



HETEROGENEOUS INTEGRATION ROADMAP 2019 Edition

Chapter 3: Internet of Things (IoT)

<http://eps.ieee.org/hir>

The HIR is devised and intended for technology assessment only and is without regard to any commercial considerations pertaining to individual products or equipment.

We acknowledge with gratitude the use of material and figures in this Roadmap that are excerpted from original sources.
Figures & tables should be re-used only with the permission of the original source.



Table of Contents

To download additional chapters, please visit
<https://eps.ieee.org/hir-2019>

CHAPTER 1: HETEROGENEOUS INTEGRATION ROADMAP: DRIVING FORCE AND ENABLING TECHNOLOGY FOR SYSTEMS OF THE FUTURE

CHAPTER 2: HIGH PERFORMANCE COMPUTING AND DATA CENTERS

CHAPTER 3: THE INTERNET OF THINGS (IOT)

1. INTRODUCTION	1
2. BENEFITS OF IOT	3
3. CHALLENGES FOR IOT	4
4. DIFFICULT TECHNICAL ISSUES	5
5. CONVERGENCE OF AI AND BIG DATA AND IOT	7
6. EXAMPLES OF HETEROGENEOUS INTEGRATION SOLUTIONS FOR IOT	8
7. IOT ECOSYSTEM AND HETEROGENEOUS INTEGRATION INFLUENCE IN HI TECHNOLOGY DEVELOPMENT	11
8. THE FUTURE OF IOT	14
9. SUMMARY	15

CHAPTER 4: MEDICAL, HEALTH & WEARABLES

CHAPTER 5: AUTOMOTIVE

CHAPTER 6: AEROSPACE AND DEFENSE

CHAPTER 7: MOBILE

CHAPTER 8: SINGLE CHIP AND MULTI CHIP INTEGRATION

CHAPTER 9: INTEGRATED PHOTONICS

CHAPTER 10: INTEGRATED POWER ELECTRONICS

CHAPTER 11: MEMS AND SENSOR INTEGRATION

CHAPTER 12: 5G COMMUNICATIONS

CHAPTER 13: CO DESIGN FOR HETEROGENEOUS INTEGRATION

CHAPTER 14: MODELING AND SIMULATION

CHAPTER 15: MATERIALS AND EMERGING RESEARCH MATERIALS

CHAPTER 16: EMERGING RESEARCH DEVICES

CHAPTER 17: TEST TECHNOLOGY

CHAPTER 18: SUPPLY CHAIN

CHAPTER 19: SECURITY

CHAPTER 20: THERMAL

CHAPTER 21: SIP AND MODULE SYSTEM INTEGRATION

CHAPTER 22: INTERCONNECTS FOR 2D AND 3D ARCHITECTURES

CHAPTER 23: WAFER-LEVEL PACKAGING (WLP)

Chapter 3: The Internet of Things (IoT)

1. Introduction

From IEEE IoT Magazine “Towards a definition of the Internet of Things (IoT)”[1], the definition of IoT is “A network of items – each embedded with sensors – which are connected to the Internet.” Wikipedia states, “The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”[2] The definition of the Internet of things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the “smart home”, covering devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. There are a number of serious concerns about dangers in the growth of IoT, especially in the areas of privacy and security, and consequently industry and governmental moves to address these concerns have begun. This chapter on IoT will articulate the difficult challenges and potential solutions linking to the other chapters in the Roadmap.

According to a report by Cisco in 2018, 500 billion devices are expected to be connected to the Internet by year 2030[3].

- Each device includes sensors that collect data, interact with the environment, and communicate over a network.
- The Internet of Things (IoT) is the network of these connected devices. These smart, connected devices generate data that IoT applications use to aggregate, analyze, and deliver insight, which helps drive more informed decisions and actions.

By 2030, consumers anticipate an IoT experience that is omnipresent, seamless and personalized[4]:

- Consumers expect to see this by 2030 everywhere in their lives, with a wide array of use cases at home, at work, outside, for healthcare, automotive services and commercial drones.
- However, trust remains a key hurdle to overcome if consumers are to be completely accepting of these new and emerging technologies and as such, most are willing to pay for guaranteed security.

For IoT to be productive and useful, it is important and necessary to integrate multiple devices with functions of sensing, connectivity for sending and receiving, power, and perhaps data analytics and actuation. This is where Heterogeneous Integration Technology comes in: to bring the promise and power of IoT into service for humanity across enterprise, energy, manufacturing, transportation, health, agriculture, consumer and many other aspects of society. And for the worldwide COVID-19 pandemic we face today, IoT is a good example of medical and health institutes using tracing and data collection in real time for health purposes.

Between 2018 and 2025, the GSMA IoT report [5] predicts the number of global IoT connections will triple to around 25 billion in 2025 compared to 9.1 billion in 2018, while global IoT revenue will quadruple to US \$1.1 trillion in 2025 as shown in Figure 1. It indicates that there will be around 13 billion new IoT connections within these five years. The top three applications based on the number of connections can be ranked as connected industry (12.5Bn), smart home (5.4Bn), and consumer electronics (3.4Bn). It will continue to grow in the future in areas like smart cities, connected industry, connected vehicles, consumer electronics, and smart home. Three key application areas where forecasters expect IoT to have the most impact in the coming 10 years are digital manufacturing, smart mobility/transportation and smart medtech. The key areas expected to dominate the next decades are often mentioned as Industrial IoT (IIoT), Smart Cities, Healthcare, Connected Cars, and AI devices.

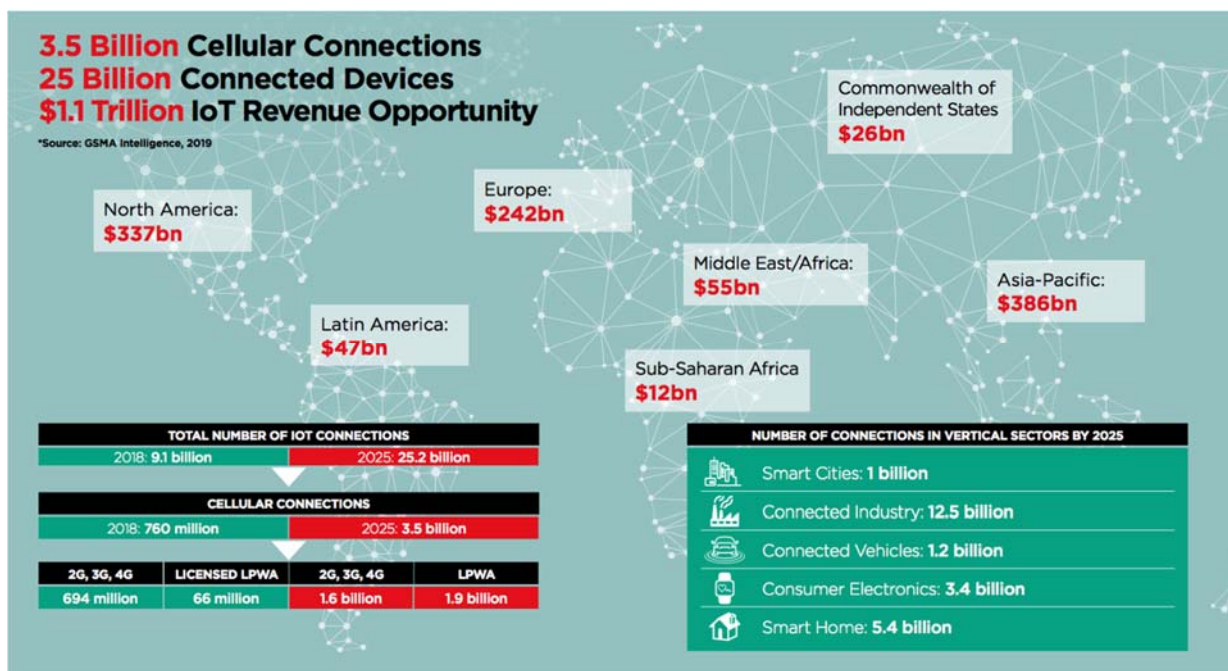


Figure 1. Internet of Things (IoT) by 2025 [5]

Another article, “Unlocking the potential of the internet of things”[6], from McKinsey Global Institute, has a similar forecast for the applications potential and the same scale of revenue by 2025, as shown in Figure 2.

