind farms, but local 5G is a system based on onshore use and is not approved for use in offshore locations.</u> ➡ 6) Expand use to the sea 

- In order to adjust to huge increase of telecommunications traffic, frequency allocations for 5G have been conducted to **broaden the mobile phone bandwidth by three times**.
- As a first step, **a frequency allocation of 2.3GHz was conducted in May 2022**. At the same time, **an indicator to evaluate instalment of base station in less favored area** was introduced.

Evaluation indexes on examination of a frequency allocation (a frequency allocation of 2.3GHz)

1. Absolute examination

1 Area expansion

- Installment plan for all prefectures

2 Equipment

- Securing place for installment, procurement of equipment, human resource procurement plan for installment
- Plan for safety and reliability of equipment.

3 Economic value of the frequency

- Fees of establishing specified base stations are more than 2.4 billion yen

4 Others

- No transferring business to existing operators.
- Plan to keep mobile phone service in the case of radio switch off for the dynamic spectrum access

2. Comparative examination

1 Area expansion

- The number of base station in whole Japan is larger than other operators.
- **The number of base station in less favor areas is larger than other operators.**
- **The number of 5G base station in 5G delayed area is larger than other operators.**

2 Advancement

- The ration of stand alone 5G specified base station is larger than other operators.

3 Economic value of the frequency

- Fees of establishing specified base stations are higher than other operators'.

4 Technology

- Whether having development and installment of technologies such as switching bandwidth without stopping radio wave or not, and whether proposing international standards or not.

Allocate frequencies

Achievement status of goals for securing frequency bandwidth by the end of FY2025

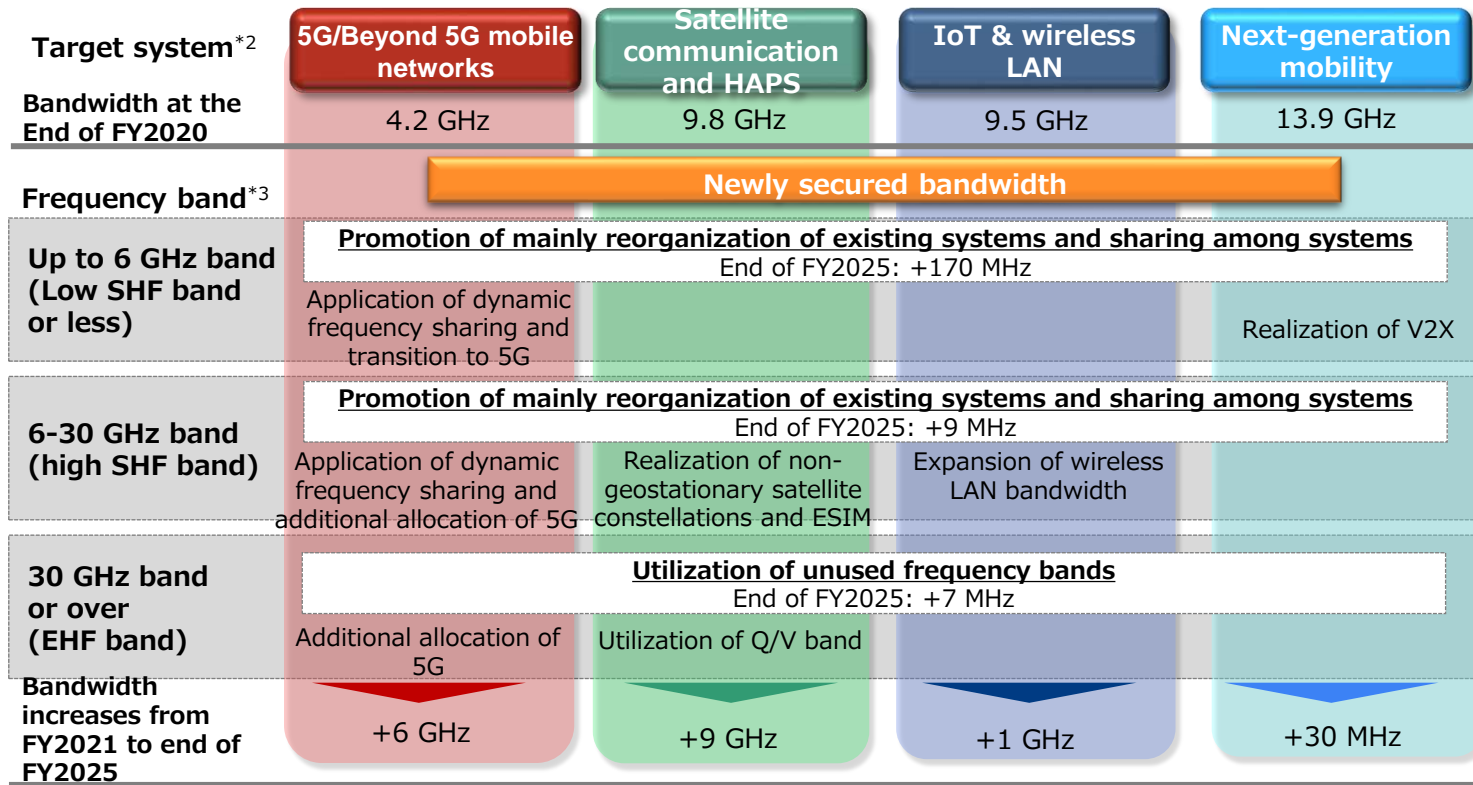
- Goals for securing frequency bandwidth by the end of FY2025 (from the report of the Radio Policy Roundtable in the Age of Digital Transformation (August 2021))

The immediate goal by the end of FY2025 is to secure bandwidth with an increase of approximately 16 GHz in total, starting from the end of FY2020, on four radio wave systems that particularly require wider bandwidth: mobile phone network systems such as 5G and Beyond 5G, satellite communications and HAPS systems, IoT and wireless LAN systems, and next-generation mobile systems.

- Progress status

A total of +3.04 GHz bandwidth (+40 MHz for mobile phone network systems, +2.5 GHz for satellite communication systems, and +0.5 GHz for wireless LAN systems) has recently been secured.

[Goals for securing bandwidth by the end of FY2025]



Total bandwidth at the end of FY2020: Approx. 37 GHz bandwidth

Goals for securing bandwidth
End of FY2025
+ Approx. 16 GHz bandwidth *1

*1 Comparison with the end of FY 2020
*2 Bandwidth shared among 4 systems is added to bandwidth for each system.
*3 Frequency band is classified based on the current implementation status of a wireless system and the possibility of future introduction (SHF: Super High Frequency, EHF: Extra High Frequency), and examples for each frequency band are added.

[Progress status]



Progress status
+3.04 GHz bandwidth

*Major revisions are in red.

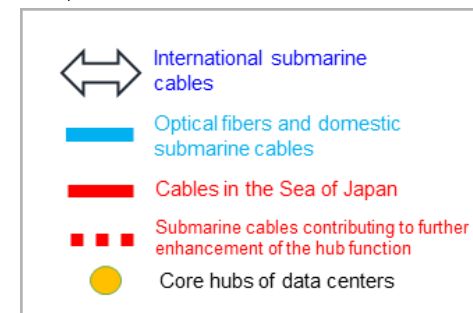
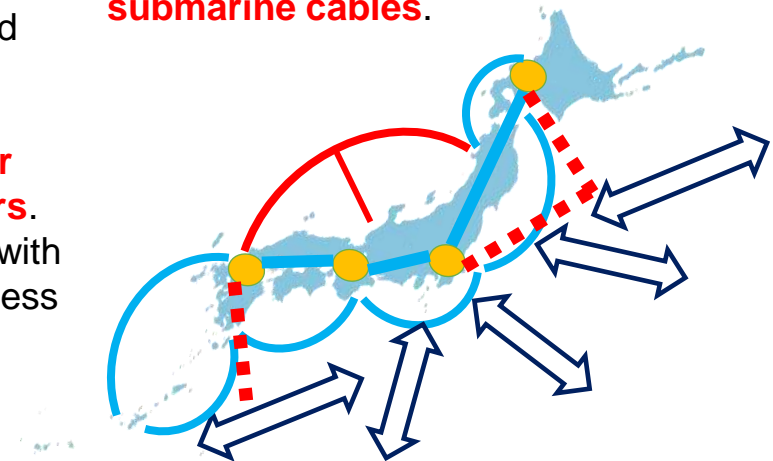
Development target

Specific Measures

1) Datacenter

- The government of Japan plans that two ministries (MIC and METI) would join force and develop 10+ regional basis for data centers in five years. .
MIC supported the development of seven regional datacenters through a supplementary budget for FY2021.
- For the time being, the two ministries **promote the consolidation of third and fourth core bases in areas of Hokkaido and Kyushu**, which would complement and possibly substitute the role of existing basis of Tokyo and Osaka..
- The two ministries continue to **study the future course of, and consider the necessary support for, the further decentralization of data centers**. This would be done in corporation with relevant ministries and agencies, with close eyes on the **greening initiatives**, emergence of MEC (multiple-access edge computing) and other technology developments.

- **Subsidized support**
- Promoting **multi-routing** of international submarine cables.
- Promoting **initiatives to safeguard international submarine cables and landing stations and enhance the installation and maintenance of submarine cables**.



2) Submarine Cable

- The construction of Japan Sea Loop Cable (Digital Garden City Superhighway) is planned to be completed in FY 2026, with decentralized landing stations in local areas.
- **Consolidate Japan's position and its functions as the hub of international data communications**
- **Reinforce the safety measures** for international submarine cables and landing stations

Development policy

Note) NTN: Non-Terrestrial Network
HAPS: High Altitude Platform Station

- Efforts will be made to promote initiatives to accelerate the introduction of HAPS and satellite communications services, including the development of related systems, with a view to **early deployment in Japan from FY2025 onward.**

Specific Measures

1) HAPS

- Promoting **international rulemaking, such as frequency expansion in WRC-23.**
- **Domestic institutional development necessary for practical application.**
- Promoting **overseas development** by seizing opportunities for **demonstrations and showcases at Expo 2025 Osaka/Kansai and other events.**

2) Satellite communications

- Promoting **the securing of frequencies and necessary institutional arrangements.**
- Promoting **the construction of Japan's own constellation of communications satellites.**

What is HAPS ?

HAPS: High Altitude Platform Station

- ✓ Flying object at an altitude of about 20 km equipped with a base station or repeater of the mobile communication system
- ✓ Capable of covering a very wide area (100km or more)
- ✓ Contributes to building disaster-resistant networks (Not directly affected by earthquakes, etc.)
- ✓ Realizes a communication network covering “three-dimensional space area” and supporting planes, drones, etc.



Super wide coverage area



Disaster recovery



3D spatial area



HAPS base station



Altitude of 20km

Ground base station

Drone



Drone

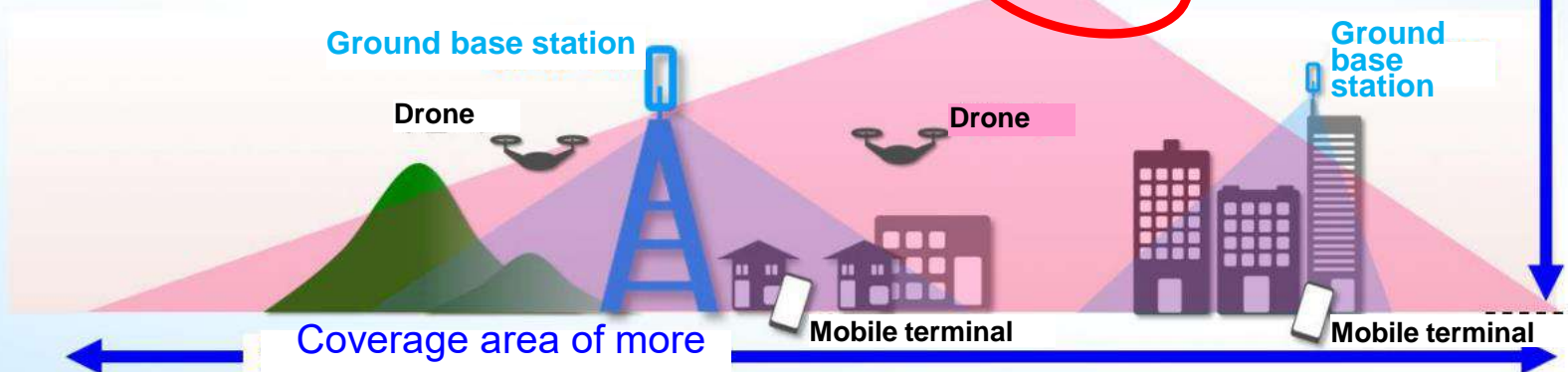


Ground base station

Coverage area of more than 100 km

Mobile terminal

Mobile terminal



Beyond 5G

Further enhancing 5G's characteristic features

1. Ultra High Speed & Ultra High Capacity

- Network Access: **10x Faster than 5G**
- Core Network Access: **100x Faster than now**

2. Ultra Low Latency

- Latency: **1/10 of 5G**

3. Ultra Massive Connectivity

- Simultaneous Connectivity: **10x more than 5G**

5G

7. Ultra Security and Ultra Reliability

- Always Ensuring Cybersecurity
- Instant Recovery from Disaster/Failure

6. Autonomy

- Autonomous coordination among devices without manual intervention

5. Scalability

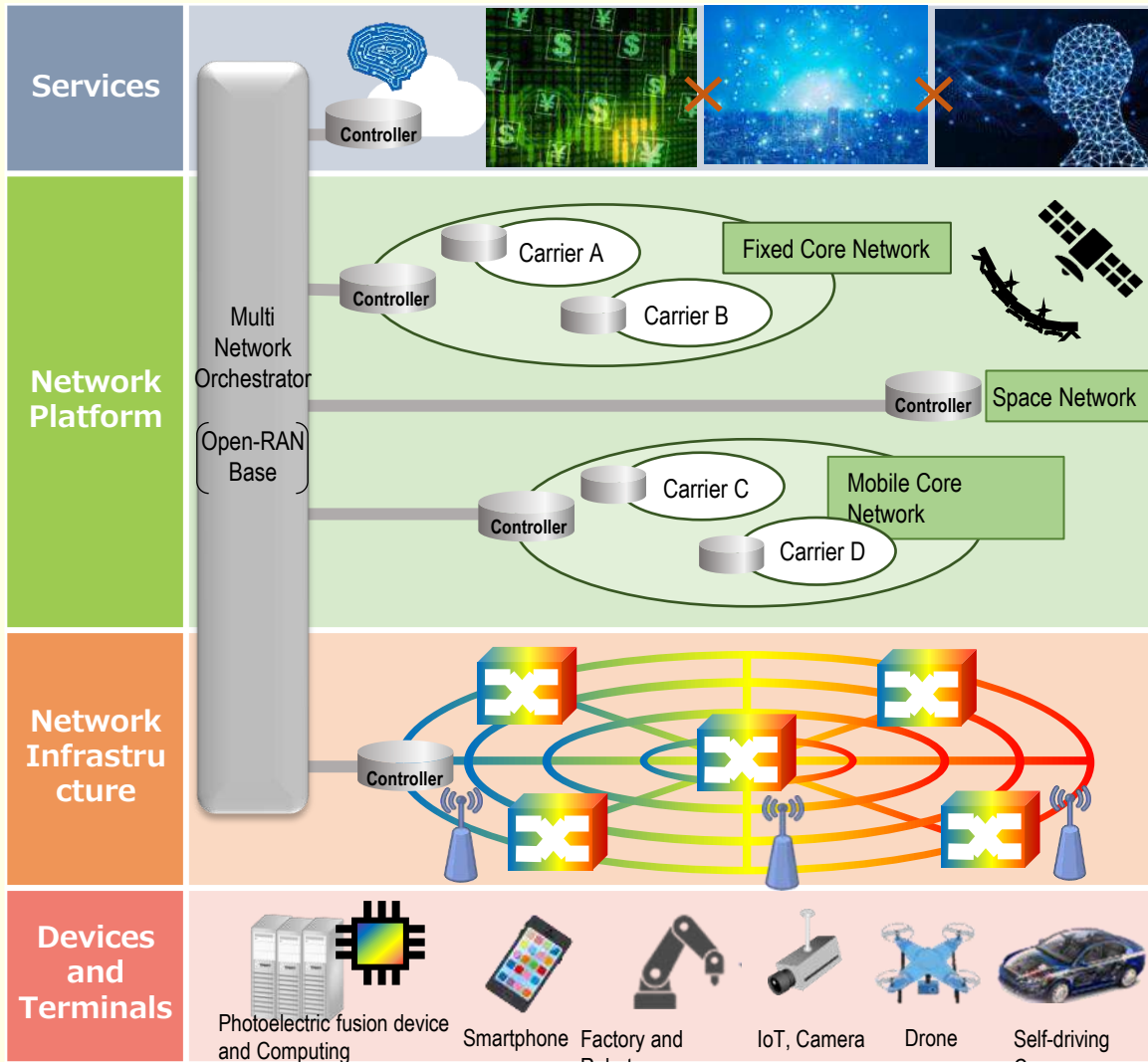
- Interconnecting devices to communicate anywhere

4. Ultra Low Power Consumption

- Power Consumption: **1/100 lower than now**

Beyond 5G

Adding new features that contribute to the creation of new value



Innovative and attractive services and content are expected to flourish.

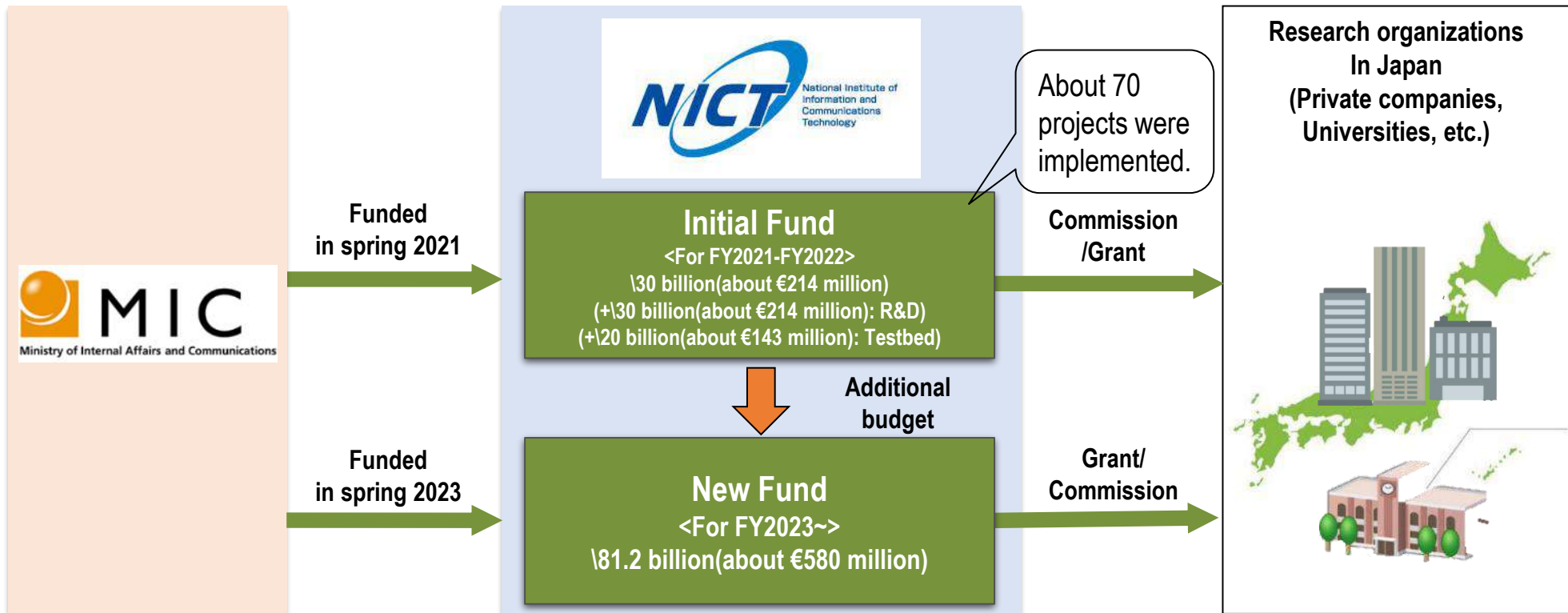
- <Key concepts and elements >
- Not only RAN* but also whole network architecture should be considered.
 - End to end high-capacity and ultra-low latency networks are desired.
 - Energy efficiency should be realized throughout the networks.
 - Communication coverage areas are expected to expand to sky, ocean, and space.
 - Security and resilience are essential factors.

Support variety of mission-critical devices/systems/services

RAN: Radio Access Network

- Japan launched a fund to support Beyond 5G R&Ds in spring 2021 with a budget of JPY 30 billion(about EUR 214 million).
- Bill to establish new R&D Fund was passed at the Diet in December, 2022.
- Additional budget of JPY 81.2 billion(about EUR 580 million) was added to the new fund in spring 2023 and MIC/NICT will support further Beyond 5G R&D projects/efforts.

EUR 1 = JPY 140



- On April 29 and 30, 2023, Japanese Government held the G7 Gunma Takasaki Digital Technology Ministers' Meeting in Takasaki City, Gunma Prefecture.
- As a result of this meeting, “Ministerial Declaration The G7 Digital and Tech Ministers’ Meeting” was adopted, which includes “G7 Vision of the future network in the Beyond 5G/6G era” in the context of “Secure and Resilient Digital Infrastructure”

※In addition to representatives from the G7 countries and the EU, representatives from India, Indonesia, Ukraine, ERIA, ITU, OECD, the United Nations and the World Bank also participated.

Ministerial Declaration of The G7 Digital and Tech Ministers’ Meeting (Excerpt)

20. In addition to these efforts to improve security and resilience of current digital infrastructure, we note the importance of sharing a vision for the next generation network in the Beyond 5G/6G era, and **endorse the G7 Vision of the future network in the Beyond 5G/6G era**. We are committed to enhancing cooperation on research, development, and international standards setting, toward building digital infrastructure for the 2030s and beyond. [Annex 2]



G7 Vision for future networks in the Beyond 5G/6G era [Annex 2]

We share a common vision for future networks with the following elements.

① End-to-End High-capacity and Ultra-low latency :

Not only radio access network but also the whole network architecture should be considered in designing and developing critical technologies and standards for future networks.

② Energy Efficiency and Environmental Impacts :

In order to minimise, the energy consumption and environmental impacts associated with increased data traffic, a significant reduction in overall network power consumption and development of eco-designed network equipment are essential factors for a sustainable digital society.

③ Multi-layered network :

Network connectivity should be enhanced through developing and deploying multi-layered networks with terrestrial networks, submarine cables, and non-terrestrial networks (NTN) such as Low Earth Orbit (LEO) Satellites and High-Altitude Platform Station (HAPS), and we recognise the importance of seamless interoperability between these networks.

④ Frequency Efficiency :

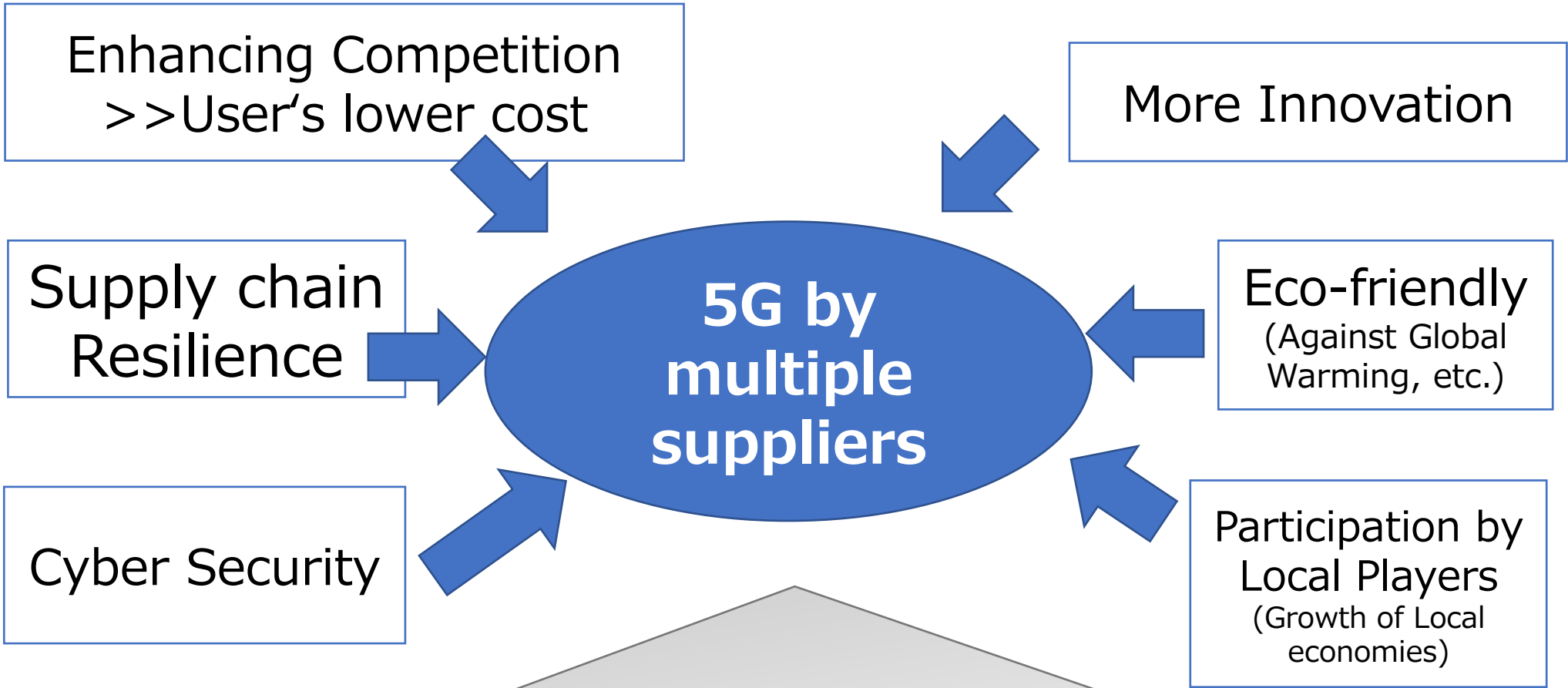
With smaller cell diameters in the same spectrum a higher frequency reuse rate can be achieved. This may reduce the energy consumption of mobile networks, such as Beyond 5G/6G networks.

In addition to the above elements, we recognise that openness, interoperability, and modularity are important elements of future networks in the Beyond 5G/6G era.

G7 Action Plan for Building a Secure and Resilient Digital Infrastructure [Annex 3](Excerpt)

We endeavour to enhance cooperation on research, development, and international standardization, toward building digital infrastructure in the Beyond 5G/6G era. In that regard, we recognise the importance of measuring and monitoring the evolution of energy consumption and environmental footprint indicators through recurrent data collection and use of indicators based on known and stable methodology.

3. Secure and Trusted Network

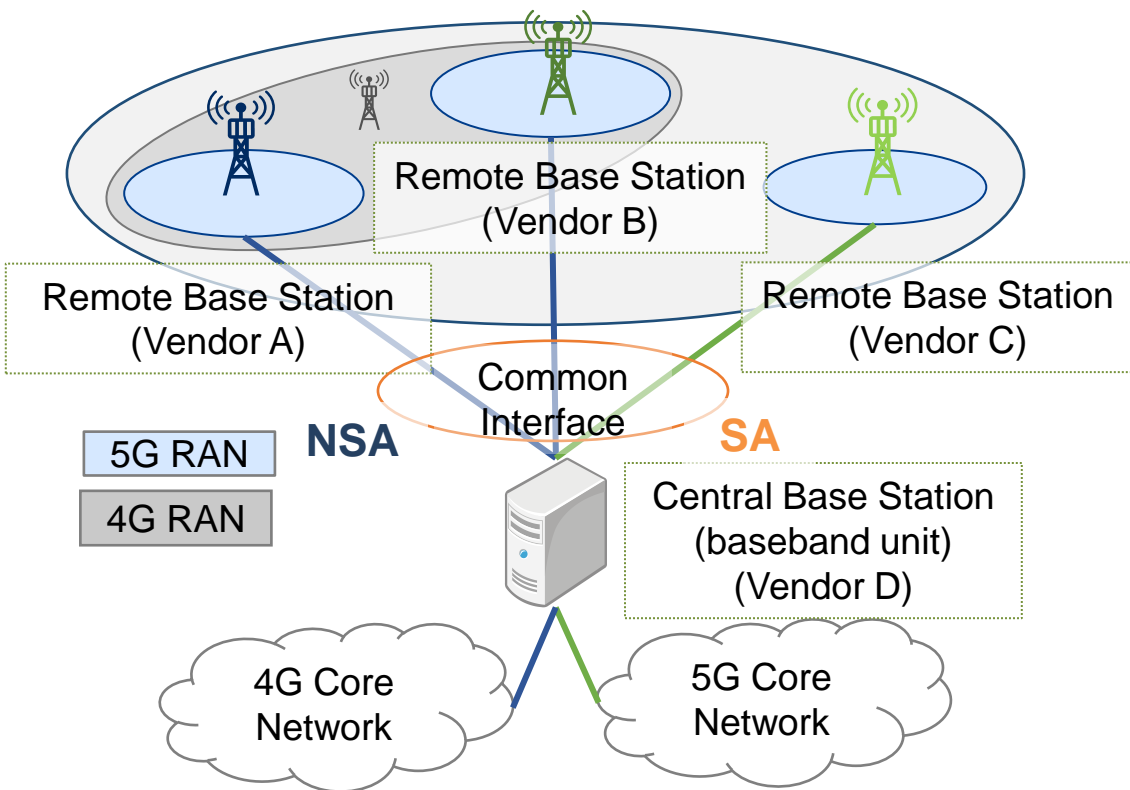


5G is a basis for our social and economic activities, also for nations

Open Architecture: O-RAN Activities

- Major operators in cooperation with vendors have been promoting O-RAN (Open Radio Access Network) for 5G networks in order to address vendor lock-in issues in RAN.
- O-RAN promotion will make operators' procurement more flexible, which will contribute to 5G supply chain risk management and deployment cost reductions.

Realizing Multi-vendor RAN by O-RAN specification



O-RAN Alliance Members (Excerpt)*



Operators (29 companies) *As of August 2021



Contributors, Vendors and Academics, etc. (273 companies)

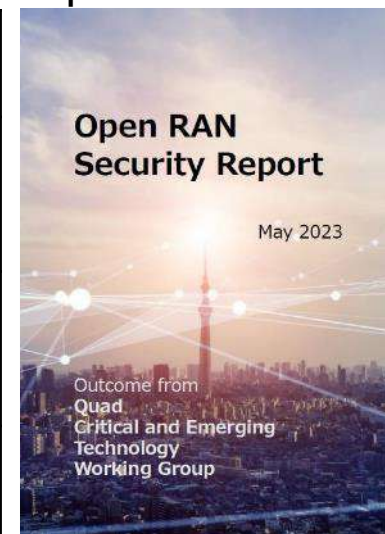


Outline of the Quad Open RAN Security Report

- As a response to the growing interest in the security of Open RAN, this 160-page report analyzes **the advantages, challenges and possibilities of overcoming challenges of Open RAN** compared to traditional RAN through **objective research and analysis including technical demonstration**.
- Released as one of the outcomes of the Quad on May 2023, based on the “Memorandum of Cooperation on 5G Supplier Diversification and Open RAN” of the **Quad Critical and Emerging Technology Working Group**.

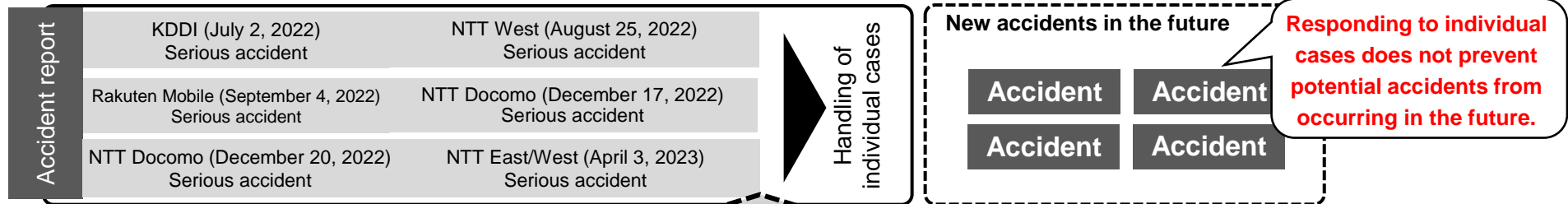
<Advantages, challenges and possibilities of overcoming challenges of Open RAN>

Advantages	Security	Easier risk management due to improved transparency, etc.
	Others	Reduction of supply chain risk and avoidance of vendor lock-in due to reduced dependence on specific suppliers, etc.
Challenges	Approximately 4% of security risks analyzed in this report are unique to Open RAN (i.e., not also present in traditional RAN), based on inclusion of new interfaces/components.	
Possibilities of overcoming challenges	Possible to reduce risks unique to Open RAN and achieve security level equivalent to traditional RAN , by meeting the security requirement in standards and the checklist attached to this report . Note: Security of Open RAN can be further enhanced by activating optional security procedures.	



Cover of the report which was published as an outcome of Quad

➔ **Use of Open RAN does not fundamentally alter the security risk landscape for telecommunications, compared to traditional RAN**, given the objective analysis as above of the advantages, challenges and possibilities of overcoming challenges.



Structural issues that cause many accidents

- 1) Insufficient identification of potential risks of telecommunication facilities
- 2) Inadequate system maintenance and management system and internal information sharing system
- 3) Insufficient education and training 4) Delay in initial notification to users
- 5) Insufficient measures through cooperation among operators, and other factors

New initiatives

■ **The following initiatives will be implemented** to address structural issues and improve the root causes of consecutive accidents.

1. Structure Problem evaluation

Verification of structural problems [Report compiled in March 2023]

- ✓ The Telecommunications Accident Verification Meeting Body will examine structural problems, including organizational and systemic issues behind each accident, and consider appropriate monitoring rules.

2. Protection of users' interests

Strengthening of publicity and awareness among users

[A report was compiled in January 2023, and guidelines were established in March 2023]

- ✓ The environment should be improved regarding the content of publicity and information provided by telecommunications carriers in the event of an accident, the diversification of means of information transmission, the emergency contact system for related organizations, etc.

3. Securing alternative means

Realization of intercarrier roaming, etc., in emergencies

[First report compiled in December 2022]

- ✓ In order to secure means of communication in emergencies, the introduction of inter-carrier roaming for cell phones and other measures were discussed. The second draft report was under public comment process from May 24 through June 15, 2023.

5. International Cooperation

<About IGF>

- One of the **most important conferences concerning public policy issues relating to the internet, hosted by the United Nations**, where all stakeholders, including governments, the private sector, the technical and academic communities, and civil society, **engage in dialogue on an equal footing**.
- Japan is to host the 2023 meeting. (The meeting has been held once a year since its establishment in 2005.)

● **Date:** Sunday, October 8 – Thursday, October 12, 2023 (5 days)

● **Location:** Kyoto International Conference Center (Kyoto City)

● **Participants:**

Estimated 5000 on-site participants from industry, government, academia, etc.(+ online)

Expected to include Prime Minister Kishida, UN Secretary-General Guterres, cabinet-level officials from various countries, and members of Congress.

● **Main Theme: 「The Internet We Want - Empowering All People」**

Approximately 300 sessions will be held simultaneously, including sessions by cabinet-level ministers and parliamentarians from various countries on the Parliamentary track.

<Key topics of discussion(tentative)>

- Freedom of speech and expression, disinformation, data distribution, data governance
- Personal data protection, online human rights protection, critical infrastructure protection, cybersecurity
- Universal access and connectivity, literacy, human resource development and capacity building
- Platform regulation, competition policy, content management and protection etc.



The 2019 Meeting in Germany
(then Chancellor Merkel and
Secretary General Guterres)

Thank You!!!



Broadband for All The French tour

26 juin 2023

Plan

1. The mobile market
2. The fixed market
3. Sustainability

The mobile market

Status of the *New Deal Mobile* at December 31, 2022

Achievements – December 2022



Prospects



Generalization of 4G

- **[98,6-99,4] %** of all the network is equipped with 4G
- Almost **96 %** of populated areas which were identified as 'Zones blanches' are covered with 4G



Enhancing the quality of mobile networks

- **[99,5-99,7] %** of the population benefits from 'good coverage'^{**}



FWA (4G)

- **FWA on 4G** available in **427 areas**
- **971 more** areas are identified by Orange and SFR



Coverage of the road system

- **Between 99,2 % and 99,9 %** of main roads identified^{**} as a priority for 4G are covered

- **100 %** of populated areas which were identified as 'Zones blanches'

- From **99,6 %** to **99,8 %** of the population benefiting from « good coverage » between 2024 and 2031

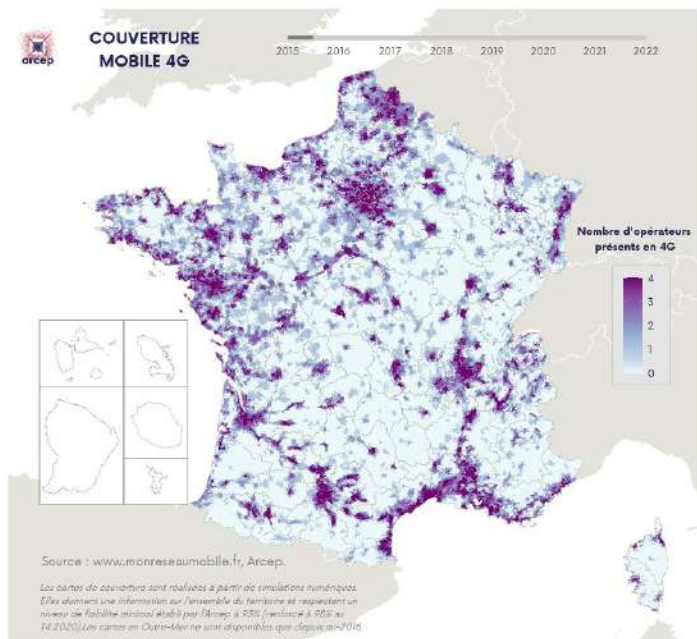
- **FWA** will be available in **544** by the end of 2023

*Possibility to receive and send data outdoors

**Identified by the government: roads between cities of a certain size on which more than 5 000 vehicles run every day (average on one year).

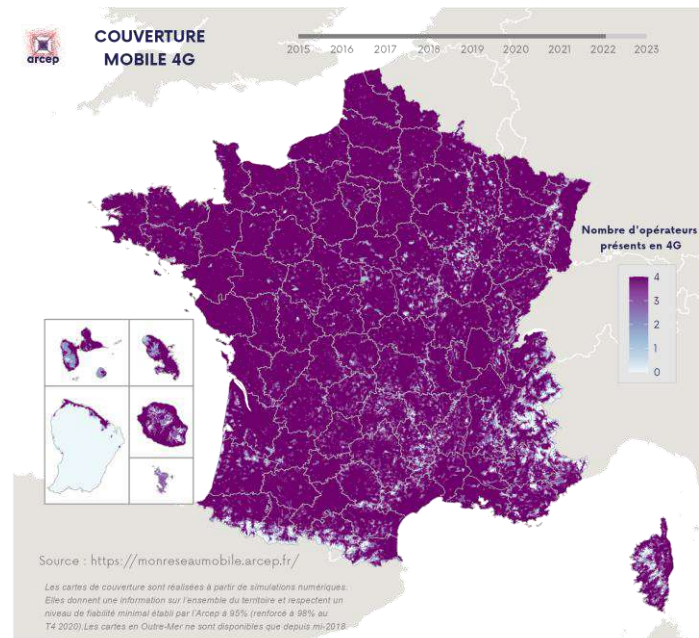
Evolution of 4G coverage between 2015 and 2022

Q2 2015



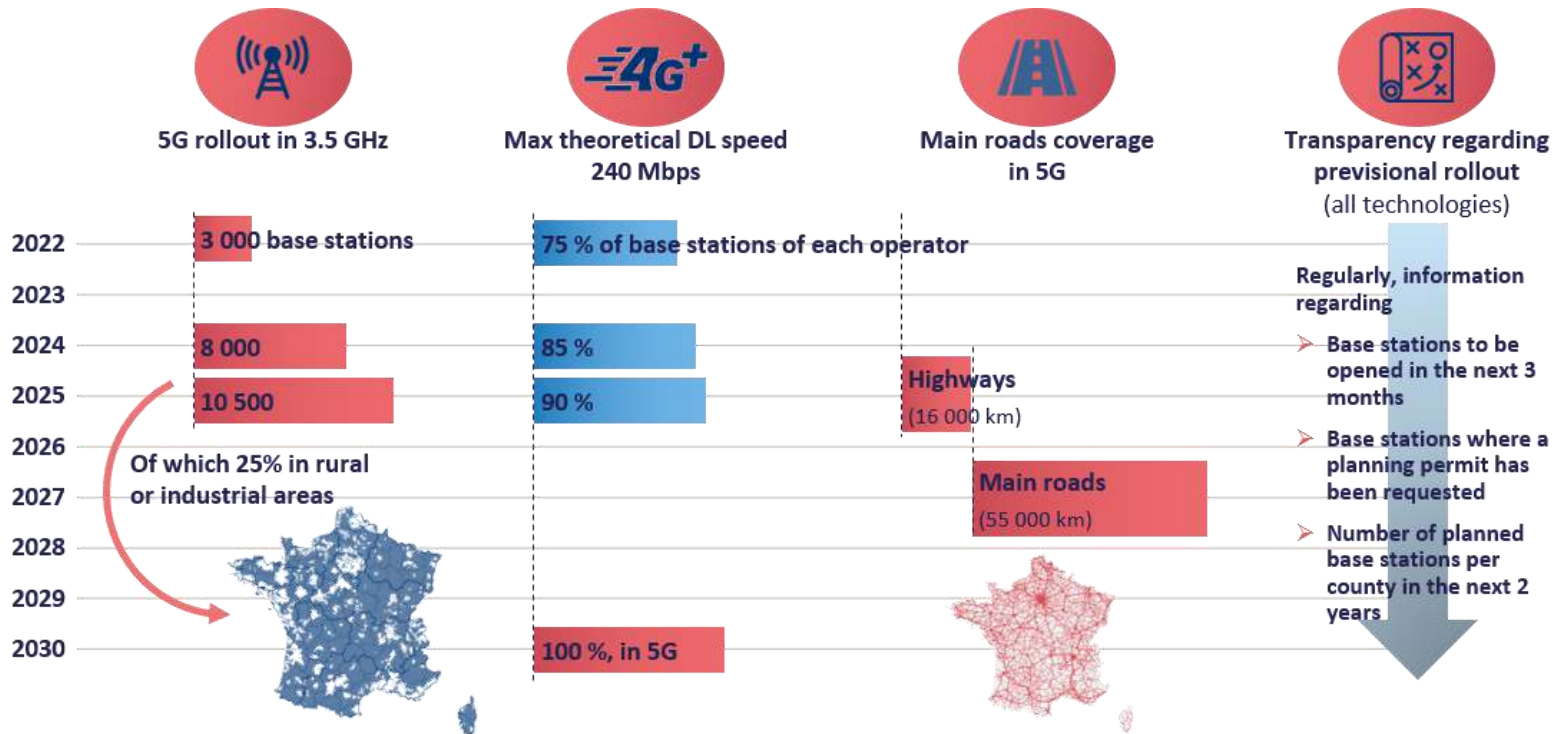
Between **52 %** and **76 %**
of the population covered by each operator

Q4 2022



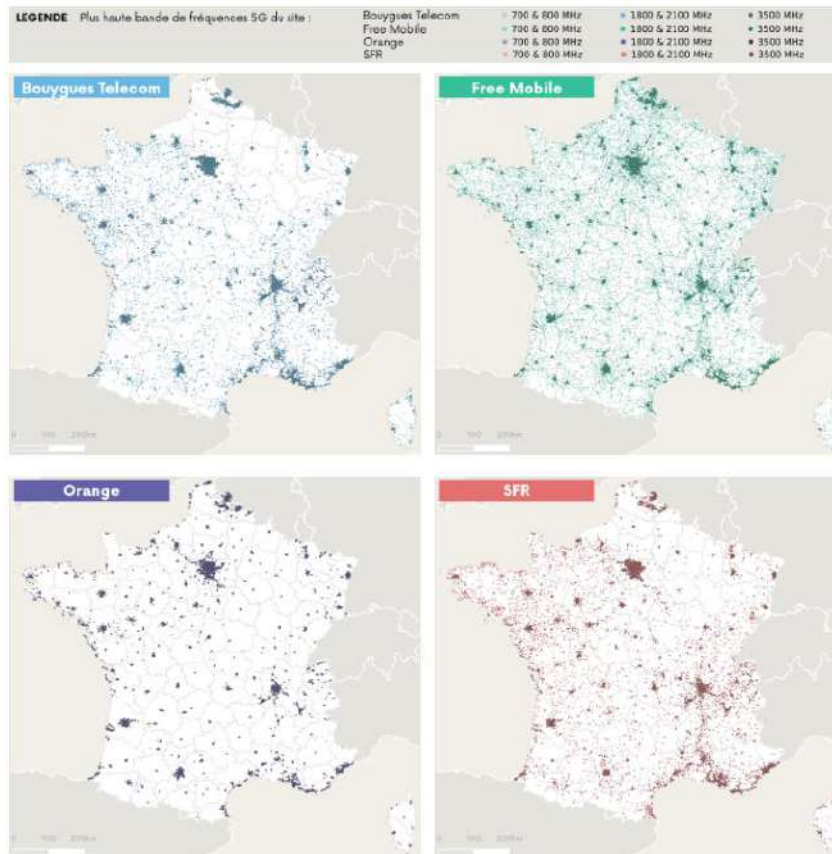
Between **99,2 %** and **99,8 %**
of the population covered by each operator

Rollout obligations linked to the 3.5 GHz licenses



Where are we now with 5G : base stations open commercially

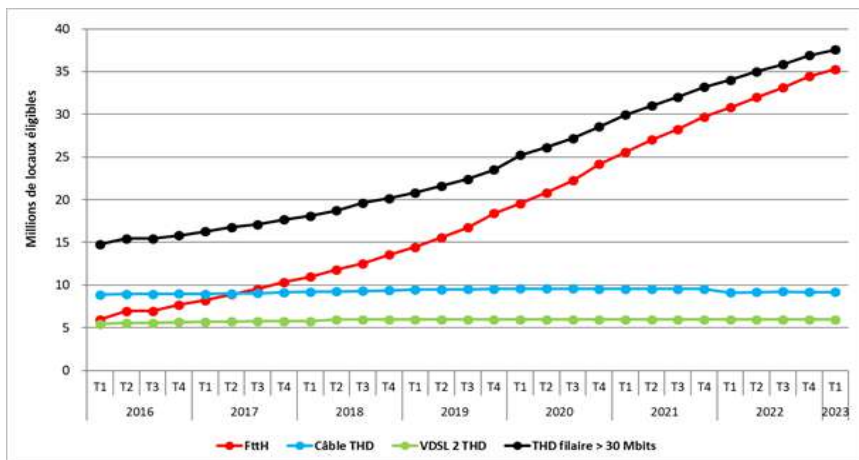
5G : number of base stations open commercially



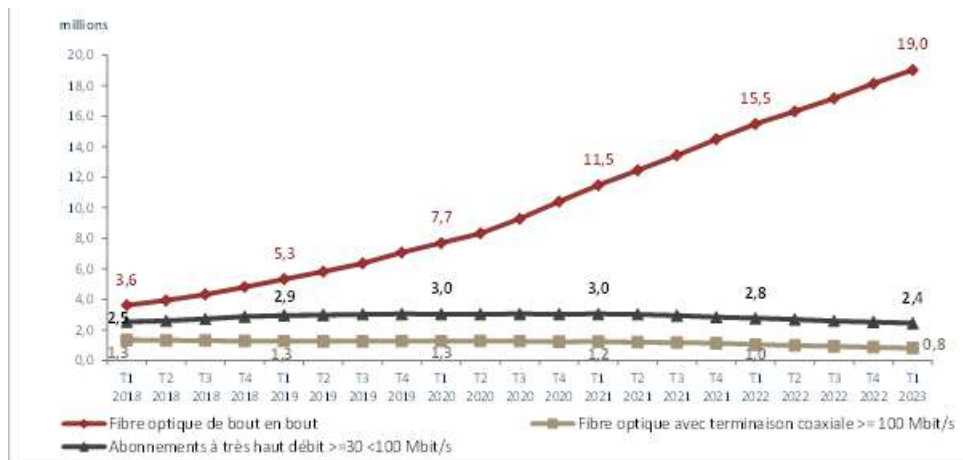
The fixed market

Where are we now with FttH : roll-out and take-up

Evolution of coverage



Evolution of the number of subscriptions



Challenges of the 7th cycle of market analysis

- **Challenge n° 1:** support the transition from copper to fiber;
- **Challenge n° 2:** maintain sufficient quality of service on copper during the transition, particularly in areas still dependent on it;
- **Challenge n° 3:** facilitate the completion of FttH network rollouts by ensuring effective access to physical civil engineering infrastructures.
- **Challenge n° 4:** improve competition on the business market.

ICT environmental footprint : a new chapter of Arcep's regulation

Why Arcep got interested in the impact of digital on sustainability?

- ❑ Digitalization is transforming our lifestyles and contributes to the decarbonization of other sectors.
- ❑ Its development implies: **growth** in data volumes, increased network and **data center capacities**, rapid **renewal** of devices and **low recycling rates...**
- ❑ All these factors led **Arcep to question the environmental footprint of digital technologies.**
- ❑ Arcep positions itself as a **neutral expert**. Its works aim at better assessing and measuring the impact of the digital sector on environment and its determinants, so as to identify levers of actions to reduce its environmental footprint.

Genesis of Arcep's step-by-step approach

- ❑ **2018:** a [new cycle of inquiries](#) to anticipate how networks are likely to evolve over the next five to ten years, **including the digital environmental impacts**. Bilateral interviews with stakeholders.
- ❑ **2019:** public release of a paper on the [digital carbon footprint](#) (in French)
- ❑ **2020:** [Arcep launches a collaboration platform](#) devoted to “Achieving digital sustainability” – **calling on all interested associations, institutions, operators, digital industry businesses, academics and experts to contribute to the platform through collaborative workshops:**
 - This collaborative approach with the digital ecosystem led to a report : [“Achieving digital sustainability” report](#) (in English) with **11 proposals** for successfully combining the ongoing increase in the use of digital tech and reducing its environmental footprint.
- ❑ **Ongoing work with a number of public and private players**, including ADEME, the French agency for ecological transition. This collaborative, step-by-step approach has resulted in :
 - **ADEME-Arcep’s “Assessment on the digital environmental footprint in France and prospective analysis”**
 - **Other workstreams such as its annual survey “Achieving digital sustainability” or the technical expert committee (see next slides)** which led to a report published in March 2023 providing a methodological gap analysis on ICT sector environmental impact assessments, including a proposal to modify the ITU recommendation specifying the methodological approach to be followed to assess the carbon footprint of the ICT sector using a life-cycle approach.

Arcep's annual survey «Achieving Digital Sustainability»

- ❑ Since 2020, Arcep has been working on the implementation of an annual publication based on the collection of environmental data from digital stakeholders: **Arcep's annual survey «Achieving Digital Sustainability»**
- ❑ This survey aims to:
 - Improve measurement to better assess environmental issues, **inform public authorities** and allow the implementation of appropriate measures.
 - Provide **incentives for economic actors** to behave virtuously.
 - **Empower consumers** through data release
- ❑ March 2020, Arcep began its environmental data collection from **the main telecommunication operators** → publication of **the first edition of the annual survey «Achieving Digital Sustainability» in April 2022** covering 3 categories of indicators: **greenhouse Gas (GHG) emissions, network energy consumption, mobile phones (sales, collection, recycling, refurbishing)**.
- ❑ Arcep's environmental data collection powers were extended by law in December 2021. Consequently, the collection of environmental data from the main telecom operators has been enriched with new indicators on the **reconditioning and refurbishing of internet and set-top boxes** → publication of the 2nd edition of the annual survey in April 2023. **A 3rd edition extended to terminal manufacturers and data centers operators will follow** in the end of 2023.
- ❑ The aim is to **build environmental indicators** (power consumption, greenhouse gas emissions, sales of refurbished terminals) from the data collected: **the data is collected directly by Arcep from digital players**, and the indicators are built by Arcep using a **transparent method that is monitored over time**.

Technical experts committee (sustainability): methodological gap analysis on ICT sector environmental impact assessments

□ An 3-steps approach :

- Build an analysis matrix to look at the compliance requirements according to the ITU standards on ICT sector environmental assessments methodology (ITU-T L.1450 recommendation)
- Illustrate the practicality of this recommendation through a sample of 3 studies to address a wide spectrum of point of view : industrial (Ericsson), think tank (The shift project) and institutional (ADEME-Arcep)
- **Provide insights and recommendations in order to improve existing referential while aiming exhaustivity and operationalization of the latter**
- **ITU-T SG 5/Q9 will launch a workstream to update the L.1450 recommendation in particular in order to improve its workability and applicability**

□ **The committee has chosen different studies (research institute from the industry, environmental think-tank, public institution) to reflect a large spectrum of point of views and authors of these studies are members of the committee**

ADEME and Arcep's study: Digital environmental footprint in France in 2020 (parts 1 et 2 of the study)

□ Part 1 : Methodology (Life cycle analysis)

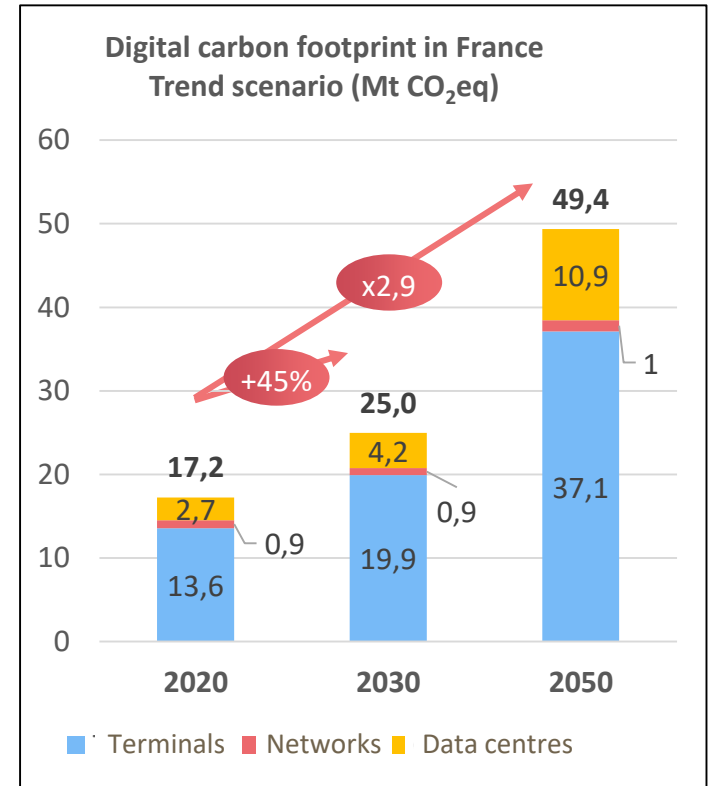
- **Multicriteria:** 12 criteria of environmental impact (carbon footprint, minerals & metals depletion, etc.).
- **Multi-component:** devices, networks and datacentres.
- **Multi-stage:** manufacturing, distribution, use, end of life.

□ Part 2: assessment of the digital environmental footprint in France in 2020

- The digital carbon footprint accounts for 2.5% of the carbon footprint in France (17,2 MtCO_{2eq}).
- **Devices** (displays, televisions, smartphones and computers in particular) are responsible for 65% to 90% of the environmental footprint, depending on the environmental indicator considered.
- **Minerals and metals depletion**, in addition to carbon footprint as well as energy consumption, emerge as relevant indicators of impact to describe the digital environmental footprint.
- **Manufacturing and use phase account for almost all** of the impact on the environment.

ADEME and Arcep's study: Prospective analysis to the 2030 and 2050 horizons (Part 3)

- ❑ In addition to the 2020 assessment, projections of the environmental footprint of the digital sector were made
- ❑ If nothing is done the carbon footprint of the digital sector could rise by 45 % to 2030 and could triple in 2050
- ❑ There is also at stake the issue of metals and minerals availability
- ❑ The prospective analysis identifies key levers of action to reduce the environmental footprint : a combination of eco-design and sobriety measures is necessary to reduce the digital environmental footprint



ADEME and Arcep's study 2030 scenarios reflect different technological choices and users' behaviours



2020-2030 evolutions



Devices' fleet



Lifespan



Consumption per device



Data traffic

Trend scenario :

Current trends continue at the same pace



+65% including IoT

=



-10%



+20%/year

Moderate eco-design scenario:

Incremental improvements of devices



+1 year



-33 %



Advanced eco-design scenario:

Significant improvements of devices



+2 years



-50 %



Sobriety scenario:

Adoption of ecofriendly behaviours stakeholder of all types (end-users, market players, public institutions, etc.)

=

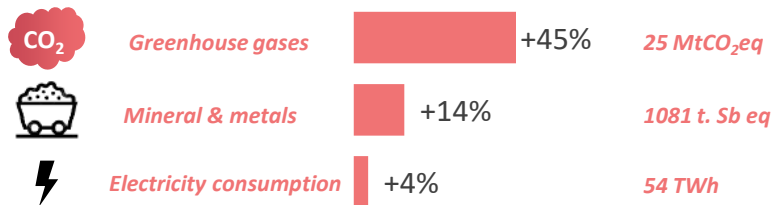
+2 years



ADEME and Arcep's study 2030 results: only the pairing of sobriety and eco-design measures can lead to a decrease of the digital environmental impact

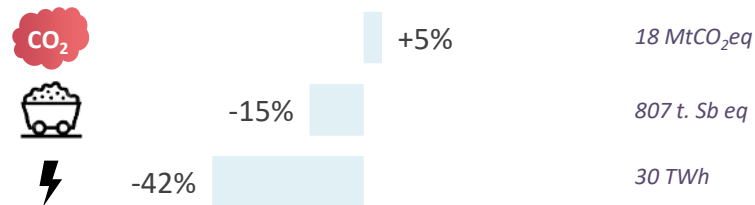
Trend-based scenario

With the current trend of devices replacement and **if nothing is done, the digital environmental impact will grow**



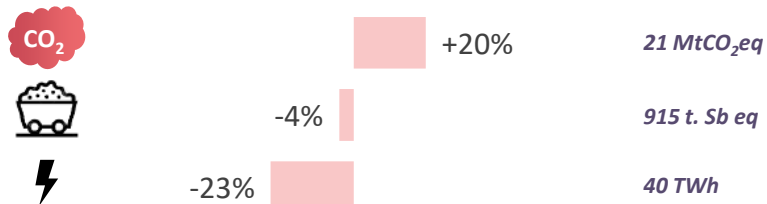
Advanced eco-design scenario

Holding this growth by pushing forward those two measures (extending devices lifetime by 2 years, further energy efficiency improvements) :



Moderate eco-design scenario

Restricting this growth by extending devices the lifespan by 1 year as well as improving energy efficiency:



Sobriety scenario

Reducing the impact by combining these previous measures with a stabilisation of the devices' fleet



ADEME and Arcep's study: conclusion of 2030 and 2050 prospective analysis

- ❑ A rigorous method to **assess the digital environmental footprint** based on a **multicriteria and multicomponent lifecycle** analysis
 - A **prospective work** with inherent limits detailed in the report
 - A prospective analysis identifying **levers of action to reduce the digital environmental footprint**
- ❑ If no action is taken to contain ICT's growing impact on the environment, **digital carbon footprint could triple between 2020 and 2050**
- ❑ In addition to carbon footprint, the study points to another significant impact of the digital environmental footprint which is the **depletion of abiotic resources (minerals and metals)** and the issue of their availability on the long term

ADEME and Arcep's study: conclusion of 2030 and 2050 prospective analysis

- ❑ **Combine sobriety with eco-design measures** to reduce the digital environmental impact:
 - **Level off the number of devices and extend device lifespan** both with eco-design (enhanced repairability, durability, etc.) and involving every stakeholders of the value chain (end-users, market players, public institutions, etc.)
 - **Eco-design of devices and digital services** to be more efficient everything else equal (i.e. considering iso-use)
 - **Involve and raise awareness among every stakeholder of the value chain (end-users, market players, public institutions, etc.) and foster sobriety**
- ❑ **Necessary commitment of all stakeholders for a sustainable digital economy** (devices and equipment manufacturers, content and application providers, network and data centre operators, users) **because of interdependencies and crossed-effects.**
- ❑ **Everybody has to take its part to achieve digital sustainability if we are to meet the Paris Agreement target by 2050**

Thank you for
your attention



Emmanuel Gabla



DEVELOPMENTS IN SPECTRUM MANAGEMENT FOR COMMUNICATION SERVICES

Verena Weber, Dr. – Head of the Communication Infrastructures and Services Policy (CISP) Unit, OECD

Broadband for All Event
Stockholm, 26-27 June 2023



The value of spectrum for society

Spectrum: The invisible engine of digital transformation

- **Spectrum** is the **primary essential input** for **wireless communications**: Necessary to ensure **Broadband for All**
- Spectrum is used for a wide variety of applications across all economic sectors that **enable our globalised & digital** world
- Spectrum management impacts the cost of network deployment and is an important tool to regulate competition in mobile markets
- ➔ Its **timely availability and efficient use** is crucial for society



All sectors of the economy, from education to health care, Industry 4.0, or SME productivity, **could benefit from more widely available access to spectrum**, including for the provision of affordable and high quality broadband services



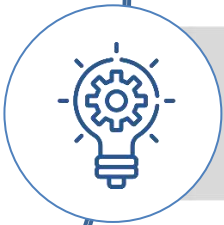
Key areas of the report “Developments in spectrum Management for Communication Services”



Importance of **efficient spectrum management**, the policy objectives guiding it, and the **rising challenges** for spectrum managers



Spectrum management approaches and tasks, including **harmonization, allocation and assignment** (licensing), with their respective **policy objectives** and **challenges**



Trends in **licensing** (including granular approaches and mmWave), developments in **flexible spectrum management approaches**, diverse models for **spectrum sharing**, and the role of **unlicensed spectrum**



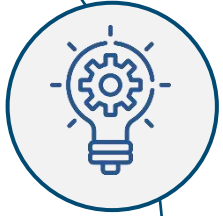
Looking ahead: Future considerations in spectrum management, including **new technological horizons** and the **environmental sustainability** of networks.



Policy vision guiding spectrum management



Ensuring efficient use of spectrum



Driving wireless innovation



Fostering affordable access



Harmonization



- The overall goal of increasing **economic & social welfare** can be broken down into several policy objectives
- **Spectrum policy “visions”** may differ (historical context)
- **Approaches** to spectrum management **embed the policy objectives** through measures:
 - Increasing **availability** of spectrum
 - Placing spectrum in the market & fostering its **efficient use**



Evolution in spectrum management: From “command and control” to flexible licensing frameworks

Early 90s

Mid-90s

2000-2010

2010-2020

2020s



“Pure command and control”

Market based approach to licensing introduced

Promotion of market-based assignments (e.g. auctions)

Flexible approach: shared use of spectrum

Balancing flexibility for innovation and investment certainty

How to balance competing demands?

How to adapt licensing for higher bands (mmWave)?



Allocation, harmonization, and licensing (assignment)

Spectrum allocation & the importance of harmonisation

Towards WRC-23

Spectrum assignment (licensing) procedures & embedded policy considerations in their design:

Coverage obligations

Spectrum caps

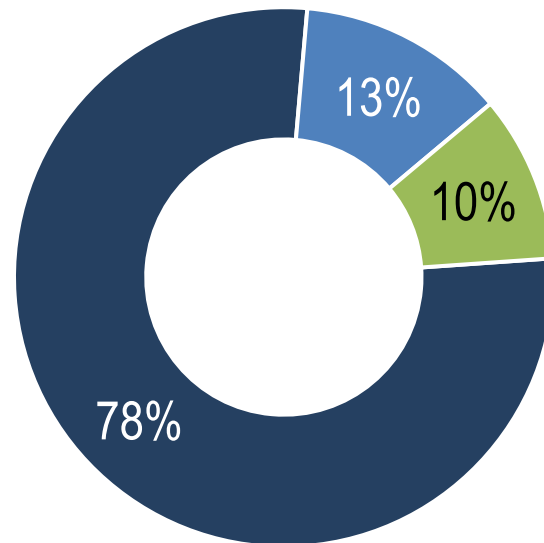
Reserving blocks

Licence renewal policies



Allocation: A case study

Example: Allocation of the 6 GHz band across OECD countries, Brazil and Singapore (Sept. 2022)



- Unlicensed use lower half 6 GHz band
- Unlicensed use full 6 GHz band
- In consultation/ considering allocation

Source: OECD based on questionnaire responses (Updated until 27 Sep 2022)

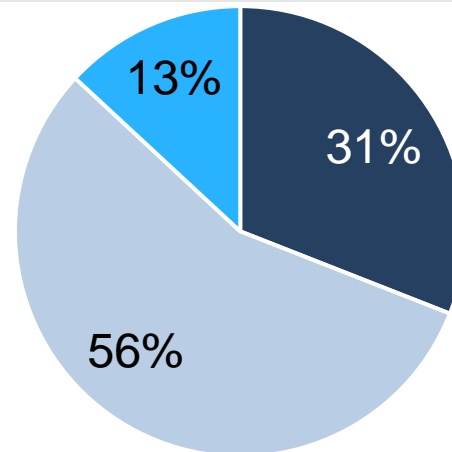


Assignment: Spectrum auctions in practice

Spectrum auctions [IMT] across the OECD and Brazil since 2016

Frequency ranges auctioned during 2016-2021

- Low range (< 1GHz)
- Mid-range (>1 GHz, <6 GHz)
- High range (> 6GHz)



Source: OECD elaboration



Auctions in practice: Auction design determines outcome (spectrum pricing)





Trends in spectrum management: Towards more flexibility

New approaches to promote efficient use of spectrum



- **Flexibility** in licensing to cater to different needs
- Developments in **mmWave & private networks**
- **Spectrum sharing** & other innovative approaches
- The role of **unlicensed spectrum**



Trends in spectrum management: Developments in licensing, towards granular approaches

Are current licensing frameworks fit for purpose as we go towards higher bands (e.g. mmWave)?

