



ASIA-PACIFIC TELECOMMUNITY

**SOUTH ASIAN TELECOMMUNICATIONS REGULATOR'S COUNCIL  
(SATRC)**

---

## **SATRC REPORT ON SPECTRUM CONSIDERATION FOR THE DEPLOYMENT OF IOT**

**Prepared by  
SATRC Working Group on Spectrum**

**Adopted by  
22nd Meeting of the South Asian Telecommunications Regulator's Council  
1 – 3 November 2021, Virtual/Online Meeting**

## CONTENT

<b>1- CHAPTER1: EXECUTIVE SUMMARY .....</b>	<b>6</b>
<b>2- CHAPTER 2: IOT VISION.....</b>	<b>7</b>
2-1- Early stages of market development.....	7
2-2- Consumer and socio-economic impact.....	7
<b>2-3- Understanding the Internet of Things .....</b>	<b>8</b>
2-3-1 Internet of Things industry sector categories .....	8
2-3-2 Example IoT smart cities applications.....	9
2-3-3 Example IoT health applications .....	9
2-3-4 Example IoT education applications .....	10
<b>2-4- Comparison of traditional telephony and IoT service provision .....</b>	<b>11</b>
<b>3- CHAPTER 3: WHAT IS IOT .....</b>	<b>13</b>
<b>3-1- The evolution of the Internet.....</b>	<b>14</b>
3-1-1- Internet of content .....	14
3-1-2- Internet of services .....	14
3-1-3- Internet of people.....	14
3-1-4- Internet of things .....	15
<b>3-2- IoT market landscape .....</b>	<b>15</b>
<b>3-3- IoT use cases .....</b>	<b>17</b>
3-3-1- Agriculture .....	17
3-3-2- Smart cities .....	17
3-3-3- Home automation .....	18
3-3-4- Environmental monitoring.....	18
3-3-5- Smart grids and metering .....	18
3-3-6- Healthcare .....	19
3-3-7- Industrial automation .....	19
3-3-8- Connected car .....	20
<b>3-4- IoT connectivity .....</b>	<b>20</b>
<b>3-5- IoT application categories .....</b>	<b>21</b>
<b>3-6- LPWA IoT design targets .....</b>	<b>22</b>
<b>3-7- Cellular IoT benefits and disadvantages .....</b>	<b>23</b>
3-7-1- Advantages of cellular IoT .....	23
3-7-2- Disadvantages of cellular IoT .....	24

<b>3-8- 3GPP work on MTC / IoT .....</b>	<b>25</b>
3-8-1- Extended Coverage GSM (EC-GSM) .....	25
3-8-2- eMTC overview .....	26
3-8-3- NB-IoT overview .....	27
<b>3-9- Non-cellular IoT.....</b>	<b>28</b>
3-9-1- Bluetooth Low Energy .....	28
3-9-2- Wi-Fi HaLow.....	28
3-9-3- ZigBee .....	29
3-9-4- ZigBee vs. Z-Wave.....	30
3-9-5- LoRa .....	31
3-9-6- SigFox.....	32
<b>3-10- Technologies Comparison: LPWANs .....</b>	<b>33</b>
3-10-1 Transceiver parameters .....	33
<b>3-11- SATELLITE BASED IoT NETWORKS.....</b>	<b>35</b>
3-11-1- Motivation for Satellite IoT Integration .....	35
3-11-1-1- Reliability in the wireless applications .....	35
3-11-1-2- Larger and broader coverage of the IoT Networks .....	35
3-11-1-3- Better Security and Protection.....	35
3-11-1-4- Economical and faster rural deployment.....	36
3-11-1-4- Multicasting of services.....	36
3-11-1-5- Longevity of the wireless networks .....	36
3-11-2- APPLICATIONS OF SATELLITE BASED IOT SYSTEMS.....	36
 <b>4- CHAPTER 4: IOT FREQUENCY BANDS.....</b>	 <b>37</b>
<b>4-1- Unlicensed Bands (class Licensing).....</b>	<b>37</b>
4-1-1- Short Range Devices .....	37
4-1-2- LPWANs .....	38
4-1-2-1- SIGFOX.....	40
4-1-2-2- Ingenu .....	40
4-1-2-3- LoRa.....	40
4-1-2-3- Frequency usage for LPWAN.....	41
<b>4-2- Licensed Bands .....</b>	<b>43</b>
4-2-1- NB-IoT Frequency bands.....	44
4-2-2-LTE Cat M1 Frequency Bands .....	45
4-2-3-LTE Cat 1 Frequency Bands.....	45
4-2-4- EC-GSM IoT Frequency .....	45
<b>4-3- Spectrum Sharing for Providing Local Area Services with QoS .....</b>	<b>50</b>
<b>4-4- Licensed Shared Access (LSA).....</b>	<b>51</b>
 <b>5- CHAPTER 5: IOT OPERATOR.....</b>	 <b>53</b>

<b>5-1- IoT implementation issues .....</b>	<b>53</b>
<b>5-2- State of LPWA network roll-outs .....</b>	<b>54</b>
5-2-1- LoRaWAN (83 operators globally) .....	55
5-2-2- Sigfox (57 operators globally) .....	55
5-2-3- NB-IoT (46 operators globally) .....	55
5-2-4- LTE-M (13 operators globally) .....	56
<b>5-3- Cellular MNO strategies for LPWAN technologies .....</b>	<b>56</b>
5-3-1- Strategy 1: Ignoring LPWAN technologies .....	57
5-3-2- Strategy 2: Focus on one licensed LPWAN technology only.....	57
5-3-3- Strategy 3: Focus on two licensed LPWAN technologies.....	57
5-3-4- Strategy 4: Focus on licensed and unlicensed LPWAN technologies.....	58
5-3-5- Trend: Adoption of multiple LPWAN technologies.....	58
 <b>6- CHAPTER 6: IOT IN 5G .....</b>	 <b>60</b>
<b>6-1- Wireless networks in 5G .....</b>	<b>60</b>
<b>6-1-1- Enhanced Mobile Broadband (eMBB).....</b>	<b>60</b>
<b>6-1-2- Ultra-Reliable Low Latency Communications (URLLC).....</b>	<b>60</b>
<b>6-2- Features employed in 5G PHY layer to support 5G-IoT .....</b>	<b>63</b>
6-2-1- Carrier aggregation .....	63
6-2-2- Massive-MIMO (M-MIMO) .....	63
6-2-3- Coordinated Multipoint Processing (CoMP) .....	63
6-2-4- Heterogeneous Networks (HetNets) .....	64
6-2-5- D2D Communications .....	64
6-2-6- Centralized Radio Access Network (CRAN).....	64
<b>6-3- Features employed in 5G networking layer to support 5G-IoT .....</b>	<b>64</b>
6-3-1- Software-Defined Wireless Sensor Networking (SD-WSN) .....	64
6-3-2- Network Function Virtualization (NFV).....	65
6-3-3- Cognitive Radios (CRs) .....	65
<b>6-4- Architectural view of 5G-IoT .....</b>	<b>66</b>
<b>6-5- QoS in 5G-IoT.....</b>	<b>66</b>
<b>6-6- Figure 30- QoS in a 5G.....</b>	<b>66</b>
<b>6-6- Standardization in 5G-IoT .....</b>	<b>66</b>
<b>6-7- Artificial intelligence use cases for 5G-IoT networks .....</b>	<b>66</b>
6-7-1- Big data processing enhancement.....	67
6-7-2- Expanding the horizon of healthcare.....	67
6-7-3- Intelligent networking .....	67
6-7-4- Smart transportation systems .....	67

6-8- 5G-IoT Frequency Bands .....	68
<b>7- CHAPTER 7: CONCLUSION .....</b>	<b>70</b>
7-1- Regulators should adopt a service and technology neutral framework to support IoT .....	70
7-2- Licensed spectrum is vital to deliver the most reliable, high quality IoT services .....	70
7-3- Regulators should work with the mobile industry to support IoT in 5G spectrum planning .....	70
<b>8- CHAPTER 8: QUESTIONS AND ANSWERS .....</b>	<b>71</b>
8-1- Questions .....	71
8-2- Answers .....	73

## **1- Chapter1: Executive Summary**

The Internet of Things (IoT) refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects. IoT is expected to spread rapidly over the coming years and this convergence will unleash a new dimension of services that improve the quality of life of consumers and productivity of enterprises.

For consumers, the IoT has the potential to deliver solutions that dramatically improve energy efficiency, security, health, education and many other aspects of daily life. For enterprises, IoT can underpin solutions that improve decision-making and productivity in manufacturing, retail, agriculture and other sectors. Machine to Machine (M2M) solutions - a subset of the IoT – already use wireless networks to connect devices to each other and the Internet, with minimal direct human intervention, to deliver services that meet the needs of a wide range of industries. In 2013, M2M connections accounted for 2.8% of global mobile connections (195 million), indicating that the sector is still at a relatively early stage in its development. An evolution of M2M, the IoT represents the coordination of multiple vendors' machines, devices and appliances connected to the Internet through multiple networks. While the potential impact of the IoT is considerable, a concerted effort is required to move beyond this early stage. In order to optimize the development of the market, a common understanding of the distinct nature of the opportunity is required.

## 2- Chapter 2: IoT Vision

### 2-1- Early stages of market development

Machine to Machine (M2M) solutions - a subset of the Internet of Things – already use wireless networks to connect devices to each other and the Internet, with minimal direct human intervention, to deliver services that meet the needs of a wide range of industries. The Internet of Things represents an evolution of M2M through the coordination of multiple vendors' machines, devices and appliances connected to the Internet through multiple networks.

According figure 1, in 2013, M2M connections accounted for 2.8% of global mobile connections (195 million), indicating that the sector is still at a relatively early stage in its development. There are significant regional variations between more established markets, such as Europe, North America and Oceania, where M2M's share of total connections exceeds the global average, and rapidly developing markets, such as Asia, which have experienced annual growth of 55% a year between 2010 and 2013

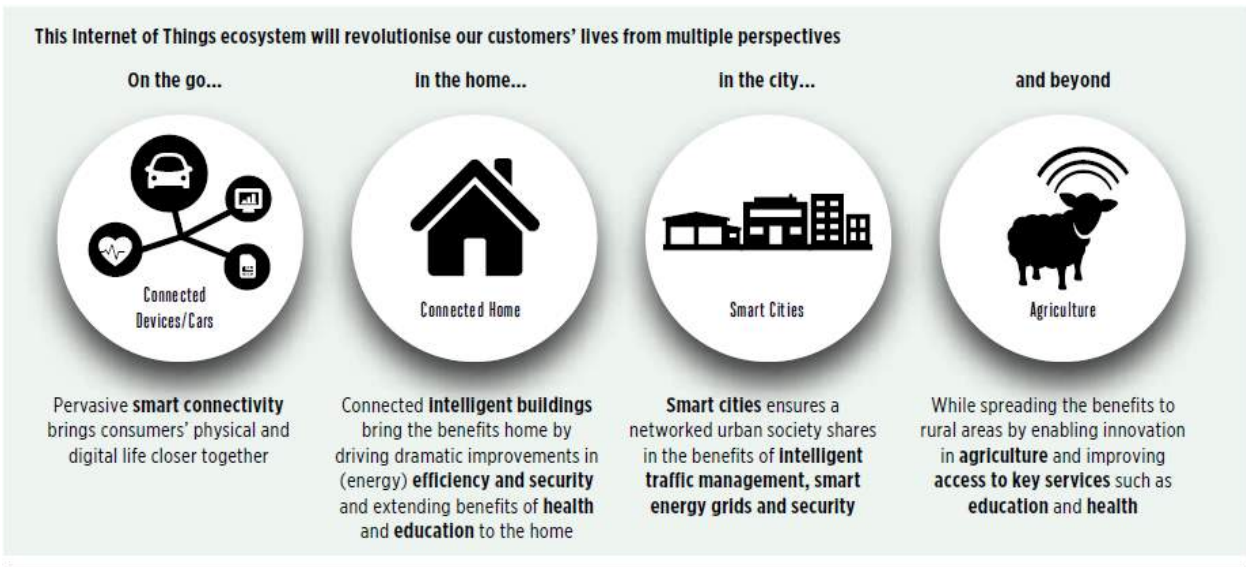
Region	M2M % total connections (2013)	M2M CAGR (2010-2013)	Connections CAGR (2010-2013)
Africa	1.0%	41.3%	15.0%
Asia	2.1%	55.0%	10.4%
Europe	5.1%	28.6%	2.4%
Latin America	2.1%	43.7%	7.8%
Northern America	9.3%	22.5%	3.6%
Oceania	5.1%	25.8%	5.5%
Global	2.8%	37.6%	8.8%

Source: GSMAI

Figure 1- M2M connections

### 2-2- Consumer and socio-economic impact

Pervasive connectivity between people and processes will enable multiple services to be delivered automatically and contextually, whenever and wherever required, ushering in the Connected Life. Supported by cross-industry collaboration, the Connected Life will have a positive impact on many sectors of the economy, such as automotive, shipping and logistics, healthcare and utilities, potentially benefitting billions of people globally. Figure 2 is shown this subject.



3. Source: Machina Research

4. Source: McKinsey & Company, 2013.

Figure 2- Consumer impact of the Connected Life

### 2-3- Understanding the Internet of Things

While the Internet of Things (IoT) will ultimately have an enormous impact on consumers, enterprises and society as a whole, it is still at an early stage in its development. As mobile operators and their partners pilot new services across multiple sectors, ranging from health to automotive, they have identified several distinctive features of the Internet of Things. A common understanding of the distinctive nature of this nascent opportunity should help hasten the development of this market. The three distinctive features are:

- i. **The Internet of Things can enable the next wave of life-enhancing services across several fundamental sectors of the economy.**

As the Internet of Things evolves, the proliferation of smart connected devices supported by mobile networks, providing pervasive and seamless connectivity, will unlock opportunities to provide life-enhancing services for consumers while boosting productivity for enterprises. As can be seen in Figure 3 below, thirteen industry sectors are likely to show significant adoption of IoT services:

#### 2-3-1 Internet of Things industry sector categories

For consumers, connectivity provided by the IoT could enhance their quality of life in multiple ways, such as, but not limited to, energy efficiency and security at home and in the city. In the home, the integration of connected smart devices and cloud-based services will help address the pressing issue of energy efficiency and security. Connected smart



devices will enable a reduction in utility bills and outages, while also improving home security via remote monitoring.

In cities, the development of smart grids, data analytics and autonomous vehicles will provide an intelligent platform to deliver innovations in energy management, traffic management and security, sharing the benefits of this technology throughout society.

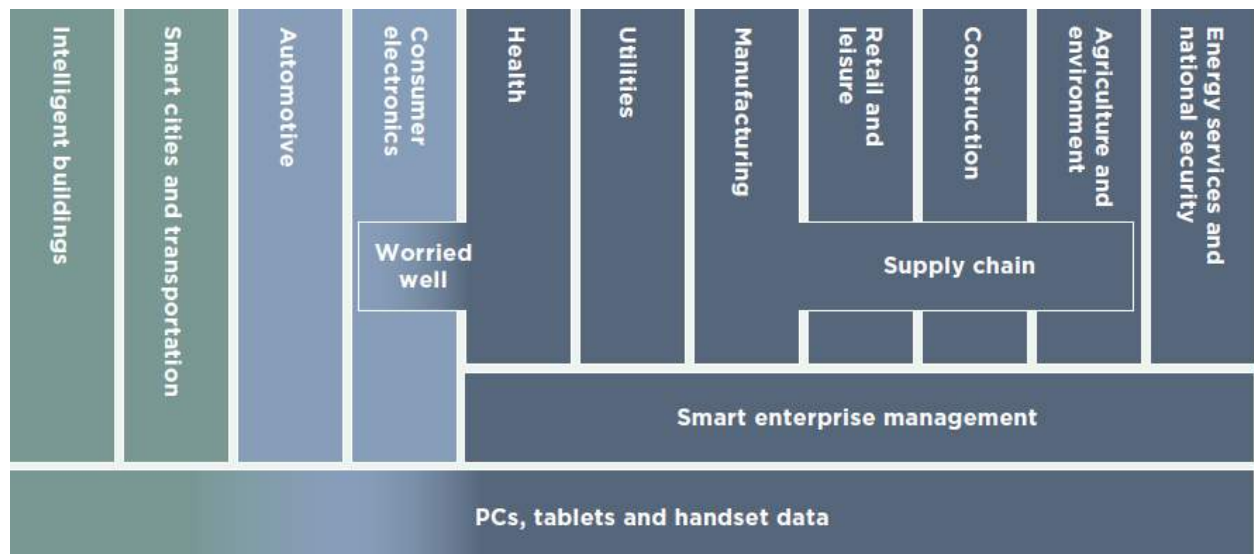


Figure 3: Internet of Things industry sector categories

### 2-3-2- Example IoT smart cities applications

The IoT will also help widen access and improve quality of education and health. As demand for healthcare doubles<sup>8</sup>, connected smart devices will help address this challenge by supporting a range of e-health services that improve access and enable monitoring of chronic diseases and age-related conditions in the home. In doing so, they will improve the quality of care and quality of life for patients, while reducing the strain on the wider healthcare system.

### 2-3-3- Example IoT health applications

Before Internet of Things, patients' interactions with doctors were limited to visits, and tele and text communications. There was no way doctors or hospitals could monitor patients' health continuously and make recommendations accordingly.

Internet of Things (IoT)-enabled devices have made remote monitoring in the healthcare sector possible, unleashing the potential to keep patients safe and healthy, and empowering physicians to deliver superlative care. It has also increased patient engagement and satisfaction as interactions with doctors have become easier and more efficient. Furthermore, remote monitoring of patient's health helps in reducing the length of hospital

stay and prevents re-admissions. IoT also has a major impact on reducing healthcare costs significantly and improving treatment outcomes.

#### **2-3-4- Example IoT education applications**

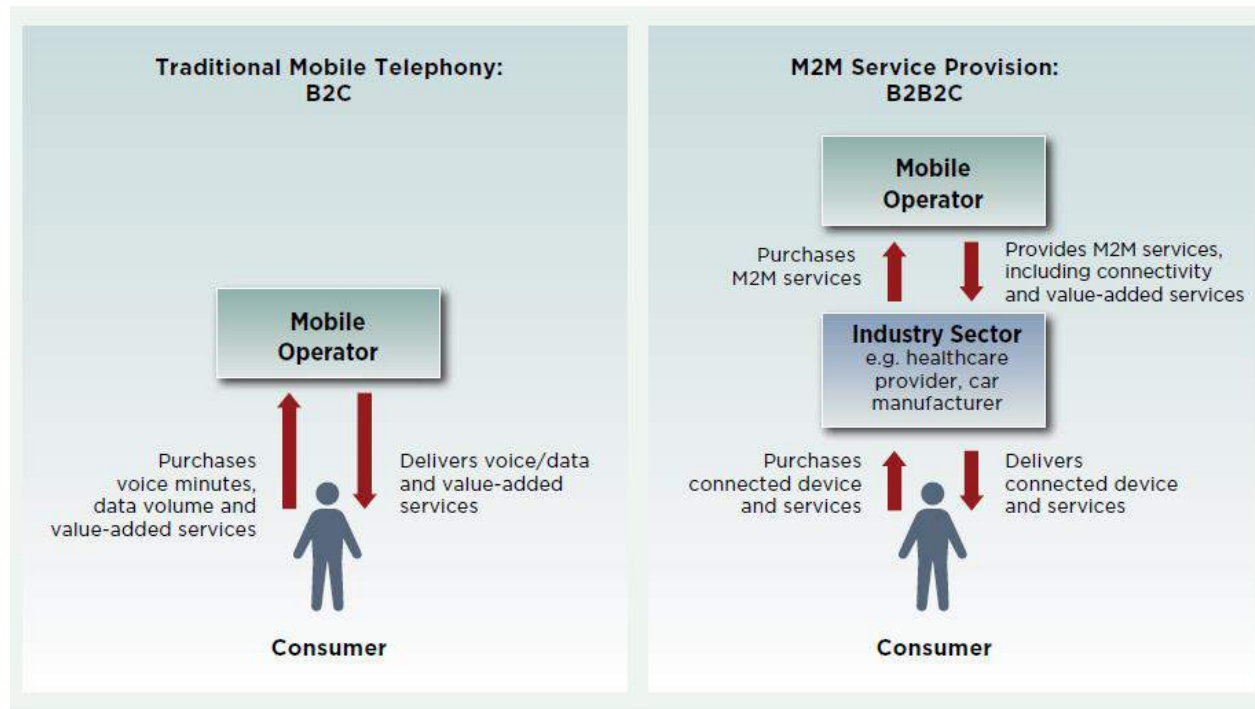
In education, mobile-enabled solutions will tailor the learning process to each student's needs, improving overall proficiency levels, while linking virtual and physical classrooms to make learning more convenient and accessible.

Mobile education solutions have already been shown to improve learners' proficiency rates and reduce dropout rates, and have the potential to enable, the education of up to 180 million additional students in developing countries who will be able to stay in school due to mEducation (Mobile Education).

For enterprises, the ability of IoT to combine innovations in data analytics, 3D printing and sensors, will improve productivity by enabling a step change in the quality of decision making, efficiency of production, personalization of retail and productivity of food production.

#### **ii. IoT presents an opportunity for new commercial models to support mass global deployments.**

In order to bring new services to market, mobile operators are partnering with adjacent industry organizations and jointly developing innovative IoT services targeted at the end consumer. A variety of commercial models are becoming more prominent, such as business to business to consumer (B2B2C) propositions where the end service is marketed by the adjacent industry partner who owns the end customer relationship. For example, a mobile operator could partner with a utilities company for smart metering capabilities, who then provides energy services to the end consumer. Figure 10 compares the B2B2C model with the traditional Business to Consumer (B2C) model which is primarily used when operators are selling voice and data communications services on mobile phones to consumers.



Source: GSMA viewpoint

Figure 4: Comparison of traditional telephony and IoT service provision

## 2-4- Comparison of traditional telephony and IoT service provision

In addition to this structural distinction, there is a fundamental difference in the nature of customer charges. While customer charges underpinning traditional telecommunication services are typically usage-based, often tied to data consumption, those supporting IoT services will be linked to service value (of which connectivity will be an indistinguishable component).

For example, consumers of connected cars may pay a monthly service fee, along with some discretionary fees for value-added services, such as entertainment, while eReader consumers may pay for the device upfront and then pay per book downloaded. In many cases, the mobile operator providing the IoT services will not be visible to the end customer, as its relationship will be with the adjacent sector organization.

Along with partnering with the leading organizations in adjacent industry sectors, mobile operators may also need to address the ‘long tail’ of smaller companies, who wish to develop mobile-enabled services, in an economically viable manner. Standardized enablers, such as Application Programming Interfaces (APIs), which expose mobile network assets or management platforms, need to be developed to achieve this. Such

enablers will allow mobile operators to support and monetize relationships with a large number of industry partners from a wide variety of economic verticals.

iii. **The majority of revenue is derived from the provision of value added services and operators are building new capabilities to address these new service areas.**

While connectivity will underpin the development of the Internet of Things, to avoid becoming commoditized, mobile operators need to leverage their networks’ potential to provide value added services and build what could become a US\$422.6 billion industry. As can be seen in Figure 11, even within the area of connectivity, enablement of services accounts for the lion’s share of revenue, where just US\$3.3 billion out of US\$39.3 billion is accounted for by mobile network traffic alone.

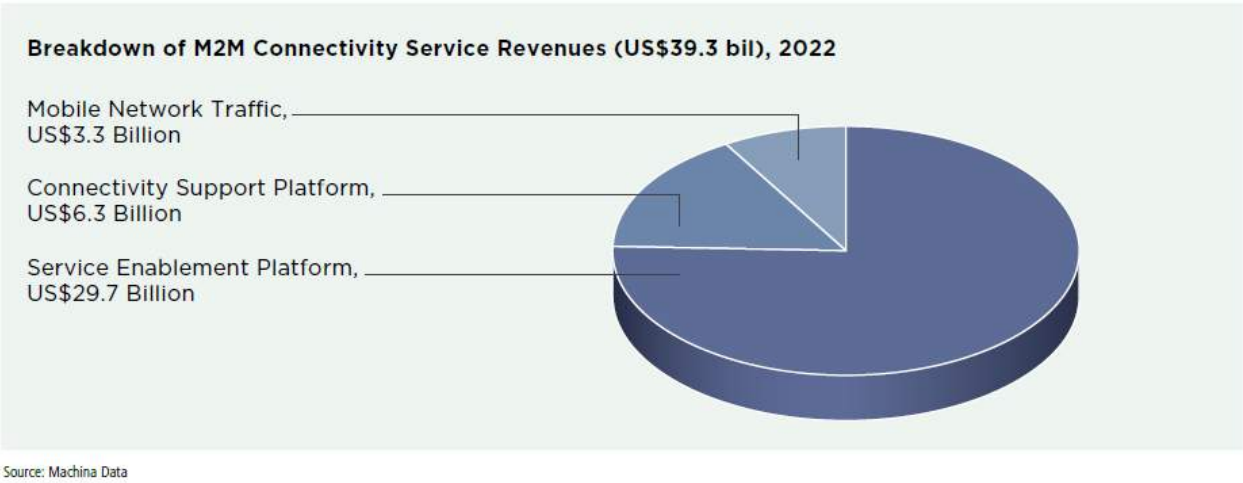


Figure 5: M2M connectivity service revenue 2022

### **3- Chapter 3: What is IoT**

Generally speaking, IoT refers to a massive network of Internet connected “things”. Many of these IoT “things” will have embedded sensors so they can generate data from their external environment or internal state, and they have embedded communication technology that lets them share that data with other things or send it to servers in the Internet. IoT can be seen as a natural continuation of how we connect devices to the Internet and to each other today.

