UNOFFICIAL MACHINE TRANSLATION

Integrating communication elements of the Internet of Things (IoT) and 5G networks

Prepared for the Ministry of Industry and Trade

30 September 2024

UNOFFICIAL MACHINE TRANSLATION

Contents

Definition of Terms

Defining key terms provides an important foundation for the subsequent sections of the study and for its practical implications.[1]

IoT (Internet of Things): The Internet of Things is a system of uniquely identified devices that collect data, which is then transmitted via the internet, analysed and evaluated, and on the basis of which actions may be carried out within or outside the system. This system has a clearly defined purpose, which is typically to increase the efficiency of processes, performance, awareness, etc.

IIoT (Industry IoT/Industrial Internet of Things): IIoT is a subset of IoT focused on industrial applications. It involves the interconnection of industrial machinery and sensors for real-time monitoring, data collection and analysis. IIoT is widely used in manufacturing, the energy sector and logistics to improve operations, safety and predictive maintenance.

mMTC (Massive Machine-Type Communication): mMTC refers to a type of IoT communication that supports a large number of low-power devices that need to be connected simultaneously. This technology is designed for applications requiring many connected devices, such as smart cities, agriculture and environmental monitoring.

Mission-Critical IoT: Mission-Critical IoT refers to IoT applications that require extremely high reliability, low latency and guaranteed performance. These applications are typically used in scenarios where failure could have serious consequences, such as autonomous vehicles, industrial automation and remote healthcare services.

Massive IoT: Massive IoT focuses on the deployment of large numbers of simple, low-cost and low-power devices that generate small amounts of data. This category of IoT is suitable for applications such as smart metering, environmental sensing and monitoring, where devices need to operate for long periods without maintenance and are usually battery-powered.

Mid-Range IoT: Mid-Range IoT encompasses applications that fall between Critical IoT and Massive IoT. These systems strike a balance between performance, reliability and cost. They are suitable for use cases such as building automation, smart lighting and connected appliances.

IoT system: A system providing the functionalities of the Internet of Things. An IoT system may include, amongst other things, IoT devices, IoT gateways, sensors and actuators.

IoT device: An end point that interacts with the physical world through sensing or control. An IoT device may be a sensor or an actuator.

Actuator: Typically a component of a mechatronic system (machines combining electronics and mechanics) that converts the informational part of a process into a technical one – for example, a command to change direction is converted by the actuator into the mechanical energy required to deviate from the machine’s current direction of movement. In the context of the IoT, an actuator is an end device that enables two-way interaction (rather than merely one-way sensing, as with a sensor).

[1] Note: Czech vs. English terms. As in many specialist fields, there are a number of terms in the fields of IoT, 5G and related solutions for which no suitable Czech equivalent has been established. As a matter of principle, newly introduced terms will also be in English, as is the case with most specialist literature. It is therefore sometimes necessary to use the original English term, or to use both the English and Czech equivalents. Another reason for using English terms is to enable users to search for further information on the topic. This is straightforward when using the original English term; using an unestablished Czech equivalent could prove problematic.

Sensor: An IoT device capable of sensing the state of its surroundings or surrounding phenomena.

IoT gateway: An entity within an IoT system that connects one or more neighbouring networks and the IoT devices within those networks to one another, and to one or more access networks using different protocols.

Further terms:

Use case	The general definition of a use case is as follows: The term 'use case' refers to a specific situation or scenario in which a product or service can be used. For the purposes of this study, a use case is defined as follows: "A task that a company needs to carry out in order to achieve a specific outcome." This definition is appropriate in that it emphasises the fact that a use case serves to achieve a specific outcome, or a range of different desired outcomes (for example, increasing process efficiency, minimising risks to employees, minimising waste, etc.).
Case Study	A specific implementation of a use case. Within a case study, a specific solution is used to fulfil the task defined in the use case. That is, a particular technology, products and services from a specific provider. Regardless of whether this implementation is already in commercial operation, or whether it is a demo implementation or a proof of concept.
Digitalisation	• Digitalisation usually focuses on specific processes or operations within an organisation. • The aim of digitalisation is to replace traditional, analogue and paper-based procedures with digital technologies in order to increase efficiency, reduce costs and improve operational management. • Digitalisation can involve automation, the transition to digital systems and processes, the elimination of paperwork, and the optimisation of specific areas of a business.
Business digitalisation	Digitalisation uses digital technologies to transform business processes and provides new opportunities for creating value. It involves converting existing analogue information into digital formats, as well as certain processes that companies can carry out more effectively using the latest technologies and tools. The aim of digitalisation is: • to increase productivity, • to improve service quality and thereby creating a competitive advantage for the business by using information and communication technologies (ICT) to streamline processes.
Digital transformation	• Digital transformation is a broader and more comprehensive concept that involves a complete overhaul of a company's strategy, culture and operations through the use of digital technologies. • It is a strategic approach that may involve the restructuring of business models, changes to business processes, the implementation of new technologies and the transformation of corporate culture. • Digital transformation need not be limited to specific operations; it can involve radical changes across the entire business ecosystem to ensure the organisation is better adapted to the digital environment and innovation trends.
Edge Computing	Edge computing refers to the practice of processing data close to the edge of the network, where the data is generated, rather than in a centralised data processing centre. 'Edge' in this context can refer to any computing and networking resources along the path between data sources (such as IoT devices) and cloud data centres. Edge computing reduces the need to send data back and forth to a central server, thereby reducing latency and bandwidth usage.
MEC (Multi-access Edge Computing)	Multi-access Edge Computing (MEC) is a network architecture concept that enables cloud computing and IT service environments at the network edge. MEC brings computing resources closer to where data is generated and consumed, reducing latency, improving processing speed and enhancing the user experience. It is often associated with mobile networks, particularly 5G, where it can process data in the vicinity of mobile base stations or other network access points. The difference between MEC and edge computing: MEC is a subset of edge computing, specifically designed to optimise network architectures and improve application performance in mobile networks, including 5G. It focuses primarily on the mobile edge, extending services within mobile network environments. In contrast, edge computing is a broader concept applicable across various networks and sectors, including the IoT, manufacturing, healthcare and others, regardless of whether the networks are mobile or fixed. Integration with mobile networks: By its very nature, MEC is designed to integrate closely with the operation of mobile networks, particularly 5G, facilitating services such as content caching, real-time processing and context-aware services. Edge computing, whilst it can operate on mobile networks, is not inherently tied to these networks and can be implemented in any local environment. Both MEC and edge computing are key to the digitalisation of societies, particularly with the advent of 5G.
Vertical	In a business context, the term 'verticals' is used to describe the categorisation of businesses or industries according to their specialisation or focus on a particular market segment. Verticals are typically industries or sectors comprising businesses that specialise in specific types of products, services or market segments.

Executive Summary

The Internet of Things (IoT) is an extremely broad concept. It is a field that has, and will continue to have, a huge impact on our lives in many ways. From this perspective, few technologies are as fundamental.

The use of the Internet of Things is an essential tool for the digitalisation of businesses and for increasing production efficiency; it leads to improvements in the standard and accessibility of healthcare, more efficient transport and a better quality of life in cities, as well as increased yields in agriculture. The IoT forms part of a vast array of use cases across various verticals, many of which are outlined in this study.

The significance of the IoT is also evidenced by the size and growth of the market. According to forecasts, the number of IoT connections is set to rise from the current figure of around 15 billion to 40 billion connected devices by 2033. The global enterprise IoT market is projected to more than double from USD 300 billion by 2030.

This study provides a comprehensive overview of the Internet of Things. It examines how IoT systems function, their layers and components, areas of IoT application, the challenges associated with using the Internet of Things, and its future.

5G technology has a fundamental impact on the IoT sector. It can be directly applied to the communication (network) layer of an IoT system and directly influences the perception layer (devices) and the edge layer. However, it also has a significant impact on the security and economics of IoT systems.

For this reason, the study devotes considerable attention to various IoT communication technologies, their capabilities and their weaknesses. In this regard, it provides a comprehensive overview covering all widely used short- and long-range technologies.

5G technology for the IoT exists in several fundamentally different variants, each suited to different use cases. From the original 4G ecosystem, NB-IoT and Cat-
M have been carried over from the original 4G ecosystem and are being further developed. The current 5G NR technology is not specifically designed for IoT. It can be used for business-critical applications. However, it is relatively costly, particularly in terms of end devices, and is also not optimised for end-device energy consumption. This is precisely why NR-light, or RedCap, has been standardised for use in the IoT sector. High expectations are also attached to another variant of 5G technology in the form of Passive IoT, the standardisation of which has not yet been finalised.

In terms of usage, the study categorises IoT systems into critical IoT, medium-scale IoT and massive IoT. These three types of IoT systems differ in their requirements. Critical IoT typically requires high performance, security, higher data speeds and very high transmission reliability. Massive IoT, by contrast, requires low energy consumption by end devices, low equipment costs and relatively low transmission speeds. Mid-range IoT, meanwhile, falls between critical and massive IoT in terms of its requirements.

The study presents a relatively unique systematic approach to selecting suitable IoT technology for various IoT use cases.

For each IoT technology, the study identifies the category of IoT system for which it is suitable. Each use case is classified into an IoT category. This makes it possible to determine, as a guide, which IoT technologies are suitable for a given use case.

A more precise choice of technology is possible by defining the full set of key required characteristics of the IoT system. A form has been provided in the study for this purpose. The requirements identified can be compared with the parameters of the technologies, which are also listed in this study. By comparing the requirements and parameters, it is then possible to identify one or more suitable IoT technologies for the given IoT system and its use cases.

The main challenges associated with the Internet of Things and its development include cyber security, as well as the still-limited interoperability and high fragmentation of protocols and technologies. Strengthening security and further standardisation therefore certainly feature among the future directions of IoT development.

In addition, we see the following key trends for the future of the IoT:

- New communication technologies within the 5G ecosystem, in particular RedCap and Passive IoT. These new technologies will help overcome the weaknesses of existing technologies, not only technical but also commercial (cost-related). As a result, they will enable the implementation of new business models and a much more widespread deployment of IoT.

- The use of AI/ML for advanced data analysis. This will bring significant added value to areas such as predictive maintenance, anomaly detection and automation in general.

- Cloud-based IoT products. Sophisticated yet relatively affordable (thanks in part to the Pay-As-You-Go model) cloud products will enable the rapid deployment of IoT systems for businesses of all sizes. With a touch of hyperbole, this can be done in just a few clicks. Cloud products will make advanced analysis using AI/ML accessible to all users without the need for specialist expertise.

Management summary

IoT (Internet of Things) is an extremely broad concept. It is an area that has had, and will continue to have, a massive impact on our lives in many ways. From this perspective, few technologies are as fundamental.

The use of the Internet of Things is an essential tool for the digitalisation of businesses, increasing production efficiency, improving the standard and availability of healthcare, streamlining transport and enhancing the quality of life in cities, and boosting agricultural yields. IoT forms part of a vast array of use cases across different sectors, many of which are highlighted in this study.

The importance of IoT is also demonstrated by the size and growth of the market. According to forecasts, the number of IoT connections is expected to rise from the current figure of approximately 15 billion to 40 billion connected devices by 2033. The global market size for enterprise IoT is projected to grow from USD 300 billion to more than double that figure by 2030.

This study provides a comprehensive overview of the Internet of Things. It examines the functioning of IoT systems, their layers and components, areas of IoT application, challenges associated with the use of the Internet of Things, and its future.

5G technology has a significant impact on the IoT. It can be directly applied within the communication (network) layer of the IoT system and directly influences the perception layer (devices) and the edge layer. It also has a substantial effect on the security and economics of the IoT system.

Therefore, the study devotes considerable attention to various IoT communication technologies, their capabilities and weaknesses. It provides a comprehensive overview, covering all widely used short- and long-range technologies.

5G technology for the IoT exists in several fundamentally different variants, suitable for various use cases. The NB-IoT and Cat-M technologies are derived from the original 4G ecosystem and have been further developed within the 5G ecosystem. Current 5G technology is not specifically designed for the IoT. It can be used for business-critical applications but is relatively costly, particularly in terms of end devices, and is not optimised for energy consumption. This is why the NR-light technology, or RedCap, has been standardised for use in the IoT field. High expectations are also associated with another variant of 5G technology in the form of Passive IoT.

From the perspective of utilisation, the study divides IoT systems into critical IoT, mid-range IoT and massive IoT. These three types of IoT systems differ in their requirements. Critical IoT typically requires high performance, security, higher data speeds and very high transmission reliability. In contrast, massive IoT requires low power consumption by end devices, low device costs and relatively low transmission speeds. Mid-range IoT requirements lie between those of critical and massive IoT.

The study offers a relatively unique systematic approach to selecting the right IoT technology for various IoT use cases. For each IoT technology, the study determines which category of IoT system it is suitable for. Each use case is categorised into an IoT category, allowing for an approximate determination of which IoT technologies are suitable for that specific use case.

A more precise choice of technology can be made by defining the key required features of the IoT system. To this end, the study includes a form. The requirements identified can be compared with the technology parameters, which are also outlined in the study. By comparing requirements and parameters, it is then possible to identify one or more suitable IoT technologies for a given IoT system.

Among the main challenges associated with the field of the Internet of Things and its development are cybersecurity, still limited interoperability, and high fragmentation of protocols and technologies. Strengthening security and further standardisation will undoubtedly be key directions for the future of IoT.

In addition, we identify the following crucial trends for the future of the IoT:

- New communication technologies within the 5G ecosystem, particularly RedCap and Passive IoT. These new technologies will help overcome the shortcomings of existing technologies, not only technically but also commercially (in terms of cost). This will enable new business models and a much more widespread deployment of IoT.
- The use of AI/ML for advanced data analysis. This will bring significant added value to areas such as predictive maintenance, anomaly detection and automation in general.
- Cloud IoT products* Sophisticated yet relatively affordable (thanks to the Pay-As-You-Go model) cloud products will enable rapid deployment of IoT systems for companies of all sizes—almost literally with just a few clicks. Cloud products will make advanced AI/ML analytics accessible to all users without the need for specialist expertise.

1 Introduction to IoT

1.1 Objectives of the study

The aim of the study is to support the further development of IoT solutions in the Czech Republic, given their significant benefits for various aspects of the economy and quality of life, particularly through the use of 5G technologies, which bring new possibilities to the IoT and pave the way for further use cases.

It aims to achieve this by providing stakeholders with a comprehensive overview of the Internet of Things, with an emphasis on 5G technologies in IoT systems. The study will familiarise readers with the parameters of a range of communication technologies for IoT, including their advantages and shortcomings, and will help them understand the appropriate use of individual technologies for various categories of IoT systems and use cases.

An understanding of the IoT, its possibilities and potential, is essential for companies wishing to lead the way in digitalisation and streamline their processes or production; for cities seeking to provide greater comfort to their residents and develop in a sustainable manner; and for healthcare facilities aiming to improve the standard of care whilst addressing the shortage of qualified staff. And so one could go on to list a number of other areas where the use of IoT brings significant added value.

However, an understanding of the IoT is also important for companies operating in other parts of the value chain: system integrators, managed service providers, communications and connectivity providers, equipment manufacturers and platform developers. The IoT presents interesting business opportunities for all these entities.

It is therefore essential for them to grasp the full scope of the Internet of Things, to understand the challenges facing the ecosystem, and to identify future development trends.

1.2 The IoT as a complex system

The Internet of Things (IoT) is a rather general and broad term. As a result, different technologies, solutions and use cases may be included (or, conversely, excluded) under the term ‘IoT’ in various materials and contexts.

Let us therefore look at some definitions of the term ‘Internet of Things’:

“The Internet of Things (IoT) is a network of physical objects that contain embedded technology for communication and sensing or interacting with their internal states or with the external environment.”[2]

“The Internet of Things (IoT) is a system of interconnected computing devices, mechanical and digital machines, objects, animals or people, which are equipped with unique identifiers (UIDs) and the ability to transmit data over a network without the need for direct interaction between people or between people and machines.”[3]

[2] Gartner IT Glossary, https://www.gartner.com/en/information-technology/glossary/internet-of-things

[3] IEEE Xplore Digital Library, https://ieeexplore.ieee.org

“The IoT involves connecting multiple devices or systems to the internet, enabling them to collect, share and analyse data. This can encompass a wide range of devices, including sensors, actuators and smart devices, which together provide enhanced services or improve operational efficiency.”[4]

“The Internet of Things (IoT) refers to physical devices that are now connected to the internet and collect and share data. This transformation has the potential to improve efficiency across various sectors by enabling smarter processes and decision-making.”[5]

“The Internet of Things, or IoT, is a network of interconnected devices that exchange data with other IoT devices and the cloud. IoT devices are typically equipped with technology such as sensors and software, and may include mechanical and digital machines and other objects.”[6]

These definitions highlight the fundamental aspects of the IoT: connectivity, data exchange, automation and the integration of physical objects into a digital framework. Each source emphasises different elements, reflecting the broad applicability and varied interpretations of the IoT.

It is certainly also interesting that people and animals are considered to be part of the Internet of Things. This is not a mistake. However, people and animals are part of the IoT system in the sense that they do not need to carry out any active interaction. For example, wearables monitor certain vital signs and parameters (of both people and animals) and transmit them for further processing and evaluation.

For the purposes of this study, we have summarised the definition of the IoT as follows:

The Internet of Things is a system of uniquely identified devices that collect data, which is then transmitted via the internet, analysed and evaluated, and on the basis of which actions may be carried out within or outside the system. This system has a clearly defined purpose, which is typically to increase the efficiency of processes, performance, awareness, etc.

Most of the above definitions of the Internet of Things agree that the IoT is a system. Let us therefore first look at a general definition of a system. We can therefore use the definition of a system as set out by Donella Meadows in her book *Thinking in Systems*[7]:

A system is a set of elements or components that are interconnected in such a way as to produce a certain pattern of behaviour over time. A system consists of three main elements:

1. Elements: These are the individual parts or components of the system. Elements may be physical objects (e.g. machines in a factory) or intangible components (e.g. rules or information flows).

2. Connections: These refer to the relationships or interactions between elements. These interactions determine how the elements work together and how they respond to external stimuli or changes within the system.

3. Purpose or function: Every system has a purpose, which may not always be explicitly stated but can be inferred from the system’s behaviour. The purpose is the goal or outcome towards which the system naturally tends as a result of the interactions between its elements.

A system is more than just the sum of its parts; it is defined by the way in which these parts cooperate and function together to achieve a common purpose. Systems can be simple or complex, but they are always characterised by feedback loops, where the output of one element influences the behaviour of other elements within the system.

---

[4] ISO/IEC 20924:2024, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:20924:ed-3:v1:en

[5] McKinsey Digital, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things

[6] TechTarget IoT Agenda, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[7] Donella Meadows, *Thinking in Systems* (Chelsea Green Publishing, 2008)

How does the IoT fit into the definition of a system?

The Internet of Things (IoT) can be understood as a system according to the framework outlined above:

1. Elements:

- **Devices**: These include sensors, actuators, smart appliances and other connected hardware that collects and transmits data.
- **Networks**: The communications infrastructure that enables devices to connect and exchange data (e.g. 5G).
- **Data processing elements:** Cloud services, edge computing devices and AI algorithms that process and analyse data collected by devices.
- **Users**: Human operators, automated systems or decision-makers who utilise the information generated by the IoT system.

2. Connectivity:

- **Data flows**: IoT devices constantly generate data, which is transmitted over networks, processed in data centres or on edge devices, and then made available for further analysis or action.
- **Feedback**: Information obtained from data analysis is often fed back into the system to adjust device behaviour, optimise operations or trigger automated responses.
- **Control mechanisms**: These include protocols, standards and APIs that determine how different IoT devices and platforms interact with one another.

3. Purpose or function:

The primary purpose of an IoT system is to enable more efficient, informed and automated decision-making processes. IoT systems are designed to improve operational efficiency, enhance user experiences, optimise resource utilisation and drive innovation across various sectors, including manufacturing, healthcare, transport and smart cities.

In short, the IoT is a system that integrates various physical and digital components to create a comprehensive network capable of sensing, analysing and responding to data. Its purpose is aligned with enhancing functionality, efficiency and decision-making capabilities across various sectors, making it a prime example of a complex, interconnected system.

1.3 A Brief History of the IoT

The Internet of Things (IoT) has evolved from the concept of connecting devices into a technology that is transforming industries, economies and everyday life. Although the term ‘Internet of Things’ was first used in 1999, the fundamental ideas behind the IoT had emerged several decades earlier. This chapter provides an overview of the key events and milestones that have shaped the development of the IoT from its beginnings to the present day.

Origins and Foundations (1970s–1990s).

The idea of connecting devices and enabling them to communicate without human intervention predates the modern internet. In the 1970s and 1980s, early concepts such as ‘pervasive computing’ began to emerge, laying the foundations for the emergence of the IoT.

1982 – The first connected device: One of the first examples of a connected device was a Coca-Cola vending machine at Carnegie Mellon University in the early 1980s. Programmers connected the vending machine to a network, enabling them to check its stock levels and verify whether the drinks were cold. This marked a milestone in the history of connected devices and became one of the earliest examples of the IoT – a device providing data to a network for remote monitoring and management.

M2M communication: Towards the end of the 20th century, machine-to-machine (M2M) communication emerged, whereby devices communicated via networks without human intervention. M2M provided the basic framework for connectivity that later evolved into the IoT, enabling devices to communicate over both wired and wireless networks. Key examples include telemetry systems in sectors such as the oil and gas industry, where devices could send performance data back to a central control system.

SCADA (Supervisory Control and Data Acquisition): SCADA systems, which emerged in the 1960s and developed in the 1980s and 1990s, were also early precursors to the IoT. These systems collected real-time data from remote locations to monitor and control equipment and processes. The evolution of SCADA towards networked systems with integrated hardware and software was a key step towards the first generation of IoT systems.

The emergence of the term and field of IoT (1999–2000s).

The term 'Internet of Things' was first officially used by Kevin Ashton, co-founder of the Auto-ID Centre at the Massachusetts Institute of Technology (MIT), **in 1999**. Ashton used this term during a presentation to Procter & Gamble (P&G) to highlight the potential of RFID (radio-frequency identification) technology to connect physical objects to the internet and improve supply chain management.

Ashton wanted to draw P&G's management's attention to RFID technology, which he believed could revolutionise stock tracking and management. To make his presentation more engaging, he called it the 'Internet of Things' and linked the then-current trend of the internet with physical objects, thereby formally using the term for the first time.

At the same time, MIT professor Neil Gershenfeld's book *When Things Start to Think* was published; whilst it did not directly use the term IoT, it described a world in which everyday objects would possess computing power and connectivity, which closely aligned with Ashton's vision.

Official recognition of the IoT: In 2005, the International Telecommunication Union (ITU) published its first report on the Internet of Things, thereby officially recognising the IoT as a significant technological concept. The report outlined the potential of a world in which virtually all objects could be interconnected and controlled remotely.

Technological convergence of the IoT (2010–2015).

As the IoT gained momentum, the convergence of wireless technologies, micro-electromechanical systems (MEMS), microservices and the internet began to break down the barriers between operational technology (OT) and information technology (IT). This convergence enabled the collection and analysis of unstructured data generated by machines to achieve operational improvements.

In 2010, the concept of the IoT ecosystem received a significant boost when the Chinese government announced that the IoT would be a strategic priority in its five-year plan. This move highlighted the potential of the IoT on a global scale and inspired other countries and industries to invest in IoT research and development.

Between 2010 and 2019, IoT technology grew rapidly thanks to the proliferation of consumer devices such as smartphones, smart TVs and connected home appliances. These devices were able to communicate with one another and connect to the internet, extending the reach of the IoT beyond industrial applications.

The growth of cloud computing and big data analytics provided the infrastructure needed to collect, store and process the vast volumes of data generated by IoT devices. Companies such as IBM, Cisco and GE led early initiatives to utilise IoT data for predictive maintenance, operational efficiency and new business models.

Expansion, standardisation and further growth (2016–present).

The rapid roll-out of IoT devices highlighted the need for standardisation, enhanced security and improved infrastructure to support billions of connected devices. During this period, significant industry initiatives were launched to address these challenges.

Organisations such as the Open Connectivity Foundation (OCF) and the Industrial Internet Consortium (IIC) were established with the aim of developing standards to ensure interoperability between IoT devices from different manufacturers.

The roll-out of 5G networks and the rise of edge computing are transforming the IoT landscape. 5G provides higher bandwidth, low latency and the ability to connect a vast number of devices, enabling the expansion of IoT applications into areas such as autonomous vehicles, smart cities and advanced industrial automation. Edge computing has brought data processing closer to the devices, thereby reducing latency and enabling real-time decision-making.

The concept of digital twins – virtual models of physical objects or systems – gained prominence after 2020, with IoT sensors providing real-time data that keeps the digital twin in sync with its physical counterpart. This technology is gradually finding applications in manufacturing, healthcare and urban planning, where it has been crucial for decision-making.

In 2023, the Connectivity Standards Alliance published the Matter standard, which aimed to address fragmentation in the smart home market. Matter facilitates seamless interaction between smart devices from different brands and highlights the ongoing effort to improve interoperability within the IoT ecosystem.

2 How the IoT works

2.1 IoT solution architecture.

The architecture of the Internet of Things (IoT) refers to a structured framework that enables the integration, processing and communication of data from connected devices. An effective IoT architecture consists of several layers, each of which is responsible for different logical functions within the overall system.[8] The individual layers are illustrated in the following figure:

Figure 1: Layers of an IoT system. Source: own work.

1. Device layer (perception layer)

Components: Sensors, actuators, cameras and other smart devices.

[8] Simmons, Adam. "Internet of Things (IoT) Architecture: Layers Explained." Dgtl Infra, 24 January 2023.

Function: The device layer is responsible for data collection and interaction with the physical environment. Sensors detect changes in the environment (e.g. temperature, humidity, movement), whilst actuators perform actions based on received commands (e.g. switching on a light, adjusting a valve).

Example: In a smart home, a temperature sensor (device layer) monitors the temperature in a room. A camera in a production hall monitors machine behaviour and deviations from the norm.

2. Network layer (Connectivity layer or Communication layer)

Components: communication networks and protocols (e.g. Wi-Fi, Bluetooth, Zigbee, 5G), routers.

Function: This layer ensures the transmission of data from the device layer to the processing layer. It comprises the communication infrastructure and protocols that enable devices to connect to the internet or local networks, thereby facilitating the exchange of data.

Example: A temperature sensor in a smart home sends its data via Wi-Fi to a central hub. An air pollution sensor sends information via NB-IoT.

3. Edge layer (Edge computing layer)

Components: Edge devices, gateways, local processing units, microcontrollers.

Function: The edge layer processes data closer to the source (i.e. the devices). By performing initial processing and filtering on edge devices, it reduces latency and bandwidth usage, enabling rapid response times and efficient data management.

Example: Data from a production line is processed locally to immediately identify defective products. The data is then sent to the cloud for trend analysis and further analysis.

Note: The edge layer may or may not form part of the IoT architecture. In some cases, data is sent directly to central components.

4. Processing layer (Data management layer, or middleware layer)

Components: Cloud servers, data storage systems, analytical tools.

Function: This layer handles large-scale data processing, storage and analysis. It is usually located in the cloud, where complex calculations and machine learning algorithms can be applied to the data.

Example: Data on production line activity is aggregated and analysed in the cloud to identify long-term patterns, enabling predictive maintenance or optimisation of energy consumption.

An IoT system typically processes vast volumes of data generated by numerous edge devices at various locations on the network's periphery. The 'middleware' in the processing layer uses a three-stage approach to prepare this data for the application layer:

- Data accumulation: the middleware identifies and assigns different types of data to the appropriate storage. Unstructured data, such as audio and video streams and images, usually requires more storage space and is stored in data lakes. Conversely, structured data, which includes, for example, log entries and telemetry data, is more space-efficient and is stored in data warehouses.

