ARM

White paper

The route to a trillion devices

The outlook for IoT investment to 2035

Philip Sparks

June 2017

Introduction

Technology vendors like to talk about data being big, really big. Petabytes of storage; gigabits of bandwidth; megaflops of processing power.

But data doesn't have to be big to be valuable. One of the most successful financial trades of all time was premised on a piece of information that could have been represented by a single bit (1 or 0).

On June 19 1815, the bond market in London was in chaos. Traders had heard rumours that Napoleon had triumphed at the Battle of Waterloo, and the British government would be unable to repay their debts. One banker, Nathan Rothschild, knew better. He operated an international network of loyal messengers, and his trusted sources informed him that Napoleon had lost. Rothschild used this binary data to inform his investment strategy – he bought all the mispriced bonds he could, netting handsome profits when the bond market eventually recovered.

Thanks to the Internet of Things (IoT), intelligence networks are no longer exclusive to the aristocracy. Today all organisations can collect information about almost anything, anywhere, and in real time.

Many companies have already deployed IoT systems to glean new insights about their customers, supply chains and operations. They are using that information to increase revenues, cut waste and hone investment decisions.

IoT technology is becoming more affordable every day, driven by innovations in semiconductor technology, cloud computing, and mobile connectivity. This trend of cost reduction is driving exponential growth in the number of opportunities for companies to profit from IoT.

ARM believes that we are entering a new era of computing. We expect that a trillion new IoT devices will be produced between now and 2035.

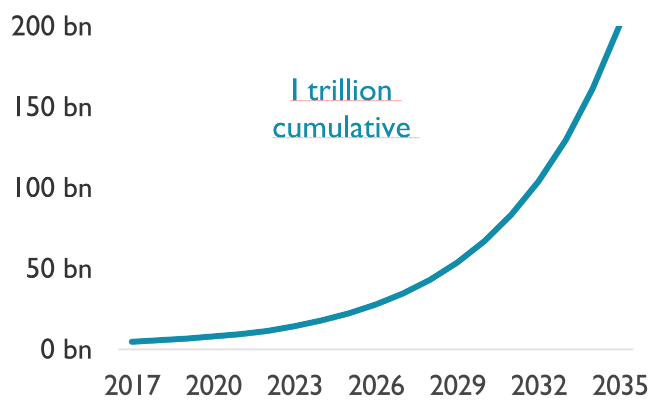
Some of these devices will provide years of service, monitoring valuable infrastructure and transmitting data over long-distances. Some will operate for a brief time only, recording data from disposable items such as smart healthcare bandages and asset tracking tags.

In every case, the build out of the IoT system will be driven by a straightforward profit incentive: systems will be deployed when the value of the information collected exceeds the cost of collecting it.

In this paper we examine the macroeconomics of IoT. We start by introducing the concept of the information profit margin, and how it drives deployment of IoT systems. Then we look at the potential for IoT to boost economic output.

After comparing the financial gains available from IoT with the cost roadmap for IoT systems, we reach our conclusion: by the year 2035, spending on IoT hardware and services will reach a trillion dollars per annum. This level of investment supports our view that a trillion IoT devices will be produced within the next twenty years.

Annual Production of IoT devices



Source: SoftBank and ARM estimates

"When historians look back at the latter half of the 1990s a decade or two hence, I suspect that they will conclude we are now living through a pivotal period in American economic history.

"New technologies that evolved from the cumulative innovations of the past half-century have now begun to bring about dramatic changes in the way goods and services are produced and in the way they are distributed to final users.

"Those innovations, exemplified most recently by the multiplying uses of the Internet, have brought on a flood of start-up firms, many of which claim to offer the chance to revolutionize and dominate large shares of the nation's production and distribution system."

Alan Greenspan, Chairman of the Federal Reserve
Boston College Conference on the New Economy, March 2000

"In the next twenty years, a trillion IoT devices are coming… We are on the brink of an information revolution that will redefine all industries."

Masayoshi Son, Chairman and CEO of SoftBank
ARM TechCon, October 2016

The information profit margin

The messengers of the early 1800s were the telecommunication networks of their day, and they had many features in common with modern data services.

