REGULATORY CHALLENGES OF INTERNET OF THINGS (IOT)

White Paper

CONTENTS

Editor in Chief
Mohd Ali Hanafiah Mohd Yunus — Communications and Digital Ecosystem Sector

Editorial Members	**Division**
Aisharuddin bin Nuruddin	Technology and Society
Badaruzzaman Mat Nor	Technology and Society
Faizal Abdul Rahman	Technology and Society
Norzailah Mohd Yusoff	Technology and Society
Mohd Shamsul Izuan Che Musa	Technology and Society
Suhada Alias	Technology and Society
Muhammad Sya'aban Abdul Hamid	Technology and Society

Published by:
Malaysian Communications and Multimedia Commission
MCMC Tower 1, Jalan Impact, Cyber 6
63000 Cyberjaya, Selangor Darul Ehsan
Malaysia

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000

www.mcmc.gov.my

Printed year:
2018

ISBN No: 978-967-15831-0-4

Executive Summary

The ability of the Internet of Things (IoT) to electronically meter, track and monitor objects in the physical world has inspired a surge of innovation and enthusiasm from multiple industries. Its potential to drive disruptive changes across various sectors presents a myriad of possible services and applications. Gartner estimated that over 26 billion devices will be connected in the year 2020 while the Internet Society projected that the number will increase to 100 billion in year 2025.

Malaysian Communications and Multimedia Commission (MCMC) as the regulator of the convergence communications and multimedia industry, have identified the regulatory challenges and implications, and offer strategies in meeting future demands and facilitating smooth roll-out of IoT in Malaysia. The purpose of this white paper is to provide an overview of IoT background, ecosystem, services and applications. Then, it further discusses on several regulatory aspects of IoT including spectrum requirement, network numbering and addressing, technical standardisation, roaming or mobility requirement, as well as security and data privacy. The paper also touches on the need for talent development and proof of concept (PoC) projects to facilitate IoT adoption.

In the discussion for each regulatory aspect, key areas and scope of study were identified to be used as a guideline for future IoT planning and development. The guideline is necessary to ensure a smooth technical cooperation and device interoperability since there are diverse IoT standards and technologies implemented in many verticals. Furthermore, participation in international organisation such as ITU-T Study Group 20: *Internet of things (IoT) and smart cities and communities (SC&C)* has provided MCMC with an avenue to keep abreast of the latest advancements and activities.

Other than regulating, it is also vital that MCMC is actively involved in the promotion and adoption of IoT in the local industry. This is indicated by MCMC's initiatives such as Digital Lifestyles Malaysia (DLM), Smart Community, and Industry Promotion and Development Grant on IoT and New Technologies. Capacity building in meeting demands of competent professionals and non-professionals in IoT technology is also required.

Finally, MCMC has formed an internal task force comprising of relevant divisions which were responsible of studying and analysing the issues at hand and further outline the way forward and recommendations for the establishment of a new IoT Regulatory Framework.

Regulatory Challenges of Internet of Things (IoT)

Introduction

In 2013, MCMC introduced the Digital Lifestyle Malaysia initiative to spearhead the development of the IoT in identified verticals or sectors. MCMC initially identified 6 key verticals or sectors which represent activities in our daily lives whereby Digital Lifestyle Malaysia initiative can be implemented through the IoT. Later on to accelerate development and adoption, these have evolved into four focus areas in the form of Traceability, Connected Healthcare, Home and Living Community, and People Friendly Commuting.

The most successful among the focus areas which gained traction and acceptance by stakeholders is the traceability initiative which was introduced in the agriculture sector in ensuring the authenticity of swiftlet nests for export to China. The traceability system in place now is indispensable in the swiftlet nests value chain and is recognised by Department of Veterinary Malaysia. The Chinese government and Department of Veterinary Malaysia have made it mandatory for exporters of swiftlet nests to utilise the system in ensuring authenticity.

In the year 2020, people will be living in an era of the IoT whereby billions of smart devices or things will be connected over clouds, generating massive volume of data. Subsequently, the data are processed and analysed into meaningful data. Gartner estimated that over 26 billion devices will be connected in the year 2020 while the Internet Society projected that the number will increase to 100 billion in year 2025. The IoT applications are crucial in improving the quality of life and efficiency of smart sustainable cities' operations in an automated manner via seamless connectivity.

In line with the global ICT development, Malaysia is set to reach an advanced economy by the year 2020 that will be built upon a knowledgeable and skilled society supported by a robust, vibrant and sustainable ICT industry. For this purpose, the IoT has been defined as one of the nine strategies set under the Re-energizing the ICT in the Eleventh Malaysia Plan (RMK 11).

The industry is in need of a new comprehensive IoT Regulatory Framework to complement the National IoT Strategic Roadmap which was launched in July 2015. As a regulator of the convergence communications and multimedia industry, it is imperative for MCMC to identify the regulatory challenges and implications, and offer strategies in meeting future demands and facilitating smooth roll-out of the IoT in Malaysia.

MCMC should identify several priority areas to help support the growth of the IoT and these areas

could include spectrum availability, data privacy, network security and resilience, network addresses, talent development, P.O.C/pilots and technology standardisation.

Background

There are many definitions of the IoT. http://whatis.techtarget.com/definition/Internet-of-Things defines IoT as "the third wave of the internet", "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to computer interaction".

