Internet of Things: Policy and Regulatory Enablers

Annual Regional Human Capacity Building Workshop for Africa

"Developing the ICT ecosystem to harness IoT"

28-30 June 2017
Mon Trésor, Plaine Magnien, Mauritius

- **Technologies is evolving fast and changing very quickly. In ICT its very visible**

- **Enabling policies and regulations should promote innovation or risk to became a barrier.**

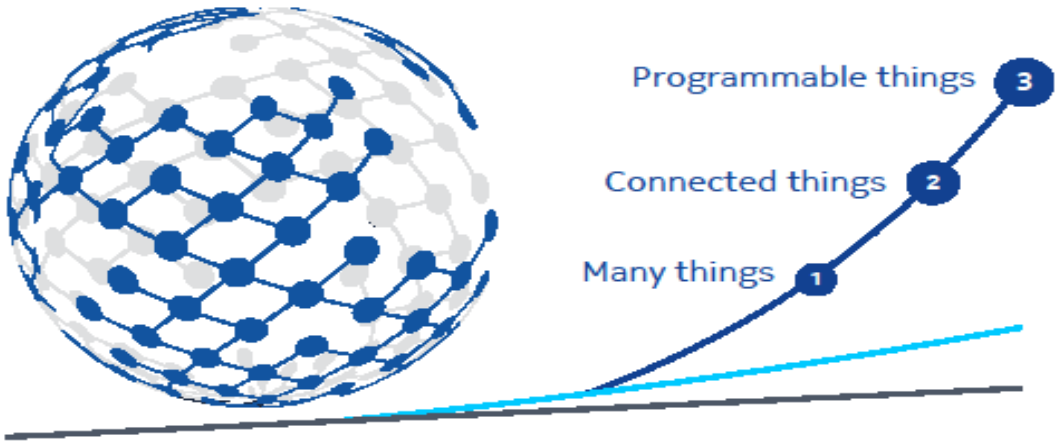
USE OF ICTs - TRENDS

- Virtually **every facet of modern life** – in business, culture or entertainment, at work and at home – **depends on information and communication technologies (ICTs). (from ITU vision 2020)**

- **More and more physical items and appliances that now have sensors and network links will increasingly be able to remotely share data about themselves, their users and their environments.**

IoTs

While the past has been about connecting people, the future is about connecting things



- Improving people's lives through automation, enhanced connectivity and intelligence
- Helping industries to become more efficient, agile and real-time

NOKIA

Internet of Things (IoT)

- Seen as a whole, this constitutes a shift from human-to-human (H2H) to machine-to-machine (M2M) and everything-to-everything communications.
- Companies and Consulting firms predict that tens of billions of IoT devices will be deployed with a total economic impact of trillions of Dolares.