- Data abstraction: This involves aggregating data from multiple sources and ensuring that the data is converted into a format that can be 'read' by application-layer software.

- Data analysis: This utilises machine learning (ML) or deep learning algorithms that are specialised in detecting patterns in large and seemingly random datasets.

5. Application layer

Components: Software applications, user interfaces, dashboards.

Functions: The application layer provides the interface through which users interact with the IoT system. It interprets and presents data in a user-friendly manner and enables users to control devices, monitor system performance and make informed decisions.

Example: A mobile app that allows a homeowner to remotely monitor and adjust temperature settings in a smart home.

6. Security layer

Components: Encryption protocols, authentication mechanisms, firewalls.

Function: This layer is responsible for ensuring the security and privacy of data as it flows within the IoT architecture. It includes measures to protect data from unauthorised access, prevent breaches and ensure that communications within the IoT network are secure.

Example: Encrypted communication between a temperature sensor and a central hub ensures that data cannot be intercepted or altered by unauthorised parties.

7. Business layer

Components: Business logic, rule management tools, policy management tools.

Functions: The business layer interprets data in the context of the organisation’s goals and objectives. It assists in decision-making processes by applying business rules and policies to data. This layer ensures that the IoT system aligns with business strategy and delivers value.

Example: In a commercial building, an IoT system can analyse energy consumption data to optimise operations, thereby reducing costs and supporting the achievement of sustainability targets.

The individual layers of the IoT architecture thus represent the logical functions of the IoT system. In real-world implementations, however, individual elements of the solution span one or more logical layers. For example, an IoT platform typically covers the processing layer, the application layer and the business layer, whilst also overlapping with the security layers.

IoT Architecture and 5G

The potential use of 5G technology affects several layers of the IoT architecture:

Perception layer – 5G devices will be utilised in this layer. These include sensors and other end devices containing a 5G modem. These may be standard 5G NR, or variants designed for IoT, namely RedCap and Passive IoT, as well as technologies incorporated into the 5G ecosystem such as Cat-M and NB-IoT.

Network layer – this layer utilises the 5G network to transport data from end devices to the edge and/or to a central platform.

Edge layer – one of the key features of 5G technology is the separation of the control plane and user plane (CUPS), which enables user data to be processed at the edge, i.e. close to the source, without the need to transmit it to a remote network core. This makes it possible to utilise the functions and benefits of the edge layer when using 5G technology.

Security layer – 5G technology is inherently highly secure, unlike many other alternatives that may also be used within an IoT system. Authentication using physical SIM cards – or, in the case of IoT solutions, e-SIMs – and advanced encryption contribute to the overall security of a 5G-based IoT system.

The processing, application and business layers, on the other hand, are in principle independent of the use of 5G technology.

2.2 IoT (transmission) technologies

2.2.1 Description and characteristics of IoT transmission technologies

IoT transmission technology ensures the transmission of data from end devices (sensors, actuators) to the edge interface and/or to the central components of the IoT system (to servers where the data is processed) and, where applicable, in the opposite direction.

IoT transmission technology and its selection therefore play a key role in:

- the perception layer (it influences which types of end devices can be used),
- the network layer.

However, it also has an impact on the edge layer, the business layer and the security layer.

From this list, it is clear just how important a role IoT transmission technology plays across the entire IoT system, and how important it is to be familiar with the various technology options and to select the most suitable one for a given IoT system.

Below is a description of the most commonly used transmission technologies for IoT solutions.

Some of these technologies were designed specifically for use in the IoT. Others are general-purpose technologies, such as those used for interpersonal communication or internet connectivity, but they are also successfully employed in IoT projects.

1. GPRS (General Packet Radio Service)

GPRS is an early mobile data transmission service developed in the late 1990s as part of the second-generation (2G) network, often referred to as 2.5G. It was designed to provide moderate data transmission speeds, enabling mobile devices to send and receive data via the mobile network. GPRS uses packet-switched technology, which means that data is transmitted in small packets rather than as a continuous stream, allowing for more efficient use of network resources compared to circuit-switched systems such as GSM. Although data speeds are relatively low, typically ranging from 56 to 114 kbps, GPRS was a revolutionary technology of its time, enabling mobile web browsing, email and basic multimedia messaging. In the context of the IoT, GPRS was used in early-generation applications such as vehicle tracking, remote monitoring and basic telemetry, particularly in areas with limited network infrastructure. However, with the advent of newer and faster technologies, GPRS is now considered obsolete for most modern IoT applications.

2. 4G/5G

4G (fourth generation) and 5G (fifth generation) are the latest generations of mobile networks. 4G, launched around 2010, introduced high-speed mobile connectivity with data speeds of up to 100 Mbps for mobile communications, enabling advanced applications such as HD video streaming and online gaming. It also supported IoT use cases that required higher data speeds and reliable connectivity, such as connected vehicles, smart cities and industrial automation. 5G, which began to be rolled out globally in 2019, builds on the capabilities of 4G and offers much higher data speeds (up to 10 Gbps), ultra-low latency and the ability to connect a massive number of devices simultaneously. Key features of 5G include enhanced mobile broadband connectivity (eMBB), ultra-reliable low-latency communication (URLLC) and massive machine-type communication (mMTC), making it ideal for a wide range of IoT applications, from smart cities and autonomous vehicles to industrial IoT and healthcare.

Neither 4G nor 5G are specifically IoT technologies. Both generations are characterised by supporting more than adequate transmission speeds from an IoT perspective; however, their end devices are relatively expensive and energy-intensive. 5G also has an advantage over 4G in that, from an architectural perspective, it is better suited to private networks.

A detailed description of 5G technology, architecture and features, including their availability, forms part of the study **'The use of 5G and other electronic communications networks for the digitalisation of businesses, including the use of modern information systems'.**

3. NB-IoT (Narrowband IoT)

NB-IoT is a technology for low-power wide-area networks (LPWAN) standardised by the 3GPP organisation as part of Release 13, which was designed specifically for IoT applications. It operates within the existing LTE spectrum but requires only a narrow 180 kHz bandwidth, making it highly efficient for transmitting small amounts of data over long distances. NB-IoT supports deep indoor signal penetration, which is a significant advantage for use cases such as smart metering, environmental monitoring and asset tracking, where devices are often located in basements or other hard-to-reach places. The technology is characterised by low power consumption, enabling devices to operate for up to 10 years on a single battery. Thanks to its simplicity, reliability and widespread adoption by mobile operators, NB-IoT is a popular choice for IoT deployments, particularly where there are large numbers of devices with low data requirements.

4. LTE-M (Long Term Evolution for Machines)

LTE-M is another LPWAN technology developed under the 3GPP standards, specifically for IoT applications that require greater bandwidth and mobility than NB-IoT. It operates on existing LTE infrastructure, but with a focus on reducing device complexity and power consumption. LTE-M supports voice services via VoLTE, making it a suitable choice for IoT applications that require both data and voice communication, such as wearable devices, health monitoring and asset tracking. It also supports higher data speeds (up to 1 Mbps), mobility and handover between cells, enabling continuous coverage in mobile scenarios such as vehicle tracking or connected transport systems. LTE-M devices can operate in sleep modes, which further extends battery life, and offer a good balance between performance, cost and coverage, making it ideal for a wide range of IoT use cases.

5. LTE Cat 1 bis

LTE Cat 1 bis is an evolution of LTE Cat 1 technology, an LTE category designed for IoT applications requiring moderate data rates. Whilst standard LTE Cat 1 requires full-duplex communication, LTE Cat 1 bis is designed for half-duplex communication, which simplifies device design and reduces costs. It supports data rates of up to 10 Mbps, making it suitable for IoT applications such as point-of-sale (POS) terminals, ATMs and telematics, where both data and voice communication are required but ultra-high speeds are not necessary. LTE Cat 1 bis is particularly valued for its ability to balance power consumption and performance, offering a good middle ground between the higher speeds of LTE categories and more energy-efficient LPWAN technologies such as NB-IoT. This technology is particularly relevant for markets where LTE infrastructure is already in place and a cost-effective IoT solution is required.

6. NR-Light/ RedCap (Reduced Capability)

RedCap, or Reduced Capability New Radio, is a feature introduced in 5G networks to support IoT devices that require moderate data rates and low complexity, yet still benefit from 5G advantages such as low latency and high reliability. RedCap is essentially a simplified version of the 5G standard, designed for IoT applications such as industrial sensors, wearable devices and smart city infrastructure, which do not require the full capabilities of 5G but still demand higher performance than LPWAN technologies. By reducing device complexity, RedCap cuts costs and energy consumption, making it a highly efficient solution for moderately demanding IoT use cases. As

5G networks continue to evolve, RedCap is expected to play a significant role in expanding the reach of IoT across various sectors.

7. 5G Passive IoT

5G Passive IoT represents the next frontier in IoT technologies, where devices are powered exclusively by energy harvested from ambient sources, such as radio frequencies, thermal gradients or mechanical vibrations. This approach eliminates the need for traditional batteries, significantly reducing maintenance costs and enabling the deployment of vast numbers of sensors across a wide area. 5G Passive IoT integrates with 5G networks to provide long-range communication, high reliability and the ability to connect a vast number of devices simultaneously. This technology is particularly well-suited to applications such as environmental monitoring, smart agriculture and supply chain management, where sensors can be deployed in remote or hard-to-reach locations. Standardisation of 5G Passive IoT is expected as part of 3GPP Release 19, with deployment anticipated in the coming years.

8. LoRa (Long Range)

LoRa is a proprietary LPWAN technology developed by Semtech, known for its ability to provide long-range communication (up to 15–20 km in rural areas) whilst consuming very little power. It operates in unlicensed frequency bands (such as 868 MHz in Europe and 915 MHz in North America), which gives it high flexibility and the ability to be deployed independently of mobile networks, making it a popular choice for IoT applications where connectivity infrastructure is lacking. Key features of LoRa include long battery life, good signal penetration and scalability, which supports large-scale networks comprising thousands of devices. It is widely used in smart cities, smart farming, environmental monitoring and consumption metering. The open LoRaWAN protocol provides the network architecture and security features required for large-scale deployment, making it the most common choice for non-cellular IoT applications.

9. ZigBee

ZigBee is a short-range, low-power wireless communication technology based on the IEEE 802.15.4 standard. It was developed after 2000 to meet the need for simple, low-cost and low-power communication between devices on a network. ZigBee operates in the 2.4 GHz ISM band and is designed for mesh networking, where devices can communicate directly with one another, thereby extending the network’s range and reliability. This makes ZigBee ideal for applications in home automation, smart lighting, energy management and building automation. Key features of ZigBee include low power consumption, which allows devices to operate for years on small batteries, and support for dense networks of up to 65,000 nodes. Although it faces competition from other wireless standards such as Wi-Fi and Bluetooth, ZigBee remains a popular choice for IoT applications that require reliable, low-cost communication over short distances.

10. Bluetooth

Bluetooth is a short-range wireless communication technology that has been widely adopted since its introduction in the late 1990s. Originally developed to connect personal devices such as headphones and keyboards wirelessly, Bluetooth has evolved to support a variety of IoT applications, particularly with the introduction of Bluetooth Low Energy (BLE) in 2010. BLE is optimised for low-power devices, enabling them to operate for long periods on small batteries, making it ideal for use in wearables, health monitoring devices, beacons and smart home applications. Bluetooth operates in the 2.4 GHz ISM band and supports data rates of up to 2 Mbps. One of Bluetooth’s key strengths is its widespread adoption and interoperability, which allows devices from different manufacturers to communicate seamlessly. Its ability to support both point-to-point and mesh networking makes Bluetooth a versatile technology in the IoT sector.

11. Wi-Fi

Wi-Fi is a well-established wireless networking technology that provides high-speed internet access and data transmission over short to medium distances. Based on the IEEE 802.11 standards, Wi-Fi operates primarily in the 2.4 GHz and 5 GHz bands and offers data rates that can exceed 1 Gbps in the latest versions. Wi-Fi's ability to handle large volumes of data makes it ideal for IoT applications requiring high bandwidth, such as video surveillance and smart appliances. However, Wi-Fi typically consumes more power than LPWAN technologies, which may limit its use in battery-powered IoT devices. Nevertheless, thanks to its ubiquity in homes, offices and public spaces, and its robust security protocols (in the new WiFi 6 and WiFi 7 versions), Wi-Fi remains a key component of IoT ecosystems, particularly for applications where devices are connected to a power supply and require high-speed connectivity.

Summary of the parameters of technologies used for IoT:

IoT technologies	Long/ Short range	Data transfer rate	Two-way communication (suitability and frequency)	Latency (ms)	Mobility support
GPRS	Long	40–171 kbps	Suitable, low frequency	High (500+)	Yes
4G/5G	Long	1 Mbps – 1 Gbps+	Highly suitable, high frequency	Low (<10)	Yes
NB-IoT	Long	up to 250 kbps	Limited suitability, low frequency	Medium (100–1500)	No
Cat-M	Long	375–1,000 kbps	Suitable, medium frequencies	Low (50–100)	Yes
LTE Cat 1 bis	Long	5–10 Mbps	Suitable, mid-range frequencies	Low (<50)	Yes
RedCap	Long	50–150 Mbps	Highly suitable, medium to high frequency	Low (<20)	Yes
5G Passive IoT	Long	<100 kbps	Limited suitability, low frequency	Low (<50)	No
LoRa	Long	<50 kbps	Suitable, low frequency	High (1000–10,000)	Limited
ZigBee	Short	20–250 kbps	Suitable, high frequency	Low (<50)	No
Bluetooth	Short	1–3 Mbps	Highly suitable, high frequency	Low (<50)	No
Wi-Fi	Short	up to 1 Gbps	Highly suitable, high frequency	Low (<50)	Limited

IoT technology	International roaming support (yes/no)	UE power consumption (low/medium/high)	Suitable for critical communicat ions	Cybersecurity level (low/medium/high)	Cost (low/medium/high)
GPRS	Yes	High	No	Medium	Medium
4G/5G	Yes	Medium to high	Yes	High	Medium to high
NB-IoT	Limited	Low	No	Medium to high	Medium
Cat-M	Yes	Low	Yes	Medium to high	Medium
LTE Cat 1 bis	Yes	Low to medium	Yes	High	Medium
RedCap	Yes	Low to medium	Yes	High	Medium
5G Passive IoT	Limited	Very low	No	High	Low
LoRa	No	Low	No	Medium	Low
ZigBee	No	Low	No	Medium	Low
Bluetooth	No	Low	No	Medium to high	Low
Wi-Fi	No	Medium to high	No	Medium to high	Low to medium

2.2.2 Categorisation of IoT transmission technologies.

Categorisation can be carried out according to several different criteria, which always provide certain information regarding the potential and suitability of a given IoT technology.

In the context of IoT transmission technologies, the terms mMTC and LPWAN are often mentioned. Let's take a closer look at these concepts and which technologies fall into these categories.

mMTC (massive Machine Type Communications)

mMTC is a key feature of 5G technology, designed to support a large number of connected devices that typically transmit small amounts of data intermittently. It is ideal for applications such as smart cities, industrial IoT and large-scale sensor networks, where there is a high density of connected devices and where energy efficiency is important. mMTC focuses on providing scalable connectivity and supports potentially millions of IoT devices per square kilometre.

LPWAN (Low-Power Wide-Area Network)

LPWAN is a category of wireless communication technologies designed for long-range, low-power communication, making it ideal for IoT devices that need to run on batteries for many years. LPWAN technologies are typically used for applications requiring long-term connectivity, low data transfer rates and infrequent communication, such as smart metering, environmental monitoring and asset tracking. LPWAN technologies operate in both licensed and unlicensed frequency bands. The following table provides an overview of how these technologies are categorised:

IoT technologies	mMTC	LPWAN
GPRS	No	No
4G/5G	Yes	No
NB-IoT	Yes	Yes
Cat-M	Yes	Yes
LTE Cat 1 bis	Yes	Yes (!)
RedCap	Yes	Yes (!)
Passive IoT	Yes	Yes
LoRa	No	Yes
ZigBee	No	No
Bluetooth	No	No

Wi-Fi	No	No

Cat-M (LTE-M) and NB-IoT vs. mMTC/5G

Somewhat paradoxically, Cat-M (also known as Cat-M1 or LTE-M – these terms are interchangeable) and NB-IoT, which are 4G technologies, are also officially classified as mMTC technologies. However, they are also factored into the 5G ecosystem and are, in principle, designed for machine-type communication and the connection of large numbers of devices.

Although mMTC is formally part of the 5G standard, NB-IoT and LTE-M were developed within the 4G (LTE) framework to meet the growing demand for massive IoT connectivity. These technologies focus on providing low-power, wide-area connectivity for a vast number of devices, which is in line with the objectives of mMTC.

Both NB-IoT and LTE-M are integrated into the broader 5G ecosystem. This integration forms part of the 3GPP (3rd Generation Partnership Project) Release 15 and Release 16 specifications, which ensure that these technologies can coexist with other 5G components.

Within the 5G framework, NB-IoT and LTE-M can be deployed either as standalone networks or as part of a 5G network using dynamic spectrum sharing (DSS). This allows them to continue operating in their existing frequency bands whilst benefiting from the improvements offered by 5G, such as lower latency and support for massive device deployment.

The industry has committed to long-term support for NB-IoT and LTE-M technologies, ensuring that they will remain relevant and widely used in the coming decades. This long-term support is crucial for sectors that have already invested heavily in these technologies.

Efforts are underway to further enhance NB-IoT and LTE-M within the 5G framework. This includes improving energy efficiency, extending coverage and increasing capacity. These enhancements are key to supporting the growing number of IoT devices expected to be connected in the coming years.

GPRS: Not classified as mMTC or LPWAN, as it is an older technology primarily used for basic mobile communications.

4G/5G: Falls under mMTC due to its ability to support a large number of devices, particularly with 5G technology.

NB-IoT: Supports both mMTC and LPWAN; it is designed for massive connectivity with low power consumption.

LTE-M: Supports both mMTC and LPWAN; suitable for IoT devices requiring moderate data rates and mobility.

LTE Cat 1 bis: Supports mMTC. It is not always classified as LPWAN – this is a rather borderline case, as it has features that support reduced energy consumption.

RedCap: Belongs to the 5G family supporting mMTC. It is not specifically designed as an LPWAN, but again this is a borderline case, as it has certain features leading to lower energy consumption.

5G Passive IoT: Designed to support the characteristics of both mMTC and LPWAN.

LoRa: A pure LPWAN technology, designed for long-term, low-energy communication.

ZigBee: Not classified as either mMTC or LPWAN; it is a short-range technology.

Bluetooth: Not classified as either mMTC or LPWAN; it is primarily a short-range personal area network technology.

Wi-Fi: Not classified as mMTC or LPWAN; used for high-speed data transmission over short distances.

2.2.3 Further ways of categorising IoT transmission technologies

By bandwidth:

This influences suitability for various applications depending on data requirements.

Narrowband, for transmitting small data volumes: GPRS, LoRa, NB-IoT

Broadband, capable of handling high or medium speeds and data volumes: standard 4G/5G, 5G RedCap, LTE-M

By power consumption:

This affects suitability for use cases where mains power is not available.

LPWAN (Low Power WAN) – specifically designed for low power consumption: NB-IoT, LTE-M, 5G Passive IoT, LoRa, RedCap (borderline case).

Others – without a specific solution to reduce the end device's energy consumption: standard 4G/5G, GPRS.

By range:

The range of the technology influences its suitability for purely local use cases, or for use cases covering a large area, nationwide or even internationally.

Short-range technologies: NFC, Bluetooth, Zigbee, RFID (according to some sources, simple RFID technologies are not counted as IoT).

Long-range technologies: LoRa (the acronym stands for 'Long Range'), NB-IoT, LTE-M and other standard 4G/5G technologies.

By use of licensed spectrum:

Some technologies are designed for use on licensed spectrum. This has both advantages and disadvantages. The advantages include resistance to interference and security. The disadvantage is the need to negotiate the project exclusively with the spectrum owners – usually mobile network operators – and the associated higher costs. Other technologies, by contrast, use unlicensed spectrum.

Licensed-band technologies: GPRS, 4G/5G, RedCap, NB-IoT, LTE-M. Unlicensed-band

technologies: LoRa, Bluetooth, Zigbee, NFC.

By standardisation

The method of standardisation can influence the direction of a technology's future development. From this perspective, it makes sense to categorise technologies primarily into 3GPP technologies, which are backed by a vast ecosystem of mobile operators, and others, whose ecosystems are typically more limited. The advantage of 3GPP technologies is the near certainty that the technology is not a dead end and will have long-term continuity. The disadvantage is usually higher costs.

3GPP technologies: GPRS, 4G/5G, RedCap, NB-IoT, LTE-M.

Others: LoRa, SigFox.

2.3 5G technology for IoT – development and use

2.3.1 NR-Light (5G RedCap) is a solution for mid-range IoT.

There is a very wide range of IoT use cases, which differ in their requirements for IoT systems. Consequently, the parameters that the technology supporting a given use case should have vary significantly. The use cases and their requirements are analysed in detail in Chapter 3.

However, it can be summarised that at one end of the spectrum (one extreme) lies **mission-critical IoT**. These are use cases requiring ultra-high communication reliability, low latency and, typically, high data transfer rates. Conversely, they do not usually require energy efficiency in end devices. Examples of mission/business-critical IoT include monitoring and control systems within the Industrial Internet of Things, the operation of various types of robots such as AMRs and cobots, autonomous systems in agriculture, and a range of healthcare use cases involving the monitoring of vital signs, etc.

Secure and reliable 5G technology can be successfully utilised for mission/business-critical IoT. In some cases, this may even involve a network supporting URLLC (ultra-reliable low-latency communication).

At the other end of the spectrum is what is known as **'massive IoT'**. These are use cases which, by contrast, do not specifically require high communication reliability or low latency. They are mostly associated with the transmission of small volumes of data at low communication frequencies with end devices. And they often (though not always) require low power consumption from end devices, which must operate on battery power. Examples of massive IoT use cases include energy metering, environmental monitoring and monitoring the availability of parking spaces.

NB-IoT and eMTC (or LTE Cat-M) technologies are already being used for massive IoT. Although originally 4G technologies (see above), they are expected to evolve within the 5G ecosystem.

There are, of course, a number of IoT use cases that fall somewhere between these extremes of mission-critical IoT and massive IoT. These can be characterised as **'mid-range IoT'**, i.e. use cases with moderate requirements. Good communication reliability and moderate data transfer speeds are required, whilst latency does not need to be ultra-low.

In theory, standard 5G technology (eMBB/URLLC) could be used for these use cases. However, this is relatively costly, particularly in terms of end devices. For mid-range applications, favourable cost-effectiveness is also expected, enabling a viable business model for these use cases.

It is precisely for these mid-range IoT use cases that ReCap technology was developed. This is to bridge the significant gap between the massive IoT technologies NB-IoT and LTE-M (eMTC) and mission-critical 5G, as clearly illustrated in the following figure.

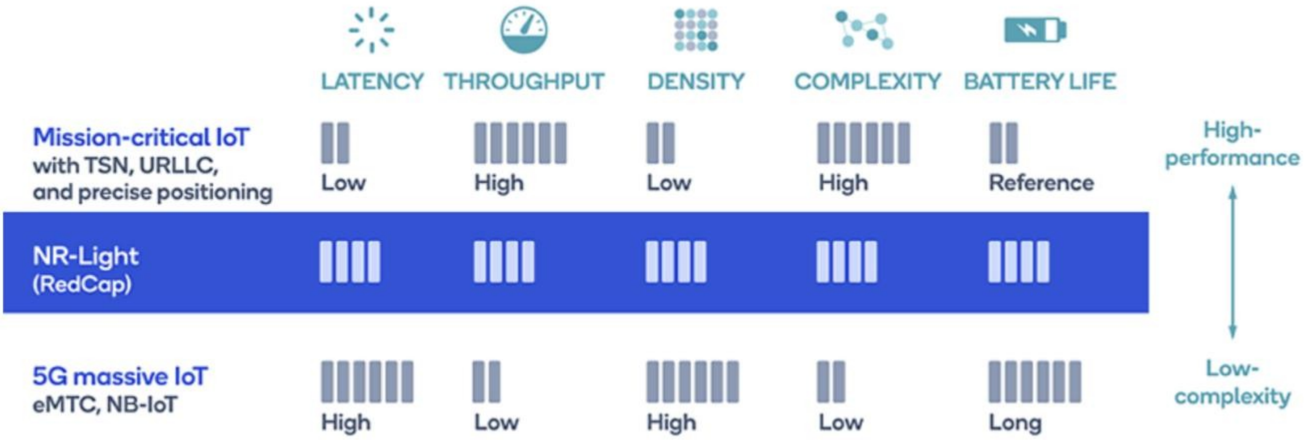

Figure 2: NR-light/RedCap as a bridge between 5G for mission-critical IoT and NB-IoT/eMTC (Cat-M) for massive IoT. Source: [9]

As part of 5G NR Release 17, the 3GPP introduced a new category of devices with reduced capabilities (RedCap), also known as NR-Light. This is a new device platform that bridges the gap in capabilities and complexity between the extremes of current 5G and is optimised for mid-range use cases. Compared with devices for 5G enhanced mobile broadband (eMBB), which can support downlink and uplink speeds of up to several gigabits per second, NR-Light devices can, thanks to the optimisations designed into them, effectively support speeds of 150 Mbps downlink and 50 Mbps uplink:

- narrower bandwidths, e.g. 20 MHz in bands below 7 GHz or 100 MHz in millimetre-wave (mmWave) bands,
- a single transmit antenna,
- a single receiving antenna, with the option of two antennas,
- optional support for half-duplex FDD,
- a lower modulation order, with 256-QAM being optional, and
- support for lower transmit power.

The reduced complexity contributes to more cost-effective NR-Light devices, longer battery life thanks to lower power consumption, and smaller device dimensions.

The first version of the 5G NR standard, 3GPP Release 15, supported two device classes for massive IoT: specifically, eMTC (Cat-M1) for 1.4 MHz channels and NB-IoT for 200 kHz channels. Thanks to the improvements introduced in 3GPP Release 16, devices using both of these technologies can coexist with 5G devices on the same 5G NR channel.

Release 16 also introduced a further tier of 5G devices for eURLLC, which meets the stringent requirements for mission-critical IoT, with support for millisecond-level latency and 99.9999% reliability.

[9] "5G NR-Light (RedCap): Revolutionising IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

NR-Light in 3GPP Release 17 can co-exist with these classes of IoT devices and eMBB devices on the same 5G NR channel. Furthermore, as the 5G NR standard continues to evolve, NR-Light is planned to be further developed in Release 18, with a focus on positioning requirements and their enhancement.

Communication between devices via the 5G sidelink interface could be a further evolutionary path for NR-Light in Release 18 and beyond.

This development of the 5G technology family, together with the evolution of the original 4G technologies, is illustrated in the following figure.