5G commercial deployments in **36/38 OECD countries** (June 2023): Most relying on mid-range and lower-bands (sub 6 GHz), and a few mmWave (e.g. US, AUS, JAP)

Approaches for mmWave licensing

National Licence

(e.g. SI, GR, JP, KR)

Hybrid approach, i.e. national + local

(e.g. DK, FI, AU)

National licence with club use

(e.g. IT)

Local licence

(e.g. DE, UK, LV)

mmWave



Availability of spectrum and wider channels that may increase spectral efficiency

mmWave



Propagation features requires network densification (\$ and energy)



Trends in spectrum management: Developments in licensing, towards granular approaches

Developments in granular approaches and a rising trend of private networks in recent years

Spectrum access models for private networks

Spectrum via MNOs
(slicing, specialised networks, etc.)

Local spectrum licenses
(e.g. DE, FR, KR)

Wholesale obligations
(e.g. CZ) or
use it or “lease it” club use licences (e.g. IT)

Shared approaches
(e.g. CBRS in US or LSA in the UK)



Trends in spectrum management: Approaches to shared use of spectrum by licensing model

Individual license

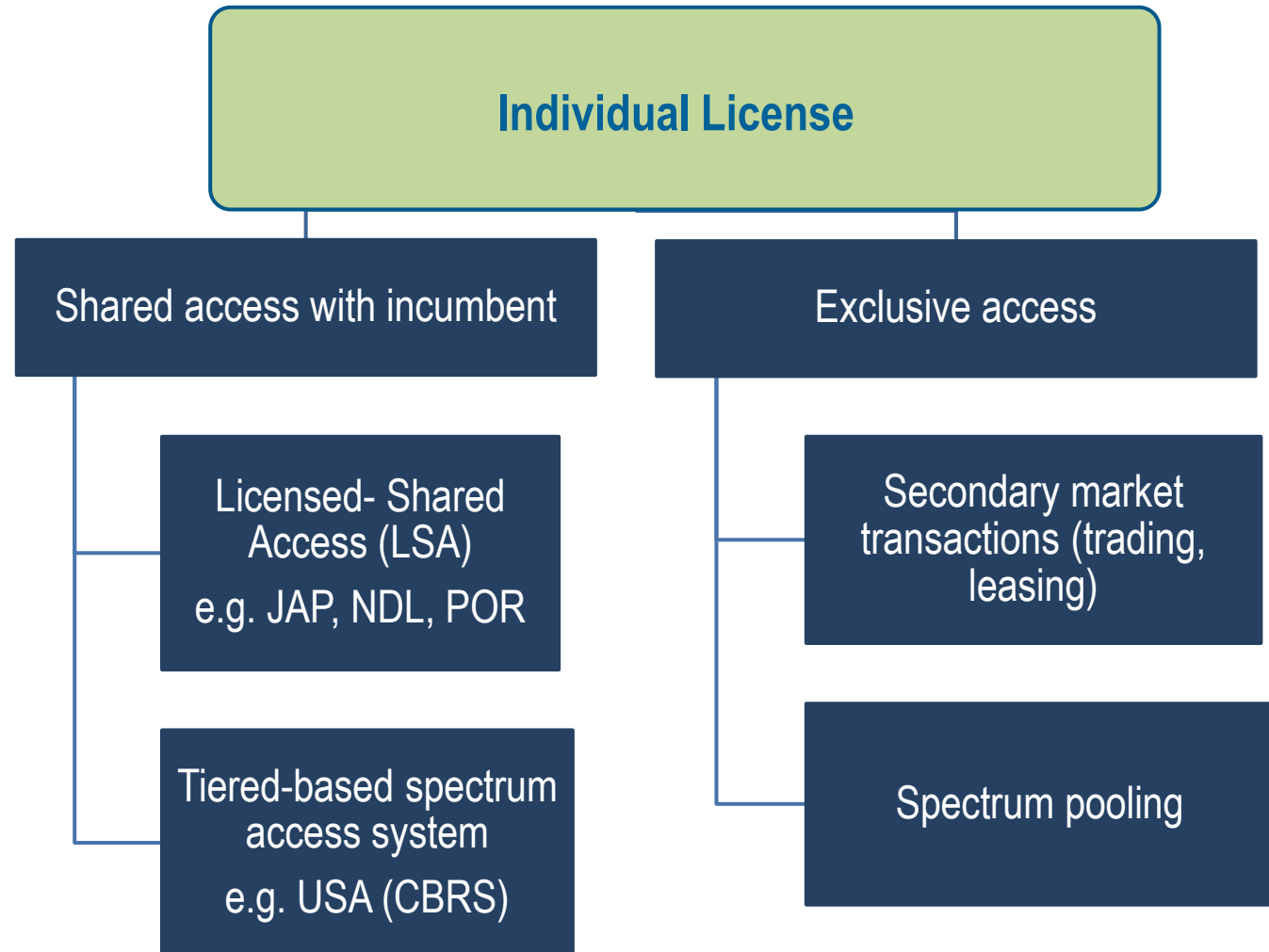
Access coordinated to allow incumbent use and shared use (static and dynamic approaches)

Light licensing

Increasing flexibility, usually larger number of users can access than sharing under individual licenses

License exempt

Most flexible model, unlimited users, bands shared by several applications and users





Trends in spectrum management: Approaches to shared use of spectrum by licensing model

Individual license

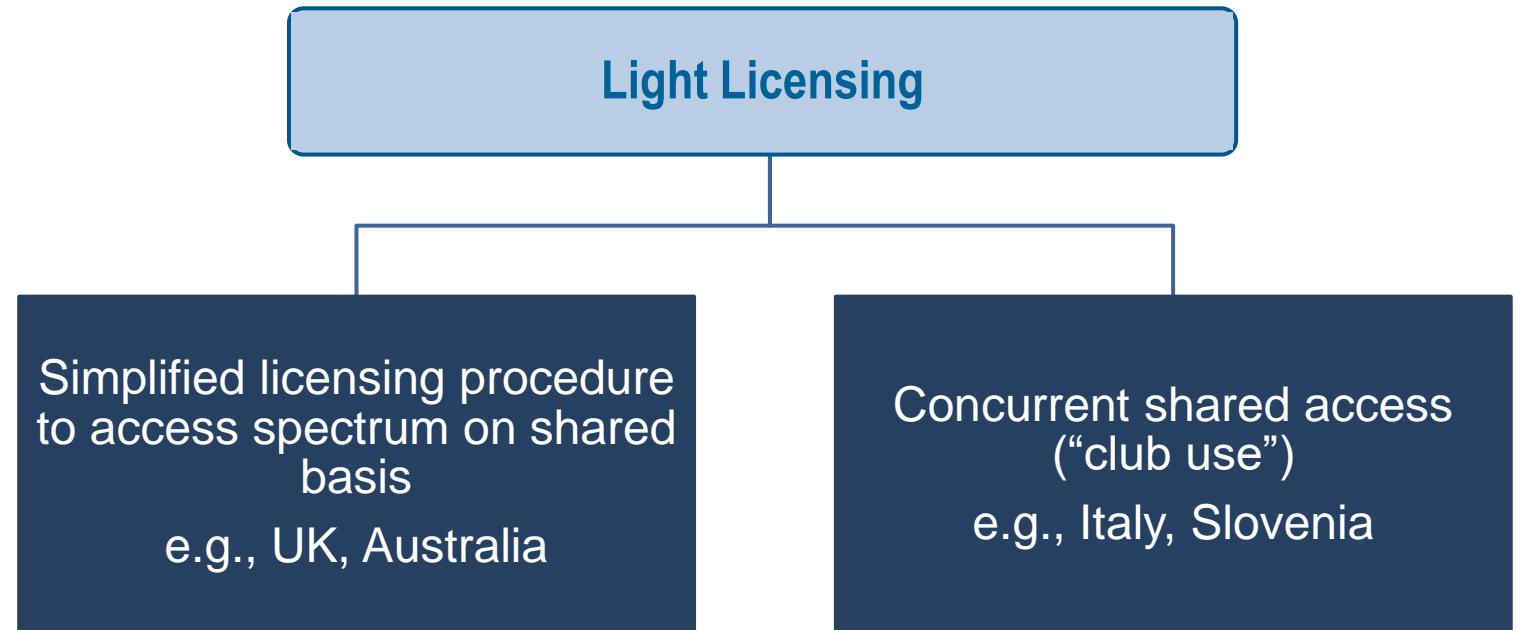
Access coordinated to allow incumbent use and shared use (static and dynamic approaches)

Light licensing

Increasing flexibility, usually larger number of users can access than sharing under individual licenses

License exempt

Most flexible model, unlimited users, bands shared by several applications and users





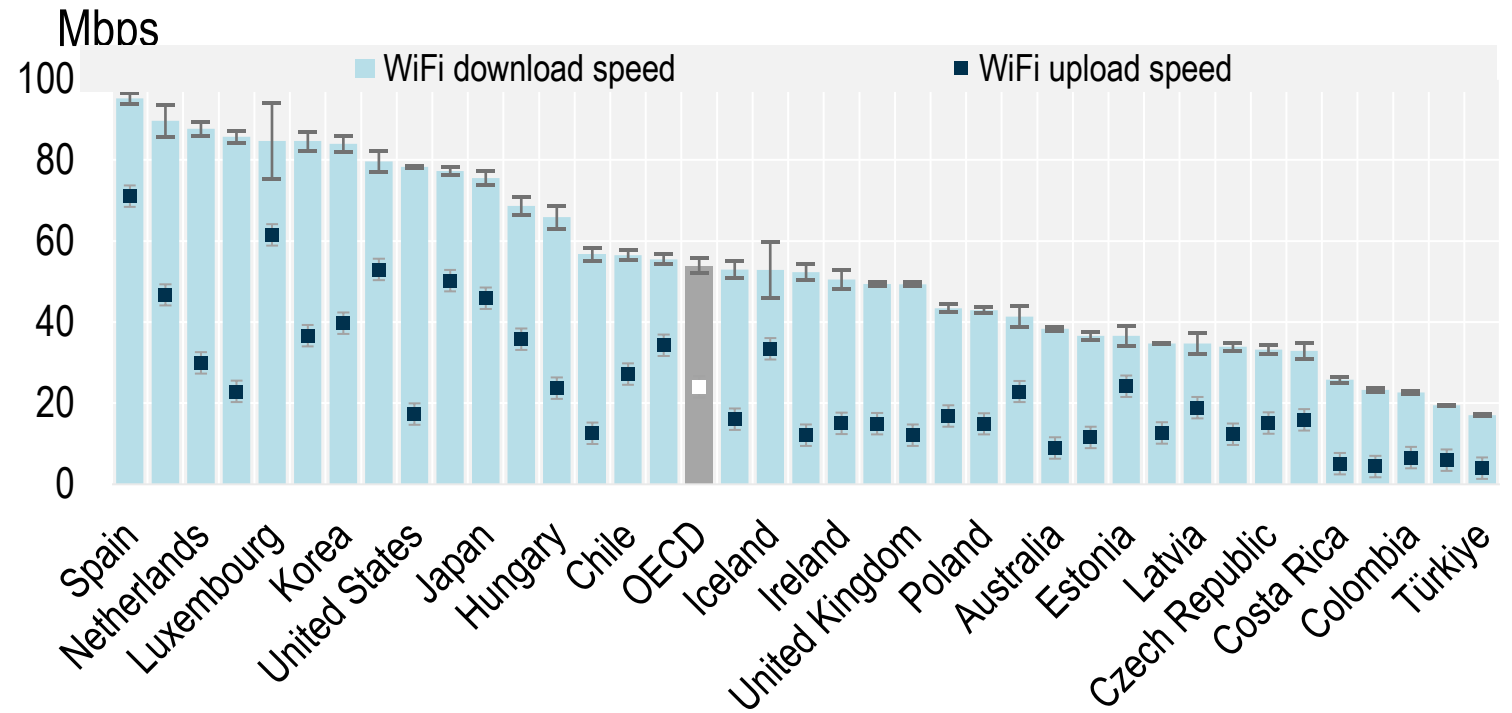
Trends in spectrum management: Spectrum sharing and unlicensed spectrum

Individual license

Light licensing

License exempt

Wi-Fi speeds experienced by smartphone users in OECD countries, 4Q 2021 (Opensignal)



Source: Opensignal



Future considerations in spectrum management



New horizons:

Fostering innovative use cases, drones, HAPS, NGSO satellite constellations, THz & beyond 5G technologies

Going ahead, policymakers may consider additional topics



Environmental sustainability of networks



Spectrum management and environmental sustainability

OECD countries have started to **study the impact of communication networks on the environment**, including with respect to spectrum management decisions (e.g. Ireland, France).

Two facets when considering **environmental sustainability of networks** and **the interplay with spectrum policy**:

1. Ensuring that communication networks are sustainable (how networks are rolled out)
2. The role of spectrum in monitoring our natural environment



Countries consider environmental sustainability in spectrum management decisions by:

- analyzing the environmental impact of the use of different spectrum bands,
- the impact of deploying base stations,
- the technology trends in the development of more energy efficient networks.





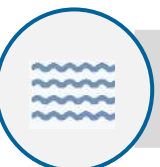



The mandate of spectrum managers and “green”

- At present, from a sample of 39 countries (comprised of 37 OECD countries, Brazil and Singapore), **49% take into account environmental considerations** (at least partially) **when managing spectrum.**
- Going forward, **the vast majority (74%) of countries** understand the importance of this issue, with many aiming to explicitly incorporate this objective as part of their spectrum management strategies.



Main takeaways

-  **Spectrum management vision:** increase **economic & social welfare** through **efficient** spectrum use
-  **Evolution of spectrum management:** Legal certainty through well-designed licensing regimes
-  **Auctions work, but design matters:** Enables **efficient** use of spectrum
-  **mmWave & private networks:** Public consultations to **explore best licensing frameworks**
-  **Spectrum sharing:** As the demands for spectrum increase, countries seek to **embed more flexibility** in their spectrum management frameworks (e.g. sharing, unlicensed spectrum)
-  **Looking ahead:** Spectrum management shaped by an evolving external context and emerging technologies (e.g. drones, NGSO, HAPS, THz and beyond 5G)



Thank you!



Let's stay in touch!

verena.weber@oecd.org



[@WeberVere](https://twitter.com/WeberVere)



[Verena Weber](https://www.linkedin.com/in/verena-weber)

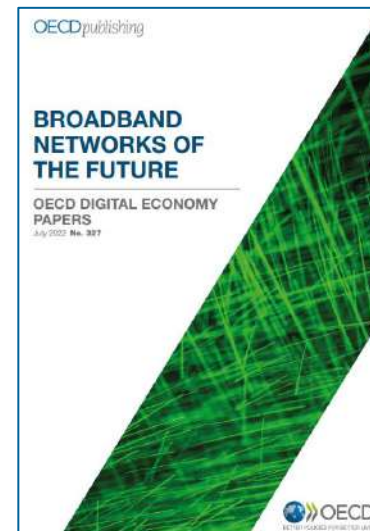
Access our OECD broadband data on:

<https://www.oecd.org/digital/broadband/broadband-statistics/>

Further reading



**Developments in
Spectrum Management
for Communication
Services (2022)**



**Broadband
Networks of the
Future (2022)**



**Communication
Regulators of
the Future
(2022)**

5G – built secure with defense in depth

Mikko Karikytö
Head of Product Security & CPSO
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios



Holistic security approach

Key conclusions

Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios

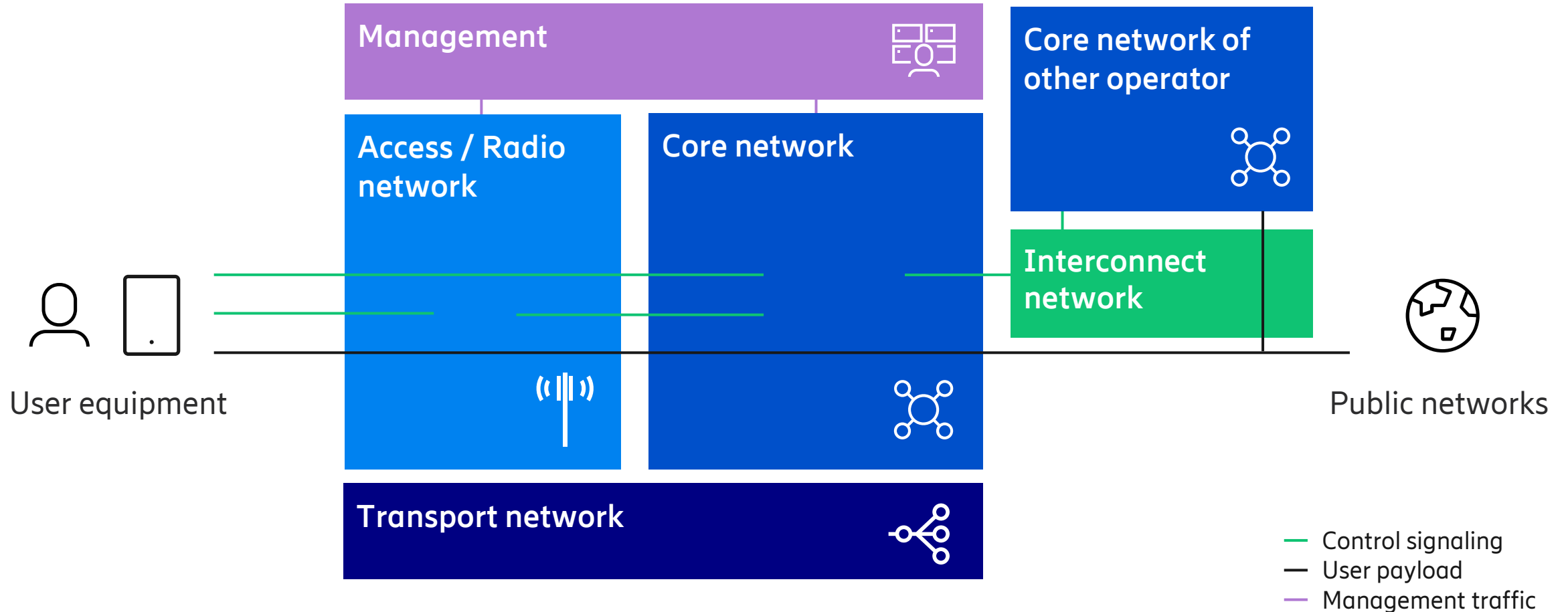


Holistic security approach

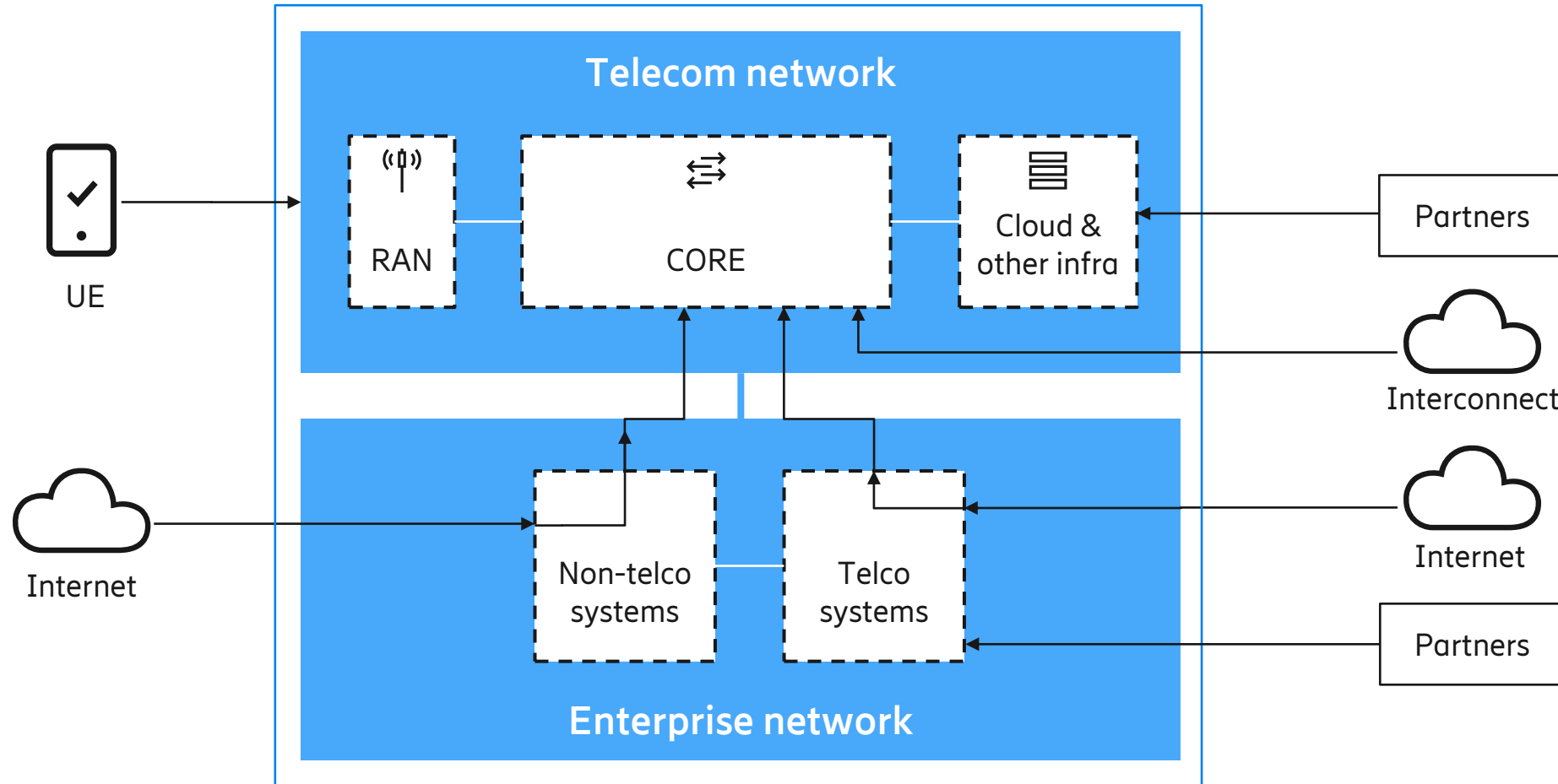
Key conclusions

High level mobile network overview

Logical elements and logical planes



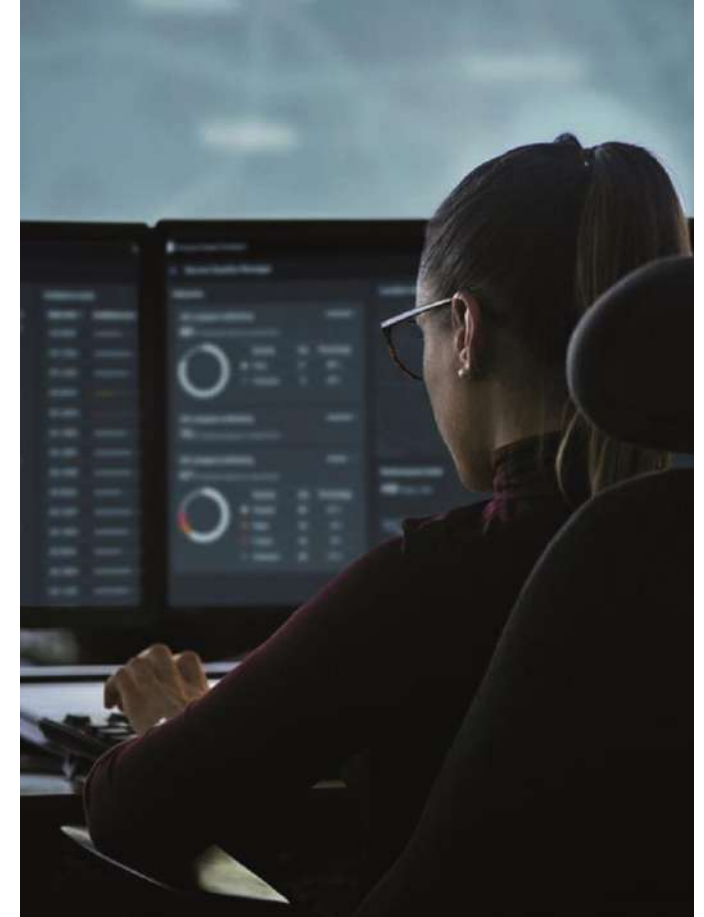
Telecom attack vectors



Challenges in securing telecommunication networks



- Large number of assets, complex, multi-vendor environments
- Diverse set of human resources required to access critical information systems (**paygrade + competence = new risk**)
 - Network operations center staff, administrative staff with privileged access
 - Vendor support staff (3rd party companies, onshore and offshore)
- Multiple, diverse operating environments
 - Cell towers in remote locations
 - Secured data-centers
 - Cloud environments operated by 3rd party companies
- Multiple generations of technologies (2G+3G+4G+5G)
 - Long product lifecycles
 - Newer generations more secure by design



Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios

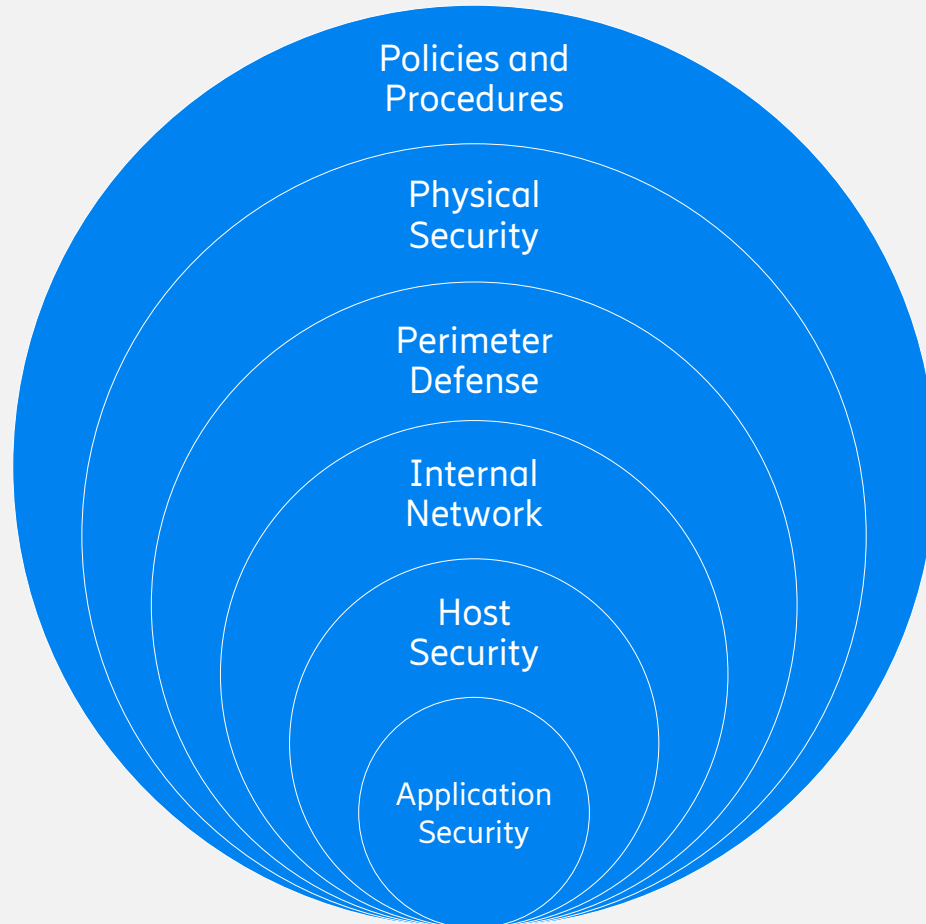


Holistic security approach

Key conclusions

Defense in depth

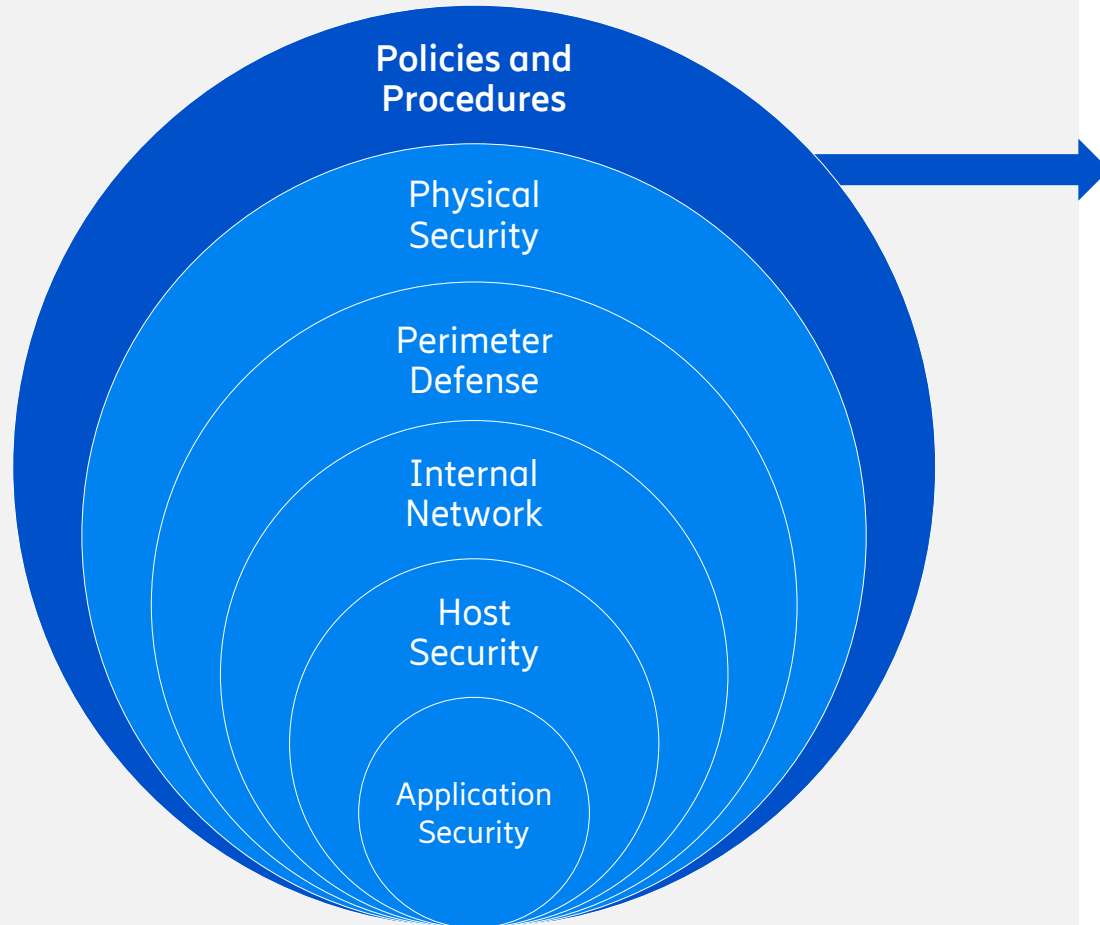
Multilayered defense



- Fundamental information security principle originating from military strategies
- Multiple, layered controls
 - Physical, technical, administrative
- Multiple layers must be broken for an attacker to achieve desired objective
- If a security control fails, other compensating controls are in place to mitigate

Defense in depth

Multilayered defense



Attacker calls up NOC staff member pretending to be IT security to obtain a login to network

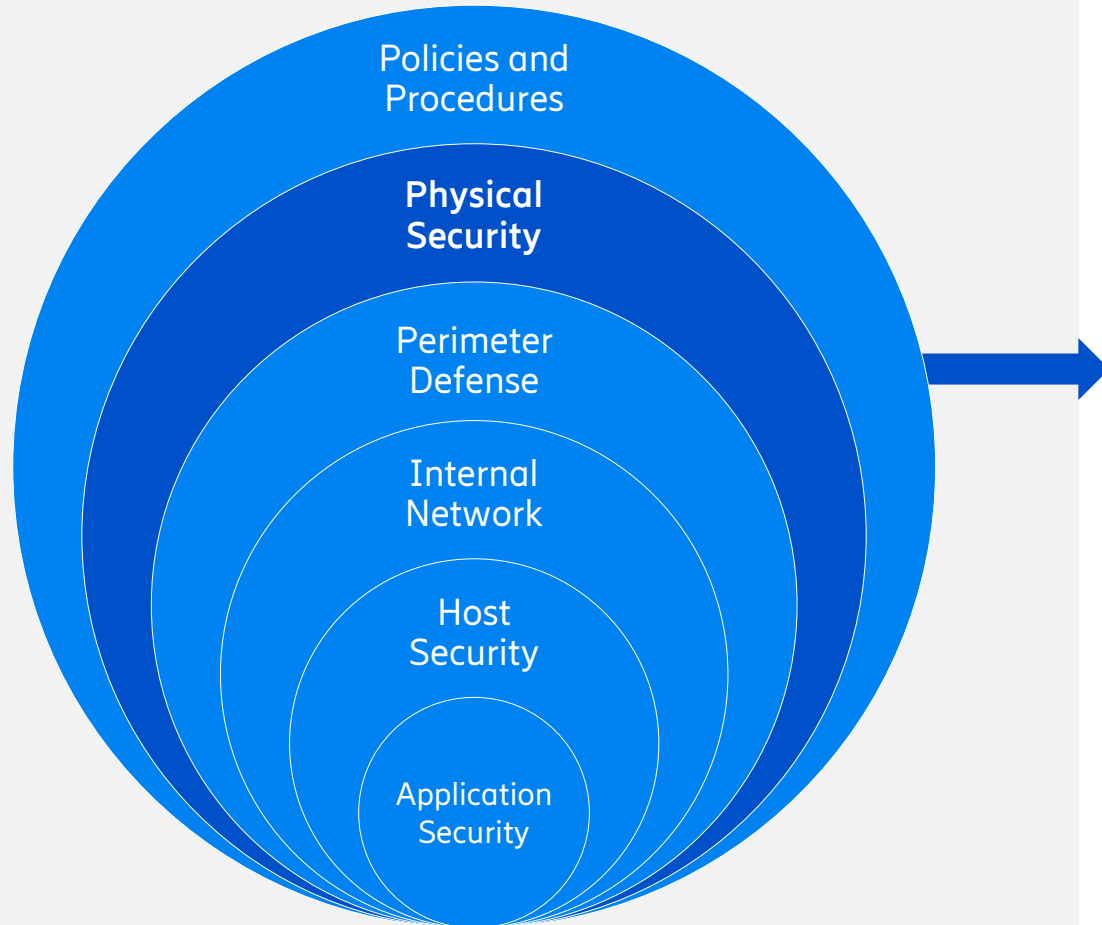


Employee recalls routine awareness / education.



Defense in depth

Multilayered defense



Attacker visits company to sneak in and plug in malicious device into the network

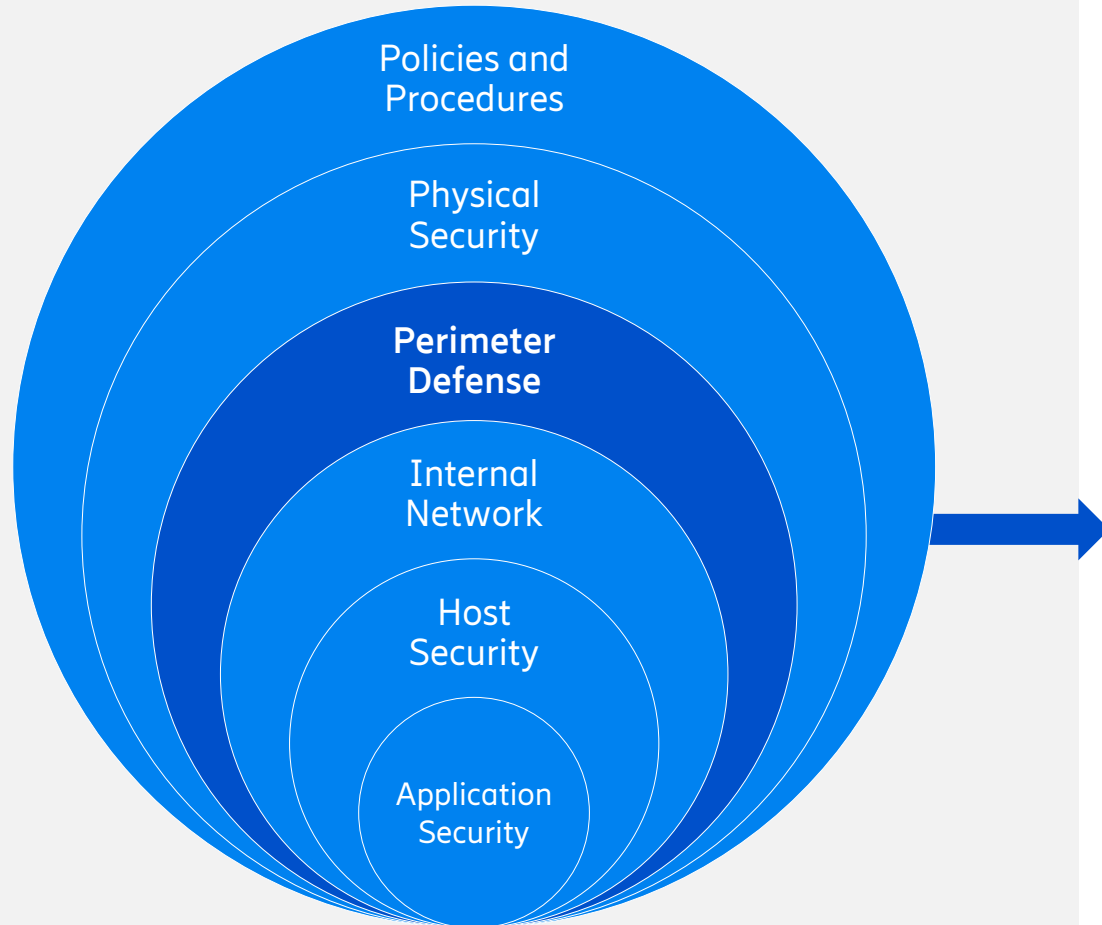


Mantrap prevents tailgating employees ID checks



Defense in depth

Multilayered defense



Attacker performs network scanning to attempt to find exposed / vulnerable system

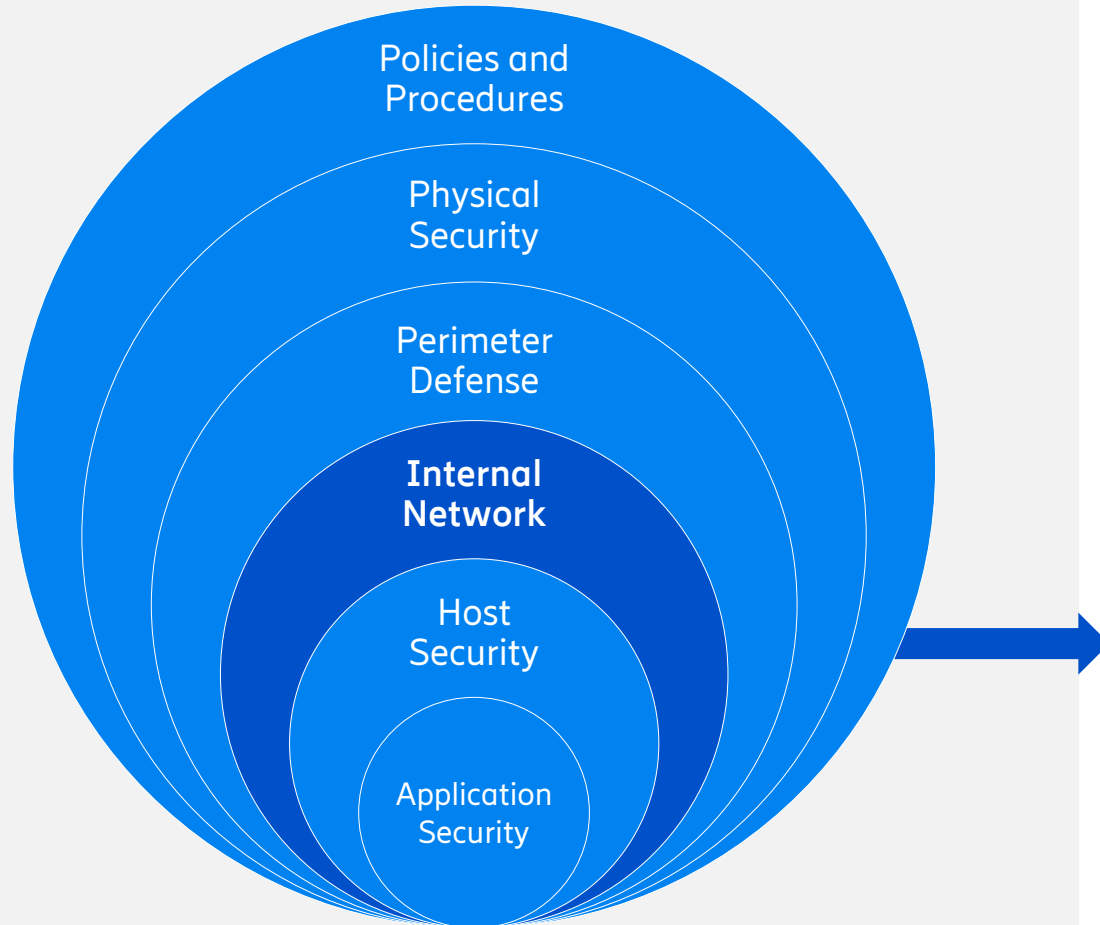


Firewalls block access from Internet and cell phone devices



Defense in depth

Multilayered defense



Attacker manages to breach enterprise network with objective to gain access to core network

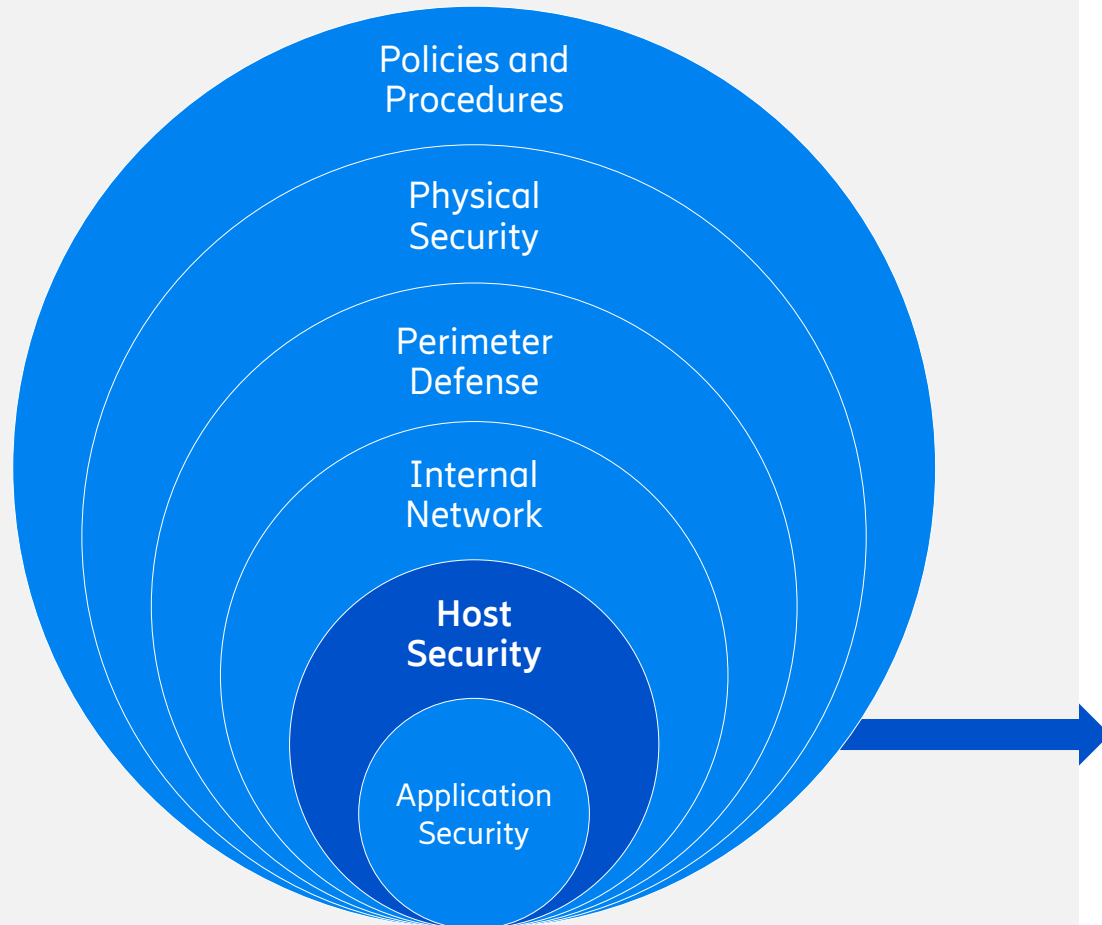


ZTA prevents access to core network assets. Only authorized employees can access during approved / planned activities / maintenance window



Defense in depth

Multilayered defense



Attacker attempts software exploit to escalate privileges

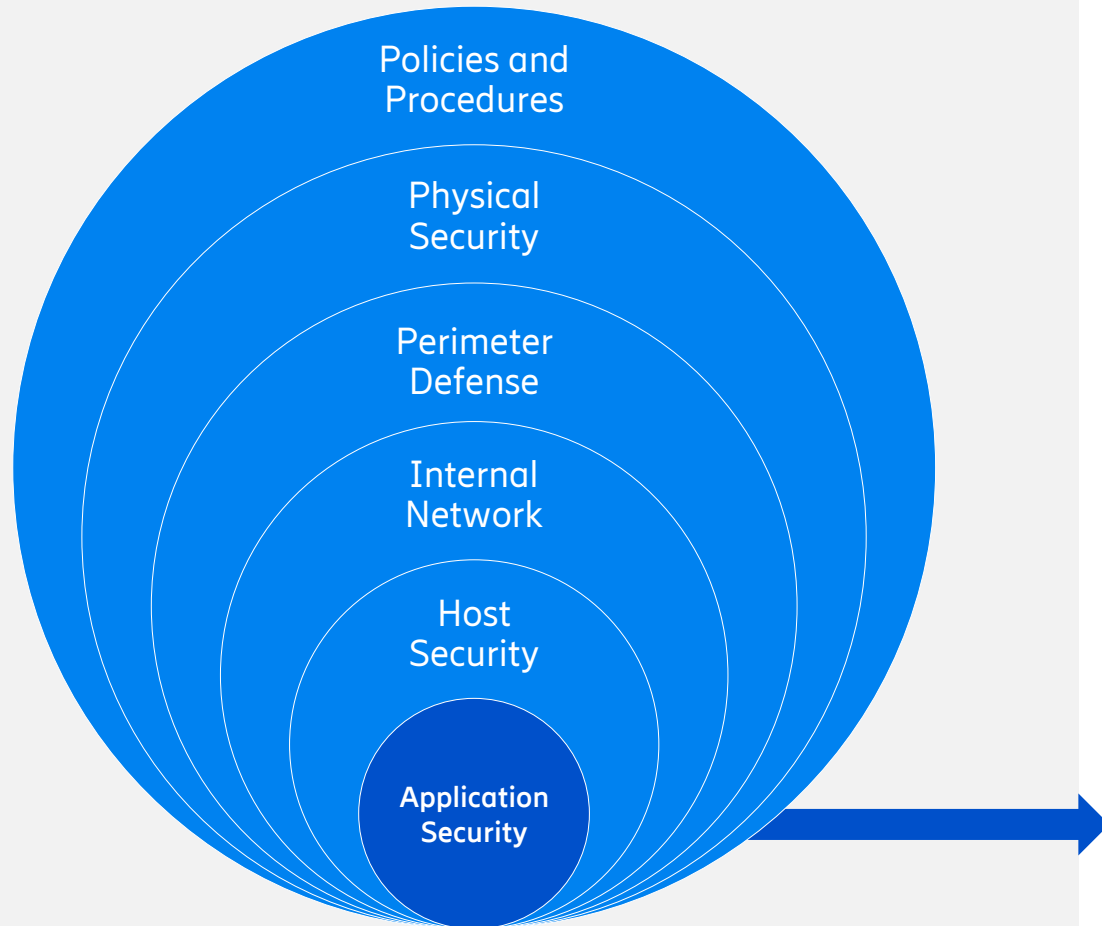


Operating system hardened by default prevents execution of exploit



Defense in depth

Multilayered defense



Attacker attempts to exploit known vulnerability in popular application



Application has been updated to latest, patched version as part of routine lifecycle maintenance

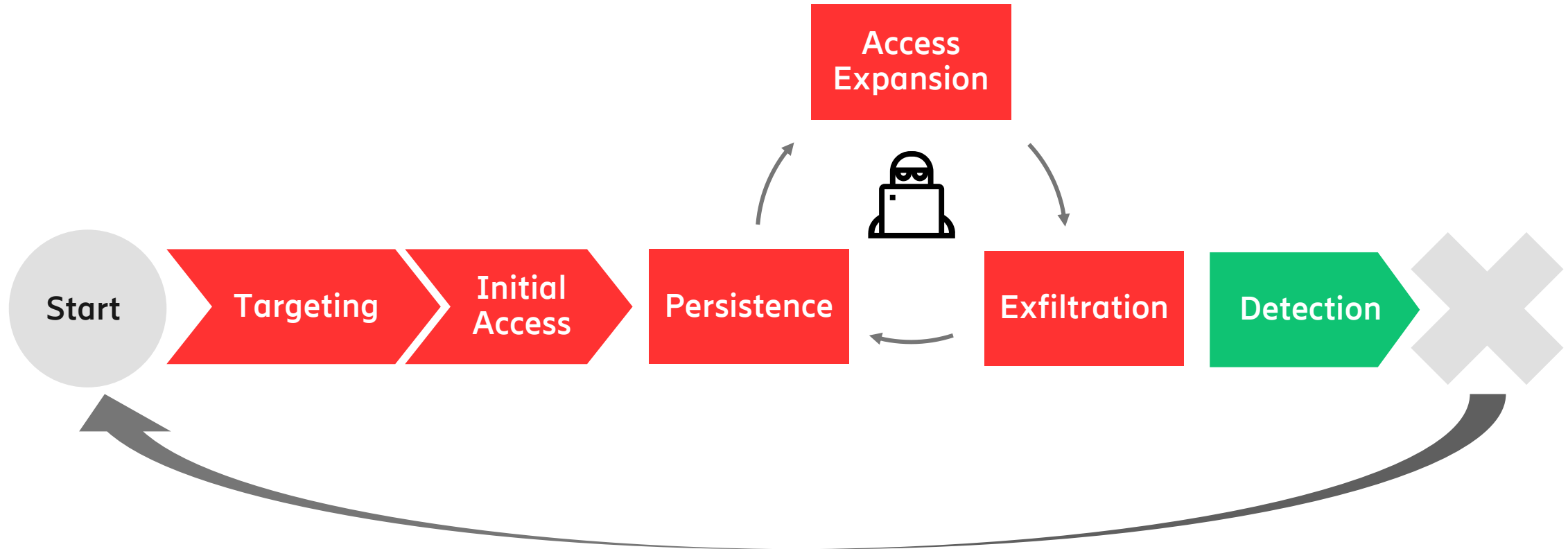


Layered controls – Scenario examples



Layered control	Example	Mitigation
Policies and Procedures	Attacker calls up NOC staff member pretending to be IT security to obtain a login to network	Employee recalls routine awareness / education.
Physical Security	Attacker visits company to sneak in and plug in malicious device into the network	Mantrap prevents tailgating employees ID checks
Perimeter Defense	Attacker performs network scanning to attempt to find exposed / vulnerable system	Firewalls block access from Internet and cell phone devices
Internal Network	Attacker manages to breach enterprise network with objective to gain access to core network	ZTA prevents access to core network assets. Only authorized employees can access during approved/planned activities/maintenance window
Host Security	Attacker attempts software exploit to escalate privileges	Operating system hardened by default prevents execution of exploit
Application Security	Attacker attempts to exploit known vulnerability in popular application	Application has been updated to latest, patched version as part of routine lifecycle maintenance

Network exploitation lifecycle



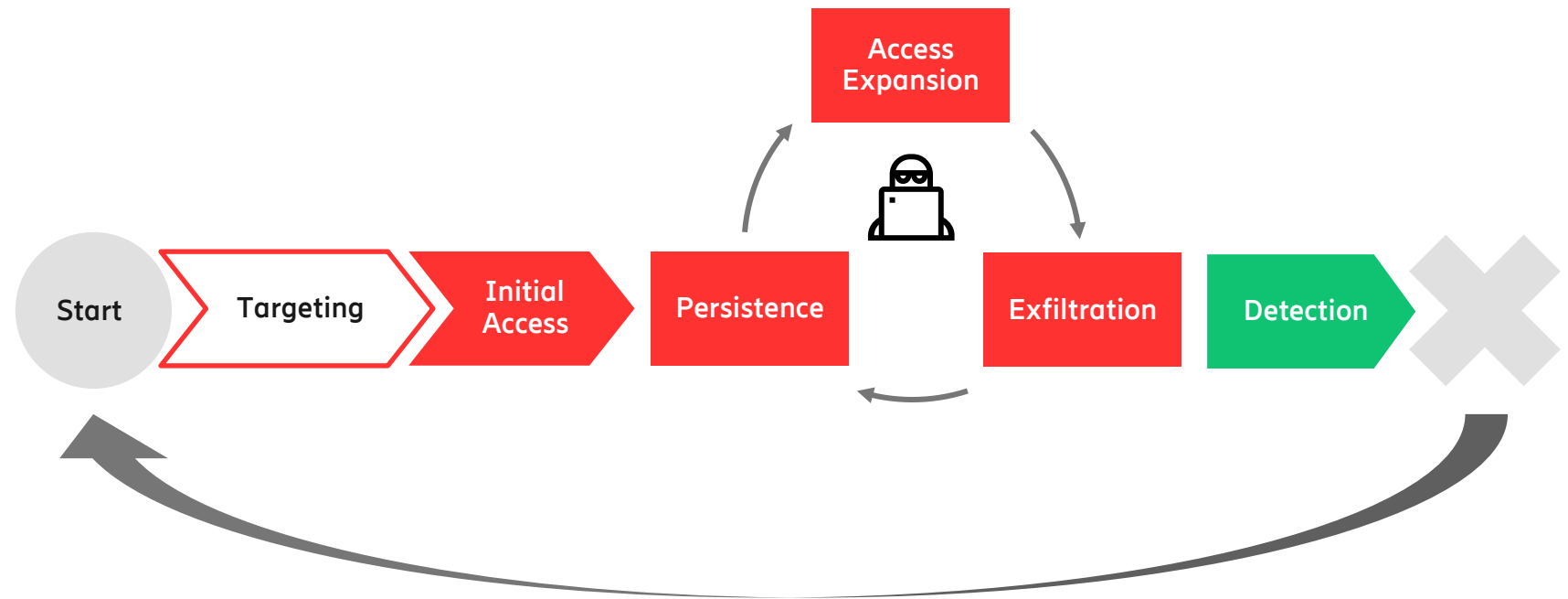
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Targeting

- Mapping out initial access opportunities (e.g. Internet exposure)
- Identifying people – names, email addresses, their tastes and weaknesses



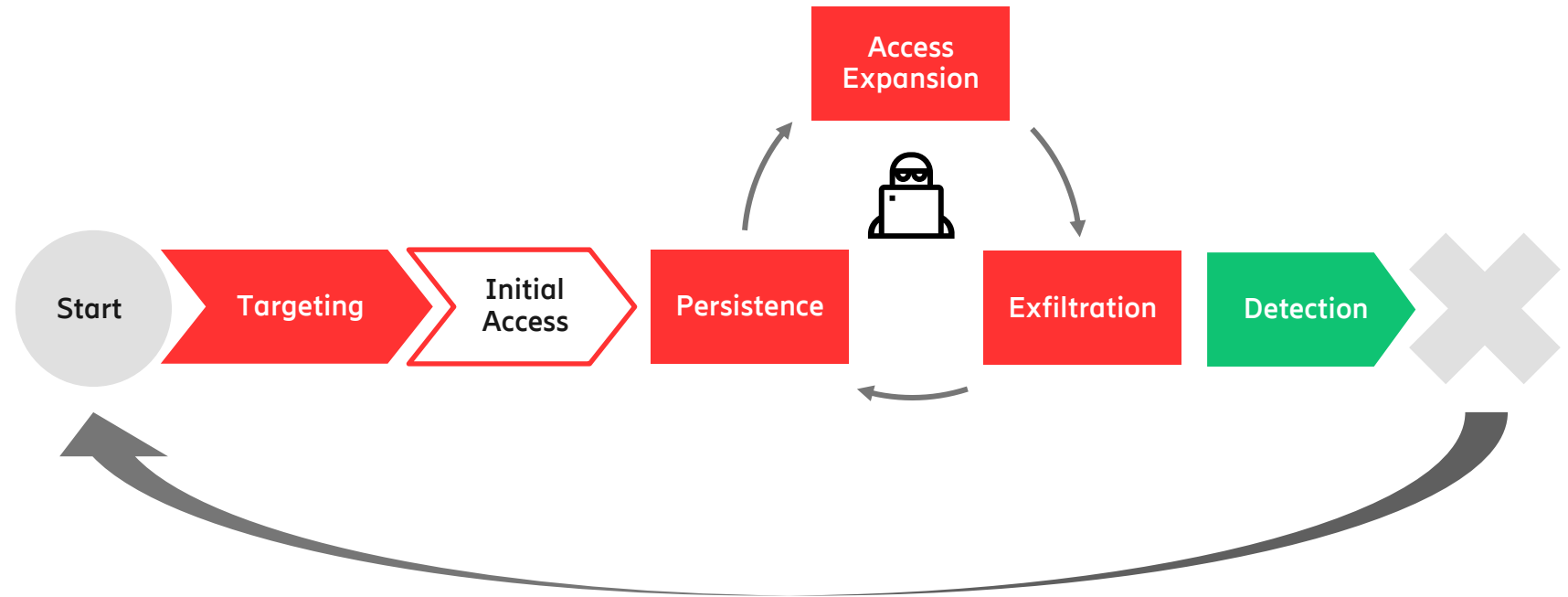
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Initial Access

- Exploitation of vulnerability to gain initial access (e.g. Internet)
- Malware detonated on employee's computer within connected to the enterprise network
- Employee credentials stolen and used for access



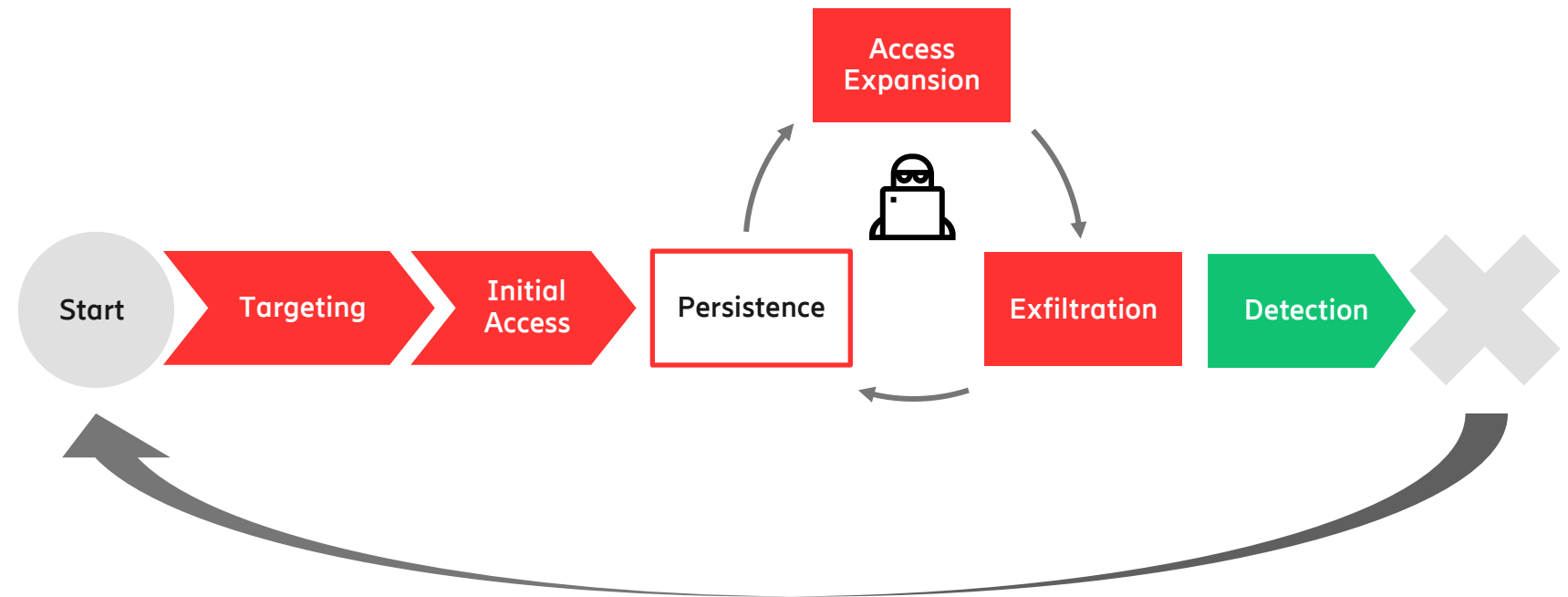
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Persistence

- Remove initial access requirements
- Install redundant backdoors / malware that provide connectivity to attacker
- Create new user accounts



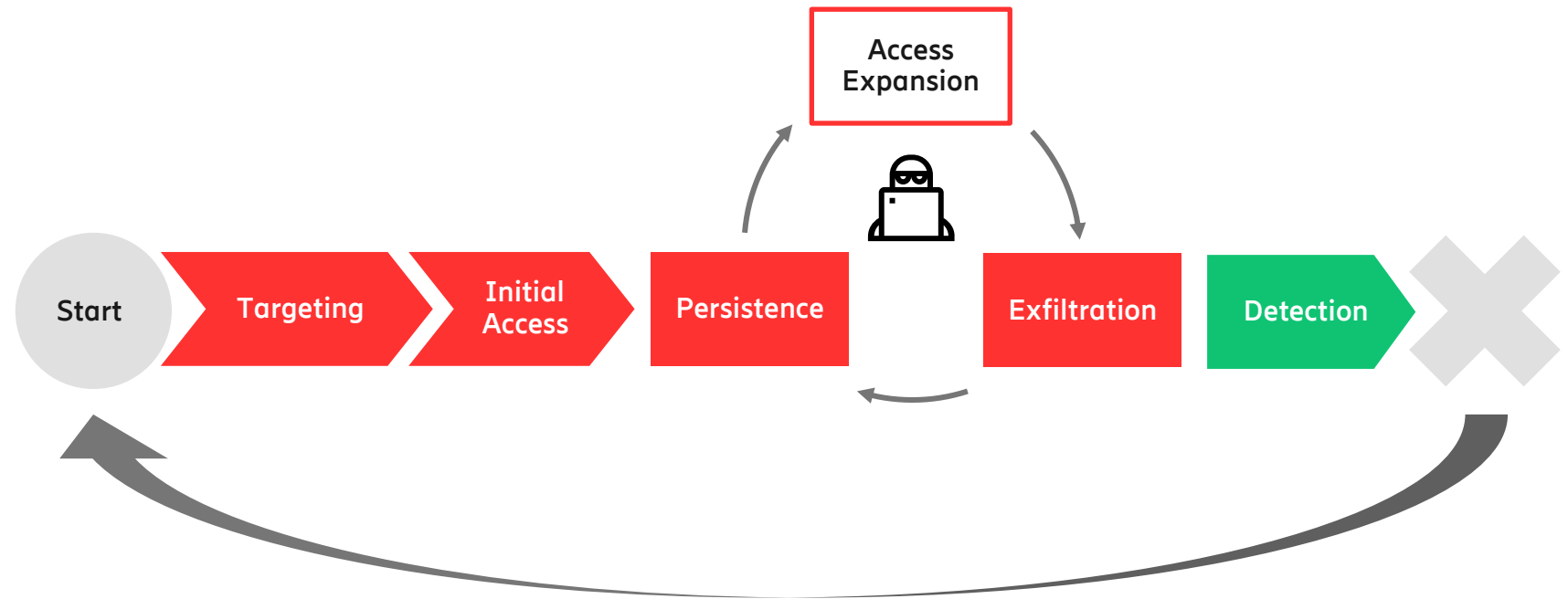
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Access Expansion

- Surveying, collecting and analyzing information for the next step of the operation – where to move and persist next



