Technical Annex: An Evidence Review of Urban 'Internet of Things' Applications

Report prepared for Future Cities Catapult

June 2018

DISCLAIMER

The views and recommendations laid out within this report are those of the consultants and academics commissioned by the Future Cities Catapult, based on their work and research, and not necessarily those of the Catapult.

ACKNOWLEDGEMENTS

We would like to thank Prof Julie McCann of the AE3SE: Adaptive Emergent/Embedded/Ephemeral Systems Engineering Group Smart Connected Futures Centre at Imperial College London for the research on the technical implementation of IoT solutions.

We would also like to thank Dr Colin Birchenall (CTO, Digital Office, Scottish Local Government), Kevin O'Malley (Partnership Development Manager, City Innovation, Bristol City Council), Geoff Snelson (Director of Strategy and Futures, Milton Keynes Council), Balazs Csuvar (Senior Project Officer, Digital Greenwich), and Sarah Butler (H2020 Sharing Cities Programme Coordinator, Digital Greenwich) for the interviews and workshops, which were essential for this research and report.

: vivideconomics

CONTENTS

LIST OF TABLES & FIGURES

1. INTRODUCTION

1.1 AIMS AND OUTPUTS

The Future Cities Catapult focuses on urban innovation and is aiming to guide the successful deployment of 'Internet of Things' (IoT) programmes in cities. IoT based technologies offer the opportunity to provide a unique set of services and to connect with citizens. With improving technologies and the increasing demands that will be placed on cities over the coming years, we are likely to see a surge in uptake of innovative, urban IoT solutions to help improve and manage areas such as health, transport and energy efficiency.

This work supports the IoT Guidance, and is split into three distinct components to supplement the three stages of delivering an IoT project:

- this technical annex in the form of an evidence review gives an overview of existing IoT systems and technologies to help formulate strategies and proposals;
- the technical guidance provides best practises and will be consulted when deploying technologies;
- case studies help to illustrate optimal management and evaluation of IoT projects.

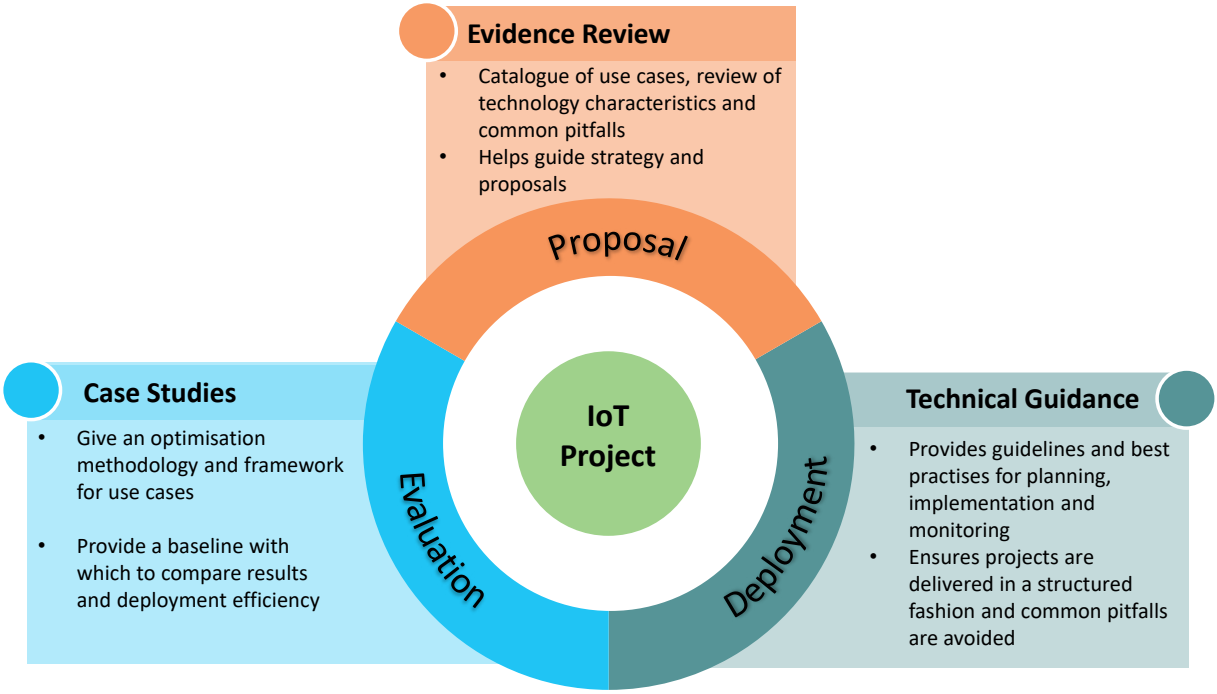

Figure 1. The three components combined provide assistance across all elements of delivering an IoT project
Source: Imperial College

The aim of this project is to provide general guidance to any city looking to procure an IoT solution. Given the recent emergence of this field, there is currently a lack of experience and knowledge of the area amongst decision makers, hindering them from deploying projects efficiently and maximising the social impacts. This body of work aims to alleviate these issues and make IoT solutions more accessible and understandable to a wide range of policy makers. Any views and recommendations in this guidance are those of the consultants and academics commissioned by the Future Cities Catapult, and are not necessarily those of the Catapult.

1.2 PROJECT FOCUS

The term 'Internet of Things' is not firmly defined – it generally refers to computing devices being interconnected via the Internet, enabling them to collect, send and receive data without human interaction. The term was first coined in 1999 to label a system where computers could directly observe and understand the physical 'things' in the world. Today, is has evolved to describe any system where computing devices collect and exchange data via the Internet – this includes an incredibly broad array of technologies, from smartphone applications like Uber to automated smart lighting. Given the range of 'Internet of Things', defining a tight scope is essential to guide the work towards the relevant areas and provide the most value.

First, this project focusses on urban IoT systems that deliver society-level benefits in health, transport and energy. The target audience for this work is primarily public purchasers of IoT, rather than business. Systems that deliver private benefits should, in theory, emerge in the market and not require public investment. In contrast, private agents will under-invest in projects with societal benefit as they are not fully remunerated for the benefits that flow to other actors. Benefits commonly arise at a social level in projects targeting health, transport and energy efficiency, which is why this document concentrates on these areas throughout.

Second, this guidance aims to guide users to projects that could provide substantial social benefit over a sustained period of time. IoT applications do not necessarily provide social benefit. A wide range of IoT applications have been deployed globally to achieve a mix of objectives, ranging from public relations exercises to those delivering social benefit. The ability to brand a city as smart and connected is often motivation enough to pursue a range of cutting edge technological activities. Against this backdrop this review attempts to guide users towards applications that have already, or could feasibly in future, deliver sustained social benefits.

The successful deployment of IoT relies on adequate security safeguards, however the issue of cybersecurity is largely beyond scope. Increasingly the constraining design factor on IoT systems is the ability to safeguard systems against malicious behaviour and security breaches. To do this topic justice, a full treatment of suitable cybersecurity standards and protocols is required, and this is beyond the scope of this guidance. This guidance addresses security in some depth, but to successfully apply IoT, a more detailed consideration of these issues should be pursued in addition to what is covered here.

1.3 STRUCTURE OF THE DOCUMENT

This Technical Annex includes a catalogue of IoT use cases in cities, reviews the characteristics of the technologies that drive them, and the common pitfalls that arise from IoT projects.

The catalogue of use cases gives an idea of what has already been deployed successfully and how IoT projects can benefit cities. The inventory of previous urban IoT projects provides a simple categorisation and highlights successful applications that urban planners can consult when considering which types of projects to potentially undertake.

The review of technical characteristics sets out the key aspects that non-technical, potential buyers should be aware of before seeking out an IoT system. The goal is to ensure that buyers understand the key technological considerations, the available options and potential limitations.

The final section highlights the issues that can arise when IoT systems are deployed without an understanding of the technology or a structured method of implementation. Whilst IoT systems are exciting opportunities, there have been some instances of poor delivery hindering projects leading to limited future capabilities and high costs that do not provide clear gains over non-IoT solutions. Examples of these common mistakes are not designing for longevity, limited consideration for avenues of real action and non-modular deployment. In most of these cases, better scoping and planning of IoT projects would have prevented this, leading to enhanced benefits and outcomes for users. The separate technical guidance report details the general steps that are involved when deploying an IoT project and lists the prudent steps to take to avoid these common mistakes.

2. CATALOGUE OF USE CASES IN HEALTH, ENERGY AND TRANSPORT

2.1 DEFINING CHARACTERISTICS

The aim of this section is to provide a catalogue of the main IoT applications (or use cases) in health, energy and transport, based on a review of what has been attempted around the globe. This review is based on a review of the evidence, interviews and detailed contributions from IoT experts at Imperial College. The objectives of this catalogue are to illuminate the most commonly applied IoT applications, to clarify their potential benefits to society and to provide a way to distinguish between the use cases without diving into too much detail.