So, what are these “things”? Well the IoT proposition is that anything that can benefit from being connected, will be connected. This includes sensors in cars, kitchen appliances, lamps, locks, fridges, sport trackers, electricity meters, vending machines, industrial pressure gauges, heart monitors, and millions and millions of other things. As the Internet of Things grows in the upcoming years, new types of devices that we have not even thought of yet will join that list.

This highly connected world is made possible by the dropping price points for wireless communication chips and sensors embedded to these devices, the continuing evolution of machine-to-machine (M2M) communications, and big data analytics.

M2M is a broad label that we use to describe all technologies that enable connected devices to exchange information over wireless and wired networks, and perform actions without the manual assistance of humans. Another term that is often used interchangeably with M2M is Machine Type Communications (MTC). Examples of M2M/MTC services include security, tracking, payment, smart grid and remote maintenance/monitoring.

### 3-1- The evolution of the Internet

The Internet as we now it has only existed for about 30 years. Within this time, and especially within the past ten years, it has gone through several evolutionary steps on how –and what we use it for. Over the past decade or so, the Internet has changed from being a static repository of information to networking humans, machines, services and various applications. Figure 6 shows the key evolutionary phases of the Internet.

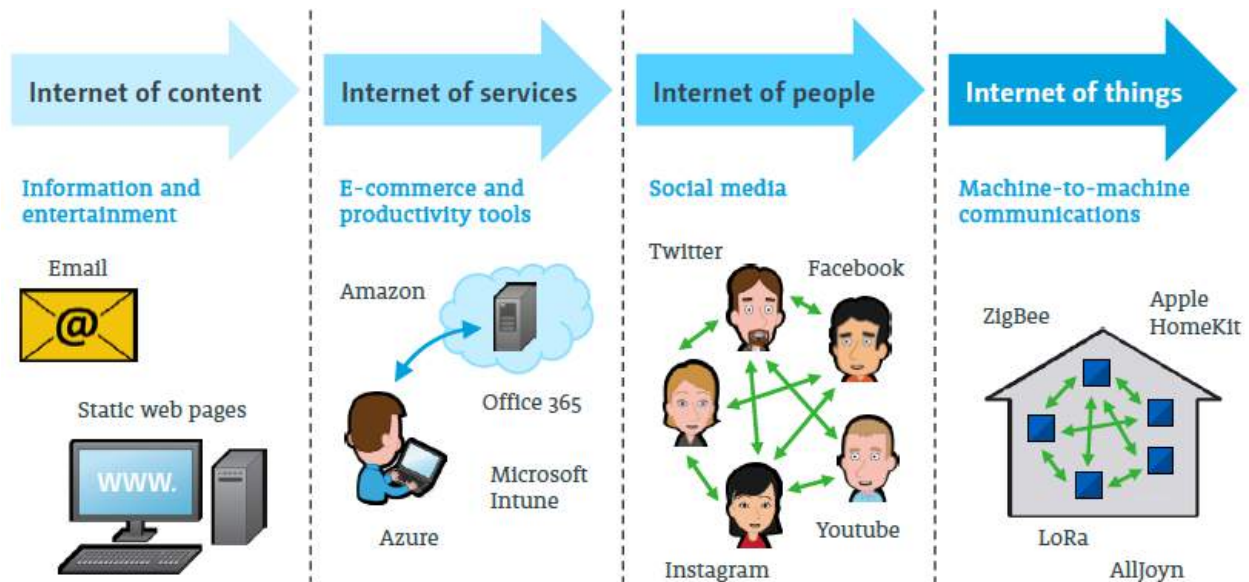


Figure 6. Evolution of the Internet

#### 3-1-1- Internet of content

The Internet, as we know and use it today started in the early 90s with the creation of the World Wide Web and the hypertext Transfer Protocol (HTTP). These are the technologies we use when browsing the web and downloading web pages. At this time the Internet was mainly used to publish and share information and entertainment content. Users would browse through static web pages and send and receive emails.

#### 3-1-2- Internet of services

The next big evolutionary step happened with the birth of e-commerce and online productivity tools. Companies like Amazon and Alibaba forever changed the way consumers purchase goods and services. Companies could also move many of their productivity applications and services to the cloud.

#### 3-1-3- Internet of people

The introduction of smartphones and tablets, and affordable broadband subscriptions, together with the explosive popularity of social networking services like Facebook and

Twitter led to the third evolutionary step of the Internet. This is where we are today, where people are connected 24/7.

### **3-1-4- Internet of things**

Now we are at the verge of the next major evolutionary step of the Internet, called “the internet of things” (IoT). IoT is described as a system where all kinds of “things” are connected to each other and to the Internet via wireless and wired connections. These IoT things refer to a variety of devices, like

Lights, locks, doors, fridges, heart monitoring implants, biochip transponders on farm animals, sensors built-in to automobiles, parking meters, or electricity meters. Basically anything that could benefit from being connected to the rest of the world.

### **3-2- IoT market landscape**

The global IoT market is expected to grow aggressively over the next decade. The number of smart meters, household automation and smart car applications that will be connected will be huge in the future. This number will be proportional to the number of people in a country. For example, the European Union Electricity Directive regulates that 80% of consumers should be equipped with intelligent metering systems by 2020. Taking into account the number of households in EU this means that around 180 million smart electricity meters will be connected within EU countries. And this is just one IoT application! The average number of cars is about 0.5 per capita, which means that smart car connections could easily surpass the number of smart electricity meters. Additionally, a massive number of industrial applications are expected to arrive from the need to automate objects in various transport industries, factories, and public service machines like vending machines, elevators, and ATMs.

Currently there are wildly different speculations and predictions on the number of connected IoT devices we will have in ten years' time. These predictions range from 25 to 50 billion connected devices by 2020, and maybe even up to 74 billion by 2025 fueling the multi-trillion-dollar economic growth across a multitude of markets.

One of the more conservative estimations comes from Machina Research report (May 2015). They predict that there will be around 27 billion connected M2M devices by 2025, as illustrated in Figure 7.

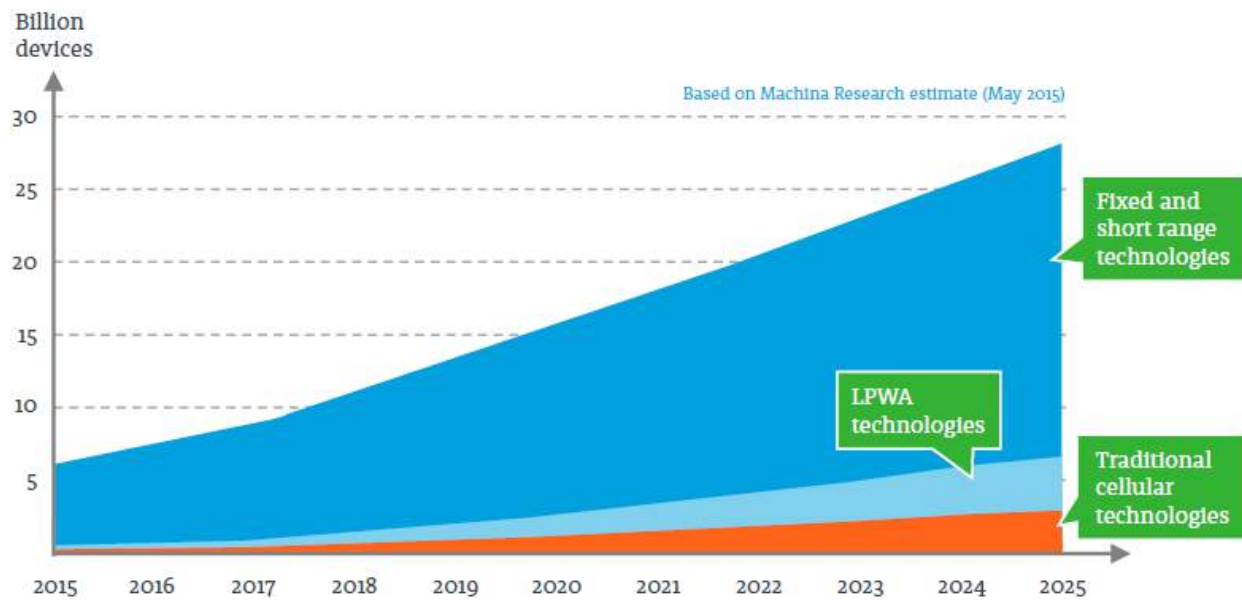


Figure 7. IoT market landscape

According to the Machina Research report, most of these M2M devices will use fixed or short-range communication technologies. They also expect that an also a significant number – around 7 billion by 2025 – of connections will use via traditional cellular and low power wireless access (LPWA) technologies. To reach this total volume of 7 billion units by 2025, the cellular IoT / LPWA market will need to grow 35% annually on average. Machina Research further elaborates.

- By 2025 around 72% of all IoT connections will be connected using a short range technology, Today this number is around 71%. Short range will be the dominant technology category mainly because of consumer electronics, building security and building automation.
- Cellular connections will grow from 334 million at the end of 2015 to around 2.2 billion by 2025. Majority of these connections will use LTE.
- Around 45% of those cellular connections will be in the ‘Connected Car’ sector, including both factory-fit embedded connections and aftermarket devices.
- Around 11% of connections in 2025 will use Low Power Wide Area (LPWA) connections such as Sigfox, LoRa and the cellular IoT technologies.
- By 2025, IoT will generate over 2 zeta bytes of data, mostly generated by consumer electronics devices. However it will account for less than 1% of all cellular data traffic.



### **3-3- IoT use cases**

IoT is expected to transform many industries and markets with innovative services and useful new information. IoT has been labeled as "the next Industrial Revolution" because of the way it can change the way people live, work, entertain, and travel, as well as how businesses interact with the world.

Below some of the key markets and use cases for IoT are covered in more detail.

#### **3-3-1- Agriculture**

- Sensors that can detect soil moisture, crop growth and livestock feed levels.
- Smart green houses where the micro-climate conditions can be monitored and controlled to maximize the production and quality of fruits and vegetables.
- Smart compost where the humidity and temperature levels can be controlled in the alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.
- Remotely controlled smart harvesters and irrigation equipment that automate many labor intensive agricultural tasks.
- Animal tracking, enabling the location and identification of individual animals grazing in open pastures or in big stables
- Toxic gas level monitoring, allowing the study of ventilation and air quality in farms and detection of harmful gases from excrements.

#### **3-3-2- Smart cities**

- Smart parking that monitors parking spaces availability in the city.
- Structural health that monitors vibrations and material conditions in buildings, bridges and historical monuments.
- Urban noise maps that monitor sound levels in bar areas and centric zones in real time.
- Traffic congestion that monitors vehicle and pedestrian levels to optimize driving and walking routes.
- Smart street lighting with intelligent and weather adaptive lighting in street lights.
- Waste management with detection of rubbish levels in containers to optimize the trash collection routes.

- Smart roads Intelligent with warning messages and diversions according to climate conditions and events like accidents or traffic jams.

### **3-3-3- Home automation**

- Energy and water consumption monitoring, with automatic advice on how to save cost and resources.
- Remote control appliances, allowing appliances on and off remotely to avoid accidents and save energy.
- Intrusion Detection Systems, which detect the opening of windows and doors and other violations to prevent intruders.
- Smart smoke detectors that can send alarms via the Internet to the owner or fire department.

### **3-3-4- Environmental monitoring**

- Forest fire detection, where sensors are used to monitor combustion gases and pre-emptive fire conditions.
- Air pollution monitoring, where sensors are used to monitor CO<sub>2</sub> emissions of factories, pollution emitted by cars and toxic gases generated in farms.
- Avalanche monitoring, where the snow levels are measured to track avalanche risks near ski tracks in real time.
- Landslide prevention, monitoring soil moisture, vibrations and earth density to detect dangerous patterns in land conditions.
- Earthquake early detection systems, where a distributed sensor network can be used to detect the originating places of tremors.

### **3-3-5- Smart grids and metering**

- Tank level monitoring, where water, oil and gas levels in storage tanks are remotely tracked.
- Water flow monitoring, where the water pressure in water transportation systems is remotely monitored and controlled.
- Silos stock calculation, where the emptiness level and weight of goods in storage silos is tracked.

### **3-3-6- Healthcare**

- Mobile health (mHealth) applications, or wearable devices that allow patients to capture their health data and empowers them to manage their own health more effectively
- Fall detection, which provides assistance for elderly or disabled people living independently. When a wearable device, or a device installed to the house notices that the person has not moved for long periods of time and is in a laying position, an alarm can be sent to a caregiver.
- Medical Fridges, that control of conditions inside freezers storing vaccines, medicines and organic elements.
- Sports care for athletes, enabling vital signs and performance monitoring during sports activities. For example changes in the vital signs can indicate increased risk of injury, and this allows preventive measures to be taken.
- Patients Surveillance can be used to monitor of people with chronic or long-term conditions and the elderly. This includes tracking the location of patients admitted to hospitals, their medication orders, as well as their current conditions based on data from wearable health devices.

### **3-3-7- Industrial automation**

- Machine auto-diagnosis enables a simple and effective way to get health status data from industrial equipment without costly and time consuming manual checks on-site. By adding sensors to plants and machinery the business can remotely monitor many parameters, like AC current consumption, vibration levels, or air pressure, and can detect equipment that needs maintenance or is approaching failure.
- Indoor air quality monitoring, which can be used to monitor toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety.
- Temperature monitoring, used in industrial areas like a pharmaceutical plant, or for industrial fridges with sensitive merchandise.
- Ozone presence monitoring, which is used in food factories. Meat packing and drying operations pump ozone, an inert airborne disinfectant, into their plants in order to prevent contamination. If a plant uses ozone as it's primary method of disinfection, it needs to be able to prove to a regulatory body that its levels of ozone are high enough, making this monitoring critical.

- Indoor asset tracking, allowing a business to find out where its assets and supplies are located in a defined area. For example an airport needs to track its buses, vehicles, luggage carts, and fuel trucks. The locating can be done by using active and passive tags (RFID/NFC).

### **3-3-8- Connected car**

- Vehicle status telemetry gathering, allowing sensors in the car to send telemetry data to the manufacturer's systems. This could be used for example for predictive maintenance.
- Companion apps, allowing the user to remotely control many car functions from their smartphone. Additionally new apps could be downloaded from the Internet to the car's infotainment system, similar to how apps can be installed to smartphones today.
- Real-time traffic condition sharing, allowing cars in a traffic jam to communicate the situation to other cars nearby. These cars could then relay the message forward to other cars on the same road.
- Internet radio receiver.
- OTA updates, allowing the vehicle's firmware to be updated over the air.
- Vehicle remote control, enabling for example the car motor to be stopped remotely in case of theft.

### **3-4- IoT connectivity**

IoT consists of a number of networks that may have different design objectives. For example, some networks only intend to cover local area, for example a single home, whereas other networks will offer wide-area coverage. When it comes to wireless technologies, all current WPAN, WLAN, and WWAN technologies may be used. Alternatively, many connections may also be made with a new generation of IoT / M2M optimized Low Power Wide Area (LPWA) technologies.

Currently, there are two alternative LPWA IoT technology tracks for IoT applications, 3GPP standardized cellular IoT (CIoT) technologies and proprietary LPWA technologies. 3GPP cellular technologies operate on licensed spectrum and have traditionally targeted mobile voice and mobile broadband (MBB) data services. Now, 3GPP has specified three new technologies for CIoT. These are called eMTC, NB-IoT, and CE-GSM. These have been specifically tailored to form an attractive solution for emerging LPWA applications.

Traditional 3GPP technologies already dominate use cases with large geographic coverage needs and medium- to high-performance application requirements. With the new CIoT technologies, 3GPP networks are taking a leap forward to cover low-cost, low-performance application requirements too.

A number of new, proprietary radio technologies, have also been created for serving the emerging LPWA applications. These technologies include SIGFOX, LoRa, and Ingenu's RPMA. They have been developed and designed solely for low-end machine-type communication (MTC) segment. Most of these technologies operate on the unlicensed spectrum, which may cause interference issues.

### 3-5- IoT application categories

IoT applications and services vary widely in terms of their requirements for data throughput, latency and connection reliability. Connectivity is the fundamental building block for IoT, and the type of connectivity required will depend heavily on the nature of the IoT application. There will be a wide range of IoT use cases in the future, and the market is now expanding towards two different IoT categories, located at different ends of the requirements spectrum. These categories are often called “Massive IoT” and “Critical IoT”, as illustrated in Figure 8.

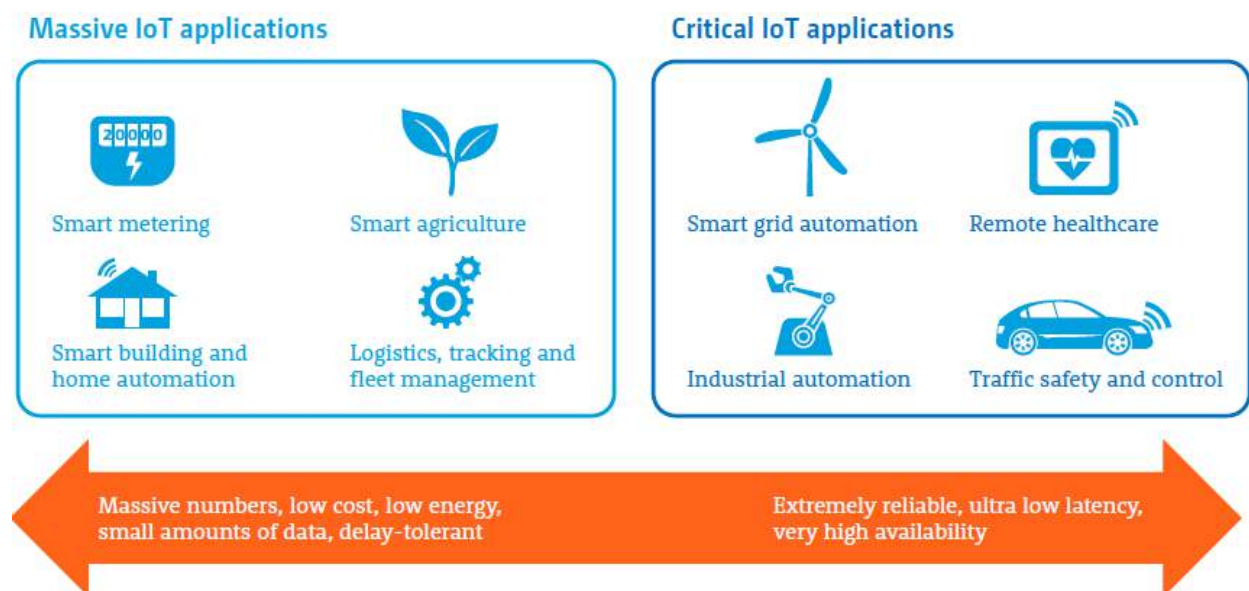


Figure 8. IoT application categories

The so-called “Massive IoT” include all applications where a large number of devices are used, which report to the cloud on a regular basis. These devices may be distributed over a large areas that may be difficult to access, and may have to operate on batteries for long periods of time without maintenance or battery replacements. This category includes for example home automation accessories and smart building sensors, smart metering applications, smart agriculture, and tracking and fleet management chips.

Due to the sheer number of devices used in Massive IoT application deployments, the device cost must be low enough for the business case to make sense. These devices need to have low energy consumption and provide good coverage. To achieve some of these goals the applications must be delay tolerant, as sending even small amounts of data may take several seconds.

The so-called “Critical IoT” include applications that have very high demands for reliability, availability and low latency. Think about applications used for smart grid automation, remote healthcare, traffic safety and control, and industrial automation and control. If any of these applications fail or the communication experiences long delays, the end results could be disastrous, possibly leading to injuries or even deaths.

With Critical IoT applications the device volumes are typically much smaller than with Massive IoT, but the business value is significantly higher.

There is no single connectivity technology that would cover all the different requirements that the different IoT applications have. Connecting all the IoT devices will require various different kinds of connectivity technologies that offer different levels of optimization to address the IoT application needs.

### **3-6- LPWA IoT design targets**

The IoT world includes a broad range of M2M applications, and among the different types massive IoT applications will be the first to take off. Massive IoT includes applications like smart metering, smart agriculture, and various types of tracking and fleet management.

The coverage and throughput need for massive IoT applications are quite different from those of mobile broadband (MBB). Massive IoT devices typically send small amounts of data, and are often placed in signal challenged locations like basements and remote rural areas. Due to the sheer numbers of devices deployed the per-device costs need to be kept low, and long battery life is essential for ensuring the overall cost-effectiveness of the system.

A number of low power wide area (LPWA) radio technologies have been developed to help connect massive IoT applications. Although different LPWA systems use different technologies, they are all designed to support the key requirements for massive IoT deployments, as illustrated in Figure 9.

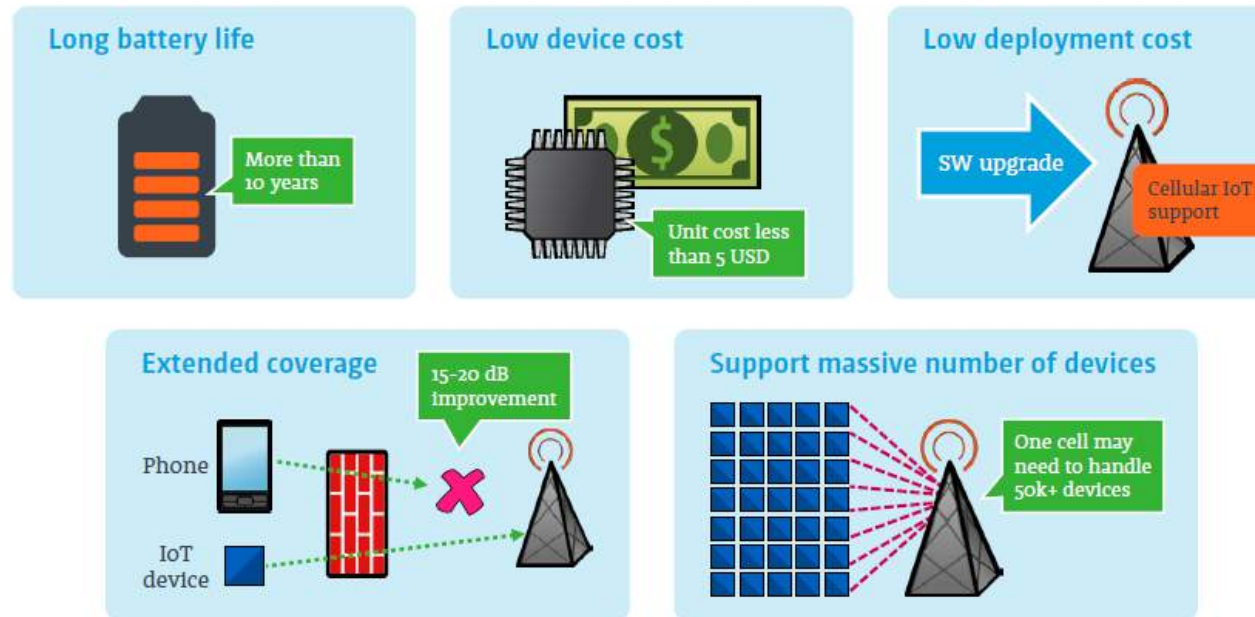


Figure 9. LPWA design targets

The key requirements and design targets for LPWA systems are:

- Long battery life
- Low device cost
- Low deployment cost
- Extended coverage
- Support for a massive number of devices

### 3-7- Cellular IoT benefits and disadvantages

#### 3-7-1- Advantages of cellular IoT

First of all, cellular networks offer global reach and interoperability. Cellular networks have been developed and deployed for over thirty years, and already cover 90 percent of the world's population. GSM will continue to offer superior coverage in many markets for years to come, with WCDMA and LTE coverage catching up. Additionally roaming

agreements between different operators allows devices to connect to the Internet from any location and network.

Cellular networks have a strong and large existing ecosystem. It includes a huge number of chipset, device and network equipment manufacturers, operators, application providers and many others. The 3GPP oversees the creation of cellular standards, and this standardization guarantees broad industry support for future developments and improvements.