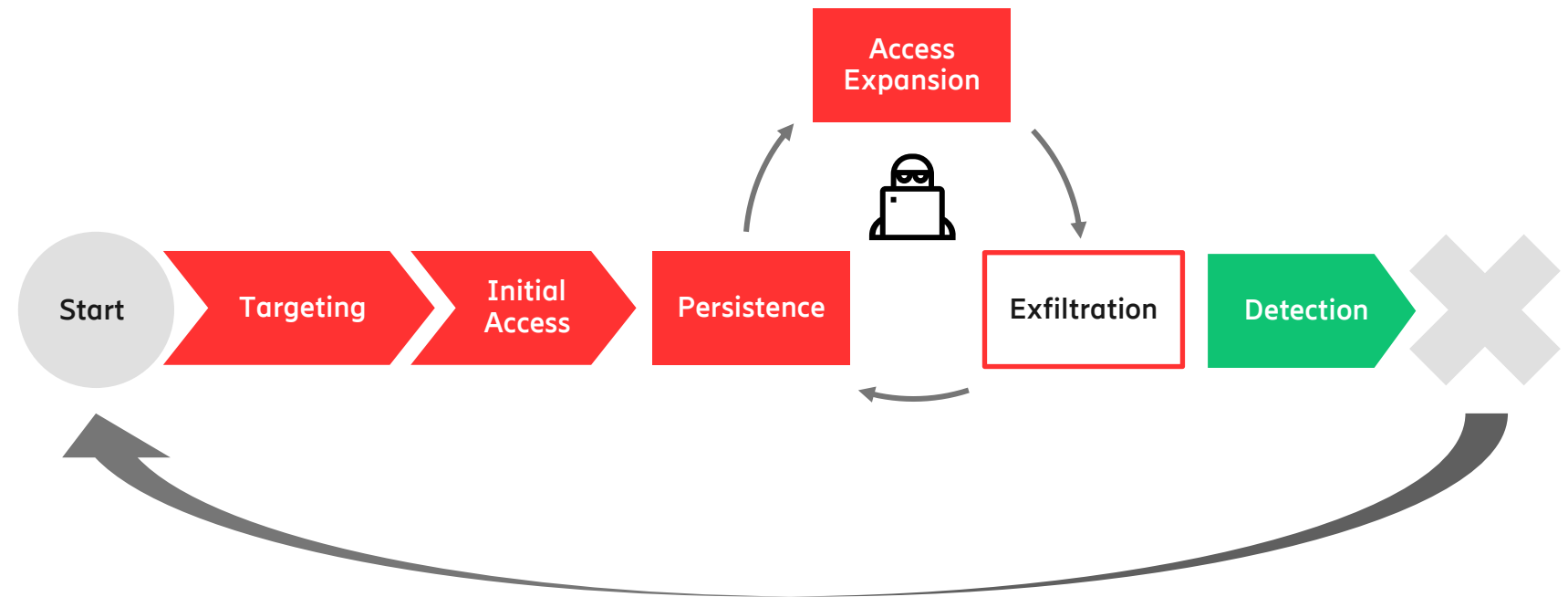
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Exfiltration

- Exfiltration – Transferring the data out of the network



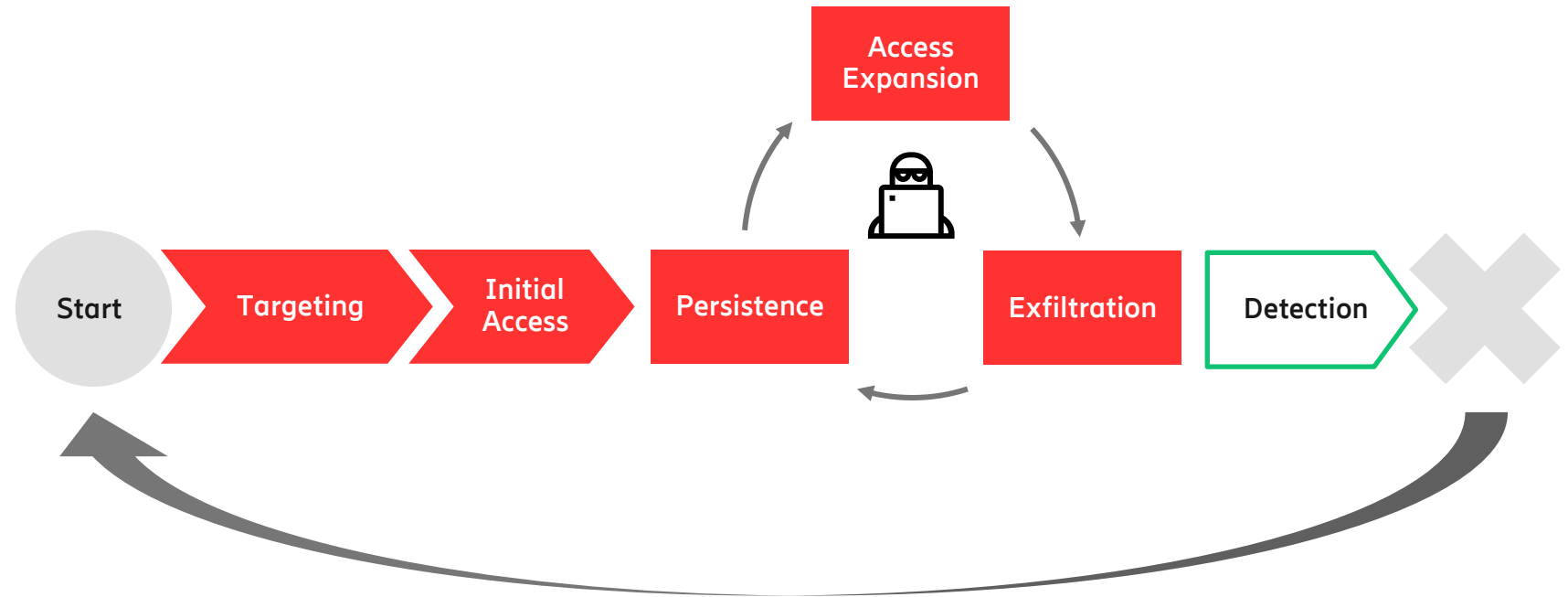
Defensive security controls prevent or disrupt each attack stage

Network exploitation lifecycle



Detection

- Defender detects, finds all points of persistence / presence and evicts



Defensive security controls prevent or disrupt each attack stage

Network exploitation attack stages

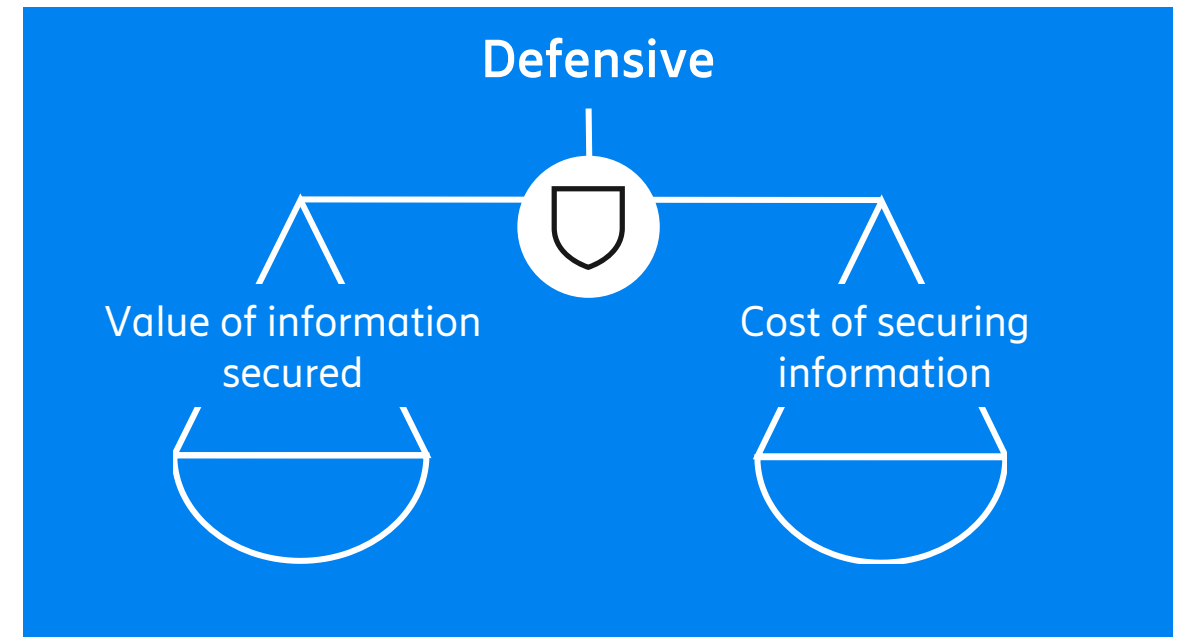
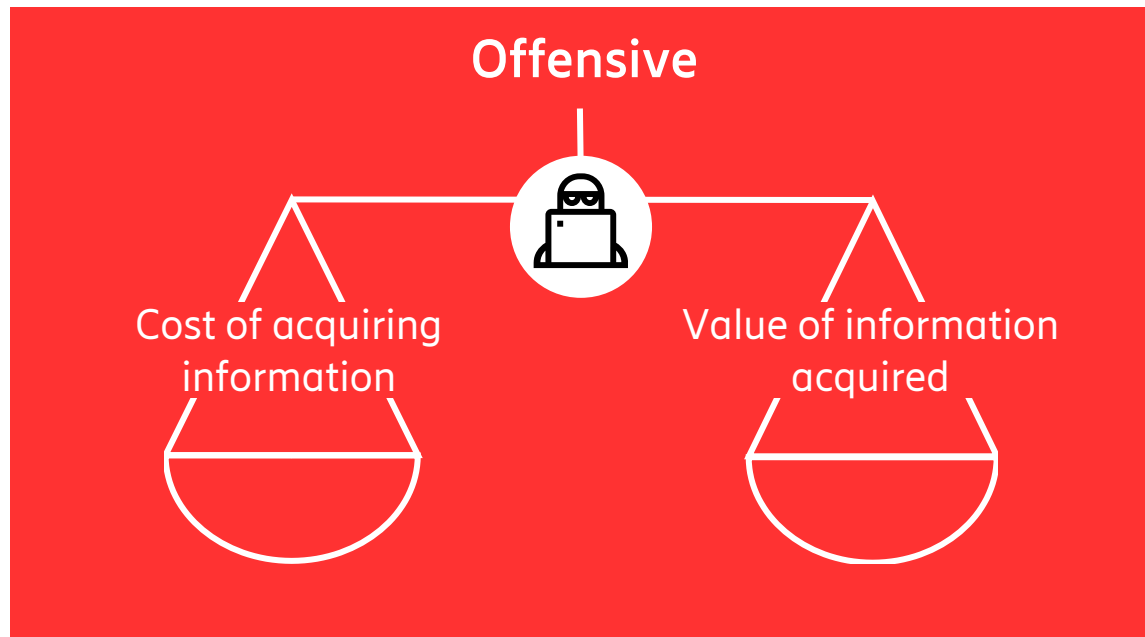


	Stage	Description
1	Targeting	<ul style="list-style-type: none">• Mapping out initial access opportunities (e.g. Internet exposure)• Identifying people – names, email addresses, their tastes and weaknesses
2	Initial Access	<ul style="list-style-type: none">• Exploitation of vulnerability to gain initial access (e.g., Internet)• Malware detonated on employee's computer within connected to the enterprise network• Employee credentials stolen and used for access
3	Persistence	<ul style="list-style-type: none">• Remove initial access requirements• Install redundant backdoors / malware that provide connectivity to attacker• Create new user accounts
4	Expansion	<ul style="list-style-type: none">• Surveying, collecting and analyzing information for the next step of the operation – where to move and persist next
5	Exfiltration	<ul style="list-style-type: none">• Exfiltration – Transferring the data out of the network
6	Detection	<ul style="list-style-type: none">• Defender detects, finds all points of persistence / presence and evicts

Successful defense of telecommunication networks



- No system or network is 100% secure.
- Objective is to influence the balance of attacker economies
- Increase the cost to attackers through multi-layered defenses



Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios



Holistic security approach

Key conclusions

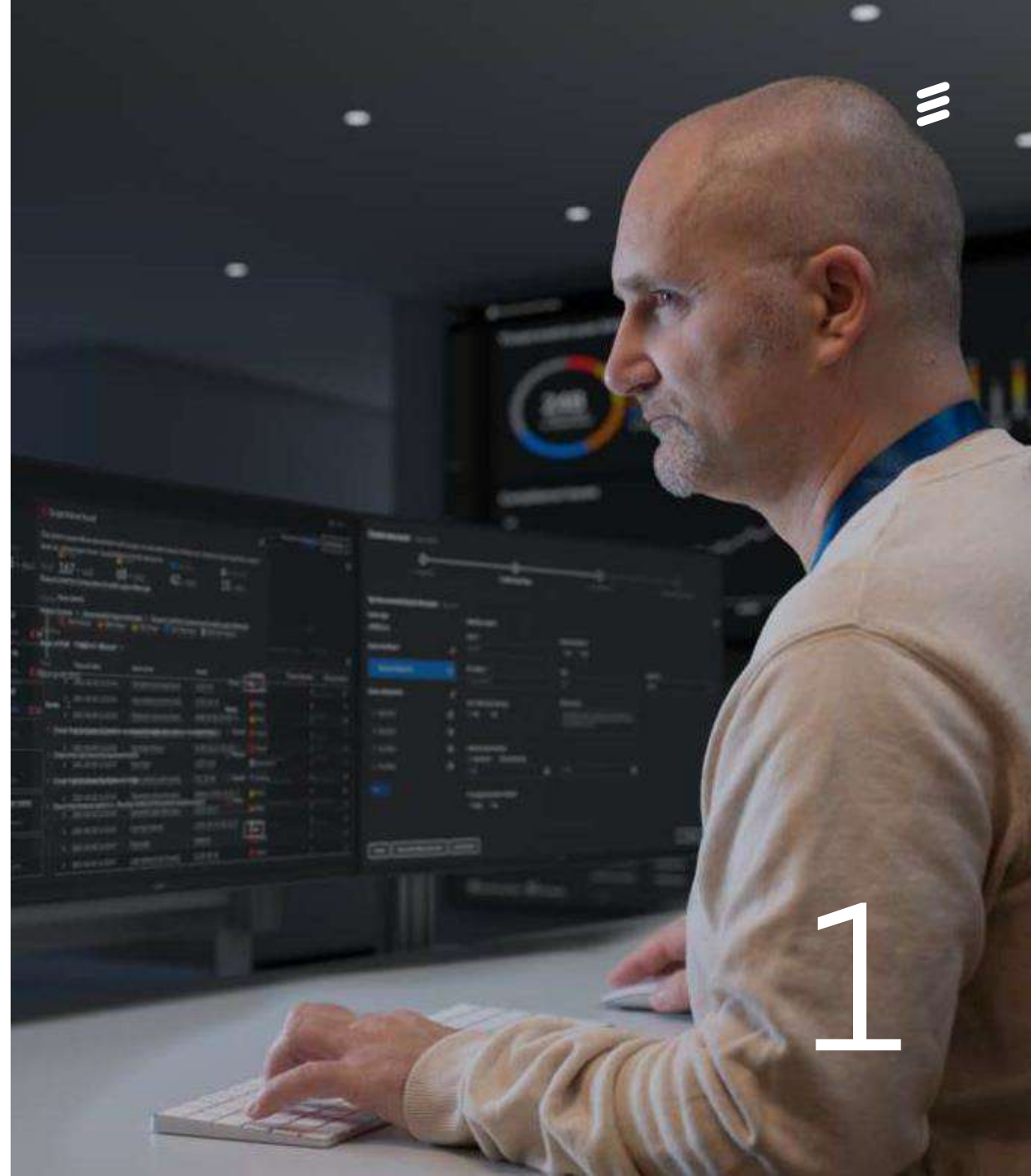
1. Identity and access management

Attacker could attempt to access target network using valid credentials through:

- Social engineer employees
- Purchase stolen (valid) credentials from dark web
- Use default credentials
- Brute force / guess credentials "I'm in"
- Access provided from insider

Defense in depth mitigations:

- Awareness training (Policies and Procedures)
- Password policies, user account management policies (Policies and Procedures)
 - Multi-factor authentication
- Segregation of duties (principle of least privilege)
- Detection systems (technical)



2. Network architecture and configuration

Attacker could obtain access to network or target system through weak / poor configuration

- **Unnecessary** exposure of the network (e.g., system connected to Internet)
- Lack of segmentation between trust domains and networks (DMZ)

Defense in depth mitigations:

- Design principles, best practice (administrative)
- Due diligence – Continuous auditing and review (administrative)
- Detection systems (technical)



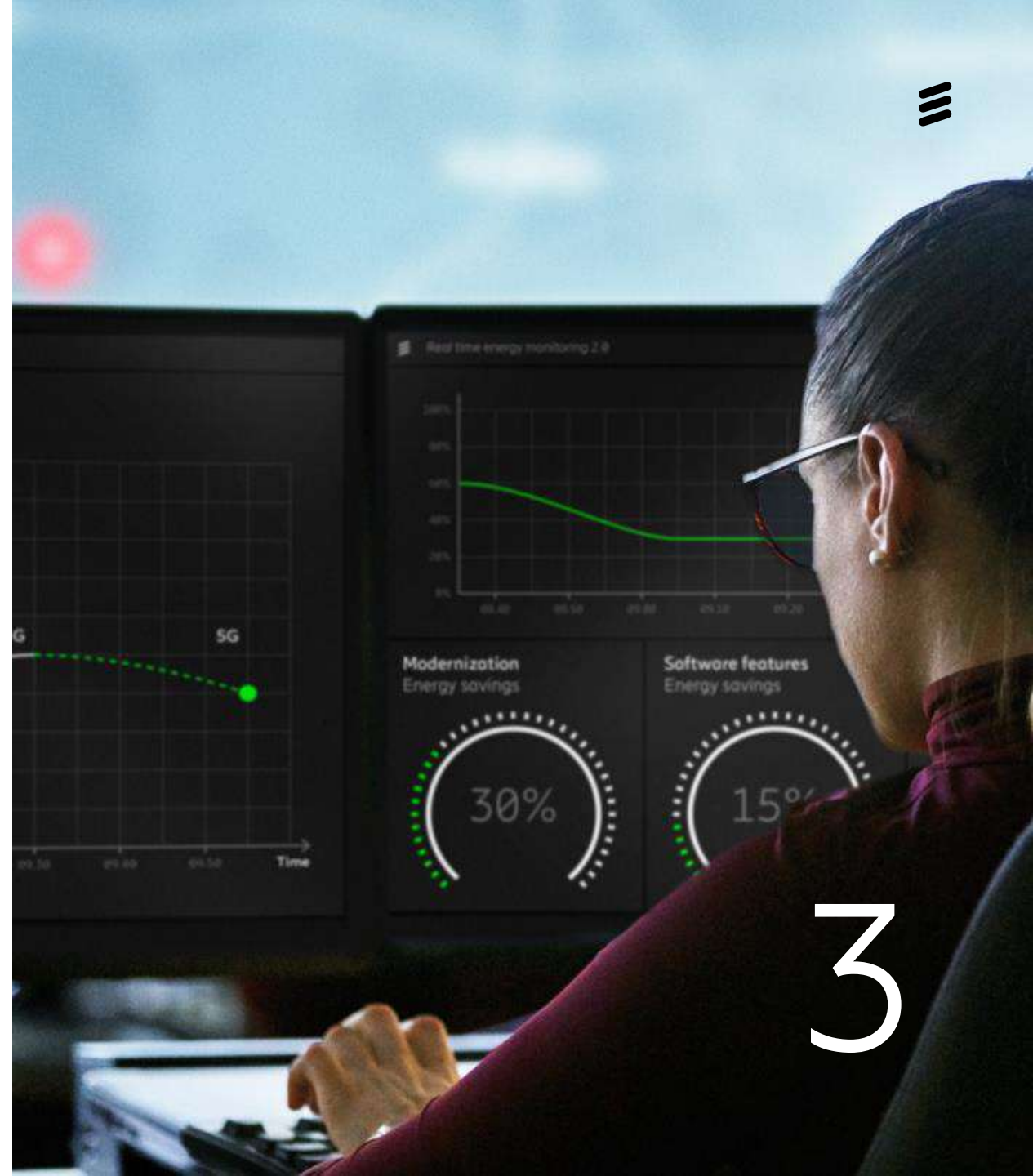
3. Software vulnerability management

Exploitation of a software vulnerability to gain access to the crown jewels

- Exploitation of a software application that processes / stores the data
- Assumed already gained initial access and are persistent in the network

Defense in depth mitigations:

- Select vendors that has mature vulnerability management processes
- Routine patch management (stability vs security)
- Detection and rapid response (technical, administrative)



Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios



Holistic security approach

Key conclusions

The foundation of security of deployed networks



Operations process

- Secure operational procedures, e.g., segregation of duties, use of least privilege and logging
- Monitoring the security performance, vulnerability management and detection of attacks
- Response and recovery after breach



Deployment process

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening



Vendor product development process

- Secure hardware and software components
- Secure development processes
- Version control and secure software update



Telecommunications standardization process

- Secure protocols, algorithms, storage



- End users' experience of network security is determined by deployed networks.
- Security status of deployed networks depends on four interdependent layers.
- Holistic approach to security includes all four levels.
- Operators are in control of operations, deployment and integrator and vendor selection.
- Vendors are in control of their product development and sourcing decisions (component suppliers).
- Standards are set in a multi stakeholder fashion.

The four tenets of secure telecommunication networks



Telecom security operations

- Network operations with security monitoring and response capability



Identity and access management

- Principle of least privilege
- Access through enterprise IT infrastructure
- Access through partners



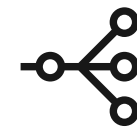
Hardened architecture and configuration

- Solid network design with security and resilience in mind.
- Configuration of security parameters, hardening



Vulnerability management

- Asset management, Version control and software updates



Security features to enable a zero-trust architecture



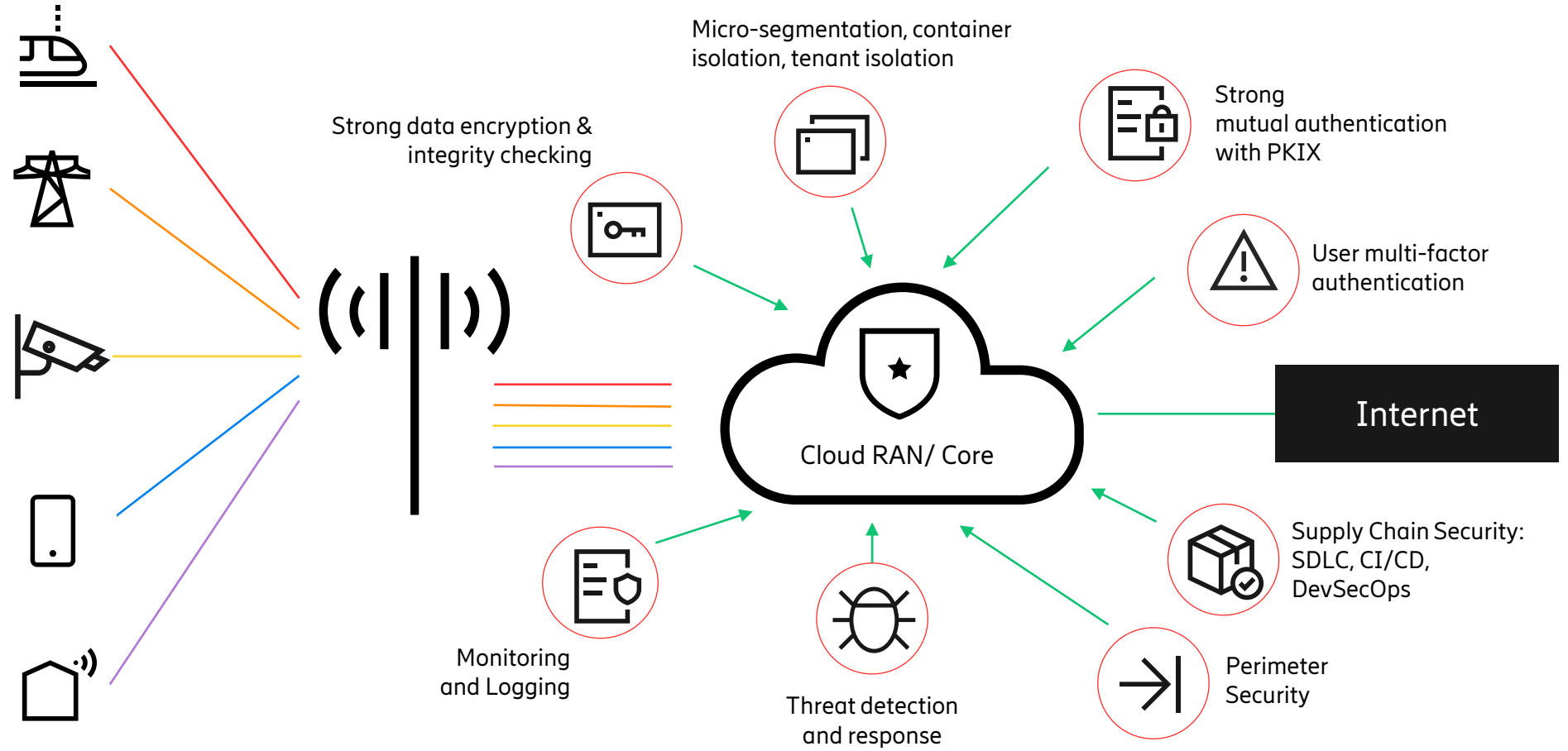
Zero-trust: Don't trust based on asset owner / location



RF fingerprinting: Intercept rogue transmitters



Security at every step of software development (agile)



Agenda



Introduction mobile network and attack vectors



Defense in depth



Three attack scenarios



Holistic security approach

Key conclusions

Key conclusions



Telecom networks are different

- Critical infrastructure scaled on the national level
- Must always be operational, always on, all the time
- (Near) real time performance for millions at once at any given time



Asymmetry of the opportunity

- Attackers often only need to find one vulnerability or weakness in operations, configuration, software or in standards
- Defenders must get it right **every time, everywhere – attackers only once, somewhere**



Risk is mitigated by layering of defenses (defense in depth)

- Ericsson trust stack incorporates defense in depth principles within a holistic security framework
- There are no technical silver bullets. All bases must be covered.
- For example, if the software is secure, network secure – the human can be exploited



Holistic approach is needed to decrease the ROI for an attacker

- Every layer of defense increases the overall requirement of resources an attacker needs to be successful
- Gaps in the defense open a venue for an attacker to bypass layers and get improved ROI
- Attacker consequences of committing cyber attack need to get higher to have a real deterrence





<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

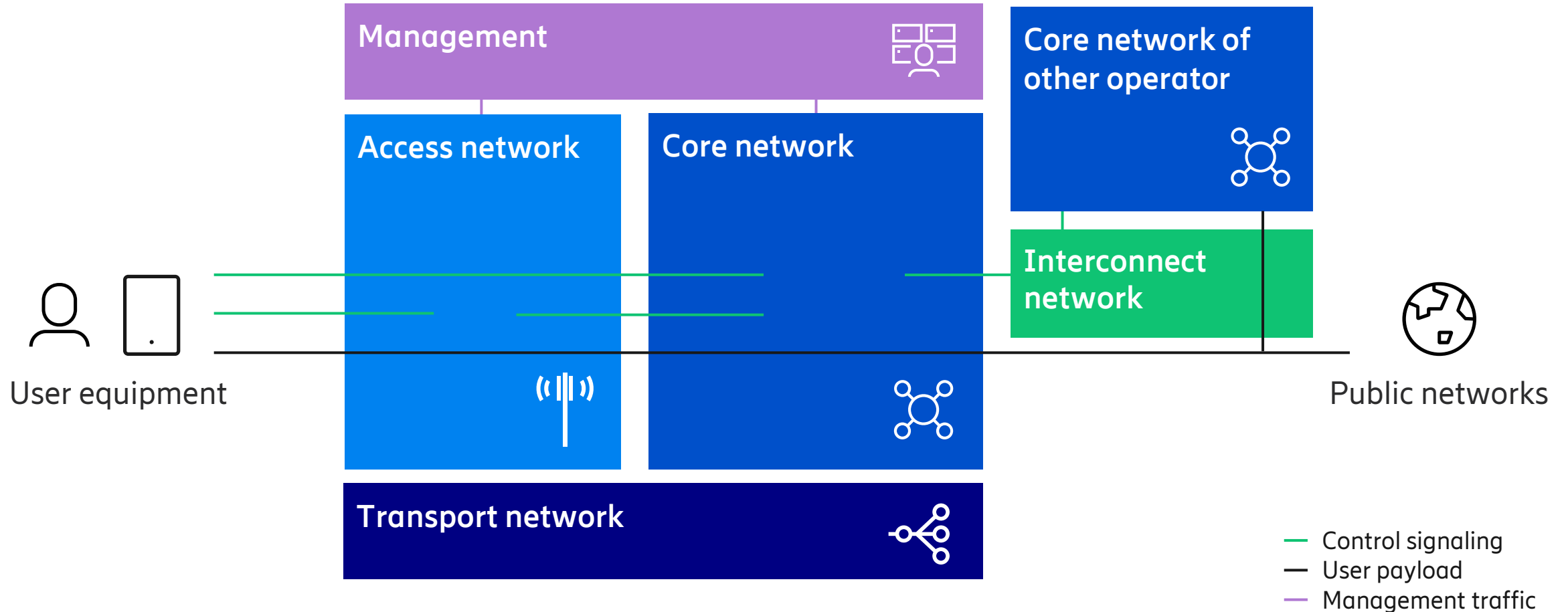
Security of deployed networks

Mikko Karikytö
Head of Product Security & CPSO
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

High level mobile network overview

Logical elements and logical planes



A telecom network today needs to be secure across multiple contexts and use-cases



As telecom networks have new, more demanding use cases, **attack motivations increase, attack vectors multiply** and the need to **protect the network grows exponentially**

Consumer services

- Call record theft
- Fraud
- Privacy violations

Critical society services

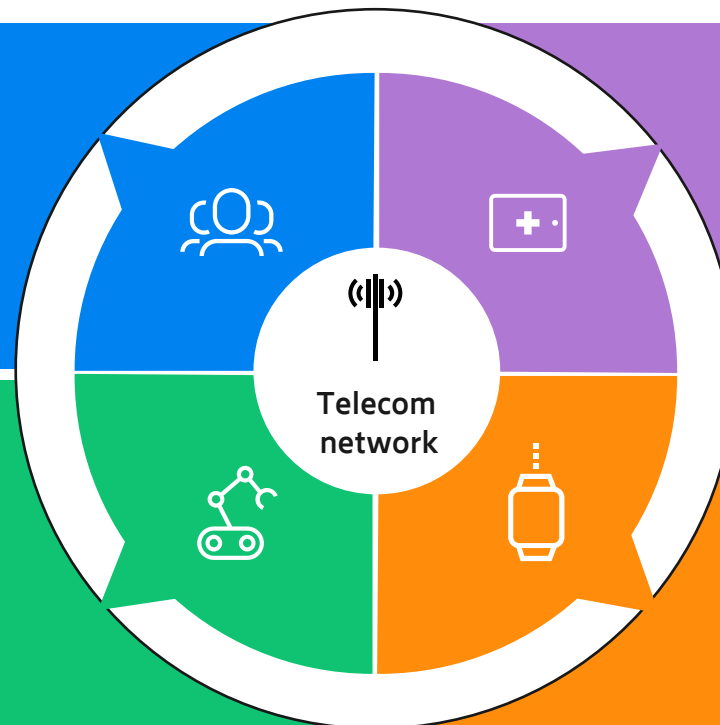
- Data manipulation
- Invasion of health profile
- Privacy violations

Industrial applications /Private networks

- Supply chain shutdowns
- Data theft
- Production line disruptions

Consumer IoT

- Data & identity theft
- Device hijacking



Increased value at stake decreased-risk tolerance



5G Game Changer



Enabler for new industrial use cases

Digitalization



Every company will become a digital company

Systems GO Mobile



New attack vectors emerge – IOT

Mission Critical ICT Infrastructure



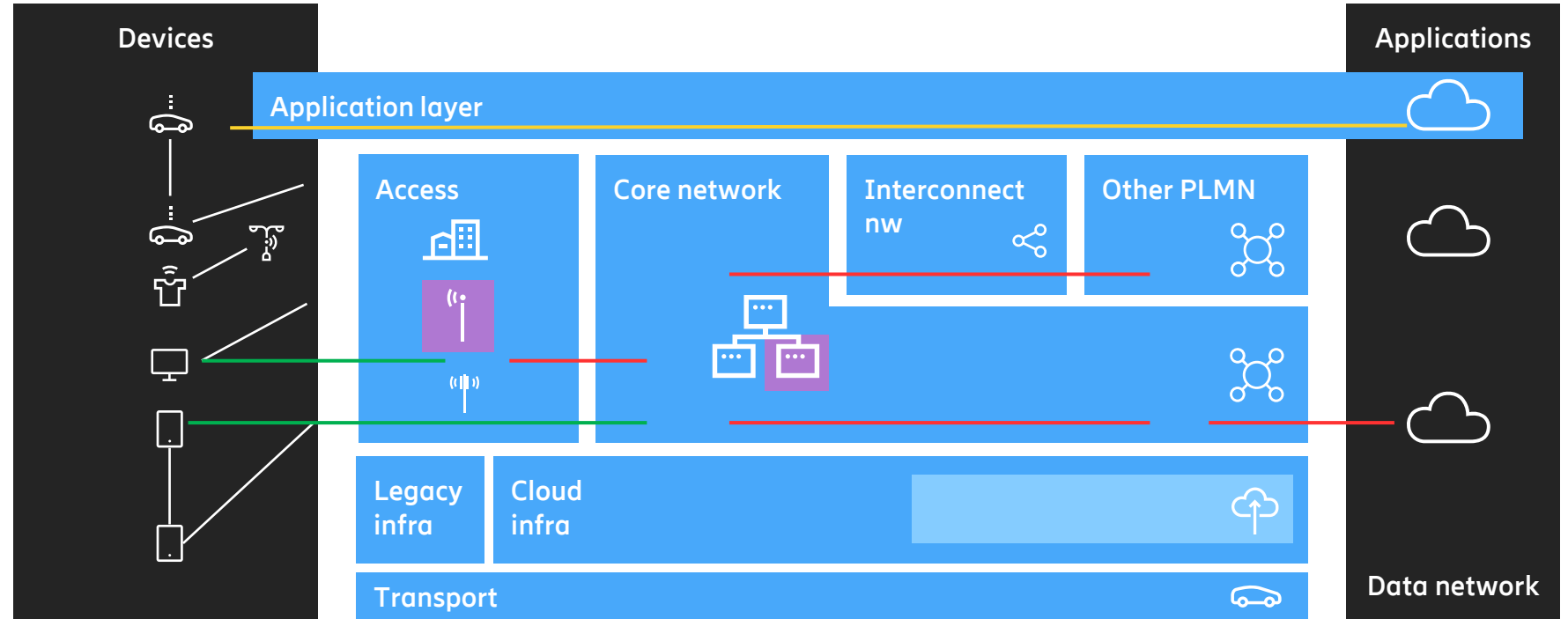
More value, concentrated more attacks

3GPP security area



In principle, all work in 3GPP SA3 can be divided into the following areas

- Application security
- UE to network access security
- Network to network security
- Security assurance
- Virtualization security*



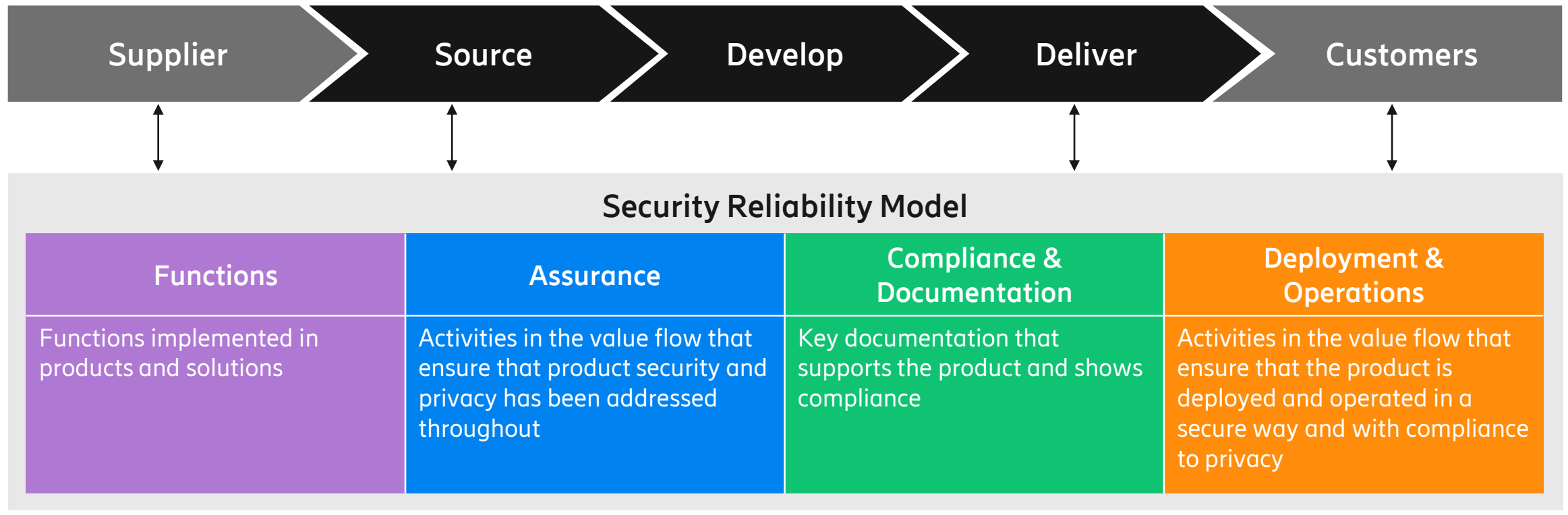
Rel(ease)-15 created the foundation of security for the 3GPP 5G system. Later releases have added enhancements to the system security and added security for features to enable new use cases.

Security Reliability Model (SRM)

Ericsson's risk management framework



Product value flow: The controls in SRM applies across the flow from component intake to operations in customer networks



Ericsson works with multiple perspectives to ensure secure networks



Develop

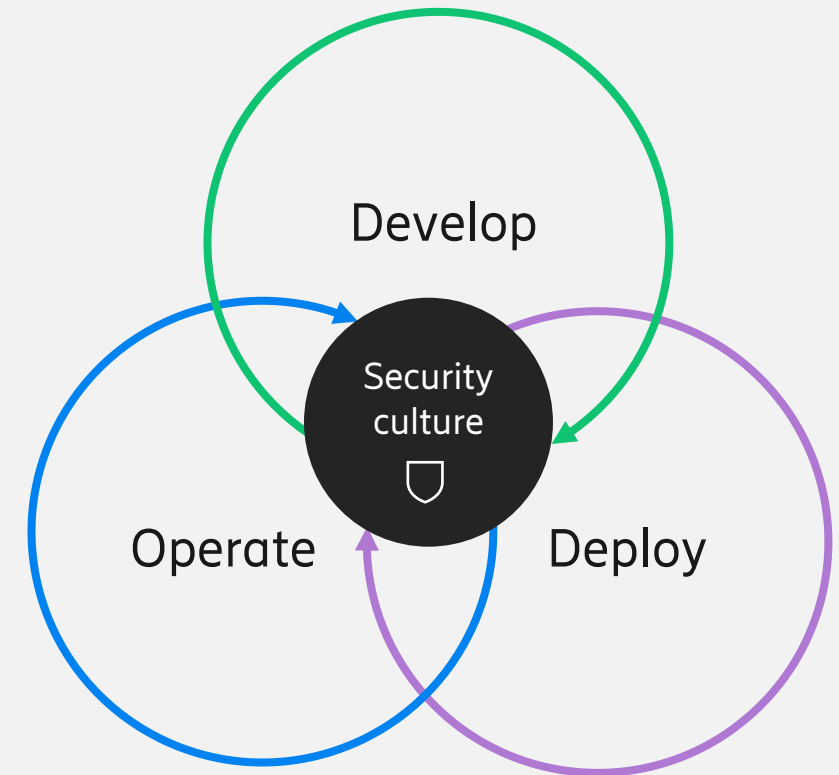
Ericsson develops secure products and solutions, built on the strong foundation of 3GPP, with a strong and rigorous security perspective, including a controlled supply chain, deep knowledge of existing and emergent threats, and the contexts where our products will be used.

Deploy

Ericsson works together with our customers to ensure solid deployments of our products and networks, with clear guidelines for secure configurations, handover and hardening of the network. We also work with our customers on to create an overarching secure architecture of the networks we build.

Operate

Ericsson works together with communication service providers in ensuring the security of networks in operations. Features in our products mitigate the risk of successful attacks; security solutions help CSPs detect, mitigate and respond to threats; and 24/7 incident response team captures and patches vulnerabilities in networks.



Security culture codified in processes and people



All teams have an appointed **Security Masters** which ensures that all design, development and testing is done in accordance with Ericsson's policies in SRM.

- Security education
- Design rules
- Security requirements
- Secure code

Champions

Guiding masters and enabling them to implement SRM



Experts

Proving subject matter expertise supporting in specialized areas on group level. Continuously evaluating SRM and contributing to its evolution



Masters

Embedding security and privacy in every step of the development and delivery



Specialists

Leading in their area of expertise by supporting and complementing teams across the organization



Supply and sourcing – Product development – Sales – Service delivery – Operations – Customer support

Ericsson security culture in numbers



Ericsson knows how important the security of our customers is – that is why we have units solely dedicated to security, such as SRM and PSIRT

25,000

Vulnerabilities analyzed by PSIRT yearly

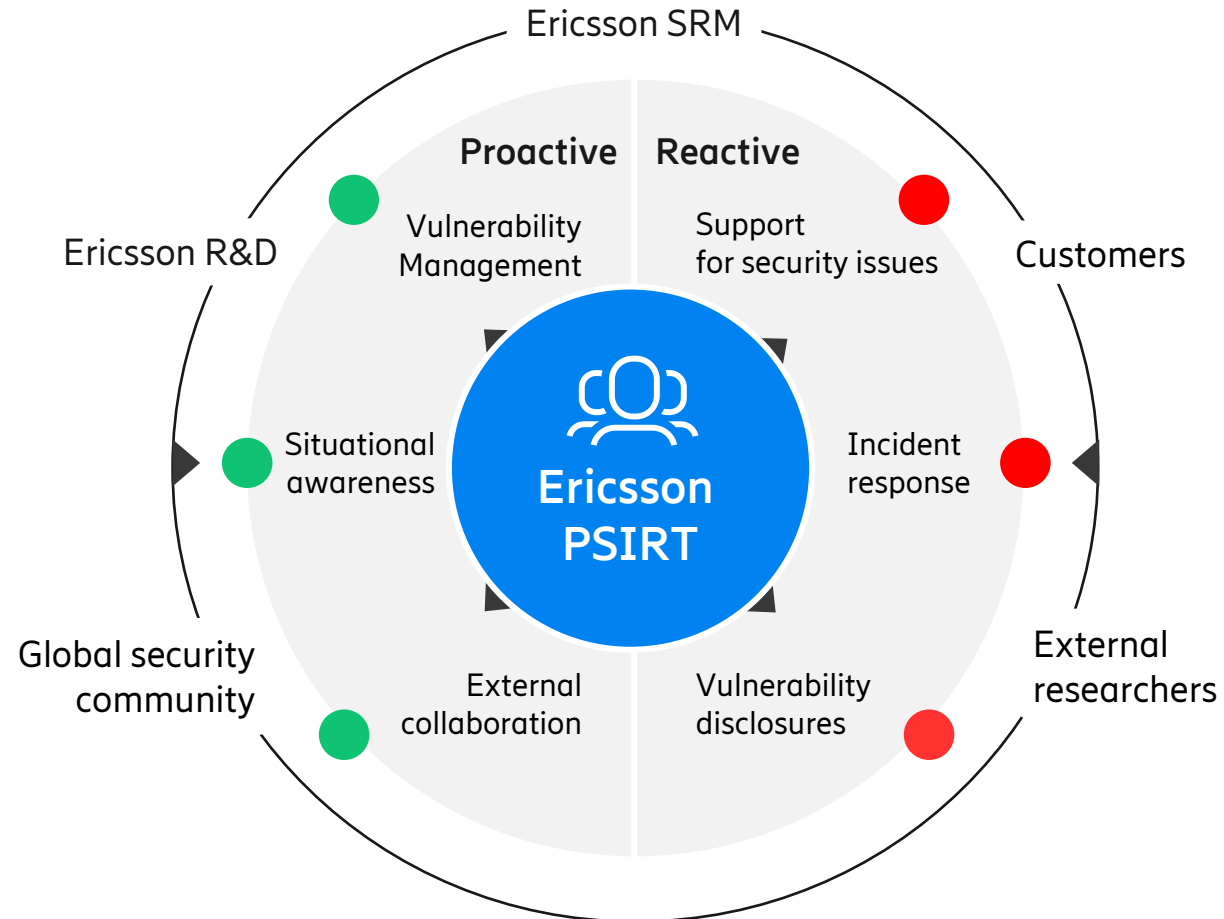
1,000

Security masters in Business Area Digital Services year-to-date

16,000

Vulnerability scans in Ericsson products year-to-date

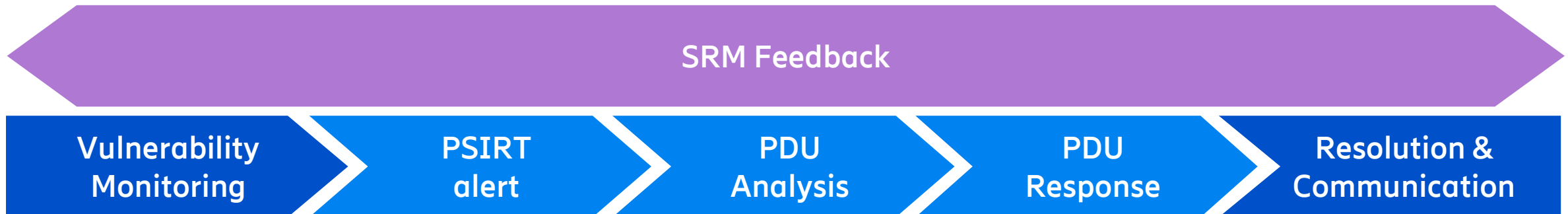
Ericsson PSIRT



Vulnerability management across the entire network



PSIRTs' in-house vulnerability management service is supported by open industry standards, including CVE¹ for identification of vulnerabilities, CPE² for structured naming of open source and commercial software, and CVSS3³ for presenting the overall vulnerability impact and severity.



¹CVE – Common Vulnerabilities and Exposures. CVE system is maintained by MITRE organization.

²CPE – Common Platform Enumeration. CPE scheme is maintained by NIST (U.S. National Institute of Standards and Technology).

³CVSS3 – FIRST organization (Forum of Incident Response and Security Teams) is responsible for CVSSv3 specification.

Strong security is built as a continuous process of learning by doing

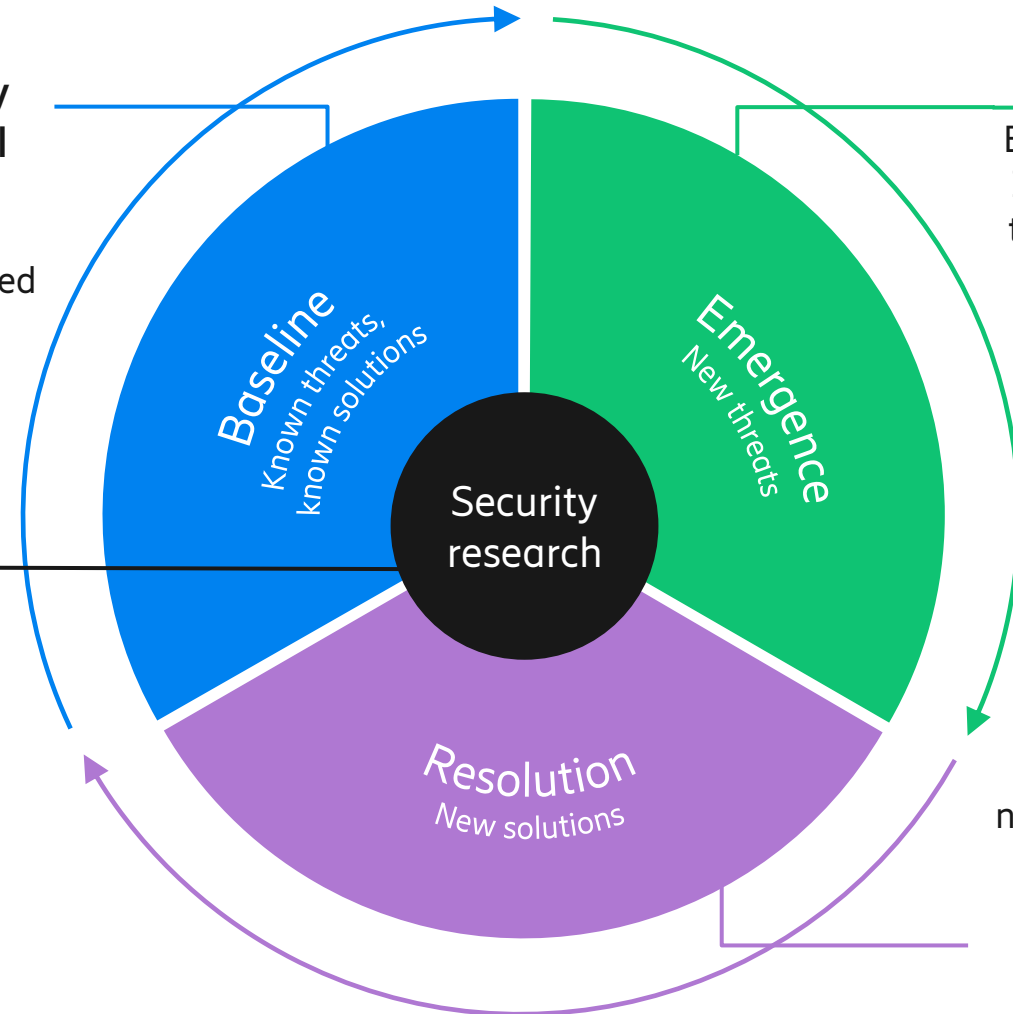


Twenty years delivering security competence, new solutions, and technical proof points in:

- **Standardization of security for mobile networks** – 3GPP, IETF, GSMA, ETSI
- **Collaboration with business areas** and other parts of Ericsson
- **External collaborations:** EU-CONCORDIA, Hexa-X, UC Berkeley, RISELab, Concordia University, RISE Sweden

Ericsson Security Reliability Model

Embodies security practices and is continuously updated over time



PSIRT

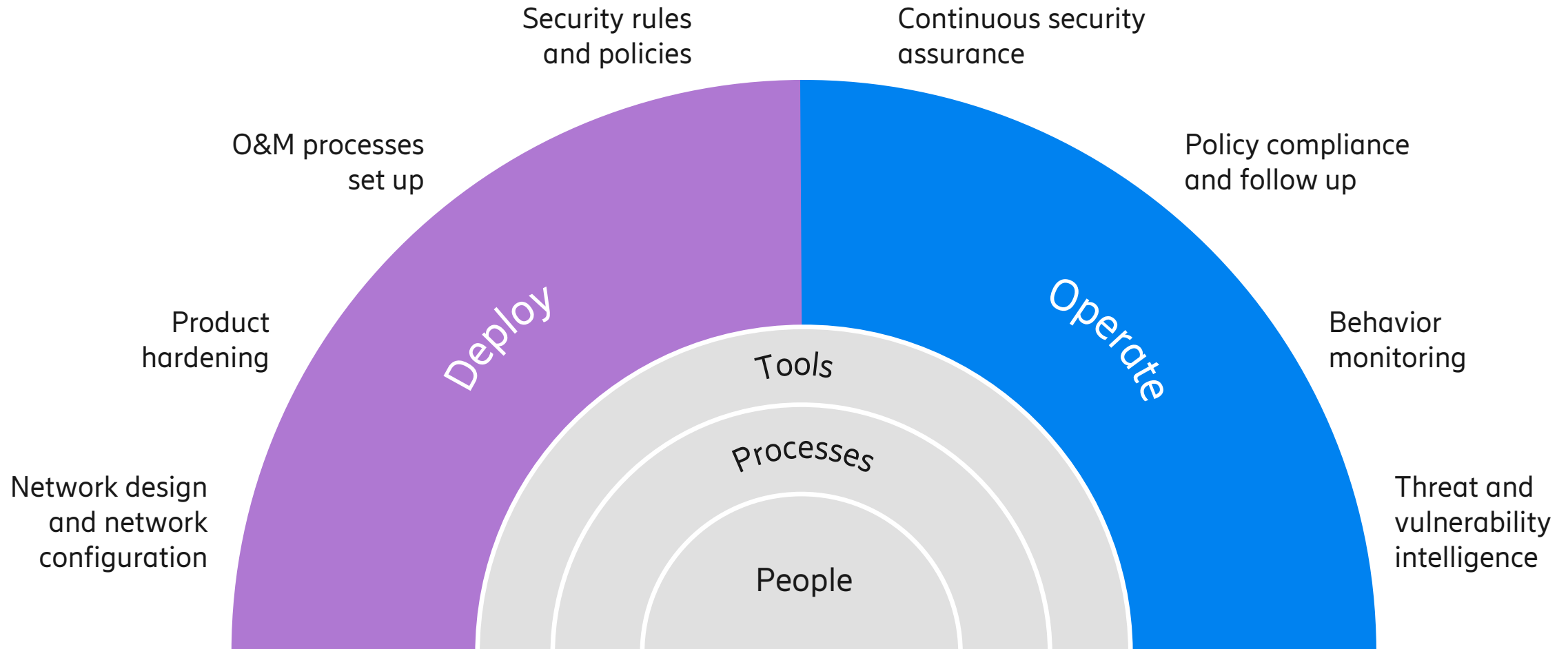
Ericsson Product Security Incident Response Team tracks emergence of new vulnerabilities and threats that feed into new product development

Data-driven development and CI/CD

Developing solutions based on data from live networks and PSIRT, that are then continuously integrated and deployed in customers networks.

Improving CSP security posture

Deployment and operational processes



A suite of capabilities to, collaboratively with CSPs, improve their security posture



Configuration and hardening

Hardening ensures product configuration to minimize the risk of unauthorized access

Centralized identity management

Centralized identity management creates a strong foundation for secure operations

Ericsson Security Manager

- Policy assurance
- Breach detection
- Centralized log data handling
- Automation

Threat and vulnerability intelligence

Threat and vulnerability intelligence keeps network secure after deployment

How we go about realizing Ericsson holistic approach to security



Ericsson
Ericsson Imagine
Studio
Grönländsgatan 8
Kista, Stockholm

Room:
Melbourne
09.00 – 11.00

Room:
Melbourne
13.00 – 17.00

Seminars:

Security – Main track Tuesday June 27, 2023

Advances in connectivity such as through the deployment of 5G create extended opportunities for digitization of all sectors of economy and public sector services and utilities. To harness this development security needs to be an integral part of the digitization process. Cyber security is multi-faceted, including research, standards, secure product development, deployment and operations. It also encompasses people, culture and process.

Ericsson has adopted a [holistic](#) approach to security that is centered on securing deployed networks with the aim to safeguard the end-users as well as to protect network assets. Security seminars at BB4All 2023 provide a unique opportunity to interact with some of Ericsson's key security experts and to inspire exchange of views and experiences between all participants.

Moderator: Rene Summer, Director, Government & Policy Advocacy

Session 1: 09.00 - 09.40

5G – built secure with defense in depth

Speakers: Mikko Karikyö, Head of Product Security & CPSO, Ericsson

Session 2: 09.50 -10.20

Security of deployed networks

Speaker: Mikko Karikyö, Head of Product Security & CPSO, Ericsson

Session 3: 10.30 -11.00

Vulnerability management

Speaker: Umair Bukhari, Head of PSIRT, Ericsson

Session 4: 13.00 -13.40

Security operation automation

Speaker: Bodil Josefsson, Business Manager Security Solutions, Ericsson

Session 5: 13.50 -14.30

Open RAN security

Speakers: Jason Boswell, Head of End-to-End Security, Ericsson North America
Joakim Järval, Strategic Product Manager, Cloud RAN, Ericsson

Session 6: 14.40 -15.20

5G readiness for zero trust architecture and evolution

Speakers: Patrik Teppo, Senior Expert Security Architecture, Ericsson

Session 7: 15.30 -16.10

Open API & 5G Network security

Speaker: Ben Smeets, Senior Expert Security, Ericsson

Session 8: 16.20 -17.00

Confidential software security assurance

Speaker: Lus Barriga, Principal Researcher Security, Ericsson

Ericsson
Ericsson Imagine
Studio
Grönländsgatan 8
Kista, Stockholm

Room:
Demo floor
11.00 – 12.00

Security – Demonstrations Tuesday June 27, 2023

Security demonstrations: 11.00 -12.00, Demonstration floor

#1 Introduction to Secure and Resilient 5G Systems

The world is undergoing a digital transformation, adopting advanced technologies through 5G, relying on predictable performance and security assurance of business, society and mission critical processes. 5G is, by design, is more secure than previous generations, but it is being deployed and operated in an evolving and complex threat landscape. New, demanding use cases served by telecom networks will increase attack motivations and attack vectors. These factors are exponentially increasing the need to protect networks.

Explore why resilience and security are critical for current and future high performing networks. Learn why a holistic security approach is needed and what Ericsson is doing at each layer in the security stack through standardization, development, deployment, and operations to help you reimagine the value of digital.

Host: Andreas Blank, Customer Security Director, Ericsson

#2 Security Automation Center

The general perception that 5G is secure, is very true at product level but what communication service providers (CSP) start to realize is, that once they deploy and operationalize network assets, they are on their own in an ecosystem that is constantly evolving and challenged by an increasing number of threats and vulnerabilities.

Join us to explore how a network is designed, deployed and operated by showcasing typical scenarios in a security operations center environment. We show Ericsson Security Manager, an intelligent security management solution that will improve the security posture, lower monitoring, engineering, and incident management costs, as well as providing a CSP business opportunity.

Host: Bodil Josefsson, Business Manager Security Solutions, Ericsson

#3 Secure and Resilient RAN

With 5G becoming the fastest-evolving mobile generation, there is also an alarming increase in the number of cyber threats, attacks, and vulnerabilities. Today, our Communications Service Providers (CSP) need secure solutions more than anything else.

Join us as we take you through a city under cyber-attack and demonstrate Ericsson's robust RAN security solution, including live demos and a digital demo, that offer you four strong security features. It is a quick and precise solution that detects and protects you against malicious attacks.

Hosts: Anna Kähre, BNEW Product Security Director, Ericsson
Prajwol Kumar Nakarmi, Strategic Product Manager RAN Security, Ericsson

Ericsson
Ericsson Imagine
Studio
Grönländsgatan 8
Kista, Stockholm

Room:
Melbourne
11.20 – 12.20

Room:
Open Box
12.00 – 13.00

Rooms:

Melbourne
Break-out room:
- One: #1
- Two: #2

Lewisville: #3

13.00 – 15.30

Security – Parallel sessions Tuesday June 27, 2023

Roundtable: 11.20 - 12.20

EU 5G Certification

The round table will discuss views on the upcoming EU5G certification scheme for network infrastructure products from EU Member States' perspective. To enhance the framework on 5G cybersecurity and secure 5G deployment in the European Union, the European Commission requested ENISA to develop a candidate European cybersecurity certification scheme for 5G networks (EU 5G scheme). European Cybersecurity Certification Scheme for 5G is being developed by ENISA, with industry experts gathered under an Ad-Hoc Working Group with the EU Commission and Member States. A first draft scheme should be available for public consultation late November 2023.

Host: Patrik Palm, Head of Frameworks, Product Security, Ericsson

- Andrea Bilet, Director, Certification and Surveillance Service, Italian National Agency for Cyber Security, Italy
- Dr. Elżbieta Andrukiewicz, Head of Cybersecurity Department, ITSEF Manager, National Institute of Telecommunications, Poland
- Peter Haigh, Principal Tech Director, Telco, Radio & EmSec, NCSC, UK
- Adriana Gutierrez, Cybersecurity Technician, Spanish National Cybersecurity Instituto (INCIBE), Spain
- Jerker Berglund, Telecom expert, PTS, Sweden

Lunch: 12.00 -13.00

Bilateral sessions with experts, 30 minutes per session between 13.00 -15.30

- #1 5G RAN – One software track security benefits for deployed networks
Host: Anna Kähre, Product Security Director, Ericsson
- #2 3GPP / SA3 Security
Host: Helena Flygare, Master researcher Platform security, Ericsson
- #3 Migration to quantum resistant algorithms in mobile networks
Host: John Mattsson, Expert Crypto Algorithms & Security Protocols, Ericsson



<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

Demystifying vulnerability management in telecom networks

Umair Bukhari
Head of Ericsson PSIRT
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Agenda



What is vulnerability?



Not all vulnerabilities are created equal



What does it take to exploit a vulnerability in telecom network?



What is in the control of a telecom network manufacturer?

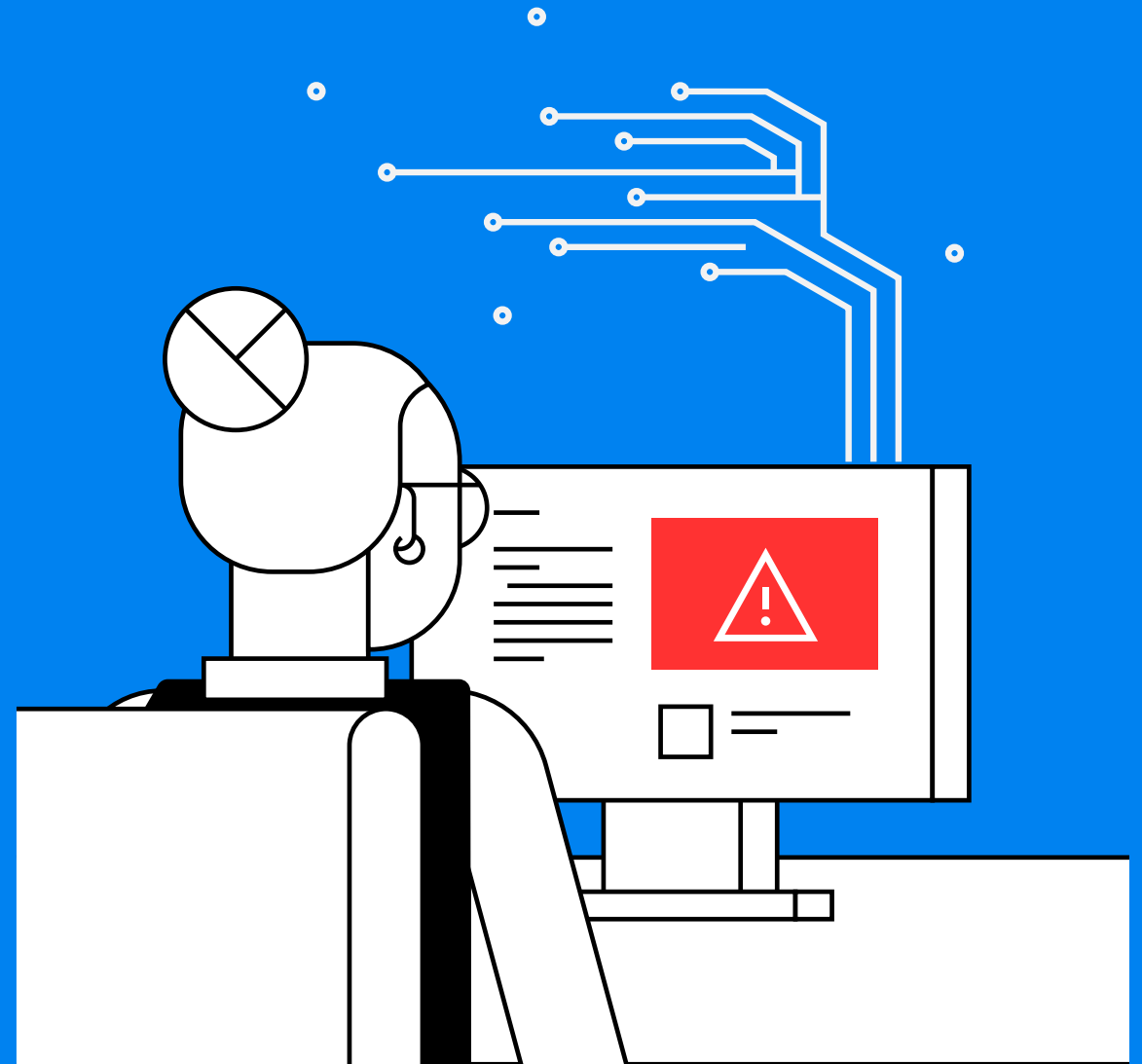


Key Takeaways

What is vulnerability?

- Commonly understood, a **vulnerability is a weakness in software** that can be exploited resulting in the compromise of security and privacy objectives.
- What is not so commonly understood is that a **vulnerability can also be caused by:**
 - The misconfiguration of a system or network,
 - A lack of hardening of software products,
 - Or a flawed architecture or deployment.

Therefore, it is incorrect to conflate the meaning of a vulnerability as just a software weakness that can be exploited.