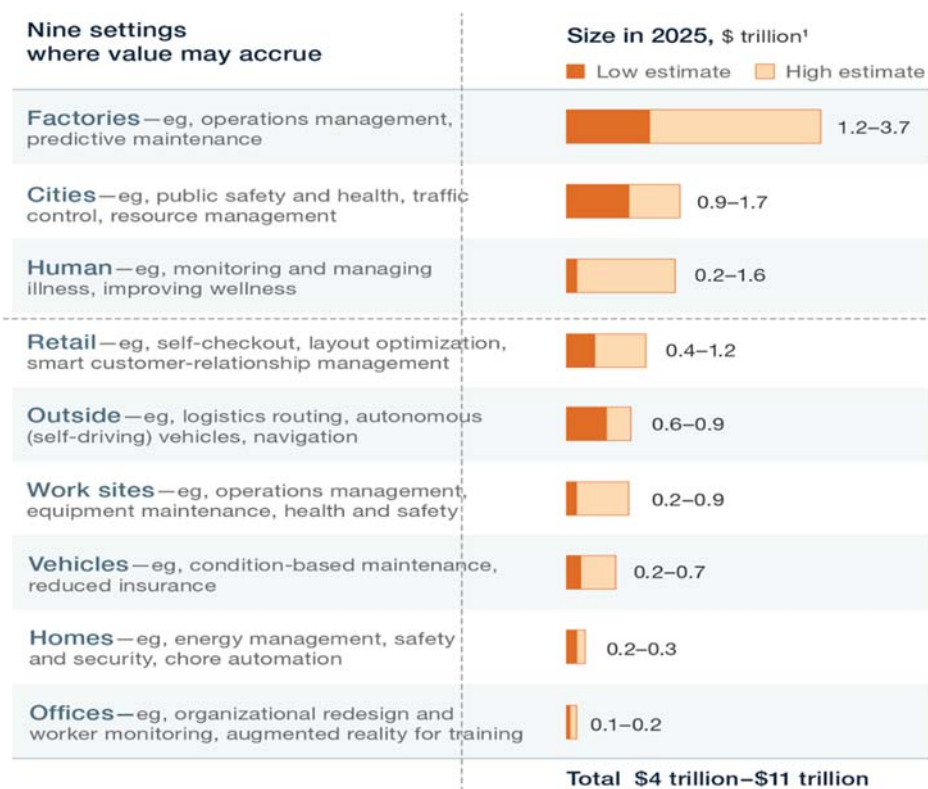


Figure 2. Internet of Things (IoT) by 2025 [6]

As the McKinsey report shows, the ranking of where values will be generated in the future highlights the importance of digital manufacturing, smart city, health, energy, and human applications. This heterogeneous integration roadmap chapter on IoT focuses on these high-value applications.

For the 5G IoT module and component market[7], McKinsey expects total revenues for 5G IoT modules to increase from about \$180 million in 2022 to almost \$10 billion by 2030. During the first years of 5G, standard modules will

probably be more popular than special-purpose and 5G Low-Power Wide-Area (LPWA) modules and thus generate the highest revenues. 5G LPWA modules should be the largest growth driver after 2025 and account for almost 30 percent of total 5G IoT module revenues in the B2B sector by 2030. As module sales increase, component providers will benefit. The greatest gains will go to providers of radio chips and application processors – the active components – with B2B revenues for this group expected to reach about \$560 million by 2025 and \$4.1 billion by 2030. Next in line should be providers of passive components, such as antennae; they will likely see revenues rise from \$188 million to \$1.3 billion over the same period. Providers of testing, assembly, and packaging should also see revenue increases.

There is no doubt that requirements from the Enterprise IoT sector including the Industrial Internet of Things (IIoT) have been one of the driving verticals for the design and development of new 5G concepts and technologies. The notion of ultra-reliable low latency communications and massive machine type communications are somehow reflecting the primary communication types needed within the Enterprise IoT domains. In addition, we have witnessed the emergence of fog and edge computing from the IIoT domain in recent years, which also has driven the architectural evolution of 5G infrastructures.[8]

2. Benefits of IoT

IoT concepts and related technologies are now proven and well understood. The focus now needs to shift from proof of concept to establishing proof of value (PoV) – either saving costs or increasing revenue. In 2020, more than ever, business and technology leaders need to view IoT as one of many tools in a toolbox and learn how to use it in conjunction with other equally important tools, such as analytics, to drive value from it.

Connected devices could account for as much as 3.5% of global energy consumption by 2027. However, IoT can also help make companies more energy-efficient. One example is Schneider Electric, which incorporated sensors into its Lexington manufacturing lines and reduced energy consumption by 12% as a result.

Typically, IoT devices send data to a cloud server where an algorithm analyzes it and triggers an action. ‘Edge’ technology, however, lets devices or nearby gateways compute and analyze data locally, with limited and sometimes no connection to the cloud. The industry has started talking about IoT at the edge and can expect to see fast growth in deployments of IoT edge tools.[9]

Energy harvesting (EH) technology allows small, standalone sensors to function continuously for extended periods of time – decades, even – without power-line connections or battery replacements. This technology greatly enhances the problem-solving capability of low-power sensors and its use is growing rapidly.[10]

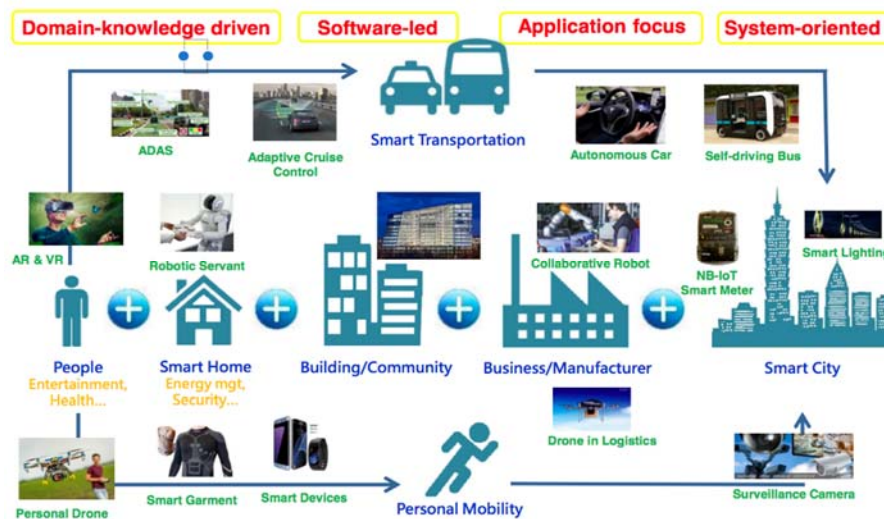


Figure 3. IoT endpoints and vertical-dependent use cases [11]

As shown in Figure 3, IoT endpoints and vertical-dependent use cases are categorized into different segments – people, smart home, smart building/community, business/manufacturer, and smart city. For many industrial IoT early adopters, the current and future generation of wireless communications technologies include WiFi, 2G, 3G, 4G and even 5G. Industrial companies will choose the connectivity solution that delivers the features and performance that is required and at the lowest cost.

3. Challenges for IoT

5G is now upon us, bringing with it the promise of a host of exciting new services. As the boundaries between mobile and the wider digital ecosystem continue to blur, and as data monetization poses a continued challenge, many operators are moving beyond their traditional telco businesses to explore new opportunities in a fast-changing competitive landscape.[12] 5G and LTE will co-exist. The private LTE and 5G network market is expected to reach \$4.7 billion in annual spending by the end of 2020, and \$8 billion by 2023.[13] Three key developments may affect how the demand for connectivity and the buildout of new networks could reach equilibrium: continued growth in online video consumption, massive growth in machine-to-machine connections, and significant adoption of augmented and virtual reality.[14]

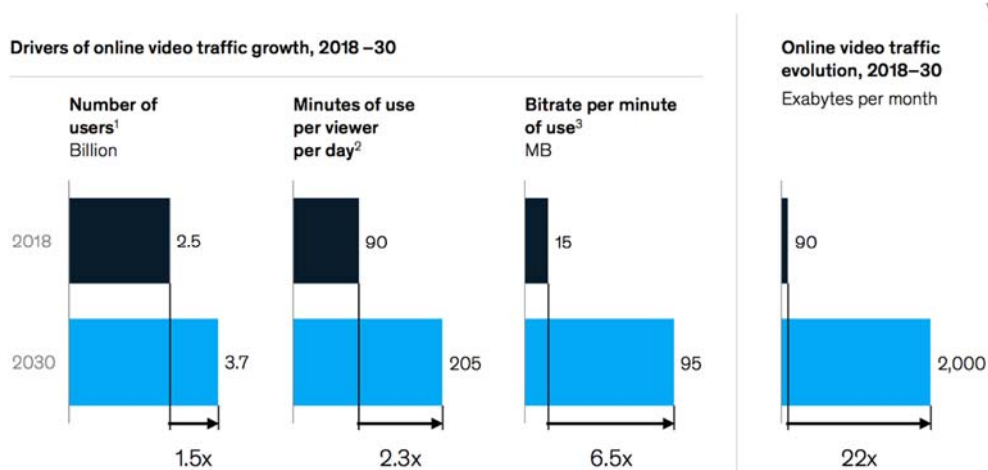


Figure 4. Drivers of online video traffic growth, 2018–2030[14]

The first development would be a continuation of existing trends, with internet traffic from online video growing 22 times larger over the next decade (Figure 4). The majority of this stems from the transition from today’s relatively low-resolution content (SD/HD) to higher-definition content. We also expect to see significant growth in the number of online viewers and more time spent viewing per user. New networks will have to accommodate rising demand for speed and capacity. Much of it will come from the same top 20 percent of power users who consume the majority of video content today; they are likely to be the early adopters of new connectivity technologies such as high-band 5G. New networks would be cheaper to operate due to higher spectrum efficiency – and crucially, they can accommodate a variety of services on the same infrastructure.

Frost & Sullivan’s analysis, “Top End User Priorities in Digital Transformation, Global” [15] measures the current use and future decision-making behavior toward IT and communications, monitors the status of digital transformation (including the implementation plans for emerging technologies such as AI, IoT and blockchain), and evaluates drivers behind investments and challenges across verticals and regions.

