Internet of Things: Policy and Regulatory Enablers

ITU ASP COE TRAINING ON

“Developing the ICT ecosystem to harness IoT”

13-15 December 2016
Bangkok, Thailand

Understanding the context of IoT policy and regulatory enablers?

What are the emerging services and infrastructures that IoT leverages?

ICTs is multi-sectoral and so are IoT applications

Emergency

Education

Health

Agriculture

Governance

Investment

Applications

Policy & Regulation

Capacity Building

Transport

IoT, Sensor Networks

Universal Broadband

Green ICT & E-Waste

Measurements

Electricity

SMART SOCIETY

Infrastructure Security

Privacy & Security

Water

Digital Inclusion

Spectrum Management

Standards, Conformity & Interoperability

Teleworking

Goals for a Sustainable Future : The SDGs

Agreed Global Telecommunication/ICT Targets - 2020

Goal 1 Growth : Enable and foster access to and increased use of telecommunications/ICTs

55%
of households should have access to the Internet

60%
of individuals should be using the Internet

40%
Telecommunications/ICTs should be **40%** more affordable

GROWTH

Goal 2 Inclusiveness – Bridge the digital divide and provide broadband for all

50%
of households should have access to the Internet in the developing world; **15%** in the least developed countries

50%
of individuals should be using the Internet in the developing world; **20%** in the least developed countries

40%
affordability gap between developed and developing countries should be reduced by **40%**

5%
Broadband services should cost no more than **5%** of average monthly income in the developing countries

INCLUSION

90%
of the rural population should be covered by broadband services

Gender equality among Internet users should be reached

Enabling environments ensuring accessible ICTs for persons with disabilities should be established in all countries

Goal 3 Sustainability – Manage challenges resulting from the telecommunication/ICT development

40%
improvement in cybersecurity readiness

50%
reduction in volume of redundant e-waste

30%
decrease in Green House Gas emissions per device generated by the telecommunication/ICT sector

SUSTAINABILITY

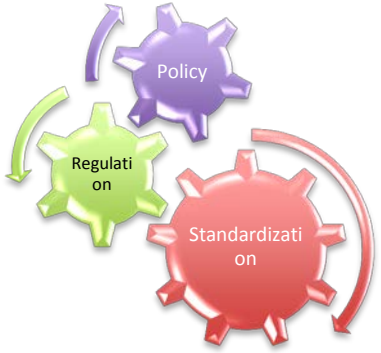
Goal 4 Innovation and partnership – Lead, improve and adapt to the changing telecommunication/ICT environment

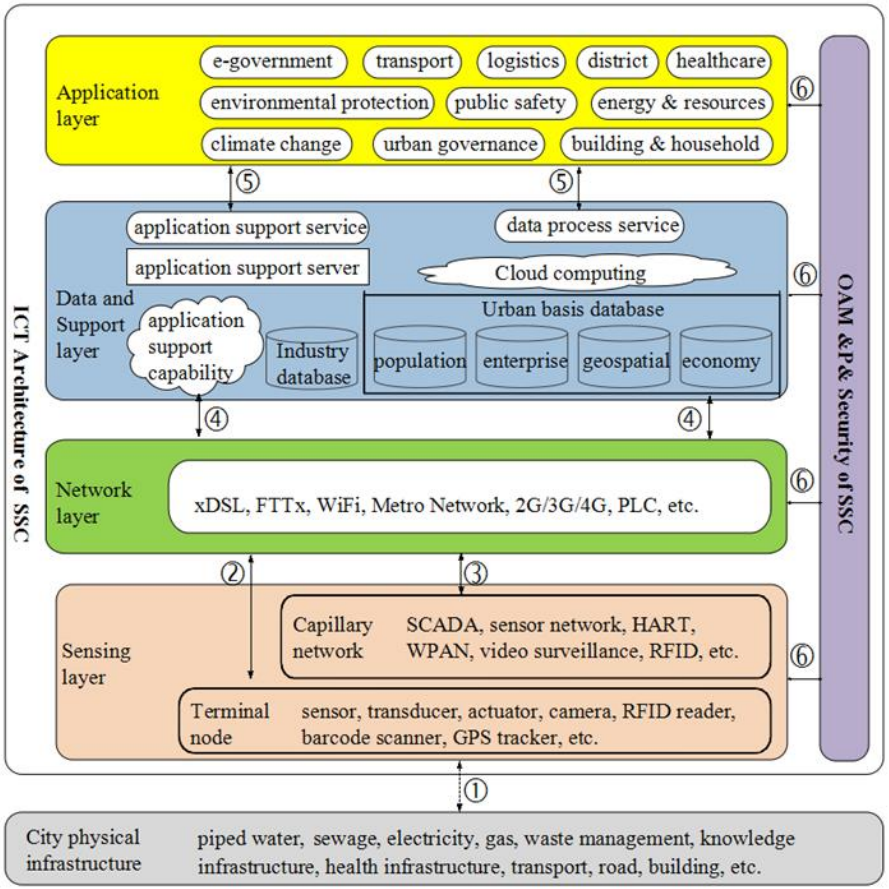
Telecommunication/ICT environment conducive to innovation

Effective partnerships of stakeholders in telecommunication/ICT environment

INNOVATION

Emerging ICT Infrastructure





Internet of Things use a wide variety of networks: mobile and fixed

Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

A multi-tier SSC (smart sustainable city) ICT architecture from communication view (physical perspective)

High-level requirements

- **Identification-based connectivity**: The IoT needs to support that the connectivity between a thing and the IoT is established based on the thing's identifier. Also, this includes that possibly heterogeneous identifiers of the different things are processed in a unified way.
- **Interoperability**: Interoperability needs to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services.
- **Autonomic networking**: Autonomic networking (including self-management, self-configuring, self-healing, self-optimizing and self-protecting techniques and/or mechanisms) needs to be supported in the networking control functions of the IoT, in order to adapt to different application domains, different communication environments and large numbers and types of devices.

Source: Recommendation **ITU-T Y.2060**

High-level requirements

- **Location-based capabilities**: Location-based capabilities need to be supported in the IoT.
- **Security**: In the IoT, every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.
- **Privacy protection**: Privacy protection needs to be supported in the IoT. Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing.

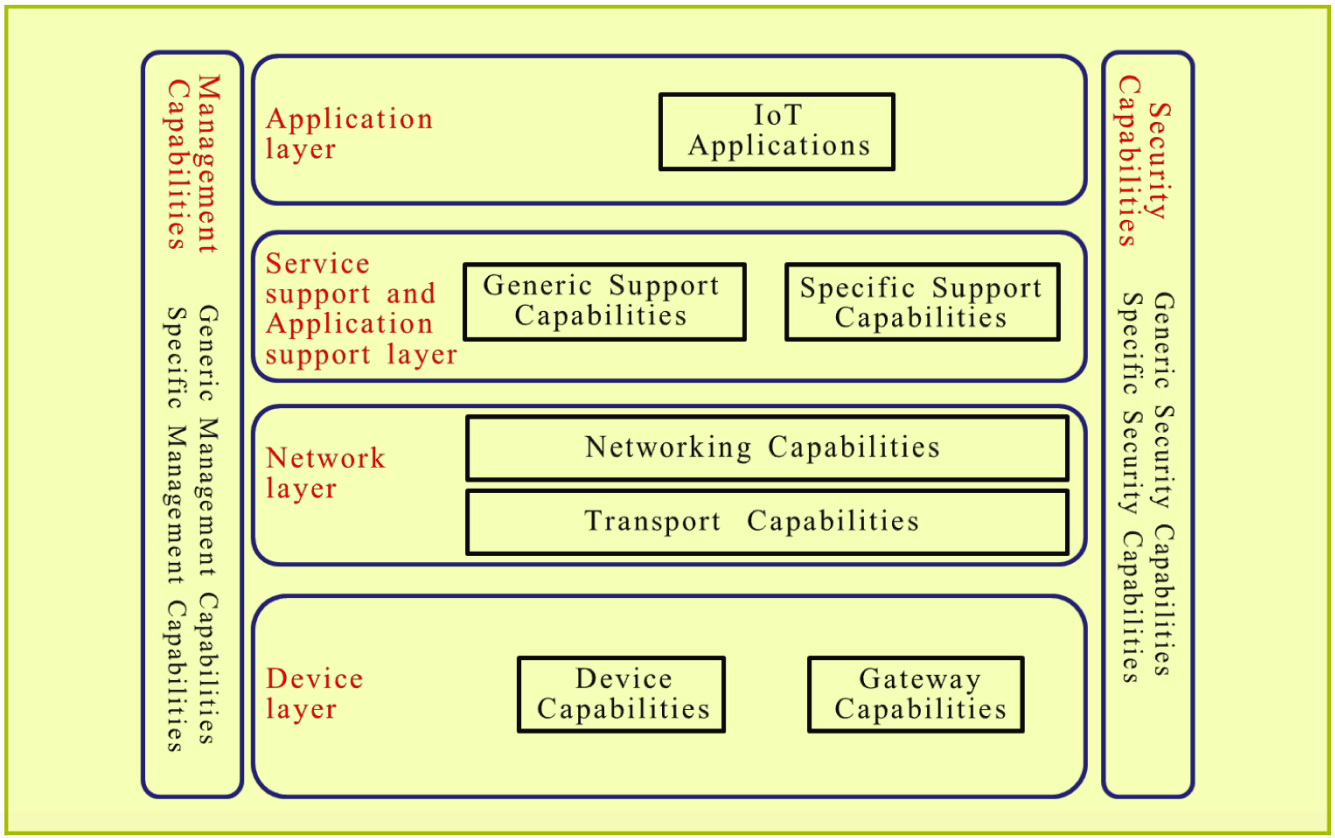
Source: Recommendation **ITU-T Y.2060**

High-level requirements

- **Plug and play:** Plug and play capability needs to be supported in the IoT in order to enable on-the-fly generation, composition or the acquiring of semantic-based configurations for seamless integration and cooperation of interconnected things with applications, and responsiveness to application requirements.
- **Manageability:** Manageability needs to be supported in the IoT in order to ensure normal network operations. IoT applications usually work automatically without the participation of people, but their whole operation process should be manageable by the relevant parties.