Another website, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand, defines IoT as "the concept of basically connecting any device with an on and off switch to the internet (and/or to each other"). It has also been referred to as "physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community".[1]

International Telecommunication Union (ITU) through its Recommendation Y.2060 defines IoT as a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

The applications of the IoT cover every aspect of life, from personal wearable to autonomous vehicles and Industrial Internet[2], built from the integration of hardware, software, technologies and connectivity.

IoT Ecosystem

From technical perspective, the IoT is a network of smart devices with the ability to detect changes in its environment, generate raw data and subsequently transmit the data over cloud to backend system for data analytics. Diagram 1.0[3] illustrates the IoT ecosystem and how elements in the ecosystem are interconnected.

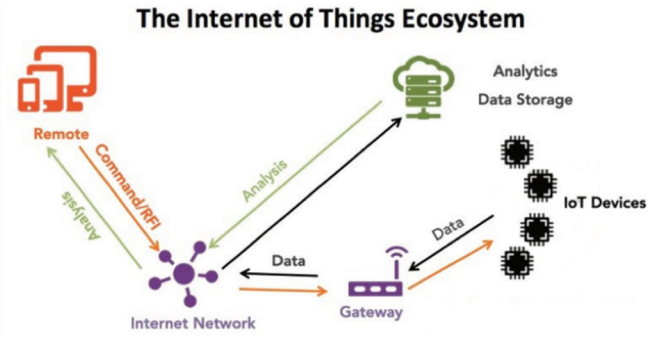


Diagram 1.0: IoT Ecosystem

The IoT will not be a single network and will comprise of many different technologies and devices. Diagram 1 provides a simplified generic overview of the IoT. This has four key elements:

a. IoT devices: As described above, the IoT is likely to grow to include hundreds of millions of devices over the coming 10 years, the majority of which will require wireless connectivity. The characteristics of these IoT devices will vary, depending on the applications they support;

b. Wireless networks: IoT devices transmit the data they have collected wirelessly to base stations, network access points or via advanced mesh networks, using a range of existing and emerging technologies. These wireless networks will require

1 https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

2 A term coined by General Electric (USA) referring to the integration of complex physical machinery with networked sensors and software. The industrial Internet draws together fields such as machine learning, big data, the Internet of things and machine-to-machine communication to ingest data from machines, analyse it (often in real-time), and use it to adjust operations.

3 http://www.businessinsider.com/internet-of-things-2015-forecasts-of-the-industrial-iot-connected-home-and-more-2015-10

access to appropriate spectrum bands to meet different capacity and coverage requirements;

c. Internet: Connecting IoT devices to a wider network or the public internet means more devices can become interconnected and the data collected can be analysed and stored in the most appropriate place. However, this interconnectivity can also raise new network security and resilience issues; and

d. Data storage and analysis: Many of the future benefits from the IoT will be delivered by new services based on the analysis of data from a wide range of sources. Some of this data may be personal or commercially sensitive, so it will be important to ensure that it is stored and processed securely and with appropriate consent.

From economic perspective, the IoT possesses a huge global market potential. Internet Society estimated a USD11 trillion opportunity for global economy in 2025 while Gartner estimated a RM42.5 billion of opportunity for Malaysia in 2025.

As a result, private and public sectors have embarked on IoT related activities to stimulate IoT promotion and development.

IoT Services and Applications

The IoT is primarily designed for serving low-power, infrequent, tiny data at lower prices. Considering such nature, major companies such as Huawei and SK Telecom are actively developing relevant services, with major focus on 3 areas:

I. Metering
Metering and collecting of usage data in facilities (e.g. gas, water, power, etc.).

II. Tracking
Collects and manages location data of automobiles, persons/properties, movable assets, etc., facilitating personal safety and industrial asset management.

III. Monitoring
Controls and manages the status and conditions of manufacturing, public and commercial facilities.

Based on these major services, the industry, academia and regulatory organisations foresee numerous and diverse applications of the IoT. The European Research Cluster on the Internet of Things (IERC)[4] vision is that "the main objectives for IoT are the creation of smart environments/spaces and self-aware things for climate, food, energy, mobility, digital society and health applications". These applications are ubiquitous and can permeate into practically all areas of everyday life of individuals, enterprises and society.

The current hype around the IoT creates an explosion of new IoT-enabled products and applications every day. IoT Analytics[5] carried out a research to identify the current top 10 IoT applications. They conducted data mining of hundreds homepages, and managed to assemble and verify 640 actual IoT project enterprises worldwide. The result for quarter 3, 2016 is shown in Diagram 1.1.[6]

Most of the projects IoT Analytics identified are in industrial settings (141 projects), followed by Smart City (128) and Smart Energy IoT projects. The Americas made up most of those projects (44%), followed by Europe (34%). There are large differences when looking at individual IoT segments and regions. The Americas and particularly Northern America are strong

