Connectivity technologies for IoT

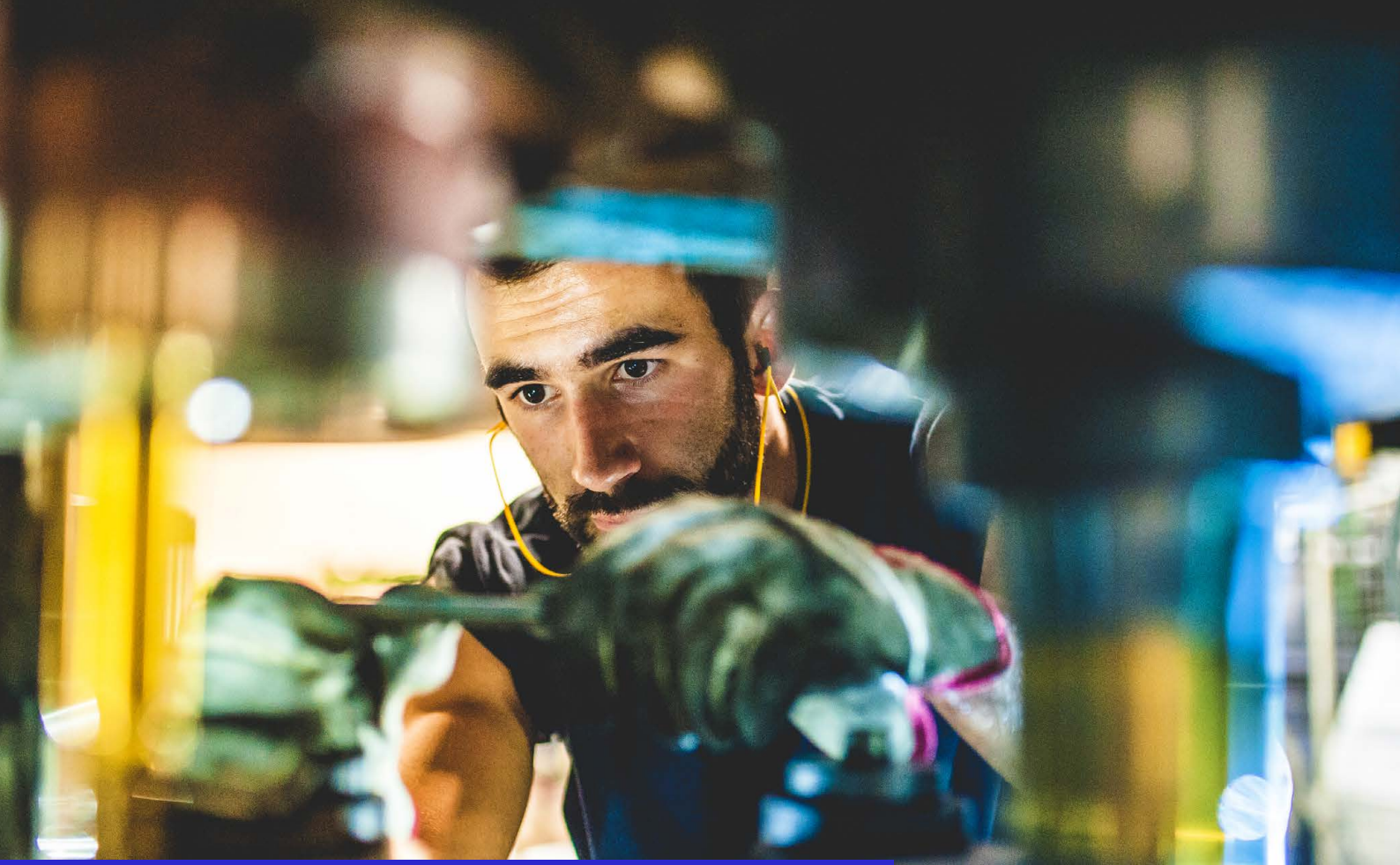
2023 Edition

This report was produced in collaboration with Accenture.

telenor IoT

accenture

Contents



Executive Summary

In recent years, enterprises have accelerated their digital transformation efforts under the pressure of the covid pandemic, various macroeconomic trends and increased competition. IoT is one of the key enablers of digital transformation. IoT solutions are becoming more advanced and delivering increasing value, going from the "monitor and measure" stage to "control and automate". IoT use cases have different and often evolving requirements and therefore enterprises need to consider and select the most suitable connectivity technology as part of designing the end-to-end IoT solution. This decision is critical to the commercial success and total cost of ownership (TCO) of the service. Poor technology choices can result in inferior performance or higher cost in the short-term and hinder long-term scalability and future readiness.

Since the first edition of this report the landscape for IoT connectivity technologies has evolved rapidly. The range of traditional cellular technologies has expanded with the introduction of 5G while previous generations such as 2G and 3G are being phased out in many countries. Low-power wide-area (LPWA) technologies that were specifically developed for IoT applications have gained maturity and scale. Which connectivity technology is most suitable for different use cases depends however on the technology requirements of each specific use case.

Our analysis identifies and groups these technology requirements into three categories – technical, commercial, and ecosystem-related, thus providing a structured approach that enterprises can use to analyse their needs:

- Technical requirements – coverage, energy efficiency, data rate, other features relevant to specific applications (mobility,

positioning, latency, density);

- Commercial requirements – TCO, reliability, security, scalability;
- Ecosystem requirements – future-proofness, global reach and interoperability.

No single technology is ideally suited to serve all potential IoT use cases so different technologies will continue to co-exist as complementing rather than competing standards. Some of the technologies are becoming leaders in their category, having been able to establish a viable ecosystem.

