# Digital Innovation Project

## Buckinghamshire County Council
## Association of Directors of Environment, Economy, Planning and Transport (ADEPT)

by

**Prof. Mischa Dohler**

**Director, Centre for Telecomms Research**
**Fellow, IEEE & Royal Society of Arts**
**King's College London**

# Executive Abstract

This report gives an in-depth summary on latest (but not all) digital approaches which could be beneficial to Buckinghamshire. It also contains a list of recommendations and best working practices in the light of the available digital tools. The most important are summarized here:

- **From Asset Monitoring to Predictive Maintenance**: Using below-summarize digital technologies, arguably the biggest opportunities lie with the digitization of the Buckinghamshire assets. Installing sensors and actuators on these assets, allows one to gather data about the assets at a temporal and spatial granularity not seen before. This, in turn, allows one building trends on their use and exhaustion. Used properly, these techniques can be very powerful to optimize the maintenance cycles. Imagine a bridge: instead of doing maintenance too early or too late, the work can be conducted when truly needed.
- **Digitizing the Buckinghamshire Workforce & Processes**: Another huge potential is in completely digitizing the workforce and the processes being done at the moment. In itself a huge undertaking, it promises to save costs mid to long term. Cloud technologies are an important enabler here, and so are drone technologies.
- **Breaking Procurement Barriers**: Digital, and in particular the Internet of Things (IoT), can help to break down procurement barriers and make the entire process much smarter. Traditionally, a city hall would set out the tender with minimum consultation and the company which meets all KPIs and is cheapest wins. This however is a recipe for failure as a) companies have little time to adapt to the true needs of the city; and b) the cheapest minimum solution may not be the best long-term. Using digital, an early engagement can be guaranteed and procurement itself can be made a much “smarter” process.
- **Real-Time Interaction with Citizens**: An interesting opportunity of digital, and particularly the Internet of Things, is that one is able to engage with the customer/citizens in real-time well after sales/installation of assets. For instance, British Gas has a smart home solution called Hive which is a smart thermostat. The smart phone app which is used to control the thermostat also includes a feedback section where customers are able to provide feedback and ideas on next products. These are then ranked among the customers and British Gas only has to execute the top one to satisfy its customers. A similar principle can be used to engage with citizens in Buckinghamshire.
- **Building an Open Data & API Eco-System**: And finally, if all of above digital approaches are accessible to third parties, then a service economy can be built on top. This requires data to be made open; and suitable APIs to be created. The opening of the data of course has to obey national privacy and security directives.

# Table of Contents

Executive Abstract 1
Table of Contents 2
List of Figures & Tables 4
Acronyms & Abbreviations 5
1. Introduction to Digital Transformation 6
1.1. Digital Revolution 6
1.2. Digital Infrastructure – Internet, Store & Compute, Things 6
1.3. Digital Insights – Big Data Analytics 7
1.4. Digital Services – Open APIs & Apps 7
1.5. Digital Black Swan Events – Security and Privacy 8
1.6. Structure of this Report 8
2. Introduction to the Internet of Things (IoT) 9
2.1. IoT Technology Challenges 9
2.2. IoT Market Challenges 10
3. Sensors, Actuators & Drones 13
3.1. Recent Market Take-Off 13
3.2. Sensing Technologies 15
3.3. Actuators, Robots & Drones 17
4. Wireless Connectivity Infrastructure 20
4.1. Techno-Economic Approach 20
4.2. Pros & Cons of Connectivity Families 21
4.2.1. Emerging LPWAN Technologies 21
4.2.2. Cellular IoT Technologies 23
4.2.3. Comparison of Technologies 26
5. Cloud and Platform Infrastructures 27
5.1. Private Server versus Cloud Infrastructure 27
5.2. Cloud Exchange Architectures 29
5.3. Digital Data Analytics 34
5.4. Data Privacy Regulations 35
6. Important Digital Standards and Alliances 40

6.1. Standards Development Organizations (SDOs) ........ 40
6.2. Industry Associations & Special Interest Groups (SIG) ........ 42
7. Application to Buckinghamshire ........ 45
7.1. From Asset Monitoring to Predictive Maintenance ........ 45
7.2. Digitizing the Buckinghamshire Workforce & Processes ........ 45
7.3. Breaking Procurement Barriers ........ 45
7.4. Real-Time Interaction with Citizens ........ 46
7.5. Building an Open Data & API Eco-System ........ 46
Bibliography ........ 47

# List of Figures & Tables

***Figure 1:*** *Estimates in the "trillion sensor vision" projection by [28].* 12
***Figure 2:*** *Improvements in accuracy of GPS for outdoor and global tracking [© GPS.gov].* 14
***Figure 3:*** *Power consumption versus processes data rate for radio tech (orange) and microcontrollers (blue) [1].* 15
***Figure 4:*** *Component and system composition of a typical connected IoT device [© Aeris].* 17
***Figure 5:*** *Force versus stroke range capabilities of various actuator families [25].* 18
***Figure 6:*** *Industrial-niche robot (DaVinci robotic surgery, left) and consumer-grade humanoid robot (Toshiba humanoid, right).* 19
***Figure 7:*** *Market segmentation for drones and robots [© Yole].* 19
***Figure 8:*** *Qualitative assessment of the ability to meet the availability and reliability criteria of the various IoT technologies discussed.* 26
***Figure 9:*** *Example reference platform architectures meeting the outlined requirements.* 28
***Figure 10:*** *The three possible cloud data sharing models: device-to-cloud model (top); device-to-gateway-to-cloud model (middle); and back-end data sharing model (bottom).* 30

***Table 1:*** *Main organizations and specific working groups in the M2M arena.* 44

# Acronyms & Abbreviations

| | |
|---|---|
| ACL | Access Control Lists |
| AI | Artificial Intelligence |
| B2B | Business-to-Business |
| B2C | Business-to-Consumer |
| CAPEX | Capital Expenditure |
| CxO | Chief x Executive |
| GDPR | General Data Protection Regulation |
| GPS | Global Positioning System |
| GSM | Global System for Mobile communications |
| IC | Integrated Circuits |
| IoT | Internet of Things |
| ISP | Internet Service Provider |
| LPWAN | Low-Power Wide Area Network |
| LTE | Long-Term Evolution |
| NB-IoT | Narrow-Band IoT |
| NEMS | Nano-Electro-Mechanical Systems |
| OPEX | Operational Expenditure |
| RF | Radio Frequency |
| SEMI | Semiconductor |
| SLA | Service Level Agreement |
| TCO | Total Cost of Ownership |

# 1. Introduction to Digital Transformation

## 1.1. Digital Revolution

Digital is a relatively modern development but arguably the one which has changed humanity most profoundly. What started as a business market (remember the first IBM mainframes) quickly turned into consumer market (Microsoft, etc) and now is back to transforming entire industries.

Digitization of documents/files/emails/etc facilitated their instant transmission across the Globe, and thereby increased effectiveness and efficiency of processes in industries. The transmission is facilitated by the Internet, and processing of the data by powerful cloud processing/storage facilities. Novel concepts such as Big Data and data science appeared which essentially deal with the crunching of large and/or heterogeneous sets of data, and building unique insights from that. But arguably the biggest value add of digital are all the services which now run on top of above infrastructure.

This report delivers a high level horizon scan on developments in digital and how they impact today's physical world.

## 1.2. Digital Infrastructure – Internet, Store & Compute, Things

Each Internet generation was believed to be the last, with designs pushed to near perfection. The first and original Internet, a virtually infinite network of computers, was a paradigm changer and went on to define the economies of the late 20th century. However, after that Internet came the Mobile Internet, connecting billions of smart phones and laptops, and yet again redefining entire segments of the economy in the first decade of the 21st century. Today, we witness the emergence of the Internet of Things (IoT), shortly to connect trillions of objects and starting to redefine yet again various economies of this decade. And currently we at the Centre for Telecommunications Research at King's College London are designing the next-generation internet, the Internet of Skills[1].

The next big step was to be able to handle the gigantic data volumes. Computing powers have increased significantly over past years; and so have storage capabilities. In fact, technology has advanced so rapidly that both store & compute have become commodity and are assumed to be a natural ingredient in any digital infrastructure deployment.

[1] Mischa Dohler, et al, "Internet of Skills, Where Robotics Meets AI, 5G and the Tactile Internet," EuCNC 2017.

The latest emerging ingredient in the digital infrastructure is the world of connected Things, referred to as the Internet of Things. Not yet fully deployed, it will play an instrumental part in delivering data insights at a spatial and temporal granularity not seen before. It includes paradigms such as sensors, actuators, drones and UAVs.

## 1.3. Digital Insights – Big Data Analytics

Data analytics algorithms is what gives the gathered data some "life". It is this real-time information, knowledge and wisdom we can extract from the data which makes digital so powerful.

Data analytics algorithms vary significantly in capabilities and scope. There are algorithms which find us the known knowns; then there are algorithms which are able to extract the known unknowns; and as of very recent there are algorithms which are even able to extract the unknown unknowns from our data sets. More on that below in this report.

## 1.4. Digital Services – Open APIs & Apps

Using above infrastructure and analytics, services are being offered. Examples are Google, Facebook, Emails, etc. Whilst most was web-based and company-owned in the past, there is an interesting trend towards an app and open application protocol interface (API) "culture".

The open API approach refers to a paradigm where interfaces (the APIs) into a closed system are being made available so that 3rd-parties can use the system without requiring the source code of the system. This allows one to decouple business processes and generally scale economies.

A prominent example is TFL: They gather and process the travel times & locations of all their assets (buses, trains, etc) and make this information available in real-time through open APIs so 3rd party developers can use the data and offer services on top. Google is thus using the data, and so is London's CityMapper.

Of course issues around licensing agreements are core to these APIs but too advanced to discuss in this report in great details.

## 1.5. Digital Black Swan Events – Security and Privacy

The two most important black-swan events in digital relate to security and privacy. In terms of security, there are two big risks one ought to be aware of:

The first is poor engineering, i.e. the human responsible for the system design fails to deliver a properly secured systems (by e.g. forgetting to encrypt one part of the system); this happens surprisingly often and we are likely to see more of such failures in the emerging Internet of Things.

The second is quantum! Our entire security ecosystem relies on the inability to factor any number into two prime numbers. Traditional computers take millions of years to break this brute force using Monte Carlo trials. Quantum, however, changes that paradigm. Once quantum computers become operational, and they will in a not-so-distant future, any of our traditional security cyphers will be easily broken. We are confident, we will find a “patch” even though it may look a little more sophisticated for these type of emerging attacks. We are also sure we will all be able to replace/upgrade all of our laptops and mobile phones, mainly because we do this anyway every year or so. What might however be a real problem is anybody fixing the billions of IoT devices which were meant to be out there for several decades. These are the same devices which control, for instance, the city’s traffic lights, the pace maker’s rhythm, the car’s brake, or the nuclear power plant’s fuel levels.

With security compromised, privacy becomes a huge problem as very private data is potentially exposed and we have had incidents in the past corroborating this threat. Therefore, mechanisms need to be put in place ensuring the security is sound and privacy can be guaranteed even if a system has been compromised.

## 1.6. Structure of this Report

To give a meaningful input to the strategic planning of the Buckinghamshire Digital Innovation Project, the report is structured as follows. After the introduction of Section 1, there follows an in-depth coverage of the Internet of Things in Section 2 which pertains to technology and market challenges. Section 3 then deals with sensors/actuators, and market dynamics. In Section 4, the wireless connectivity infrastructure is discussed in some details. Cloud and platform infrastructure approaches are discussed in Section 5; this section also includes a truly important exposure on data privacy regulations. In Section 6, I discuss the most important digital standards and alliances. And, finally, in Section 7, I hint on how all of that can be used in the context of Buckinghamshire.