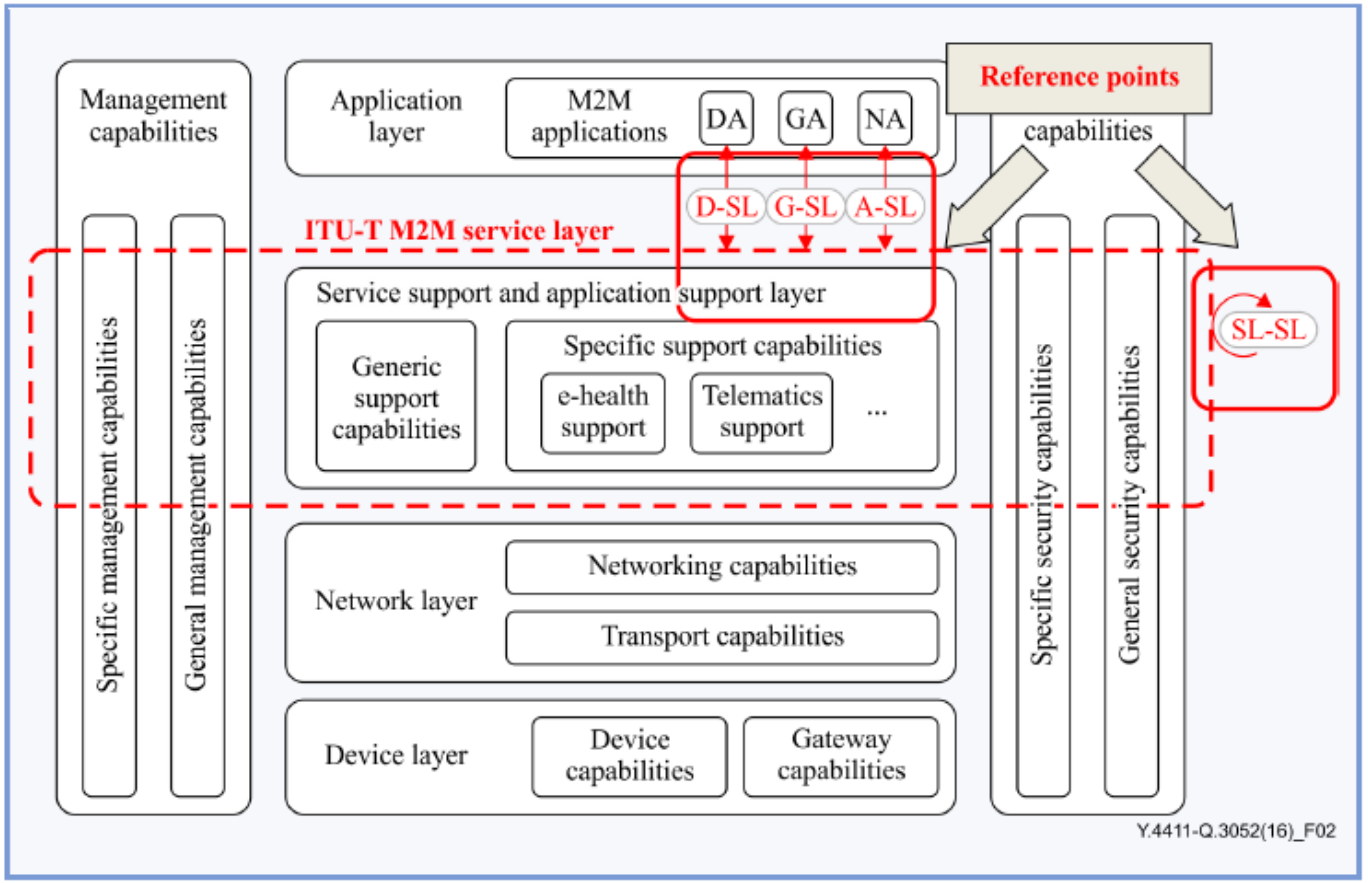
Source: Recommendation **ITU-T Y.2060**

IoT reference model



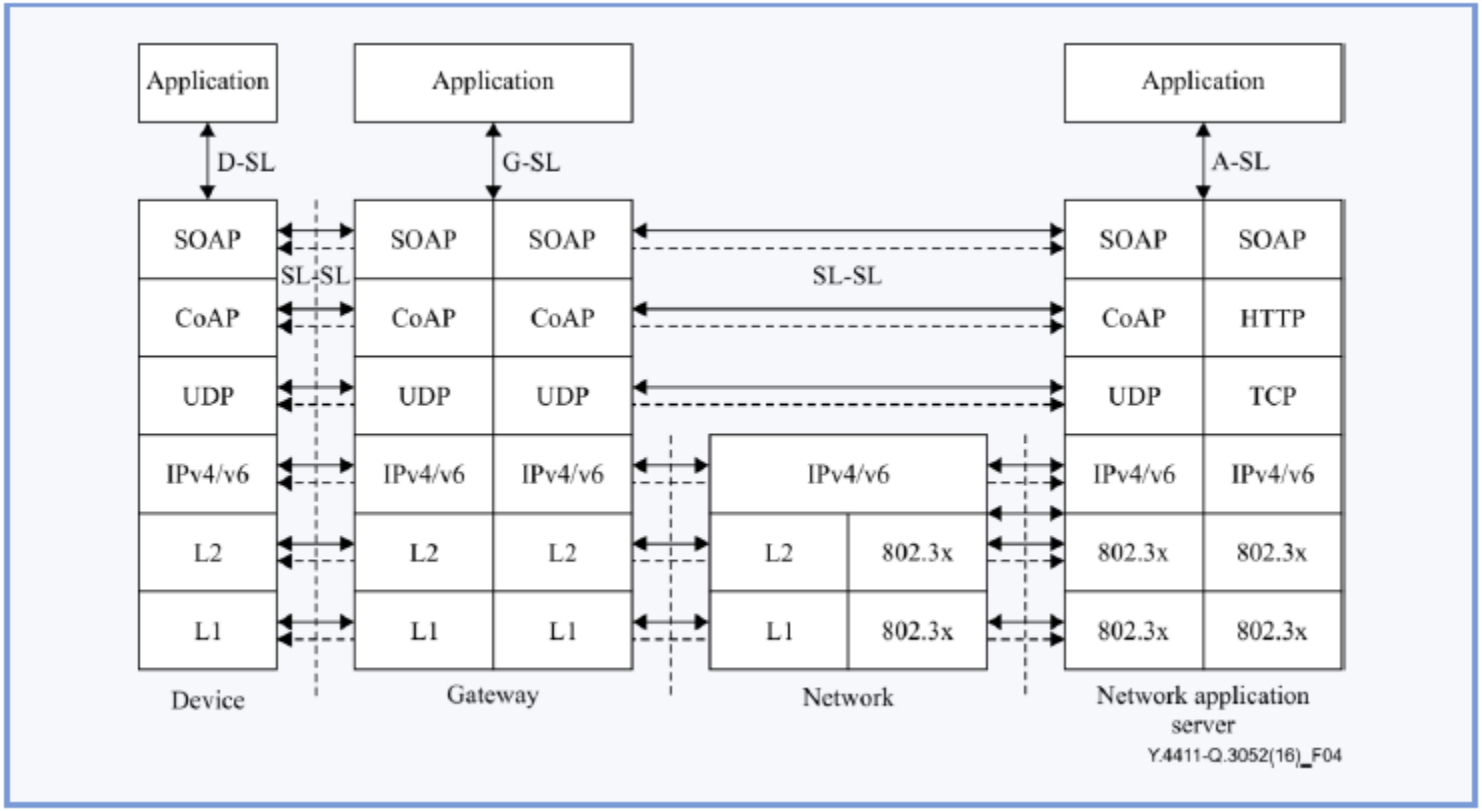
Source: Recommendation **ITU-T Y.2060**

Reference points of the ITU-T M2M service layer



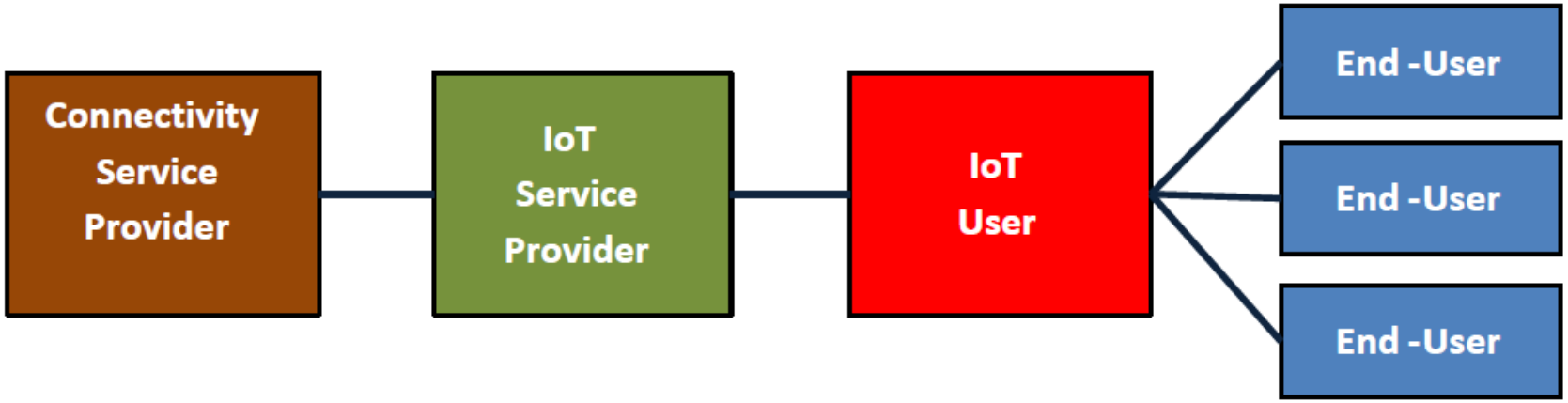
Source: ITU-T Recommendation **Y.4411/Q.3052 (02/2016)**

Example of protocol stacks in the component-based M2M reference model



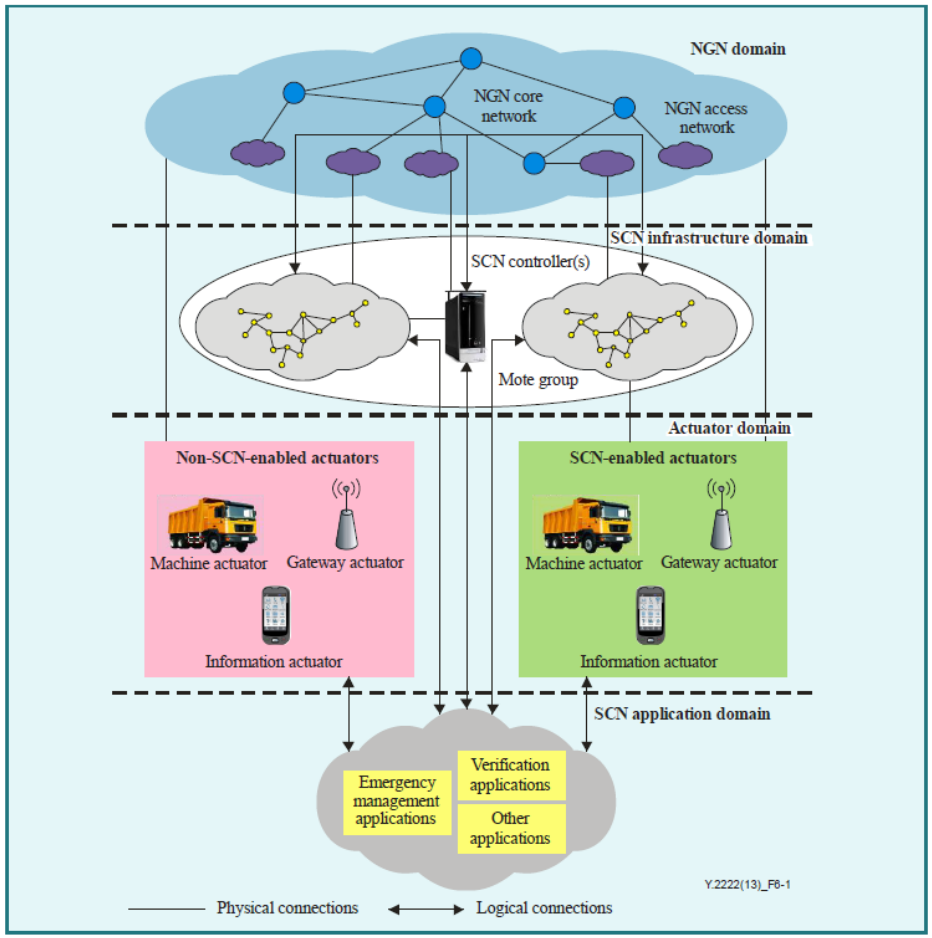
Source: ITU-T Recommendation **Y.4411/Q.3052 (02/2016)**

IOT Value Chain



Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016

Overview of Sensor Control Network (SCN)