4 IERC Cluster SRIA 2015 - Internet of Things Beyond the Hype: Research, Innovation and Deployment.

5 Market insights for the Internet of Things (IoT), M2M, and Industry 4.0, https://iot-analytics.com/

6 IoT Analytics 2016 Global overview of 640 enterprise IoT use cases (August 2016).

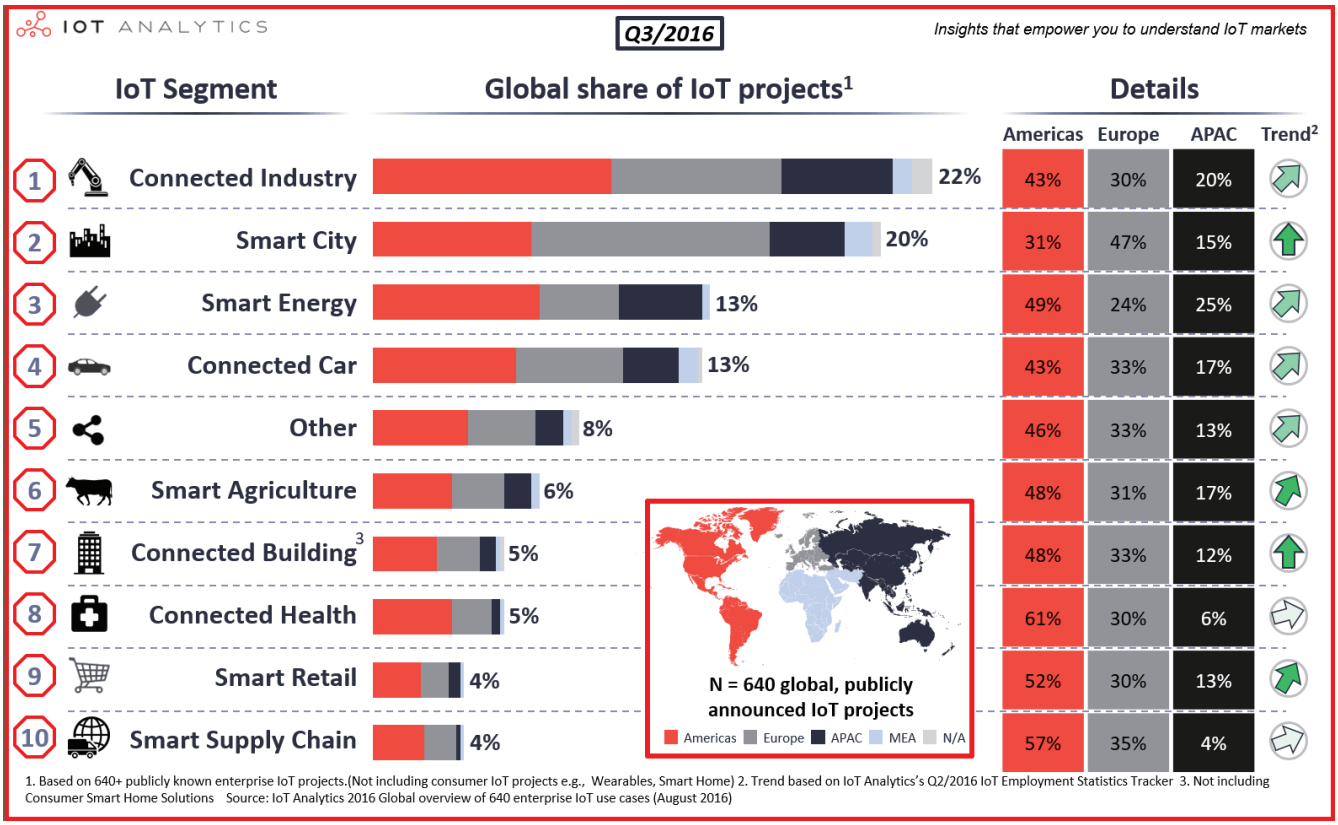


Diagram 1.1: The Top 10 IoT Application Areas

in Connected Health (61%) and Smart Retail (52%), while the majority of Smart City projects are located in Europe (47%). The Asia/Pacific region is particularly strong in the area of Smart Energy projects (25%).

Regulatory Challenges

Even though the IoT technologies are driven by market forces, MCMC foresees that IoT rollout would be challenging without facilitation from the regulator. In understanding the issues, MCMC has studied a number of reports[7] from several international bodies and identified five (5) regulatory aspects under the purview of MCMC of which it will take heed and subsequently address the potential challenges mainly on resources, technical challenges, competition, data privacy and security.

a. Resources: Spectrum Requirement

Diversity in various IoT verticals utilises a myriad of applications and devices which will employ a range of technologies and spectrum bands in delivering IoT services. In enabling the IoT, different wireless communication standards operating in either unlicensed or licensed spectrum may be used and the selections depend on the purpose and the distance coverage. There are two types of wireless communication standards: short-range and long-range as shown in Diagram 1.2[8]. For instance, Low Power Wide Area (LPWA) technology such as LoRa

7 i. International Telecommunication Union (ITU), Global Symposium for Regulators, June 2015 - GSR discussion paper Regulation and the IoT

ii. Internet Society (ISOC), October 2015 – The IOT: Understanding the Issues and Challenges of a More Connected World,

iii. Body of European Regulators for Electric Communications (BEREC), February 2016 – Report on Enabling the IoT

