INTERNET OF THINGS (IOT)
TECHNICAL REGULATORY ASPECTS & KEY CHALLENGES

TECHNICAL REPORT

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 by:
Digital Perspective Sdn Bhd

Printed year:
2018

ISBN No: 978-967-13284-9-1

Table of Contents

Chairman's Foreword 2
Preface 3
Executive Summary 4
Introduction 6
Internet of Things (IoT): Technical Regulatory Aspects

Spectrum Requirement 7
Background
Challenges
Requirement
Class Assignment
Way Forward

Network Numbering and Addressing 9
Background
Challenges
Requirement
E.164 and E.212
IPv6
Way Forward

Technical Standardisation 10
Background
Challenges
Requirement
- Technical Codes
- Testing
- Certification
- Labelling
- Importation

Way Forward

Roaming or Mobility Requirement 14
Background
Challenges
Requirement
- Inter-operator charging models
- Projected revenue growth

Way Forward

Security and Data Privacy 16
Background
Challenges
Requirement
- Data Privacy Protection
- Technical Codes Development
- Annual CMI Sector Cyberdrill Exercise
- ISMS & BCMS Implementation

Way Forward

Capacity Building 19
Background
CTPR Master Class for ASEAN Countries
CTPR Professional Master Class on Smart Digital Nation, Cities and Communities

Advocacy and Awareness 20
Background
myMaker Initiative
Digital Lifestyle Malaysia – Experiential Learning Space
Digital Lifestyle Malaysia – Pilot Projects
- Track and Trace
- Healthcare
- Transportation
- Retail & Payment
- Agriculture

Conclusion 22

Use Cases
LoRa Platform, Application & Services 24
FAVORIOT - Quest towards 100k IoT Professionals 25
Security and Integrated Flood Operation Network (SAIFON) 29
IoT Enabled Connected Life Services 34
Information Security Management System 47
MyMata: Cloud Surveillance with Artificial Intelligence 47

Chairman's Foreword

As the Fourth Industrial Revolution sweeps over the global front, the Malaysian Communications and Multimedia Commission (MCMC) irrefutably takes up the challenges to bring the nation one step ahead in the digital era. Understanding that this new industrial revolution brings on bigger and more intricate challenges, MCMC has positioned itself as the key driver to prepare Malaysia with the platform for borderless information, brought forward by the Internet of Things (IoT). The IoT will empower the general public with broader and deeper data which they can use in daily lives and in return contributing to greater efficiency, higher productivity, and better quality of life. This is in line with the Re-energising the ICT strategy outlined in the Eleventh Malaysia Plan (RMK 11).

IoT's dynamic characteristics have allowed start-up companies, universities, and Makers community to venture into developing IoT applications and services. Intelligence, enormous scale, and dynamism have allowed creativity to flow trans-border, thus promoting the creation of useful and effective new applications and services across various verticals.

It is imperative to ensure that any initiatives to develop and design IoT systems and services comply with technical regulations stipulated in the Communications and Multimedia Act 1998, as this will ensure safety and interoperability.

MCMC envisages that this Technical Report becomes a reference for the stakeholders in rolling out IoT applications and services in Malaysia, especially start-up companies, universities and Makers community who are less than familiar with such technical regulatory requirement. This Technical Report defines the requirement and procedures to achieve compliance to the technical regulatory requirements including Spectrum Requirement, Network Numbering and Assignment, Technical Standardisation, Roaming or Mobility Requirement, and Security and Data Privacy in order to implement IoT applications and services in Malaysia.

MCMC ensures continuous updates on this document so as to reflect progression in technology.

Thank you.

TAN SRI DR. HALIM SHAFIE
Chairman
Malaysian Communications and Multimedia Commission

Preface

The seamless interconnectivity empowered by the Internet of Things (IoT) makes it one of the key technologies shaping both the real and virtual world. The connectivity across services, processes and verticals definitely creates opportunities for innovation and creativity. MCMC has taken steps to study Malaysia's readiness for IoT implementation from the technical regulatory aspects. Through the *Regulatory Challenges of Internet of Things (IoT) White Paper*, MCMC has identified challenges with regards to Spectrum Requirement, Network Numbering and Addressing, Technical Standardisation, Roaming or Mobility Requirement, and Security and Data Privacy. This report outlines in great detail these challenges, their requirements and identified solutions.

Executive Summary

The Internet of Things' (IoT) potentials to drive disruptive changes across various verticals presents a myriad of possible applications and services. According to a Gartner, Inc. report (Jan, 2017), it is forecasted that over 20.4 billion devices would be connected digitally by the year 2020.

IoT can be viewed as a global infrastructure for the information society, as it enables advanced services, interconnecting both physical and virtual things either on existing or evolving interoperable information and communication technologies (ICT). Since interconnectivity[1] and things-related services[2] are the two main fundamental characteristics of IoT, it is imperative for MCMC as the regulator of the Malaysian communications and multimedia industry to ensure a smooth and efficient roll-out of IoT applications and services.

Regulatory Challenges of Internet of Things (IoT) White Paper, which was produced in April 2017, identifies requirements and highlights key challenges of IoT implementation, specifically on technical regulatory aspects. Subsequently, MCMC has formed a task force which is responsible in ensuring regulatory challenges in IoT implementation are addressed in facilitating smooth roll-out in Malaysia.

This Technical Report ('Report') accords clarity on technical regulatory requirements for the IoT roll-out and serves as technical reference for interested stakeholders.

Five (5) technical regulatory challenges were identified and discussed; the challenges discussed were (1) Spectrum Requirement; (2) Network Numbering and Addressing; (3) Technical Standardisation; (4) Roaming or Mobility Requirement; and (5) Security and Data Privacy. The Report also highlights the needs for talent development and Proof of Concept (PoC) projects in order to accelerate IoT adoption.

1 With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

2 The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

Feedback from the Industry Working Groups (IWGs) of the Malaysian Technical Standards Forum Bhd (MTSFB) was acquired to understand the views and concerns from the industry. Furthermore, the task force also reviewed several use cases from different verticals which played pivotal roles in developing this Report. Amongst others are:

- LoRa[3] Platform – a collaboration between Atilze Digital Sdn Bhd and Cyberview Sdn Bhd on the development, and deployment of the LoRa platform, application and services;
- Favoriot Platform – a collaboration between Favoriot Sdn Bhd and 15 universities to develop and deploy a platform for lab experiments, and final year and research projects;
- Security and Integrated Flood Operation Network (SAIFON) project – implemented by Ingeniworks Sdn Bhd;
- Connected Home and Smart Hotels project – developed by BNetworks Sdn Bhd;
- Information Security Management System – developed and implemented by Digi Telecommunications Sdn Bhd; and
- Cloud Surveillance with Artificial Intelligence Project – developed and implemented by Ipinfra Networks Sdn Bhd.

MCMC would like to stress to all interested IoT stakeholders on the importance of adhering to the technical regulatory specifications set out in this Report so as to ensure not only smooth roll-out but also for the best interest of the general public safety and privacy.

3 LoRa is a spread-spectrum technology with a wider band (usually 125 kHz or more). Its frequency-modulated chirp utilizes coding gain for increased receiver sensitivity.

Introduction

The IoT provides seamless interconnectivity of people and smart devices across services, processes and verticals. Along with 5th generation mobile network (5G), cloud computing, big data and software-defined network (SDN), IoT will be the key technology shaping the world beyond 2020. With IoT, virtually endless possibilities and connections can be realised, giving a magnitude of impact on daily lives.

Multiple verticals have started to benefit from innovations and enthusiasm on utilising IoT. This has definitely created opportunities. Needless to say, challenges too come with every benefit and opportunity.

MCMC acknowledges that IoT is a challenging emerging area for regulators and policy makers as it is a rapidly developing environment and its technology spans many industries and uses. Therefore, as the regulator of the communications and multimedia industry in Malaysia, MCMC is obligated to facilitate the smooth roll-out of IoT in the country.

Internet of Things (IoT): Technical Regulatory Aspects

The Malaysian communications and multimedia industry is governed by the Communications and Multimedia Act 1998 (CMA). As the regulator, MCMC has identified the technical regulatory challenges and implications, and offered strategies in meeting future demands and facilitating smooth roll-out of the IoT in Malaysia.

The Technology and Society Division of MCMC has produced the *Regulatory Challenges of Internet of Things (IoT) White Paper* based on reports by international bodies and agencies, including the following:

i. International Telecommunication Union (ITU), Global Symposium for Regulators, June 2015 - GSR discussion paper: Regulation and the Internet of Things;

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; and

iv. The Office of Communications (OfCom) – Promoting investment and innovation in the Internet of Things.

Through this white paper, MCMC was able to further grasp the technical regulatory requirements and challenges in order to facilitate IoT roll-out in Malaysia. The five main technical regulatory challenges identified were:

i. Spectrum requirement;

ii. Network numbering and addressing;

iii. Technical standardisation;

iv. Roaming or mobility requirement; and

v. Security and data privacy.

In addition to these, talent development and PoC were also noted as the key challenges for the IoT implementation in Malaysia.

The MCMC IoT Task Force (Task Force) was formed comprising both internal and industry experts to further study and investigate each and every aspect of the IoT roll-out, and to ensure that MCMC is ready to facilitate IoT deployment in Malaysia smoothly. To understand the benefits, values, context and even the technologies of IoT, use cases and examples across various applications and industries were analysed. The Task Force enabled MCMC to highlight and further understand aspects which may be overlooked.

The Task Force, led by the Chief Officer of Communications and Digital Ecosystem Sector, comprised of seven (7) MCMC divisions as well as external experts. The Task Force members are:

i. Technology and Society Division (TSD);

ii. Licensing and Assignment Division (LAD);

iii. Digital Services and Data Platform Division (DSDPD);

iv. Spectrum Planning Division (SPD);

v. Digital Surveillance Division (DSD);

vi. Market Regulation Division (MRD);

vii. MCMC Academy;

viii. Malaysian Technical Standards Forum Bhd (MTSFB); and

ix. IoT Working Group of MTSFB.

It is in MCMC's best interest to ensure that this Report is referred to by IoT stakeholders prior to their IoT applications and/or services deployment.

Spectrum Requirement

Background

MCMC as the key regulator requires that the use of spectrum in Malaysia must be regulated and enforced in accordance with the CMA and its Regulations. Pursuant to section 172 of the CMA, MCMC developed and published the Spectrum Plan, which contains information on radio frequency allocation for various wireless services in Malaysia.

The Spectrum Plan sets out the allocation of frequency bands to various services based on Article 5 of the International Telecommunication Union (ITU) Radio Regulations. It must be referred to in planning and implementation of wireless communication services in Malaysia. Pursuant to section 169 of the CMA, MCMC has also developed and published the Class Assignment (CA) document which provides details on the use of unlicensed or license-exempted spectrum in Malaysia. The CA document is consistent with the Spectrum Plan.

Challenges

The coexistence of both licensed and unlicensed spectrum usage are equally essential to meet the expected demand for wireless connection between IoT networks since both categories serve different purposes. Hence, the selection of the right spectrum usage is crucial in delivering IoT applications and services.

The IoT stakeholders prefer the usage of spectrum to be technology neutral and to have allocation for specific blocks to focus on sub-1 GHz due to its wide area coverage and in-depth building penetration characteristics.

On the other hand, IoT using Low Power Wide Area (LPWA) i.e. LoRa, SigFox and others operating at unlicensed spectrum, may face roaming issue moving forward.

Requirement
Different IoT applications and services require different methods of spectrum usage. A licensed spectrum is required for the IoT applications and services that need to have a guaranteed quality of service (QoS) and more secured connection. For local area network and low security requirements, unlicensed spectrum may be more suitable.

Class Assignment
In December 2015, MCMC allocated 4 MHz of spectrum in the frequency band 919-923 MHz for the use of Short Range Device (SRD) as addition to bands 433-435 MHz, 2.4 GHz and 5.8 GHz that can be used for IoT applications.

To support the growth of IoT in Malaysia, in September 2017, MCMC expanded a total of 4 MHz of spectrum in the frequency band 916-919 MHz and 923-924 MHz under SRD as stipulated in the CA No.1 of 2017. The use of the frequency 916-924 MHz is aligned with most countries in the Asia-Pacific region and some European countries. Furthermore, it is also a part of the frequency bands allocated in the Americas.

The 2nd Schedule of CA No.1 of 2017 specifies the use of these frequency bands which are governed by maximum transmit power and other operating conditions including duty cycle limits. The following frequency bands listed below are made available to SRD including the IoT:

Frequency Bands	Operating Conditions
433 - 435 MHz	100 mW EIRP
916 - 919 MHz	25 mW EIRP with duty cycle of <1%, Frequency Hopping or LBT
919 - 923 MHz	500 mW EIRP
923 - 924 MHz	500 mW EIRP with duty cycle of <1%, Frequency Hopping or LBT
2.4 GHz	500 mW EIRP
5.8 GHz	1 W EIRP

More information on class assignment can be obtained at https://www.skmm.gov.my/skmmgovmy/media/General/pdf/Class-Assignment-No-1-of-2017-15112017.pdf

Way Forward
One of the agenda items for the World Radiocommunication Conference in 2019 (WRC-19), is to carry out study on the technical and operational aspects of radio networks and systems as well as spectrum needed, including possible harmonised use of spectrum to support the implementation of narrowband and broadband machine-type communication (MTC) infrastructures in order to develop ITU Recommendations, Reports and/or Handbooks, whereby MTC is another term used for IoT. MCMC will continue to monitor the progress of this agenda at regional level such as Asia Pacific Telecommunity (APT) and at international levels such as ITU-R Study Group and Working Party.

On the same note, the 3rd Generation Partnership Project (3GPP) has incorporated the IoT technical specifications in its portfolio to include new International Mobile Telecommunications (IMT) based technologies such as Narrowband IoT (NB-IoT) and Long Term Evolution enhanced MTC (LTE-eMTC) also known as LTE Cat-M1. Aside from that, 3GPP also supports the use of Extended Coverage – GSM – Internet of Things (EC-GSM-IoT) for the IoT applications and services using current GSM technology which also support IoT roaming services. These IoT infrastructures utilized the licensed spectrum bands shared with mobile networks which are allocated to the Mobile Network Operators (MNO). This development could be an alternative for IoT stakeholders in delivering the IoT applications and services with the engagement of MNOs.