Public postal services were slow (*low bandwidth*), unreliable (*dropped packets*) and served only major cities (*limited coverage*). Frustrated by these limitations, the Rothschild family hired private couriers (*a proprietary network*) who pledged that their messages would be relayed quickly and accurately (*a service level agreement*). Letters were written in abbreviated code (*compressed, encrypted*), sealed with the family coat of arms (*authenticated*), and carried by pigeons to reduce transit time (*latency*).

The Rothschild's network was expensive to run, but the investment was easily justified by the rewards on offer. In other words, it had a positive *information profit margin:* the value of data collected by the network was greater than the cost of collecting it.

The quest for a positive information profit margin has driven the deployment of data networks ever since.

Before the phrase 'Internet of Things' took hold, autonomous data collection systems were described using terms such as telematics, remote monitoring or machine-to-machine communications. Early systems, developed in the 1990s, were bespoke, proprietary and costly. GE and Rolls-Royce invested millions in systems that recorded data from jet engines while they were in flight. Formula One teams introduced radio telemetry systems to monitor the performance of their cars as they raced around a track. In the early noughties, the Mayor of London embarked on a £250m project to automatically identify and invoice every driver entering the city's congestion zone at peak hours.

Over the last twenty years, the cost of compute and connectivity has fallen dramatically. The entry cost of an ARM-based chip has come down from ten dollars to ten cents[1], and telecoms companies have built wireless data networks with ubiquitous coverage and consumer-friendly pricing.

As a result, the remote monitoring technology that first appeared in jet engines for airliners (list price: $10m; annual production: <1,000) will soon be fitted as standard in petrol engines for family cars (list price: $2,000; annual production: >80m).

The value of information

Information is not only becoming cheaper to collect; it is becoming more valuable to own. The latest developments in artificial intelligence and machine learning have enabled us to look deeper into the vast pools of data stored in servers across the world, and researchers are uncovering new insights from previously disparate and unwieldy datasets.

Medical diagnosis, crime prevention, pharmaceutical development and traffic planning are some of the many fields currently benefitting from advances in data science.

Thanks to machine learning, data does not follow the usual rules of diminishing returns: the more we collect, the more valuable it becomes.

To a company, the value of information can be quantified by assessing its impact on profitability:

- How much additional revenue can I generate from the information?
- How much cost can I save using this information?
- How much can improve profitability by using the data to make better decisions?

Companies can use information to increase revenue by adding value to their products (e.g. personalising insurance premiums), by creating new business streams (e.g. selling predictive maintenance services), or by enhancing customer loyalty. They can reduce costs by eliminating waste, managing supply chains, and utilising their assets more efficiently. They can make better decisions by ascertaining facts and reducing uncertainty.

[1] Based on ARM royalty reports from Q1 1997 and Q1 2017

The potential for technology to improve corporate efficiency is so profound that it has become a hot topic among sociologists and journalists. Commentators use phrases such as 'artificial intelligence' and 'automation' to evoke images of a dystopian future, where humans have been replaced by machines. But this pessimistic view is based on a one-sided analysis; the commentator focuses solely on job roles that exist today, ignoring the fact that new roles will be created as companies use technology to evolve and improve their operations.

When companies become more efficient, they open-up new opportunities to invest, to expand and to employ more people. This was evident in the 1990s, when the US economy enjoyed a long period of strong growth, full employment and low inflation. In March 2000, Alan Greenspan, then Chairman of the Federal Reserve, attributed this increase in productivity to the widescale adoption of Internet technologies:

"Since 1995, output per hour in the nonfinancial corporate sector has increased at an average annual rate of 3.5%, nearly double the average pace over the preceding quarter-century.

Until the mid-1990s, the billions of dollars that businesses had poured into information technology seemed to leave little imprint on the overall economy. The full value of computing power could be realized only after ways had been devised to link computers into large-scale networks. As we all know, that day has arrived.

Before this quantum jump in information availability, most business decisions were hampered by a fog of uncertainty. Businesses had limited and lagging knowledge of customers' needs and of the location of inventories… Decisions were made from information that was hours, days, or even weeks old.