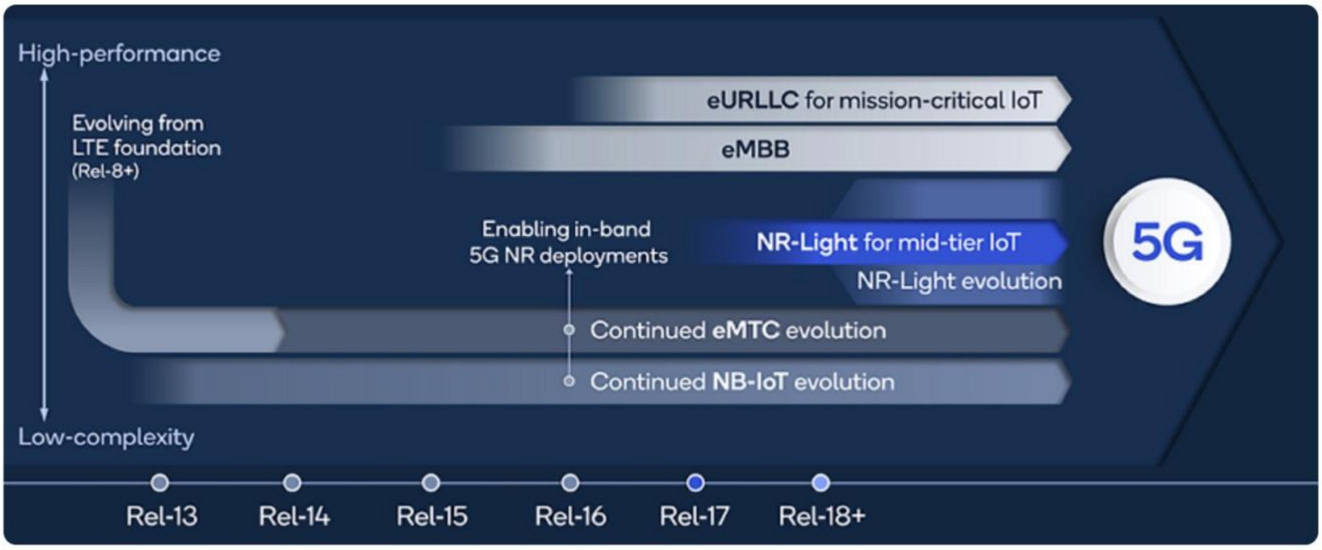

Figure 3: Roadmap of 5G technologies according to 3GPP releases. Source: [10]

At present, mid-range IoT projects rely on LTE Cat-1bis technology (and, to some extent, LTE Cat-4, which is not specifically an IoT technology) for widespread wireless connectivity and mobility. Although LTE networks are expected to coexist with 5G networks for the foreseeable future, 5G NR-Light may offer a new level of capability, efficiency and flexibility. NR-Light can provide higher throughput, lower latency, longer battery life, improved network security and an optimised cost structure for such applications. As the evolution of 5G continues, there will come a time when communications service providers begin to transition from 4G to 5G. With this in mind, 5G NR-Light will become the preferred platform for delivering mid-range IoT projects.

[10] "5G NR-Light (RedCap): Revolutionising IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

The following figure compares the specifications of technologies for mid-range IoT. These are LTE Cat 1bis at present and 5G NR-Light in the future. In contrast, LTE Cat-4 is an LTE technology that has not been optimised for IoT projects in terms of, for example, lower complexity and power consumption in end devices.

	LTE Cat-1bis	LTE Cat-4	5G NR-Light (Rel-17)
Bandwidth	20 MHz	20 MHz	20 MHz (sub-7 GHz)
Peak data rate DL/UL	10/5 Mbps	150/50 Mbps	150/50 Mbps or higher
Duplexing	FD-FDD, TDD	FD-FDD, TDD	HD-FDD, FD-FDD, TDD
Tx/Rx chain	1 Tx, 1 Rx	1 Tx, 2 Rx	1 or 2 Tx, 1 or 2 Rx
MIMO layers DL/UL	1/1	2/1	1 or 2/1
Maximum coupling loss	140 dB	144 dB	140 dB

Figure 4: Comparison of mid-range IoT technology parameters. Source: [11]

So, for which IoT use cases is NR-Light (5G RedCap) suitable?

5G NR-Light offers a combination of parameters – such as data transfer speed, battery life and device density – that is required to support various use cases cost-effectively.

It will find a wide range of applications within **the Smart City** framework: environmental sensors, consumption metering, and high-resolution camera systems. It is certainly a solution for **Industry 4.0**, including potential use within **5G private networks**.

NR-Light delivers reliable wireless connectivity and seamless mobility. It does so cost-effectively, particularly from the perspective of end devices, which can play a major role in the economics of a given use case. Examples include replacing cabling, process monitoring, smart camera systems, and even wearable devices.

The small size of the devices, long battery life and high throughput of NR-Light devices make them an attractive option for the future, including for many mobile consumer applications (i.e. within **Consumer IoT**), such as smart watches, health monitors, broadband access for basic devices such as tablets, augmented reality (AR) glasses, etc.

2.3.2 Passive IoT opens up new possibilities for IoT

Passive IoT (P-IoT) technology is associated with high expectations. In particular, the third phase – P-IoT III – is set to be standardised as part of 3GPP Release 19 and will integrate P-IoT with cellular networks.

P-IoT is a system designed to address the limitations of traditional IoT systems in terms of energy consumption, costs and scalability. Unlike active IoT devices, which rely on batteries or external power sources, passive IoT devices operate by harvesting energy from their surroundings, such as radio waves, thermal energy or mechanical vibrations. This energy is used to power the devices, which then communicate using backscatter techniques. This means that they reflect signals transmitted by a reader or base station and embed their data into these reflections, which are subsequently decoded by a receiver.

[11] "5G NR-Light (RedCap): Revolutionising IoT | Qualcomm," n.d. https://www.qualcomm.com/news/onq/2022/07/what-is-5g-nr-light--a-k-a--redcap--and-how-will-it-accelerate-t.

Standardisation and Deployment Phases of P-IoT

The development of Passive IoT can be divided into three main phases:

1. P-IoT I: This phase is characterised by a single-point architecture that primarily utilises UHF RFID technology. In this setup, passive tags are activated by the reader's RF signal and use backscatter to transmit their data back to the reader. The main limitation of this phase is the short communication range, typically less than 10 metres, which makes it suitable for applications such as managing small warehouse stocks.

2. P-IoT II: This phase introduces a network architecture in which the RFID system is divided into a tag activator and a receiver. The tag activator triggers the passive tags, whilst the receiver collects and processes the data. This division improves the system's sensitivity and extends the communication range to over 100 metres, enabling the management of large assets and regional coverage.

3. P-IoT III: The final phase involves integration with mobile networks utilising the extensive 5G infrastructure. Passive IoT at this stage benefits from the advanced capabilities of mobile networks, such as interference suppression, adaptive coding and long-range communication. This phase aims to provide comprehensive coverage and connectivity, supporting a wide range of applications across various sectors.

Typical use cases for Passive IoT:

1. Localised warehouse management: Passive IoT can automate stock-taking in warehouses, offices and retail environments. Tags attached to goods or assets are read by strategically placed receivers, enabling real-time tracking and management. This reduces the costs and errors associated with manual stock-taking, increases efficiency and improves security.

2. Tracking across large areas: In this scenario, Passive IoT is used to track the movement of people, vehicles or assets across large areas. Applications include logistics, where the tracking of goods within supply chains becomes seamless, or urban management, where assets such as transport infrastructure or public safety equipment can be effectively monitored and managed.

3. Comprehensive management and administration: This category encompasses comprehensive management across entire processes or supply chains. Passive IoT can track items from production through logistics to final sale, ensuring transparency and traceability. This is particularly valuable in sectors such as manufacturing, cold-chain logistics and the management of high-value commodities.

The position of P-IoT amongst other IoT technologies

Within the spectrum of other IoT technologies, Passive IoT stands out as an ultra-low-cost, easy-to-implement technology with low energy consumption. Whilst traditional IoT devices are limited by battery life and energy requirements, Passive IoT devices can be deployed on a massive scale without the need for frequent maintenance or recharging.

Compared with active IoT solutions, Passive IoT is better suited to applications requiring the mass deployment of sensors or tags, where energy efficiency and cost are key. Furthermore, as 5G networks continue to expand, the integration of Passive IoT into these networks will enable new use cases requiring extensive coverage and reliable connectivity, which will further enhance the capabilities of IoT ecosystems.

Passive IoT will become a key element of the future of IoT, particularly in scenarios where traditional IoT solutions are impractical or too costly. Its development through the P-IoT phases is closely linked to the development of 5G.

The following figure illustrates the positioning of 5G technologies for the IoT and the types of applications for which they are suitable:

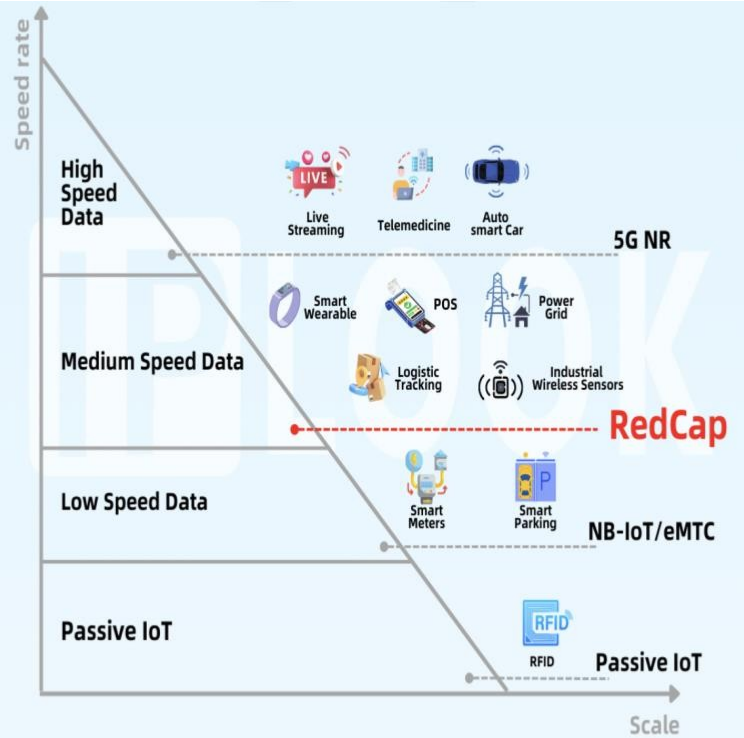

Figure 5: Applications of 5G technologies in the IoT. Source: [12]

2.4 IoT devices

2.4.1 Types and categories of IoT devices

IoT devices form a key part of every IoT ecosystem. Generally speaking, they are physical objects equipped with sensors, software and other technologies that enable them to connect to the internet, exchange data and communicate with other devices or systems. IoT devices play a key role in real-time data collection.

IoT devices not only form the perception layer of an IoT system, but also significantly influence all other layers. Naturally, this includes the communication layer – which determines the type of transmission technology used and, consequently, the type of connectivity that must be incorporated into the end devices.

However, end devices also determine what information the IoT system can acquire, thereby influencing the processing layer as well. They can also represent a significant cost item, thus affecting the business layer of the IoT system.

With the advent of 5G technology, IoT devices can be more powerful, but they are also more expensive. From this perspective, the arrival of the 5G NR-light version will be highly desirable for the IoT ecosystem.

IoT devices are primarily divided into sensors and actuators. Whilst sensors collect data from their surroundings and transmit it to the system, actuators are used to control physical elements. Depending on whether the system

[12] Iplook. "IPLOOK," 5 January 2024. https://www.iplook.com/info/redcap-cellular-iot-technology-for-the-5g-era-i00354i1.html.

contains sensors and/or actuators, IoT systems can be classified as one-way or interactive; see their detailed characteristics in section 3.1.1.

However, there are a whole range of other IoT devices. These are typically larger and more complex devices that incorporate one or more sensors, or possibly actuators.

The most important and widespread categories of IoT devices are described below.

1. Sensors

Sensors collect data from the environment or system in which they are embedded. This data may include temperature, humidity, movement or more complex metrics such as vibration or chemical composition.

Sensors act as the ‘eyes and ears’ of an IoT system. They provide critical input data that forms the basis for analytics, decision-making and triggering automated responses.

Examples: Temperature sensors, humidity sensors, accelerometers, air quality sensors.

2. Actuators

Actuators convert electrical signals into physical action. They control devices, machines or systems based on instructions from the IoT system.

Actuators are the ‘hands’ of the IoT system. They enable interaction with the real world by adjusting physical states or conditions based on data received from sensors and processed by central systems.

Examples: Electric motors, pumps, smart locks, robotic arms.

3. Edge devices

Edge devices perform data processing closer to where the data is generated, often directly within the device or on a local network.

Edge devices reduce the need to transfer large amounts of raw data to centralised cloud systems by performing analytics locally, thereby reducing network load and latency. They are essential for applications requiring fast response times or offline operation.

Examples: Industrial gateways, edge servers, smart cameras.

4. Wearables

Wearables are devices worn on the body that collect data relating to the user or their surroundings.

Wearables provide continuous data streams relating to personal health, activity or environmental factors, which is essential for sectors such as healthcare, fitness and worker safety.

Examples: Smartwatches, fitness trackers, AR/VR headsets, health monitors.

5. Connected consumer devices

These are everyday household appliances that have been enhanced with IoT capabilities to improve the user experience, enable automation or offer advanced features. Examples include the automation or remote control of the home environment or consumer products.

Examples: Smart fridges, smart speakers, home security systems, smart lighting.

6. Industrial IoT (IIoT) devices

These devices are designed for use in industrial environments, where they monitor, control and optimise machinery and processes.

Industrial IoT devices form the basis of Industry 4.0, enabling smart factories, predictive maintenance and the optimisation of production processes in real time.

Examples: Connected robots, industrial sensors, automated quality control systems, industrial routers.

7. Vehicles and transport equipment

These devices include connected vehicles, autonomous vehicles and other smart transport systems. In transport, IoT devices play a key role in ensuring safety, enabling autonomous functions, monitoring vehicle condition and improving traffic management.

Examples: Autonomous vehicles, connected lorries, fleet management systems, smart traffic lights.

2.4.2 IoT devices and protocols

IoT devices use various protocols for communication. These are tailored to the needs of IoT systems, such as low power consumption, different levels of QoS or system criticality. They also involve a type of communication that is not point-to-point in nature, but involves a large number of endpoints sending information to a central location for processing.

It is therefore useful to understand the principles behind how IoT protocols work and how they are used. The best-known protocol at present is MQTT, though there are also various alternatives.

MQTT (Message Queuing Telemetry Transport) is a lightweight communication protocol specifically designed for communication in IoT systems. Its purpose is to enable efficient, low-latency data exchange between devices, often over unreliable or bandwidth-constrained networks. MQTT is widely used in the IoT due to its simplicity, low overhead and ability to operate in environments with intermittent connectivity.

The main purpose of MQTT is to enable machine-to-machine (M2M) communication. IoT devices often need to send and receive small data packets, such as sensor data or control commands, over unreliable or limited networks. MQTT's lightweight design enables efficient handling of these communications, minimising network bandwidth consumption and device power usage. This is particularly important for IoT devices with limited resources that are battery-powered or operate on networks with limited bandwidth, such as mobile networks.

MQTT operates on a publish/subscribe model, which differs from traditional point-to-point models such as HTTP. This architecture is advantageous for IoT environments as it separates message producers (publishers) from message consumers (subscribers), enabling scalable and flexible communication. It works as follows:

- Broker (server): The broker is the hub of MQTT communication. It is responsible for receiving messages from publishers and distributing them to subscribers. The broker acts as an intermediary, which facilitates the management of multiple devices in complex systems.
- Publishers (producers): Devices or applications that send messages to the broker. A publisher does not need to know who the subscribers are – it simply sends its data to the broker.
- Subscribers (consumers): Devices or applications that express an interest in specific types of messages (topics). A subscriber subscribes to the topics that interest them, and the broker delivers the relevant messages to them as soon as they are published.

- Topics (Topics): Messagesare sent sent as part of specific topics (e.g. `sensors/temperature/living-room`). Subscribers subscribe to the topics that interest them, and the broker ensures that they receive only relevant messages.
- Quality of Service (QoS) levels: MQTT supports three QoS levels that ensure reliable message delivery:

- QoS 0 (at most once): Messages are delivered once without acknowledgement.
- QoS 1 (at least once): Messages are delivered at least once, with an acknowledgement required.
- QoS 2 (exactly once): Guarantees that messages will be delivered exactly once, which is the highest level of reliability.

- Persistent messages: Publishers can send persistent messages, which means that the broker stores the latest message for future subscribers who connect later.
- Last Will and Testimony (LWT): MQTT supports the ability to notify subscribers in the event that a device unexpectedly loses connection, by the broker sending a pre-configured message (LWT).

The Relationship Between MQTT and the IP Protocol

MQTT is an application protocol that relies on underlying transport protocols for communication. It most commonly runs over TCP/IP, utilising TCP for reliable message delivery. As TCP/IP forms the basis of internet communication, MQTT can operate on various types of networks, such as Ethernet, Wi-Fi, 4G/5G or even satellite communications. Although MQTT uses TCP for reliability, the specific transport layer is abstracted within MQTT. The use of the IP protocol ensures interoperability between different devices and systems across various types of networks.

For environments where TCP may be too cumbersome or slow, MQTT can also run over other transport layers, such as WebSockets, which enable communication via HTTP ports.

So, should IoT devices support MQTT?

Yes, IoT devices often benefit from MQTT support, particularly when they need to communicate with other devices or cloud platforms in an efficient and lightweight manner. This brings a number of advantages, notably:

- Low power consumption and bandwidth: Many IoT devices operate on limited power (e.g. battery-powered) or on networks with limited bandwidth (e.g. 2G, LoRaWAN). MQTT is optimised for these conditions thanks to its minimal packet size and low overhead.
- Decoupled architecture: The publish/subscribe model decouples devices, allowing devices to be easily added or removed without disrupting the system. This is useful in dynamic environments where devices may frequently connect to or disconnect from the network.
- Reliability and flexibility: Thanks to its QoS levels and the ‘Shutdown and Last Message’ feature, MQTT ensures reliable message delivery and enables notifications if a device loses connection.
- Scalability: MQTT supports many-to-many communication models, meaning that multiple devices can publish to the same topic and multiple devices can subscribe to the same topic. This makes it a highly scalable protocol for large-scale IoT deployments, such as smart cities or industrial environments.

Alternatives to MQTT

Although MQTT is very popular in the IoT sector, there are several alternatives, each of which has its own advantages depending on the specific use case:

- CoAP (Constrained Application Protocol):
  - A web protocol optimised for use in constrained networks and devices (similar to MQTT).
  - It uses UDP instead of TCP, which is lighter but less reliable. CoAP is often used in environments where latency is critical, such as in sensor networks.
  - Suitable for low-power devices, but not as widely adopted as MQTT.
- AMQP (Advanced Message Queuing Protocol):
  - A protocol with more features than MQTT, offering built-in support for queues, routing, security and reliability.
  - AMQP is typically used in enterprise environments where more sophisticated message processing is required (e.g. in financial services or logistics).
  - It is heavier than MQTT, which makes it less suitable for IoT devices with limited resources.
- HTTP/REST:
  - A traditional web protocol that is sometimes used in IoT, particularly for simple, one-way communication (e.g. sending data to a cloud platform).
  - HTTP is stateless, meaning that devices must send complete data with every request, which is inefficient for low-power, low-bandwidth IoT devices. However, it is simple and widely supported.
- DDS (Data Distribution Service):
  - DDS is designed for real-time systems that require deterministic, high-performance data exchange.

2.4.3 IoT Device Management

In all IoT systems, effective device management is essential to ensure long-term functionality, security and scalability. IoT device management encompasses a set of processes, tools and platforms that enable businesses (or other users of IoT systems) to remotely monitor, control, update and secure their IoT devices. As IoT networks grow in complexity and scale – sometimes comprising thousands or millions of devices – the ability to centrally manage these devices becomes crucial.

For potential customers of IoT systems, understanding device management is essential to ensure that their deployment is not only functional but also secure, efficient and scalable as their business grows, or as their IoT systems expand. The purpose of IoT device management is to simplify the oversight and control of large-scale IoT environments, enabling businesses to focus on utilising the data and functions provided by these devices.

The main activities and functions of IoT device management are as follows:

- Device deployment and configuration.

When new IoT devices are added to the system, they must be correctly configured to communicate with the network. Commissioning ensures that devices are authenticated, connected and set up correctly with a predefined configuration for communication.

- Monitoring and diagnostics.

  Continuous monitoring of IoT devices is important to ensure they are functioning as expected. Device management platforms enable businesses to monitor the status and performance of devices in real time and diagnose issues such as connection problems, low battery levels or faulty sensors.

- Firmware and software updates.

  Over-the-air (OTA) updates are a key part of IoT device management. As devices are used over time, it is essential to update their firmware or software to add new features, fix bugs and apply security patches. Device management ensures that updates can be deployed efficiently across the entire network without the need for physical access to individual devices.

- Security and access control.

  Managing security across a large fleet of IoT devices is a considerable challenge. Device management solutions ensure security configurations, including permission settings, credential rotation and the implementation of encryption protocols. Regular updates also help mitigate security risks such as vulnerabilities and unauthorised access.

- Device lifecycle management.

  Every IoT device has its own lifecycle, from deployment to decommissioning. Device management platforms provide tools for tracking devices throughout their lifecycle, enabling the easy replacement or decommissioning of devices that are no longer functional or have become obsolete. This ensures efficient operation and reduces the overall maintenance costs of the IoT infrastructure.

  IoT device management typically operates via centralised platforms that provide a range of tools for managing and monitoring devices across the network. These platforms act as a bridge between IoT devices (which are often geographically dispersed) and a central control system (usually hosted in the cloud or on-premises).

Examples of IoT device management solutions

There are many platforms that help businesses manage their IoT devices effectively. Some notable examples are listed below:

- AWS IoT Device Management:

- Part of Amazon Web Services. AWS IoT Device Management offers a comprehensive set of tools for registering, organising, monitoring and managing devices at scale. It includes features such as bulk registration, device grouping and automated provisioning.

- Key features: OTA updates, device monitoring, logging and troubleshooting.

- Microsoft Azure IoT Hub:

- Azure IoT Hub is Microsoft’s IoT platform, offering fully-featured device management. It supports both cloud-to-device and device-to-cloud communication and enables users to monitor device status and security.

- Key features: Device digital twin (digital copy of device status), integration with other Azure services, security management.

• Google Cloud IoT Core:

- Google Cloud IoT Core offers scalable services for managing connected devices. It enables the deployment, monitoring and updating of devices and integrates with Google's analytics tools and machine learning.

- Key features: Real-time monitoring, security protocols, integration with BigQuery and AI tools.

• Cisco IoT Operations Dashboard:

- Cisco provides device management solutions focused on secure IoT deployments across industries such as manufacturing, energy and transport. It offers real-time insights, diagnostics and secure management of IoT devices.

- Key features: Predictive maintenance, anomaly detection, secure device deployment.

• Bosch IoT Suite:

- Bosch offers a comprehensive solution for managing IoT devices in industrial environments. It provides tools for OTA updates, diagnostics, remote access and secure communication.

- Key features: Focus on industrial IoT, comprehensive monitoring and lifecycle management.

For potential customers, choosing the right solution for managing IoT devices is key to the successful deployment of an IoT system. A good management platform should offer scalability, security and the ability to automate processes. The platform should support a wide range of device types and communication protocols (e.g. MQTT, HTTP, CoAP) to ensure flexibility and compatibility with various hardware and software environments.

A device management platform can be standalone, or it can form part of an overall IoT platform, which is described in detail in the next chapter.

2.5 IoT platforms

An IoT platform is a comprehensive solution that provides the necessary tools and infrastructure for connecting, managing and controlling IoT devices and data flows. It serves as a central hub within the IoT ecosystem, enabling interaction between devices, the cloud, applications and end users. IoT platforms facilitate the integration of hardware, software, data analytics and network connectivity.

Essentially, IoT platforms function as middleware – a layer that bridges the physical world of devices and sensors with the digital world of data processing and analysis.

Functions of IoT platforms

IoT platforms provide a wide range of functions that enable the effective deployment and management of IoT systems. For clarity, the functions of an IoT platform can be divided into two main areas:

1. Data services – for processing, storing and analysing data.

2. Services for the management and control of IoT devices and systems.

Management and control services

- Device connection and management:

- IoT platforms facilitate the connection, configuration, authentication and monitoring of devices. They enable secure communication between devices and the cloud using various communication protocols (e.g. MQTT, HTTP, CoAP).

- Device management includes real-time monitoring, diagnostics, software updates and over-the-air (OTA) firmware updates, as well as remote troubleshooting.

- Automation:

- Some platforms support automation features, such as setting triggers or rules that activate devices based on specific conditions (e.g. switching on the heating if the temperature falls below a certain threshold).

- Security:

- Security is key in any IoT system. IoT platforms provide tools for encryption, secure data transmission, authentication and access control to protect the integrity of both devices and data flows.

Data services

- Data collection and processing:

- Platforms collect data from IoT devices (sensors, actuators) and ensure reliable data transmission to a central repository or analytics services.

- They also offer data pre-processing (e.g. data cleansing and aggregation) before passing the data on to higher-level applications for advanced analytics.

- Data storage:

- Data collected from IoT devices can be stored in databases, which are often part of cloud services for long-term storage, analysis and visualisation.

- Analytics and reports:

- IoT platforms often integrate with analytics tools to generate actionable insights from the data collected by devices. These analytics may include integration with machine learning algorithms.

- Integration with third-party applications:

- Many IoT platforms offer APIs (application programming interfaces) that enable integration with external applications, enterprise systems (e.g. ERP, CRM) or other cloud services for data analysis, visualisation or automation.

The IoT platform is the element that connects all the components of an IoT system. It sits between the device layer (sensors, actuators, gateways, etc.) connected via the communication layer and the application layer (user interfaces, dashboards, enterprise systems). The IoT platform manages communication between these layers and ensures that data flows smoothly and securely from devices to applications and back. In a typical IoT system, this communication process can be described in the following steps:

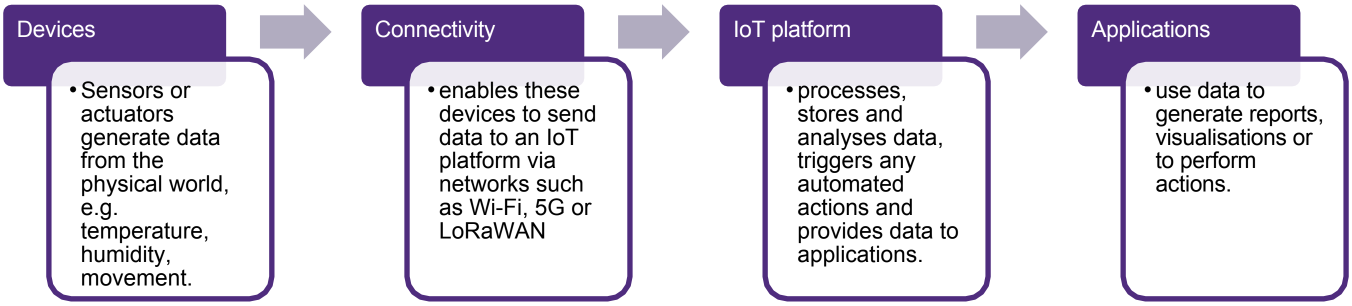

Figure 6: Communication process within an IoT system with an IoT platform. Source: Own work.

Listed below are some of the leading IoT platforms

AWS IoT (for a detailed description of the AWS IoT platform, see the appendix):

- AWS IoT Core is a comprehensive IoT platform provided by Amazon Web Services. It offers device management, real-time data processing and advanced analytics. AWS IoT Core integrates seamlessly with other AWS services, such as Lambda (serverless computing) and S3 (data storage).

Microsoft Azure IoT Hub:

- Azure IoT Hub is part of the wider Azure IoT suite. It offers robust tools for deployment, monitoring and two-way communication between devices and the cloud. Azure IoT Hub integrates with Azure data services, enabling powerful analytics and AI capabilities.

