ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 1

Internet of Things (IoT)

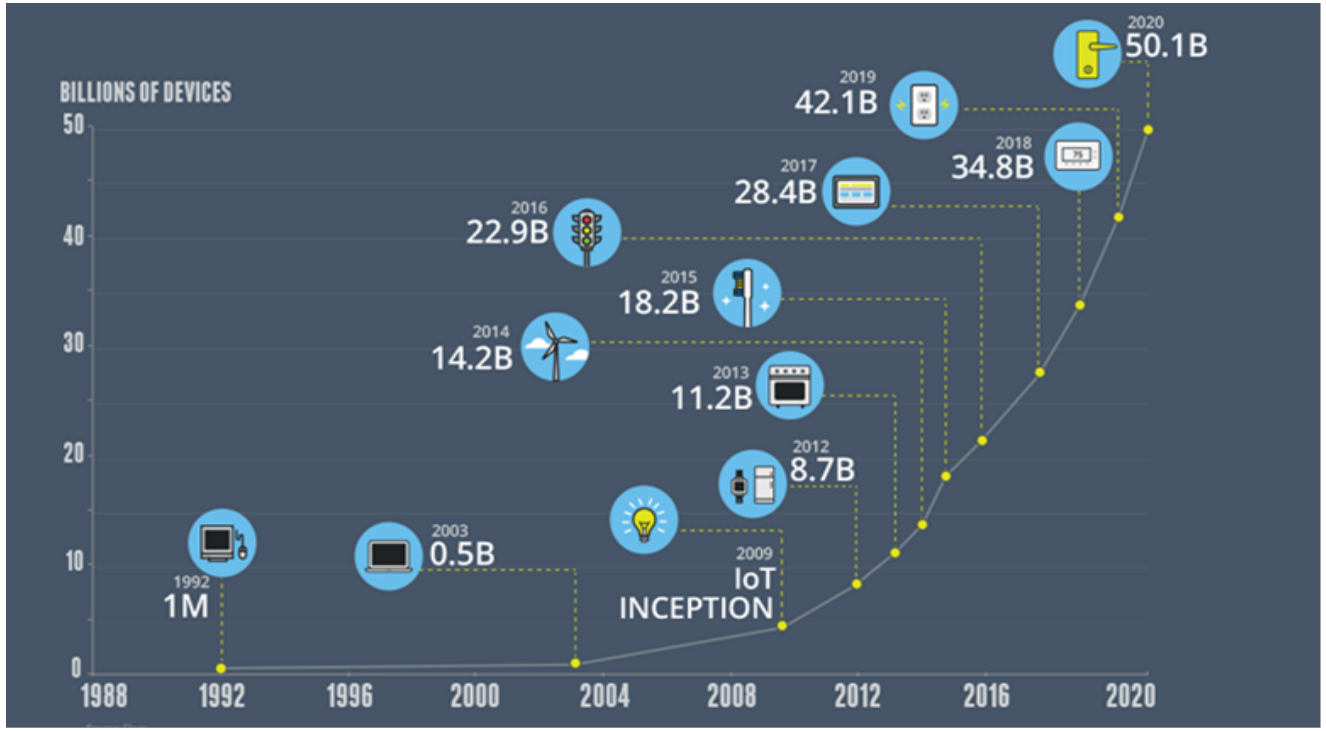
for Smart Sustainable Cities (SSC):

Challenges and Opportunities

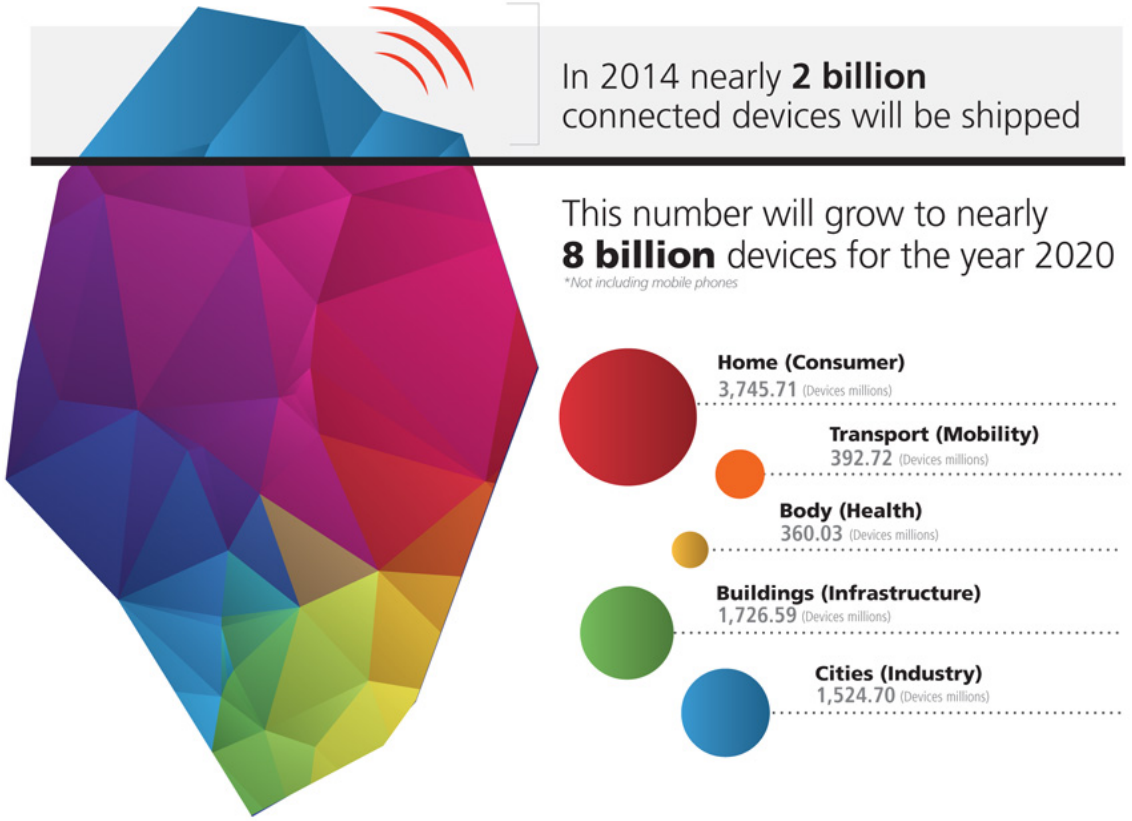
Dr. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

