Session 7: Conformity and Interoperability of Internet of Things in the 4th Industrial Revolution

15 – 19 November, 2021

NATIONAL COMMUNICATIONS AUTHORITY

Roland Kudozia & Isaac Laryea

OBJECTIVE:

ENHANCE CAPACITY, FOCUSING ON INTERNATIONAL ISSUES RELATED TO THE C&I REGIMES.

Outline

Introduction to Internet of Things

- Characteristics of IoT
- Categories of IoT Services/Applications

Introduction to Machine to Machine

- What is M2M
- Difference between M2M and IoT

Diffferences between IoT and M2M

Infrastructure

Networking Technologies and Protocols

Role of the Regulator

Conformity and Interoperability of Internet of Things

Benefits of Conformity and Interoperability of IoT

Need for Standardization of Internet of Things

IoT Interoperability Testing

Use Cases

Business Application Model

Introduction to Internet of Things (IoT)

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

The IoT defines new dimension to the ICT world, called “any-thing communication”, in parallel with “any-time communication” and “any-where communication”

The IoT is connecting people, places and devices at a rapid pace. By Qualcomm

IoT is a global infrastructure for the information society enabling advanced services by interconnection of different physical and virtual things, based on ICTs (Information and Communication Technologies). (ITU-T Recommendation Y.2069)

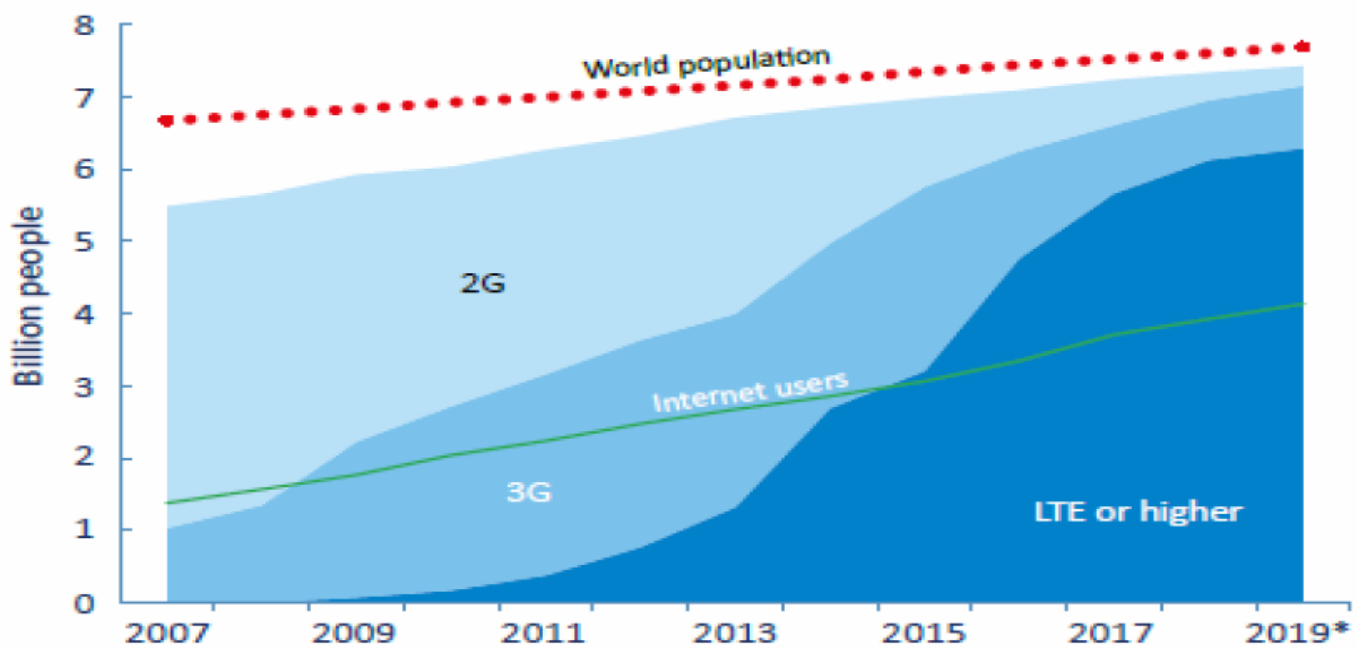
Introduction to Internet of Things (IoT)

Study Group 20 is working to address the standardization requirements of Internet of Things (IoT) technologies, with an initial focus on IoT applications in smart cities and communities (SC&C).

Smart city standardization at the ITU level to allow devices to interconnect with each other

IoT is contributing to the convergence of industry sectors, and SG20 provides the specialized IoT standardization platform necessary for this convergence to rest on a cohesive set of international standards.

Introduction to Internet of Things (IoT)



Source: ITU

The growth of IoT is driven by widespread use of Internet and IP technologies and availability of fixed and mobile access networks everywhere.

Growth is also propelled by the evolution of network technologies coupled with the heterogeneous design.

Characteristics of IoT

Categories of IoT Services/Applications

Massive IoT

IoT services based on low cost, low energy consumption, small data volumes generated or transferred etc.

Applications : includes capillary sensor networks, smart city, smart agriculture, smart metering, tracking and fleet management devices, smart buildings etc

Requirements: tolerant to packet losses, delays, low bitrates, no strict Qos requirements

Critical IoT

IoT services which require ultra reliable, very low latency and very high availability.

Applications: remote manufacturing, remote surgery, smart grids, traffic safety and control, distance healthcare

Requirements : strict QoS, best effort internet network, network neutrality, managed IP networks with QoS guarantees

Concerns of IoT

Challenges Impacts on IoT devices and services

- Security Policy
- Data Privacy & Protection
- Firmware Malfunction
- Disruption in IoT services
- Network Challenges
- …

=

Impact on use of critical IoT applications

Impacts on critical infrastructure

- Distributed denial of service attacks
- Distributed cyber-physical attacks
- …

What is Machine to Machine (M2M)

- Machine to machine (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.
- M2M is about communication among machines without (or only limited) human intervention
- Often used for remote monitoring
- It forms the basis for the concept of Internet of Things (IoT).