Cellular networks provide flexibility to support many different types of IoT use cases. While many competing LPWA technologies are designed only for very low-end IoT applications, cellular networks can serve a wide range of applications with varying requirements. This includes supporting both massive IoT and critical IoT use cases.

Cellular networks include built-in Quality of Service (QoS) mechanisms, which are essential for many IoT applications. This enables a single network to correctly prioritize critical IoT applications, massive IoT applications, and voice and mobile-broadband traffic on the same carrier. Additionally, unlike most competing LPWA technologies, cellular networks operate on licensed spectrum, which means less interference. LPWA systems operating on unlicensed spectrum, where there can be many systems operating on the same frequency, will have a harder time guaranteeing QoS.

When it comes to scalability, cellular networks are designed from the ground up to handle very large volumes of mobile broadband (MBB) traffic. Compared to the MBB traffic volumes, the traffic from typical IoT applications will be small, even when there are millions of such applications connected to the network.

This means that existing cellular operators can start by first offering connectivity for a small number of IoT applications, and then expand (as the IoT market grows) with only small additional investment.

One major concern for the millions of connected IoT devices is security. Cellular networks have strong built-in security mechanisms. Subscribers are authenticated based on a physical SIM cards inserted to their devices. This SIM-based authentication method can be extended to IoT devices, with additional options of using an embedded SIM card (SIM chip embedded to the device) or by using a soft-SIM solution (software running on a tamper-proof environment in the device).

### **3-7-2- Disadvantages of cellular IoT**

Many people in the industry also have concerns about using cellular networks for IoT connectivity. The major issue that these people talk about is that the current cellular



networks have not been optimized for IoT. The networks have been designed with voice and mobile broadband (MBB) services in mind, and then needs of these services are very different from many IoT applications needs.

MBB services are generally characterized by bursts of data during active periods with a higher demand on downlink. However, many IoT applications have different traffic characteristics. There small and infrequent data is generated from a huge number of IoT devices, imposing higher traffic volumes on uplink. Examples of such uplink-centric infrequent data transmissions include smart metering devices and vending machines. Furthermore, most of the IoT devices are inexpensive with limited computational and power resources.

These requirements have not been thought of in current cellular networks. For example LTE technology was never designed to be super power efficient, to handle tens of thousands of devices per cell, or to support cheap, low complexity devices that only transport small amounts of data.

### 3-8- 3GPP work on MTC / IoT

Major work started from Release 12 onwards

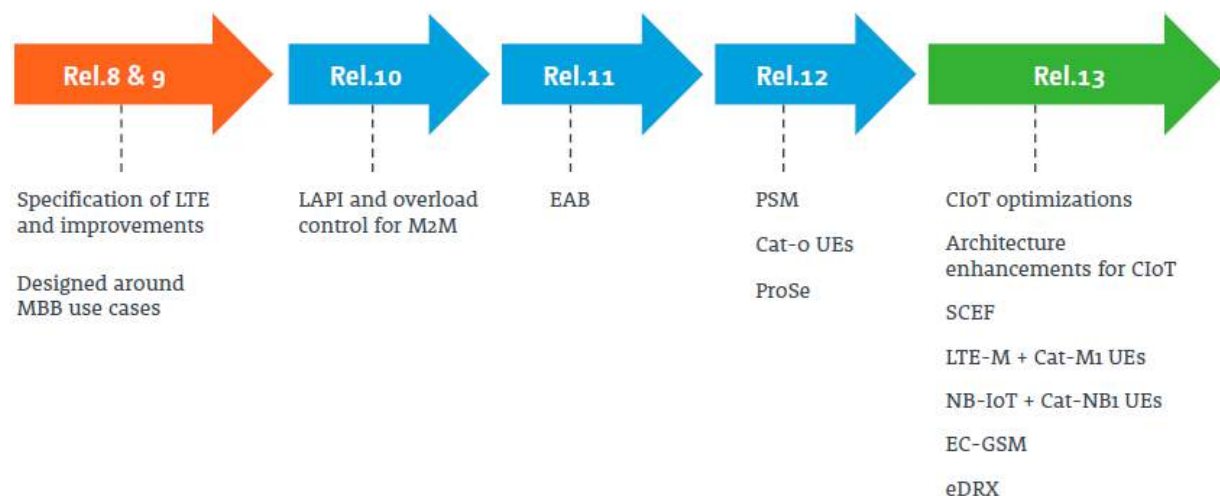


Figure 10. 3GPP work on MTC / IoT

#### 3-8-1- Extended Coverage GSM (EC-GSM)

Extended coverage GSM (EC-GSM) is a 3GPP specified Low Power Wide Area technology that can be deployed to existing GSM networks. This ensures coverage and accelerates time to-market. It is based on EDGE and designed to provide GSM networks with support for Massive IoT applications. More specifically it provides up to 20 dB

coverage extension compared to legacy GPRS, increased battery life, and support for a larger number of devices.

EC-GSM has been designed to be backwards-compatible with existing GPRS/EDGE networks, so that radio channel resources can be shared between IoT devices and legacy GSM/GPRS devices, as illustrated in Figure 59. ECGSM can be deployed to existing networks as a software upgrade, it doesn't require new hardware to the RAN or core networks. The first EC-GSM commercial launches have started in 2017, supported by all major mobile equipment, chipset and module manufacturers.

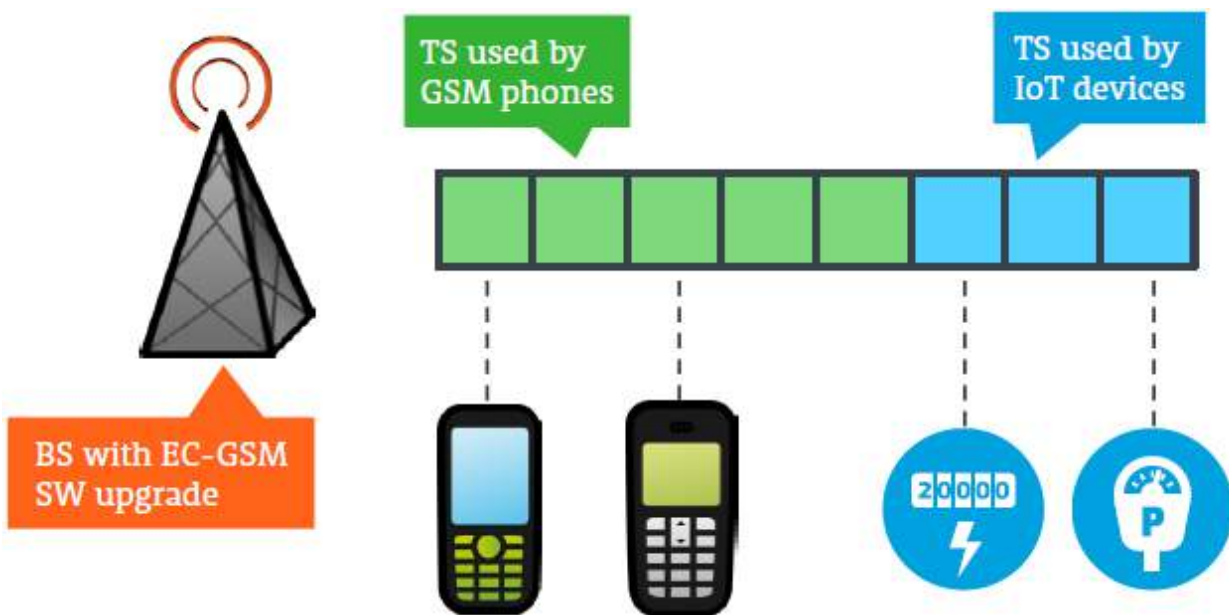


Figure 11. EC-GSM upgrade to existing networks

### 3-8-2- eMTC overview

Before NB-IoT specification, 3GPP had already started work on the design of another LTE radio access for supporting massive IoT applications. This technology is known as enhanced MTC (eMTC), sometimes also called LTEM.

The eMTC technology uses a new UE category, Cat-M1. This device category is designed to be low cost (similar cost to GSM/GPRS terminals) and provide long battery life (10 years with PSM and eDRX), as well as extended coverage (+15 dB by using repetitions and PSD boosting). Also Cat-M1 devices can be made in the new 20 dBm power class. Cat-M1 device data rate can range from around 10 kbps to 1Mbps, depending on the coverage needs.

eMTC can reuse existing LTE eNBs with SW upgrade, and can be deployed in any LTE spectrum. The idea is that the eMTC transmission (1.4 MHz or 6 PRB) can be embedded

within any existing LTE system bandwidth so that both eMTC and regular LTE device traffic is sent over same LTE radio channel. This is illustrated in Figure 12.

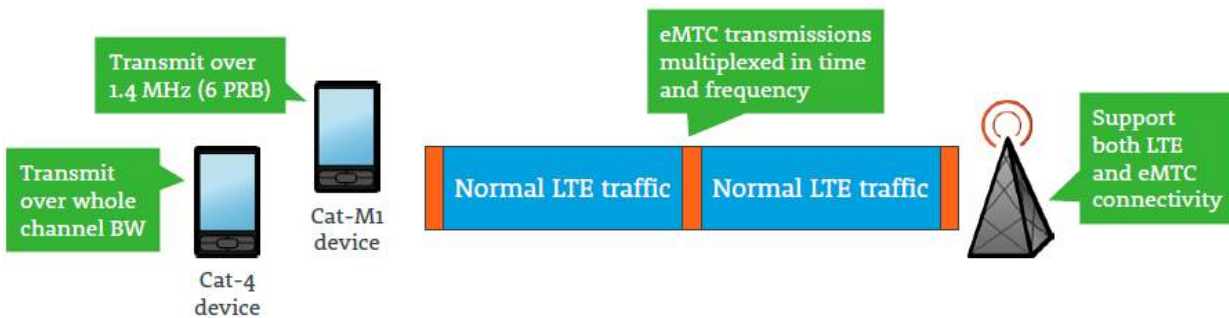


Figure 12. eMTC

### 3-8-3- NB-IoT overview

As part of Release 13, 3GPP has specified a new radio interface, the Narrowband Internet of Things (NB-IoT). As the name implies, NB-IoT has been optimized specially for IoT use cases and M2M communications.

There are many types of IoT applications, with different communication requirements. For example, a surveillance camera has to deliver large amounts of delay-sensitive UL data while typically being stationary, whereas devices used for fleet tracking have a small amount of data to transmit, while being highly mobile and needing optimized handovers.

NB-IoT was designed for another class of IoT devices. These “simple” devices are often stationary, and only need to send small amounts of non-delay sensitive data. Examples of such “simple” IoT devices include:

- Smart metering for electricity, gas, or water consumption
- Facility management services
- People and animal tracking
- Smart city infrastructure, such as street lamps, smart parking sensors or trash bins
- Connected industrial appliances, such as welding machines or air compressors

The number of these types IoT devices are expected to be very large, up to several orders of magnitude compared to traditional mobile devices. Due to their amount of required devices, they have to be very low cost. These devices are often installed at places without power supply, and so they run completely on battery. It may be very expensive to change the battery, because they may only be accessed by trained staff. Hence, in some cases the battery lifetime can even determine the lifetime of the whole device.

NB-IoT's design goals were to keep the devices simple as possible in order to reduce device costs and to minimize battery consumption. At the same time it is designed to offer significant coverage extension compared to traditional cellular, and support for a massive number of IoT devices.

### **3-9- Non-cellular IoT**

#### **3-9-1- Bluetooth Low Energy**

Bluetooth Low Energy (BLE) - introduced originally as a feature of Bluetooth version 4.0 - is a short range wireless technology capable of providing low energy point-to-point connections between devices. Generally, the point-to-point set-up includes a central device, such as a smartphone, which runs a dedicated application that is used to connect to the specific BLE device.

BLE is completely different from what we call Classic Bluetooth, which is used to connect our device to a variety of peripherals, like Bluetooth speakers, mice, keyboards and so on. BLE is based on new low energy Bluetooth communication specifications, also referred to as profiles. These profiles are not backwards compatible with older Bluetooth versions.

BLE operates on the same unlicensed 2.4 GHz band as Wi-Fi. The technology has a range of between 50 m to 100 m in line of sight. Indoors the practical range is reduced to around 10m to 20m.

The secret behind the low energy consumption of BLE is its radio, which is switched off for most of the time. The radio is turned on only for very short periods of time when a connection is established. Furthermore, transmissions are very short bursts of data, again, minimizing the time that the radio is powered on. This allows for BLE devices to run, for instance, on small coin-cell batteries, which can provide years of operating time.

BLE is best suited for short range applications that transfer small amounts of data periodically. Currently, the most prominent uses are wearable technology, such heart rate monitors, smart watches and fitness trackers. In addition, various sensors, beacons, actuators and smart meters use BLE.

#### **3-9-2- Wi-Fi HaLow**

Wi-Fi HaLow is the name for the new IEEE 802.11ah Wi-Fi standard developed by the Wi-Fi Alliance. Wi-Fi HaLow is a new type of Wi-Fi that is designed for low power connections, specifically with IoT applications in mind.

WiFi HaLow operates on unlicensed frequency bands below 1 GHz (900 MHz in the U.S.), much lower frequencies than the 2.4 and 5 GHz bands used by other mainstream Wi-Fi

technologies (such as IEEE 802.11 b/g/n/ac). It also promises to double the range of traditional Wi-Fi technologies, so in theory, it could extend to ranges of up to 1 km. You can see a comparison of Wi-Fi HaLow with other Wi-Fi technologies in Figure 13.

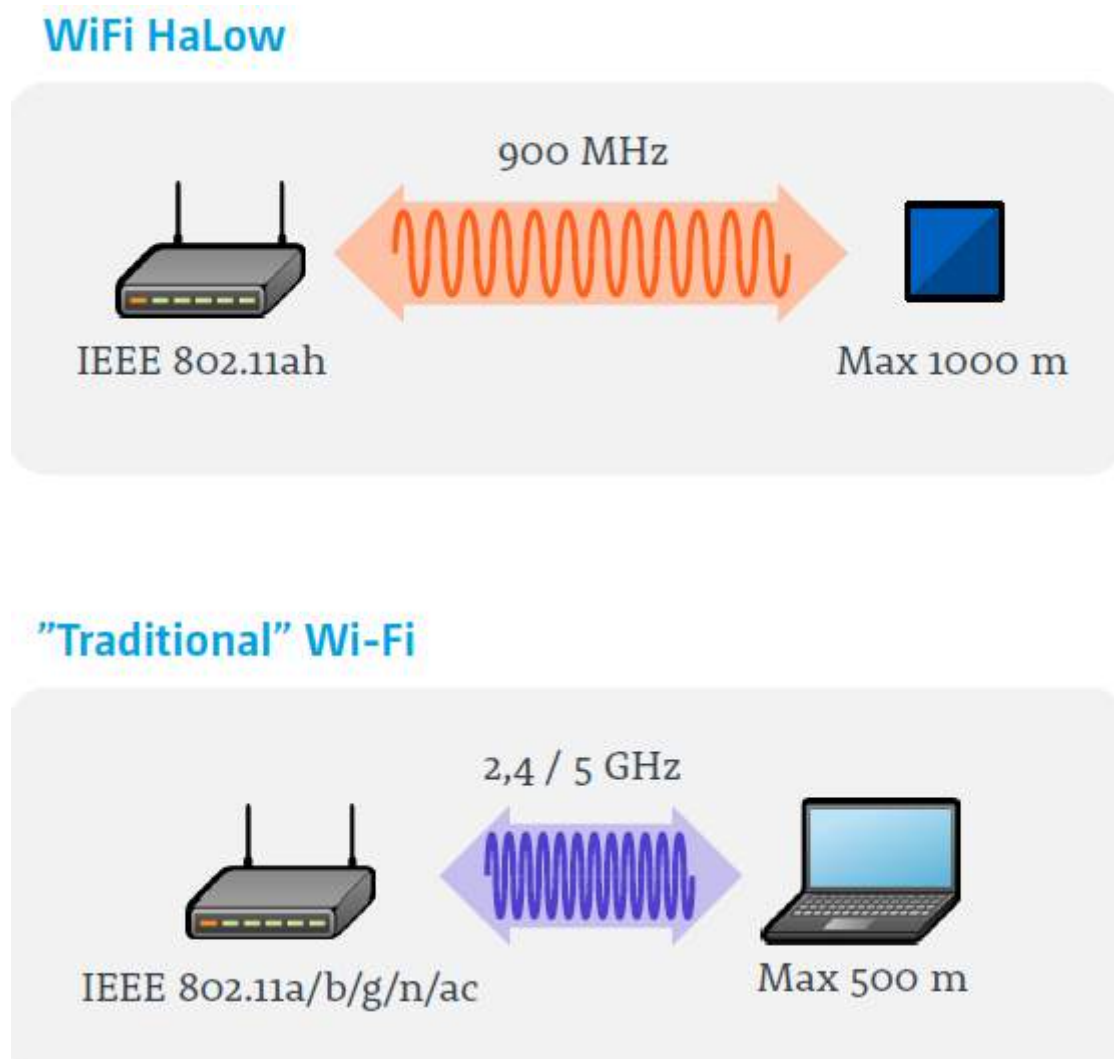


Figure 13. Wi-Fi HaLow vs. traditional Wi-Fi technologies

### 3-9-3- ZigBee

ZigBee is a low-power, short-range Personal Area Network (PAN) radio protocol. It's optimized for IoT applications such as Home Automation and energy monitoring. Most of the standard-based, low-power radio modules on the market are currently based on ZigBee.

The ZigBee architecture is illustrated in Figure 93. The range of a single ZigBee radio link is from 10 to 100 meters. A key feature of ZigBee is that it can form a mesh network, with a ZigBee node forwarding messages to and from other nodes. With its maximum of 4 hops a ZigBee network can easily span a single home.

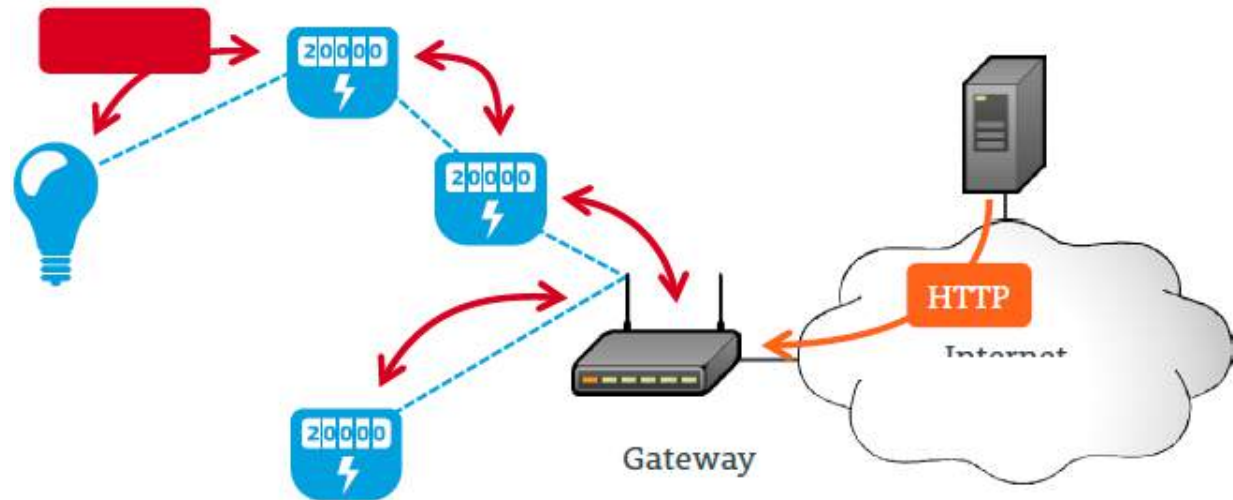


Figure 14. ZigBee architecture

ZigBee specifications are developed by the **ZigBee Alliance** ([zigbee.org](http://zigbee.org)). The current version of ZigBee is 3.0. It's a further development of the earlier ZigBee Pro, or ZigBee 2007 specification.

Figure 14 shows the ZigBee protocol stack. Note that ZigBee uses the IEEE 802.15.4 PHY and MAC layers. Other layers are specific to ZigBee. The network and security layer implements the mesh network functionality.

Note that ZigBee does not use IP. This is not a limitation for applications where both the client and server are connected to the ZigBee network, or where a gateway can be used. To directly participate in IoT frameworks such as OCF the ZigBee device would need an IPv6 address. The short packet structure of 802.15.4 makes it unsuitable for TCP, but UDP transport can still be supported.

To address the need for IP connectivity, the ZigBee Alliance has released the **ZigBee for IP** specification that provides direct IP access for ZigBee devices (but in a separate ZigBee network).

The ZigBee IP specification was originally created to server specific applications cases in home energy management. The **Thread group** offers a competing specification based on a clean-sheet design with 6LoWPAN on top of 802.15.4.

### 3-9-4- ZigBee vs. Z-Wave

ZigBee is often confused with Z-Wave. Both are based on 802.15.4, both support a mesh network topology and both are widely deployed in IoT networks. However, the systems

are incompatible. Originally developed as a proprietary home automation system, Z-Wave uses Frequency Shift Keying

(FSK) while ZigBee uses Direct Sequence Spread Spectrum (DS-SS). Z-Wave does not support the global 2.4 GHz ISM band. As the only provider of Z-Wave radios is Sigma Designs it does not suffer from vendor compatibility issues that are a problem for ZigBee.

### **3-9-5- LoRa**

LoRA stands for Long Range Radio. LoRa is an open-standard governed by the LoRa Alliance, it was developed by a company called Semtech. It is a wireless protocol designed for long range and low power communications. Targeting M2M and IoT networks, Lora enables public or multi tenant networks to connect a number of applications running on the same network.

Lora is similar to Sigfox as they both are mainly for applications that have many end-points and require Uplink only. Being a multiple access protocol it follows star-on-star topology to relay messages. Communication to the central server is done using gateways and done by sending information on different frequency channels and data rates using coded messages. This method is efficient as the messages are less likely to collide and interfere with one, it therefore increases the capacity of the gateway. LoRa provides mobility, a bi-directional communication which is secure, and localization services to provide simple, seamless interoperability among smart Things.

LoRa has several classes of end-point devices to address the different application needs, all these devices are bi-directional:

- Class A devices: these devices uplink transmission followed by two short downlink receive windows.
- Class B devices: In addition to downlink windows as described in Class A, these devices open extra receive windows at scheduled times.
- Class C devices: Other than when they are transmitting these devices have nearly continuously open receive windows, only closed when transmitting. They use a lot of power.

In Figure 15, LoRa Network architecture is shown.



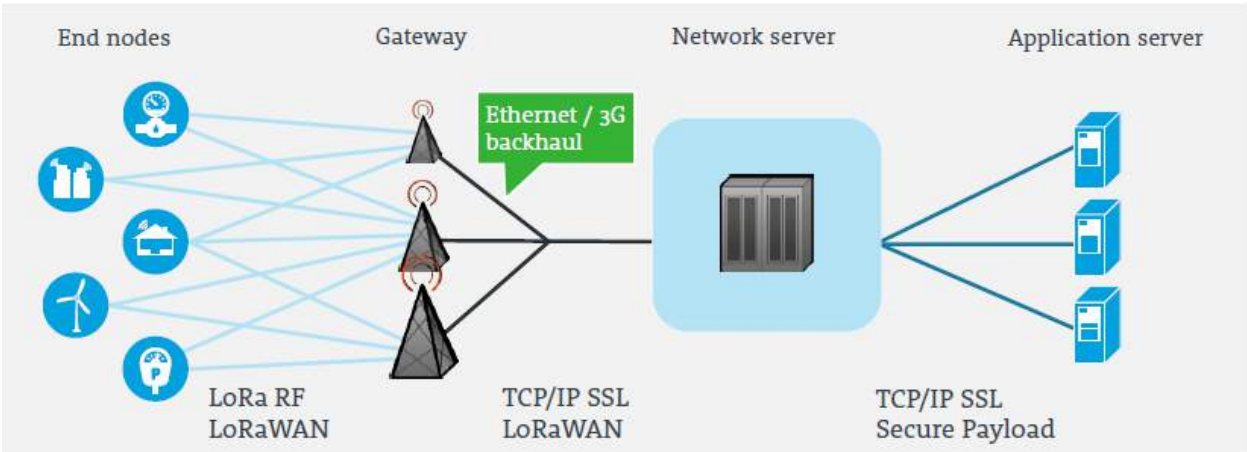


Figure 15. LoRa Network architecture

### 3-9-6- SigFox

Arguably has the most traction in the LPWAN space due to its successful marketing campaigns in Europe. It also boasts a great ecosystem of vendors including Texas Instruments, Silicon Labs, and Axom.