According to our analysis, LoRa and NB-IoT are good alternatives for IoT deployments in remote/wide areas, that do not have high requirements for data speed or latency and will together address a large share of this market. The dynamic open ecosystem of LoRa is well suited for private networks with customised deployments, enabling enterprises to operate own infrastructure and have high flexibility. The cellular LPWA options NB-IoT and LTE-M are backed by major mobile operators, utilizing the huge investments already made in deploying and operating mobile networks and offering standardised connectivity with global reach. Other proprietary technologies may address certain niche segments.

For applications requiring a high data rate, the most suitable technology options are either 4G, 5G, or Wi-Fi, depending on the scope of the IoT deployments. 5G is addressing the needs of use cases with high and complex requirements, for example autonomous vehicles. LTE Cat-1 and in the near future 5G RedCap are well suited for the needs of the medium speed use cases. For local short-range applications, the choice of connectivity technology is less obvious and often the interface and implementation of platform and application layers are most critical.

Finally, this paper provides some case studies and discusses the needs of various application areas, such as automotive, industrial manufacturing or utilities in order to illustrate which technologies can be best suited to serve those needs.

1. Introduction

The Internet of Things (IoT) is transforming many industries and creating value for both businesses and their customers. This paper aims to provide a structured approach that enterprises can use to analyse their requirements for connectivity technology, deliver insights about the connectivity technologies available and how they can serve the needs of specific application areas and use cases.

1.1 Connectivity Technology in the Context of IoT Launch Strategy

Selecting the most suitable connectivity technology is one of the strategic decisions with long-term implications that enterprises need to make when deploying IoT solutions. The IoT journey typically starts with defining the vision and objectives – these can be to increase revenues by enabling new services and business models or to decrease costs in internal production processes and within the supply chain. The main question to ask is how the connected product and the data generated are going to be used and deliver value to the enterprise and its customers.

Once the business strategy is clear, companies can proceed to identify the technology requirements and select the most suitable technologies and vendors. As illustrated in Figure 1, deploying IoT entails securing an end-to-end technology stack that includes device hardware (such as connectivity module, sensors, processor) that are embedded in the connected "thing", connectivity technology that

determines how the device will connect to the internet and transfer data, cloud platform where data is captured, processes and stored and applications (software) for data analytics, machine learning, device management and various business applications. The different elements of the technology stack are usually pieced together into one solution with the help of a system integrator.

Each of these components is important and carries its own requirements. In this paper, we focus on providing insights and analyses regarding how enterprises can select the most suitable connectivity technology among several alternatives such as traditional cellular (2G/3G/4G/5G), a range of low-power wide-area (LPWA) options, Wi-Fi and more.

Every use case has specific characteristics and needs (depending on the complexity and value delivered) that translate into certain technology requirements – technical, commercial, and ecosystem-related. We have identified and described these major technology requirements in the next section of this paper. For some use cases the choice of technology can be very straightforward, while for others the enterprise may need to choose among a number of technologies that can in theory satisfy the needs, but likely with different trade-offs.