# 2. Introduction to the Internet of Things (IoT)

The technology which will change industries most profoundly is the one of the emerging Internet of Things (IoT). We thus dedicate a separate section to introduce the technology, and it will be the main thread throughout the entire document.

## 2.1. IoT Technology Challenges

The IoT has not yet taken off, despite decades of design, standardization and production. There are thus still issues remaining which are discussed here. The first relates to “inter” in the name inter-net of things, the second to “net” and the third to “things”. In reverse order:

- **Things** (in Internet of Things): It is worth highlighting the transformation the Internet has undergone. Not even 20 years ago, the Internet experience was all about laying Ethernet cables through buildings and dorms and installing routers; oh, yes, there was also Netscape somewhere for browsing but it came secondary. Zoom forward to today and ask anybody in the street what the Internet means to them. The answer will be simple: Snapchat, Twitter, Facebook, Amazon. That is, the Internet has undergone an amazing transformation from being infrastructure-driven to opportunity and service-driven.

The IoT has still to undergo that very same transformation as indeed most conversations and sales exercises around the IoT gravitate around the actual “things”, the sensors, the connectivity, etc., but little about the value the solution yields. We thus need a substantial transformation to take place from a "things"-driven mindset to a service/opportunity-driven mindset. Suppliers shouldn’t come into a sales meeting with an IoT “box”; and clients ought to terminate/divert discussions with clients who bring their IoT “box”. The cost of these “things” and “boxes” has dropped sufficiently now, allowing to focus on the value of IoT.

- **Net** (in Internet of Things): When it comes to networking and connecting the IoT devices, we struggle. Wireless is the obvious choice but the technologies put forward to date (GSM, then Zigbee) have not materialised the promised exponential growth of the IoT. We are now in the (possibly hype) phase of Low Power Wide Area Networks (LPWANs). It is paramount to understand some pros and cons of the most important of these technologies:

*Sigfox* runs an operator model and uses great tech, which works today, at a reasonable cost, and gives no headache during rollouts. On the downside, the company Sigfox is a single point of failure in case it runs into cashflow problems and has to close; furthermore, the spectrum used is heavily regulated in terms of transmission power (impacts mainly downlink range), duty cycle (impacts number of packets per day), license-exempt usage for all (impacting interference and spectrum congestion) and the prohibition to offer service license agreements (SLAs) over that spectrum (impacting business opportunities, insurance, etc.).

*Lora* suggests a vendor model offering proven technology which is open for further developments, sells at a reasonable cost, and is supported by a wide ecosystem. On the downside, it uses the same spectrum as Sigfox and therefore suffers the same problems; another issue is that rollout is typically project driven which means that full national/international coverage is a very long away and the data usage may become very fragmented.

*Narrowband-IoT/NB-IoT* is promoted by the cellular operator industry. It enjoys a massive and proven eco-system, is easy to upgrade at global scale, has no usage headache, offers SLA capabilities, has an equal up and downlink, and enjoys a wide availability of spectrum. On the downside, the power consumptions of the radio chips are not yet at the level of Sigfox/Lora; and the business model for the operators is not clear yet either.

In summary, we have a few novel technology families emerging as of 2015/2016 and they may just be the key to unlocking the networking problems we experienced in the past.

- **Inter** (in Internet of Things): Arguably the most important point is that the IoT has not yet made the transformation from today's Intranet of Things to a true Internet of Things. We urgently need mechanisms in place which enable such a transition to an IoT where data is shared globally and horizontally across sectors, where "things" are discoverable and IoT data searchable.

## 2.2. IoT Market Challenges

Above-cited problems with the technology are of course not the only reason for the IoT Big Bang not to occur (yet). Another truly important factor is the interplay between demand and supply. In the context of the IoT, this translate to the following:

- **Supply-Side Bias:** There is a very strong supply-side bias in IoT which implies that not only is the market flooded with an endless array of sensors, radios, platforms, analytics and services but – more importantly – the vision of what this Internet of Things should really be/deliver/enable is heavily influenced/biased by that supply-side eco-system. The advantage is that solutions generally are operational as the technology is readily available; on the downside, it often misses the guiding principles of a true Internet of Things as discussed above.

- **Demand-Side Absence/Silos:** Given the nascence of the IoT, with very few proven deployments at scale, demand remains consistently low. This is in-line with typical up-take behaviour of technology and correlates with Gartner's hype cycle. In addition, the very few demand-side driven projects (such as smart parking in Barcelona), are silo'ed in that data is not shared freely with anybody but the company running the solutions; it thus defeats the very nature what an Internet should be about. However, demand will eventually pick up and I feel that a few more years (see subsequent Sections) are needed to see exponential growth.

Above demand-supply relationship really regulates the market. It is important to note however that demand should not be confused with need. There is clearly a massive need for IoT solutions, corroborated by many business models in any vertical of interest; that, however, does not mean that the technology will be procured, deployed and used.

The discrepancy between supply and demand is further amplified by the fact that it takes today roughly 48h to come up with a good IoT prototype, simply because of the very advanced state of open prototyping, open codes and 3D printing. Inexperienced startup founders who are typically at the helm of an IoT company believe that above-described need together with the quickly prototyped solution is sufficient to scale-up an IoT company. A few months (if lucky some 3 years) later, when the VC cash runs out, they understand that the demand-side sales cycles are orders of magnitude longer than the supply-side development cycles.

The biggest factor therefore for the Internet of Things to succeed is to create or enable the creation of demand. And whilst technology at scale is important to ensure that the IoT is cheap, scales and is sufficiently reliable, it is really the business side which needs to ensure that the IoT is less cost but more value driven. In other words, a CxO of a company ought to understand the value of the IoT solution first before even starting to talk about costs.

The IoT, however will take off as corroborated by predictions shown in **Figure 1**.

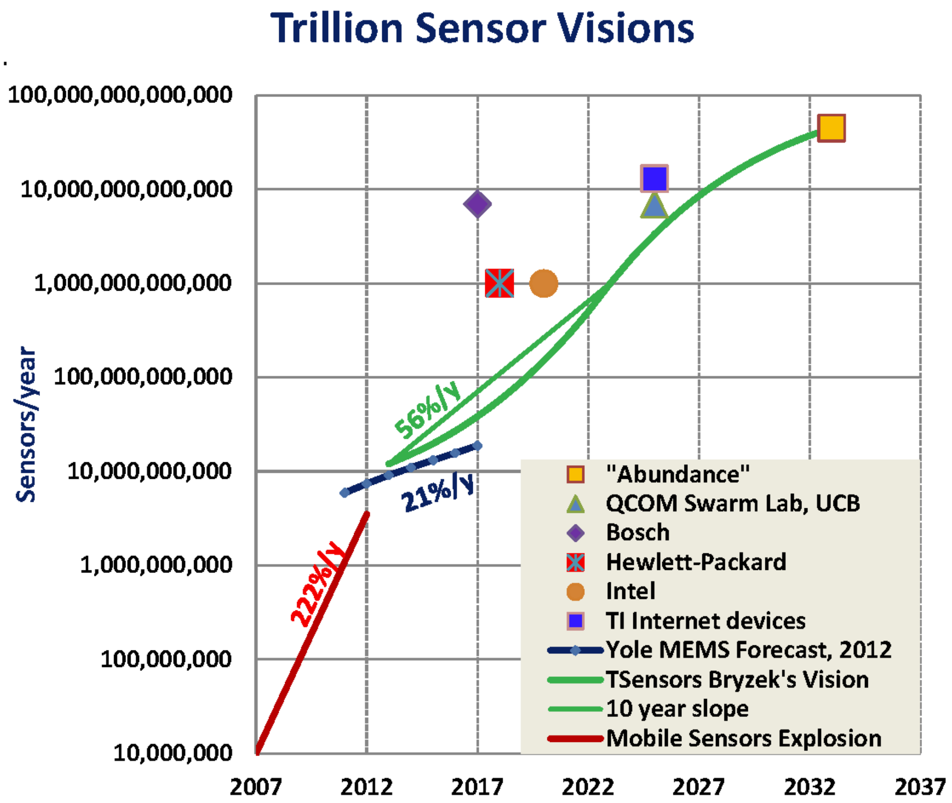


**Figure 1:** Estimates in the "trillion sensor vision" projection by [28].

# 3. Sensors, Actuators & Drones

The physical end-devices in the digital ecosystem are starting to play a more prominent role due to their ability to be connected to the Internet. We will thus revisit some of the fundamental design drivers in this section.

## 3.1. Recent Market Take-Off

The catalyst for the significant growth is for the following three reasons:

1. **Miniaturisation**: Significant advances in research and innovation have ensured that devices have shrunk in physical dimensions. The biggest disruption here was the commercial introduction of Micro-Electro-Mechanical Systems (MEMS), a technology which was more than 50 years in making ever since its discovery by Bell Labs, US. Smaller sensors excited demand, and thereby higher sales volumes and easier batch manufacturing.

2. **Diminishing Cost**: Due to larger volumes and other factors, costs of sensors have fallen over past years; in average the cost has halved every 10 years. This, in turn, has spurned demand, increased sales and allowed for further cost reductions over the years.

3. **Reduced Power Consumption**: In parts due to the smaller designs, the power consumption of the sensors has fallen significantly. This, in turn, allowed the usage of batteries rather than tethered power supply, and introduced a prior unprecedented flexibility in use and deployment.

Whilst above three trends have truly catalysed the growth of sensing technologies, there are two other trends which have had a positive impact on the ecosystem:

4. **Improved Power Storage Capabilities**: Batteries and energy capacitors have improved over the years, mainly in energy storage density, reduction in leaking currents and improvement in charging capabilities. This allowed the introduction of smaller batteries/capacitors and/or longer deployment times. In recent years,

energy harvesting capabilities have also improved, increasing the likelihood that battery-less IoT solutions are on the near-term horizon.

5. **Improved Location Capabilities**: The ability to locate end-devices is paramount to an increasing amount of applications. Devices connected through near-field communications are easily located through the location of the associated basestation/access point. However, outdoors solutions rely on GPS technology which have become more accurate over the years. Illustrated in **Figure 2**, technological accuracy is now well below 1m. Note that the consumer market does not fully profit from these improvements, mainly because the US military heavily regulates released GPS precision. Also note that the lower ceiling in resolution has already been reached; terrestrial-assisted technologies are being used to enhance location precision further.

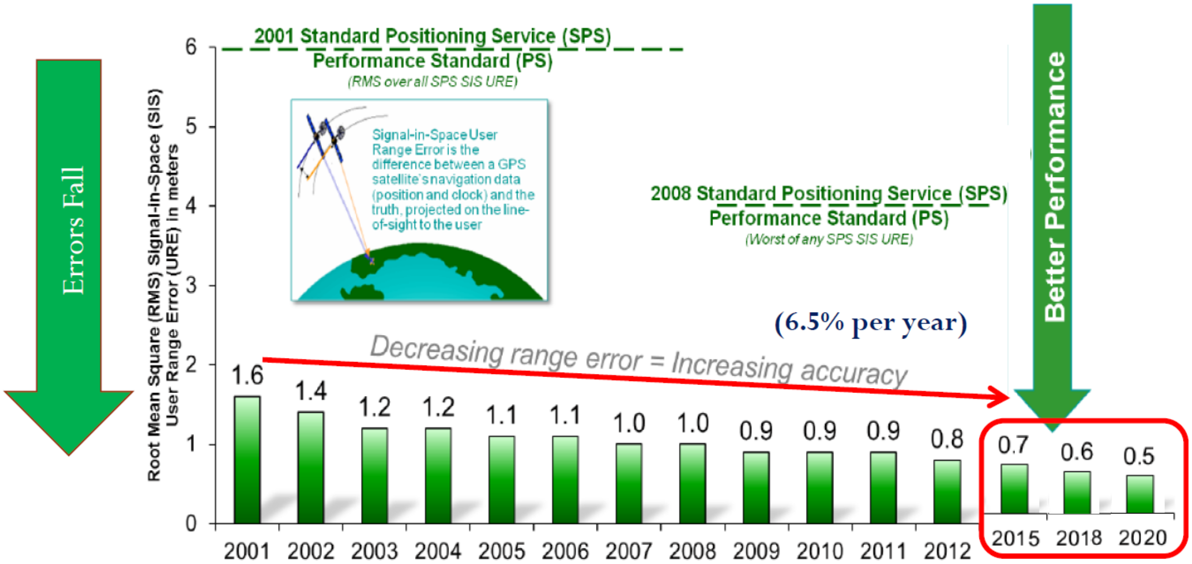


**Figure 2:** Improvements in accuracy of GPS for outdoor and global tracking [© GPS.gov].

Regarding the diminishing power consumption, as per **Figure 3**, there is a direct correlation of data processing requirements in bits/s and the consumed power by the underlying silicon. The rule of thumb suggests an order increase in rate requires an order increase in power consumption. Furthermore, at any given rate, the power consumption of the radio technology is an order of magnitude higher than the processing power. Since the end device is generally expected to underpin low-rate applications, the power consumption is generally low where microcontrollers already consume in the order of 100uW and radios around 1mW.