But information has become vastly more available in real time… This surge in the availability of more timely information has enabled business management to remove large swaths of inventory safety stocks and worker inefficiencies. Stated differently, fewer goods and worker hours are now involved in activities that, although perceived as necessary insurance to sustain valued output, in the end produced nothing of value."

In the last two decades, the Internet transformed our ability to access data saved on remote computers. In the next two decades, the Internet of Things will transform our ability to *capture* data from the world around us.

Just as the Internet boosted US productivity by ~3% as it reached critical mass in the 1990s, ARM believes the Internet of Things will boost global economic output by at least 3% by 2035, by which time IoT systems will be deployed on a massive scale.

Potential output boost attributable to IoT

Sector	* Sector value-add (% of GDP)	** Potential output boost from IoT	Areas where IoT can improve productivity
Food Production and Distribution	2	+5%	Food waste reduction, water/fertiliser/pesticide reduction, yield increase
Heavy Industries**	8	+3%	Energy savings, enhanced safety, preventative maintenance
Manufacturing	12	+5%	Throughput increase, preventative maintenance, after-market revenues
Wholesale and Retail	12	+5%	Targeted advertising, inventory management, supply-chain management
Transport and Logistics	3	+5%	Fleet management, asset utilisation, fuel savings, paperwork elimination
Finance and Insurance	7	+3%	Risk measurement, hassle-free payments, real-time commodities tracking
Real Estate Rentals	13	+1%	Energy savings, tenant comfort
Professional Services	12	~0%	
Health care and social assistance	7	+5%	Preventative medicine, drug research, home care, patient monitoring
Telecoms, Media and IT Services	5	+2%	Targeted advertising, energy savings, customer relations
Leisure and other services	5	+3%	Targeted advertising, ticketing, yield management
Government, education and defence	14	+3%	Traffic monitoring, crime prevention, pollution control, waste management
Total	100	+3%	

* Source: U.S. Bureau of Economic Analysis
** Source: ARM estimates
*** Extractive Industries, Energy Production, Construction and Utilities

Based on OECD forecasts, a 3% boost to GDP could equate to $5 trillion of additional output in 2035.

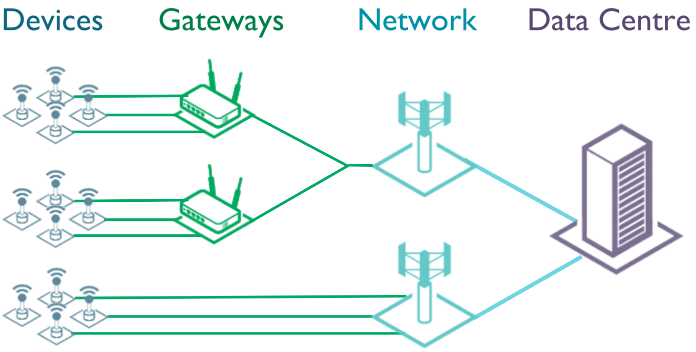
The cost of information

IoT systems

IoT systems collect information, analyse it and act upon it. They consist of *devices* (aka ‘things’, or ‘endpoints’) that collect information and/or are controlled by the system; *networks* that transport data around the system; and *data centers* that store and process information gathered by the system.

A key characteristic of IoT systems is that the collection of information is autonomous – data is generated and analysed with minimal human interaction. Some systems collect data purely for analytical purposes, they pass their output to humans who use it to inform decisions. Other systems use data to take automated actions, e.g. charging a customer, switching a traffic signal, turning on a water sprinkler.