Key findings include: The retail (44%) and transportation (43%) sectors are ahead of others in their digital transformation. More than two-thirds of companies feel that the sales and marketing department will be the most impacted department by their digital transformation. Enhancing customer experience, digital presence, and sales and marketing effectiveness are the three major drivers for IT/telecom investment over the next two years. Improving operational efficiencies is a top priority in Asia-Pacific and Latin America, while upgrading customer experience and satisfaction is the most important corporate goal in North America and Europe for 2020. Cyber security is the greatest concern; further discussion can be found in Chapter 19, Cyber Security. Malware (41% of companies) remains the greatest security threat, followed by security misconfiguration and hacking. Malware is common in both smartphone and desktop platforms. The Internet of Things is being used by 65% of companies. Almost 42% of organizations are developing IoT through a third-party service provider. Government is the predominant developer of IoT in-house. IT and communications, finance, banking, and insurance are the top industries implementing artificial intelligence. Cost of integration remains a major impediment to the adoption of new digital technologies. The most common problems that companies face with IIoT solutions is cost.[16,17]

There are nine main security challenges for the future of the internet of things (IoT) which are: Outdated hardware and software; Use of weak and default credentials; Malware and ransomware; Predicting and preventing attacks;

Difficulty in finding whether a device is affected; Data protection and security challenges; Use of autonomous systems for data management; Home security; and last but not the least, Security of autonomous vehicles.[18]

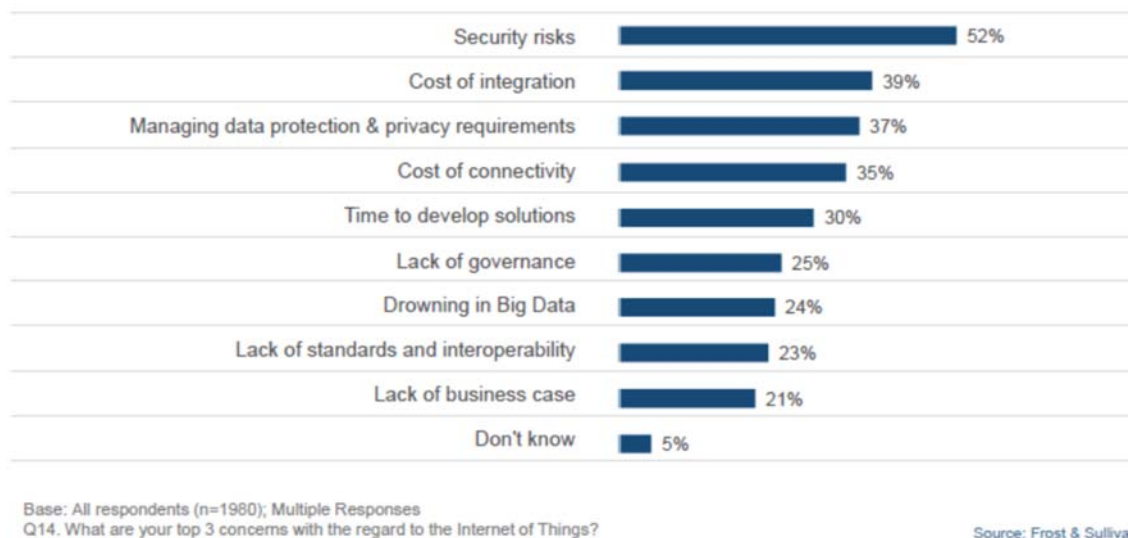


Figure 5. Top Concerns for IoT Deployment [15]

Top Challenges for IoT deployment are security risks, cost of integration and connectivity, data protection and privacy, and time to develop solutions. All the major challenges found by Frost & Sullivan are summarized in Figure 5.

- Gartner's 2016 IoT Backbone Survey [19] found that internally focused IoT projects, particularly those addressing operational efficiencies, topped the priority list for organizations.
- Leveraging thousands of sensors within the data center, collecting data such as temperatures, power, pump speeds, and using DeepMind reinforcement learning, reduced Google's data center cooling bill by 40%, improved computing power around 3.5 times, while using the same amount of power consumption.[20]

4. Difficult Technical issues

Based on the previous section on the challenges of IoT, most of the approaches for different applications cannot be solved by the traditional single packaging technology or regular SiP. Packaging solutions for IoT products need to include light weight, small form factor, low-profile, low power consumption, good electrical performance and low cost. Therefore, the approaches of integrated multiple chips through heterogeneous integration technology will be the best candidate to meet the requirements of IoT. For the hardware heterogeneous integration solution, IoT can be realized by useful deployment of multiple technologies that cover the domains of Hardware, Software and extremely robust applications around each domain of industries and operating sectors. This section will present the technology areas enabling IoT, identify the research and development challenges, and outline a roadmap for future research activities to provide practical and reliable solutions.

Some of the key technology areas that will enable IoT are: identification technology, IoT architecture technology, communication technology, network technology, network discovery technology, software and algorithms, hardware technology, data and signal processing technology, discovery and search engine technology, relationship network management technology, power and energy storage technology, security and privacy technologies, and standardization. Some of these key technology enablers are discussed briefly in the following subsections.

Figure 6 shows the sensing, connectivity, and data in/out with a basic description of key elements of IoT and related device functions. To illustrate the major difficult challenges and technical issues, we selectively address connectivity, IoT home devices, wearables, sensors, and edge AI devices. See other Roadmap chapters for some details.

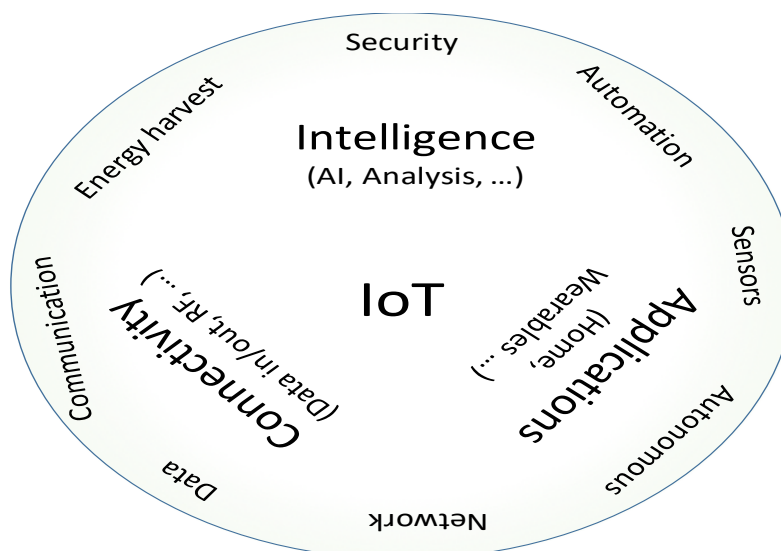


Figure 6. Key elements of IoT

Connectivity:

Limitations of the current Internet architecture in terms of mobility, availability, manageability and scalability are some of the major barriers to IoT. Particularly for upcoming 5G, there is a need to design beamforming antennas to send Radio Frequency (RF) signals to different network and client devices.

In addition, the suppression of electromagnetic interference (EMI) and prevention of noise from affecting different working functional areas are other considerations.[21] As for connectivity, there is a need to design a beamforming antenna, noise reduction, etc. For further information, refer to chapters 7 and 12, on Mobile and RF/5G.

IoT home devices:

The demand for IoT devices (e.g., smart TVs, smart speakers, smart toys, and so on) has increased dramatically and keeps growing. The challenges for future IoT devices with even more functionality are requirements for ever denser interconnects, a smaller package size, better electrical performance, and more cost-effective solutions.[23]

IoT and wearables:

To meet the increasing demand for IoT and wearables products, the challenge of heterogeneous integration is how to reach wafer-level system miniaturization with a smaller form factor, higher performance and increased functionality without compromising manufacturing cost.[24]

Sensors:

In the IoT era of smart manufacturing or of autonomous driving, highly integrated and low-cost sensor packaging solutions are required. The challenges of different sensors – including MEMS packaging, biosensor packaging, optical sensor packaging and RF/mmWave packaging – come from stress-sensitive and fragile membranes, the necessity for direct environmental access to this membrane, temperature-dependent monitoring, and other considerations.[25]

Edge AI devices:

In general, AI systems are running on high-performance graphics processing units (GPUs) using software-defined algorithms mostly in cloud environments. High power consumption is a major issue in such systems. However, intelligent and autonomous IoT systems can be realized by using edge-located AI processing power. Compared to high performance computing (HPC) applications, the computation within the IoT device is dramatically reduced when compared to on-board AI systems. A major challenge to implementing new autonomous IoT systems is how to develop low-cost and high-density packaging technologies through 3D stacking.[22]

As shown in Figure 3, with all those IoT devices and technology, a lot of unstructured data will be generated around all of us – data gathered from shopping online, interactions – study, all done through modern channels of communication such as social media. This data is unstructured and vague, and provides very little information for analysis; this requires data to be converted to structured data. The Artificial Intelligence of Things represents the use of Artificial Intelligence (AI) technologies within Internet of Things (IoT) infrastructure (platforms, servers, devices,

chipsets, software, etc.) to improve IoT operations, improve human-machine interactions, and enhance data management, analytics and decision-making capabilities. One such AI technology, machine learning, provides IoT networks/systems with the ability to learn from data, transforming IoT-enabled assets into “learning machines”. AI also transforms IoT data into useful information, facilitating improved decision making. Accordingly, AI is a foundation technology for moving towards IoT Data as a Service (IoTDataS).