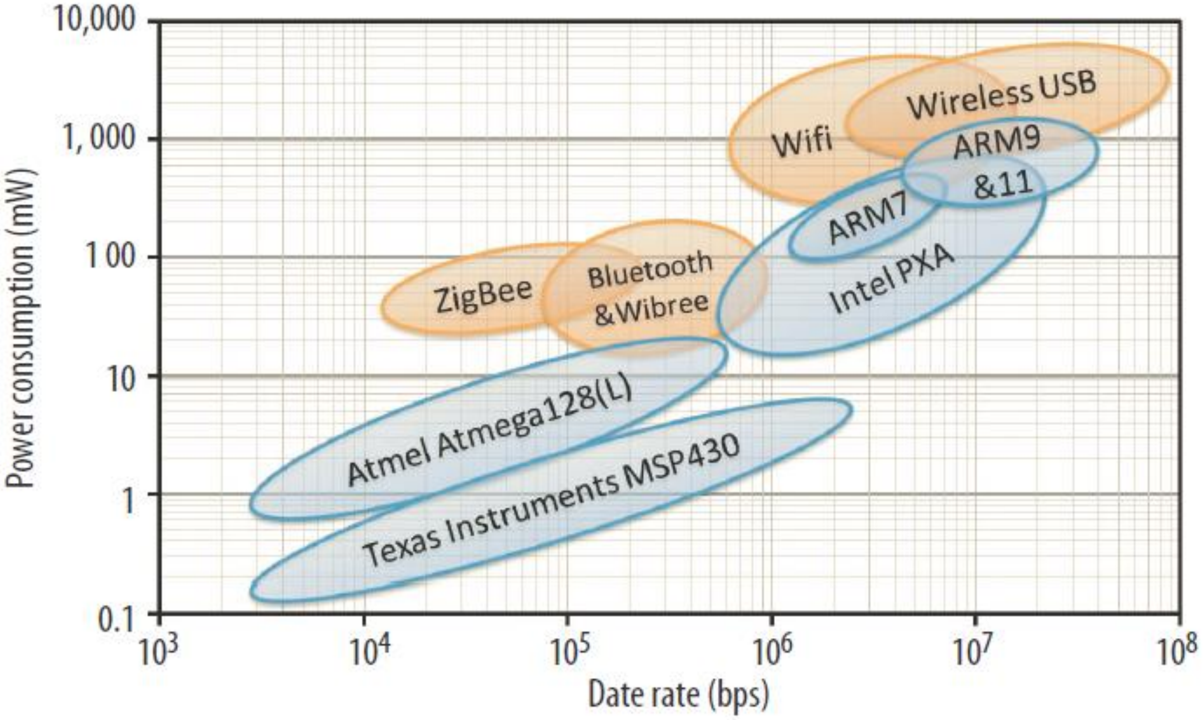


**Figure 3:** Power consumption versus processes data rate for radio tech (orange) and microcontrollers (blue) [1].

## 3.2. Sensing Technologies

Sensors have been used for more than a century. Accordingly, the field is not only well established but also offers an enormous variety of sensor types and applications. An example list of sensors can be found under [22], and an example list of companies manufacturing them can be found under [23].

Sensors act as transducers which convert a natural/physical value, such as pressure or chemical composition, into an electrical one which can be processed by computers. Several sensor taxonomies are in use today [22], such as active vs passive sensors; classification based on properties; and classification as per application family:

- **Classification based on power requirements:** Sensors can be split into active versus passive sensors which has an important impact on energy consumption:

  - *Active Sensor*: They require constant or intermittent power supply; example: photoconductive cells.
  - *Passive Sensor*: They do not require power supply and function either without power at all or are powered by the sensing process or are powered by the sensing electronics reading the values; example: film photography.

- **Classification based on sensing properties:** Given the wide array of sensing properties, we only quickly review the most important ones:
  - *Acceleration:* gyroscopes, accelerometers, etc.
  - *Pressure*: fibre optic, vacuum, elastic liquid based manometers, electronics.
  - *Proximity/displacement:* photoelectric, capacitive, magnetic, ultrasonic, etc.
  - *Level Sensors:* differential pressure, ultrasonic radio frequency, radar, etc.
  - *Temperature*: thermistors, thermocouples, integrated circuits, etc.
  - *Image:* charge coupled devices, CMOS, etc
  - *Flow*: electromagnetic, differential pressure, positional displacement, etc.
  - *Gas and chemical:* semiconductor, infrared, conductance, electrochemical.
  - *Biosensors: r*esonant mirror, electrochemical, etc.
  - *many other sensor properties:* see e.g. [22].

- **Classification based on markets:** The large majority of the sensor technologies addresses two market groups:
  - *Specialised Niche:* A comparably small number of sensors is used in high-value and high revenue markets, such as medical or heavy structural sensors. They solve very specific needs but generally do not scale.
  - *Consumer-Grade Markets:* The vast majority of sensors deployed today globally is used in the context of consumers, i.e. either B2C or B2B2C. Note that many of the niche-sensor technologies have scaled into B2C markets because of advances in manufacturing.

In practice, an engineer would determine the specific choice of sensor based on a set of criteria. Typical criteria are: i) accuracy; ii) operational resistance to environmental conditions; iii) measurement range; iv) calibration capabilities and requirements; v) resolution of measurements; vi) the total cost of ownership (including calibration efforts, etc); and vii) repeatability, i.e. how often the measurements can be taken.

The interplay of these components is exemplified in **Figure 4**. In there, a set of sensors is connected to an RF module, all of which is powered by a battery/energy harvester and controlled by power management circuits. The sensed data is then delivered wirelessly to the Internet, where it is then being transmitted to dedicated or cloud servers. Different services can then be offered, using the data and the insights generated from the data.

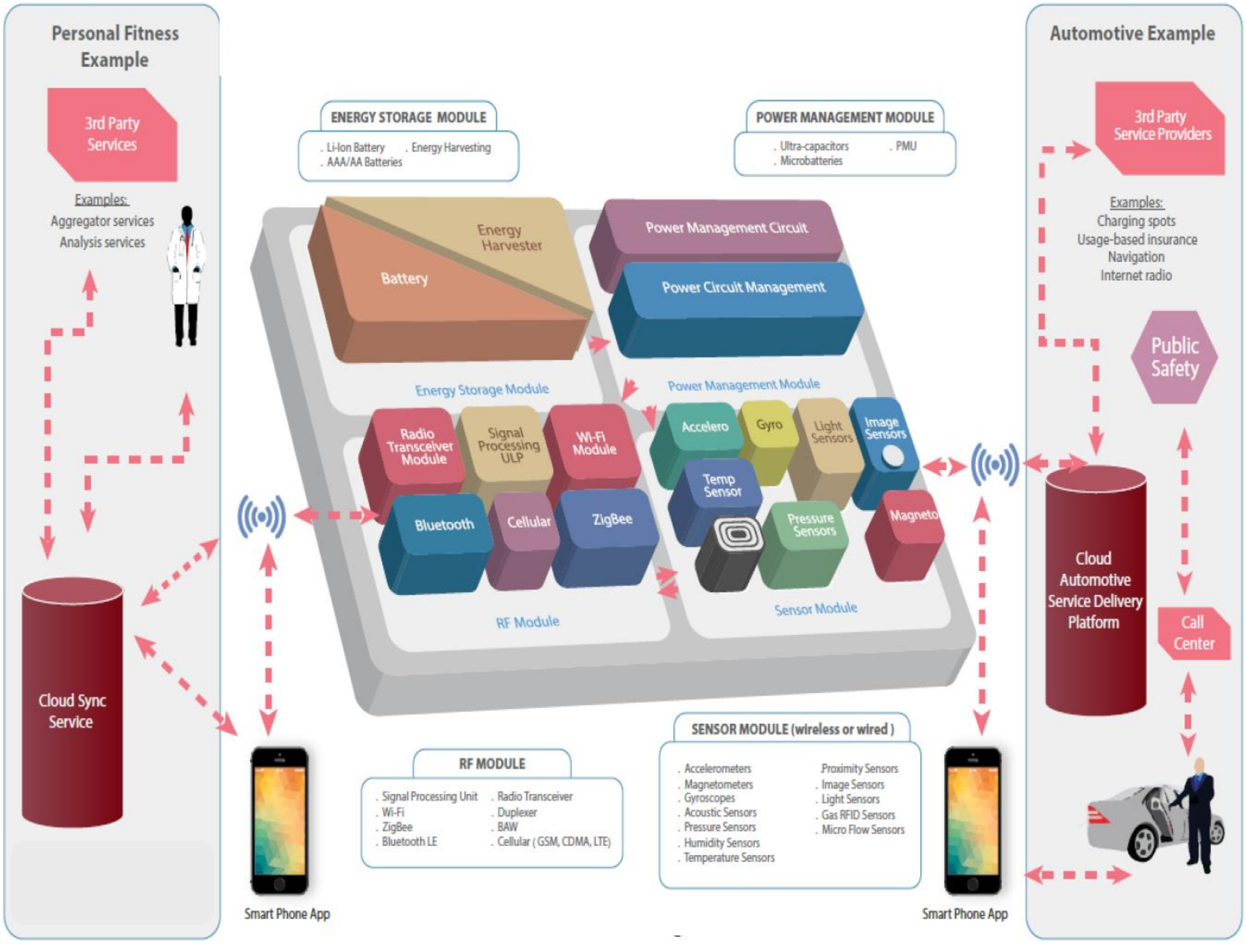


**Figure 4:** Component and system composition of a typical connected IoT device [© Aeris].

## 3.3. Actuators, Robots & Drones

An actuator is a mechanical device which takes input energy in the form of electric current, hydraulic fluid pressure or pneumatic pressure and converts it into a motion. For example, they are the part that takes the electric current in robotic arms and makes the robot move. The most frequently used actuation methods are enabled by hydraulic, pneumatic, electric, thermal and mechanical energies.

An important metric for actuators is the force versus stroke tradeoff; the former quantifies the mechanical force an actuator can impose and the latter quantifies the actuation boundaries in spatial dimensions. Exemplified in **Figure 5**, one observes a wide variety of actuator capabilities. Microscopic actuations can be exerted by devices in the lower-left quadrant; and macroscopic skill-like actuation in the upper-right quadrant.