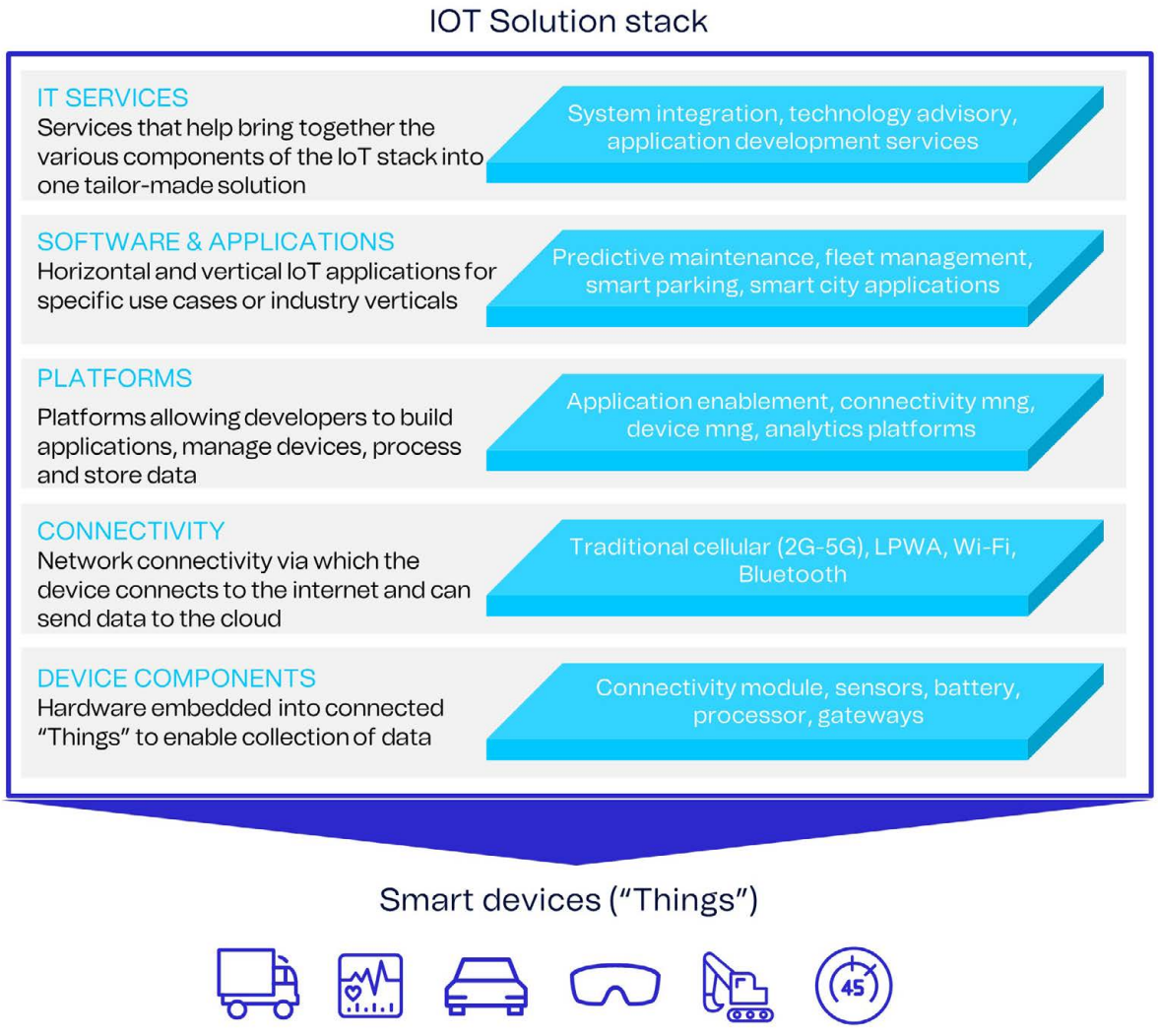


Figure 1: Main components of an end-to-end IoT solution

1.2 The importance of choosing the right connectivity technology

Selecting the right connectivity technology (and vendor) can impact the commercial success both in the short and long term, which is why both perspectives should be considered. In the short-term, a poor choice can result in inferior performance or higher cost than budgeted; in the long run it can hinder scalability as device numbers increase or devices necessitate an expensive swap if the technology does not show to be sufficiently future ready to support long product lifecycles.

There are different types of connectivity technologies available for IoT based on both licensed and unlicensed spectrum. Over the past years, certain connectivity technologies have gained traction and emerged as leaders in their category, but no single technology or solution is ideally suited to serve all IoT use cases. An array of technologies (and vendors) will continue to coexist alongside as complementing rather than competing standards. The choice of connectivity technology for an enterprise depends on the specific use case requirements and competitive environment. In any case, a phased approach is recommended, where companies start small and scale gradually.

Figure 2: Connectivity technology requirements

2. Connectivity technologies for IoT

The IoT landscape consists of a few main categories of wireless connectivity technologies. Short-range IoT includes technologies such as Zigbee, Bluetooth and Wi-Fi that are suitable for local networks connecting a single building or campus. For wide-area IoT use cases that cater to multiple locations spread over a geographic area, cellular technologies are the main choice and satellite services can be used where cellular is not a viable option.

Traditional cellular technologies such as 2G/3G/4G were originally designed for the needs of consumer and business voice and data services. Due to lack of alternatives in the early days of IoT, 2G and 3G were the default choice for connecting cellular IoT devices. However, in 2021 broadband IoT (4G/5G) reached critical number and overtook 2G and 3G as the technology that connects the largest share of all cellular IoT devices[1].

In addition, several technologies have been introduced in the past years to connect things that were previously too expensive or remote to connect. They cater to use cases that entail large numbers of low-cost devices with low power consumption and low-to-medium throughput requirements. These are generally known as Low Power Wide Area (LPWA). We divide them into two main categories:

- Proprietary LPWA – technologies that operate on unlicensed spectrum, for example LoRa. They are typically deployed by non-telecom actors but in some cases by telecom operators.
- 3GPP[2] standardised LPWA (for simplicity often referred to as "cellular LPWA") – technologies deployed on licensed spectrum and managed by telecom operators. The two examples here are NB-IoT and Cat-M1 (also called LTE-M) that have been commercially available since

[1] Ericsson Mobility Report, Nov 2022.
[2] 3GPP is the industry group specifying wireless networking standards.

2017. Since then, the number of devices on this type of networks has steadily grown.

While NB-IoT and LTE-M are the low-cost and energy-efficient options, LTE Cat-1 is a medium speed LTE standard that is designed to serve the needs of more feature-rich IoT applications requiring higher data speeds, to enable video streaming or voice support.

To choose the right option for a specific IoT application when facing such a diverse selection of technologies, requires an understanding of technology from many different angles. As illustrated in Figure 2, our framework divides the criteria into three main dimensions: technical, commercial and ecosystem related requirements. In the following section we will describe the relevance of these requirements.

2.1 Requirements in selecting IoT Connectivity Technology

Technical Requirements

The three main technical requirements for any enterprise looking into IoT connectivity technology are coverage, energy efficiency and data rate. No single technology can excel in all these aspects, as these are trade-offs every radio technology faces (see Figure 3).

Coverage

All IoT applications need good coverage to connect devices but some need to cover only certain indoor areas while others require extensive coverage in rural or remote regions. A technology with long range is better suited to connect devices scattered in a wide area.

Traditional cellular technology, such as 3G or 4G are a typical example of a wide area solution with excellent outdoor device radio range in most urban areas. LPWA technologies further improve the connectivity range by employing more robust coding schemes, which makes them ideal for reaching remote areas and penetrating deep indoors. Short range technologies, such as Wi-Fi and ZigBee, are suitable for connecting many devices deployed in close vicinity.

Energy efficiency

The energy efficiency of a connectivity technology has a significant impact on the lifetime or the maintenance cycle of IoT devices relying on battery or energy harvesting and is dependent on range, topology, and complexity of the connectivity technology. The overall energy consumption of the device also depends on the usage of the application, such as the frequency and duration of message transmission.

Short range technologies like ZigBee rely on mesh topology to forward messages from one device to another over multiple hops. That way ZigBee can extend its coverage but may deplete batteries more quickly as an individual device must constantly listen and be ready to relay messages. Wide area technologies, such as 2G, rely instead on star topology and keep most of the intelligence and complexity at the base station where power supply is not a limiting factor. LPWA technologies, such as NB-IoT, further reduce the energy consumption by stripping down the signalling protocol and reducing the amount of overhead to the bare minimum, thus enabling longer battery life (up to 10 years).