Simplified schematic of an IoT system



Source: ARM

IoT modules

Every IoT device contains a module of electronics that performs the following functions:

- Data collection. Modules can use sensors (temperature, movement, light, etc) to collect information about their surroundings, or they can collect data via their interaction with other devices in the system. A contactless travel card, for example, generates information about the owner's location when the user taps the card on ticket barriers at the start of a journey.
- Data processing. IoT modules perform several functions that are controlled by microprocessors and software. As a minimum, a module must collect information and manage a communications protocol. Most modules will run software to manage device wake time, analyse sensor signals and encrypt data, some may also have a human user interface, e.g. a thermostat.
- Data communication. IoT devices need to access a data network, and in many cases, the most convenient solution is a radio. Many radio standards are suitable for IoT, and the optimal choice for a particular module will depend on the amount of data being transmitted, the required range and whether the user is willing to pay access charges for licensed spectrum. For some applications, wired connections such as ethernet-over-powerline may be appropriate.
- Power. Modules need access to an energy source with sufficient power to drive the all the electronic components described above. This could be a battery, a mains connection, or an energy harvesting device with on-board energy storage (e.g. a solar cell and a capacitor)

Every IoT application has its own requirement for data collection, processing and connectivity. Device designers have a wide choice of sensors, controllers, radios and power supplies, and will seek components that meet the specification at minimum cost.

Specification of IoT components

Function	Specification			
	Minimal	Low	Medium	High
Data collection	The device uses proximity radio to sense the presence of other devices, e.g. a contactless travelcard passing through a ticket barrier, or a smartphone detecting a nearby beacon	The device has a single analogue sensor chip (temperature, pressure, light, etc).	Multiple sensors	HD camera
Data processing	A single ARM Cortex-M0 microprocessor that handles sensor data and communications	Separate ARM Cortex-M0 processors for sense, control and comms	An ARM Cortex-A applications processor	An ARM Cortex-A applications processor with on-board vision processing
Data communication	Near-field radio such as NFC or RFID	Bluetooth, Zigbee, NB-IOT	WiFi, LTE-M	LTE
Power supply	No dedicated power supply, either because the module uses RF energy harvesting, or because the host device has its own power source, e.g. a light bulb, a thermostat	Small solar cell with capacitor	Coin cell battery	Mains electricity

The chart below depicts an approximate Bill of Materials for a typical configuration for IoT modules, split into six categories (see the appendix for a description of each).

The cost of a module will depend on the complexity of the data being collected and the amount of data being transmitted back to the network. These parameters influence the choice of processor, amount of memory, and the power of the radio transmitter, and the specification of all these components determines the size and cost of the power supply.

Over the next twenty years we expect to see chip designers and module makers focus on cost-reduction technologies for IoT, e.g. single-chip solutions for data collection, processing and connectivity; new techniques for assembling and packaging modules, including printed electronics; energy-harvesting power supplies designed specifically for IoT applications.

The combination of these cost-reduction efforts could see the cost of IoT modules fall by two-thirds, helping production to grow from billions of units a year in 2017 to hundreds of billions by 2035.

Cost roadmap for IoT modules

Module type *	Power supply	Connectivity	Bill of materials (BOM) for a basic** IOT module	
			2017	2035
Smart Tag	RF energy harvesting	NFC or RFID	$0.40	$0.15
Smart Sensor	Solar cell, coin cell battery	Unlicensed radio or LPWAN	$4.00	$1.50
Smart Camera	Mains electricity	WiFi, LTE or ethernet	$8.00	$3.00
IoT Beacon	Solar cell, coin-cell battery	Unlicensed radio †	$3.00	$1.00
IoT Receiver	Solar cell, coin-cell battery	Unlicensed radio or LPWAN ‡	$3.00	$1.00
IoT Gateway	Mains electricity	Unlicensed radio + internet access	$8.00	$3.00

Source: 2017 BOM: ARM estimates based on Octopart catalogue prices and ARM royalty reports. 2035 BOM: ARM estimates

* See Appendix for detailed description of each module type

** 'Basic' means a minimal configuration which is sufficient for most applications. For high performance applications, designers have the option to add more memory, larger power suppliers, additional processing power, etc.

† Bluetooth, WiFi, Zigbee

‡ Low Power Wide Area Network, e.g. NB-IoT, LoRa, Sigfox

The whole life cost of IoT systems

The price of the IoT modules is only a part of the overall cost of an IoT system. The modules have to be fitted into devices, devices are shipped to the end-user, the end-user must install the devices on-site. Once the devices are in situ, they must be connected to a data network and configured to communicate securely with the system's data centers. The information passed to the data centre will be processed by software running on servers, and the results stored on hard disk drives.