8 Samsung Networks:- Internet of Things, Introducing innumerable opportunities

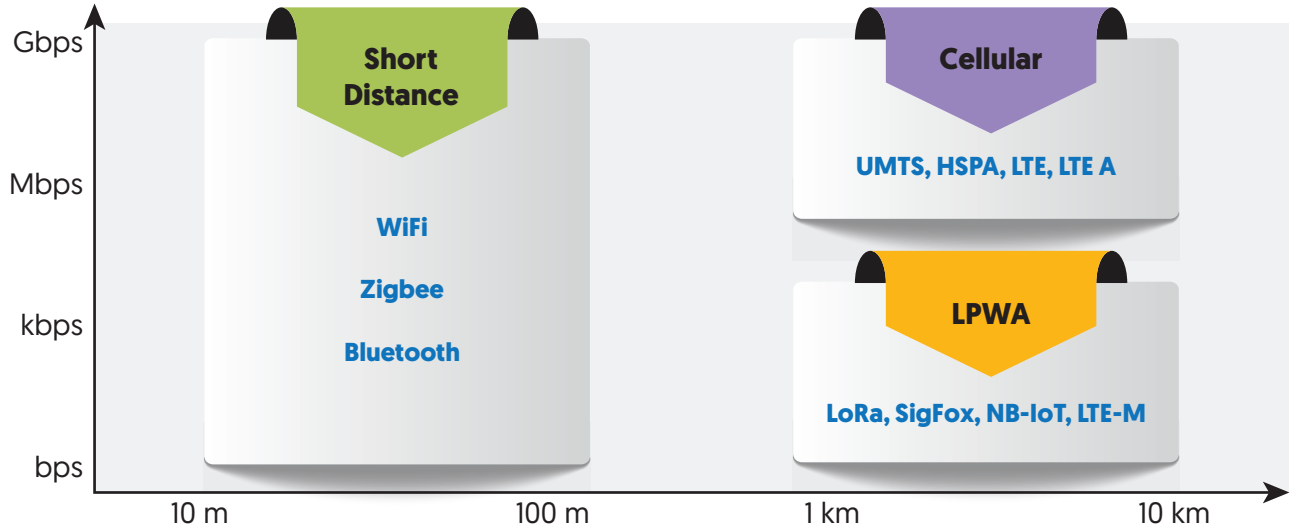


Diagram 1.2: Short-range and long-range communications standards

and Sigfox would be able to cover maximum distance up to 10 km using unlicensed narrowband spectrum. Keysight Technologies[9] indicated that there are more than sixty (60) legacies and new communication standards being developed for IoT-related applications as shown in Attachment A.1.
The development of wireless communication standards continues to grow at a fast pace. As the authority for national spectrum, it is important for MCMC to ensure availability of spectrum for a wide range of IoT applications.

There are a few factors which will determine spectrum requirement as described in diagram 1.3 below:

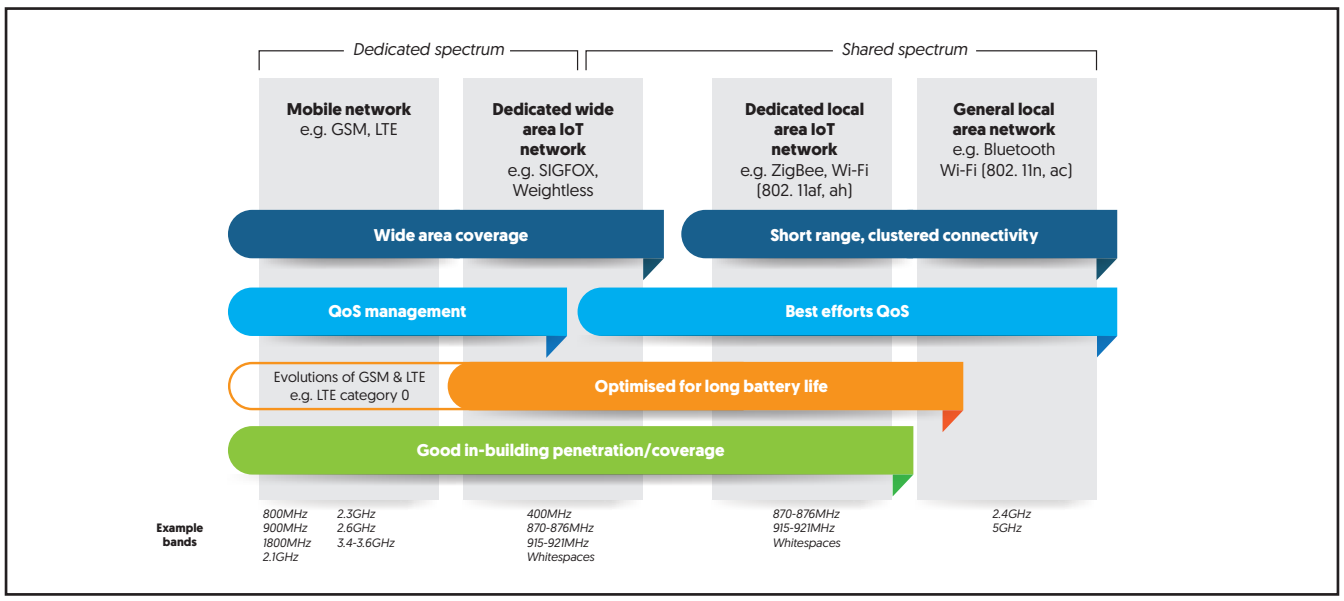


Diagram 1.3: Framework for IoT Spectrum Requirement

9 Keysight Technologies, or Keysight, is a US company that manufactures test and measurement equipment and software.

While experts are considering use of white space as the spectrum for IoT, the critical issues that MCMC foresees to surface is Quality of Service (QoS) issues arising out of potential spectrum congestion for IoT operating in unlicensed spectrum - a situation whereby large numbers of IoT devices transmit simultaneously using frequencies that are close to each other. Mission critical IoT applications such as connected driverless vehicles would require excellent QoS to ensure uninterrupted operation.