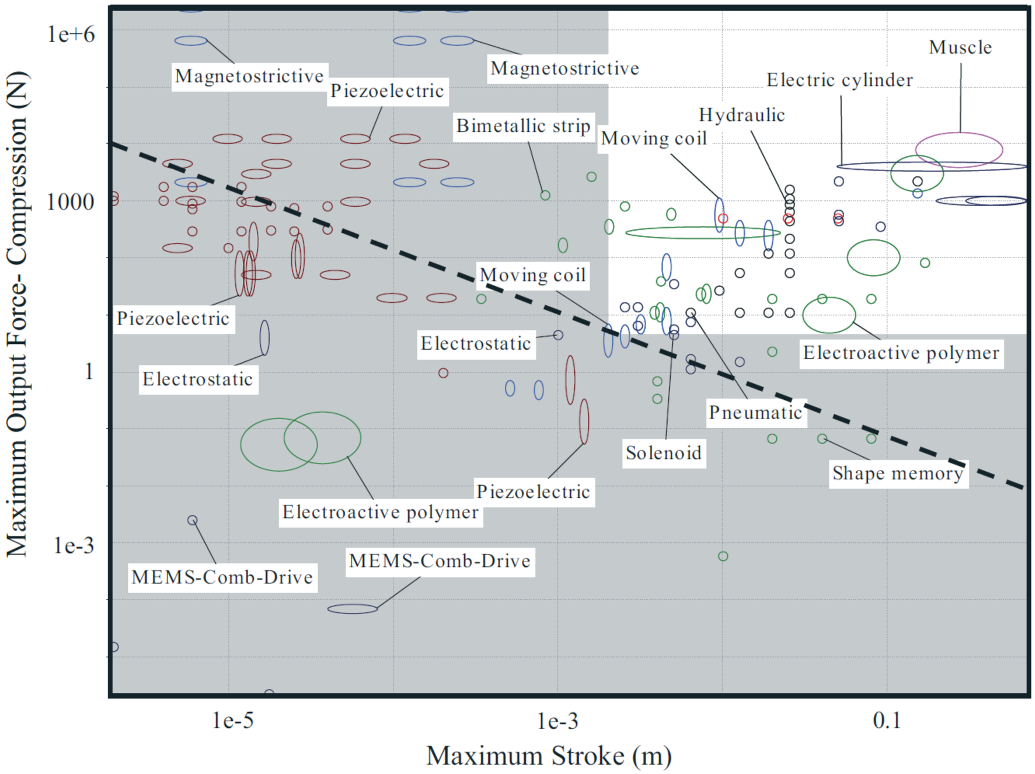


**Figure 5:** Force versus stroke range capabilities of various actuator families [25].

Actuators with a very large and mobile stroke capability are typically known as Robots. They can be autonomous or semi-autonomous; they range from consumer-driven humanoids to industrial robots and medical operating robots; see **Figure 6**. (The world of robots is also starting to expand into nano-robots; see subsequent section on MEMS and NEMS.) Robots are able to replicate a lifelike appearance with autonomous movements, and thus typically conveys a sense of intelligence or eigen-life.

**Figure 6:** Industrial-niche robot (DaVinci robotic surgery, left) and consumer-grade humanoid robot (Toshiba humanoid, right).

Robots lived a recent renaissance due to the massive advances in artificial intelligence (AI), thus giving them a much higher degree of autonomy. The improvements of mechanics and introduction of MEMS-actuation has further enhanced capabilities. Given these technology trends, the industrial robot market is experiencing significant growth and the consumer robot market is expected to pick up by 2025.

Drones are actuators with the largest actuation range; they are in essence flying robots and also known as unmanned aerial vehicles (UAVs). These UAVs may be remotely controlled or can fly autonomously through software-controlled flight plans in their embedded systems working in conjunction with GPS. UAVs have traditionally been associated with the military but they are increasingly entering industrial niche-markets and also consumer markets. An example segmentation for robots and drones can be found in **Figure 7**.

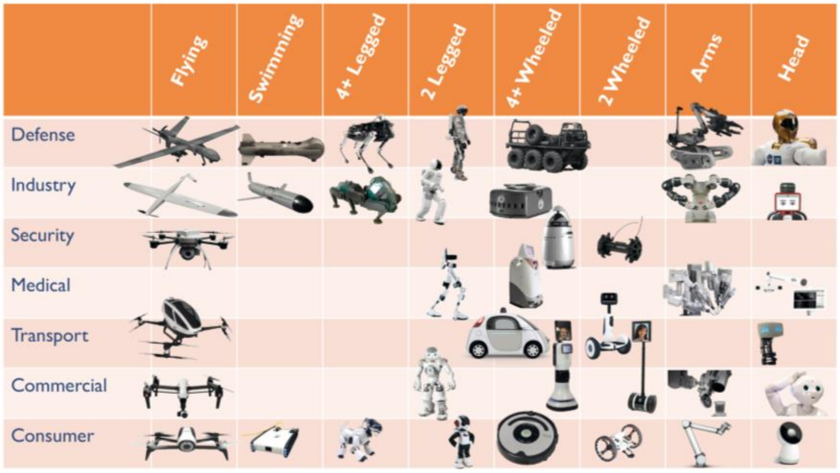


**Figure 7:** Market segmentation for drones and robots [© Yole].

# 4. Wireless Connectivity Infrastructure

## 4.1. Techno-Economic Approach

Technology, no matter how perfected and optimised, only becomes viable when certain techno-economic requirements are met. Said requirements are typically shaped and impacted by the market and surrounding conditions. Whilst the digital market is not yet fully formed, three core requirements seem to solidify:

- **Availability:** It refers to the ability of the technology to provide largest possible (if not global) coverage, accessibility, roaming and mobility support, and critical mass in rollout. In other words, the CEO of a digital asset company would choose the most available connectivity technology for which he/she has to worry least about connectivity no matter *where* the company deploys/sells. An example of a highly available technology is cellular.

- **Reliability:** It generally refers to the ability to provide resilience against interference, enables throughput guarantees, ensures low outages and provides high security. In other words, once the technology is deployed, the CEO would go for the one which operates most efficiently no matter *when* the company operates the network. An example of a highly reliable technology is the cable.

- **Total Cost of Ownership (TCO):** The total CAPEX and OPEX expenditures ought to be the lowest possible. TCO is clearly a function of availability and reliability as non-available technologies need to be deployed (high CAPEX) and non-reliable technologies need to be maintained (high OPEX). However, TCO also includes insurance which, in turn, relates to the legality of supporting service level agreements (SLAs). An example of a technology which legally prevents the issuing of SLAs in the UK is Sigfox.

Subsequently, we discuss the pros and cons of connectivity families which we deem most suitable to connect digital assets such as owned by Buckinghamshire.

## 4.2. Pros & Cons of Connectivity Families

### 4.2.1. Emerging LPWAN Technologies

a) Tech Overview:

Low-power wide area networking (LPWAN) technologies have recently emerged specifically focusing on low-end IoT applications which require low cost device, long battery life time, small amounts of data exchanged – an area for which traditional cellular M2M systems have not been optimised. The term LPWAN which was introduced by Machina Research to the market, stands for high reach, low cost, low power Wide Area Networks. The technology operates in license-exempt spectrum, and it is currently available in many different proprietary solutions (Amber Wireless, Coronis, LoRa, M2M Spectrum Networks, NWave, Ingenu (formerly On-Ramp Wireless), Senaptic, Sigfox, Weightless, etc). While most of these technologies have been present in the market for some time, it is Sigfox with its Network Operator strategy that has recently kick-started the LPWAN market, tightly followed by Lora's open Alliance approach and Ingenu's 2.4GHz-ISM technology strategy.

The key features of LPWANs can be summarized as follow: (i) wide area coverage (up to some tenths of km), (ii) low cost, (iii) long battery life (up to 10 years from a single AA battery), and (iv) low bandwidth communication. The latter limits the LPWAN range of applications to a reduced number of use cases characterised by low data rate, and infrequent transmissions (few hundred bytes of data).

b) Pros and Cons:

The advantages of LPWANs can be summarised as:

- **Key-Enabler**: They are expected to be a key enabler for IoT deployments in early market rollouts and for limited IoT applications, mainly since the major technology families such as LP-Wifi and cellular IoT are not fully operational yet.
- **Cost**: Available LPWAN technologies are very cost efficient today both from CAPEX as well as OPEX point of view, particularly when compared to the TCO of Zigbee and today's cellular solutions.

The disadvantages of LPWANs can be summarised as:

- **Mostly Proprietary Technologies**: Whilst some of the technologies are being standardised through ETSI Low Throughput Networks (LTN) and IEEE, none of these working group are globally important. Therefore, LPWAN technologies remain largely proprietary which limits the long-term deployment and use, and will likely make them not competitive on the long run (see below for more discussions).

- **Transmission Power Asymmetries**: The effective radiated power (ERP) in that part of the sub-GHz license-exempt band is heavily regulated in terms of allowed transmission powers (after antenna gain), duty cycles and access mechanisms. Since antennas at the basestation and at the IoT device have entirely different gain capabilities, the link capabilities in up and downlink are skewed with the uplink having a link budget advantage of up to 19dB. While European regulation allows for a boosted downlink power of 13dB, a difference of at least 6dB remains which means that truly symmetrical connectivity cannot be guaranteed. This means that simple operations, like sending an acknowledgement, cannot be executed seamlessly as in 3GPP technologies. Consequently, only a limited set of IoT applications can be supported through this technology.
- **Regulation on Duty Cycles**: There are regulations which limit the duty cycle, i.e. the frequency at which a device is allowed to transmit at a given power. This greatly limits the applications and services which can be supported. Sigfox, e.g. caps the number of messages allowed to be transmitted per day which prohibits the use of event-driven IoT applications or those with frequent readings.
- **Interference & Scalability**: Moreover, LPWANs cannot fulfil the scalability requirements of large-scale IoT deployments, due to an impeding spectrum congestion and access inefficiencies [Xavi paper]. According to predictions in this report, there will be billions of IoT devices connected to the Internet shortly. With such explosion of devices connected through IoT, millions of devices may appear within the coverage area of a single LPWAN base station. Many of those will be using other radio technologies that share the spectrum with LPWAN, such as LP-Wifi, Z-Wave, IEEE 802.15.4g, etc. All these transmission will be perceived as interference by the LPWAN device, having low receiver sensitivity for long-range communication.

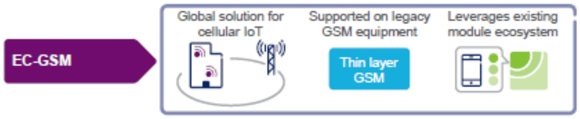
### 4.2.2. Cellular IoT Technologies

a) <u>Tech Overview:</u>

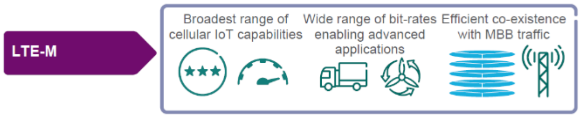
Since no single technology or solution is ideally suited to all the different potential IoT applications, market situations and spectrum availability, the mobile industry is standardising several LPWAN technologies, which have largely reduced to three technology families: 2G Extended Coverage GSM (EC-GSM), 4G LTE-M and 5G NB-IoT.

LTE-M, NB-IoT and EC-GSM are all superior solutions to meet IoT requirements as a family of solutions, and can complement each other based on technology availability, use case requirements and deployment scenarios. LTE-M consisting of category-Cat 1, Cat 0 and Cat M and supports a wide range of IoT applications, including those that are content-rich (i.e. high bandwidth); NB-IoT covers ultra-lowend IoT applications with a cost and coverage advantage over LTE-M; and EC-GSM serves IoT services for all (legacy) GSM markets.

For example, a logistics application may use EC-GSM technology to provide LPWAN connectivity in markets where it can be deployed on existing 2G networks; NB-IoT technology may be used for smart-metering applications with extreme coverage requirements in underground locations. On the other hand, e.g. smart city applications that need to support machine-to-machine (M2M) video traffic may use LTE-M.