ICTs are multi-sectoral


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

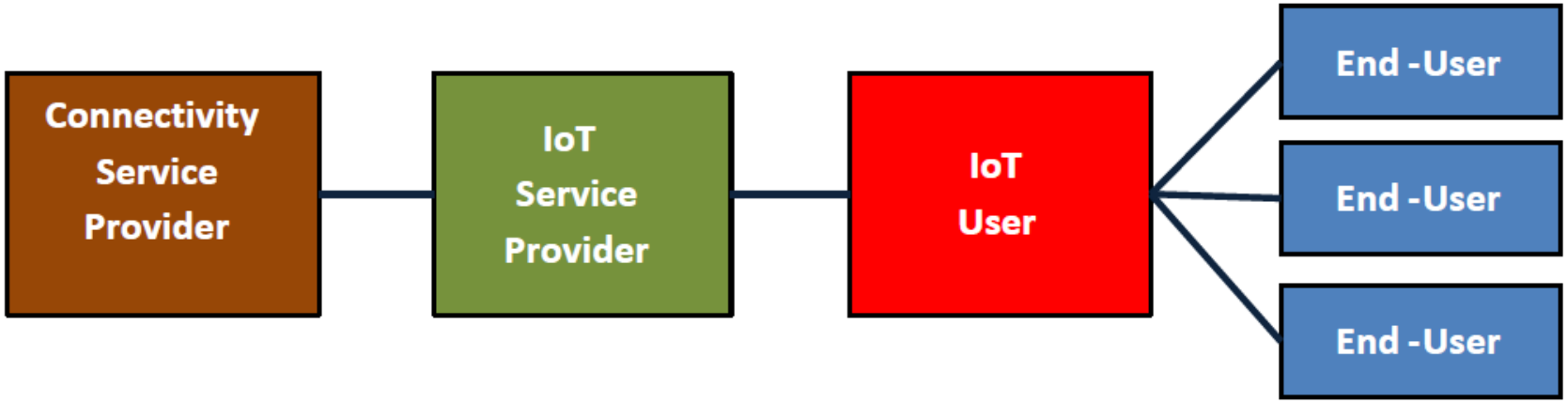

Digital Inclusion


Spectrum Management


Standards, Conformity & Interoperability


Finance

IOT Value Chain



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

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.

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.