Characteristics of M2M

- **Time Restrictions:** Data can only be sent or received during defined periods of time.
- **Time Tolerance:** It is possible that data transport will be delayed.
- **Monitoring:** This feature is intended to provide the capabilities of detecting and reporting on events.
- **Triggering an M2M device in a certain location:** Triggering an M2M device inside a predetermined area.
- **Low power consumption:** The system is capable of providing efficient service to M2M systems.

Building Blocks of M2M

- The fundamental blocks of M2M can be summarized as the process of connecting a physical device to the communication hardware.

- To comprehend the more general notion of M2M and its application possibilities, it is necessary to first comprehend the crucial functions played by each of these six (6) pillars of M2M.

RFID	Network Sensors	Telemetry	Smart Device	Telematics	Remote Monitoring
Radiofrequency Identification' deals with the identification and tracking of objects in the electromagnetic field	Sensor network contains some connected devices and a wireless connection used to monitor the readings of the connected sensors	It is a wireless technology, used to automatically transfer & record data obtained from connected devices on a remote system	Intelligent devices that reduces human effort and makes smart decisions, along with human thinking to complete a specific task.	Deals with long-distance information transmission. It is also used for computing any far-reaching communication system along with the transmission.	Allows us to access multiple connected devices from a remote location by connected devices and software to create a system to control large-scale automation

Obtaining the best business results, achieving automation

Drawbacks of M2M communication

- The security of large-scale data collection and the collection of sensitive information are major concerns.
- The software and hardware were created and optimized to be utilized by a limited number of linked devices.
- Interoperability between cloud and Internet of Things devices in such networks is frequently restricted.
- The use of cloud computing in M2M creates a reliance on others.
  -may limit the ability to innovate and adapt quickly.
- M2M communication requires a consistent network connection with a reasonable speed. In order to function properly

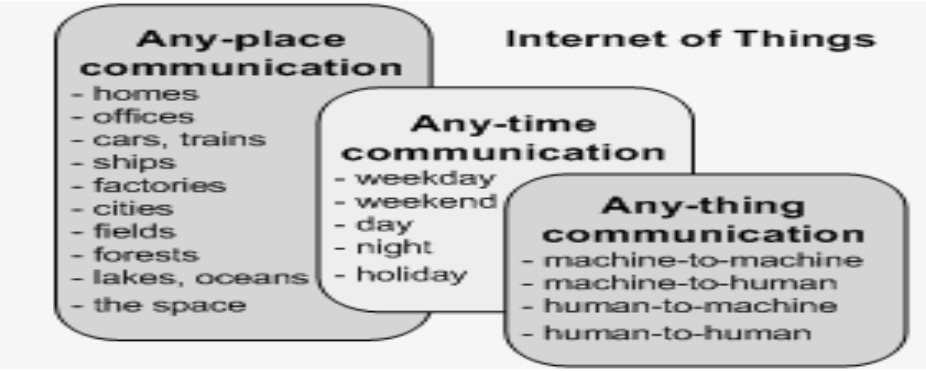
Security Issues Affecting M2M

Before developing an M2M communication system, it is necessary to address a number of risk considerations, including privacy, fraud, the exposure of critical applications, as well as the physical security of the devices.

- Ensuring that machines and gadgets are resistant to tampering
- Integrating security elements into all of the equipment that are connected
- Encrypting all communication between devices and safeguarding back-end services are important.
- The segmentation of M2M devices onto individual networks, as well as the management of device identity and availability.

M2M systems are similar to those affecting any other communication system, and can range from network infiltration to physical device hacking

Differences between M2M and IoT



- The IoT refers **to any communication** between **machines** and **objects** over **Internet**. Such technologies include (but are not limited to) Radio Frequency Identification (RFID) wireless sensor networks and Machine-to-Machine (M2M) communications.

- Both terms relate to the **communication of connected devices**.
  - -M2M systems are often isolated, stand-alone networked equipment.
  - -IoT systems take M2M to the next level, bringing together different systems into one large, connected ecosystem.

M2M and IoT are not the same. IoT needs M2M, but M2M does not need IoT.

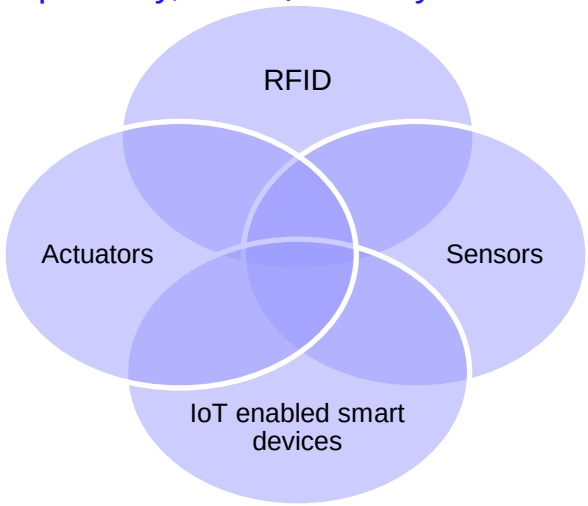
Infrastructure

- Service Perspective
  - QoS, health & safety, security etc
- Network Perspective
  - Heterogeneous, reliability, etc
- Device Perspective
  - Compatibility, interoperability