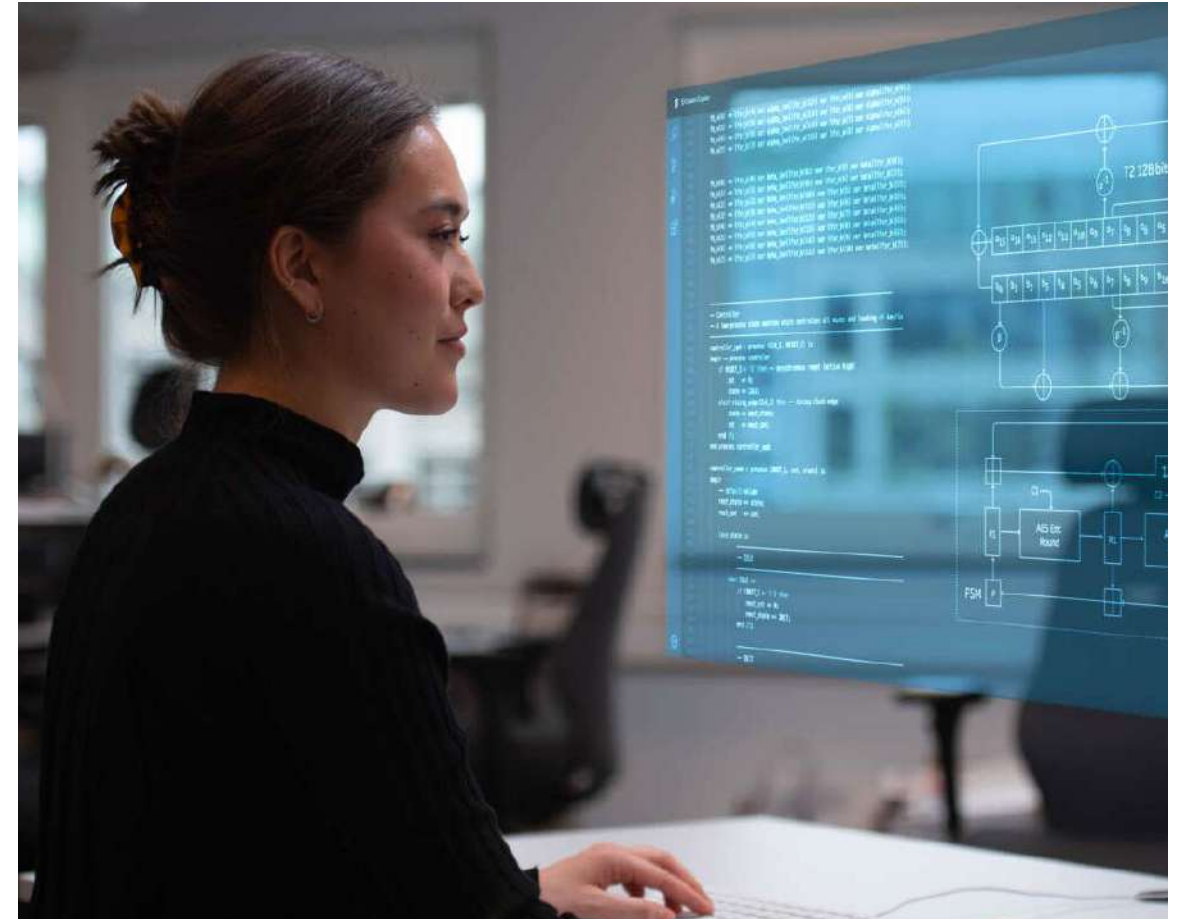
Common misconceptions around software vulnerabilities



“Code almost always contains vulnerabilities. It would be unrealistic to attempt to “free” all code of any vulnerability.” (OECD)

- **We agree with the OECD** and acknowledge that the number of newly discovered software vulnerabilities is high and rising.
- However, there are numerous misconceptions regarding software vulnerabilities, which are all untrue. Examples include:
 - **Fear that a single vulnerability or so-called “0-day-vulnerability”** by itself instantly provides any hacker with an immediate golden egg.
 - **A one size fits all approach to vulnerability management.**
 - **Emphasis on speed, expediting and disclosing excessive or confusing information.**

Source: [Encouraging vulnerability treatment \(oecd-ilibrary.org\)](https://www.oecd-ilibrary.org/encouraging-vulnerability-treatment)



Agenda



What is vulnerability?



Not all vulnerabilities are created equal



What does it take to exploit a vulnerability in telecom network?



What is in the control of a telecom network manufacturer?



Key Takeaways

Not all vulnerabilities are equal!



- To help identify the severity of a vulnerability, **a globally recognized standard exists.**
 - **CVSS – Common Vulnerability Scoring System.**
- **The base CVSS score** (as often discussed in the media) only considers the vulnerability in isolation.
- In reality, systems and telecom networks are implemented in a **security context.**
 - Layers of protective measures.
- **This security context is captured in the CVSS by the environmental and temporal security relevant criteria.**



Source: <https://www.first.org/cvss/>

Not all vulnerabilities are equal!



The environmental and temporal security relevant criteria:

- The **environmental situation** is scored by contextualizing the vulnerability in a specific environment.
 - It also considers the exposure (for example, internet facing),
 - If the system is monitored and administered by security professionals.
- The **temporal score** quantifies the temporal or timely aspects of a vulnerability.
 - After the discovery of a vulnerability, documentation, and tools for exploitation become available,
 - But also, mitigations and patches mature. Both factors respectively increase or decrease the risk of a vulnerability.



Not all vulnerabilities are equal!

Log4Shell example

- When discovered, the Log4Shell vulnerability had a CVSS score of 10.0.
- Contextual factors significantly impact if and how the Log4Shell vulnerability can be exploited.
- When Log4Shell score was calculated for telecommunication systems, the scoring and therefore, the risk was much lower.
- For this reason, despite the global attention and active exploitation, no major incidents were observed anywhere.

Proof points

- The annual report from ENISA on Incidents in Telecom security, only identified a single incident caused by a software vulnerability.
- This finding is also corroborated by the annual report from Verizon based on their incident response work where only 7% of incidents can be related to software vulnerabilities.

Sources: <https://en.wikipedia.org/wiki/Log4Shell> and <https://blog.cloudflare.com/exploitation-of-cve-2021-44228-before-public-disclosure-and-evolution-of-waf-evasion-patterns/> and https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

Sources: [Telecom Security Incidents 2021 – ENISA \(europa.eu\)](#) [2022-data-breach-investigations-report-dbir.pdf \(verizon.com\)](#)

– Figure 35, Figure 40, Page 31

Agenda



What is vulnerability?



Not all vulnerabilities are created equal



What does it take to exploit a vulnerability in telecom network?



What is in the control of a telecom network manufacturer?



Key Takeaways

The telecom-specific contextual environment



- The security posture of a deployed network depends on **four processes**, which are separate but interdependent.
- The security of a deployed network is **enabled by the previous process but made effective by the next process**.
- Any measure not implemented or implemented with a (software) weakness constitutes a vulnerability in the overall environment.
- These weaknesses when deployed in the network can later be abused by an attacker.

Operations process

- Secure operational procedures, e.g., segregation of duties, use of least privilege and logging
- Monitoring the security performance, vulnerability management and detection of attacks
- Response and recovery after breach

Deployment process

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening

Vendor product development process

- Secure hardware and software components
- Secure development processes
- Version control and secure software update

Telecommunications standardization process

- Secure protocols, algorithms, storage

What does it take to exploit a software vulnerability in a telecom network?



- Often the presence of a software weakness is not a sufficient condition for successful exploitation.
- Due to the multifaceted, multivendor, and highly interdependent nature of how telecom networks are realized, executing a successful attack is not trivial in networks with appropriate security hygiene.
- A successful attack on a deployed telecom network would require multiple security controls and processes to fail.

Operations process

- Secure operational procedures, e.g., segregation of duties, use of least privilege and logging
- Monitoring the security performance, vulnerability management and detection of attacks
- Response and recovery after breach

Deployment process

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening

Vendor product development process

- Secure hardware and software components
- Secure development processes
- Version control and secure software update

Telecommunications standardization process

- Secure protocols, algorithms, storage

What does it take to exploit a software vulnerability in a telecom network?



- This design means the exploitation of a vulnerability only happens,
 - If these protective measures are compromised,
 - An attacker has many options far beyond software vulnerability exploitation that also require less investment to achieve a broader set of objectives.
- Minimizing of critical software vulnerabilities is necessary, but not sufficient if the ultimate objective is to minimize cyber incidents.
- System vulnerabilities and effectiveness of protective measures, matter a lot
- Need to be considered by policymakers when developing vulnerability management policy frameworks.

Operations process

- Secure operational procedures, e.g., segregation of duties, use of least privilege and logging
- Monitoring the security performance, vulnerability management and detection of attacks
- Response and recovery after breach

Deployment process

- Solid network design with security and resilience in mind
- Configuration of security parameters, hardening

Vendor product development process

- Secure hardware and software components
- Secure development processes
- Version control and secure software update

Telecommunications standardization process

- Secure protocols, algorithms, storage

Agenda



What is vulnerability?



Not all vulnerabilities are created equal



What does it take to exploit a vulnerability in telecom network?



What is in the control of a telecom network manufacturer?



Key Takeaways

Lifecycle of a vulnerability

In a commonly used software component



Lifecycle of a vulnerability

Identification of a vulnerability by a security researcher

1

Disclosure of the vulnerability to the component vendor, e.g., an operating system vendor

2

Operating system vendor assessment; is their software vulnerable or not? In this case it is

3

Identification of the impacted version/s of the OS

4

Development of a fix

5

Communication of the vulnerability along with the instructions on how to fix

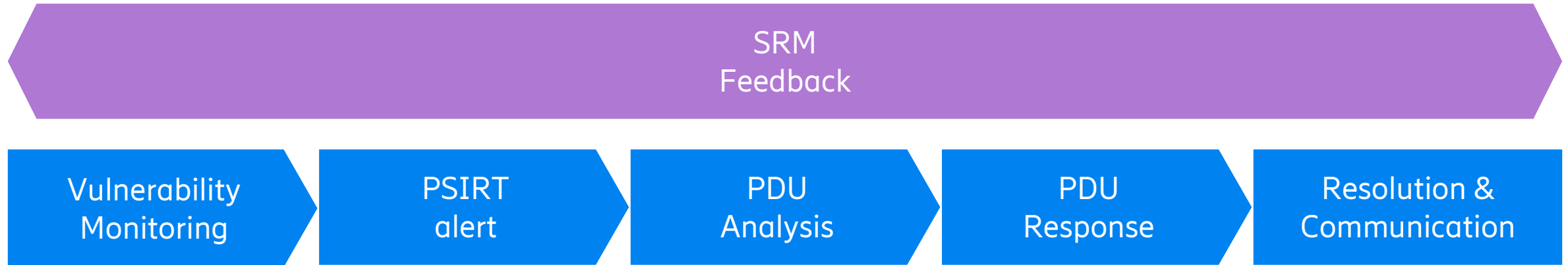
6

Ericsson vulnerability management process picks up and processes the vulnerability producing the fix

7

- Telecom manufacturers must have a process to discover and handle vulnerabilities throughout the entire life cycle.
- Telecom products have strict availability and performance requirements.
- Speed of fix delivery and ensuring flawless network functionality needs to be balanced.

Vulnerability management across the entire network



PSIRTs' in-house vulnerability management service is supported by open industry standards, including CVE¹ for identification of vulnerabilities, CPE² for structured naming of open source and commercial software, and CVSS3³ for presenting the overall vulnerability impact and severity.

1. CVE – Common Vulnerabilities and Exposures. CVE system is maintained by MITRE organization.

2. CPE – Common Platform Enumeration. CPE scheme is maintained by NIST (U.S. National Institute of Standards and Technology).

3. CVSS3 – First organization (Forum of Incident Response and Security Teams) is responsible for CVSSv3 specification.

PSIRT incident handling process and feedback loop

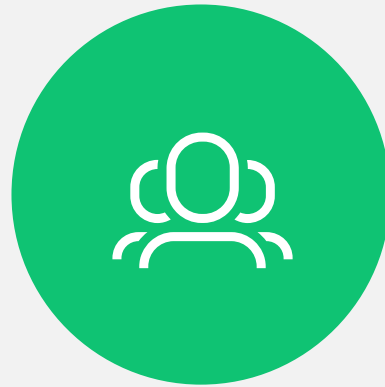


Triage



Ensure that the reported event is classified as a product security incident.

Investigation



Investigation team is set up and determines the scope of security and privacy impact based on collected evidence.

Containment, Eradication and Recovery



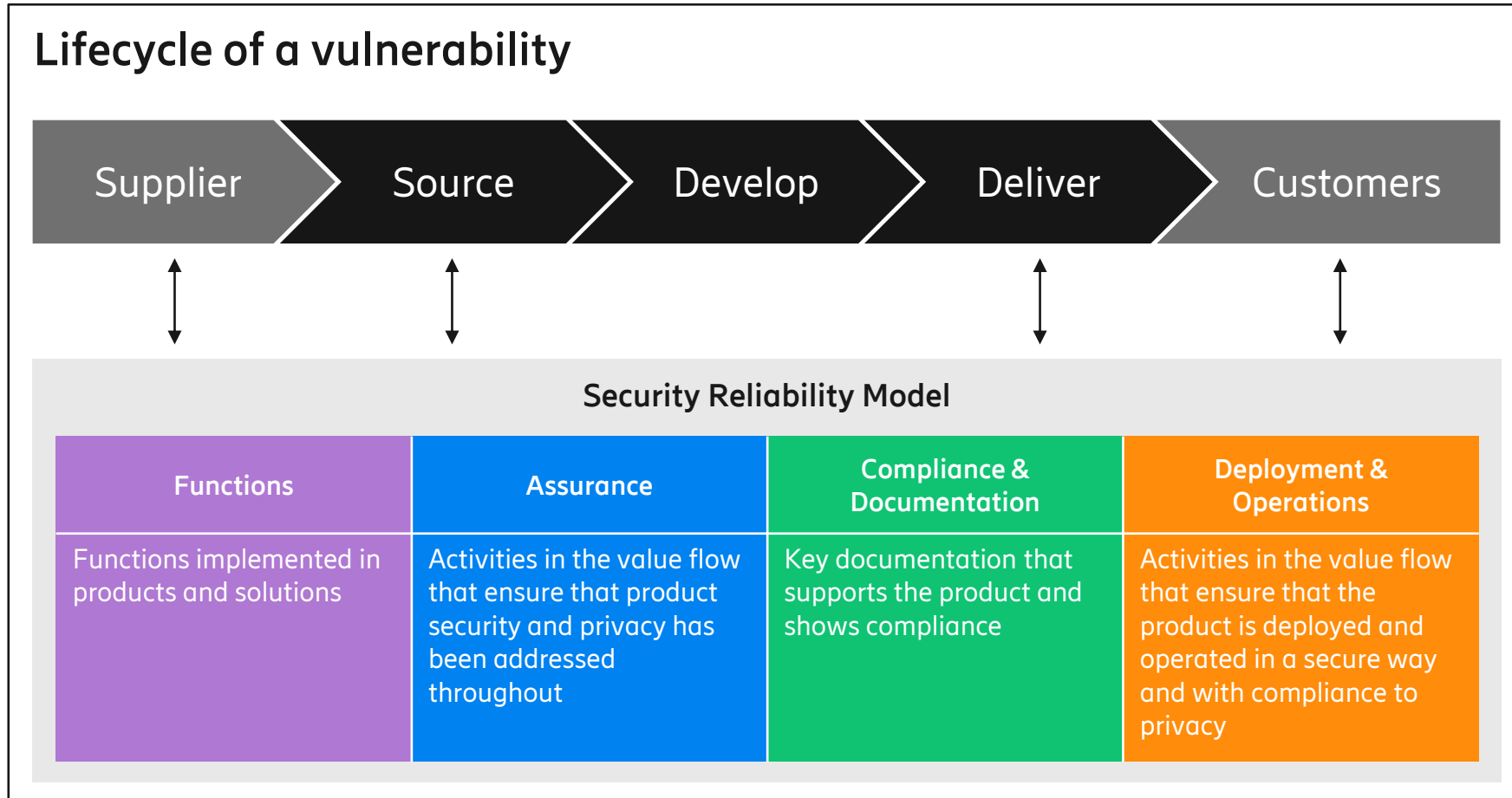
Containment efforts start immediately. A root cause analysis is done in parallel to devise both a short- and long-term recovery plan.

Post-Incident Activity and Feedback Loop



Systematic root cause analysis and lessons learned activities. Feedback is shared with all concerned parties.

What is in the control of a telecom network manufacturer?



- Manufacturers need to implement multiple measures that together help ensure the development of secure products.
- Ericsson **Security Reliability Model (SRM)**.
- The SRM enables managed, risk-based software development processes to ensure security and privacy implementation of requirements tailored to the target environment (context) and demands.

Agenda



What is vulnerability?



Not all vulnerabilities are created equal



What does it take to exploit a vulnerability in telecom network?



What is in the control of a telecom network manufacturer?



Key Takeaways

Recommendations to policy makers



- The following key attributes merit managing vulnerabilities differently in the context of telecom networks compared to consumer devices or enterprise (corporate) IT networks:
 - Criticality of the system
 - Active security management and monitoring of the system
 - Bilateral communication channels for vulnerability disclosure
- Rather than aiming to remove all vulnerabilities, the most effective measure is to take a holistic approach and ensure that security best practices are implemented at all levels.
- Doing so guarantees that systems are protected against all types of attacks, apart from targeting software weaknesses for improving overall security and minimizing the risk of a security or continuity incident.



Recommendations to policy makers



Vulnerability management in the context of telecommunications networks, Ericsson suggests:

- Define and implement a multiparty 'Common Vulnerability Disclosure' (CVD) process including all relevant parties
- Ensure that system vulnerabilities and software vulnerabilities are addressed in an all-encompassing way.
- Obligations should be symmetrical for all security-relevant stakeholders.
- Provide all responsible parties in the trust stack with incentive to implement the required processes and tooling to minimize weaknesses during standardization, development, deployment, and operations.





<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

Security Operation Automation

Bodil Josefsson

Business Manager Security Solutions
Ericsson

June 26-27, 2023

Conference for Governments and Regulators

Agenda



Introduction



Security Operations in Telco Networks. What is it?



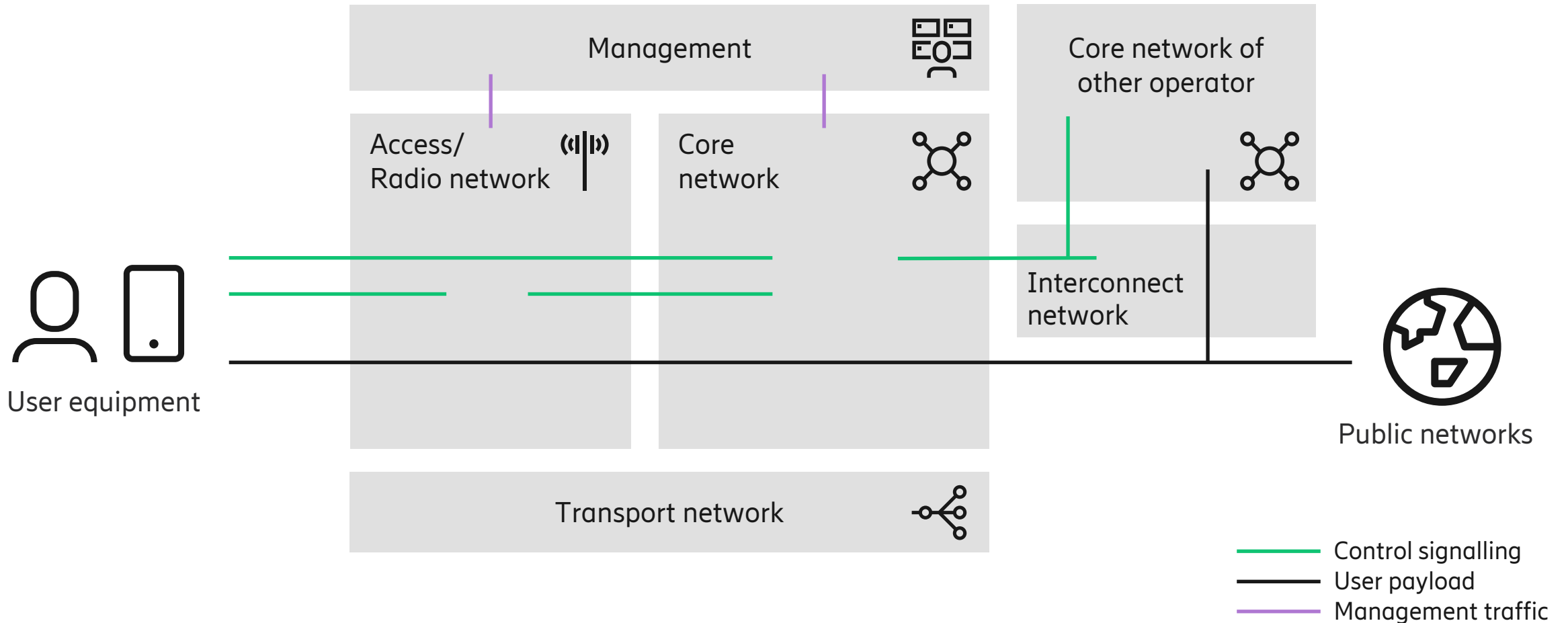
Automated Security Operations. Why do we need it?



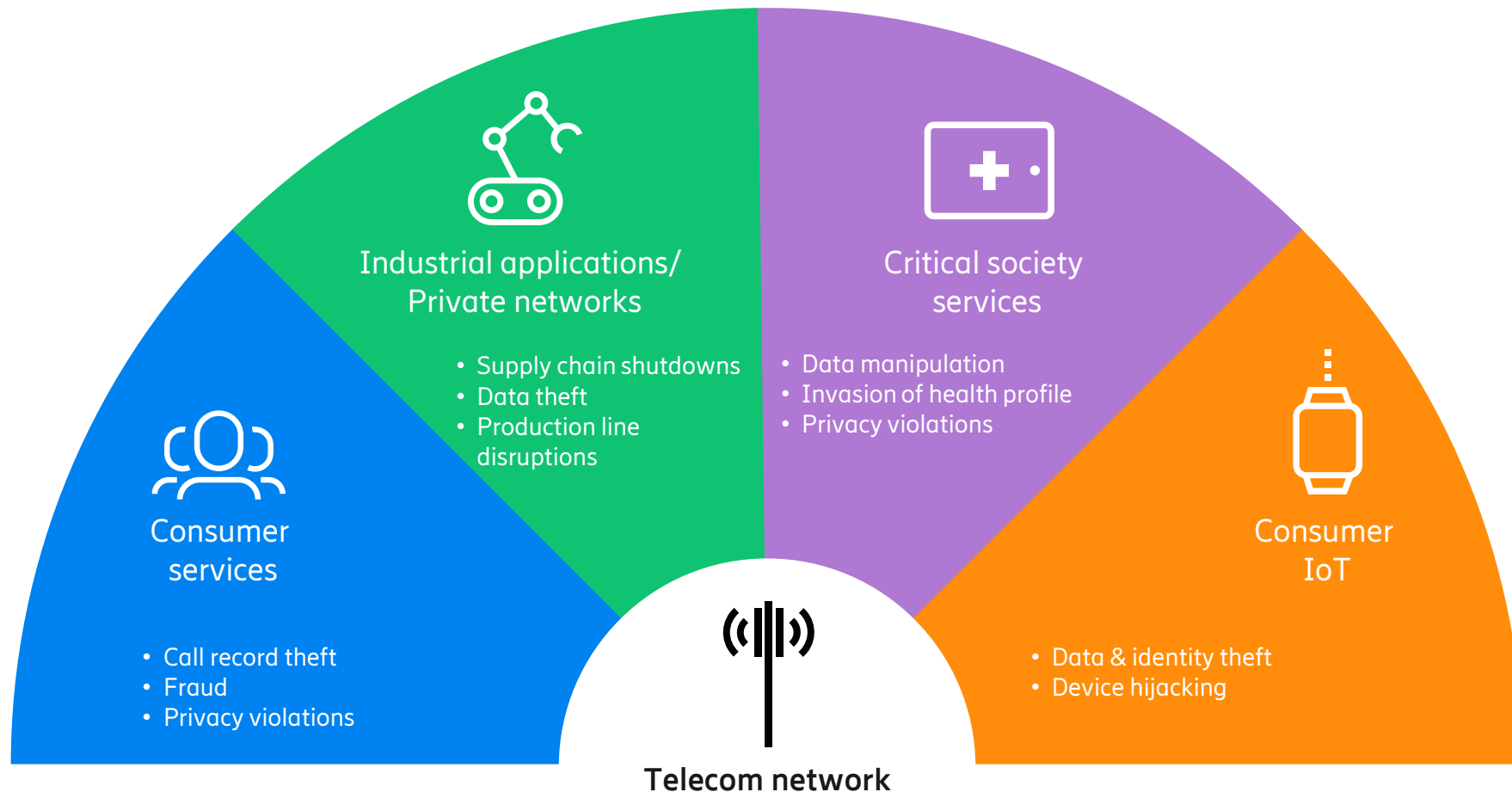
Key conclusions

High level mobile network overview

Logical elements and logical planes



A mobile telecom network needs to be secure across multiple contexts and use-cases



Agenda



Introduction



Security Operations in Telco Networks. What is it?

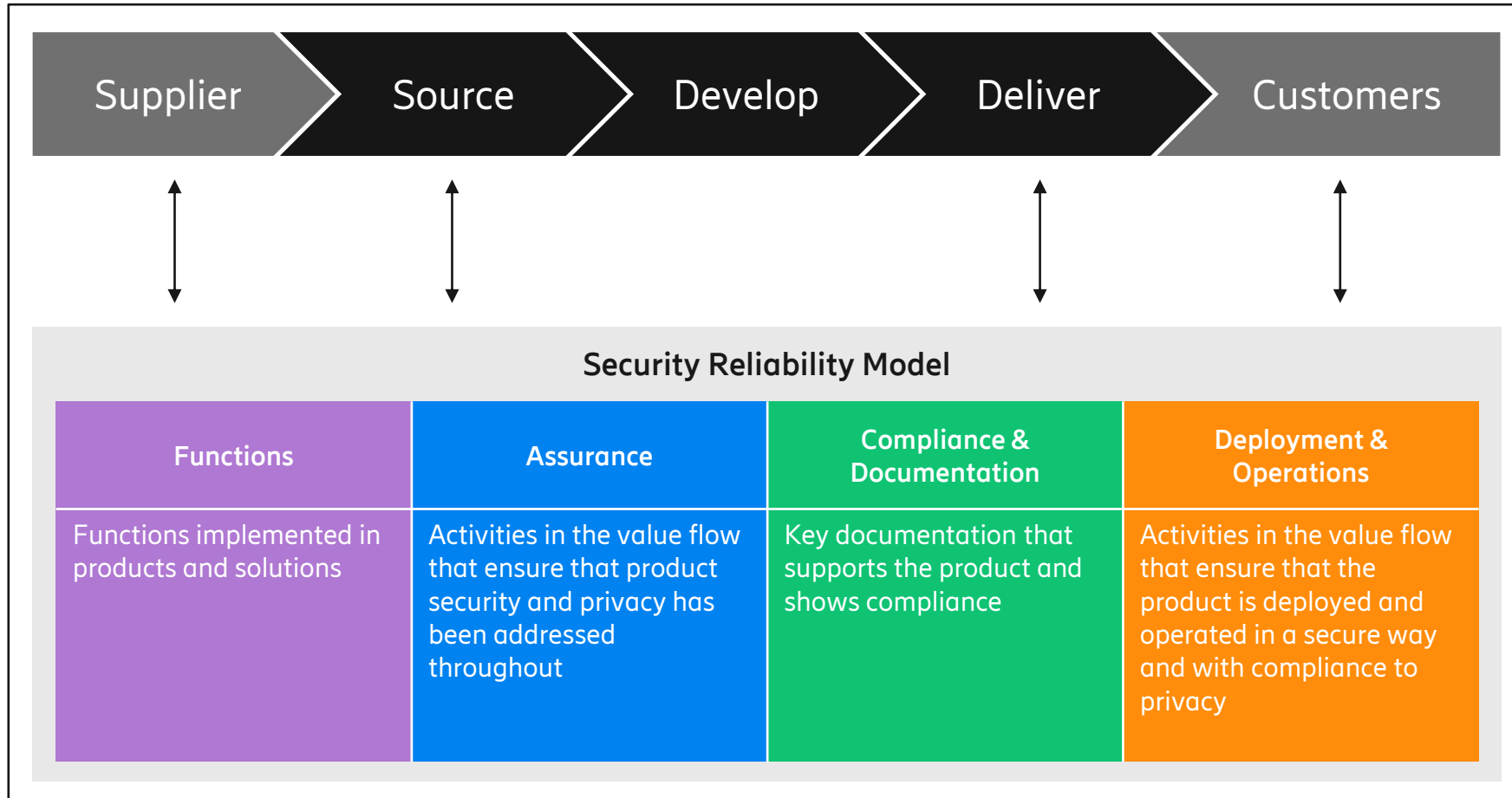


Automated Security Operations. Why do we need it?



Key conclusions

Securing a telecom network product is a must ...

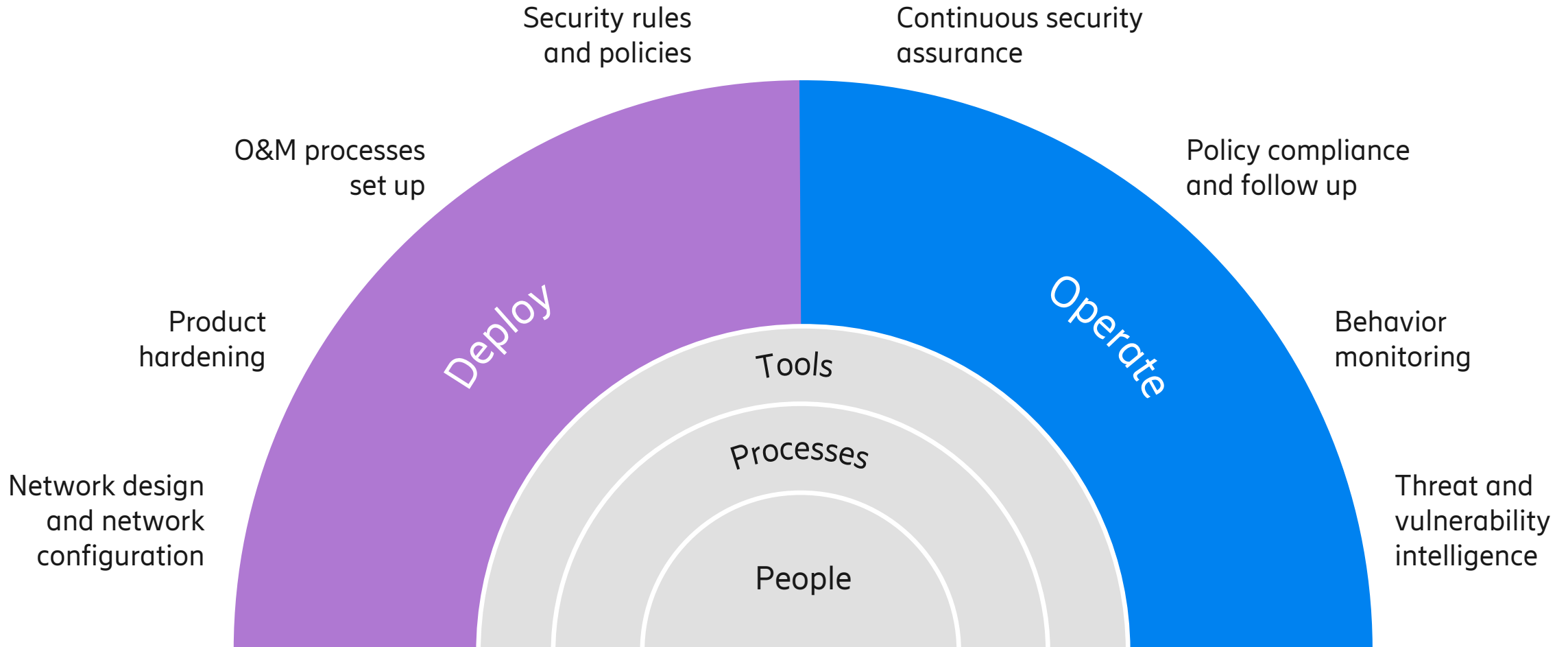


...but not sufficient

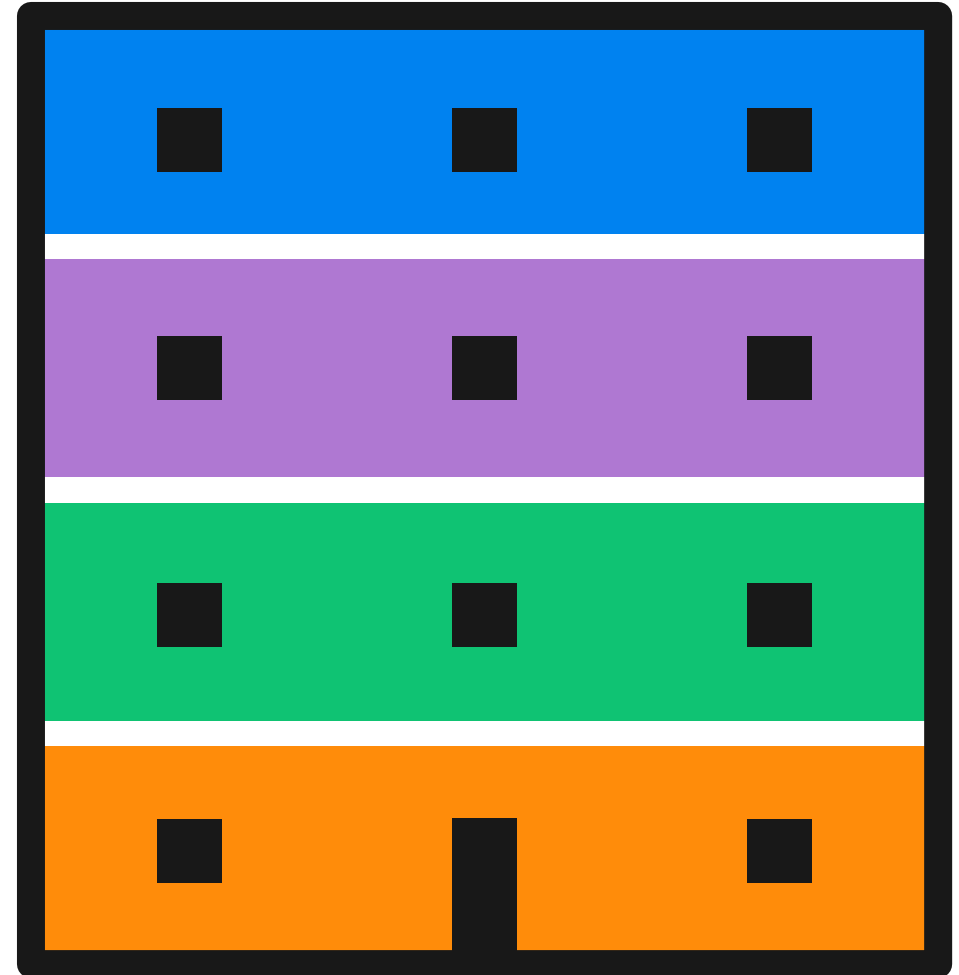
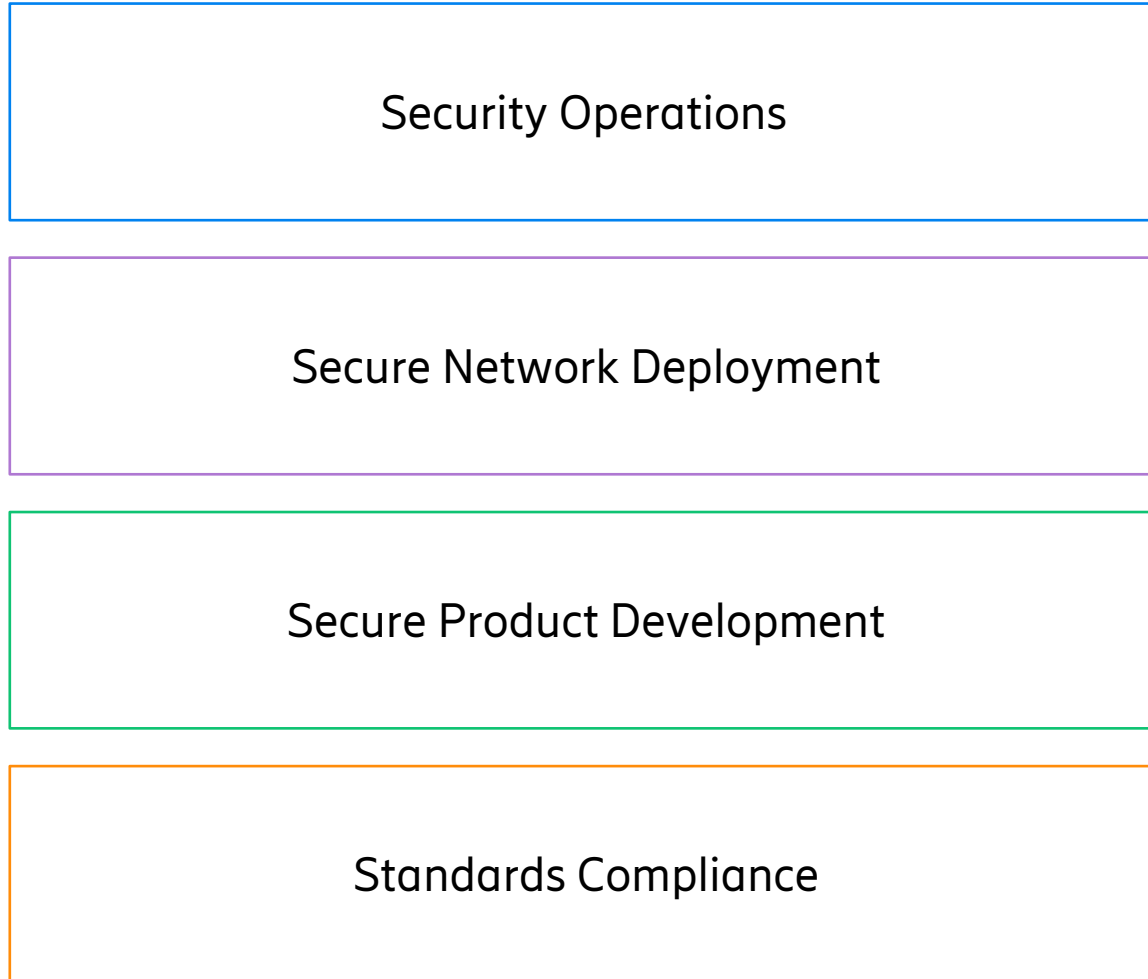
...you also need to build and use the network in a secure way



Deployment and operational processes



Telecom security is like building a secure house...



...in the end, the actions determine whether it is safe or not



Agenda



Introduction



Security Operations in Telco Networks. What is it?



Automated Security Operations. Why do we need it?



Key conclusions

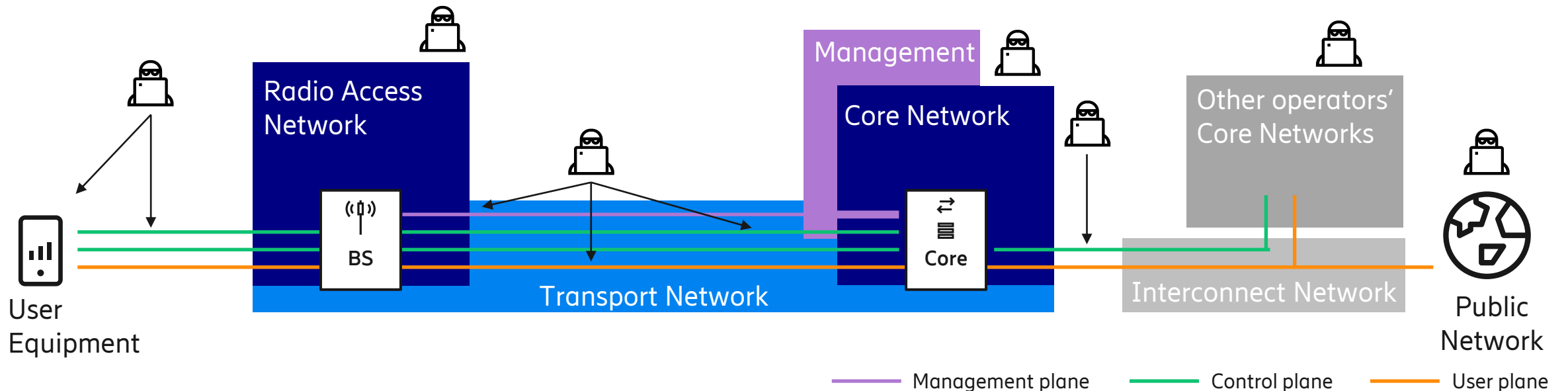
Most common issues resulting in security breach or incident



- Security policy not enforced
- Poor operational procedures

- Lack of hardening
- Unsecure or incorrect network configuration

- Lack of visibility, control and continuous monitoring



A paradigm shift is required to ensure continuous high security posture



From



Security designed for a static network



Manual security processes



Limited security visibility



To



Security for dynamic and distributed networks

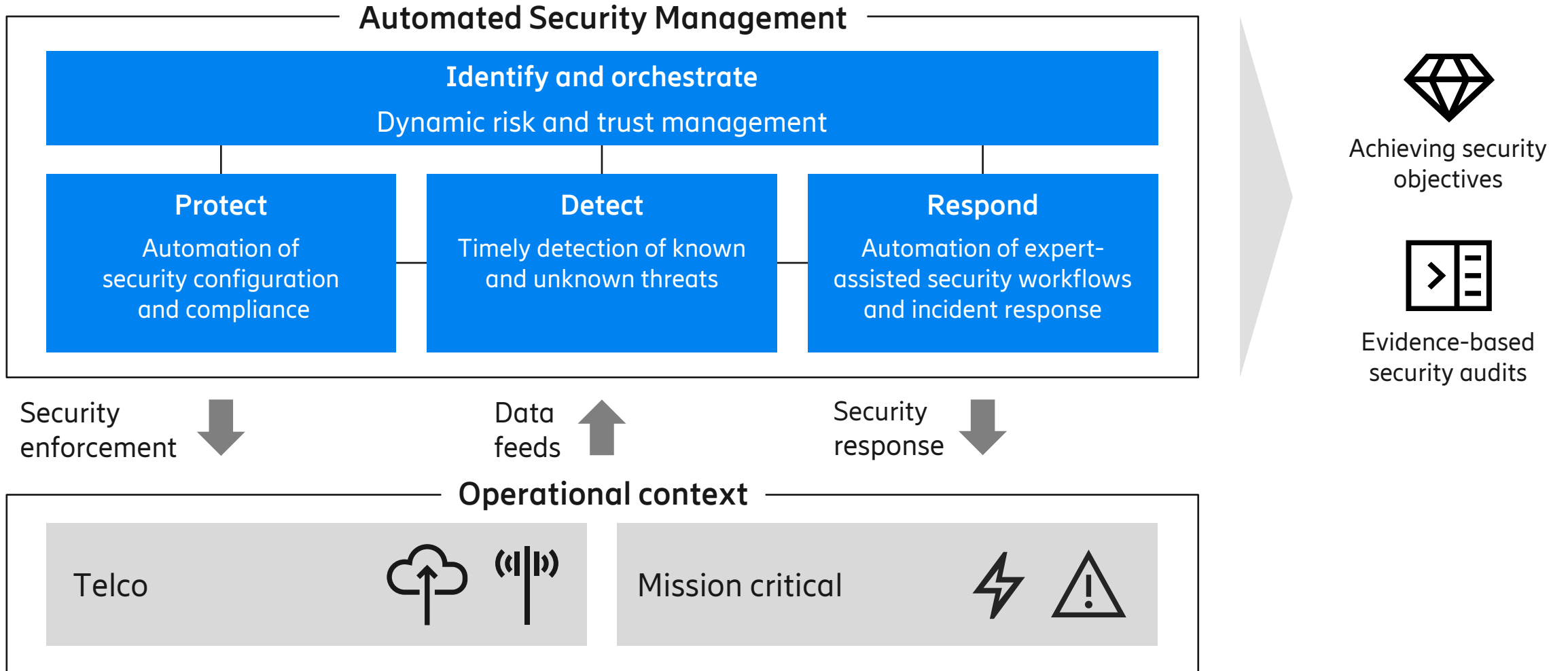


Automated security processes



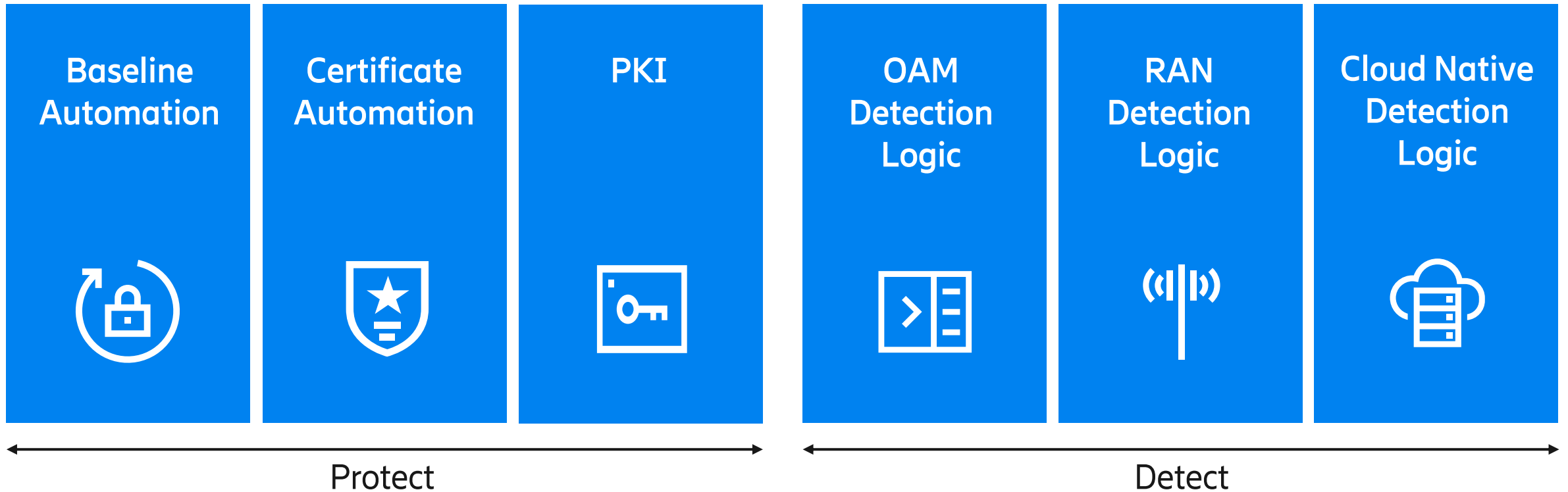
End-to-end security visibility

Automation is the key to high security posture



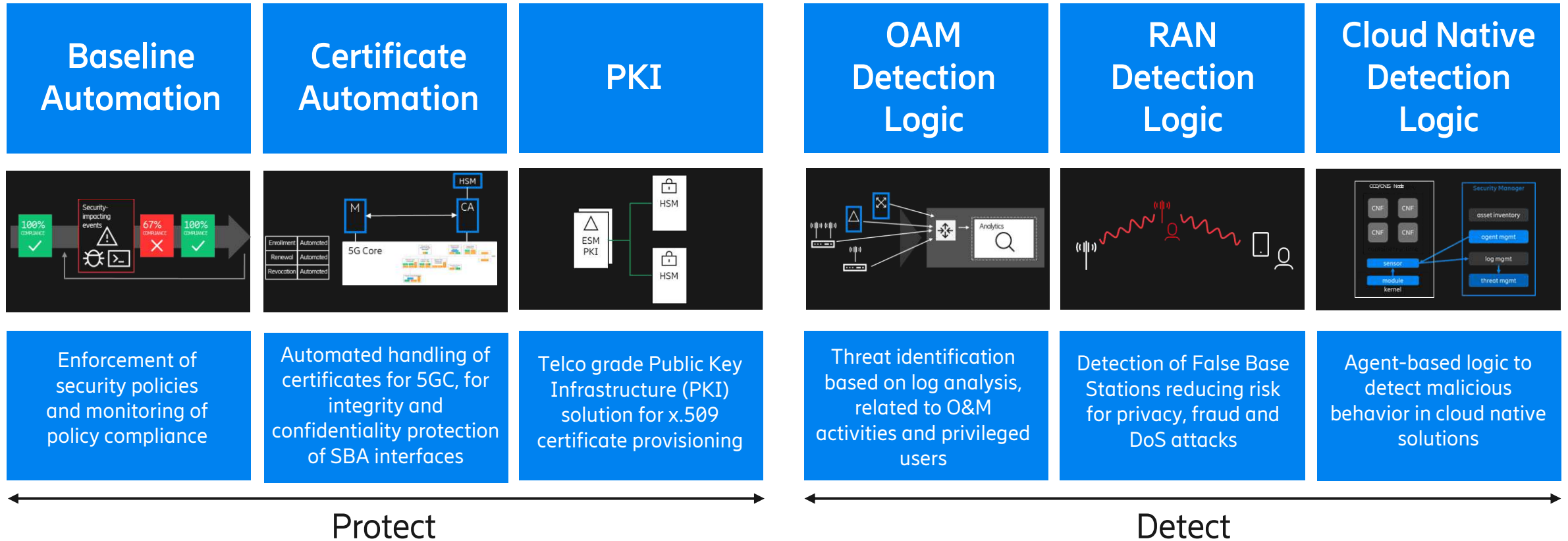
Ericsson Security Manager

Use cases for security management



Ericsson Security Manager

Use cases for security management



Benefits from security automation



Customer feedback on Ericsson Security Manager



Customers in 4 out of 5 Market areas



Industry leading security solution



Swisscom as lead customer



Customer feedback

Swisscom on Security policy visibility: "With ESM we have turned lights on in a cave"

Asian customer: "With ESM we can comply and show compliance status to regulators (IMDA)"

North American customer: "ESM selected as the 5G Security Monitoring solution"

Erillisverkot: "With ESM we will have the most reliable, secure, and sturdy network"

DnB, Malaysia: "With ESM we will have assurance that cyber threats are being efficiently monitored and managed"

Agenda



Introduction



Security Operations in Telco Networks. What is it?



Automated Security Operations. Why do we need it?



Key conclusions

Key conclusions



- A mobile telecom network needs to be secure across multiple contexts and use-cases
- In addition to developing secure products, we need to make sure that they are deployed and operated securely
- A paradigm shift is required to enable high security posture of deployed networks
- Automation is a must in order to ensure security and privacy for the end-users





<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

Current state of evolving Open RAN security

Jason S. Boswell, CISSP
VP, Head of End-to-End Security
Ericsson North America

Joakim Jardal
Cloud RAN Security SPM
BNEW

June 26-27, 2023
Conference for Governments and Regulators

RAN Terminology



• OpenRAN

Industry term for open radio access network architecture. A RAN with open interoperable interfaces, RAN virtualization, and big data and AI-enabled RAN

• O-RAN

Refers to O-RAN Alliance architecture

• OpenRAN

Refers to initiatives driven by TIP'S OpenRAN Project Group

RAN Terminology

• Cloud RAN

Cloud RAN is a virtualized RAN that is designed to be cloud native, built in a future proof architecture and incorporating key elements such a microservices, CI/CD, and containerization

• vRAN

Technical approach to run RAN functions as disaggregated software on common hardware platform, generating additional RAN architecture flexibility, platform harmonization, and simplification

US FCC CSRIC VIII report states: "Open RAN includes O-RAN, vRAN, Cloud RAN, and other technologies."

Open RAN Security Posture



Security Advantages¹

Open-source software enables transparency and common control

Open interfaces ensure transparency, use of standard protocols, and interoperability of secure protocols

Disaggregation enables supply chain security through diversity

AI/ML enables visibility and intelligence to achieve greater security

Security Risks

▶ Malicious actors can introduce and exploit vulnerabilities in open-source software

▶ O-RAN's new open interfaces must be built on a foundation of security specifications.

▶ Disaggregation expands the attack surface by adding new functions and interfaces while also introducing supply chain risks.

▶ AI/ML is known threat vector across society and must be protected in O-RAN deployments

¹O-RAN Alliance paper, "O-RAN Minimum Viable Plan and Acceleration towards Commercialization", July 2021.

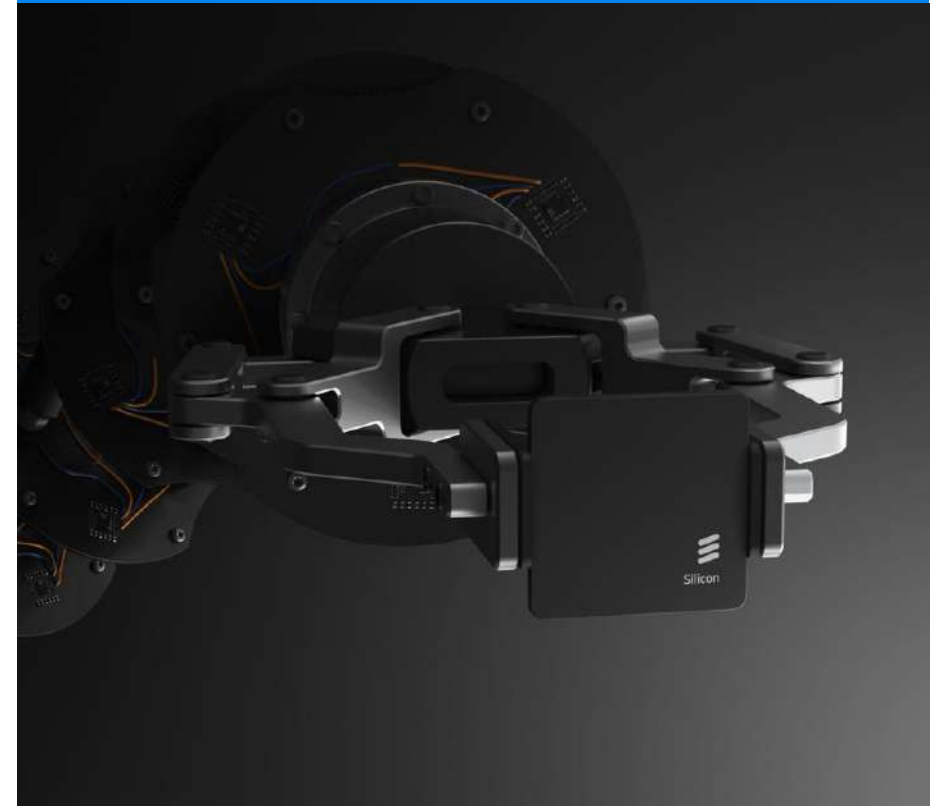
O-RAN WG11 Security Enhancements

(thru of March 2023)

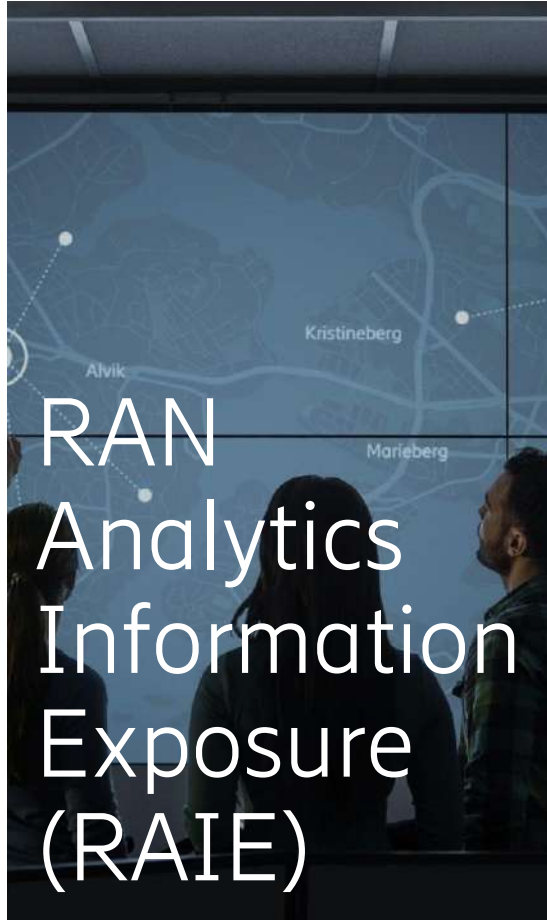


- TLS 1.2 and TLS 1.3.
 - TLS and mTLS versions 1.2 and 1.3 have been specified across O-RAN interfaces
- Certificate-based mutual authentication
 - mTLS with PKI X.509 certificates on O-RAN internal and external interfaces.
- CMPv2 for certificate management
- OAuth 2.0 for machine-to-machine authorization
- IEEE 802.1X port-based network access control on Open Fronthaul
- Robustness against volumetric DDoS attacks
 - Supported at all network functions terminating all network interfaces
- Lifecycle management for network functions and applications
- Security event logging
- Software Bill of Materials (SBOM)
- Secure credentials
 - Encrypted key storage, Hardware root of trust, Chain of trust, and Remote attestation

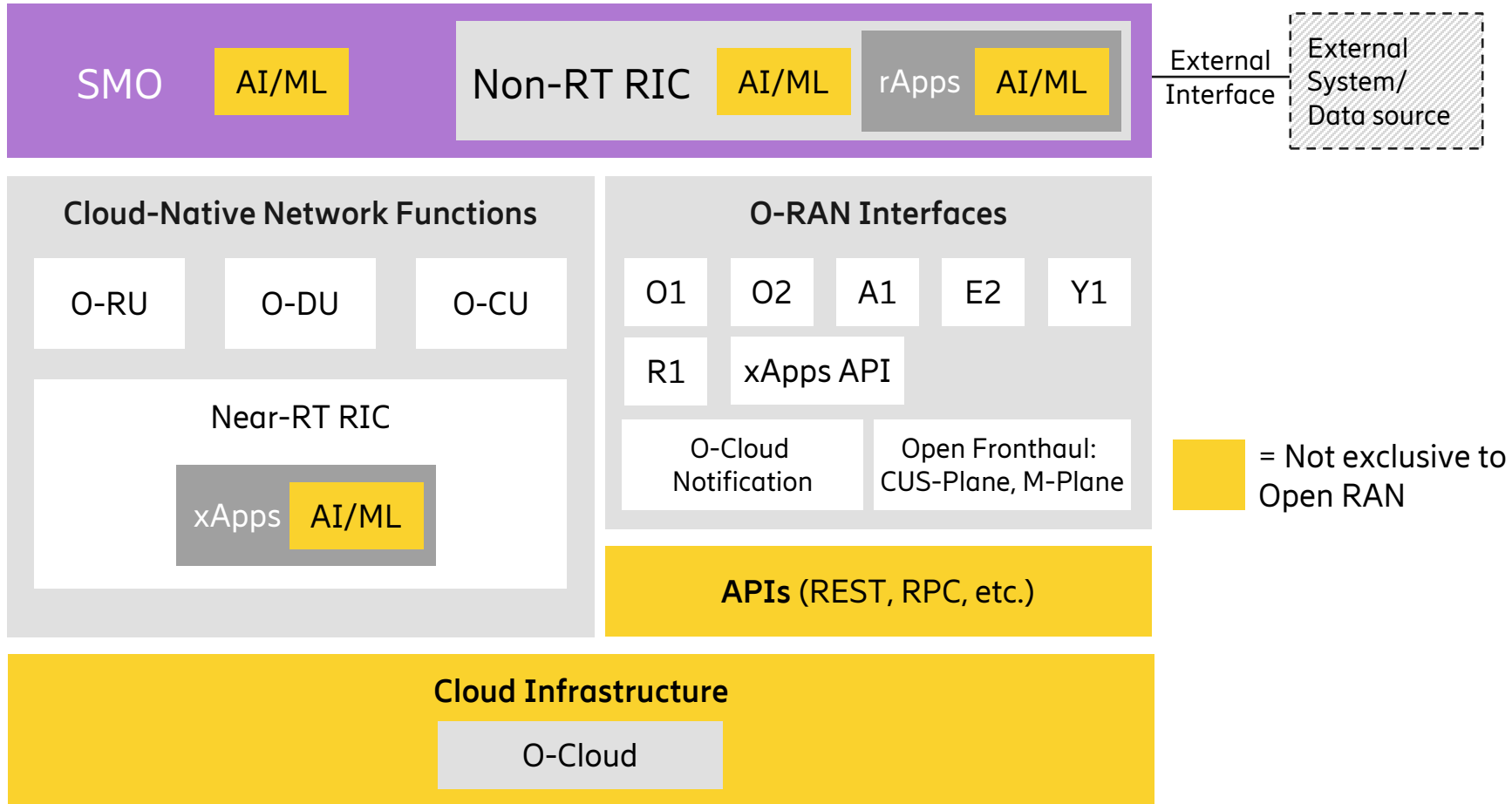
Ericsson has been a leader in the O-RAN Alliance WG11 to add security requirements



Evolving O-RAN attack surface



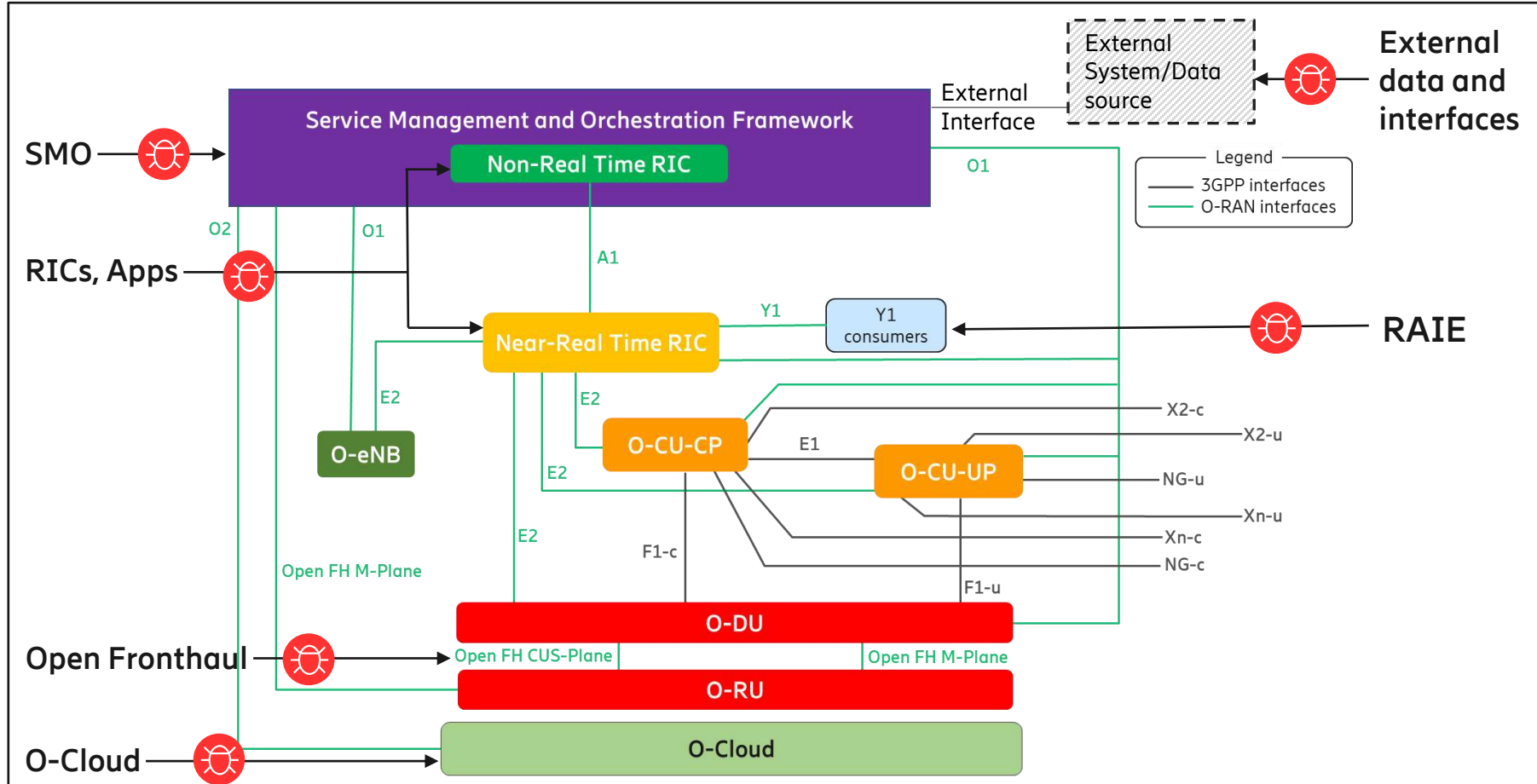
Open RAN Attack Surface



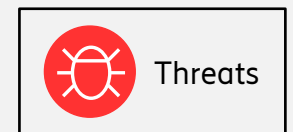
- Not exclusive to Open RAN**
- AI/ML
 - APIs
 - Cloud-native technologies
 - Cloud Infrastructure

- O-RAN Architecture**
- SMO
 - Non-RT RIC and Near-RT RIC
 - O-RU, O-DU, O-CU
 - O-Cloud
 - O-RAN Interfaces