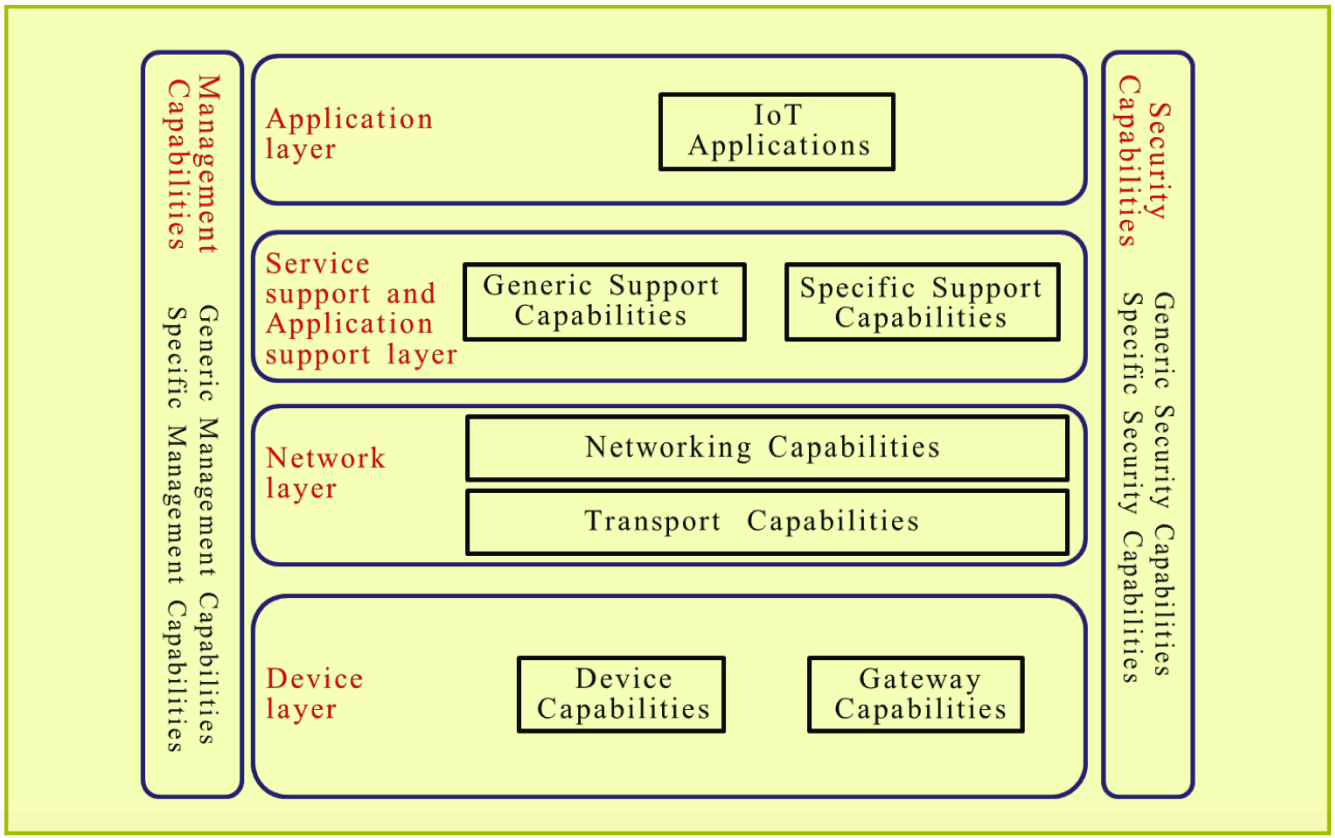
Source: Recommendation **ITU-T Y.2060**

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**

Emerging ICT Infrastructure and Policy and Regulatory issues

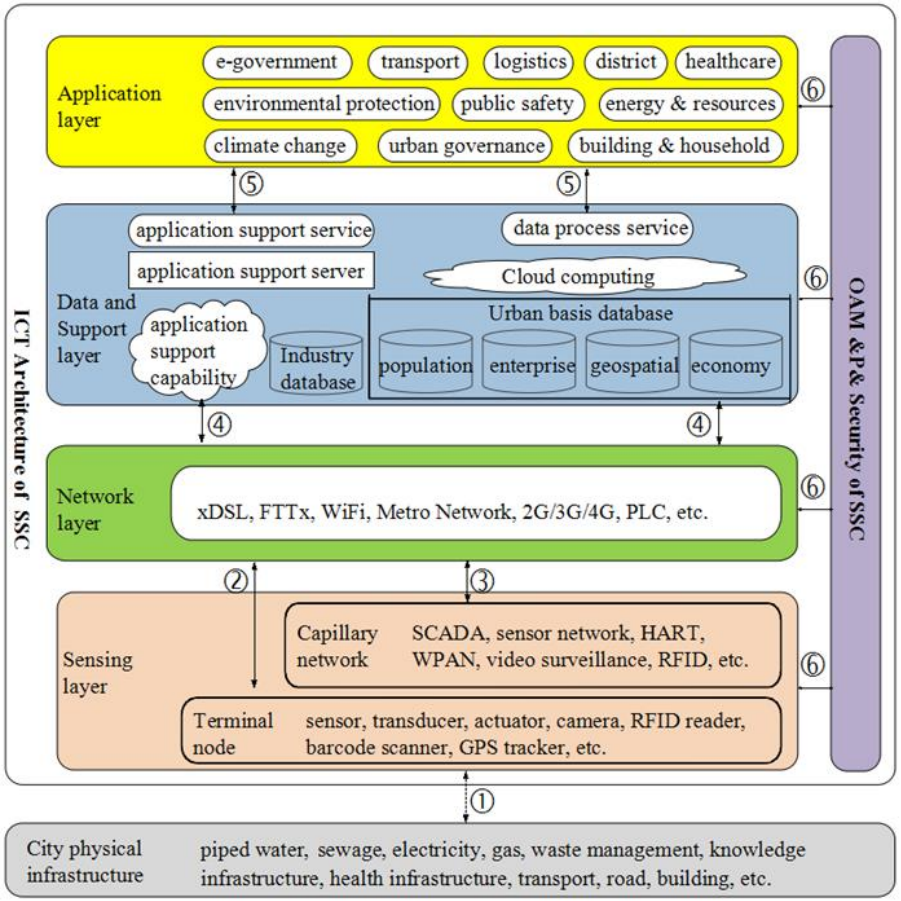
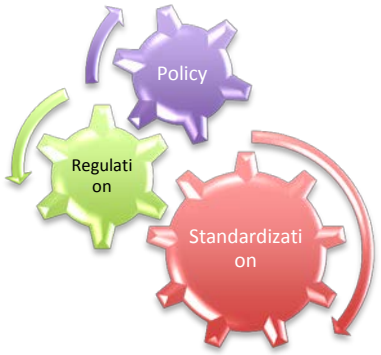


Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

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

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

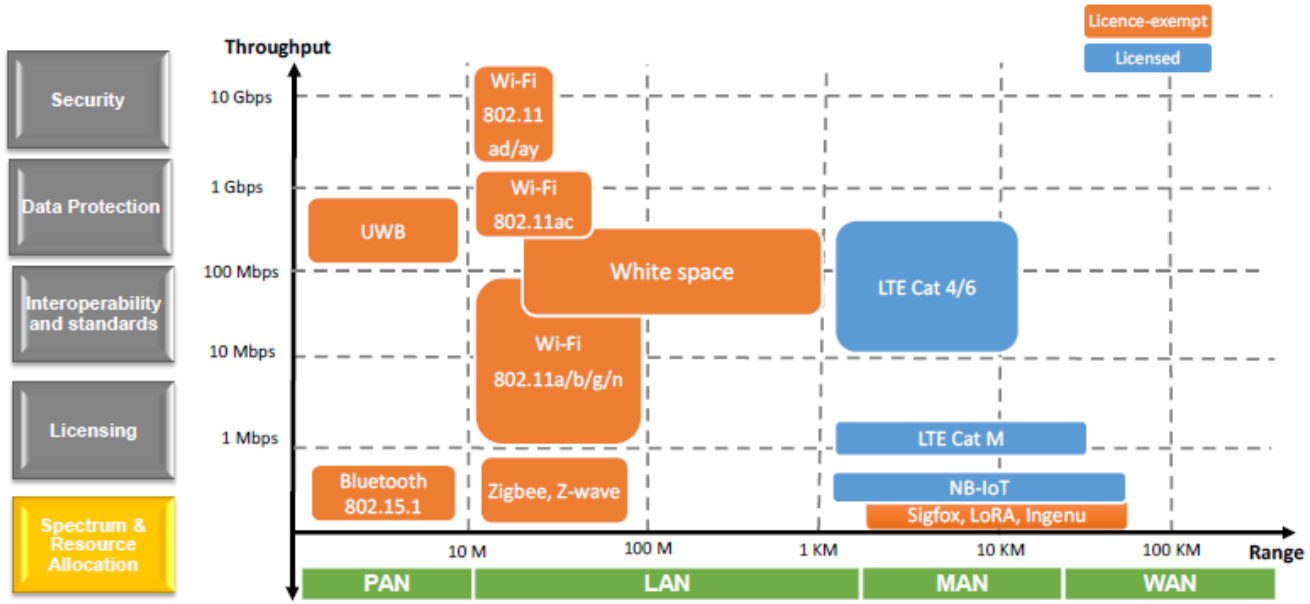
SPECTRUM ISSUES

- 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

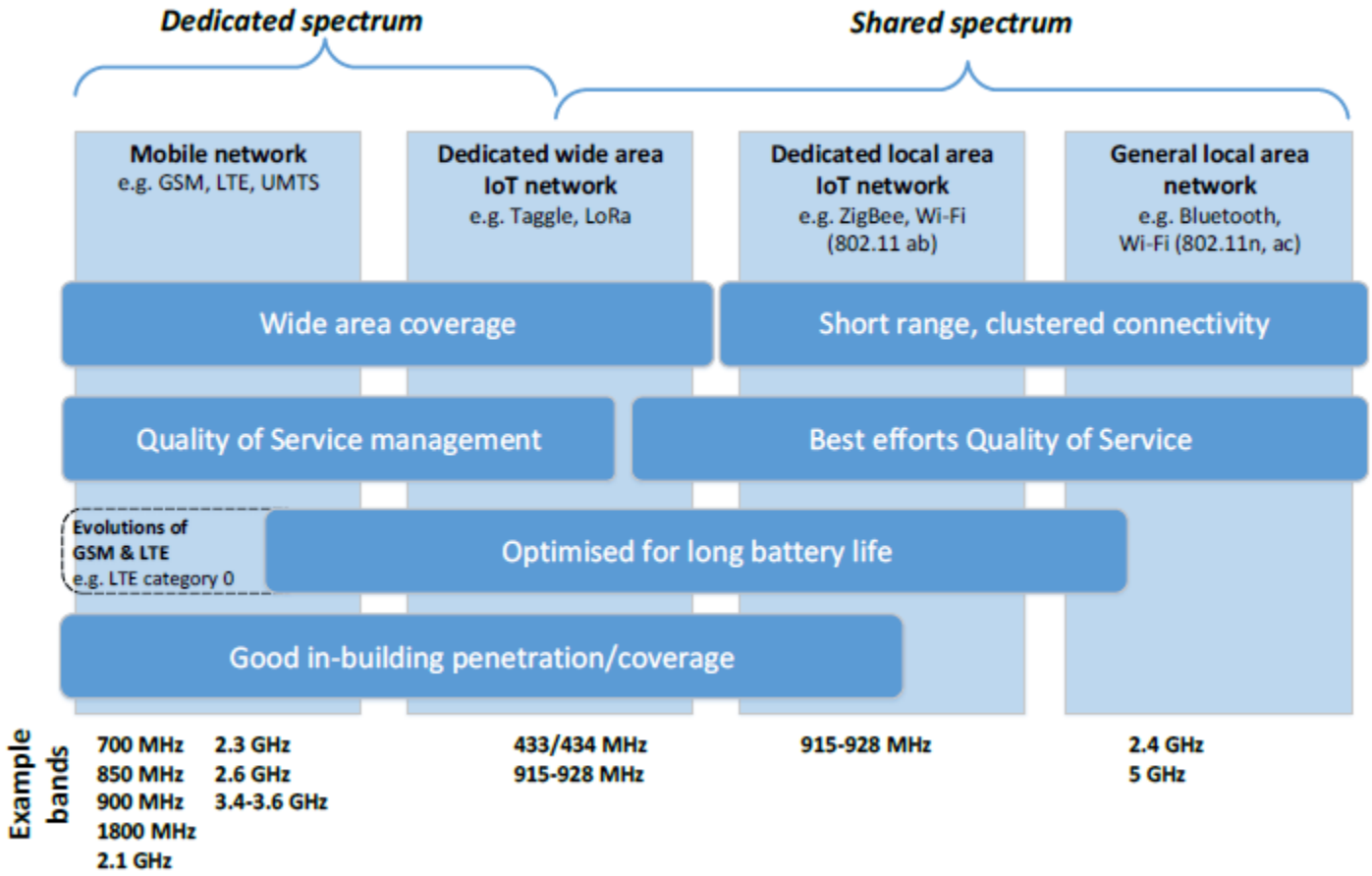