Sigfox is simple full-stack technology whereby a binary phase shift keying (BPSK) modulation scheme is used to send data. It uses an ultra-narrowband of 100 Hz, sending very small data (12 bytes) very slowly (300 baud). SigFox is an example of using a slow modulation rate to achieve longer range. Due to this design choice, SigFox is an excellent choice for applications where the system only needs to send small, infrequent bursts of data. Possible applications include parking sensors, water meters, or smart garbage cans. However, it also has major drawbacks; downlink capabilities are severely limited and collisions become a huge issue.

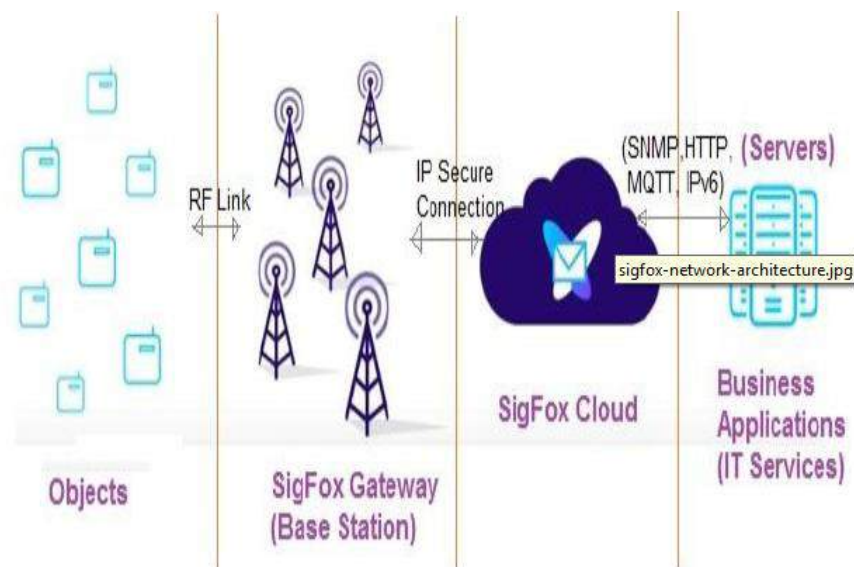




Figure 16. LoRa Network architecture

### 3-10- Technologies Comparison: LPWANs

#### 3-10-1 Transceiver parameters

- i. **Transmitter output power/radiated power**  
Typical values range (e.i.r.p.) between 200 mW to 4 W for the access stations and 5 mW to 500 mW for the end-points.
- ii. **Antenna characteristics**  
Most of the transmitters use omnidirectional antenna. Typical value ranges between 0 dBi to 6 dBi.
- iii. **Class of emission**  
There is no specific class of emission used for LPWAN systems. Most of the systems use complex or combination of digital modulations.
- iv. **Modulation bandwidth**  
This parameter depends upon the technology used. Typical modulation bandwidths range from 100 Hz to 500 kHz.
- v. **Unwanted emissions**  
Low power devices (LPD) must comply with the unwanted emissions set by relevant regulations and standards. Typical limits of the ITU Regions are based on Recommendation ITU-R SM.329 and are further described in the Report ITU-R SM.2153 on technical and operating parameters for short-range radio communication devices. These limits should be defined in accordance with services and systems allocations in adjacent bands.
- vi. **Receiver sensitivity**  
LPWAN systems have extremely high sensitivity (i.e. -140 dBm in 100 Hz) which enables low power devices and equipment to provide long range communication. This is a key characteristic of LPWAN systems, which rely on various techniques such as follows:  
Ultra-narrow bands (UNB) solutions, where high selectivity filtering combined with narrower signal bandwidth improves sensitivity threshold (see ETSI TR 103 435 V1.1.1).  
Direct Spread Spectrum or Chirp Spread Spectrum (CSS) techniques which reduce the sensitivity level below the noise floor thanks to coding gain depending on the spreading factor (see ETSI TR 103 526 V1.1.1).
- vii. **Other characteristics**  
Other characteristics mention in following table:

Parameter	LoRa	SigFox	EC-GSM	LTE-M	NB-IoT
Range (36)	<15Km	<50Km	<15Km	<11Km	<15Km
Maximum coupling loss (37)	157dB	153dB	164dB	160dB	164dB
Max peak data rate (37)	50kbps	100bps	74kbps	1Mbps	250Kbps
Spectrum	Unlicensed EU 868, 433MHz US 915MHz (41)	Unlicensed EU 868-869MHz US 902-928MHz (42)	GSM bands	LTE bands	LTE in-band, guard bands, stand-alone
Bandwidth	<500KHz (36)	100KHz (36)	200KHz per ch.(38)	1.08MHz (38)	180KHz (38)
Radio Tecnology	Spread Spectrum (36)	Ultra Narrow Band (39)	TDMA/FDMA	OFDM	OFDM
Bidirectional modes (37)	Yes	Yes	Yes	Yes	Yes
Voice (Ericsson)	No	No	No	Yes	No
Device max transmitted power	14dBm	20dBm	23,33dBm (38)	20, 23dBm (38)	23dBm (38)
Autonomy (36)	>10years	>10years	>10years	>10years	>10years

Parameter	LoRa	SigFox	EC-GSM	LTE-M	NB-IoT
Re-use existing cellular networks	No	No	yes	yes	yes
Link adaption	Yes	No	Yes	Yes	yes
Device categories	yes	No	yes	yes	yes
Operational mode	Public or private	Public	Public	Public	Public
Handover	No	No	Not seamless	yes	Not seamless
Data confidentiality (37)	Yes (AppSKey)	No	Partial (GEA4/5)	Yes (EEAx)	Yes (EEAx)
Network authentication (37)	Optional	No	UMTS AKA	LTE AKA	LTE AKA
Typical module cost (37)	Low	Very low	Low	Medium	Low
Technology availability	Now	Now	On trial	Now	Now

### **3-11- SATELLITE BASED IoT NETWORKS**

Normally, satellites and IoT do not seem to be natural partners in the communication world. However, due to the compulsions of some specific situations they meet each other in several instances. Therefore there are several reasons the IoT should be combined with the satellites to meet these special demands. Here in this section we present the major reasons for their conjugation. In Fig. 1 we show a satellite based IoT network. The coverage area of the satellite has been shown as an oval within which lies the IoT network. The IoT trans-receivers are the triangular towers and the red dots are the sensor nodes. Both the IoT and the satellite links are wireless.

#### **3-11-1- Motivation for Satellite IoT Integration**

##### **3-11-1-1- Reliability in the wireless applications**

Reliability of wireless communications is still a challenging issue. Normal wireless networks do not provide the high reliability required in the mission critical applications. These issues can be addressed through the satellite networks. Satellites are normally available with a better reliability than the cellular networks. With proper constellation arrangements satellites provide more than 99.9% availability which is much higher than the current cellular networks. This is essential for the mission critical applications such as disaster management and military communications. High availability ensures high reliability under diverse conditions.

##### **3-11-1-2- Larger and broader coverage of the IoT Networks**

IoT networks are generally deployed over the existing cellular infrastructure. The cellular networks are oriented according to the human presence. Therefore the coverage of the cellular networks are very much limited. In case of the very high towers the coverage radius is around 20 km. High towers are not suitable for green applications as their radiation densities are high. However, satellite networks can cover a large area and they do not discriminate any part of the terrain. Thus, for a large scale multi-purpose deployment of IoT satellite based IoTs are preferred over the cellular IoTs.

##### **3-11-1-3- Better Security and Protection**

SIoT networks are very much oriented according to the presence and availability of the satellites. Intercepting and manipulating these systems are very rare and needs a lot of addition to the above, satellite networks have added security measures such as anti-jamming mechanisms and strong cryptographic coding which cannot be manipulated easily.

#### **3-11-1-4- Economical and faster rural deployment**

Economics plays an important role in every communication technology. In case of IoT, it has even more important roles as the numbers of ground terminals or the sensors are too many. Rural deployment of any IoT is very much dependent on the associated economy. SIoT is very promising in this regard as satellites have wider coverage and the satellite based IoTs need less resources than the cellular IoTs. Of course, the specific energy efficient versions of the IoTs would serve this sector better.

#### **3-11-1-4- Multicasting of services**

Each satellite has its own coverage area. These are dependent of their beam widths. Normally, the coverage area of a satellite is much larger than the cellular transmitters. Therefore multicasting through satellites is much easier and cost effective than the cellular transmissions. For the IoT based multicasting where the energy constraints are very much stringent it is very much beneficial.

#### **3-11-1-5- Longevity of the wireless networks**

In general the longevity of the satellite constellations is much higher than the cellular networks. The main problem with the cellular networks in this regard is the changing situations. Every decade several changes come into picture in the cellular networks. In the recent decades we see a new generation of mobile communication is replacing the existing ones. However, the satellites networks remain active for more than two to three decades. Therefore, the longevity of satellite networks ensures its supported ground networks to have a longer presence than the cellular networks.

### **3-11-2- APPLICATIONS OF SATELLITE BASED IOT SYSTEMS**

There are several applications of the SIoT networks. Some of them are the existing ones and the rest are emerging in the changing scenarios. Right now the major focus is on the critical applications where the availability of the network has to be more than 99%. In addition to that other advantages of satellite networks such as larger coverage play the main roles in the SIoT applications.

- i. Mission Critical Applications
- ii. Location Based Services
- iii. Navigation Systems
- iv. Agriculture
- v. Tracking
- vi. Healthcare

## 4- Chapter 4: IoT Frequency Bands

Spectrum was identified as an infrastructure and device enabler for IoT. It was noted that the immediate focus in spectrum planning is concerned with accommodating M2M and IoT applications within the existing licensing framework and the identification of candidate spectrum bands to address expected future demand.

When it comes to spectrum to support M2M and IoT applications, a mix of licensing arrangements and variety of frequency bands may be required to support different IoT use cases (see Figure 17).

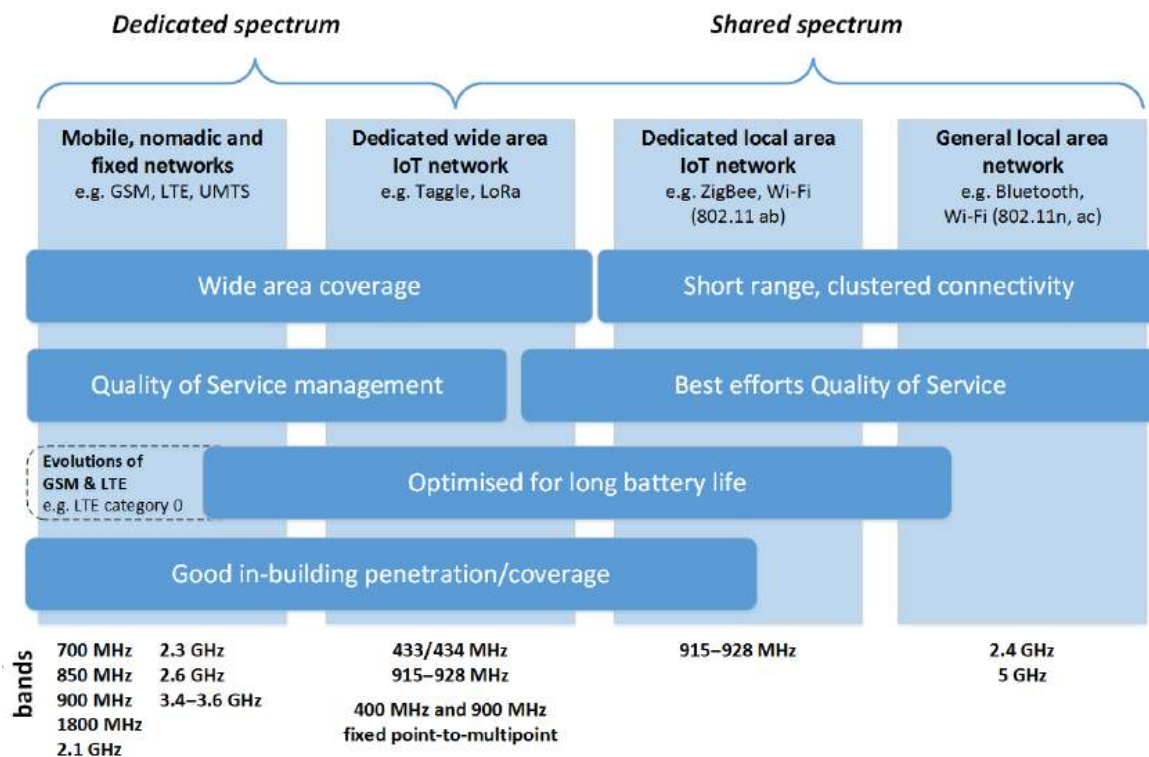


Figure 17. IoT Frequency Bands

### 4-1- Unlicensed Bands (class Licensing)

#### 4-1-1- Short Range Devices

Currently, spectrum that is globally available at a low cost (or free as class licensed spectrum) is in the Industrial Scientific Medical (ISM) bands, which include the 900 MHz band, the 2.4 GHz band and the 5.8 GHz band. ISM bands are to a large degree globally harmonized although the regulatory arrangements can vary. In figure 18 is shown list of some SRD frequency bands.

RADIO TECHNOLOGIES FOR THE PHYSICAL LAYER OF WIRELESS INTERNET OF THINGS

Category	Technology	Governing Body / Standard	Frequency bands	Capacity (kbps)	Multiple Access	Modulation
Low power versions of LANs & PANs	WiFi	WiFi Alliance IEEE 802.11a/b/g/n/ac	2.4 GHz, 5 GHz	11000-6900000	OFDM, DSSS, OFDMA	CCK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
	Bluetooth (4.0/4.1/4.2 LE)	Bluetooth special interest group (SIG)	2.4 GHz	1024	TDMA	ASK, FSK
	ZigBee	ZigBee Alliance IEEE 802.15.4	<1 GHz, 2.4 GHz	250	CSMA/CA	DSSS, BPSK, O-QPSK
	Thread	Thread Group IEEE 802.15.4	2.4 GHz	250	CSMA/CA	DSSS, O-QPSK
	Z-wave	Z-Wave Alliance ITU G.9959	<1 GHz	100	TDMA	FSK, GFSK
	EnOcean	EnOcean Alliance ISO/IEC 14543-3-1x	<1 GHz	125	TDMA	ASK, FSK
	WiGig	WiFi Alliance IEEE 802.11ad	60 GHz	6760000	SC-SS	$\pi/2$ -BPSK, QPSK, QAM16, SQPSK, QAM64
	Dash7	Dash7 Alliance	<1 GHz	167	TDMA	(G)FSK

Figure 18. List of some SRD frequency bands.

#### 4-1-2- LPWANs

Most LPWANs operate in the unlicensed ISM bands centered at 2.4 GHz, 868/915 MHz, 433 MHz, and 169 MHz, depending on the region of operation. The radio emitters operating in these frequency bands are commonly referred to as “Short Range Devices” a rather generic term that delivers the idea of coverage ranges of few meters, which was indeed the case for the previous ISM wireless systems. Nonetheless, the ERC Recommendation 70-03 specifies that “The term Short Range Device (SRD) is intended to cover the radio transmitters which provide either uni-directional or bidirectional communication which have low capability of causing interference to other radio equipment.” Therefore, there is no explicit mention of the actual coverage range of such technologies.

LPWAN solutions are indeed examples of “short-range devices” with cellular-like coverage ranges, in the order of 10–15 km in rural areas, and 2–5 km in urban areas. This is possible thanks to a radically new physical layer design, aimed at very high receiver sensitivity. For example, while the nominal sensitivity of ZigBee and Bluetooth receivers is about -125 dBm and -90 dBm, respectively, the typical sensitivity of a LPWAN receiver is around -150 dBm

The downside of these long-range connections is the low data rate, which usually ranges from few hundred to few thousand bit/s, significantly lower than the bitrates supported by the actual short-range technologies, e.g., 250 Kbit/s in ZigBee and 1–2 Mbit/s in Bluetooth. However, because of the signaling overhead and the multi-hop packet forwarding method, the actual flow-level throughput provided by such short-range technologies is generally

much lower than the nominal link-layer bitrate, settling to values that are comparable to those reached by the single-hop LPWANs. While such low bitrates are clearly unsatisfactory for most common data hungry network applications, many Smart City and IoT services are expected to generate a completely different pattern of traffic, characterized by sporadic and intermittent transmissions of very small packets (typical of monitoring and metering applications, remote switching control of equipment, and so on). Furthermore, many of these applications are rather tolerant to delays and packet losses and, hence, are suitable for the connectivity service provided by LPWANs.

Another important characteristic of LPWANs is that the things, i.e., the end devices, are connected directly to one (or more) gateway with a single-hop link, very similar to the classic cellular network topology. This greatly simplifies the coverage of large areas, even nation-wide, by re-using the existing infrastructure of the cellular networks. For example, LoRa TM systems are being deployed by telecommunication operators like Orange and Bouygues Telecom in France, by Swisscom in Switzerland, and by KPN in the Netherlands, while SIGFOX™ has already deployed a nation-wide access network for M2M and IoT devices in many central European countries, from Portugal to France. Furthermore, the star topology of LPWANs makes it possible to have greater control of the connection latency, thus potentially enabling the support of interactive applications that require predictable response times such as, for example, the remote control of street lights in a large city, the operation of barriers to limited-access streets, the intelligent control of traffic lights, and so on.

Besides the access network, the similarity between LPWANs and legacy cellular systems further extends to the bridging of the technology-specific wireless access to the IP-based packet switching core network. Indeed, the LPWAN gateways play a similar role as the Gateway GPRS Support Node (GGSN) in GPRS/UMTS networks, or the Evolved Packet Core in LTE, acting as point-of-access for the end devices to the IP-based core network and forwarding the data generated by things to a logic controller, usually named Network Server.

Therefore, LPWANs inherit the basic aspects of the legacy cellular systems architecture that, however, is stripped of most advanced features, such as the management of user mobility and resource scheduling. The combination of the simple but effective topology of cellular systems with a much lighter management plane, makes the LPWAN approach particularly suitable to support services with relatively low Average Revenue Per User, such as those envisioned in the Smart City scenario.

In this section there are quickly overview of three of the most prominent technologies for LPWANs, namely SIGFOX, Ingenu, and LoRa. In particular, the LoRa technology, which is gaining more and more momentum, and whose specifications are publicly available, thus

making it possible to appreciate some of the technical choices that characterize LPWAN solutions.

#### **4-1-2-1- SIGFOX**

The first LPWAN technology proposed in the IoT market, was founded in 2009 and has been growing very fast since then. The SIGFOX physical layer employs an Ultra Narrow Band (UNB) wireless modulation, while the network layer protocols are the “secret sauce” of the SIGFOX network and, as such, there exists basically no publicly available documentation. Indeed, the SIGFOX business model is that of an operator for IoT services, which hence does not need to open the specifications of its inner modules. The first releases of the technology only supported unidirectional uplink communication, i.e., from the device towards the aggregator; however bi-directional communication is now supported. SIGFOX<sup>TM</sup> claims that each gateway can handle up to a million connected objects, with a coverage area of 30–50 km in rural areas and 3–10 km in urban areas.

#### **4-1-2-2- Ingenu**

An emerging star in the landscape of LPWANs is Ingenu, a trademark of On-Ramp Wireless, a company headquartered in San Diego (USA). On-Ramp Wireless has been pioneering the 802.15.4k standard. The company developed and owns the rights of the patented technology called Random Phase Multiple Access (RPMA), which is deployed in different networks. Conversely to the other LPWAN solutions, this technology works in the 2.4 GHz band but, thanks to a robust physical layer design, can still operate over long-range wireless links and under the most challenging RF environments.

#### **4-1-2-3- LoRa**

LoRa is a new physical layer LPWAN solution, which has been designed and patented by Semtech Corporation that also manufactures the chipsets. More specifically, the PHY is a derivative of Chirp Spread Spectrum (CSS), where the innovation consists in ensuring the phase continuity between different chirp symbols in the preamble part of the physical layer packet, thus enabling a simpler and more accurate timing and frequency synchronization, without requiring expensive components that generate a stable local clock in the LoRa node.

The technology employs a spreading technique, according to which a symbol is encoded in a longer sequence of bits, thus reducing the signal to noise and interference ratio required at the receiver for correct reception, without changing the frequency bandwidth of the wireless signal. The length of the spreading code can be varied, thus making it possible to provide variable data rates, giving the possibility to trade throughput for coverage range, or link robustness, or energy consumption.

The system has been designed to work in the 169 MHz, 433 MHz and 915 MHz bands in the USA, but in Europe it works in the 868 MHz band, the radio emitters are required to



adopt duty cycled transmission (1% or 0.1%, depending on the sub-band), or the so-called Listen Before Talk (LBT) Adaptive Frequency Agility (AFA) technique, a sort of carrier sense mechanism used to prevent severe interference among devices operating in the same band. LoRa (as well as SIGFOX) uses the duty cycled transmission option only, which limits the rate at which the end device can actually generate messages. However, by supporting multiple channels, LoRa TM makes it possible for an end node to engage in longer data exchange procedures by changing carrier frequency, while respecting the duty cycle limit in each channel.

	<b>SIGFOX<sup>TM</sup></b>	<b>Ingenu<sup>TM</sup></b>	<b>LoRa<sup>TM</sup></b>
Coverage range (km)	rural: 30–50 urban: 3–10	$\approx 15$	rural: 10–15 urban: 3–5
Frequency bands (MHz)	868 or 902	2400	various, sub-GHz
ISM band	✓	✓	✓
Bi-directional link	✓	✗	✓
Data rate (Kbps)	0.1	0.01–8	0.3–37.5
Nodes per BS	$\approx 10^6$	$\approx 10^4$	$\approx 10^4$

Figure 19. Non cellular LPWAN compression

#### 4-1-2-3- Frequency usage for LPWAN

A summary Frequency usage in ITU regions is shown in figure 20.

<b>Frequency range</b>	<b>Relevant Recommendation and Report</b>	<b>Remarks</b>	<b>Region 1</b>	<b>Region 2</b>	<b>Region 3</b>
865-870 MHz	Rec. ITU-R SM.1896 Report ITU-R SM.2153	The whole of this band can be considered as a tuning range. Only parts of this tuning range are operationally available for LPWAN in a number of countries due to the use by commercial mobile systems or restrictions on the scope of SRD applications. See national regulations.	Available	Not available	Available in some countries
902-915 MHz	Rec. ITU-R SM.1896 Report ITU-R SM.2153	902-928 MHz is an ISM band in Region 2 (RR No. <b>5.150</b> ). The whole band can be considered as a tuning range. This band is not operationally available for LPWAN in a number of countries including in Region 2, due to the use by commercial mobile systems	Not available	Available in some countries	Not available
915-928 MHz	Rec. ITU-R SM.1896 Report ITU-R SM.2153	902-928 MHz is an ISM band in Region 2 (RR No. <b>5.150</b> ). The whole band can be considered as a tuning range. Only parts of this tuning range are operationally available for LPWAN in a number of countries due to the use by commercial mobile systems or restrictions on the scope of SRD applications. See national regulations.	Available in some countries.	Available	Available in some countries

Figure 20. frequency usage for LPWAN

## 4-2- Licensed Bands

### *Why use licensed spectrum solutions?*

Mobile operators already provide reliable, end-to-end secured IoT platforms that allow customers to scale and manage their business requirements. They also have unrivalled global network coverage as well as technical and business support to react to a customer's changing needs. As trusted providers of reliable solutions, operators and their ecosystem partners are therefore best placed to extend their reach to serve the full range of IoT applications.

This means solutions deployed in licensed spectrum will:

- Support very low in power consumption – a battery life measured in years, in excess of 10 years for some applications,
- Be optimized for brief messages – about the length of an SMS,
- Have a very low device unit cost – the connectivity module will eventually cost a few dollars,
- Have good coverage both indoors and outdoors in previously unreachable locations, often beyond power sources,
- Be easy to install on to current networks, reusing existing cellular infrastructure wherever possible,
- Be scalable by being able to support large numbers of devices over a wide geographic area,
- Deliver end-to-end secure connectivity and support for authentication appropriate to the IoT application,
- Be able to be integrated into a mobile operator's unified IoT platform.

In licensed spectrum, IoT LPWA standards are primarily developed and implemented by the organizations that are already involved in the development and implementation of mobile networks. For operators of mobile networks and vendors of mobile network equipment, the existing platforms provide a good starting point for provisioning LPWA IoT connectivity. The main technical engineering challenges are to allow the existing standards to work in low power use cases, while maintaining as much compatibility with, and as much as the performance of existing standards as possible.

Development of mobile-based LPWA IoT connectivity is focused on the following design goals:

- Simplifying standards and thereby hardware requirements, to allow devices to be built at a cost lower than \$5.
- Providing long-range coverage, even more so than existing mobile networks, at the expense of data throughput.

- Providing low-power operation, such that a device will be able to operate for 10 years on a single battery given it transmits only a few messages per day.