The split between upfront hardware costs and ongoing service costs varies from one system to another. In particular, the proportion of costs devoted to installation is extremely variable, ranging from almost 0% (e.g. IoT modules soldered into white goods during manufacture) to almost 100% (e.g. seismic sensors concreted onto a volcano).

Even though the cost of IoT modules is set to fall by around 65% between now and 2035, we expect the relative split of services and hardware costs will be stable over time, thanks to cost reduction trends in all aspects of IoT systems.

The cost of telecoms connectivity is coming down thanks to investment in networks and new standards such as 5G and NB-IoT; the cost of data centre hosting is coming down thanks to Moore's Law and new generations of ARM-based server chips; and the cost of managing large IoT systems is coming down thanks to advances in data science and new platforms for device management (e.g. ARM mbed Cloud).

The table below shows ARM's estimate of how overall spending on IoT systems could be distributed in 2035.

Distribution of spending on IoT systems in 2035

IoT Services 65%	IT services	45%	Systems integration (design, procurement, project management) Data centre hosting (renting out servers and storage space) Device lifecycle management (provisioning, updating, decommissioning) Analytics software (sold under software-as-a-service contracts)
	Telecoms services	15%	Carrier networks (mobile, wireline) Internet Service Providers
	Financial services	5%	Financing; payments processing
IoT Hardware 35%	Installation	10%	Installing devices on-site
	Distribution	5%	Transporting components to assemblers, devices to end users
	Assembly	5%	Assembling components into modules, modules into devices
	Components	15%	Semiconductor chips, analog components, circuit boards

Source: ARM estimates

The route to a trillion devices

On page five, we estimated that the deployment of IoT technologies could add 3% to global GDP by 2035. This could equate to $5 trillion of additional output (2017 prices). To what extent will this value creation drive investment in IoT systems?

Today, companies spend on IoT when the financial case for doing so is obvious. With IoT systems in their infancy, there are still many easy wins available, where the cost of a suitable IoT system is small compared to the financial benefit it accrues.

As companies become more familiar with IoT technology and its capabilities, they will be willing to pursue opportunities with a narrower profit margin; for example, a retailer may be willing to spend $1m pa on a smart beacon system that boosts gross profit by $5m pa, an information profit margin of 5x. This, we believe, is a reasonable estimate for the average information profit margin accrued by IoT systems in 2035.

With that 5x figure in mind, if the deployment of IoT systems yields productivity gains worth five trillion dollars pa by 2035, the gains would support a total available market ($TAM) for IoT technology of one trillion dollars per annum.

Annual spend on IoT systems in 2035

Service / Component	2035 $TAM
IT services	$450 bn
Telecoms services	$150 bn
Financial services	$50 bn
Installation services	$100 bn
Distribution services	$50 bn
Assembly services	$50 bn
Digital electronic components *	$100 bn
Other electronic components**	$50 bn
Total	**$1000 bn**

Source: ARM estimates

* *Microcontrollers, apps processors, radio controllers, memory*
** *Sensors, batteries, solar cells, antennae, circuit boards, etc*

The table above gives an estimate for the 2035 $TAM for IoT components: $150 bn. Combining this with the growth trajectory shown on page 1, we find that the cumulative spend on IoT components between 2017 and 2035 could reach $750 bn.

We can use this number to test the feasibility of our vision of a trillion IoT devices being produced between 2017 and 2035. If the $750bn spend on components were spread over a trillion devices, the average bill of materials per device would be $0.75.

Referring to the BOM cost projections on page 7, the $0.75 figure suggests that the world can indeed afford a trillion IoT devices. This assumes that our three other estimates are reasonable: widescale IoT deployments boost global GDP by 3% by 2035, the cost of IoT modules falls by ~65% between 2017 and 2035, and IoT systems yield an economic benefit (on average) which is 5x greater than their cost.

As an illustration, the mix of modules shown below has an average BOM of $0.75, based on the cost projections shown on page seven.