Each application is described in terms of its primary benefit to society, scale, critical thresholds, new infrastructure and level of automation. Although many other differentiating factors exist, these factors are important from the perspective of an IoT purchaser at the early stages of selecting an IoT intervention:

- **Primary benefit to society:** For public bodies, there is a need to identify the benefits to society over and above what would be delivered privately through the market. This provides an economic rationale for public investment.

- **Scale:** the size of the applications is important given that many case studies have only been applied at a small scale, and therefore the lessons may have limited transferability or be context specific. This parameter helps the reader distinguish between small pilot studies and large scale deployments.

- **Critical threshold:** This aspect is to help IoT purchasers determine whether the application would provide benefits in a new context. Some applications can be implemented in a modular fashion, whereas others require a large scale of rollout to provide meaningful benefits. For each application, we identify whether it can be applied at the level of individuals, at a neighbourhood/ district level or whether it requires citywide deployment in order to deliver benefits.

- **New infrastructure:** Some IoT applications require the rollout of new infrastructure whereas others can be built onto existing systems, such as mobile phones. This is important for public bodies as it gives an indication of the likely level of difficulty and cost associated with rolling out a particular application. Three levels of infrastructure are identified:

  - **Level 1** projects do not require any new hardware;

  - **Level 2** projects include software and a set of devices (for example sensors) to be installed;

  - **Level 3** projects involve software, hardware and a new underlying network (e.g. of low power wide area networks) in addition to what may already exist.

  In future, there is the potential for an additional type of project which only involves the deployment of a network, the underlying infrastructure for third parties to provide a range of IoT devices and services. We discuss these opportunities later in the technical guidance.

- **Automation:** A distinguishing feature of IoT is whether they simply collect information (Assimilate); process information (Analyse) or, in the most active case, automatically change decisions based on the information (Act). This is an important distinguishing feature because applications which simply collect information are less reliable in delivering benefits than those which analyse and act on this information. Applications which

rely on users changing behaviour in response to the provision of information do not necessarily provide benefits, but rely on a set of behaviour changes which may be much more difficult to realise than simple technology deployment.

2.2 METHODOLOGY FOR EVIDENCE REVIEW

The list of case studies was assembled using a mix of desktop research, interviews and validation with IoT experts. The desktop research included keyword searches to obtain an initial database of potential evidence around IoT applications, technologies and evaluations. We conducted a rapid search of key databases (Google Scholar, Microsoft Academy, Science Direct) using a literature review search tool (Publish or Perish). The output of this task was an excel workbook listing all the related literature by number of citations, journal, authors, and search terms. A selection of the key search words used is listed in Table 1 below. Essential words were required to be included in the source, whilst the optional and specific words were desirable and helped flag more relevant sources.

Essential	Optional	Specifics
Internet of Things	Health	Santander
Smart	Transport	Barcelona
Urban	Energy	Parking
City	Cloud computing	Pollution
	Automation	Congestion

Table 1. The keywords used to obtain the initial database
Source: Vivid Economics

Sources with sufficient citations and key-words were briefly reviewed to assess their fit within our defined scope and any pertinent evidence was extracted. The first cut of evidence involved removing sources with less than 25 citations per year and those without at least two keywords in the title. The remaining sources were filtered according to the relevance of their abstracts and introductions. The criteria for relevance was that they referred to at least one of the following: examples of smart cities, policy approaches to deliver IoT projects, technologies for IoT projects and evaluation of urban IoT cases. Evidence was collected from the sources that passed this screening.

The lack of a robust set of literature on urban IoT solutions necessitated additional targeted searches and interviews to obtain a more well-rounded body of evidence. Deployments of IoT solutions in cities are still not particularly wide-spread, which creates a bias towards anecdotal evidence and short descriptions of projects rather than in-depth evaluations. As such, interviews were carried out to gain deeper insights into strategies and deployment decisions, and to highlight the leading examples of urban IoT projects. Further targeted searches helped to both fill gaps in knowledge around specific use cases and gather broader information from less academic sources.

This process produced a filtered set of use cases and technologies, which was then reviewed and added to by leading academics from Imperial College. A team of Imperial academics, led by Prof Julie McCann, provided their expertise and insights in the field of IoT to assess the accuracy and relevance of the filtered evidence and supplement it with their own additions.

Economic assessment experts from Vivid laid out the framework for categorising IoT use cases, whilst the Imperial academics summarised the key features of the technologies. The catalogue of use cases was created simply by placing the set of use cases into a structured framework that highlights the most significant features. The Imperial academics focused on leveraging their knowledge of IoT technologies to create an accessible, high-level review of the key technological characteristics potential buyers should be aware of. The list of common pitfalls was developed following evaluations if the historical examples and discussions between Vivid and Imperial. Figure 2 below summarises the method for the evidence review.

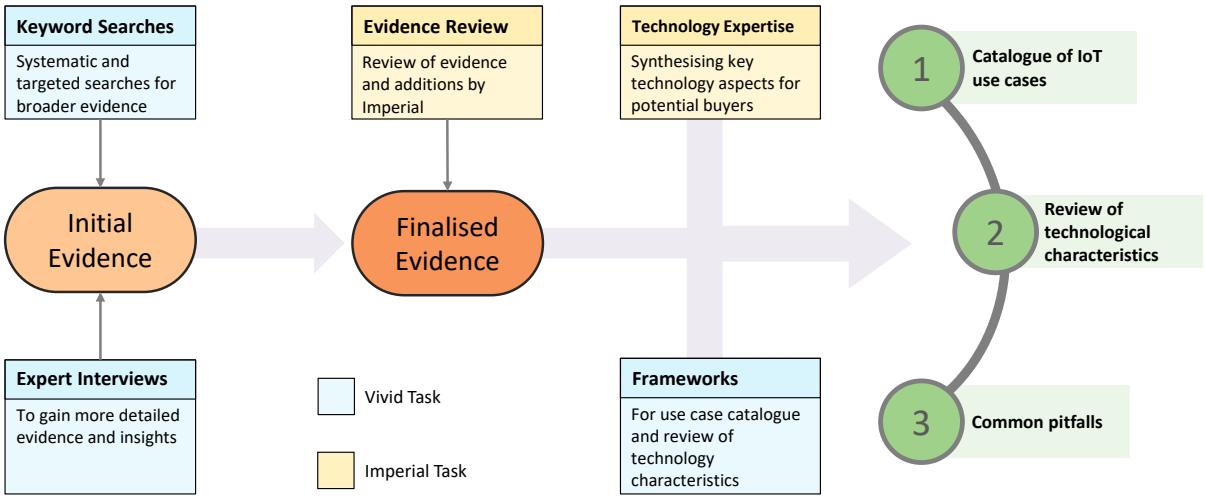

Figure 2. An illustration of the methodology and output for the evidence review report
Source: Vivid Economics and Imperial College

2.3 CATALOGUE OF URBAN IOT USE CASES

This section sets out the key use cases for urban IoT and their characteristics. The focus is on three areas of application - health, energy and transport - in turn, although some applications have cross cutting benefits. For example, smart buses may both monitor the air pollution level of a city and the speed and position of the buses. This kind of application, therefore, could be classified as having both transport and health benefits.

2.3.1 Health

Remote monitoring of patients

In terms of health, the main opportunity of IoT has been to monitor patients. The aim is the use of sensors around the house or hospital and wearable devices to collect data from the patient's vital signs and inform the doctor remotely. Efficient remote monitoring is important to reduce overcrowding in hospitals, to minimise the stress of transporting patients and to help doctors and nurses to better attend to the public.

MEDiSN[1] is a platform for monitoring vital signs of patients at emergency rooms (Ko, et al., 2010). Custom built motes called miTAGs periodically measure a patient's heart rate and blood pressure, transmitting this data through the Internet. The platform was deployed in 2008 at John Hopkins Hospital, Baltimore, USA, and 46 patients were monitored over a period of ten days. The project was also featured on Discovery Channel Tech in 2009[2].

Fall detection and movement tracking systems for elderly people or dementia patients

The population of people over the age of 60 have been increasing in the last 30 years. According to the World Health Organisation[3], it is expected that around two billion people will be older than 60 years by 2050, with 80 percent of this old population living in low and middle-income countries. This brings costs, both economic and human, to provide the necessary assistance to the elderly. In order to improve the quality of life of this population, giving more independence to the patients while helping nurses and doctors to closely monitor their health, IoT systems have been proposed to track vital signals and detect potential falls.

The most successful project in this field is the HomeAssist[4], a platform developed by INRIA, France. HomeAssist proposes a systematic approach for introducing an Assisted Living Platform for elderly people. It offers an online catalogue of applications that can be used by patients and carers. These applications are categorised in three domains: daily activities, such as medication reminder and meal preparation; home or personal safety, like entrance monitoring and lights in the corridors to facilitate walking through the house; and social participation, with activities to encourage socialising and physical and mental activities.