Network Numbering and Addressing

Background
The provision of section 179 of CMA provided that MCMC is vested with the control, planning, administration, management and assignment of the numbering and electronic addressing of network and applications services. The Numbering and Electronic Addressing Plan (NEAP) serves as a legal instrument under section 180 of CMA, for MCMC to administer the numbering and electronic addressing.

Challenges
The growth of global IoT devices to support the IoT applications and services are expected to increase tremendously by year 2020. The general concern expressed by many is the adequacy of numbering resources to meet the demand for numbers by a high number of IoT devices in the near future.

Currently, there are no ranges of numbers exclusively allocated for the IoT in Malaysia. However, there are ranges of numbers that have been allocated or, identified from the existing mobile number ranges for machine-to-machine (M2M) communications.

Requirement
Numbering and electronic addresses have long been recognised as the key facilitators in the communications services. Hence, IoT stakeholders are required to comply with NEAP for IoT implementation in Malaysia.

E.164 and E.212
MCMC has adopted ITU-T Recommendation E.164 for its public telecommunications network numbering. The E.164 numbering refers specifically to the unique identifiers for all communications within the purview of the CMA other than Internet Protocol (IP) addresses, Autonomous System Numbers (ASN) and domain names.

Based on the above, MCMC has allocated 015 prefix numbers which are categorised under ranges of mobile numbers for M2M. To date, there are sufficient amount of prefix 015 numbers in reserve which also can be used for IoT.

International Mobile Subscriber Identity (IMSI), which conforms to the ITU-T Recommendation E.212 numbering standard for cellular networks, is deemed sufficient to support IoT in Malaysia.

For this purpose, any Network Service Provider Individual licensee under the CMA requiring the use of a number may apply to MCMC for an assignment. Submission of application can be made via MCMC Numbering Management System (NUMSYS) at https://numsys.skmm.gov.my/numsys/module/online/.

IPv6
IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4). Many features have been built into the basic IPv6 specifications that are very useful for both the operations and the deployment of IoT. Among the features are larger address space, simplified header, mobility, auto-configuration, authentication, and privacy capabilities.

In 2015, MCMC has mandated that all Network Service Providers (NSPs) are to be IPv6 enabled to ensure adoption of IPv6 in Malaysia via Commission Direction No.2 of 2015.

Provision of IPv6 are currently obtained from Asia-Pacific Network Information Centre (APNIC). APNIC assigns IPv6 blocks based on an open policy as outlined at https://www.apnic.net. These open policies have been developed and are reviewed in conjunction with the users and other interested parties from time to time under the Internet Corporation for Assigned Names and Numbers (ICANN) Request for Comments (RFC) Procedure.

Way Forward
MCMC will continue to allocate numbers for the IoT applications and services from the existing mobile number ranges (the 015 prefix numbers, which are designated for M2M). MCMC will follow ITU's direction in this area, look at global developments and practices, and work with industry to take the necessary measures to plan and address these concerns effectively. The focus here will be to study and develop a strategy to meet the demand for numbering resources, and to consider the introduction of new number ranges and longer numbers digits for IoT.

MCMC will continue its participation in ITU-T Study Group 2: Operational aspects of service provision and telecommunications management and ITU-T Study Group 20: Internet of Things, smart cities and communities to keep abreast with the international standards development with regards to network numbering and addressing for IoT.

Technical Standardisation

Background
The Communications and Multimedia (Technical Standards) Regulations 2000 or "TSR2000" requires communications equipment, both network facilities and customer equipment, to be certified to ensure they comply with the applicable technical standards[4]. The certification is to ensure communications equipment are safe, interoperable, not causing any frequency interference and provide protection for consumers. This requirement also covers IoT devices since they transmit data over a communications network or communicate wirelessly.

Challenges
The certification of communications equipment shall be carried out by a certifying agency registered under TSR2000[5]. A certified communications equipment shall also bear a certification mark or label to indicate that it complies with technical standards. Under the Customs (Prohibition of Imports) Order, communications equipment may only be brought into the country if they are accompanied with an import permit which may only be issued for certified communications equipment.

Most of the IoT stakeholders are new start-up companies, small medium enterprises, R&D organisations, universities, and Makers community, which are lacking awareness of the above technical regulatory requirements.

4 As defined in technical codes.

5 As of March 2018, SIRIM QAS International Sdn Bhd is the only registered certifying agency for certification of communications equipment.

Requirement

1. Technical Codes

Manufacturers, importers and suppliers who place IoT devices in Malaysian market will have to establish compliance with the published technical codes by getting the devices certified according to TSR2000. The following table explains on the technical requirements covered by the technical codes.

Safety	Interoperability	Radio Frequency
Electrical safety Specific Absorption Rate (SAR)	Performance characteristics	Frequency band Maximum power limit Electromagnetic Compatibility (EMC)

More information on the technical codes can be obtained at https://www.mcmc.gov.my/legal/registers/cma-registers.

2. Testing

IoT devices shall be tested by local or foreign testing laboratories, which are accredited according to ISO/IEC 17025 by an accreditation body under ILAC[6] or APLAC[7]. The test reports issued by these laboratories are to be submitted to a registered certifying agency for evaluation and certification process.

3. Certification

The following table explains on the types of equipment or device certification carried out by a registered certifying agency.

Type of Certification	Description
Compliance Approval/Type Approval	Granted to a specific model of communications product/module/card complying with the technical codes.
Special Approval	Granted to a specific model of communications product/module/card which is exclusively used by the applicant for the following purposes: • For individual or company's own use • For research and development • For trial, market survey, demonstration or exhibition • For training Equipment or device certified under Special Approval shall be subject to defined parameters such as duration, location, specifications and other conditions. The devices shall not be for sale to the public.

In the case of SIRIM QAS International Sdn Bhd, submission of the application for Compliance Approval or Special Approval may be made via e-ComM portal at https://ecomm.sirim.my/. More information on the certification of communications equipment may be obtained at http://www.sirim-qas.com.my/. The applicant is also required to submit a sample of device for verification.

A Certificate of Compliance (CoC) will be issued to the applicant for each model of equipment or devices that is certified. The certificate is valid up to the maximum of five years.

6 International Laboratory Accreditation Cooperation.

7 Asia Pacific Laboratory Accreditation Cooperation.

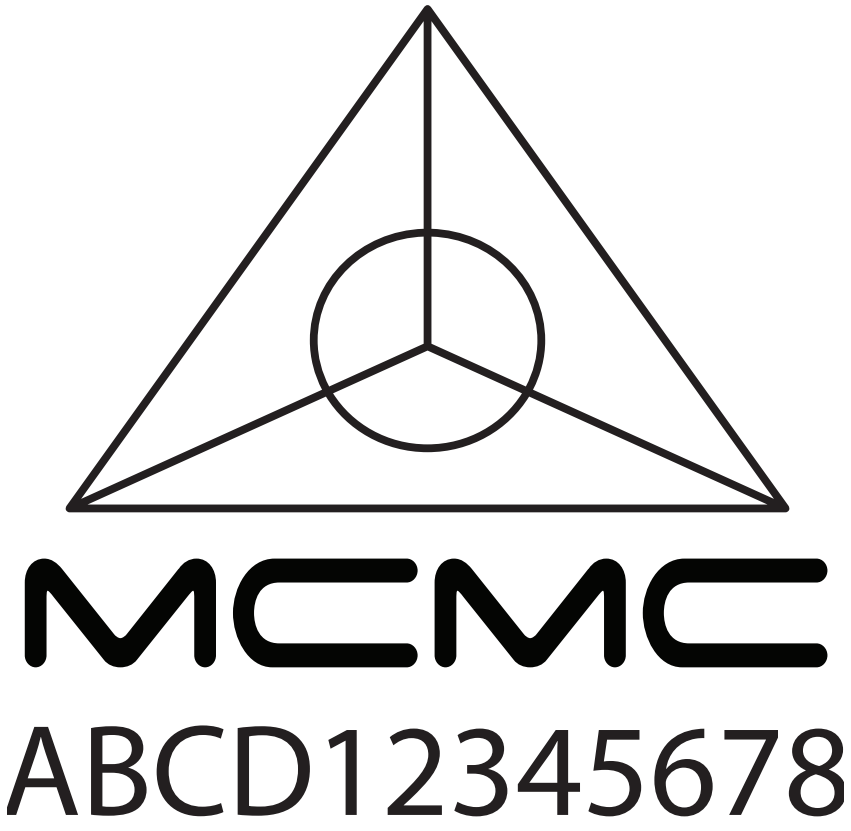
4. Labelling

All certified equipment or devices shall bear a certification mark (MCMC label) to indicate that they are in compliance with the technical standards.

The MCMC label can be in the form of physical label (sticker, embossed, engraved or printed) or electronic label stored in a device firmware.

Certificate holders are required to register and obtain a supplier identification number from a registered certifying agency before they can produce and use the MCMC label.

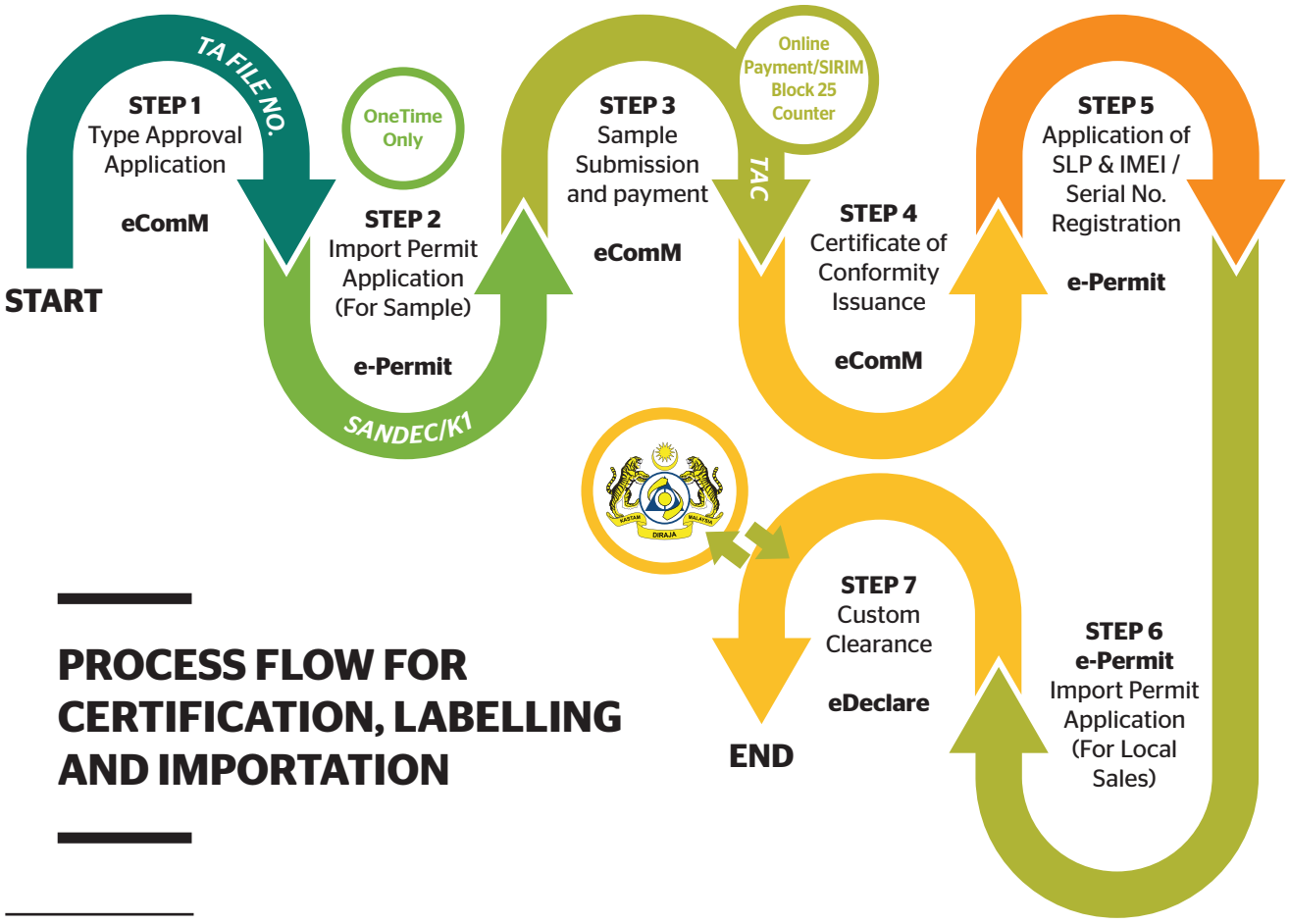
MCMC CERTIFICATION MARK



5. Importation

The importation of IoT devices shall be accompanied with an import permit issued by a Cross Border Regulatory Agency[8] (CBRA) appointed by the Royal Malaysian Customs Department (RMCD). The import permit may only be issued after the devices are verified as in compliance with the technical codes and certified under TSR2000. Importers are also required to register the IMEI or serial number of IoT devices prior to the issuance of the import permit.

The process flow for SIRIM QAS International Sdn Bhd for the certification, labelling and importation of IoT devices is described in the figure below.



PROCESS FLOW FOR CERTIFICATION, LABELLING AND IMPORTATION

Way Forward

Moving forward, MCMC is to undertake an engagement programme with the IoT stakeholders by targeting new start-up companies, small medium enterprise, R&D organisations, universities, and Makers community, to create the awareness and educate them on the certification, labelling and importation requirements to facilitate adoption of IoT in Malaysia.

8 As of March 2018, SIRIM QAS International Sdn Bhd is the only CBRA for communications equipment appointed by RMCD.

Roaming or Mobility Requirement

Background

Part VI of the CMA establishes the regulatory framework for economic regulation of the communications and multimedia industry. In addition, Part VIII of the CMA contains provisions on consumer protection, particularly Chapter 4 on rate regulation in which subsection 198 of the CMA establishes the principles of rate setting.