Data rate (on up- and downlink)

Data rate requirements for IoT applications vary from hundreds of bit per second (bps) for metering to several megabits per second (Mbps) for video surveillance on the uplink. Furthermore, with the advent of more sophisticated IoT applications, end devices need to be able to receive data packages with sufficiently high speeds, i.e., have high enough downlink capabilities.

Wi-Fi and traditional cellular networks such as LTE have used large bandwidth and complex waveforms with adaptive

modulation rate to support high data rate. But they either consume more power or have a shorter range. In contrast, most LPWA technologies, for example NB-IoT and LTE-M, have lower data rate and lower energy consumption as they employ a more robust modulation scheme and run on commodity-priced micro-controllers with limited bandwidth.

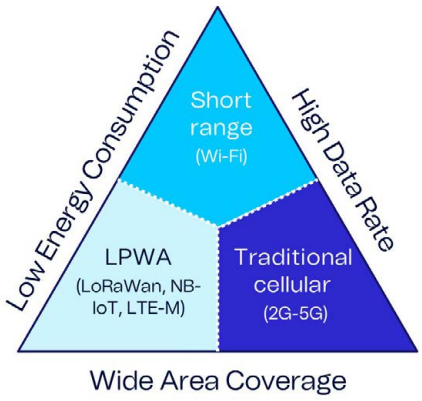


Figure 3: Trade-offs on the technical level

As illustrated in Figure 3, traditional cellular technologies' strengths lie in data rate (mostly 4G, 5G) and range with complex designs optimised for mass consumer voice and data service. Short range technologies like Bluetooth Low Energy (BLE) and ZigBee focus on data rate and battery life at the expense of connection range; LPWA technologies such as NB-IoT, provide superior battery life and coverage, but low data rate on the downside.

Other technical features

In addition to the main technical considerations discussed above, there are other technical features that can be highly relevant for certain applications.

Mobility

In many IoT applications, a device will be installed at a fixed location and paired to a single access point for the entire lifetime, but other applications may require the device to be operational as it moves through the coverage of different access points. While most of the technologies support device relocation to different access points, the relocation process can be as seamless as in the cellular network or occur only at scheduled intervals.

Positioning

Device location is often valuable information. But GPS tracking is not always feasible due to its limited indoor coverage and the extra cost and complexity. Therefore, native support for positioning is a desirable feature. Most wide area technologies can use triangulation to determine the device location, but the accuracy is rather limited for technologies with narrow channel bandwidth and situations where the device is static without direct signal path. Wi-Fi and Bluetooth are constantly improving their positioning capability as the algorithm is getting more sophisticated. For example, Bluetooth Low Energy now includes features that enable one device to determine the presence, distance, and direction of another device.

Latency

Low latency is critical to IoT applications relying on remote control and with minimal delay tolerance (latency) of signal transmission. Latency critical applications range from simpler cases like car heaters to very complex cases such as remote control of drones, industrial automation and autonomous driving.

Device density

The more devices are connected, the more important it becomes for a connectivity technology to be able to handle large numbers of connections within a certain area. The challenge is to deliver reliable connectivity while minimising interference between the various signals. Typically, device density within the massive IoT context is considered in number of devices per square kilometre.

Commercial requirements

Total cost of ownership (TCO)

The TCO for an IoT solution is impacted by the module, subscription and deployment and maintenance cost of the connectivity technology.

Module cost

The connectivity module is one of the main components of an IoT device, as illustrated in Figure 4. The connectivity module cost is directly proportional to the complexity of the technology, ranging from low cost LPWA modules to more expensive LTE or 5G modules due to their pricier hardware and IP royalties. Generally, the price of modules decreases over time as a technology starts to mature and achieves a certain scale. This has been the case for LPWA modules although the global chip shortage disrupted this trend and put upward pressure on prices. Since 2019, we have also seen mass adoption of the LPWA dual mode (NB-IoT + LTE-M) module, as many operators have chosen to support both technologies.

Figure 4: Main cost components of an IoT device

Subscription cost

Cost per subscription is charged by a network operator for providing connectivity services. The subscription cost for cellular connectivity is mainly driven by the data usage and roaming but consists of several components including the monthly base fee and added services. The subscription cost can be zero if the enterprise operates its own private network. However, the complexity of deploying and maintaining the respective IoT network brings additional costs into the picture which must be evaluated separately in order to get the full TCO picture.

Operators typically offer managed IoT connectivity services that include in one contract a global SIM, connectivity, security, SLAs and additional services that help to simplify IoT management.

Deployment and maintenance cost

The cost of deploying and maintaining a network varies substantially with network scale, existing infrastructure, and network ownership. For instance, running an IoT solution on a public cellular network (be it LPWA or standard 2G-5G) is significantly simpler (and thus cheaper) than having to deploy a private cellular network in, e.g., a larger-scale connected factory environment. Traditional cellular networks do have excellent existing coverage in most locations and cellular LPWA can be implemented on top of them with only marginal extra cost.

For regional and national use cases, LPWA technologies generally have a lower total cost than traditional cellular options. Proprietary LPWA networks may require the least investment for providing a regional coverage (e.g., for local smart metering deployments) with a few low-cost base stations, although more sites will eventually be needed to cope with the interferences as the unlicensed spectrum becomes more crowded. For national and global use cases, however, deployment and maintenance cost will speak in favour of cellular options.

Similar considerations can be made within the Wi-Fi space. Short-range networks like Wi-Fi have a low cost per access point but require dense deployments, fixed broadband access, configuration and maintenance that drive up the TCO for providing a wider coverage. In a situation in which cellular infrastructure is readily available and sufficient to serve the use case in question, Wi-Fi would be comparatively costly due to higher deployment and maintenance cost.

Reliability

Reliability requirements can vary significantly for different IoT applications and while in some cases poor reliability may affect user satisfaction, in other cases good reliability is an essential use case criterion. Reliability requirements hence differ strongly between delay-tolerant metering applications to mission-critical remote-control systems that necessitate high reliability (and low latency).