An initial field study was conducted over nine months in 2013 with 24 participants at different levels of autonomy, from frailty to initial stage Alzheimer. Since 2015, the project is passing to a Randomised Controlled Trial (RCT) with up to 500 participants matched with non-equipped participants. This intervention involves monitoring as well as compensation services to support independent living and will take around two years.

Environmental condition monitoring

Environmental conditions, such as air pollution and ultraviolet radiation, may cause several health issues to the population in medium and long term. Monitoring and analysing these conditions with sensors can help citizens, companies and nonprofit organisations to keep track of the levels of pollution or radiation in their city, empowering them to request better actions from the public sector. Universities and research centres may also benefit from this data, allowing to better understand the causes and effects of the main health issues in a city and ultimately providing solutions for such problems.

The most common monitoring system of this type is via air pollution detection. Air pollution is a growing concern in urban areas due to the high density of transport and industries harboured within a small area. Chinese cities such as Beijing and Shanghai are very interested in this due to China's fast economic and technological development in the last 10 years and the country's great population (1.37 billion people in 2015). A study of carbon emissions in urban areas (Churkina, 2008) concluded that 80 percent of CO2 emissions originate in cities around the world, even though urban areas cover only 2.4 percent of the total land area of the planet. According to the World Health Organisation, many respiratory problems, such as asthma and chronic bronchitis are caused by air pollution[5]. However, high levels of pollution may also contribute other more aggressive problems, such as lung cancer, strokes, nervous systems issues, hence sensing becomes important.

CitySee and Ekobus are two examples of air pollution monitoring systems. Ekobus[6] is a system that monitors levels of air pollution and tracks busroutes. It is a collaboration project developed by Libellium and Ericsson and founded in 2012. The system was implemented in the Serbian cities of Belgrade and Pancevo. Waspmotes nodes were deployed on top of 65 buses to monitor six different

1. http://hinrg.cs.jhu.edu/joomla/projects/61-medisn.html
2. https://www.youtube.com/watch?v=DNdeTy1DfwA
3. http://www.who.int/mediacentre/factsheets/fs404/en/
4. http://phoenix.inria.fr/research-projects/homeassist
5. http://www.who.int/mediacentre/news/releases/2014/air-pollution/en/
6. http://www.libelium.com/smart_city_environmental_parameters_public_transportation_waspmote/

parameters: temperature, relative humidity, carbon monoxide, carbon dioxide, nitrogen dioxide and GPS location. The collected air quality data can be viewed on a website and an Android app. Citizens can request details about bus routes through SMS messages. In a similar way, CitySee[7] is a platform designed to measure pollutant emissions on large-scale areas accurately and thoroughly in a real -time and long-term manner. In the project's first deployment in August 2011, 1,196 sensors were deployed in the urban area of Wuxi City, China, collecting multidimensional environmental data, such as temperature, light level, CO2, NO2, etc. These sensors were deployed in trees and lamp posts with a minimum distance of 2.5m between nodes. The system continuously collected data until 2014, and according to the authors of the paper (Liu, et al., 2013), it was the first large-scale system to monitor air conditions in a city.

A unique and very successful project is the platform developed and used in Fukushima, Japan, to measure the levels of radiation. Following the Fukushima disaster in April 2011, Libelium decided to develop a radiation sensor shield for Arduino boards[8]. In less than a month, several of these boards were shipped to the Tokyo Hackspace and other working groups in Japan. The idea was to empower people to develop their own applications to monitor the level of radiation without depending of government authorities. In this open and enthusiastic environment, the SAFECAST initiative was born[9]. SAFECAST is a global volunteers based science project working to empower people with data about the environment. It has the largest open database of radiation measurements ever collected and currently it is building its own wireless sensor network to monitor air quality. The data collected is open, as mentioned, and anyone can suggest and build a project, which is usually crowd founded by different people around the world.

Fitness and athletes care

Another application of IoT in health is in the field of sports and training. Systems usually consist of sensors embedded in the shoes or sports clothes of an athlete (wearable devices) or in the main equipment used in a gym, and their main purpose is to guide the user during exercise. The data collected can be used to monitor the learning process or performance of the user during weeks or months of exercise as well as warn them about possible dangerous conditions that may cause injuries. The most popular examples are smartwatches and fitness trackers, such as Apple Watch and Fitbit, which have become increasingly widespread since their launch in 2015. These devices offer innovative services, including fitness tracking, heart rate monitoring, quality of sleep, etc. along with various capabilities typically found in modern smartphones. Another example of wearable devices for fitness tracking is the Altra Torin IQ Smart Shoe[10]. Considered a "running coach in a shoe", the sensors deployed in the shoe allow the user to monitor the impact rate (how hard the runner hit the ground each step), the landing zone, the cadence (the live pulse of the runner) and the ground contact time of each foot, enabling the runner to adapt and improve running patterns to achieve better results. The information is easily displayed in an app compatible for both Android and IOs systems.

More accurate and reliable data can also help coaches to better guide their athletes in training and competitions. Researchers at Imperial College London designed a sensor for monitoring performance of athletes in real time[11]. The sensor is designed to be worn behind the ear and measures biomechanical data, such as posture and gait, during an activity. A computer collects data from the sensor and assesses the performance of athletes in real time.

A company that is making huge efforts in sports and technology is TuringSense[12]. Pivot, its main product, is a multi-sensor system for full body analysis developed to coach tennis players[13]. The system is capable of recreating joint and body movements without the use of cameras or wires. The sensors deployed in the players body and the tennis racquet send accurate data to a tablet, where an installed app analyses the data and compares it with a database of previous movement. The pattern recognition algorithm helps the user to monitor evolution during the training process as well as possible injuries.

7. http://www.greenorbs.org/all/citysee.htm
8. http://www.libelium.com/fukushima_crowdsourcing_radiation_social_project
9. http://blog.safecast.org
10. https://www.altrarunning.com/iq
11. https://www.newscientist.com/article/dn12640-ear-sensor-could-help-athletes-go-for-gold/
12. https://www.turingsense.com/
13. https://www.turingsense.com/about-pivot/

2.3.2 Energy

Managing energy costs in buildings

IoT systems can be used to efficiently collect data about the energy consumption in a building, accurately indicating the consumption of each equipment or rooms. The purpose is to inform residents about their energy consumption patterns, so they can detect abnormal behaviours and take action to reduce energy costs. Smart meters are an example of an information system[14]. Some of these solutions, such as Eve Energy[15] allow the user to remotely control devices; others use sensors to automatically adapt the house to the appropriate conditions, like the nest smart thermostats[16]. Unfortunately, most of these technologies are not standardised and focus only on one type of equipment (lights or heaters, for example). The main challenges of home smart energy are (i) the compatibility between different equipment and the (ii) the interface between sensors and the existing infrastructure.

To improve energy consumption, wireless sensor networks were deployed in four convenience stores (Chen & Lee, 2011). The sensors collected data on ambient temperature and humidity and an algorithm was developed to determine the ideal temperature. A control system regulated the air-conditioners in order to save energy while keeping the store temperature comfortable for clients. Experiments over three years showed energy savings of 53 percent and the costs of installation of the system were recovered within five months. In an extension of this project (Cheng & Lee, 2014), it is proposed to use smartphones and wearables to understand the behaviours of clients to better adjust the building temperature.

Another example of this field is the Project SWELL by Energy Local corporation[17]. According to UK regulation, energy cannot be traded by private companies. Energy produced locally from harvesting technology such as solar panels feeds into smart grid communities where only one power meter is used, and energy can be inter-exchanged between different sources. The project SWELL consists of 48 houses with testing equipment designed to control electrical devices (in particular storage heaters and water heaters) operated for the duration of a year. The project started in October 2015 and the aim was to monitor the local demand and match it with the correct solar energy generation necessary to support it. The control system then shifts the electricity usage to the solar panel during periods of low price energy, allowing the houses to use different and cheaper energy sources.

The project was a collaboration between Energy Local, Energy Devices, Oxford University, De Montford University, Moixa, West and Energise Sussex Coast. Currently another project is being deployed in Wales. Called Cyd Ynni (Energy Together), it currently installed an updated version of the energy control devices on 100 houses and it was recently shortlisted in the Renewable Energy Association awards[18].

Automatic remote meter reading

The most common approach to collecting energy data from houses is to employ technicians to go by car or foot to every house or building of a neighbourhood to read energy meters. This is not a very scalable and accurate method, and with the rapid growth of cities, it is necessary to employ more people to perform the task and more time to check all the houses.

One possible solution to improve the efficiency of this process is to automatically collect data from meters using sensors or smart meters. EMMNET, heterogeneous wireless sensor network for electricity meter monitoring, was deployed in two cities in China, Huaian and Yangzhou, and collected data from 2024 meters for three months. A number of sensors collected data from energy meters and a group of gateways collected the data from different sensors and sent them to a server for analysis. Residents can monitor their energy cost through a website and electricity providers can remotely monitor the meters. As future work, the developers of the project plan to extend EMMNET to monitor gas and water usage in houses (Lin, et al., 2010).