Further studies on the following areas are essential to ensure adequate resources for IoT applications in the longer term as the market develops.

Key Area	Scope
Spectrum Requirement for the IoT	Study and keep tabs with the development of new communication standards for the IoT. Identify modulation technologies, Duty Cycle and EIRP limits which can mitigate congestion in Class Assignment frequencies
Market Study	Study on the size and shape of Malaysia's market to determine the future demand for spectrum for IoT applications.
Additional Spectrum Band for the IoT	Study on the feasibility of making new bands available for IoT applications.

b. Resources: Network Numbering and Addressing

Like every communication equipment, IoT devices need to be identified before connecting to a network where numbering resources and addressing serve as the identifiers. Naturally, the identifiers for IoT devices operating in public networks will be based on E.164[10], E.212[11] , IPv4 or IPv6 depending on which network they are connected to. For instance, IP addresses are used as identifiers for devices connected to IP network while E.164 are used for devices connected to public telecommunication network. One concern that may surface in the long run is the adequacy of E.164.

IPv4 addresses in Malaysia is already in short supply and proliferation of IoT devices utilising IP addresses would raise the demand for IP addresses. MCMC's proactive role for the past three years on mandating NSP and ASP licensees to eventually migrate to IPv6 addressing would deal with the enormous demand forecasted to be generated by IoT roll-out. MCMC does not foresee any issue on availability of IPv6 addresses for IoT roll-out.

For IoT applications that are using licensed spectrum, Embedded Subscriber Identity Module (e-SIM) is considered effective and efficient in managing a huge number of IoT devices especially when it comes to SIM replacement. To put it into perspective, it is costly to dispatch a technician to a remote area just to replace a physical SIM installed, whereby with e-SIM it can be done remotely over the network.

Further study on the following areas is essential to ensure adequate numbers are available for IoT applications.

Key Area	Scope
E.164	Study the existing numbering plans to accommodate IoT deployment either by opening up a dedicated numbering range or increasing the capacity.
e-SIM	Study on e-SIM requirement and capabilities.

10 International public telecommunication numbering plan - ITU.

11 International identification plan for public networks and subscriptions - ITU.

c. Technical: Standardisation

The main purposes of standardisation in telecommunications sector are to prevent barriers to trade and to promote facilitation of technological cooperation in ensuring the safety and interoperability of communication equipment and system. The latter is done through certification activities conducted by the appointed certifying agency, which in this case is SIRIM QAS.

Standardisation in the IoT is an enormous challenge as there are various sectors or verticals using many technologies championed by diverse alliances of Standard Developing Organisations (SDOs). Diagram 1.4[12] below depicts the current scenario in standardisation world.