The next trillion IoT modules – potential mix

Module type	Potential production 2017 to 2035
Smart Tag	500 bn
Smart Sensor	250 bn
Smart Camera	10 bn
IoT Beacon	100 bn
IoT Receiver	120 bn
IoT Gateway	20 bn
Total	**1000 bn**

Source: ARM estimates

ARM ecosystem: our journey to a trillion

The route to a trillion devices will follow a path of cost reduction, and ARM is enabling IoT providers to develop large-scale systems at affordable prices. From sensors to servers to services, ARM technology touches all aspects of IoT hardware and software.

- Chip vendors. ARM's Cortex-M processors provide low cost compute, ease of programming and Trustzone security, and can be combined with ARM Cordio connectivity IP in cost-optimised single-chip solutions for IoT devices. For richer IoT devices such as industrial controllers and smart cameras, ARM's Cortex-A processors and visual computing accelerators enable sophisticated system-on-chips that cost less than $2
- Device OEMs. IoT will redefine all industries, and every manufacturer will become a tech company. The ecosystem of ARM-based chip vendors provides OEMs with an abundance of innovative silicon designs, all using a common software platform. ARM's mbed developer platform enables start-ups to create new IoT products in a matter of days, and OEMs to add IoT features to their products with minimal effort.
- Systems integrators. Building out a secure IoT system can be a daunting undertaking, and once the system is in place, the systems integrator has an ongoing responsibility to keep it safe from increasingly sophisticated cyber attacks. This means providing regular security patches to vast numbers of little devices which connected intermittently to low bandwidth networks. ARM's mbed Cloud device management takes care of device provisioning and firmware updates so that systems integrators can concentrate their development efforts on features that differentiate their offering.

Conclusion

In the late 1990s, Alan Greenspan noted that an information revolution was having a significant impact on economic growth. In the two decades that followed, the internet completely transformed the way humans communicate. Today more than two billion people have a smartphone in their pocket that can access messaging, browsing and location-based services; these technologies barely existed seventeen years ago – now we can barely remember what life was like without them.

The coming two decades will see another phase of this information revolution. The next wave of transformation will be driven by the Internet of Things, and technologies that are nascent today will become so widely adopted that we will barely notice them. Consumers will consider it normal that the cost of their car insurance depends on how well they drive, that their car alerts the local mechanic when a part is about to fail, and that street lights dim when their road is empty.

By 2035, the technology companies that sell IoT hardware and services could be serving a market worth a trillion dollars per annum. That is an exciting figure, but an even greater value will flow to the companies that utilize the information collected by those systems, and to the consumers who will benefit from widespread efficiency gains across the economy.

Further reading

The Rothschild intelligence network

Alan Greenspan's speech: 'The revolution in information technology', March 2000

Acknowledgements

The author would like to thank the following colleagues who were consulted during the research of this report:

- Diya Soubra, Senior Product Manager, IoT (Cost roadmap for IoT modules)
- James Myers, Principal Research Engineer (Cost roadmap for printed electronic modules)
- Rob Aitken, ARM Fellow and Director of Technology (Cost roadmap for IoT power supplies)
- David Maidment, Director of Product Strategy (Definition of 'IoT Device')
- Steve Steele, Director Product Marketing, Imaging and Vision Group (Definition of 'Smart Camera')

Appendix: IoT module types

Smart tag

RFID tags have been around for decades. Passive tags harvest radio energy from a reader device. With no onboard power supply, they are extremely cheap and able to remain in service indefinitely. Tags have limited radio range - a few centimetres for passive tags, a few metres for tags with a battery.

The most basic form of tag does nothing more than transmit a unique ID number to any scanner that comes within a few metres. Advanced tags have sufficient compute performance to implement security protocols; these are commonly found in applications that use sensitive data, such as e-passports and payment cards.

Tags become 'IoT devices' when they are used to generate data for analysis in real time. The most common application is tracking assets as they move through a factory, warehouse or the supply chain. When tags are used alongside sensors and data loggers (e.g. to monitor the temperature history of frozen food as it is transported to a supermarket) they become a form of smart sensor (see below).

By 2035, we may find that smart tags are printed rather than assembled. It is possible to produce processors, radios and batteries using a printing processes, and researchers are working hard to commercialise printed IoT modules. If these efforts succeeed, the cost of a smart tag could eventually fall to a few cents.