14. https://www.britishgas.co.uk/smart-home/smart-meters.html
15. https://www.elgato.com/en/eve/eve-energy
16. https://nest.com/uk/thermostat/meet-nest-thermostat/
17. http://www.energylocal.co.uk/projectswell/
18. http://www.energylocal.co.uk/newsletters/newsletter-April-2017/

Monitoring of energy distribution infrastructure

Another application of IoT in the energy field is to monitor the energy distribution infrastructure. The aim is to avoid accidents or detect malfunctions in the transmission lines. Situations like overheating of the conductor's cables and overgrowth of vegetation near transmission lines, for example, may cause blackouts and fires, posing risks for public safety and the local economy.

A wireless sensor network could monitor the vegetation surrounding high voltage transmission lines and detect situations of concern (Ahmad, Malik, Abdullah, Kamel, & Xia, 2015). Vegetation may cause short circuits at power lines. Usually, the visual inspection of these lines is done by technicians nearby or, more recently, remotely using drones. These methods are not very scalable or accurate; a wireless sensor network of cameras capable of acquiring and sending images to a base station is a potential improvement.

The cameras are mounted on power poles near the transmission lines and are responsible for capturing images to save energy. At the base station, an image processing algorithm employs pattern recognition techniques to identify excess of vegetable encroachment near the conductor's cables. In a proof of concept experiment, one camera and one base station were used to measure the feasibility of the system and the accuracy of the image processing algorithm. A graphical user interface was also developed to assist technicians in the monitoring process.

2.3.3 Transport

Urban traffic management

The main application of IoT in the transport sector is in urban traffic management, by informing drivers about potential traffic updates. Traffic has a great impact on a country's economy through productivity and the transportation of goods and products. The quality of fruit and vegetables are particularly affected by the temperature conditions and time spent between origin and destination. (Nellore & Hancke, 2016).

1. **Intelligent transportation systems**
   Just like urban traffic monitoring systems, transport monitoring systems aim to track the public transport network (buses, trains, taxis) to inform users about the arrival time and routing options. IoT offers easier and cheaper methods for local government to monitor and manage transport systems and propose improvements (Alam, Ferreira, & Fonseca, 2016) (Rhoades & Conrad, 2017).

2. **Roadside applications**
   The use of IoT to improve transport efficiency is also relevant outside the urban environment, particularly around accident monitoring and prevention, post-accident management and logistics. Deploying sensors around roads could improve the safety of the drivers, warning about accidents and obstacles, as well as informing drivers in real-time about the best routes.

Trentino Research & Innovation for Tunnel Monitoring[19] is a project founded by the project members of the Autonomous Province of Trento, Italy, that aims to study and monitor the conditions of tunnels around the province. Trento consists of a mountainous area of 6,200 km^2 and great part of traffic to and from the province passes through one of the 150 tunnels. The central application of this project is adaptive lighting, which aims to dynamically adapt the light intensity along the tunnel based on the weather conditions and the illumination level inside the tunnel. Adaptive lightning is both relevant to avoid accidents, especially in two-way tunnels, and to reduce the costs of maintenance and energy consumption. As the lighting conditions vary along the tunnel, especially between the extremities and the middle part, the proposed system also measures the veil luminance, which is the contrast between the tunnel entrance and its backgroun d, in order to adapt the light level to reduce the effects on drivers.

There are challenges involved in deploying a closed loop control system while integrating it with existing infrastructure (Ceriotti, et al., 2011). The initial tests were run in a 260m long tunnel, with 40 sensors and 16 high pressure sodium lamps. Two gateways, responsible to collect the data and send it through the Internet, were installed at 2m and 80m from the entrance of the tunnel. The tests ran for a period of seven months, from August 2009 to February 2010, and helped to understand the main problems caused by the harsh environment of tunnels, such as interference, package collision, responsiveness. During these tests, the authors discovered that the sensors are also useful for detecting fire in the tunnel.

19. http://triton.disi.unitn.it/index.html

Car park assistance

The number of citizens in a city usually grows faster than the scope of services the city can provide. This can cause problems of insufficient resources, such as water, energy, houses and transport. Prof Donald Should, of UCLA, has closely studied the effects of free car parking in his book "The high cost of free parking" (Planners Press, 2011)[20]. According to him, searching for a free parking spot contributes to about eight percent of the traffic congestion. In addition, cars circulating around a city for long periods of time contributes to increasing air pollution levels.

A smart parking system can tackle this problem by monitoring in real time the available spaces and informing citizens through electronic signs or mobile applications. A successful example is Santander Smart Parking[21]. Smart Santander[22], a partnership project between several companies and institutions such as Telefonica and University of Catanbria, designs, deploys and analyses a set of sensors, actuators, cameras and screens to offer useful information to citizens.

This project has been operational since 2012 in the city of Santander, Spain. On of the successful projects is a smart parking platform, which is based on 375 libelium waspmotes across 22 zones in the city. The nodes measure differences in the magnetic field to detect if a parking space is occupied. This parking information is available at visual panels around the roads and on a website.

A smart parking solution is also being employed in the Shanghai International Tourist and Resort Zone, China. In 2015, Huawei, together with Shanghai Unicom and the China Unicom Network Technology Research Institute, initiated the pilot operation of the project using technology based on 4.5G NB-IoT (Narrow Band IoT)[23]. According to Huawei, which provides end-to-end solutions for both the traditional network devices and Narrowband IoT commercial deployment, the deep coverage gains are up to 100 times higher and the level of connectivity provided by Narrowband IoT is over 1,000 times higher than those provided by LTE. The power consumption of Narrowband IoT terminals amounts to only one tenth of that of LTE terminals. In addition, Narrowband IoT only uses the 200 kHz spectrum and can reuse resources of inventory networks to help operators rapidly construct networks. The pilot project of intelligent parking in Shanghai requires that parking stall detectors periodically report status data to the server through Narrowband IoT. Drivers can then conveniently query the stall usage with a mobile application.

Vehicular ad hoc network applications

A recent IoT application in the transport field is the use of vehicular networks for car diagnosis and helping drivers to monitor their driving behaviour. An interface between the VANET of different cars and the sensor network present in roads can be used to automatically control the car speed at roads and avoid accidents (Rasheed, Gillani, Ajmal, & Qayyum, 2017) (Cunha, et al., 2016).

Table 2 below provides an overview of IoT applications to services and technologies.

20. https://books.google.co.uk/books?id=5vzKYgEACAAJ&source=gbs_book_other_versions
21. http://www.libelium.com/smart_santander_parking_smart_city
22. http://www.smartsantander.eu
23. http://carrier.huawei.com/en/success-stories/Products-and-Solutions/chinaunicom_nbiot_smartparking

Use cases	Service provided	Implementation Scale to-date	Critical user network **Individual:** any deployment is beneficial **District:** can be deployed in small areas **City:** needs near city-scale deployment for effect	New infrastructure requirements **Level 1:** Just software **Level 2:** Software and hardware **Level 3:** Software, hardware, and a network	Level of automation **A:** Assimilation of data **AA:** Assimilation and analysis **AAA:** Assimilation, analysis and action
Project AIR - Smart Inhalers (USA)	Health - monitor incidence of asthma attacks	300 inhalers issued in Louisville, USA	**Individual:** Single users can benefit, but more users creates potential for large data analysis	**Level 2:** GPS enabled inhalers and a smartphone application	**AA:** Data is logged, and common problem areas are highlighted so users can avoid these.
HomeAssist – INRIA (France)	Health - illness monitoring, movement tracking	24 participants during 9 months at initial stage. Ongoing evaluation of impact through a randomised control trial with 500 participants.	**District:** can be deployed at houses, hospitals or nursing homes to help both patients and carers.	**Level 2:** the system uses off-the-shelf sensors that need to be deployed at the house. The pervasive software platform is developed by the project and capable of managing different sensors and integrating other applications, such as Google calendar. The system uses the internet infrastructure to communicate.	**AA:** Data is collected and analysed to help patients to improve their quality of life and carers to take better actions.
CitySee (China)	Health - air pollution monitoring	1196 sensors deployed at the Wuxi city in China collecting data since August 2011.	**District** or **City**: can be deployed in a neighbourhood but better results are obtained in a whole city.	**Level 3:** the system uses off-the-shelf sensors installed in tree and post lamps. The software and protocol are developed by the project.	**AA:** Data is collected and analysed for studying the air quality around the city and inform public policy.
EkoBus (Serbia)	Health - air pollution monitoring	65 nodes deployed in buses around 2 cities in Serbia.	**City:** requires the use of the transportation system of a city	**Level 2:** the system uses waspmotes nodes to monitor 6 different environment conditions and track buses' movement. A website and an Android app are used to show the data.	**AA:** The purpose of the project is to inform the population about the pollution levels and buses routes, enabling them to avoid pollution.
SAFECAST (Japan)	Health - nuclear radiation monitoring	The largest open dataset of radiation measurements	**Individual:** a node can be used by one single user around the city. However, the bigger the number of users, the larger the database and more accurate the data collected	**Level 2:** the hardware was developed by libelium using Arduino boards and geisers sensors. The software was developed by different groups like Tokyo Hackspace.	**AA:** Project helped the population of Fukushima, Japan, to measure the nuclear radiation around the city and ask actions from the authorities.
EMMNET (China)	Energy - Remote meter monitoring	2024 nodes were deployed in two different cities in China and tested for 3 months	**District or city:** can be applied at small residential areas or cities.	**Level 3:** it is necessary to install the meter devices at houses and power poles, and use the software and network protocols developed to have better results.	**AA:** The project aims to inform the population and the energy companies about the energy consumption of the houses, so they can act to reduce it.
Project SWELL - energy local (United Kingdom)	Energy - Managing energy costs	48 houses in 3 different villages in Oxfordshire (Watchfield, Shrivenham and Longcot) were tested during a year.	**District:** the aim of the project is to better manage local energy demands	(Few information about the devices)	**AAA:** The system monitors the energy demand and solar energy production, and swaps the different energy sources in order to reduce costs.