Massive IoT vs. Critical IoT

IoT Growth

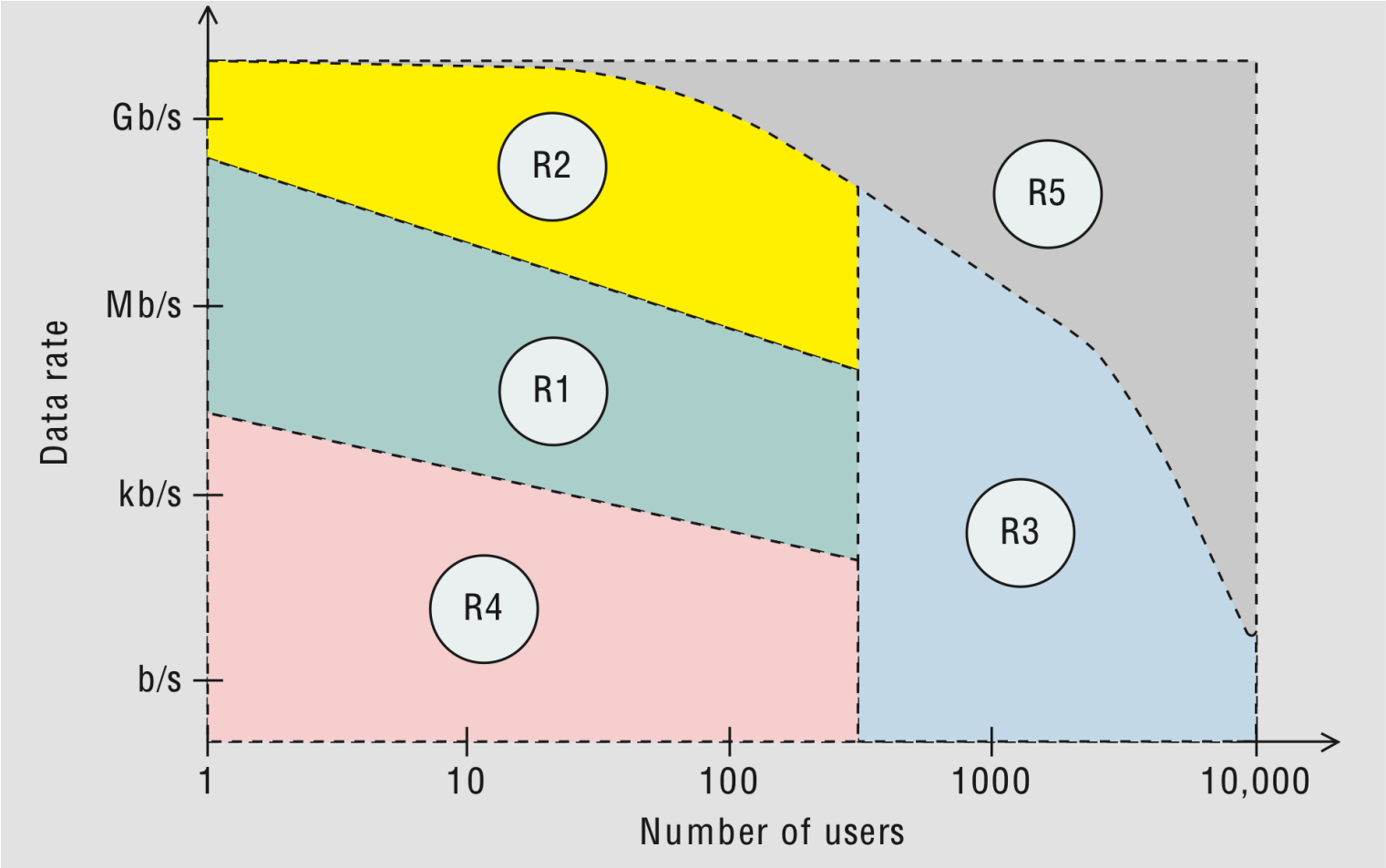


Source: Cisco.