While connectivity suppliers for almost every technology provide a certain degree of reliability assurance, typically solutions relying on licensed spectrum can guarantee a higher degree of reliability. In cellular networks, SLAs are commonly used by major actors to guarantee certain levels of reliability and general quality of service for customers. On the other hand, technologies operating in unlicensed spectrum, such as LoRa and Wi-Fi, are generally designed on a best effort basis with limited quality of service assurance as they are subject to potential interferences from other uncoordinated technologies and networks. Regulatory requirements can in some cases (e.g., utilities) mandate certain SLAs which impacts the choice of connectivity technology.

Security

IoT devices are vulnerable to network attacks such as data thefts, phishing attacks, spoofing and denial of service (DDoS). Therefore, security is essential to IoT devices. Some of the typical IoT cybersecurity challenges include security of the hardware to resist physical intrusion, software and firmware vulnerabilities, insecure communications, or data leaks from cloud environments where data is stored.

Higher security for IoT applications typically requires more processing power for data encryption/decryption and identification/ authentication. This raises yet another concern – the size of overhead data associated with IoT information. While security solutions are being developed for proprietary LPWA technologies such as LoRa, comprehensive and easily accessible protection still has a long way to go. Cellular networks rely on Subscriber Identify Modules (SIM) as the basis for the authentication, security, and privacy mechanisms. Since cellular networks have been deployed for more than three decades, this has allowed to evolve and harden their security. Wi-Fi and Bluetooth Low Energy also employ advanced encryption mechanisms. In more advanced applications, security is done in higher levels of the technology stack, which potentially drives further overhead.

Scalability

Given the high expectations for growth in IoT devices, an IoT network should possess the ability to quickly and cost effectively scale up its capacity as needed. The scalability of a network is not just about the number of devices that can be connected to a single access point, but also about how many of them can actively transmit concurrently and if the network would be negatively affected by interferences from external sources.

Cellular networks have an advantage in this regard for applications that foresee a large volume with sustained growth. Centralised coordination in cellular networks allows more devices to transmit simultaneously, and their exclusive access to licensed spectrum protects the transmissions from any external interferences. Most of the short-range technologies and proprietary LPWA solutions instead employ uncoordinated and unlicensed spectrum which may constrain their long-run scalability. From a cost perspective, public cellular networks allow to scale up by paying for every additional device added, while increasing capacity in private networks needs to happen in a more planned stepwise approach.

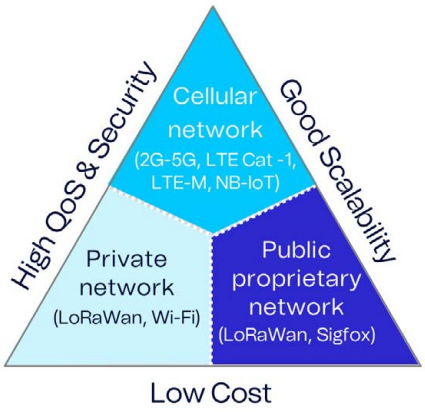


Figure 5: Trade-offs on the commercial level

As illustrated in Figure 5, cellular networks have the necessary scale and capability for delivering high quality of service, security, and scalability at a higher cost (LPWA networks such as NB-IoT and LTE-M, however, have a lower price point than traditional 2G/3G/4G/5G). On the other hand, proprietary LPWA networks that are deployed as a public network, such as Sigfox, may have lower cost of connectivity but may be more complex to operate with limited reliability and scalability. Enterprises can purchase capacity directly from public networks based on either cellular or proprietary technologies.

Other technologies, such as Wi-Fi and LoRa, can be deployed as either a public network or a customised private network. A private network for dedicated use by the enterprise could be a cost- efficient solution. Private networks can meet specific requirements and hand more control of the network to the enterprise but are difficult to scale up and replicate for global applications.

Ecosystem requirements

Future ready

The future readiness of a technology encompasses longevity to assure its availability in the future and long-term economic viability in terms of long-term cost reduction potential. Technology longevity is a crucial consideration for IoT applications with logistical and cost challenges of replacing deployed devices. Understanding the strategic intention of key stakeholders that back the technology can help predict the future direction of its development. For instance, Sigfox, which was funded by venture capital and had built a network spanning 75 countries, filed for bankruptcy protection in 2022, citing slow sales of its products and challenging conditions in the IoT industry due to the impact of covid-19. An open standard approach by the likes of LoRa promises a better sustainability than technologies with closed systems. The latter pose risk for single point of failure while the former create opportunities for multiple service providers and vendors.

Selecting a technology with the potential to achieve economies of scale ensures the investment is economically sustainable as the business grows. A mature ecosystem, like that of cellular or Wi-Fi, not only develops a strong technical roadmap with industrywide cooperation but also promotes heavy competition in the commercialisation among numerous vendors and service providers.

Some regional differences have also emerged because of government stimulus and endorsement from specific service providers early on. For example, NB-IoT got a big push in China while most US operators chose to rely on LTE-M. Many telecom operators have over time chosen to support both of these technologies, thus ensuring they are both future ready.

Global reach and interoperability

Global companies need global solutions to achieve economies of scale and to avoid having different technologies and network operators for each single market. Products sold in one market may be deployed by the customer in another market where they need to work "out of the box". Global reach and interoperability (across networks of the same technology) also create markets of larger volume and global competition, both of which help to drive down cost.

Many of the predominant short-range technologies, such as Wi-Fi and ZigBee, are developed by IEEE standardisation association and supported by global industrial alliances to promote international interoperability. They operate in the 2.4 GHz ISM band, which is available globally.