Google Cloud IoT Core:

- Google Cloud IoT Core enables secure connection and management of devices at scale. It integrates with Google's big data and machine learning tools, making it an ideal choice for businesses wishing to apply AI to their IoT data.

ThingWorx:

- ThingWorx is an industrial IoT platform from PTC that focuses on the rapid development and deployment of IoT solutions, particularly in the manufacturing and industrial sectors. It offers device management, analytics and augmented reality (AR) capabilities.

Bosch IoT Suite:

- Bosch IoT Suite is a comprehensive IoT platform designed for large-scale enterprise IoT projects, particularly in industrial environments. It provides a wide range of services, from device management to data analytics and edge computing.

However, IoT platforms are also being developed and offered by Czech and Slovak companies. Examples of local IoT platforms include Heliotics CORE and České Radiokomunikace's Multi-tech Cloud. Further information on this platform is provided in Appendix 2.

2.6 International IoT coverage

Many use cases for IoT systems – and therefore also for customers – require international connectivity. This may be a static or dynamic requirement. In the case of a static requirement, it involves an isolated solution, such as the use of IoT technologies in a hospital, which the customer wishes to replicate in other countries. A dynamic requirement is more challenging – it presupposes the seamless provision of the service not only across the entire national territory, but also across borders.

Mobile operators' roaming services have traditionally been used to meet international connectivity requirements. This is a tried-and-tested, standardised process. It is underpinned by a long history of technological development and an ecosystem which, in addition to the operators themselves, also includes various types of brokers who facilitate the exchange and billing of roaming data, as well as technology firms that assist with the implementation of value-added services or the handling of potential fraud (misuse of services).

In addition to a range of technologies, standards and the entire ecosystem, establishing international coverage requires many years of effort in negotiating and implementing roaming agreements.

For this reason, it is difficult for a new mobile operator to establish global roaming coverage in a short space of time. The solution, therefore, is to use so-called roaming brokers. These are often mobile or integrated operators who offer solutions based on dual (or multi) IMSI. IMSI stands for International Mobile Subscriber Identity. It is a unique identifier used by mobile networks to identify individual subscribers. The IMSI is stored on the subscriber's SIM card and is sent to the network for verification and authorisation of the user's access to network services, including during international roaming. A roaming broker thus enables its customers' users to utilise its IMSI (identity).

However, this solution (multi-IMSI) is not limited to new mobile operators. It can also be utilised by an IoT service provider (acting as an MVNO) to ensure international coverage for its IoT customers.

International roaming works for 2G, 3G, 4G and 5G technologies used by mobile operators in accordance with 3GPP standards.

But what about transmission technologies specific to the IoT?

In the case of the 3GPP ecosystem, these are primarily the LPWAN technologies NB-IoT and LTE-M. Roaming solutions also exist for LTE-M and NB-IoT, making it possible to obtain international coverage. However, this coverage is currently significantly more limited than for 'standard' 3GPP technologies. For example, emnify states that it provides LTE-M coverage in 51 countries across five continents.

For NB-IoT, the situation is even more complex. Although the technology was standardised back in 2016, its roll-out is proceeding slowly (as evidenced, incidentally, by the situation in the Czech Republic). To date, NB-IoT is available in only around one-third of the countries where 3GPP technologies otherwise provide coverage. For international IoT projects, for example, emnify recommends using devices that can communicate via access technologies other than just NB-IoT.

Note: It should, however, be noted that NB-IoT technology does not support mobility and is therefore not suitable for use cases such as international transport, etc.

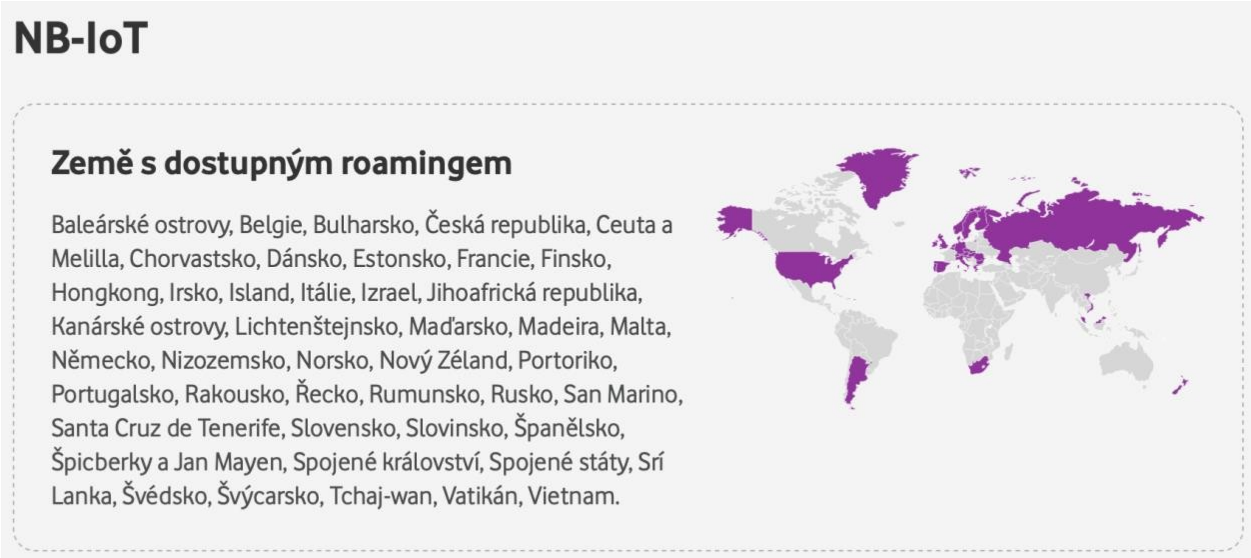

Figure 7: NB-IoT coverage whilst roaming. Source: Vodafone Czech Republic.

Figure 8: Cat-M coverage whilst roaming. Source: Vodafone Czech Republic.

Outside the 3GPP ecosystem, the main technology in question is LoRa. This is because it makes little sense to address international coverage for short-range technologies such as Wi-Fi or Bluetooth.

The LoRa network for the Internet of Things is also capable of international roaming. The LoRa Alliance is responsible for its standardisation and expansion. Compared to 3GPP technologies, however, its coverage is as yet more limited. For example, the LoRa network operated by České Radiokomunikace supports international roaming. It is available in 26 countries within the LoRa Alliance, and this also applies to satellite coverage.

Solutions based on international roaming present certain challenges and limitations for the IoT:

- Restrictions on permanent roaming: in some countries and with some operators, permanent roaming is restricted. This means that it is not possible to use the roaming service continuously for longer than a specified period (typically 60 to 90 days). For some IoT use cases, this is not a problem – for example, tracking vehicles abroad. However, it means that it is not possible to implement IoT use cases with a permanent location abroad using roaming.

- Data sovereignty: some countries require that data (within the context of IoT use cases) must not leave their territory. This may conflict with certain types of roaming solutions.

- Commercial terms: the wholesale terms associated with roaming can be so unfavourable, particularly for long-term roaming, that it is not cost-effective to provide IoT services.

Solutions for overcoming the limitations arising from roaming include:

A direct agreement with a local mobile operator. The IoT provider then utilises the local operator's IMSI as part of a multi-IMSI solution. However, securing such agreements is not easy, and this approach is therefore more viable for large IoT providers, such as Wireless Logic or KORE.

An improvement on the multi-IMSI approach is the eUICC-based solution. The embedded universal integrated circuit card (eUICC) is a programmable SIM (Subscriber Identity Module) technology that allows the device's user profile with a mobile network operator (MNO) to be changed without the need to replace the physical chip. Where roaming is not possible, this capability opens up such markets to global IoT companies in a much simpler way than physically replacing the hardware in their devices. As the eUICC is reprogrammable, it can host several MNO profiles simultaneously in its flash memory. The profile-changing process also involves Remote SIM Provisioning (RSP) software. The eUICC hardware works in conjunction with RSP to carry out the profile switching process. However, only one profile can be active at any one time, and the process of switching between networks may still require considerable time and resources.

Another option is to establish a local presence (PoP) or set up a local MVNO. These are, however, very costly solutions. From the perspective of companies wishing to implement their IoT projects on a global scale, it is therefore important to note that it is possible to secure international IoT coverage. However, its scope, limitations and commercial terms depend to a large extent on the type of IoT technology chosen and the connectivity provider.

It is therefore important to pay close attention to whether an IoT project has an international scope. If so, this is one of the key factors in selecting IoT technology. Alternatively, the need to utilise multiple IoT technologies may arise precisely because of this international reach. This must also be taken into account when selecting end devices. Last but not least, it is advisable to consider various providers of global IoT connectivity. These may include mobile network operators, but also specialist companies that provide global IoT connectivity via MVNOs (mobile virtual network operators). In addition to the examples of Wireless Logic and KORE already mentioned, Appendix 3 describes the Conexa platform in detail as a possible solution to the requirement for international connectivity.

3 What can the IoT be used for?

3.1 Types of use cases and IoT systems.

3.1.1 IoT use cases and systems by interactivity

To describe the various ways in which IoT systems can be utilised, it is important to categorise them. Different types of IoT offer very distinct ways of use.

An important classification of IoT from the perspective of usage (and thus different use cases) is based on whether the IoT system allows only a one-way flow of information, which is processed and evaluated, or a two-way flow, which enables certain processes to be controlled directly within the IoT system and thus automated.

In the first case, sensors are used as end devices; in the second case, actuators are used.

Classifying the IoT into categories based on the direction/interactivity of communication (unidirectional/bidirectional systems) yields two basic ways of utilising IoT systems:[13]

- Information and analysis
- Automation and control

These two categories of IoT therefore differ in that the first category (Information and analysis) utilises one-way communication using sensors as endpoints, whilst the second category utilises two-way communication and endpoints in the form of actuators. As a result, this two-way IoT system is capable of carrying out actions. Three types of applications are then identified for these two categories of IoT.

Information and Analysis	**Automation and Control**
1. Behaviour monitoring	**1. Process optimisation**
Monitoring the behaviour of people, objects or data in space and time.	Automated control of closed (stand-alone) systems
Examples: Sensors monitoring material wear and tear in aircraft. Tracking stock and the supply chain, e.g. using RFID.	Examples: Maximising the throughput of a lime kiln using wireless sensors. Continuous, precise adjustments on production lines.
2. Improved situational awareness	**2. Optimised resource consumption**

[13] Chui, Michael, Markus Löffler, and Roger Roberts. “The Internet of Things.” McKinsey & Company, 1 March 2010. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-internet-of-things#/.

Achieving real-time awareness of the physical environment.	Consumption management to optimise resource utilisation within the network
Example: Overview of the security status of the premises.	Examples: Smart meters and energy grids that adjust loads and generation capacity to reduce costs. Data centre management to optimise energy, storage and processor utilisation.
3. Sensor-based decision analytics	**3. Comprehensive autonomous systems**
Supporting decision-making through in-depth data analysis and visualisation	Automated control in open environments characterised by high uncertainty
Examples: Oilfield planning with 3D visualisation and simulation Continuous monitoring of chronic conditions to help doctors determine the best treatment	Examples: Collision-avoidance systems that detect objects and automatically apply the brakes Clearing hazardous materials using robots.

3.1.2 Use case requirements for IoT technology parameters

Different IoT use cases have very different requirements. Some require the transmission of large amounts of data in real time for further processing, for example using AI-enhanced analytical tools. Others, by contrast, involve the transmission of very small amounts of data, but in return, the devices must be able to operate for years on battery power without the possibility of connecting to the mains. Some use cases are business-critical, and any outage would have far-reaching consequences for users of the IoT system; for other use cases, however, the low cost of the entire solution is key. And so the list goes on. Within the broad concept of IoT, there are solutions with requirements for technical implementation that are practically 180 degrees apart and which therefore require, amongst other things, different communication technologies for their realisation. In few other areas would we find such a high degree of diversity in requirements as in IoT.

It is therefore essential to define the requirements correctly at the start of the project. Ultimately, the requirements of a given use case determine the choice of suitable technology.

Despite the great diversity of requirements across individual IoT use cases, it is possible to broadly categorise IoT systems into three distinct groups, as already defined in Chapter 2:

1. Mission/business-critical IoT
2. Mid-range IoT (mid-range IoT)
3. Massive IoT

To broadly determine the appropriate type of IoT technology for a given IoT category, we can use a table showing the suitability of individual technologies for Critical, Mid-range and Massive IoT:

IoT technology	Critical IoT	Mid-Range IoT	Massive IoT
GPRS		✓	

4G/5G	✓	✓	
NB-IoT			✓
Cat-M		✓	✓
LTE Cat 1 bis		✓	
RedCap		✓	
5G Passive IoT		✓	✓
LoRa			✓
ZigBee		✓	✓
Bluetooth		✓	✓
Wi-Fi		✓	

However, we can obtain a more accurate result by examining in detail the key requirements of IoT use cases in relation to the parameters of IoT technology:

Use case requirement	**Definition of requirement**
Data transfer rate	It is necessary to define the required transmission speed for both the uplink and downlink, as well as the typical or maximum size of data packets.
Direction and frequency of communication	Is symmetrical two-way communication important for our use case, or is it typically a one-way data collection process? What is the required frequency of communication with end devices?
Latency	Does our use case specifically require low latency, or is latency practically irrelevant (as is the case, for example, with energy meter readings)?
Mobility support	Does our use case involve moving end devices… and if so, within what radius? Or, conversely, will the end devices be statically located?
Geographical scope	In what area is our IoT use case intended to operate – is it a local solution, for example in a production hall or a hospital? Or does it require coverage across the whole of the Czech Republic?

	Or is our use case intended to operate abroad, in selected countries or even globally? And if abroad, will it be a static operation, or do we need continuous connectivity for a moving device?
Power consumption	Does our use case require very low or low energy consumption from end devices, as it is not possible to connect them to a power supply? Or will the end devices be connected to a power supply, meaning that power consumption is not a significant factor?
System Criticality	Does this represent a use case for business/mission-critical communication? If so, what are the required service level parameters?
Cyber security	Does this use case have high cybersecurity requirements, given its nature, company standards or regulatory requirements?
Cost	A use case can only be implemented if it has a viable business model. Costs play a significant role in this. Does the use case require low-cost technology, or is this not a decisive factor?

If we define the requirements for an IoT use case according to the structure/form outlined above, we can compare these requirements with the parameters of the individual IoT technologies listed in section 2.2 (IoT technologies) and identify the most suitable IoT technology for our use case – whether a single technology or a shortlist of options for further analysis.

The table below illustrates examples of use cases that are suitable or, conversely, unsuitable for the given IoT technologies.

IoT Technologies	Suitable types of use cases	Unsuitable types of use cases
GPRS	Basic tracking vehicles, SMS notifications, simple M2M applications.	High-volume data transfers, applications requiring low latency (e.g. real-time video streaming).
4G/5G	Industrial automation, autonomous vehicles, smart cities, real-time video streaming.	Long battery life for static sensors, very low data transfer rates.
NB-IoT	Smart metering, environmental monitoring, air quality sensors.	Applications requiring high data transfer rates, applications requiring real-time and two-way communication. Mobile use cases.
LTE-M	Parcel tracking, mobile healthcare devices, smartwatches, wearables.	High-volume data transfers, applications requiring very low latency (e.g. autonomous driving)
LTE Cat 1 bis	Urban surveillance cameras, voice services in IoT devices, telematics.	Applications with very low power consumption, very long battery life.
RedCap	Industrial IoT applications, medical devices, security systems.	Applications requiring extremely low power consumption, static sensors with low transmission frequency.

5G Passive IoT	Passive sensors in warehouses, parcel tracking, smart packaging.	Applications requiring high transmission speeds, mobile applications with high mobility.
LoRa	Smart farming, environmental monitoring, water meter monitoring.	Applications requiring high data transfer rates, applications requiring low latency.
ZigBee	Home automation, smart lighting, short-range health monitoring.	Long-range transmissions, applications requiring high data rates.
Bluetooth	Wearables, short-range file transfers, indoor positioning services	Long-range applications, applications requiring high data transmission security.
Wi-Fi	Smart homes, video streaming, IoT devices in the home	Applications requiring long battery life, use cases outside a limited perimeter, with high security requirements.

3.1.3 IoT systems by area of application.

Categorisation by area of application is easy to grasp and is therefore also used in various studies and reports on the IoT market, its size and dynamics.

In practice, this is a classification based on individual verticals, with an emphasis on those verticals that account for a key share of the IoT market. These are, in particular:

- **Industry** – often referred to as 'Industry IoT'. Well-known use cases include predictive maintenance. Modern Industry IoT, incorporating advanced analytics and cloud technologies, is gradually transforming traditional closed and proprietary SCADA systems.

- **Automotive** – part of the industrial sector, but plays such a significant role in the IoT that it is often reported on separately. It includes, for example, fleet management, connected infotainment, predictive maintenance, V2X communication and support for autonomous driving, emergency connectivity in the event of an accident, etc.

- **Healthcare** – this primarily involves patient monitoring, whether locally within healthcare facilities or via remote monitoring.

- **Finance** – this includes insurance telematics, such as usage-based insurance, as well as connected ATMs.

- **Energy** – this includes monitoring energy consumption, as well as active measures linked to this monitoring.

- **Government and local authorities** – this includes, in particular, the broad field of smart cities, where there is a wide range of use cases, from environmental monitoring through traffic management and energy monitoring to waste management.

- **Other verticals** – IoT finds applications in virtually every conceivable vertical. Although, in terms of the number of devices or revenue, these may not yet be among the largest. Other verticals with great potential include agriculture, transport and logistics, and retail.

The consumer IoT sector is then assigned to these verticals. This sector primarily includes wearables (wearable electronics), smart homes, connected cameras and televisions.

The categorisation of IoT systems by area of application or vertical does not, in itself, determine the IoT technology used or the type of IoT system (unidirectional/bidirectional). For example, LTE-M technology can be used just as successfully for monitoring in the energy sector, in healthcare, or in the smart city sector.

3.2 IoT Use Cases

Selected IoT use cases in individual verticals are listed below.

These use cases have been selected primarily for their potential to utilise 5G technologies in their implementation. However, this does not mean that the use cases listed here could not, in some instances, be implemented using technologies other than 5G – it always depends on the specific requirements of the use case in question.

Many IoT use cases are also use cases for business digitalisation utilising 5G technology, as outlined in the study **'The use of 5G and other electronic communications networks for business digitalisation, including the use of modern information systems'.** This is a logical overlap, as a significant proportion of business digitalisation is linked precisely to IoT technologies. Furthermore, there are, of course, cases of digitalisation using 5G that are not IoT-based, as they involve human-initiated communication – for example, group communication, or the use of AR (augmented reality) for remote assistance or staff training. Conversely, there are, of course, a number of IoT use cases that are not related to business digitalisation. First and foremost, these are cases where the entities involved are not businesses but, for example, central and local government bodies, or end users (consumer IoT).

It will be highly appropriate and effective to address certain IoT use cases using 5G network slicing technology. These use cases are outlined in the study **'The Use of 5G Network Slicing for Public and Non-Public Networks'.** This study also outlines the advantages and challenges associated with the use of network slicing, which are therefore also relevant to the field of IoT.

For each individual use case, the study specifies the scope within which the IoT system is to be implemented. That is, whether it is a local use case with clear boundaries (for example, a factory, hospital or city), or whether the use case requires nationwide coverage (for example, domestic transport or services provided within the Czech Republic), or whether the use case even requires international coverage (for example, parcel tracking or vehicle connectivity).

It is also specified which of the three IoT categories the given use case falls into, based on its requirements for criticality, reliability and other parameters. In other words, whether it is Critical IoT, Mid-range IoT or Massive IoT. This is a broad classification. If we were to select the ideal IoT technology for a given use case, we would need to define the requirements for all key parameters – as set out in section 3.1.2.

3.2.1 Industry and Manufacturing (Industry IoT)

The Industrial Internet of Things (IIoT) represents a fundamental shift in how the industrial sector operates, connecting machines, sensors and systems to increase efficiency, productivity and safety. By integrating advanced data analytics, real-time monitoring and automation, the IIoT enables organisations to optimise processes, minimise downtime and make data-driven decisions. From predictive maintenance and smart manufacturing to supply chain optimisation and energy management, examples of IIoT applications demonstrate the enormous potential of connected technologies to revolutionise industrial operations across various sectors. The following examples provide an insight into practical applications of the IIoT.

Use Case Name	Description	Scope	IoT Category
Lonely worker protection	Protection of workers in the event of loss of consciousness, a fall, etc. It utilises sensors on the end device and location tracking. The person is therefore part of the system, but communication takes place without their active interaction (which is why it falls under IoT)	Local/na tional	Critical
Connected tools	Not only workers, but their hand tools themselves can be connected to improve work efficiency. As well as for diagnostics, this can also be used to track the location of tools.	Local	Mid-range
Quality control of production outputs	This use case utilises 5G-enabled cameras and machine vision systems for real-time inspection and fault detection in manufacturing processes. The high bandwidth and low latency of 5G enable rapid processing of visual data and the identification of defects or discrepancies on the production line. AI-powered image analysis is typically utilised as part of the solution.	Local	Mid-range
Predictive maintenance (machine monitoring)	Automated monitoring of the condition of assets (machinery) enables manufacturers to optimise maintenance and ensure that downtime due to inadequate maintenance is avoided. It also reduces the consumption of spare parts and minimises unnecessary routine work for staff. Unplanned downtime is one of the biggest obstacles to manufacturers achieving maximum productivity. Studies have shown that unplanned downtime costs industrial manufacturers approximately USD 50 billion annually, with 42 per cent of this downtime being caused by equipment failures.	Local	Mid-range
Operation of AMRs (autonomous mobile robots)/AGVs	5G facilitates the operation of AMRs (Autonomous Mobile Robots) in manufacturing facilities. These robots can transport materials efficiently and safely and adapt to changing layouts and operational requirements. The use of (private) 5G connectivity is particularly beneficial for transmitting data from AMR cameras for processing via edge computing. It is also useful when teleoperation of AMRs is required.	Local	Critical
Site and worker safety in manufacturing	Safety improvements are often achieved through the use of a high-resolution CCTV system combined with AI analytics, which detects undesirable occurrences (missing protective equipment, presence in restricted zones, etc.). Another option is to enhance safety through solutions that prevent collisions between staff and robots, utilising sensors and similar technologies.	Local	Critical
Collaborative robots (cobots)	Collaborative robots, or cobots, work alongside operators to carry out manufacturing tasks such as operational work, drilling or assembly, as well as automatic quality checks on products whilst they are still on the production line. In this way, all parts can be checked automatically, not just samples. Thanks to cobots, factories can inspect every part without increasing the time required to carry out the inspection, thereby improving overall quality and customer satisfaction.	Local	Critical
Digital twins in manufacturing	Effective use of a digital twin requires the processing and management of vast amounts of data. This applies to both the creation and operation of the digital twin. Sensors built into the machines transmit performance data to the digital twin in real time. This data is used to model efficient production processes, configure production lines, etc., but also to plan servicing and reduce maintenance costs.	Local	Mid-range

Transfer of data files to machines or products in production	As part of the manufacturing process, data files need to be transferred – with high reliability and at high speed. These may be files containing production programmes for individual machines, or firmware to be uploaded to products on the production line – for example, vehicles in the automotive sector.	Local	Mid-range

3.2.2 Automotive (Automotive Industry)

The automotive industry is a dynamic and technology-driven sector that encompasses the design, development, manufacture, marketing and sale of motor vehicles. Whilst it is, in principle, part of the wider industrial sector, it is such a significant sector – particularly from an IoT perspective and in terms of its relatively unique and specific IoT use cases – that it makes sense to present IoT use cases in the automotive sector separately.

This vertical encompasses not only passenger cars but also commercial vehicles, motorcycles and the manufacture of spare parts. The automotive industry is at the forefront of technological innovation, driven by advances in autonomous driving, electric vehicles and connected car technologies. Growing consumer demand for greater safety, efficiency and comfort has led to the integration of sophisticated electronics and IoT technologies into vehicles. This development is transforming vehicles into complex, connected systems. Looking ahead, we can expect to see a shift in how vehicles communicate with one another and with external infrastructure, paving the way for smarter, safer and more efficient transport.

Automotive IoT enables real-time data exchange between vehicles, infrastructure and drivers, leading to improved safety, efficiency and user experience. From fleet management and connected infotainment systems to vehicle-to-everything (V2X) communication and automated responses to emergency situations, IoT applications are transforming the automotive industry.

UC Name	Description	Perimeter	IoT Category
Fleet management	IoT fleet management systems use GPS tracking, telematics and real-time data analysis to monitor vehicle locations, optimise routes and manage fuel consumption. This increases operational efficiency, reduces costs and improves safety through adherence to maintenance schedules and monitoring of driver behaviour.	International	Mid-range
Connected infotainment	Connected infotainment systems provide passengers with access to entertainment, navigation and communication services via integrated in-car displays. These systems use IoT to connect to the internet, enabling real-time updates, streaming services and integration with smartphones, thereby enhancing the in-car experience.	International	Mid-range
Vehicle-to-Everything (V2X)	V2X communication enables vehicles to communicate with each other (V2V), with infrastructure (V2I), with pedestrians (V2P) and with networks (V2N). This technology improves road safety by enabling vehicles to share information about road conditions, traffic and potential hazards, facilitating smarter decision-making and helping to avoid collisions.	International	Critical

Emergency Call in the Event of an Accident (eCall)	eCall systems automatically initiate an emergency call to local emergency services in the event of a serious accident. The system provides vital information such as the vehicle's location, the time of the accident and vehicle details, which reduces response times and potentially saves lives.	International	Critical
Remote diagnostics and predictive vehicle maintenance	Remote diagnostics tools use IoT sensors to monitor the condition and performance of vehicles in real time. Data from various sensors can be analysed to diagnose problems before they become serious, enabling timely maintenance and repairs and improving vehicle reliability and safety. Predictive maintenance alerts drivers or fleet managers to servicing requirements, reducing unexpected breakdowns, minimising downtime and extending the vehicle's service life.	International	Mid-range
Remote software updates in vehicles (OTA)	OTA (Over-the-air) updates enable vehicle manufacturers to remotely update software in automotive systems. This applies not only to infotainment and navigation, but also to safety features and autonomous driving functions. This reduces the need for physical recall campaigns and ensures that vehicles remain up to date with the latest features and security patches.	International	Mid-range

3.2.3 Healthcare

The integration of IoT in healthcare is fundamentally changing the way patient care is delivered and managed. Through real-time data collection, remote monitoring and automated processes, IoT in healthcare improves patient outcomes, increases operational efficiency and reduces costs. IoT devices and systems are transforming everything from the management of chronic conditions and hospital operations to personalised care and emergency response. These technologies provide healthcare providers with valuable insights that enable them to make informed decisions, deliver timely interventions and, ultimately, improve the quality of care. The following examples illustrate ways in which IoT is being applied in healthcare.