Infrastructure

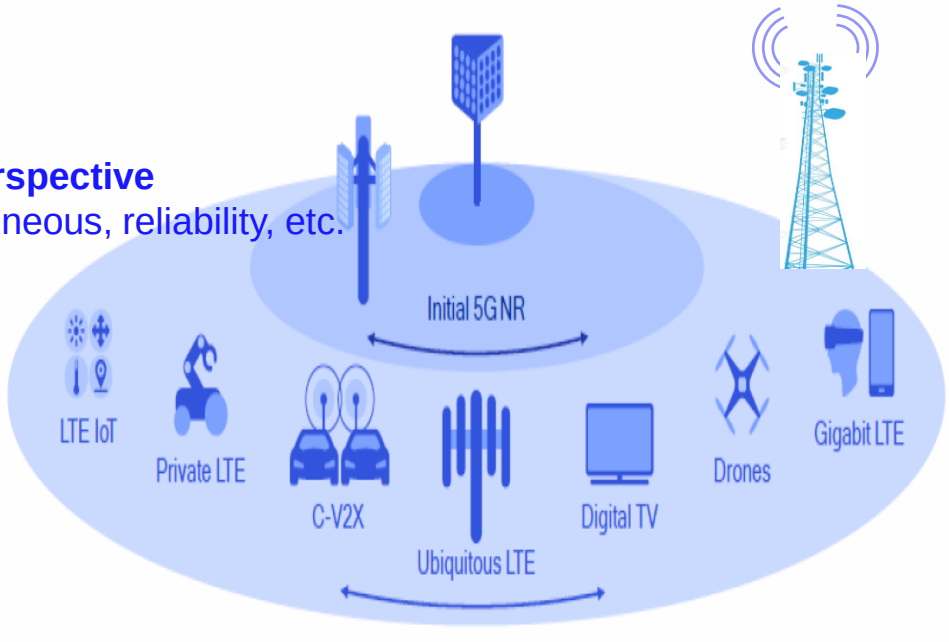
Device Perspective

✓ Compatibility, interoperability



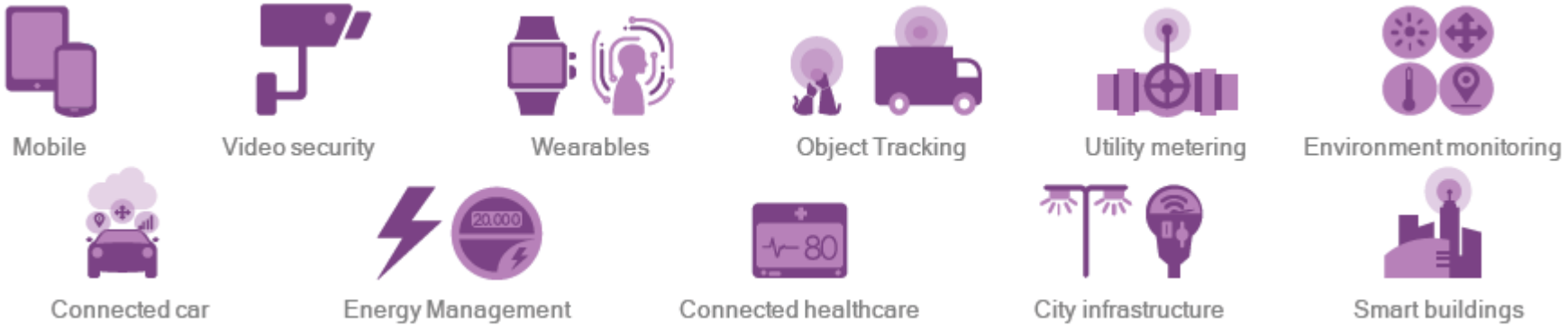
Network Perspective

✓ Heterogeneous, reliability, etc.