Energy Savings at convenience stores (Taiwan)	Energy - Managing energy costs	4 convenience stores in Taipei, Taiwan, were tested during a period of one year	**District:** can be deployed in one or more buildings	**Level 2:** the seeing and control system were developed by the authors, as well as an algorithm to estimate the ideal temperature level.	**AAA:** The system sense and control the environment temperature to reduce the energy costs of the air conditioning.
Santander smart parking (Spain)	Transport - smart parking	375 waspmotes nodes deployed in 22 different zones of the city of Santander. The system has been used since 2012.	**District** or **City:** can be deployed in a neighbourhood but better results are obtained at a city scale.	**Level 2:** sensors and panels need to be installed around the city. Software for collecting data was developed by the project.	**AA:** The purpose of the project is to help drivers to reduce the time spent looking for parking spaces.
TRITon (Italy)	Transport - infrastructure monitoring	Initial stage deployment used 44 sensors and 16 lamps in a 260m long tunnel in the province of Trentino, Italy. Currently deployment is installing 88 sensors in a 630m two-line operational tunnel.	**District:** can be deployed in one or more tunnels	**Level 3:** it is necessary to install sensors and special lamps to adjust the light level along the tunnel. A special communication protocol is also necessary to avoid problems with interference and collisions.	**AAA:** The data collected is used as feedback by the lamps to adjust the lighting levels.
High voltage transmission lines monitoring (USA)	Energy - monitoring the energy distribution infrastructure	Proof of concept one camera one base station system	**District:** can be deployed in small to medium areas with transmission lines	**Level 2:** the camera and base station are off-the-shelf devices that need to be installed at power poles. The image processing algorithm was developed by the authors of the paper.	**AA:** The aim of the project is to analyse the data and identify excess of vegetable encroachment.
MEDISN (USA)	Health - remote patient monitoring	Proof of concept system deployed during 10 days at John Hopkins ER, Baltimore, Maryland (USA)	**District:** can be deployed in one or more rooms in a hospital.	**Level 2:** the sensors and software are custom-built	**AA:** Help doctors and nurses to monitor patients.

Table 2. Inventory of IoT applications to services and technologies
Source: Vivid Economics and Imperial College

3. REVIEW OF TECHNOLOGICAL CHARACTERISTICS

The aim of this section is to set out the key technical concepts to be aware of to effectively plan for and implement an IoT system.

3.1 MIST-FOG-CLOUD ARCHITECTURE

Mist-Fog-Cloud architecture has become one of the most promising backbone technologies for near future IoT applications. In this section, the key technological components of this architecture are described.

3.1.1 Mist computing

Mist computing is a lightweight and rudimentary form of computing power that resides directly within the network fabric. This is at the extreme edge of the network fabric using microcomputers and microcontrollers to feed into Fog Computing nodes and potentially onward towards the Cloud Computing platforms.

Processors

Microcontrollers are low power, low cost micro control units with limited memory and computation power designed to handle simple tasks, including collecting sensor readings, sending control signals to peripherals and performing simple computations. They are typically used with other radio chips that support intercommunication between devices in IoT applications.

- **General micro control units** – Among the different micro control units, the Atmega AVR family micro control units from Atmel (recently acquired by Microchip) are often preferred because of their low cost and the prefiltration of a widely accepted open-source platform, Arduino. MSP430 family micro control units from Texas Instrument are also widely adopted. These micro control units have great computation performance while having relatively lower energy consumption, which is preferable for battery-powered IoT devices, they are relatively more expensive. Although less supported, micro control units produced by other manufactures (e.g. Microchip and National Instruments) can also be good solutions as per requirement.
- **IoT Dedicated micro control units** – To better support IoT applications, some manufacturers start producing micro control units that are dedicated for wireless sensor networks, which typically consist of low-power, low-cost sensing devices that communicate through radio frequencies. These micro control units have integrated radio functions and are capable of communicating through radio frequencies without having additional radio controllers. This can potentially reduce costs and barriers to implementation. Micro control units CC2650 (2.4GHz) and CC1350 (868MHz) from Texas Instrument and Atmega128 RF from Atmel are state-of-the-art products. They are widely used by open-source projects and IoT technology companies.
- **Powerful micro control units / central processing units for Embedded Systems** – To handle complex tasks and computations, ARM cortex-M series and Intel Edison are more powerful alternatives while ARM cortex-A series is also adopted in some higher performance applications. Although they consume much more power than aforementioned micro control units, they can be energy efficient compared to ordinary central processing units as they are designed for embedded systems with better power efficiency. Due to their higher power consumption and computational power, they can be used in gateways or Fog servers where data collected from IoT devices is pushed onto the Clouds through Internet.

Networks - Wireless communication technologies

Wireless communication is one of the key components in IoT. Currently the most commonly used are:

- **Traditional wireless communication protocols (all in star topology with various power consumption)**
  - **Wi-Fi (900MHz, 2.4GHz, 5GHz)** – widely used wireless communication protocol providing reliable high-speed links. However, it consumes a lot of power and has a limited communication range (about 10m-100m as per scenario and frequency).
  - **Bluetooth (2.4GHz)** – Low energy bluetooth provides lower bandwidth than Wi-Fi; however, it is more power efficient and therefore more suitable for battery powered devices. It also has limited communication range (about 10m).
  - **GPRS (850/900/1800/1900 MHz)** – Cellular mobile network is a sophisticated infrastructure that is readily available in most developed cities for long distance communication. The maximum network capacity is caused by RF interferences (i.e. Shannon theory) and power consumption is high.
- **IoT dedicated protocols (allows multiple topology and lower power consumption)**
  - **IEEE 802.15.4 (2.4GHz and 868MHz)** – This is a standard for low-rate wireless personal area networks (LR-WPANs). It was originally designed for lower-power light-weight smart devices in wireless sensor networks. It provides multiple network topologies and therefore devices are easy to install; however, due to its limited RF coverage, it cannot guarantee reliable communication. Most of the IoT dedicated products (e.g. TI CC2650) and RF modules (e.g. XBee) supports this protocol.
  - **LoRa** – This new RF technology was released in 2013. As an RF protocol that is dedicated to IoT applications, it is a Low-Power Wide-Area Network (LPWAN) technology that has significantly longer communication range (e.g. >15km in the wild) while remaining power efficient. It can operate in different frequencies (i.e. 433MHz is used in Asia, 868GHz in Europe and 915MHz in North America).
  - **NarrowBand IoT** – Narrowband IoT is another LPWAN radio technology that was released after LoRa. It is designed for low-power smart devices with low data transmission rate (i.e. maximum 250kbps). As part of the LTE standard, it is naturally comparable to the current cellular infrastructure. Compared to LoRa, smart devices with Narrowband IoT are easy to deploy in the areas with cellular coverage. LoRa can be more secure because it uses private networks.
  - **Sigfox** – This is another narrow band solution which provides about 300bps. It is very power efficient and typically much cheaper than LoRa and Narrowband IoT. However, it only accepts uplinks (i.e. only end devices can send data to base stations). This limits its usability and applications.
  - **LTE-M** – This is a new LTE standard designed for machine-type communications . Its 1.4 MHz standard can provide a higher data rate (i.e. 1M Mbps in theory and about 512kbps in practice) then Narrowbang solutions. As it works within the current LTE networks, the current cellular network can be easily upgraded by uploading new software to turn on this new feature.
  - **NB-LTE-M** – This is a narrowband version of LTE-M, which uses 200kHz instead of 1.4MHz, providing longer transmission distance.

Software - Operating systems[24]

- **TinyOS –** Initiated in 2000 by UC Berkeley. It is an open source operating system dedicated to wireless sensor networks under a Berkeley Software Distribution (BSD) license. It comes with a software network simulator, Tossim, which is a text-based simulator that is lightweight. It can be run on microcontrollers with very limited resources, it is able to handle different types of applications

24. Those solution listed are all open-source. We are not aware of any closed proprietary systems that would be relevant to this market.

and it has good energy conservation mechanism. However the programming language (necC) is not straightforward for general use and the maintenance is discontinued, the latest version was released in 2012.