UC Name	Description	Perimeter	IoT Category
Patient monitoring using wearables and other devices	Remote patient monitoring is considered a key factor in delivering healthcare services more effectively and proactively, and in managing chronic conditions. Using sensors, wearable devices and e-health devices, patient data can be collected and analysed without patients having to travel to a primary care facility or attend a face-to-face appointment with a doctor.	National/International	Mid-range
Connected ambulance	A connected ambulance and its crew act as a means of collecting and transmitting patient information – whether via wearable devices, sensors or HD video/body camera streaming – back to the hospital A&E department whilst the patient is being transported. This enables hospital staff to gain a better understanding of the patient before their arrival. Network slicing is the ideal solution for this use case.	National	Critical

Monitoring patient behaviour within facilities using video analytics.	In hospitals, care homes, psychiatric centres, etc., video analytics can be used in corridors to identify patients who are behaving unusually, have had an incident such as a fall, or are posing a danger to themselves or others. Hosting analytics on-premises using smart cameras can result in disproportionately expensive hardware; therefore, analytics should be carried out in the cloud (or, ideally, using edge computing to maintain data localisation and security).	Local	Mid-range
Transmission and processing of diagnostic and other data	In healthcare, there are many high-resolution images and files that may require high-performance computing for diagnosis and treatment planning. With 5G, for example, once an MRI or CT scan has been received, the images can be sent in real time to where they need to be analysed in order to make a diagnosis. Furthermore, connecting devices to 5G can also be used to track their location within a hospital.	Local	Mid-range
Monitoring patients' vital signs in bed	Multifunctional mats, naturally equipped with connectivity, not only transmit information on patients' vital signs but also monitor their positioning to prevent pressure sores. Hospitals often face problems with highly congested Wi-Fi networks. Therefore, such critical communication definitely belongs on a private 5G network. This also preserves the necessary mobility for moving beds.	Local	Critical
Smart medicine dispensers and implants	Smart medication dispensers remind patients to take their medication on time and dispense the correct dose. This process can be automated, as is the case with insulin pumps, for example. These devices can also alert carers or healthcare providers if a dose has been missed, which improves treatment adherence and reduces the risk of complications.	National/International	Mid-range

3.2.4 Finance and insurance

The **Finance and Insurance** sector encompasses a wide range of activities, including banking, financial services, insurance and investment management. This sector is crucial to the global economy, as it facilitates transactions, manages risks and provides financial protection and growth opportunities for both individuals and businesses. As this sector becomes increasingly digital, the integration of IoT technologies is transforming the way financial and insurance services are delivered. IoT enables real-time data collection, personalised services and more efficient risk management, which ultimately improves the customer experience and operational efficiency.

The following examples illustrate how the IoT is transforming the financial and insurance sectors by offering smarter, more connected and faster services.

UC Name	Description	Perimeter	IoT Category
Insurance based on actual risk levels	IoT devices, such as in-vehicle telematics or wearable devices, collect data on user behaviour (e.g. driving habits or health metrics) to tailor premiums to the actual level of risk. This approach offers more personalised and fairer pricing that rewards safer behaviour with lower premiums.	National/International	Mid-range

Pay-as-you-go insurance	Insurance is charged based on actual usage, using automatically transmitted information. Examples include motor insurance or travel insurance, which is automatically activated when crossing borders.	International	Mid-range
ATM management using IoT	IoT technologies are used to monitor and manage ATMs in real time. Sensors and connected devices can monitor cash levels, detect potential problems such as malfunctions or tampering attempts, and even predict maintenance needs before a failure occurs. In addition, IoT can help optimise cash replenishment schedules, reduce operating costs and ensure that ATMs are always operational and safe for customers.	National	Mid-range

3.2.5 Energy and utilities

The **Energy and Utilities** vertical encompasses industries involved in the production, distribution and management of essential resources such as electricity, natural gas, water and renewable energy sources. This sector is essential to modern life, powering homes, businesses and industry whilst ensuring the efficient and sustainable use of natural resources. With growing demand for energy and the need for sustainable practices, the integration of IoT technologies is becoming increasingly important. IoT enables real-time monitoring, smart grid management, predictive maintenance and improvements in energy efficiency, which are key to modernising energy and utilities infrastructure.

UC Name	Description	Perimeter	IoT Category
Smart metering	Smart metering uses IoT technology to monitor electricity, gas or water consumption in real time. It provides detailed insights into consumption patterns, enables remote meter reading and supports dynamic pricing models, helping both consumers and utility companies to manage resources more efficiently.	National	Massive
Smart grid	A smart grid is an advanced electricity network that utilises IoT technology, data analytics and automation to manage the generation, distribution and consumption of electricity more efficiently and reliably. Unlike traditional energy networks, which operate statically and in a single direction, a smart grid enables two-way communication between the utility and consumers, as well as between different parts of the network. This allows for real-time monitoring, dynamic load balancing and better integration of renewable energy sources.	National	Mid-range
Utility Management – Water	IoT devices monitor water distribution networks for leaks, pressure changes and quality issues. Real-time helps utilities to quickly identify and resolve issues, reduce water losses, ensure water quality and optimise water usage.	National	Massive
Smart Buildings and HVAC (Heating, Ventilation and Air Conditioning) Systems	IoT devices in homes and buildings help manage energy consumption by controlling HVAC (heating, ventilation and air conditioning) systems, lighting and appliances based on real-time data and user preferences. These systems optimise energy use, reduce costs and contribute to a more sustainable energy ecosystem.	National	Massive
Smart street lighting	IoT-enabled smart street lighting systems automatically adjust lighting levels according to environmental conditions, time of day or footfall. These systems reduce energy consumption, lower maintenance costs and enhance the safety of public spaces by providing adequate lighting where it is needed.	Local/National	Massive

3.2.6 Municipality and Smart Cities

The **Municipalities and Smart Cities** vertical encompasses public sectors responsible for managing and delivering services to communities and citizens, including infrastructure, public safety, transport, environmental management and utilities. This sector is increasingly utilising IoT technologies to create more efficient, sustainable and liveable urban environments. By integrating connected devices, real-time data analytics and automation, governments and municipal authorities can improve service delivery, manage resources more efficiently and engage citizens more effectively. The concept of smart cities, in which the IoT plays a key role, focuses on using technology to improve quality of life, increase efficiency and promote sustainable development in urban areas.

Some use cases are, in fact, common to both the Energy sector and Smart Cities. These include, in particular:
- Smart buildings and HVAC systems.
- Smart street lighting.
- Smart metering.

Smart cities are, in fact, major energy consumers, and energy costs account for a significant proportion of the municipal budget. It is therefore in the vital interest of local authorities to adopt modern technological solutions that will help them optimise energy consumption. And IoT systems are a key part of these solutions.

UC Name	Description	Perimeter	IoT category
Traffic Management	Real-time traffic monitoring and management supported by IoT systems can reduce traffic congestion and improve urban mobility. Another application is the monitoring of parking spaces and dynamic vehicle guidance based on occupancy. 5G will provide suitable connectivity for this use case wherever it is not possible or cost-effective to use fixed connectivity.	Local/National	Critical
Connecting public transport vehicles	Connecting public transport vehicles is necessary for a number of reasons. These include optimising public transport capacity utilisation, communication with control centres and management systems, transmitting data from cameras, providing information services to passengers, and, where applicable, connectivity for passengers, etc. Some of these scenarios fall within the IoT category.	Local	Mid-range
Environmental monitoring	There is a wide range of environmental parameters that it is beneficial to monitor using various types of sensors – air quality, water quality, CO_2 concentration, humidity, waste, etc. This is typically an IoT scenario and therefore lends itself to the use of 5G mMTC.	Local/National	Massive
City security	City security is managed by surveillance systems and applications used by the city police. In these cases, guaranteed service availability with defined parameters is once again crucial.	Local	Mid-range
Energy and utilities for a smart city	Energy expenditure often constitutes a significant cost item in a city's budget. Modern approaches to managing energy resources and consumption can significantly reduce costs. These include, for example, advanced facility management of municipal buildings, including smart metering and public lighting control. IoT systems and reliable connectivity are essential prerequisites for all these modern solutions.	Local	Massive

Waste management	IoT sensors installed in litter bins and waste containers monitor fill levels and optimise waste collection routes. This reduces operating costs, minimises the environmental impact and ensures more efficient waste collection, preventing overflow and improving the cleanliness of public spaces.	Local	Massive

3.2.7 Agriculture and Food

Vertical **Agriculture** is essential for global food production and encompasses activities related to farming, livestock rearing, crop cultivation and the overall management of agricultural resources. This sector is increasingly utilising technology to boost productivity, efficiency and sustainability in the face of challenges such as climate change, resource scarcity and a growing global population. IoT technologies play a key role in modernising agriculture by providing real-time data, enabling precision farming and automating processes. These advances help farmers make informed decisions, optimise resource use and, ultimately, increase yields whilst reducing environmental impacts.

UC Name	Description	Perimeter	IoT Category
Autonomous tractors and agricultural machinery	Autonomous tractors and other agricultural machinery use 5G to receive and transmit data in real time, enabling them to carry out tasks such as planting, weeding and harvesting more efficiently, with minimal human intervention. As with other autonomous vehicles, 5G enables efficient teleoperation where necessary and the transmission of data from cameras on the machinery for immediate analysis.	Local	Critical
Automated harvesting systems	Automated harvesting systems use robotic machines to harvest crops autonomously. These systems typically consist of self-driving vehicles equipped with sensors, cameras and robotic arms that can identify ripe crops, cut or pick them with precision, and collect the produce. The effectiveness of these systems depends on their ability to process vast amounts of data in real time, make rapid decisions and operate with high precision across large areas of agricultural land.	Local	Mid-range
Smart irrigation systems	Smart irrigation systems utilise a network of sensors distributed across the entire agricultural field. These sensors measure various environmental and soil parameters, such as moisture levels, temperature and even the nutrient status of the soil. The sensors send data to a central system for analysis. This may be an edge server. Based on the analysis, commands are sent to the irrigation system to adjust the irrigation schedule as required. This may involve switching sprinklers on or off, adjusting the flow rate or changing the timing of irrigation. The system can target specific zones within the field to ensure that each area receives the precise amount of water required.	Local	Massive
Livestock Monitoring	Monitoring focuses on tracking the location and health status of animals. Wearable IoT devices collect data on the location, health and behaviour of livestock. 5G ensures the continuous transmission of this data, which can be used for real-time health monitoring, disease prediction and the optimisation of breeding cycles.	Local	Massive

Crop and Soil Monitoring	Crop monitoring systems utilise various sensors deployed across the field. These include soil moisture sensors, nutrient level sensors and climate sensors that measure parameters such as temperature, humidity and CO_2 levels. Drones provide additional data that is essential for assessing crop health on a larger scale. These images can detect variations in colour, size and crop development, which indicate the crop's health and nutritional status. Data collected from ground-based sensors and aerial imagery are integrated and transmitted to a central unit, where advanced data analysis is carried out. The system provides useful information that can be utilised immediately. For example, if a potential pest infestation is detected, the system can recommend specific areas for pesticide application.	Local	Massive
Tracking products from farm to point of sale	This UC addresses a key aspect of the agricultural supply chain: ensuring transparency, traceability and efficiency from the point of origin right through to the consumer. Products are tagged at farm level using barcodes, RFID tags or smart sensors capable of capturing and recording various data, including harvest time, origin, treatments and quality assessments. Stakeholders can track the status and progress of goods as they move through the supply chain. This monitoring helps with logistics management, route optimisation, responding to delays and ensuring compliance with safety and quality standards.	National/International	Massive
Monitoring of transport conditions for agricultural produce	UC focuses on maintaining the integrity and quality of agricultural goods during transport from farms to markets or to processors. Sensors are integrated into transport vehicles or individual product packages. During transport, these sensors monitor various environmental parameters, such as temperature, humidity, vibration and atmospheric pressure – factors that are crucial for maintaining product quality. The data is transmitted to a central unit, analysed and subsequently used to generate relevant reports.	National/International	Massive
Automated greenhouses	IoT-enabled greenhouses use sensors and automation to control temperature, humidity, lighting and ventilation. These systems create optimal growing conditions, improve crop yields and reduce the need for manual intervention.	Local	Massive

3.2.8 Transport and Logistics

The **Transport and Logistics** sector is crucial to global trade and the movement of goods, encompassing transport network management, freight transport, warehousing and supply chain operations. This sector is responsible for ensuring that products reach their destinations efficiently, safely and on time. The integration of IoT technologies into transport and logistics is transforming the sector by enabling real-time tracking, route optimisation, improved fleet management and enhanced overall visibility across the supply chain. These advances help companies reduce costs, increase efficiency and respond more effectively to dynamic market demands, whilst improving service quality and customer satisfaction.

Some use cases in the Transport sector overlap with those in the Automotive sector, specifically:

- V2X communication between vehicles and infrastructure
- Fleet management.

Use Case Name	Description	Scope	IoT category
Digital twin of a logistics organisation	A digital twin of a complex system such as a logistics centre – in many cases a port, or in our context, for example, a railway terminal – enables the efficiency of the entire hub to be improved through the modelling of 'what-if' scenarios and the analysis of vast amounts of data collected by sensors and cameras from the real environment and fed into the digital twin.	Local	Mid-range
Inventory management	Monitoring and managing stock. Ideally in real time. For example, in the form of a so-called 'smart shelf'. And/or using RFID and barcode scanners. In any case, all information must be held in digital form and the data transmitted to a central component, which may be located at the edge. Everything is then managed using warehouse management system software.	Local	Massive
Asset tracking	Tracking items during transport is an important part of managing the entire supply chain and a prerequisite for its efficiency. Nationwide coverage technology is required, specifically from the LP-WAN category. In the case of 5G, this could therefore be RedCap or Passive IoT.	National/International	Massive
Product packaging using computer vision	The use of 'computer vision' for packaging quality control in logistics. Computer vision is a field of artificial intelligence that trains computers to interpret and understand the visual world. Using digital images from cameras and videos, along with deep learning models, computer vision systems can accurately identify and classify objects and then respond to what they 'see'.	Local	Mid-range

4 IoT business models

IoT solutions must have a viable business model. In this context, an IoT solution is a set of products and services based on them, tailored to meet the needs of customers in a given vertical.

Historically, the absence of a viable or suitable business model has been one of the reasons why the growth of IoT services has generally failed to meet very ambitious forecasts.

Let's first look at what a business model actually is and what it consists of. The general definition of a business model is as follows:

A business model defines how a company creates value, delivers it to customers and receives value in return from them.

A business model therefore has three main areas:

1. **Value creation** – what customer problems you solve, what needs you satisfy through the products and services you provide to the customer. This is how the customer derives value. This value is defined as the Value Proposition. Ideally, it differs from the value provided by competitors; it is unique, hence the term Unique Value Proposition.
2. **Value delivery** – what is the cost structure of the products and services, how are they distributed to the customer and made available for their use?
3. **Capturing value** – the way in which the company recoups value for itself. This is determined by its revenue model.

For a business model to work, the following rules must apply:

- The value perceived by the customer must be greater than the value returned to us. This is the essence of a sound Value Proposition.
- At the same time, the value the company recovers must exceed the cost of delivering that value.

These general rules will, of course, also apply to the Internet of Things and the solutions offered in this field.

This means, therefore, that for an IoT solution to be successful, the customer must clearly perceive the benefits of the IoT system and be willing to pay for them.

Let us first look at the general business model for an IoT solution. We can use the Lean Canvas,[14] and the Value Proposition Canvas to focus on how value is created, delivered and recouped.

[14] Maurya, A. (28 February 2012). *Running Lean*. (O'Reilly Media, Inc.).

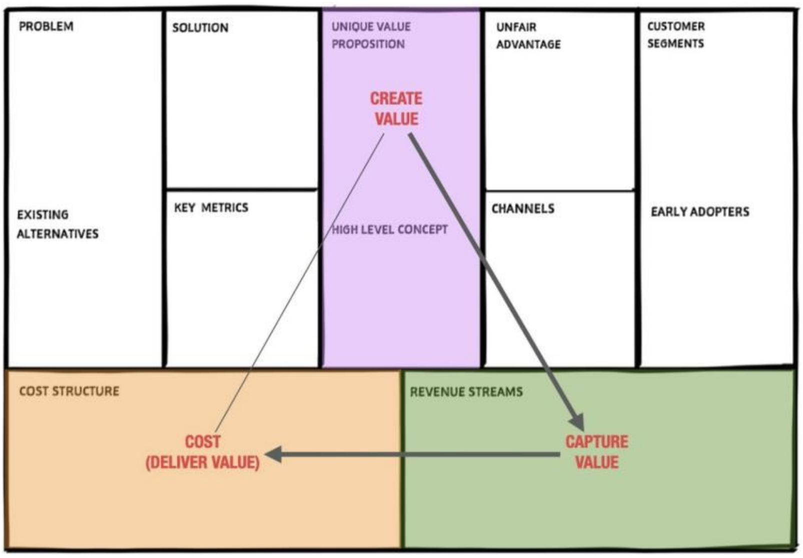

Figure 9: Lean Canvas. Source: [15]

1. The value delivered by an IoT solution (Value Proposition)

IoT systems typically generate and deliver **information** as **value**. As discussed in section 3.1.1, there are two main types of IoT systems:

- One-way systems provide information for further analysis.

Monitoring of stock levels, machine wear and tear, health data, air quality and a myriad of other examples. This information must be analysed further and may lead to certain actions and measures, which, however, take place outside the system.

- Interactive systems utilise the information directly for automation and control.

Based on the information generated within the IoT system, the system's active components (actuators) directly carry out actions leading to the optimisation of production processes, optimisation of energy consumption or other actions.

It is clear that in both these types of IoT systems, the information and its use can be of enormous value to the IoT system's customer. What determines this value? **The output from the IoT system must address a genuinely significant problem or need of the customer. At the same time, this problem or need is not sufficiently met by any other existing solution.**

For example: for a company suffering from high machine maintenance costs and/or frequent machine downtime due to breakdowns, predictive maintenance using an IoT system can be an excellent, high-value solution. However, if a company's machines operate virtually fault-free and require only simple maintenance, the company's willingness to invest in an IoT system for predictive maintenance will not be high.

When creating value – that is, designing an IoT system that will generate value – it is essential to focus primarily on identifying and defining the problem or need of the customer and users of the IoT system, and on devising a solution to it.

It is possible and advisable to use the Value Proposition Canvas to define the Value Proposition. This comprises the customer area and the product area.

Customer section:

- On the left: the tasks the customer needs to carry out ('jobs to be done').
- Bottom: Pains/pain points, i.e. the problems that trouble the customer.

---

[15] Maurya, A. (28 February 2012). *Running Lean*. (O'Reilly Media, Inc.).

- Top: Gains, i.e. the improvements expected by the customer.

Product area (in this case, an IoT solution):

- Right: Product or service features that enable the customer to carry out their tasks.
- Bottom: Painkillers, i.e. features of the product or service that eliminate the customer's individual pain points.
- Top: Vitamins, i.e. features of the product or service that will bring the customer the expected improvements.

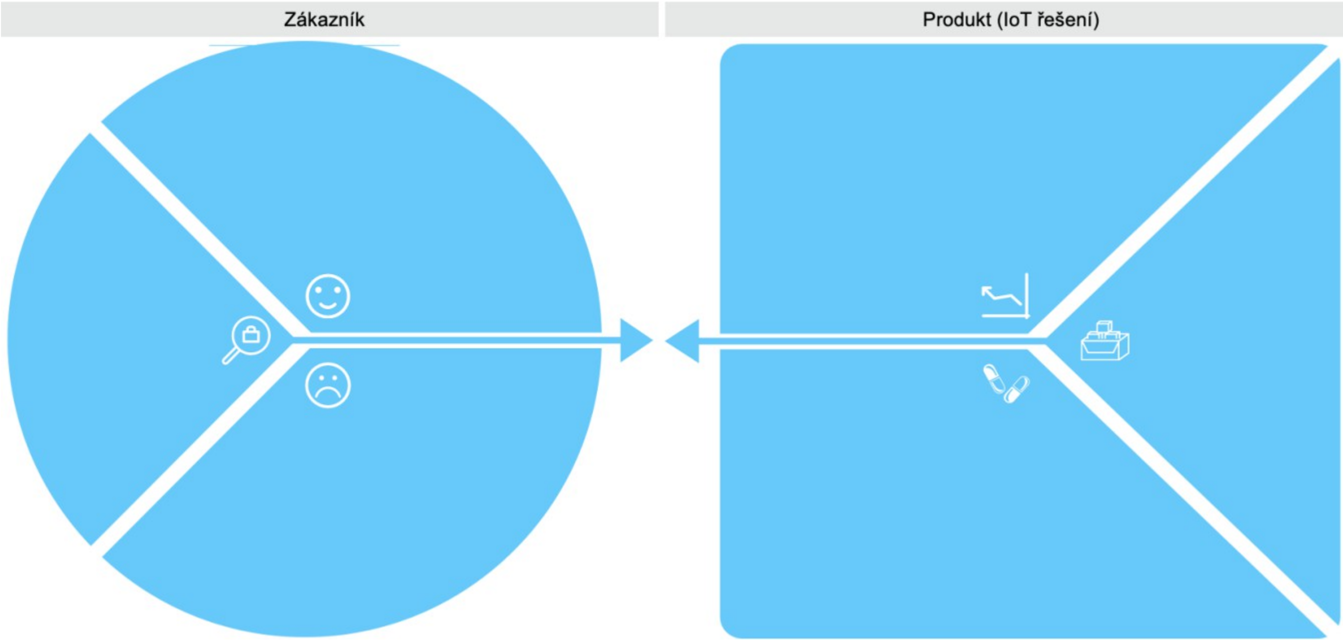

Figure 10: Value Proposition Canvas template. Source: Own work.

Technical aspects such as the type of end devices, transmission technology, etc., will be addressed in the next phase.

2. Value delivery and cost structure.

In the IoT sector, value is delivered via a complex system. As outlined in Chapter 1.2, the elements of an IoT system primarily consist of:

- Devices: These include sensors, actuators, smart appliances and other connected hardware that collects and transmits data.
- Networks: The communications infrastructure that enables devices to connect and exchange data (e.g. 5G).
- Data processing elements: Cloud services, edge computing devices and applications that process and analyse data collected by devices.
- Users: Human operators, automated systems or decision-makers who utilise the information generated by the IoT system.

IoT systems often utilise standardised devices, technologies and services. On the other hand, with the exception of Consumer IoT, these systems are typically bespoke solutions designed for customers such as manufacturing firms, energy companies, hospitals or, for example, cities. These are technologically complex solutions that often require the involvement of several suppliers and a systems integrator capable of combining the individual elements of the solution into a functional system.

From a cost structure perspective, it is also a complex system that may involve various cost categories. For example:

- One-off costs associated with end-user equipment, the provision of professional services, etc.
- Ongoing costs associated with the use of communication technologies, system monitoring, etc.
- Usage-based costs associated with the use of cloud services.

3. Value creation – revenue model.

Generally speaking, there are a number of revenue models. For example:

- A one-off sale of a product.
- A one-off fee for services provided.
- Subscription/rental – a recurring monthly/annual fee for the use of a product or service.
- Transaction fees (compared to a subscription, the key difference is that the fee is not necessarily recurring, but transaction-based).
- Metered services (Pay-As-You-Go) – metered services are billed according to actual usage over a specific period.
- Marketplace – a model based on facilitating transactions between buyers and sellers.
- Big data – a model based on the use and monetisation of generated data.

And, of course, combinations of different revenue models.

In the case of IoT, the situation is complicated by the fact that the cost side typically involves various cost categories, making it difficult to set up a simple revenue model – for example, in the form of a single fixed monthly fee. This could entail risks for IoT solution providers. It will therefore be more common to combine several revenue models within a single IoT system.

For example:

- A one-off fee for IoT hardware (end devices – sensors).
- A recurring monthly fee for each connected IoT device. The total amount will therefore depend on the number of devices.
- A monthly fee based on actual resource consumption for cloud services – computing resources, storage and other services.

However, the ‘as a service’ model is also beginning to gain ground in the IoT sector. This means a model based on the IoT solution provider managing the relevant area and providing it to the customer as a service under clearly defined terms (it is therefore not a one-off transactional business in the form of a product sale). These models are more likely to succeed in situations where the area does not cover the entire IoT system. For example:

- ‘Device-as-a-Service’ model: IoT hardware is offered under a subscription model, whereby the user pays for the value delivered by the device (e.g. smart lighting, connected industrial equipment). The subscription covers both the hardware and connectivity.
- ‘Data-as-a-Service’ model: Companies collect and sell (anonymised) data generated by IoT devices. This is possible in sectors such as agriculture, where data from sensors can be monetised. In principle, companies pay for the data received; the price already includes the entire ecosystem required to generate it.
- ‘Platform-as-a-Service’ (PaaS) model: IoT platforms provide the software infrastructure for managing, analysing and integrating data streams from devices, often on a subscription basis. The cost of the platform will usually need to be considered alongside the costs of other parts of the IoT ecosystem, such as devices, connectivity, etc.

- Outcome-based models: Providers charge customers based on the results or effects achieved through IoT solutions, such as improvements in efficiency or reductions in production or energy management costs.

The role of 5G within the IoT business model

As already mentioned, 5G technology affects not only the communication and perception layers, but also the security and business layers. It therefore logically plays a significant role in shaping the IoT business model.

5G technology is, in principle, relatively expensive, partly due to its advanced features requiring sophisticated technical solutions, and partly due to the high development costs that suppliers must factor into their prices. Furthermore, it is typically provided on a licensed spectrum, which is therefore subject to high costs.

On the other hand, 5G offers the potential for high efficiency and capabilities that can enable solutions which would not be possible with inferior technology. This applies in particular to IoT solutions in the ‘Critical IoT’ category. This means that IoT solutions built on 5G technology can deliver high perceived value to the customer. This makes it possible to present a viable business model even when charging a relatively high price.

The roles of the provider and user of IoT solutions

When developing a new product or solution, the standard procedure is for the company developing the product to define the value proposition based on an understanding of its customers’ needs.

In the case of IoT solutions, the situation is potentially even more complex in that the IoT solution provider is an expert in the technology stack required to implement the IoT system. However, it is typically the user who is able to define how the information obtained from the IoT system will be utilised. From this perspective, it is important that the user of the IoT system is involved in its design. Only then can the IoT system deliver maximum value to the user in the form of the right information needed to gain deep insights into the issue at hand, or directly for the management and automation of processes.

5 The current state and future of IoT

5.1 IoT Market Overview

5.1.1 The Global IoT Market and Its Development

Measuring the IoT market is extremely challenging, as it encompasses a vast number of different use cases, verticals, technologies and solutions. IoT is a truly broad concept and, in practice, there is no single methodology that would allow for a uniform classification. Consequently, the figures presented by various agencies and analyst firms may differ considerably.

For example: if a solution includes a connected camera, should the full value of the camera be counted as part of the IoT market, or only a specific portion corresponding to the value of the wireless module?

Figures on the IoT market must therefore be interpreted with these specifics in mind. Nevertheless, they still provide useful information on the overall size, structure and growth dynamics of the IoT market. And they demonstrate that this is a truly significant sector.

The following chart shows a forecast by Transforma Insights[16]of the number of IoT connections between 2022 and 2033, which is expected to rise linearly to 39.6 billion connections.

The company defines an IoT connection as a connection to remote sensing and control devices, and also includes related aggregation devices.

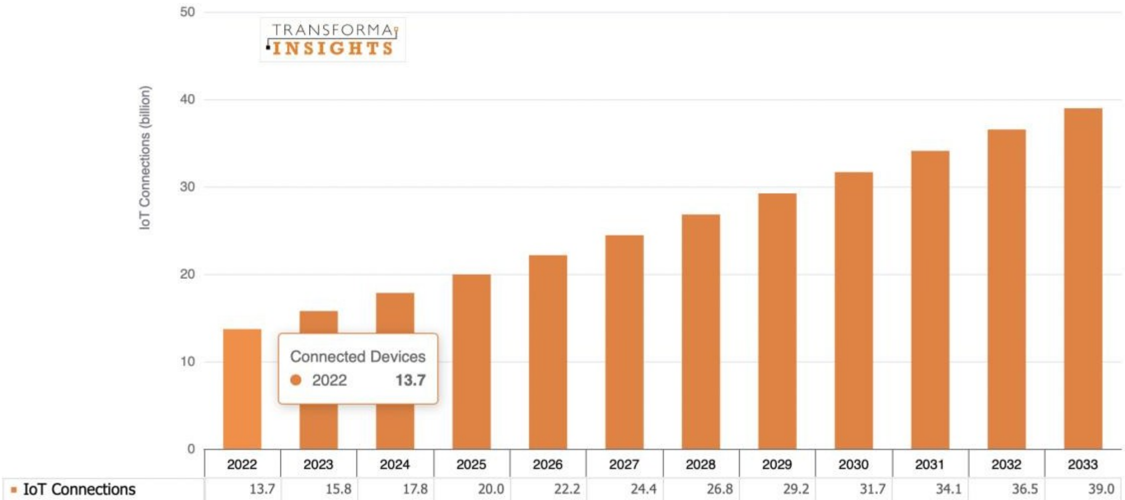

Chart 1: Number of IoT connections 2022–2033. Source: “Current IoT Forecast Highlights – Transforma Insights.”