The key is for the two technology sets (AI and IoT) to work together in a mutually beneficial, reciprocal value-added manner[26]:

- AI adds value to IoT: Through machine learning and improved decision making
- IoT adds value to AI: Through connectivity, signaling, and data exchange

This will require interoperability at the device level (such as chipsets), software level (operating systems and programs), and platform level. Since many early implementations of AI are rather monolithic and vertical-solution oriented, there will ultimately be a need for Application Programming Interfaces (API) to open up interoperability between devices, software, and platforms for more horizontal leveraging of Artificial Intelligence of Things capabilities.

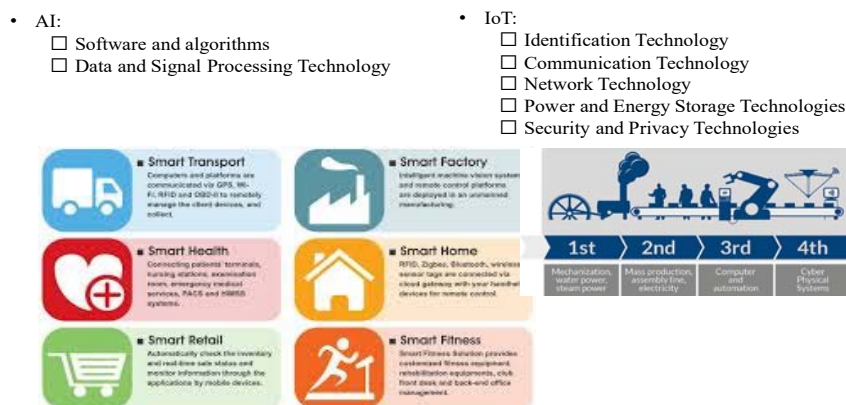
Energy Harvesting:

Today’s state-of-the-art RF harvester typically requires a received energy of at least -30 dBm. More importantly, the desired application must be low power enough to operate with the harvested energy. Bluetooth Low Energy SoCs are being designed to operate with microwatt active power and microwatt-level average power in low duty cycle applications. Combined with an integrated RF energy harvester, this BTLE SoC can create a full-function and yet battery-free Bluetooth solution. The potential applications can be grouped into three categories: by power range: proximity (>100mW), table top (100mW~10uW), and room (around 10uW or below).[27]

5. Convergence of AI and Big Data and IoT

- The missing piece of the puzzle for IoT is to find a killer application; AI’s missing puzzle piece is data. They complement each other.
- Three Phases of AI Adoption for IoT Projects: image/speech-related applications, transfer learning from these applications, and real digital transformation with machine learning and reinforcement learning.
- By 2022, more than 80% of enterprise IoT projects will have an AI component, vs less than 10% today.

AI + IoT Technology



Source: Gartner, DeepMind (2016), Bosch, <https://www.microtom.net/solutions/industry-4-0>

Figure 7. Key elements of AI & IoT Technology[28]

Big data from inspection as an example within the Enterprise IoT domain – defect detection is very critical for ensuring product quality and root cause analysis. With the widespread use of cameras and the availability of machine vision systems, automatic optical inspection (AOI) systems generate a huge amount of image data in a factory every day. Considering the cost, consistency, accuracy and repeatability, an AOI system can replace most human inspection originally done by operators. Although the AOI system has become more convenient and much more efficient than human inspection, the reality on the production line is that the false alarm rate of an AOI system is still too high because of the strict parameters that are set to avoid high escape rates. Therefore, there are two to four verify-and-

repair systems (VRSs) deployed after a single AOI station to perform labor-intensive manual inspection. The solution to solving these kinds of production issues in daily manufacturing is to converge AI and IoT as an AIoT platform or so-called IoTDaaS (Figure 7).

Based on the convergence of big image data and installed IoT sensors, a new AIoT system (auto-VRS) can integrate machine learning technology into an AOI system; this can filter AOI-reported defects and remaining real defects, to reduce the AOI false alarm rate to 20%. It can also reduce VRS operator requirements. The new system mainly uses two technologies – namely a fast circuit comparison algorithm and a deep learning-based defect classification algorithm. The fast circuit comparison algorithm is used to find the region of interest (ROI) of the AOI defect image, improve the accuracy of defect classification, and reduce the escape rate of real defects. The deep learning technique is to classify defects to improve defect recognition and classification accuracy. The implementation of the proposed system is a software module, which can be easily deployed on a cloud server, AOI machine or VRS without any additional equipment.

As shown in Figure 8, the new AIoT system installed as one of the edge devices become one solution in the digital transformation of IIoT. With connectivity becoming increasingly commoditized, mobile operators are looking to expand their role in the value chain – from providing essential tools and capabilities for ecosystem partners, to building IoT solutions, to becoming end-to-end IoT solution providers themselves.

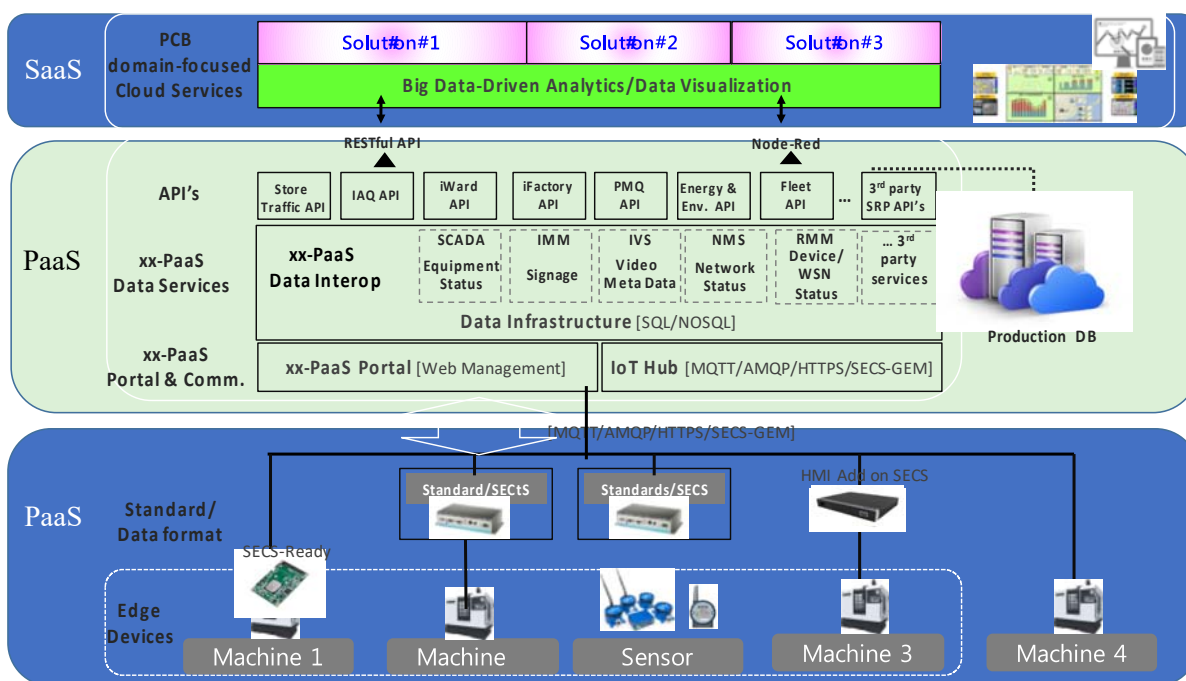


Figure 8. Digital Transformation of IIoT[29]

6. Examples of Heterogeneous Integration Solutions for IoT

Refer to Roadmap chapters 12, 21, 22, and 23 for good examples of 5G, 2D/3D, SIP/Module, and WLP examples.

A. Connectivity

- Small form factor and high thermal performance are required for IoT and 5G, as shown in Figure 9. See chapters 12 and 20, on 5G/RF and Thermal.
- A 3D System-in-Package (3D SiP) can include double side molding and antenna in package (AiP)

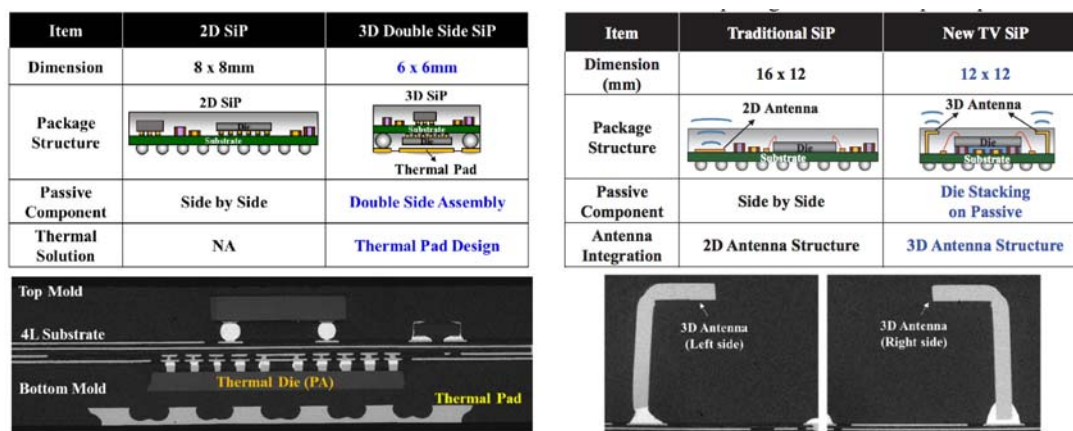


Figure 9. 3D System in Package (3D SiP) [29]

B. Autonomous IoT systems

More intelligent and autonomous IoT systems can be realized by equipping devices with AI (Figure 10).