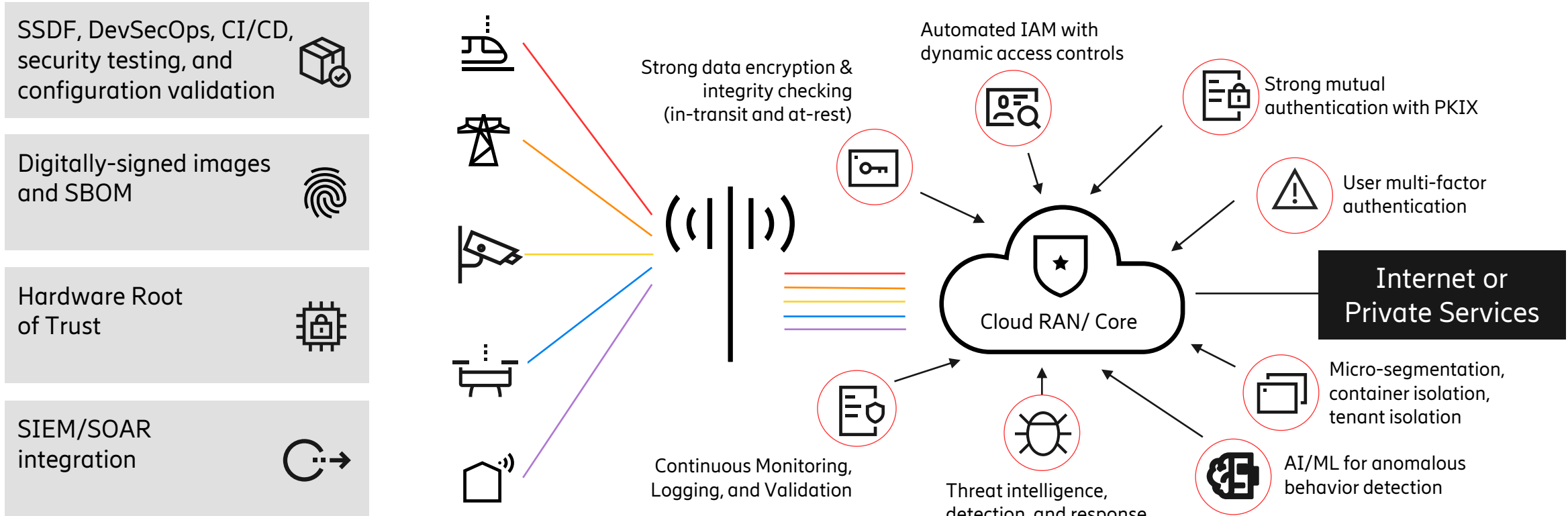
Open RAN attack surface needs ZTA



- O-RAN Alliance is pursuing a ZTA in accordance with NIST SP 800-207
- ZTA changes how we think about securing RAN to protect against external and internal threats



Zero Trust Architecture is the path forward to Secure Open RAN



Cloud providers and MNOs may share security responsibilities in a manner that requires the operators to take responsibility to secure their tenancy “in the cloud.” – US DHS CISA

Zero Trust Maturity Model for Telco

[Zero Trust Maturity Model | CISA](#)



Traditional

- Perimeter-based approach
- IAM for management plane

Initial (Telco entry level)

- Strong encryption of sensitive data in transit and at rest using standardized ciphers
- Identity and Access Management (IAM), including principle of least privilege on signaling and user planes
- PKI-based Mutual Authentication for machine-to-machine communications
- Network micro-segmentation and isolation
- Secure software development with Security-by-design with and automated vulnerability testing
- Security Information Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR) integration
- Continuous Monitoring, Logging, and Alerting
- Digitally-signed images

Advanced

- Multi-Factor Authentication (MFA) for human users
- OAuth 2.0 for authorization between digital systems
- Threat Intelligence (TI)
- Software bill of materials (SBOM)
- Key Management backed by Hardware Security Module (HSM)
- Secure software development based upon DevSecOps

Optimal

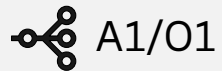
- Strong sensitive Data Encryption for data-in-use using TEE and NIST approved ciphers
- IAM with dynamic access control policies
- Anomalous behavior detection, using artificial intelligence/machine learning (AI/ML)
- Threat and Endpoint Detection and Response (TDR/EDR)
- Secure software development based upon NIST SSDF

Ericsson Cloud RAN's security posture



Ericsson Cloud RAN evolution

EIAP (SMO)



Ericsson Cloud RAN SW

Cloud platform (CaaS)

General purpose HW



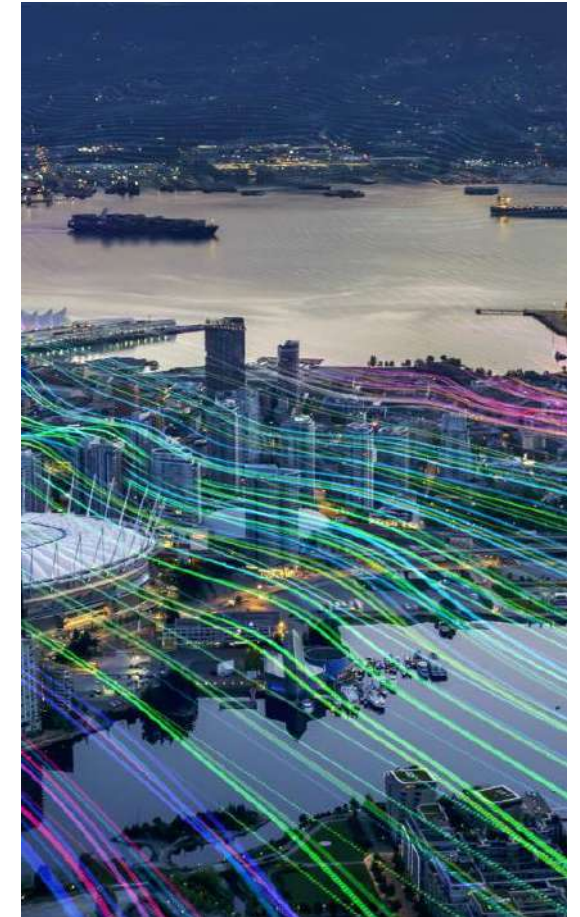
Open Fronthaul 7-2x
with ULPI

Radio



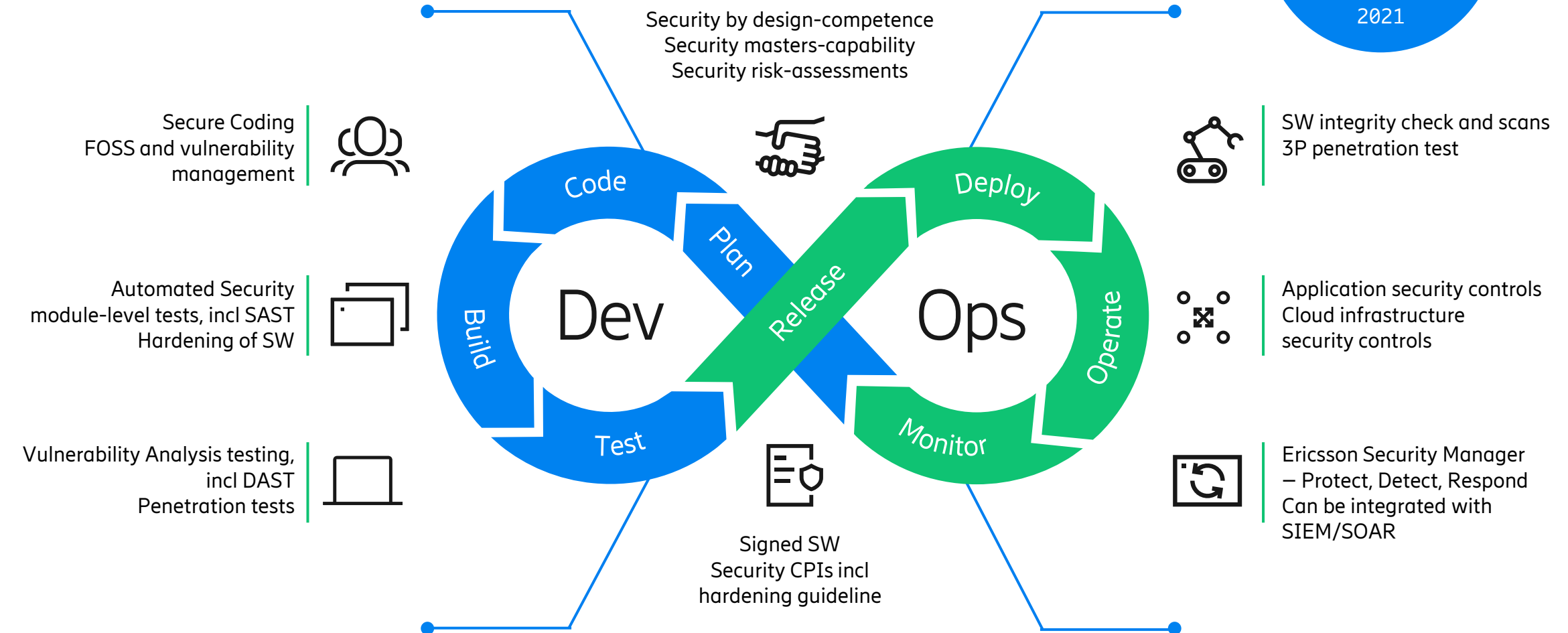
Ericsson Security Posture

- Ericsson SRM
- Industry best security practices
- ZTA security controls
- O-RAN security compliant



Secure product development

Leveraging company-wide security by design principles (Ericsson SRM) and experiences from Integrated RAN



Security functions in Cloud RAN to enable ZTA

Comparison with Integrated RAN and O-RAN

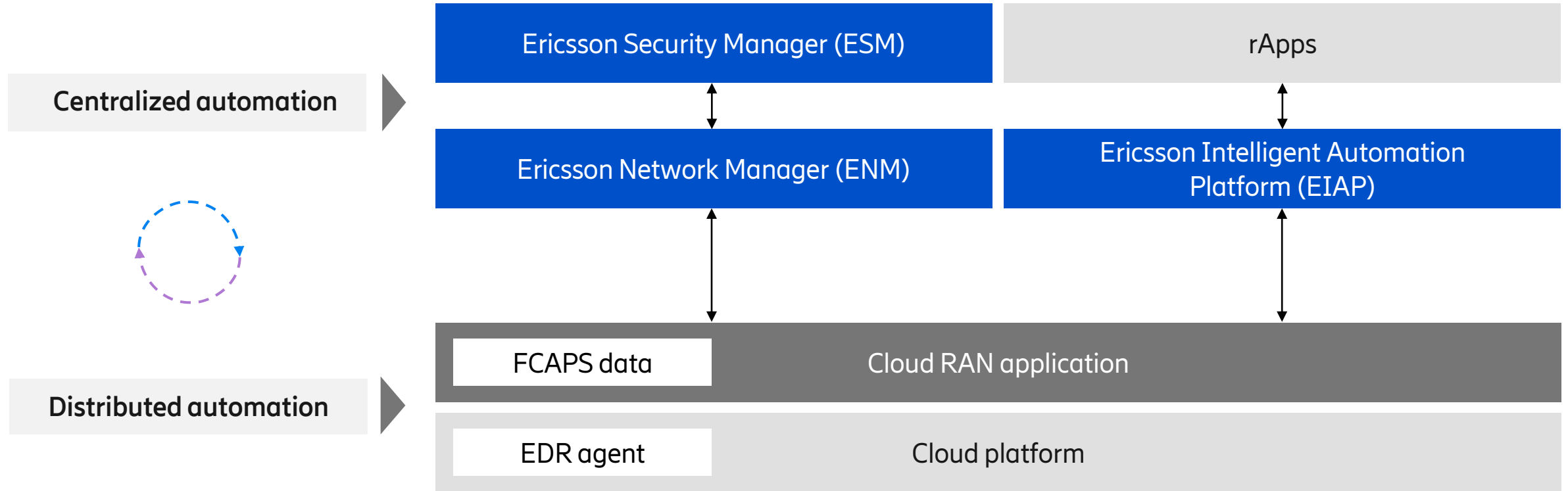


Protect surface	Integrated RAN	Cloud RAN	O-RAN
Secure storage	●	● Cloud platform responsibility	●
Secure environment	●	● Cloud platform responsibility	●
Access control	●	● Cloud platform + Application	●
Trustworthy software	●	● Cloud platform + Application	●
Monitoring and logging	●	● Cloud platform + Application	●
Protection of internal interfaces	●	●	●
Protection of external interfaces	●	●	●
Protection of O&M data	●	●	●

● In scope ● Not in scope ● Specification in progress

Intelligence and automation for security

Ericsson Security Manager (ESM) and/or rApps

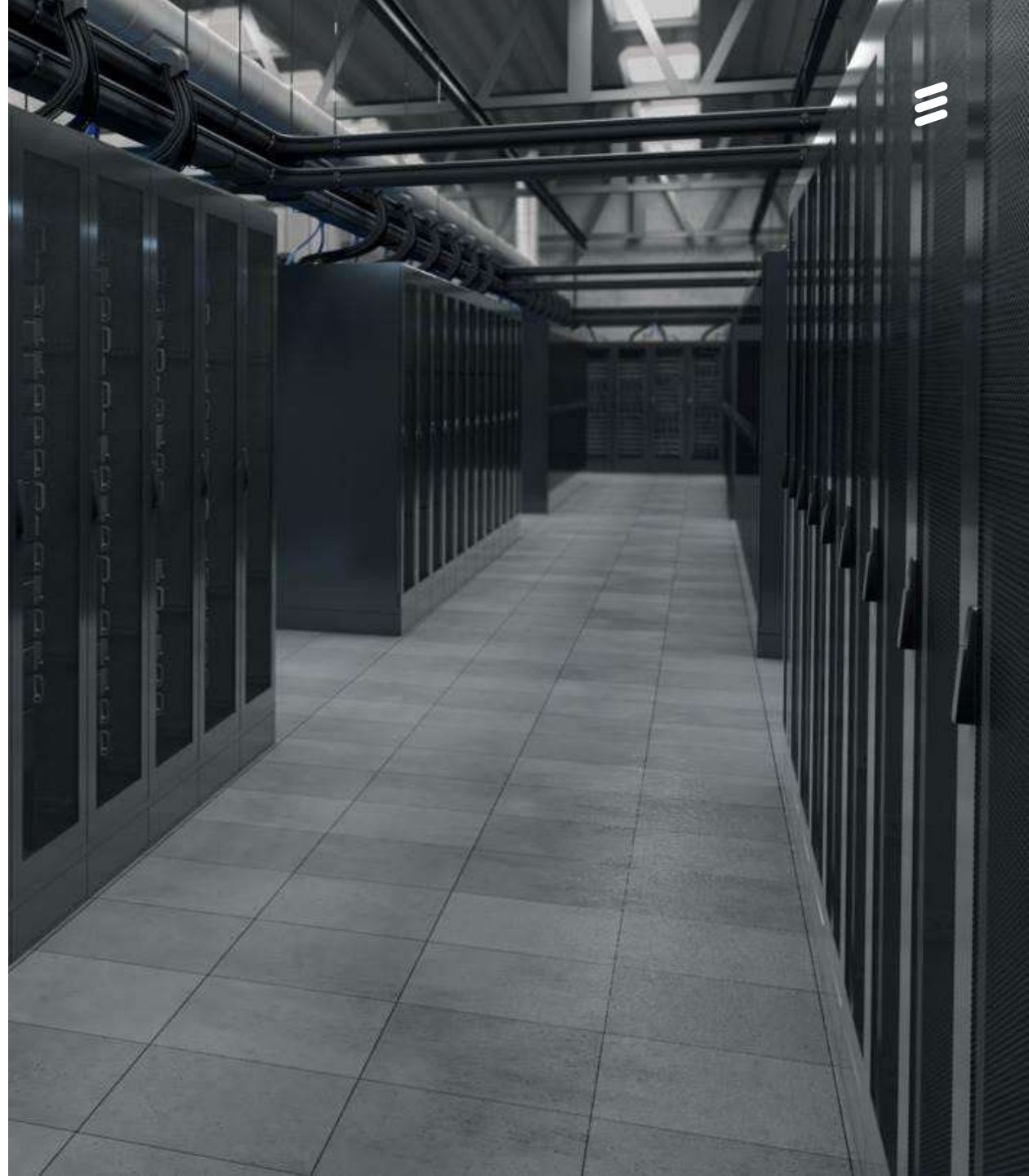


Centralized security baseline automation and detection capabilities

<https://www.ericsson.com/en/blog/2022/6/why-smo-provides-an-ideal-platform-for-intelligent-open-ran-security>

Key Takeaways

- Open RAN includes O-RAN, Cloud RAN, and other technologies.
- The Open RAN attack surface area is the sum of:
 - O-RAN architecture
 - General Open RAN features, such as AI/ML and APIs
 - Deployment considerations, such as cloud-native technologies and cloud deployment models .
- The path forward to a secure Open RAN is a Zero Trust Architecture.
- O-RAN Alliance WG11 has enhanced the O-RAN security posture, with Ericsson's leadership, but there is more work to be done.
- The O-RAN architecture continues to evolve introducing new security risks. Ericsson is leading to secure the new functions and interfaces.
- Cloud RAN and EIAP are Ericsson's secure Open RAN solution.





<https://www.ericsson.com/en/5g>
<https://www.ericsson.com/en/security>



Parking Lot

Current top threats to O-RAN architecture

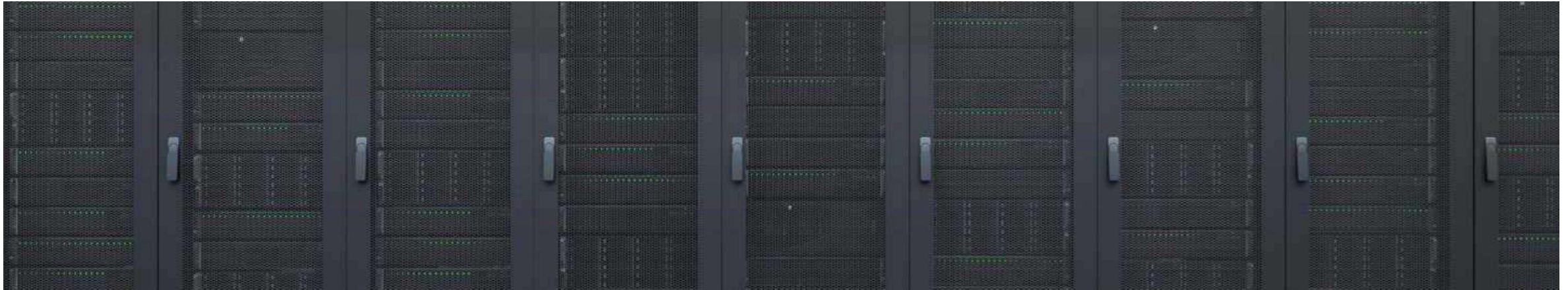


- External threat actor exploits SMO's External Interfaces by poisoning external AI/ML data imported to SMO
- External threat actor exploits API vulnerability to gain access to SMO via an External interface
- Threat actor on SMO uses O2 interface to attack or penetrate O-Cloud
- Threat actor on O-Cloud uses O2 interface to attack or penetrate SMO
- Conflicts between 3rd-party rApps/xApps degrade RAN availability or performance
- Supply chain for 3rd party rApps/xApps could introduce untrusted or malicious software
- Brute force attacks on Open Fronthaul M-Plane password-based authentication. The M-Plane specification allows optional use of passwords instead of PKI-based certificates.
- Internal threat actor modifies plain-text Open Fronthaul C-Plane messages
- Internal threat actor can spoof Master Clock on Open Fronthaul S-Plane due to lack of authentication



The threat analysis considers external and internal threats actors, in pursuit of a ZTA for O-RAN

US National Cybersecurity Strategy



[National-Cybersecurity-Strategy-2023.pdf \(whitehouse.gov\)](#)

- White House Office of the National Cyber Director (“ONCD”)
- March 2, 2023

“Departments and agencies will direct RD&D projects to advance cybersecurity and resilience in are such as ... cloud infrastructure, telecommunications ... used in critical infrastructure.”

“This Administration is committed to improving Federal cybersecurity through long-term efforts to implement a **zero trust architecture** strategy and modernize IT and OT networks.”

Open RAN/O-RAN has an expanded threat surface



Ericsson

August 2020

“Secure, Open RAN systems will require **additional security measures** not fully addressed in the standards”



EC NIS Cooperation Group

May 11, 2022

“An **expanded threat surface** and a more complex environment leading to higher risks of vulnerability or failure, which could also lead to undesirable data and information flow to new third-party applications”



O-RAN Alliance

June 2021

“The O-RAN Architecture includes new interfaces and functions, **expanding the threat surface** to introduce new security risks”



US NSA ESF

Sept 15, 2022

“By nature, an open ecosystem that involves a disaggregated multi-vendor environment requires specific focus on **changes to the threat surface** area at the interfaces between technologies integrated via the architecture...The deployment of Open RAN introduces **new security considerations** for mobile network operators”



Germany BSI

November 9, 2021

“medium to **high security risks**... from... the interfaces & components specified in O-RAN”



5G readiness for zero trust architecture and evolution

Patrik Teppo
Senior Expert Security Architecture
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Agenda



Zero Trust Architecture



ZTA on different levels



ZTA principles in 5G networks

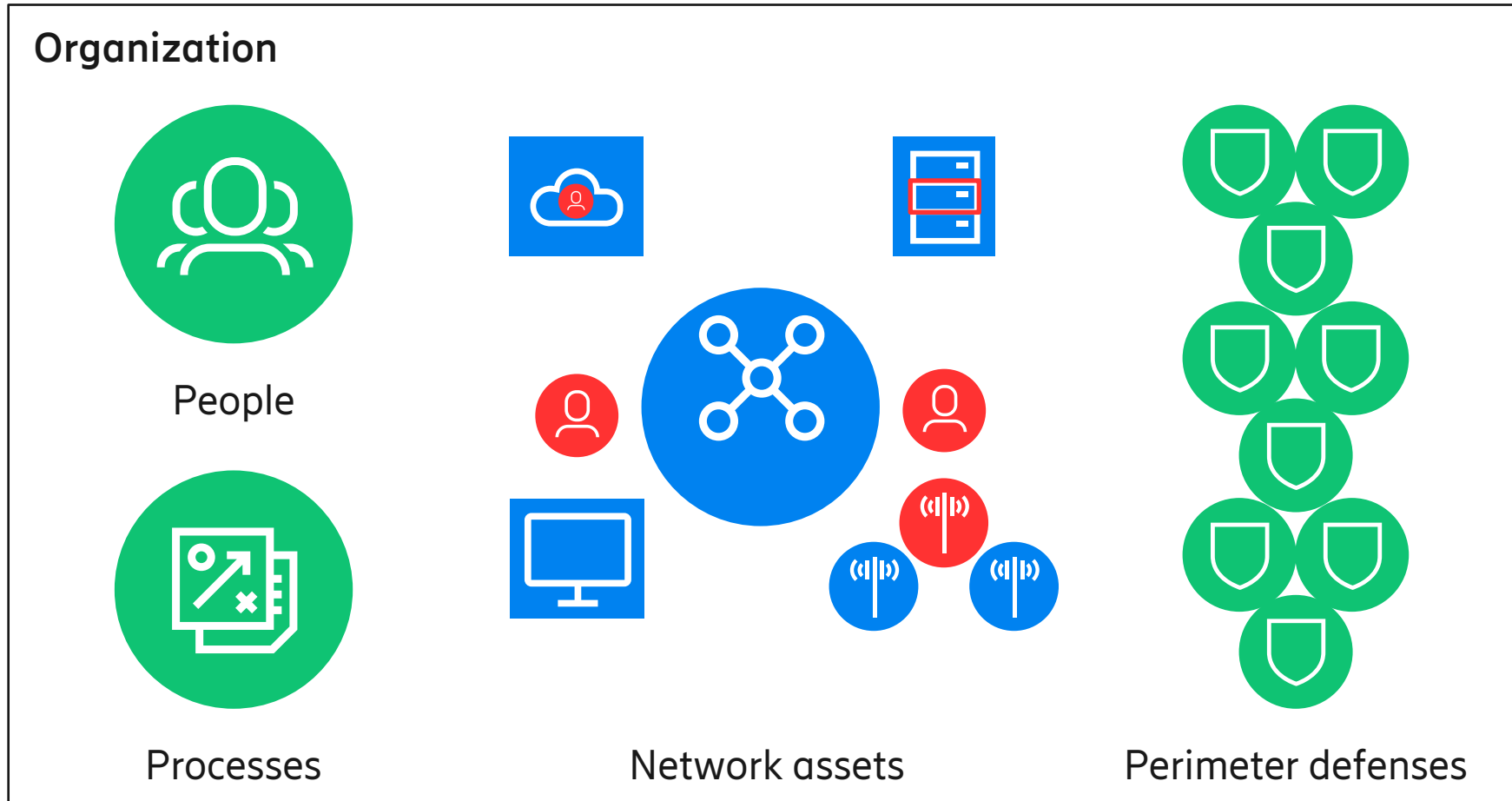


Machine vs Human communication

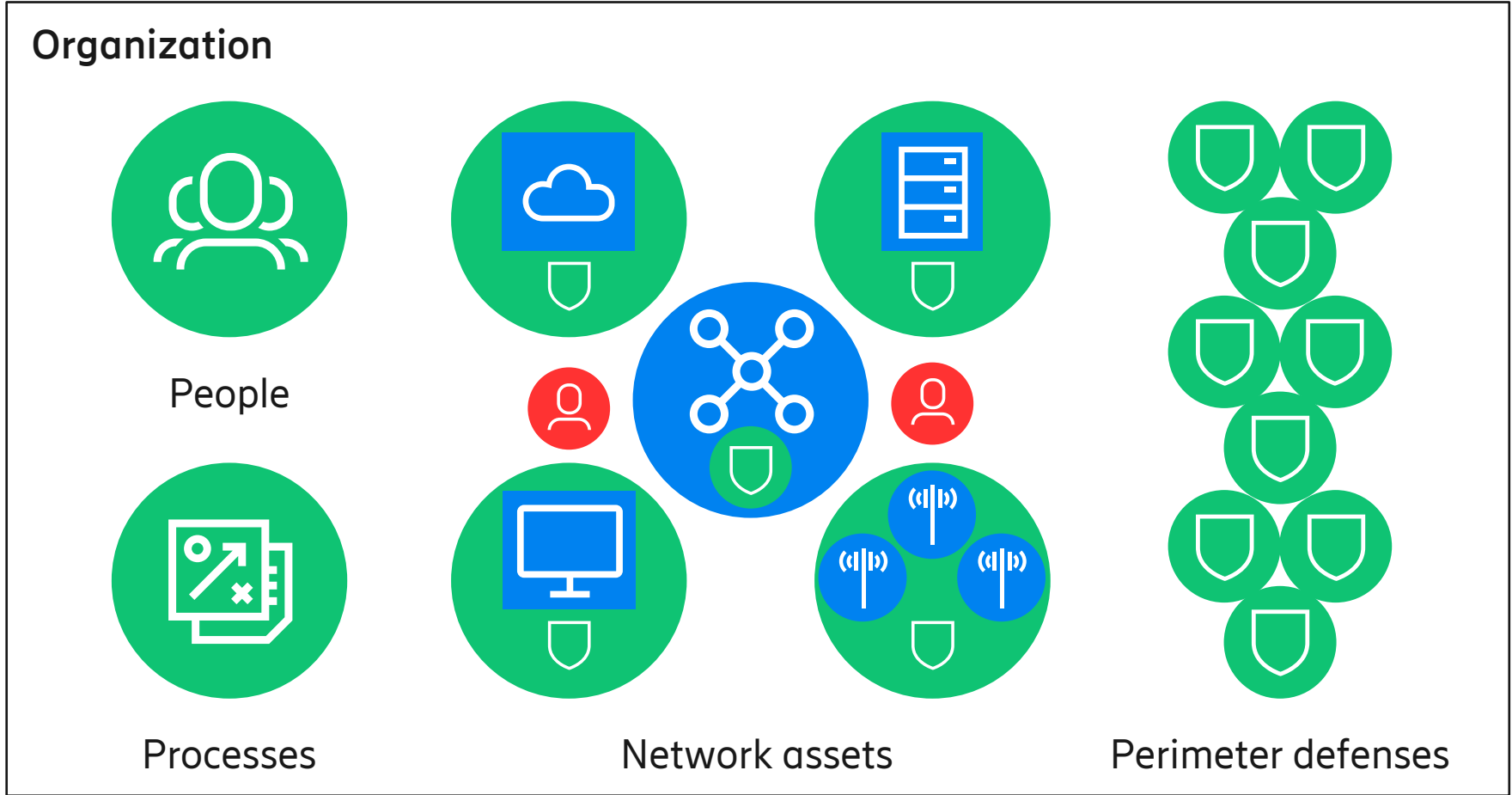


5G/6G ZTA evolution

Why a Zero trust security model



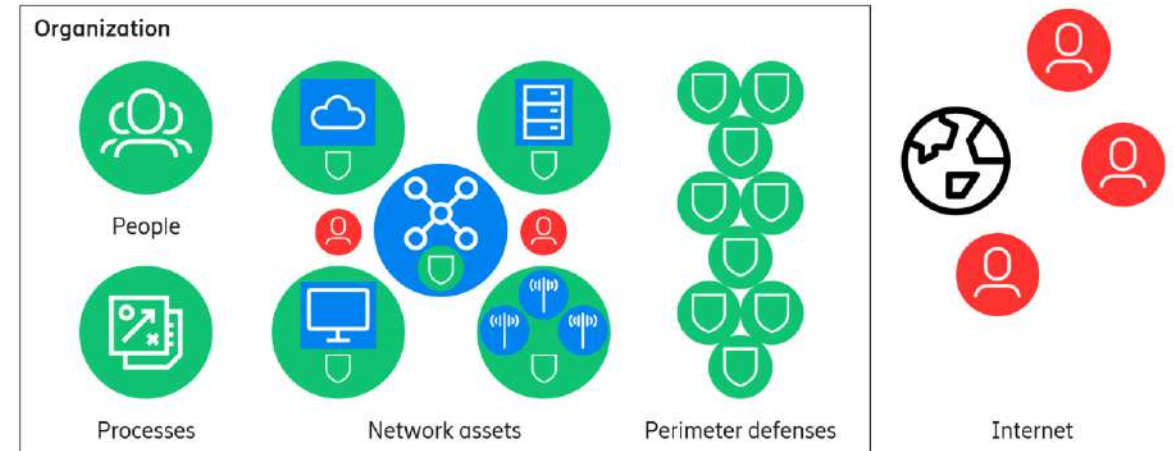
Zero trust security model



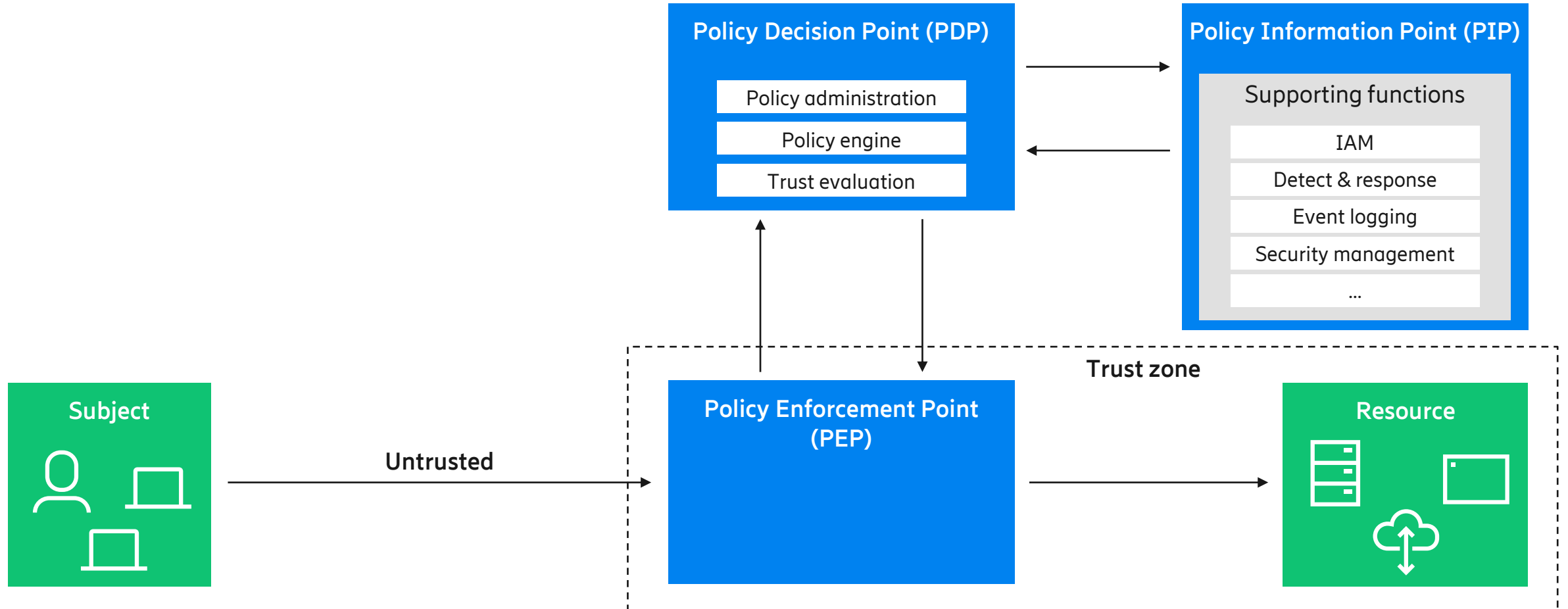
Zero trust architecture model



- Network security concept for **“don’t trust – always verify”** and **“assume breach”**
 - No implicit trust based upon ownership, physical location, or network location
- ZTA principles (summary)
 - All communication secured
 - Access control enforced per-session basis
 - Dynamic policies based on client state
 - Monitor and measure security of all assets as base for access control



Logical architecture



Agenda



Zero Trust Architecture



ZTA on different levels



ZTA principles in 5G networks

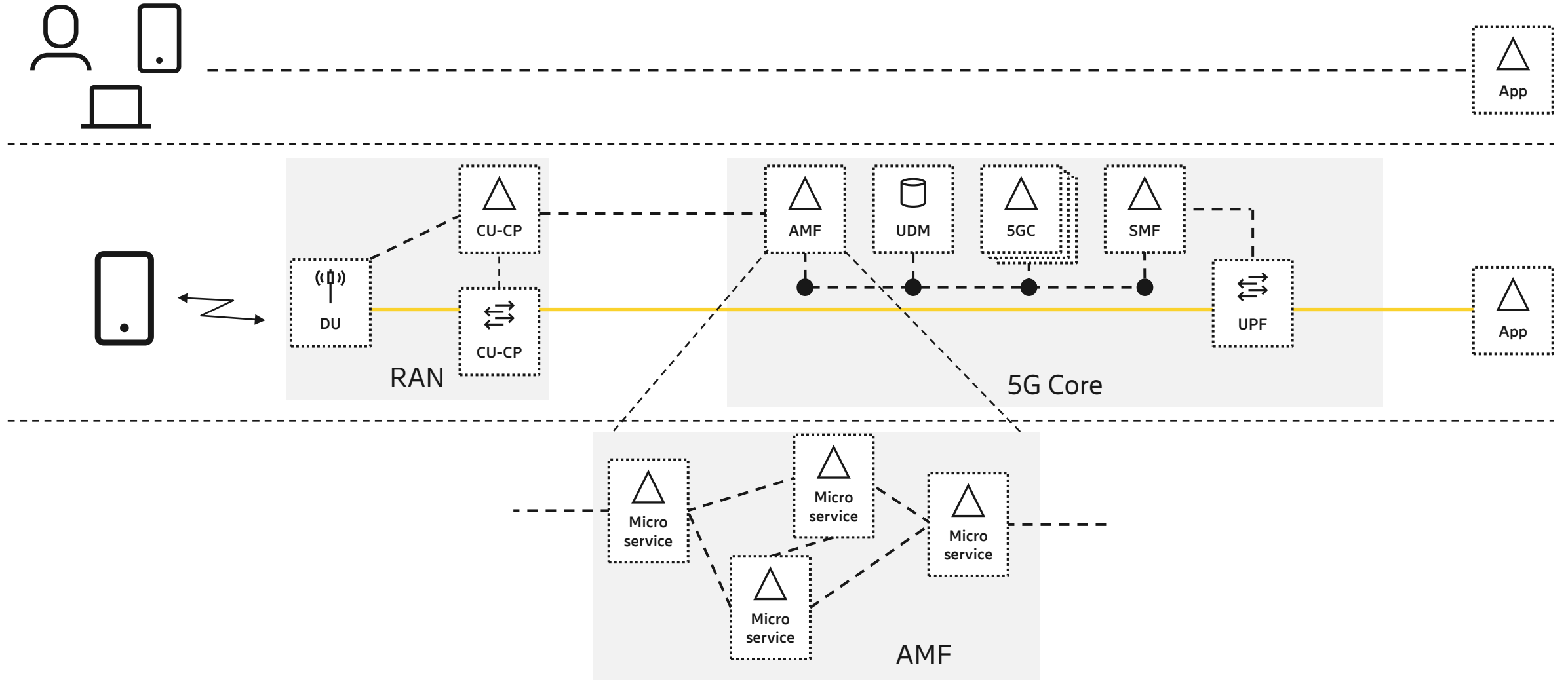


Machine vs Human communication



5G/6G ZTA evolution

ZTA on different levels



Agenda



Zero Trust Architecture



ZTA on different levels



ZTA principles in 5G networks



Machine vs Human communication



5G/6G ZTA evolution

3GPP security, access and core networks



5G

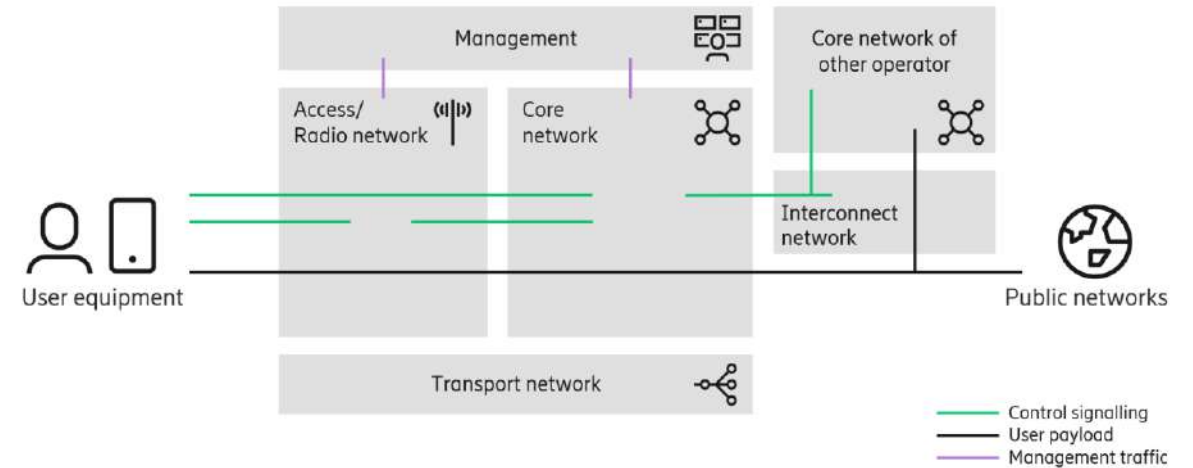
- RAN to Core interfaces with IPsec or DTLS
- 5GC with Service Based Architecture security
- RAN fronthaul with MACsec

3G/4G

- Perimeter protection
- Network Domain Security

2G

- Initially used trust between operators
- Perimeter protection introduced later



Enabling a trustworthy 5G system

<https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system>

A guide to 5G network security

<https://www.ericsson.com/4a66f8/assets/local/news/2021/09172021-a-guide-to-5g-network-security-2.0.pdf>

Security features to enable a zero-trust architecture



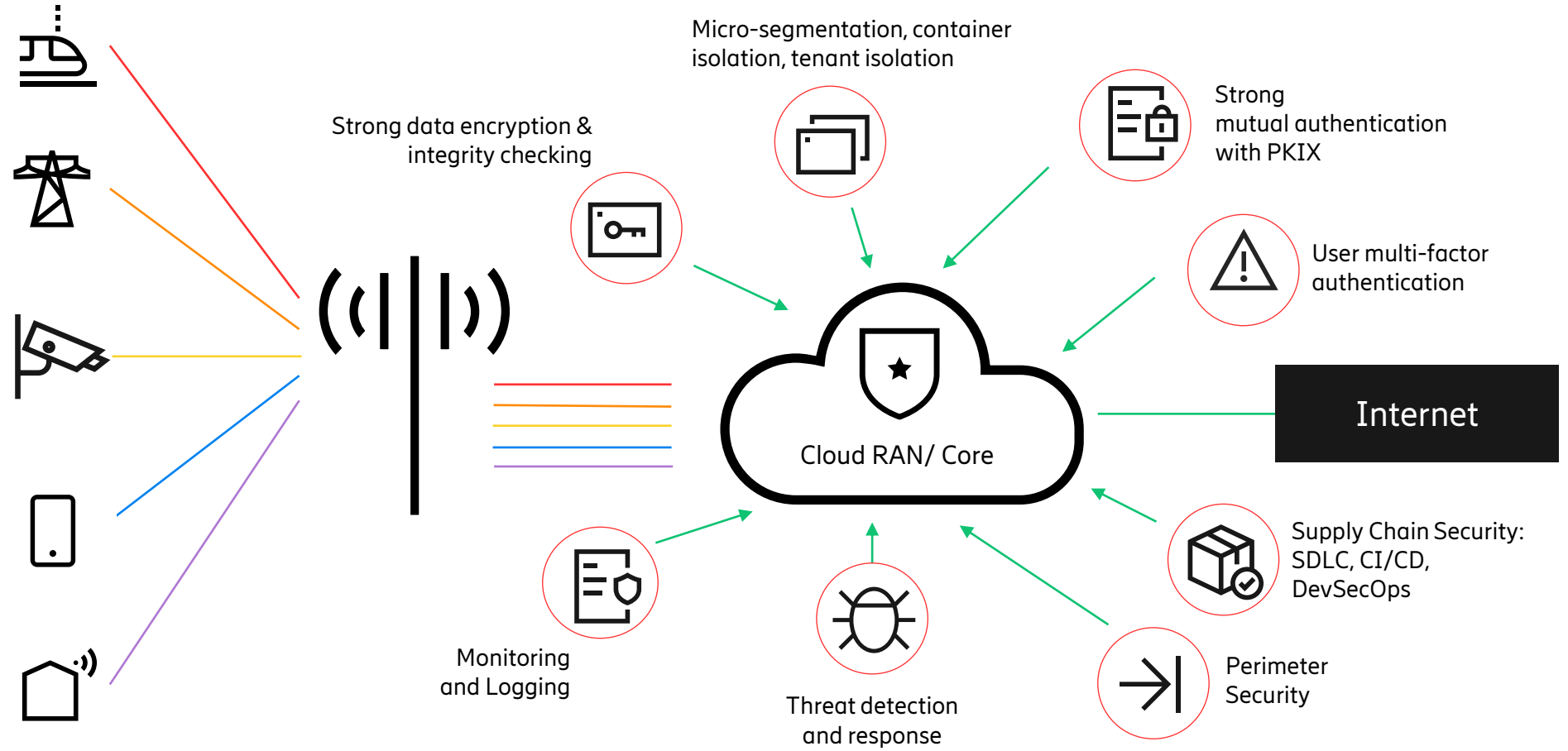
Zero-trust: Don't trust based on asset owner / location



RF fingerprinting: Intercept rogue transmitters



Security at every step of software development (agile)



Agenda



Zero Trust Architecture



ZTA on different levels



ZTA principles in 5G networks



Machine vs Human communication



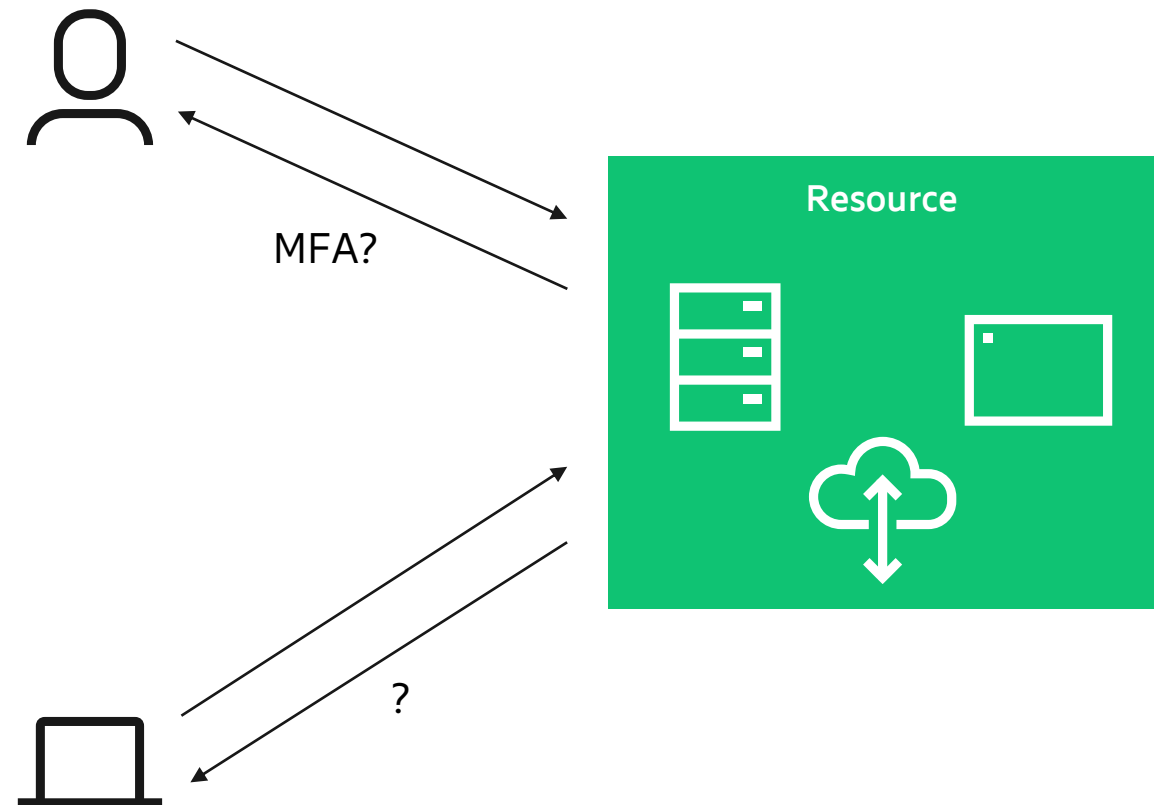
5G/6G ZTA evolution

Machine vs Human



NIST SP 800-207 Enterprise centric with humans accessing assets

- Authentication
 - **Humans:** Identifier and different types of credentials
 - **Machines:** Generally only have one on identifier and credential
- Access control
 - **Humans:** Level of access (from read only to admin)
 - **Machines:** Binary only?



Agenda



Zero Trust Architecture



ZTA on different levels



ZTA principles in 5G networks

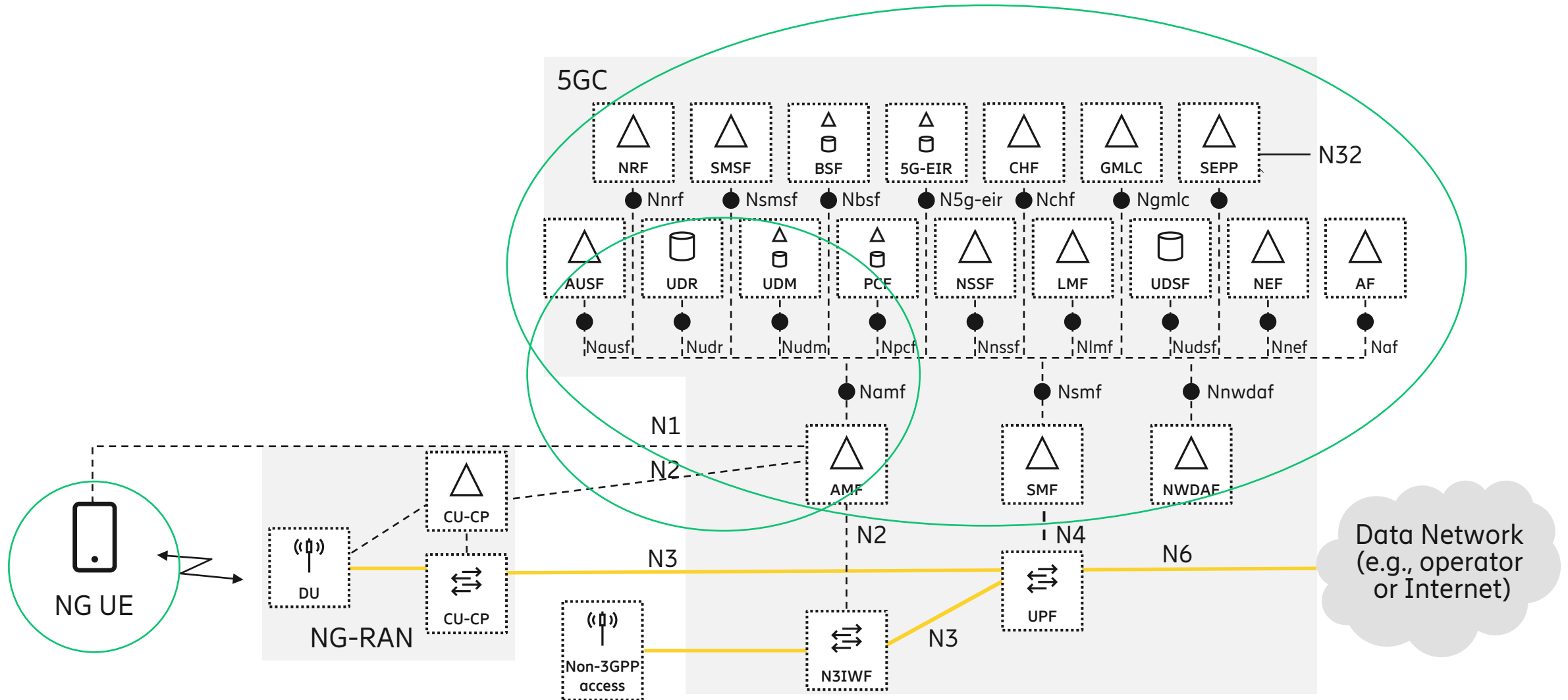


Machine vs Human communication



5G/6G ZTA evolution

5G architecture



ZTA evolution in 5G/6G



Zero trust and 5G – Realizing zero trust in networks

<https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g>

Evolving 5G security for the cloud

<https://www.ericsson.com/en/blog/6/2022/evolving-5g-security-for-the-cloud>

Why Enterprise Zero Trust Architecture matches 5G security

<https://www.ericsson.com/en/blog/2022/2/zero-trust-architecture-enterprise-5g-security>

A zero trust approach to 5G signalling networks

<https://www.ericsson.com/en/blog/2022/7/a-zero-trust-approach-to-5g-signaling-networks>

5G security for public and hybrid cloud deployments

<https://www.ericsson.com/en/reports-and-papers/further-insights/5g-security-for-hybrid-cloud>



<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

Network APIs & 5G Security

Michael Liljenstam
Principal Researcher Security
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Agenda



Why APIs are ubiquitous



API security in Enterprise IT



API security in mobile networks: 5G and O-RAN



API security in mobile network development and deployment

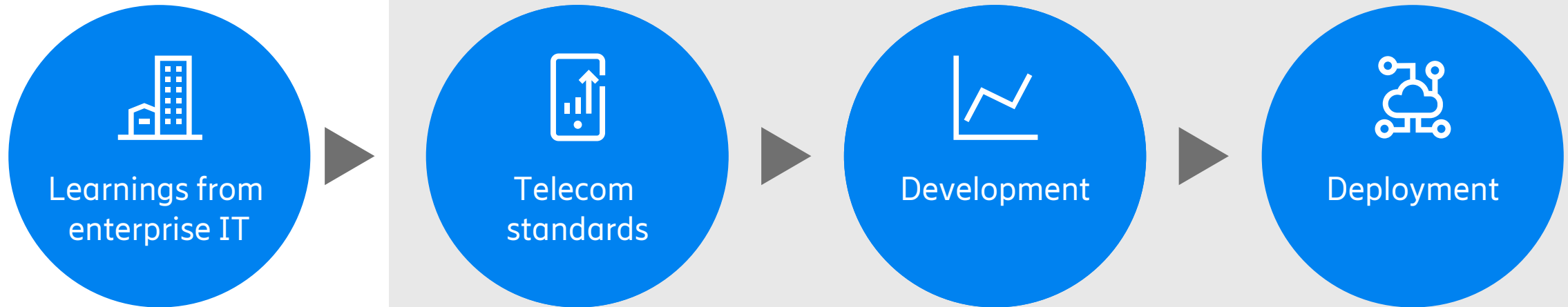


Research and standardization on APIs and security for telco

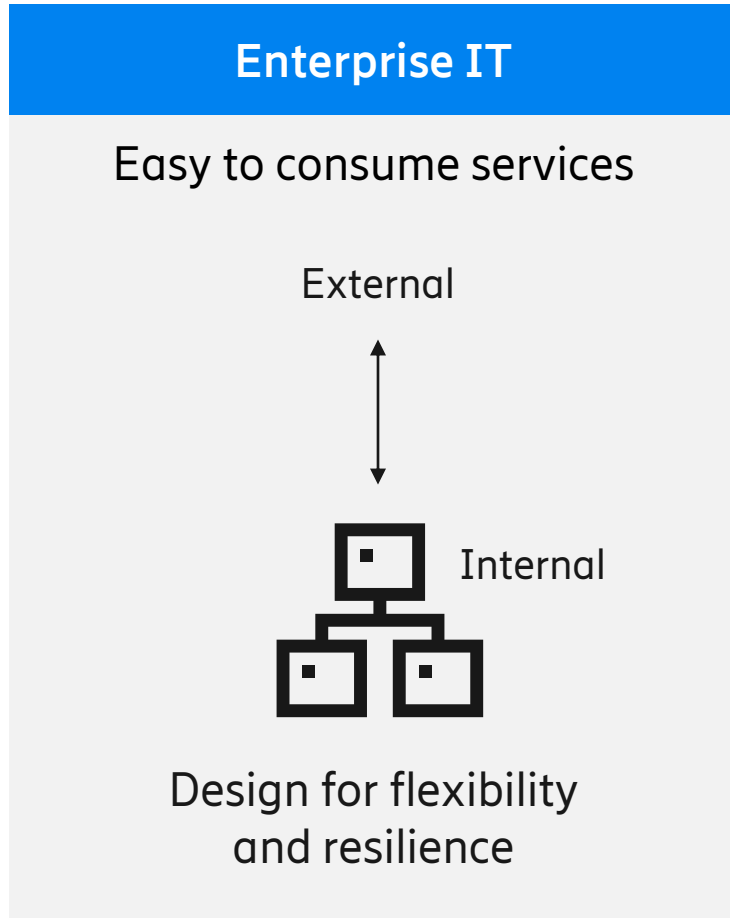


Way forward

Why use Application Programming Interfaces (APIs) & how to do it securely



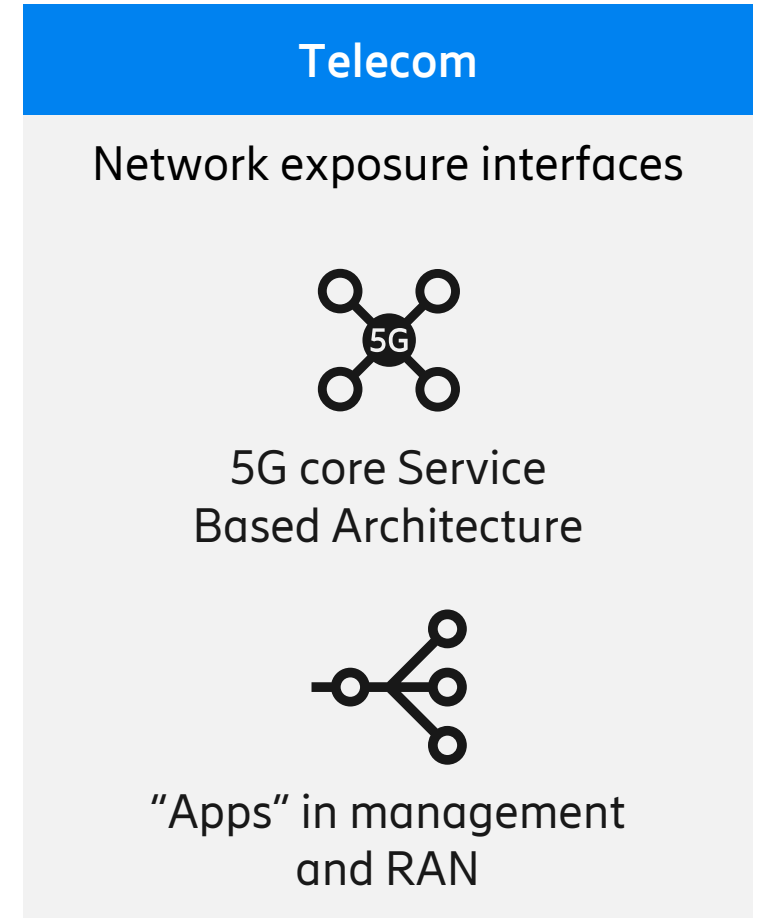
Why APIs are becoming ubiquitous



Telco industry is increasingly using same technology as IT industry in general

Drivers/mindset

- Speed, flexibility, reuse
- Support innovation ecosystem



Adopt – with care...



Adoption of design using APIs is already under way in telecom systems... (to make networks more useful – increase utility)

... But we have to consider a different trade off point for systems that we critically depend on...

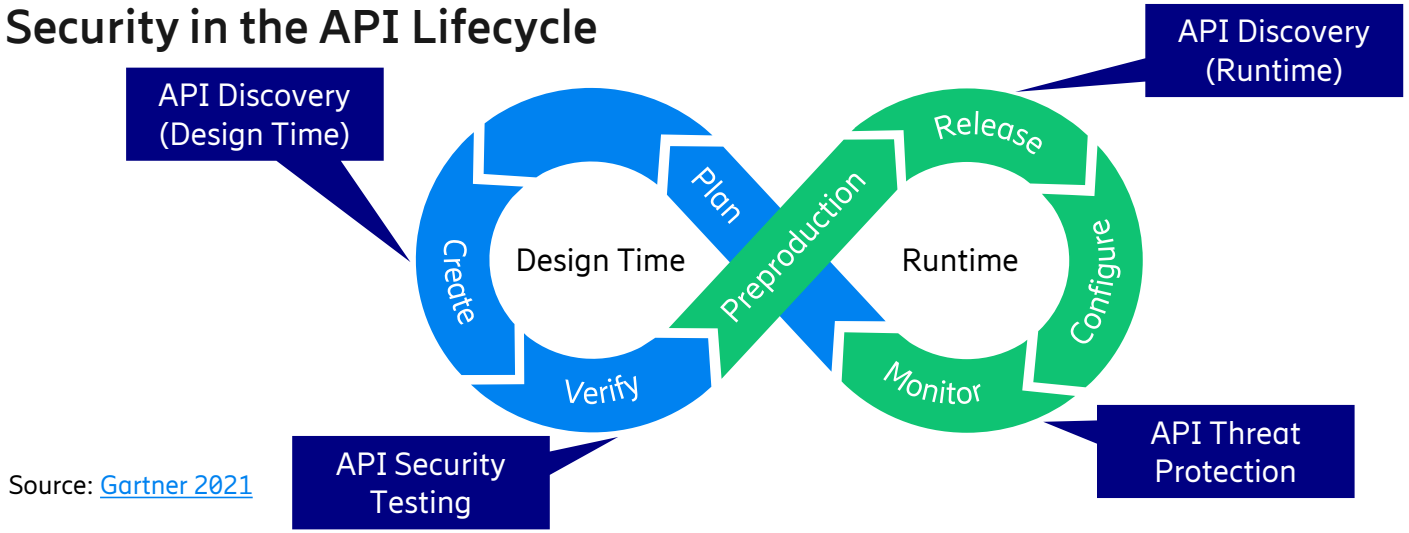
... on the other hand, timing is on our side – we have the benefit of hindsight, as we can draw upon lessons already learned in the enterprise IT space.