Service Perspective

✓ QoS, health & safety, security etc



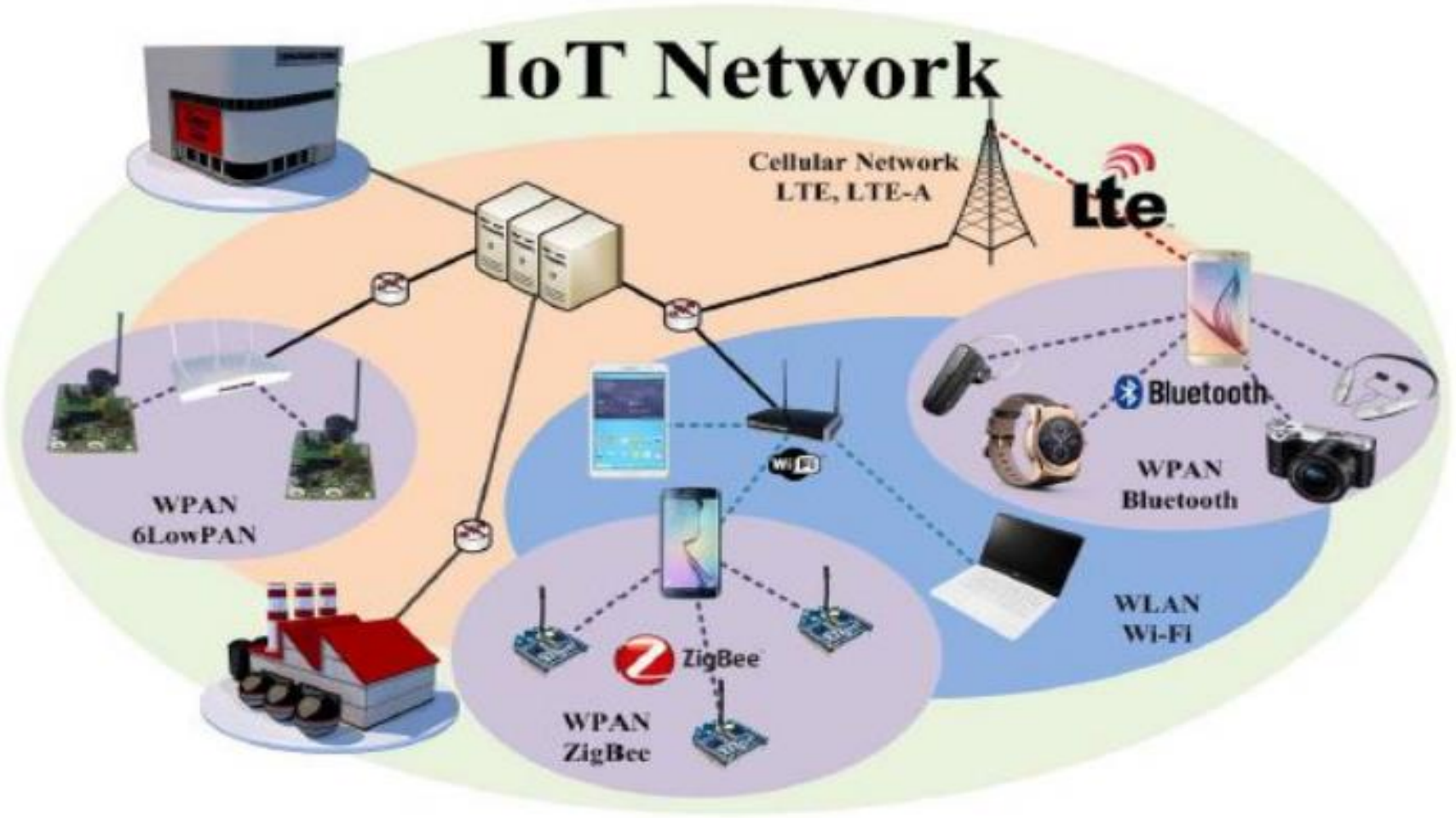
Networking Technologies and Protocols

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

- Connection of IoT devices via Wi-Fi, Bluetooth, Mobile Devices, Cellular Network Technologies (2G,3G,4G,5G),specialized Radio Networks (LTE, LTE-A, LTE-PRO, NR, etc), Global Internet, Network Naming and Addressing Protocols (IPV4 & IPV6), Numbering, etc

- M2M systems use **point-to-point** communications between machines, sensors and hardware over cellular or wired networks, while IoT systems rely on IP-based networks to send data collected from IoT-connected devices to gateways, the cloud or **middleware** platforms.

Networking Technologies and Protocols



In your view, how should the C&I process for IoT/M2M be, considering the issues discussed?

In our view/opinion, We think the following needs to be considered in the C&I of IoT Devices;

- Additional steps should be added to the existing type approval regime to make it more fit for purpose and robust as long as IoT is concerned.
  - ✓ Cybersecurity awareness

- Need for regulators to come up with certain framework to ensure service providers meet the minimum requirements in terms of the application layer
  - ✓ Type of software
  - ✓ Data protection issues
  - ✓ Classification of firmware installed on IoT devices according to their security levels, usability, scores, etc
  - ✓ Levels of checks of conformity for massive IoT should not be the same as critical IoT.

- Strict Data Protection policies between the regulator and the agencies responsible for data protection as well as the cybersecurity agency.

- Strong collaboration between tax agencies to control and avoid unnecessary cost and bottleneck to the process of C&I regulation. This may increase the cost of IoT devices on the market

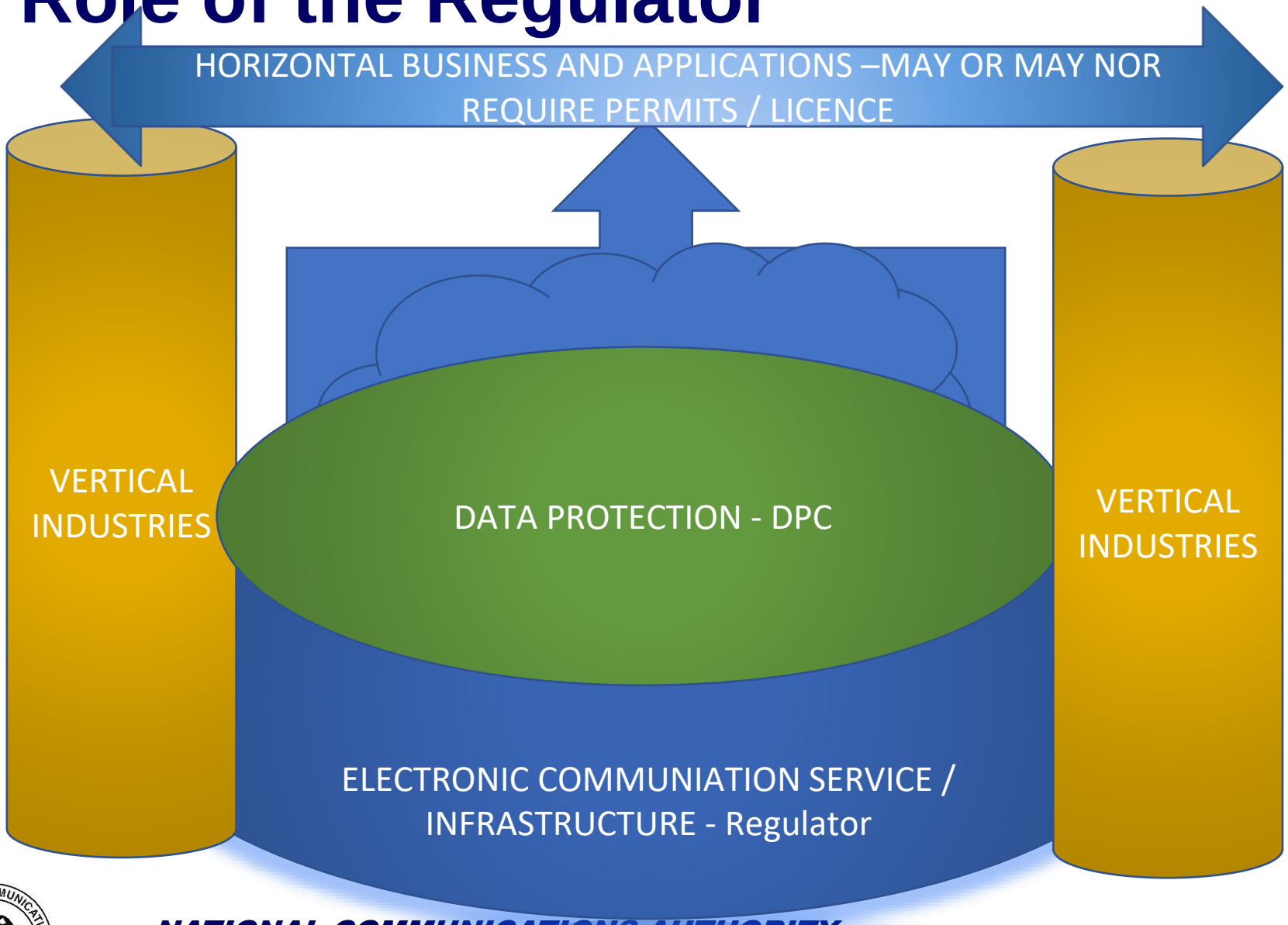
Role of the Regulator

Do we need to act any differently?