In performing its statutory functions under the CMA, MCMC is guided by the National Policy Objectives (NPOs) set out in subsection 3(2) of the CMA. The objectives that are particularly linked to Part VI include the following:

i. To regulate for the long term benefits of the end user;

ii. To promote high level of consumer confidence in service delivery from the industry; and

iii. To facilitate the efficient allocation of resources such as skilled labour, capital, knowledge and national assets.

Roaming service enables users to continue using their existing mobile services while travelling abroad. This is made possible through technical coordination and commercial negotiations between roaming partners of the participating countries. Mobile roaming initially began with the traditional services namely voice, Short Messaging Service (SMS) and data.

Challenges

From the technical perspective, there would be no major issue to the IoT roaming on licensed spectrum since it can leverage on the existing roaming system. However, the challenges are on the IoT devices, applications, and services which are based on Low Power Wide Area (LPWA) technologies using unlicensed spectrum such as LoRa and SigFox. The existing roaming system will need to be enhanced to support LPWA.

The MNOs utmost challenge in implementing IoT roaming lays in deciding on the appropriate pricing for the service. Although roaming partners adhere to Groupe Speciale Mobile Association (GSMA) standards, the MNOs in Malaysia currently do not make distinction between traditional roaming traffic and IoT roaming traffic.

This is however not a new phenomenon and is consistent with issues faced by MNOs worldwide. For example, a study published by Rocco[9] on *Roaming Internet of Things Strategy Report 2017*, MNOs find it challenging to determine their Inbound and Outbound traffic scenarios as well as working with their roaming partner to provide transparency on the IoT roaming traffic requests in their network.

Rocco also reported that the issue with inbound IoT roaming is the amount of traffic permanently roaming on the mobile network. This is a cause for concern as the mobile network will have to support for the duration of life span of the device which is estimated to last between 5 to 15 years.

Requirement

1. Inter-operator charging models

Currently, the inter-operator rates are commercially negotiated and can be in various forms such as subscription based or pay per use, with bulk discount where applicable. Furthermore, bundling of equipment, solutions and provisions may also be factored in.

9 Rocco has been around since 2012. Its main office is in the UK while the branch offices are in Spain and Italy. Rocco's primary focus is in conducting research, training and consultation. The reports produced are mainly on roaming and interconnect.

In order to have full transparency of the IoT roaming traffic with the roaming partners, independent roaming agreements need to be established which clearly provide Transferred Account Data Interchange Group (TADIG) codes for the particular traffic to ensure that the roaming partners will be able to bill correctly.

2. Projected revenue growth

Rocco in its 2017 strategic analysis report on the IoT, estimates that approximately 70% of traditional roamers globally are switching off roaming services, as reflected in the decline in traditional roaming revenue.

Nevertheless, the IoT provides opportunities for the business players, particularly MNOs for new stream of revenue growth. As MNOs unlock this new business opportunity, careful planning of the network is required to support these applications that are constantly using the network. MNOs will need to quantify the return before embarking on this new infrastructure, considering new processes and resources that they need to expand on.

Way Forward

Despite the many challenges, telcos in Malaysia have begun providing connectivity for IoT services via their data packages. For example, Maxis has partnered with Modus and introduced MDrive, a vehicle tracking device; Digi launched their iFleet services for B2B fleet tracking solution services; U Mobile and Axiata are working with Atilze to provide connectivity to facilitate its integrated car solution while edotco has provided 25 sites to allow Atilze's LoRa gateways to be installed on edotco's telecommunication towers.

Current roaming arrangements are negotiated commercially. This is because the industry believes that market forces can deliver optimal solutions. Regulatory intervention should only occur when there is market failure. The industry prefers bilateral commercial negotiation for roaming arrangements as it allows for better bargaining powers for both parties and encourages product innovation.

It is evident that the service providers are still grappling with a lot of issues related to IoT roaming as they do not have the relevant information. Given the circumstances, it is prudent to abstain from regulatory intervention. MCMC will step in if there is market failure.

Further study and analysis on IoT roaming services are crucial to resolve the challenges faced with regards to managing and controlling IoT roaming traffic. Understanding the underlying cost and distinction between traditional and IoT roaming traffic is also necessary to support IoT roaming services. One of the approach to achieve this is by leveraging on the network slicing capability that will be able to support numerous and varied services envisioned in 5G.

The ITU-T Study Group 3, which looks into tariff and accounting principles and international telecommunications/ICT economic and policy issues, has identified Guidelines on Tariff and regulatory aspects of IoT and Roaming for IoT as work items for study period 2017-2020. This is mainly because high roaming tariffs may act as barriers to innovation and hamper the growth of digital economy. The focus of the study with regards to IoT is to identify international roaming issues and principles for lowering international roaming rates to enable access, availability and affordability for users worldwide.

More information on IoT roaming can be obtained at https://www.key4biz.it/wp-content/uploads/2017/03/ROCCO-Roaming-Internet-of-Things-Report-2017-Strategic-Analysis.pdf and https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.14-v1.0.pdf

Please refer to the following websites for additional information on some of the IoT initiatives and implementation in Malaysia:

- https://www.maxis.com.my/mdrive
- https://www.axiata.com/mroom/news-article/140/
- https://themalaysianreserve.com/2017/06/09/digi-makes-foray-into-iot-space/
- https://www.nst.com.my/business/2017/06/246953/digi-launches-ifleet-b2b-vehicle-fleet-tracking-solution
- https://www.digitalnewsasia.com/business/atilze-u-mobile-collaborate-offer-connected-car-solutions
- https://www.digitalnewsasia.com/digital-economy/edotco-atilze-roll-out-first-lora-network-malaysia

Security and Data Privacy

Background

Section 3 (1) (a) of the CMA provides that the objective of the CMA is to promote NPOs for the communications and multimedia industry which also includes to ensure information security and network reliability and integrity, among others. The IoT provides significant benefits to end users in various verticals of daily lives. Without appropriate controls, the ability to collect, analyse and transform data could be detrimental in terms of security and data privacy.

As smart devices proliferate the IoT, so do the risks of cyber-attacks via this new type of connectivity. Distracted by the new features and capabilities of IoT, requirements for security and data privacy aspects have been overlooked. It is not surprising that the number of complaints related to IoT has escalated in many parts of the world over the last three years.

Challenges

Trust is an attribute which provides assurance that end users' personal identifiable information is sufficiently protected and only used for agreed purposes. Hence, it is imperative for a successful adoption of the IoT in Malaysia. The IoT amplifies concerns about potential increase of tracking in view of the amount of sensitive data that can be collected by devices operating in users' homes, businesses and public environments. Sometimes these devices collect data on individuals without their knowledge or informed consent. Challenges arise if the data collected is deemed as personal or sensitive and is subject to data protection laws in multiple jurisdictions.

The IoT has changed the nature of communications in the sense that M2M communication requires no human interaction in a communications chain, thus it challenges the effectiveness of the existing regulatory structure. This is a new challenge on the management of notice and consent for

communications that do not involve individuals in the information exchange. Traditionally, regulation has always relied on an individual or entity to hold the responsibility for any particular outcome or behaviour.

While the privacy challenges are considerable, they are not insurmountable. Strategies could be developed to promote transparency, to widen user choice in data collection and handling, and to enhance security, user privacy and expectations to foster innovation in technology and services.

Requirement

1. Data Privacy Protection

The key regulator in data privacy in Malaysia is the Personal Data Protection Department (PDPD). However, other regulators may have roles to play, particularly when it comes to direct consumer education and interaction under their respective remit. Whilst regulators cannot control every system deployed, they can work with established industry players and new entrants, as well as government, to drive good practice.

The IoT will only flourish if important aspect of network security and privacy issues are properly addressed. Thus, privacy protection and legal certainty in relation to data collection and flow are necessary to promote end users' trust and confidence in the various IoT stacks including devices, data processing and exchange layer, systems and smart services provided by device manufacturers and IoT service providers. Solving privacy, reliability and interoperability concerns may elevate the importance of standards-setting and design controls, not only for devices, but also for data exchanged between machines.

2. Technical Codes Development

The development of technical codes in network security is to help the industry including IoT stakeholders to implement the security measures in line with the regulatory needs. The development of the technical codes is by referring to the relevant international standard development organisation, such as International Organization for Standardization (ISO), ISO/IEC[10] and ITU.

3. Annual CMI Sector Cyberdrill Exercise

MCMC, in line with the NPOs in ensuring a reliable and secured network, has established a proactive platform known as the MCMC Network Security Centre (MCMC NSC). The MCMC NSC in dealing with the emerging cyber threats such as Botnet, Virus, Malware and complex Phishing attacks, collaborates with various renowned international organisations to ensure that the undertaken efforts are effective in addressing the cyber threats.

MCMC NSC conducts cyber drill exercise on a yearly basis since 2014 with the Internet Access Service Providers (IASP) in Malaysia. The cyber drill exercise is a simulated and coordinated process where mock threats are handled by the IASP Computer and Emergency Response Team (CERT) with MCMC NSC as the coordination entity. The main objective of the exercise is to assess the cyber security emergency readiness and incident response capabilities of Malaysian IASP in mitigating cyber threats.

10 A joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission (IEC).

4. ISMS & BCMS Implementation

The high dependency of today's business operation on ICT has increased the cyber threat with unpredictable risks and impact to the organisation's operation, security, financial and reputation.

The implementation of relevant information and network security standards such as Information Security Management System (ISMS) and Business Continuity Management System (BCMS) (or any similar initiatives) is crucial to the Critical National Information Infrastructure (CNII) organisations to ensure that the security incidents can be managed holistically and systematically as well as to guarantee the continuity of business even when disaster occurs.

The implementation are in accordance with Directive No. 24: National Cyber Crisis Management Policy and Mechanism by National Security Council (MKN). The Directive clearly outlines that each Sector Lead is responsible in ensuring that each of CNII organisations implement the ISMS and BCMS to reduce the risk and impact of security incidents and that the continuity of business and services are safeguarded.

Furthermore, in the year 2010, the Cabinet Meeting has decided that CNII organisations in Malaysia must be certified with ISO/IEC 27001 ISMS and the implementation needs to be coordinated and monitored by relevant ministries and agencies that are responsible over the specific CNII.

Way Forward

A collaborative governance approach, one that draws on the expertise and engagement of a wide range of stakeholders, is necessary to develop effective and appropriate solutions to the challenges. The MCMC could take on a coordinating role by working with industry, Government and other regulatory authorities in order to facilitate the development of a common framework for the IoT.

In particular, MCMC sees the merit in working with PDPD and a range of stakeholders on the issue of privacy as a better way to have an in-depth understanding on matters relating

to information security and design regulatory or non-regulatory initiatives, which includes developing best practices and guidelines in these areas.

It is important to address aspect of network security and privacy issues for the successful deployment of IoT. Thus, it is necessary to promote end users' trust and confidence in the various IoT stacks including devices, data processing and exchange layer, systems and smart services provided by device's manufacturers and IoT service providers. Existing privacy guidelines imposed on operators can also be applied to IoT applications and services.

Since IoT is a rapidly developing environment, it is a new challenge that requests the regulators to collaborate with both established and new stakeholders of the industry, as well as the Government, to find effective and appropriate solutions. The MCMC is taking on a coordinating role, working with industry, Government and other regulatory authorities to facilitate the development of a common framework for IoT.

As the sector lead for the communication sector, it is important that MCMC prepares the communication sector to be capable and well-equipped to handle cyber security incidents. Based on the drill outcome, improvement can be made to:

- The standard operating procedures between MCMC NSC and the IASP on the incident escalation and response;
- The efficiency of communication channels during normal operations and emergency operations; and
- Update point of contacts of each IASP and MCMC.

The drill scenario can be enhanced to focus on IoT security.

Capacity Building

Background
The fundamental of capacity building is about improving an individual or organisation's performance and enhances the sustainability to stay relevant within a rapidly changing environment. Similarly, capacity building in IoT will result in the adoption of new skills and knowledge of IoT ecosystem which will be beneficial to the IoT stakeholders. For these purposes, MCMC through its Academy has introduced a Master Class programme that offers a holistic and up-to-date worldview of all matters related to the converged telecommunications space including IoT.

CTPR Master Class for ASEAN Countries
The Converged Telecommunications Policy and Regulations (CTPR) Master Class is designed for mid to senior level executives in national regulatory agencies, relevant government ministries, telecommunication service providers, broadcasters, manufacturers or vendors in the ASEAN countries and Asia Pacific Region.

The CTPR Master Class for ASEAN countries is a collaboration programme between Multimedia University (MMU), GSMA and MCMC, together with the host ASEAN countries. This intensive programme brings together an international, collaborative network of academicians, regulators and industry experts to highlight current global approaches to CTPR issues.

CTPR Professional Master Class on Smart Digital Nation, Cities and Communities
As smart cities being few of IoT applications and services, the CTPR Professional Master Class in Smart Digital Nation, Cities and Communities (SDNCC) is designed to help stakeholders address challenges related to smart city ecosystems, as well as the business models of IoT solutions and governance of smart cities.

Advocacy and Awareness

Background
Community initiatives are being introduced to reach out to every level of the community including but not limited to rural and sub-urban population, students and SME entrepreneurs. Through MCMC Digital Lifestyle Malaysia (DLM) platform, various outreach programmes and pilot projects are being conducted to ensure that the communities are ready to embrace the benefits of the IoT.

myMaker Initiative
myMaker is an initiative by MCMC to raise public awareness on Science, Technology, Engineering and Mathematics (STEM), incorporating IoT development for technology enthusiasts, educators, tinkerers and students.

myMaker, through myMaker IoT Lab and myMaker.io, enables the Makers society to be creative and innovative towards a smart digital nation in the areas of 3D printing, drone, embedded system, electronic, virtual reality, IoT programming and many other areas. The initiative will drive regional and national harmonisation through building myMaker community by organising events and programmes related to STEM and IoT.

Digital Lifestyle Malaysia – Experiential Learning Space
The MCMC Digital Lifestyle Malaysia – Experiential Learning Space (DLM-ELS) is the centre that provides informative and interactive displays on communications and multimedia. It explains how communications and multimedia is driving innovations to transform, improve and create new digital services and how it impacts many aspects of governance, business and living as the nation marches towards a developed digital economy and a Smart Digital Nation, Cities and Communities Malaysia.