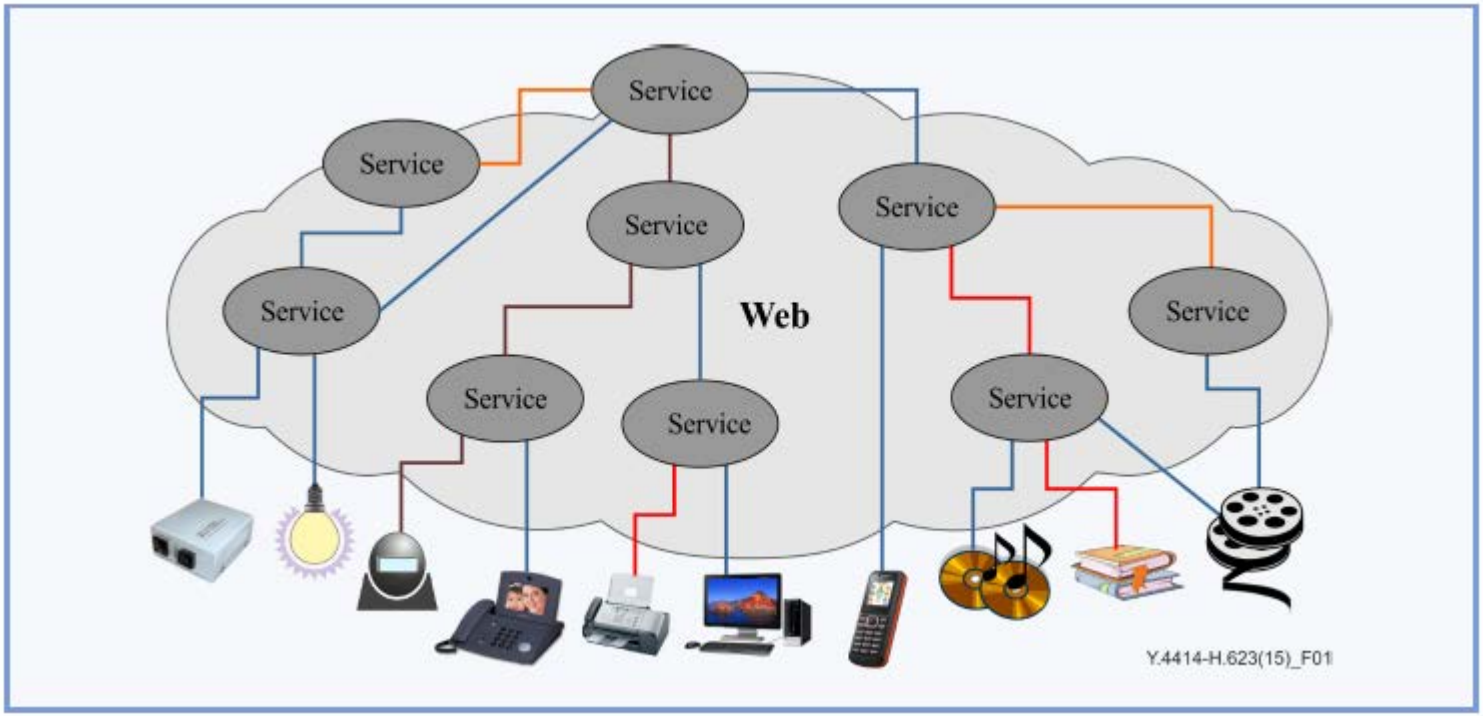


Source: Recommendation ITU-T T.4250/Y.2222

Service requirements of SCN applications

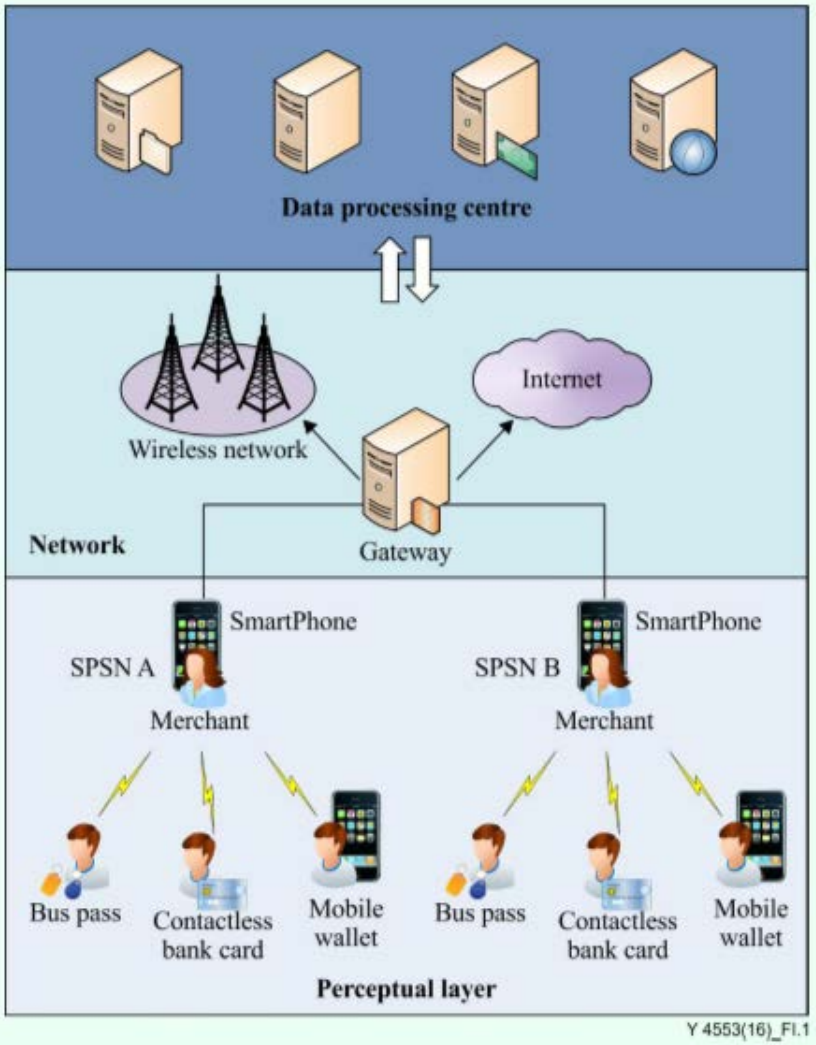
- Connectivity
- Mobility support
- Context awareness
- Location awareness
- Presence awareness
- Traffic and load awareness
- Fault awareness
- Routing
- Load balancing
- Scalability
- Fault tolerance
- Quality of service
- Management
- Pledging of security of decisions
- Open service environment (OSE) support
- NGN service integration and delivery environment (NGN-SIDE) support
- Mass mobile user terminal support
- Emergency management applications
- Security

General Concept of Web of Things



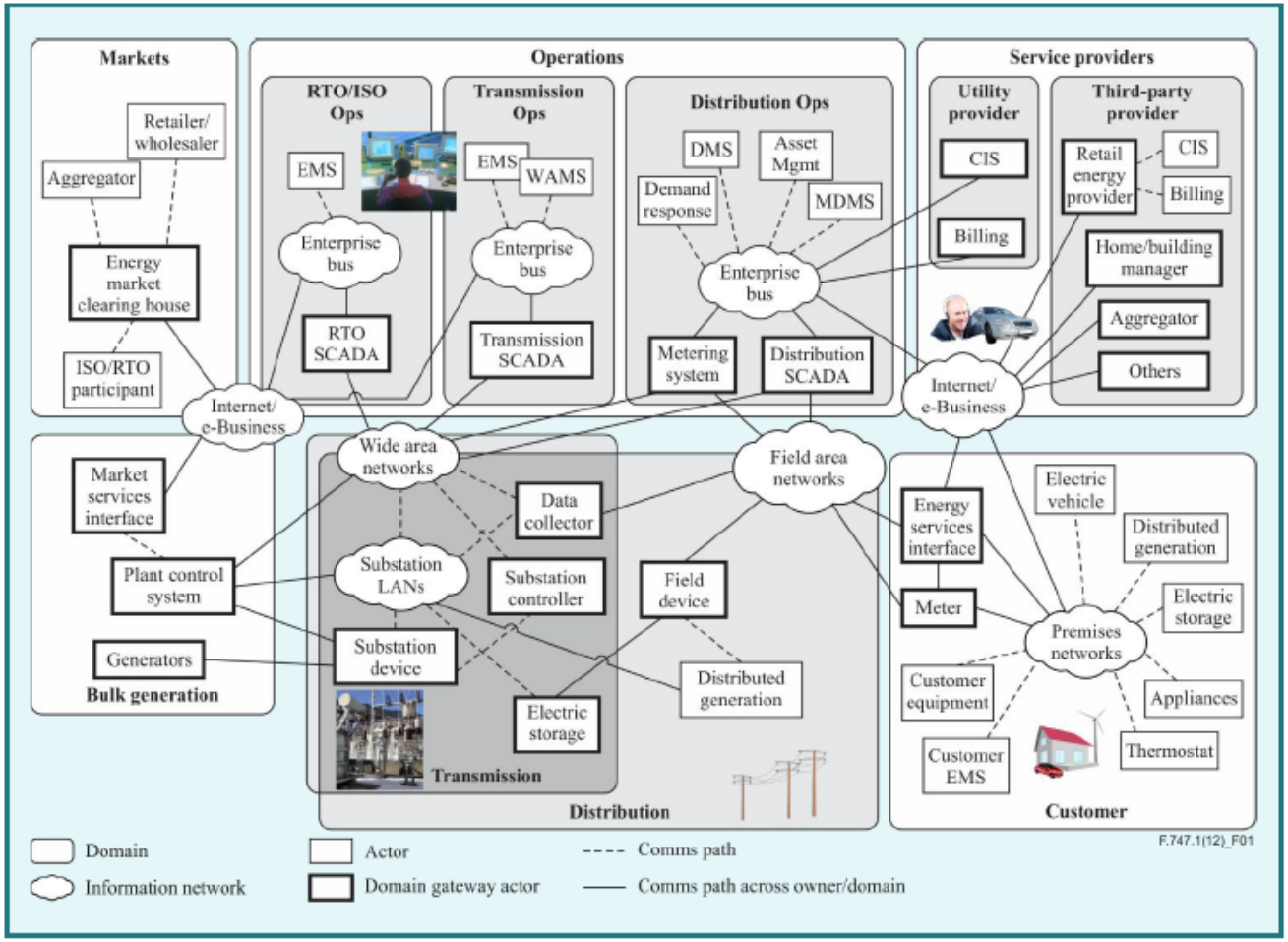
Source: Recommendation ITU-T **Y.4414/H.623 (11/2015)**

Scenario of the SPSN used for commercial merchant



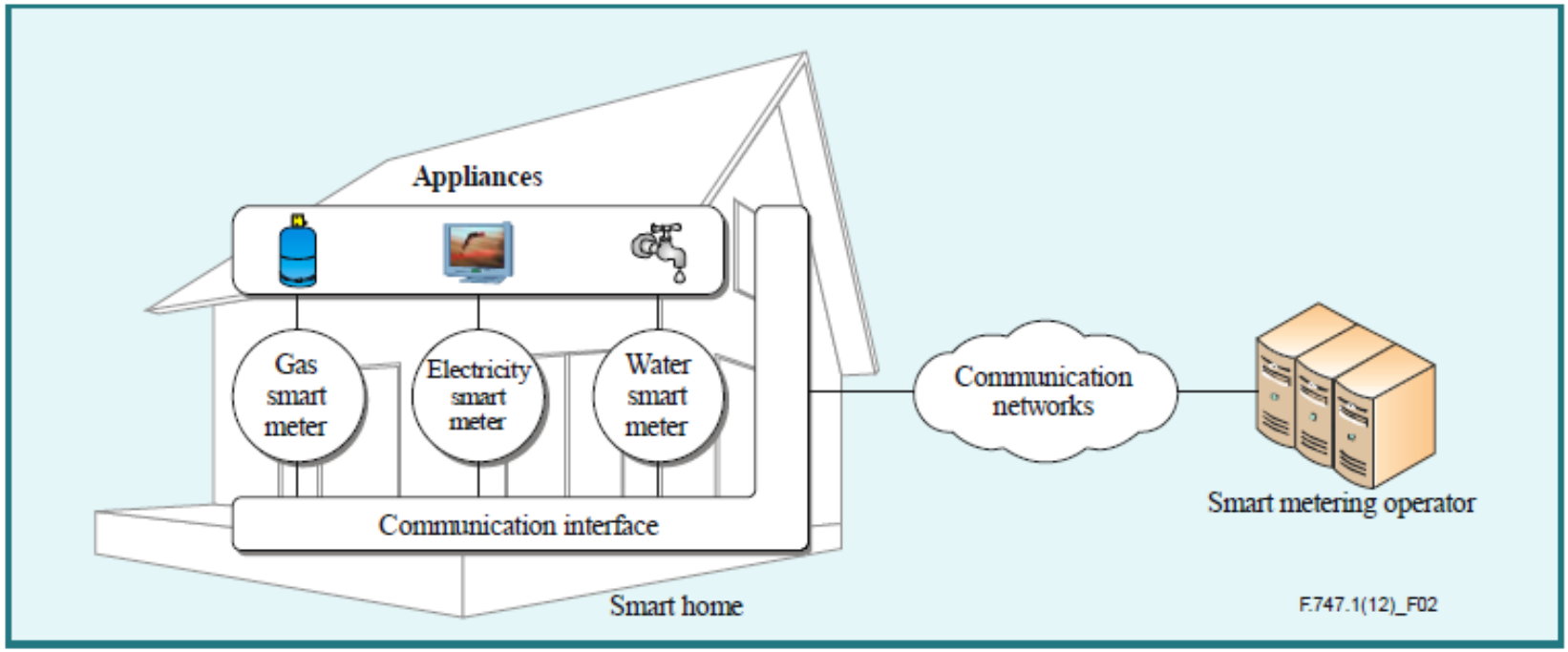
Source: Recommendation ITU-T Y.4553 (03/2016)

IOT Example: Smart Grid Architecture



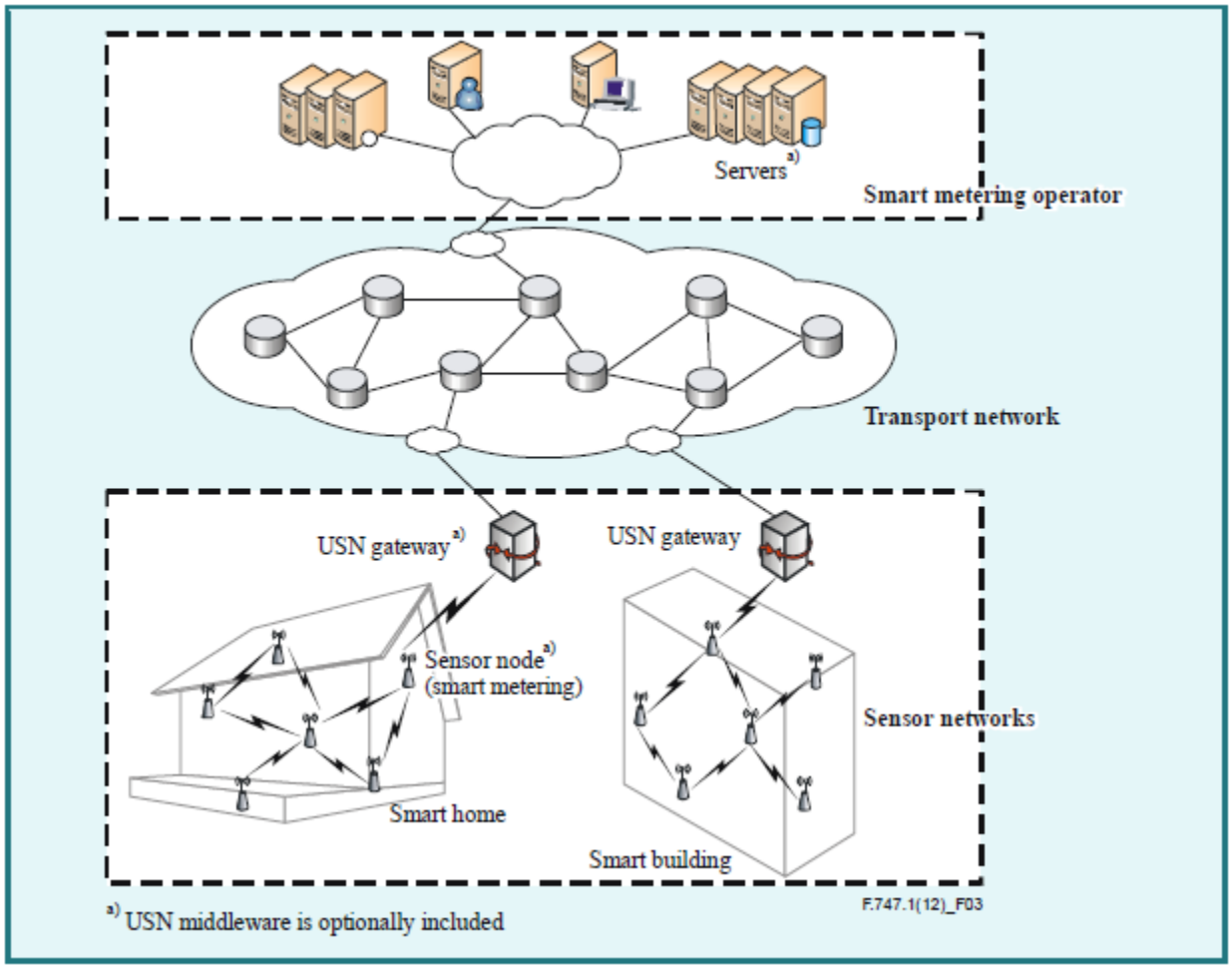
Source: Recommendation ITU-T Y.4251/F.747.1 (06/2012)