- An ultra-small IoT system, which is smaller than a grain of salt and having low cost;
- Future small IoT systems with AI devices comprising an intelligent sensor network, high density and low-cost packaging technologies (as further discussed in chapter 21: SiP and Module).

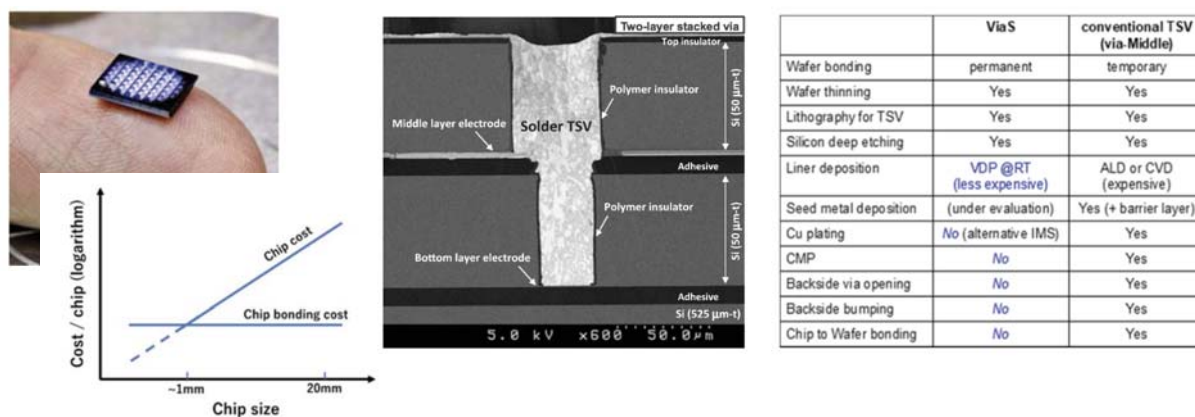


Figure 10. Small IoT systems with AI devices[22]

C. Edge AI devices

Fan-out (FO) packages are widely used in handheld, mobile consumer, and Internet of Things (IoT) devices due to the facility they provide for greater I/O density and the integration of multiple components in a single package (Figure 11).

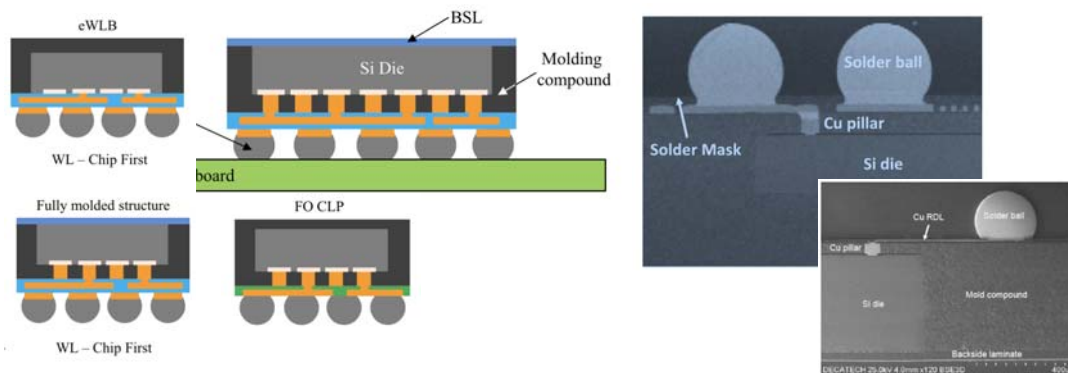


Figure 11. Fan-out (FO) packages [23]

[Note: Fan-Out packaging technology can also be applied to Connectivity (section A), Autonomous IoT Systems (B) and Sensors (E), and is not limited to Edge AI Devices (C).]

D. IoT and Wearables

Common IoT packaging requirements include low cost, good power dissipation (low power for the silicon portion), and good RF shielding in packages that support multiple RF standards such as BTLE, WiFi, or ZigBee. Miniaturization will drive the need for packages that provide greater functionality in thinner and smaller spaces for both medical-grade and consumer-grade-based health monitors, as well as implantable and other medical devices (Figure 12). The adoption and continued innovation in flexible hybrid electronics (FHE) is expected to drive this industry in the years to come. For further discussion, see chapter 4, Medical, Health and Wearables.

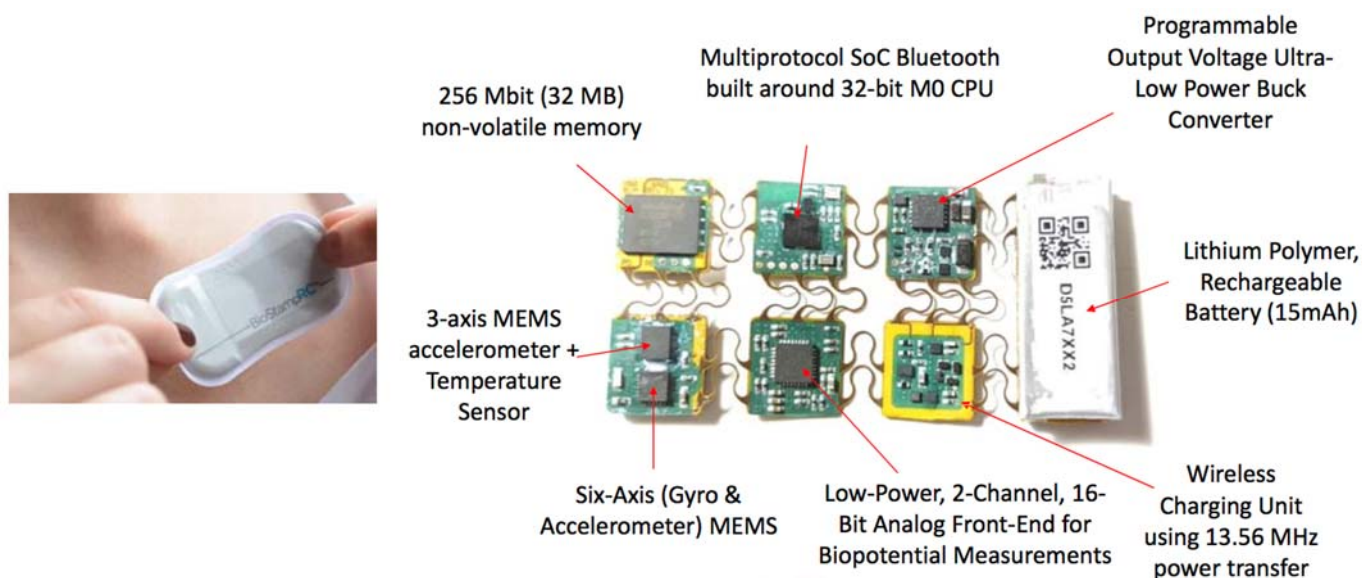


Figure 12. Wearable electronics [Refer to chapter 12 of this Roadmap]

IoT packages must also be production ready, since waiting for a new custom package is often not an option due to time-to-market constraints. Finally, regardless of whether the solution is discrete or integrated, the footprint must be small. The integration SiP technology offers is especially valuable for products like wearables, smart lights, or smart home applications, where space and size are important. It illustrates several SiP design options that could include wafer-level packages, 2.5D or 3D structures, flip-chip, wire bonding, package-on-package, and more.[31] Cavity-based solutions are popular when sensors are involved, especially when there are stimulus delivery requirements such as portholes for microphones. A SiP can also include embedded passives, conformal shielding, filters, and an antenna. Insightful package integration can reduce the size of an IoT solution. Figure 13 shows a new sensor development kit which combines sensor technology and optimized power consumption to provide a ready-to-use prototyping platform for developing IoT applications with lasting battery life.

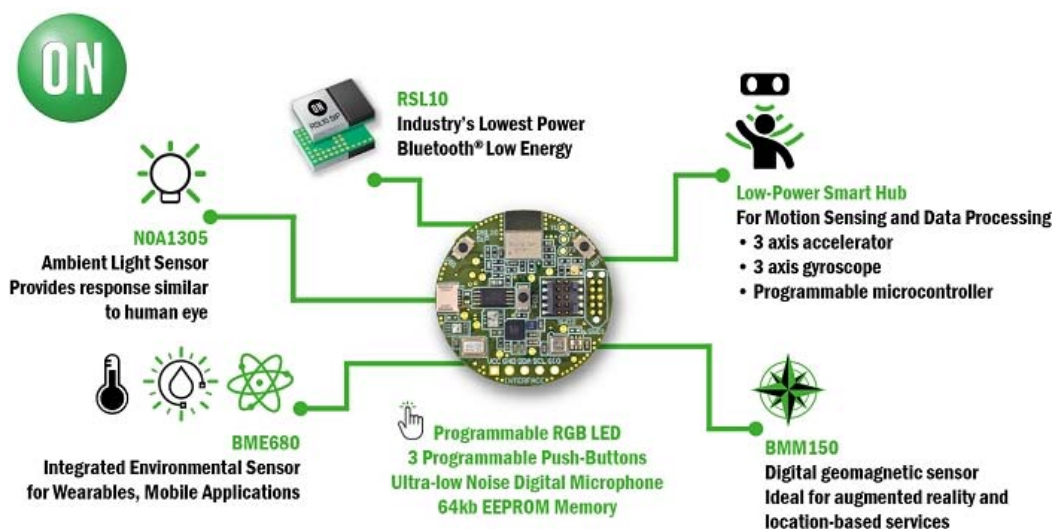


Figure 13. New Sensor Development Kit for Low Power Wearable IoT Applications [32]

E. Integrated Sensor Packaging

Highly integrated and low-cost sensor packaging solutions are required for smart manufacturing or for autonomous driving. Fan-out Wafer Level Packaging (FOWLP) is currently the hottest packaging trend in microelectronics for IoT applications, as shown in Figure 14.