Proprietary LPWA technologies often face a trade-off between global reach and interoperability. An open standard approach, as in the case of LoRa, creates a vibrant ecosystem encouraging innovation and wide adoption globally, but leaves too much room for proprietary variants that are not be able to communicate to each other. There is currently no global LoRaWan network. On the other end of the spectrum, a closed standard approach as in the case of Sigfox ensures interoperability but restricts the ecosystem scale and reach.

The cellular industry has created global standards and cellular networks that currently offer the best global reach.

2.2 Cellular LPWA technologies – NB-IoT and LTE-M

NB-IoT and LTE-M are the two cellular LPWA technologies that were specifically designed for wide-area IoT use cases. They both use simplified versions of regular 4G which reduces hardware complexity and cost once the technology is operating at scale. Since their commercial introduction in 2017, the number of networks globally has been steadily growing. The number of devices connected by these technologies was expected to reach almost 500 million by the end of 2022[3].

Initially, LTE-M was predominantly rolled out by North American operators while European and Asian operators (in particular in China) launched NB-IoT. While NB-IoT currently has a larger global footprint, many operators have been embracing a dual mode (NB-IoT + LTE-M) strategy, which allows enterprises more flexibility to choose the best fit technology. While both NB-IoT and LTE-M are designed to address LPWA use cases, there are some differences.

The main distinguishing factors between LTE-M and NB-IoT are the uplink/downlink speeds and latency. LTE-M has significantly higher bitrates and lower latency. Thus, LTE-M is the only technology of the two that is suitable for applications necessitating a fast and stable response time. Another important difference is that LTE-M supports voice functionality via Voice over LTE (VoLTE) which makes it suitable for applications requiring human interaction, such as certain types of connected health, security alarms, as well as automotive applications. It is important to note though that not all operators may have enabled that functionality.

NB-IoT is designed for static devices, and it can lead to interruptions if devices are moved while LTE-M is the better choice for moving devices. For devices with a long lifespan of 10 to 15 years it is furthermore crucial to consider device updates. LTE-M is considerably better at handling device updates driven by security improvements and software development, as its higher throughput can handle more data. In general, LTE-M is very well suited for applications within transportation, logistics, home security, connected health, smart grid, wearables and industrial asset management.

For cases in which requirements are static and known from the start, NB-IoT can be a better choice since it comes with a longer range and excellent penetration in underground and indoor settings. NB-IoT is ideally suited for low bandwidth, infrequent communication from simpler, relatively static sensor applications in use cases such as smart meters, agriculture, smart cities, home automation. NB-IoT is optimal for remote environmental sensors that need to send regular updates from a fixed location while optimising battery life.

Roaming on cellular LPWA networks is a

[3] Ericsson Mobility Report, Nov 2022

crucial factor, especially for use cases such as logistics tracking, which may involve containers crossing multiple national borders. LTE-M has been designed for roaming from the start and can leverage existing roaming and wholesale business models between operators. It is expected that LTE-M will be relevant for international IoT solutions earlier than NB-IoT.

2.3 Traditional cellular

For enterprises deploying wide-area network use cases, it is crucial to consider how the connectivity technology landscape will evolve in the future. Many IoT applications were initially deployed using 2G connectivity as these networks were widely available globally and had a mature ecosystem thanks to being in operation for more than 30 years. Since many IoT solutions have a long lifespan (often a decade or more), there are still large volumes of devices that operate on 2G networks. However, as 4G networks proliferated globally and then 5G networks were added and are now under deployment, it became necessary to free up spectrum for the new generations of technology that will be in place for the next decades and reduce complexity in the networks. This led to operators in many countries deciding to sunset their 2G and 3G networks. The timing of such network shutdown varies across countries and regions, depending on local market conditions such as the amount of legacy traffic still managed on those networks and regulatory considerations. Decommissioning of 2G and/or 3G has already been completed in some parts of the world and is underway or planned in other countries.

In the US, most major US operators had shut down their 2G and 3G networks by the end of 2022. In Asia, many operators are prioritizing to sunset 2G first in order to re-use spectrum for 4G, which has high adoption across the region. Countries like Taiwan and Singapore were early in decommissioning both their 2G and 3G networks. In Europe, the situation varies across countries, but generally there seem to be a tendency to switch off 3G networks faster than 2G networks, both in terms of actual sunsets completed and announced future plans[4]. Some operators have even extended the dates for switching off their 2G networks. Africa is trailing the other regions and has few sunsets currently announced as 2G in particularly is still widely used.

For enterprises that have legacy devices deployed on 2G or 3G networks, it is important to proactively prepare for the shutdown to avoid devices becoming inoperable and potential liability towards customers. The first step is to evaluate what part of the installed base depends on 2G or 3G connectivity and to what extent – if devices depend entirely on it or are only using it as a fallback when other primary technologies are unavailable. Second, for enterprises with multi-country deployments, it is important to identify and closely monitor the key dates since those vary across countries. Based on this, enterprises need to create a migration plan with a roadmap for transitioning to another solution. This may entail switching to another connectivity technology provided by the respective operator partner, replacing legacy devices that are near end of life or updating and retrofitting those devices.

For enterprises deploying new devices aiming to rely on cellular connectivity and be future ready for the next ten years, NB-IoT, LTE-M or LTE Cat 1 are suitable candidates depending on the use case. LTE Cat1 is an excellent alternative to replace 2G/3G in many automotive use cases (such as fleet management or vehicle telematics) thanks to its support for voice, mobility, and good bandwidth. NB-IoT and LTE-M provide a simpler and more cost-efficient way to support small, battery powered devices such as sensors.

[4] GSMA Intelligence

2.4 Assessment of Leading Connectivity Technologies

While there is no single technology that can excel in serving all use cases, several of the technologies have gained prominence in terms of technology maturity, ecosystem support and scale of commercial availability. For IoT deployments in wide areas or remote locations, LoRaWan, NB-IoT, LTE-M or LTE Cat 1 are good complements that address the needs of most use cases.