- **Contiki** – The project started since 2003. It is an open source operating system dedicated to a wireless sensor network and IoT applications under a BSD license. It also comes with a software network simulator, Cooja. It provides graphical interfaces allowing developers to test their designs and protocols with simulations. It is supported by more than 30 platforms. Among all, SensorTags (both CC2650 and CC1350) are the primary Contiki platforms providing complete tool chains for wide applications.

- **Linux** – Arch Linux is a lightweight simple open source Linux that is widely adopted in IoT applications under General Public License, which requires all modifications to be open source. It provides more sophisticated drivers and tools then the aforementioned two operating systems; consequently, it also requires higher processing power and memory and is typically used to run on more powerful processors such as Intel Edison or ARM core-A series. Due to its computation and resource management capability, it can also be used on lightweight Fog servers.

- **OpenWSN** – Instead of an operation system, OpenWSN provides open-source implementations of a complete protocol stack based on IoT standards, on a variety of software and hardware platforms including Linux, Windows and OS X (macOS) platforms.

3.1.2 Fog computing

Fog computing, also known as Edge Computing or fogging, refers to the edge of an enterprise's network. It facilitates the operation of computation, storage, and networking services between end devices and the Cloud in the enterprise's network. It has a medium weight and intermediate level of computing power.

As an intermediate layer in the three-tier architecture, Fog servers are typically in forms of gateway at the edge of the network as opposed to servers in a data centre. They are typically maintained by utility companies and services are provided in collaborative manner. OpenFog Consortium plays a significant role in the development of fog computing. Many leading companies including ARM, Intel, Cisco, Microsoft, At&T and Foxconn are members in this Consortium.

The main objectives of Fog Computing can be summarised as follows:

- **Minimised latency and fast response time.** As the edge node in local areas, Fog servers should be able to make local decision that quickly respond to local requirements. Which place is best depends partly on how quickly a decision is needed. Extremely time-sensitive decisions should be made closer to the things producing and acting on the data. In contrast, big data analytics on historical data needs the computing and storage resources of the Cloud.

- **Collective data/stream processing.** Due to the typically high volume of IoT data and the limited capacity of existing information communication technology infrastructures, it is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the Cloud. Nor is it necessary, because many critical analyses do not require Cloud-scale processing and storage.

- **Multitenancy.** As Fog servers typically work in a collective manner, it is practical to build a multi-tenancy infrastructure that can be shared by multiple users. Here, resource allocation, pricing and scheduling become important issues that have to be handled by the Fog system. Also, security and privacy become more practical issues for operators as channels and servers are shared by multiple users.

- **Operation reliability.** IoT data is increasingly used for decisions affecting citizen safety and critical infrastructure. The integrity and availability of the infrastructure and data cannot be in question.

3.1.3 Cloud computing

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store,

manage, and process data, rather than a local server or a personal computer. Cloud Computing can be a heavyweight and dense form of computing power.

Massive amounts of cross-disciplinary data streams (e.g. medical observations and sensor readings) are continuously generated by billions of smart devices in the Mist. Rich knowledge and insightful information can therefore be obtained by applying stream queries and analytics, such as similarity search, clustering, and regression. All these computations require heavy computing power which can only be provided by the Cloud.

Small-scale data analysis and visualisation

For small scale users, a simple easy-to-use solution can be a better option than the complex Cloud solution. To this end, one of the more reliable online solutions is Mathwork Thingspeak. It's a relatively light weight solution providing basic data analysis tools and online data visualisations. It can also be easily integrated with Matlab and provides online functions that can generate Matlab programmes as per user requirements.

Large scale big data and stream processing

To better handle the massive amounts of cross-disciplinary data streams for complex tasks, large-scale solutions are required. One of the most widely accepted Cloud solutions is Hadoop ecosystem. This ecosystem enables various distributed Cloud services including, data management, task allocation, data stream processing and distributed machine learning. Users can construct their own Cloud with the services provided as per requirement.

There are multiple off-the-shelf online Cloud-based solutions. The most sophisticated solutions currently available for general users are Microsoft Azure IoT Suite and Amazon AWS IoT. Both solutions are based on their previously developed Cloud infrastructures (i.e. Azure and AWS). In addition, Google Cloud Platform provides an IoT interface accepting massive amount of streaming data from IoT devices; while IBM Watson IoT provides a complete IoT solution for enterprise users with better integrated AI and machine services.

3.2 CHALLENGES AND OPPORTUNITIES RELATING TO THE OPERATING ENVIRONMENT

The purpose of this section is to outline the key challenges and the opportunities for mitigating them.

Developers are aware that the operating environment can potentially impact the success of an IoT intervention, however they are often unprepared for what occurs in practice. Many deployments of IoT systems may overlook the definition of the environment in advance of deployment. They may have an idea of the type of environment, and measure the system's performance only after deployment. Due to the complexity of the natural and ICT environments in which the system may be placed, developers tend to make generalising assumptions regarding how the environment will impact the system at design time. When testing at a pre-deployment stage, typically using simulators, these assumptions are sufficient. However, real-world behaviours may impact the performance of the deployment either at implementation time or later while operational as the environment changes (Stankovic, 2004).

3.2.1 Challenges

The physical city environment presents challenges because it consists of objects made from many differing materials, buildings of various heights, mobile objects such as cars and people etc. and all of these affect the radio signal's ability to transmit data, but also can impact the safety and security of the box that hosts the IoT units. For example, squirrels can eat through waterproof plastic. The physical space dictates the characteristics of the housing of the system in terms of size, human interaction and aesthetics. Further, the hardware components in the IoT devices will have been designed and tested with an operational environment in mind and will guarantee operation within those bounds. For example, a sensor reading may provide accuracy of measurement between -30 and +40 degrees Celsius but may lose accuracy if placed in an environment with temperatures beyond those bounds. The microcontroller may also begin to produce errors in extreme temperatures etc.

Physical disruption can also occur inside the IoT device itself. Even with watertight boxes, in some atmospheres, the environment inside the box can change and affect the device. For example, the deployment of devices in soil in watertight boxes may find that humidity builds up inside the box and makes it faulty. Therefore, it is not unheard of to include sensors inside the device to understand its operating conditions to understand if a fault will occur.

IoT systems are susceptible to network disruption. Many IoT systems in urban environments benefit from the flexibility of using wireless communication to transfer data. The shape of, and materials in, the physical environment can impact wireless transmission and the main physical effects are: attenuation, reflection, scattering, diffraction, and refraction. The first three effects are most concerning. Attenuation of the radio signal is where the signal strength becomes weaker as the signal is sent over greater distances. Some networks are designed to be used over larger distances (LPWA networks) and they can add power to the signal to provide strength across the distance or operate at lower frequencies which travel further.

IoT systems are often incompatible with systems already in place (backward compatibility) or future installations (forward compatibility). Related to good planning procedure and requirements capture, a suite of IoT devices may be required to be operational over longer lifespans and therefore forward and backwards compatibility should be part of the maintenance programme. IoT nodes with more traditional operating systems (or those that are essentially a mobile phone) will have the benefits of the compatibility that the mature system brings. However, compatibility, much like standards, are often largely ignored. As the subject matures, this issue will come to the fore and therefore there are opportunities to discuss how this should manifest now.

IoT system often suffer from being challenging to deploy due to technical complexity. Networked IoT systems promise a smart world revolution. However, real-world examples are proving notoriously difficult to deploy and maintain, and as yet only relatively small scale successes have been well publicised. Scientific problems with IoT systems strike hard against the limits of knowledge about how to organise, analyse, and adapt large, loosely-coupled, intercommunicating, and increasingly autonomous, distributed systems. This topic is timely because there is mounting pressure from various industries and government bodies to be able to place their trust in sensing based infrastructures for decision-making.

Further interactions with the system may introduce more complexity. For example, an IoT system for water sustainability may monitor water distribution systems for leaks and then move water away from the leaks so as to save water. This requires a sophisticated monitoring and control solution to operate in semi-real time. Essentially, two networks are operational, the cyber system which consists of hardware, software, and communications infrastructure and the water network itself. The cyber network's behaviour is one of data flows and has digital properties, the water network adheres to the laws of physics and in particular hydraulics that determine the pressure, flow and movement of water in the pipe.

If we have an IoT system controlling this, we have a tight interaction between the cyber and the physical system. Further, if we use vibrations on the pipe to supply power to the cyber system (ie the IoT device has energy harvesting hardware attached) we are not only controlling the movement of water but also the ability of the cyber system to operate. That is, we can send more waves down the pipe to generate power for the IoT node. The interactions between all these systems are complex and as such, at the moment we do not have techniques and methods to sufficiently understand or predict. However, there are a number of initiatives beginning to address this problem. These projects will treat the IoT system not in isolation but as part of a system of systems, whereby the environment and operational surroundings of the systems are involved in the development and operation of the computer based system. Nevertheless, many systems can be deployed without deep understanding of such interactions; with enough adaptivity such as auto-reboot when the node misbehaves sufficing to fix many of the unforeseen problems.