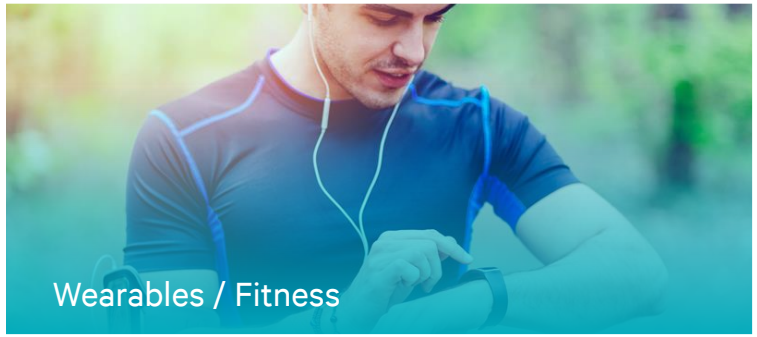


Source: Harbor Research, 2017

IoT Device Regions



Wide Area IoT



Power efficient

Multi-year battery life

Lower complexity

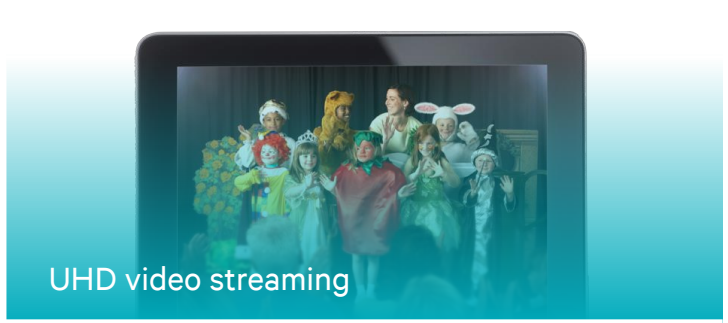
Lower device and network cost

Longer range

Deeper coverage

Source: Qualcomm, Jun. 2016

eMBB



Higher throughput

multi-gigabits per second

Lower latency

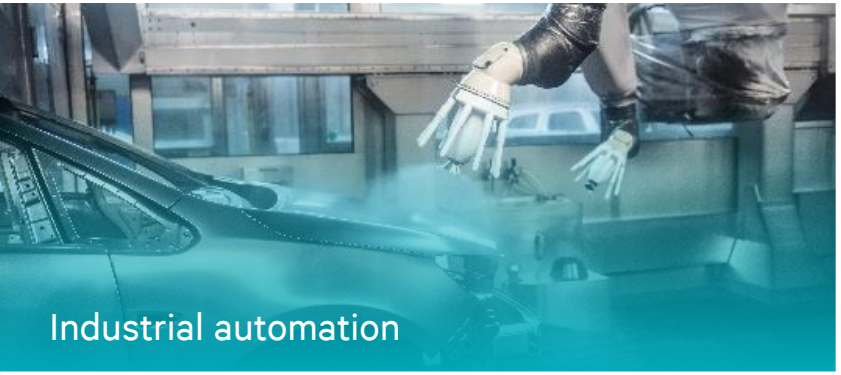
Significantly reduced e2e latency

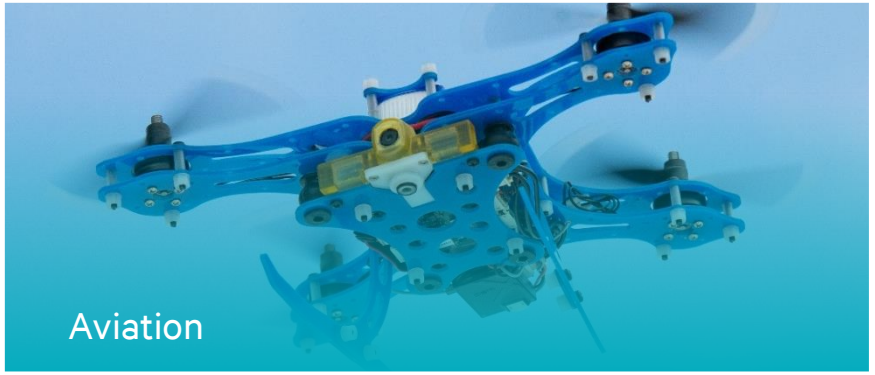
Uniform experience

with much more capacity

Source: Qualcomm, Jun. 2016

High Reliability Control





Higher reliability

Significantly reduced packet loss rate

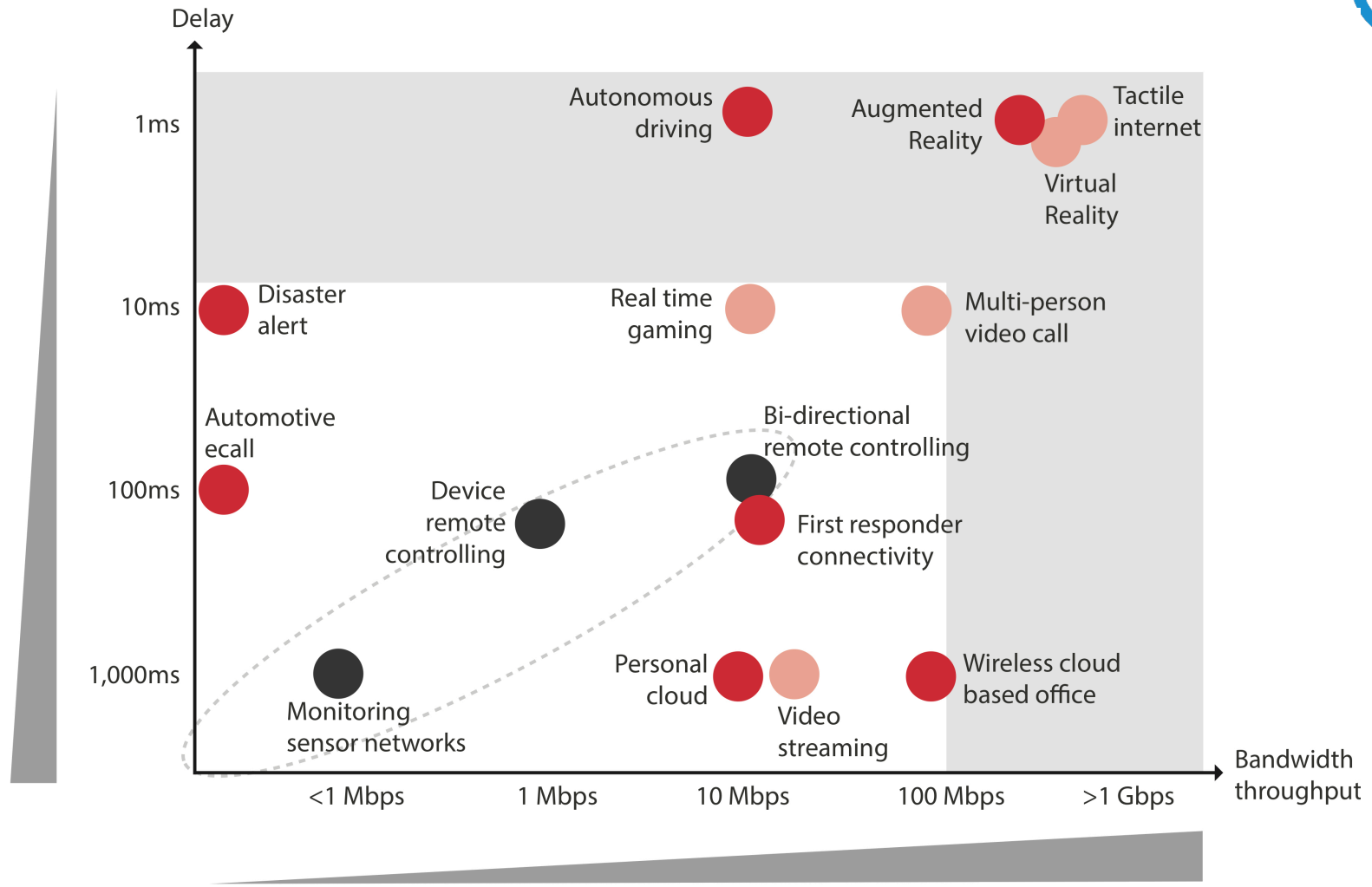
Lower latency

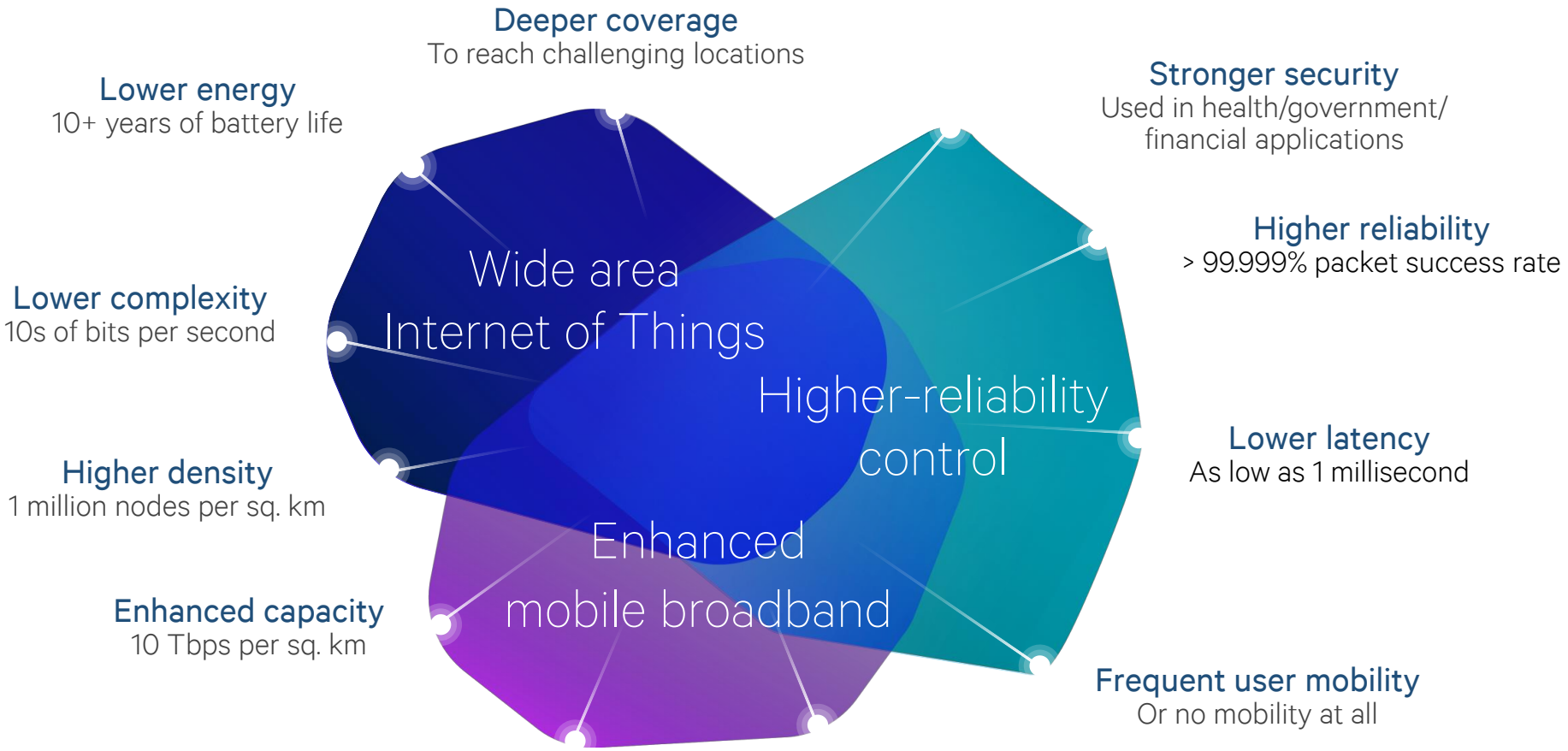
Significantly reduced e2e latency

Higher availability

Multiple links for failure tolerance and mobility

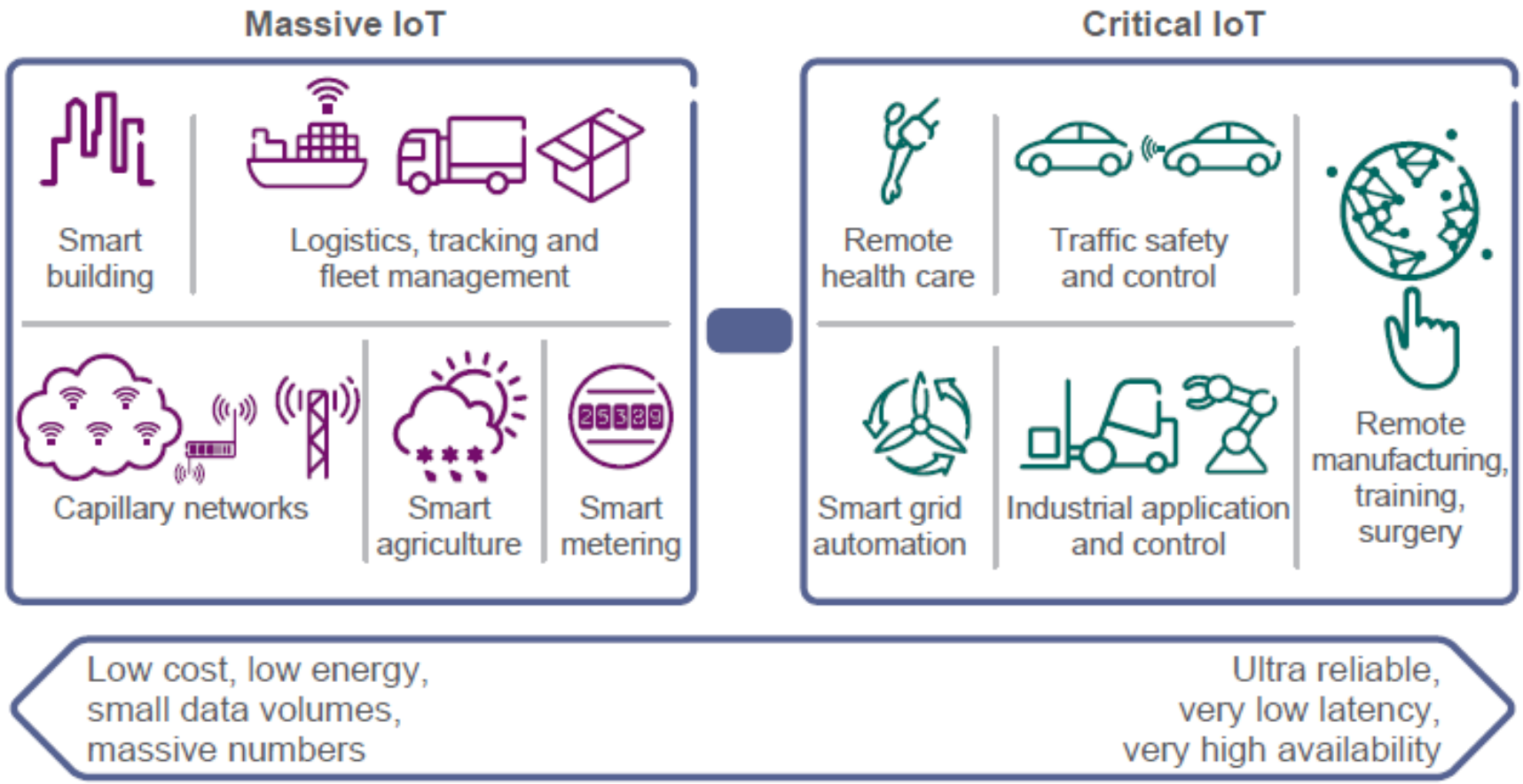
Source: Qualcomm, Jun. 2016


Delay
1ms
10ms
100ms
1,000ms
Autonomous driving
Augmented Reality
Tactile internet
Virtual Reality
Disaster alert
Real time gaming
Multi-person video call
Automotive ecall
Bi-directional remote controlling
Device remote controlling