The various IoT connectivity technologies have different strengths and weaknesses, depending on the technical, commercial and ecosystem angle. Table 1 illustrates their performance across key metrics.

Low Medium High

Technical considerations	Traditional cellular				Other cellular	LPWA Cellular		Proprietary LPWA	Short range		
	2G	3G	4G	5G	LTE Cat-1	LTE-M	NB-IoT	LoRaWan	Wi-Fi	Zigbee	Bluetooth LE
Outdoor range											
Indoor coverage											
Energy efficiency											
Typical uplink data rate											
Typical downlink data rate											
Mobility											
Positioning											
Latency											
Device density											
Commercial considerations	**Traditional cellular**				**Other cellular**	**Cellular LPWA**		**Proprietary LPWA**	**Short range**		
	2G	3G	4G	5G	LTE Cat-1	LTE-M	NB-IoT	LoRaWan	Wi-Fi	Zigbee	Bluetooth LE
Module cost											
Subscription cost	yes	yes	yes	yes	yes	yes	yes	yes/no	no	no	no
Deployment & maintenance cost											
Reliability											
Security											
Scalability											
Ecosystem considerations	**Traditional cellular**				**Other cellular**	**LPWA Cellular**		**Proprietary LPWA**	**Short range**		
	2G	3G	4G	5G	LTE Cat-1	LTE-M	NB-IoT	LoRaWan	Wi-Fi	Zigbee	Bluetooth LE
Future proofness											
Global reach & operability											

Table 1: Main technologies for IoT with strengths and weaknesses

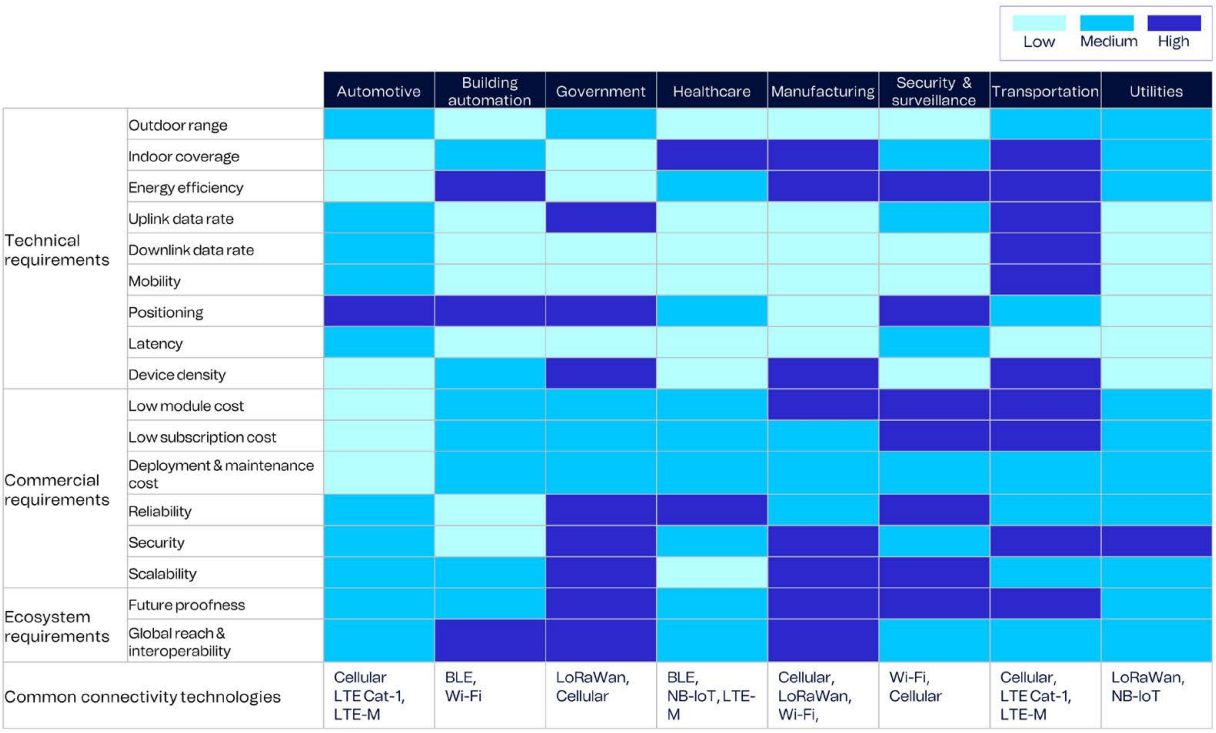
3. Application area technology mapping

This section assesses the connectivity technology needs of major application areas of IoT devices in the current market in terms of the outlined technical, commercial and ecosystem requirements. This assessment forms the logic for conclusions with regards to most common connectivity technologies per application area[5].

Application areas consist of a variety of use cases, some with heterogeneous connectivity technology requirements.

Hence the resulting assessment in Table 2 is based on a weighted average of use case requirements where the weight of the use case depends on the number of IoT connections over a five-year horizon. Government for instance covers the use cases outdoor surveillance as well as city asset tracking which have very heterogenous data rate requirements.

[5] Most common technology lists the technologies with currently highest number of connections. These can change given increasing scale and complexity of use cases.