iDA SINGAPORE

ITU ACADEMY

Australia

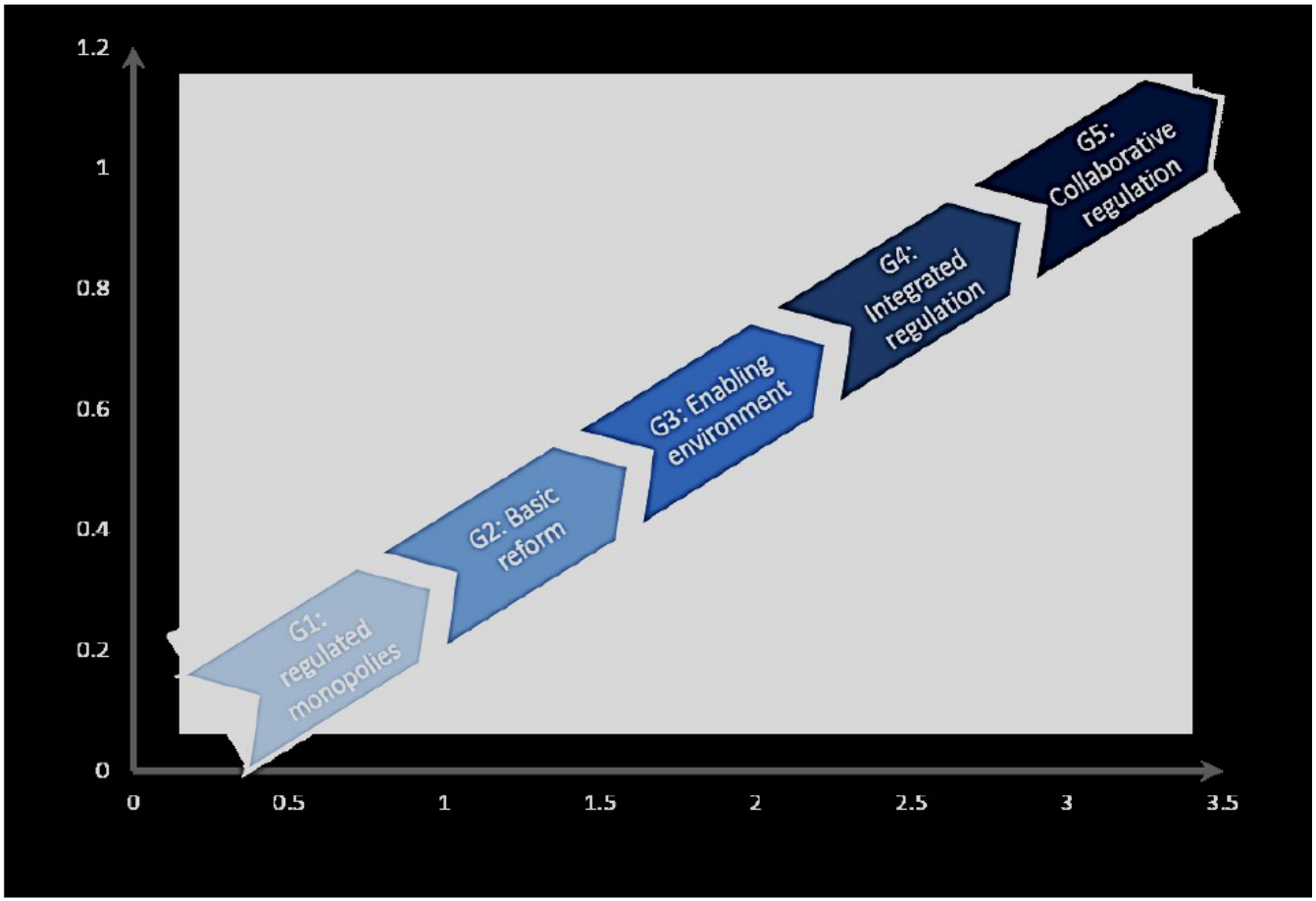
Figure 2: Spectrum identified for IoT applications



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

Evolution of ICT Regulation



Source: ITU

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

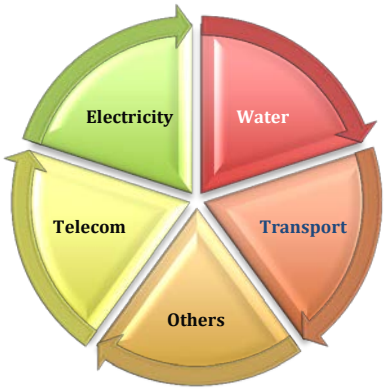
Teleworking

Infrastructure Security

SMART SOCIETY

REGULATORY COLLABORATION

Examples



MULTI UTILITY REGULATOR

Conclusion
IoT Key Policy Domains

Connectivity & Spectrum
Standardization
Net Neutrality
Data protection/ ownership/ location
Security
Digital Skills

Thank You