First responder connectivity
Monitoring sensor networks
Personal cloud
Video streaming
Wireless cloud based office
<1 Mbps
1 Mbps
10 Mbps
100 Mbps
>1 Gbps
Bandwidth throughput
Services that can be delivered by legacy networks
Services that could be enabled by 5G
Fixed
Nomadic
On the go
M2M connectivity



Source: Qualcomm, Jun. 2016

Different contexts - Different requirements



Source: Ericsson, Jan. 2016

Different Considerations

Technical

Coverage determines where the device can be deployed and connected

Energy efficiency affects battery life and maintenance cycle

Latency determines whether time sensitive services can be provided

Throughput limits the amount of data transmitted at any given time

Commercial

QoS ensures the value the IoT service can deliver

Security protects privacy and integrity of IoT users

Cost decides the business viability of implementing and operating the IoT service

Scalability determines the flexibility for managing growth

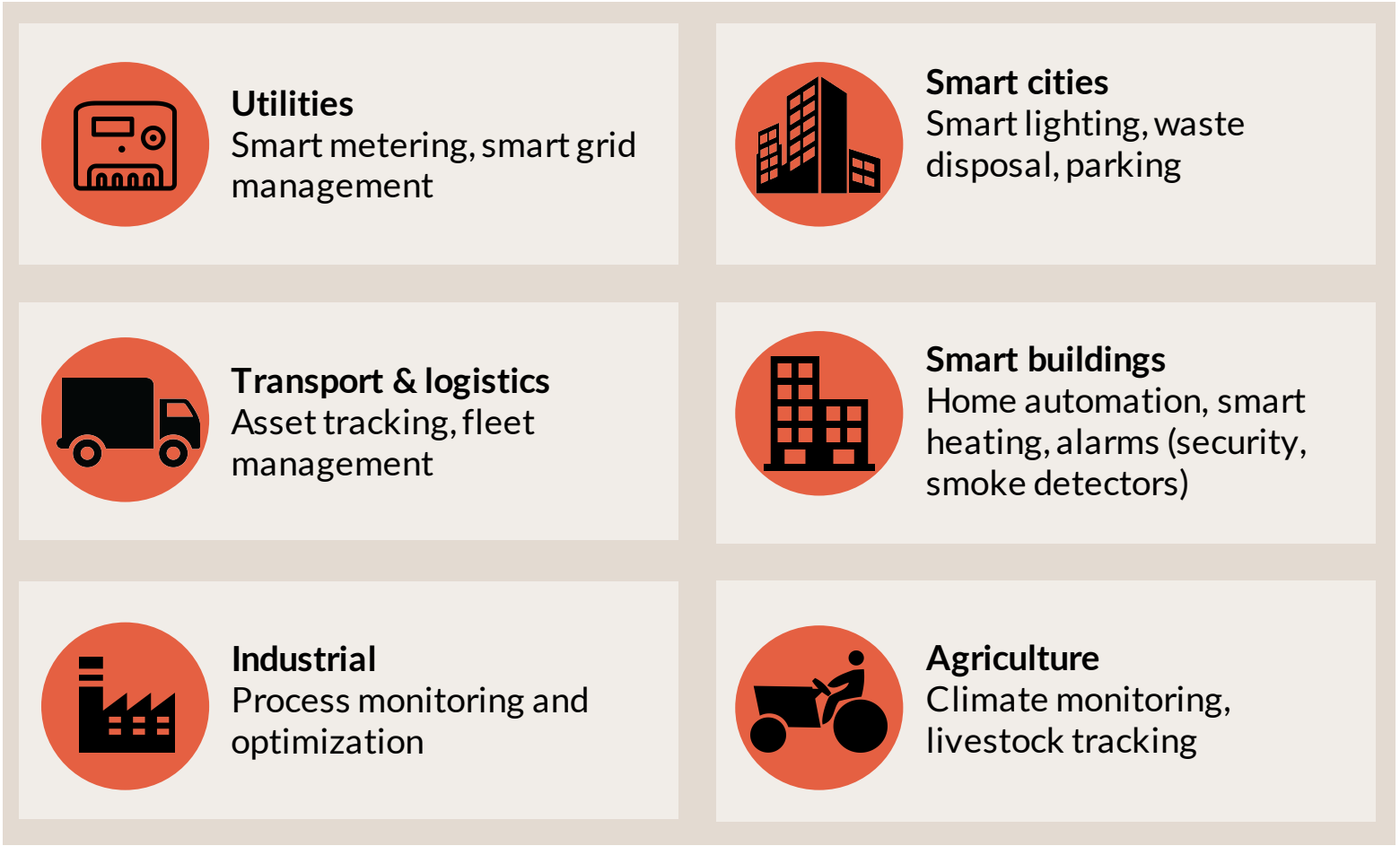
Ecosystem

Future proofness ensures the strategic investment in IoT is economically and technologically sustainable in the long run