Things to consider

- Policy Direction
- Data Security and Privacy issues
- Revamp Regulatory Framework
- Network Security and Resilience
- IoT/M2M Standards Development
- Legal Framework
- Reconsider Resource Requirement & Allocation
  - Numbering
  - Spectrum Resource
  - Role of VAS licensees

Role of the Regulator



Regulatory Aspects

Set Ground Rules

- Manufacturers, Dealers or Authorized Agents of Electronic Communication Equipment (ECE) require Authorisation and Dealership before they can sell ECE's.

- The Authorised Equipment come with Authorisation Certificate (Type Approval Certificate)

- Manufacturers, Dealers or Authorized Agents must be informed prior to the importation of any ECE into the country.

- Upon arrival of equipment, clearance including physical examination at the ports is required as part of the market surveillance activities.

- Cybersecurity framework and testing of devices due to firmware running on the background of the devices.

Regulatory Aspects cont.

Key Type Approval Activities

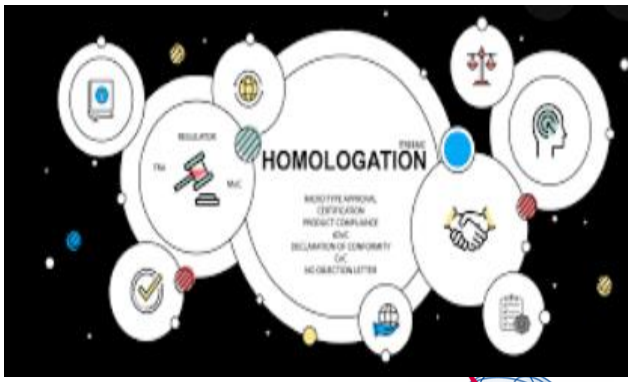
- Robust Type Approval Regulations or regime in place

  -Type Approval Administrative Framework and Guidelines

- Dealership Licensing for IoT terminal equipment

- IoT User Equipment Testing

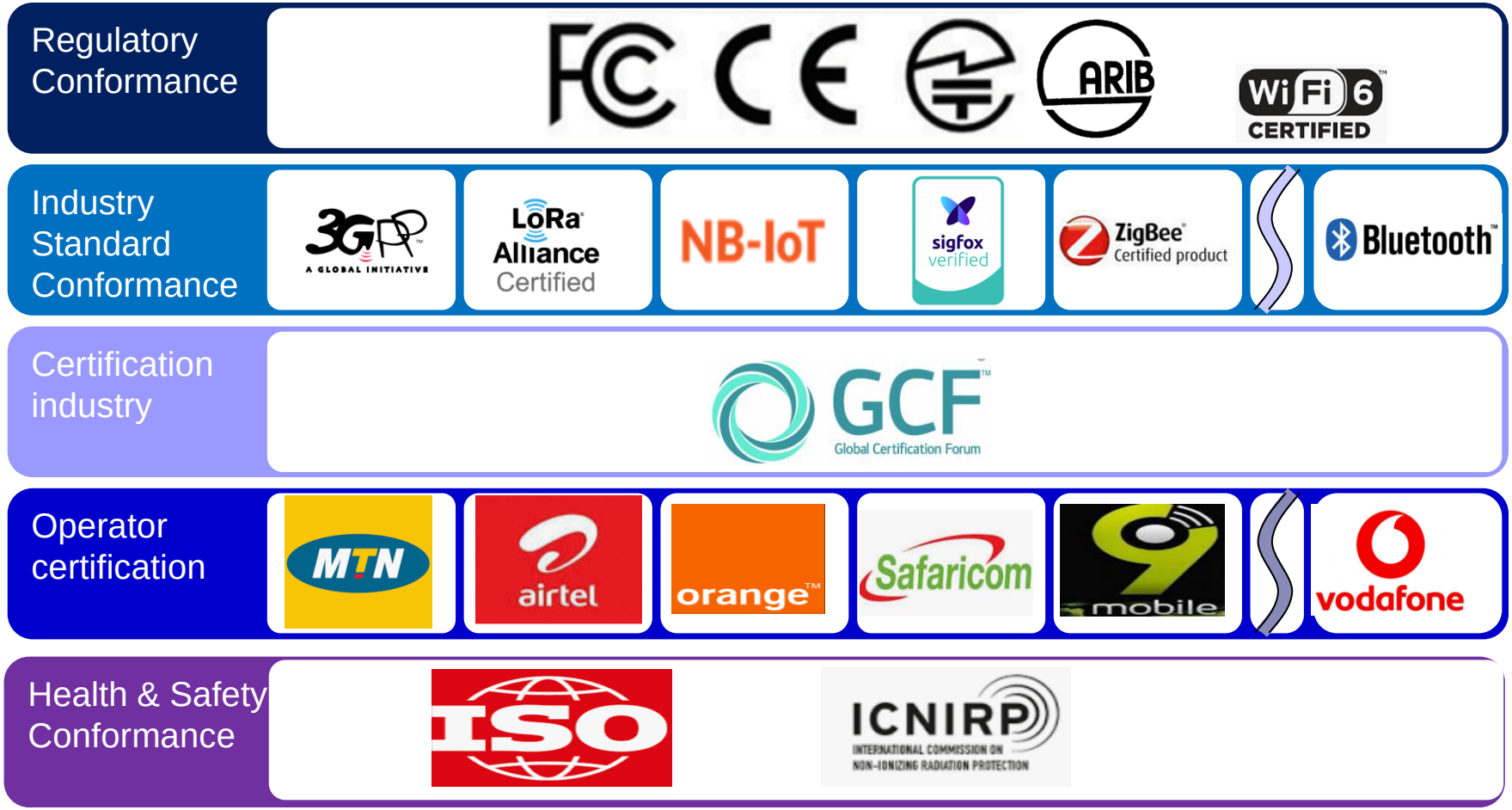
- Pre and Post Market Surveillance for IoT devices