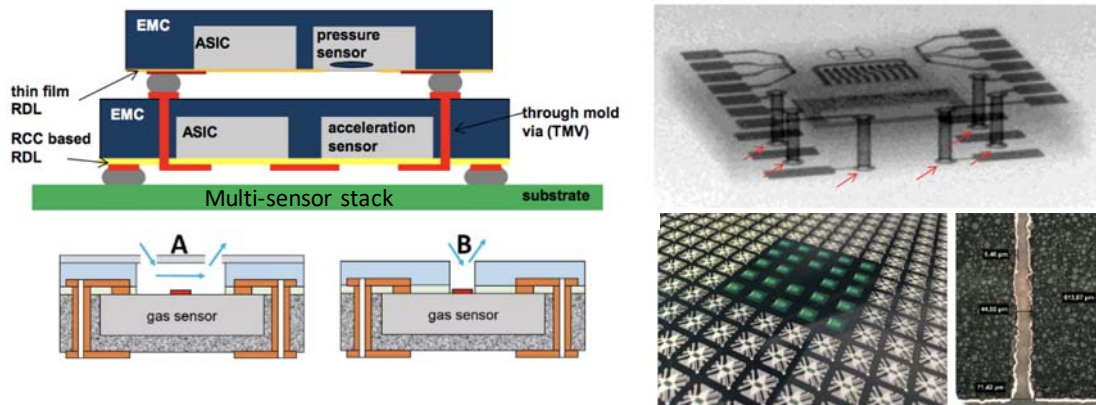


Figure 14. Fan-out Packaging (FO) [25]

F. Heterogeneous Integration of IoT Basic Elements

Figure 15 below illustrates a highly integrated package for IoT applications. The same functions had a footprint of 10 mm² with discrete packages, but only 6 mm² is required with the integrated package solution – a reduction of 40%. Further space saving would be achieved by signal routing in the integrated solution.[6]

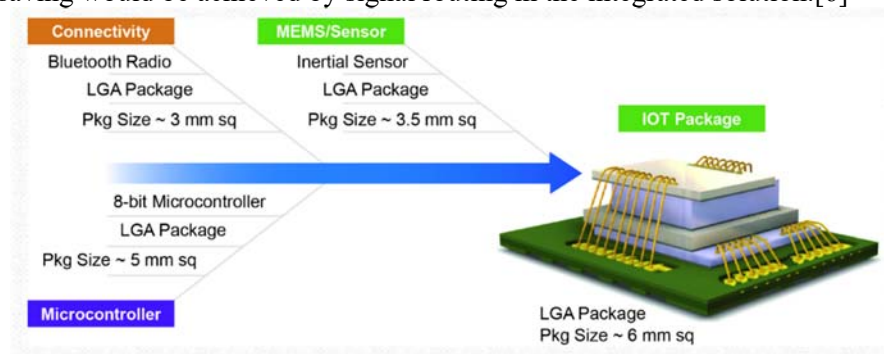


Figure 15. Heterogeneous Integration of IoT Basic Elements [31]

7. IoT Ecosystem and Heterogeneous Integration Influence in HI Technology Development

Some of the latest HI technologies make use of Wireless Sensor Networks (WSNs), which have been applied successfully to fields like train monitoring[34], telemetry[35,36], Industry 4.0 [35,36,37,38] or public safety [39,40]. At present, ZigBee is arguably the most popular technology for creating WSNs and it has been included in some of the latest commercial[41] and academic home automation developments.[42,43,44,45,46,47,48]

Other researchers have also proposed home controllers and gateways for home automation systems that support only WiFi[48,50,51], only ZigBee [45] or both technologies [46,47,48]. Most of them [45,46,47,48] do not use open messaging systems but proprietary ad hoc protocols, while some of the latest use MQTT [52,53] or Extensible Messaging and Presence Protocol (XMPP).[49]

IoT has becoming an application-oriented platform which includes a multi-layer architecture: eg. cloud, network, and end-device. It requires a combination of various transmission technologies and network infrastructure to apply these technologies to achieve various scenarios in different application domains. Currently, driven by the decline of the cost and high popularity of smart phones, the IoT platform and ecosystem have gradually formed. Based on the booming cloud technology, IoT is enabling the development of wireless communication technologies, low-power computing technology (eg. low power MCUs), diversified sensor technology, and low-power management chips and memory.

In general, IoT devices require multi-function processing and low power consumption to extend standby time. To distinguish by functions, semiconductor devices for IoT devices can be categorized into five functional blocks,

namely MCU, Sensor, PMIC (Power Management IC), Memory, and Connectivity. Each of these five functional blocks corresponds to the required wafer-level integration process technology. In terms of processor and memory, wafer level packaging (WLP) can be a good candidate to meet the requirement of low power consumption and small form factor. The newly developed Fan-Out WLP can further achieve the thinner structure by eliminating the organic substrate, and lowering the cost by adopting an integrated molding process. System-in-package (SiP) and Fan-Out WLP can also be stacked in PoP (Package on Package) format, the most popular packaging solution for area-saving integration in mobile devices. As the memory is stacked on the top of the processor, lower power consumption (shorter paths) and higher transmission speed (better SI and PI) can be achieved. Another alternative technology to shorten the transmission path is 3D-IC and TSV technology; it can connect the stacked ICs in the shortest path, thereby achieving vertical integration of the stacked chips and meeting the industry's high-frequency requirements. Due to cost limits, it is mainly used for high-end memory (high-bandwidth Memory, HBM) and stacked image sensor module application.

In terms of the low power requirements of connectivity and PMIC, which have lower pin counts, chip embedded technology can be effectively applied for integrating passive components and the PMIC into an organic carrier/substrate. The remaining area on the top or bottom surface of the carrier/substrate is designed for other chips or passive components with different functions, to form an embedded SiP module. Finally, in terms of sensors, there are many needed to monitor external environmental conditions in smart manufacturing, smart city and smart life applications. Wafer level packaging is very suitable for MEMS and sensors driven by strong demands from IoT applications.

A. Example of Regional IoT Development in Taiwan

As an example, Taiwan is planning to build an innovative ecological environment by mastering the international trend of rapid economic development, and make Taiwan a new base for global networks, big data, and Internet of Things. Taiwan's Internet of Things promotion program has established seven major alliances, including: Taiwan Internet of Things Alliance, Asia IoT Alliance, IoT by GT Alliance, Taiwan Wisdom Taiwan Smart City Solution Alliance, Cloud Computing & IoT Association in Taiwan, IoT Intelligent Sensing Industry Alliance, Taiwan Internet of Things Industry Technology Association, and Taiwan IoT Technology and Industry Association.

Taiwan's Internet of Things market is divided into nine major categories:

- smart transportation
- smart logistics
- smart manufacturing
- smart energy efficiency
- environmental monitoring
- smart business
- smart home
- smart agriculture
- smart healthcare

Already well-known as semiconductor Silicon Island, Taiwan is becoming a good trial site for a variety IoT applications. Taiwan's Internet of Things economic opportunity is set to increase global market share from 3.8% in 2015 to 4.2% in 2020, and to 5% in 2025. At the end of 2018, the value of Taiwan's Internet of Things grew by 19% to \$39.1 billion, accounting for 4.24% of the global Internet of Things (Figure 16).

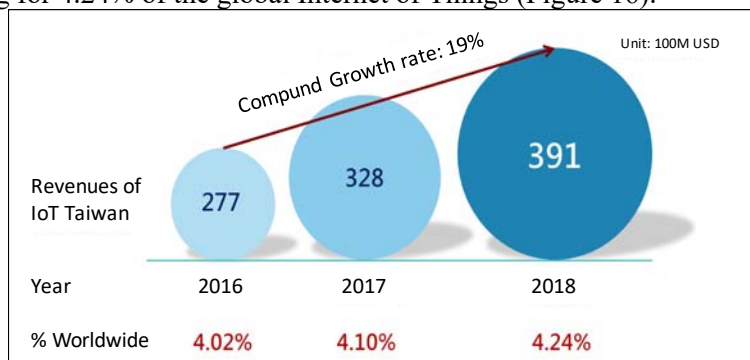


Figure 16. Taiwan's Internet of Things market, Source: ISTI of ITRI (2019)

B. Smart IoT Chip and Design Platform Solution

The future Artificial Intelligent Internet of Things (AIoT) is expected to dramatically change the lives and work of people, enabling people in this ecosystem to connect to each other easily, and to use information more quickly, intelligently and efficiently. The three most important benefits of using AIoT are improving operational efficiency, increasing annual compensation, and improving quality performance. For example, smart phones and smart speakers, which have been popular over the past two years, include Apple, Xiaomi, Amazon and Google, all of which have launched related products. The market response is also very enthusiastic, and related applications have formed an ecosystem.