Visitors to the DLM-ELS are exposed to many points of interest namely, distributed on items in the learning spaces which they can explore, interact and experience using smartphone camera by either scanning (Quick Response code) or touching it (Near-Field Communication tag) to know more about it or experience some of the smart digital lifestyle applications featured on the day.

Digital Lifestyle Malaysia – Pilot Projects
MCMC in collaboration with strategic organisations focuses on five key verticals namely Track and Trace, Healthcare, Transportation, Retail and Payment, and Agriculture.

1. Track and Trace

The development of Edible Bird's Nest (EBN) Traceability System answers to PEMANDU[11] Entry Point Project (EPP) Track and Trace for Malaysian Economic Transformation Programme (ETP). The Government of Malaysia represented by Department of Veterinary Services (DVS) has entered into MOU with MCMC, to establish and develop traceability systems for EBN Industry in 2011. The system was successfully handed over to DVS in December 2016, towards the end of the 5 years' MOU tenure.

11 Performance Management And Delivery Unit (PEMANDU) was formally established on the 16th of September, 2009 and is a unit under the Prime Minister's Department. PEMANDU's main role and objective is to oversee the implementation, assess and facilitate the progress, as well as support the delivery and drive the progress of the Government Transformation Programme (GTP) and the Economic Transformation Programme (ETP).

2. Healthcare

The development of RAPITA Active RFID Asset Management System (RAMS), which is a solution that provides Real Time Asset Tracking aimed to overcome asset tracking and monitor challenges faced by hospitals. RAMS enables hospital personnel to locate the hospital assets immediately by a single click which subsequently resulting in increased productivity and efficiency. This project is in collaboration with Sunway Medical Centre.

3. Transportation

The development of LocAware IoT Solution – a system to track school bus and students using a combination of IoT gateway, Global Positioning System (GPS), cellular communication and mobile application to notify parents when their children arrived at their schools by tracking the time stamp of their children entering/leaving the bus and entering the school. This project is in collaboration with Brainy Bunch International Islamic Montessori and UNITEN Smart UniverCity Program.

4. Retail & Payment

The development of Bluetooth Low Energy (BLE) Proximity Marketing - an IoT solution with Bluetooth 4.0 Beacon, which allows personalisation of marketing information to be sent to the user smart devices. The mobile app, which will be developed on Android and iOS Platform, allows integration with online payment gateway for the user to purchase the offered products immediately online. This project is in collaboration with Segaris Art Center, an art gallery owned by UiTM Art and Design Sdn Bhd.

5. Agriculture

The development of Greenify, an IoT solution utilising sensors and data analytics for precision agriculture and urban farming. The smart concept of modern gardening is equipped with smart watering and lighting system whereby plants' ambient status such as water pH level, water level, temperature, lighting and electro-conductivity are analysed in near real time for precision agriculture. The indoor and outdoor units of Greenify are displayed at MCMC DLM-ELS.

Conclusion

The IoT is accelerating a transition towards increasingly complex connections enabled initially by the digitalisation of networks and content. MCMC is aware of the building blocks to support increasing connectivity and has begun putting in place enabling infrastructure for network digitalisation, ensuring adequate spectrum availability as well as anticipating demand for numbering and electronic addressing.

MCMC is also aware that besides collaborative governance, there are enabling or facilitative regulatory approaches that could be adopted to foster IoT development and support innovation. These approaches also respond to potential risks posed by emerging issues which is provided for within the regulatory framework under the CMA. The framework includes the following toolkits:

1. Impose industry self-regulation or co-regulation created by the industry through the forums established under the CMA. Under this arrangement, the industry participants work in tandem with MCMC to provide mechanisms in addressing concerns of a fast converging industry landscape;

2. Exercise regulatory forbearance as a short term measure while regulatory measures are being developed. This would be applicable for temporary issues occurring in fast changing market environment. Considerations for the application of regulatory forbearance may be based on proportionality, fairness and the cost and benefits of such action;

3. Deploy targeted communication strategies in order to raise awareness. Such action includes educational campaigns to inform the public about the benefits as well as emerging issues of concern relating to IoT and create feedback mechanism for the public to provide response or suggestions on how to address some of the concerns; and

4. Conduct inquiries or consultation with industry and stakeholders to obtain feedback on methods to tackle emerging issues concerning IoT.

The above regulatory tools embedded within the CMA regulatory framework enables MCMC to take an agile approach in fostering innovation and facilitate industry development whilst simultaneously navigating emerging issues in IoT implementation.

Through this Report, MCMC acknowledges the technical regulatory challenges faced by the IoT players and recognises the needs to assess the current regulatory framework, in assuring that the framework is suitable for way forward and is future proof.

In addressing the lack of awareness among new IoT stakeholders, MCMC will implement action plans by collaborating with industry, studying worldwide trends and approaches, and by looking at the direction provided by ITU.

As for existing on-going implementation, MCMC will continue to be in the loop on the development of LPWA technologies especially on matters concerning roaming issues, and will retain its efforts in developing myMaker and PoCs.

Use Cases

LoRa Platform, Application & Services

Prepared by: Atilze Digital Sdn Bhd & Cyberview Sdn Bhd

Challenges

Security

1. Presently, Atilze has deployed a city-wide IoT platform that serves as the centralised IoT data aggregator, processor and distributor of data (Northbound and Southbound) to enterprise customers and start-up ecosystem in Cyberjaya via Cyberview Sdn Bhd's Integrated Command-Centre Platform project.

2. There is a pervasive fear that such enterprise bus system may intrude and publish unauthorised data to 3rd party vendors for financial gains. However, this is untrue because according to the LoRaWAN specification, data is encrypted with device-specific keys from the device to the application (and vice versa). Such is true if the network server used is providing full multi-tenancy support. The network operator does not get access to any decrypted/plain application data or application (session) keys. In such a setting, the network operator is in no position of selling or providing plain application data to a third party to start with.

Capacity Building

1. Atilze plays a pivotal role to deliver training programmes for Smart Cities and Smart Urban Farming Solutions. The training aims to equip participants with information from various industries, integrating industry knowledge and technical modules and providing opportunities for participants to embark into IoT projects of their own.

2. Atilze will participate in local and international IoT industry programmes. Atilze have been invited to many IoT awareness programmes such as MCMC's annual Digital Lifestyle Malaysia (DLM) event, Asia IoT Business Platform, Smart Cities Event by the Selangor Government, Regional IoT World Asia, TM Forum, Digital Big Bang organized by DEPA Thailand and local Malaysian events for Smart Cities and Smart Agriculture via 10ESD MCA for Smart Agribusiness for young entrepreneurs.

Atilze was named Top 25 IoT service provider in Asia Pacific by CIO Outlook in July 2017 and also awarded for IoT Best Deployment in Asia by IoT World Asia in Marina Bay Sands, Singapore in October 2017.

FAVORIOT – Quest towards 100k IoT Professionals

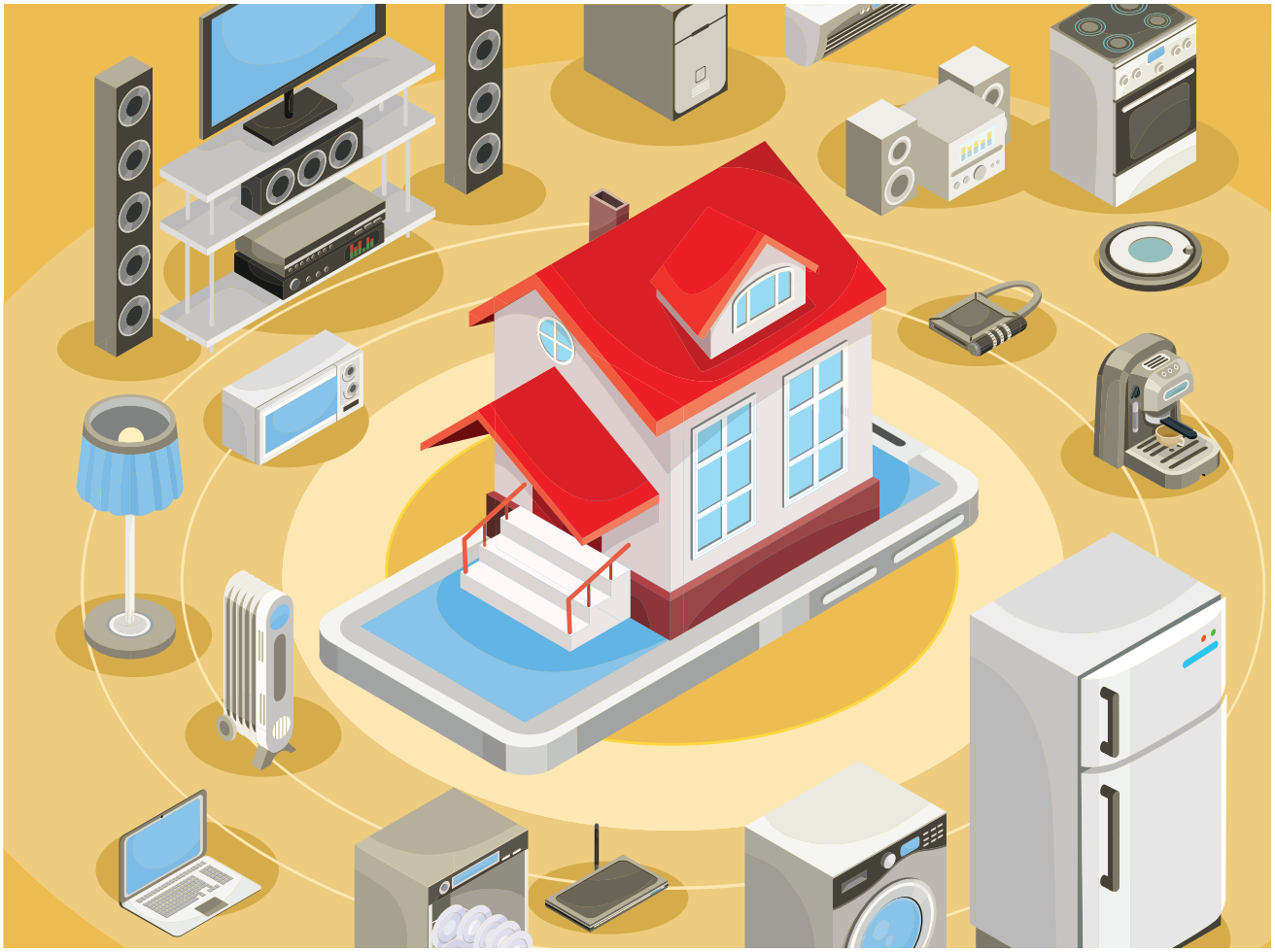
Prepared by: Favoriot Sdn Bhd

Introduction
Generation-IoT That Will Disrupt the World

The 3rd Internet Tsunami is Coming
Whether we like it or not, we will be hit by the 3rd Internet Tsunami i.e. Internet of Things. Many of us have seen the 1st Internet Tsunami of fixed Internet and the 2nd Internet Tsunami of Mobile Internet. What many of us do not realise that as Things get connected, the connectivity will bring massive transformation into our lives and the way we work.

Businesses will get disrupted and probably face extinction if we are not prepared to adopt the IoT. Regulators will face big challenges if they are slow in understanding the impact and make changes to their current regulation. They can remain status quo but it will definitely stifle innovation in that country.

Who will drive this 3rd Internet Tsunami?
They are the Generation-IoT. We have heard about Baby Boomers, Gen-X, Gen-Y (also known as Millennials) and the Gen-Z (also known as iGeneration or Post-Millennials) but what is Gen-IoT exactly?



As defined by Maciej Kranz in the article "Generation IoT: The Key to Business Survival in the 21st Century" the following are the traits of Generation-IoT:

- They are pioneers in IoT.
- All are willing to learn and take risks and are good at building virtual teams internally and partnering externally.
- You can recognise these new winners not by their age or their titles—but by their ability to build and deploy agile, flexible business solutions.
- A new generation of leaders, makers, thinkers, and doers is meeting that change with flexibility and optimism and transforming it into opportunity.
- These are the people who see the transformational power of IoT-driven processes, business models, and new revenue streams.
- They are eager to champion and drive these opportunities in their organisations.
- These people know that IoT is not just one project, one training session, one change.
- They know that in order to succeed, they and their organisations need to adjust and re-learn, over and over again.

Provided Solution

Project Description

In the quest to generate 100k IoT Professionals (or so-called the new Generation-IoT) in the country, FAVORIOT, the latest IoT Start-up in Malaysia partnered with 15 Malaysian universities to review, refresh and include not only IoT elements in the curriculum and syllabus but also introduce a more practical method for the university students to be familiar with IoT middleware and how to create their first IoT application and project.

Universities which joined the programme are as follows (the first 10 Universities listed joined the FAVORIOT-University Programme since May 31, 2017):

- Universiti Teknologi Malaysia (UTM)
- Universiti Tun Hussein Onn Malaysia (UTHM)
- Universiti Kuala Lumpur (UniKL)
- Universiti Malaysia Sarawak (UNIMAS)
- Universiti Sultan Zainal Abidin (UniSZA)
- Universiti Tenaga Malaysia (UNITEN)
- Universiti Teknikal Malaysia Melaka (UTeM)
- Universiti Sains Malaysia (USIM)
- Universiti Malaysia Perlis (UniMAP)
- Asia Pacific University (APU)
- Taylor's University
- Universiti Teknologi Petronas (UTP)
- International Islamic University Malaysia (IIUM)
- Universiti Utara Malaysia (UUM)
- Universiti Teknologi Mara (UiTM)

It is expected about 450 graduates every year will be utilising FAVORIOT platform for their Lab experiments, Final Year or Research projects. The programme allows more than 2250 devices to be connected to the platform.

University of Glasgow, Singapore
Thanks to Dr. Keoh Sye Loong from the University of Glasgow Singapore, three IoT projects are now under development using FAVORIOT platform. The projects are:

- Fleet IoT Security Hardening and Audit Automation
- Smart Waste Sensing for Efficient Waste Management
- Design and Development of an Intelligent Aquaponics System with Internet of Things

UTHM
Project: Temp and Humidity Monitoring Using FAVORIOT for Green Building Applications by UTHM

Dr. Ansar from FKEE, UTHM used DHT11, NodeMCU v3 with FAVORIOT platform to collect temperature and humidity data in a project which is at a beginning stage for Green Building application.