3.2.2 Opportunities

There are opportunities to mitigate the impact of the physical environment. For example, wireless radio signal strength drops as it is sent over longer distances and signal reflection, scattering and fading impact the delivery of data network protocols and

hardware designed for long-ranges of kilometres are quite different from those that are designed to transfer data over short hops of metres and practitioners are able to select the appropriate system based on the design requirements. The constraints associated with the results of requirements analysis should indicate the costs, performance characteristics, size of units, power available etc. that are suitable for the project and these must be traded off against the environment's impact on the system. Practitioners may also articulate the ethics of the system in terms of how it impacts on its environment.

A first general principle is that radio signals sent between IoT units without objects interfering with them (ie line of sight) will be more successful. Examples where data was sent with buildings or people between sender and receiver were less successful (as people are largely comprised of water, they are very good at absorbing radio signals). Also, metal objects interfere and one should be cautious of not placing devices near them.

A second principle is that placing transmitters as high as possible ensures a better line of sight transmission and fewer data errors. The remaining physical effects are due to the signal bouncing off buildings, rough surfaces etc., impacting the signal's ability to successfully send data. Most modern transceivers are able to accommodate signal bounce.

To improve reliability, some IoT systems may mix wireless and wired communication. Typically, it is easier to use wireless devices where it is more difficult or expensive to run wires to either power up or support wired communication. However, in many instances such devices then communicate to a gateway device and many of these gateway or base-station devices are laptop-class computers that are powered from the mains and wired to the Internet. Many wired devices may communicate to a single gateway device. An example of using existing infrastructure is smart meter systems that use Internet in the home to send data. Network disruption can affect the link between the IoT devices and interfere with analytics. Where the IoT device is measuring or recording sensor data, the IoT device may continue doing so and attempt to send data to no avail, meaning the data is lost or storage on the device fills up and the device fails.

An alternative approach is to build an adaptive feature into the design of the system to cope with environmental change (Khan, 2015). Examples of this can be found in the mesh-based routing mechanisms that detect the failure of any links in the data transfer chain seek alternative ways to route data across the network. This essentially provides the same sort of resilience as what is found in the Internet.

For many practitioners, the complexity of IoT systems to support urban environments rests with choosing the correct hardware, coding up the application and deploying it in environments. Although IoT systems are traditionally composed of simple devices, there is an underlying set of complexities that are not yet well understood and may cause system failures. For example, deploying a small subset of devices to test an IoT idea may allow the practitioner to debug the software, but it will not capture all behaviours and when deployed on a larger scale the system may behave differently.

Scaling a system requires an understanding of each of the devices in that system and any reliance between those devices. When the network is dense, offline devices can be compensated with alternative routes through the network that enable communication. However, if the network is sparse (or becomes sparse due to battery depletion or node-sleeping), there are fewer options and communication is more likely to be interrupted. However, denser networks, or networks in close proximity to one another, are more prone to interference.

3.2.3 Security and privacy risks

Cyber security is a serious concern for IoT devices. The focus on producing minimally viable products can result in poor security measures and update practices. The security risks that come with IoT deployments are often fodder for headlines about maligned refrigerators and hackable pacemakers. However, these extend beyond a single device hack which was demonstrated through several highly-publicized distributed denial-of-service (DDoS) attacks in 2016. Compromising IoT products for use in botnets (which are needed to launch DDoS attacks) poses a risk when IoT products are shipped with no password protections, or using default passwords for local access. Attackers are able to identify these products quickly and employ them for their malicious purposes.

In developing new solutions for IoT, one must consider the larger context and implications of security and privacy from the very beginning. Also, they must keep in mind that people purchase IoT devices as objects of everyday use. The first thought after buying a smart refrigerator for instance is more likely going to be "How do I adjust the temperature?" rather than "How do I update security settings?". The benefit of collecting data on, for instance, smart meter operations, has to justify consumer exposure to new privacy risks.

IoT devices are often deployed in accessible areas which makes them vulnerable to all kinds of physical attacks. On the other side, to make IoT deployments economically viable, many limitations in energy, communication and computations are imposed onto devices at the expense of security (Perrig, 2004). Due to the physical exposure and resource restrictions of IoT devices, security techniques used in traditional networks become inadequate and alternative security mechanisms are needed. An example could be traditional key-establishment protocols that do not scale well with hundreds or thousands of sensor nodes. Besides the physical exposure and resource restrictions of IoT devices, data security as a concept is new to many manufacturers and there is limited security planning in development methodologies. To keep prices affordable, security sponsorship and management support may be limited. Standards and reference architecture for secure IoT systems are not yet clearly defined and recruitment of experts in the field can present a challenge.

Traditional systems security practice is based on three main requirements (Whitman, 2012):

- **Confidentiality** – the use of cryptography measures for the data encryption at the endpoint devices to prevent information disclosure to unauthorised users.
- **Integrity** – the assurance that the data transmitted cannot be altered during transmission until it reaches its original destination.
- **Availability** – to ensure the persistent connectivity, i.e. endpoint devices must be able to constantly communicate with each other, end-users, and back-end services.

However, the security needs in the IoT are higher. This is because IoT systems include numerous interactions among different components, operate in a heterogeneous set of networks, involve cyber-to-physical connections and run on volatile and dynamic networks (Ali, 2015). For example, if the IoT network is improperly configured or deployed an attacker may intercept traffic between devices and Cloud-based management systems (known as man-in-the-middle attack). A flood of false traffic may overload the device disable the system.

The wide range of IoT strategies, programmes, and systems requires different levels of security. There are many factors to consider when choosing the appropriate security mechanisms, including the physical environment, the type of end points, the type of data to be collected (high or low value, personal data), connectivity (constantly connected to the Internet, intermittently connected, or not connected at all), etc.

There are opportunities to incorporate security into design. To sufficiently protect the network, devices, data and applications, the following five security functions are the minimum required:

1. **Identity** – More intelligent devices with sufficient processing power will be capable of announcing themselves to the network in the identification phase. Embedded modules may provide additional support. Identity verification, such as complex usernames and passwords, enhance protection from botnets. Ideally, all IoT devices in an IoT system will feature security hardware or crypto processors. An example is the Embedded SIM, a new secure element for mobile networks, which is designed as trust anchor that integrates security by default.

2. **Access and User Management** – Simple hardware steps, such as encrypting and anonymising chips, automatic lock-outs based on idle time or maximum attempts to authenticate, help to prevent unauthorized users getting access to a device. A remote control facility is particularly important under deployment in harsh or difficult to access environments. Adequate access control is needed to allow the device to access resources that support its specific role only.

3. **Encryption** – Encryption is a challenging part of IoT security because it directly relates to the level of protection the customer may need and the protocols used in the IoT device. Encryption algorithms must have a small processing footprint so that they can be applied to low-memory and low-energy IoT devices. To avoid data leaks, data needs to be protected while at rest, in transit, and in use, which usually leads to encryption at multiple points.

4. **Analytics** – The security system should follow the development of IoT devices. As these become smarter, the security system should too. Therefore, one should be aware of the latest advances and prepared to update the systems as new technologies are released.

5. **Network Security** – The security of IoT devices and gateways is not enough if the network itself is not secured. More connected devices mean more traffic on the network, which can be seen as a weak point of IoT solution if not handled properly. Network traffic monitoring is usually needed, in addition to device and endpoint management.

The security life cycle does not stop at this juncture. This ever changing ecosystem requires continuous service throughout its lifetime. The same applies to the security requirements, which change over time in order to ensure confidentiality, integrity, availability, authenticity, or any other security requirement. For example, cryptographic algorithms may become outdated or deprecated, unable to counteract new attacks and new ways to defend might be needed. It is unrealistic to expect manufacturers to create software products that are bug-free; thus the update availability and adequate support has to be provided where communication with stakeholders is absolutely necessary. Software updates can often be automated and they are less expensive than hardware replacement. However, their authenticity and integrity have to be verified.

Guidelines for the IoT security have been produced. A good example of how to apply the set of guidelines to evaluate the IoT device/service is given in IoT Security Guidelines provided by GSM Association [GSMA guideline]. The security model is evaluated from the perspective of the endpoint and the service side, respectively, where a simple heart rate monitor, a small personal drone device and a vehicle sensor network are used as examples. Figure 3 below summarises four examples of existing IoT security guidelines.

New York City Guideline **[NYC guideline]** Can be used for deployment of an IoT solution in a public space (e.g. parks, public buildings, etc.) or using City assets (e.g. City government funding, light poles, etc.).	***IoT Security Guidelines*** **from GSM Association [GSMA guideline]** Developed for the benefit of service providers who are looking to develop new IoT services to provide recommendations on how to mitigate common security threats and weaknesses within IoT Services.
Special Publication 800-160 (the "Guidance") **from National Institute of Standards and Technology (NIST) [NIST Guideline]** Provides a framework for software engineers to better address security issues and to develop more defensible and survivable systems in a sustainable manner throughout the life cycle of these devices.	***Strategic Principles for securing the Internet of Things (IoT)*** **from U.S. Department of Homeland Security [Homeland guideline]** Provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Figure 3. Examples of existing guidelines [25]
Source: Imperial College

25. [NYC guideline] https://iot.cityofnewyork.us/ ; [NIST guideline] http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf ; [GSMA guideline] http://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/ ; [Homeland guideline] https://www.dhs.gov/securingtheIoT

4. COMMON PITFALLS

This section sets out the common pitfalls in IoT applications where a technical guidebook could provide support. This motivates the Technical Guidance document.