Among smart IoT devices, the products with large output value or rapid growth are smart TVs, automatic driving assistance systems (ADAS), intelligent security monitors, smart watches and smart speakers. The output value of each sector in 2023 is expected to reach \$3,446 million, \$2,802 million, \$2,705 million, \$1,964 million and \$850 million, respectively. The compound annual growth rates from 2018 to 2023 were 7%, 199%, 62%, 16% and 44% respectively.

C. IoT application Platform

AIoT platform I: for smart home, smart city and smart factory[54]: AP chip solution with high-speed AI edge computing capability to help accelerate the development of the IoT industry chain, providing solutions for smart home, smart city and smart factory, assisting artificial intelligence technology and Internet of Things. The platform's powerful AI recognition capabilities provide technical support for face-identification and payment for unstaffed stores, as well as face access for smart buildings and company attendance systems. In smart factories, it can assist unstaffed vans to automatically identify obstacles to avoid accidents. In sports and fitness applications, through the 3D human body posture recognition function on the platform, not only can the user provide correction suggestions for fitness posture, but also can automatically detect dangerous postures in life and work, so as to issue early warnings in advance.

AIoT platform II: for smart home: With standard ARM-core MCUs, plus power-saving 802.11b/g/n WiFi, suitable for use in a variety of IoT products, such as smart sockets, smart appliances, low power consumption wireless cameras, home security, and environmental sensing devices. These are particularly suitable for battery-powered products because of their low power consumption.

D. IoT and Agriculture

Agriculture, one of the oldest endeavors of mankind, represents a major opportunity for AIoT in cultivating and harvesting living plants, raising animal live stock, and aquaculture. With AIoT incorporating data, AI, and ML, there is great opportunity to bring about a widely adopted database and AI knowledge-based IoT, driving an agricultural revolution.



Figure 14: Illustration of IoT and Agriculture: Source: IEEE Internet of Things Magazine December 2019 cover page

In a special issue of IEEE *Internet of Things Magazine*, the guest editor Raffaele Giafreda has selected specific papers from around the globe illustrating the high complexity and difficult challenges, the needs for research and innovations and profound opportunities for benefit across the whole agriculture ecosystem in this time of climate change and global sustainability. He said “IoT technology has a huge role to play in such a landscape, as it can provide an unprecedented source of monitoring data at a very detailed granularity level; with huge amount of data comes the ability to interpret it for a meaningful and business-viable purpose.” The article “Energy Neutral Machine Learning based IoT Device for Pest Detection in Precision Agriculture” by D. Brunelli *et al*, points to a need for LPWANs (Low Power Wide Area Network technologies) to cover large rural areas as opposed to Smart Cities. One example of “edge computing” is an affordable way to monitor for a pest (the codling moth) occurrence in apple orchards and send a signal on the network only when the moth image is recognized and verified. In another article “Precision Aquaculture,” F. O’Donncha and J Grant described data acquisition from sensors deployed in ocean waters and the atmosphere. The hundreds of interconnected sensors then store and serve data, interact with other sensors and devices, and connect with a fog and cloud ecosystem. Mathematical models enable the implementation of this precision aquaculture concept to provide data-driven insight and decision that promotes ecologically sustainable intensification of aquaculture. These two examples demonstrate the vast expanse for IoT application innovation and fascinating variety of application platforms.[55,56,57,58]

8. The future of IoT

Three major categories including security & privacy, data format, and sensing are addressed here for researchers to understand the challenges for the future needs of IoT:

- **Security and Privacy:** how to make an effective and cheap security and privacy solution for IoT.

Identification is the first step for security. The vast majority of traditional security controls and discovery tools just don’t exist for IoT devices. Identification is well-established for desktops, laptops and servers, but the same concept doesn’t yet apply for IoT. Although IP address can be applied for an IoT device, it certainly doesn’t show what the device is, where it sits, what it’s connected to, whether controls are running on it and if there are any vulnerabilities.

Secondly, an IoT device can also act as a gateway to access internal and previously segregated networks. This lack of visibility results in security teams being completely unaware of the risks they pose and where they have any vulnerabilities that can be exploited by hackers. There is also the threat of physical damage, which will go unaddressed. This might not be a problem in a factory setting, but a medical diagnostic device in a hospital that isn’t working correctly could result in a loss of life.

Third, security hasn’t been incorporated during the design phase. There have been some recent advances in standards, with the passing of a law in the UK that states all consumer smart devices sold in the UK should adhere to the three basic security requirements for IoT, but we are still very much in the infancy of IoT security.

Finally, many IoT devices have not even been configured to receive or run software updates, not to mention that some devices are running on battery so they don’t have the resources to run security controls on them.

Future research should be focused on assuring that every IoT device is counted and evaluated, that hardware is protected, and that software updates can be accommodated.

- **Data format: data integration**

All the sensing behaviors including the variety of different applications, data sources, exchange formats, and transport protocols require a high level of flexibility and scalability.[58] Things on the IoT need to exchange data with each other and with other users on the Internet. Semantic annotation of the data can provide machine-interpretable descriptions upon which the data represents where it originates from, how it can be related to its surroundings, who is providing it, and what are the quality, technical, and non-technical attributes. IoT data usually originates from a device or a human, and refers to attributes of a phenomenon or an entity in the physical world. The data can be combined with other data to create different abstractions of the environment, or it can be integrated into the data processing chain in an existing application to support context and situation awareness. Besides data integration, a number of semantic approaches remain to be taken into account.

Newer and more sophisticated methods for data integration and aggregation are required to enhance the value of real-time and historical IoT data. The pervasive nature of IoT data presents a number of

privacy threats because of intermediate data processing steps, including data acquisition, data aggregation, fusion and integration. How to deal with data in IoT applications is an important topic to fulfill different systems on sharing and integrating data and information. The privacy threat of information linkage and how to address it by technical and legal approaches in a heterogeneous IoT ecosystem is another research interest.

- **Sensing: autonomous and sensor fusion**

It is predicted that new diseases and pandemics, such as Covid-19, in the future. How to adopt IoT technology to reduce or isolate infected people during diagnosis, analysis/measurement, treatment and recovery through M2M (machine to machine) interactions is one of the key approaches in the research of IoT sensing. In terms of sensing, more unique functions of sensors should be developed to strengthen or improve the five human senses: vision, hearing, smell, taste and touch. For example, next-generation artificial tiny nose systems or cubic smelling gadgets can find out in real time the difference between individuals, chemicals, foods, or even diseases. Beyond mimicking the mammalian system, future artificial noses not only can combine cross-reactive sensor arrays with pattern recognition algorithms to create robust odor-discrimination systems, but also interact and communicate with other sensors directly. These can become autonomous IoT sensing systems.

9. Summary

In summary, IoT is the key to digital transformation. IoT technology starts with connectivity, but it's digitization where things get interesting. All companies, big and small, can transform into digital companies by using an IoT platform able to digitize their physical products. IoT will combine AI technology into AIoT which represents the use of Artificial Intelligence (AI) technologies within the Internet of Things (IoT) infrastructure (platforms, servers, devices, chipsets, software, etc.) and big data to improve IoT operations, improve human-machine interactions, and enhance data management, analytics and decision-making capabilities.

Consumers can anticipate an IoT experience that is omnipresent, seamless and personalized by 2030, and will expect to see this everywhere in their lives, with a wide array of use cases at home, at work, outside, for healthcare, automotive services and commercial drones. However, trust remains a key hurdle to overcome if consumers are to be completely accepting of these new and emerging technologies and as such, most are willing to pay for guaranteed security. Heterogeneous integration should play an important role as enabler in enabling IoT devices and systems implementation to fulfill the above-mentioned challenges and hurdles.

Key Contributors

- Wei-Chung (Robert) Lo, chair (ITRI)
- Bill Chen (ASE USA)
- Rockwell Hsu (Cisco)
- Sebastian Liao (ITRI)

Acknowledgments

The IoT TWG would like to thank the cooperation and support of all the contributors listed below, and especially Dr. Chih-I Wu, General Director of Electronic and Optoelectronic Systems Research Laboratories (EOSL)/ITRI.