EC-GSM
Global solution for cellular IoT
Supported on legacy GSM equipment
Thin layer GSM
Leverages existing module ecosystem

In more details regarding EC-GSM, 2G GSM is still the dominant mobile technology in many markets, and the vast majority of cellular M2M applications today use GPRS/EDGE for connectivity. GSM is likely to continue playing a key role in the IoT well into the future, due to its global coverage footprint, time to market and cost advantages. Recognising this – and identifying the requirements for (massive) IoT discussed earlier in introduction – an initiative was undertaken in 3GPP Release 13 to further improve GSM. The resulting EC-GSM functionality enables coverage improvements of up to 20dB with respect to GPRS on the 900MHz band. From an investment point of view, no new network carriers are required: new software on existing GSM networks is sufficient and provides combined capacity of up to 50,000 devices per cell on a single transceiver.


LTE-M
Broadest range of cellular IoT capabilities
Wide range of bit-rates enabling advanced applications
Efficient co-existence with MBB traffic

In more details regarding LTE-M, 4G LTE is the leading mobile broadband technology and its coverage is expanding rapidly. So far, the focus has been on meeting the huge demand for mobile data with highly capable devices that utilize new spectrum. The advent of LTE-M signifies an important step in addressing MTC capabilities over LTE: LTE-M brings new power-saving functionality suitable for serving a variety of IoT applications; indeed. Power Saving Mode and eDRX extend battery life for LTE-M to 10 years or more. LTE-M traffic is multiplexed over a full LTE carrier, and it is therefore able to tap into the full capacity of LTE. Additionally, new functionality for substantially reduced device cost and extended coverage for LTE-M are also specified within 3GPP.

NB-IoT
Scalable ultra-low-end cellular IoT solution
Ultra-low bit rates and extreme coverage
Native narrowband solution
In-band
LTE
200kHz

In more details regarding NB-IoT, this pre-5G technology has been standardised as part of 3GPP Release 13 [29]. NB-IoT is a self-contained carrier that can be deployed with a system bandwidth of only 200kHz, and is specifically tailored for ultra-low-end IoT applications. It is enabled using new network software on an existing LTE network, which will result in rapid time to market. NB-IoT provides lean setup procedures, and a capacity evaluation indicates that each 200kHz NB-IoT carrier can support more than 200,000 subscribers per basestation; this can further scaled up by adding multiple NB-IoT carriers when needed. NB-IoT also comes with an extended coverage of up to 20dB, and battery saving features, Power Saving Mode and eDRX for more than 10 years of battery life. NB-IoT is designed to be tightly integrated and interwork with LTE, which provides great deployment flexibility. The NB-IoT carrier can be deployed in the i) LTE guard band, ii) embedded within a normal LTE carrier, or iii) as a standalone carrier in, for example, GSM bands. NB-IoT reduces device complexity below that of LTE-M with the potential to rival module costs of unlicensed LPWAN technologies discussed above, and it will be ideal for addressing ultra-low-end applications in markets with a mature LTE installed base.

b) Pros and Cons:

The advantages of cellular IoT solutions can be summarised as:

- **Mature Eco-System**: The cellular mobile industry represents a huge and mature ecosystem, incorporating chipset, device and network equipment vendors, operators, application providers and many others. The global cellular ecosystem is governed by the 3GPP standardization forum, which guarantees broad industry support for future development.

- **Truly Global Coverage**: In terms of global reach, cellular networks already cover 90 percent of the world's population. LTE is catching up, but GSM will offer superior coverage in many markets for years to come. Cellular networks have been developed and deployed over three decades, and they will be around for the foreseeable future.
- **Scalability**: When it comes to scalability, cellular networks are built to handle massive volumes of mobile broadband traffic; the traffic from most IoT applications will be relatively small and easily absorbed. Operators are able to offer connectivity for IoT applications from the start-up phase and grow this business with low TCO and only limited additional investment and effort. Operation in licensed spectrum also provides predictable and controlled interference, which enables efficient use of the spectrum to support massive volumes of devices. Furthermore, the automated device management solutions used in cellular will enable true scalability.
- **QoS and SLA Support**: Quality of service (QoS) mechanisms will be essential for many IoT applications. Cellular systems have mature QoS functionality, and this enables critical MTC applications to be handled together with traffic from sensors, voice and mobile-broadband traffic on the same carrier. QoS, along with licensed spectrum as described above, provides a foundation for long-term Service Level Agreements (SLA) with a specific grade of service.

The disadvantages of cellular IoT solutions can be summarised as:

- **Cost**: Whilst the TCO is at par if not lower when compared to Zigbee and the likes, cellular cannot (yet) compete with LPWAN solutions offered today. Notably, radio modules are more expensive by a factor 3x-10x; and subscription is also more expensive by about the same ratios.
- **Energy Consumption**: The energy consumption of cellular is still not at par of LPWAN solutions, such as Sigfox and Lora. That means that solutions are unlikely to work on an AA battery for a decade; however, many (particularly industrial) IoT applications do not require such a long life-time and also often allow for larger batteries, such as industrial Saft D batteries.
- **Business Model(s)**: The biggest uncertainty is around the business model for cellular IoT in that the average return per unit (ARPU) is so low that supporting only

connectivity is not worth for the operators. For them to draw business opportunities, they need to capitalise on the data, horizontal platform and applications; however, their operations are not geared towards this.

### 4.2.3. Comparison of Technologies

With reference to the techno-economic requirements discussed above and illustrated in **Figure 8**, the introduced technologies fare as follows:

- **Availability**: Cellular is undoubtedly the most available technology in terms of coverage, roaming, mobility support, and critical mass in rollout. Since demand for IoT is not yet growing exponentially, this is closely followed by LPWAN technologies; however, once demand picks up, the gap between cellular and LPWANs will be large. LP-Wifi will also be available, once rolled out in in-doors setting. The availability of Zigbee and related technologies is very poor.
- **Reliability**: In terms of resilience against interference, throughput guarantees, outages and security, both cabled as well as cellular solutions are in pole position. This is followed by LPWAN and LP-Wifi technologies; and, again, reliability of Zigbee and related technologies is very poor.
- **Total Cost of Ownership (TCO)**: Not shown in the figure but exemplified above, the TCO of LPWAN and NB-IoT solutions is best, followed by all the other technologies.

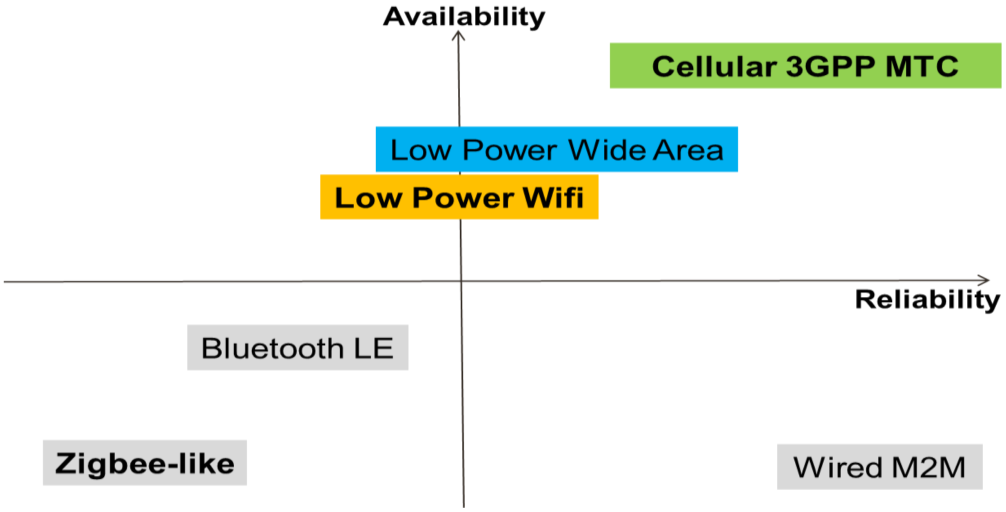


**Figure 8:** Qualitative assessment of the ability to meet the availability and reliability criteria of the various IoT technologies discussed.

# 5. Cloud and Platform Infrastructures

## 5.1. Private Server versus Cloud Infrastructure

To answer the question if data ought to be handled in a private server or a cloud, it is instrumental to understand the IoT data characteristics:

- **Volume:** Commercial IoT applications, particularly those at scale, capture and typically store most if not all of the sensor data. While a single sensor, e.g. a smart city parking sensor, may only generate some MB of data per year, the sheer number of sensors puts this quickly into the high PB range.

- **Variety**: There are many different data formats being used today. Some of that data is unstructured text, or binary and/or compressed textual formats, videos, audio traces, etc. None of this data is relational on its own, and a platform able to handle and, importantly, relate such data sets is instrumental for the success of the IoT.

- **Velocity**: Many IoT applications, particularly in industrial settings, requires a very high IoT data transmission rate. The ability to handle both infrequent as well as zero-delay IoT data streams is thus truly important to the success of the IoT.

Above characteristics thus translate into the following infrastructure requirements:

- **Raw data support**: In terms of data ingestion and processing, any platform should be able to natively deal with variety of IoT data. Solutions like Hadoop allow incoming data to be processed in any of its raw formats (such as JSON, log files, etc.). For subsequent optimisation, it then converts data to more sophisticated data formats such as Parquet.

- **Support for a variety of workload types:** IoT applications usually require that the platform can natively support stream processing, and that it can deal with low-latency queries against semi-structured data items, at scale.

- **Business continuity:** Commercial IoT applications usually come with SLAs in terms of availability, latency and disaster recovery metrics (Recovery Point

Objective/Recovery Time Objective). Hence, the platform should be able to guarantee those SLAs, innately. This is especially critical in the context of IoT applications in domains such as health care, where people's lives are at stake.

- **Security & Privacy:** Not surprisingly, any platform must ensure a secure end-to-end operation, including integration with existing authentication and authorisation systems in the enterprise such as LDAP or SAML. Equally importantly, user privacy must be warranted by the platform, from access control lists (ACLs) over data provenance support to data encryption and masking.

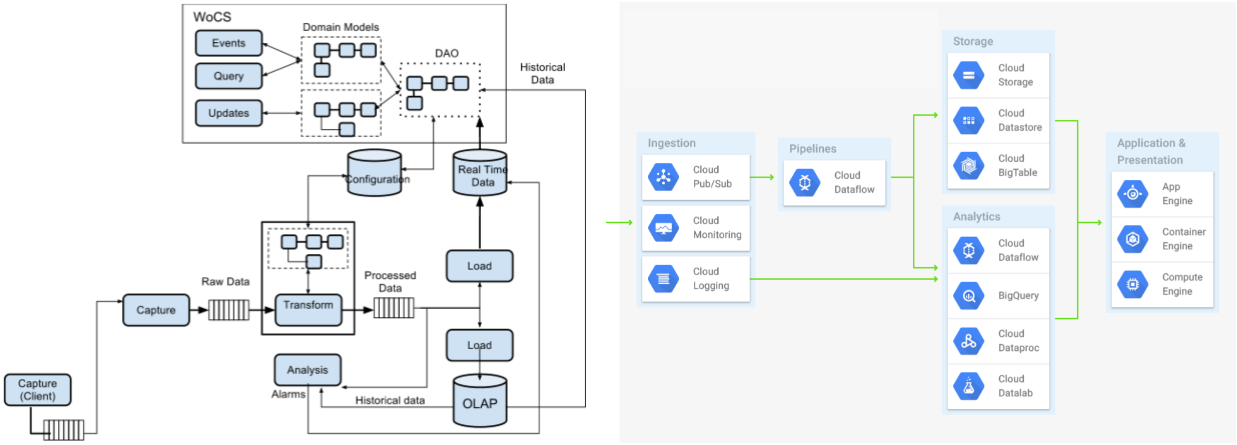


**Figure 9:** Example reference platform architectures meeting the outlined requirements.

Above requirements are met by example reference data architectures shown in **Figure 9**. The specific embodiment on the right is used by Google and on the left is being used by Worldsensing with building blocks being generic across most available platforms today. We at Worldsensing initially wrote most libraries from scratch and also hosted the solution at our company private servers; however, the solution would frequently freeze and it didn't scale to the millions of IoT readings hitting the platform per day.