Initial Implementation Roadmap

- Licensing
  - Need to License new operators or use existing ones
- Spectrum Requirements
  - Identification and Allocation of spectrum for use
- Regulatory Requirements
  - Need to revamp type approval regime
  - Network neutrality
- Legal Framework

Conformity and interoperability of IoT



Conformity and Interoperability of IoT

The minimum essential requirement are to meet the objectives of International Standards

Environmental Health And Safety Standards

Electromagnetic Radiation And Emissions

Radio Frequency Requirements

Network Compatibility

- Quality of Network Support
- Verification of Stated Technology support

Conformity and interoperability of IoT

- **Coexistence of multifarious Systems**
  - Devices/Sensors/Equipments/etc
- **Manufacturer-design of multi-version systems**
  - Application design
- **Introduction of new things with newer protocols**
- **Existence of low power devices**
  - Which needs to exchange data over lose in network (no likelihood of power recharge over a long period)
- **User Protection and Safety**
- **Electromagnetic Compatibility**
- Radio/RF aspects related with the efficient use of the allocated radio spectrum, without causing harmful radio interference

Benefits of Conformity and interoperability of IoT

- Device will be made to conform with certain requirements which will be safe for the users.
- Firmware and other security interfaces of devices may have to meet adopted standards before being passed for use.
- The user benefits because he can communicate with whom he wants or needs anywhere and anytime with a single terminal.
- The network operator benefits because it can select the best equipment from different manufacturers according to the best price and performance.
- The manufacturer benefits because it can sell the same equipment to different countries or operators and benefit from economies of scale in fabrication and marketing.

Need for Standardization

- To provide interoperability in the increasing demand for standardization and unification of standards (e.g. few standards supported by most of the devices).
- Ensures Conformance
- Scalability on the use of different components and protocols in a product or service
- Security and Reliability (prevents cyber attacks)
- To provide harmonized standards for IoT devices to allow the market to reach its full potential

Need for Standardisation

- **The IoT/M2M standards**

Machine-to-machine technology does not have a standardized device platform, and many M2M systems are built to be task- or device-specific. Several key M2M standards, many of which are also used in IoT settings, have emerged over the years, including:

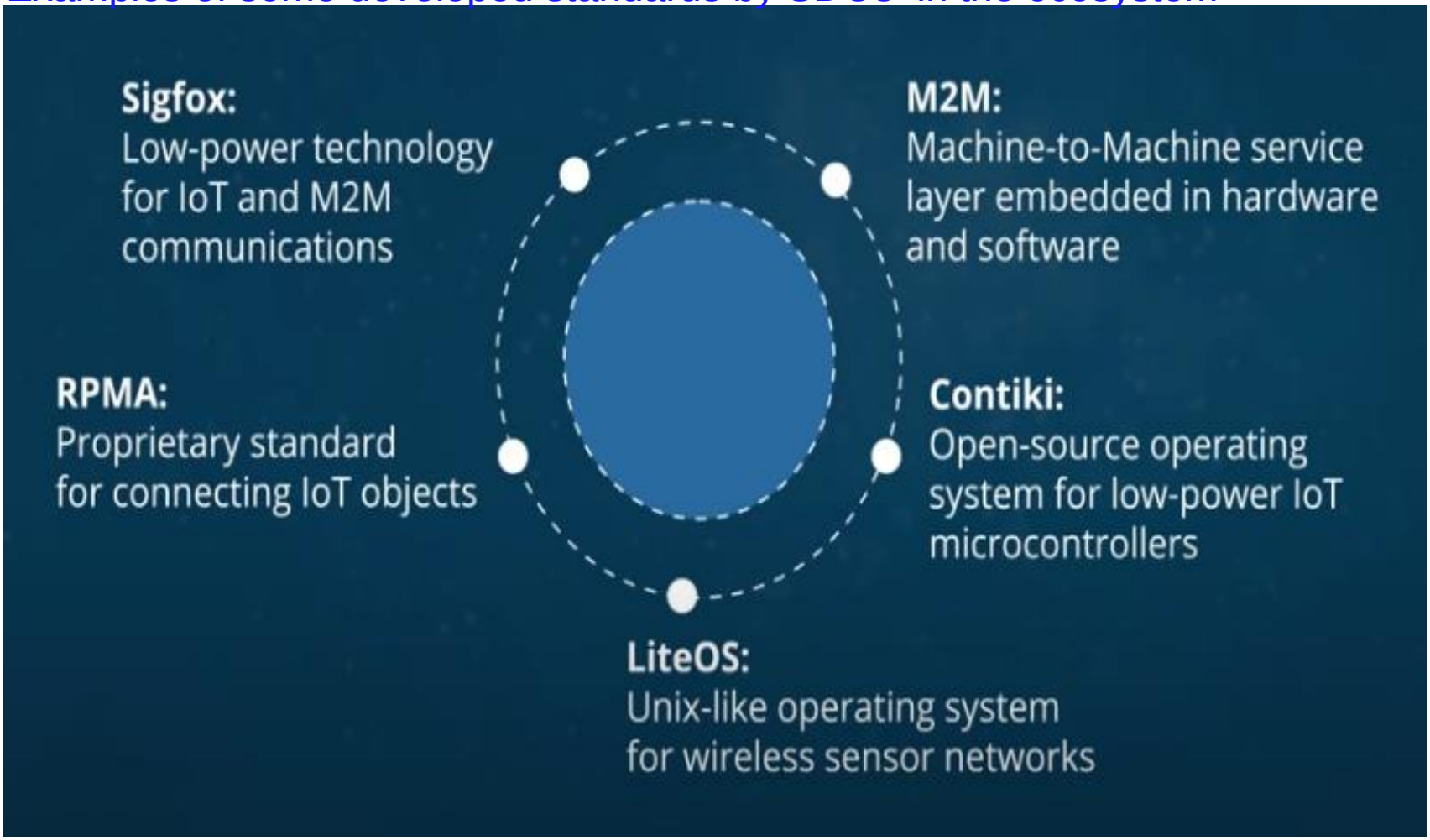
- OMA DM (Open Mobile Alliance Device Management), a device management protocol
- OMA LightweightM2M, a device management protocol
- MQTT a messaging protocol
- TR-069 (Technical Report 069), an application layer protocol
- HyperCat, a data discovery protocol
- OneM2M, a communications protocol
- Google Thread, a wireless mesh protocol
- AllJoyn, an open source software framework