IOT Example: Technical Overview of Smart Metering



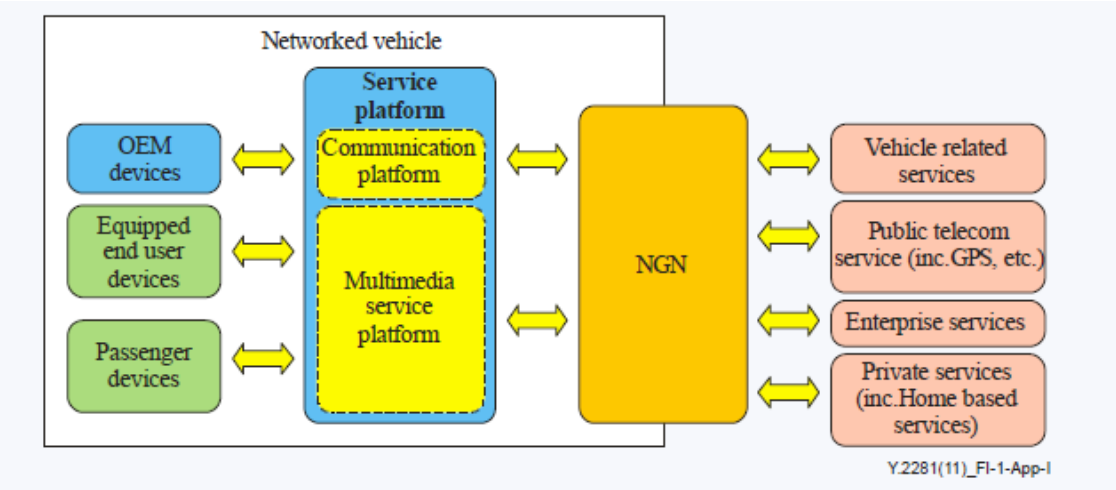
Source: Recommendation ITU-T Y.4251/F.747.1 (06/2012)

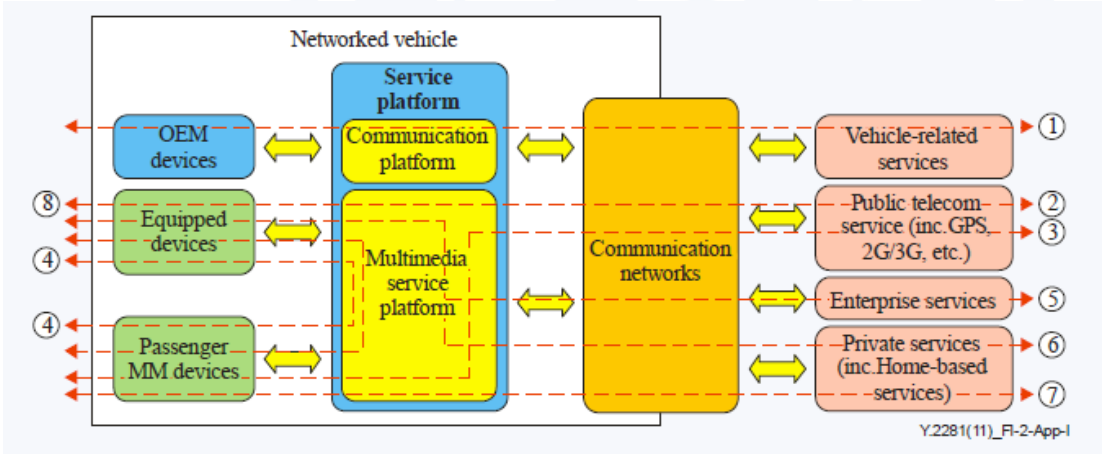
IOT Example: USN-based smart metering services



Source: Recommendation ITU-T Y.4251/F.747.1 (06/2012)

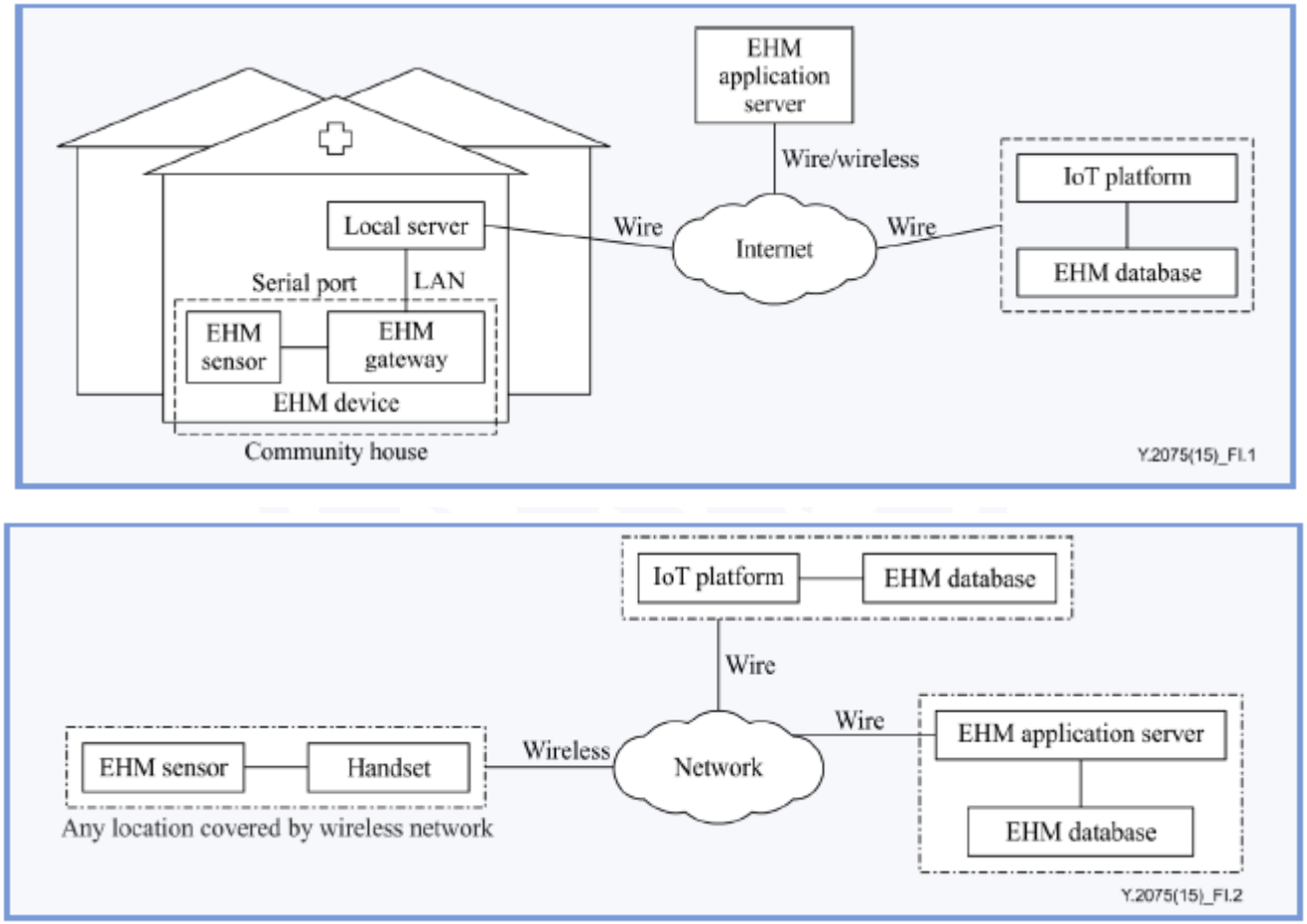
IOT Example: Service configuration model of a networked vehicle





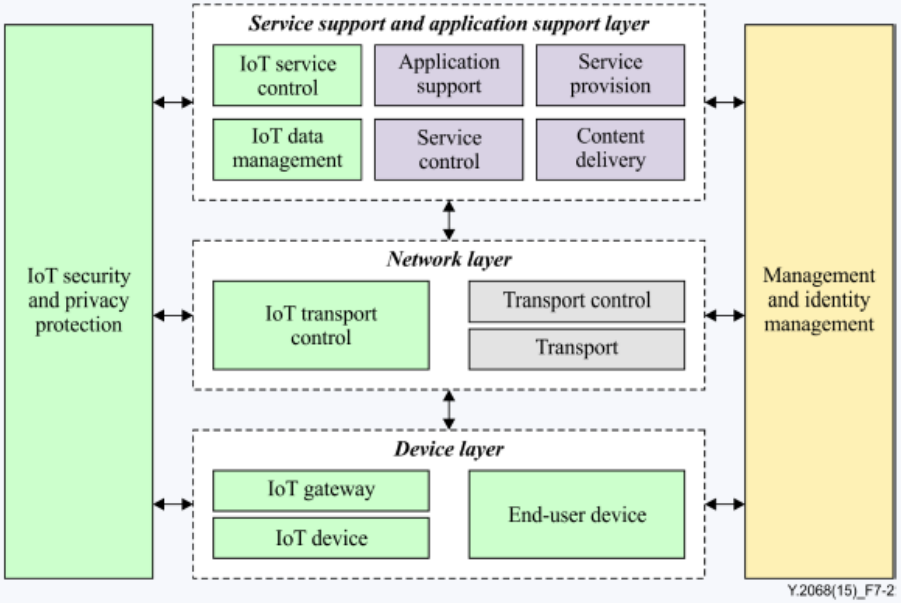
Source: Recommendation ITU-T **Y.4407/Y.2281 (01/2011)**

IOT Example: E-Health Monitoring (EHM) service deployment technical scenarios

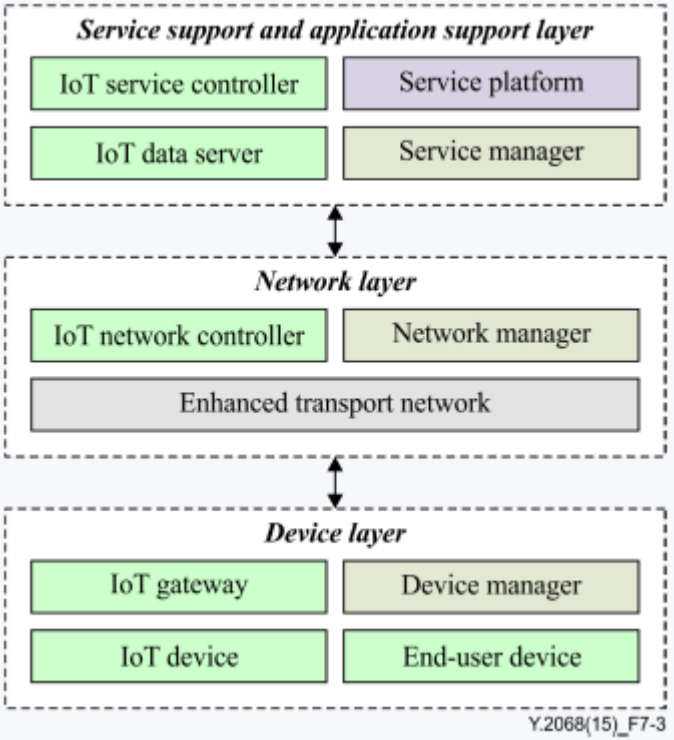


Source: Recommendation ITU-T **Y.4408/Y.2075 (09/2015))**

Implementation view of the IoT functional framework building over the NGN functional architecture