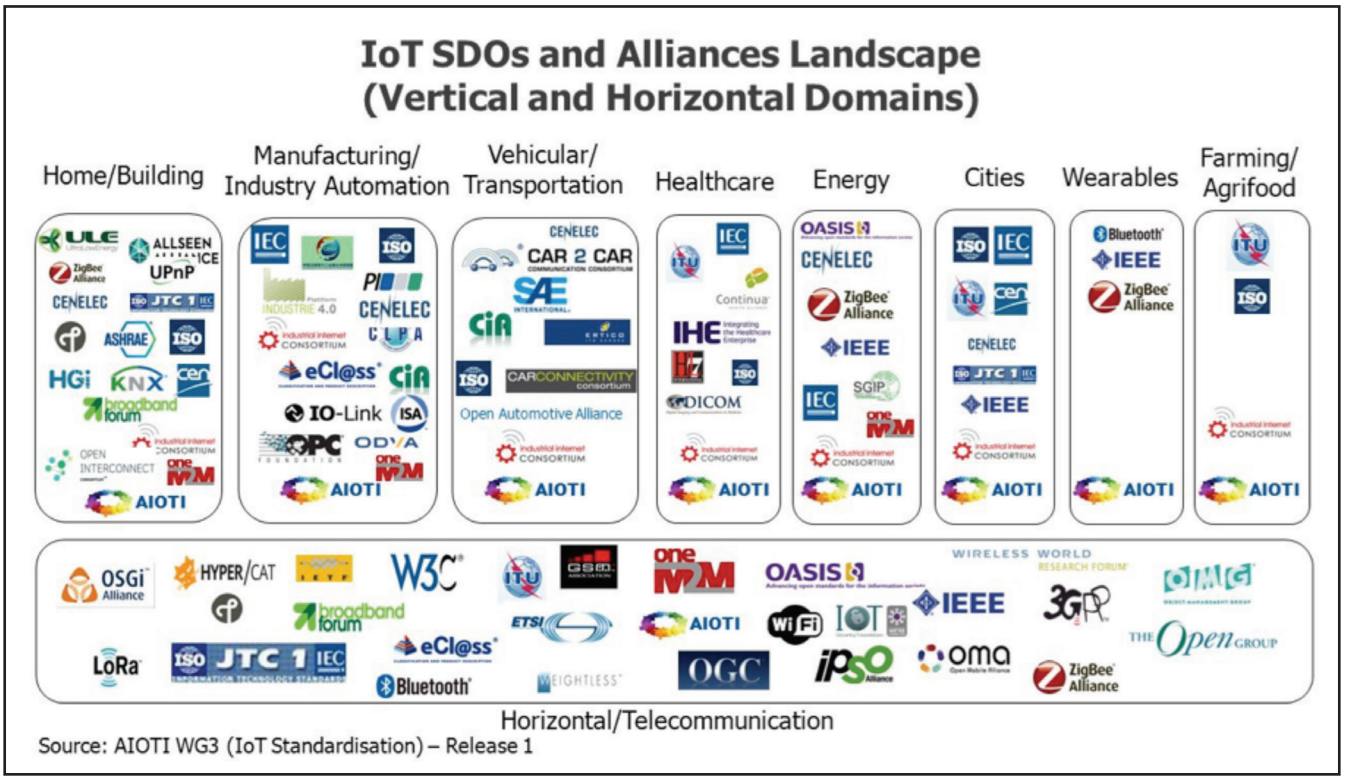


Diagram 1.4: IoT SDOs and Alliances Landscape

12 AIOTI WG3 (IoT Standardisation) - Release 1

MCMC's involvement in ITU-T Study Group 20 should be further enhanced for it to keep abreast of latest development in standardisation activities. Further study on each of the following areas is necessary to ensure IoT devices entering the market in the future are safe to operate and interoperable with legacy and new networks. This can be achieved through standards development in the form of Technical Code, Best Practices and Guidelines.

Key Area	Scope
Device Safety	Study on the relevancy of the current exercises that cover electrical safety, Electromagnetic Compatibility and Radio Frequency safety for IoT devices.
Interoperability	Facilitate interoperability challenges between legacy and new networks through adoption of International standards.
Proficiency	Study the needs to expand the scope of current proficiency exercise from cabling work to installation work of IoT devices.
Human Health	• Study the implications of EMF emitted from IoT devices. • Study the requirement for proper disposal of end-of-life IoT devices.

d. Technical: Roaming or Mobility Requirement

In mobile communications, roaming services allow users to continue using mobile services when travelling out of the country without the needs to change SIM card. This is made possible through technical and commercial coordination between roaming partners of the participating countries. Likewise, in the IoT, roaming is an important feature to ensure that IoT devices continue to function seamlessly when roaming from one country to another. Transportation sector such as logistics or retail industry in GS1[13] scheme using IoT services consist of vehicle and goods movement between countries would require IoT services coverage throughout the countries.

Technically, MCMC foresees that IoT roaming on cellular network would not create a major issue since it can leverage on the existing roaming system. However, the challenges are on IoT devices/services which are based on Low Power Wide Area (LPWA) technologies using class assignment frequency bands such as LoRa and Sigfox. A new roaming system needs to be developed to support LPWA roaming especially operating in class assignment band. Hence, further study on IoT roaming requirement is deemed crucial.

Key Area	Scope
IoT Roaming Requirement	• Study on IoT roaming requirement and capabilities. • Keeping tabs with IoT roaming development in neighbouring countries.

e. Security and Data Privacy

On 21 October 2016, Domain Name System (DNS) of Dyn[14] was brought down by Distributed Denial of Service (DDOS) attack launched by large number IoT devices that have been compromised by botnet called Mirai. This attack caused major websites such as Twitter, Netflix, Amazon and many more to become unreachable. The incident has prompted the urgency for a new IoT cyber security policy and strategies.

IoT system and devices to be installed here in Malaysia may be subjected to close scrutiny and certified to a minimum level of vulnerability and penetration testing. For this purpose, a certification scheme on vulnerability and penetrability of IoT devices can be created to ensure risk of DDOS attacks using botnet of IoT devices are minimised.

MCMC believes that IoT security would not solely depend on cyber security but also on the physical security of the devices. While cyber security minimises service interruption, physical security would minimise theft and vandalism, both of which are not good for businesses.

13 GS1 is a non-profit organisation that provides supply chain standards. The standards define ways to store and transfer data whereby the organisations can exchange information smoothly. i.e barcoding, Radio Frequency Identification (RFID).

14 Dyn, Inc. (US) is an Internet performance management company, offering products to monitor, control, and optimise online infrastructure, and also domain registration services and email products.

As IoT is about collecting data for processing, data privacy is expected to be an issue that will require coordination effort with the Department of Personal Data Protection. Further studies on the following areas are crucial to ensure that IoT applications are running smoothly and without being compromised virtually or physically.

Key Area	Scope
Security	• Feasibility to incorporate security test in the device security programme. • Coordination effort with other agencies i.e Cybersecurity Malaysia, Majlis Keselamatan Negara, Polis Di Raja Malaysia. • Certification scheme on vulnerability and penetrability of IoT systems and devices
Data Collection	Coordination effort with the Department of Personal Data Protection.