Therefore, despite the pressure from some industrial clients to keep all on a local server, we migrated to cloud-based middleware application based on standard J2EE technologies able to support millions of data queries. In more details:

- **Sensor Network Management**: It allows for easy configuration of multiple types of sensors under a unified management interface; and its features are: plug & web, standard APIs, cloud-enabled, highly scalable (used e.g. by Google & Facebook).

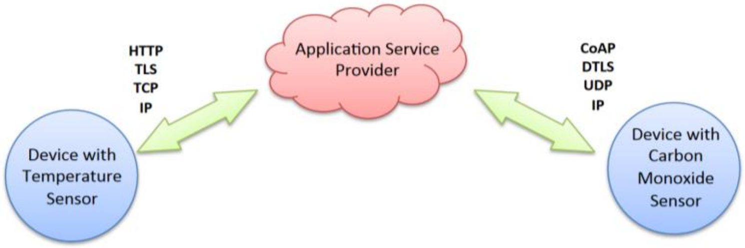
- **Sensor Data Processing**: It decouples data capture from data processing; and it is based on open tools developed and tested by large Internet services like Facebook and Yahoo to process millions of events a day.

- **Sensor Data Analysis**: It is a truly flexible model to capture business specific needs; it is highly scalable based on an optimised Online Analytical Processing (OLAP) infrastructure with standard interfaces like CVS & SQL queries which had been jointly developed with experts from IBM.

From above experience in Worldsensing and the challenges summarised in [31], one understands that designing and maintaining a viable, reliable and scalable IoT platform is a massive endeavour. **It is hence generally accepted now that digital ought to be provisioned in the** (public, private, edge and/or hybrid) **cloud, and not in private company servers.** The main drivers are flexibility, scalability, elasticity, security, robustness as well as CAPEX and OPEX costs.

## 5.2. Cloud Exchange Architectures

Illustrated in **Figure 10**, the resulting data exchange architectures are i) device-to-cloud model; ii) device-to-gateway-to-cloud model; and iii) back-end data sharing model [34].


HTTP
TLS
TCP
IP
Application Service Provider
CoAP
DTLS
UDP
IP
Device with Temperature Sensor
Device with Carbon Monoxide Sensor

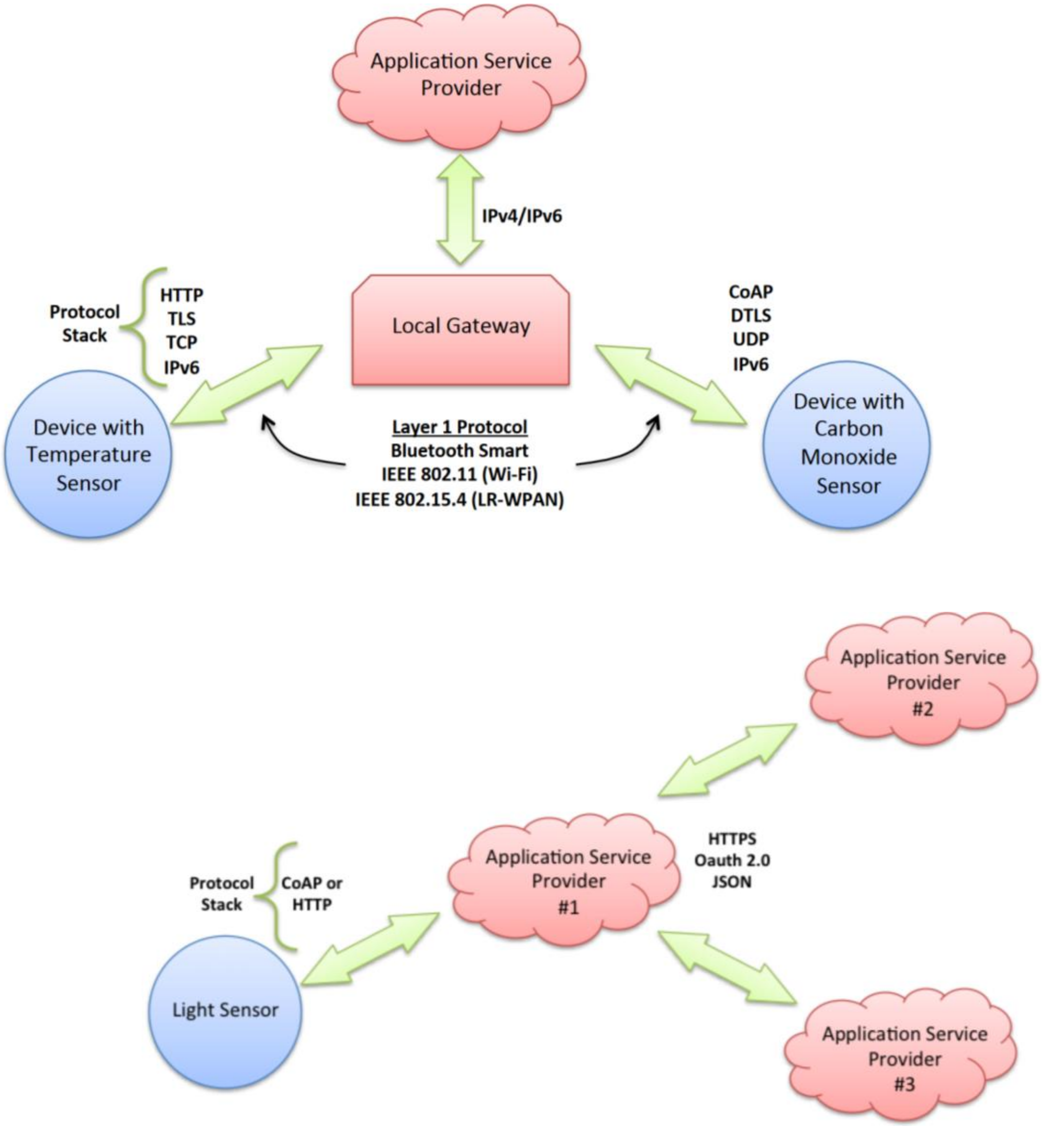


**Figure 10:** The three possible cloud data sharing models: device-to-cloud model (top); device-to-gateway-to-cloud model (middle); and back-end data sharing model (bottom).

- In a **device-to-cloud model**, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or WiFi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service.

  This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat and the Samsung SmartTV. In the case of the

Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyse home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or web interface, and it also supports software updates to the thermostat. Similarly with the Samsung SmartTV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV.

In these cases, the model adds value to the end user by extending the capabilities of the device beyond its native features. However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as “vendor lock-in’’, a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

- In the **device-to-gateway model**, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.

  Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they often rely on smartphone app software to serve as an intermediary gateway to connect the device to the cloud.

  The other form of this device-to-gateway model is the emergence of “hub” devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the SmartThings hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices. It then connects to the SmartThings cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection.

This communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. A downside of this approach is that the necessary development of the application-layer gateway software and system adds complexity and cost to the overall system. It is expected that in the future, more generic gateways will be deployed to lower cost and infrastructure complexity for end consumers, enterprises, and industrial environments. Such generic gateways are more likely to exist if IoT device designs make use of generic Internet protocols and not require application-layer gateways that translate one application-layer protocol to another one. The use of application-layer gateways will, in general, lead to a more fragile deployment, as has been observed in the past.

- The **back-end data-sharing model** refers to a communication architecture that enables users to export smart object data from a cloud service in combination with data from other sources. This architecture supports "the user's desire for granting access to the uploaded sensor data to third parties". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where IoT devices upload data only to a single application service provider'. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analysed; *it also allows for edge-clouds*.

  For example, a corporate user in charge of an office complex would be interested in consolidating and analysing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyse the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end datasharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

  The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve

> interoperability of smart device data hosted in the cloud. This architecture model is an approach to achieve interoperability among these back-end systems. Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors."
>
> This communication model is thus only as effective as the underlying IoT system designs. Back-end data sharing cannot fully overcome closed system designs.

These basic communication models demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that **device interoperability and open standards are key considerations in the design and development of internetworked IoT systems**.

From a general user perspective, these communication models help illustrate the **ability of networked devices to add value to the end user**. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. For example, the devices ultimately connect to data analytic services in a cloud computing setting. By creating data communication conduits to the cloud, users, and service providers can more readily employ data aggregation, big data analytics, data visualisation, and predictive analytics technologies to get more value out of IoT data than can be achieved in traditional data-silo applications.

In other words, effective communication architectures are an important driver of value to the end user by opening possibilities of using information in new ways. It should be noted, however, these networked benefits come with trade-offs. Careful consideration needs to be paid to the incurred cost burdens placed on users to connect to cloud resources when considering an architecture, especially in regions where user connectivity costs are high.

While the end user benefits from effective communication models, it should be mentioned that effective IoT communication models also enhance technical innovation and open opportunity for commercial growth. New services can be designed to take advantage of IoT data streams that didn't exist previously, acting as a catalyst for further innovation.

## 5.3. Digital Data Analytics

Data analytics algorithms is what gives the gathered IoT data some “life”. **It is this real-time information, knowledge and wisdom we can extract from the data which makes the Internet of Things so powerful.**

Data analytics algorithms vary significantly in capabilities and scope. There are algorithms which find us the known knowns; then there are algorithms which are able to extract the known unknowns; and as of very recent there are algorithms which are even able to extract the unknown unknowns from our data sets:

- **Known Knowns:** An example of the first class of algorithms, the known knowns, is simple linear regression. For example, assume we instrumented a shop with sensors which are able to measure the amount of goods on the shelves. If we now plotted that amount against time, linear regression would allow us to establish the best fit for how quickly the shelves are being emptied.

- **Known Unknowns:** An example of the second class of algorithms, the known unknowns, is machine learning. Here sophisticated algorithms are able to arrange data into clusters of prior specified characteristics. In addition, these algorithms are able to predict most likely events to occur. With our previous example, machine learning would be able to establish which products are being taken off at what rate and thereby enable better supply chain decisions.

- **Unknown Unknowns:** The third class of algorithms, the unknown unknowns, is currently pushing the boundary of what is possible in artificial intelligence. These deep-learning algorithms, some of which also rely on machine learning approaches, are able to get insights from data which we humans even didn’t imagine existed. Coming back to our example of a smart shop, deep learning analytics may reveal why certain products fly and others don’t.

Generally, we aim of above analytic tools is to get insights into the following:

- **Short-Term Alarms/Anomalies:** IoT and data analytics allow us to detect anomalies in real-time, which in turn would trigger an alert of something going wrong or about to go wrong. For instance, if we detected that a specific product run out in a shop, an alert could be sent to the shop owner to order more stock; that alert could even be sent to the supply chain without the shop owner noticing.

- **Long-Term Patterns:** On the other hand, collecting all the data and crunching it over time allows us to detect long term trends, which in turn allows us to construct policies. For example, imagine we observe that a specific product does not sell in winter but is really popular in the summer; the shelf stocking policy could then be adapted to these long-term patterns.