Taylor's University
Taylor's University has improved its standing among universities in Asia by 29 places to break into the top 150 positions, as announced by QS Asia University Rankings today. Taylor's is also listed in the top 1 percent of universities in Asia, an outstanding achievement and an important milestone for the University.

Dr. Mohsen Nabipoor *(Programme Director – Electric & Electronic Engineering)* from School of Engineering shared his IoT Projects using FAVORIOT platform.

1. An IoT Tyre Management System.

The device reads truck's identification number as well as individual tyre pressure and tread depth and uploads them to the FAVORIOT cloud. An Android app will read data from the cloud, displays the data and creates proper notifications based on the data.

2. An IoT Breath Sensor.

The device measures human breathing pattern and rate and sends the data to FAVORIOT cloud. The data will be retrieved and processed by the server to diagnose possible respiratory problems.

3. An IoT Air Conditioning System

The device measures few parameters such as the electrical power, refrigerant pressure as well as the pressure drop across the filter and sends them to the FAVORIOT cloud. An app will analyse the data and create proper notifications for maintenance of the unit and filter. It also compares the data with similar units installed elsewhere to provide the comparison results to the user or the manufacturer.

UniSZA
MyDuino.com conducted another IoT Workshop with hands-on using FAVORIOT Platform (Oct. 20-21, 2017). The 2-day workshop is conducted at UniSZA Besut Campus.

FAVORIOT also offered very affordable rates (as low as RM 100 per year) for Beginners who want to use an IoT middleware to connect their sensors. This platform allows users to develop IoT prototype in a very short time.

MyDuino also offers the FAVORIOT IoT workshop at customer's premises.

This is our effort to increase more IoT talents in Malaysia. Our training partners have been aggressively conducting several workshops nationwide. For those who can start doing their hands-on independently, they can check the full documentation at Favoriot's website.

UTM

UTM Skudai – Centre for Communication and Technology (CICT) in cooperation with Advanced Telecommunication Research Group (ATT) of UTM conducted a Workshop on "Internet of Things Hands-on Experience" using FAVORIOT recently.

This is probably the first series of IoT Workshops that will be hosted and trained by the experts from Universiti Teknologi Malaysia. The attendees are from within UTM (Staff and Students) including people from the industry.

The excitement and compelling need for more IoT professionals are growing steadily in Malaysia. UTM will be a good anchor University located south of the Peninsular Malaysia to grow the IoT talents in relation to the needs of the Industry 4.0 and Smart Cities plans in Johor.

Recommendation

If Malaysia's Asean Data Analytics Exchange (ADAX) aims to produce 20,000 data professionals (10% of them data scientists) by 2020, having already produced 1,000 data professionals and 200 data scientists last year, how many IoT professionals must Malaysia produce to achieve the targeted figure?

If we look at the IoT value chain, we must consider the people working in the areas of the chipset, devices, middleware (cloud), system integration and applications and if the calculation is one professional per area, we need 5 people (minimum) to support 1 data professional. That will add up to 100,000 IoT professionals to be trained by 2020. It looks like a realistic figure, but how many of them will be from the University. Let's assume 10 local universities in Malaysia are focusing on training this 100,000, will it be around 10,000 for the next 3 years?

Thus, while we are so hyped up with the number of data professionals, we should not forget the rest of the value chain that is responsible for developing new products, connecting the devices, collecting data and build IoT applications. Without them, we simply cannot turn Malaysia into an IoT hub for the region.

However, universities cannot be the only ones shouldering the responsibilities of producing IoT professionals. We must also train the professionals who are already working and practising ICT.

Security and Integrated Flood Operation Network (SAIFON)

Prepared by: Ingeniworks Sdn Bhd

Introduction

Project Description

Under the Smart Community initiative, Malaysian Communications and Multimedia Commission (MCMC) has developed key programmes to foster challenges in fulfilling the vision of Smart Nation which includes access to information and communication infrastructure. One of the programmes is called Security and Integrated Flood Network (SAIFON). SAIFON is a monitoring system that is equipped with a centralised monitoring centre. SAIFON consists of basic IoT components which are hardware, network and data analytics to bring solution to the communities in creating a better way of life through the use of ICT. This is also in line with one of the objectives of Smart Community. The system is fully developed by Malaysians and currently being used at Kota Belud Smart Community. There are three sensors installed at major rivers in Kota Belud. Twelve closed-circuit televisions (CCTVs) are installed at strategic location in Kota Belud to help local agencies (District Office and Malaysia Civil Defence Force - APM) to monitor, plan and take action effectively in ensuring the safety of the community during emergency. The system is being monitored by centralised monitoring centre located at Kota Belud APM's office.

Objectives

The main objectives of this project are:

1. To monitor and alert water level of the main river in Kota Belud ;
2. To monitor the environment quality in Kota Belud; and
3. To provide awareness platform to Kota Belud community.

Problem Statement

Some areas in Kota Belud are often hit by flash floods caused by heavy rains. The flooding caused traffic jams in which dozens of vehicles were stranded and crowding the streets around town when people rushed to move vehicles to higher ground. It is advisable for the public to exercise precautions and plan their trip to avoid being caught in case of flash flood. Thus, this system is developed to monitor the water level in the river and to prepare the public in case of flood. The public will be well-informed on how to cope with floods and can find alternative routes to avoid the flood. Below is photo taken from Bernama where rain continued throughout the day which caused flash floods in Kota Belud town and its surrounding areas.

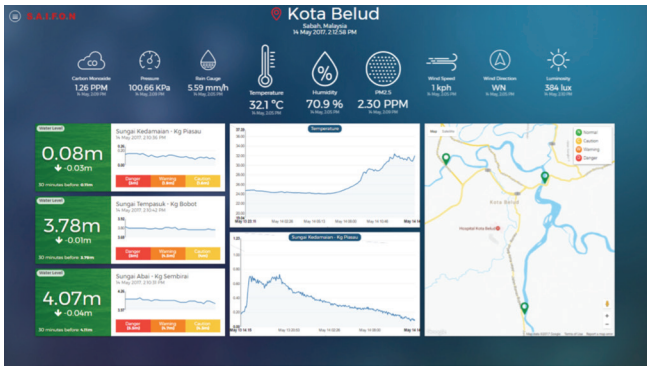
Collaboration
In the project implementation, the collaboration between following parties is necessary:

- Kota Belud District Office
- Malaysia Civil Defence Force (APM)
- Department of Irrigation and Drainage, Sabah (JPS)
- PDRM Sabah – Kota Belud
- Fire and Rescue Station Kota Belud
- Jabatan Kerja Raya (JKR) Kota Belud
- MSD Digital Intelligence

Technology/ solution used
Kota Belud is one of the areas that can benefit from the IoT whereby everything can be connected. The IoT is the network of physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. There are many established communication technologies used such as WiFi, Bluetooth, ZigBee and 3G/4G cellular. Depending on the application, factors such as range, data requirements, security and power demands and battery life will dictate the choice of one or some form of combinations of technologies. Latest technologies used in Kota Belud are 4G and WiFi communication to send data to server.

Features

SAIFON Dashboard Web View
SAIFON dashboard web view will display graph of water level and daily weather forecast. Water level conditions can be directly viewed on the Map section. Icon colours will change according to alert level along with graphics indicator on the water level section.



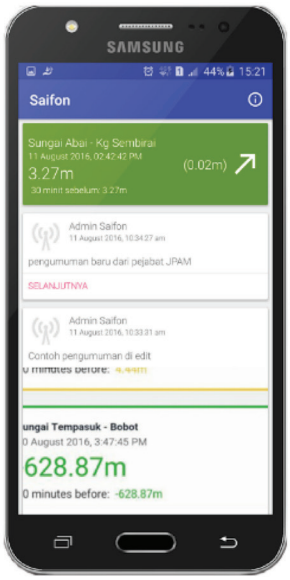
SAIFON Mobile Apps
We have developed the SAIFON mobile apps for both iPhone and Android platforms.

The purpose of this mobile application is to provide information on the flood and receive alert notifications according to alert level.

The application S.A.I.F.O.N. can be downloaded from Google Play and Apple Store

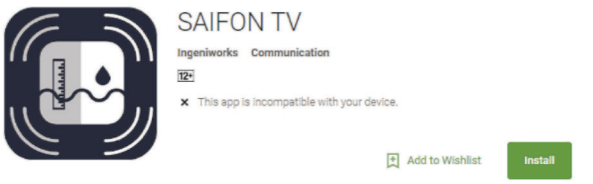
Available on the App Store

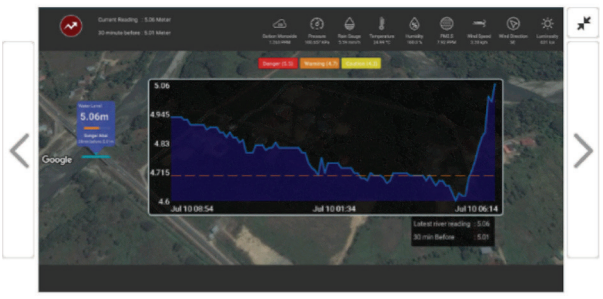
ANDROID APP ON Google play



SAIFON Android TV

The SAIFON app has been developed in the form of Android TV Apps. Android TV is a smart TV platform developed by Google. Based on the Android operating system, it creates an interactive television experience through a 10-foot user interface. Large display screens make it easier for the authorities to monitor the current situation of rivers involved.





Key challenges

There are numerous challenges we faced when implementing and developing SAIFON. The following are some of the main challenges:

Implementation

Currently in implementation phase, we have encountered issues regarding a suitable location because it involved many authorities. For example, location of SAIFON command centre has already been moved twice from its original location. It requires some other surveys to be done in limited time. Collaboration with *Jawatankuasa Bencana* Kota Belud gives a lot of advantages in this implementation process.

Approval process, standards, spectrum

There are several phases that need to be addressed to obtain approval from the authorities and meet the standards needed in the development of this project. In term of spectrum, since early 2017, spectrum such as 868 MHz for LoRa usage had been discontinued by MCMC. In order to solve the connectivity issue, M2M connectivity had been selected until now.

Since the IoT is still new in Malaysia, there are not much guidelines and standards that can be followed. Most IoT companies implement what they assume is right. The other issue encountered is in obtaining certification from SIRIM. Some IoT providers had difficulty to bring their device to Malaysia. There is no reference from previous record because each time items are imported, different tariff codes are used.

Security/ safety

It is crucial to follow the guidelines and precautions in safety aspects in the process of installing sensors in the river. We also seek consultation and recommendation from JPS and JKR in term of sensor installation.

Data accuracy

Data accuracy is the degree in which information given are true or of accepted values. Data accuracy is an issue pertaining to the quality of data and the number of errors contained in a database. It is possible to consider horizontal and vertical accuracy with respect to geographic position where sensor is installed.

Awareness for the communities to use the Apps

Several programmes have been conducted in selected villages around Kota Belud to provide awareness to the public about the use of these SAIFON apps. The key challenges of this programme are to get support from communities and to convince them on the benefit of the apps. Participants will need to download the SAIFON app on their smartphone. Below are some of the areas involved in the awareness programme:

- KG LINGKODON
- KG SIASAI (KUMPANG)
- KG MENUNGGUI/ KARANG BENAI
- KG BOBOT
- KG EJUK
- KG GUNDING
- KG LINAU LIANG
- KG SADOK-SADOK
- KG SIASAI (TAMU)
- KG DONGGOI
- KG PITURU DARAT

Conclusion

The IoT requires three components namely Sensor Device, Data Transmission and Monitoring Software. SAIFON Pilot Project in Kota Belud has shed a new light on the importance of these three components. Sensors device could take many forms and sometimes require modification and customization. Because of non-compliance with the standards, it is difficult to get certified by SIRIM. It may take some time before it is finally certified since they need to process the device we bring in.

Currently, data transmission is through the standard cellular phone service. They require more power and network coverage is an issue at some locations. The IoT specific data transmission standard in Malaysia will help with this and will ensure data connectivity.

SAIFON benefits the community through providing water level sensor reading. As SAIFON mobile app is in collaboration with Jawatankuasa Bencana and supported by MCMC, we have been able to gain trust from the local community.

Local community participating in the SAIFON Application Awareness Programme organised together with APM - This awareness programme ensures that the communities will receive early notification of floods through SAIFON

IoT Enabled Connected Life Services

Prepared By: BNetworks Sdn Bhd

Overview

Connected Life Services

The Internet of Things (IoT), described aptly as the convergence of the digital and physical world is transforming the concept of modern living. Most importantly we have to understand that IoT is not about things, it's about service. Devices and products (things) are simply tools that help businesses to turn those devices and products into service-delivery vehicles and capable of continuously unlocking new value for customers . Incorporating IoT and smart sensors as parts of the Connected Life and Smart Living will deliver extraordinary value propositions that can help property developers to capture the new generation of home buyers.

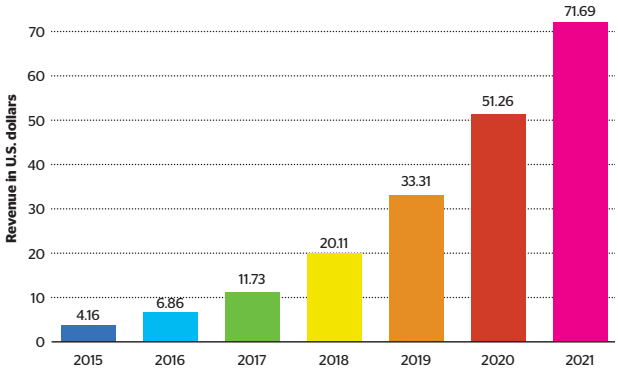
The phenomenal growth of the Internet of Things (IoT) has triggered availability of smart or internet connected devices from all over the globe. This has and will create a series of new challenges to end users and implementation entities. One of the biggest challenges in Malaysia and S.E.A region will be the limited IoT devices players in the ecosystem. As such, almost 100% of the IoT sensors and connected devices sold to customers are being imported. Subsequently the same users may continue to add-on and expand their solution with more devices. As such, locally made IoT sensors and devices leveraging on Zigbee, ZWave or WiFi have a huge opportunity to cater to domestic market as well as being exported to regional market.