Need for Standardisation

Several Standards Developing Organisations (SDOs) remains independent in normal business operations

Need for Standardisation

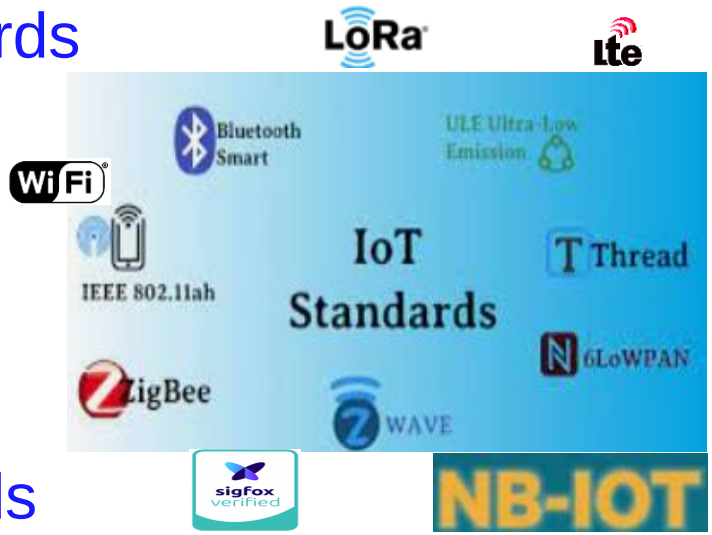
Examples of some developed standards by SDOs in the ecosystem



Need for Standardization

- **The IoT/M2M standard system contains**

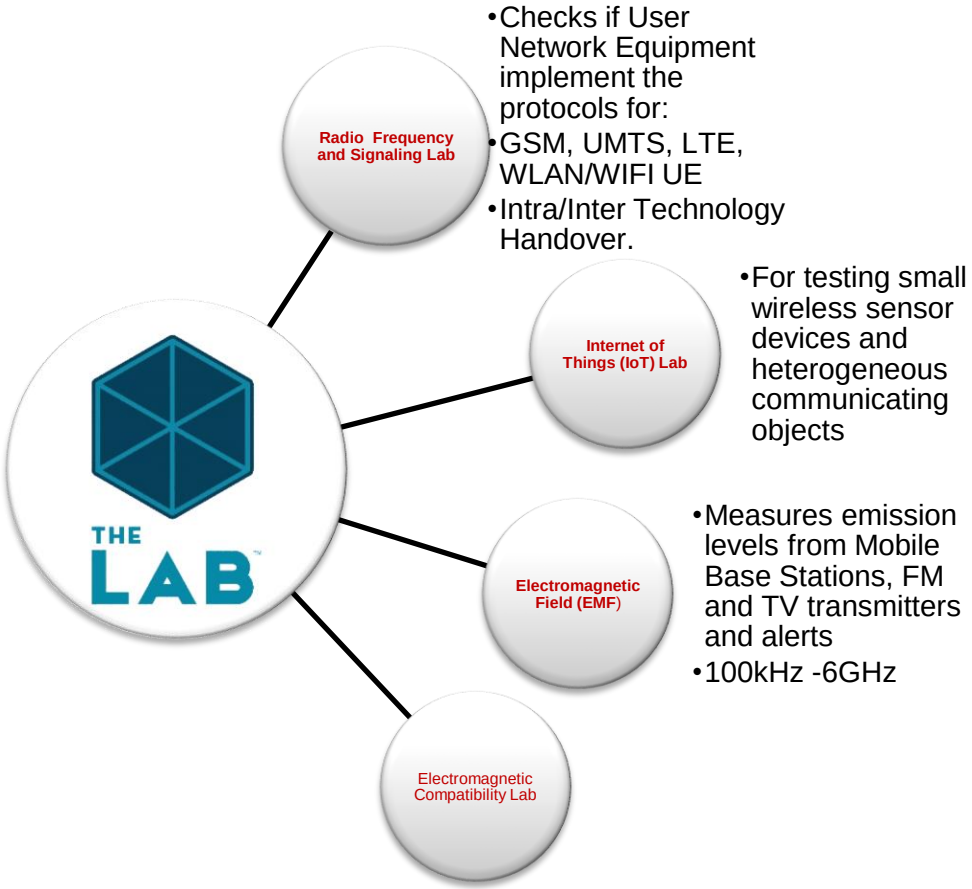
  - Architecture standards
  - Application requirements standards
  - Communication protocol standards
  - Identification standards
  - Security standards
  - Application standards
  - Data standards
  - Information processing standards
  - Public service platform standards.



IoT Interoperability Testing

- Radio Frequency Spectrum efficiency
- Health, Safety & Environmental issues
- Network Compatibility and Interoperability
- Quality of Service & Experience
- Check Counterfeit IoT devices

IoT Interoperability Testing



IoT Interoperability Testing

- Checks the behavior of an ICT device in relation to other ICT equipment in its environment
  - Emissions – Conducted and Radiated
  - Electrical Fast Transient (EFT) and Surge

- RF Testing (typical parameters for radio transmit and receiver conformance)
  - Unwanted Emissions
  - Type of Modulation and Quality
  - Device Receiver Sensitivity
  - Throughput Performance
  - Power Requirement
  - Demodulation

The RF and signaling system has the capability of testing Wifi and Bluetooth which are key to IoT and therefore only a software upgrade is required to enable the lab perform other IoT functions such as;

- Sensors
- Smart watches
- IoT controls
- etc

Use Cases

- Track and Trace Use Case
  - Fleet Management
  - Emergency Call (eCalls)
  - Fleet Management
  - Traffic Control Management
- Monitoring Use Case
  - Smart Utility metering ((delivery of water and electricity)
  - Waste Management
  - Person/animal position monitoring
  - Object Position monitoring
- Transaction Use Case
  - Point of Sale (PoS) Services
- Health Use Case
  - Wearables, Remote Surgery,
- Control Use Case
  - Entry Control, Vending Machines, Production lines

Use Cases

1.Surveillance will bring values to the cities as the citizens will feel safe. Real time video analytics sends alerts on the smart phones of police in that area

2. Wearable health devices may help in monitoring the health parameters especially in rural areas for remote monitoring and advising, help in reducing burden on hospitals.