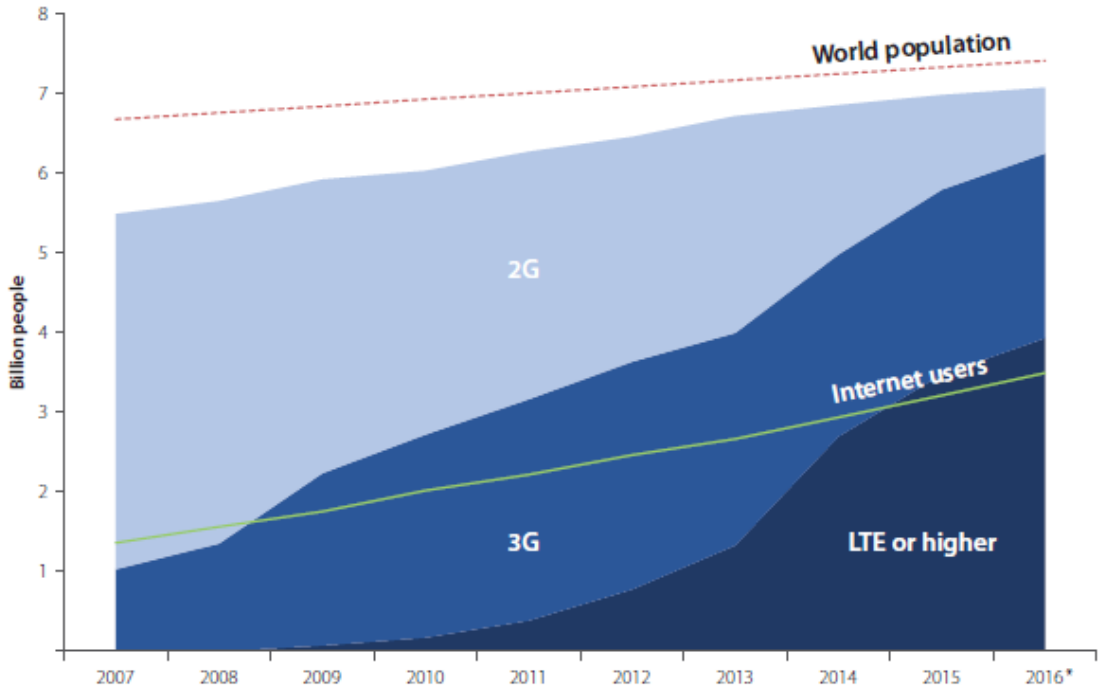
Deployment view of the IoT functional framework building over the NGN components



Source: Recommendation ITU-T Y.4401/Y.2068 (03/2015))

IOT and IMT 2020…

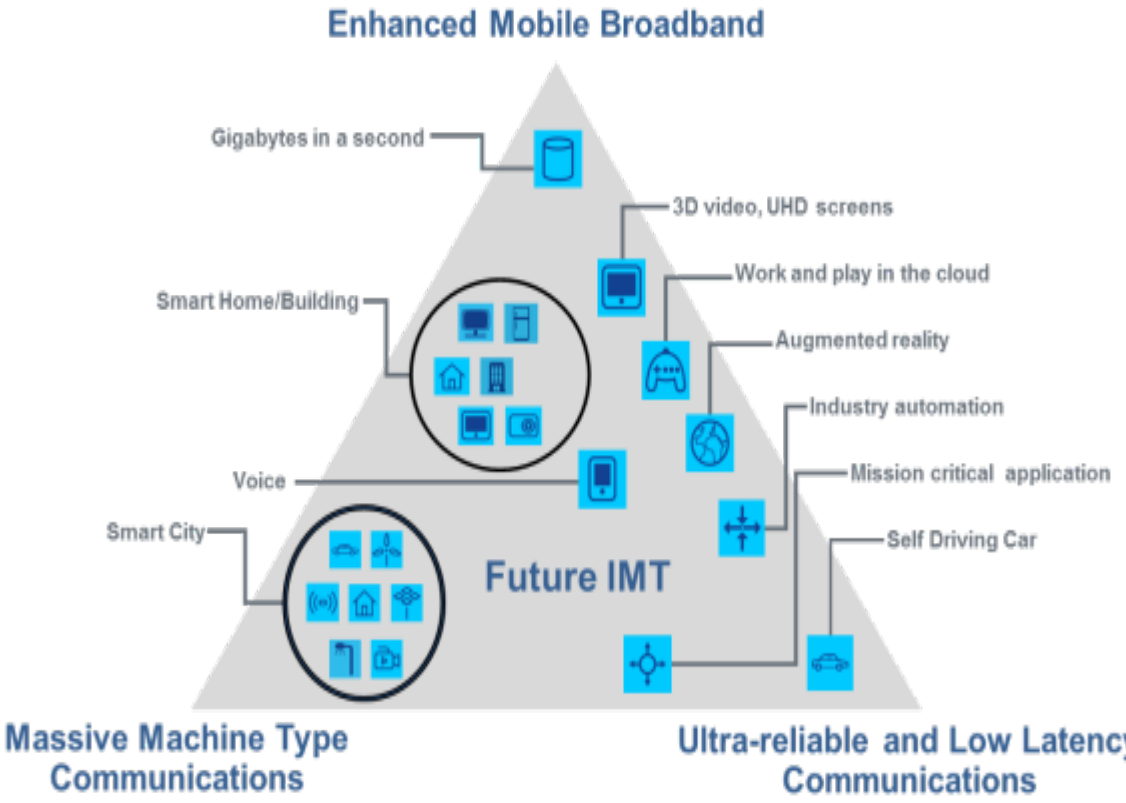
Mobile network coverage and evolving technologies



Source: ITU.
Note: * Estimates. Mobile network coverage refers to the population that is covered by a mobile network.

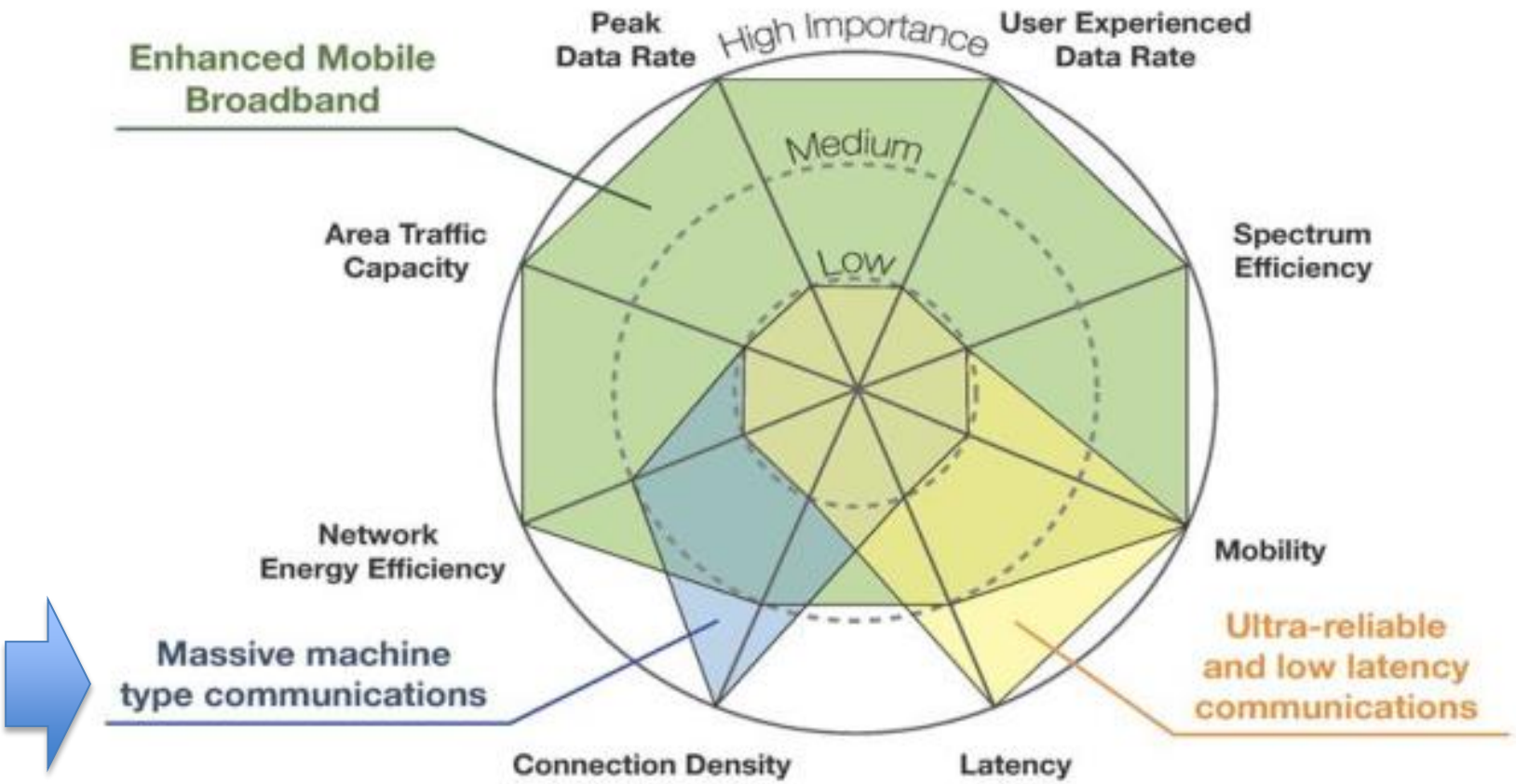
Newer generations of mobile have had faster take up…

Usage Scenarios for IMT 2020

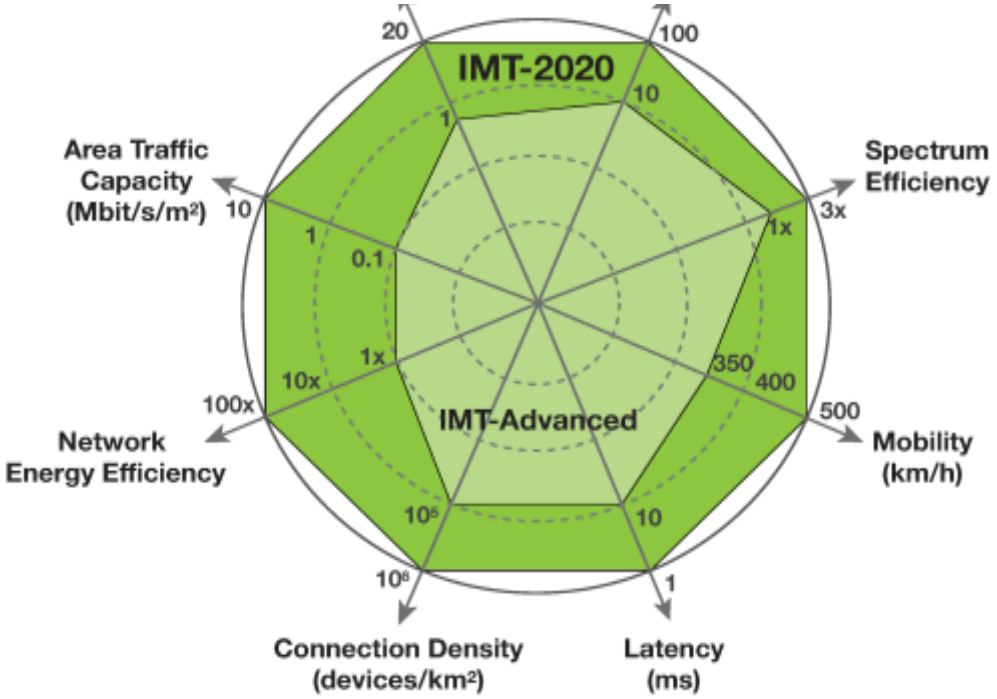


Massive machine communications an important aspect of IMT 2020

M2M: The importance of key capabilities in different usage scenarios

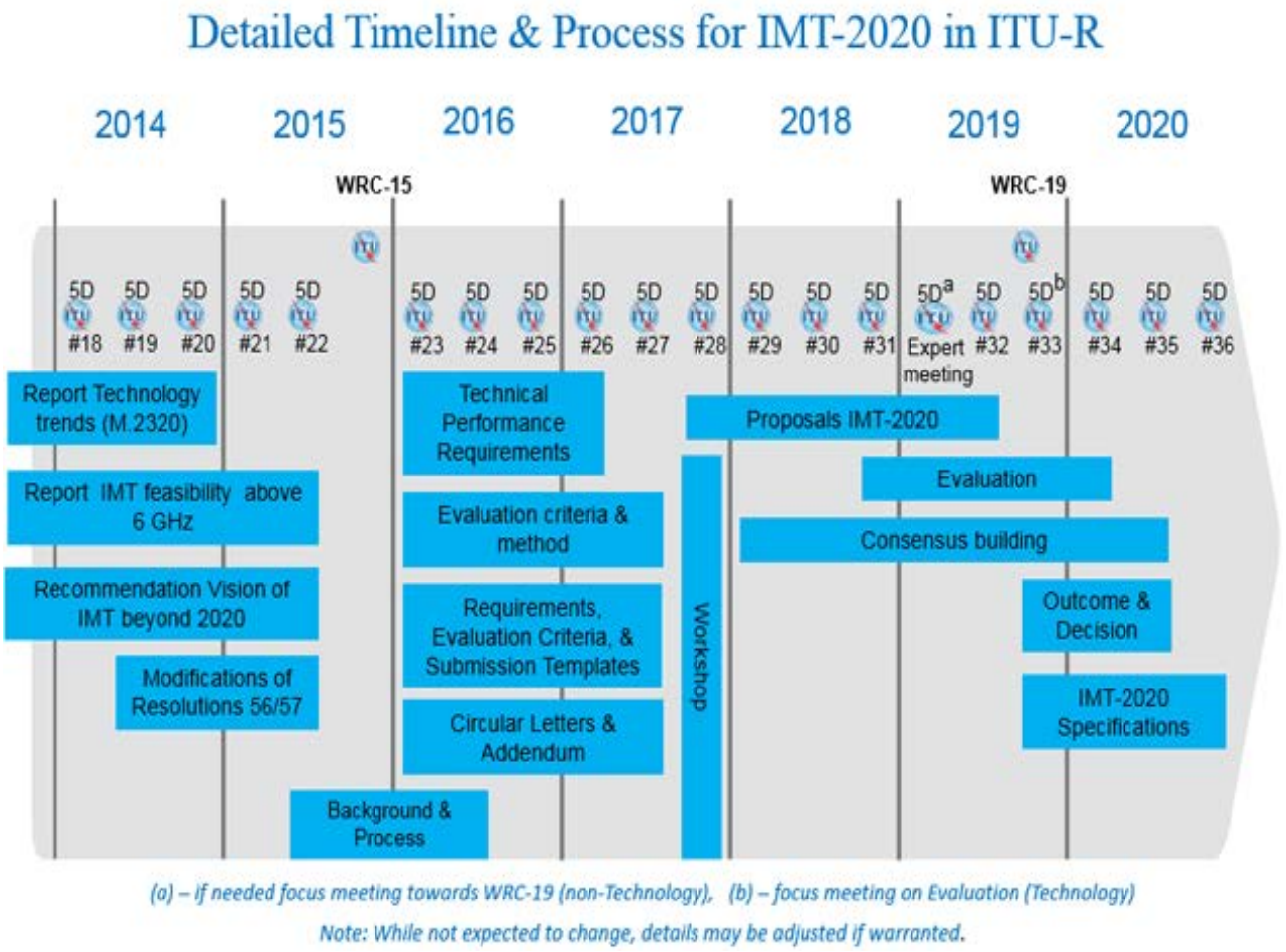


Future Mobile Generation: Enhancement of key capabilities from IMT-Advanced to IMT-2020



Source: ITU-R Recommendation M.2083-0 (09/2015)

What is the ITU-R IMT 2020 (5G) Roadmap?