With a rich set of data analytics algorithms available today, the IoT is generally a great enabler of Big Data approaches. **IoT data gives us sufficient temporal and spatial data granularity to obtain meaningful real-time and long-term insights to make industries and processes more efficient and more effective.**

## 5.4. Data Privacy Regulations

As outlined above, the IoT will generate a massive variety of data from “connected devices” – such as sprinklers, fitness trackers, connected cars. That data will have strong privacy implications, because personal information can be deduced either directly or by correlating with other information sources. Privacy concerns are amplified by the way in which the Internet of Things expands the feasibility and reach of surveillance and tracking. Characteristics of IoT devices and the ways they are used, completely redefine the debate about privacy issues, because they dramatically change how personal data is collected, analysed, used, and protected:

- The traditional “notice and consent” online privacy model, in which users assert their privacy preferences by interacting directly with information presented on a computer or mobile screen (e.g. by clicking “I agree”), breaks down when systems provide no mechanism for user interaction. IoT devices frequently have no user interface to configure privacy preferences, and in many IoT configurations users have no knowledge or control over the way in which their personal data is being collected and used. This causes a gulf between the user’s privacy preferences and the data-collecting behaviour of the IoT device. There might be less incentive for IoT vendors to offer a mechanism for users to express their privacy preferences if they regard the data collected as being non-personal data. However, experience shows that data not traditionally considered personal data might actually be personal data or become personal data when combined with other data.

- Assuming an effective mechanism can be developed to enable a user to express informed consent of their privacy preferences to IoT devices, that mechanism needs to handle the large number of IoT devices a user must control. It is not realistic to think that a user will directly interact with each and every IoT device they encounter throughout the day to express their privacy preferences. Instead, privacy interface mechanisms need to be scalable to the size of the IoT problem, while still being comprehensive and practical from a user perspective.

- The Internet of Things can threaten a person’s expectations of privacy in common situations. There are social norms and expectations of privacy that differ in public spaces versus private spaces, and IoT devices challenge these norms. For example, IoT monitoring technologies like surveillance cameras or location tracking systems that normally operate in public spaces are migrating into traditionally private spaces like the home or personal vehicle in which our expectations of privacy are very different. In doing so, they challenge what many societies recognise as the “*right to be left alone*” in one’s home or private space. Also individuals’ expectations of privacy in spaces they consider to be public (e.g. parks, shopping malls, train stations) are being challenged by the increased nature and extent of monitoring in those spaces.

- IoT devices often operate in contexts in which proximity exposes multiple people to the same data collection activity. For example, a geolocation tracking sensor in an automobile would record location data about all occupants of the vehicle, whether or not all the occupants want their location tracked. It may even track individuals in nearby vehicles. In these kinds of situations, it might be difficult or impossible to distinguish, much less honour, individual privacy preferences.

- Big data analytics applied to aggregated personal data already represents a substantial risk of privacy invasion and potential discrimination. This risk is amplified in the Internet of Things by the scale and greater intimacy of personal data collection.

IoT devices can collect information about people with an unprecedented degree of specificity and pervasiveness; aggregation and correlation of these data can create detailed profiles of individuals that create the potential for discrimination and other harms. The sophistication of this technology can create situations that expose the individual to physical, criminal, financial or reputational harm.

- The ubiquity, familiarity, and social embrace of many IoT devices might create a false sense of security and encourage individuals to divulge sensitive or private information without full awareness or appreciation of the potential consequences of doing so.

From above, it is therefore not surprising that regulators have highlighted concerns and also released privacy guidance/frameworks for the IoT. US, Asia and Europe have all very different approaches to data regulation. The most stringent regulations however are about to be put in place in Europe. Any global IoT company will need to operate in Europe, so understanding the details of the European IoT regulations is paramount.

The European Commission's Article 29 Working Party on Data Protection (WP 29 Report), looked in 2014 at the IoT via EU data protection principles and highlighting below concerns for IoT manufacturers, developers and data collectors:

- **Lack of control:** Interconnectivity means a greater potential for automatic flow of data among devices (and vendors) *without* notice to users.

- **Additional purposes:** Interconnectivity also may lead to use of gathered data by *third* parties for other than the original intent.

- **Consent:** Because users lack full disclosure of data flow, their consent to initial data collection may be inadequate.

- **Profiling:** Fine-grained user monitoring and profiling could result from the type of information collectable from connected devices.

- **Limiting anonymity:** More use of connected devices suggests lower likelihood for maintaining anonymity.

- **Security:** Large volumes of data transferring over connected devices may lead to considerable security risks.

To address above concerns, the WP 29 Report recommends that IoT manufacturers, developers and data collectors commit to the following:

- **conduct a privacy impact assessment** before releasing a device;
- **delete raw data** from the device as soon as it has been extracted;
- **follow privacy-by-design** and privacy-by-default principles;
- in a **user-friendly way**, provide a privacy notice, and obtain consent or offer the right to refuse;
- design devices to inform both users and people interacting with them (e.g., people being recorded by a camera in a wearable technology) of the data processing by the entity providing the device;
- **inform users** of data that has been collected and enable them to access, review and edit that data before it is transferred; and
- **give users granular choices** on the type of processing as well as time and frequency of data gathering.

These principles apply whenever a connected device is used in the EU, even if the device did not originate in the EU. While the WP 29 Report is not a binding law, it has had a very strong impact onto the General Data Protection Regulation (GDPR).

The European GDPR was published in the Official Journal of the European Union in May 2016. All companies dealing with data, including with data from the IoT, has **until 25th May 2018 to ensure that data processing activities are compliant** with the newly adopted rules; in case of failure, there are **sanctions up to 4% of the global turnover** of the breaching entity.

This must not be taken lightly! And the status as of Q4 2016 is not encouraging: The data protection authorities of 26 countries (being part of the Global Privacy Enforcement Network) ran an investigation into IoT technologies and discovered that over 60% of them are not fully privacy compliant.

Notably, out of 300 reviewed devices, 59% does not provide adequate information on how personal data is collected, used and communicated to third parties; 68% does not provide appropriate information on the modalities of storage of data; 72% does not explain to users how their data can be deleted from the device; and 38% does not guarantee easy-to-use modalities of contact for clients that are willing to obtain clarifications on privacy compliance. To top that, some health related devices triggered security issues since they transmitted data to medical practitioners with encrypting them.

Clearly, **if the IoT industry wants to succeed, it needs to be trusted by users**. But, in order to do that, users need to be adequately informed on how their data is processed and have full control on them, being able to also delete them at their discretion. This, in essence, was one of the rationales of putting the GDPR in place. The adoption of a privacy by design approach is thus the sole solution that can mitigate the potential risks of privacy sanctions.

# 6. Important Digital Standards and Alliances

## 6.1. Standards Development Organizations (SDOs)

- The **European Telecommunications Standards Institute (ETSI)** produces global ICT standards including fixed, mobile, radio, converged, broadcast and internet technologies. In ETSI, most of the standardisation work in the M2M arena is conducted within the Machine-to-Machine Communications Technical Committee (TC-M2M). This committee was established in 2009 with the mission of ensuring that M2M services deployed worldwide are interoperable.
  ETSI-M2M defines a Service Capability Layer (SCL) on top of connectivity layers. Hence, for the network domain, it leverages on existing technologies such as 3GPP's GERAN/UTRAN/eUTRAN (i.e., 2G, 3G, 4G or 5G networks), WIMAX or other fixed or satellite networks. Likewise, for the M2M area network domain it relies on the availability of short-range communication technologies such as Wi-Fi, Zigbee, or Power Line Communications (PLC), to name a few. ETSI released in 2012 and 2013 the first and second versions respectively of its M2M standard. The core specs in this suite are those describing service requirements, the functional architecture and communication interfaces.
  The activities conducted by ETSI's Smart Card Platform Technical Committee (TC-SCP) are very relevant to M2M communications too. To give an example, the availability of embedded and remotely programmable subscriber identity modules (SIM), a topic under the umbrella of this committee, is instrumental for the successful deployment of M2M networks. For 3GPP technology-related developments, ETSI-SCP actively collaborates with GSMA's (Global System for Mobile Communications Association's) Smart Card Application Group (SCAG), as well as 3GPP's Core Network and Terminals Working Group 6 (CT6, Smart Card Application Aspects).

- The **Third Generation Partnership Project (3GPP)** is responsible for the development and maintenance of the Global System for Mobile Communications (GSM), the Universal Mobile Telecommunications System (UMTS) and its Long Term Evolution (LTE) and beyond, and the Internet Protocol Multimedia Subsystem (IMS) specifications. Hence, 3GPP is a key standardization body as far as delivering

M2M communications over cellular (wide area) networks or, in the 3GPP jargon, Machine-Type Communications (MTC) is concerned. Differently from ETSI, 3GPP deals with specific systems and protocols. A high number of Working Groups (WG) under e.g., the Technical Specification Groups for Radio Access Network (TSG-RAN), or Service and Systems Aspects (TSG-SA) contribute very actively to the work on MTC-related optimizations for LTE networks. The prioritization of topics and activities is discussed in Work Items such as the one on NB-IoT of Release 13.

- The **Institute of Electrical and Electronics Engineers (IEEE)** has introduced several enhancements to its air interface for broadband wireless access systems (i.e., IEEE 802.16) in order to more effectively support M2M applications. To that aim, two amendments (IEEE 802.16p and 802.16.1b) were developed by the IEEE 802.16's Machine-to-Machine (M2M) Task Group. Complementarily, the IEEE 802.15 working group on Wireless Personal Area Networks develops standards for short-range wireless networks composed of e.g. Personal Digital Assistants (PDAs), cell phones, and, in general, mobile and computing devices. In particular, Task Group 4 investigates low data rate solutions with multi-month to multi-year battery life and very low complexity. The e, g and k amendments to IEEE 802.15.4 are particularly relevant to M2M communications, and are reaching maturity as of 2014. In more details, the IEEE 802.15 Task Group 4e is aimed to define a MAC amendment to the existing standard 802.15.4-2006. According to its foundational chart, the intent of this amendment is to enhance and add functionality to the 802.15.4-2006 MAC to better support the industrial markets and permit compatibility with modifications being proposed within the Chinese WPAN. The role of IEEE 802.15 Smart Utility Networks (SUN) Task Group 4g is to create a PHY amendment to 802.15.4 to provide a global standard that facilitates very large scale process control applications such as the utility smart-grid network capable of supporting large, geographically diverse networks with minimal infrastructure, and potentially millions of fixed endpoints. Last but not least, the IEEE 802.15.4k amendment addresses applications such as critical infrastructure monitoring.

- Within the **International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)**, the Focus Group M2M, established in 2012 and terminated in 2013, was responsible for studying the requirements and specifications for a common M2M Service Layer (incl. architecture, protocols, API aspects). The strategy was to reuse to the largest extent possible what has already been specified by other SDOs. Yet such service layer is aimed to support different application domains, such as e-Health, Smart Grids, or Industrial Automation; the focus of the group was on e-health (e.g., remote patient monitoring, ambient assisted living).

- According to its foundational charter, the TR-50 Smart Device Communications Engineering Committee of the **Telecommunications Industry Association (TIA)** is in charge of developing interface standards for the communication of events and information between M2M systems and smart devices, applications or networks. In this context, TR-50 is developing a smart device communication framework which is agnostic to the underlying transport and access networks (both wired and wireless); and to the vertical application domain by means of a suitable Application Programming Interface (API). The IEEE 802.15.6TM-2012 standard is optimised to serve TIA's TR-50 Committee around Body Area Networking. TR-50 also fosters collaboration and pursues coordination with other SDOs. As an example, it supports (and hosts) the Machine-to-Machine Standardization Task Force (MSTF) of the Global Standards Collaboration (GSC). Besides, TIA is a founding member of the OneM2M initiative.
- Finally, the (on-going or past) work conducted by a number of working groups within the **Internet Engineering Task Force (IETF)** is also relevant to M2M systems. Mostly it addresses networking aspects in the so-called capillary networks, that is, beyond the M2M gateway in ETSI's architecture. This includes, but is not limited to, the ROLL (Routing over Low Power and Lossy Networks), CoRE (Constrained REstful Environments), MEXT (Mobility EXTensions for IPv6), 6LoWPAN (IPv6 over Low power WPAN), and 6TSCH (Deterministic IPV6 over IEEE 802.1.5.4e Timeslotted Channel Hopping) working groups.