[16] "Current IoT Forecast Highlights - Transforma Insights," Transforma Insights, n.d., https://transformainsights.com/research/forecast/highlights.

Given the size of the consumer market, consumer IoT—including devices such as smart TVs and smartwatches—is forecast to dominate in 2033. Specific vertical markets are much more fragmented, but also include smart metering applications, which account for a significant number of connections and are expected to increase by a further 88 million connections in Europe alone between 2024 and 2028[17] . Vertical (enterprise) markets include vertical-agnostic applications, such as connected heating, ventilation and air-conditioning systems and connected security systems deployed in an enterprise context. The largest region is China (and Taiwan), followed by Europe and North America.

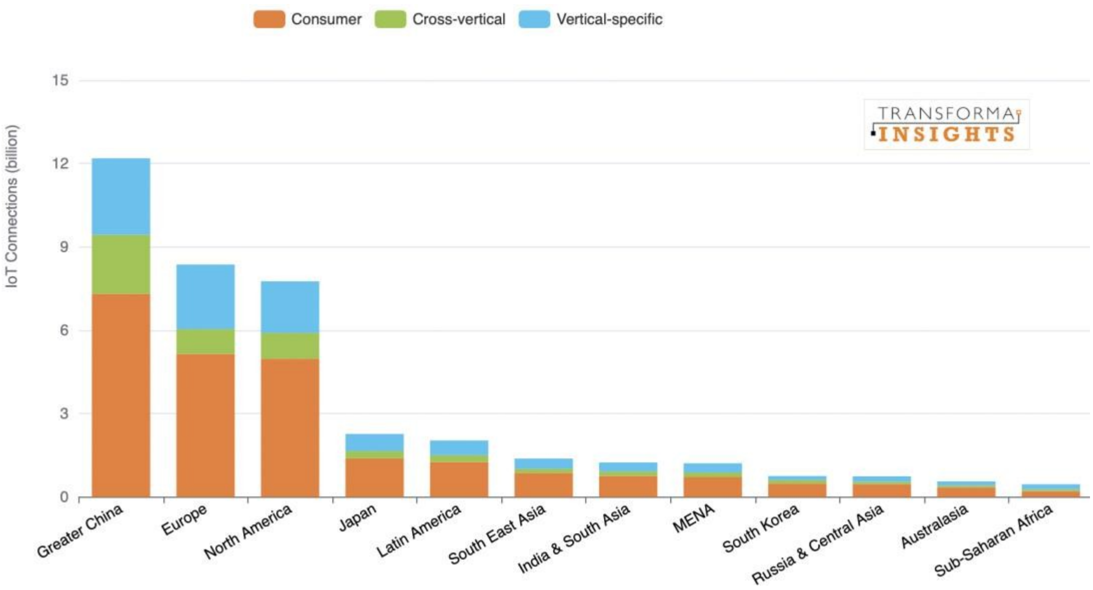

Figure 2: Forecast for IoT connections in 2033 by region. Source: "Current IoT Forecast Highlights – Transforma Insights."

Looking specifically at cellular IoT connections (i.e. technologies provided via mobile networks), the forecast indicates a high expected growth in 5G mMTC technologies. For the purposes of this overview, mMTC includes not only RedCap and Passive IoT, but also the original 4G technologies NB-IoT and LTE-M. Conversely, a gradual phase-out of 2G and 3G networks can be expected.

[17]https://www.smart-energy.com/industry-sectors/smart-meters/326-million-smart-meters-across-europe-by-2028-report/

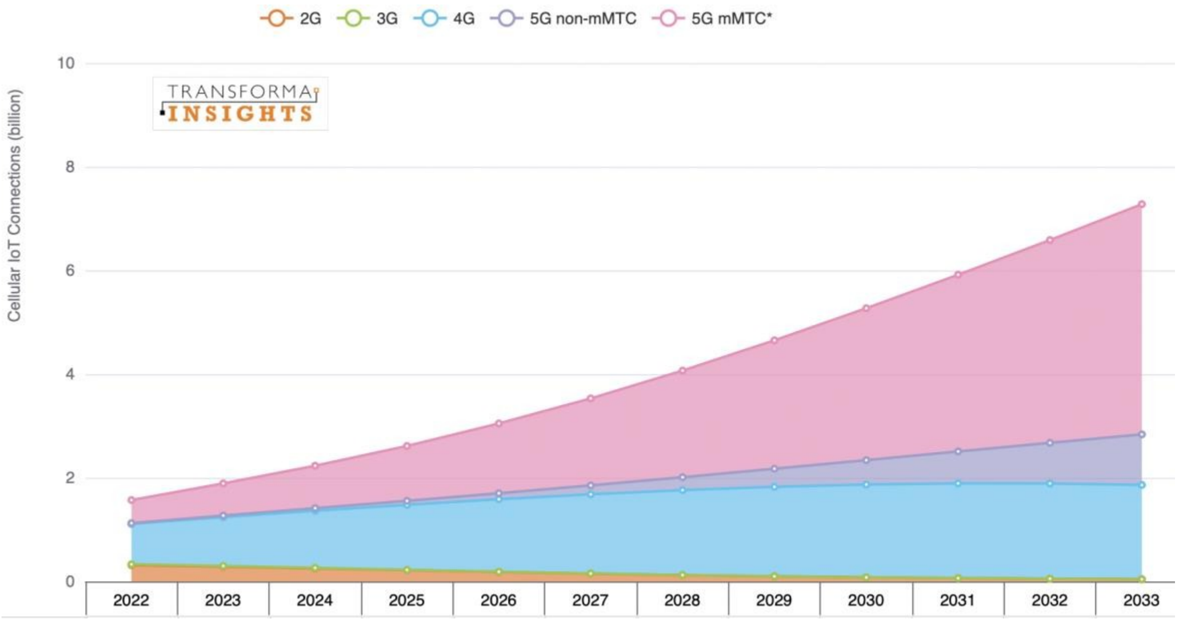

Figure 3: Cellular IoT connections by technology. Source: "Current IoT Forecast Highlights – Transforma Insights."

According to IoT Analytics, the market for enterprise IoT solutions reached a value of USD 269 billion in 2023, representing a year-on-year increase of 15 per cent. It should be noted that, in this case, the market is defined in terms of enterprise expenditure. The largest share of this expenditure, by technology, was accounted for by IoT hardware at 49 per cent, followed by IoT software and IoT services, both at 24 per cent. Once again, the smallest share, at 2
% as part of the solution. Next year, the company estimates that, given global economic developments, this growth will slow to 12 per cent, before accelerating again in 2025 to reach USD 690 billion by 2030. The company defines the IoT as a network of physical objects connected to the internet. Data from devices connected to the Internet of Things is often used to create new applications for end users. Connected personal computers, tablets and smartphones are not considered part of the IoT, even though they may form part of the solution setup. Devices connected via extremely simple connection methods, such as radio-frequency identification or quick response codes, are not considered to be IoT devices. Verticals are divided into eleven categories, such as the automotive sector or process manufacturing, which are expected to see the highest growth in the future, primarily due to the transition to electromobility, autonomous driving, or increased operational efficiency and modernisation of operations in the case of process manufacturing. The increasing number of companies achieving a positive ROI from IoT adoption is also expected to contribute to global growth.[18]

[18] Joaquin Fernandez, "IoT market update: Enterprise IoT market size reached $269 billion in 2023, with growth deceleration in 2024," IoT Analytics, 9 July 2024, https://iot-analytics.com/iot-market-size/.

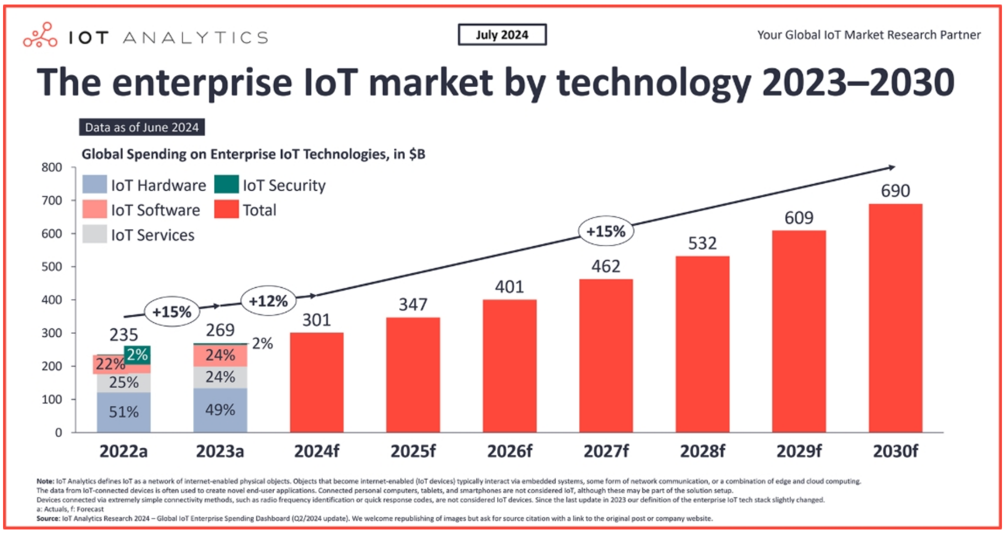

Figure 4: Enterprise IoT market. Source: https://iot-analytics.com/iot-market-size/

The complexity of measuring the size **of the 5G IoT market** is illustrated by the differing figures provided by research agencies. In this case, the 5G IoT market includes all devices, as well as other components of solutions that utilise 5G Standalone or 5G Non-Standalone technologies – in other words, those that utilise 5G architecture either fully or at least partially. Whilst SkyQuest estimated its size at USD 8.53 billion in 2022[19], Precedence Research put the figure at USD 4 billion[20]. Forecasts also differ in terms of market size (e.g. USD 136.18 billion and USD 481.93 billion for 2031) and growth rates (34.12% and 70.4%), although both companies classify the verticals into the same eight categories:

- Manufacturing (e.g. industrial automation, predictive maintenance, asset monitoring),
- Healthcare (e.g. remote patient monitoring, connected ambulances, connected healthcare facilities)
- Energy and Utilities (e.g. smart grids, smart meters, pipeline management),
- Automotive and Transport (e.g. fleet management systems, connected vehicles, autonomous vehicles),
- Supply Chain and Logistics (e.g. asset tracking, inventory management, logistics and warehouse automation),
- Government and Public Safety (e.g. smart parking, smart street lighting, environmental monitoring),
- Agriculture (e.g. precision farming, livestock tracking, asset tracking),
- others (e.g. retail, smart buildings and education).

The global consumer Internet of Things (IoT) market was valued at USD 75.10 billion in 2022 and is expected to grow to approximately USD 193.58 billion by 2030, at a compound annual growth rate (CAGR) of approximately 12.71 per cent between 2023 and 2030. Governments and the private sector are increasing internet and infrastructure penetration, leading to widespread

[19] "5G IoT Market Size, Share, Trends, Analysis and – Industry Growth | 2031," n.d., https://www.skyquestt.com/report/5g-iot-market.

[20] Precedence Research, "5G IoT Market Size To Hit USD 823.14 Bn By 2032," 23 August 2023, https://www.precedenceresearch.com/5g-iot-market.

the use of voice assistants and smart home devices. Advanced household appliances and wearables will continue to be the main segments of this market.[21]

Statista forecasts that revenue in the European IoT market will grow steadily between 2024 and 2029, totalling 107.2 billion US dollars, representing an increase of 60.55 per cent. According to the chart above, revenue is expected to peak in 2029 at 284.3 billion US dollars. According to the company, internet penetration is a key factor influencing the Internet of Things market. Widespread and reliable internet connectivity is essential for the seamless operation of IoT devices, enabling them to communicate, transmit data and receive updates. Current trends influencing the development of the IoT include 5G networks, artificial intelligence of things (AIoT), IoT security and edge computing.[22] With regard to security, it is worth noting the growing trend of cyber-attacks on IoT devices, which reached 112.3 million in 2022, representing a year-on-year increase of 87 per cent.[23]

In addition to revenue, investment in IoT-related solutions is also on the rise. The International Data Corporation estimates that European organisations will invest approximately $260 billion in 2024 and also forecasts that spending on the Internet of Things will continue to rise in 2024 as the European economy recovers, recording a five-year compound annual growth rate (CAGR) of 11.8 per cent and reaching nearly $368 billion by 2027.[24]

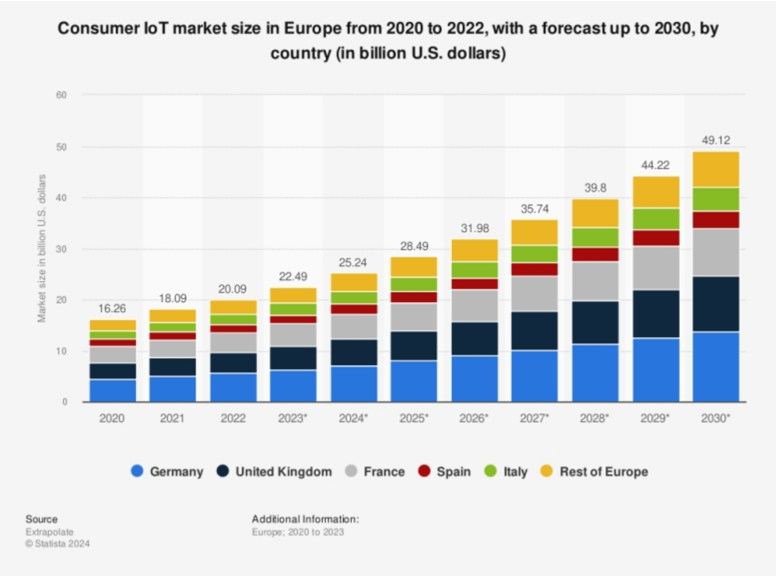

Figure 5: Forecast of the size of the European consumer IoT market for the period 2020–2030.
Source: https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

Statista also provides a more detailed overview of the European consumer IoT market, estimating its size at US$20.9 billion in 2022 and forecasting growth to US$49.12 billion by 2030. The UK, France and Germany are set to be the largest players in Europe. Germany, in particular, is expected to reach USD 13.8 billion by 2030, with a growth rate of 11.7 per cent.

[21]https://www.extrapolate.com/information-technology-communication-iot/consumer-iot-market/87454

[22] "Revenue of the Internet of Things industry in Europe 2019–2029," Statista, 5 July 2024, https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

[23] "Global annual number of IoT cyber attacks 2018–2022," Statista, 3 May 2023, https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/.

[24]https://www.idc.com/getdoc.jsp?containerId=prEUR251780724

5.1.2 The IoT market in Germany

The German market, both in the 5G and IoT sectors, is among the most advanced in the world, thanks in part to its strong industrial base. The industrial sector requires digitalisation to remain competitive on a global scale. This, in turn, leads to a need for advanced communication technologies and, specifically, IoT solutions, particularly in the fields of Industrial IoT and the automotive sector. It is fair to say that the German 5G and IoT market is several years ahead. It therefore serves as a good indicator of how the market in the Czech Republic is likely to develop.

At the same time, the German market is well mapped out, as its size makes it attractive to suppliers from all parts of the value chain.

The following chart shows the structure of the German IoT connectivity market by vertical sector.[25]

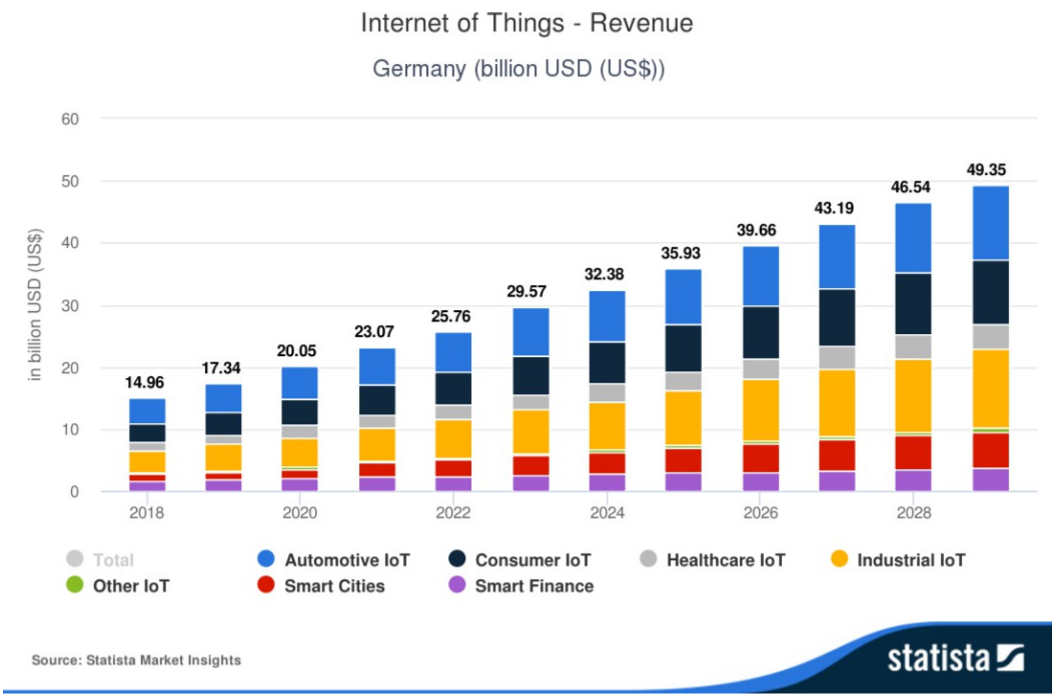

Chart 6: The IoT market in Germany by vertical sector. Source: Statista.

The utilities sector has the highest number of connections

The utilities sector will have a total of 51.6 million IoT connections by 2032, representing 27 per cent of the total number of IoT connections in Germany. This sector is supported by government initiatives; the aim is to achieve 95 per cent deployment of smart meters by 2030. Part of the €28 billion that Germany received from the EU's Recovery and Resilience Fund following the COVID-19 pandemic has been earmarked to support these efforts.

[25] 'Revenue of the Internet of Things industry in Europe 2019–2029', Statista, 5 July 2024, https://www.statista.com/forecasts/1283723/revenue-from-internet-of-things-in-europe.

The automotive industry is the largest sector in terms of IoT revenue

51 per cent of IoT revenue in 2032 will be generated by the automotive sector. Germany is home to some of the world's largest car manufacturers, such as BMW, Daimler and Volkswagen, all of which have contracts for connected vehicles. Car manufacturers typically have contracts for international connectivity, as many vehicles are manufactured in Germany but sold elsewhere (the SIM card is activated outside Germany). The table below shows the overall size of the IoT connectivity market in terms of the number of connections, revenue and growth rate.

	2015	2022	2032	CAGR 22–32
Number of wireless connections	4.8 m	43.1 m	142.0 m	12.7%
Connectivity revenue	74.9 m EUR	381 m EUR	686 m EUR	6.0%
ARPU from connectivity	1.6 EUR	EUR 0.73	0.39 EUR	–6.1%

As the number of connections grows significantly, the average price per connection will fall. However, the rate of growth will be high enough that total revenues will grow at a solid annual rate of 6 per cent.

As regards the structure of IoT connectivity, the majority of the market will be served by technologies that could be collectively referred to as 3GPP or operator-based. The expected high share of NB-IoT is particularly noteworthy. We believe, however, that in the medium to long term, this technology may be replaced by newer technologies such as RedCap and Passive IoT.

Mobile operators operating in Germany are also the largest providers of IoT connectivity in Europe: Deutsche Telekom, Telefónica and Vodafone.

In addition to these, several major players provide IoT connectivity. Some of them use LoRa WAN technology and thus their own networks, whilst others operate as MVNOs, utilising the networks of various mobile operators. Their services run on 2G, 3G, 4G, LTE-M and NB-IoT technologies, depending on requirements and availability.

This overview of providers is also interesting because many of them offer IoT connectivity services on both a European and global scale, and may therefore also be an option for Czech companies seeking global connectivity for their IoT projects.

IoT connectivity provider	**Type of provider**
1NCE	MVNO
emnify	MVNO
InsideM2M	MVNO
Things Mobile	MVNO
Wireless Logic	MVNO
Digimondo	LPWAN
komro	LPWAN

Minol Zenner	LPWAN
Sigfox Germany (Heliot)	LPWAN
Netze BW	Enterprise

5.1.3 The IoT market in the Czech Republic

For a macro view of the IoT market in the Czech Republic, we will examine data from Statista[26]. Revenue in the Czech Republic's Internet of Things market is projected to grow at a compound annual growth rate (CAGR) of 9.30% between 2024 and 2029. This growth trajectory is expected to result in a market size of USD 2.87 billion by 2029. Among the various verticals, automotive and industrial IoT will dominate. The forecast is based on various market indicators, such as consumer spending, internet penetration, 4G coverage, and current and historical trends.

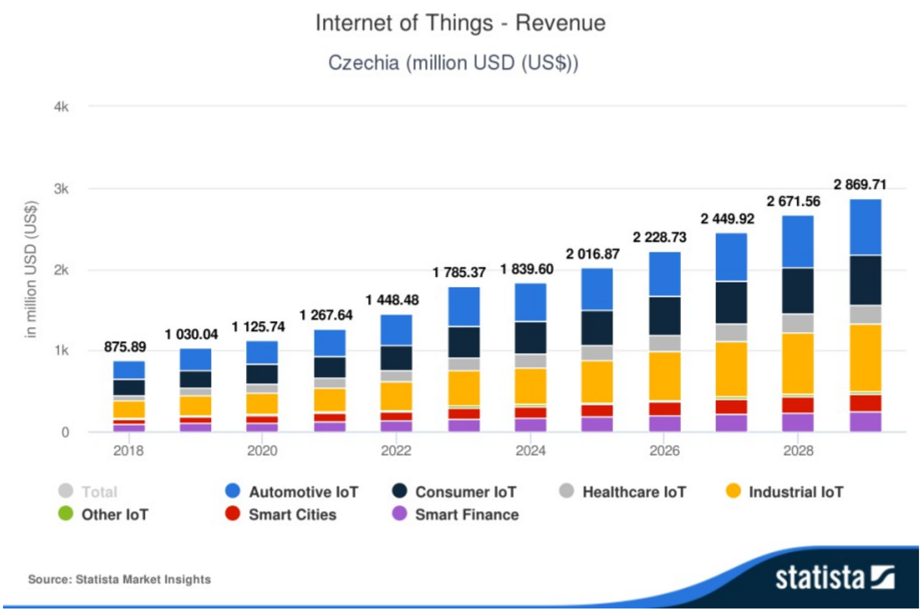

Chart 7: The IoT market in the Czech Republic in terms of revenue by vertical. Source: Statista.

If we look at the IoT market in terms of the number of connections and their structure, the largest total number of devices connected to IoT technologies (in both long-range and short-range IoT) comes from the consumer IoT segment. Next in terms of the number of connections are the industry, smart cities and automotive verticals. In terms of structure, therefore, the IoT market in the Czech Republic is comparable to that of other industrially advanced countries, including Germany.

[26] Statista. "Internet of Things – Czechia | Statista Market Forecast," n.d. https://www.statista.com/outlook/tmo/internet-of-things/czechia.

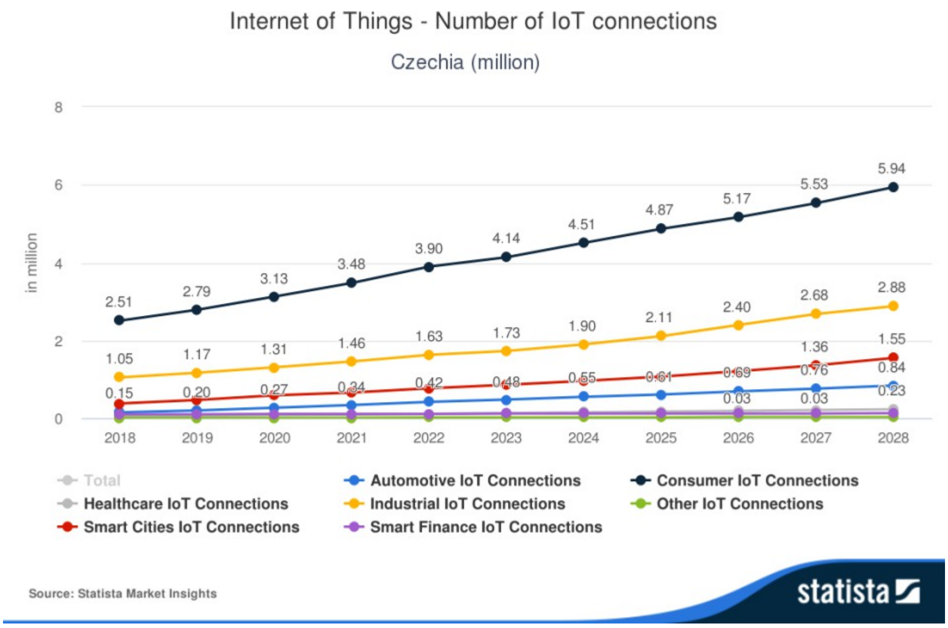

Chart 8: Forecast of the number of IoT connections in the Czech Republic for the period 2018–2028 by sector

Key players in the IoT market in the Czech Republic

The IoT value chain encompasses a wide range of players, each of whom plays a vital role in delivering comprehensive IoT solutions. Manufacturers and suppliers of IoT devices provide the hardware foundation; connectivity providers enable communication; whilst platform providers and analysts offer data management, analytics and interpretation. System integrators ensure that all IoT components form a functional system. Managed service providers can take care of the operation of IoT systems on behalf of customers. Cybersecurity solution providers and regulatory authorities also have a role to play.

Some players fulfil several roles simultaneously; for example, they provide complete IoT solutions encompassing end devices, connectivity and a data processing platform.

When viewed through the lens of the emerging 5G technology, the role of IoT connectivity providers is crucial.

These can be divided into two main groups:

1. Mobile operators: these provide transmission technologies on licensed spectrum.

2. Communications service providers offering IoT transmission technologies on unlicensed bands.

The first group includes mobile operators T-Mobile, O2 and Vodafone. They provide technologies based on 3GPP standards. For IoT, 2G, 4G, 5G, LTE-M and NB-IoT are used. The second group includes providers of long-range technologies such as LoRa and SigFox, as well as short-range technologies such as Wi-Fi. České Radiokomunikace provides a nationwide LoRa network, which also offers international roaming.