Global reach and interoperability brings simplicity and efficiency to international IoT deployments

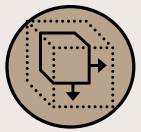
Source: Northstream, 2017

Massive IoT Applications



Source: Northstream, 2017

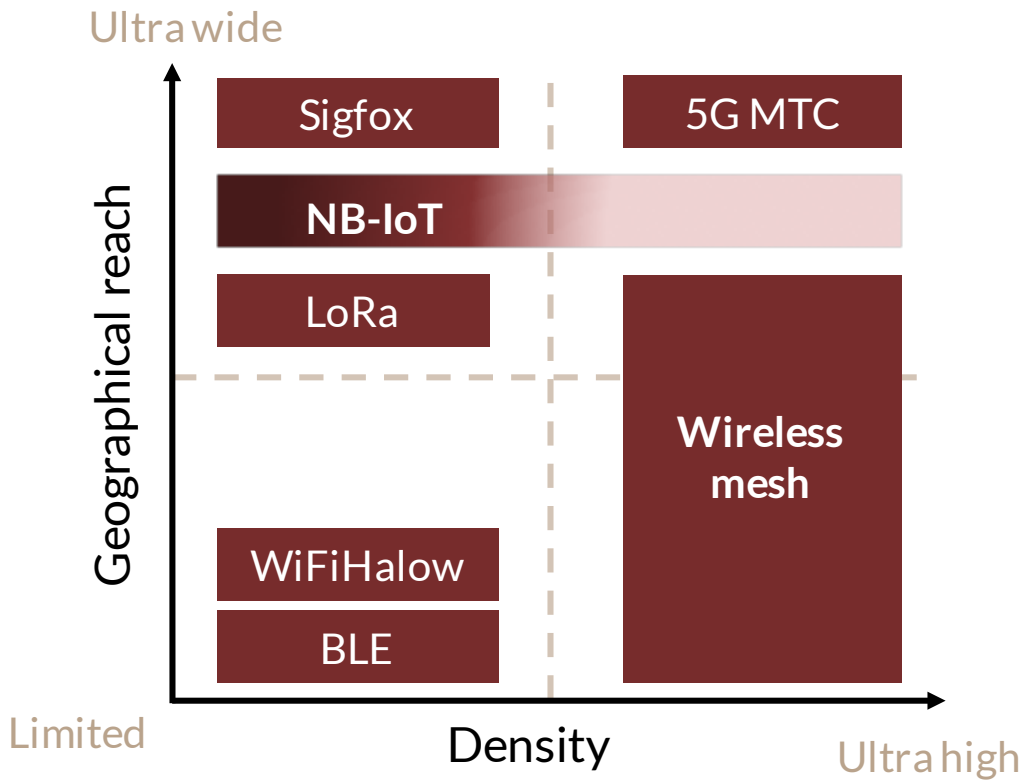
Key Requirements for Massive IoT

	**Long battery life:** devices are often battery powered, and expensive to replace after deployment
	**Strong coverage:** networks must penetrate deep indoors and underground for many use cases, such as mining
	**Low cost:** affordable device and low operational cost necessary to create a business case with high volumes
	**Scale & density:** networks must easily scale to handle a huge number of devices as use cases grow
	**Performance flexibility:** networks must be able to handle multiple applications with differing performance requirements, e.g. for latency and throughput