Other Aspects to Facilitate IoT Adoption

f. Talent Development and Proof of Concept

Even though the myriad of technologies currently available in every IoT ecosystem provide good options for choice, it still could work against acceptance of IoT by the industry as the disparate technologies could not convince the industry to invest in IoT roll-out. Proprietary technologies could turn out to be not future proof nor interoperable with other IoT network and this would discourage investment in IoT systems.

European Community realising these challenges has taken the necessary steps to issue through ETSI a Technical report titled IoT Standards Landscape and Future Evolution as a guide for European Community members to implement Large Scale Pilots (LSP).

Even though Malaysia cannot afford Large Scale Pilot like the European Community, some initiatives must be in order as not to be left out in understanding the range of technologies and systems in IoT Ecosystem. The Smart Community projects in Kemaman, Kota Belud, Lundu, Putrajaya and Proof of Concept (PoC) projects utilising IoT Grants through Malaysian Technical Standards Forum Bhd (MTSFB) are two initiatives which can create better understanding of the technologies and systems in IoT Ecosystem. The PoC project grants should be increased to cater for this need.

The Industry Promotion and Development Grant on IoT and New Technologies provide funding for PoC and test-bed deployments that later can be used as reference to develop standards and other relevant regulatory tools via MTSFB.

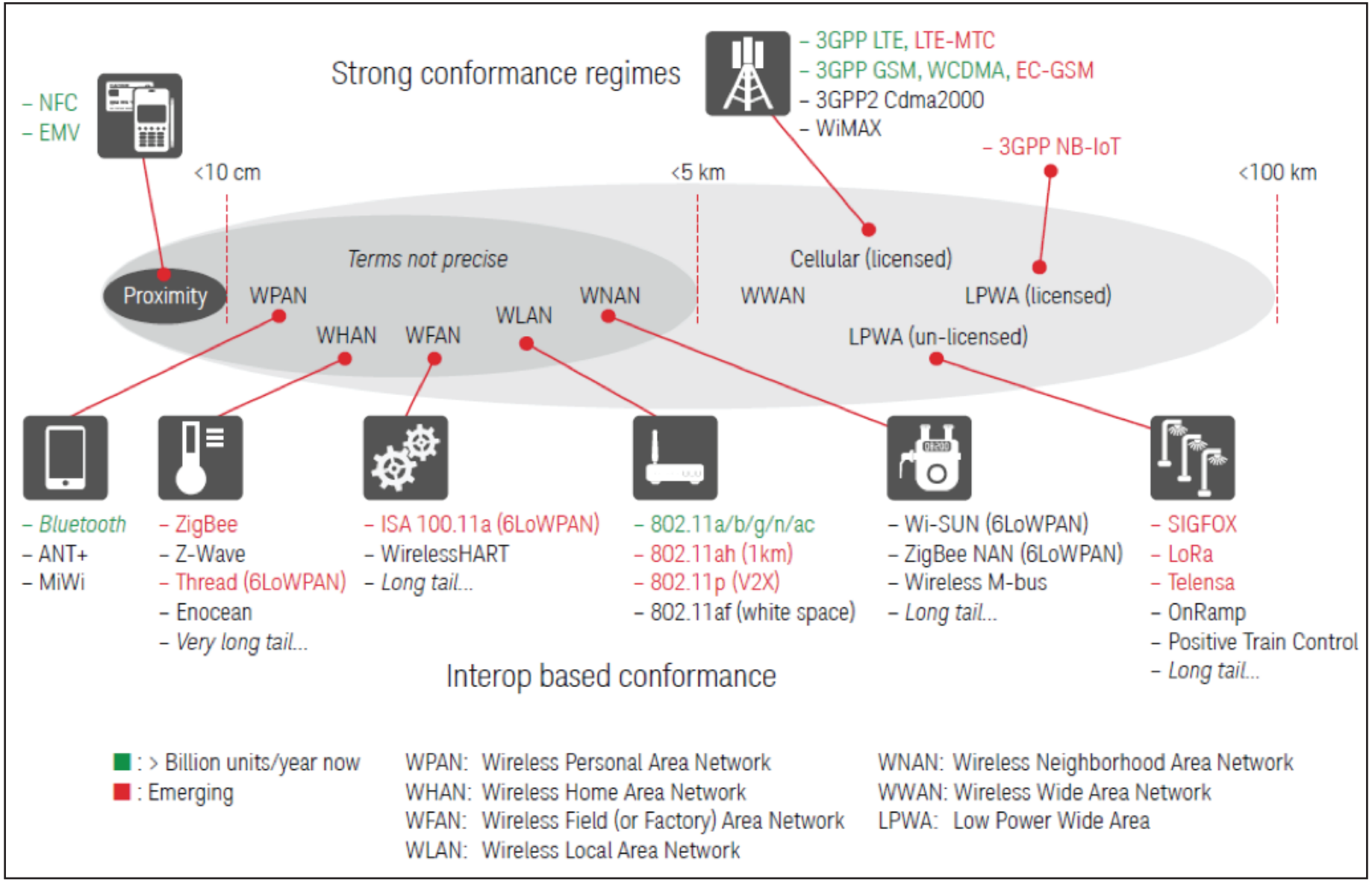
These ranges of technologies and system in IoT Ecosystem are usually state of the art and new to Malaysian. Roll-out of IoT technologies would create enormous demand for competent technicians, data analysts and engineers in the IoT. In response to the need of professionals competent in IoT technology, MCMC has initiated measures to meet talent development needs such as collaboration with

Universiti Sains Malaysia (USM) in providing platform for comprehensive training in the IoT for the industry. However, the courses offered by USM are geared towards engineers and at the moment there seems to be none geared towards Sijil Pelajaran Malaysia leavers/Technical certificates/diploma holders.