The main technologies for LPWA IoT in licensed spectrum are those currently developed or under development by the 3GPP. These technologies are designed as add-ons to currently existing mobile cellular networks, employing parts of spectrum currently allocated to these networks. The first addition to the LTE standard in the direction of LPWA IoT connectivity are the ‘category 1’ (introduced in Release 8) and ‘category 0’ (Release 12) device categories. These categories define profiles for low-power, low-cost devices with reduced connectivity needs.

As the cost, power and connectivity of category 0 and category 1 device profiles still exceeds the typical requirements for true IoT devices, new standards are in development aimed at even lower cost, lower power and lower bitrate scenarios. Currently there are two separate tracks of standardization within 3GPP regarding cellular LPWA IoT, of which the technology is usable within the time horizon for this study. Both are evolutions of current LTE technology under the label ‘LTE Category M’, which comes in two flavors:

	Cat-4 device	Cat-1 device	Cat-0 device	Cat-M1 device	Cat-NB1 device
Modem complexity	100%	80%	40%	20%	10%
DL max data rate	150 Mbps	10 Mbps	1 Mbps	1 Mbps	~200 kbps
UL max data rate	50 Mbps	5 Mbps	1 Mbps	1 Mbps	~200 kbps
Antennas	2	1	1	1	1
Duplex mode	Full duplex	Full duplex	Full/half duplex	Full/half duplex	Half duplex
Channel bandwidth	20 MHz	20 MHz	20 MHz	1.4 MHz	180 kHz
Transmit power	23 dBm	23 dBm	23 dBm	20/23 dBm	20/23 dBm
Max coupling loss	144 dB	144 dB	144 dB	156 dB	164 dB

Figure 20. 3GPP development

#### 4-2-1- NB-IoT Frequency bands

There are 26 NB-IoT frequency bands in total, more than 60% of them are in the sub-GHz frequency range, and less than 30% are above the 1800 MHz. Four NB-IoT frequency bands are allocated for global use, and there are five regional frequency allocations. NB-IoT spectrum does not include Time Division Duplex (TDD) bands. NB-IoT is positioned as a highly robust and power-efficient protocol with a low-bandwidth, which is reflected by the low band-heavy spectrum profile. The frequency bands is shown figure 21.

#### **4-2-2-LTE Cat M1 Frequency Bands**

LTE Cat M1 provides more bandwidth compared to NB-IoT, and the LTE Cat M1 spectrum also contains more bands in the higher range. Over 20% of the 29 frequency bands allocated for Cat M1 are in the above 2 GHz range, compared to 15% in NB-IoT.

Five Cat M1 frequency bands are allocated for global use. Six regional frequency allocations include also a few TDD bands in China. The frequency bands is shown figure 22.

#### **4-2-3-LTE Cat 1 Frequency Bands**

LTE Cat 1 spectrum is nearly evenly split between sub-GHz bands (55%), and bands above the 1.8 GHz (45%). Five LTE Cat 1 frequency bands are allocated for global use, and there are six regional frequency allocations. The frequency bands is shown figure 23.

#### **4-2-4- EC-GSM IoT Frequency**

Extended Coverage GSM IoT protocol spectrum is allocated across 13 GSM/EDGE frequency bands ranging from 395 MHz to 1960 MHz In addition to the globally allocated bands, there are three regional frequency allocations for EC-GSM IoT. The frequency bands is shown figure 24.

Brand	Name	Downlink (MHz)			Bandwidth (UL/DL) (MHz)	Uplink (MHz)			Duplex spacing (MHz)	Duplex Mode FDD/TDD	Geographical Area	3GPP Release	Downlink (Earfan)			Uplink (Earfan)	
		Low	Middle	High		Low	Middle	High					Low	Middle	High	Low	Middle
1	2100	2110	2140	2170	60	1920	1950	1980	190	FDD	Global	13	0	300	599	18000	18300
2	1900 PCS	1930	1960	1990	60	1850	1880	1910	80	FDD	NAR	13	600	900	1199	18600	18900
3	1800+	1805	1842,5	1880	75	1710	1747,5	1785	95	FDD	Global	13	1200	1575	1949	19200	19575
4	AWS-1	2110	2132,5	2155	45	1710	1732,5	1755	400	FDD	NAR	15	1950	2175	2399	19950	20175
5	850	869	881,5	894	25	824	836,5	849	45	FDD	NAR	13	2400	2525	2649	20400	20525
8	900 GSM	925	942,5	960	35	880	897,5	915	45	FDD	Global	13	3450	3625	3799	21450	21625
11	1500 Lower	1475,9	1485,9	1495,9	20	1427,9	1437,9	1447,9	48	FDD	Japan	14	4750	4850	4949	22750	22850
12	700 a	729	737,5	746	17	699	707,5	716	30	FDD	NAR	13	5010	5095	5179	23010	23095
13	700 c	746	751	756	10	777	782	787	-31	FDD	NAR	13	5180	5230	5279	23180	23230
14	700 P5	758	763	768	10	788	793	798	-30	FDD	NAR	15	5280	5330	5379	23280	23330
17	700 b	734	740	746	12	704	710	716	30	FDD	NAR	13	5730	5790	5849	23730	23790
18	800 Lower	860	867,5	875	15	815	822,5	830	45	FDD	Japan	13	5850	5925	5999	23850	23925
19	800 Upper	875	882,5	890	15	830	837,5	845	45	FDD	Japan	13	6000	6075	6149	24000	24075
20	800 DD	791	806	821	30	832	847	862	-41	FDD	EMEA	13	6150	6300	6449	24150	24300
21	1500 Upper	1495,9	1503,4	1510,9	15	1447,9	1455,4	1462,9		FDD	Japan	14	6450	6525	6599	24459	24525
25	1900+	1930	1962,5	1995	65	1850	1882,5	1915	80	FDD	NAR	14	8040	8365	8689	26040	26365
26	850+	859	876,5	894	35	814	831,5	849	45	FDD	NAR	13	8690	8865	9039	26690	26865
28	700 APT	758	780,5	803	45	703	725,5	748	55	FDD	APAC,EU	13	9210	9435	9659	27210	27435
31	450	462,5	465	467,5	5	452,5	455	457,5	10	FDD	Global	14	9870	9895	9919	27760	27785
66	AWS-3	2110	2155	2200	90 / 70	1710	1745	1780	400	FDD	NAR	13	66436	66886	67335	131972	132322
70	AWS-4	1995	2007,5	2020	25 / 15	1695	1702,5	1710	300	FDD	NAR	14	68336	68461	68585	132972	133047
71	600	617	634,5	652	35	663	680,5	698	-46	FDD	NAR	15	68586	68761	68935	133122	133297
72	450 PMR/PAMR	461	463,5	466	5	451	453,5	456	10	FDD	EMEA	15	68936	68961	68985	133472	133497
73	450 APAC	460	462,5	465	5	450	452,5	455	10	FDD	APAC	15	68986	69011	69035	133522	133547
74	L-band	1475	1496,5	1518	43	1427	1448,5	1470	43	FDD	NAR	15	69036	69251	69465	133572	133787
85	700 a+	728	737	746	18	698	707	716	30	FDD	NAR	15	70366	70456	70545	134002	134097

Figure 21. Global NB-IoT frequency bands

Brand	Name	Downlink (MHz)			Bandwidth (UL/DL) (MHz)	Uplink (MHz)			Duplex spacing (MHz)	Duplex Mode FDD/TDD	Geographical Area	3GPP Release	Downlink (Earfcn)			Uplink (Earfcn)	
		Low	Middle	High		Low	Middle	High					Low	Middle	High	Low	Middle
1	2100	2110	2140	2170	60	1920	1950	1980	190	FDD	Global	8	0	300	599	18000	183
2	1900 PCS	1930	1960	1990	60	1850	1880	1910	80	FDD	NAR	8	600	900	1199	18600	189
3	1800+	1805	1842,5	1880	75	1710	1747,5	1785	95	FDD	Global	8	1200	1575	1949	19200	195
4	AWS-1	2110	2132,5	2155	45	1710	1732,5	1755	400	FDD	NAR	8	1950	2175	2399	19950	201
5	850	869	881,5	894	25	824	836,5	849	45	FDD	NAR	8	2400	2525	2649	20400	205
7	2600	2620	2655	2690	70	2500	2535	2570	120	FDD	EMEA	8	2750	3100	3449	20750	211
8	900 GSM	925	942,5	960	35	880	897,5	915	45	FDD	Global	8	3450	3625	3799	21450	216
11	1500 Lower	1475,9	1485,9	1495,9	20	1427,9	1437,9	1447,9	48	FDD	Japan	8	4750	4850	4949	22750	228
12	700 a	729	737,5	746	17	699	707,5	716	30	FDD	NAR	8,4	5010	5095	5179	23010	230
13	700 c	746	751	756	10	777	782	787	-31	FDD	NAR	8	5180	5230	5279	23180	232
14	700 PS	758	763	768	10	788	793	798	-30	FDD	NAR	8	5280	5330	5379	23280	233
18	800 Lower	860	867,5	875	15	815	822,5	830	45	FDD	Japan	9	5850	5925	5999	23850	239
19	800 Upper	875	882,5	890	15	830	837,5	845	45	FDD	Japan	9	6000	6075	6149	24000	240
20	800 DD	791	806	821	30	832	847	862	-41	FDD	EMEA	9	6150	6300	6449	24150	243
21	1500 Upper	1495,9	1503,4	1510,9	15	1447,9	1455,4	1462,9	48	FDD	Japan	9	6450	6525	6599	24450	245
25	1900+	1930	1962,5	1995	65	1850	1882,5	1915	80	FDD	NAR	10	8040	8365	8689	25040	263
26	850+	859	876,5	894	35	814	831,5	849	45	FDD	NAR	11	8690	8865	9039	25690	268
27	800 SMR	852	860,5	869	17	807	815,5	824	45	FDD	NAR	11,1	9040	9125	9209	27040	271
28	700 APT	758	780,5	803	45	703	725,5	748	55	FDD	APAC,EU	11,1	9210	9435	9659	27210	274
31	450	462,5	465	467,5	5	452,5	455	457,5	10	FDD	Global	12	9870	9895	9919	27760	277
39	TD 1900+	1880	1900	1920	40	TDD	TDD	TDD	-	TDD	China	8	38250	38450	38649	TDD	TD
40	TD 2300	2300	2350	2400	100	TDD	TDD	TDD	-	TDD	China	8	38650	39150	39649	TDD	TD
41	TD 2500	2496	2593	2690	194	TDD	TDD	TDD	-	TDD	Global	10	39650	40620	41589	TDD	TD
66	AWS-3	2110	2155	2200	90 / 70	1710	1745	1780	400	FDD	NAR	13,2	66436	66886	67335	131972	1323
71	600	617	634,5	652	35	663	680,5	698	-46	FDD	NAR	15	68586	68761	68935	133122	1332
72	450 PMR/PAMR	461	463,5	466	5	451	453,5	456	10	FDD	EMEA	15	68936	68961	68985	133472	1334
73	450 APAC	460	462,5	465	5	450	452,5	455	10	FDD	APAC	15	68986	69011	69035	133522	1335
74	L-band	1475	1496,5	1518	43	1427	1448,5	1470	43	FDD	NAR	15	69036	69251	69465	133572	1337
85	700 a+	728	737	746	18	698	707	716	30	FDD	NAR	15,2	70366	70456	70545	134002	1340

Figure 22- Global LTE CAT M1 frequency bands



Brand	Name	Downlink (MHz)			Bandwidth (UL/DL) (MHz)	Uplink (MHz)			Duplex spacing (MHz)	Duplex Mode FDD/TDD	Geographical Area	3GPP Release	Downlink (Earfcn)			Uplink (Earfcn)	
		Low	Middle	High		Low	Middle	High					Low	Middle	High	Low	Middle
1	2100	2110	2140	2170	60	1920	1950	1980	190	FDD	Global	8	0	300	599	18000	18300
2	1900 PCS	1930	1960	1990	60	1850	1880	1910	80	FDD	NAR	8	600	900	1199	18600	18900
3	1800+	1805	1842,5	1880	75	1710	1747,5	1785	95	FDD	Global	8	1200	1575	1949	19200	19575
4	AWS-1	2110	2132,5	2155	45	1710	1732,5	1755	400	FDD	NAR	8	1950	2175	2399	19950	20175
5	850	869	881,5	894	25	824	836,5	849	45	FDD	NAR	8	2400	2525	2649	20400	20525
7	2600	2620	2655	2690	70	2500	2535	2570	120	FDD	EMEA	8	2750	3100	3449	20750	21100
8	900 GSM	925	942,5	960	35	880	897,5	915	45	FDD	Global	8	3450	3625	3799	21450	21625
12	700 a	729	737,5	746	17	699	707,5	716	30	FDD	NAR	8,4	5010	5095	5179	23010	23095
13	700 c	746	751	756	10	777	782	787	-31	FDD	NAR	8	5180	5230	5279	23180	23230
18	800 Lower	860	867,5	875	15	815	822,5	830	45	FDD	Japan	9	5850	5925	5999	23850	23925
20	800 DD	791	806	821	30	832	847	862	-41	FDD	EMEA	9	6150	6300	6449	24150	24300
26	850+	859	876,5	894	35	814	831,5	849	45	FDD	NAR	11	8690	8865	9039	26690	26865
28	700 APT	758	780,5	803	45	703	725,5	748	55	FDD	APAC,EU	11,1	9210	9435	9659	27210	27435
31	450	462,5	465	467,5	5	452,5	455	457,5	10	FDD	Global	12	9870	9895	9919	27760	27785
39	TD 1900+	1880	1900	1920	40	TDD	TDD	TDD	TDD	TDD	China	8	38250	38450	38649	TDD	TDD
41	TD 2500	2496	2593	2690	194	TDD	TDD	TDD	TDD	TDD	Global	10	39650	40620	41589	TDD	TDD
66	AWS-3	2110	2155	2200	90 / 70	1710	1745	1780	400	FDD	NAR	13,2	66436	66886	67335	131972	132322
72	450 PMR/PAMR	461	463,5	466	5	451	453,5	456	10	FDD	EMEA	15	68936	68961	68985	133472	133497

Figure 23- Global LTE CAT 1 frequency bands



Brand	Downlink (MHz)			Bandwidth (UL/DL) (MHz)	Uplink (MHz)			Duplex spacing (MHz)	Geographical Area	Channel Number	
	Low	Middle	High		Low	Middle	High				Arfcn
<b>380 T-GSM</b>	390,2	395	399,8	9,6	380,2	385	389,8	10	n/a	Dynamic	
<b>410 T-GSM</b>	420,2	425	429,8	9,6	410,2	415	419,8	10	n/a	Dynamic	
<b>450</b>	460,6	464	467,4	6,8	450,6	454	457,4	10	n/a		259 - 293
<b>480</b>	489	492,4	495,8	6,8	479	482,4	485,8	10	n/a		306 - 340
<b>710</b>	728,2	737,2	746,2	18	698,2	707,2	716,2	30	n/a	Dynamic	
<b>750</b>	747,2	755,2	763,2	16	777,2	785,2	793,2	-30	n/a	Dynamic	
<b>810 T-GSM</b>	851,2	858,7	866,2	15	806,2	813,7	821,2	45	n/a	Dynamic	
<b>850</b>	869,2	881,5	893,8	24,6	824,2	836,5	848,8	45	CALA, NAR		129 - 251
<b>900 P</b>	935,2	947,5	959,8	24,6	890,2	902,5	914,8	45	ITU Regions 1 and 3		2 - 124
<b>900 E</b>	925,2	942,5	959,8	34,6	880,2	897,5	914,8	45	APAC, EMEA		0 - 124 975
<b>900 R</b>	921,2	940,5	959,8	38,6	876,2	895,5	914,8	45	ITU Regions 1 and 3		0 - 124 955
<b>1800 DCS</b>	1805,2	1842,5	1879,8	74,6	1710,2	1747,5	1784,8	95	ITU Regions 1 and 3		512 - 885
<b>1900 PCS</b>	1930,2	1960	1989,8	59,6	1850,2	1880	1909,8	80	CALA, NAR		512 - 810

Figure 24- Global EC-GSM IOT frequency bands

a. <sup>^ a b c d</sup> T-GSM is *Trunking-GSM*.

b. <sup>^ a b</sup> CALA: *Canada, US, Caribbean, and Latin America*

c. <sup>^ a b</sup> NAR: *North American Region*

d. <sup>^</sup> P-GSM is the standard or primary GSM-900 band

e. <sup>^</sup> E-GSM is the extended GSM-900 band: a superset of the standard GSM-900 band.

f. <sup>^ a b c</sup> APAC: *Asia-Pacific*

g. <sup>^ a b c</sup> EMEA: *Europe, the Middle East and Africa*

h. <sup>^</sup> R-GSM, or *GSM-R*, is the Railways GSM-900 band, which also includes the standard and extended GSM-900 bands.

i. <sup>^</sup> DCS: *Digital Cellular System*

j. <sup>^</sup> PCS: *Personal Communications Service*

### 4-3- Spectrum Sharing for Providing Local Area Services with QoS

The focus in this framework is on licensed bands and possible ways to introduce local area services. It will also facilitate wide availability of equipment since the frequency bands are also used by Mobile Network Operators (MNOs) in case of e.g. IMT-bands.

The possible sharing methods for providing local area services focusing on QoS are:

1. Mobile network operators can offer dedicated local area services using their licensed frequencies.
2. Mobile network operators can lease out part of their spectrum locally to local area service providers.
3. Spectrum licensed to local area service providers:
  - Sharing the band by offering services in many different local areas nationally.
  - Example of local area definitions are e.g. real estate boundaries.
4. Part of the licensed band is using light licensing with control and limits on use, in this case, frequency planning/coordination is needed and limitations of the number of users in same area can be imposed. The use may be authorized by the national regulatory. Thus, this type of light licensing scheme can be categorized as an individual authorization but with a simplified procedure for issuing the license compared to individual licensing. QoS could therefore be possible to support:
  - QoS can be difficult to guarantee, unless the networks are non-overlapping or can be controlled to provide a certain QoS guarantee.
  - Sharing the band by offering services in many different local areas nationally.
  - Example of local area definitions are e.g. real estate boundaries.

The possible spectrum access options in 1 to 4 above for QoS enabled local networks can be achieved using alternatives 1 to 3 only. It may also be possible to use the controlled light licensing method, as described in number 4 above, given that the needed level of QoS can be provided and guaranteed. However, there is uncertainty based on the fact that knowledge of the real deployments and actual traffic cannot be known with enough accuracy such that the control can be made efficient. Note that in real-world deployments combinations may be possible where e.g. 1) and 3) is used in a local deployment when an MNO provides roaming services and other expertise as well as enabling even higher capacity in terms of spectrum availability.

The basic spectrum access methods which provide local IoT services are (see Figure 24-x):

1. Mobile network operators can offer dedicated local area services using their licensed frequencies
2. Mobile network operators can lease out part of their spectrum locally to local area service providers
3. Spectrum can be licensed to local area service providers

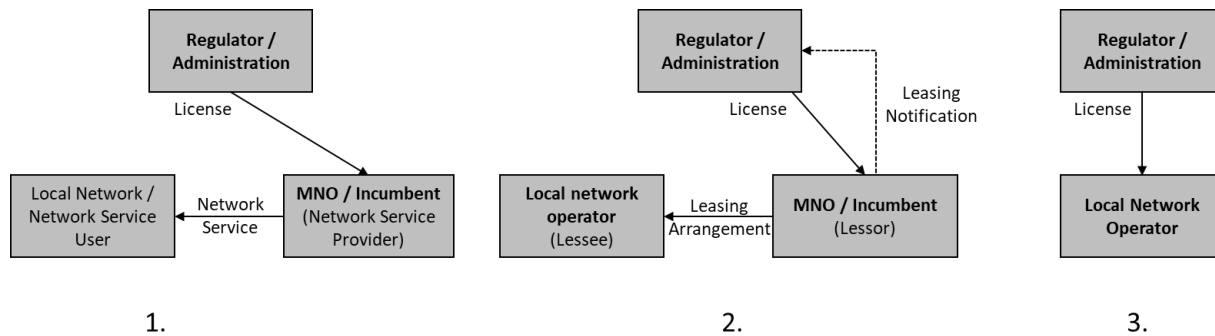


Figure 24-x: Three basic spectrum access methods for local IoT services. 1) MNO offered service, 2) Leasing of spectrum, 3) Local license.

#### 4-4- Licensed Shared Access (LSA)

The LSA concept, described in APT AWG report 68 and also in CEPT, is a complementary spectrum management tool that fits to an "individual licensing regime". LSA foresees the introduction of new users (licensees) in a frequency band while maintaining incumbent services in that band. At first, an appropriate 'sharing framework' is to be defined by the Regulator, also known as a National Regulatory Authority (NRA), including all relevant stakeholders. Here, a set of sharing rules constitutes the regulatory and legal basis that ensures QoS levels for all authorized users.

LSA focuses on nation-wide, long-term sharing arrangements between incumbents and LSA licensees. The deployment of an LSA system requires the introduction of two new architecture building blocks: the LSA Repository and LSA Controller (see Figure 14a). The LSA Repository holds information such as spectrum resources for sharing, protection requirements of incumbents, LSA usage rights and sharing conditions in general. The LSA Controller is a management entity relaying this information to licensee networks it is connected to.

In CEPT countries the first practical use case of LSA is to access the spectrum for mobile broadband services (MFCN) in the 2.3 GHz – 2.4 GHz band.

ETSI proposed the LSA system architecture depicted in Figure 14b. Based on the work in ETSI, 3GPP opened a new study item considering the impact of LSA on their specifications. Several trials have successfully proved the applicability of respective technologies

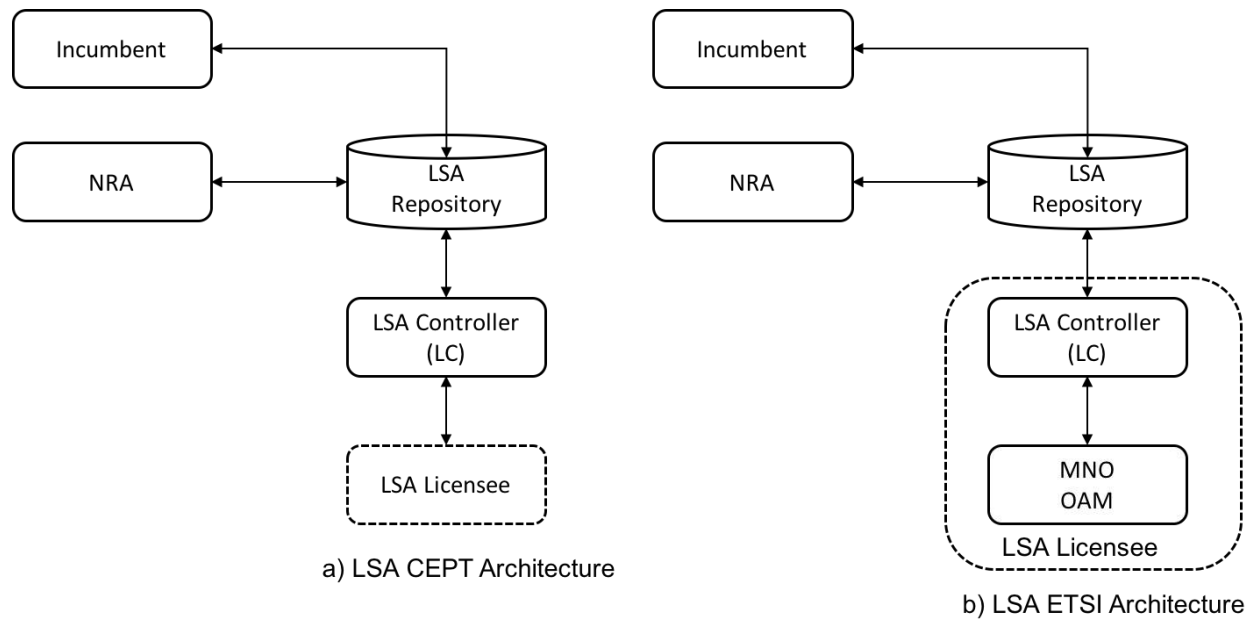


Figure 14: a) Baseline LSA architecture as described by CEPT;  
b) Baseline LSA architecture as defined by ETSI for mobile broadband applications  
in the 2,3 GHz - 2,4 GHz band

## **5- Chapter 5: IoT Operator**

### **5-1- IoT implementation issues**

Organizations are increasingly turning to the IoT as new sources of data, which are derived from continuously monitoring a wide range of things within a variety of situations, become available. However, there are several technological and regulatory challenges that need to be addressed. The most important of them are related to data ownership such as security, privacy and the sharing of information. It is clear that the implementation of IoT for e-commerce faces a variety of impediments. Researchers consider security and privacy to be the main obstacles for a full acceptance of IoT. The sensitivity levels of the information are a crucial aspect to be considered by the access control mechanism. Disclosure of user data could reveal sensitive information such as personal habits or personal financial information. The unauthorized access to this information can severely impact user privacy. In this way, IoT requires novel approaches to ensure the safe and ethical use of the generated data, requiring a strong data governance. A weak form of data governance can impede the safe and ethical use of data generated by IoT devices.