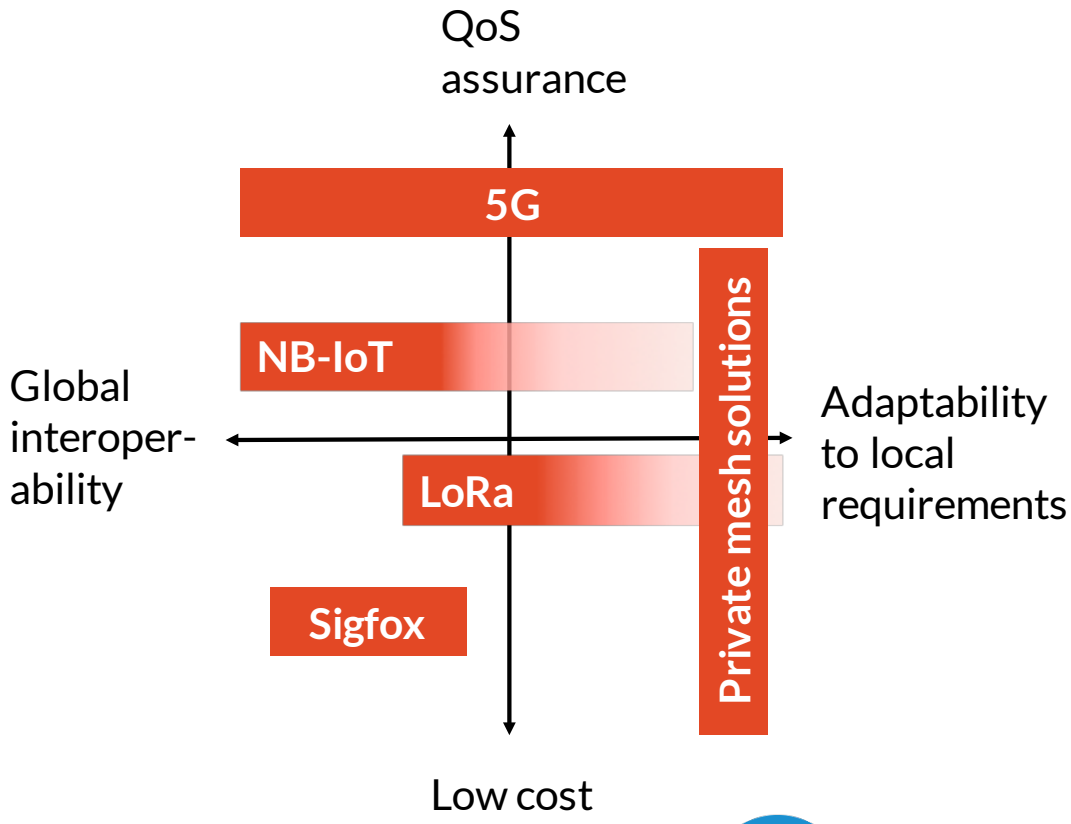
Source: Northstream, 2017

Technology Options for Massive IoT

Coverage vs. Density

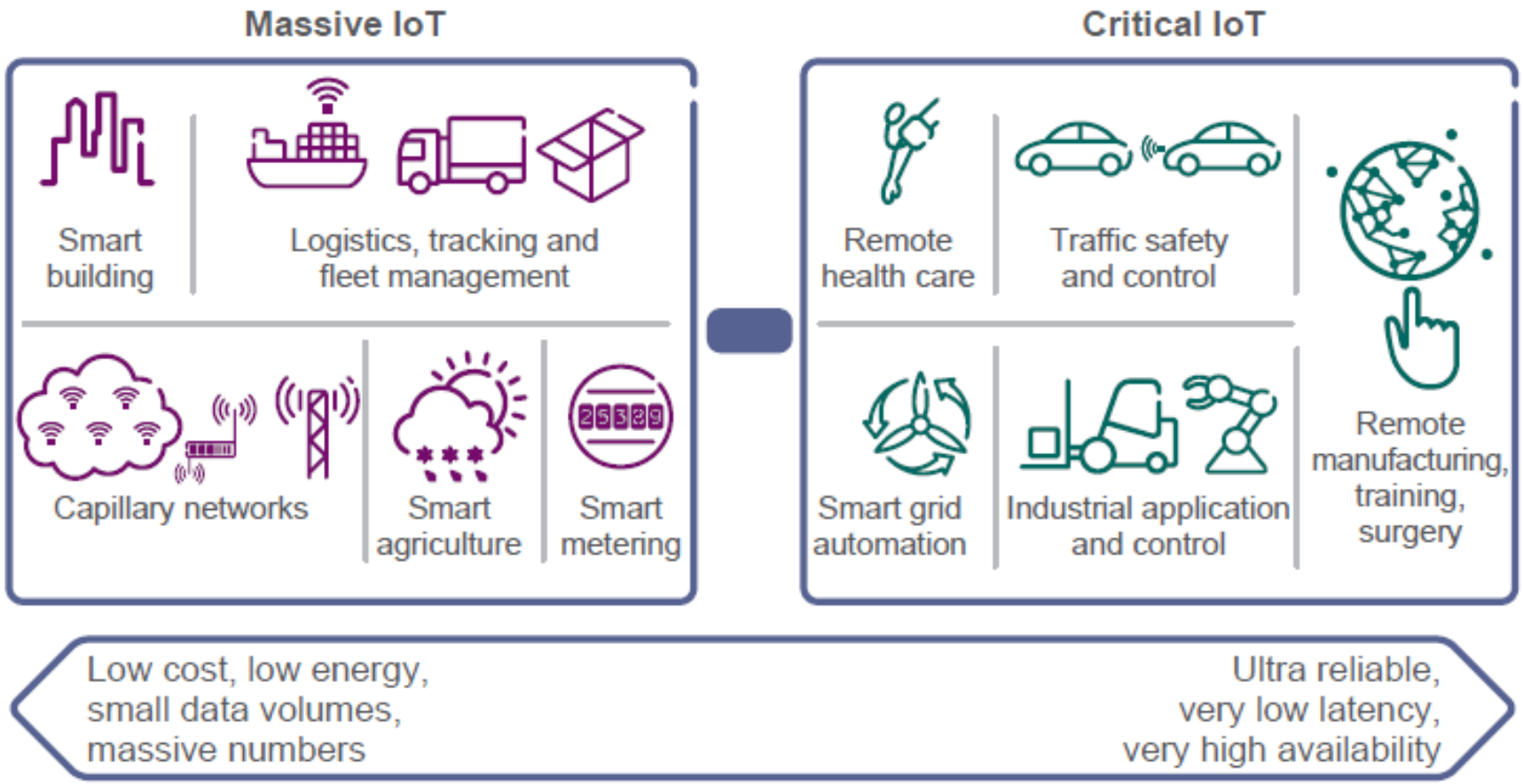


Tradeoffs



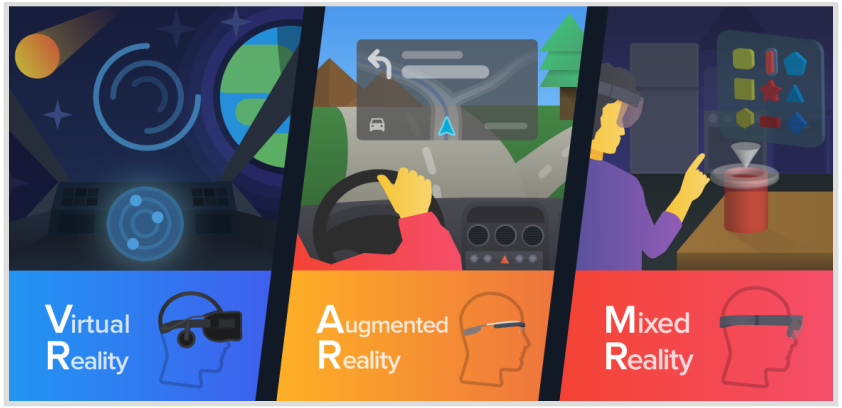
Source: Northstream, 2017

Different contexts - Different requirements



Source: Ericsson, Jan. 2016

Critical IoT Applications

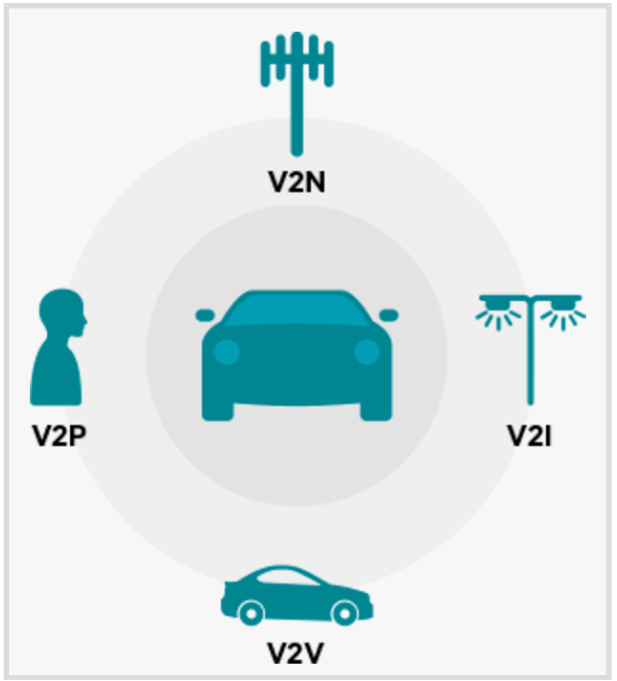


VR/AR/XR

Robotics & Factory 2.0

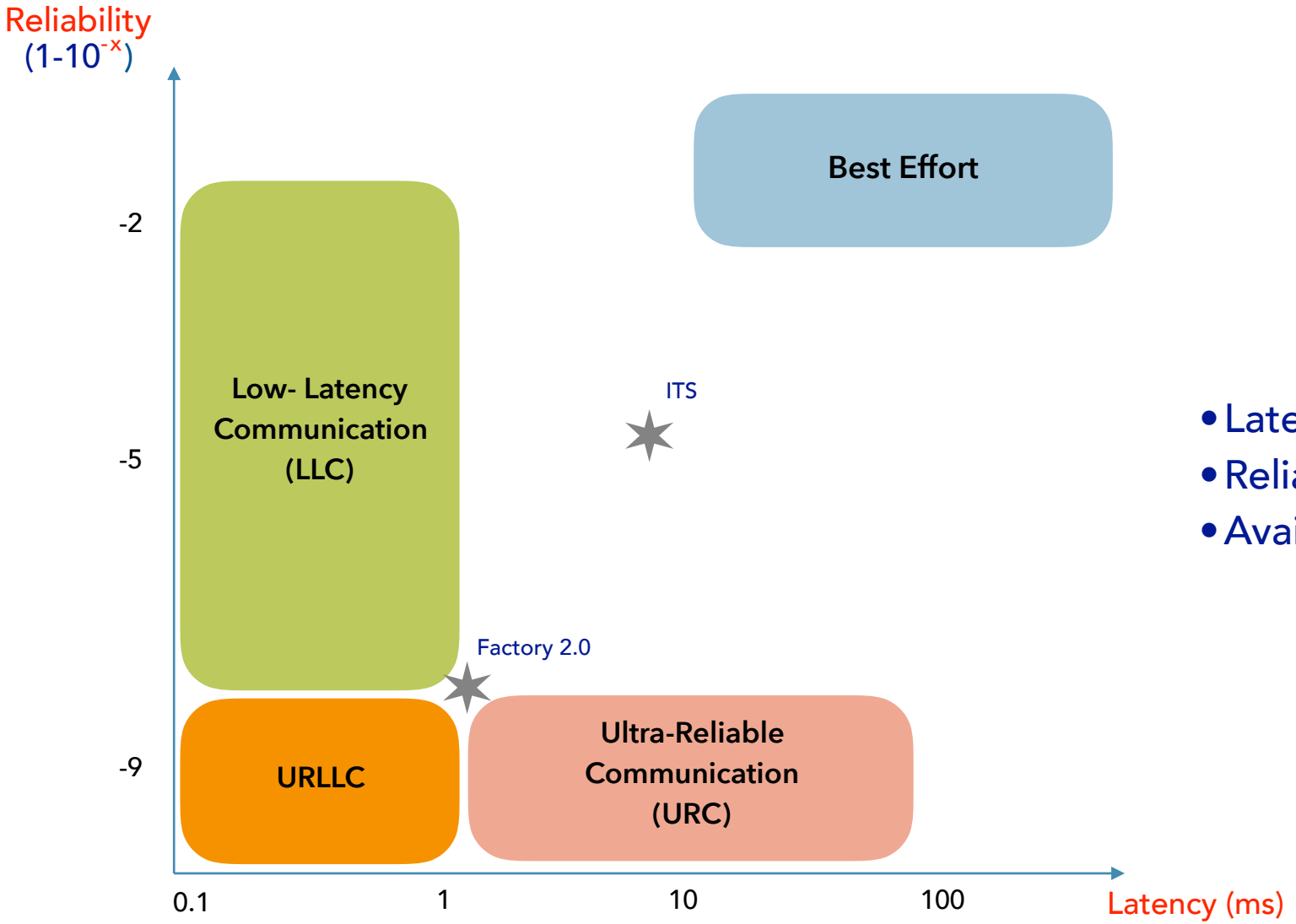
Telemedicine

Drones and UAVs



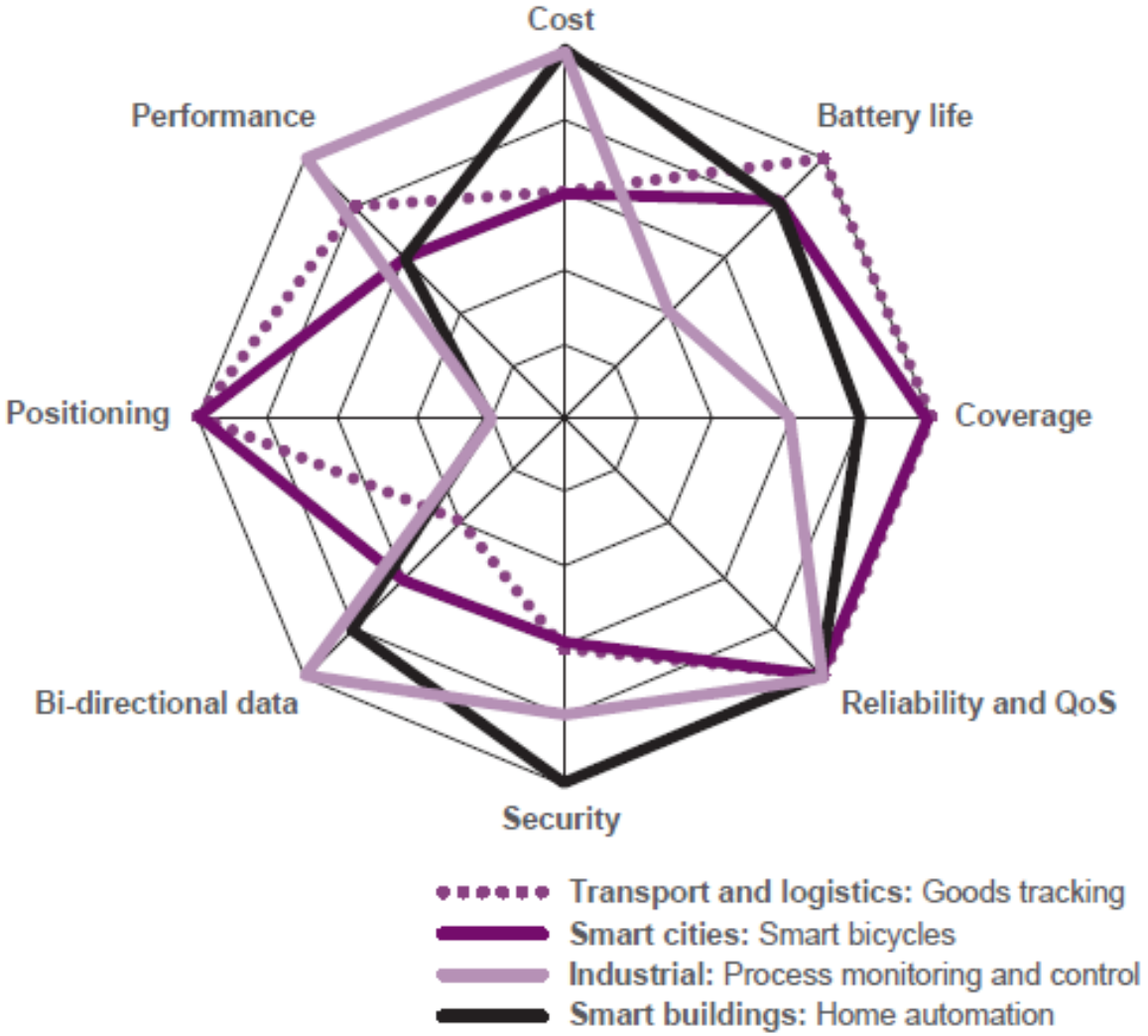
Autonomous Driving & V2X

Key Requirements for Critical IoT



- Latency *(E2E, user/control plane)*
- Reliability *(FER, Outage, …)*
- Availability *(probability, time/space uniformity, …)*

Examples – Comparison



Source: Ericsson, Jan. 2016

Thank You

شكراً

ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 1

Internet of Things (IoT)

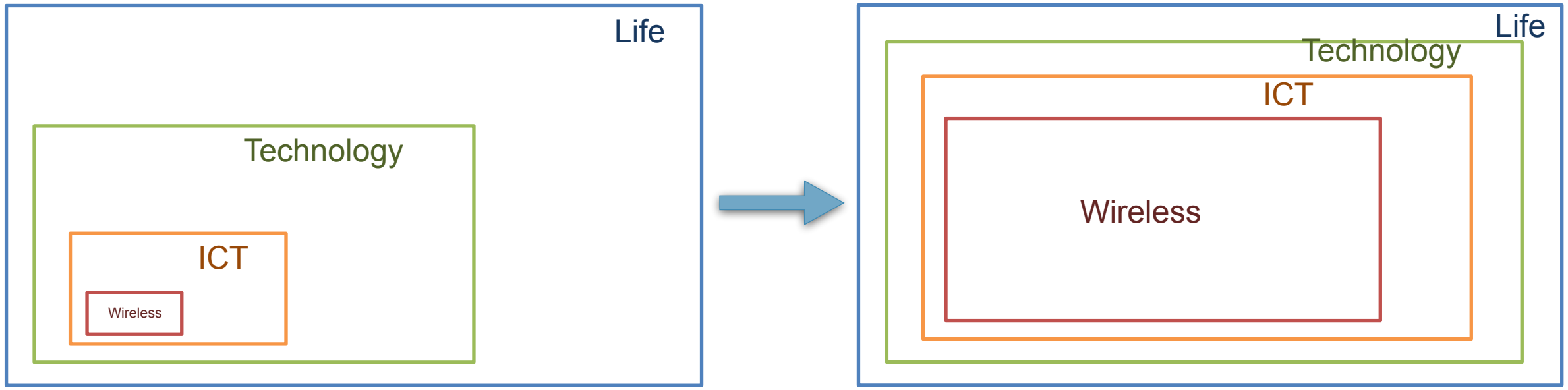
for Smart Sustainable Cities (SSC):

Challenges and Opportunities

Dr. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

Policy and Regulation Challenges

Anything that can be connected will be connected …



The IoT Transformation

- Dramatic transformation from isolated systems to Internet of Things (IoT).
- Driven by the convergence of:
  - increasingly connected devices,
  - computing and data economics,
  - proliferation and acceleration of cloud and big data analytics.
- Unprecedented opportunities for public and private sectors to:
  - develop new services, new and innovative user experiences;
  - enhance productivity and efficiency;
  - improve real-time decision making;
  - solve critical societal problems.