## 6.2. Industry Associations & Special Interest Groups (SIG)

The activities carried out in the aforementioned SDOs are nicely complemented by the efforts made by a number of industrial associations and SIGs (which are often fed into the above discussed standardisation bodies). Since the number of industrial associations is quite high, we will focus on a particularly relevant subset only.

- The **Global System for Mobile Communications Association (GSMA)** gathers around 800 mobile operators worldwide, as well as more than 200 companies in the broader mobile ecosystem (e.g., handset makers, software companies, media and entertainment). Within GSMA, the work conducted in the Smart Card Application Group (SCAG), which is aimed to promote smart card adoption, identification of mobile operator requirements and favour functionality/quality enhancements (form factor, embedded versions, over-the-air re-programming, etc.), is of notable importance for players in the M2M arena.

- As for **Weightless SIG**, it promotes the adoption of an open standard for cellular M2M communications. To date, over 1500 organizations have joined the Weightless SIG. Its specification, for which version 1.0 already available (Weightless, 2013), is specifically tailored for the operation of M2M networks in white space spectrum (TV bands, UHF). Some salient features and design requirements include the optimization for low-cost hardware, extended coverage (to reach e.g., metering devices in home basements or in remote places), ultra-low power operation to enhance network lifetime, and secure and guaranteed message delivery. Ever since the acquisition of Neul by Huawei and its departure from Weightless, the SIG is driven by nWave and other embodiments.

- The **Alliance for Telecommunications Industry Solutions (ATIS)** launched its M2M Committee in July 2012. It aims to define the elements of a common service layer leveraging on network capabilities, as well as the requirements for the interfaces towards the application and transport layers. ATIS is one of the founding members of the oneM2M Alliance.

- In an attempt to stimulate global harmonisation and avoid duplication of activities between SDOs, we have recently witnessed the advent of supra-SDO and supra-SIG initiatives. This includes, for instance, the **oneM2M Partnership Project** which was formed in July 2012 with the support of ETSI, TIA, ATIS, CCSA, TTA, ARIB and TTC as founding members. oneM2M pursues the following: (i) the definition of a common service layer allowing an independent view of end-to-end services; (ii) the design of open/standard interfaces, APIs and protocols; and (iii) to facilitate interoperability, this including test and conformance specifications.

- Likewise, the goal of the **Machine-to-Machine Standardization Task Force (MSTF)** of the Global Standards Collaboration (GSC), a group of major SDOs centered on the International Telecommunication Union, is to "facilitate global coordination and harmonization in the area of M2M standardization by reaching out to a broad range of participants in the field and openly sharing relevant M2M information".

To close this section, in **Table 1** I summarise the main players (standardisation bodies, associations, SIGs) and the specific working groups within those organisations working towards the standardisation of communications systems underpinning the emerging IoT.

**Table 1:** Main organizations and specific working groups in the M2M arena.

| **Standards Development Organization / Association/ SIG** | **Main relevant Working Group(s), Committees, Amendments** |
|---|---|
| ETSI | M2M, SCP |
| 3GPP | NB-IoT, EC-GCM, LTE-M, (and TSG-RAN, TSG-SA, TSG-CT as well as WGs thereof) |
| IEEE | 802.15.4g, 802.15.4k, 802.15.4e, 802.16p, 802.16.1b |
| ITU-T | Focus Group M2M |
| TIA | TR-50 |
| IETF | ROLL, CoRE, MEXT, 6LoWPAN, 6TSCH. |
| GSMA | SCAG |
| Weightless SIG | PHY, MAC, Security, Regulation |
| ATIS | M2M Committee |
| oneM2M | Requirements, Architecture, Security, Management |
| GSC | MSTF |

# 7. Application to Buckinghamshire

## 7.1. From Asset Monitoring to Predictive Maintenance

Using above technologies, arguably the biggest opportunities lie with the digitization of the Buckinghamshire assets. This includes road signs, bridges, roads, tunnels, traffic lights, benches, rockfall protection, among many others.
Installing sensors and actuators on these assets, allows one to gather data about the assets at a temporal and spatial granularity not seen before. This, in turn, allows one building trends on their use and exhaustion.
Used properly, these techniques can be very powerful to optimize the maintenance cycles. Imagine a bridge: instead of doing maintenance too early or too late, the work can be conducted when truly needed --- something which can be picked up by properly installed sensors [40].

## 7.2. Digitizing the Buckinghamshire Workforce & Processes

Another huge potential is in completely digitizing the workforce and the processes being done at the moment. In itself a huge undertaking, it promises to save costs mid to long term. Cloud technologies are an important enabler here, and so are drone technologies.

## 7.3. Breaking Procurement Barriers

Digital, and in particular the IoT, can help to break down procurement barriers and make the entire process much smarter. Traditionally, a city hall would set out the tender with minimum consultation and the company which meets all KPIs and is cheapest wins. This however is a recipe for failure as a) companies have little time to adapt to the true needs of the city; and b) the cheapest minimum solution may not be the best long-term. Using digital, an early engagement can be guaranteed and procurement itself can be made a much “smarter” process.

## 7.4. Real-Time Interaction with Citizens

An interesting opportunity of digital, and particularly the Internet of Things, is that one is able to engage with the customer/citizens in real-time well after sales/installation of assets.

For instance, British Gas has a smart home solution called Hive which is a smart thermostat. The smart phone app which is used to control the thermostat also includes a feedback section where customers are able to provide feedback and ideas on next products. These are then ranked among the customers and British Gas only has to execute the top one to satisfy its customers.

A similar principle can be used to engage with citizens in Buckinghamshire.

## 7.5. Building an Open Data & API Eco-System

And finally, if all of above digital approaches are accessible to third parties, then a service economy can be built on top. This requires data to be made open; and suitable APIs to be created. The opening of the data of course has to obey national privacy and security directives.

# Bibliography

[1] Auto-ID Labs, Available online: http://www.autoidlabs.org.

[2] European Commission Communication on RFID, European Union. COM(2007) 96., March 2007.

[3] Council of The European Union, Transport, Telecommunications and Energy, Available online: http://www.internet-of-things-research.eu/documents.htm, 27 November 2008.

[4] U.S. National Intelligence Council (NIC), Global Trends 2025: A Transformed World, NIC, Available online: www.dni.gov/nic/NI-2025-project.html, November 2008.

[5] Y. Huang and G. Li, "Descriptive Models for Internet of Things," in International Conference on Intelligent Control and Information Processing, ICICIP, August 2010.

[6] INFSO D.4 Networked Enterprise RFID INFSO G.2 Micro Nanosys-tems in Co-operation with the Working Group RFID of the ETP EPOSS, "Internet of Things in 2020, Roadmap for the Future, Version 1.1," European Commission, Information Society and Media, Tech. Rep., May 2008.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, October 2010.

[8] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From Todays's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View," IEEE Wirelesss Commun., vol. 17, no. 6, pp. 44 – 51, December 2010.

[9] L. Coetzee and J. Eksteen, "The Internet of Things - Promise for the Future? An Introduction," in IST-Africa Conference Proceedings, May 2011.

[10] E. Fleisch, "What is the Internet of Things? - An Economic Perspective," Auto-ID Labs, Tech. Rep., 2010.

[11] European Research Cluster on Internet of Things (IERC), Internet of Things - Pan European Research and Innovation Vision, IERC, Available online: http://www.internet-of-things-research.eu/documents.htm, October 2011.

[12] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: A Survey," in 19th International Conference on Software, Telecommunications and Computer Networks, SoftCOM, September 2011.

[13] J. P. Vasseur and A. Dunkels, Interconnecting Smart Objects with IP: The Next Internet. Morgan Kaufmann, 2010.

[14] O. Hersent, D. Boswarthick, and O. Elloumi, The Internet of Things: Key Applications and Protocols. Wiley, 2012.

[15] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, HyperText Transfer Protocol – HTTP/1.1, RFC 2616, Internet Engineering Task Force RFC 2616, June 1999. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2616.txt

[16] J. Postel, Internet Protocol, RFC 791, Internet Engineering Task Force RFC 791, September

1981.

[17] Transmission Control Protocol, RFC 793, Internet Engineering Task Force RFC 793, September 1981. [Online]. Available: http://www.rfc-editor.org/rfc/rfc793.txt

[18] G. Lawton, "Machine-to-Machine Technology Gears up for Growth," Computer, vol. 37, no. 9, pp. 12 – 15, 2004.

[19] ETSI TS 102 689 v1.1.1, "Machine-to-Machine communications (M2M): M2M service requirements," August 2010.

[20] Demosthenes Vouyioukas and Alexandros Karagiannis (2011). Pervasive Homecare Monitoring Technologies and Applications, Telemedicine Techniques and Applications, Prof. Georgi Graschew (Ed.), InTech, DOI: 10.5772/21439. Available from http://bit.ly/2dadeoI.

[21] "Energy Harvesting Powers Wireless Sensors," available from http://bit.ly/2d1q6z1.

[22] "List of Sensors", available from https://en.wikipedia.org/wiki/List_of_sensors.

[23] "Sensor Manufacturers Association List," available from http://bit.ly/2dvnwV0.

[24] "Actuator," available from https://en.wikipedia.org/wiki/Actuator.

[25] Marc Zupan, Mike Ashby and Norman Fleck, "Actuator Classification and Selection," Advanced Engineering Materials journal, available from http://bit.ly/2dkjI9x.

[26] "What is MEMS Technology," available from http://bit.ly/2dlG2zZ.

[27] "International Roadmap for Semiconductors," ITRS Executive Report 2015.

[28] "Roadmap to the Trillion Sensor Universe," Dr. Janusz Bryzek, VP Development, MEMS and Sensing Solutions, April 2, 2013; available from http://bit.ly/1mnG3w5.

[29] Eric Wang, Xingqin Lin, Ansuman Adhikary, Asbjörn Grövlen, Yutao Sui, Yufei Blankenship, Johan Bergman, Hazhir S. Razaghi , "A Primer on 3GPP Narrowband Internet of Things (NB-IoT)," available from https://arxiv.org/abs/1606.04171.

[30] "Zigbee and Z-wave are out. Broadcom's new chips bet on Bluetooth and Wi-Fi for IoT," available from http://bit.ly/1vAZxY2.

[31] "Overview of Internet of Things at Google," available from http://bit.ly/2dKfb0f.

[32] "IoT Security Foundation," available from https://iotsecurityfoundation.org/.

[33] "Baby monitors 'hacked': Parents warned to be vigilant after voices heard coming from speakers," available e.g. from http://ind.pn/1PLomnI.

[34] K. Rose, S. Eldridge, L. Chapin, "An Overview Understanding the Issues and Challenges of a More Connected World," Internet Society, 2015; available from http://bit.ly/1XutBNO.

[35] "Wikibon: A Wiki for Sharing Technology & Business Knowledge," available from www.wikibon.org.

[36] Cloud comparison platform; available from http://cloudcomparison.rightscale.com.

[37] "Relation between base station characteristics and cost structure in cellular systems,“ available from http://bit.ly/2dRp3pz.

[38] "A Cloud Infrastructure Service Recommendation System for Optimizing Real-time QoS Provisioning Constraints," available from http://bit.ly/2dxp5Rf.

[39] "The Vital Role of Edge Computing in the Internet of Things," available from http://bit.ly/1TYKyPq.

[40] Worldsensing, "Loadsensing Product"; available under www.worldsensing.com.