IoT brings with it a wealth of new business opportunities. There is enormous scope for developing applications and selling new services. But a lack of, or poorly coordinated, policy and regulations regarding IoT can also greatly impede the implementation and application of IoT. Organizations need to develop policy and regulations and position themselves carefully within this arena. In this regard, organizations should consider the role they play in enabling IoT development very carefully. Market forces of supply and demand can play substantial roles in the success or failure of IoT.

Furthermore, the Internet of things is more than one device, application or network. In order to ensure sustainable connectivity, all interfaces and communication protocols require unified industry standards. However, the large number of standards-setting organizations has led to a situation in which the top standard has not yet been set. Vendors are free to choose which standard they find best fits their production line, leading to a wide variety of available types. This may impede interoperability and integration of data. IoT requires that a large number of devices be integrated with the existing Internet. These devices can be diverse in terms of data communication methods and capabilities, computational and storage power, energy availability, adaptability, mobility, etc. Heterogeneity at the device level is a serious impediment to IoT adoption.

Data management issues are also of concern. Organizations are often faced with a complex legacy of data and applications when implementing IoT solutions. Many organizations may have several generations of systems running in parallel, and much of the data fed into the system has been done manually, with associated risks in terms of data quality.

In short, IoT faces a variety of barriers related to the proper use (privacy and security for example) and proper management of the data collected by the vast number of interconnected things. Strategic/political barriers are: data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces. Tactical barriers include: costs, interoperability and integration issues, acceptance of IoT, and trust related issues. Operational issues are: a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues.

## 5-2- State of LPWA network roll-outs

In order to achieve widespread, global coverage for each of these technologies, a good set of local mobile network operators (MNOs) is required. MNOs are providers of wireless communication services that own or control the complete telecom infrastructure necessary to sell and deliver services to their subscribed mobile users.

IoT Analytics counted 199 public LPWA networks that were commercially deployed and that operate on one of these 4 technologies. Each of these networks have been deployed by a different MNO either on a national, regional or city-wide scale, but there may actually be more networks than we are not aware of. If you are reading this in a major city, chances are that a LoRaWAN, Sigfox, NB-IoT, or LTE-M network is available at your current location right now.

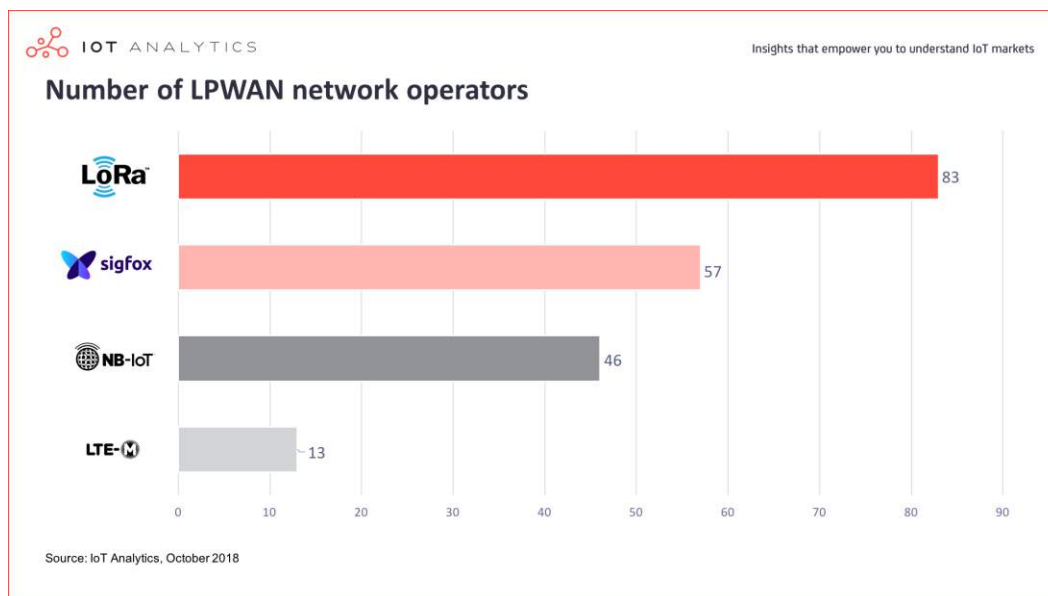


Figure 25- number of operators (2018)

### **5-2-1- LoRaWAN (83 operators globally)**

According to the LoRa Alliance, by October 2018 there were 83 operators that have rolled-out a public LoRaWAN network, providing coverage in 49 countries.

If we also count the open-source community of the Things Network and a few other entities that have deployed private LoRaWAN networks, the number of countries with LoRaWAN deployments grows to 95.

The majority of these LoRaWAN public networks are built and managed by small non-cellular operators and have a limited geographical footprint (often on a city-wide or regional scale). Some of these operators are new companies that were formed specifically to be a LoRaWAN operator, but there are also many players coming from other IoT or telecom related businesses, such as wired broadband internet and telephony providers, radio and television broadcasters, as well as providers of various other telecommunication services and IoT end-to-end solutions.

Lora operator examples include ZTE, Tata Communications, Orange, and KPN. Overall, the range of LoRaWAN operators is the most heterogeneous when compared to other LPWAN technologies.

### **5-2-2- Sigfox (57 operators globally)**

According to Sigfox, by October 2018 their LPWAN network was present in 57 different countries worldwide.

In December 2017, the company claimed to have coverage in over 45 countries, while in November 2016 Sigfox was present in 26 countries. Thus, the number of countries with Sigfox coverage has more than doubled over the past two years.

A look at the Sigfox coverage map shows that nation-wide coverage is provided only in Western European countries, while in the rest of the world the network coverage is rather spotty and limited to a few major cities and high-traffic areas. In terms of network operators, Sigfox provides exclusive rights to deploy its network to one operator per country. None of the Sigfox operators are cellular MNOs, and many of them are actually new actors in this space.

Notable examples include Sigfox itself that acts as a network operator in a few countries, such as France, Spain, Germany and USA, and WND, that has national subsidiaries in UK and in several countries in Latin America, all acting as independent Sigfox operators.

### **5-2-3- NB-IoT (46 operators globally)**

According to GSMA, by September 2018 there were 46 commercially launched NB-IoT networks over 28 different countries (17 in Europe, 8 in APAC, 3 in Middle East and Africa).

The operators deploying these networks are all cellular MNOs with an LTE network already in place such as Vodafone, T-Mobile, Orange, Telefonica, and the three major Chinese operators (China Mobile, China Telecom, China Unicom).

For them, rolling-out a NB-IoT network is quite straightforward, as they can re-use their existing LTE infrastructure, and in many cases, they are only required to firmware upgrade their LTE base stations to enable NB-IoT support.

Note that in our count, we considered national MNOs, i.e. one MNO for each nation-wide network. For example, Vodafone as a global company has deployed 9 NB-IoT networks over 9 countries, but in this blog post it was counted as 9 different MNOs since it has a national subsidiary in each country.

#### **5-2-4- LTE-M (13 operators globally)**

According to GSMA, by September 2018 there were 13 commercially launched LTE-M networks in 12 countries:

- 6 in Asia Pacific
- 2 in Europe
- 1 in North America
- 1 in Latin America
- 2 in Middle East and Africa

As for NB-IoT, these are all cellular MNOS such as AT&T, Verizon, KPN and Orange that in many cases only need to upgrade their LTE base stations to provide LTE-M coverage.

Also in this case we considered in the count one different MNO for each nation-wide network even if these are national subsidiaries of the same global MNO. For example, AT&T has deployed two nation-wide LTE-M networks in USA and Mexico respectively, and it was counted twice since these are national subsidiaries of the same company.

#### **5-3- Cellular MNO strategies for LPWAN technologies**

Out of the over 750 cellular MNOs currently operating worldwide (according to GSMA-2018), only 52 have deployed commercial LPWAN networks up to date, which is less than 7%.

If we look at how these MNOs are reacting to the emergence of LPWAN technologies, we can distinguish 4 different strategies.



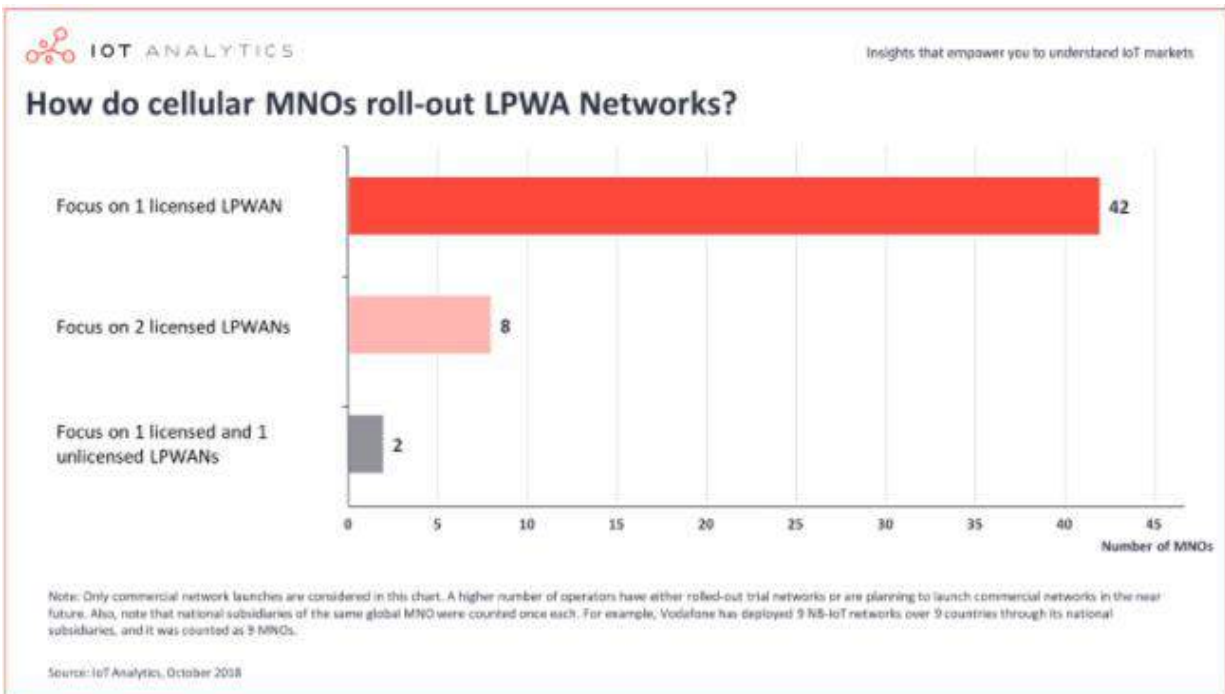


Figure 26- MNO roll-out LPWAN

#### 5-3-1- Strategy 1: Ignoring LPWAN technologies

We have heard that some operators (particularly small ones) don't believe LPWAN is particularly relevant for their business and are thus not planning to adopt any of these technologies, at least in the near future. Others, especially in the less developed countries, either have no LTE infrastructure in place or this has a poor coverage, while they are still seeing a lot of traction for their GSM networks. For them, investing in LPWAN would be too expensive when compared to the expected additional revenues from LPWAN connectivity, and they will likely wait for a consolidation in the 5G standard before making additional investments in their infrastructure.

#### 5-3-2- Strategy 2: Focus on one licensed LPWAN technology only

Among the cellular operators that have jumped on the LPWAN bandwagon, the majority are betting on only one licensed technology (either NB-IoT or LTE-M), specifically the one they believe is stronger and would have the highest market traction within their local markets. Currently we count 42 national MNOs who have already launched a commercial LPWAN based on only one licensed technology, but some more are currently rolling-out an LPWAN or have announced plans to do so in the near future.

#### 5-3-3- Strategy 3: Focus on two licensed LPWAN technologies

A minority of the MNOs deploying LPWANs are betting on both NB-IoT and LTE-M at the same time. According to the information from GSMA, by September 2018 there were 8 national MNOs that have launched commercial LPWA networks based on both licensed technologies within the same country, with some more that have announced their plans to do so in the near future, the majority of which are in the Asia Pacific region. These are:

- AIS (Thailand)
- APTG (Taiwan)
- Dialog Axiata (Sri Lanka)
- Etisalat (UAE)
- Orange (Belgium)
- SingTel (Singapore)
- Telstra (Australia)
- Turkcell (Turkey)

#### **5-3-4- Strategy 4: Focus on licensed and unlicensed LPWAN technologies**

While still a minority, a small number of cellular MNOs have either deployed or shown interest in both licensed and unlicensed LPWANs, specifically LoRaWAN.

At the moment, IoT Analytics is only aware of two operators that have already done that:

- KPN in the Netherlands
- SK Telekom in South Korea

Both have nation-wide LTE-M and LoRaWAN networks. French MNO, Orange, has deployed NB-IoT and LTE-M networks in Belgium, while in France it has a LoRaWAN network. Other cellular operators, including Swisscom, Proximus, SoftBank and Bouygues Telecom (through its subsidiary Objenious) have joined the LoRa Alliance and have already deployed a LoRaWAN network. While they made no announcements regarding licensed technologies, it is safe to assume that they may complement their LoRaWAN offering with either NB-IoT or LTE-M in the future, if not both.

#### **5-3-5- Trend: Adoption of multiple LPWAN technologies**

We see a trend towards strategies 3 and 4, i.e. cellular MNOs betting on more than one LPWAN technology. This is motivated both by technical and by strategic reasons.

- **Technical rationale:** Combining multiple technologies allows the operator to address a larger spectrum of IoT use cases and requirements, given the complementarity of the different technologies. While the complementarity of LTE-M and NB-IoT is well known, with the former more suited for higher-end applications with higher data transmission needs, a few LoRa suppliers have recently highlighted how LoRaWAN can be used in conjunction with licensed technologies. A possible model of collaboration between LoRaWAN and licensed technologies would be to use LoRaWAN to improve the coverage in areas at the edge of the licensed networks or to provide it in areas previously uncovered at a low cost, thus expanding the coverage beyond the LTE infrastructure.
- **Strategic rationale:** Betting on more than one technology typically requires a small additional cost for the network infrastructure – in the case of LTE-M and NB-IoT, upgrading to both at the same time should cost only 20% more than upgrading to just one – but it allows an operator to differentiate its investment and reduce the risks. While some technologies like LoRa and NB-IoT are gaining more and more acceptance and are likely here to stay, most LPWAN technologies still have an

uncertain future and may not experience the device volumes that were initially anticipated. What happened in USA with LTE-M is just one example. There, AT&T and Verizon had initially bet on LTE-M only to address the demand for IoT connectivity, and network roll-outs were completed in 2017, but following the low market traction of the technology and the high customer demand for NB-IoT, both operators have recently announced their plans to deploy nation-wide NB-IoT networks within 2019.

This trend should not come as a surprise to industry experts. For a few years, some of them had already highlighted how no single LPWAN technology that can cover all use cases. In the end, we believe that a multi-technological strategy will be key for the success of this market, and it seems that operators have come to the same conclusion and are getting ready to do that.

## **6- Chapter 6: IoT in 5G**

### **6-1- Wireless networks in 5G**

The wireless technologies has significantly enhanced the deployment of IoT, a number open standard for IoT have been released, such as NB-IoT based on 3GPP. The 5G will be able to provide connection massive IoT, where billions of smart devices can be connected into the Internet.

The 5G networks will provide a flexible and faster networks, It's unleashing a massive IoT ecosystem where networks can serve billions of connected devices, with the right trade-offs between speed, latency, and cost.

The 5G technology can significantly expand IoT network and will enable IoT devices to interact with smart environment to a new level through intelligent sensors connected. The 5G wireless network can also significantly enlarge the scope and scale of coverage of IoT by providing the fastest communication and capacity.

The three main usage scenarios for 5G, as defined by ITU-R M.2083, are ultra-reliable low latency communications (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communications (mMTC).

#### **6-1-1- Enhanced Mobile Broadband (eMBB)**

eMBB focuses on a higher data rate, with a large payload and prolonged internet connectivity based applications. Potential applications could include cloud office/gaming, virtual/augmented reality (VR/AR) and three-dimension/ultra-high definition (3D/UHD) video.

#### **6-1-2- Ultra-Reliable Low Latency Communications (URLLC)**

URLLC focuses on an ultra-responsive connection with ultra-low latency. The data rate is not expected to be very high in URLLC, but offers high mobility. Potential applications of URLLC include industrial automation, autonomous driving, mission critical applications, and remote medical assistance.

#### **6-1-3- Massive Machine-Type Communications (mMTC)**

mMTC focus on providing connectivity to a large number of devices (IoTs), but with low reliability. It can provide long-range communication with energy efficiency and asynchronous access. Such features are very suitable for low power devices in a massive quantity. NB-IoT and LTE-M technologies are part of the mMTC category of 5G

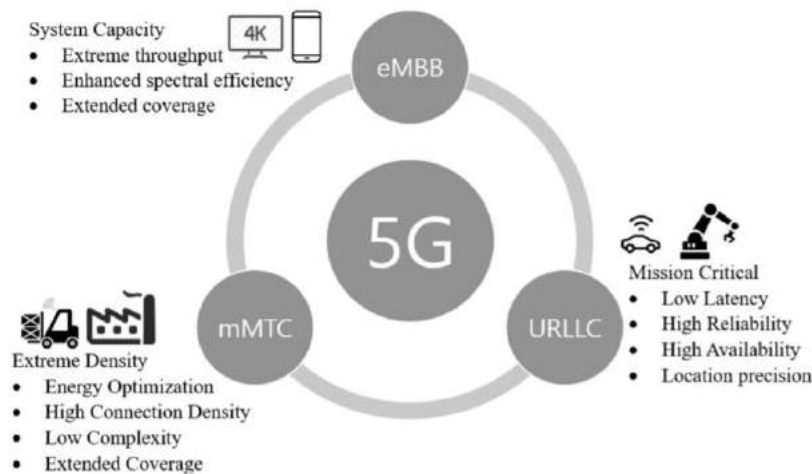


Figure 27- 5G scenarios

#### 6-1-4- Importance of URLLC and mMTC in 5G-IoT

According to figure 28 every scenarios in 5G can give some advantages to IoT. URLLC is critical for enterprise IoT use cases and in the consumer sector for smart city and smart home applications.

For example, smart cities could use URLLC IoT devices to manage traffic more efficiently, prevent congestion and warn of accidents ahead, benefitting road-users. In smart homes, URLLC capabilities will bring a number of benefits, supporting online gaming and AR/VR devices.

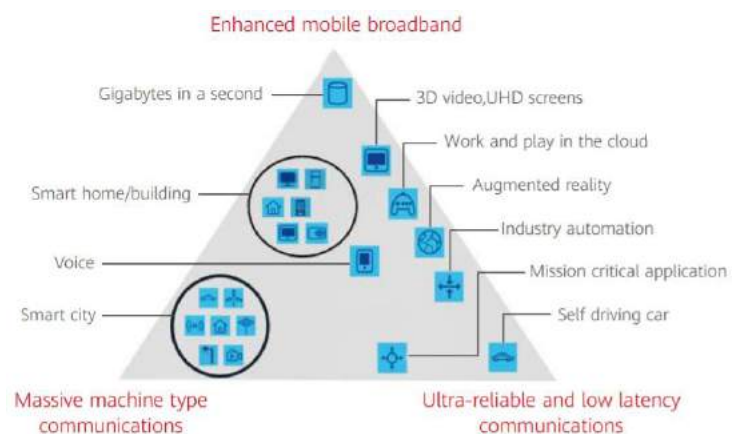
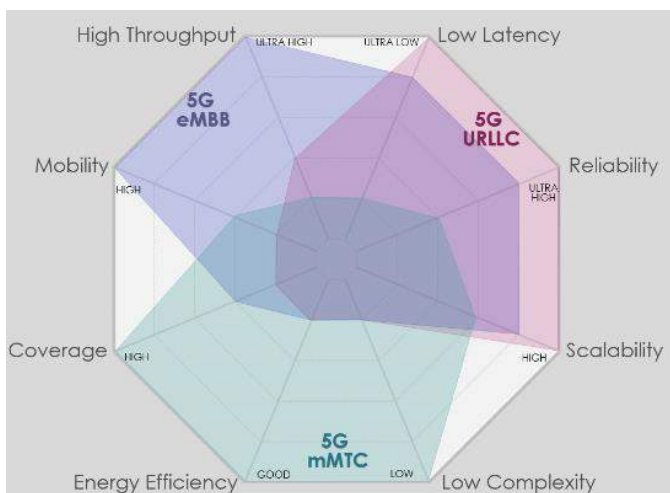


Figure 28- specifications of 5G scenarios

Faster response times and higher reliability will reduce transmission delays, providing a more immersive experience. Low latency connectivity is important for machines that drive themselves, such as autonomous vehicles, or perform critical tasks, such as control of industrial devices. Low latency will allow a 5G network to be optimized to process huge volumes of changing data in real time, a capability not possible with other technologies

Developed in consultation with industrial and end users, the 3GPP Study on Communication for Automation in Vertical Domains (TR 22.804) has identified a set of performance targets for industrial automation using 5G. These are summarized, according to the use case and across various other criteria, in Figure 29.

Use Case (High Level)		Availability	Cycle Time	Typical Payload Size	# of Devices	Typical Service Area
Motion control	Printing machine	>99.9999%	< 2 ms	20 bytes	> 100	100 m x 100 m x 30 m
	Machine tool	>99.9999%	< 0.5 ms	50 bytes	~20	15 m x 15 m x 3 m
	Packaging machine	>99.9999%	< 1 ms	40 bytes	~50	10 m x 5 m x 3 m
Mobile robots	Cooperative motion control	>99.9999%	1 ms	40-250 bytes	100	< 1 km <sup>2</sup>
	Video-operated remote control	>99.9999%	10-100 ms	15-150 kbytes	100	< 1 km <sup>2</sup>
Mobile control panels with safety functions	Assembly robots or milling machines	>99.9999%	4-8 ms	40-250 bytes	4	10 m x 10 m
	Mobile cranes	>99.9999%	12 ms	40-250 bytes	2	40 m x 60 m
Process automation (process monitoring)		>99.99%	> 50 ms	Varies	10,000 devices per km <sup>2</sup>	

Source: 3GPP, 7VFI

Figure 29- URLLC use cases

eMTC concept includes a set of radio and techniques, thus enabling the expected growth rate in the number of terminal devices and related services and applications. A mMTC network usually consists of billions of low-complexity low-power machine-type devices as nodes. A good example of this type of networks are smart grids where the data from a very large number of nodes (smart meters) needs to be collected.

likelihood

## **6-2- Features employed in 5G PHY layer to support 5G-IoT**

MIMO, CoMP, and the HetNets, etc. are some of the features that have been standardized for LTE/LTE Advanced (LTE-A) technology. These technologies show encouraging results in providing massive connectivity and high data-rate. Therefore, 5G technology employs these concepts. These concepts are discussed at first to get their insight in the next sub-sections:

### **6-2-1- Carrier aggregation**

Carrier aggregation was introduced in 4G LTE\_A based on Release 10 of the 3GPP. It aggregates up to 5 component carriers (CCs) of LTE. A having 20 MHz of bandwidth thus enhancing the overall bandwidth to 100 MHz.

In carrier aggregation, it is possible that the mobile device may receive more than one CC. Multiple CCs with different bandwidths can be aggregated in the uplink and downlink, where the number of uplink aggregated CC may not be higher than the number of aggregated CC in the downlink.

The CC may belong to the same band known as intra-band carrier aggregation or to the different band known as inter-band carrier aggregation. In each type of carrier aggregation, it is also possible to perform contiguous and non-contiguous component carrier aggregation. In uplink and downlink, one of the CC must be selected as a primary component carrier (PCC) while others as a secondary component carrier (SCC). The number of CCs in different 3GPP releases has increased significantly.

### **6-2-2- Massive-MIMO (M-MIMO)**

The MIMO technology is considered a necessary part of LTE-A, and is based on the concept of spatial multiplexing. Data streams from multiple antennas are multiplexed and are transmitted over a variety of spatially separated channels.

On the other hand, M-MIMO is an integral part of the 5G infrastructure. At mmWave, many antenna elements are needed so that highly directional narrow beam can be produced to counteract the path-loss. This technique becomes feasible to implement the high-order multi-user MIMO (MUMIMO) to enhance the small cell capacity. In 5G radio access network (RAN), is based on M-MIMO in “macro assisted small cells”. The control-plane traffic is provided in the macro cell at lower band frequencies using omnidirectional antenna while user-data traffic is delivered using highly directional M-MIMO beam at mmWave band frequencies.