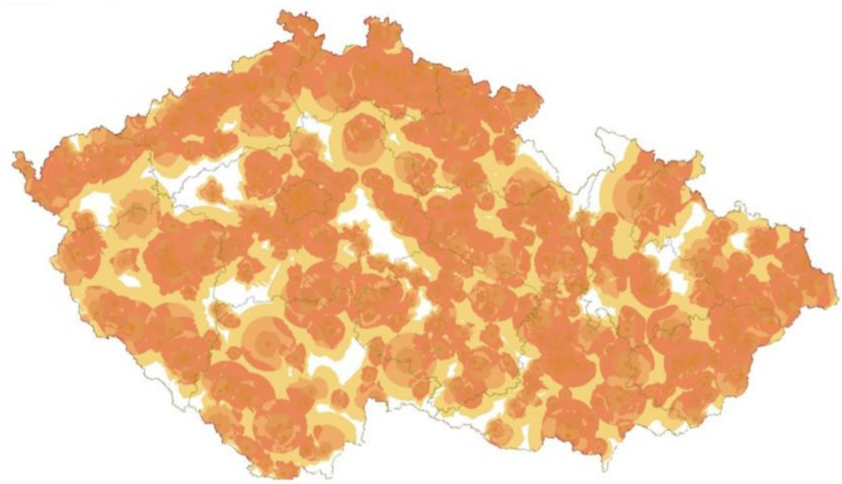

Figure 11: Coverage of České Radiokomunikace's LoRaWAN networks. Source: ČRa.

The SigFox network was operated by SimpleCell under a French franchise. However, this network is no longer operational in the Czech Republic and SimpleCell is in liquidation. In addition, there are a number of local connectivity providers. For IoT projects, they primarily offer LoRa technology. This can be operated relatively easily on the unlicensed 868 MHz band, for example by a local authority for its own needs. Mobile operators in the Czech Republic currently operate both NB-IoT and LTE-M (Cat-M) networks. Whilst the NB-IoT network was launched by Vodafone as early as 2017, the roll-out of Cat-M networks took place later (in the case of O2 and Vodafone, not until 2023). The range of connectivity options is now therefore complete in terms of NB-IoT and Cat-M, and the networks provide virtually nationwide coverage.

5.2 Challenges associated with the IoT

The entire IoT sector is developing rapidly and, according to optimistic forecasts, this trend is not only set to continue but even to accelerate, as shown in the data and charts above.

These optimistic forecasts contrast somewhat with the reality experienced by participants in the IoT ecosystem, as they face many challenges and obstacles which, as a result, mean that the development of IoT projects is slower than planned. Consequently, IoT projects are failing to deliver the expected returns on the one hand, and sufficient value for customers on the other. Let us therefore take a closer look at the main challenges facing the IoT ecosystem.

5.2.1 IoT cybersecurity

With a large number of devices connected to the internet, IoT systems are vulnerable to cyber-attacks. Many IoT devices have weak security protocols, making them easy targets for hackers. Furthermore, IoT devices often process sensitive data, which poses a significant risk to privacy. A single security breach in an IoT network can compromise critical systems, leading to financial losses, data theft and damage to a brand's reputation. It is therefore fair to describe the cyber security of IoT systems as one of the main challenges for both users of IoT systems and their providers.

Cybersecurity challenges in the IoT are multifaceted, ranging from ensuring the security of data transmission using encryption protocols to ensuring that security is a cornerstone of system design. Encryption plays a vital role in protecting the confidentiality and integrity of data, whether through native encryption in protocols such as AES and ECC, or as an additional layer (e.g. TLS/SSL) for unprotected protocols such as MQTT. **The transition to 5G significantly strengthens encryption standards and network security in IoT systems.**

The main security aspects of IoT systems are:

- Security by Design: incorporating cybersecurity – and therefore cybersecurity experts – into the design of IoT solutions from the outset.

- Encryption protocols: Implement encryption for all IoT data transmissions.

- Regular software updates: Ensure that IoT devices can receive firmware and software updates to protect them against emerging vulnerabilities. Ideally, firmware and software should be updated remotely via an over-the-air (OTA) connection. However, not all IoT technologies are suitable for this purpose. This applies in particular to narrowband technologies such as NB-IoT. A further prerequisite for effective firmware and software updates is an advanced IoT device management platform that enables this.

Security as a fundamental element – Security by Design in IoT systems

'Security by Design' refers to an approach in which security considerations and mechanisms are built into the architecture and design of IoT systems from the very outset. Rather than addressing security as an afterthought (where vulnerabilities are patched later), security is integrated throughout the entire lifecycle of an IoT solution, including hardware, software, network protocols and the overall system architecture.

<u>Key elements of Security by Design in IoT:</u>

- Secure hardware components: Hardware security mechanisms, such as secure boot, trusted execution environments (TEEs) or hardware security modules (HSMs), can ensure that devices boot securely and that critical operations (e.g. cryptographic key generation) are isolated from other functions.

- Firmware integrity and updates: IoT devices should have mechanisms to verify the integrity of their firmware during boot-up and support secure over-the-air (OTA) updates. These updates should be authenticated and encrypted to prevent the installation of malicious firmware.

- Secure communication protocols: Select communication protocols that support encryption and authentication natively, or that can be augmented with additional security features, such as TLS for MQTT or DTLS for CoAP.

- Authentication and access control: Every IoT device must have a strong, unique identity. Where relevant, it is advisable to use multi-factor authentication (MFA) to prevent unauthorised access. Role-based Access Control (RBAC) can also restrict the scope of access based on users' roles.

Should the design of IoT systems be carried out with cybersecurity experts?

Definitely yes. Cybersecurity should not be left solely to general system designers or engineers, who may not possess specific expertise in the field of security. This is particularly for the following reasons:

- Specialised knowledge: Cybersecurity experts bring deeper knowledge of threat modelling, encryption standards, vulnerability management and secure system architecture. They can identify attack vectors and potential vulnerabilities at an early stage of the design process that other team members might overlook.

- Compliance with standards and best practices: Cybersecurity experts ensure that the design adheres to best practices and meets the requirements of regulations such as NIS2, GDPR, HIPAA or other local and international standards. They can also guide IoT system designers in implementing the latest secure design recommendations, such as those from NIST (National Institute of Standards and Technology) and ENISA (European Union Agency for Cybersecurity).

- Continuous monitoring: As part of the 'Security by Design' approach, experts help set up continuous monitoring systems capable of detecting and responding to security incidents in real time, thereby ensuring ongoing protection even after deployment.

How to implement Security by Design:

- Threat modelling: It is important to carry out a threat analysis at an early stage of the design process. Map out potential threats to the system and identify critical areas that require stronger security measures.

- Secure Software Development Life Cycle (SDLC): Part of the implementation is the SDLC, which includes security checkpoints at every stage, from design through to coding, testing and deployment. It is essential to ensure that all software is tested for vulnerabilities before release.

- Cross-team collaboration: It is advisable to bring together security specialists, developers, product designers and network engineers at an early stage of the design process. This multidisciplinary collaboration ensures that security issues are addressed across all layers – hardware, software and network infrastructure.

Security by Design ensures that IoT solutions are resilient to attacks from the ground up. This approach requires close collaboration with cybersecurity experts, whose expertise in threat modelling, secure coding and compliance with standards is essential for minimising risks.

Encryption protocols in the IoT

Encryption protocols are algorithms and techniques used to encode data so that only authorised parties can read or access it. In the IoT, encryption is essential for protecting data transmitted between devices, gateways and back-end systems.

<u>Commonly used encryption protocols in the IoT:</u>

- TLS/SSL (Transport Layer Security / Secure Sockets Layer): Used to secure data transmission over the internet. It provides end-to-end encryption between IoT devices and servers, protecting against eavesdropping, tampering and message forgery. TLS is widely used in IoT devices, particularly those connected to cloud services.

- DTLS (Datagram Transport Layer Security): A variant of TLS designed for datagram protocols such as UDP. DTLS is better suited to IoT use cases where devices rely on low-latency, connectionless communication, which is particularly effective in resource-constrained environments.

- AES (Advanced Encryption Standard): AES is a symmetric encryption algorithm commonly used in IoT devices for on-device encryption (e.g. storing data on the device). It is lightweight and efficient, making it ideal for devices with limited processing power.

- ECC (Elliptic Curve Cryptography): ECC is an asymmetric encryption technique that provides strong security with shorter key lengths compared to traditional methods such as RSA. This is important for IoT devices with limited computational capabilities, as it allows them to maintain strong encryption without excessive resource consumption.

- MQTT with TLS: MQTT, a popular communication protocol in the IoT, is often combined with TLS to ensure secure data transmission between devices and brokers. MQTT is lightweight but does not have native encryption of its own, which is why TLS is usually used as an additional layer to secure communications. Encryption is therefore not always a native part of IoT communications. It depends on the technology and how it is used.

<u>Native encryption in protocols:</u>

Some IoT protocols (such as MQTT or CoAP) do not include encryption natively, but rely on an additional layer, such as TLS/SSL, for security. Other protocols, such as Zigbee, LoRaWAN and Z-Wave, have built-in encryption mechanisms, mostly based on AES, which ensure confidentiality during communication between devices or between devices and the network.

<u>5G and encryption for the IoT:</u>

In 5G networks, encryption is an integral part of the network architecture. 5G utilises 128-bit and 256-bit encryption to secure communications, which is significantly stronger than the encryption methods used in 4G. Furthermore, 5G introduces network slicing, which allows different IoT applications to have isolated virtual networks, ensuring that even if one slice is compromised, the others remain secure. The 5G standard also supports IPsec and end-to-end encryption, thereby enhancing the security of IoT applications that rely on mobile networks.

<u>Recommendations for encryption in IoT:</u>

- Use end-to-end encryption (E2EE): Ensure that data is encrypted from the IoT device right through to the backend server. This helps prevent man-in-the-middle (MitM) attacks or eavesdropping that could occur if data were exposed to potential misuse during transmission.

- Lightweight encryption algorithms: Given the limited resources of many IoT devices (e.g. limited battery life, memory and processing power), it is essential to use lightweight yet strong encryption algorithms, such as ECC and AES with shorter key lengths.

5.2.2 Interoperability and fragmentation in the IoT ecosystem

The IoT ecosystem comprises a wide range of devices, platforms and communication protocols, many of which are not compatible with one another. The lack of standardisation leads to fragmentation, making communication between devices from different manufacturers difficult. This hinders scalability, increases integration costs and limits the ability to develop truly interoperable solutions.

Interoperability refers to the ability of different systems, devices and platforms to communicate and work together seamlessly. In an ideal IoT environment, devices from different manufacturers should be able to exchange data, interpret commands and function as part of a unified ecosystem. However, in the current situation, this often does not work.

Fragmentation refers to the proliferation of different technologies, standards and protocols that are not mutually compatible. This diversity can occur at various layers of the IoT, including hardware (different devices), connectivity (different communication protocols) and software (different platforms or data formats). Fragmentation can create 'silos' of data and functionality, where devices or systems are unable to exchange information or collaborate effectively.

Key challenges include:

- Lack of standardisation: IoT devices utilise a range of protocols, such as MQTT, CoAP, Zigbee and LoRa. Furthermore, IoT device suppliers have historically often opted to implement proprietary protocols, between which there is frequently no compatibility. This leads to difficulties in integrating devices from different suppliers.

- Vendor lock-in: Many IoT providers create proprietary systems that limit cross-compatibility. This results in isolated systems where businesses are tied to a specific vendor's ecosystem, reducing flexibility and increasing long-term costs.

- Data inconsistency: Without common data formats and standards, different IoT systems may not interpret or use data in a consistent manner. This can lead to misunderstandings between devices or platforms, reducing the accuracy and efficiency of IoT-controlled operations.

- Increased complexity: The more fragmented the ecosystem, the more difficult it is for companies to integrate, manage and scale their IoT solutions. This increases the total cost of ownership (TCO) and reduces the return on investment (ROI) from IoT projects.

To mitigate the problems associated with interoperability and fragmentation, the following steps can be recommended:

- Require open standards and interoperability: Companies implementing IoT solutions should prioritise suppliers that adhere to open standards and avoid dependence on proprietary ecosystems. This will ensure greater flexibility and protect their future investments in IoT.
- Invest in middleware solutions: In situations where different systems need to coexist, middleware can help bridge the gaps between different devices and protocols. Investing in middleware platforms that support multi-protocol interoperability can simplify operations and reduce the complexity of integration.
  Note: An example of a platform that enables the integration of different protocols and devices is ČRa's Multi-tech Cloud IoT platform, which is presented in Appendix 2.
- Collaborate with industry stakeholders: IoT customers should collaborate with industry groups and forums that promote greater standardisation and interoperability. Active involvement in these communities will give companies a voice in shaping future standards and ensure that their requirements are taken into account.
- Pilot operations in a multi-vendor environment: To avoid dependence on a single supplier, companies should test IoT solutions in a multi-vendor environment before proceeding to a larger-scale deployment. This will help to identify any interoperability issues at an early stage and ensure smoother scaling of IoT solutions.

5.2.3 Selection and implementation of IoT communication technology

The complexity and a certain degree of fragmentation of the IoT also give rise to a further challenge faced not only by potential users of IoT systems but, somewhat paradoxically, also by IoT solution providers. This is because both groups face a difficult task when it comes to choosing a transmission technology.

The choice of transmission technology will influence the characteristics of the entire IoT system. Furthermore, it determines the type and availability of IoT end devices. An unsuitable choice can pose a significant problem, as changing the communication technology may require the replacement of end devices, of which there may be hundreds or even thousands within an IoT system. This is costly and can also be a very time-consuming process. Typically, changing the communication technology can be a greater challenge than replacing a central component, such as a data storage system or analytical tools.

There is a relatively large number of transmission technologies, as Chapter 2.2 demonstrates. Objectively speaking, they have various advantages and disadvantages; it is not possible to define one technology as unequivocally better or worse than another. Furthermore, the choice is complicated by the fact that technology suppliers often provide data that is not entirely objective regarding the technologies' characteristics, available coverage, and so on.

The following steps can therefore be recommended for making a selection:

- Familiarise yourself with the full range of technologies and their characteristics. This study may also be helpful in this regard.
- Carefully define the use cases that the IoT system will implement. This will then enable you to define the requirements of these use cases for the IoT system. This is described in detail in section 3.1.2.
- For each use case, it is advisable to define a complete set of requirements for the IoT system using the provided form. These requirements should then be compared with the characteristics of the technologies described in Chapter 2.
- Verify the characteristics and suitability of the technology using a Proof of Concept (PoC). As part of the PoC, it may be advisable to test and compare multiple technologies.
- Transparency from the provider regarding long-term support for the selected technology should be required. IoT projects are typically implemented with a time horizon of 10–15 years.

In addition to the technical characteristics of the transmission technology, the commercial and cost aspects of the chosen technology are, of course, also important for users of IoT systems.

The costs associated with using the relevant technology are not determined by the technology itself alone. The volume of data traffic transmitted within the IoT system plays a major role. In the case of IoT, charges are levied precisely on the basis of the volume of data transmitted. **Optimising communication within the IoT system** therefore plays a major role**.** The use of edge computing and a suitable architecture can lead to orders of magnitude differences in the volume of data transmitted, and consequently to dramatically different costs. Without such optimisation, the operating costs of an IoT system can reach a point where the entire solution no longer makes economic sense, or where the business model is unviable.

5.3 The Future of IoT

The Internet of Things (IoT) landscape is evolving rapidly, with future growth driven by numerous technological innovations. Key trends include the development of new communication technologies based on 5G standards, the integration of artificial intelligence (AI) and machine learning (ML), and the growing role of advanced cloud services. These elements are transforming the way in which businesses can utilise the IoT to achieve greater efficiency and develop new business models.

Below, we outline the key areas and other emerging trends that will define the future of the IoT.

5.3.1 New communication technologies (RedCap, Passive IoT)

Although a relatively wide range of communication technologies for the IoT is already available, this field is undergoing constant development aimed at eliminating the weaknesses of existing technologies and delivering solutions that meet all the requirements of IoT system users.

One area of development is the need to provide a technology that:

- is fully compatible with the 5G ecosystem,
- ensures a high level of security,
- provides sufficiently fast data transfer speeds,
- is therefore suitable for business-critical applications and use cases,
- all at a cost that will not hinder the implementation of IoT projects.

This development path is driven by **RedCap** technology and its evolution.

RedCap is a 5G feature that offers a compromise between high-performance 5G devices and low-cost IoT devices. It supports data speeds and features optimised for IoT applications, such as smart wearables, industrial sensors and other uses that do not require the full 5G bandwidth. RedCap offers reduced device complexity and lower power consumption, making it a cost-effective option for large-scale IoT deployment, whilst still benefiting from the low latency and reliability of 5G networks.

RedCap technology is currently (as at the date of publication of this study) already available on a limited scale. Some Asian suppliers are already offering the option to implement RedCap within private 5G networks. There is only a limited ecosystem of devices. However, it is expected that the scope of the RedCap ecosystem will expand steadily in the coming months and years.

Another area of development involves the need for even lower costs and even lower energy consumption, particularly on the part of end devices, which would enable a much more widespread deployment of IoT and, as a result, the digitalisation of areas for which it is still too costly. This direction of development is represented by **Passive IoT**.

Passive IoT devices, such as passive tags and battery-free sensors, can operate without traditional power sources, instead harnessing energy from their surroundings (e.g. electromagnetic waves, light or heat). This technology significantly reduces deployment and maintenance costs, enabling the interconnection of large numbers of small, low-cost devices in sectors such as logistics, manufacturing, retail, healthcare and agriculture. Passive IoT has the potential to be revolutionary in applications where size, energy consumption and cost are critical factors.

Passive IoT, as described in Chapter 2.3, will be rolled out in several phases. At present, this technology is not available in Europe; the first experimental implementations are underway in China.

However, European research organisations and manufacturers do not wish to be left behind either. For example, the German Fraunhofer IIS is working on its own concept of Passive IoT, which it calls Ambient IoT. The essence of the technology is the same; it utilises the technique of backscattering. However, it seeks to accommodate the European regulatory environment and utilise existing signal sources for backscattering, rather than an actively generated signal. The solution is still at a relatively early stage of research; the device currently runs on a small battery, with the aim of achieving a fully passive device.

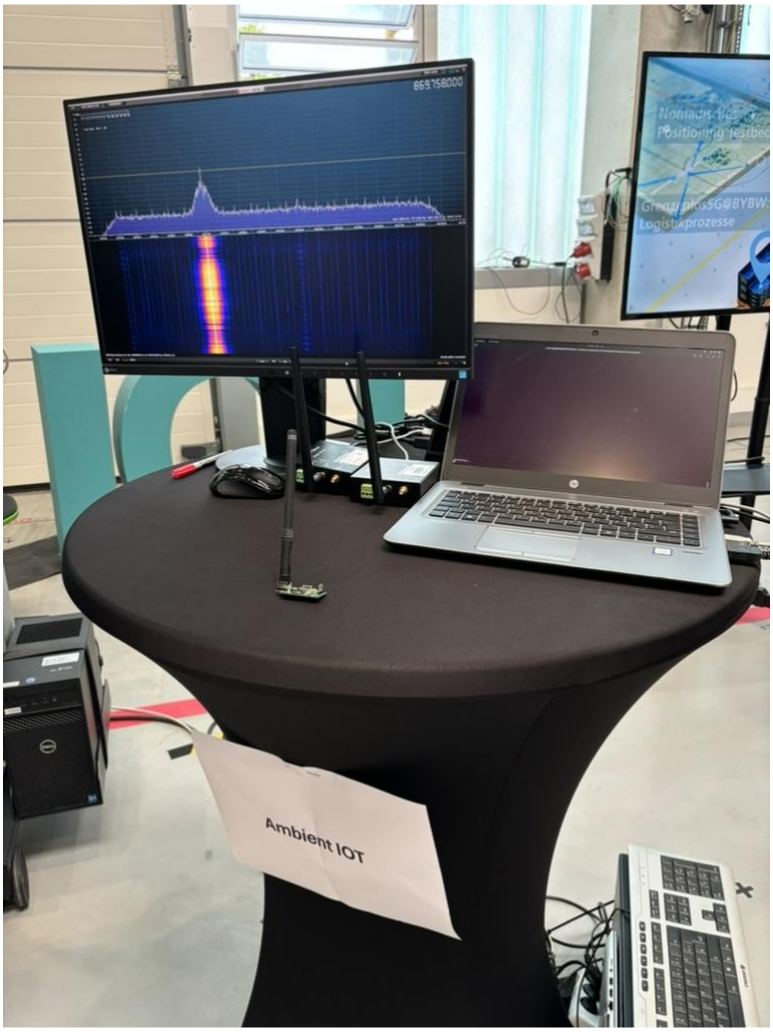

Figure 12: Experimental device for Ambient IoT utilising 'back scattering'. Source: Fraunhofer IIS, 5G Connect Advanced (19 September 2024).

5.3.2 AI/ML for advanced data analysis

The integration of artificial intelligence (AI) and machine learning (ML) is transforming the IoT landscape through the possibility of advanced data analysis. This can be utilised, for example, for predictive maintenance, anomaly detection and automation in general. AI and ML algorithms process the vast amounts of data generated by IoT devices, thereby converting raw data into actionable insights that deliver real value to businesses.

Although AI/ML models are an extremely complex matter, an increasing number of products are becoming available to both providers and users of IoT services, enabling the practical application of AI/ML tools within IoT systems without the need for specialist know-how. This will undoubtedly lead to the rapid adoption of these tools. Their use will bring significant added value in areas such as the following:

- Predictive maintenance: AI models can predict equipment failures before they actually occur, thereby reducing downtime and maintenance costs. This is particularly valuable in sectors such as manufacturing, energy and transport, where unplanned outages can be very costly.

- Anomaly detection and quality control: ML algorithms can detect patterns and deviations in real time, enabling immediate corrective action on production lines or within supply chains. This results in better quality control and reduced waste, which directly impacts operational efficiency.

- Automation and decision-making: AI-driven automation enables IoT systems to make autonomous decisions, ranging from optimising energy consumption in smart buildings to adjusting production parameters in real time in manufacturing plants. This reduces the need for human intervention and significantly improves process efficiency.

5.3.3 Cloud services (AWS IoT, Azure IoT, Google Cloud IoT)

Cloud platforms are playing an increasingly important role in IoT by providing a robust and scalable infrastructure that simplifies the deployment and management of IoT solutions. Services offered by platforms such as AWS IoT, Microsoft Azure IoT and Google Cloud IoT provide powerful tools that enable the development, connection and management of IoT devices with minimal effort.

Cloud platforms enable businesses to scale their IoT systems flexibly without the need for significant upfront capital expenditure (CAPEX). They offer flexible, usage-based pricing models, making IoT accessible to businesses of all sizes.

Note: Some investment is, of course, required in hardware in the form of end devices.

Modern cloud-based IoT platforms offer advanced features such as real-time data analysis, device management and security monitoring via user-friendly interfaces. This democratises access to sophisticated IoT capabilities, enabling businesses to deploy comprehensive IoT solutions with just a few clicks.

Advanced cloud-based IoT platforms no longer need to function solely as centralised hubs; they now support edge computing, which brings data processing closer to the source where it is generated. This reduces latency and bandwidth costs whilst enhancing data protection, making IoT applications more responsive and efficient.

A more detailed description of the AWS suite of cloud IoT products is provided in Appendix 1 as an example of this type of service.

5.3.4 Enhanced security and privacy

As IoT networks expand, ensuring robust security and privacy is becoming increasingly important. Cyber threats are evolving in parallel with IoT technology, requiring advanced approaches to safeguarding the integrity, confidentiality and availability of data.

In addition to the approaches already mentioned above (see the chapter on ‘Challenges Associated with IoT’), such as ‘Security by Design’ and an emphasis on the end-to-end use of encryption protocols, the cybersecurity of IoT systems can be further strengthened in the future through the use of advanced technologies such as blockchain and the modern ‘Zero Trust’ approach.

- Using blockchain for IoT security: Blockchain technology is being explored for its potential to enhance IoT security by providing decentralised, immutable records of IoT transactions and device interactions. This technology can reduce the risks associated with data breaches and unauthorised access.

- Zero Trust security models: The adoption of Zero Trust architectures, which require continuous verification of devices and data flows, can significantly improve the security posture of IoT ecosystems. This approach assumes that threats can originate from both inside and outside the network, and emphasises rigorous authentication and authorisation processes.

5.3.5 Improvements in IoT interoperability and standardisation

The lack of interoperability between different IoT devices and platforms continues to pose a significant barrier to wider adoption. Consequently, interoperability and the fragmentation of the IoT ecosystem are listed among the key challenges for IoT

The future of IoT is likely to bring, in addition to the use of various middleware platforms, greater efforts towards standardisation and the development of universal protocols that will enable seamless integration across different

IoT ecosystems.

In industrial settings, several protocols that are important for IoT and advanced automation and robotics will play a key role. These include, in particular**, MQTT, OPC UA, Industrial Ethernet and TSN**.

In the case of consumer IoT, the **Matter** project is a good example of efforts towards interoperability.

Matter is an open-source standard for the connectivity of smart home devices, developed by the Connectivity Standards Alliance (CSA), formerly known as the Zigbee Alliance. Matter aims to improve interoperability between IoT devices by enabling them to communicate regardless of manufacturer, platform or communication protocol. Matter seeks to simplify the smart home ecosystem by ensuring that devices from different brands can work together reliably and securely.

Matter introduces a common language for IoT devices, enabling them to work together across ecosystems such as Apple HomeKit, Google Home, Amazon Alexa and Samsung SmartThings. It achieves this by defining a universal application layer for smart home devices. Matter incorporates robust security protocols, including device authentication and encryption, which ensure data integrity and protect user privacy.

Matter also simplifies device setup and operation, making it easier for users to add devices to their smart home networks. Devices can be easily set up using QR codes or NFC tags, which simplifies the onboarding process. The protocol is designed to work across various communication technologies, including Wi-Fi, Thread and Ethernet, providing flexibility in how smart home devices communicate. It is based on open-source principles, enabling developers and manufacturers to contribute to the standard's development and to foster innovation and widespread adoption.

Matter devices communicate via a shared protocol, enabling them to discover one another, interact and work together. For example, a Matter-certified smart bulb can work with a Matter-compatible smart home app, regardless of whether the bulb is from Philips and the app is from Apple, Google or Amazon. This cross-brand compatibility represents a significant change from the past, when smart home devices often required specific hubs or apps associated with a particular brand.

An example of Matter in use: Smart HVAC systems.

Matter-compatible thermostats, temperature sensors and smart fans are used to control a home's heating and cooling. These devices can coordinate their actions automatically. For example, when a thermostat detects a change in temperature, it can signal the fans to adjust the airflow, even if these devices are from different manufacturers.

Crucially, Matter has received significant support from major technology companies, including Apple, Google, Amazon and Samsung, as well as from device manufacturers such as Philips, Yale and IKEA. These companies are actively working to certify both their existing and future products with Matter, which is accelerating the standard's adoption.

Matter addresses one of the biggest challenges in the smart home sector: fragmentation. By offering a universal standard, Matter significantly reduces complexity for both consumers and developers, making smart home devices more accessible and reliable. As its adoption grows, Matter is expected to become the de facto standard for connectivity in smart homes, simplifying the way we interact with IoT devices and reap their benefits in our everyday lives.

Matter thus represents a significant step forward in the IoT ecosystem, improving device interoperability, security and the user experience. It opens up new opportunities for businesses and consumers and makes smart home technology more cohesive and practical than ever before.

The future of the IoT is being shaped by technological innovations, particularly in the fields of communications technology, AI/ML and cloud services. Alongside improvements in security and interoperability, these innovations are driving the development of smarter, more cost-effective and more scalable IoT solutions that can help transform industries and unlock new business models. This will enable businesses and service providers to fully realise the potential of the IoT.

Appendix 1 – AWS IoT: a suite of cloud products for the IoT sector

Basic information about the service provider – Amazon Web Services

Amazon Web Services (AWS), a division of Amazon, is a global leader in the provision of cloud solutions. AWS offers a broad portfolio of services, including computing power, storage, databases and analytics tools, as well as comprehensive services for the Internet of Things (IoT). Thanks to its flexibility, global infrastructure and security standards, AWS enables businesses to rapidly digitise their processes and utilise state-of-the-art IoT technologies.