The U.S and Europe markets are saturated with home systems for many years and in most cases these products do not address the use cases for this region. It is also common that IoT hubs and controllers from U.S or Europe are built to support and in partnership with their market device makers (e.g Nest, Philips Hue, Sonos Speakers). Whereas devices from China and Taiwan such as Orvibo (WiFi devices), Netvox (Zigbee HA profile devices) and Wulian (Zigbee non-HA profile devices) have their limitation for China consumer preference.

Most of the smart home products are standalone and usually only linked to user's smart phones. There will be no linkage between systems in the residential unit to their building management (condo) or security rooms. Those systems remain as conventional smart home products and a property developer will not be able to provide a more holistic connected service. Smart home hubs/gateways must be positioned as an enabler to link each and every home to the building management during an emergency for security, medical or duress. This will require a cloud based backed software integration and development of front-end App for the building management.

Thirdly, consumers are accustomed to interacting with their mobile phones and tablets to access all services. An integrated Smart Service app will allow users in a community to interact with each other, manage visitors, receive and post feedback, book facilities and report security and safety concerns with ease. The problem with the solutions in the market is the solutions provided are completely detached and no interoperability between Homes, Communities and City.

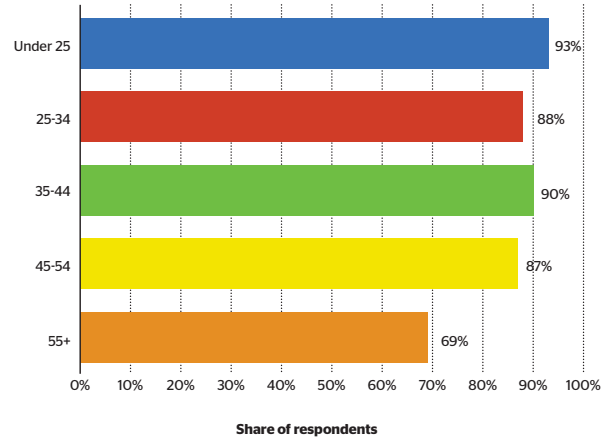
Revenue of the smart home automation market in Malaysia from 2015 to 2021 (in million U.S. dollars)*



About this statistic

The statistic shows a revenue forecast for the smart home automation market in Malaysia from 2015 to 2021. The overall revenue of the smart home automation market in Malaysia is forecasted to reach 51.26 million U.S. dollars in 2020.

Daily internet usage rate in Malaysia in 2016, by age group



About this statistic

This statistic shows the daily internet usage rate of online users in Malaysia in 2016, sorted by age group. During the survey period, it was found that 88 percent of internet users between the ages of 25 and 34 accessed the internet every day.

Core Challenges

Providing a Device and Platform Agnostic Solution for End Users to resolve 4 highly critical problems in implementation of IoT enabled solutions for mass market:

Redundancy

Proliferation of IoT devices creates redundancy and serious non-interoperability between them i.e Multiple Apps to operate each smart device.

Complexity

Each smart device requires its own set of device credentials which transform into complications e.g when user upgrades smartphones.

Fragmented

Each smart device works on different protocols (WiFi, BLE, Zigbee,ZWave) without a unifying solution and interoperability.

Unsecured

Independent smart devices hosted on unknown and unsecured cloud by the manufacturer and highly vulnerable to ransomware attacks.

IoT Devices Security, Data Privacy and Approach

The most recent IoT botnet revealed recently is the Reaper. Unlike Mirai it doesn't rely on exploiting devices with simple default credentials that can easily be detected by auditing of newly released or imported IoT device. Rather it exploits numerous vulnerabilities in different IoT devices and uses sophisticated techniques to hack various smart devices. And this list of vulnerabilities always grows.

Security experts estimate that around 378 million devices are potentially vulnerable to hacking now, growing to more than 900 million potentially susceptible devices by 2020. Every month we read about newly found

serious vulnerabilities in IoT releated protocols, like recent WiFi KRACK attack or Bluetooth Blueborne.

And the only way to protect smart devices is to ensure long-term support with constant release of firmware updates during whole cycle of device life. Another problem is that most WiFi smart devices from China create network connections with covert servers and exchange with them some hidden information. This approach introduces additional security holes, and can compromise overall system security, because network connection is initiated from the inside of local network, and network firewall is useless in this situation.

Meanwhile, there are many smart systems that require constant Internet connection to remote server for normal functionality. This approach can lead to serious security breaches when server is shutdown or not available due to DDoS attack. Smart devices become just pieces of junk when the company decides to shutdown service completely. The most famous event of this kind happened with customers of Revolv smart hub. The company simply shutdown their main server after being acquired by Google' Nest in 2016, leaving customers' devices completely useless.

IoT Devices Security: Proposal for Registry and Ratings
One of the possible solutions for most of the above problems would be to create nationwide public-available registry of devices with security ratings that reflect how "secure" is a device based on AP (Approved Permit) set of parameters such as:

i. How often firmware updates are released for device;

ii. How fast manufacturer reacts on 0-day exploits like WiFi KRACK or Bluetooth Blueborne; and

iii. Openness and interoperability of device protocol:

- Does the device use fixed default login credentials.
- Does the manufacture open any list of server that are used by devices and what information are extended between device and server.
- Does the device require constant internet connection for functionality or etc.

Use Cases: Connected home, Smart hotels

IoT for Connected Homes
The Connected Home implementation will be enabled with IoT gateway/hub and IoT devices as per required by end user. The solution should give maximum flexibility to end users (homeowners) to select the wireless devices and functions to suit their requirements.

The following are some of the necessary (not mandatory) features for a Connected Home Solution:

- Surveillance
- Intercom
- Security And Safety
- Energy Management
- Entertainment
- Climate Control
- Voice Activation
- Smart Mirror
- Medical and Wellness Tracker
- Integration to Guard House
- Smart Community App

Functions and Features

Security & Safety
The security and safety features will comprise of:

- Door Sensors: This will show real-time status of the door in the App Homescreen (Open, Close, Intrusion, etc). For homeowners, it will notify them during a security breach or even in cases when the balcony sliding door is being opened (child safety tracking).

- The automation lights in Living and Master bedroom area can be programmed to flash/ blink or change colour during emergencies. This will alert homeowners the type of emergency (Intrusion, Medical or Fire).

- Homes should be linked to the main guard house to send alert notifications during security breach or emergencies.

Surveillance
The indoor camera will show the capability of system that allows homeowners to unplug and plug them in any location within their home to suit their necessities. For example, they can monitor the sleeping baby, domestic maid, monitoring elderly parents or even part time cleaners while they are away at work. The recording of the camera can be retrieved from built-in SD card in bWave or via subscription to Cloud storage.

The outdoor camera on the other hand will show the possibility of linking the Security cameras in Guard House to the smart home system for Visitor Verification purposes.

The Security Guard may intercom/call the homeowners to verify the visitor from the App before they are registered/allowed.
This provides a very novel approach of visitor verification for security reasons with minimal infrastructure cost.

Climate Control
The air-conditioner Universal remote can be installed in the Living Room and Bedrooms to show the capability to turn ON/OFF and adjust the fan speed.

The capability to switch on and adjust the temperature remotely before homeowners return home would be a more energy saving and efficient way compared to manual preset timer in air conditioners.

With Geo-fencing capability, the home system will have the intelligence to adjust the temperature automatically before the homeowners arrive to create a more comfortable climate.

IoT For Hospitality Industries
In the hospitality industry, providing outstanding customer service has always been a key success factor for any establishment, whether for a global hotel chain or a local hotel. This involves understanding the customer, their expectations and their needs. The ideal customer service experience is provided through the delivery of a seamless, personalised service, exactly when the customer is expecting it: in some cases, even before they thought they need it.

Marriott International, Hilton Group and Starwood's Hotel and Resorts are just some of the global hotel chains adopting new technologies to achieve customer satisfaction; as well as improve business efficiencies. In recent years, the most significant factor driving the need to adopt new technologies is a shift in demographics.

By 2020, Millennials are projected to become the largest segment of consumers with disposable income. With 52 percent of Millennials ranking far above average for technology adoption, companies in the hospitality industry are at risk of falling behind customer expectations. Added to the expectations and changing behaviour of customers, the hospitality industry stands

Example of Connected Home Control App

to benefit from the adoption of technology for engaging employees and improving operational efficiencies.

Improving customer satisfaction

Pre-empting customer needs, through understanding customer behaviour, is key to providing impeccable customer service and ensuring repeat and loyal customer. It's important that companies take a holistic view, to look at the entire guest journey from start to finish, in order to identify where improvements can be made. The Internet of Things in addition to an intelligent backend, may help hotel owners to understand more about their buildings or assets, guest preferences and deliver new services.

An example of this comes from bWave Hospitality Solution (BHS), which provides a robust system and platform to enable the establishment of smart hotel rooms. It combines intelligent room management, energy management, in-room controls and content management services in one user-friendly platform. This ensures that the system can optimise each room for energy efficiency, while also providing convenient entertainment options for guests, enhancing their overall experience.

Example of Security and Safety App with Integration to SmartCity Intelligent Operation Centres (IoC)

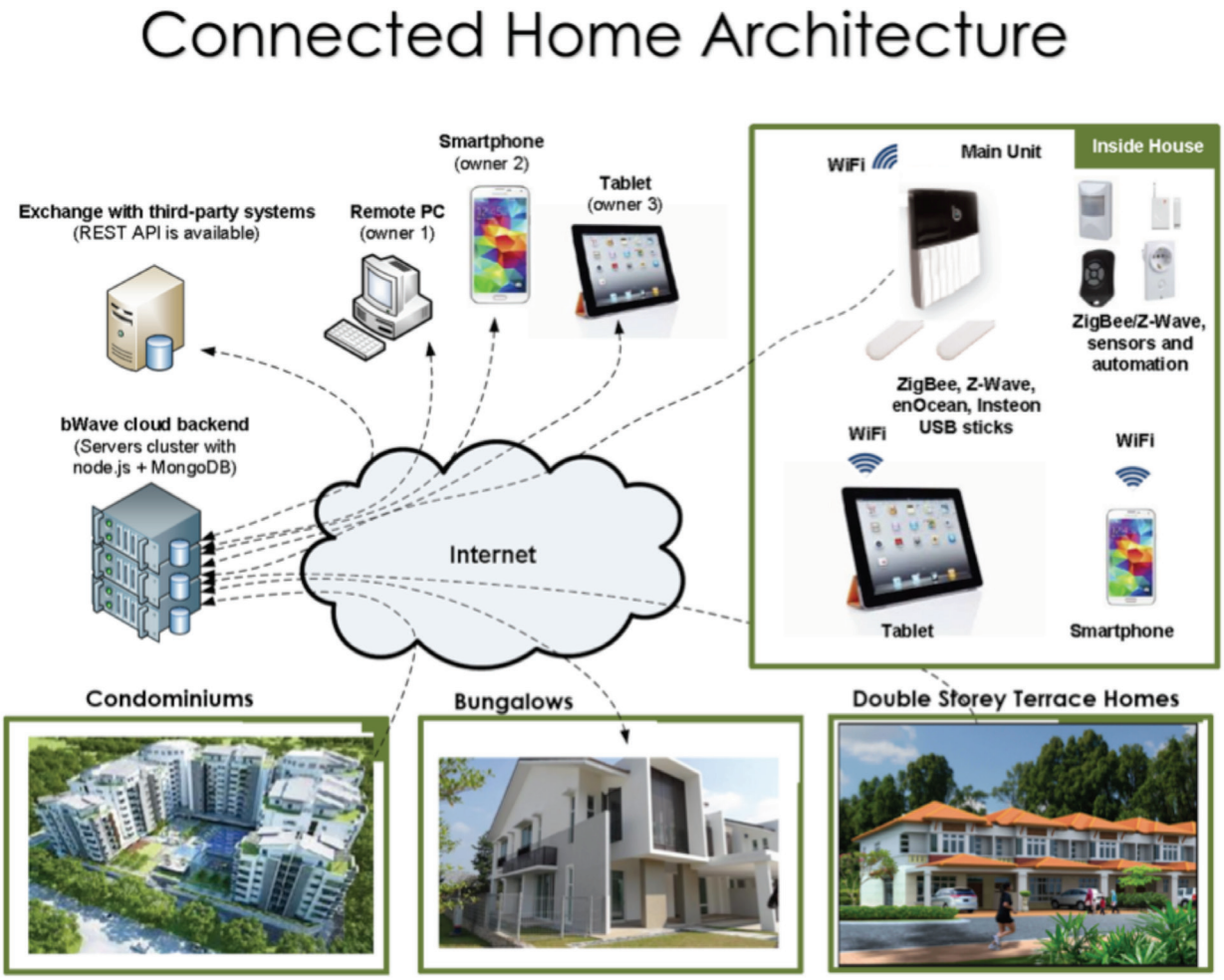
Example of Home Video Surveillance with Secured Cloud Platform

Improving business efficiencies

Maintaining and reducing operational costs, whilst being environmentally conscious has always been a focus for the hospitality industry. With often large properties to manage, ensuring that assets are managed properly and efficiently, could save companies significantly.

By implementing smart sensors, hotel managements are able to manage energy usage and assets more effectively. For example, sensors can be used in guest rooms to measure natural light and therefore dim smart lighting or turn them off when there is no occupancy. Sensors can be used to automatically notify maintenance when assets show distress. Incorporating such IoT devices in guest rooms can save money by identifying maintenance issues before they become costly problems. For example, an overflowing bathtub and a burst water pipe can cause serious damage to the floor and ceiling, as well as render the room completely uninhabitable until the problem is fixed. By addressing maintenance issues early, it

Home Climate Control Menu for Lifestyle Needs and Energy Efficiency



IoT Network Architecture : Connected Homes for Smart Cities

can be dealt with properly and promptly by the person in charge, and the room will be available for guests with little, if any, delay.

Summary

Incorporating the IoT and smart sensors as part of the operations will deliver business intelligence that can help to cut costs and improve customer service. However, with IoT still in its relative infancy, it is important to implement technology neutral solutions such as bWave IoT Hub which works with devices and sensors from various protocols and standards.