- Chih-I Wu (ITRI), Shih-Chieh Chang (ITRI), Rolf Aschenbrenner (Fraunhofer IZM), Harrison Chang (ASE), CK Chung (SPIL), Gamal Refai-Ahmed (Xilinx), Li Li (Cisco), Robert Kao (NTU)
- Jerry Peng (ISTI/ITRI), Chi-Hsin Yang (ISTI/ITRI), Che-Hao Fan (ISTI/ITRI), Bor-Feng Jiang (ISTI/ITRI), Ray Yang (ISTI/ITRI)

REFERENCES

1. "Towards a definition of the Internet of Things (IoT)", IEEE IoT Magazine 2015, <https://iot.ieee.org>
2. Wikipedia, https://en.wikipedia.org/wiki/Internet_of_things
3. Cisco 2018, "Cisco Edge-to-Enterprise IoT Analytics for Electric Utilities"
4. Gemalto survey analysis report 2018, "Connected Living 2030: The voice of the customer"
5. GSMA report: "The GSMA guide to the Internet of Things 2019" and "The mobile economy 2020"
6. McKinsey Global Institute analysis 2015 "Unlocking the potential of the internet of things", <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>

7. McKinsey Global Institute report 2020 “The 5G era: New horizons for advanced-electronics and industrial companies”
8. “5G for the Industrial Internet of Things 2019” IEEE 5G World Forum (2019)
9. <https://www.informationweek.com/cloud/5-iot-challenges-and-opportunities-for-this-year/a/d-id/1336721>
10. <https://www.renesas.com/tw/zh/doc/whitepapers/energy-harvesting-low-power-sensor-systems.pdf> Renesas (2015)
11. Source: ISTI/ITRI known as IEK/ITRI
12. <https://www.communicationstoday.co.in/the-roller-coaster-ride-called-telecom/> Communications Today 2019
13. <https://5g.co.uk/news/private-lte-5g-network-spending/5084/> “Private LTE and 5G network spending to hit \$8B by 2023”, 5G 2019
14. McKinsey Global Institute report 2020 “Connected world: An evolution in connectivity beyond the 5G revolution”
15. “Top End User Priorities in Digital Transformation, Global”, Frost & Sullivan 2019
16. <https://iotbusinessnews.com/2020/02/04/62104-frost-sullivan-evaluates-top-priorities-in-digital-transformation-for-global-companies/>
17. <https://iiot-world.com/connected-industry/frost-sullivan-the-major-challenges-facing-the-iiot-solution-market-in-2018/>
18. <https://readwrite.com/2019/09/05/9-main-security-challenges-for-the-future-of-the-internet-of-things-iiot/>
19. <https://www.gartner.com/en/documents/3563218/survey-analysis-2016-internet-of-things-backbone-survey> Gartner Research (2017)
20. <https://deepmind.com/blog/article/deepmind-ai-reduces-google-data-centre-cooling-bill-40> DeepMind (2016)
21. Y.-W. Lu, B.-S. Fang, H.-H. Mi, K.-T. Chen “Mm-Wave Antenna in Package (AiP) Design Applied to 5th Generation (5G) Cellular User Equipment Using Unbalanced Substrate”, ECTC (2018) , pp.208-213
22. H. Mori, T. Aoki, E. Nakamura, A. Horibe, K. Sueoka, and T. Hisada, “Low Cost and High Density Packaging Technologies for Ultra Small IoT Computing Systems”, IEEE EDTM (2019), pp.206-208
23. M. Shih, C.-Y. Huang, T.-H. Chen, C.-C. Wang, D. Tarn, and C. P. Hung, “Electrical, Thermal, and Mechanical Characterization of eWLB, Fully Molded Fan-Out Package, and Fan-Out Chip Last Package”, IEEE CPMT, VOL. 9, NO. 9, 1765 (2019)
24. A. Martins, M. Pinheiro, A. F. Ferreira, R. Almeida, F. Matos, J. Oliveira, H. M. Santos, M. C. Monteiro, H. Gamboa, R. P. Silva, “Heterogeneous Integration challenges within Wafer Level Fan-Out SiP for Wearables and IoT”, in Proc. 68th Electronic Components and Technol. Conf. (ECTC), 2018, pp.1485-1492
25. T. Braun, K.-F. Becker, O. Hoelck, S. Voges, R. Kahle, P. Graap, M. Wöhrmann, R. Aschenbrenner "Fan-out Wafer Level Packaging - A Platform for Advanced Sensor Packaging", in Proc. 69th Electronic Components and Technol. Conf. (ECTC), 2019, pp.861-867
26. <https://mindcommerce.com/artificial-intelligence-of-things/>
27. <https://www.5gtechnologyworld.com/how-energy-harvesting-can-power-todays-iiot-applications/>
28. Gartner, deep mind(2016), <https://www.microtom.com/products/industry-4-0-software>
29. ITRI's project with partners
30. M. Tsai, R. Chiu, D. Huang, F. Kao, E. He, J. Y. Chen, S. Chen, J. Tsai and Y.-P. Wang, "Innovative Packaging Solutions of 3D Double Side Molding with System in Package for IoT and 5G Application", in Proc. 69th Electronic Components and Technol. Conf. (ECTC), 2019, pp.700-706
31. Amkor <https://www.edn.com/electronics-blogs/eye-on-iiot-/4442447/Packaging-advances-needed-to-ensure-IIoT-growth>
32. On Semi, “IoT solutions”, <https://www.onsemi.cn/PowerSolutions/document/BRD8075-D.PDF>
33. IoT White papers, <https://iotbusinessnews.com/white-papers/>
34. Fraga-Lamas, P.; Fernández-Caramés, T.M.; Castedo, L. Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways. *Sensors* 2017,17, 1457.
35. Hernández-Rojas, D.L.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Escudero, C.J. Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT Telemetry Applications. *Sensors* 2018,18, 57.
36. Hernández-Rojas, D.L.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Escudero, C.J. A Plug-and-Play Human-Centered Virtual TEDS Architecture for the Web of Things. *Sensors* 2018 ,18, 2052.
37. Fraga-Lamas, P.; Noceda-Davila, D.; Fernández-Caramés, T.M.; Díaz-Bouza, M.; Vilar-Montesinos, M. Smart Pipe System for a Shipyard 4.0. *Sensors* 2016,16, 2186.
38. Fraga-Lamas, P.; Fernández-Caramés, T.M.; Noceda-Davila, D.; Vilar-Montesinos, M. RSS Stabilization Techniques for a Real-Time Passive UHF RFID Pipe Monitoring System for Smart Shipyards. In Proceedings of the 2017 IEEE International Conference on RFID (IEEE RFID 2017), Phoenix, AZ, USA, 9–11 May 2017; pp. 161–166.
39. Fraga-Lamas, P.; Fernández-Caramés, T.M.; Noceda-Davila, D.; Díaz-Bouza, M.; Vilar-Montesinos, M.; Pena-Agras J.D.; Castedo, L. Enabling automatic event detection for the pipe workshop of the shipyard 4.0. In Proceedings of the 2017 56th FITCE Congress, Madrid, Spain, 14–16 September 2017; pp. 20–27.
40. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0. *IEEE Access* 2018,6, 25939–25957.

41. Fraga-Lamas, P. Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios. Ph.D. Thesis, University of A Coruña, A Coruña, Spain, 2017
42. Fraga-Lamas, P.; Suárez-Albela, M.; Fernández-Caramés, T.M.; Castedo, L.; González-López, M. A Review on Internet of Things for Defense and Public Safety. *Sensors* 2016, 16, 1644.
43. Qivicon Smart Home Alliance. Available online: <https://www.qivicon.com> (accessed on 5 July 2018).
44. Nedelcu, A.; Sandu, F.; Machedon-Pisu M.; Aalexandru, M.; Ogrutan, P. Wireless-based Remote Monitoring and Control of Intelligent Buildings. In Proceedings of the IEEE International Workshop on Robotic and Sensors Environments, Lecco, Italy, 6–7 November 2009; pp. 47–52, *Sensors* 2018, 18, 2660 38 of 42
45. Zamora-Izquierdo, M.A.; Santa J.; Gómez-Skarmeta, A. An Integral and Networked Home Automation Solution for Indoor Ambient Intelligence. *Pervasive Comput.* 2010, 9, 67–75.
46. Baraka, K.; Ghobril, M.; Malek, S.; Kanj, R. Low Cost Arduino/Android-Based Energy-Efficient Home Automation System with Smart Task Scheduling. In Proceedings of the Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Madrid, Spain, 5–7 June 2013; pp. 296–301.
47. Li, Z.; Song, M.; Gao, L. Design of Smart Home System Based on ZigBee. *Appl. Mech. Mater.* 2014, 635–637, 1086–1089. [CrossRef]
48. Cruz-Sánchez, H.; Havet, L.; Chehaider, M.; Song, Y.Q. MPIGate: A Solution to Use Heterogeneous Networks for Assisted Living Applications. In Proceedings of the 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, Fukuoka, Japan, 4–7 September 2012; pp. 104–111.
49. Huang, F.L.; Tseng, S.Y. Predictable smart home system integrated with heterogeneous network and cloud computing. In Proceeding of the International Conference on Machine Learning and Cybernetics (ICMLC), Jeju, Korea, 10–13 July 2016; pp. 649–653.
50. Vivek, G.V.; Sunil, M.P. Enabling IoT services using WIFI-ZigBee gateway for a home automation system. In Proceedings of the IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, India, 20–22 November 2015; pp. 77–80.
51. Wenbo, Y.; Quanyu, W.; Zhenwei, G. Smart home implementation based on Internet and WiFi technology. In Proceedings of the 34th Chinese Control Conference (CCC), Hangzhou, China, 28–30 July 2015; pp. 9072–9077.
52. Bhatt, A.; Patoliya, J. Cost effective digitization of home appliances for home automation with low-power WiFi devices. In Proceedings of the 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 27–28 February 2016; pp. 643–648.
53. Kodali, R.K.; Soratkal, S. MQTT based home automation system using ESP8266. In Proceedings of the IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Agra, India, 21–23 December 2016; pp. 1–5.
54. <https://www.mediatek.com/products/iot>
55. Giaffreda, Giaffreda “Introduction to the Special Issue on IoT and Agriculture” *IEEE Internet of Things Magazine*, December 2019, pp 7-9.
56. Brunelli, D. et al “Energy Neutral Machine Learning based IoT Device for Pest Detection in Precision Agriculture” *IEEE Internet of Things Magazine*, December 2019, pp 10-13.
57. F. O’Donncha and J. Grant “Precision Aquaculture” *IEEE Internet of Things Magazine*, December 2019, pp 26-30.
58. <http://www.opengroup.org/iot/iotwp/p4.htm>

Edited by Paul Wesling