Security best practices from enterprise



Security in the API Lifecycle

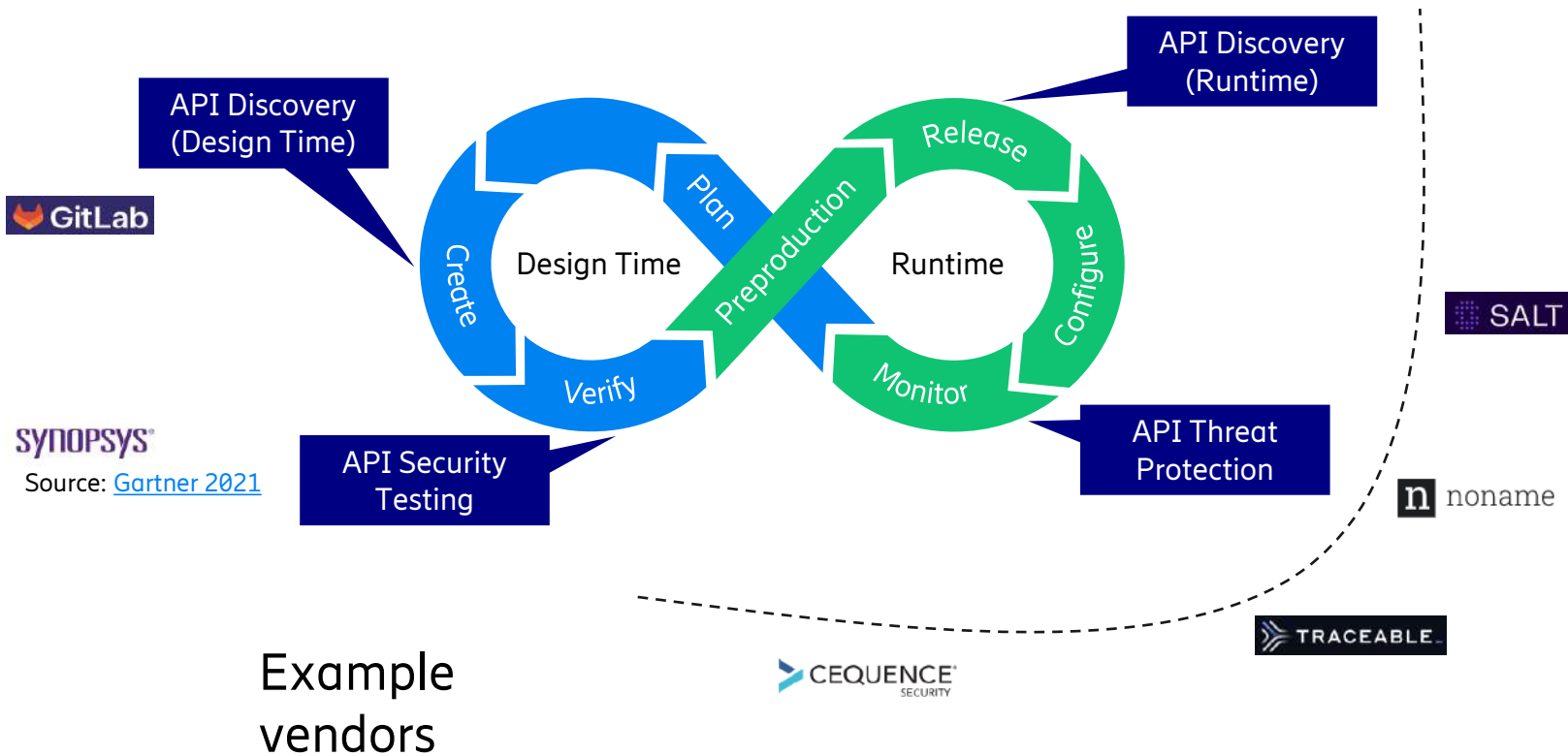


Source: [Gartner 2021](#)

Security vendor landscape



Security in the API Lifecycle



"API security" space is very active

- Startups
- Incumbent vendors moving in

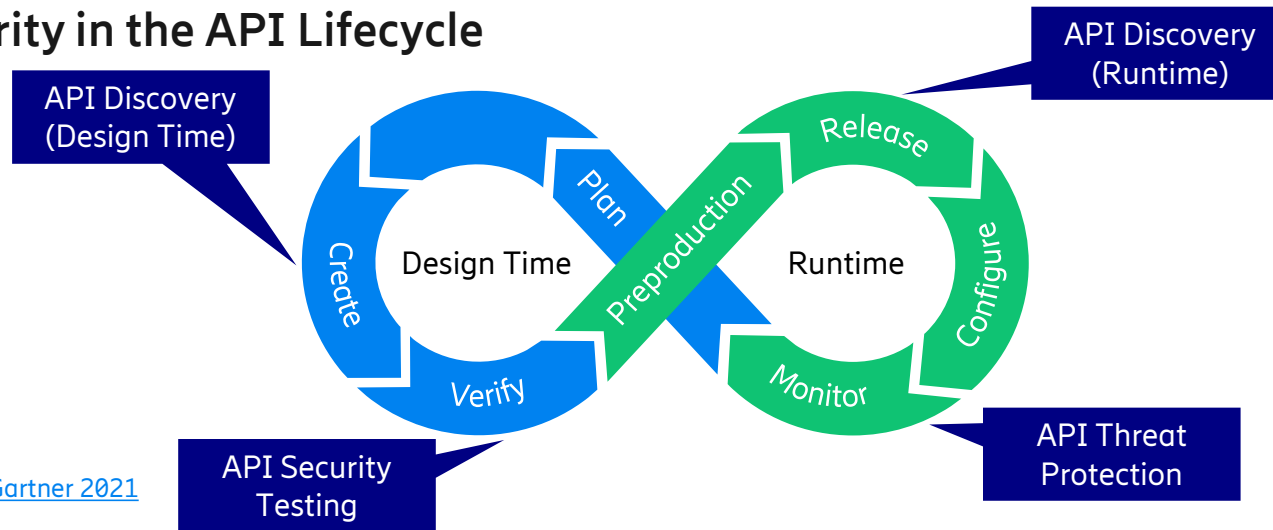


Security best practices from enterprise

And identified issues



Security in the API Lifecycle



Source: [Gartner 2021](#)

OWASP API Security Top 10 (2023RC)

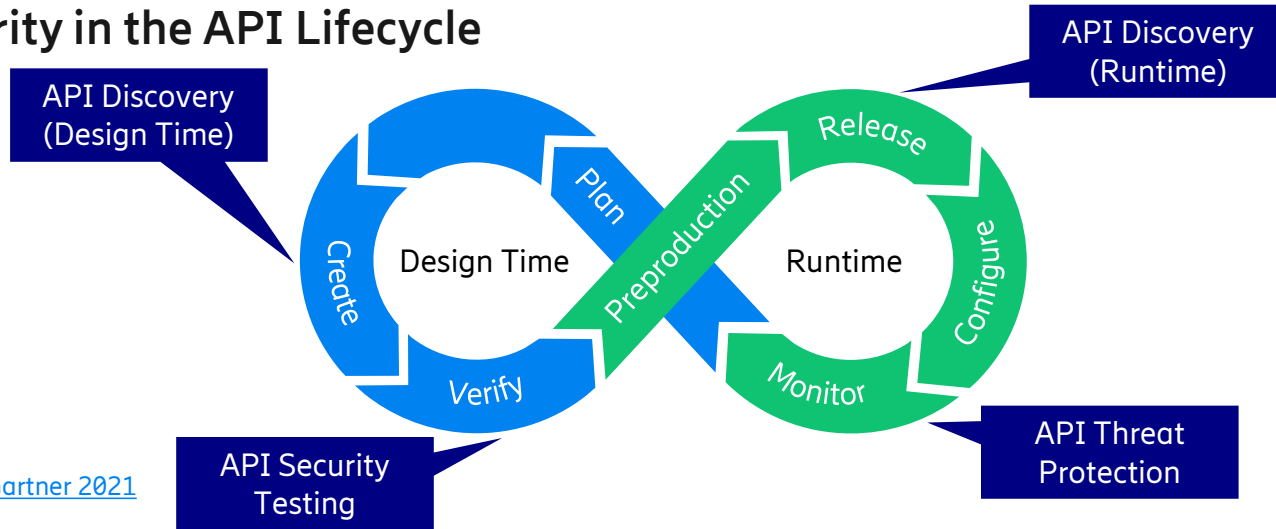
- Broken object-level authorization
- Broken authentication
- Broken object-property-level authorization
- Unrestricted resource consumption
- Broken function-level authorization
- ...
- Security misconfiguration

From enterprise into telecom standards and practices

Standards



Security in the API Lifecycle



Source: [Gartner 2021](#)

OWASP API Security Top 10 (2023RC)

- Broken object-level authorization
- Broken authentication
- Broken object-property-level authorization
- Unrestricted resource consumption
- Broken function-level authorization
- ...
- Security misconfiguration

Defined in telecom standards:



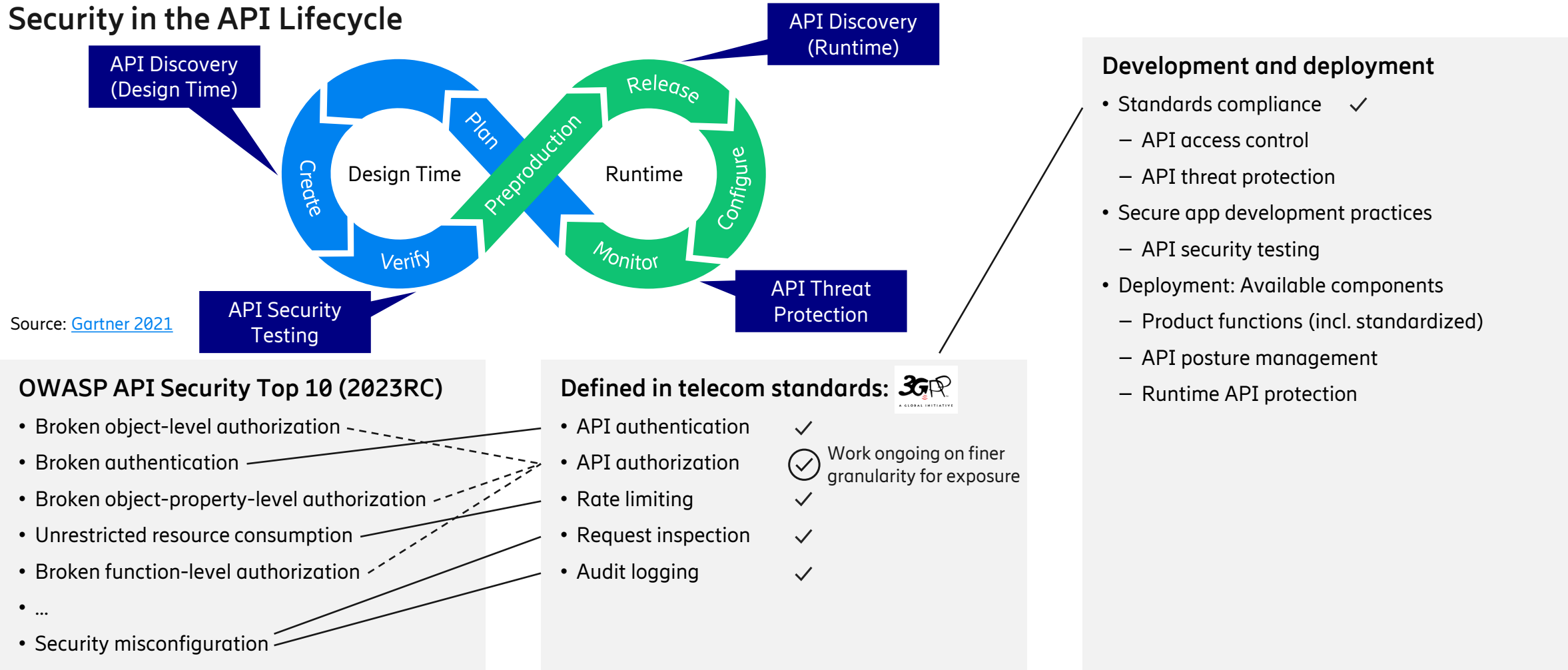
- API authentication ✓
- API authorization ✓ (Work ongoing on finer granularity for exposure)
- Rate limiting ✓
- Request inspection ✓
- Audit logging ✓

From enterprise into telecom standards and practices

Development and deployment



Security in the API Lifecycle



Source: [Gartner 2021](#)

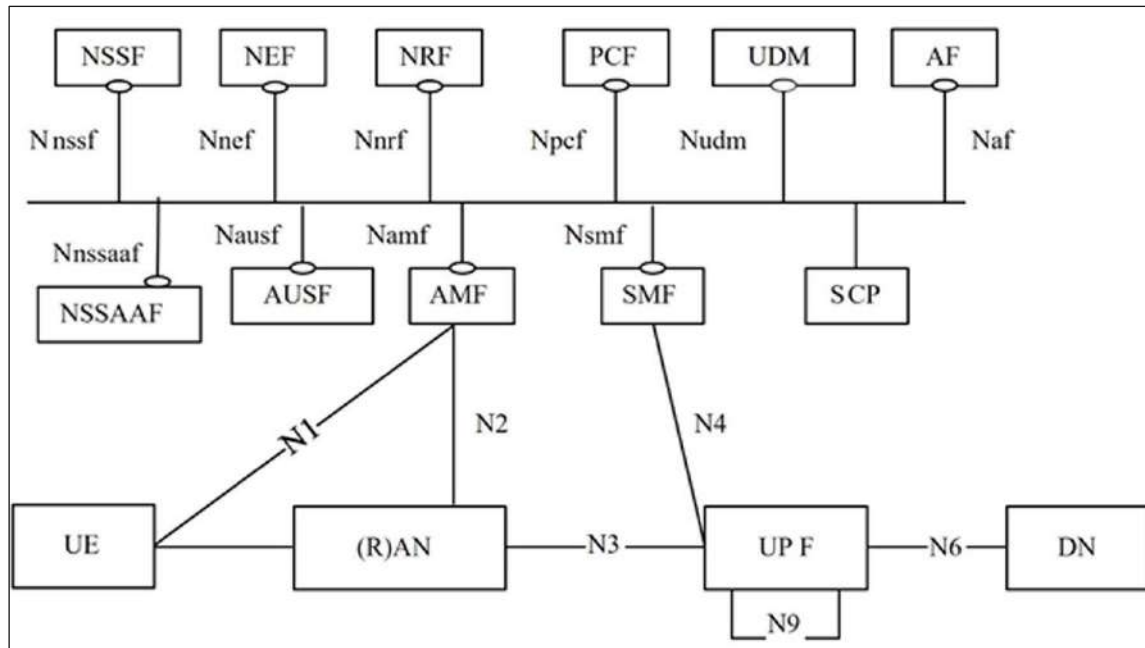
Mobile network standardization



5GC Service Based Architecture (internal interfaces)



- Mutual authentication and transport security
- Authorization (token-based)



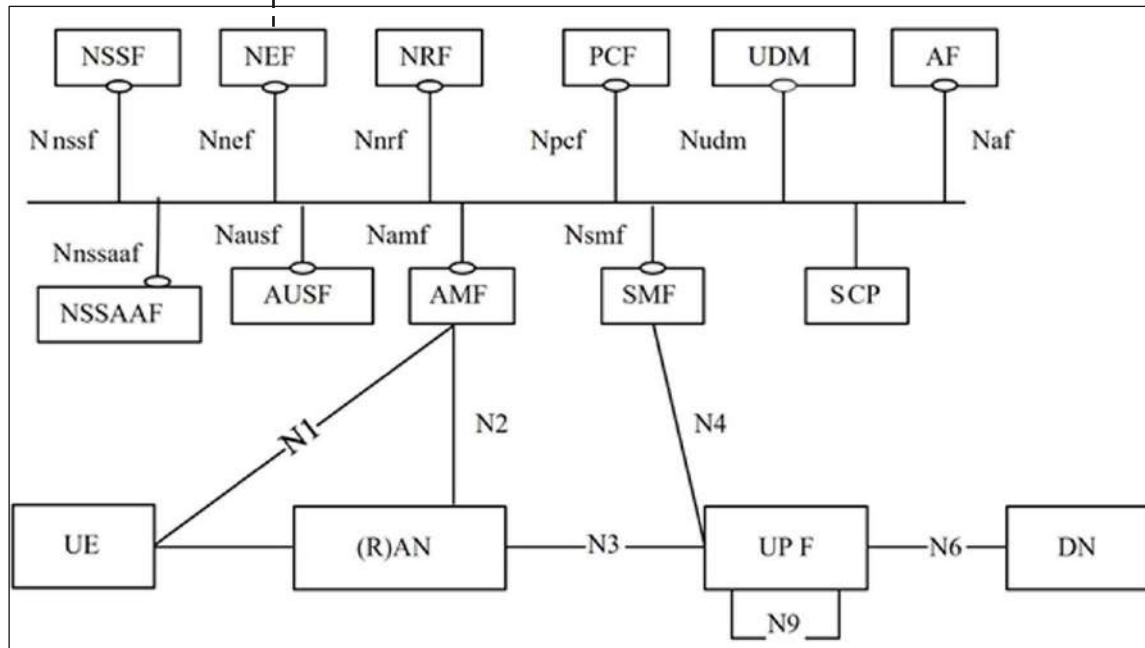
<https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture>

Mobile network standardization



5GC Service Based Architecture (internal interfaces)

- Mutual authentication and transport security
- Authorization (token-based)



5G Network Exposure (external interfaces)

- NEF – Network Exposure Function
Authentication, Authorization, rate limiting, request inspection, audit logging
- CAPIF – Common API Framework
Common functions for: Authentication, authorization, audit logging + API management (client onboarding, ...)

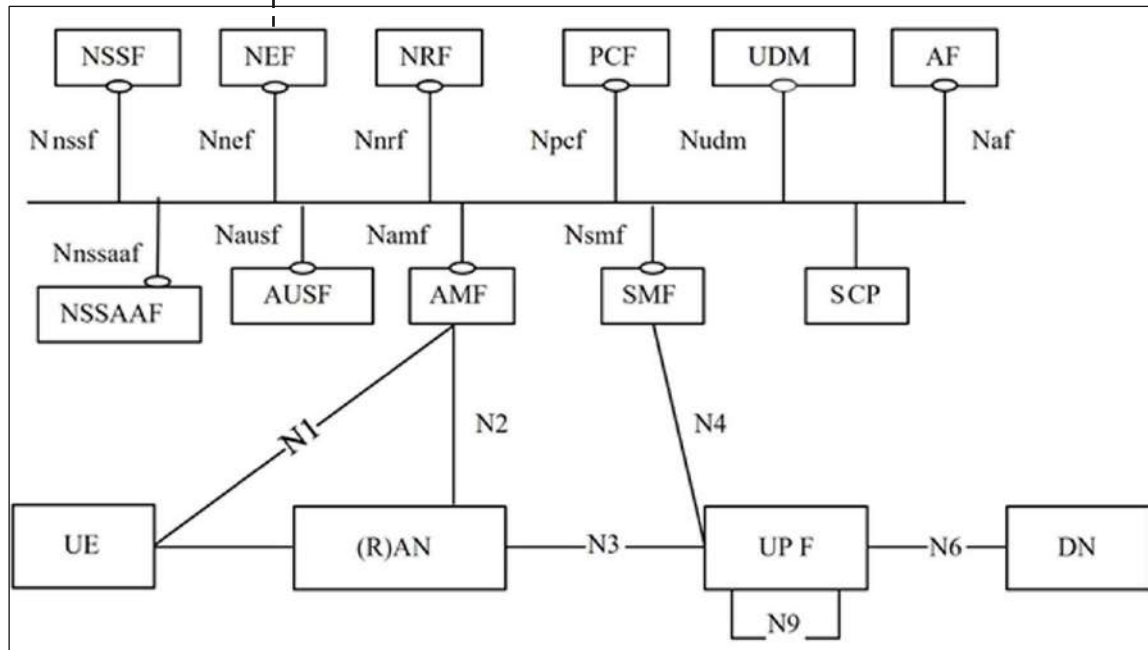
<https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture>

Mobile network standardization



5GC Service Based Architecture (internal interfaces)

- Mutual authentication and transport security
- Authorization (token-based)



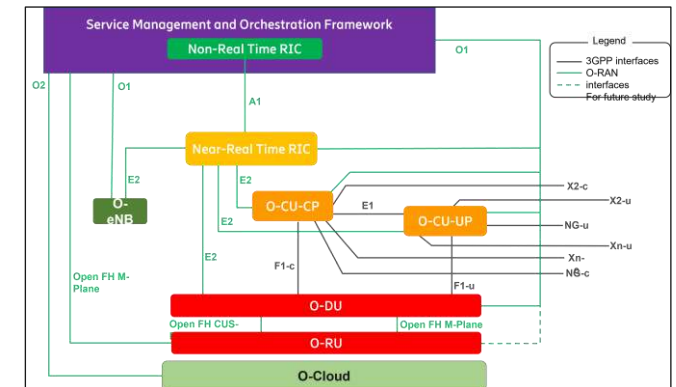
<https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture>

5G Network Exposure (external interfaces)

- NEF – Network Exposure Function
Authentication, Authorization, rate limiting, request inspection, audit logging
- CAPIF – Common API Framework
Common functions for: Authentication, authorization, audit logging + API management (client onboarding, ...)

O-RAN Apps (interfaces for components potentially from 3rd parties)

- Mutual authentication and transport security
 - Authorization
 - Security event logging
- (See presentation “Open RAN Security”)



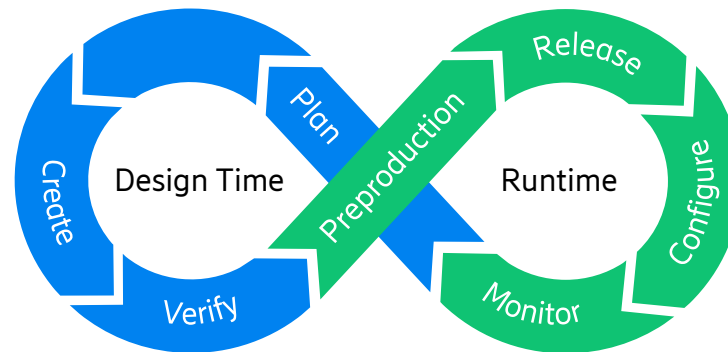
Development & deployment



Development

- Secure coding practices
- Code security defect checking: static and dynamic
- Documentation of APIs and generation of OpenAPI specifications
- Discovery of undocumented API endpoints in code
 - Security testing using generated specifications

Many enterprise settings: single organization
Telecom: shared responsibilities vendor/operator



Deployment

- Product security functions
 - API Gateway functions (based on CAPIF)
 - Request inspection and controls
- Applicable tools (As a vendor we can give recommendations)
 - Runtime API discovery: “outside”/“inside” perspective
 - API Posture management: Detect misconfigurations
 - Runtime API protection (augment)
 - Detect patterns indicating malicious behavior
 - Anomaly detection (may use machine learning)
 - Inline protection

Research for 6G



Context: Pre-standardization research

- Expected increased exposure of network functionality
 - explored in projects/initiatives



Possibilities include:

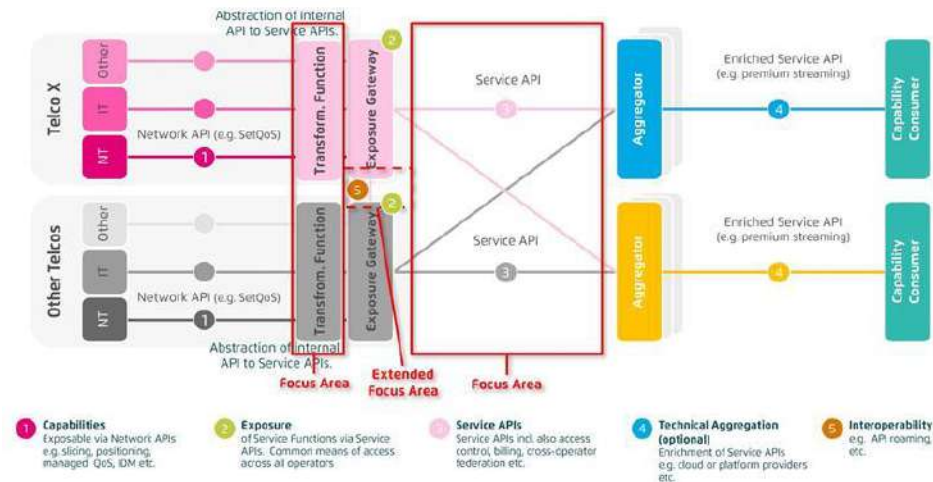
- Management capability exposure
- Exposure between communication layers and application layer

As well as

- Edge exposure
- AI-as-a-Service

Internal security research

- Threat analysis for network exposure
 - Starting from high level view (CAMARA project)

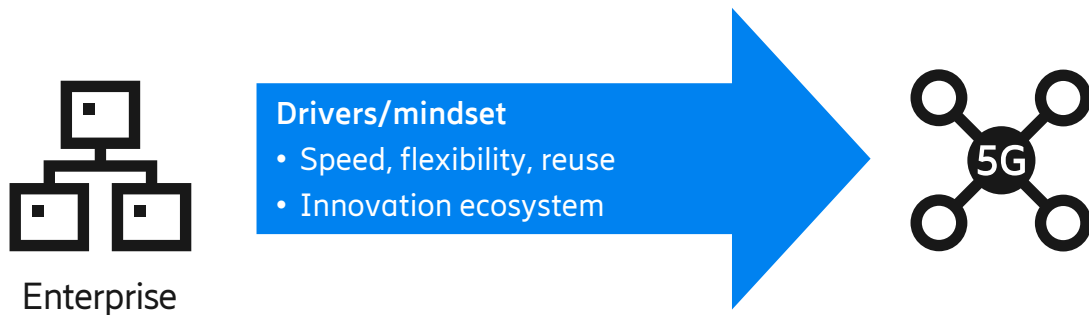


- Explore new additional security controls

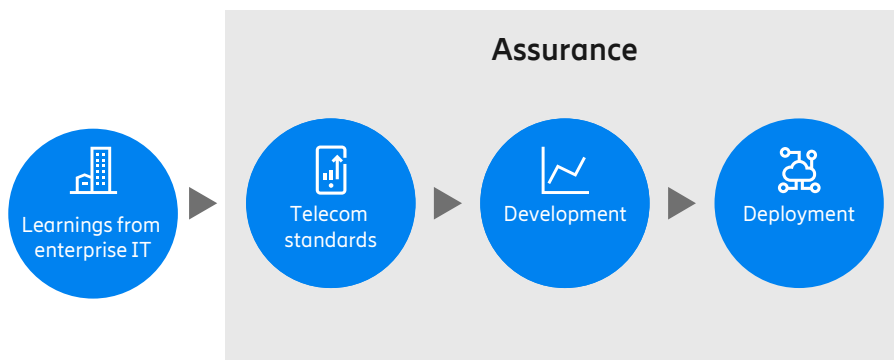
Way forward



Design using APIs is here and likely to stay



Important how do it to uphold security



Vendors/CSPs and regulators

- Start active discussions/dialog on the topic
- Learn from the enterprise API security space
- Evolve standards to ensure appropriate protection measures and procedures are in place

Regulators

- Establish assurance methodologies

Vendors/CSPs

- Protection strategy across the API lifecycle
- Forward looking research to continue enhancing API security in next generation systems



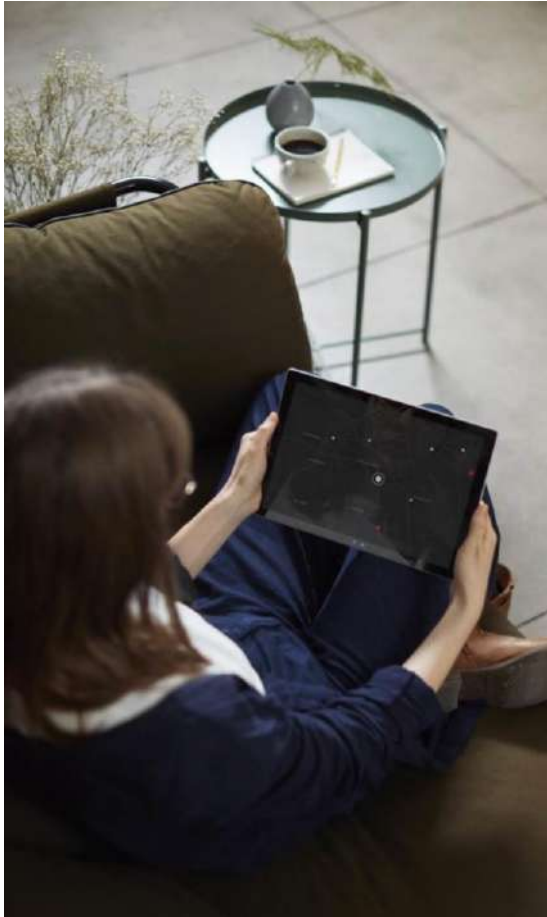
<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

Confidential software security assurance

Luis Barriga
Principal Researcher Security
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Agenda



Motivation – Softwarization & regulations



Challenge – Risks during software security assurance



Solution – Confidential software security assurance



Q&A



Caveat

Research and Innovation Project



Short story



Motivation

Softwarerization and security assurance regulations

Network Equipment Security Assurance

NESAS



Adopted in Germany and under adoption in EU



**Network Equipment Security Assurance Scheme –
Development and Lifecycle Security Requirements**

Version 2.2

20 October 2022

Source code must be reviewed by vendor

7.3.1 [REQ-IMP-01] Source Code Review

[Requirement Text: The Equipment Vendor shall ensure that new and changed source code dedicated for a Network Product is appropriately reviewed in accordance with an appropriate coding standard. If feasible, the review should also be implemented by means of utilising a Source Code Analysis Tool and automation where appropriate.] [O_VUL_INT]

Keep track of the software bill of materials (SBOM)

7.8.6 [REQ-GEN-06] Sourcing and Lifecycle Management of 3rd Party Components

[Requirement Text: The Equipment Vendor shall have processes in place to ensure the quality of 3rd party components during the product lifecycle. The Equipment Vendor shall select supported 3rd party components and shall avoid using those reaching the end of life.]

Indian Telecommunication Security Assurance Requirements (ITSAR)



सत्यमेव जयते

**PROCEDURE
FOR
SECURITY CERTIFICATION
OF
TELECOMMUNICATION EQUIPMENT**

Doc. No.: NCCS/SC/01/30032020

Source code must be reviewed by authorized Labs

2.3.3 Source code security assurance

Requirement:

a) OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).

Vendor to provide the software bill of materials to Labs

2.3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the UPF shall not be present.

Orphaned software components /packages shall not be present in UPF.

OEM shall provide the list of software that are necessary for UPF's operation.

In addition, OEM shall furnish an undertaking as "UPF does not contain Software that is not used in the functionality of UPF."

UK Telecoms Security Regulations and Code of Practice



Vendor security assessment

Assessing the security of network equipment.

Binary code must be reviewed by authorized Labs

V.D.1: Heap protections	The vendor makes use of modern heap protection mitigations to help prevent heap-based memory corruption attacks against the product.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use heap protections throughout their product.	Verify that heap mitigations are enabled by (automatically) inspecting the product for this mitigation.
V.D.2: Stack protections	The vendor only ships executable code that has been compiled using modern stack mitigations.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use stack protections throughout their product.	Verify that stack mitigations are enabled by (automatically) inspecting the product for this mitigation.

Provide the software bill of materials for verification by Labs

V.A.7: Use of tools, software and libraries	Third party tools (e.g. code compilers) software components and software libraries that are used within and in the development of the product are inventoried. Any of the above that are	Out-of-support tools, software components, software or libraries are unlikely to use modern security features. If exposed, they can cause known vulnerabilities to be embedded in	The Security Declaration describes how third party software components are maintained, explicitly stating when, if ever, out-of-support components will be included in any product versions	For a customer-selected product, the vendor provides a list of third party components that are material to the security of the product, (e.g. those components exposed via interfaces). Verify that these components are still	Scan product interfaces to inventory known third party tools and determine if they are being maintained. Examine the product to verify that the vendor's component list appears accurate.
--	--	---	---	--	---

Enhancing Software Supply Chain Security (US E014028)



Executive Order 14028 — Improving The Nation's Cybersecurity

Source code must be reviewed

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update

Provide the software bill of materials to Labs for verification

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

Verification of Components

For those cases where the SBOM consumer (or the SBOM creator) is concerned with verifying the information in an SBOM, there exist frameworks for assessing the maturity of the creation. These include Open Web Application Security Project (OWASP) Software Component Verification Standard (SCVS) and [ISO 5230](#).

Summary – Regulations on assurance



PROCEDURE FOR SECURITY CERTIFICATION OF TELECOMMUNICATION EQUIPMENT
Doc. No.: NCCS/SC/01/30032020

National Cyber Security Centre
Vendor security assessment
Assessing the security of network equipment.

Deutsches Bundesamt für Sicherheit in der Informationstechnik
Deutschland Digital•Sicher•BSI
Technical Guideline TR-03163: Security in Telecommunications Infrastructure

Executive Order 14028 – Improving The Nation's Cybersecurity

EU CYBERSECURITY CERTIFICATION

EU5G Mobile Networks

NESAS GSMA

3GPP TS 33.117

Common Criteria

Source code / executables review

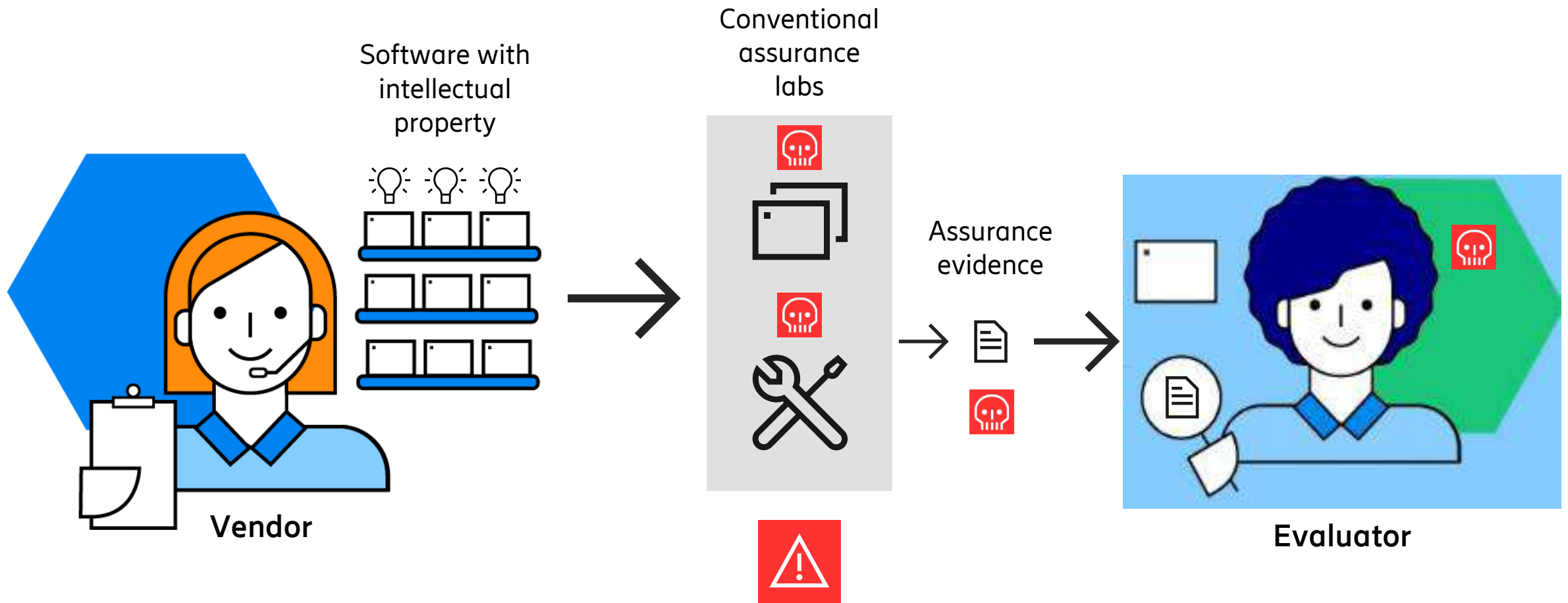
Software should be evaluated

- Product source code
FOSS, proprietary, supply-chain
- Product executables
Vulnerabilities, mitigations in place

Software bill of materials (SBOM)

List of software components used in products – whole supply chain. **Verification, provenance, pedigree, life-cycle management**

Conventional software security assurance





Dilemma

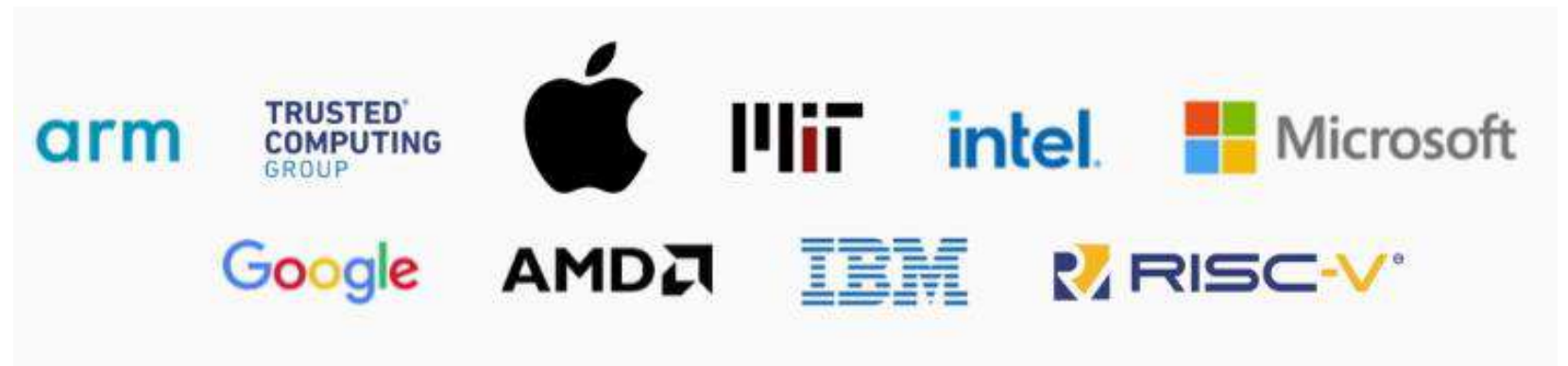
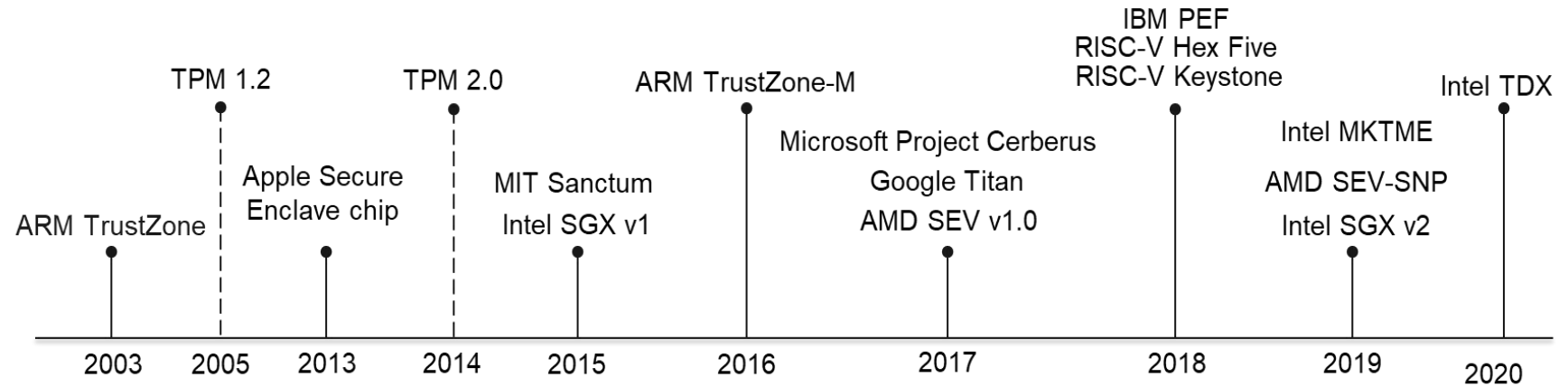
Software transparency vs. software confidentiality



Challenge

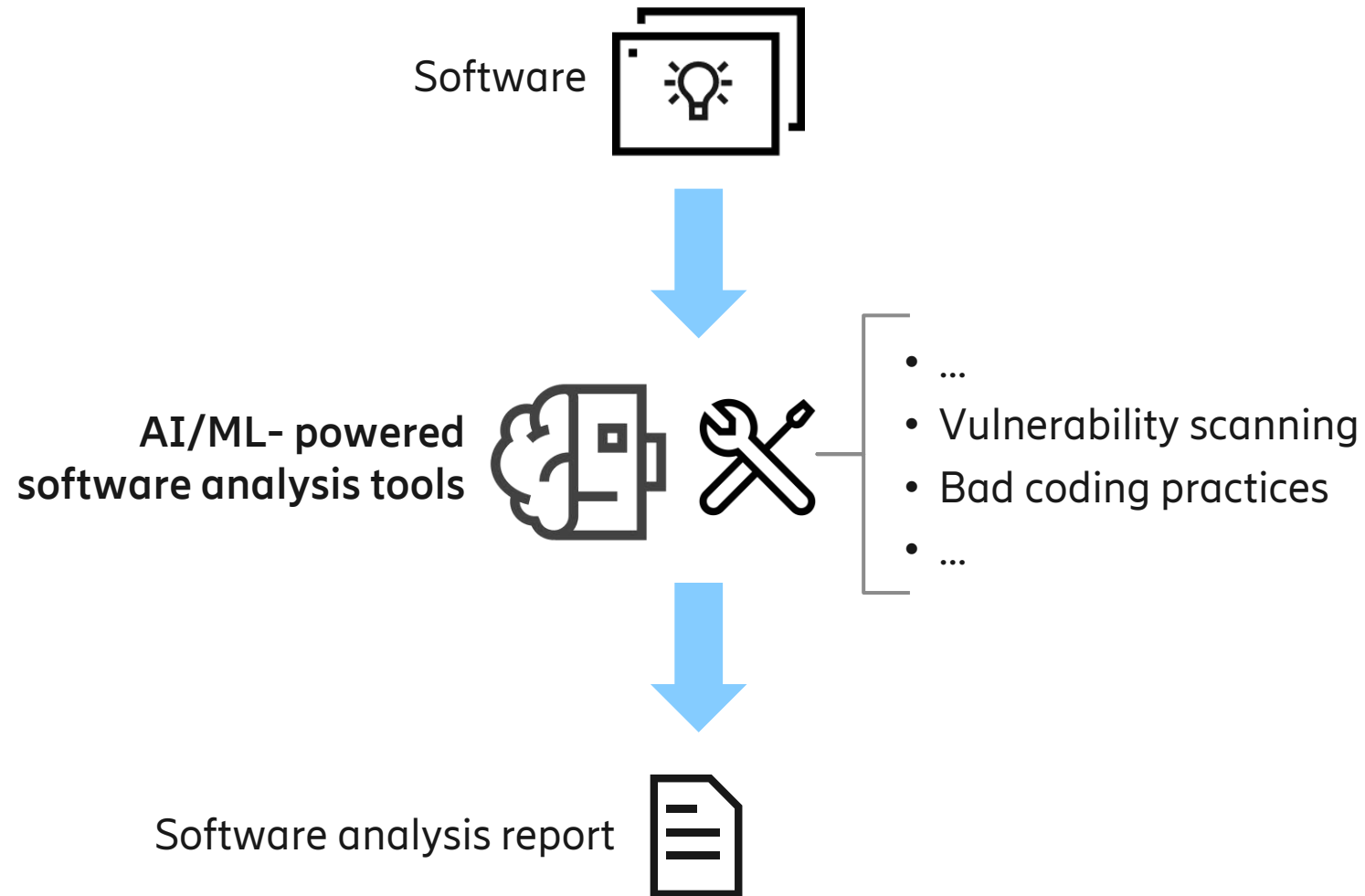
How can the software supply chain be compliant allowing evaluators to conduct software security assurance but without disclosing the source code?

Technology enabler 1 – Confidential Computing



Assurance evidence

Technology enabler 2 – AI/ML

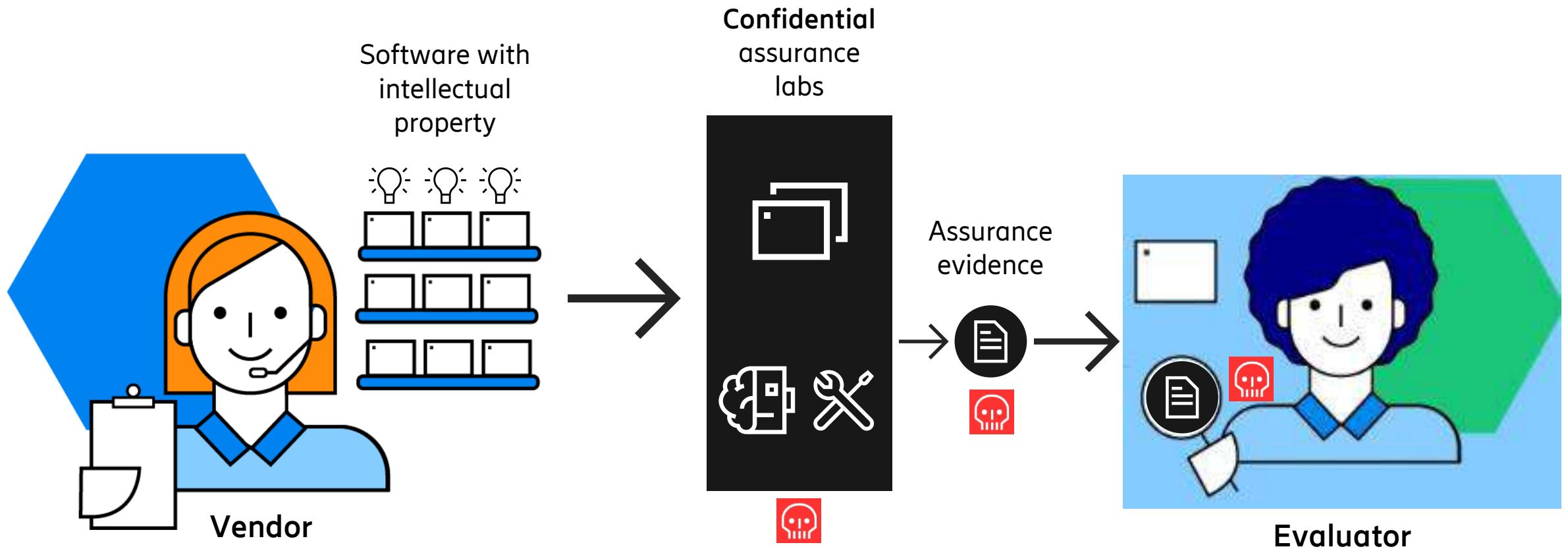




Solution

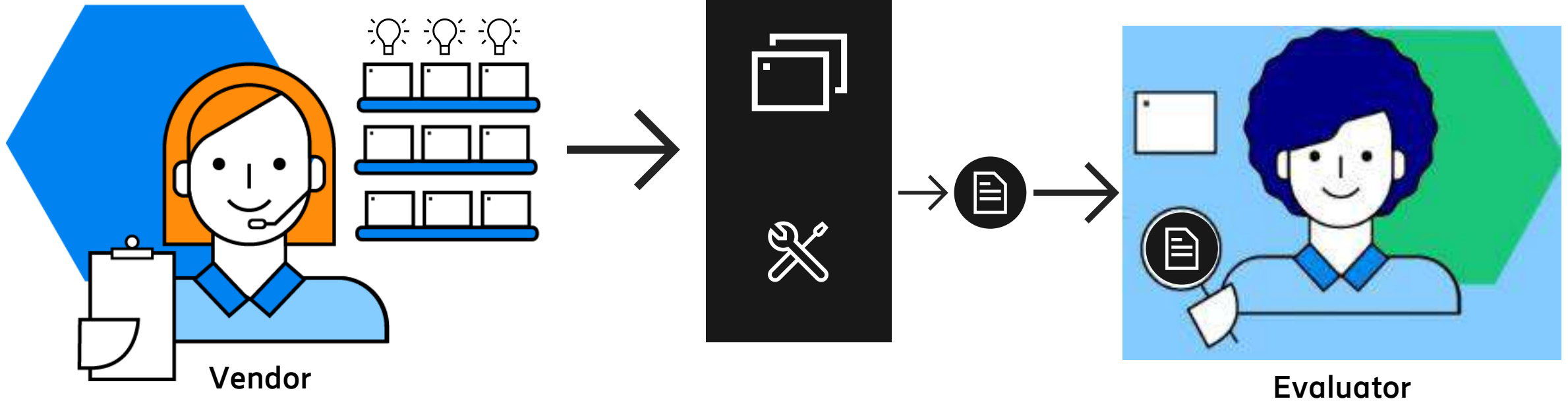
Confidential Software Security Assurance

Confidential software security assurance



Proof of Concept

Assurance as a Service



- Remote Attestation
- Secure software upload

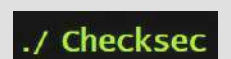
- Software Analysis
- SBOM generation

- Remote attestation
- Evidence collection

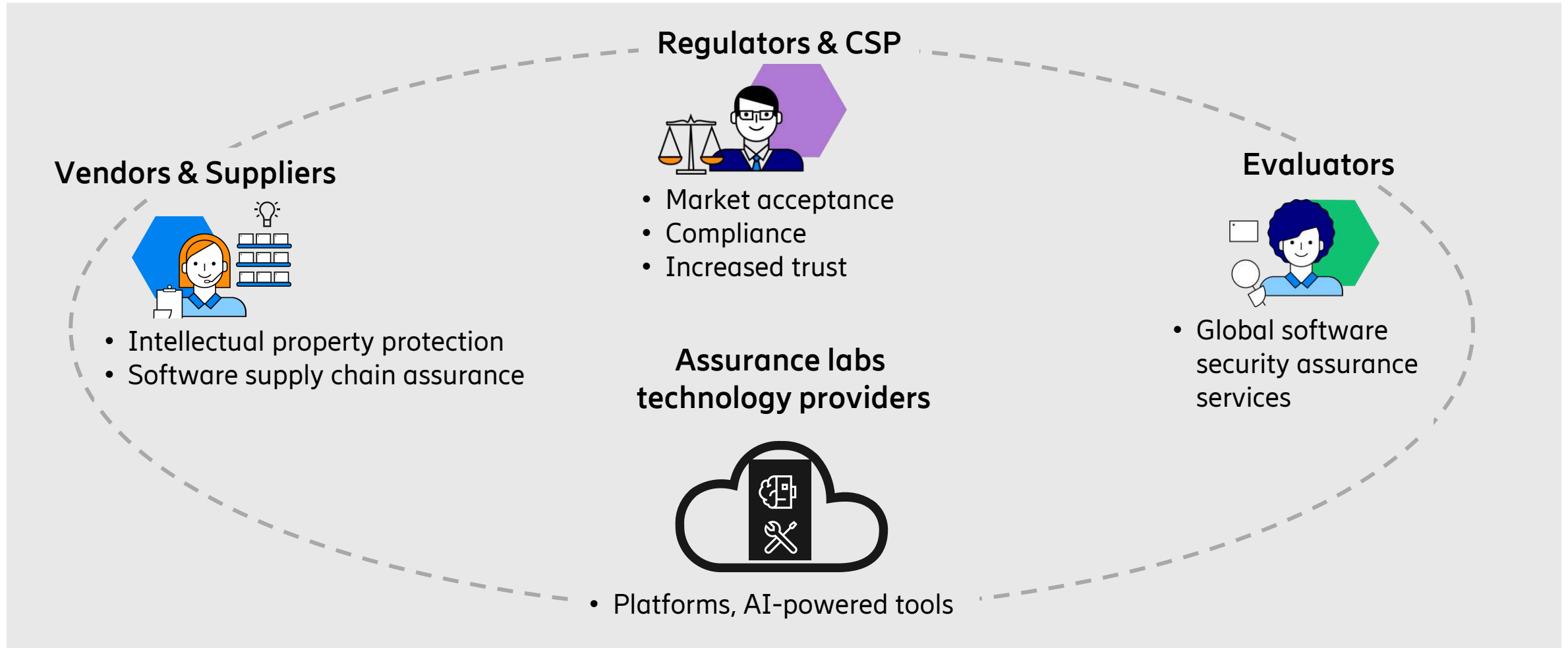
4G/5G targets of evaluation



Supported software analysis tools



The confidential assurance ecosystem





Q&A



<https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security>

6G Research and standardization update

Patrik Persson
6G Program Director
Ericsson

June 26-27, 2023
Conference for Governments and Regulators

Content



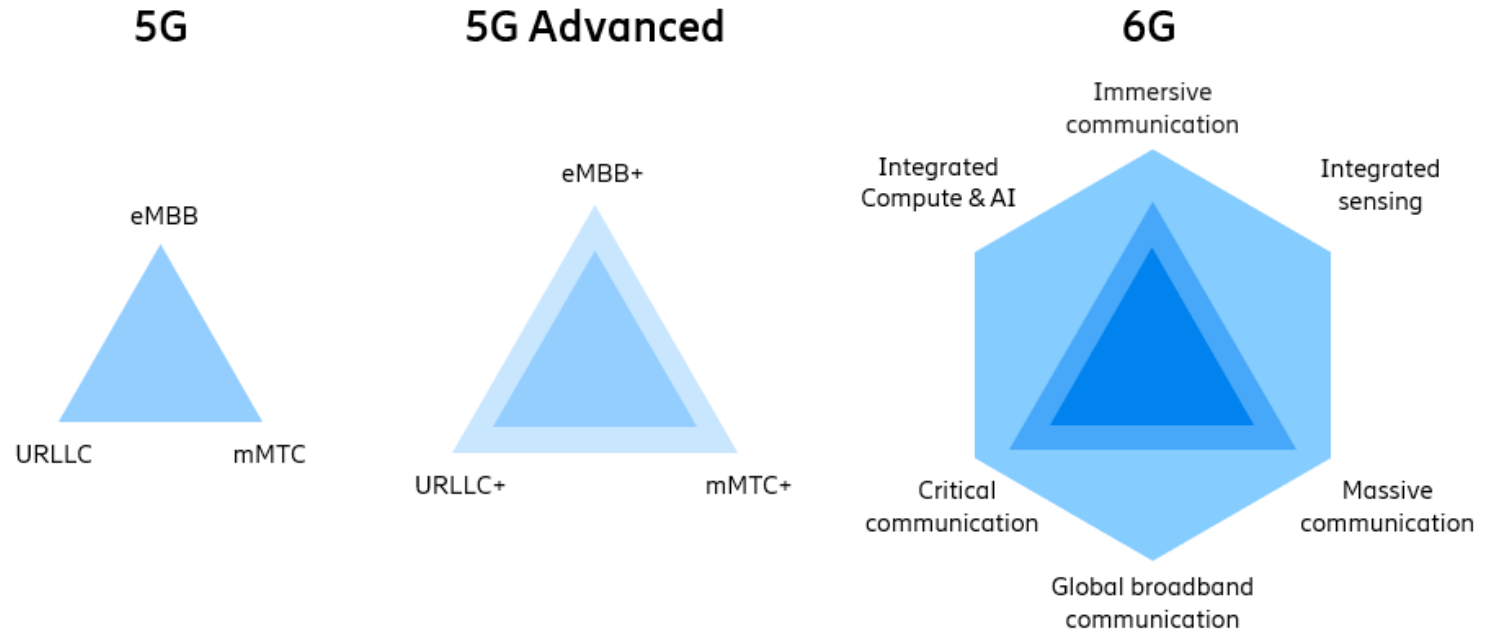
Introduction

Connecting a cyber-physical world

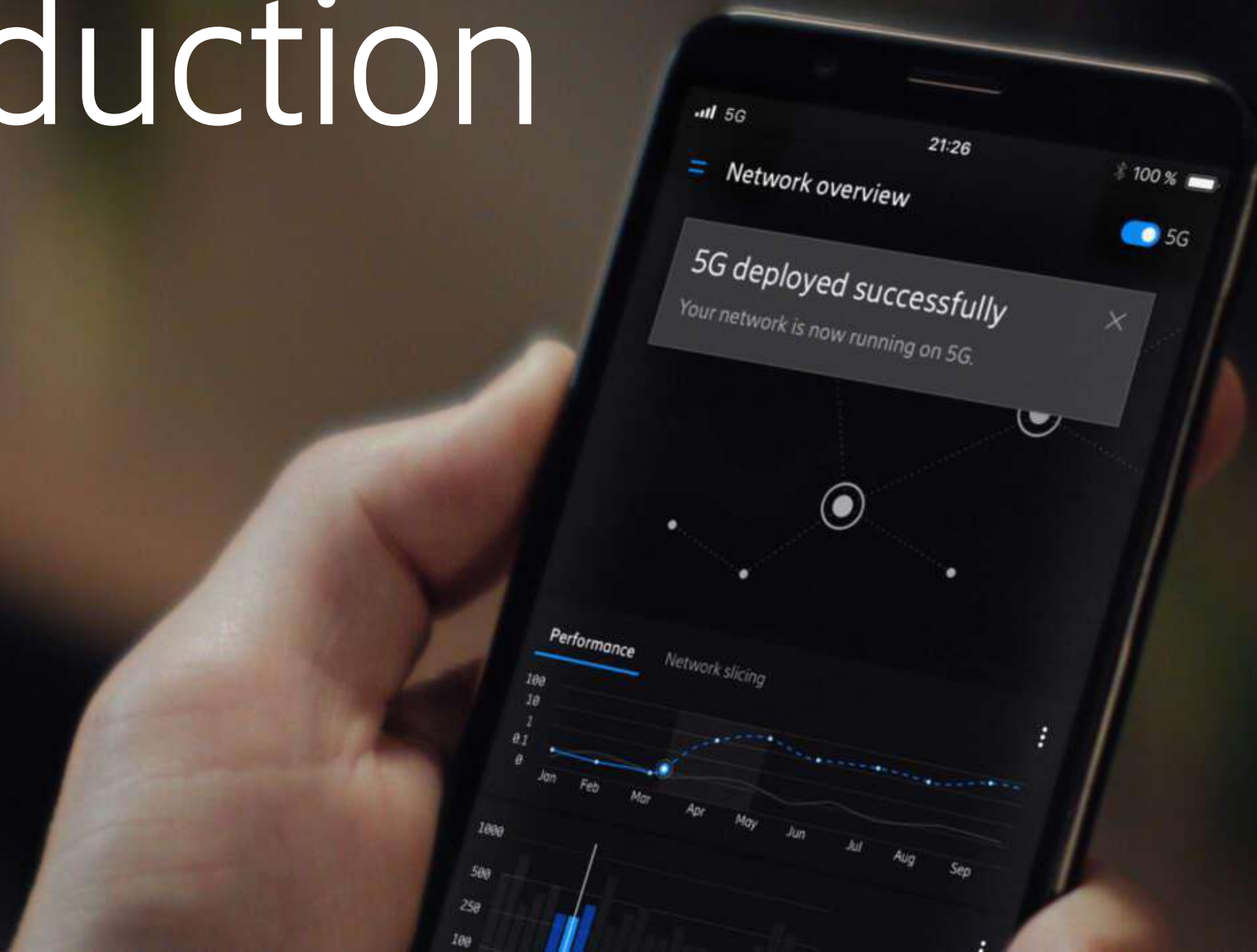
6G network platform

Some examples

Summary



Introduction



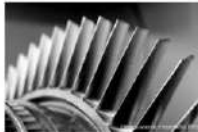
5G – going beyond the smartphone



Complex metalworks not possible to monitor today

Development

- Ericsson has together with the Fraunhofer IPT research center optimized the production of Bladed disks, BL15Ks, through 5G technology.
- A BLISK is used in turbines such as jet engines. It consists of a rotor disk and multiple blades around it.
- BLISKs are one of the most difficult machining parts to produce, and the rework rates are very high (~25%).
- A key aspect of BLISK production (and metal processing in general) is that the process is not monitored – if data can be collected during manufacturing and used to fine-tune the process, rework rates can be significantly reduced.



5GEM 5G Enabled World Class Manufacturing

- Evaluate 5G technology in a manufacturing industry
- Understand ICT opportunities and solutions

Use cases: Data analysis, Factory wireless communications, Mobile control panel

- Improved production efficiency
- Increased flexibility
- Excellent traceability
- Social and environmental sustainability



Partners: SKET, CHALLENGE, ERICSSON

REMOTE OPERATION Robot remote control with haptic feedback over LTE

- Evaluate mobile communication in industrial remote operation
 - Remote operations in mines – an industrial use case with strict requirements on reliability and latency.
 - Explore the use of industrial haptic communication in mobile networks
- Greatly improved health and safety
- Increased availability of personnel
- Capture key requirements for 5G



Partners: ABB, ERICSSON

CMA Test Site for Future Automated and Shared Mobility Systems

- Exploring the use of 5G networks for intelligent transport systems
- Investigating "as-a-service" offerings for network operators and automotive OEMs
- Reduced vehicle fleet operations cost
- Better service awareness and reduced travel time for passengers
- Usage of cellular networks in new markets



Partners: SCANIA, ERICSSON, ABB – INDUSTRIAL DIGITIZATION, VOLVO GROUP

5G NETMOBIL

- Develop overall communication infrastructure for tactile connected driving beyond the self-contained sensor-based autonomous driving
 - Improved road traffic safety, less environmental impact, and higher efficiency of road transportation
- Provide 5G communication technologies and network architecture for tactile connected driving
 - Low latency required by real-time vehicle control and cooperative maneuvers
 - High reliability and availability for highly mobile environments
- Use cases:
 - Parallel cooperative driving of a fleet of farm machinery in off-road areas
 - Tactile connected driving of vehicles at intersections of urban roads
 - High-density platooning of trucks in automotive test field



Partners: octicom, BOSCH CARAS, ERICSSON, Fraunhofer, MUEHLER, NOKIA, VOLKSWAGEN

PIMM Pilot for Industrial Mobile Communication in Mining

- Explore future 5G Use Cases in underground mining
- Evaluate mobile communication infrastructure in an industrial context
- Increased Productivity and improved Safety
- Industrial 5G requirements
- Understand eco system, business models, etc.