The other important aspect would be security measures implemented to ensure the smart devices are not vulnerable to cyber threats and hackers. All IoT devices must be connected to a dedicated and independent IoT hub like bWave instead of building's or hotel's general WiFi network. bWave IoT platform ensures all communications are encrypted with modern cryptography and presence of strict firewall protocols. Cyber threats will be constantly monitored and automatic security patch will be updated to all bWave hubs deployed.

Hospitality has the potential to be one of the early adopters of the Internet of Things, as it is already an industry that works closely with both people and technology. Through a closer understanding of the assets, operations and the guests, IoT provides access to analytics and a level of control to a hospitality environment, which was not available before.

Use Cases: Digital Voice Assistant

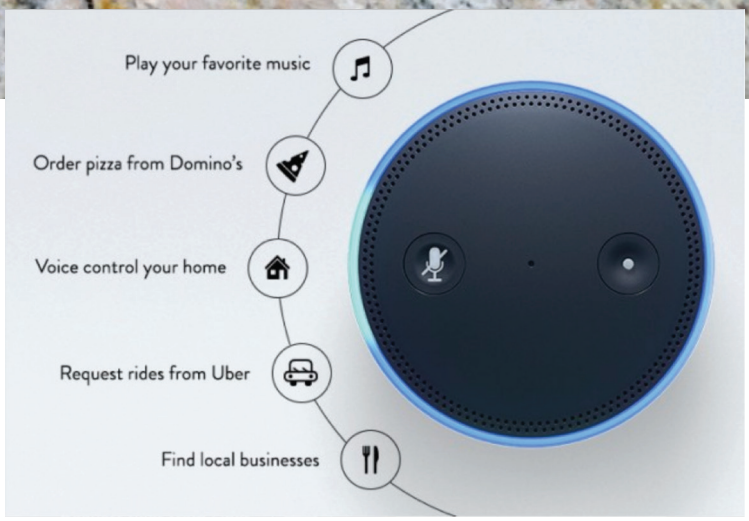
Amazon's Echo speakers, Alexa virtual assistant that is built into them — have become one of the most popular voice assistant device of all time, and hospitality industries are embracing them, too. The digital voice assistant will be able to do things like control lights, temperature, play music, movie selection as well as access thousands of skills in the Amazon skills marketplace.

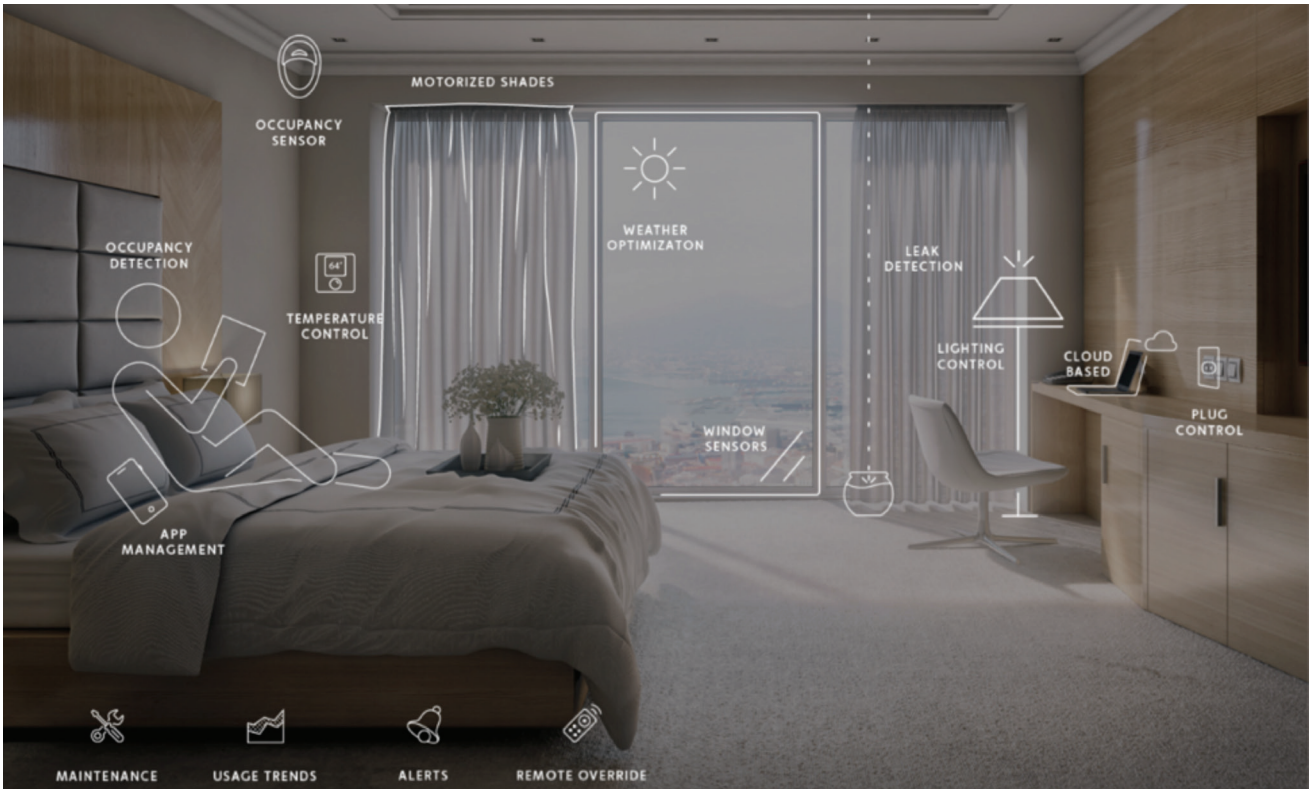
Use Cases: Light and Ambience Control

The light automation feature will comprise of installation of Smart Light solutions to allow simultaneous dimming and light control by a single touch in the user App or via Voice commands. The smart bulbs can be installed in any floor standing lamp shades, wall lights or etc.

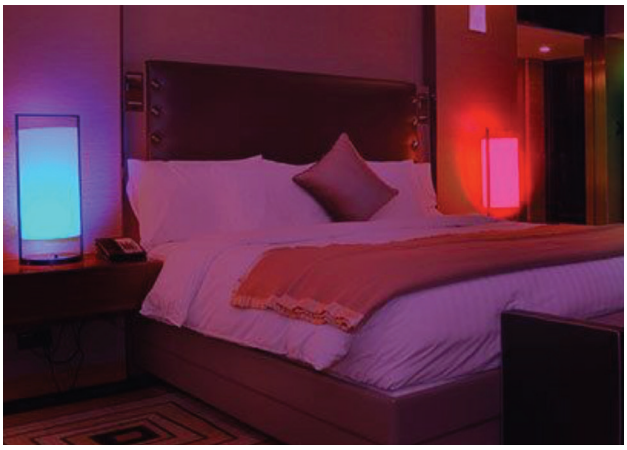
By providing these smart light bulbs in the guest room, the guest will experience more personalized room ambience according to outdoor weather, day/night and their mood:- Single touch "All Off" feature to turn Off lights when rushing out of home.

Digital Voice Assistant in Smart Hotel Rooms





"The thing that Amazon has done with Alexa is quite perfect. If I have ever seen anything in my 49 years of developing resorts that has made our job of delivering a perfect experience to our guests easier and help us get to another level, it is Alexa," said Wynn Resorts CEO Steve Wynn in a statement.



Smart Hotel Room Ambience Settings

Use Cases : Smart Temperature Control

Each room will have a wall-mounted unit that can be retrofitted to any existing air-conditioner models. It gives maximum flexibility to guests to control their preferred room temperature and fan speed by any of the following method:

- Manually from the control panel.
- bWave App.
- Voice Activated Devices.

Apart for the comfort level within the room, the Sensi controller also allows automated control of fan speed and room temperature depending on the occupancy level. The capability to switch on and adjust the temperature remotely before guest return to their room would be a more energy efficient way compared to manual preset timer in air conditioners.

Guest room air-conditioner can be switched ON once guests complete their check-in processes and the room temperature will be adjusted according to the outdoor temperature. The built-in Humidity sensor will allow housekeeping to monitor and take precautionary tasks to ensure the guests rooms are in perfect stay condition.

Smart Hotel Room Air-conditioning Management for Energy Efficiency

Use Cases: Energy Management

The Energy Management feature will comprise of solution for both energy monitoring within each guest room and for the entire building. Both solutions will work independently and the management will have an option to deploy them according to the requirement.

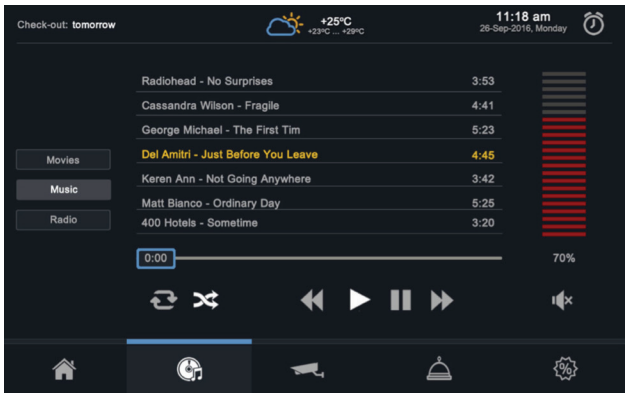
Guest Room

Real time energy level within each and every Guest Room. The WiFi Energy Monitor module will be installed in every sub-Distribution Box (incoming power supply) to every guest room. The energy usage will be transmitted to bHS Software which will compile and display analysis for every room. This information will be vital for management:

- To derive the approximate amount of electrical usage during each stay.
- Maintenance team to identify if there is any form of leakage, unusual usage or defective appliances.

Energy Monitoring for each Smart Hotel Rooms

Movies/ Videos- The bWave App by itself can be used as a centralized remote to select and play favorite videos (movies). Movies can be stored in bWave built-in SD card and local streaming will be done. Alternatively a Smart TV from Samsung can be used for in-room entertainment.



Music and Video Control App

Building Energy Management

The Building Energy Management solution will require installation services for energy efficient equipment which reduces overall energy consumption in the building. Some of such energy efficient devices include voltage optimizers, power factor correction, maximum demand control and energy efficient lighting systems. It enables buildings to be more energy efficient through a combination of energy management systems, smart building controls, energy efficiency products as well as a unique & easy-to-implement Energy Conservation Measures (ECM).

Use Cases: In-Room Entertainment

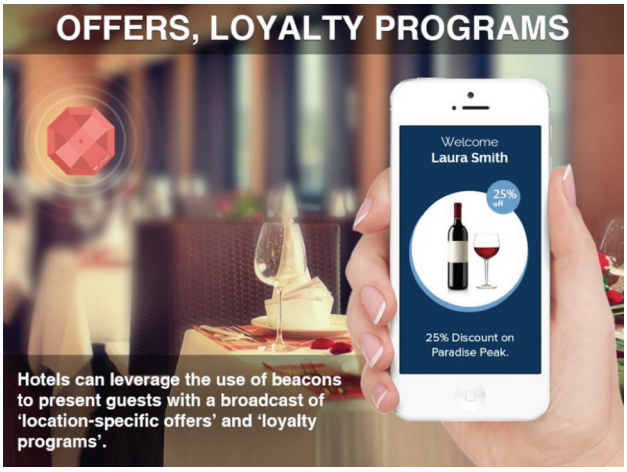
The Entertainment functions within the rooms allow Guests to experience the following:

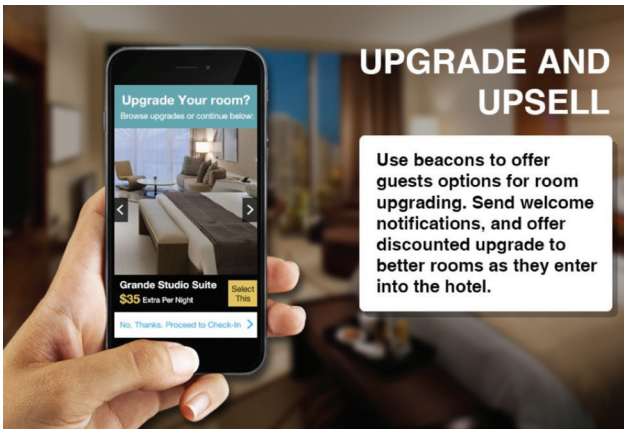
Music- Hotel Guests will be able to experience music library and enjoy their favorite music from the App or Alexa voice commands (e.g : Music will be automatically played during Welcome Mode, Evening scene with light ambience). In addition they will be also able to stream songs from their very own devices to the Bluetooth speakers in their room.

Use Cases: Proximity Marketing and Promotions

Proximity Marketing is a form of location-based marketing that is suitable for indoor locations – particularly for hotels and hospitality industries. Proximity devices such as Wi-Fi or beacons are placed in strategic places inside the hotel. Those proximity devices then communicate with the guest's mobile phones when they come into range.

Coupons/vouchers can be geo-targeted to hotel guests' smartphones during their stay in the hotel. Using Beacon technology, the hotel could send guests push notifications on their mobile devices as they moved about in the property. Offers were tailored to specific Granada Signature locations, ranging from food and beverage to spa to travel.





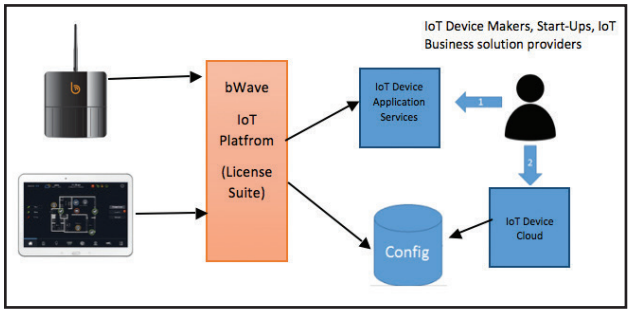
About bWave

bWave® is an Internet of Things (IoT) enabler developed and manufactured in Malaysia. The solution has been successfully commercialised since end of 2016 . It is an award winning and patent pending solution positioned as a lifestyle consumer home electronics for Connected Home applications. Prominent property developers in Malaysia are leveraging on IoT and smart services solutions enabled by bWave® to add value to their new property offerings to the market.

bWave promotes convergence by bringing or connecting all the IoT devices from multiple technologies, vendors and origins to a universal IoT hub (bWave Hub), managed by a single unified App and a secured IoT Platform (bWave Cloud IoT Services).