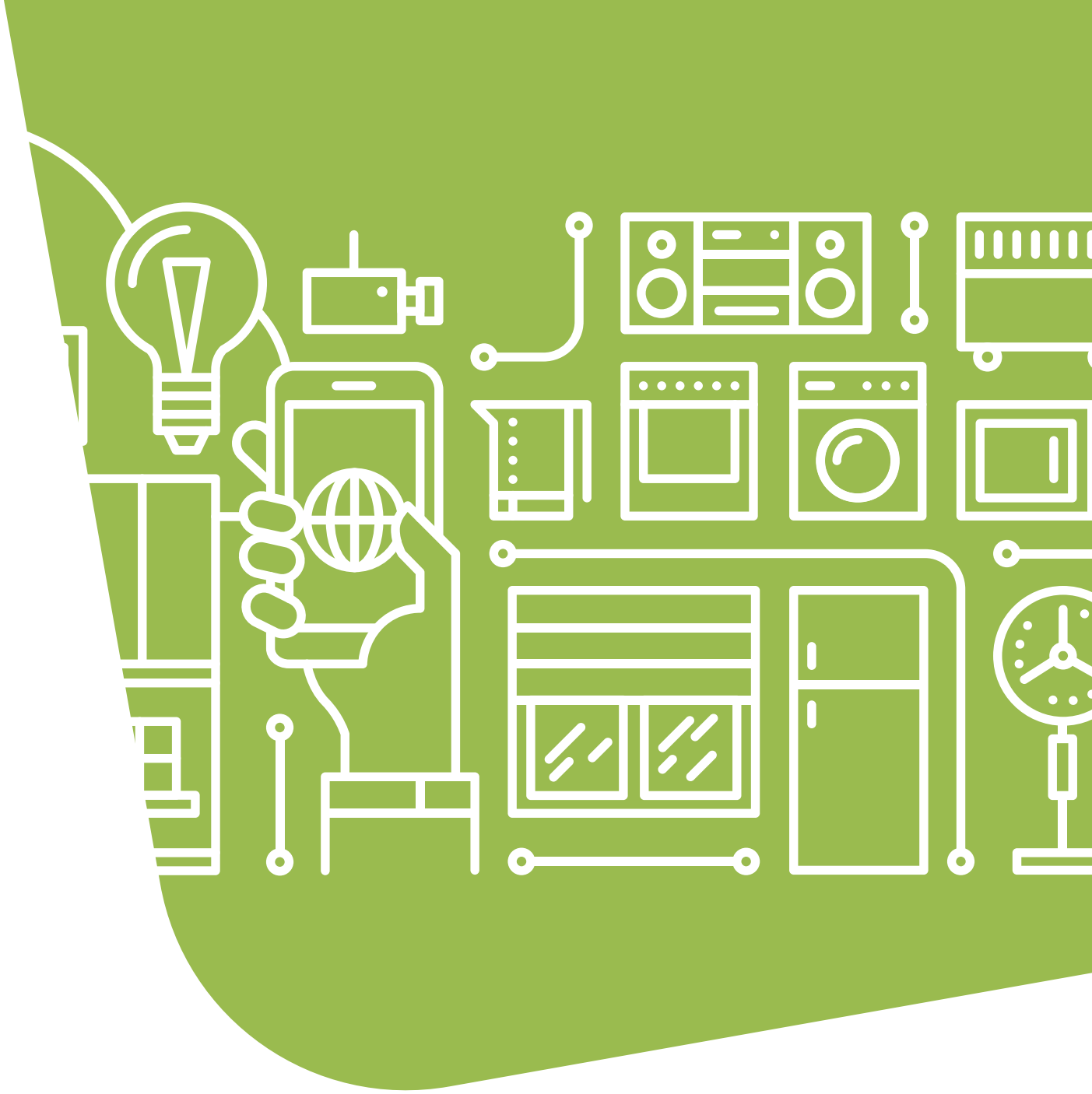
Smart partnership with Ministry of Human Resource's Skill Malaysia programme and Community Colleges under Ministry of Education would be another potential area to explore in creating courses for technician level in the IoT.

Conclusion

A new comprehensive IoT technical report which aims to outline the guiding principles and mechanics from the regulatory point of view is considered necessary in facilitating IoT deployment and adoption in Malaysia.



Attachment A.1: Keysight Technologies: legacies and new communication standards being developed for IoT-related applications.



Suruhanjaya Komunikasi dan Multimedia Malaysia
Malaysian Communications and Multimedia Commission
MCMC Tower 1, Jalan Impact, Cyber 6
63000 Cyberjaya, Selangor Darul Ehsan, Malaysia.
Tel +603 8688 8000 **Fax** +603 8688 1000
E-mail tdd@cmc.gov.my

www.mcmc.gov.my

9 789671 583104