Partners: TeliaSonera, VOLVO, ABB, BOLDEN, ERICSSON, NOKIA

WITOOOL Wireless Internet of Tools

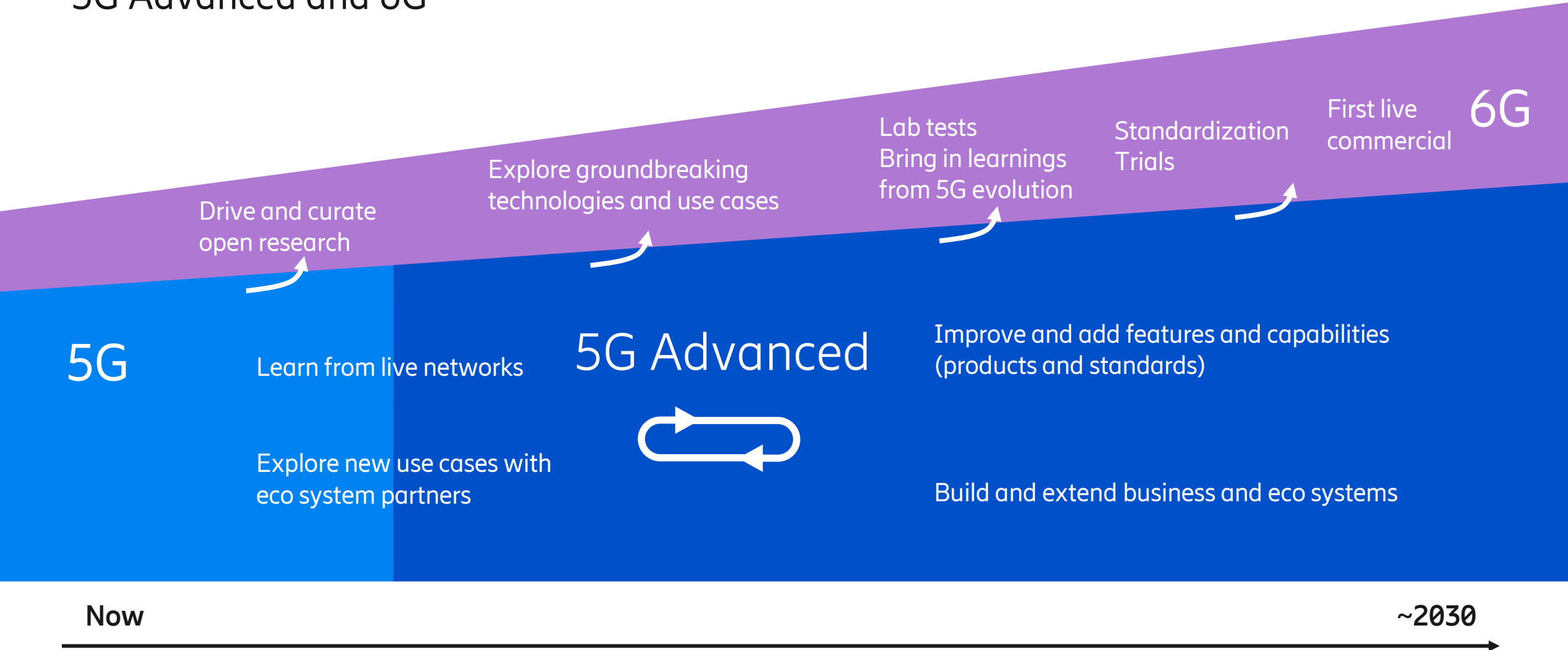
- Enable IoT for construction equipment OEM (trucks and mobile companies: Cranes)
- Capillary network connectivity, cloud service enablement and machine analytics capabilities
- Demonstrate through automation of return process of machines at Crane depot
- Efficient fleet management enabled by predictive maintenance and resource planning
- Automated processes, for example return process
- New business models
- Making use of generated data to improve products



Partners: HUSQVARNA, ERICSSON

Evolution and long-term horizon

5G Advanced and 6G



Connecting a cyber-physical world

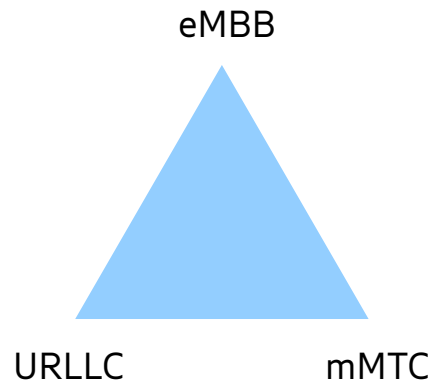


Journey to 6G

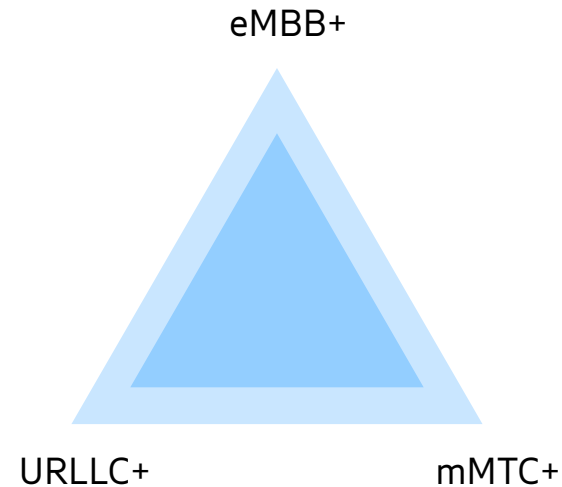
New advances in connectivity create new opportunities for digitalization



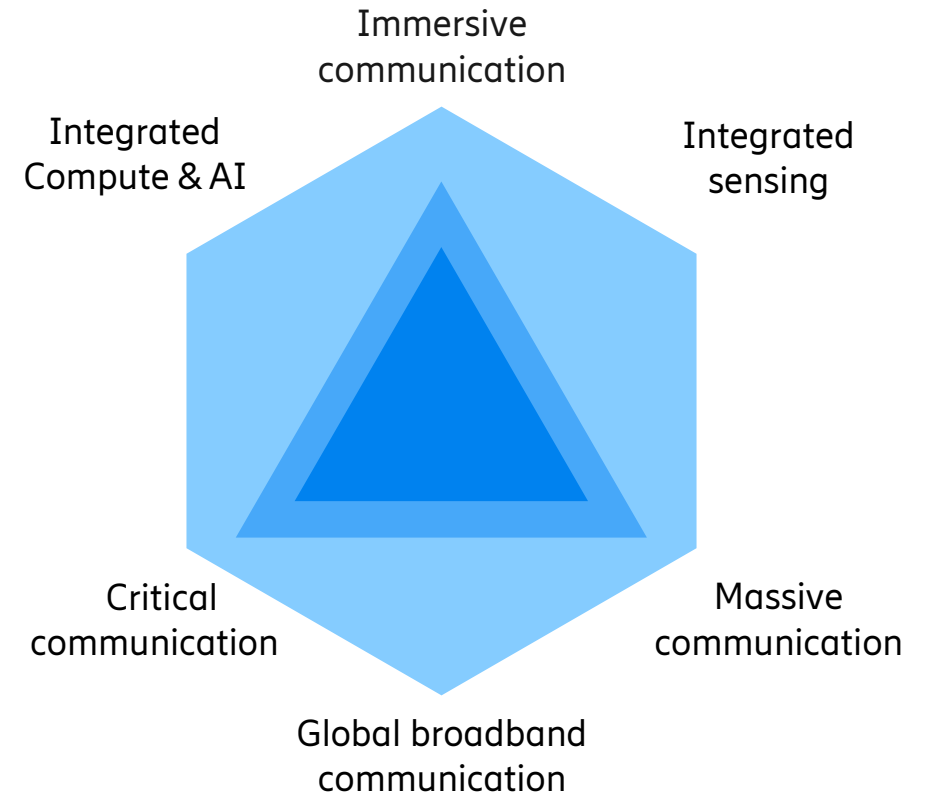
5G



5G Advanced



6G



6G focus areas



Communication beyond 5G & Further enhanced MBB



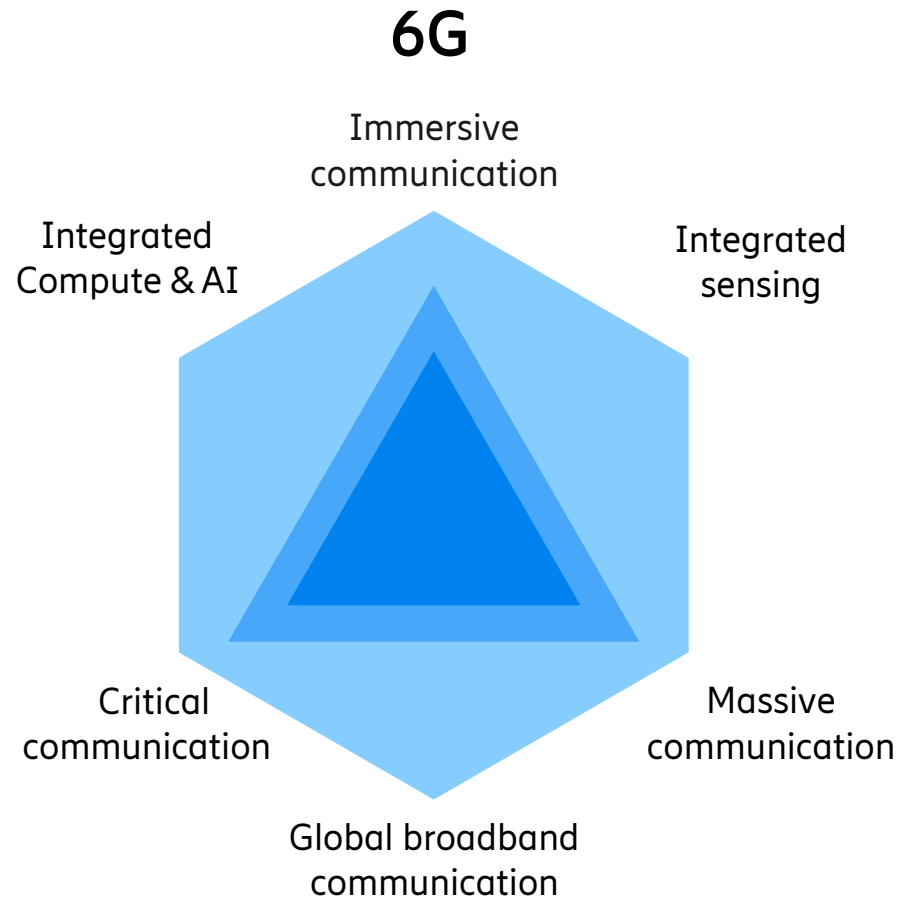
Immersive communication –
expanding on eMBB



Critical communication –
expanding on URLLC



Massive communication –
expanding on mMTC



Beyond-communication networks



New services on 6G platform

Sustainable and trustworthy networks



Sustainability and trust
imperatives

Some 6G usage scenarios



New advanced services



Merged reality

- New ways of meeting and interacting with other people
- New possibilities to work from anywhere
- New ways to experience culture and scenes far away



Massive twinning

- Connecting all equipment and tracking material
- Using the network as a platform for many ecosystems
- Allowing accurate predictions and detailed control



Situational awareness

- Sensing surroundings and locating objects
- Guiding robots and vehicles with digital maps
- Interacting with collaborative robots

Efficiency and Sustainability



Sustainable Food Production

- Soil-plant and weather data collection for minimized resource use
- Optimized harvesting (demand-storage-transport availability-based)
- Knowledge and equipment sharing for small scale farmers



Efficient Global Broadband

- Optimized resource consumption of key network components (spectrum, energy,...)
- Extending coverage, simplifying deployability
- Intelligent QoS vs resource efficiency balance
- Getting more out of the existing grid

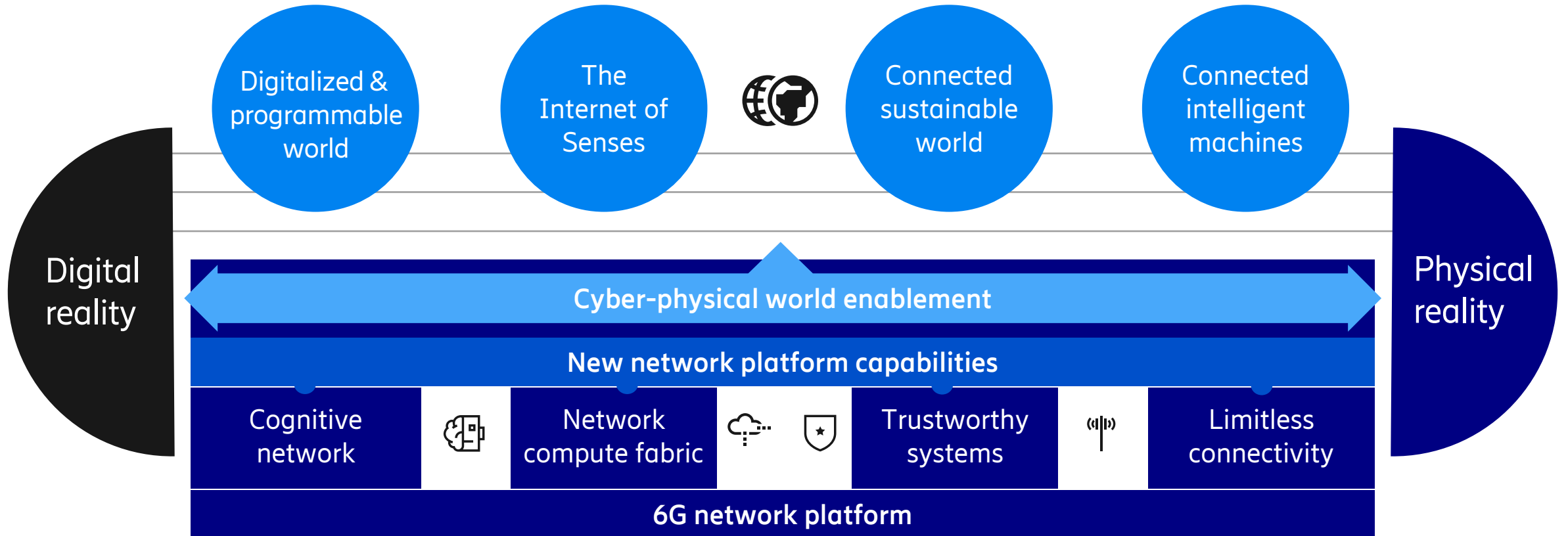


E-health for all

- Basic health-care everywhere, including simple monitoring
- Basic video services everywhere
- Privacy and data confidentiality

Connecting a cyber-physical world

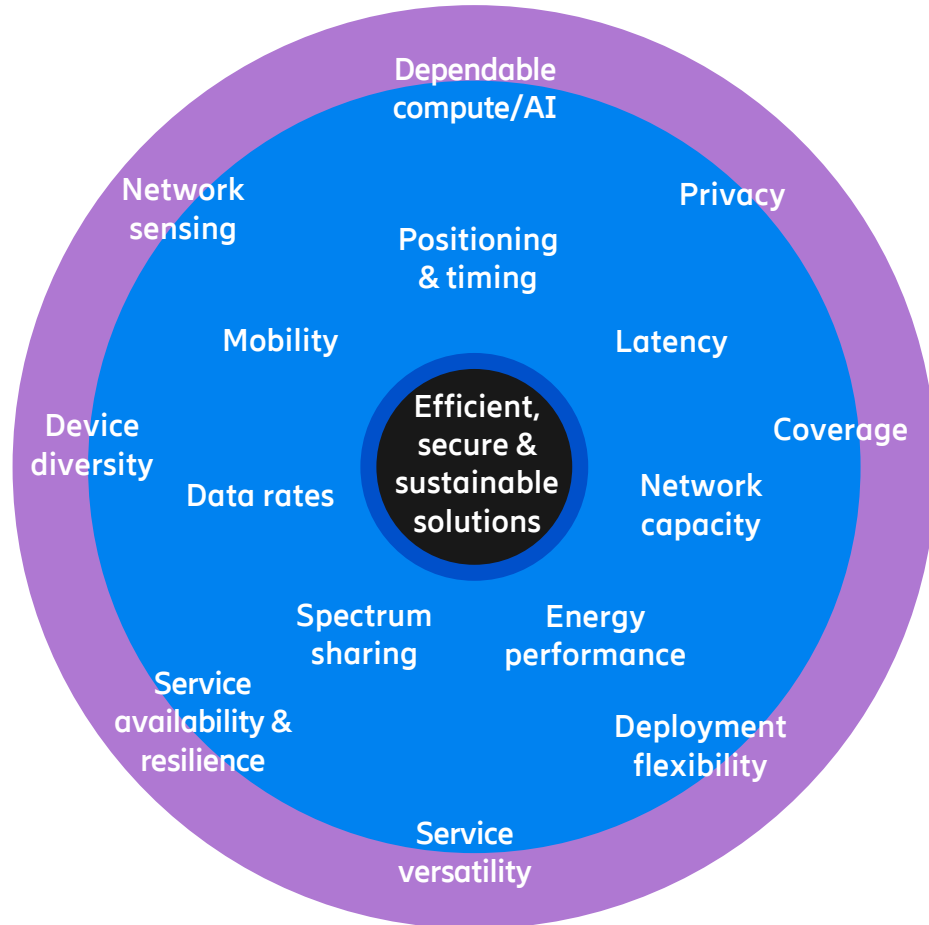
Arriving at the 6G destination – 6G network platform



6G Network Platform



6G capabilities



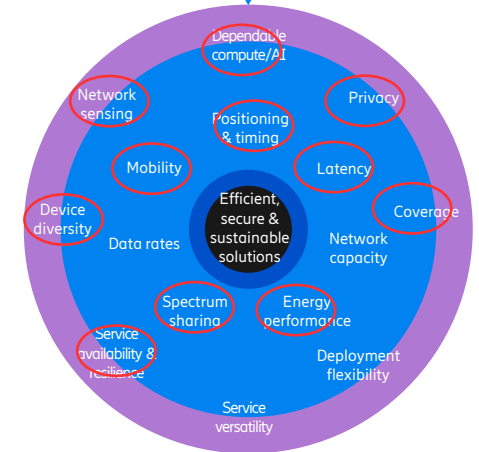
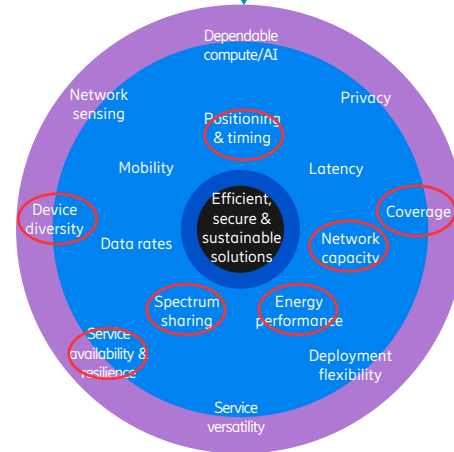
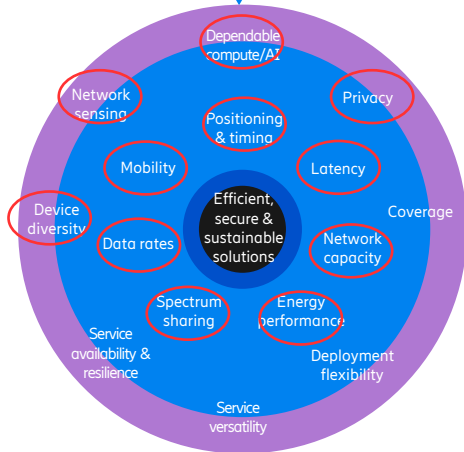
Beyond-communication networks

Communication beyond MBB

Further enhanced MBB

Efficient network operation

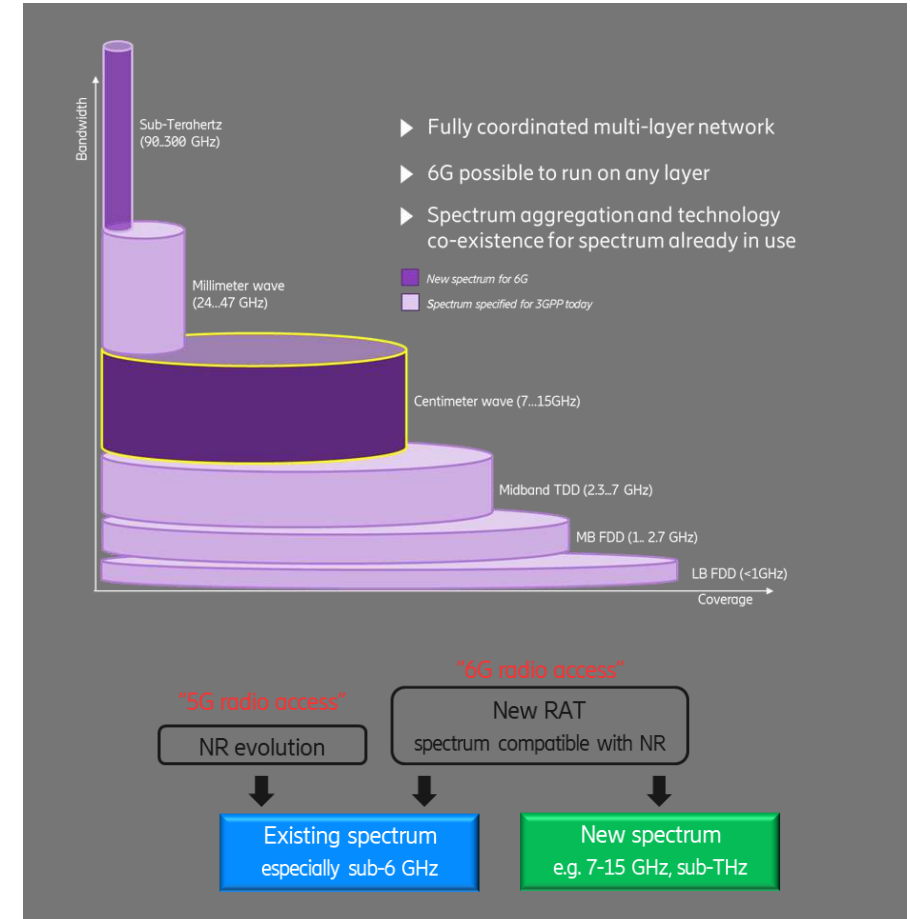
6G use cases driving capabilities



Key 6G Principles



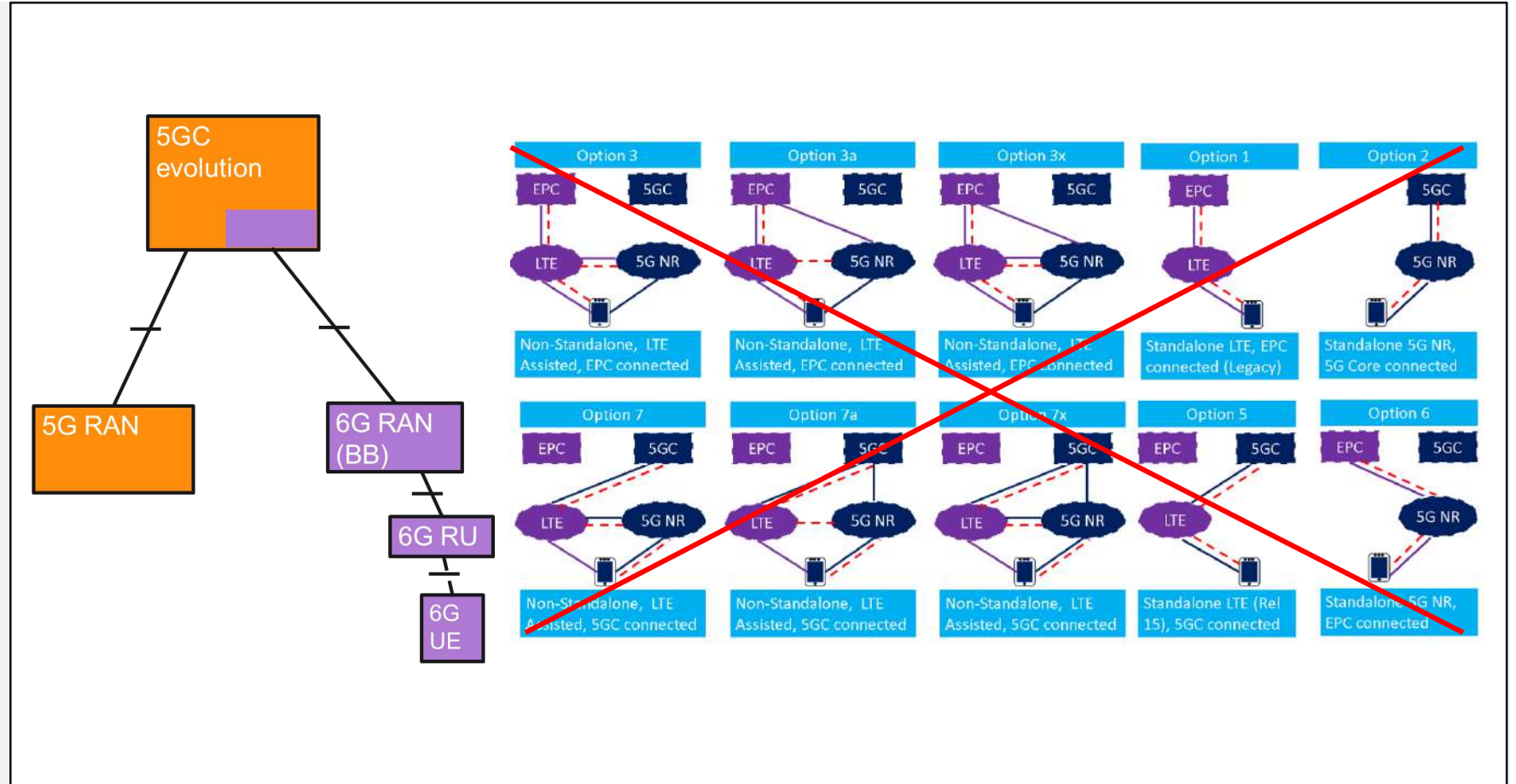
- 6G shall be possible to **operate in all existing 3GPP bands** and in new bands, when allocated & specified
 - Critical to this evolution is the mid-band/centimetric range (i.e., 7-15 GHz range)
- 6G is a **new Radio Access Technology**
- **6G Spectrum Sharing** shall be supported with selected 3GPP technologies
- The standardized 6G architecture should include **open interfaces** to facilitate a healthy ecosystem
 - 6G RAN shall have a **standalone** architecture
 - **Reuse investment in 5G Core**, allowing smoother 6G introduction, and alignment of migration paths
- 6G shall include evolved solutions for enterprise and dedicated networks



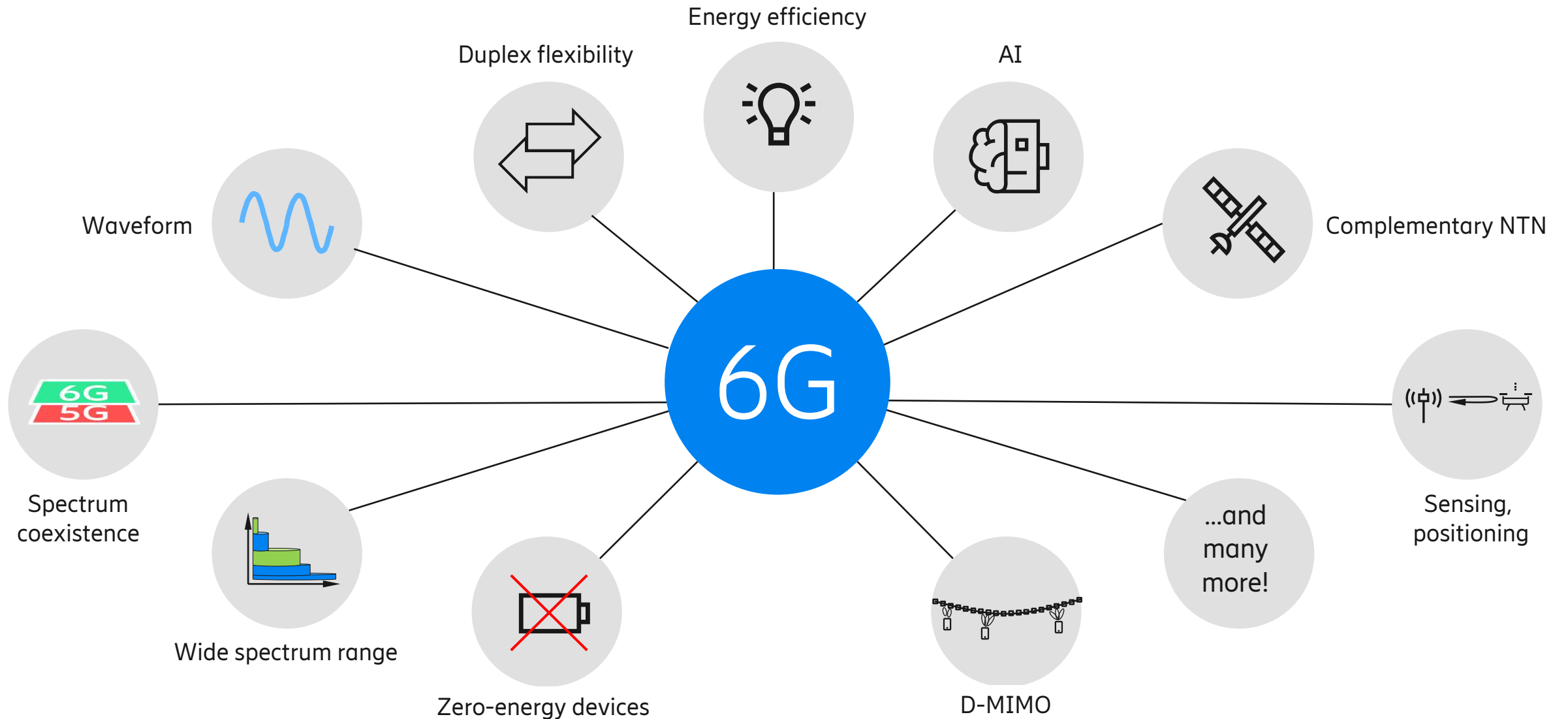
Important of smooth 6G introduction



- Alignment within industry on **key migration path** prior to start of standardization
- **Enable fast deployment of SA 6G** by avoiding unnecessary deployment options
- Aim to **simplify the 6G architecture**, by aligning industry on key interfaces for standardization
- **Reuse investment in 5GC**, allowing smoother 6G introduction, and alignment of migration paths



6G technologies – some examples



Some examples



Ericsson 6G demos @ MWC 2023



Digital twin of a
6G network

Extreme performance
in sub-THz spectrum

Centimetric spectrum
and its essential role
for 6G

Zero-energy
devices

Energy-harvesting — no need to change battery



Enabling sustainable asset trackers, on-body sensors and mass deployment sensors

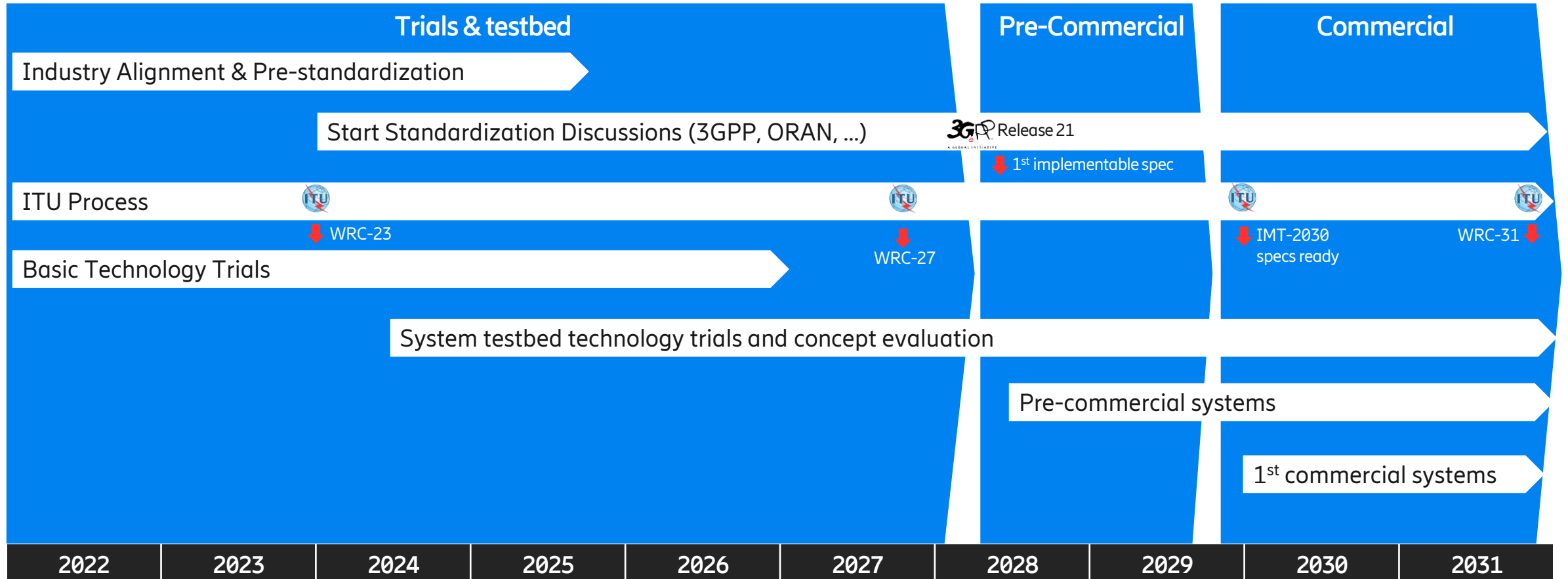
Summary



6G Timeline – Ericsson View



High-level 6G timeline



The 6G Ambition



Use Case Areas

- Immersive XR
- Global Broadband
- Situational Awareness
- Massive Digital Twinning
- Omnipresent low energy sensors
- For consumers, enterprise & society

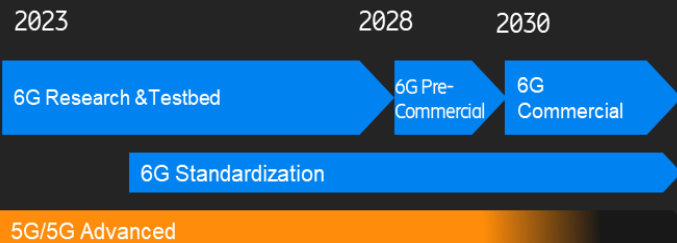
Technology Focus

- Spectrum Aggregation, Spectrum Sharing
- Multi-dimensional RAN co-ordination
- Intent-based automated E2E SLAs
- Energy Efficient Solutions
- Operation in new spectrum
- Precise Spatial locating
- Coverage Extension

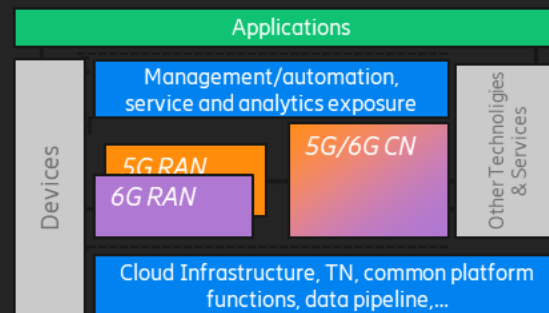
Network Capabilities

- >100 X capacity
- 100% Global Coverage,
- Positioning accuracy <cm
- Peak data rates of 100Gbps+
- Trustworthy, Secure, Sustainable
- Wide area consistent latency <5ms
- Public, private indoor and outdoor solutions

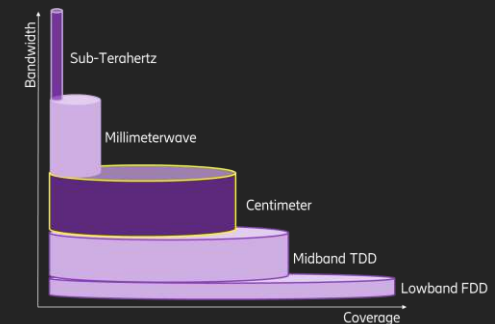
6G Timeline



Future Network Platform



Future Network Platform





Artificial Intelligence in mobile infrastructure

Caroline Jacobson

Head of system management, Global AI Accelerator
Ericsson

June 26-27, 2023

Conference for Governments and Regulators

New applications place higher demands on networks & create new opportunities



2G

A network for voice services

3G

A network for voice & data services

4G

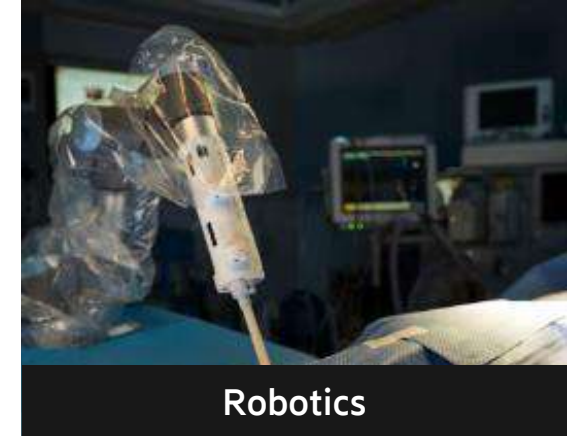
A network for video & data services

5G

A network for a million different needs



Autonomous vehicles



Robotics

6G

Ever-present intelligent communication



Augmented reality



Converged digital physical world

Telecom AI – For current and future technology



Limitless connectivity



AI for ultra-reliable connections

Cognitive network



AI for openness in technical & business interfaces

Connected sustainable world




AI for Energy Efficiency

Trustworthy systems



AI for trustworthiness

Network compute fabric

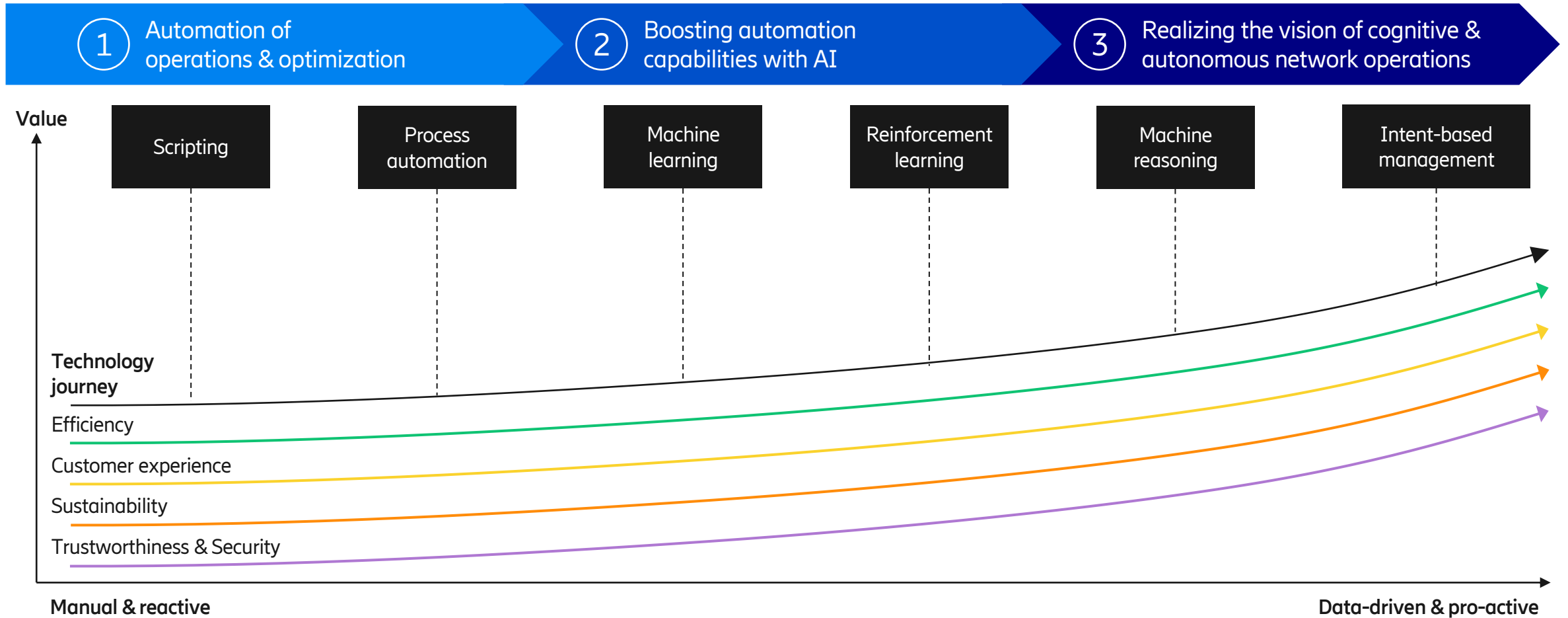


Edge Compute for AI



ericsson.com/ai

Evolution of automation



Ericsson holistic take on intelligent automation leveraging AI



Executed where it makes sense. Ensures optimal efficiency and performance

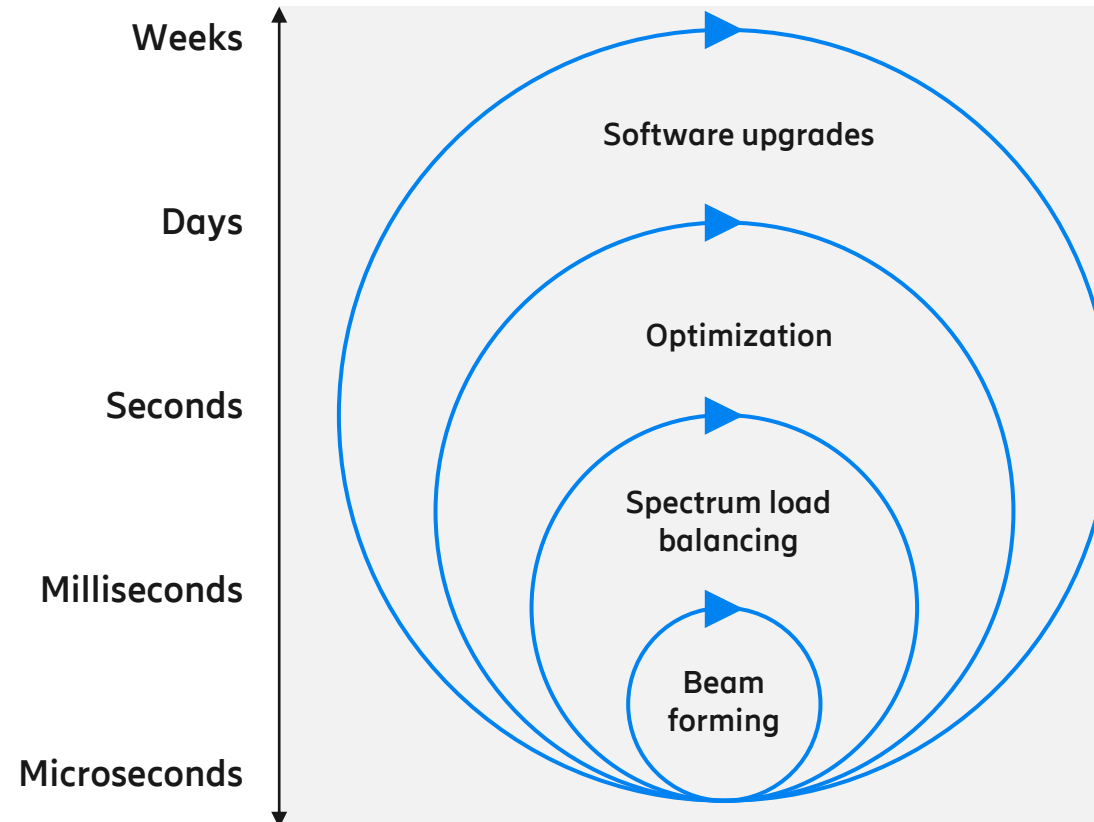
Centralized automation

- Network wide coordination
- Multi-technology/vendor
- More time available to make complex decisions
- Human interaction



Distributed automation

- Local
- High volume of decisions
- Fully automatic



Example use cases

Common data collection, governance and management

Vision of – Intent based networks



Business Intent

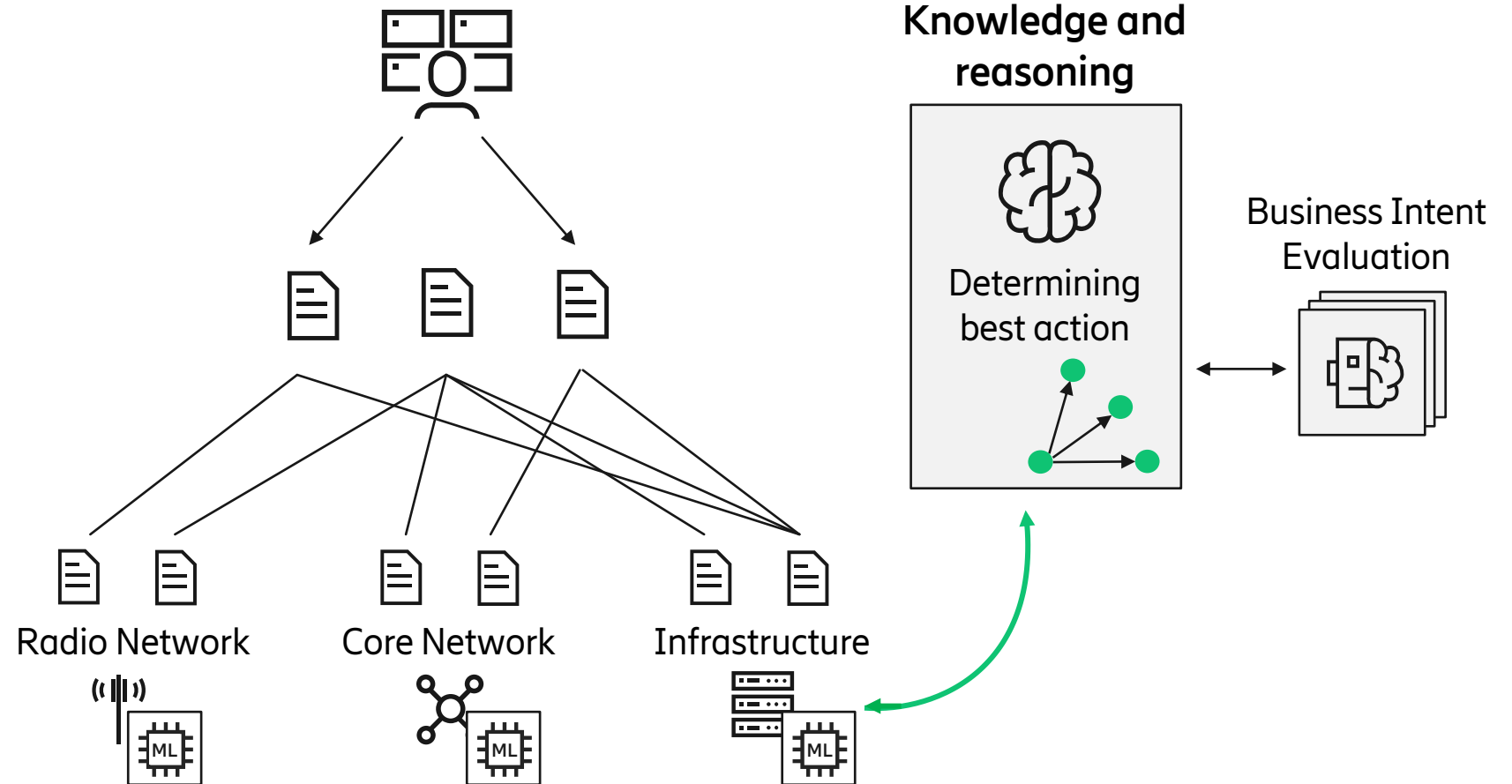
#1 network quality

Service Level Goals

e.g., perceived throughput improvement

Network Level Goals

e.g., reduce traffic congestion, interference



Trustworthy AI for telecom



Humans Oversight

Humans in the loop

Robustness

- AI security
- Model verification

Privacy & Data

- Data quality & data transfer
- Privacy data

Fairness

Bias between sites

Sustainability

Energy Efficient AI

Transparency

Explainable AI

Energy Savings – LTE Cell Sleep Mode Optimization using AI

Services

Ericsson rApps

EIAP (SMO)

ENM

RAN

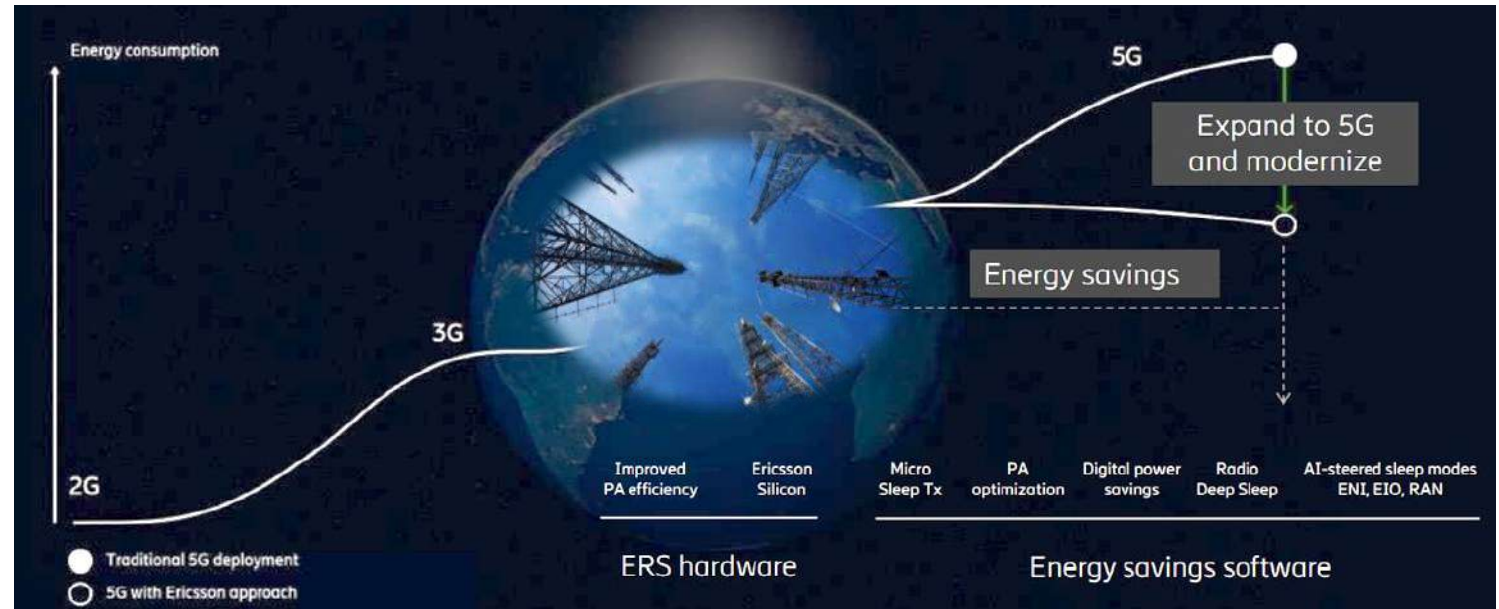
Local training Humans
in loop Deep NN



Reduced energy consumption levels per cell by dynamic configuration of Cell Sleep Mode without degrading the network performance

12% Reduced Energy Consumption

- Implemented energy savings framework on live network
- Observed Up to 12% improvement in energy consumption
- New service offering with Customer Unit by demonstrating Ericsson's AI competence and domain expertise



This AI driven solution enabled a mechanism to provide dynamic thresholds to the cell sleep mode by selecting the best threshold candidates for the ENM energy-saving feature.

Automatic Cell Outage Management

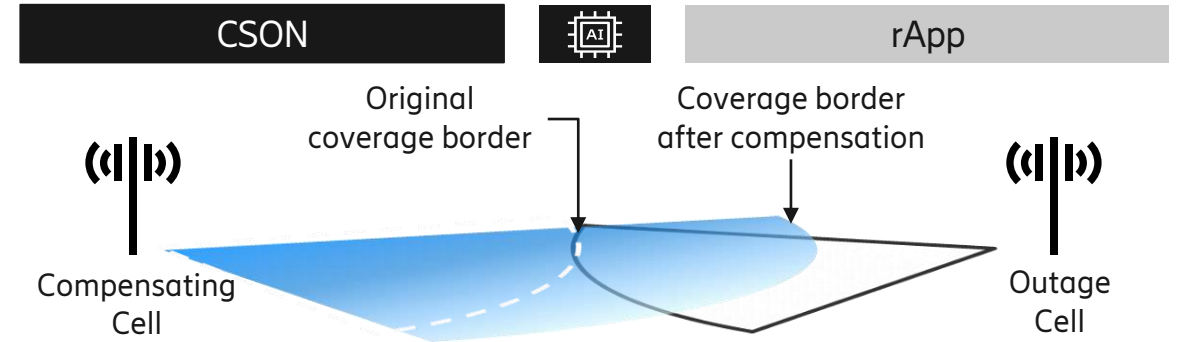


Automatic Cell Outage Compensation with zero manual intervention

Cell Outage Compensation automatically detects and compensates for cell outages in the LTE network. Actions are automatically reverted once the cell returns from outage. Extend neighbor cells coverage to minimize the impact of a cell out of service, while meeting acceptable service level.

Benefits & differentiators

- Autonomously detect cell outages and thus removes manual work
- Fast response to cell outages (Closed-Loop Automation)
- Increase the network availability
- Enhance the user satisfaction and the churn reduction
- Reduce the need for unplanned visits



>1200 h

Of outage compensated in one month spread over 500 single-cell and site outages¹

Based on real customer outcomes:

4G, 5G (roadmap)

"A great help for a well staffed and prepared operator, a revolution for the unprepared"²

1. European Operator
2. North-American Operator

MásMóvil – improving customer experience during peak hours



- Improve congestion and downlink throughput during busy hours in Malaga, Spain
- Antennas fitted with RET permit tilting adjustments via remote software commands instead of site visits, ideally suited for innovation towards the vision of zero-touch network optimization

12%

Increased **downlink** user throughput by using RL to optimize RET



Summary

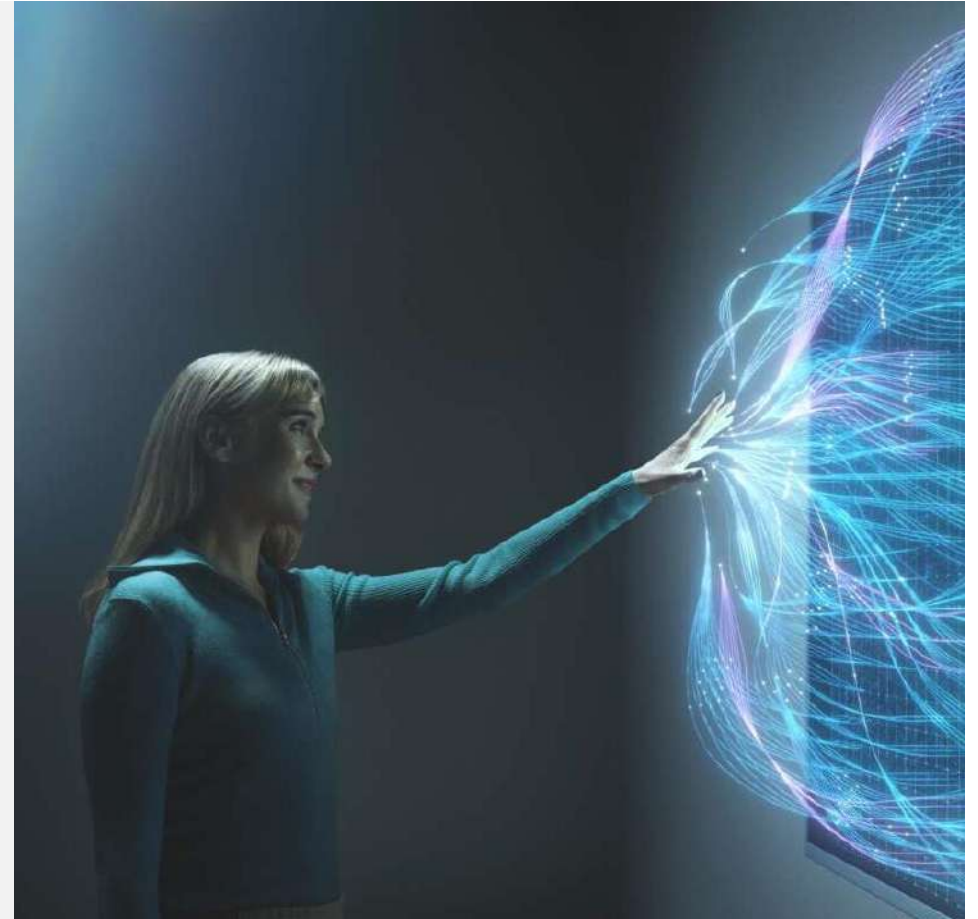


Ericsson's vision put high and diverse demands on the network

A world where limitless connectivity improves lives, redefines business and pioneers a sustainable future

AI is an important enabler

- Limitless connectivity everywhere
- Energy Efficiency
- Resilience
- Trustworthiness



Ericsson AI strategy based on strong research and development



Our AI is built on a strong foundation of deep telecom expertise combined with data science and AI-knowledge



Ericsson AI research areas



AI in Control



Distributed Intelligence



Trustworthy AI



Cognitive Networks



AI Infra



Generative AI

AI related launches

[Performance Optimizers](#)

[Network Data Analytics Function \(NWDAF\)](#)

[Intelligent Automation Platform](#)

[Intelligent RAN Automation](#)

[Intelligent Deployment](#)

[Service Continuity](#)



Open APIs for advanced digitalization

Christer Boberg

Head of Technology & Strategy, Global Network Platform
Ericsson

June 26-27, 2023

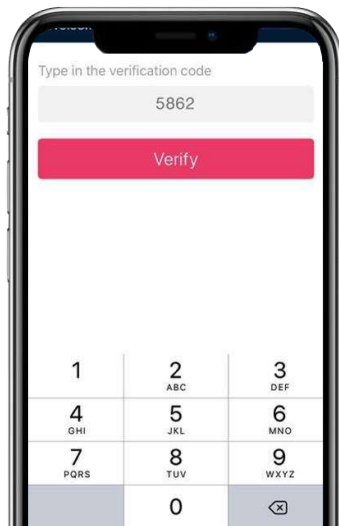
Conference for Governments and Regulators

Today: Developers creatively engaged customers with SMS and voice APIs creating stickiness & a new industry



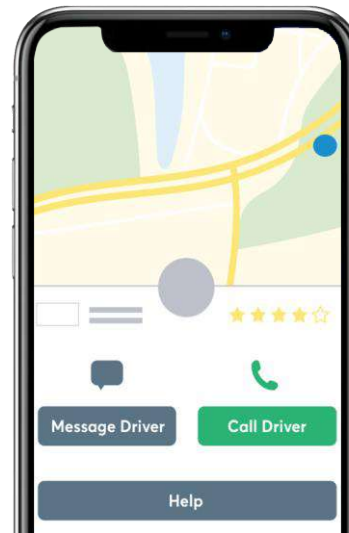
Two Factor Authentication

Application validates users via their mobile devices with one time passcode via SMS



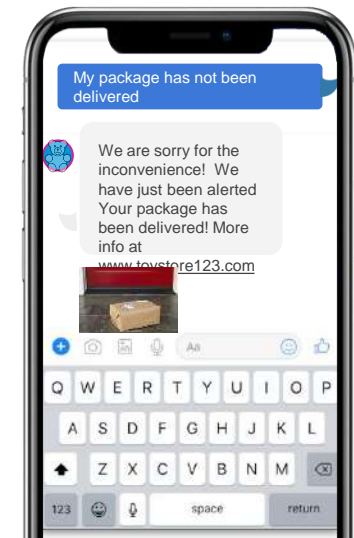
Private Voice Communication

Application sets up a call between the driver and the passenger

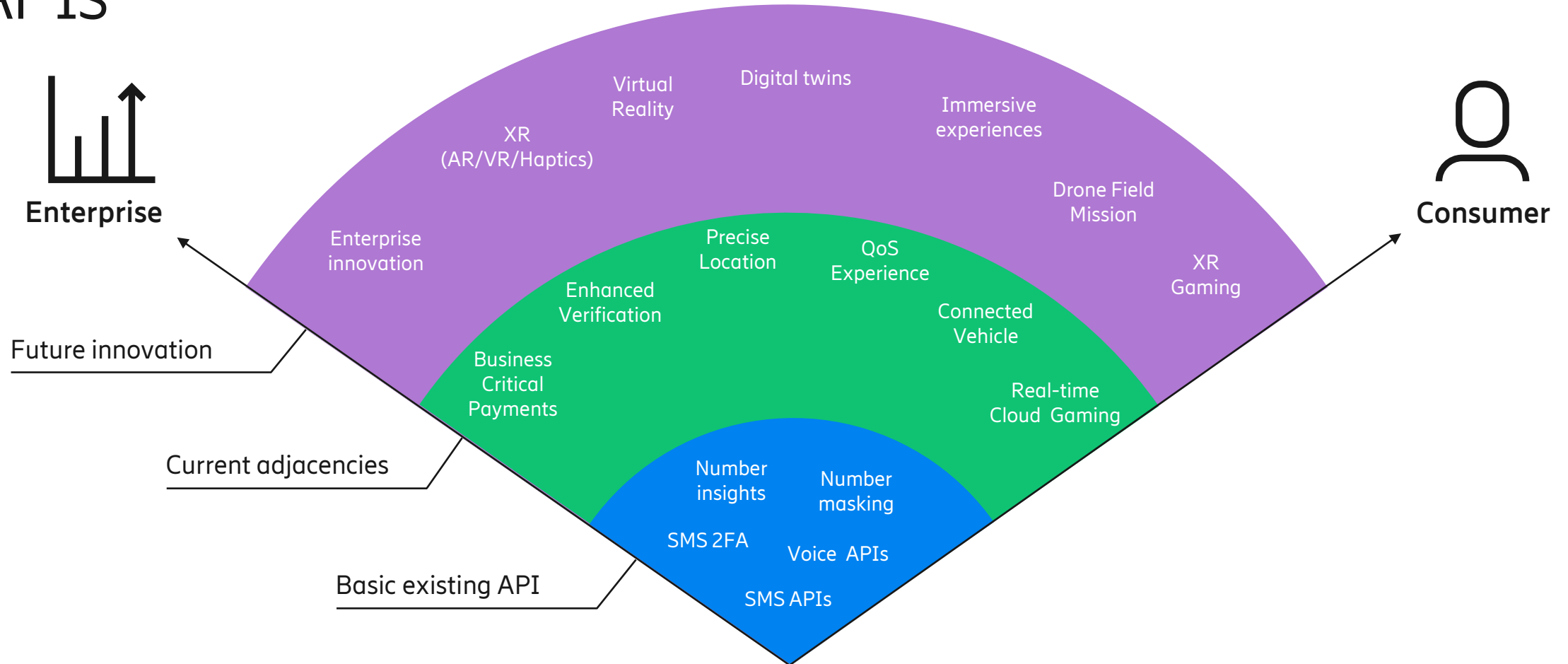


Programmable Messaging

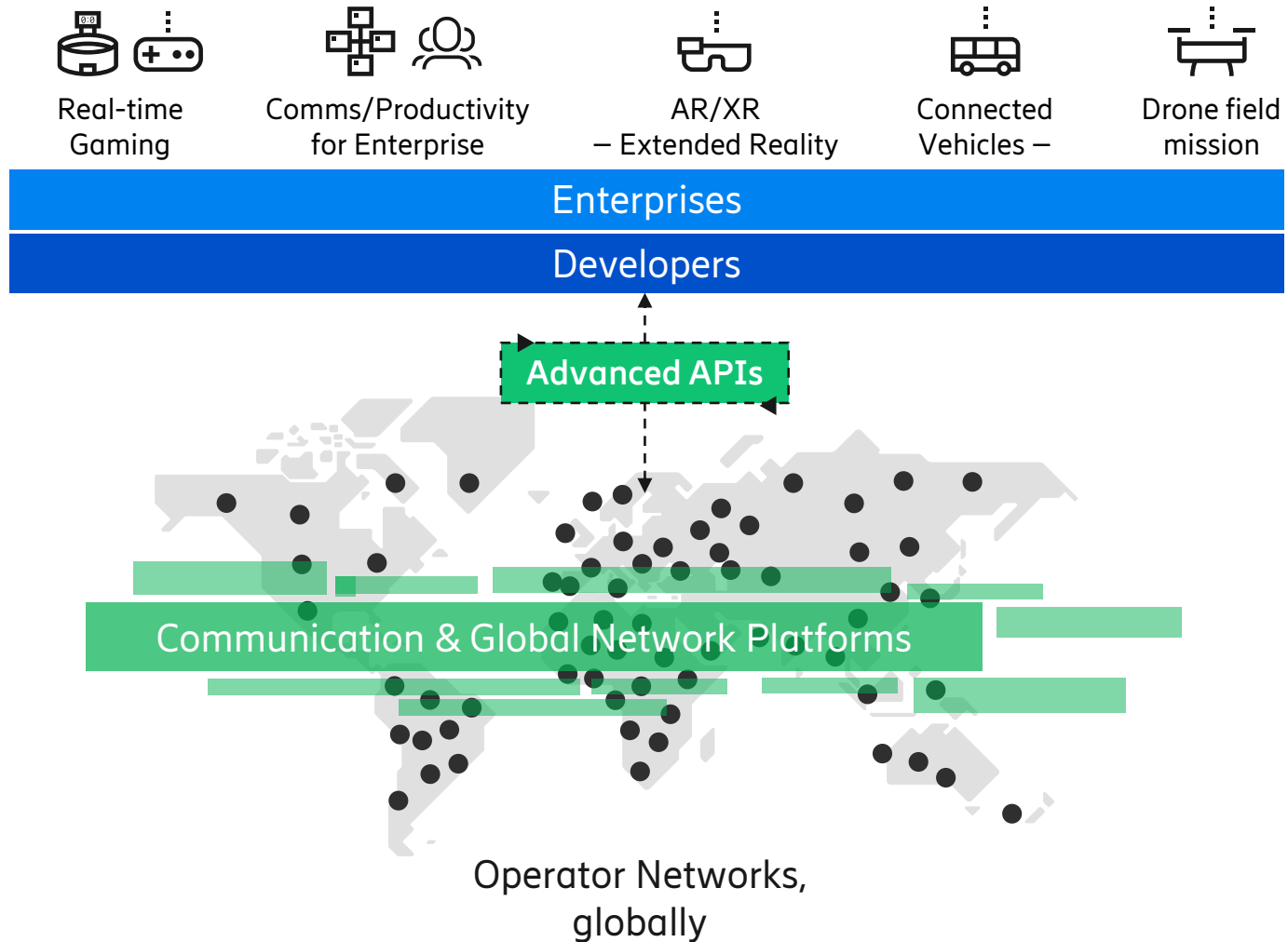
Customer can send SMS to courier to confirm delivery options and receive live updates



Tomorrow: Accelerate evolution & monetization through app development using new network-based APIs

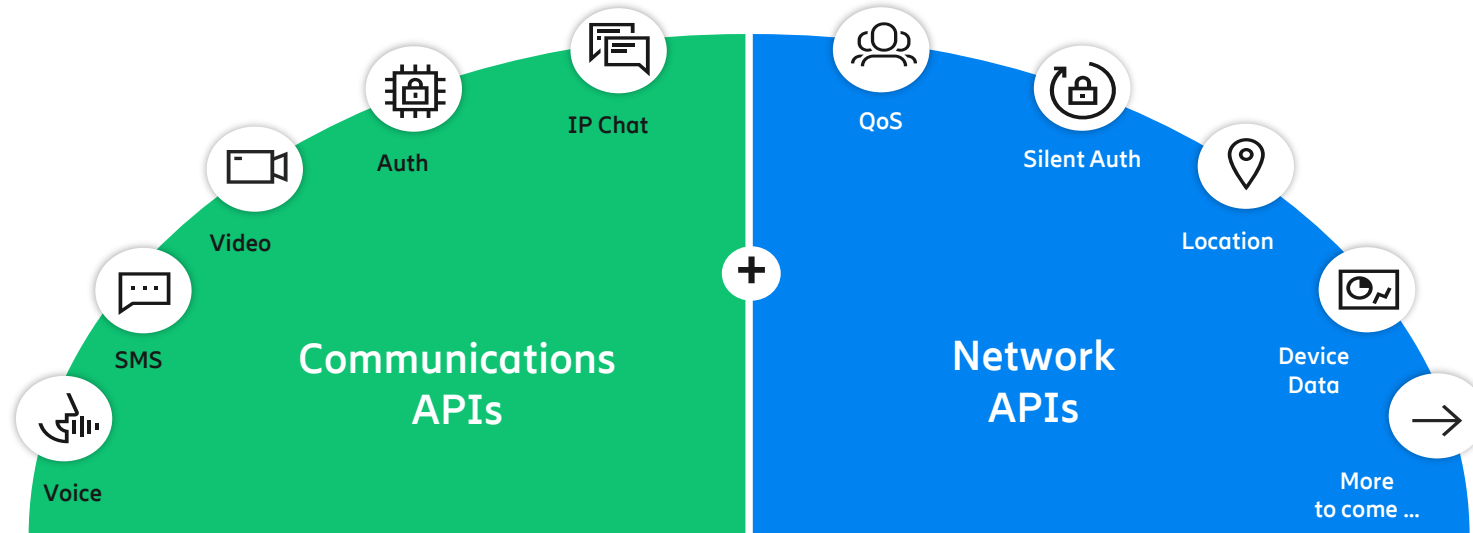


Global Network Platform



- Leading global network platform for open innovation on top of 5G
- “Put the power of the network at the fingertips of developers”
- 5G and the global operator community - the foundation for high performance networks and new capabilities
- Enabling the next wave of premium and new communication experiences

Communications and network APIs drive innovation



APIs empower developers, simplify application creation, and optimize performance



High speed & Low latency



Reliability



Wireless edge solutions



Security



Network slicing

Worldwide 4G and 5G networks

CAMARA – The Telco Global API Alliance



- An [open-source project](#) within Linux Foundation to define, develop and test the harmonized telco APIs
- Close collaboration with the GSMA Operator Platform Group and 5GFF
- Announced in MWC 2022
- Over 135 companies participating (MWC 2023)

Anonymized Subscriber ID	Carrier Billing Checkout	Device Identifier	Device Location
Device Status	Edge Cloud	Home Devices QoD	Identity and Consent Mgmt
Number Verification	OTP Validation	Quality on Demand	SIM Swap

Long term vision for a thriving eco system



Real-time
Gaming



Comms/Productivity
for Enterprise



AR/XR
– Extended Reality



Connected
Vehicles –



Drone field
mission

Devices / Apps / Platforms / Enterprises / Value Added Resellers

Developer Ecosystem

API

Operator
B2B

CPaaS
platforms

HCP
Marketplaces
and
Platforms

Ericsson
Global Network
Platform (GNP)

E.g., Camara
and TM Forum

API

API

API

API

API

Operator 1

Operator 2

Operator 3

Operator 4

Operator 5

- An open eco system to maximize market exposure and reach
- Any network vendor, any operator, any aggregator
- Standardization will improve usability and scale
- Aggregators will consistently expose to developers on global scale

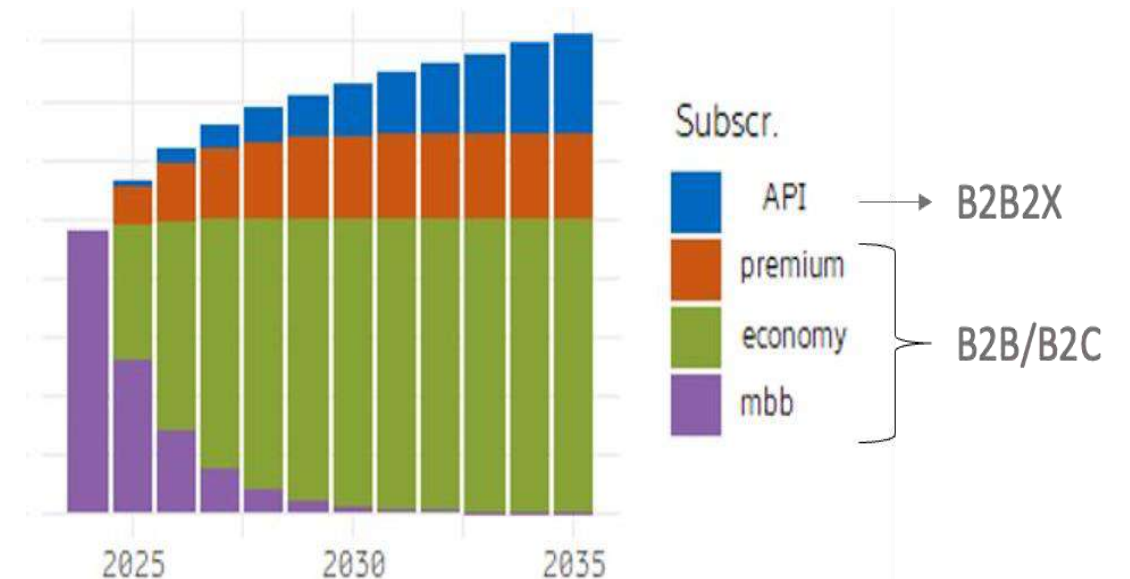
Going from B2C/B2B to B2B2C



Two models for CSPs to monetize in 5G networks.

1. Via a **subscription**, where end-user (consumer or enterprise) pays the operator for a service. This model is also referred to as **standard B2B/B2C** model.
2. Via **service exposure API**, where an Application Service Provider (ASP) pays the CSPs for a service. This model is also referred to as **B2B2X** model.

These models are complementary and a combination of B2B/B2C and B2B2X models is a preferred model to serve both standard subscription and API based monetization.



Regulative aspects



New network services will open up for new markets and monetization but will put new requirements on regulations

New network APIs such as QoD, Verify Location, Device Status, Silent Authentication, Capacity booking will all require detailed understanding of the regulative aspects

Net Neutrality, Privacy, Data Sovereignty etc.