IoT – Cross-Layer Transversality

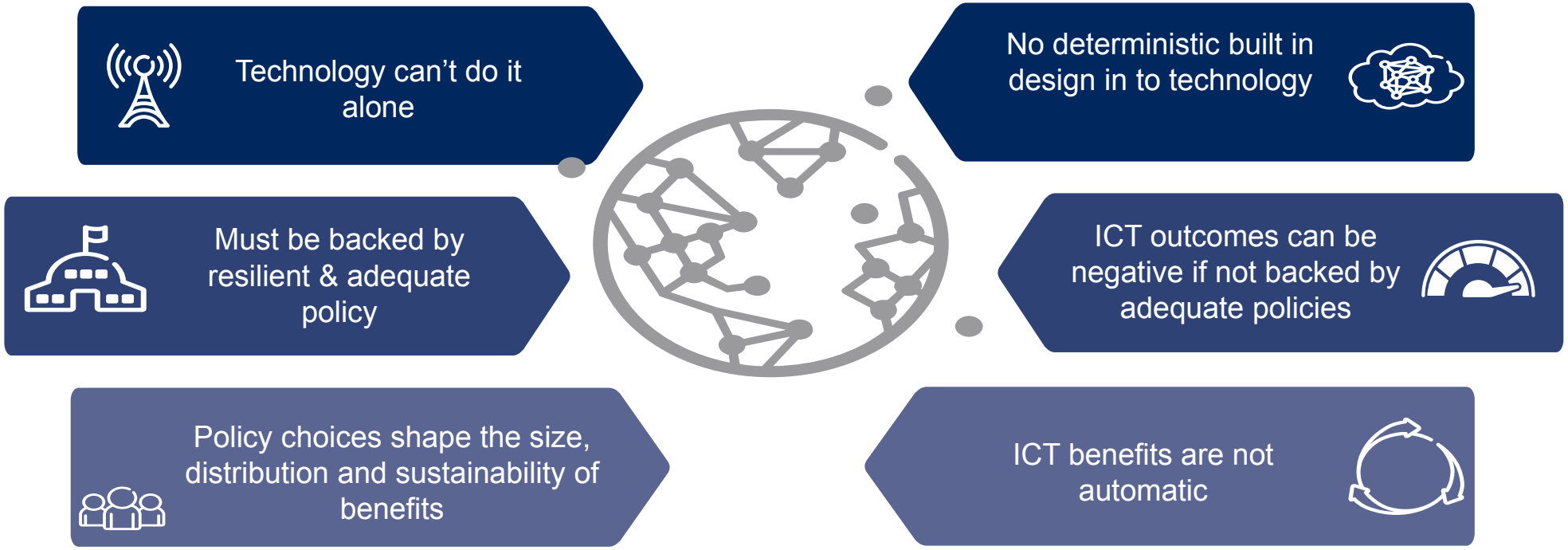
Many Topics and Sectors

- Privacy — Data Protection — Identity and authentication
- Big Data
- Network Security — Device Security
- Health — Smart Homes — Environment —Transportation
- B2B and Industrial

Many Layers

- Hardware and physical layers
- Communication Protocol Layers
- Network Typology
- Application
- Data storage and access

Need for policy actions



Source: Ericsson AB 2017.

Policy versus Regulation

- Plenty of room for confusion and conflict in the IoT context.
- Ideally:
  - Policies are general, and set broad directions and incentives to achieve desired outcomes.
  - Regulations define the terms of compliance in detail and are restrictive in nature, often outlining penalties for non-compliance.
  - Policy and regulation more effective when complementary, that is policies set broad new avenues for growth while regulations define the rules of the road.
- Separation is linked to how different polities delegate power from elected or selected representatives to policy-making and regulatory bureaucracies and quangos.

Policy versus Regulation

- In IoT context:
  - Policies generally focusing on incentives to accelerate the expansion of IoT and promoting investments to bring economic and social benefits. The goal is to promote IoT.
  - Regulatory issues emerge in two ways:

    i) how previous regulations are being affected by the growth of connected things,
    ii) how this new wave of connected machines raises issues that may require new regulation (privacy in the digital age, for instance).

- In practice, however, policy makers frequently set incentives that include regulations embedded into laws and policy directives, while regulators like to create compliance mechanisms that fill out the holes in policy documents.

Initiatives and Interventions

- Industry Working Groups and Consortiums
- Multilateral/Multinational Institutions
- Standards Bodies
- National Regulations/Regulators.

General Policy Principles

- Connectivity and Interoperability
- Privacy and Security
- Intelligent analytics and big data
- Open standards
- Data and device discoverability
- Public-Private Partnerships

New policy and regulation challenges

- Digitization predominantly driven by private investments
- IoT embedded in all sectors — convergence
- Broader policy toolbox
- Changing competitive dynamics
- Aligned sector & framework policy objectives
- Key policy objective is promotion of investment and innovation

High-level requirements

- Identification-based connectivity
- Interoperability
- Autonomic networking
- Location-based capabilities
- Security
- Privacy protection
- Plug and play
- Manageability

Source: ITU Recommendation ITU - T Y.2060

Global versus Local

Common global challenges:

- Data ownership & accessibility
- Liability in case of problems
- Spectrum/resources usage
- Impact of product/service on privacy
- End-user protection
- Availability guarantees
- Legislation influence on systems interoperability

Specific local/national contexts:

- Priority settings
- Presence/absence of regulation
- Presence/absence of standards
- Encouragement vs. Obligation
- Obstacles vs. Opportunities

Examples: Directions and Issues

- Services licensing issues:
  - Countries still have service specific licensing frameworks
  - Definition of telecom services provided by IoT
  - Cross-sectorial services (licensed vs. non-licensed services)
  - Rights and obligations applying (licensees, resellers, others, …?)

- Spectrum Issues:
  - Traffic and spectrum availability
  - Licensing (allocation method, terms and conditions, technology aspects, license period)
  - Technical (low/high range)
  - Energy Efficiency (e.g. battery life)
  - Commercial

Examples: Directions and Issues

- Numbering, Addressing, and Number Portability Issues:
  - Sufficiency of numbering resources.
  - IP addresses (IPv4 to IPv6 transition).
  - MAC addresses.
  - Portability — How to switch IoT devices when changing operators?
  - Over-the-air (OTA) programming of SIMs.

- Privacy and Security Issues
  - Data is collected and shared automatically by devices, and some may be of critical nature.
  - National vs International collection and sharing of data — Consent of data owner? — Data classification and processing — Who can have access to collected data? — Entity responsible for data protection — Applicable laws — Data protection vs Open data …
  - Security of device and data.
  - Consumer protection.
  - IoT devices should follow a security and privacy "by design" approach.

Example: GSMA Perspective

- Avoid explicit IoT regulation and avoid extending legacy regulation.
- Support for interoperable, industry-led specifications and standards.
- Support for global and harmonized spectrum.
- Encouragement of trust development by industry.
- International engagement to avoid global fragmentation.

Thank You

شكراً