(a) – if needed focus meeting towards WRC-19 (non-Technology), (b) – focus meeting on Evaluation (Technology)

Note: While not expected to change, details may be adjusted if warranted.

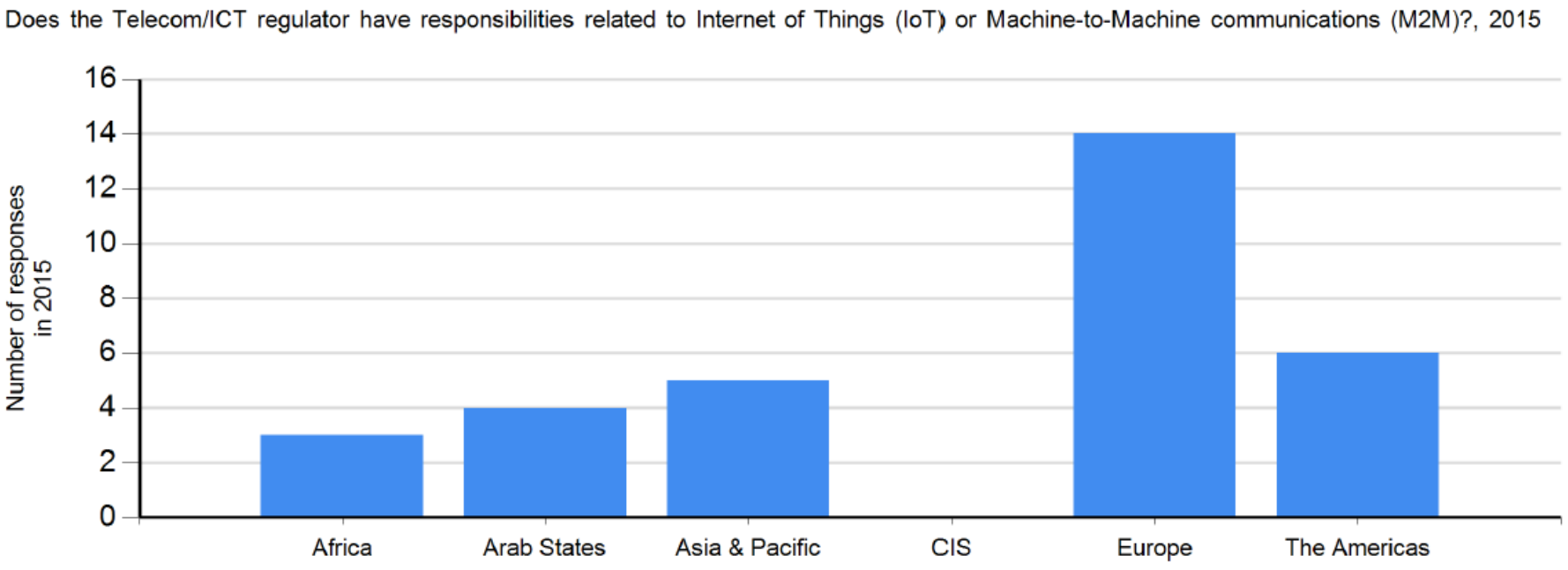
Policy and regulatory enablers

Analyzing the IoT definition in the policy and regulatory context

Internet of things (IoT) [ITU-T Y.2060]: A **global infrastructure** for the **information society** enabling **advanced services by interconnecting (physical and virtual) things** based **on existing and evolving, interoperable information and communication technologies**.

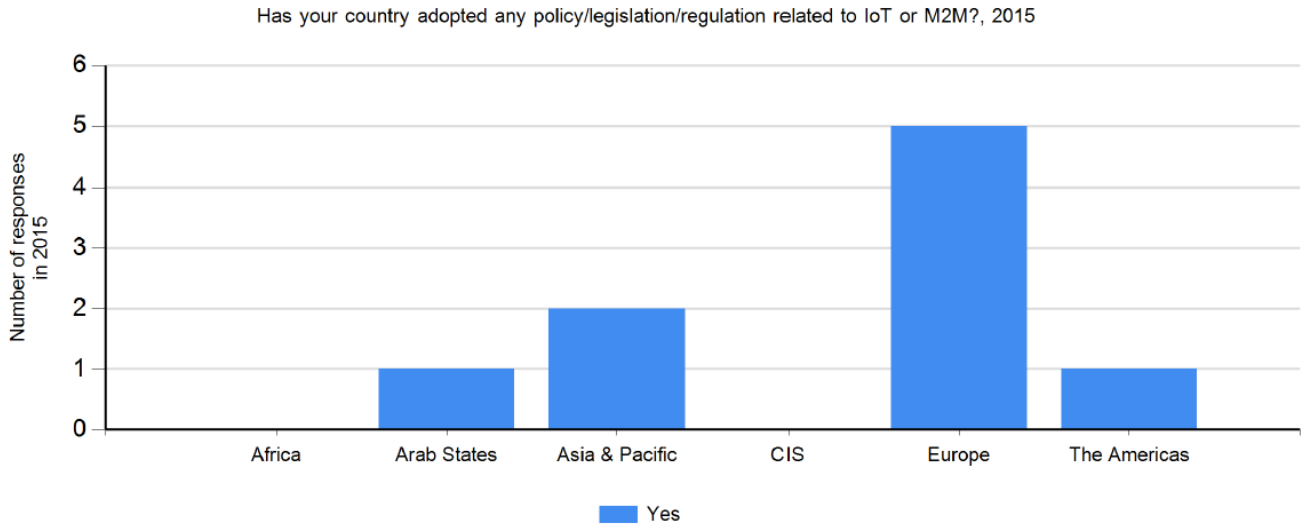
NOTE 1 (from [ITU-T Y.2060]) – From a broad perspective, the IoT can be perceived as a vision with technological and societal implications.
NOTE 2 (from [ITU-T Y.2060]) – Through the exploitation of **identification, data capture, processing and communication capabilitie**s, the IoT makes full use of things to **offer services to all kinds of applications**, whilst ensuring that **security and privacy requirements** are fulfilled.

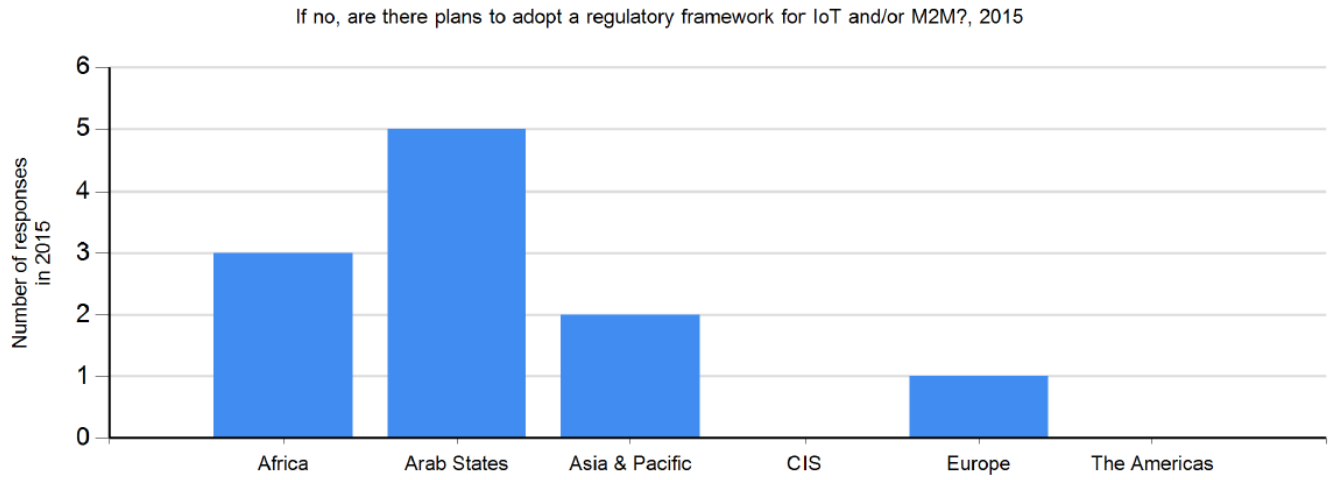
IOT AND REGULATORY AUTHORITY



Source: ITU World Telecommunication Regulatory Database

IOT policy and legislation





Source: ITU World Telecommunication Regulatory Database

Emerging ICT Infrastructure and Policy and Regulatory issues

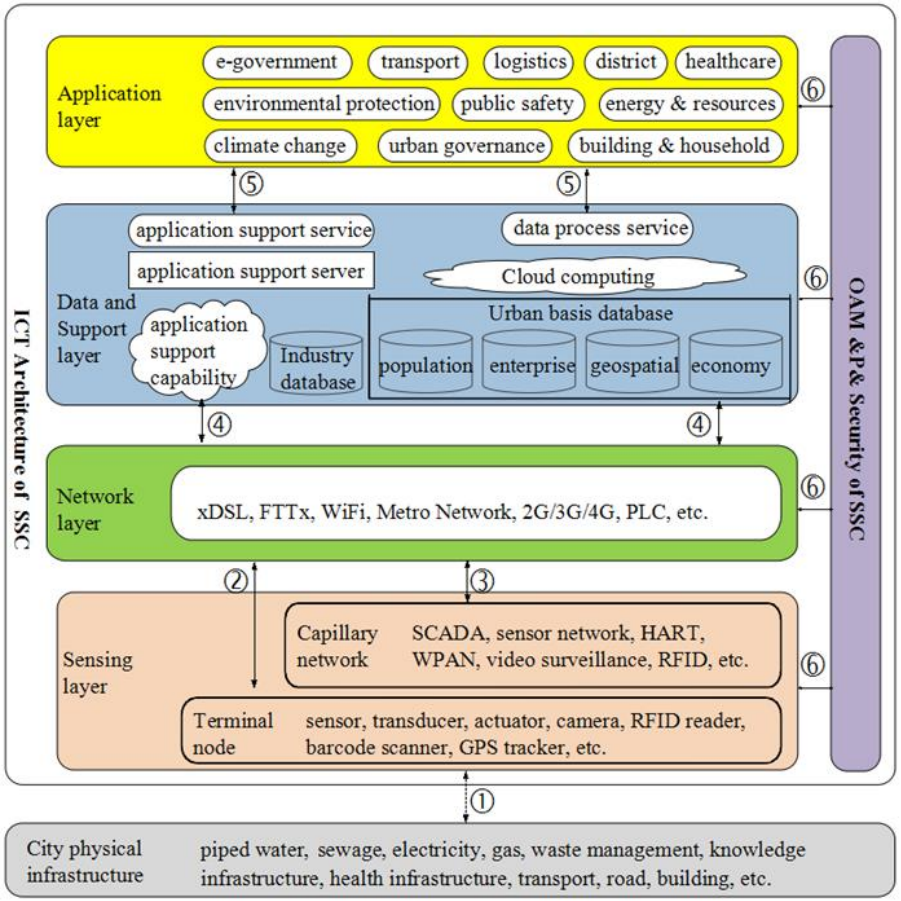
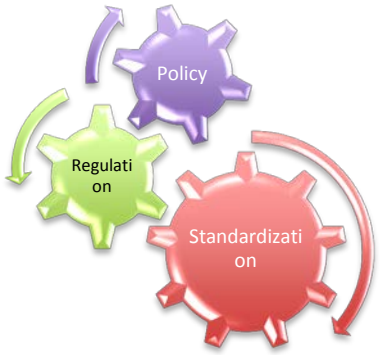


Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

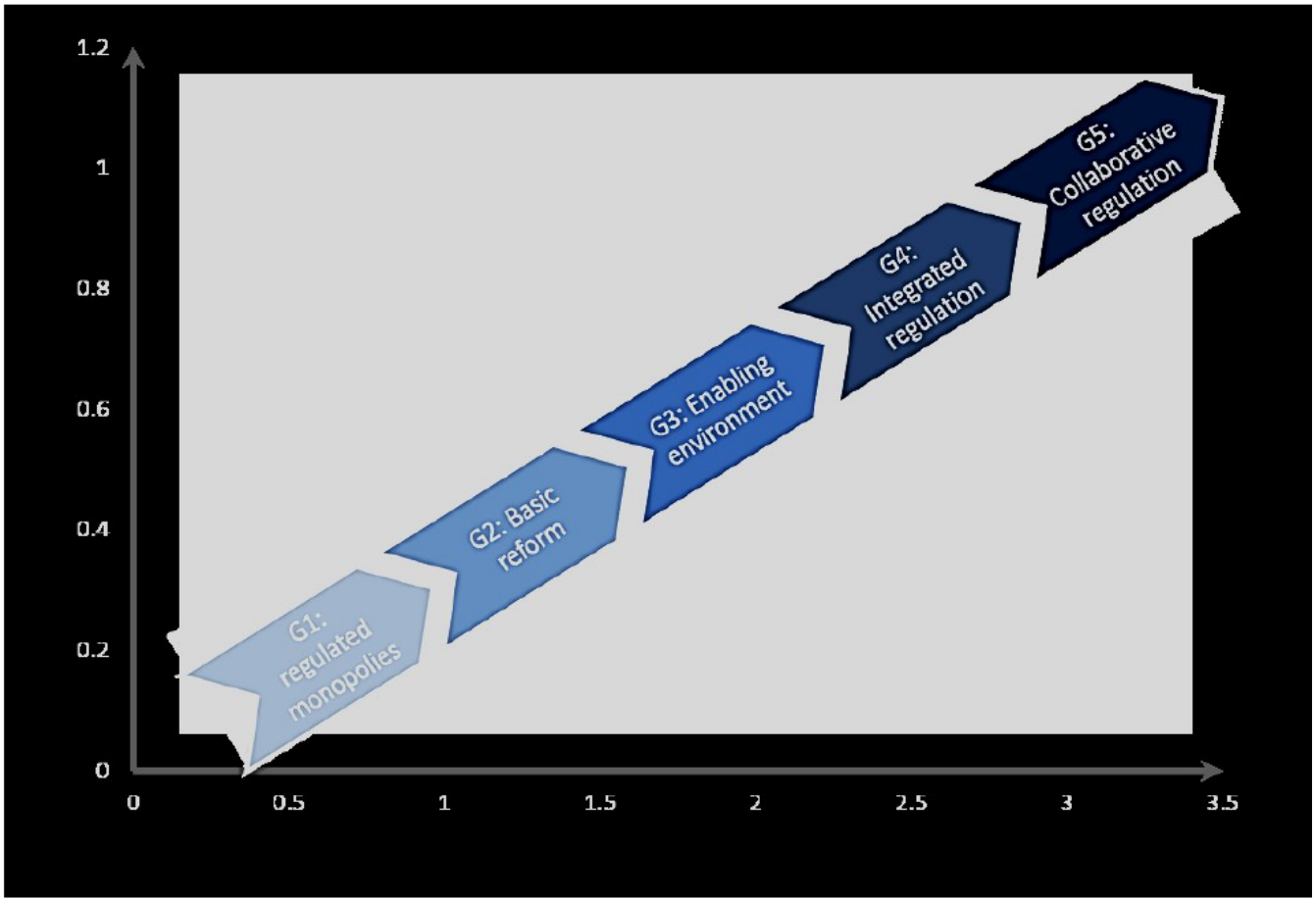
A multi-tier SSC (smart sustainable city) ICT architecture from communication view (physical perspective)

Telecom/ ICT Sector Issues (examples)



- Cross-Sector Collaboration
- Competition
- Investment
- Licensing
- Spectrum
- HetNets
- Broadband
- Cloud
- Roaming
- Interoperability
- QoS/QoE, Consumer
- Numbering & Addressing
- Big Data & Open Data
- Security
- Privacy
- Right of Way
- Green ICTs
- Infrastructure Sharing
- Data Centres
- e-Waste
- Number Portability
- Emergency Telecommunications

Evolution of ICT Regulation



Source: ITU

Different Services, Different Requirements - Examples

PPDR services

• **Constant availability** –

• **Ubiquitous coverage** – not just outdoors, but inside buildings (including large ferroconcrete structures such as shopping malls) and in tunnels (including subways).

• **Regionally harmonised spectrum** –

• **Differentiated priority classes** .

• **Support for dynamic talkgroups,**

• **Automatic identification with authentication.**

• **Automatic location discovery and tracking**

• **The ability to maintain connectivity**

• **Fast call setup** (<200ms) and immediate access on demand: the **Push-to-talk** (PTT)function and **all-calls** (internal broadcasts).

• **Relay capabilities**

• **Support for Air-Ground-Air (AGA) communication** when and where needed.

• **Adequate quality of service**

• **The ability to roam onto commercial networks**

•**Interworking between various PPDR services,** and increasingly, across borders.

Utility industry :

•**Teleprotection** – safeguarding infrastructure and isolating sections of the network during fault conditions whilst maintaining service in unaffected parts of the network.

•**Data monitoring** via SCADA (Supervisory, Control And Data Acquisition) systems.

•**Automation** – systems to autonomously restore service after an interruption or an unplanned situation.

• **Security** – systems to ensure the safety and security of plant.

• **Voice services** –.

• **Metering** – collecting data from smart meters and communicating with them for various reasons, such as demand management and to implement tariff changes.

• **Connectivity** – telecommunication networks to interconnect the above services in a reliable and resilient manner under all conditions.

• Other operational requirements include:

• **Coverage of all populated areas with points of presence throughout the service territory**

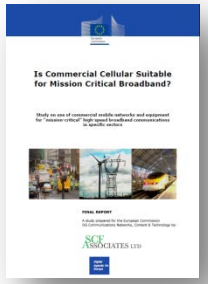
• **Costs must be low**

• **Continuity of service is vital,** and price stability

• **Utilities want network separation,**

Intelligent Transport Services… *and more*

ITU



What type of network is required to deliver Mission Critical services?

- Private networks
- Public networks

What preparations are required to make best use of commercial networks to deliver smart services (some of them such as Emergency Telecommunication, Utilities, Transportation critical in character)?

- Technical (e.g. coverage, resilience, quality, spectrum, interoperability)
- Commercial (e.g. availability, long term pricing, SLAs
- Policy & Regulatory (e.g. critical services as priority, quality of service, long term tariffs, security, privacy, USO, infrastructure sharing, licensing)

EXAMPLE – EUROPE

For IoT services to thrive several preconditions need to be fulfilled which relevant authorities

- Firstly, sufficient resources (like spectrum as well as numbers, IP addresses and other identifiers) in order to underpin and support the service
- Secondly, an EU Telecommunications Framework which fits to IoT services
- Thirdly, consumers' acceptance of IoT services, which depends among other things on the information provided to them about the level of privacy, network and data security and interoperability of services, devices and platforms.

Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016

SERVICE LICENSING ISSUES

- A large number of countries still have service specific licensing framework
- What type of telecom service does the IoT provides?
- What about services that are cross-sectoral in character? Licensed Vs Non-licensed services
- How and to whom do the rights and obligations apply? Licensees, Resellers, Others…?

		Number of countries/economies						
		Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Authorization type *	Unified / Global License	9	3	5	0	0	8	25
	Multi service	1	0	3	0	0	1	5
	Multiservice individual license	4	2	6	3	5	4	24
	Service-specific individual license	20	11	13	4	9	18	75
	General Authorization (Class License)	4	4	4	0	20	4	36
	License Exempt	2	1	1	0	1	0	5
	Simple notification	1	0	0	2	9	0	12
Remarks		11	4	9	1	21	13	59
Region size		44	21	40	12	43	35	195

* This indicator allows multiple choice per country/economy

Source: ITU World Telecommunication/ICT Regulatory Database

ITU ICT-Eye: http://www.itu.int/icteye

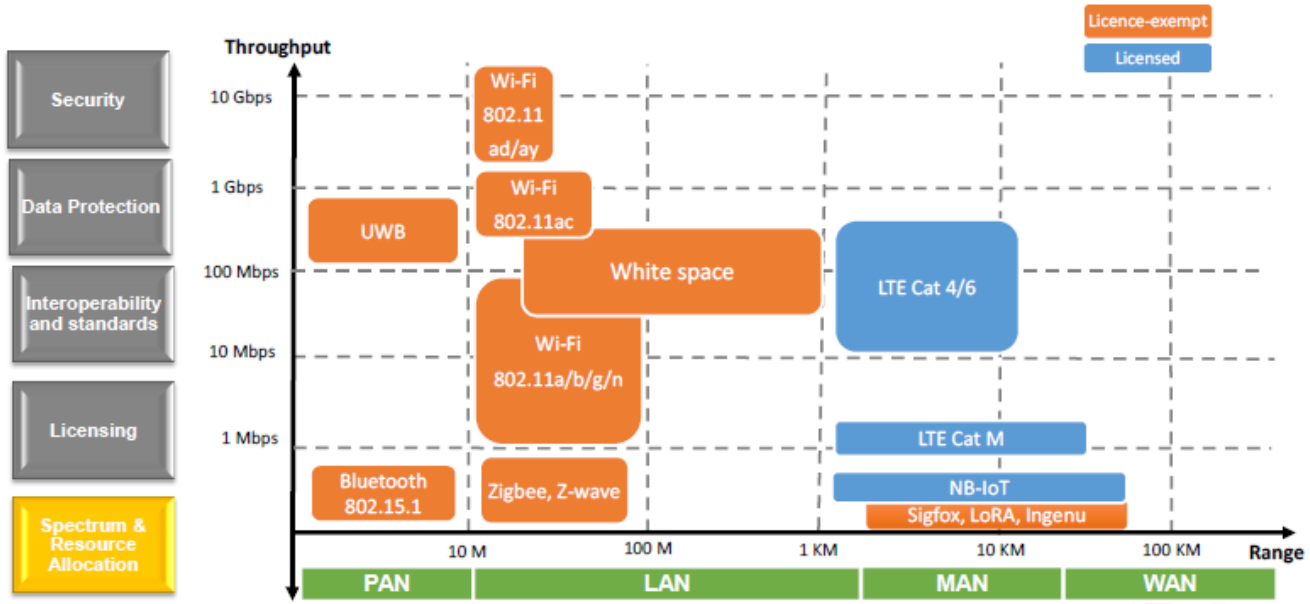
SPECTRUM ISSUES

- Traffic and spectrum availability
- Licensing (Allocation method, terms and conditions, technology aspects, license period)
- Technical (Low range, high
- Energy Efficiency (e.g. Battery Life)
- Commercial

Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016,

Maintaining flexibility to ensure IoT devices can be supported with sufficient spectrum

- Currently unclear whether majority of IoT devices are going to ride on licensed or licence-exempt spectrum as well as type of devices

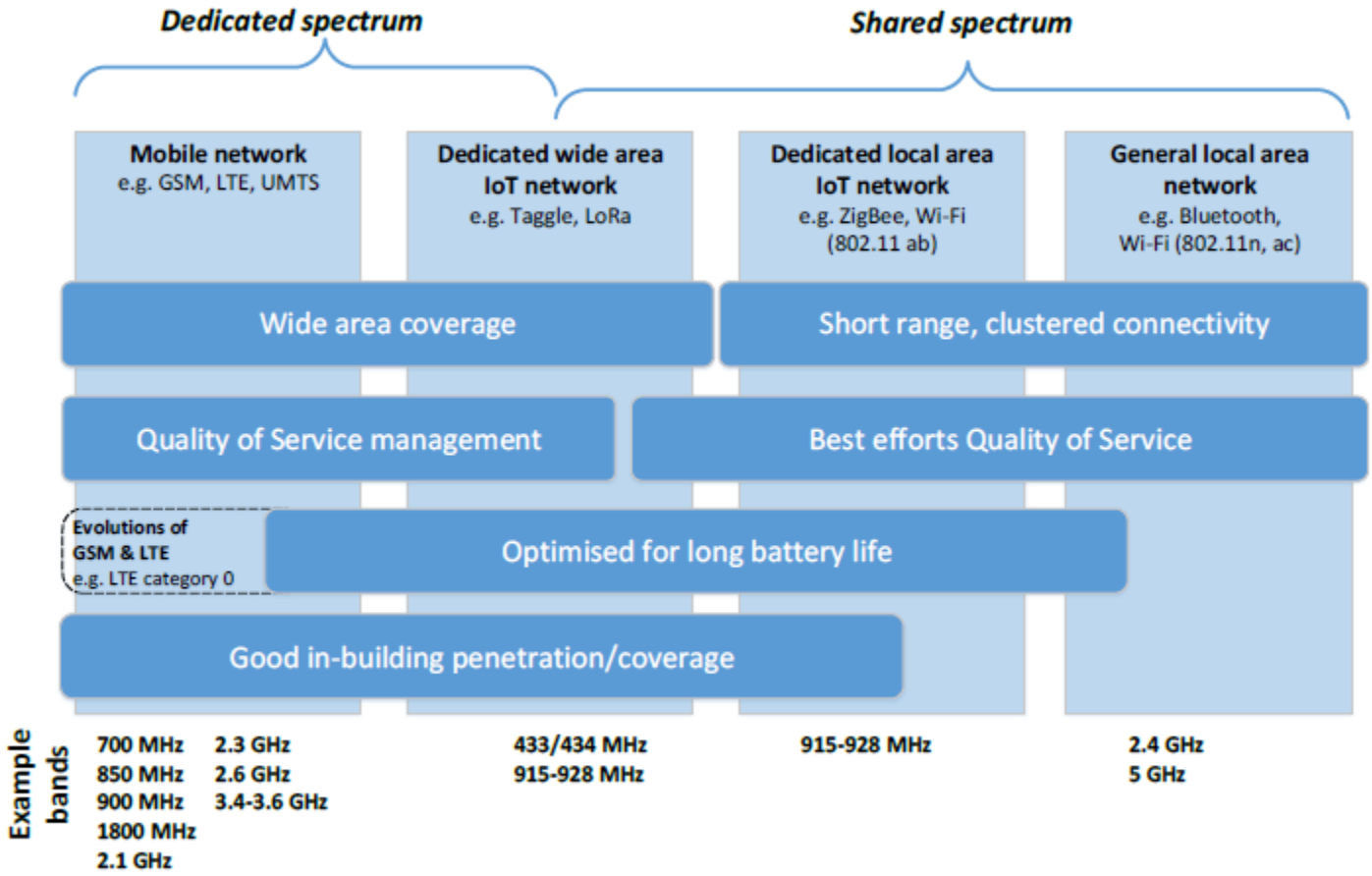


iDA SINGAPORE

ITU ACADEMY

Australia

Figure 2: Spectrum identified for IoT applications



Source: ACMA, based on Ofcom model 2015, updated for Australian spectrum band plans.