Key takeaways



Network APIs will be fundamental for new industry use cases and for CSPs to monetize

Standardization in e.g., Camara and TM Forum for broad adoption

Access to critical mass of developers utilizing Network APIs will be key factor of success

An open eco-system with aggregators and developer platforms

Exposure of new types of Network APIs will put new requirements on regulatory frameworks

Regulations protecting consumers enabling a thriving API eco-system



5G for Autonomous Shipping: highlights, concerns, prospects

Paolo Pagano

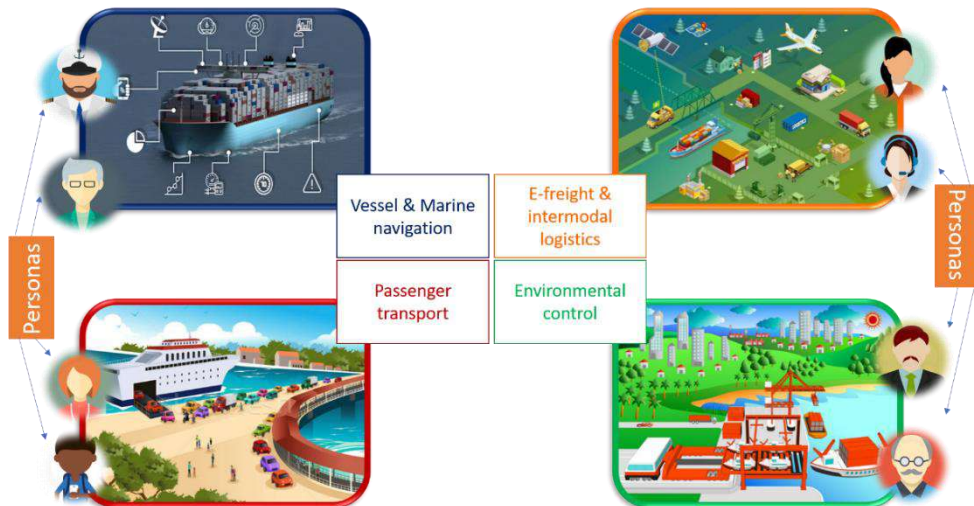
Head of «Technology Transfer» Research Sector
Director of CNIT Laboratory @ Port of Livorno

<http://jlab-ports.cnit.it>

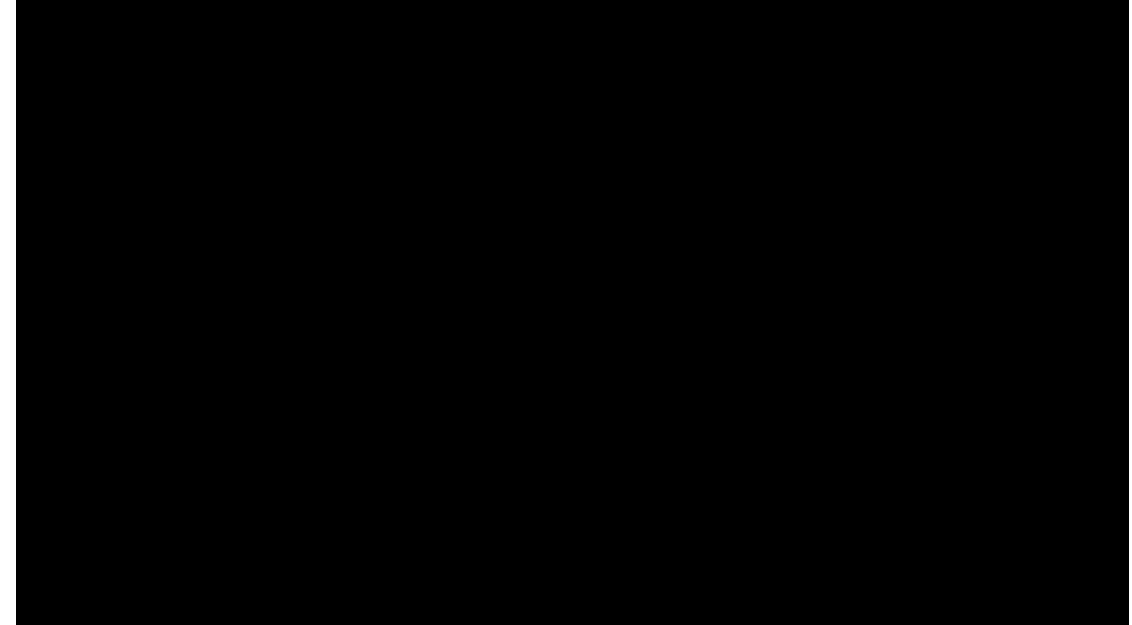


E/// B4A
Stockholm, 27/6/2023

- CNIT (National Inter-University Consortium for Telecommunications)
 - 41 Italian Universities + 8 CNR research units + 7 National Labs
 - technology transfer in ICT towards industry, 1300+ researchers; 100+ own employees
- JLAB in Livorno:
 - Founded in 2015, framework agreements w/ Port Authority and the National Coast Guard until 2025, part of CITEM – Livorno Center of Innovation and Technology for the Blue Economy.
- Objectives:
 - Digital Innovation through standardization (data, networks and services) in four verticals:



© CNIT - not for public use



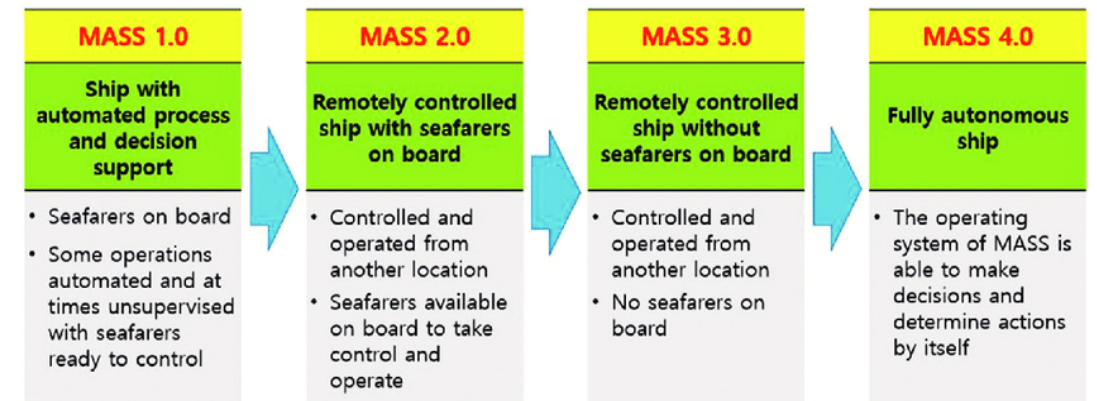
- The Autonomous Ship (setting the scene):
 - Regulatory framework;
 - Gap analysis and challenges.
- ITCG and ESA for uncrewed shipping in Italy
 - Background and prospects in Livorno;
 - The 5G MASS experience.
- Takeaway message to industry, authorities, and regulators.

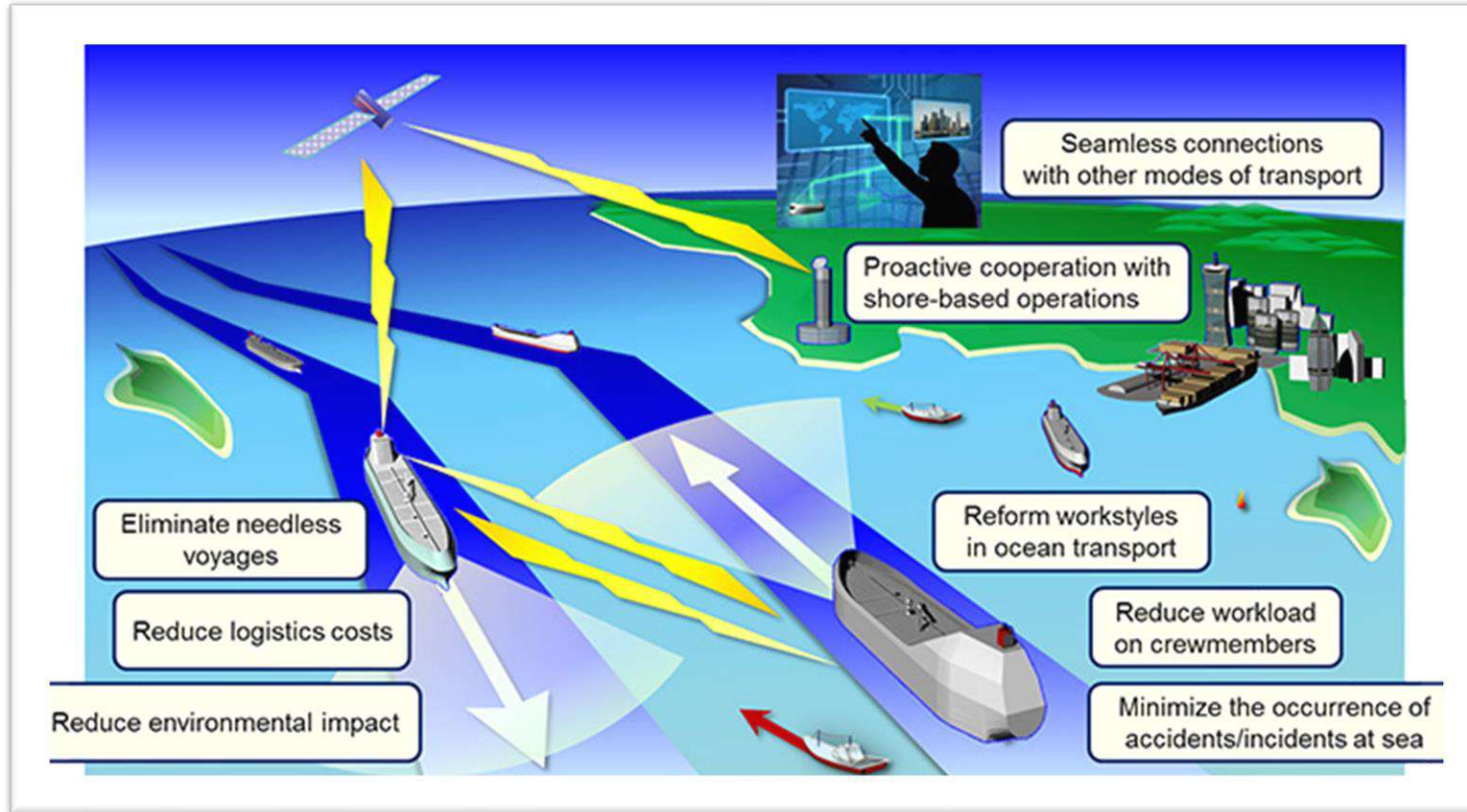


Background and Motivations



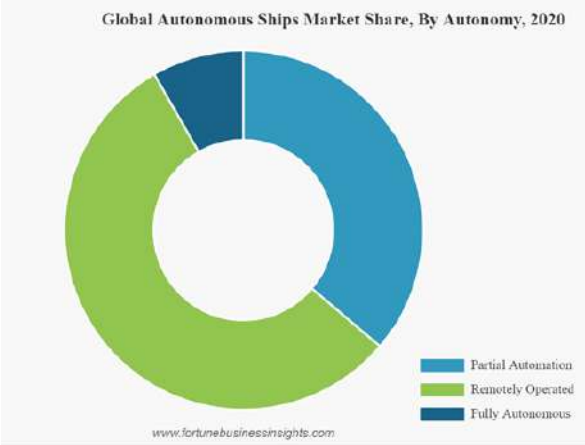
- Larger and faster ships, greater congestion and reduced manning levels.
- An autonomous ship should be able:
 - to monitor its own health and environment,
 - communicate obtained information, and
 - make decisions based on that without human supervision.
- The idea of autonomous ships has existed for decades and is becoming a reality:
 - IMO Maritime Safety Committee @ the 8th session (1964).
- Fully automatic dynamically positioned vessels:
 - common in the offshore industry in the 1970's;
 - use of on autonomous cargo ship demonstrated in Japan in the 1980's.
- Today, fully autonomous Unmanned Surface Vessels (USV's) are widely used in ocean research, coast guard and military applications while Maritime Autonomous Surface Ship (MASS's) are experimented by some flag states (e.g. Norway, Korea, Japan) and expected to turn operational soon.



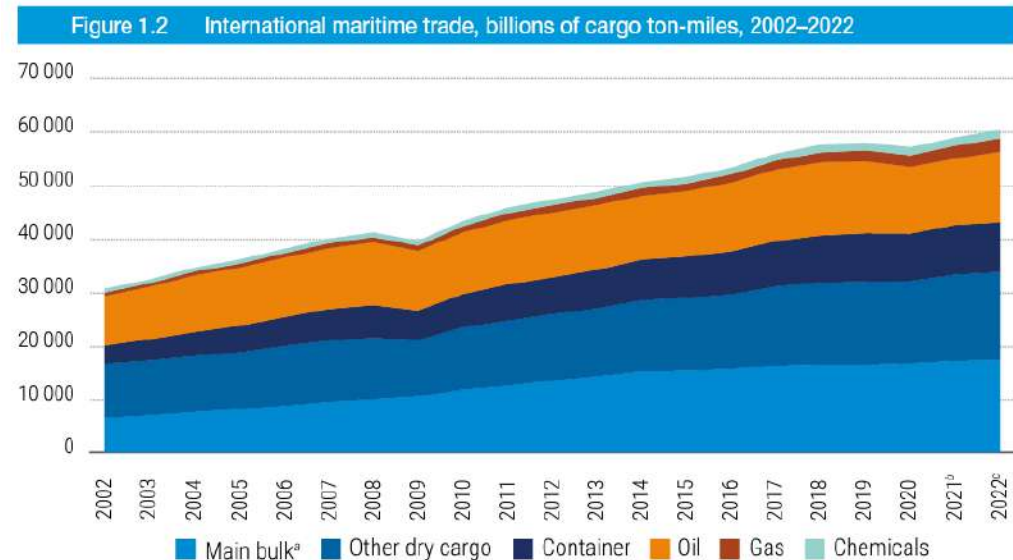


Courtesy of Vice Admiral
(ITCG) Luigi Giardino

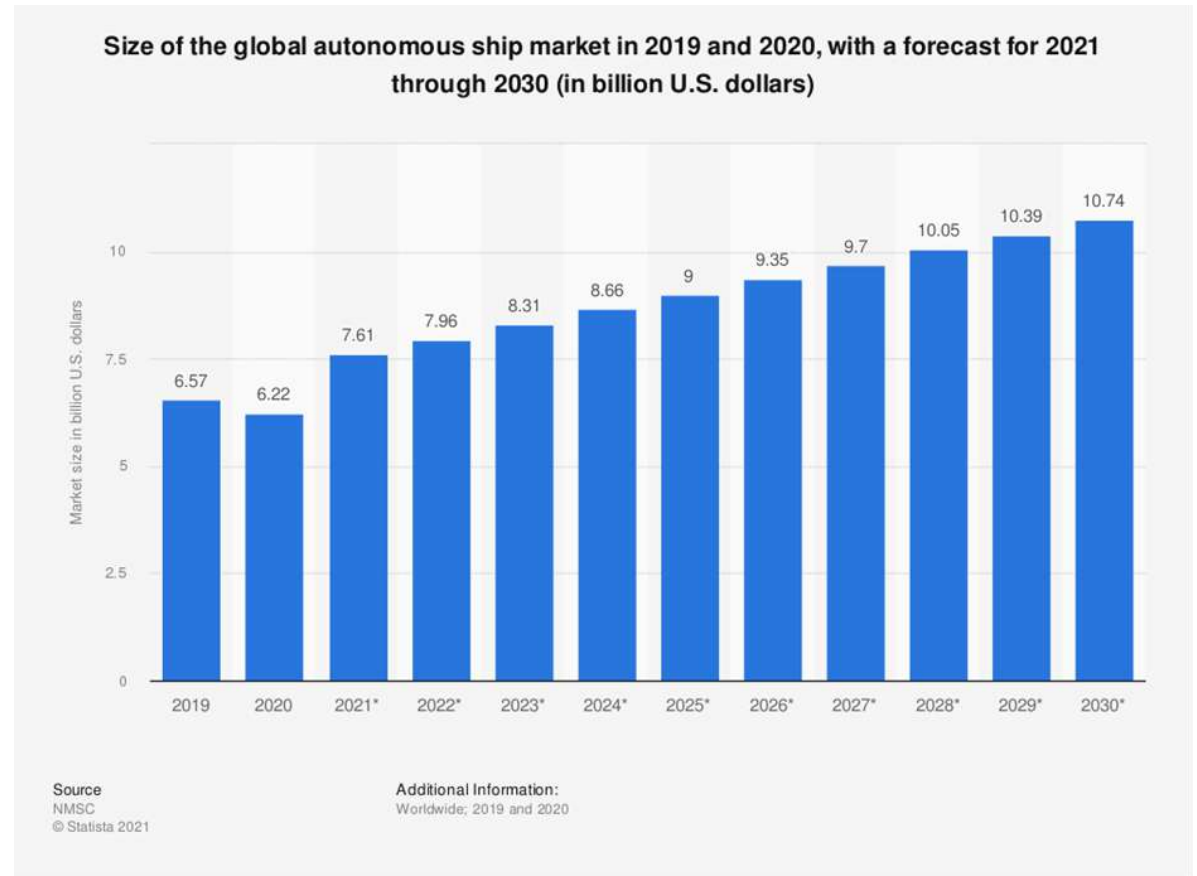




- (A growing) ratio of the business around international shipping will come from MASS



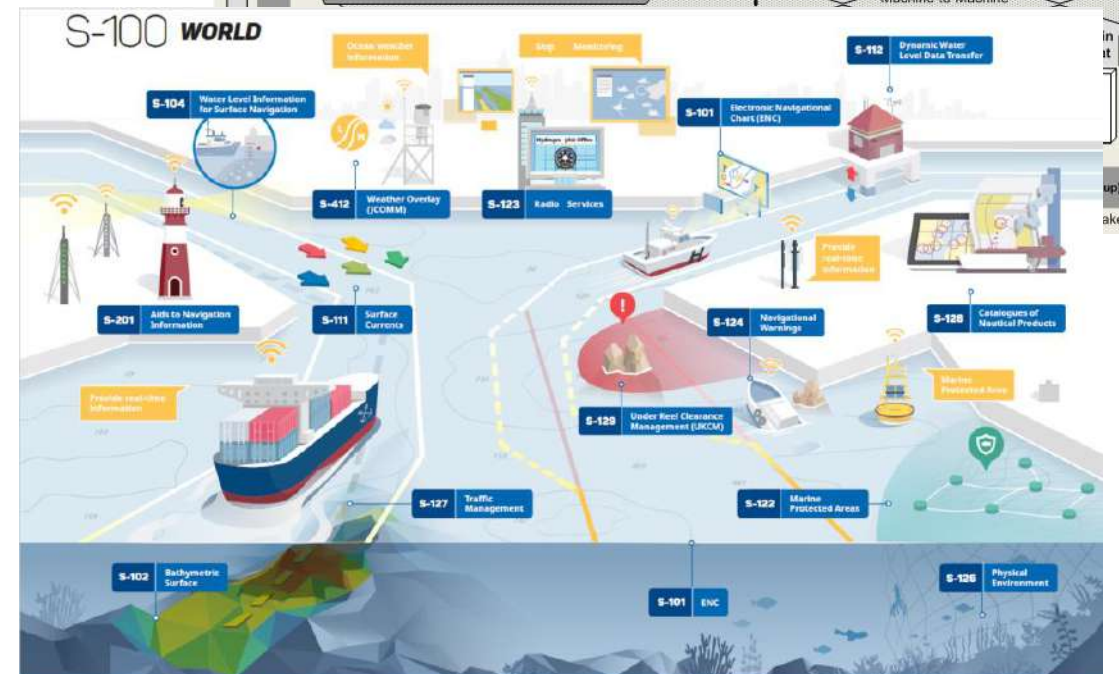
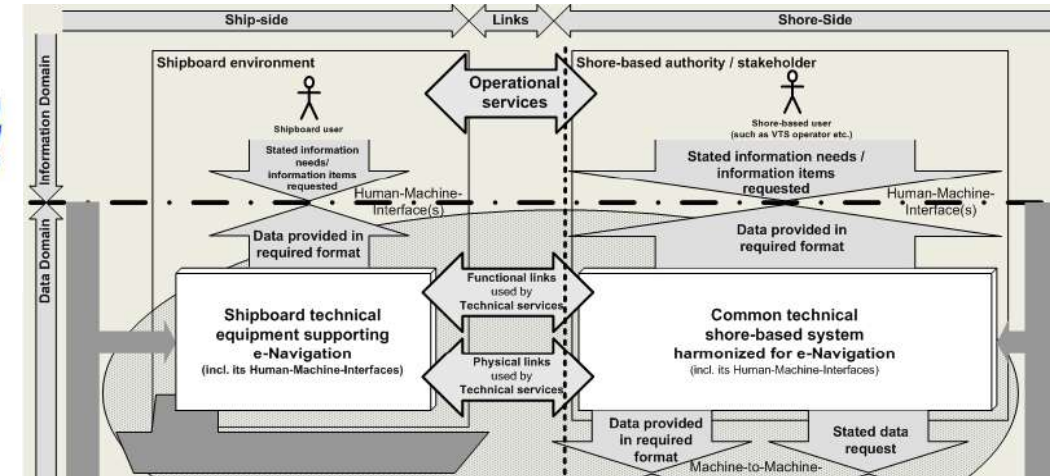
Source: UNCTAD secretariat, based on estimates from Clarksons Research (Clarksons Research, 2022b).



Source: NMSC © Statista 2021

Additional Information: Worldwide; 2019 and 2020

- e-Navigation:
 - future, digital concept for the maritime sector.
- Ship-side linked to shore-side system
 - need to equip shipboard users and those ashore responsible for the safety of shipping with modern, proven tools that are optimized for good decision making;
 - integrate existing and new navigational tools, in particular electronic tools, in an all-embracing system.



- Draft MASS code available:
 - MSC 107/9 June 2023 (rapporteur Marshall Islands);
- With high-level directives for:
 - ROC functionality;
 - ship assets;
 - port physical/digital infrastructure;
- expected to be released (see the IMO MASS Code roadmap):
 - voluntary code by the end of 2024 (adopted 2025);
 - normative code by June 2026 (adopted 2028).

ANNEX 1

**DRAFT INTERNATIONAL CODE OF SAFETY
FOR MARITIME AUTONOMOUS SURFACE SHIPS (MASS CODE)**

PREAMBLE

1 Existing IMO instruments have historically been developed on the basis that the ship will have at least a minimum level of manning on board to carry out the various tasks required to ensure safe, secure, and environmentally sound ship operations.

2 The ever-increasing use of automation in the operation of ships, along with the anticipated increase in the use of remote control and autonomous operation of key functions, will require a different approach, and therefore some adjustment of the accepted norms regarding onboard manual intervention and control as contained within SOLAS and other IMO instruments.

3 In facing these challenges, it is recognized that some aspects associated with MASS may not be adequately or fully addressed in SOLAS or other IMO instruments and that additional guidance may be required on the design and operation of MASS to achieve a level of safety that is at least equivalent to that expected of a conventional ship.

4 This Code addresses the functions needed to obtain safe and reliable operations of MASS insofar as they are not adequately or fully addressed in other applied IMO instruments, such as SOLAS, while ensuring that required safety levels are maintained or enhanced through the implementation of remote control, or autonomous operation, of key functions.

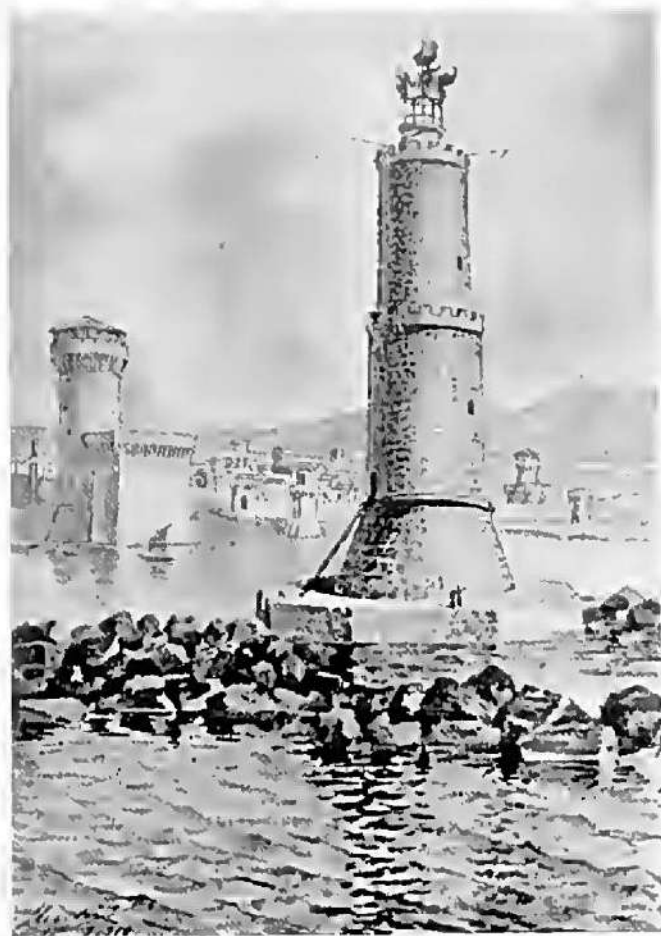
5 This Code is intended as a supplement to other IMO instruments, such as SOLAS, and provides a regulatory framework for the performance of remote control and autonomous operation of key functions, as applicable.

6 The safety principles and objectives of this Code reflect changes in the operational risks (increases or reductions) which may result from the introduction of remote control and autonomous operation of key functions and address their management and reduction through mitigation measures and controls.

7 This Code has been developed based on the *Generic guidelines for developing IMO Goal-based Standards* (MSC.1/Circ.1394/Rev.2) and the *Principles to be considered when drafting IMO instruments* (resolution A.1103(29)).

8 The provisions of this Code should be implemented for individual remotely controlled or autonomous functions even where persons are on board to handle other functions.

9 This Code takes into account that certain operational functions may be controlled from a location, or locations, remote from the MASS and addresses necessary aspects of such remote operations centres.



LIVORNO CON LE PRIME MURA PISANE E IL FANALE
RIPRISTINATO. (DA ANTICA STAMPA).

(an attempt) of Gap Analysis

cnit

- Part 1 – Introduction and definitions
- Part 2 – Main principles
- Part 3 – Goals, functional requirements and provisions
- Part 4 – Subdivision, stability and watertight integrity
- Part 5 – Fire safety
- Part 6 – Life saving appliances and equipment
- Part 7 – Management of Safe operations
- (Part 8)
- Part 9 – Security (SOLAS and ISPS)
- Part 10 – Search & Rescue
- Part 11 – Cargo Handling
- Part 12 – Personnel safety and comfort
- Part 13 – Towing and Mooring
- Part 14 – Marine engineering/machinery installations
- Part 15 – Electrical and Electronic Engineering
- Part 16 – Maintenance and Repair (including ICT appliances)
- Part 17 – Emergency Response

- Part 2 – Main principles:
 - high-level requirements and authorization responsibilities, operation safety assessment, operational responsibility and safe fallback, supervision
- Manning and Autonomy :
 - FA—full autonomy, AC—autonomous control (operator on call), OA—operator assisted, OE—operator exclusive;
 - Operational Design Domain and complementary fallback

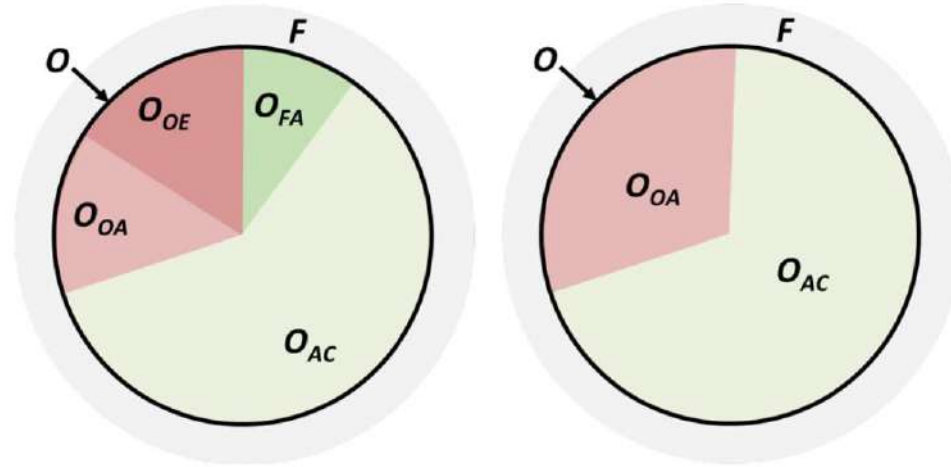


Table 3 Elements of the operational envelope

State space \mathbb{O}		Function mapping FM	
Environment	System	Function	Resp.
Traffic density	Sensors	Navigation	Both
Wind	Engine state	Energy prod.	Automation
Temperature	Ship stability	Cargo handling	Human

O. Rodseth et al., Journal of Marine Science and Technology (2022) 27:67–76

- Part 3 – Goals, functional requirements and provisions:

- Navigation

- preparation for departure,
 - situational awareness,
 - route planning safe grounding, collision avoidance, heading, speed and track control,
 - alert management, data recording, redundancy, HMI
 - override and safe fallback

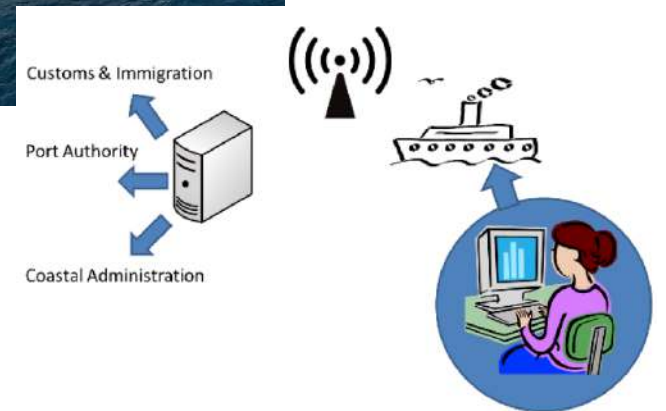
- Remote Operations

- functional requirements of one (or multiple) ROCs,
 - remote operators and interfaces,
 - transfer of control,
 - software specs and data custody

- Communications

- ship-to-ship, ship-to-shore,
 - distress alerts,
 - urgency and safety,
 - Search & Rescue,


- Outcome of the IMO RSE (2021) :
 - on-board equipment (Radar, ECDIS, Autopilot, distributed sensors, etc.) and port-based data sets (berths, meteo, sensors, etc.);
 - an operator (seafarer) at ROC will check and monitor MASS Level 2+ in all phases of navigation, including port ones.
- New ship navigation systems:
 - will allow the ship to approach itself to the port up to the mooring and viceversa;
 - will perform a real-time calculation of sufficient manning;
 - require re-skilling of maritime operators (e.g. seafarers, pilots) as well as supervisors/regulators (e.g. coast guard, police, authorities).



IMO MSC.1/Circ.1610, 2019

- Vessel interacts with Ports offering and consuming digital services:
 - for vessel traffic management (approaching/leaving), berth allocation, pilotage/towing, manouver, requested mooring time, freight announcement;
 - need of standardization for the same services worldwide around the «three invariants»
 - Digital Ship, Digital Port (ROC), Network infrastructure

Tug operation



Tug's operation

- Status
- Duration
- End of completion
- Etc.


Transit



Ship's request

- Size
- ETA
- # of tugs
- Etc.

Stevedores operation




CMA-CGM North Europe French West Indies, 2023

- Logistics efficiency and green operations:
 - minimization of the cycle-ship (reduction of stop at the quay);
 - reduction of consumption, CO2 emissions, staff working time.

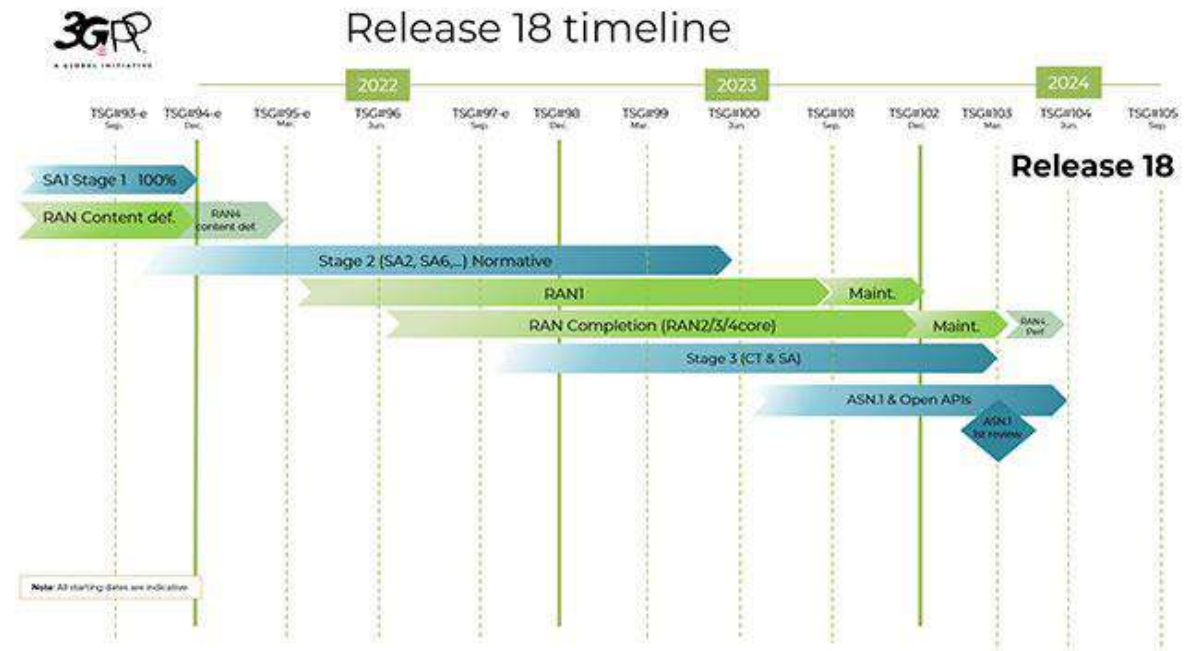
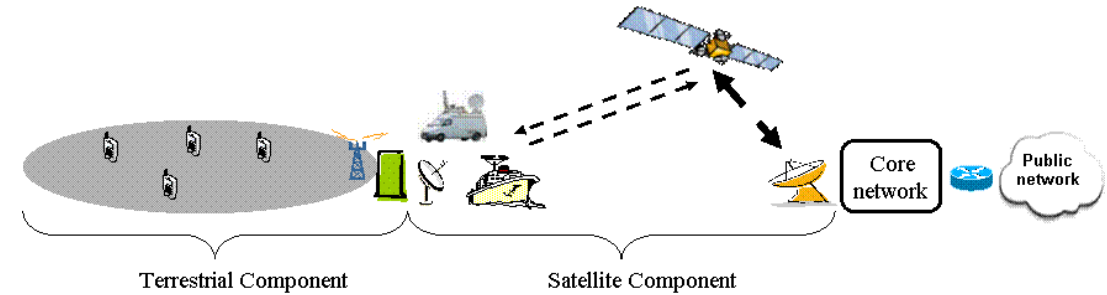


Credits: GloMEEP

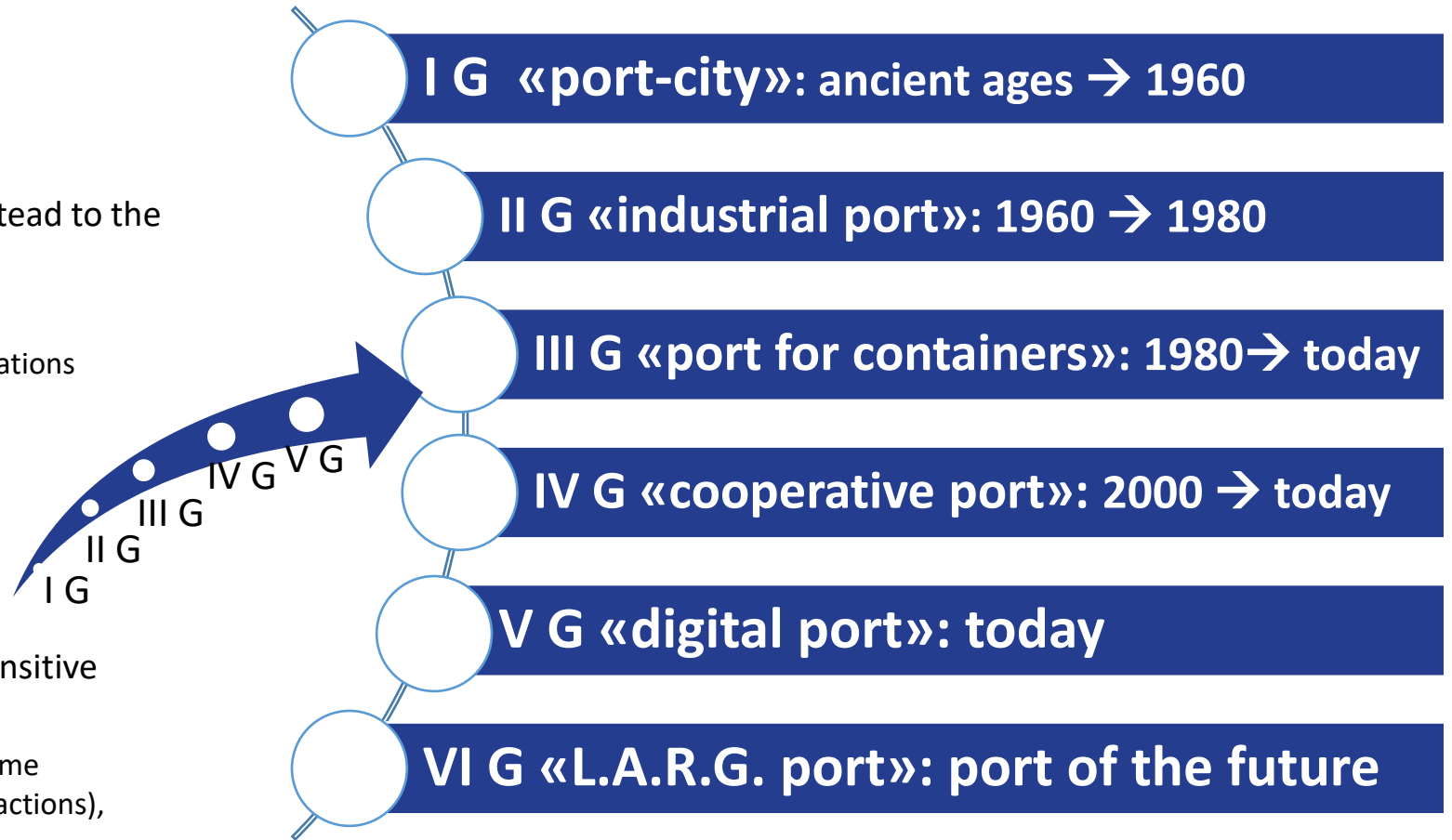


- integration of shipboard and port ICT infrastructures enables:
 - JIT arrival, berth pre-booking, pre-booking of yard resources, customs pre-clearing, early detection of incidents and pollution events.

- Unmanned shipping is aligned with 5G evolution, R18:
 - enhances «Satellite component in the 5G architecture» (started in R17);
 - standardizes 5G system with satellite backhaul;
- includes:
 - UAV (Unmanned Aerial Vehicles), UAM (Urban Air Mobility), and UAS (Unmanned Aerial Systems),
 - USV (Unmanned Surface Vehicles) and MASS? Inputs to RAN studies by H. Koo (3GPP Liaison Person for IALA)

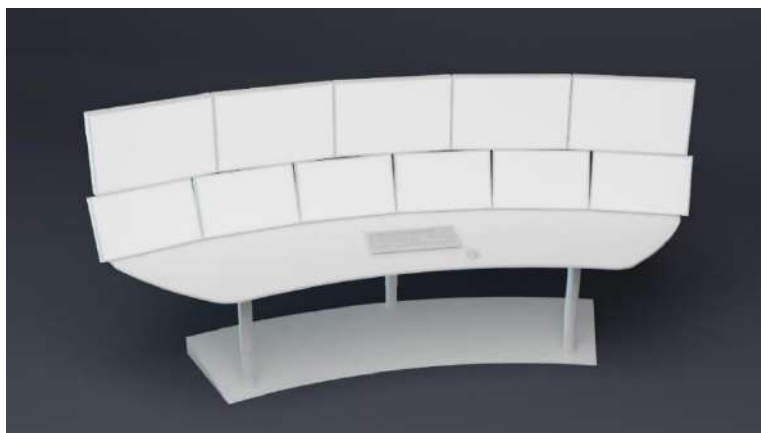


- **LARGEness:**
 - Lean, Agile, Resilient, GrEen.
- **A cyber-secure digital infrastructure:**
 - covering the seaways connecting the oadstead to the berths:
 - standalone separate network (NPN?)
 - network services tailored to target specifications (slices?);
 - Internal and Perimeter security.
- **ROC:**
 - secure communications (see IEC 63173);
 - safe fallback of control.
- **Data Mgmt (maritime processes rely on sensitive data):**
 - Trustworth, Irrevocability, Immutability, Time Reference, Manipulation (History of transactions), Privacy (DLT?)



Credits: prof. Francesco Russo – Easylog final event, May 27th, 2021

- Examples of Day X Maritime Services (w/ PCS and TOS functions):
 - Real time vessel tracking and monitoring in deep sea sailing and in port waters;
 - Develop plan for operating the vessel, update plan according to changes and feedback;
 - Vessel Collision Avoidance (early detection of dangerous situations, best path recalculation);
 - Vessel Arrival Slot Management (JIT arrival, berth pre-booking, pre-booking of yard resources, customs pre-clearing);
 - Calculation and measurement of pollution level (including COx and noise);
 - (Containerized and General) cargo pervasive monitoring and control in port areas and along the logistics chain.



- How does it look like?
 - Placed ashore, accessible, integrated with port infrastructure and with the ships.
- High-Level-Tasks of ROC personnel:
 - Monitoring, Direct Control, Communication , Planning/Organisation, Documentation

Belgian delegation to IMO, MSC 107/INF.14 (March 2013)



C-Ports: A proposal for a comprehensive standardization and implementation plan of digital services offered by the "Port of the Future"

Paolo Pagano*, Silvia Antonelli, Alexandr Tardo

Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNT), Parma 43124, Italy

ARTICLE INFO

Article history:
Received 21 March 2021
Received in revised form 16 September 2021
Accepted 5 October 2021
Available online xxx

Keywords:
5G mobile communication
Real-time systems
Virtual reality
Artificial intelligence
Containerized vessels
• Freight
Logistics
Industry 4.0
IoT-based monitoring
Port community systems
Terminal operating systems
Smart port index

ABSTRACT

In this paper we address the topic of a possible path to standardize the ICT services expected to be delivered by the so-called "Port of the Future". How the most relevant technologies and information systems are used by the Port Communities for their businesses is discussed together with a detailed analysis of the on-going actions carried out by Standard Setting Organizations. Considering the examples given by the C-ITS Platform and the C-Roads programs at EU level, a proposal of contents to be considered in a comprehensive standardization action is given. The innovation services are therefore grouped into four bundles: (i) Vessel & Marine Navigation, (ii) e-Freight & Intermodal Logistics, (iii) Passenger Transport, (iv) Environmental sustainability. The standardized version of these applications will be finally labeled as C-Port services. Alongside the standardization plan, a proposal for ranking the ports on the basis of a specially-defined C-Port vector is discussed with the purpose of addressing the well-known lack of consensus around the mathematical definition of the Smart Port Index. Considering the good practice and the background offered by the Port of Livorno in terms of innovation actions, the prospective final user applications are then labeled as Day 1, Day 1.5, and Day 2 services in consideration of the technical and commercial gaps to be filled. As a case study about the evolution in the C-Port vector experienced by the Port of Livorno in the last years will also be discussed.

© 2021 Elsevier B.V. All rights reserved.

1. INTRODUCTION

Seaports are genuine intermodal hubs connecting seaways to inland transport lines such as roads and railways. Seaports are located at the focal point of institutional, industrial, and control activities, in a jungle of interconnected information systems.

As seaports operate in freight and passenger businesses, the main vertical applications are in the domain of logistics and digital offer targeted to citizens and tourists. Ports also represent important industrial innovation hubs where local business, together with institutional and public bodies can interact and generate added value services. The valorization, and consequently the transfer, of scientific and technological results from research centers, hold a crucial and increasingly relevant role in terms of economic development. Indeed, it is considered the driver for the transition from a "manufacturing-based economy" to a "knowledge-based economy".

Traditionally, logistics has been considered as a "non-core process", an activity that does not contribute to the value creation process. In fact it was considered a process based on downward competition and where investments had a tendency to be "limited", if compared to those resources allocated for those main "core" processes.

The concept of "Lean", typical approach of the so-called Industry 4.0, based on the streamlining, digitalization, automation and efficiency of the logistics chain upstream and downstream processes can also be applied to other sectors, firstly, to distribution and maritime logistics. Logistics and maritime processes have been re-designed with a view of creating value and eliminating all those wastes imputable to inefficiencies and lack of organization. In this way, ports are becoming increasingly automated and optimized, thanks to the contamination between ICT and robotics as well as to the integration with other attractors located towards the hinterland and overseas.

Although Research and Innovation Actions funded by European Programmes (supporting the development of frontier technologies ranging from 5G to autonomous vessels) do include standardization

* Corresponding author.
E-mail address: paolo.pagano@cnit.it (P. Pagano).

<https://doi.org/10.1016/j.comind.2021.103556>
0166-3615/© 2021 Elsevier B.V. All rights reserved.

see here a possible classification
(<https://arxiv.org/abs/2104.13175>)



Livorno, background and
the 5G MASS project at a
glance

cnit

see the MASS workshop held on March 30th in Livorno (in ITA)
<https://www.youtube.com/watch?v=5r86SuqOwxI>

- Mid-size historical port:
 - passengers and freight;
 - multipurpose (containers, break/dry/liquid bulk);
 - freight village, car stocking (25,000 cars capacity);
 - along TEN-T SCANMED corridor (core node);
 - door of Tuscany;
 - minor ports (Piombino, Elba) under the same organization.



5G Trailblazers

5G Innovation Su

Paolo Pagano

Blazing the way in port communications system capabilities.

5G Trailblazer | Pioneer



5G Testbed 2017/21



A final example can be found in the potential of the world's 835 currently active ports [8]. One case study examining the private 5G network trial for the automation of China's Port of Qingdao indicated that a 70-percent labor cost savings could be achieved if 5G automation were to be fully implemented [9]. Our own research engagements in Italy's **Port of Livorno** suggest much the same, with the potential for significant savings in port and quay operations as well as reduced berthing times for vessels and shortened cargo release times.

Ericsson White Paper
GFTL ER 20:003151
June 2020



5G MASS: 2022 - 2024



March '22



February '24



Under the supervision of the ITCG



© CNIT - not for public use

- Submitted to ESA Smart and Uncrewed Shipping Call for Proposals:
 - Supported by ASI;
 - led by TIM as prime contractor;
 - Framed a posteriori into ESA/ITCG SMTF.
- Objectives:
 - integration of on-board, land-based and nomadic equipment with technological solutions already available from the ICT world;
 - standardization and replicability;
 - field trials and risk assessment;
 - end user requirements and valorization of skills already acquired.

HOME

BUSINESS INCUBATION

NEWS

HOW TO APPLY

AMBASSADORS

PORTFOLIO

ESA INVESTOR FORUM
CONTACT

Search



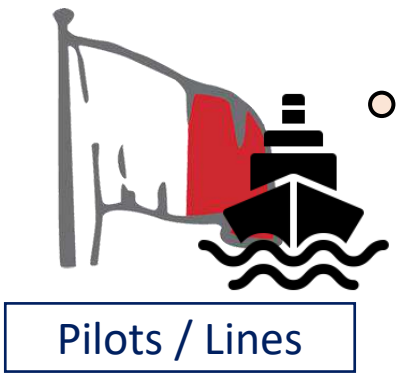
Smart and Uncrewed Shipping



We can exploit a 24/7 port with full digital support to logistics services

I can check the current positioning of the vessel; maneuvering is easier with the port open data and digital systems

I can communicate with the port (remote control center) while approaching

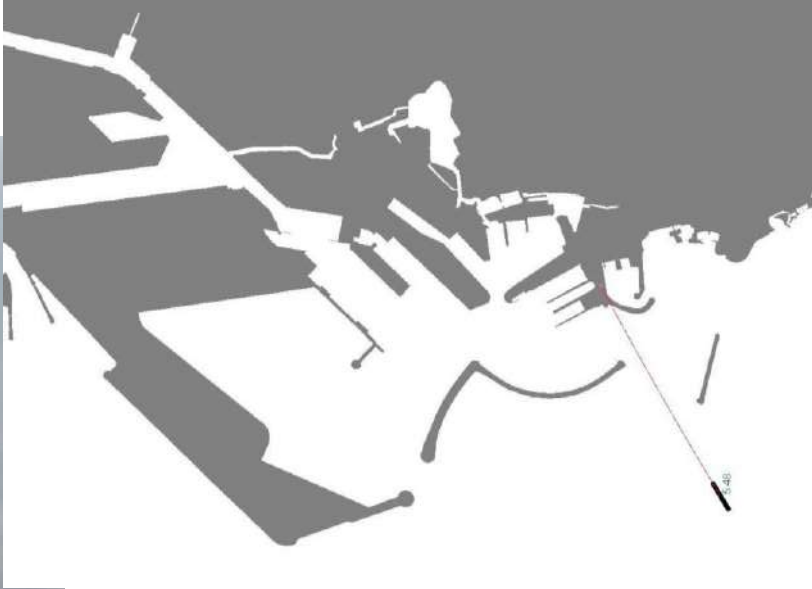
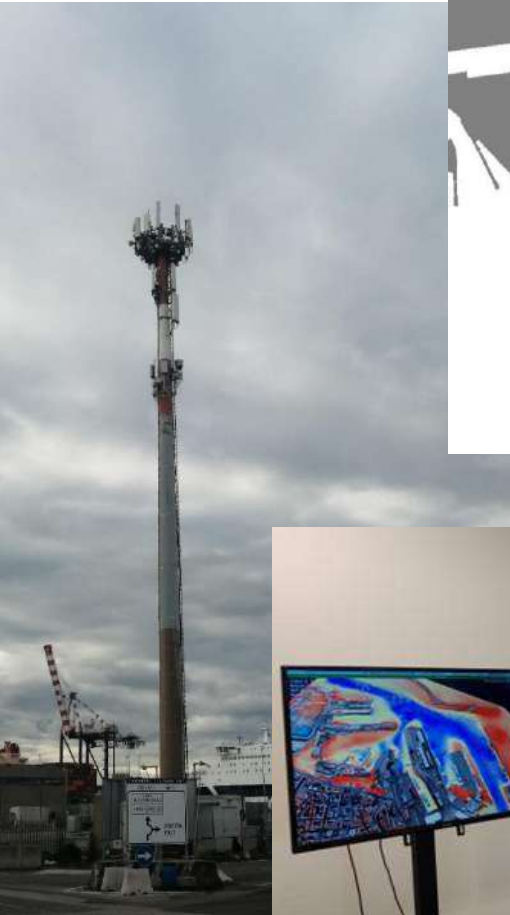


We can early assess the feasibility of MASS in ports

I can access a complete dataset containing real-time meteo-marine observations

We can manage Naval Traffic in a safer and more efficient manner (even in difficult meteo-marine conditions)





- Integration of:
 - shipboard, shore, and nomadic equipment for effective situation awareness
- Network:
 - new 5G mmWave NPN w/ localization and bi-directional broadband communication
- Nomadic equipment:
 - ECDIS interfaces
 - Augmented Reality support
- Track control:
 - Fully-aware update of best path and calculation of deviation
- Remote Operational Center:
 - Monitor and (enabled) remote control
 - Risk Assessment on EU/EMSA tools



Conclusions

cnit

- Unmanned shipping:
 - is a comprehensive full-digital domain subject to complex international regulations, needing to be supported by international standards;
 - is going to be legally viable from 2025;
 - port readiness:
 - challenges on network architecture and performance, port layout and ROC functionalities, final-user service definitions and specifications.
- Italy is on the forefront of the innovation, starting from 5G and ROC deployment in Livorno:
 - results from Italy will have an impact at international level providing a preliminary assessment of the feasibility of unmanned shipping in historical ports.



Courtesy of:



CORPO PILOTI DEL PORTO DI LIVORNO

PTS Spectrum Seminar

Swedish Post and Telecom Authority

BB4All, 27 June 2023

Jonas Wessel

Director PTS

Rapporteur DD, RSPG

Anna Beckius

Head of Unit PTS

Spectrum Analysis

The logo for the Radio Spectrum Policy Group (RSPG) features the acronym 'RSPG' in a bold, orange, sans-serif font. The letters are contained within a white, rounded rectangular shape that has a slight 3D effect, appearing to float above a dark blue horizontal band. The background of the slide is a gradient of red and orange at the top, transitioning to white below.

RSPG

RADIO
SPECTRUM
POLICY GROUP

What is the RSPG?

- The RSPG is a high-level advisory group that assists the European Commission in the development of radio spectrum policy
- Brings together all Europe's national spectrum managers
- The RSPG was established by the European Commission 2002, and it adopts opinions, position papers and reports, as well as issuing statements, which are aimed at assisting and advising the Commission at strategic level on:
 - radio spectrum policy issues,
 - coordination of policy approaches and,
 - harmonised conditions, where appropriate, with regard to the availability and efficient use of radio spectrum necessary for the establishment and functioning of the internal market.
- It has been Europe's expert on spectrum policy for 20 years.

The logo for the Radio Spectrum Policy Group (RSPG) features the acronym 'RSPG' in a bold, orange, sans-serif font. The letters are contained within a white, rounded rectangular shape that has a slight 3D effect, appearing to float above a dark blue, textured horizontal band. The background of the slide is a vibrant, abstract composition of red and orange flames or light streaks at the top, transitioning into a dark blue band with a white, wavy, textured pattern below it.

RSPG

RADIO
SPECTRUM
POLICY GROUP

RSPG deliverables since June 22

- Adopted deliverables
 - Dec 22: Opinion on the ITU WRC-23
 - May 23: Opinion on the future of the EC sector and its infrastructure
 - Feb 23: Report on mobile technology evolution
 - Feb 23: Annual Report on Peer Review
- Public Consultation launched in June 2023
 - Opinion on “the strategy on the future use of the frequency band 470-694 MHz beyond 2030”
 - Opinion on “the development of 6G and possible implications for spectrum needs and guidance on the rollout of future wireless broadband networks”.

RSPG WRC 23 Opinion

- Consistent with the work of MS within CEPT
- Recommended EU positions on WRC-23 AIs which may affect common rules or where desirable
- Major compromises on most contentious items
- AI 1.2 IMT in 6 GHz: **“accepting IMT identification while not advocating...”** since EU will consider later the best usage between IMT, WAS/RLAN or a shared framework
- AI 1.5 470-694 MHz: recommending as a compromise between other options a **secondary mobile allocation + possible upgrade at WRC-31**
- **EU Council Decision** under development
- EU position have to be **“implemented”** in a **proposal to WRC-23 (eg ECP)**.

RSPG opinion on the future of the EC sector and its infrastructure

- Fast track opinion triggered by EC consultation, particularly questions on spectrum management
- Several fundamental issues, in a context of EU digital sovereignty, addressed in the Opinion
- Pan-EU selection/authorization: specific case of satellite and verticals
- Role of CEPT: harmonization process, WRC preparation
- Cross-border coordination with third countries: role of good offices.

The logo for the Radio Spectrum Policy Group (RSPG) features the acronym 'RSPG' in a bold, orange, sans-serif font. The letters are contained within a white, rounded rectangular shape that has a slight 3D effect, appearing to float above a dark blue horizontal band. The background of the slide is a gradient of red and orange at the top, transitioning to a dark blue band, and then to a white background with a subtle grid pattern.

RSPG

RADIO
SPECTRUM
POLICY GROUP

RSPG Report on Mobile technology evolution

- Practices, sharing experiences
 - Phasing out of legacy technology
 - Migrating obligations to latest technologies
- Existing deviations from technology neutrality principles
 - GSM directive, e-Call
- Phasing out of 2G and 3G legacy systems in next decade
- Report in **February 2023.**

Strategy on the future use of the 470-694 MHz band beyond 2030 in the EU - Consultation

- Assessing the existing flexibility in Article 4 of Decision (EU) 2017/899
 - In order to implement at a national level:
 - 5G Broadcast, mobile SDL?
 - 600 MHz band Plan?
 - Cross-border coordination challenges
- Technically feasible national scenarios for post 2030
 - Scenarios depend on national situation

6G RSPG Opinion - Consultation

- Lessons from 5G
- Role of **unlicensed** spectrum for offloading and **NTN** for coverage of undeserved areas
- Need for **early recognition of 6G spectrum needs**
- Which **coverage and capacity needs**?
- Which use cases and usage scenarios?
- Need for a strategy for timely launch of 6G services by 2030.

So, what is happening in Sweden?

Apart from...

...BB4All...

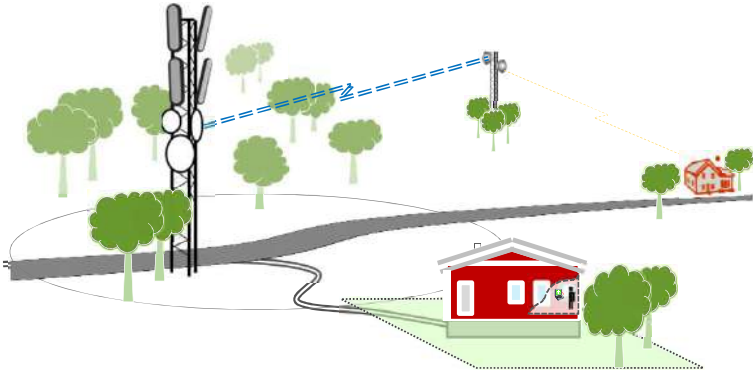
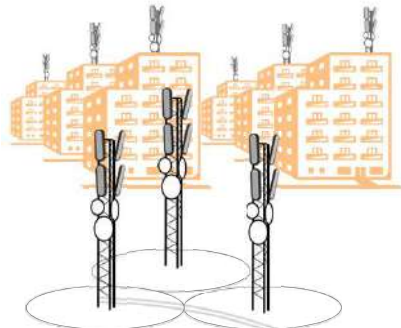
...well deserved summer holidays...

... midsummer...

... and midnight sun?



The Swedish market

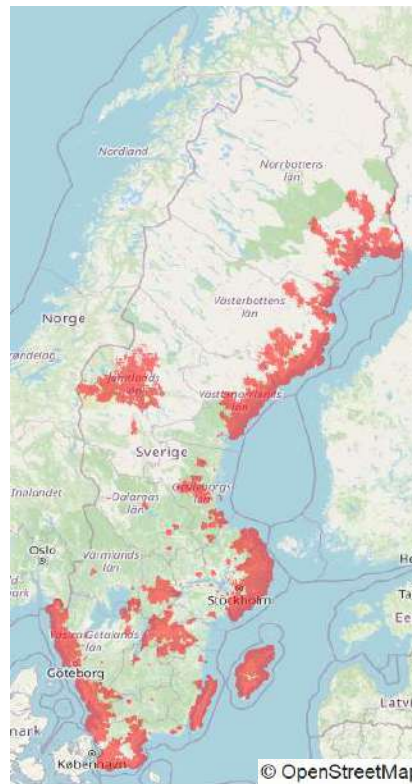


4G/5G deployment in Sweden

October 2021



October 2022



4G October 2022



PTS Swedish Spectrum strategy

Objectives

- Maximize the long-term societal benefit of radio spectrum
- Sufficient radio spectrum for the needs of society, today and in the future.

Measures

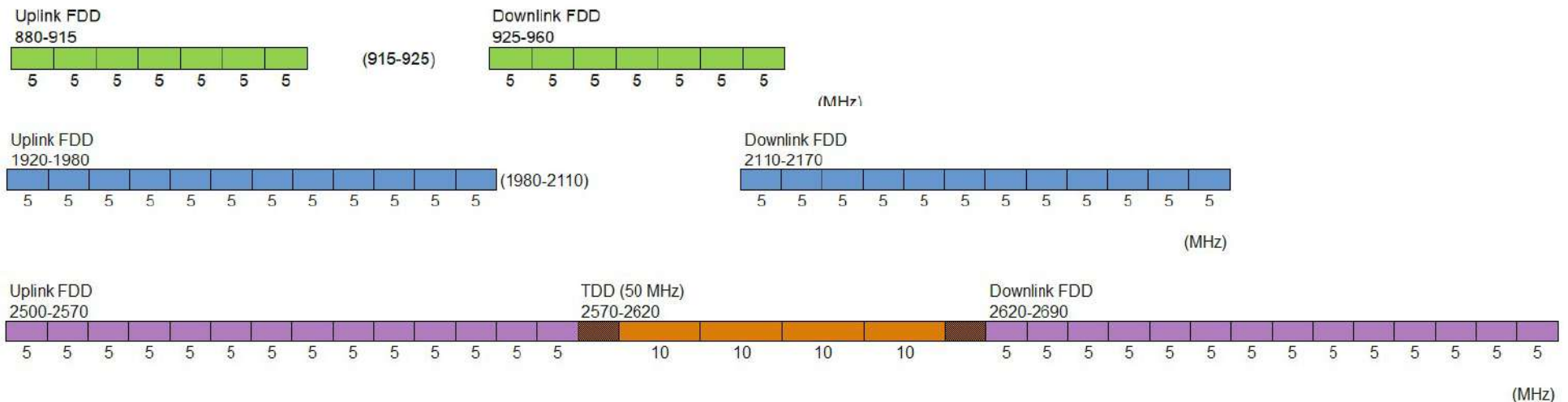
- Create the conditions for a diversity of spectrum uses
- As few restrictive conditions as possible (only those required to facilitate efficient spectrum use)
- Clear and long-term spectrum management that is transparent and predictable

Recent and upcoming awards

- 700 MHz (2x20 MHz) awarded in 2018
- 3.6 and 2.3 GHz - January 2021
- 900 MHz, 2.1 and 2.6 GHz – September 2023
- 1800 MHz planned for 2025

The upcoming 900 MHz, 2.1 GHz and 2.6 GHz award

- 900 MHz (2×35 MHz), 2.1 GHz and 2.6 GHz (300 MHz)
– national licenses
- FDD: 2×5 MHz-blocks TDD: 1×10 MHz-blocks

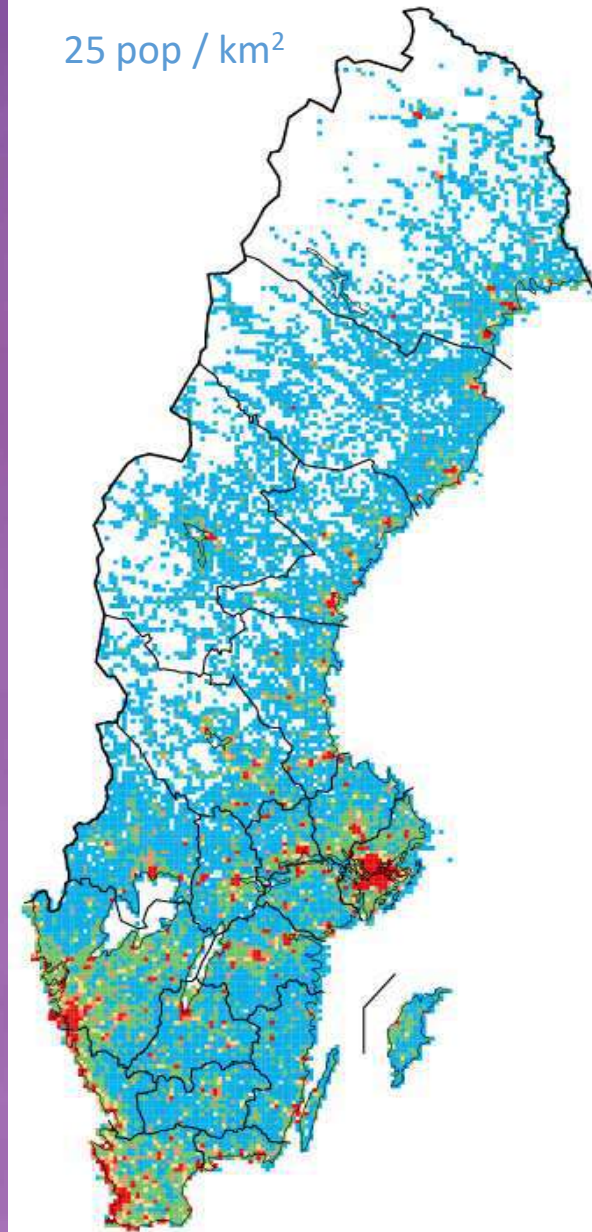


Local licenses

- Background and purpose

- Lower entry barriers to harmonised spectrum
- A demand in the market for "non-national" licenses, sharing, verticals etc.
- Increase competition by enabling opportunities to establish "own" private networks
- Promote innovation by creating opportunities for new business models that can propel digitalisation.

25 pop / km²



Local licenses opened up by November 2021

- Limited geography licenses (property based)
- 3760–3800 MHz and 24.25–25.1 GHz (indoors initially)
- Open for all (no bias for any specific type of user)
- TDD, max 38 dBm / 23 dBm/200 MHz TRP per cell, edge limit
- 5+5 years



- Chunks of 10 / 50 MHz
- Geographical restrictions in some cases
- Use it or lose it!
- And a bunch more fine print...

A sunset landscape with a bright sun in the sky and mountains in the foreground. The sun is a large, glowing yellow circle in the upper center of the frame. The sky is a gradient of orange and yellow. Below the sun, there are dark, silhouetted mountains. In the foreground, there is a body of water reflecting the sun's light.

Thank you for your attention!