-Digital health is the part of health policy released in 2017 in India.

-NoFN BW shall be used for extending health services in the rural areas.

3. Save electricity by using smart lighting system in cities and homes.

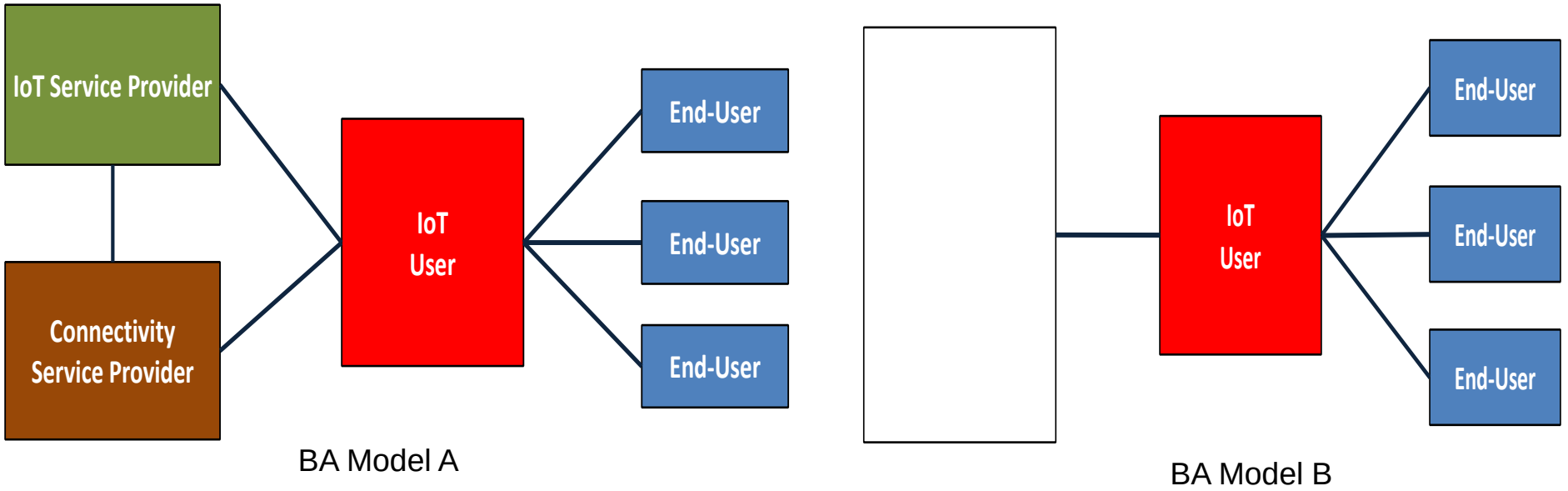
-Smart street lighting system are being implemented in a number of cities.

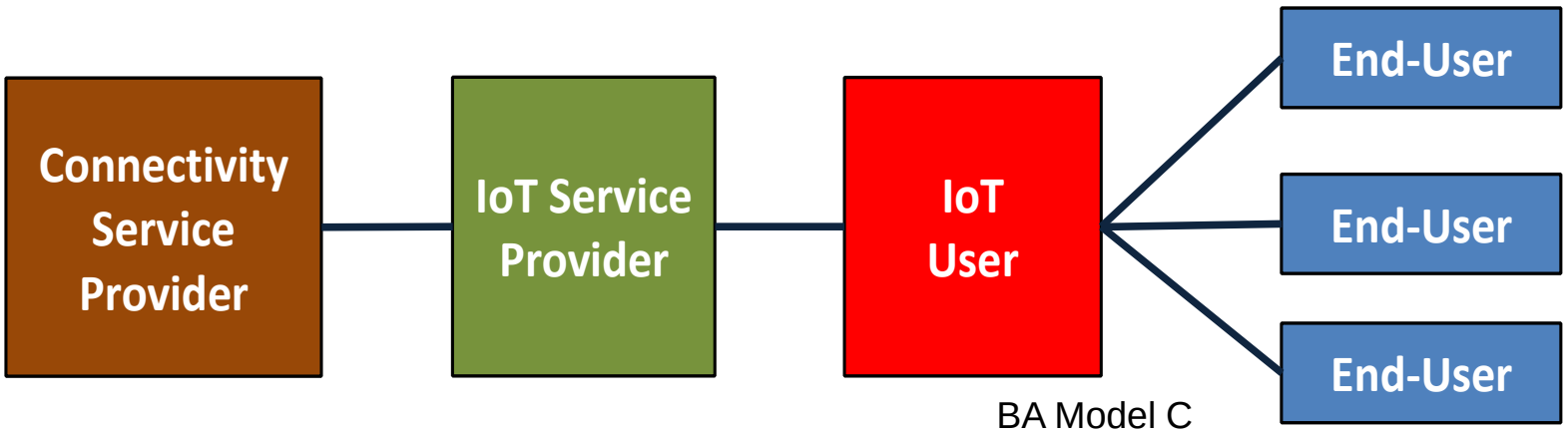
-Smart metering projects are in progress.

Example;
Ghana uses drones to deliver drugs to rural areas and is in the process of deploying Smart Traffic Management System to forestall crime

Please Share any examples from your country!!!

Business Application Model





Business Application Model

- Less Time more work
- Automation
- Digital Farming
- E-Health
- E-Governance
- E-Learning
- Vertical Industries

IoT Business Model

The Internet of Things has the power to revolutionize everything

Our Homes...

Our Businesses...

Our Cities...

Thank you.

Any Questions?