Partnership and Collaboration

bWave is driving a shift to open technology model where solution providers form an ecosystem of partners. These partners could be IoT device makers, cloud services providers, connectivity vendors, security/medical response providers and many more whereby each participant provides its best-in-class capabilities to contribute to a complete IoT solution and enhanced experience to their customers.



The above diagram shows the implementation of the bWave IoT platform license suite which will allow start-ups, business entities and IoT related device developers to leverage on bWave IoT ecosystem. This is a mutually benefiting model for both business model as well as the device partners/developers as it will be a catalyst to drive the IoT enablers in Malaysia.

Information Security Management System

Prepared by: Digi Telecommunications Sdn Bhd

Introduction

Project Description
Digi is practising and certified with ISO/IEC 27001:2013 ISMS (Information Security Management System). We have been certified since Dec 2012 in line to support MCMC call for all CNII to be certified with ISMS. This initiative was run as a part of Information Security initiatives focussing on systems and processes within Digi's production environment.

Objectives
Our main objective is in improving our information security management system, process and tools to ensure Digi has the right approach to manage security risks and remediate accordingly in order to provide a secured and safe environment to our customers and employees.

The ISMS is conducted through following the ISMS framework where there are several stages.

The stages we follow are Security Risk Assessment, Risk Identification, Risk Analysis, Risk Treatment Plan and Continuous Improvement.

Problem Statement
Digi's ISMS scope is focussing on the protection of production data of critical application systems. This is to ensure necessary controls measures and protections are applied to protect our data and information.

Key Regulatory Challenges
No regulatory challenges as Digi is part of the CNII, we ensure it's our duty to comply as security is the top priority for our organisation.

Recommendation
Digi recommends all organisation to embark and adopt ISMS as it is very beneficial to any organisation to have a structured security management system. You will be able to have good governance for your organisation in terms of proper risk management that covers risk assessment, risk mitigation and risk acceptance based on your organisation risk landscape.

Digi has seen a lot of benefit in process and risk management in terms of how identified risk are treated and how to reduce exposure for the company, or how to get overall view of vulnerabilities in environment and plans and roadmap to bring in relevant tools to support and mitigate as well as enhance security metrics.

Having ISMS also has given positive reflection to our partners and stakeholders who then have a better assurance that Digi is handling their data, information and services in a secured and managed way.

MyMata : Cloud Surveillance with Artificial Intelligence

Prepared by: Ipinfra Networks Sdn Bhd

Video surveillance is one of the fastest growing segments in the physical security industry. In the prevailing security environment, the need for video surveillance is growing exponentially. From smart cities to stadiums, from retail mega-markets to homes, video surveillance has become a pervasive phenomenon. Several petabytes of video data are being generated globally every year from this growing number of video surveillance installations.

However, a large amount of video which is captured is never analysed for actionable intelligence and, in many cases, a large team of human operators is required to monitor the video feeds and many of video surveillance only in passive mode where there is no preventive

alert and notifications. As video archives grow in size and quality, traditional storage and analysis methods are found to be high cost and do not support timely analysis and action. In many environments, video feeds are required to be stored for durations ranging from months to years for compliance purposes, adding to the lifecycle costs of video surveillance solutions. Standalone video surveillance solutions are, therefore, not truly efficient or optimised for cost and need to be augmented with physical security staff.

In the digital era, the securities system is also very important everywhere with the need for more technological and very simple security technologies. This MYMATA product is a new evolution in the field of securities in this country conceptualised by using the idea of a bumiputera company Ipinfra Networks Sdn Bhd. The system uses the latest technology of 'cloud recording and artificial intelligence video' whereby users can access CCTV video directly and can monitor recorded videos for a week and a month. Videos that have been stored in the 'cloud server' enable the parties to access the videos via mobile phones, tablets and computers anywhere and anytime. The main advantage of this product is proof of recording is still stored in the cloud server even if the digital recorder of CCTV (DVR) video is damaged or stolen (DVR is the recorder in conventional system that has been incorporated into 'cloud recording' in MYMATA). MyMata also adapts the latest security technologies by using cloud based such as deep learning, artificial intelligence and analytics. The company is very optimistic to expand the marketing of this MYMATA product into a wider market in various sectors. This product has the potential to set a new higher level of security system in Malaysia.

Challenge on IoT Surveillance Video Related

The need of the IoT on Security

As enthralled as we are with the individual capabilities of IoT devices, in the security world, the more important aspect of this trend is how all the components work together to solve a tangible challenge. First of all, IoT-based systems must be easy to design, install, maintain and use. However, one size does not fit all.

To maximise the potential of the IoT, it requires an in-depth knowledge by suppliers who (1) understand how each feature or component

works together, (2) can design a solution that can be used to solve specific challenges, and (3) are able to deliver it as an integrated offering that has a better long-term value than just the sum of its parts.

This is especially true as security solutions move well beyond their roots in cameras. Indeed, largely because of the IoT, the security sector's traditional boundaries continue to become unclear. For example, network cameras can be used for Building Information Management (BIM), Business Intelligence (BI) in retail and even leaping into scientific research with real-time analysis of traffic patterns and crowd movements. The IoT will allow for combined systems integrating previously disparate devices such as video surveillance cameras, smoke detectors, access control panels and loudspeakers into a common management console providing a 'single pane of glass' overview across entire buildings and sites.

The result is a huge opportunity for security solutions that are purpose-built to share useful data with other connected devices, all of which can be monitored remotely. This connectivity between devices will provide end users with more complete situational awareness across multiple locations.

Security as a service: The cloud emerges

Cloud-based computing has touched just about every industry and it will continue to reshape the security and surveillance sector as well. Security can now be offered as a service that is managed remotely, freeing up valuable human and capital resources that no longer need to be on site at every location that requires monitoring. Secure remote access to security systems will increase in use, including by end users who want the convenience and real-time benefits of being able to monitor property and events without having to be physically present.

Cloud storage is another important aspect of how systems are becoming more efficient in this model. Much larger volumes of data can be stored, cost-effectively and securely, at dedicated server facilities, allowing users to archive video and associated data for longer periods of time and improve its accessibility as well.

There are challenges to protect the cloud system from cyber-attacks. Cyber security specifically designed for networked and cloud-based security systems are emerging. This is critical to protect against vulnerabilities, such as hacking, and will be an important aspect of how physical security and surveillance solutions are designed and implemented.

A growing concern for cyber security threats

While the vision of the IoT is enticing for the convenience, capabilities and flexibility vast networks of connected devices offer, there is a growing risk for security threats and breaches as the number of entry points into a network dramatically increases. In a recent survey by Cisco, 73 percent of business decision makers said they expect the IoT to cause security threats to increase in severity over the next two years. More worrying, 78 percent of IT security professionals are either unsure about their capabilities, or believe they lack the visibility and management required to secure new kinds of network connected devices.

As a general rule of thumb, as you increase availability and access to any network device, it potentially increases exposure to cyber threats. Because security camera systems will become increasingly internet-connected with the rise of the Internet of Security things, offering benefits such as remote access and third party integration, just as with other network connected devices, it is critical to do a risk assessment and implement security polices in the design and implementation of a network video system.

Risk assessments have been common practice in the design of physical security systems for years, particularly for enterprise installations. Integrators should apply the same thought process to the configuration of network video devices, even though unlike other devices on the networks such as laptops, desktop or mobile devices, a network camera is not exposed to the common threat of users visiting potentially harmful websites, opening malicious email attachments or installing untrusted applications.

However, as a network device, a camera or other connected physical security devices may expose risk. Consequently, it is important to reduce the exposure area of these risks and minimising the attack surface area is a common cyber protection measure. If there is no necessity for the interaction between the devices, services and applications, the connectivity can be done with certain limitations. Additionally, segmenting the video system from the core network is a good overall protection measure, thereby reducing risks of video resources and business resources adversely affecting each other.

More cameras mean Big Data

According to market researchers, video is now the fastest growing type of data in the world, and video generated by security and surveillance systems is no small reason. While this vast amount of video data is largely being used for security purposes, as mentioned above, it is increasingly valuable as a source of business intelligence.

However, there still remains a significant challenge to effectively manage and use the endless amounts of video data being generated, so-called big data.

Big data is difficult to process through traditional data processing applications. We expect to see more investment in tools and other resources that can effectively mine and derive actionable intelligence from the big data that security systems are producing.

This technology can put structure around vast amounts of unstructured video data, helping better understanding on significant patterns and trends.

In the coming years, look for improvements in and greater use of video management systems (VMS) to search big data in order to pull up relevant events, people, locations, times, colours and keywords. Such tools will assist business operators to turn big data into critical information that aids in loss prevention, marketing, operations, and customer service.

Wifi technology evolution
Wireless technology has transformed our lives in many ways, from mobile phones, to WiFi connectivity. We have already seen the benefit and convenience of remote security monitoring via smartphones and tablets.

Video surveillance systems of up to ten network cameras can be managed entirely via mobile devices, no longer requiring a desktop PC to run video management software. Especially for SMBs, this significantly lowers the technology hurdle as users are more open to using a smartphone app than having to overlook a more comprehensive and detailed video management software on a desktop PC. It also reduces overall system and maintenance costs.

Expect to see more use of wireless technology in security and video surveillance, particularly as an enhancement to business optimisation and improvement of the customer experience. Wifi technology become more evolves on technology such as from 802.11g to 11n and now to 11ac. Security camera also need to rapidly follow the trend of the WiFi.

Higher resolution
Security cameras have insatiable appetite for more clarity and detail in the images produced by their video surveillance systems. This is especially true as the adoption of intelligent video analytics continues to grow. So continued improvement in megapixel technology is certainly our future. Enhanced techniques to handle challenging low-lighting conditions in new ways are coming to market, making cameras even more useful in a wider array of applications and use cases.

However, higher and higher resolutions also result in increasing storage consumption. Intelligent video compression algorithms such as Axis' Zipstream technology allow for a reduction in storage needs by an average 50% or more.

This is achieved by analysing and optimising a network camera's video stream in real-time. Scenes containing interesting details are recorded in full image quality and resolution while other areas are filtered out to optimally use available storage. Important forensic details

like faces, tattoos or license plates are isolated and preserved, while irrelevant areas such as white walls, lawns and vegetation are sacrificed by smoothing in order to achieve better storage savings.

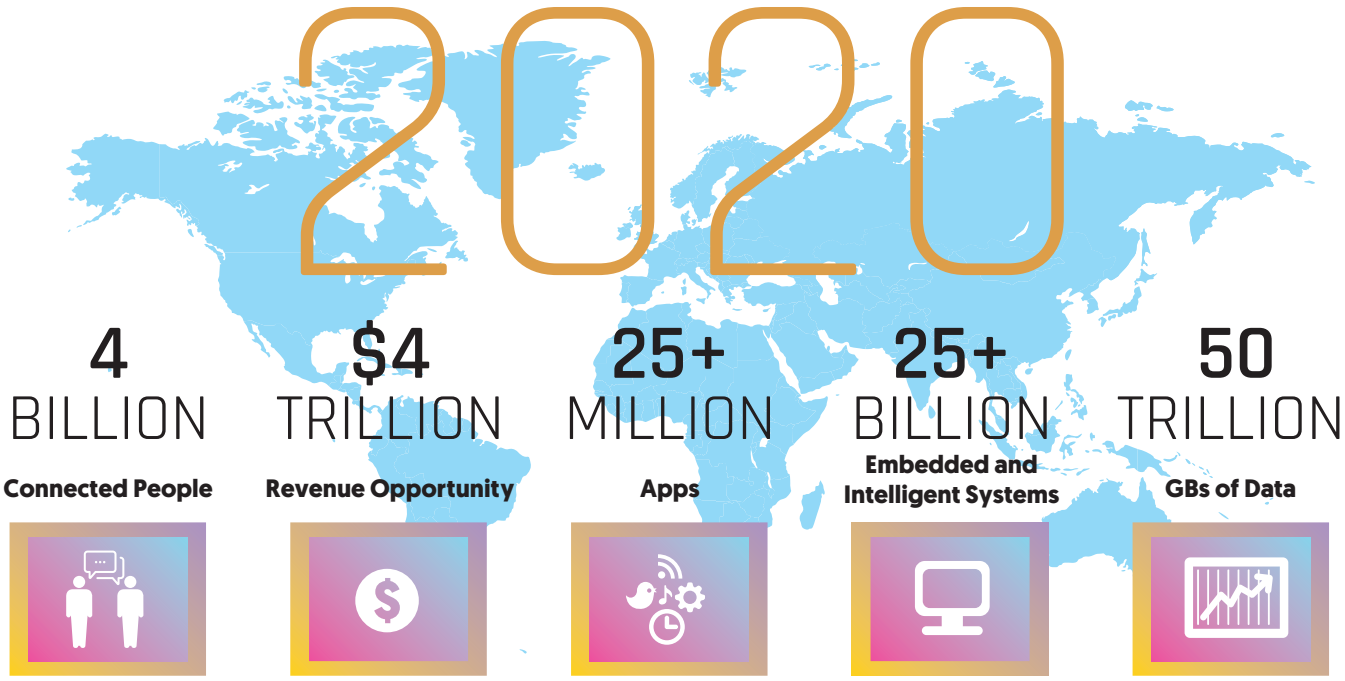
The needs of Analytics provide the brain for smarter systems

If IoT devices are the eyes and ears for increasingly interconnected systems, then analytics technology is the brain. We expect to see continued adoption of sophisticated video and audio analytics in the coming year, helping security systems evolve from passive monitoring to intelligent and adaptive recognition, situational awareness and analysis systems.

Analytics go far beyond security uses. Retailers, for example, are increasingly using video analytics to gain business intelligence insights that allow them to optimise shop floor plans, merchandise display or checkout queue management.

In our recent survey, 'CCTV in Retail', one third of retailers across Northern Europe want better customer insights such as age and gender analytics and other IP applications such as people counting, queue management and dwell time. This opens up entirely new user groups to video surveillance. For example, in-store traffic flow and behaviour analysis can help guide advertising and promotion campaigns.

WORLDWIDE INTERNET OF THINGS FORECAST



Credit: Mario Morales, IDC

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 328491