### **6-2-3- Coordinated Multipoint Processing (CoMP)**

Coordinated Multipoint (CoMP) was first introduced and Standardized by 3GPP in Rel-10 and employed in LTE-A. CoMP transmission in downlink and reception in uplink is a very effective way to enhance the cell-edge user throughput. CoMP utilizes distributed MIMO

for transmission and reception from different antennas, which may not belong to the same cell to reduce, received spatial interference and enhanced the received signal quality.

#### **6-2-4- Heterogeneous Networks (HetNets)**

A network comprising of different types of cell layers (femtocells, pico-cell, micro-cell and macro-cell) and different RATs. These networks consist of low power nodes needed for data of loading. The HetNets supports the green aspect of 5G by maximizing the spectral efficiency through reusing the spectrum tightly and with low uplink and downlink power transmission making it spectrum and energy efficient. Sharing the spectrum by the massive number of user equipment an ultra-dense network (UDN) requires an intelligent interference mitigation technique.

In order to cater for the interference, the HetNets uses enhanced inter cell interference coordination (e-ICIC) and further enhanced ICIC (feICIC). These features allow it to handle massive traffic and large node density; hence; making it suitable for satisfying the requirements of service-driven 5G enabled IoT. The HetNets enabled 5G-IoT based solutions are provided in.

#### **6-2-5- D2D Communications**

The HetNets realizes the coordination between macro-cell BS and the low power BS. However, for short-range communication, it does not prove to be efficient. Hence, the D2D communication is evolved that allows low power consumption, better QoS and load balancing between the devices for short-range communication ( $< 200\text{m}$ ). In light of this, the BS will either have the full control over allocating the resources among source, destination and relaying nodes or have partial control.

#### **6-2-6- Centralized Radio Access Network (CRAN)**

The CRAN is another concept towards greener and cleaner communication by reallocating the functions of BSs. It only allocates the radio functions to the BS that is remote radio unit or remote radio head. Other unit like baseband unit (BBU) is distributed to the cloud-based central processor.

This enables centralized intelligence, cooperative communication among cells, improved cell utilization and reduces complexity and cost at the BS end.

### **6-3- Features employed in 5G networking layer to support 5G-IoT**

These network architectures previously hardware-based, will now have to manage the exponentially growing traffic, deployment/induction of new nodes, efficient network forwarding infrastructures and the network expansion flexibility. To achieve these objectives, different network-enabling technologies are developed which are now emerging. Some of them are discussed below.

#### **6-3-1- Software-Defined Wireless Sensor Networking (SD-WSN)**

Conventional methods to deploy cellular technology are generally hardware-based. The hardware-based deployment limits the flexibility of network expansion. Hence, SD-WSN,



a promising paradigm, is developed to overcome this limitation. The SD-WSN is a blend of SDN inside the WSNs.

The SDN found its applications in data centers (wired communication networks) and for Internet connectivity. Currently, it is envisaged as 5G technology enabler. The primary purpose of using this model for deployment of 5G networks is to decentralize the control logic plane from the network device and providing the centralized mechanism to program the entire network.

Due to the increasing demands of the massive connected devices, a centralized software-based paradigm like SDN is necessary to full the requirements of maintaining consistent QoS. The SDN will simplify the network management issues such as link/node down issues, allocation of resources, and deployment of new links/nodes by manifold. Different proposed SDN solutions are Soft Air, Cloud RAN and CONTENT. Hence, it is seen as a pivotal enabler of future next-generation 5G technology.

### **6-3-2- Network Function Virtualization (NFV)**

The NFV virtualizes the network functions. These functions can then be implemented into software packages which can later be used for providing network service requirements [85]. The NFV and SDN are mutually exclusive. The NFV concept is originated from the perception of virtual machines, which can be installed on different operating systems on the same server. Some foreseen use cases related to NFV are core virtualization and centralized baseband processing within RANs.

The NFV is a promising candidate for the successful deployment of 5G enabled IoT. Since, the network virtualization concept supports the network scalability mechanism, network slicing over the distributed cloud, real-time processing capability (optimizing speed and capacity in sliced networks) and maintains its heterogeneity one of the significant features and requirements of 5G over IoT. Not only this, the NFV is also energy and cost-efficient, thereby reducing the capital and operational expenditure.

Therefore, a lot of research is going on this technology as recently (2019) Intel and Ericsson have developed the 5G platform that incorporates the software and hardware management, NFV and cloud services for 5G.

### **6-3-3- Cognitive Radios (CRs)**

The current IoT applications from massive to critical IoT represents massive connectivity and overloading of the network resources resulting in the scarcity of spectrum. Hence, there is a dire need to use the spectrum efficiently and intelligently to satisfy the growing demand. The CR handles this issue perceptively, by using/sharing the spectrum resources in an opportunistic manner.

A CR can be defined by a radio that can change its transmitter parameters based on the interaction with the environment in which it operates". Hence, this leads to the concept of cognitive capability and reconfigurability. The former refers to capturing the spatial and temporal variations with reduced interference in a radio environment.

#### 6-4- Architectural view of 5G-IoT

As discussed in the previous section, the IoT technology has immense demands. Hence, a 5G architecture should be capable of proving a scalable network, network virtualization facility, cloud services, network densification capability, mobility control services, radio access control, efficient resource allocation mechanism, and big IoT data analysis tools. In a nutshell, a 5G-IoT based architecture should provide an independent HetNets, which is self-configurable as per the application requirement.

#### 6-5- QoS in 5G-IoT

The QoS in a 5G cellular network can be comprehended by its spectral efficiency and latency. The spectral efficiency in a 5G network can be achieved by using non-orthogonal signals and radio access methods, whereas latency demands vary in case of a user and control plane traffic.

A typical 4G and 5G network cell spectral efficiency in the uplink and downlink is shown in figure 30, and the latency in the control and user plane is shown in figure 30, respectively.

It can be seen from about 50% decrease in latency can be seen in the control plane in case of 5G network with significant improvement in the cell spectral efficiency.

Latency	5G Technology	4G Technology
User plane (msec)	1	10
Control plane (msec)	50	100

Cell Spectral Efficiency	5G Technology	4G Technology
Uplink (bps/Hz)	05	1.8
Downlink (bps/Hz)	10	2.6

Figure 30- QoS in a 5G

#### 6-6- Standardization in 5G-IoT

The standardization process in the 5G-IoT involves mainly two types of standards. One is the technology standards that deal with network technology, protocols, and wireless communication and data aggregation standards. Second is a regulatory standard that comprises of security and privacy of data.

#### 6-7- Artificial intelligence use cases for 5G-IoT networks

The higher data-rates possible in 5G-IoT makes it possible for the implementation of data-hungry and computation intensive Artificial Intelligence (AI) algorithms for various user applications.

With high data transmission capacity of the network comes a possibility of the use of efficient deep learning algorithms such as virtual speech recognition and video classification over wireless 5G-IoT nodes. The combination of 5G, IoT and AI has a higher potential of changing the landscape of businesses by making intelligent decisions in real-time. With the availability of powerful hardware for IoT nodes, the inclusion of intelligence on IoT nodes or a fog node closer to end devices decreases latency, improves link capacity, and upgrades the network security.

Interestingly, AI based techniques could also be employed over 5G-IoT networks to further optimize its own performance at application, physical and network layers to further enhance data rates by predicting traffic patterns on the network, thus facilitating the provisioning of AI based user applications. For example, at the application layer, AI techniques could be utilized for studying network traffic and capacity trend analysis to make the network self-configurable, self-organized and self-adaptive [96]. On physical and network layers, AI based optimization algorithms could facilitate dynamic spectrum management, structuring of huge data, integration of heterogeneous devices, ultra-deification of devices, IoT nodes interoperability, and improved battery life.

#### **6-7-1- Big data processing enhancement**

The latest techniques practiced in IoT and the reliable and fast speed of 5G network incubates the environment of creating applications which utilize big data to its maximum potential, such as natural language processing, face recognition, which can run in the terminal. Ever-present connectivity provided by 5G leads to the creation of an enormous amount of data. This data set can also be utilized as a mean of exchange in 5G IoT-based networks for making intelligent decisions.

#### **6-7-2- Expanding the horizon of healthcare**

The combination of 5G and AI in the field of healthcare can improve the lives of millions of people by upgrading the existing system. The system is designed a personalized emotion-aware healthcare system using 5G that emphasizes on the emotional care, especially for children, and mentally ill and elderly people.

Genetic algorithm and simulated annealing were utilized to find the best position for 5G drone base stations within the constraints of coverage, energy and cost.

#### **6-7-3- Intelligent networking**

One of the applications of AI is the implementation of 5G networks, which is shown in the CogNet project in which an architecture of an autonomic self-managing network extending NFV management with the machine learning based decision-making mechanism is discussed. The reason behind deploying a more adaptive controlling mechanism next to base NFV functionalities is the pursuit to reduce the costs of the system, whilst keeping QoS on a competitively high level.

#### **6-7-4- Smart transportation systems**

Vehicles with continuous connectivity, are becoming a reality with the integration of 5G with IoT. This integration has given the ability to access the internet in a more efficient

way. Now, car manufacturers have developed their interest and are exploring different markets to bring this technology in the field of transportation systems. Researches have been performed regarding a self-driven vehicle with the use of connecting to the internet. A smart transportation system can provide communication between the smartphone of passengers and the vehicle itself. Just like other IoT devices, a smart transportation system can also provide new features for more control.

The installation of sensors in traffic lights provide the data which helps in making decisions for efficient traffic routes reducing the propagation time of vehicles. The integration of IoT with 5G has improved the overall traffic system. IoT has helped with reducing manual labor in areas such as managing traffic; this can help to reduce costs.

### **6-8- 5G-IoT Frequency Bands**

To address diversified requirements from the envisioned usage scenarios in different phases of 5G, 5G needs access to “high”, “mid” and “low” frequency bands (Figure 31), exploiting specific characteristics of different portions of the spectrum: frequencies between 2 and 8 GHz (e.g., 3300-4200, 4400-5000, 2500- 2690, 2300-2400, and 5925-7125 MHz) in combination with frequencies below 2 GHz (e.g. 700 MHz) and above 8 GHz (e.g. 24.25-29.5 and 37-43.5 GHz). A sufficient amount of harmonized spectrum in each layer should be made available by national regulators in a timely manner to enable mobile operators to deliver 5G services.

The assignment of contiguous wide spectrum bandwidth in each layer reduces system complexity associated with carrier aggregation, which will improve energy efficiency and reduce network cost.

Mid-bands between 2 to 8 GHz are crucial to support most 5G usage scenarios in wide-areas. The unpaired (TDD) bands at 3300-4200, 4400-5000, 2500-2690 and 2300-2400 MHz deliver the best compromise between wide-area coverage and high capacity.

Taking into consideration that eMBB services are dominant in the initial phase of 5G, it is highly recommended to release the mid-bands at first. In this respect, at least 80-100 MHz of contiguous spectrum bandwidth from such mid-bands should be secured as the first step for each 5G network operator in the 5G multi-layer spectrum assignment process.

Low frequency bands (below 2 GHz) will extend the 5G mobile broadband experience to wider areas and deeper indoor environments. Moreover, uRLLC and mMTC type services will also greatly benefit from superior coverage at the low frequency bands.

The available low frequency bands (e.g. 700, 800, 900, 1800 and 2100 MHz) may be exploited for LTE/NR uplink spectrum sharing in combination with NR in the 3300-3800 MHz band to allow operators to ensure faster and cost-effective deployment. High frequency bands (above 24 GHz) will prove indispensable for providing additional capacity and delivering the extremely high data rates required by some 5G eMBB applications at

specific locations (“hotspots”). At least 400-800 MHz of contiguous spectrum per network operator is recommended from higher frequencies to achieve good return on investment and meet service requirements. The low and high frequency bands layers can be released as the second step to meet different usage requirement in the later phases of 5G development, e.g. the requirements for better coverage, lower latency or higher capacity

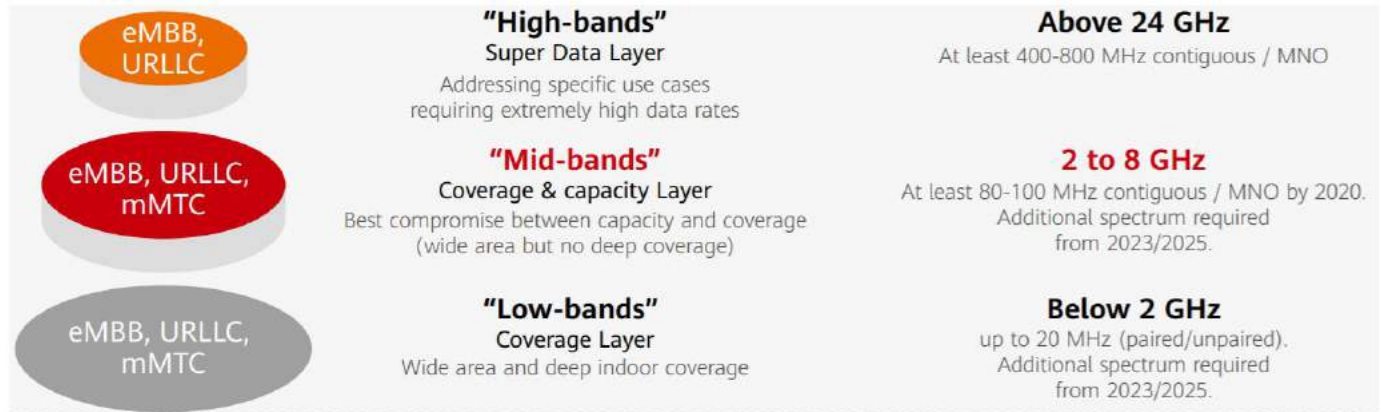


Figure 31- 5G frequency bands

## **7- Chapter 7: Conclusion**

The Internet of Things is a hugely important and rapidly growing market. Internet of Things is one of the most important trends in modern technology and is set to transform countless industries.

On the basis of the responses received from some of the SATRC member countries it can be concluded that the complete regulatory framework is yet to evolve although the IoT services are already working in the member countries and this sector is growing at a rapid pace. It is also necessary to have clear spectrum bands for IoT networks in SATRC countries.

LORa and Sigfox as LPWAN solutions, which are designed to operate in a shared spectrum environment in the sub-GHz range, are anticipating deployment in SATRC countries. The implementation of the same spectrum access techniques and minimum requirements as those used for SRDs is particularly appropriate to support a very large number of low power and low throughput devices.

### **7-1- Regulators should adopt a service and technology neutral framework to support IoT**

It is essential that SATRC members provide a regulatory framework for licensed spectrum that facilitates the development and growth of IoT, and does not impose service or technological restrictions that hold back innovation. Operators should not be prevented from deploying the latest cellular IoT technologies in their licensed spectrum bands due to technological restrictions. The regulatory environment should be designed to nurture this evolution in the capabilities of mobile networks and allow the market to decide which solutions thrive.

### **7-2- Licensed spectrum is vital to deliver the most reliable, high quality IoT services**

Licensed spectrum is uniquely able to provide high quality of service guarantees over wide areas, as operators are not at risk of interference and can control usage levels. As a result licensed cellular IoT may be the only choice for services which require concrete assurance levels such as for security and medical applications amongst others.

Licensed spectrum also encourages sustainable, long-term investment in networks as access and quality levels are assured. Contrastingly, unlicensed spectrum is intrinsically less suited to wide-area IoT applications, especially those requiring higher quality of service levels.

### **7-3- Regulators should work with the mobile industry to support IoT in 5G spectrum planning**

5G is expected to play an important role in the evolution of cellular IoT and therefore suitable provisions need to be made in future band planning. 5G should support the growing number of forecasted end points along with efficient signaling and addressing, while also delivering even lower device costs and making more efficient use of spectrum. It is also likely to provide higher quality of service or even guaranteed service, much lower latency, increased integration within the mobile network, and even longer range.

## 8- Chapter 8: Questions and Answers

### 8-1- Questions

#### Question 1:

Which types of IoT applications have been deployed in your country? (e.g. Smart city, Agriculture, Transportation, Environment, Healthcare, etc.)

#### Question 2:

Is there any specific regulatory framework that applies to IoT in your country? If yes, please attach.

#### Question 3:

Based on ITU-T Recommendation Y.2060 Figure I.1, which organization issues license or permission to following roles for different IoT application types:

- Platform provider: ...
- Network provider: ..
- Device provider: ..
- Application provider: ...
- Application customer: ..

#### Question 4:

Which type of telecom operator(s) is eligible to apply for IoT business?

MNO	MVNO	FWA	PSTN	ISP	SAP	BO
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Question 5:

Do you impose license-fee and/or spectrum fee for IoT? If yes please describe (Note: license-fee is a single-pay amount that is not necessarily for spectrum utilization)

#### Question 6:

Describe spectrum requirement, candid frequency bands, radio license type and employed technologies for IoT in your country.

#### Question7:

Do you have any mechanism/method for assignment of the spectrum mentioned in Q.6? (e.g. according to number of devices, coverage area, etc.)

#### Question 8:

What is/are technical specification(s)/standard(s) the IoT requires to comply with? (For example cellular /IoT, Sigfox, LoRa, ETSI, IEEE standards, and etc.)

#### Question9:

If there are other useful regulations such as how to store or transfer IoT's data, privacy, security, SLA, cross-border, device identification, numbering, etc. please describe.

**Question10:**

Are there any provisions in place for Type Approval of IoT devices? [If exist any document(s) please provide link on this answer]

**Question 11:**

Is your administration or any domestic company member of any international IoT alliance? (if yes please mention name, date of membership and alliance topic(s)).

**Question 12:**

Please inform, if there is any researching activity and IoT manufacturer in your country.



## 8-2- Answers

### Answer of Afghanistan:

Since the regulatory frame work and spectrum for IoT is under work in Afghanistan and there is no IoT network/services in Afghanistan, we escape this questionnaire.

### Question 1:

<b>Pakistan</b>	<p>At present, Cellular Mobile Operators are conducting NB-IOT trials in collaboration with vendors and IoT device manufacturers. In November 2019, Telenor Pakistan launched the first ever Narrowband Internet of Things (NB-IoT) site in Pakistan. The site was launched in collaboration with ZTE (vendor) and Linked Things (IoT device manufacturer, <a href="https://www.linked-things.com/">https://www.linked-things.com/</a>). Telenor plans to conduct trials for smart metering, smart water monitoring, smart homes, smart fire systems, and smart agriculture etc.</p> <p>In absence of identified spectrum in un-licensed bands for IoT, LoRaWAN applications have not been deployed yet. Solutions are being offered by IoT vendors but they are based on licensed bands and the sensors are SIM based. In most outdoor cases, power is being supplied through solar.</p> <p>Following solutions are available in the market:</p> <p>1) Home Automation:</p> <ul style="list-style-type: none"><li>• Outdoor Automation:</li><li>• Light</li><li>• Gate controls</li><li>• Cameras</li></ul> <p>(a) Indoor Automation:</p> <ul style="list-style-type: none"><li>• Lights</li><li>• Curtains</li><li>• ACs</li><li>• Power plugs</li></ul> <p>(b) Power Meter:</p> <ul style="list-style-type: none"><li>• Voltage</li><li>• Current</li><li>• Power</li><li>• Frequency</li></ul> <p>(c) Water Meter:</p> <ul style="list-style-type: none"><li>• Water level in tanks</li><li>• Water motor control</li></ul> <p>2) Office Automation:</p> <p>(a) Asset Monitoring:</p> <ul style="list-style-type: none"><li>• Tilt and movement</li><li>• Position and location</li><li>• Vibrations</li></ul> <p>(b) Power Monitoring:</p> <ul style="list-style-type: none"><li>• Voltage</li><li>• Current</li><li>• Power</li><li>• Frequency</li></ul> <p>(c) Power Source Identifier:</p>
-----------------	---

	<ul style="list-style-type: none"> <li>• Identifies power source</li> <li>• Identifies power consumption</li> </ul> <p>(d) Environment Monitoring:</p> <ul style="list-style-type: none"> <li>• Temperature</li> <li>• Light</li> <li>• Movement</li> <li>• Smoke</li> <li>• Sound</li> <li>• Locking</li> </ul> <p>(e) Water Monitoring:</p> <ul style="list-style-type: none"> <li>• Water level in tanks</li> <li>• Water motor control</li> </ul> <p>(f) General Monitoring:</p> <ul style="list-style-type: none"> <li>• Fuel Monitoring</li> <li>• Oil Pressure</li> <li>• Temperature Monitoring</li> </ul> <p>3) Agriculture:</p> <p>(a) Soil Monitoring</p> <ul style="list-style-type: none"> <li>• Moisture Level</li> <li>• pH</li> <li>• NPK</li> </ul> <p>(b) Weather Monitoring:</p> <ul style="list-style-type: none"> <li>• Wind speed</li> <li>• Wind direction</li> <li>• Solar lighting levels</li> <li>• Rainfall</li> </ul> <p>(c) Water Monitoring</p> <ul style="list-style-type: none"> <li>• Soil Moisture</li> <li>• Barrage and canal water level monitoring</li> <li>• Flood alerts</li> <li>• Flow measurement</li> </ul> <p>4) Power:</p> <ul style="list-style-type: none"> <li>• Real-time power usage information from all three phases</li> <li>• Alerts on high consumption</li> <li>• Monthly bill prediction based on your tariff</li> <li>• Historic data available for analysis</li> </ul> <p>5) Environment:</p> <ul style="list-style-type: none"> <li>• Indoor and outdoor air quality monitoring</li> </ul> <p>6) Vehicle Tracking and on-board diagnostics monitoring</p>
<b>Bangladesh</b>	<p>The following types of IoT Applications are currently being deployed in Bangladesh:</p> <p><u>Smart City:</u></p> <ol style="list-style-type: none"> <li>1. Smart Parking</li> <li>2. Smart Metering System</li> <li>3. Smart Water Management System</li> <li>4. Smart Home &amp; Building Automation System</li> </ol> <p><u>Smart Agriculture:</u></p> <ol style="list-style-type: none"> <li>1. Smart Irrigations</li> <li>2. Automated Mushroom Cultivation System</li> </ol> <p><u>Smart Livestock Management:</u></p>

	<ol style="list-style-type: none"> <li>1. Digital Livestock Solution</li> <li>2. Smart Brooder</li> </ol> <u>Smart Transportation:</u> <ol style="list-style-type: none"> <li>1. Vehicle Tracking System</li> <li>2. Container Tracking</li> </ol>
<b>Nepal</b>	In Nepal, the IoT applications have been deployed in various sectors like agriculture, transportation, healthcare, wild life protection etc., but there is no complete integrated system in any field. Recently, Government of Nepal has approved Digital Nepal Framework, 2019 and it has been planned for the deployment of IoT applications in agriculture (smart irrigation project, wildlife management), healthcare (next-generation healthcare facilities), energy (smart metering, smart building, GIS smart grid project), smart city as urban infrastructure (water ATM, smart metering for water, connected public transport, intelligent traffic management, intelligent parking lot management) sectors.
<b>Maldives</b>	As of now we don't have any IoT implementation and development, this may due to lack of demand. The existing license to the service providers, does not rejects in providing IoT service.
<b>I. R. of Iran</b>	<ol style="list-style-type: none"> <li>1. <i>Metering of power consumption:</i> Operation of the network has started some years ago and its purpose is gathering information from energy metering devices. Type of the network is LoRa WAN. This network has been developed in two major cities including Tehran and Isfahan. Almost 20,000 devices installed at this project.</li> <li>2. <i>IoT in Agriculture field:</i> The objective of the project is improving productivity of land by better management of irrigation. It is done by measurement of soil moisture, air temperature, air pressure, wind speed and direction as well as sunlight. The land area is about 100 km<sup>2</sup>.</li> <li>3. <i>Tracking transportation goods between customs (RFID field)</i> The project has been run by customs administration for better supervision and controlling of vehicles that are carrying goods between customs by tracking through RFID networks. This project improves customs process from the point of saving transportation time and cost.</li> </ol>
<b>India</b>	IoT applications in India are multi-sectoral such as Manufacturing, Utilities - power, sanitation, smart home, Transportation and logistics – Intelligent Transport System (ITS), fleet management, Smart parking, Agriculture, Oil and gas, Healthcare and Smart cities maintenance like Smart grids, Smart urban lighting, and many more. However, presently, they are at a nascent stage.
<b>Bhutan</b>	No definite IoT applications deployed as of now

#### Question 2:

<b>Pakistan</b>	PTA is in the process of identification of un-licensed spectrum for IoT in collaboration of Frequency Allocation Board. A Working Group has also been formulated to prepare draft Framework for IoT.
<b>Nepal</b>	The IoT regulatory framework is being drafted.
<b>Maldives</b>	In the case of Maldives IoT could be applied to the electric and water meter reading
<b>I. R. of Iran</b>	We have two types of license regime applied for IoT. The first section is license of mobile broadband operators. According to the license, operators can run narrowband IoT networks as a value-added service in their bands.