Source: The Internet of Things and the ACMA's areas of focus Emerging issues in media and communications Occasional paper, Nov 2015

NUMBERING , ADDRESSING AND NUMBER PORTABILITY ISSUES

- Public Numbers
  - National E.164 numbers;
  - International/global E.164 numbers assigned by the ITU;
  - National E.212 IMSI (International Mobile Subscriber Identity);
  - International/global E.212 IMSI with MNCs under MCC40 901 assigned by the ITU.
- Eligibility to receive MNCs
- Sufficiency of numbering resources
- IP addresses (IPv4 to IPv6 transition)
- MAC addresses
- How to switch the IoT devices when changing operators?
- OTA (Over-the-air) programming of SIMs

Source: BEREC **Report "Enabling the Internet of Things"**12 February 2016,

PRIVACY AND SECURITY ISSUES

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

Open data and APIs	IoT data is often held in “silos” that are difficult to integrate without time-consuming data discovery and licensing. IoT platforms can be industry and vendor-specific, limiting opportunities for SMEs and startups to participate.	City and country initiatives to provide for the sharing of information by individuals and organizations under non-proprietary, open source licences.	Further work to encourage cataloguing of and contributions to open datasets. National and local government authorities are in a key position to do this, and could collaborate through Open Government Partnership.

Figure 10– GSMA IoT Privacy by Design Decision Tree

PRIVACY AND SECURITY ISSUES: Potential regulatory measures

R&D on more hardware and software security and privacy mechanisms for resource-constrained IoT systems, particularly targeted towards start-ups and individual entrepreneurs that lack resources to easily develop this functionality.

Incentives for companies to develop new mechanisms to improve transparency of IoT personal data use, and for gaining informed consent from individuals concerned when sensitive data is gathered or inferences drawn.

Greater use of Privacy Impact Assessments by organisations building and configuring IoT systems.

Development of further guidance from global privacy regulators on application of the principles of data minimisation and purpose limitation in IoT systems.

More cooperation between telecoms and other regulators such as privacy/data protection agencies.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015**

Security and privacy protection capabilities

- The security and privacy protection group includes communication security capability, data management security capability, service provision security capability, security integration capability, mutual authentication and authorization capability, and security audit capability.
- Communication security capability involves the abilities of supporting secure, trusted and privacy-protected communication [C-7-1].
- Data management security capability involves the abilities of providing secure, trusted and privacy-protected data management [C-7-2].
- Service provision security capability involves the abilities of providing secure, trusted and privacy-protected service provision [C-7-3].
- Security integration capability involves the abilities of integrating different security policies and techniques related to the variety of IoT functional components [C-7-4].
- Mutual authentication and authorization capability involves the abilities of authenticating and authorizing each other before a device accesses the IoT based on predefined security policies [C-7-5].
- Security audit capability involves the abilities of monitoring any data access or attempt to access IoT applications in a fully transparent, traceable and reproducible way based on appropriate regulation and laws [C-7-6].

NOTE – These security and privacy protection capabilities include also the ability of coping with the security and privacy protection issues for operations across different domains.

Source: Recommendation ITU-T Y.4401/Y.2068 (03/2015))

Please refer Annex A Recommendation ITU-T Y.4401/Y.2068 for the IoT capabilities list

INTEROPERABILITY AND STANDARDS

- IoTs have both public and proprietary standards currently
- Standardization is important for Interoperability, reducing costs and barriers to entry
  - ITU-T SG 20 (IOT and Smart Cities, Smart Communities)
  - National Standardization bodies
  - International Standardization bodies
- How to coordinate interoperability amongst public and private sector entities?

  e.g. parking meters, thermostats, cardiac monitors, tires, roads, car components, supermarket shelves
- Cross-sectoral collaboration is very important as IoT are deployed in multiple sectors

INTEROPERABILITY AND STANDARDS

Standards (from the ITU and other organisations)	Technical standards have evolved for different applications and stakeholders, so harder to make them coherent. Smaller national markets may lack scale to support development of local IoT solutions, unless they are built on international standards. Specific software often needed per-system, increasing user load. Premature standardisation can constrain innovation; but partial or late standardisation can create industry coordination problems and fragmented technology options.	ITU has Global Standards Initiative to develop IoT standards and provide "umbrella" for other standards organisations. Wider-focus IoT and application-specific standards groups and frameworks.	Further cooperation between key standards bodies such as ITU, IEEE, IETF, IoT-specific standards organisations, and industry groups such as GSMA. Governments can encourage further standardisation through standards body participation (already prioritised in China, Korea and India), R&D funding and procurement policies. Development of common user interface mechanisms, especially via web browsers.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015, Prof. Ian Brown**

COMPETITION ISSUES

- Licensed Vs Non Licensed services
- Area of license
- OTT
- Net Neutrality
- Infrastructure sharing
- Access to data and open IOT platforms
- Data analytics
- Customer lock-in
- Mobile data roaming
- Consumer protection
- Quality of Service

COST AND RELIABILITY

Due to the immature and fragmented markets for many IoT services, which increase development and operational costs, a Korean government review found limited application of IoT e-government pilot projects, and a low rate of introduction of IoT services in small and medium-sized enterprises (SMEs). To encourage new businesses to develop and use IoT applications, a number of governments (including Korea, China, India and the UK) are supporting the development of IoT business incubators and innovation centres, which include platforms and testbeds for startups and SMEs. These can increase market entry and hence increase competition and reduce cost.

What?	Why?	What is done today/best practice	Possible way forward
Cost and reliability	Most tags and readers not yet cheap enough to be ubiquitous. Limited consumer use of QR codes, and perceived negative impact on aesthetics. Costs can be too high for adoption by SMEs. Very high reliability requirements in large-scale systems with thousands of tags and devices. Power sources are challenging for cheap but long-life sensors. Large investments needed to take full advantage of "smart city" systems.	Ongoing development and deployment of cheaper, more efficient and reliable hardware and protocols. Innovation centres in countries to stimulate market entry and competition. Public-private partnerships and cooperation between municipalities, businesses and contractors to reduce costs and share resources.	Standardised functions in smartphones to interact with tags and sensors, including via web browsers. Great attention to aesthetics of tags, such as dotless visual codes.[38] Further R&D in areas such as energy scavenging, low energy protocols and algorithms, and high-reliability systems.

Source: **GSR discussion paper Regulation and the Internet of Things, 2015, Prof. Ian Brown**

Collaboration Mechanisms

Emergency

Education

Health

Electricity

Governance

- Integrated Policy
- Legislation
- Co-Regulation
- Standardization (International / National)
- MoU or Cooperation Agreement
- Coordination Committee
- Projects, Coordination on Case to Case basis

Transport, Trade, Logistics

Water

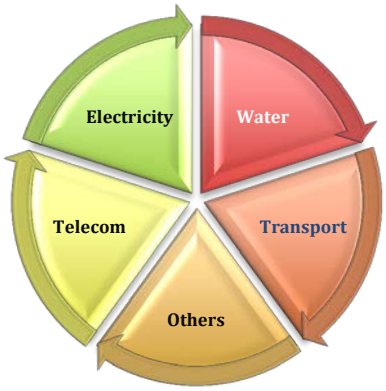
Teleworking

Infrastructure Security

SMART SOCIETY

REGULATORY COLLABORATION

Examples

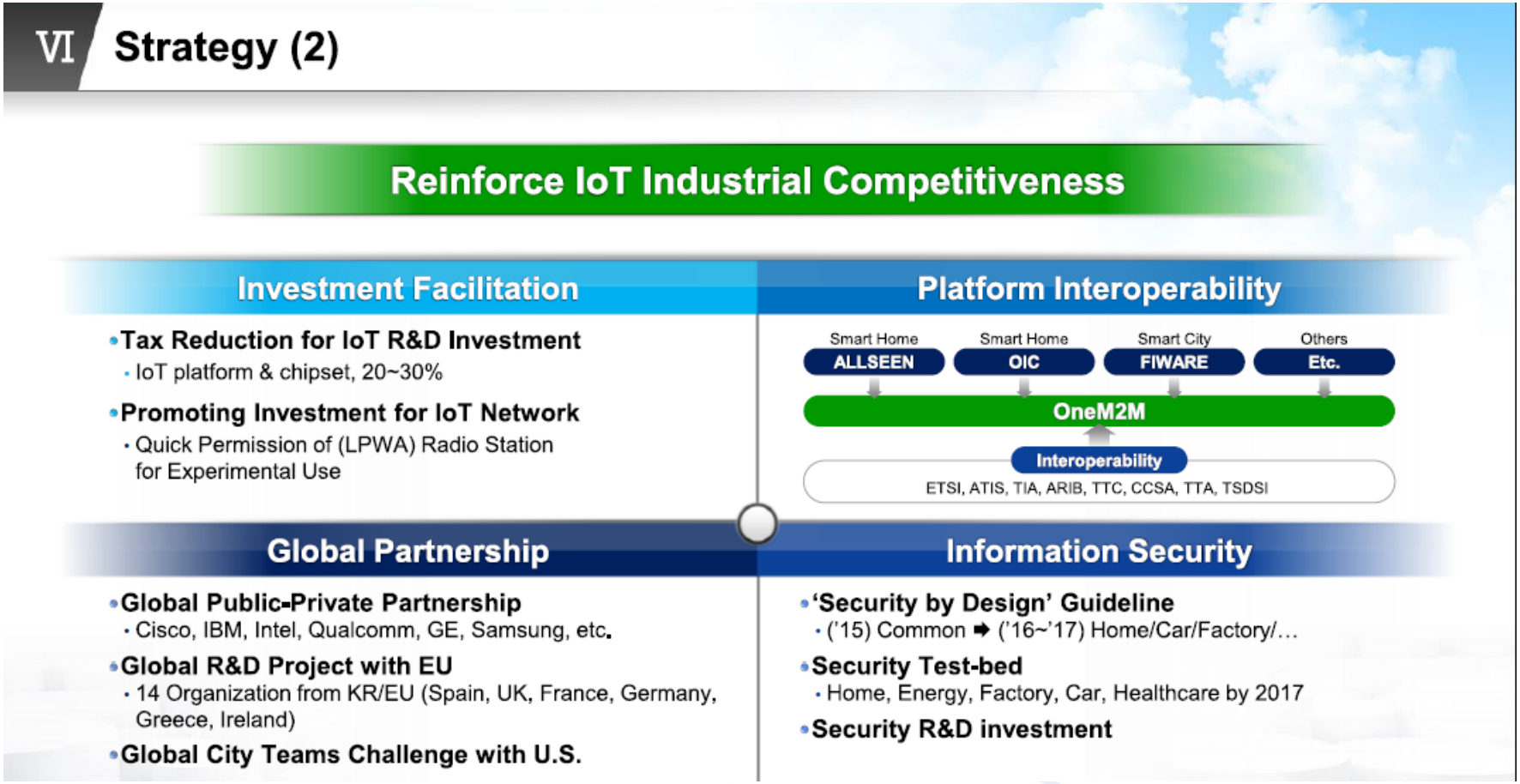


MULTI UTILITY REGULATOR

EXAMPLE: REPUBLIC OF KOREA

Source: Supporting growth of IoT, Presentation by Mr. Choi Jae-You, Vice Minister, MSIP, 23 Feb 2016

EXAMPLE: REPUBLIC OF KOREA



Source: Supporting growth of IoT, Presentation by Mr. Choi Jae-You, Vice Minister, MSIP, 23 Feb 2016

Thank You