4.1 TECHNOLOGY DRIVEN RATHER THAN SERVICE DRIVEN APPLICATION

Many IoT systems have failed because they were designed with technology rather than service demand in mind. Successful IoT solutions are often based on identified problems and needs of customers and using technology to address them. This applies equally to the connectivity aspect of IoT, which enhances the value of products, but does not by itself provide enough motivation for customer purchase.

The appeal for innovative and ubiquitous connectivity aspects of IoT technology can result in the adoption, of products and services. The early adoption, may deliver short-term benefits, but technology can become rapidly obsolete because of the unprecedented pace at which it evolves. IoT solutions therefore need to adapt with technology.

To prevent this situation, companies have to introduce a clear set of requirements, which determine the different features provided by their products and services as well as operational conditions. This stage is called requirement analysis and is a well-established practice in the domain of software engineering.

4.2 NAIVE DESIGN DECISIONS

Undeniably, to experience the usefulness of IoT technology, the design of products and services is critical to ensure their usability, paving the way for successful adoption. That is why companies must rely on experts in user-centred design who understand end users and the experience they are looking for. However, in practice, design decisions are often taken by technologists themselves and are based on intuition rather than fundamental knowledge of user-centred design.

The HomeAssist project[26] is a good example demonstrating the importance of multi-disciplinary knowledge in the design of IoT products and services. This project proposes a systemic approach to introducing an assisted living platform for old people. The aim of this project is to improve people's well-being and the efficiency of the caregiving environment. To achieve these goals, HomeAssist has been designed by a trans-disciplinary team of experts in the field of assistive technologies, human factors and human-computer interaction, as well as software engineers and caregivers. It is important to highlight that HomeAssist has been successfully adopted by elderly mainly because of effective platform design. Furthermore, the absence of experts in the design of the platform could have had catastrophic consequences for users since IoT technology is used to ensure their safety and security.

4.3 POOR INTEROPERABILITY

To harness the full potential of IoT, innovative products and services critically rely on applications. To enable the development of applications for IoT, companies must accompany their products and services with application programming interfaces (APIs). APIs

26. http://phoenix.inria.fr/research-projects/homeassist

are crucial for programming applications in the IoT as they abstract low-level details of devices and expose their data and functionality to a wide audience of software developers. Companies mostly provide end-user applications for their IoT solutions. However, APIs allow programmers to come up with innovative user scenarios that may go beyond the initial use cases, thus exploring the full potential of IoT.

5. CONCLUSIONS

This evidence review sets out a summary of the key applications and technological concepts associated with IoT, design challenges and opportunities for IoT purchasers, and common pitfalls that have occurred in practice.

A wide range of IoT applications have been implemented and this review is focused on those providing public benefit. In order for public authorities to select opportunities, it is important to identify the potential for public benefit, the scale at which this benefit becomes material and the reliability with which the benefits can be delivered. This may require the implementation of additional marketing, education, awareness or incentives to ensure correct usage.

Cloud-Mist-Fog computing provides the backbone of IoT architecture. Not all of these aspects are required for all IoT opportunities. It is important to understand, at an early stage, if the IoT application simply requires new software, devices, support systems or new underlying network infrastructure to operate successfully.

The key design challenges are the physical environment, network disruption, complexity, security and forward and backward compatibility. A number of opportunities exist for addressing these challenges, including avoiding physical interference, combining wired with wireless technology, building adaptiveness into the design so that problems are addressed as they occur, and choosing the correct hardware.

As a result of these challenges, a set of common pitfalls have occurred in practice. These include:

- Technology rather than service driven deployment
- Not specifying the requirements of IoT deployment in detail
- Poor design leading to poor usability of devices and/or software
- Lack of expertise on software design
- Poor interoperability.

In order to avoid these pitfalls in future, purchasers of IoT should follow technical guidance for IoT applications, including the design, deployment, monitoring and evaluation. This Annex is supported by a Technical Guidance document, which sets out the key steps in deploying IoT in a way that maximise the chances of success.

REFERENCES

Ahmad, J., Malik, A. S., Abdullah, M. F., Kamel, N., & Xia, L. (2015). A novel method for vegetation encroachment monitoring of transmission lines using a single 2D camera. Pattern Analysis and Applications, 18(2), 419-440.

Alam, M., Ferreira, J., & Fonseca, J. (2016). Introduction to Intelligent Transportation Systems. In M. Alam, J. Ferreira, & J. Fonseca, Intelligent Transportation Systems (Vol. 52, pp. 1-17). Springer International Publishing. doi:10.1007/978-3-319-28183-4_1

Ali, S. Q. (2015). Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable Pipeline Condition Monitoring. Sensors 15, (pp. 7172-7205).

Ceriotti, M., Corrà, M., D'Orazio, L., Doriguzzi, R., Facchin, D., Gună, S., . . . Torghele, C. A. (2011). Is there light at the end of the tunnel? Wireless sensor networks for adaptive lightning in road tunnels. 2011 10th International Conference on Information Processing in Sensor Networks (IPSN).

Chen, C. S., & Lee, D. S. (2011). Energy saving effects of wireless sensor networks: A case study of convenience stores in Taiwan. Sensors, 11(2), 2013-2034.

Cheng, C.-C., & Lee, D. (2014). Smart Sensors Enable Smart Air Conditioning Control. Sensors, 14(6), 11179-11203. doi:10.3390/s140611179

Churkina, G. (2008). Modeling the carbon cycle of urban systems. Ecological Modelling, 216(2), 107-113. doi:https://doi.org/10.1016/j.ecolmodel.2008.03.006.

Cunha, F., Villas, L., Boukerche, A., Maia, G., Viana, A., Mini, R. A., & Loureiro, A. A. (2016). Data communication in VANETs: Protocols, applications and challenges. Ad Hoc Networks, 44, 90-103.

Economics, V. ([Month] [Year]). Type report name here in Italics. report prepared for: [Type client name here].

Hossain, M. M. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,., (pp. 21-28).

Khan, F. M. (2015). Wireless sensor network based flood/drought forecasting system. Sensors 15, (pp. 1-4).

Ko, J., Lim, J. H., Chen, Y., Musvaloiu-E, R., Terzis, A., Masson, G. M., . . Dutton, R. P. (2010). MEDiSN: Medical emergency detection in sensor networks. ACM Trans. Embed. Comput. Syst., 10(1). doi:http://dx.doi.org/10.1145/1814539.1814550

Lin, Z.-T., Zheng, J., Ji, Y.-S., Zhao, B.-H., Qu, Y.-G., Huang, X.-D., & Jiang, X.-F. (2010). EMMNET: sensor networking for electricity meter monitoring. Sensors, 10(7), 6307-6323.

Liu, Y., Mao, X., He, Y., Liu, K., Gong, W., & Wang, J. (2013). CitySee: not only a wireless sensor network. IEEE Network, 27(5), 42-47.

Nellore, K., & Hancke, G. P. (2016). A Survey on Urban Traffic Management System Using Wireless Sensor Networks. Sensors, 16(2), 157.

Perrig, A. S. (2004). Security in Wireless Sensor Networks. Communications of the ACM, (pp. 53-57).

Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications. Vehicular Ad-Hoc Networks for Smart Cities, pp. 39-51.

Rhoades, B. B., & Conrad, J. M. (2017). A survey of alternate methods and implementations of an intelligent transportation system. IEEE SoutheastCon 2017. Charlotte NC: IEEE. doi: 10.1109/SECON.2017.7925303

Stankovic, J. A. (2004). Research challenges for wireless sensor networks. SIGBED Rev., , (pp. 9-12).

Whitman, M. a. (2012). Principles of Information Security. 4th ed., Cengage Learning.

Get in touch:

IoTUK.org.uk

Info@IotUK.org.uk

@IoTUKNews

CONTACT US

Vivid Economics Limited
26-28 Ely Place
London
EC1N 6TD
United Kingdom

T: +44 (0)844 8000 254

E: enquiries@videconomics.com

COMPANY PROFILE

Vivid Economics is a leading strategic economics consultancy with global reach. We strive to create lasting value for our clients, both in government and the private sector, and for society at large.

We are a premier consultant in the policy-commerce interface and resource and environment-intensive sectors, where we advise on the most critical and complex policy and commercial questions facing clients around the world. The success we bring to our clients reflects a strong partnership culture, solid foundation of skills and analytical assets, and close cooperation with a large network of contacts across key organisations.

: videconomics