	The second section is a class license for IoT devices the same as SRD devices. the license is including some regulations such as allowed radio channels, power transmitter limitation and other specifications, IoT devices should be considered these regulations and the license is public. IoT networks before establishing and running should be notified to the regulatory.
<b>Bangladesh</b>	Bangladesh suspected a considerable growth of IoT in the country with the deployment of 4G services throughout the country. In 2018, BTRC issued Instructions titled 'Instructions on IoT Devices Importation in Bangladesh'. Under these instructions BTRC issues 'Enlistment Certificate' to 'Importers' who are willing to import IoT devices into Bangladesh. The 'Enlistment Certificate' specifies the frequency bands and power output of the devices to be used for IoT applications.
<b>India</b>	The Government of India has issued National Machine-to-Machine (M2M) Roadmap in May 2015. Issues such as formulation of KYC norms for SIM embedded M2M Devices, Registration of MSP (M2M Service Provider) and M2M Pilots are under active consideration of the government. The numbering scheme for cellular M2M/ IoT has already been finalized and implemented. Department of Telecommunications (DoT) has so far not prescribed any licensing mechanism for IoT providers, therefore, currently, IoT providers are not regulated. However, registration of M2M service providers is under consideration in DoT.
<b>Bhutan</b>	Not yet developed

### Question 3:

<b>Pakistan</b>	As described in ITU-T Recommendations Y.2060, the IoT ecosystem players can have a variety of relationships in real deployments based on different possible business models. The license or permission to Platform Provider can be issued by the relevant Authority regulating that particular domain. The Network Providers will be PTA Licensees, The Device Providers will have to have their devices Type Approved from PTA, the Application Provider needs to be a company registered with Security and Exchange Commission of Pakistan (SECP).
<b>Nepal</b>	There is no such a clear licensing mechanism for IoT application. But in general, Nepal Telecommunications Authority (NTA) issues licenses related to telecommunication services, such as network provider, internet service provider, and type approval and Ministry of Communication and Information Technology issue the radio dealer's license and license to keep and use of radio devices
<b>Maldives</b>	We will allocate the bands as per international standard; As of now we haven't have any licensing policy.
<b>I. R. of Iran</b>	<ul style="list-style-type: none"> <li>Platform provider: it depends on type of applications, for example in power metering power distributes Company is responsible for issuing the license and controlling the relative process.</li> <li>Network provider: The administration</li> <li>Device provider: The Administration and Ministry of Industry, Mine and Trade</li> <li>Application provider: Platform provider Guidance</li> <li>Application customer: Ministry of Culture and Islamic Guidance</li> </ul>
<b>Bangladesh</b>	Currently there is no licensing regime for IoT in Bangladesh. But as mentioned in the response to the Question 2, in 2018, BTRC issued Instructions titled 'Instructions on IoT Devices Importation in Bangladesh'. Under these instructions BTRC issues 'Enlistment Certificate' to 'Importers' who are willing to import IoT devices into Bangladesh. The

	<p>‘Enlistment Certificate’ specifies the frequency bands and power output of the devices to be used for IoT applications. The aforesaid Instructions are available in native language Bangla at <a href="http://www.btrc.gov.bd/sites/default/files/notice_files/Instructions%20on%20IoT%20Devices%20Importation%20in%20Bangladesh.pdf">http://www.btrc.gov.bd/sites/default/files/notice_files/Instructions%20on%20IoT%20Devices%20Importation%20in%20Bangladesh.pdf</a></p>
<b>India</b>	<p>No license is required to provide most of the services, except for Network providers, for which a telecom license is required.</p> <p>Department of Telecommunications (DoT) under the Ministry of Communications is the Nodal organization for framing Policy, Licensing and Coordination matters relating to telegraphs, telephones, wireless, data, facsimile and telematic services and other like forms of communications under the Indian Telegraph Act, 1885. DoT is the administrative ministry with respect to any of the matters specified in the Indian Wireless Telegraphy Act, 1933 (17 of 1933). Network Provider commonly termed as Telecom Service Provider in India is governed by the license issued by DoT. Telecom Service Provider is the sole entity who acts as Network Provider to provide the service through wired and wireless access. As of now there is no such provision to issue license to the Device provider. Department of Telecommunications has decided for setting up a National Trust Centre. Framework for a National Trust Centre for Connected Objects, relevant to the Indian context of IoT and M2M, envisages for:-</p> <ol style="list-style-type: none"> <li>Registration of M2M Service Providers</li> <li>Registration of M2M Applications using a Class 2 / Class 3 Certificate taken from the Commercial CA in India</li> <li>M2M ASP interactions coupled through standards based M2M architectures</li> <li>Registration of Devices, which may include following:- <ol style="list-style-type: none"> <li>Record the Embedded Machine Identity or “Machine KYC”</li> <li>Identify the Machine’s Capability, Configuration and Purpose or Use Case</li> <li>Record the Identity [APP ID] of the Application / Server that the Machine is parented to</li> <li>Record the Identity [M2M SP ID] of the M2M Service Provider who is responsible for the Machine with the possibility of admitting changes of the M2M SP</li> <li>Identify the Owner of the Machine with the possibility of admitting changes of the owner</li> <li>Command the Machine to reveal its Identity, configuration</li> <li>Ensure Location Discovery</li> <li>Locking of the Connectivity element to the Remote / Dispersed / Mobile Object</li> <li>Ensure Lawful Intercept and Block / Shut Down</li> </ol> </li> <li>Remote provision of Connectivity</li> <li>High Quality of Service in Connectivity meant for mission critical use cases.</li> </ol>
<b>Bhutan</b>	<ul style="list-style-type: none"> <li>Platform provider: ...N/A</li> <li>Network provider: ...Regulator BICMA</li> <li>Device provider: ...N/A</li> <li>Application provider: ...N/A</li> <li>Application customer: ...N/A</li> </ul>

#### Question 4:

<b>Pakistan</b>	MNO	MVNO	FWA	PSTN	ISP	SAP	BO	CVAS	...	...
-----------------	-----	------	-----	------	-----	-----	----	------	-----	-----

	<div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div></div>
Nepal	There is no specific regulation framework. However, PSTN/MNO/ ISP are providing some IoT applications.
Maldives	We have planned to have license free spectrum such as 433 MHz
I. R. of Iran	<div><div>MNO</div><div>MVNO</div><div>FWA</div><div>PSTN</div><div>ISP</div><div>SAP</div><div>BO</div><div>...</div><div>...</div><div>...</div></div> <div><div><input checked="" type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input checked="" type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div><div><input type="checkbox"/></div></div>
Bangladesh	At present as there is no specific licensing framework for IoT in the country, the permission to provide the IoT service is granted in a case to case basis considering the merit of the applicant.
India	As per the provisions of license issued by DoT, the licensee as MNO, MVNO, PSTN, ISP can provide connectivity to the M2M Service Provider (MSP). However, guidelines for the registration of MSP are yet to be finalized by DoT.
Bhutan	MNO, PSTN, ISP, SAP

#### Question 5:

<b>Pakistan</b>	It is to be decided during IoT Framework related consultations. But for ISM bands, there is no fee. Also, for use in licensed spectrum by MNOs, there is no restriction either since the spectrum is allocated on technology neutral basis.
<b>Nepal</b>	For ISM band of 2.4 GHz (Non-cellular IoT), there is no spectrum fee. For Cellular IoT, most of the spectrums are allocated in technology neutral basis, and thus the IoT service provider can work with telecom operators. In that case, there is no extra frequency fee.
<b>Maldives</b>	As of now we don't have band allocation plans
<b>I. R. of Iran</b>	<p>No, we don't impose any fee for IoT services directly. in fact, the IoT networks have developed by the mobile broadband operators, we had received license fee when we issued the license them.</p> <p>Also, the IoT networks that are included in the class license, we don't impose any fee.</p>
<b>Bangladesh</b>	According to the aforesaid instruction issued from BTRC, 'Importers' who are willing to import IoT devices into Bangladesh has to pay an <i>Enlistment Fee</i> of Tk 28,750/- (USD 338 approx.). For personal users, there is no <i>Enlistment Fee</i> but an <i>Application Fee</i> of Tk 6,350/- (USD 75 approx.) will be applicable.
<b>India</b>	As on date there is no license issued to the entities providing IoT services. The draft registration guidelines for M2M Service Providers issued by DoT does not envisage for license fee as such. However, these guidelines are yet to be finalized by the government.
<b>Bhutan</b>	Not yet done

**Question 6:**

		No.	Spectrum Requirement (MHz)*	Candid Frequency Bands (MHz)		IoT Technology (ies)	Licensed	Unlicensed	Re-farming requirement	
				Lower edge	Upper edge				Yes	No
<b>Pakistan</b>		1	433MHz			Non-cellular technologies		✓		
		2	865 -868 MHz			Non-cellular technologies		✓		
		3	915-927 MHz			Non-cellular technologies		✓		
		4	2.4 GHz ISM band			Non-cellular technologies		✓		
		5	5.7 GHz ISM band			Non-cellular technologies		✓		
		6	3GPP Bands			IoT cellular technologies	✓			

Nepal		No	Spectrum Requirement (MHz)	Candid Frequency Bands (MHz)		IoT Technology (ies)	Licensed	Unlicensed	Re-farming requirement		Remarks
				Lower edge	Upper edge				Yes	No	
		1.	2.4 GHz	2.4 GHz	2.4835 GHz	:		Y			
		2.	5.1 GHz	5.15 GHz	5.35 GHz	:	Y				
		3.	5.8 GHz	5.725 GHz	5.825 GHz		Y				
		3.	433 MHz	433 MHz	434.69 MHz			Y	Yes		Proposed
		4.	868 MHz	865 MHz	868 MHz			Y			Proposed
		5.	700 MHz, 800 MHz, 850 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2600 MHz, 3300 MHz, 3400 MHz, 3600 MHz,				Y				Proposed for Cellular-IoT
		As of now we don't have.									
		Maldives									
I. R. of Iran		No.	Spectrum Requirement (MHz)	Candid Frequency Bands (MHz)		IoT Technology (ies)	Licensed	Unlicensed	Re-farming requirement		
Lower edge				Upper edge	Yes				No		



		1	7 MHz	863	870	Non-cellular technologies		✓		✓
		2	1.7 MHz	433.05	434.750	Non-cellular technologies		✓		
		3	75 KHz	169.4	169.475	Non-cellular technologies		✓		✓
		4	3GPP Bands			IoT cellular technologies	✓			✓
Bangladesh		No.	Spectrum Requirement (MHz)	Candid Frequency Bands (MHz)		IoT Technology (ies)	Licensed	Unlicensed	Re-farming requirement	
				Lower edge	Upper edge				Yes	No
		1	...	433.05	434.79	:		Y		
		2	...	866	868	:		Y		
		3	...	2400	2483.5	:		Y		
		4	...	5725	5875	:		Y		
		India	As per the provisions of license issued by DoT, the M2M Service Provider (MSP) can take connectivity from MNO, MVNO, PSTN and ISP, as per the standard technology. Thus, spectrum holding of MNO in any band may be used for providing connectivity services to MSP. Details of the licensed spectrum bands identified for IMT services are given below:							
Band			Uplink Frequency				Downlink frequency			
700 MHz			703 -748 MHz				758-803 MHz			
			(35 MHz has been earmarked for Access services)							
800 MHz			824-844 MHz				869-889 MHz			
900 MHz			890-915 MHz				935-960 MHz			
1800 MHz			1710-1785 MHz				1805-1880 MHz			
			(55 MHz has been earmarked for Access services)							
2100 MHz			1920-1980 MHz				2110-2170 MHz			
2300 MHz			2300-2400 MHz							
2500 MHz			2500-2690 MHz							
3300 -3600 MHz			3300-3600 MHz							
			(25 MHz spectrum (3400 MHz - 3425 MHz) is identified for ISRO’s use in Indian Regional Navigation Satellite System (IRNSS))							
Unlicensed bands for low power devices :										

	No.	Spectrum Requirement (MHz)	Candid Frequency Bands (MHz)		IoT Technology (ies)	Licensed	Unlicensed	Re-farming requirement	
			Lower edge	Upper edge				Yes	No
	1	1 MHz	433	434		N	U		
	2	2 MHz	865	867	:	N	U		
In case of the unlicensed spectrum in India, earlier, only 2.400-2.4835 GHz and 5.825-5.875 GHz were unlicensed bands for indoor and outdoor use of low power equipment. Recently, 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz and 5725-5875 MHz frequency bands have been included as unlicensed for use in indoor and outdoor environment. Availability of additional 605 MHz unlicensed frequencies will ease the capacity constraints for Wi-Fi and low power equipment and will contribute to further growth of telecom deployments particularly in urban areas and smart cities.									
<b>Bhutan</b>	Not yet done								

#### Question 7:

<b>Pakistan</b>	For ISM bands, applications are processed by PTA. Mechanism for award of other unlicensed spectrum is yet to be defined.
<b>Nepal</b>	Not defined yet.
<b>Maldives</b>	As of now we don't have.
<b>I. R. of Iran</b>	<ol style="list-style-type: none"> <li>1. In unlicensed bands, the equipment can radiate accordance with relative regulations. There is a regulation about SRD devices for IoT equipment is required.</li> <li>2. In licensed bands, in present, MNOs can only use license bands, so the operators make decisions about the amount of using spectrum in their self IoT networks according to the business plan.</li> </ol>
<b>Bangladesh</b>	Spectrum band mentioned in response to Q.6 are assigned for various IoT applications in a case to case basis.
<b>India</b>	Licensed Spectrum is assigned as right to use with complete protection. Assignment of the licensed spectrum is through the auction process for a period of 20 years. The licensee shall have to obtain Wireless Operating License (WOL) from WPC Wing of DoT upon assignment of frequencies and before start of the services through particular base station. Whereas, there is no license required for Unlicensed spectrum, only Type Approval and conformity of the standards by the devices are the criteria for utilization of Unlicensed spectrum. However, there is no protection mechanism for utilization of Unlicensed spectrum bands.
<b>Bhutan</b>	May be administrative process if required

#### Question 8:

<b>Pakistan</b>	They are yet to be finalized and will be part of the IoT Framework. PTA follows international standards.
<b>Nepal</b>	Not standards set yet but we follow any internationally recognized standards, such as ETSI, IEEE, FCC, etc.
<b>Maldives</b>	As of now we don't have.

I. R. of Iran	Frequency Band (MHz)	Technology	Transmit Power (EIRP)	Spectrum Access Technique (e.g. Frequency hopping, Duty cycle, Listen before talk, etc)	Max Transmission Duration	Channel Bandwidth	Spurious Emission	Others (please specify)	
	169.4-169.475	According to answer of question 6	500 mW e.r.p.		≤ 1.0 % duty cycle	≤ 50 kHz	ECC/DEC/(05)02		
	433.05-434.79		10 mW e.r.p.		≤ 10 % duty cycle	Not specified	ETSI EN 300 220		
	863-875.8		ERC REC. 70-03						
	2400-2483.5		10 mW e.i.r.p	-	-	-	EN 300 440		
	5725-5875		25 mW e.i.r.p	-	-	-	EN 300 440		
	880-914.9 /925-959.9		According to 3GPP standards						
	1710-1785 /1805-1880								
	1925-1980 /2110-2170								
	2500-2570 /2620-2690								

<b>Bangladesh</b>	Technology for any specific type of IoT application is approved in a case to case basis. At present LoRa, SRD Communication, RFID and GSM/GPRS based applications have been approved.
<b>India</b>	<p>Telecommunication Engineering Center (TEC) is a technical body representing the interest of DoT, Government of India. TEC has the mandate to prepare specifications of common standards with regard to Telecom network equipment, services and interoperability. TEC provides specifications released as Generic Requirements (GRs), Interface Requirements (IRs) and Service Requirements (SR). TEC also deals with the issuing Interface Approvals, Certificate of Approvals, and Service Approvals &amp; Type Approval.</p> <p>Typical examples of conformity assessment activities are sampling, testing, inspection, evaluation, verification, certification, registration, accreditation and approval, as well as any of their combinations.</p> <p>There is as such no restriction on technical specification(s)/standard(s) deployed by the vendor / service provider subject to the conformity with the specification designed for the same. Presently, all the standards mentioned above are permitted to be used for IoT deployment.</p>
<b>Bhutan</b>	No specifications developed yet

#### Question 9:

<b>Pakistan</b>	IoT specific regulations are yet to be devised. However relevant provisions of Telecom Act, Regulations and License Conditions do apply on Mobile Network Operators planning to offer IoT in licensed bands.
<b>Nepal</b>	No specific regulation yet. However, telecommunication act, regulation, and license condition drive for regulation of cellular IoT.
<b>Maldives</b>	As of now we don't have.
<b>I. R. of Iran</b>	<p>There is a regulation in the country about non-radio conditions that as summary includes:</p> <ol style="list-style-type: none"> <li>1. The IoT must be developed based on the promotion of welfare, social justice, Economy productivity indexes.</li> <li>2. Developing and transferring IoT technology to the country, must be done for known applications based on the prioritized needs.</li> <li>3. All the members of the IoT services chain must be identifiable and authenticable with respect to user privacy and public security.</li> <li>4. Education, research, and training of human resources must be based on the country's prioritized needs.</li> <li>5. The safety principles of users in connecting to the IoT networks must be considered to ensure security and healthy.</li> <li>6. For arriving IoT networks in the country must be considered vital infrastructure risks.</li> <li>7. The IoT ecosystem must only be realized on the National Information Network platform with "Certified relative segments" and "Non-Governmental Stakeholders, especially in data aggregation and processing layers" and "universal business model".</li> <li>8. Systematic localization of the IoT ecosystem components must be done with due regard to strategic priorities and national interests;</li> <li>9. IoT services must be hosted within the range of the possibility of the country's sovereignty.</li> </ol>

	10. All aggregated big data of IoT networks' users must be considered as national assets and must be included data protection requirements.
<b>Bangladesh</b>	At present there is no such regulations devised in Bangladesh.
<b>India</b>	<p>13-digit number scheme for SIM-based devices / Gateways has already been approved by DoT and implemented by TSPs. This scheme will coexist with the 10-digit number system (for voice calling). Other actionable points are a spectrum for low power wireless devices, Embedded SIM, Interoperability, etc.</p> <p>Telecom Engineering Center (TEC) has also come out with 9 technical reports on M2M detailing sector specific requirements/use cases to carry out gap analysis and future action plans with possible models of service delivery. The reports published by TEC are as below: -</p> <ul style="list-style-type: none"> <li>(i) <a href="#">Gateway &amp; Architecture</a></li> <li>(ii) <a href="#">Power Sector</a></li> <li>(iii) <a href="#">Automotive (Intelligent Transport System) Sector</a></li> <li>(iv) <a href="#">Remote Health Management</a></li> <li>(v) <a href="#">Safety &amp; Surveillance Systems</a></li> <li>(vi) <a href="#">Number resource</a></li> <li>(vii) <a href="#">V2V / V2I Radio communication and Embedded SIM</a></li> <li>(viii) <a href="#">Spectrum requirements for PLC and Low power RF communications</a></li> <li>(ix) <a href="#">Smart Homes</a></li> </ul> <p>TEC on 8th January 2019 has released technical report titled “Design and Planning Smart Cities with IoT/ICT”. The report has elaborated upon role of ICT in Smart Cities and related use-cases along with future work to be carried out, work on gap analysis, analyzing the Key Performance Indicators, and studying different Smart City designs worldwide that can be taken as sources of information for the design and development of Smart Cities in India.</p> <p>These documents can be accessed through <a href="http://www.tec.gov.in">www.tec.gov.in</a>.</p>
<b>Bhutan</b>	<ul style="list-style-type: none"> <li>- Information Communications and Media Act 2018</li> <li>- National Radio Rules</li> </ul>

#### Question 10:

<b>Pakistan</b>	Type Approval Regulations can be found at this link: <a href="https://www.pta.gov.pk/en/type-approval">https://www.pta.gov.pk/en/type-approval</a> Specific Regulations for IoT devices have not been framed yet.
<b>Nepal</b>	There is not specific IoT device Type Approvals but we have general Type Approval provision. The corresponding link is given as: <a href="http://nta.gov.np/wp-content/uploads/2012/06/Type_Approval_Working_Procedure_2073.pdf">http://nta.gov.np/wp-content/uploads/2012/06/Type_Approval_Working_Procedure_2073.pdf</a>
<b>Maldives</b>	As of now we don't have.
<b>I. R. of Iran</b>	According to national regulations, all radio equipment at the time of import into the country or production must have a type approval certificate from the regulator to approve its radio

	specifications with predetermined standards and regulations. However, IoT devices are also subject to these regulations.
<b>Bangladesh</b>	Currently Type Approval of IoT devices is not applicable in Bangladesh. The permission for using IoT service is granted in a case to case basis according the aforesaid Instructions. The Instruction are available in native language Bangla at <a href="http://www.btrc.gov.bd/sites/default/files/notice_files/Instructions%20on%20IoT%20Devices%20Importation%20in%20Bangladesh.pdf">http://www.btrc.gov.bd/sites/default/files/notice_files/Instructions%20on%20IoT%20Devices%20Importation%20in%20Bangladesh.pdf</a>
<b>India</b>	Same as response in Q.8
<b>Bhutan</b>	We don't have relevant legislation for IoT Type Approval but we have general Type Approval Rules <a href="https://www.bicma.gov.bt/bicmanew/data/publications/rules-regulations-guidelines/Rules_and_Regulations_on_ICT_Type_Approval_2019.pdf">https://www.bicma.gov.bt/bicmanew/data/publications/rules-regulations-guidelines/Rules_and_Regulations_on_ICT_Type_Approval_2019.pdf</a>

#### Question 11:

<b>Pakistan</b>	PTA Administration or Government agencies are not yet member of any international IoT alliance. However, PTA has applied for institutional membership of LoRa Alliance.
<b>Nepal</b>	Government agencies, including NTA, are not the member of any international IoT alliance.
<b>Maldives</b>	As of now we don't have.
<b>I. R. of Iran</b>	Internet of Things Academy (IoT Academy) by the International Telecommunication Union (ITU) as a Center of Excellence field of the Internet of Things in the Asia Pacific for the period 2022-2019 was elected for 4 years.
<b>Bangladesh</b>	Currently the Administration of Bangladesh is not involved in any international IoT alliance.
<b>India</b>	Telecommunications Standards Development Society, India (TSDSI), is one of the core members of oneM2M alliance. TSDSI is working in collaboration with oneM2M in transposing the international standards into Indian standards. TSDSI is also working in collaboration with oneM2M on Common Service Layer architecture.
<b>Bhutan</b>	No

#### Question 12:

<b>Pakistan</b>	There is no dedicated national research lab for IoT, however, many academic institutions are conducting research on various aspects of IoT. Also, there are small scale IoT manufacturers in Pakistan who are focusing on limited use cases. But things will change once IoT Framework is in place. Government of Pakistan considers IoT as one of the future technologies which is essential for fourth industrial revolution.
<b>Nepal</b>	Only few companies and academic institutions are working on it.
<b>Maldives</b>	We don't have.
<b>I. R. of Iran</b>	<a href="#"><u><i>IoT Academy</i></u></a> According to the experience of designing various conferences, workshops and training courses in this field, international interaction and also as one of the corporations who plays one of the main roles in training and spreading the knowledge of IoT at the international level, IoT Academy has designed and implemented several laboratory facilities in this area and provides various

	<p>organizations, centers, universities, companies, and industries in the country with IoT laboratory equipment according to their needs.</p> <p><u><b>PARSNET Company</b></u></p> <p>PARASNET Company (private equity) under the commercial name of Parsnet Communication Techs, was founded in 2016 by Pars Online holdings with the intention of working in the field of IoT. The ultimate purpose of this company is to create an IoT infrastructure with national coverage. This nationwide coverage will be established within three years. The reason behind choosing this strategic purpose is the convergence of different factors which all indicate the necessity of entering this business. As one of the operators of the Sigfox network in the world and its exclusive representative, Parsnet Communication Techs has started its activities in Iran and has implemented the IoT infrastructure in the country.</p>
<b>Bangladesh</b>	<p>Different private organizations and academia institutions are working on it. Currently, approximately 30 organizations have been working for the deployment of IoT in Bangladesh.</p>
<b>India</b>	<p>A lot of research is being undertaken by various institutions on many aspects of IoT. Some of the broad topics of research are :</p> <ul style="list-style-type: none"> <li>• IoT network design and Cloud networks</li> <li>• IoT enabled Software Architectures and Middleware</li> <li>• Mobile cloud and IoT services</li> <li>• Data and Knowledge Management</li> <li>• Context-awareness and Location-awareness</li> <li>• Security, Privacy and Trust</li> <li>• Software-defined Networking (SDN) support for Cloud and IoT</li> <li>• Performance Evaluation and Modelling in IoT</li> <li>• Networking and Communication Protocols</li> <li>• Energy Efficiency</li> <li>• Virtualization</li> </ul>
<b>Bhutan</b>	Not yet