Customers and their needs

Customers of AWS IoT services are businesses from various sectors, such as manufacturing, energy, agriculture, healthcare and logistics. These customers are looking for solutions that will enable them to manage their processes more efficiently through automation, monitoring and real-time data analysis. They require a robust and secure environment for connecting, managing and analysing data from a large number of IoT devices, often on a global scale.

Product description (AWS IoT)

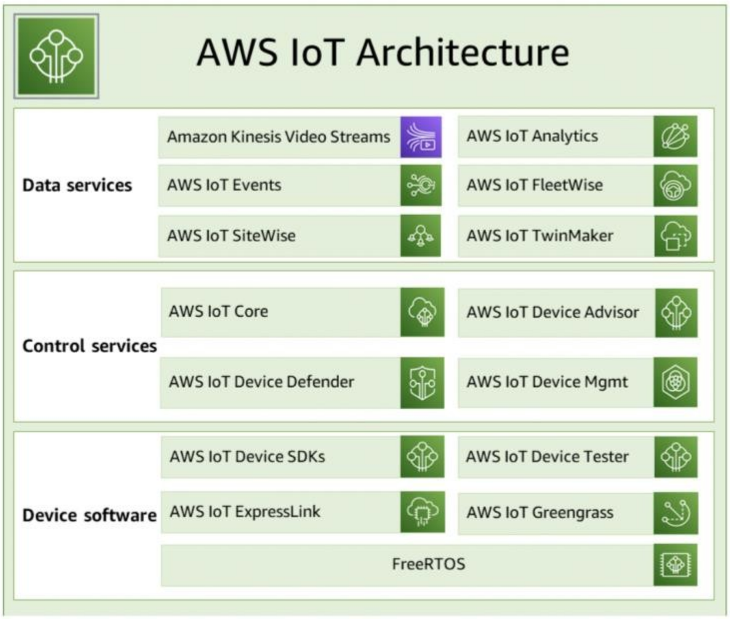

Figure 13: Overview of the AWS IoT architecture. Source: [27]

AWS IoT comprises several key products which together form a comprehensive platform for IoT solutions. The products can be divided into three areas (see figure above):

- Data services – for processing, storing and analysing data.
- Control services – for device management and security.
- Device software – for connecting and ensuring the interoperability of IoT devices.

[27]https://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html

The main products and their detailed descriptions are listed below:

1. AWS IoT Core

AWS IoT Core is a core service that enables IoT devices to connect to the AWS cloud and communicate with one another. IoT Core supports communication protocols such as MQTT, HTTPS and LoRaWAN. Its advantages include secure device connections using X.509 certificates and regular updates to security standards.

IoT Core enables easy integration with other AWS services, such as Amazon DynamoDB, AWS Lambda and Amazon S3, meaning that data from devices can be analysed or stored without the need for manual intervention.

2. AWS IoT Greengrass

AWS IoT Greengrass brings computing power closer to the devices – that is, at the 'edge'. This means that IoT devices can process data locally and respond in real time without having to constantly communicate with the cloud. This model reduces latency and data transfer costs and is ideal for applications where a rapid response is crucial, such as in industrial automation or healthcare. Greengrass also supports offline operation and automatic data synchronisation once the connection is restored.

3. AWS IoT Device Management

This service simplifies the management, monitoring, updating and diagnostics of large numbers of devices. With AWS IoT Device Management, organisations can easily organise devices into groups, monitor their health, manage software updates and set security policies for individual devices or groups of devices.

This enables the efficient management of an entire fleet of IoT devices, which is essential for large organisations deploying thousands of devices across multiple locations.

4. AWS IoT Device Defender

AWS IoT Device Defender is a security service that continuously monitors IoT devices and ensures their secure operation. It checks whether device configurations meet security standards and alerts organisations to potential threats, such as unauthorised use of certificates or suspicious device activity.

The advantage of this service is that organisations can respond quickly to security issues and protect their data and devices from cyber-attacks.

5. AWS IoT Analytics

AWS IoT Analytics enables easy analysis of data from IoT devices. It automates steps such as filtering, transforming and enriching data to prepare it for analysis. Analytical data is stored in time series, enabling advanced analysis and predictions. Both standard SQL queries and machine learning tools can be used for analysis.

This enables businesses to better understand their operations, identify trends and anomalies, and optimise processes.

6. AWS IoT Events

AWS IoT Events monitors data from sensors and automatically detects predefined events or anomalies. Examples include the detection of movement or changes in temperature, which trigger further actions such as activating an alarm or starting a machine. This service is crucial for applications that require an immediate response to real-time changes.

7. AWS IoT SiteWise

AWS IoT SiteWise is a service designed for industrial companies, which facilitates the collection, structuring and analysis of data from industrial equipment and sensors. Using SiteWise, businesses can easily monitor and analyse operational data from various devices, enabling them to optimise production and reduce downtime.

Why choose an AWS IoT solution?

AWS IoT offers several key advantages over other options:

- Scalability and global availability: AWS has one of the most extensive global networks of data centres, meaning customers can easily scale their IoT solutions and ensure their availability worldwide.

- Security: AWS is renowned for its high security standards. AWS IoT solutions offer integrated security at both the device and cloud levels, including end-to-end encryption and secure device authentication using certificates.

- Integration with other AWS services: One of the greatest advantages of AWS is its deep integration with other cloud services, such as machine learning, data analytics and database systems. This allows IoT solutions to be easily extended with advanced analytical and predictive capabilities.

- Flexibility and support for various protocols: AWS IoT supports various communication protocols, including MQTT, HTTPS, LoRaWAN and others, enabling businesses to easily integrate different devices into a single IoT ecosystem.

A key advantage is the ability to analyse data using advanced machine learning. IoT Analytics enables data to be prepared so that it can be easily analysed using the AWS SageMaker tool.

Amazon SageMaker is a cloud platform for developing, training and deploying machine learning (ML) models. In IoT projects, SageMaker can be used to analyse large volumes of unstructured data generated by IoT devices. SageMaker enables businesses to:

- Create predictive models: Based on historical data, SageMaker can identify patterns, anomalies or trends that help predict future events (such as predictive machine maintenance).

- Process and analyse data in real time: When combined with Amazon Kinesis, SageMaker can analyse IoT data in real time, which is crucial for applications such as monitoring the health of devices or predicting breakdowns.

- Machine learning automation: SageMaker supports the deployment of ML models directly to edge devices (e.g. using AWS IoT Greengrass), enabling rapid data processing without the need to send it to the cloud.

Compatibility of 5G devices with AWS IoT

AWS IoT supports the connection of 5G devices and enables the use of advanced communication protocols for efficient data management and transmission. The core protocols that 5G devices should use for seamless integration with AWS IoT include:

- MQTT (Message Queuing Telemetry Transport): This lightweight protocol is ideal for IoT devices with limited resources and for data transmission over 5G networks, providing low latency and reliable communication.

- HTTPS: This is used for data transfers between IoT devices and AWS IoT services with a high level of security.

- TLS (Transport Layer Security): TLS version 1.3 is used to secure communication between 5G devices and AWS IoT.

AWS IoT, combined with 5G networks and powerful analytics tools such as SageMaker, enables companies to create robust IoT solutions with high reliability, fast response times and secure data management.

Appendix 2 – České Radiokomunikace's Multi-tech Cloud

MTC is at the heart of ČRa's IoT services. Every customer using both LoRaWAN and ČRa's SIM services gains access to a platform where they can manage their services and thus control all their IoT technologies and IoT devices from a single location. Thanks to MTC's advanced features, all data traffic from all IoT devices can be aggregated in MTC and delivered to the user in a standardised format to the customer's production server. MTC is not a standalone service, but a standard component of any CRA IoT communication service – Connection to the LoRa IoT network, Connection via MQTT, Connection via UDP, Connection via Data SIM. This premium add-on, which forms a standard part of IoT services, provides customers with a new level of added value: in addition to transferring data from IoT devices, it performs advanced data processing to ensure that data from all technologies is delivered in the same format and to the same customer server.

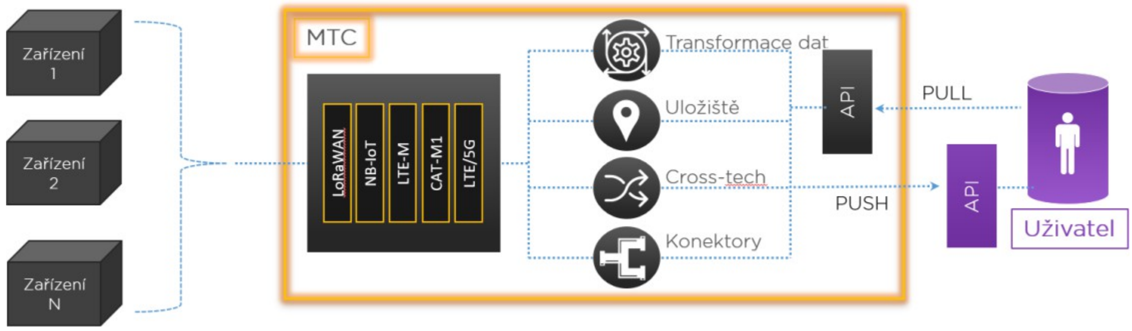

Figure 14: Diagram of the MTC integration platform. Source: ČRa.

How it works

This is a platform whose primary purpose is the routing and transformation of data from IoT devices, device management, user management, data storage and service management. It naturally processes data from LoRaWAN devices using the CRA IoT network, from devices connected to the internet via a local network, or from SIM cards in devices using NB-IoT, LTE-M, CAT-M1 and LTE/5G technologies. It supports the most widely used communication protocols: LoRaWAN, MQTT, HTTP and UDP.

Benefits

- Significantly reduces the need for data transformation on the customer's side
- One place to manage your IoT, one SLA, one supplier
- Extends SIM communication to include data routing on the platform side
- Option for customised data transformations according to your own requirements
- Option to forward data from SIM to LoRa devices and vice versa
- Connectors for integration with the most widely used data tools
- Open, documented API
- Data storage

Who is the customer

- IoT solution providers
- ICT integrators
- IoT operators
- Anyone who combines LoRaWAN with other technologies

MTC solution features

- Data routing – As with LoRaWAN, data from NB-IoT devices can be routed to MTC, where it is processed and delivered to a single customer REST API
- Data transformation – data from all technologies is transformed into the same format
- Data storage – Data is stored in MTC's internal database
- Cross Tech – Messages from LoRaWAN can be delivered to NB-IoT, CAT-M1 and LTE-M devices, and vice versa
- Connectors – connectors to more than 250 renowned platforms such as AWS, Azure, Microsoft, Google, Oracle, Snowflake, MySQL, Databricks, etc.
- Device management – management of IoT devices, configuration records, descriptions
- User management – creation of projects, users, hierarchies and permissions
- Service management – reordering SIM cards, tariff management,

Appendix 3 – The Conexa platform for international IoT coverage

Wireless Logic is a leader in providing connectivity for the Internet of Things (IoT). It bridges the physical and digital worlds with seamless, secure and scalable solutions for businesses across all sectors.

The global deployment of IoT solutions presents significant challenges for device manufacturers, solution providers and the companies that want and need to use IoT solutions. The complexity of operations across diverse commercial, technological and regulatory environments requires robust solutions capable of overcoming these challenges seamlessly. Conexa, a comprehensive solution from Wireless Logic, meets these requirements by utilising advanced SIM technologies—eSIM, iSIM and multi-IMSI—to optimise global IoT connectivity, reduce operational costs and increase overall efficiency.

Challenges in global IoT deployment:

The international deployment of IoT devices requires a thorough understanding of the complex landscape of mobile network operators (MNOs), each of which has its own commercial interests, regulatory constraints and varying levels of service quality. Traditional roaming SIM cards, whilst commonly used for global connectivity, present limitations such as limited control over network selection, higher latency and potential restrictions due to local regulations. Furthermore, concerns regarding data sovereignty and security further complicate the landscape, as different countries impose varying requirements on data storage and transmission.

The Conexa platform will help address the challenge of managing global IoT deployment:

Conexa is a scalable, enterprise-grade platform that integrates the strengths of multi-IMSI and eSIM/iSIM technologies to provide a comprehensive service for its users. It supports the entire lifecycle of IoT devices—from initial factory testing through to deployment, ongoing management and eventual redeployment. Conexa ensures that devices remain compliant with local regulations, achieve optimal connectivity and minimise operational costs, making it the ideal solution for cross-border IoT deployments.

eSIM and iSIM technologies:

Conexa utilises eSIM (embedded SIM) and iSIM (integrated SIM) technologies, which enable remote SIM provisioning (RSP). These technologies allow for over-the-air (OTA) management of SIM profiles, enabling seamless switching between networks without the need for physical SIM card replacement. eSIM and iSIM enhance the flexibility and scalability of IoT deployments by allowing devices to be reconfigured remotely, thereby ensuring uninterrupted connectivity and compliance with local regulations.

Multi-IMSI SIM functionality:

The multi-IMSI SIM functionality within Conexa allows a single SIM card to store multiple International Mobile Subscriber Identities (IMSI), enabling devices to switch between different networks as required. This ensures optimal coverage, redundancy and compliance with local regulations that may restrict permanent roaming. The SIM-based profile management applet autonomously selects the appropriate IMSI based on predefined rules, thereby optimising connectivity across different regions without the need for manual intervention.

Benefits of the Conexa platform and SIM cards:

By utilising multiple pre-installed IMSIs, Conexa SIM cards ensure maximum network coverage and redundancy, thereby enhancing reliability across different geographical regions.

Regulatory compliance: Conexa enables seamless switching to local networks, thereby ensuring compliance with data sovereignty laws and other regulatory requirements in various countries.

Cost optimisation: With the ability to update profiles over-the-air, Conexa enables dynamic selection of the most cost-effective network, thereby reducing overall operating costs.

Flexibility and scalability: Conexa supports various formats (SIM cards, eSIMs, iSIMs) and can be tailored to specific business needs and regulatory environments, making it a future-proof solution for global IoT operations.

Conexa from Wireless Logic offers a robust solution for global IoT deployment. By integrating state-of-the-art SIM technologies with a comprehensive management platform, Conexa facilitates seamless international connectivity, optimises network utilisation and ensures compliance with local regulations. This solution enables businesses to overcome the traditional challenges of international IoT connectivity and ensures efficient, reliable and cost-effective operations worldwide.

Appendix 4 – Case Study: Virtual IoT Sensors from InovecTech

Key information about the solution provider

InovecTech is a global pioneer in virtual IoT sensor technology for manufacturing, an approach that utilises artificial intelligence to flexibly collect data from production facilities, warehouses and transport. Edge devices equipped with cameras can be deployed rapidly and begin collecting visual data immediately. Artificial intelligence, with human oversight, distributed across multiple layers between the edge and the cloud, analyses this data into easily interpretable and verifiable signals that can power real-time digital twins and be used to optimise processes and decision-making.

Customers, users and their needs

Manufacturing is a process of constantly battling variability. A seemingly small competitive advantage gained from optimising conversion costs through process improvements can mean the difference between success and failure. Improving manufacturing requires appropriate, easily interpretable and accessible data, which we achieve through the digitalisation of manufacturing. Conventional methods for digitising production are very slow, costly and inefficient. The use of physical (or hardware) sensors requires lengthy planning, testing and the involvement of experts in data interpretation, which restricts and slows down implementation, thereby making digitisation unfeasible for small businesses, for whom flexibility is key. For the successful introduction of digitalisation, it is essential that it is implemented quickly, without the need for high initial investment, and with a rapid return on investment that does not disrupt the company's cash flow. Virtual sensors enable production to be digitised much more quickly and adapt better to the needs of the business. InOEE, an MES based on virtual sensors, enables the collection and evaluation of data from production equipment, leading to greater efficiency through faster troubleshooting, improved statistical analysis and increased transparency of production processes.

Case study:

The company derives most of its business from being a Tier 2 automotive supplier. It has six main large production assets – presses with a tonnage of less than a hundred tonnes. Each press had its own control system, but none had a system in place to collect relevant data into a central repository, which made it difficult to begin analysing the data quickly and improving production efficiency. The OEE of one of the machines was as low as 40 per cent, and without accessible data, it was not possible to increase this figure.

Product/solution and its implementation

The InOEE product, an AI-based MES for SMEs that can be installed in a single day, operates on the principle of data collection via cameras positioned in production halls, which record the production equipment. These recordings are then processed using on-premises computing capacity. Virtual sensor technology transforms image data into signals that correspond to the outputs of hardware sensors; for example, a signal indicating whether a press is open or closed. This data is then processed into useful information for people, such as cycle times, machine utilisation and a breakdown of losses, enabling a detailed analysis of production equipment efficiency. Monitoring and training of the artificial intelligence take place in the cloud; the AI gradually improves and learns from the data, thereby increasing accuracy and reliability and expanding the applicability of both traditional and advanced analyses. The results are presented to the customer via clear web dashboards or online spreadsheets, tailored to their needs. For example, Pareto analysis or an OEE waterfall chart with a breakdown of losses, an overview of the number of units produced and OEE for the last few shifts, etc. The system is designed to communicate with the cloud, whilst the data remains with the customer, apart from individual images from videos that are required for training neural networks. An important part of the solution is artificial intelligence with human intervention, where an annotator connected to the cloud classifies situations in which the AI has incorrectly assessed a condition. This ensures continuous improvement of the system and its rapid deployment, as there is no need to collect weeks of camera footage – just a few hours will suffice. This reliability monitoring enables rapid, virtually immediate deployment, whilst also ensuring high reliability and low costs. In addition to the CCTV footage itself, it is useful to have input from an operator who, for example, using a tablet installed on the production floor, can classify the reasons for production equipment stoppages.

On the first day or two, we installed the hardware, cameras and computing capacity, and laid the Ethernet cabling. On the third day, the first data collection began, which served as the basis for calibrating the system and identifying key points in the production process. During the first and second months, we fine-tuned the data collection, customised the user interface and defined the specific types of data to be collected and analysed, such as detailed OEE measurements recorded at one-minute intervals. This phase was followed by live operation, which commenced in the third month, by which time the system was fully ready for standard production and analysis. This was the first implementation of its kind, so it was necessary to carefully fine-tune all parameters. For future implementations, we expect live operation to commence as early as the fifth day, particularly for standard types of analysis, where we are able to quickly transition to a fully functional system.

5G/P5G

5G is not strictly essential for digitalisation using virtual sensors. However, given that virtual sensors transmit high-resolution images, the use of a private 5G network ensures a truly stable and high-quality service. Another major advantage of using a private 5G network is the ability to flexibly position and relocate virtual sensors.

Why this solution was chosen

The solution was chosen due to its rapid deployment, which enables data to be collected and analysed within just a few days of installation. The system’s flexibility ensures it can be easily adapted to various types of production equipment and processes without the need for complex modifications. Another key benefit is the prevention of so-called ‘data waste’, as the system collects only the relevant data necessary to improve efficiency, thereby minimising the volume of unnecessary information. Furthermore, the solution is cost-effective, allowing it to be deployed even in smaller businesses without the need for high initial investment.

Project status

The project is currently operational. There are plans to extend it to other, less critical machines.

Project evaluation and benefits

Traditional MES systems typically deliver a roughly 10% increase in production simply through their implementation; however, given seasonal fluctuations, such as during the summer months, it is as yet too early to assess specific benefits. The main advantages include accurate time calculation, adjustment of the standard cycle, and increased productivity. The system also enables the identification of problematic moulds and helps to reduce the team’s error rate.

Potential uses and future applications

InOEE has been deployed across a wide range of operations; InovecTech has already installed over 100,000 virtual sensors. The greatest advantage over conventional methods lies in the digitisation of discrete manufacturing in companies with a wide range of machinery, typically with machine cycle times ranging from 10 ms to 1 hour, and with an hourly rate (depending on the type of calculation – ranging from depreciation costs, through total conversion costs per hour of production, to the margin per hour of machine operation) ranging from 10 to 1,000 EUR. This represents approximately 5,000 as yet non-digitised enterprises in the Czech Republic. An analysis of a similar industry in Slovakia estimates the potential for GDP growth resulting from the unlocked potential of digitalisation to be in the order of several tenths of a per cent.

Appendix 5 – Case Study: Geolocation Data Platform by Mapotic and Hardwario

Basic information about the solution provider

Mapotic is a Czech technology company focused on developing a platform for the processing and visualisation of geolocation data, including the processing of sensor data from IoT devices. It collaborates, for example, with Hardwario on the development of the Chester Motion platform for battery-powered online IoT counters, which are used primarily in the tourism sector. It offers tools for interactive maps, IoT data management and mobile applications. Its aim is to provide simple and user-friendly solutions based on geolocation technologies.

Customers, users and their needs

Customers span a range of sectors, including environmental monitoring, sustainable tourism, logistics and public administration. They need quick and easy ways to monitor and analyse data from IoT devices in real time, and to visualise it effectively for decision-making or public presentation.

Use cases for this solution

Mapotic and Chester-based IoT devices are used in various fields, such as wildlife tracking, where IoT sensors and GPS devices are deployed to monitor animals in the oceans or protected areas. Another example is environmental monitoring, which focuses on the long-term tracking of parameters such as air quality, soil moisture or pollution levels, to optimise environmental strategies.

In the field of logistics and planning, Mapotic is used, for example, in winter road maintenance, where sensors monitor the condition of road surfaces and help to optimise winter maintenance planning based on current and historical data.

Effective infrastructure planning, such as road development, the placement of litter bins and rest areas. This system provides accurate data on visitor movements, thereby eliminating the need to rely on irregular manual counts or estimates.

Another project involved the deployment of road monitoring in the Liberec Region, where IoT devices were installed to monitor road surface temperatures. This system provides more accurate data than traditional weather stations, enabling better planning of winter maintenance.

The company is also involved in a pilot project in Prague focused on monitoring tourism. Counters are installed both outside and inside historic buildings, where they enable clients to track tourist movements. The data helps to improve marketing planning and infrastructure adjustments.

Product description

Hardware – HARDWARIO CHESTER

An expandable edge device for Industry 4.0, smart cities, e-metering and agricultural applications. It connects sensors, actuators, PLCs and other devices to the internet. Flexible power supply and LPWAN communication technologies enable reliable and stable connectivity even from remote and hard-to-reach locations. Messages are transmitted via NB-IoT/LTE-M or LoRaWAN technologies, with real-time GNSS positioning.

Implementation process

The implementation process begins with gathering requirements from the client, identifying suitable locations for sensor installation, and the deployment itself. Our devices are battery-powered and, depending on the frequency of data transmission and environmental conditions, can remain operational for several years. We provide connectivity as part of the solution. Data is updated regularly, usually at half-hourly intervals. Calibration and verification measurements are carried out during operation to ensure the results are as accurate as possible. We are also testing a new generation of devices that will be capable of tracking the direction of movement and will allow for remote configuration and calibration of the sensors.

5G/P5G

The company utilises the 5G network thanks to its widespread coverage and collaboration with operators, which enables us to achieve the best possible coverage and broad compatibility not only in the Czech Republic but also across Europe and the USA. This network is crucial for the company’s future, as our solutions often operate in locations without access to the mains electricity supply and require reliable wireless communication.

The devices are equipped with communication chips that enable not only the use of 5G but also other technologies such as NB-IoT and LoRaWAN. These technologies are particularly advantageous for transmitting smaller volumes of data – which is sufficient for these applications – whilst also enabling significant battery savings. Given that the company’s devices often operate in outdoor environments where there is no access to the mains supply, efficient energy consumption is a crucial factor.

This combination of technologies enables the company’s IoT solutions to operate efficiently even in remote locations, thereby delivering reliable results even under the most demanding conditions.

Why this solution was chosen

In the case of the public sector, the company was successful in a tender where affordability was one of the main criteria. The devices are designed to provide the highest quality at the most affordable price possible, which is important for customers who need efficient and reliable solutions for real-time monitoring.

Another key criterion is battery operation and the ability to communicate online, which enables clients to receive data in real time or near real time. There are still relatively few devices on the market that can offer this combination of affordability, quality and reliability. Competitive solutions are either significantly more expensive or have technical shortcomings, such as problems operating in extreme conditions, such as freezing temperatures.

The devices can withstand extreme temperatures, as demonstrated, for example, by projects in the Tatra Mountains, where temperatures dropped to as low as -30 °C and the batteries continued to function without any significant drop in performance. This resilience to extreme conditions is one of the key advantages our solution offers over the competition.

Project status

A new generation of devices is currently being tested, offering significant technical improvements. Key new features include greater accuracy thanks to two sensors, which not only enable more precise measurements but also allow the direction of movement to be determined. Another important innovation is the ability to configure the devices remotely, meaning that measurement parameters, the frequency of telemetry data transmission and other settings can be adjusted without the need for physical intervention.

The company plans to test this new generation in collaboration with selected partners on the Czech market over the coming months. The aim is full commercialisation from 2025, when we plan to launch an intensive promotional campaign, particularly in the sustainable tourism segment, not only in the Czech Republic but also in foreign markets.

Project evaluation and benefits

Some data and measurements from the project’s case study can be found here. Here are a few outcomes directly from the client (Tatra National Park – High Tatras Region)

- Tourist information offices – are able to inform visitors about less or more popular destinations and, based on this, assess which hikes they can undertake in light of this data

- Nature conservation – The TANAP Authority conducts an annual visitor count at the most popular sites, but this system provides a year-round overview of visitor movements

- It is a useful tool for resolving disputes over how many people visit particular sites

- Given rising electricity prices, it is also a useful tool for assessing where the local authority can switch off or regulate public lighting in line with visitor movements

- During the winter season, counters are also installed along cross-country skiing trails, which is important for monitoring which sections are being used; this is also linked to the assessment of trail maintenance, for which the TANAP administration receives grant funding from the Slovak Ministry of Transport

This solution is particularly well-suited to sustainable tourism, national parks and the monitoring of people's movements. By aggregating data from our sensors with other channels, such as mobile or web applications, organisations can effectively manage tourism based on accurate and up-to-date data. This may involve managing parks, distributing tourist flows away from high-impact areas, or using this data alongside other data channels (mobile apps, campaigns) to enable more informed decision-making. These solutions thus enable better infrastructure planning, visitor distribution and the protection of natural areas. Thanks to these benefits, the solution is suitable for a wide range of applications, from tourism to public administration and industrial monitoring.

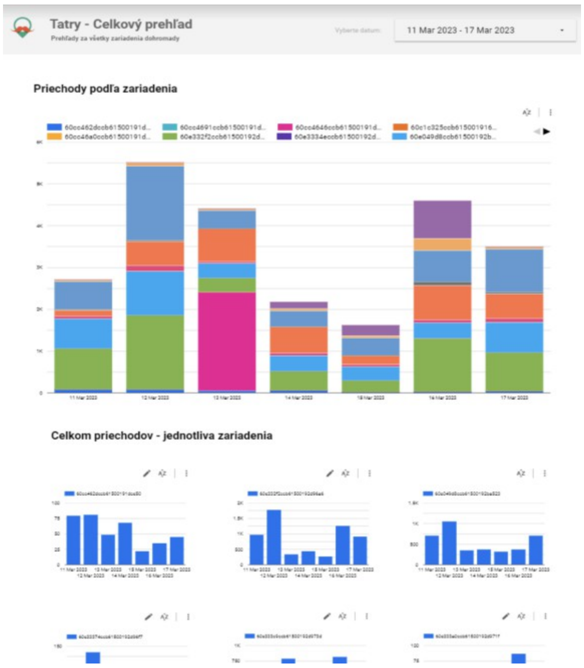

Figure 15: Example of Mapotic platform outputs. Source: Mapotic.