Smart sensor

A smart sensor is the archetypal IoT device: it monitors its immediate environment and transmits information to a data centre for further analysis. Sensors contain an analog chip for reading 'real world' information, e.g. temperature, pressure, movement; the analog signals are converted into digital data by a microcontroller chip.

For some little data applications (e.g. 'the room is occupied', 'the temperature is 26° C'), a microcontroller chip with a single Cortex-M processor can manage the sensor and the radio. For anything more complex, the module will require separate processors for sensor control, communications and data analysis. For example, a wearable health monitor might contain: (1) a Cortex-M microcontroller to digitise signals generated by a heartbeat sensor; (2) a Cortex-M processor to control a Bluetooth radio; and (3) a Cortex-A processor that analyses heartbeats and runs a user interface.

Smart sensors can be standalone units (e.g. a vibration sensors installed on a bridge), or they can be integrated into other devices at the point of manufacture (e.g. a light switch that can sense if a room is unoccupied). Standalone sensors typically use coin cell batteries or solar cells for their power source; integrated sensors are powered by their host device.

Designers of smart sensors have a wide range of connectivity options. They can use unlicensed spectrum (WiFi, Bluetooth, Zigbee, etc) to communicate with IoT gateways (see below), or they can communicate directly with mobile networks (GSM, LTE-M, NB-IOT).

Sending large amounts of data to remote data centres has implications for the cost of the device power supply and fees for network access. Designers can minimise data transmissions by performing some data analysis on the device itself. For example, the health monitor described above can minimise data transfers by contacting the data centre only when its on-board signal processor detects an anomalous heartbeat.

Smart camera

The latest advances in visual compute technology means that cameras with built-in intelligence are increasingly being used as IoT sensors. Smart cameras are being used to record the number plates of cars using toll roads, to perform quality checks on manufactured goods as they move through of production lines, and assist security staff monitoring crowded spaces.

For some use cases, the flexibility and capability of a smart camera justifies its relatively high cost. For example, a car park operator could monitor whether individual parking spaces are occupied by (1): installing a proximity sensor in every one of its parking spaces, or (2) installing a single camera that monitors all parking spaces at once.

IoT Beacon

Like IoT tags, IoT beacons generate information via their interactions with other devices in the system. A beacon repeatedly broadcasts a small piece of information, e.g. a unique ID or a web address. If a compatible device moves close enough to the beacon to receive the message, an automated action occurs.

Applications include asset tracking, location-based advertising and mobile payments. At MWC 2017, ARM and IBM demonstrated a payment system enabled by a beacon in a parking meter – when a smartphone was placed close the meter, the phone's browser connected to the parking operator's website, and enabled the phone owner to make a quick payment for that meter.

As beacons do not contain sensors, their IoT module is essentially a short-range connectivity chip with a power supply (typically a coin cell battery or solar cell).

IoT Receiver

Many IoT systems include devices that are controlled by the system: e.g. automated garden sprinklers that turn on/off according to the weather forecast, smart street lights that dim or brighten according to live traffic data, e-ink shopping labels that display prices updated daily.

If the controlled device provides no information to the system other than its state (e.g. the sprinkler is switched on/ the sprinkler is switched off), the requirements for its IoT module are similar to those of beacon: basic connectivity only. The main difference is that an IoT receiver could use a long-range radio, e.g. NB-IOT.

IoT Gateway

IoT devices that communicate using unlicensed radio spectrum (e.g. Bluetooth, WiFi, Zigbee) connect to the internet via gateway devices. A gateway operates two or more communication protocols, enabling data to flow from one network to another.

The most familiar example of a gateway is a home router. This uses WiFi radio and ethernet cables to communicate with multiple devices around the home, and a modem (cable or ASDL) to communicate with the homeowner's broadband service provider. Similarly, a smartphone can act as a gateway, using Bluetooth and NFC radios to interact with IoT devices close to the phone, and an LTE radio to communicate with the phone-owner's mobile service provider.

Example IoT gateways

Tag reader

Source: Zebra

Smartphone

Source: Fitbit

WiFi router

Source: Linksys

Satellite transceiver

Source: OneWeb

Trademarks