		Automotive	Building automation	Government	Healthcare	Manufacturing	Security & surveillance	Transportation	Utilities
Technical requirements	Outdoor range								
	Indoor coverage								
	Energy efficiency								
	Uplink data rate								
	Downlink data rate								
	Mobility								
	Positioning								
	Latency								
	Device density								
Commercial requirements	Low module cost								
	Low subscription cost								
	Deployment & maintenance cost								
	Reliability								
	Security								
	Scalability								
Ecosystem requirements	Future proofness								
	Global reach & interoperability								
Common connectivity technologies		Cellular LTE Cat-1, LTE-M	BLE, Wi-Fi	LoRaWan, Cellular	BLE, NB-IoT, LTE-M	Cellular, LoRaWan, Wi-Fi,	Wi-Fi, Cellular	Cellular, LTE Cat-1, LTE-M	LoRaWan, NB-IoT

Table 2: Application areas, typical requirements and most common connectivity technologies

3

Automotive

The connected car provides car manufacturers and vehicle owners with great amounts of data on driving behaviour, car performance, need for maintenance, and safety features such as eCall. IoT in the automotive space aims to improve the driving safety and experience while enabling data analytics for better product design. The use cases are constantly expanding and some of the main ones are:

- Fleet management – allows owners of vehicle fleets to monitor the location and status of their vehicle and enables remote assistance.
- Vehicle analytics – provides data to improve driver behaviour, fuel usage and safety while optimizing vehicle maintenance.
- Infotainment – enables onboard entertainment services such as streaming video, and navigation services.
- Insurance – allows Usage-based insurance (UBI) models where the premium is adjusted based on driving behaviour.
- Autonomous driving, V2V (vehicle-to-vehicle), vehicle-to-infrastructure (V2I) and V2X (vehicle-to-everything) communication – increasingly allows vehicles to crowdsource information from their surroundings and thus improve not only the individual driving experience but also contribute to smart cities that are less polluted and congested.

Constant data transmission and the high mobility of vehicles necessitate wide-area coverage for automotive IoT applications. High reliability of the network is needed to ensure the faultless operation of features such as voice calls and remote access to car functions as well as real-time navigation, automatic crash notification and roadside assistance. Security is a major consideration given the nature of personal data collected and strict safety requirements. Connected cars furthermore require a high data rate to support infotainment services for music and video streaming. Low latency is becoming increasingly relevant as use cases requiring real-time operation emerge, e.g., autonomous driving.

Vehicles have long development cycles and lifespan, which necessitates a connectivity technology that has long-term commitment by technology vendors and operators and that supports over the air software updates. With the GSMA embedded SIM specification, automakers can remotely provision connectivity over the air to vehicles.

High requirements on outdoor device radio range, reliability and security, mobility and especially data rate leave cellular connectivity such as LTE-Cat1, LTE-M or 4G/5G, as the best long-term options.

Transportation

Rising global traffic and public transport fuels growth for the main segments in transportation – connected buses and aircraft. Connected transportation entails use cases such as driver interaction, fleet tracking and predictive maintenance aiming to reduce vehicle downtime while increasing overall productivity. Such applications have complex technology requirements – reliable coverage in urban and rural areas, global connectivity across countries and continents, positioning capabilities for location tracking, a high quality of service to ensure that assets do not "go dark", and future readiness of the technology. The latter means that the devices have SIMs and modules supporting over-the-air updates to avoid the need for costly swapping out in the field. The advancement of use cases that require real-time responsiveness and analytics additionally strain bandwidth requirements. Hence, 4G/5G and LTE-Cat1 are well suited for most transporting solutions given low price sensitivity and flexible energy efficiency requirements.

For other use cases with lower data requirements and higher energy and cost efficiency requirements, such as asset tracking of packages or luggage, NB-IoT and LTE-M are suitable solutions. Through cellular LPWA technology, a large number of widely dispersed objects can be tracked, and status updates be transmitted at low cost.

Building Automation

Automated and connected buildings gather data on building climate, lighting, energy consumption and space utilisation. This allows real estate owners/ managers to reduce their operating expenses while improving the experience of tenants. Connected lighting and commercial heating, ventilation, and air conditioning (HVAC) management are the two primary use cases. They can optimize the room climate and provide substantial savings if synchronised with actual and expected occupation, daylight harvesting and outside temperature. The adoption of those technologies is fuelled by greater awareness for sustainability, stricter government regulations and the increased focus on employee wellbeing and safety.

Building automation solutions, especially connected lighting, are mostly based on large-scale deployments of low-cost devices. Hence, connectivity technologies for building automation need to be cost-efficient and able to handle a high density of devices, especially for lighting solutions. At the same time, energy efficiency is critical to minimise maintenance of large-scale deployments. Wi-SUN and Bluetooth Low Energy are the most suitable technologies. Wi-SUN networks can cover an entire building or even campus, while also satisfying requirements for high energy and cost efficiency and the ability to handle device density. Bluetooth Low Energy with mesh has specifically been designed for a large number of devices and is well suited for building automation – now supporting longer ranges as well as energy harvesting.

Government

Increased urbanisation and population growth strain public infrastructure prompting governments to better utilise public space and resources in order to improve urban life quality and public health. Government IoT use cases primarily aim to address those needs while optimising public expenditures. Road toll, traffic management and tracking of public assets are the main

use cases. Governments globally are furthermore pushing for increased outdoor surveillance which fuels the growth of outdoor surveillance cameras.

Road toll management enables governments to streamline and optimise toll charges according to the vehicle's impact on the infrastructure, traffic, and environment (based on weight of the car, time of the day, pollution produced). This improves traffic and gives incentives for more environmental vehicle purchases. In the long run it improves not only traffic planning but also city planning.

Asset tracking sensors are relatively low cost and enable substantial cost savings. Tracking the condition and location of various types of public assets such as gardening and snow-clearance equipment or manholes allows to reduce equipment downtime and theft.

Government use cases require a long battery life (10+ years), low cost and good scalability but have low bandwidth requirements – except for camera surveillance with high bandwidth needs. The large scale of sensor deployments per individual access point/base station places high demands for network scalability, especially as new devices are constantly added. Proprietary LPWA technologies such as LoRa are offering good cost efficiency given limited scale. Since LoRa is using unlicensed spectrum, it may face long-run scalability challenges as more networks and billions of devices are deployed using the same unlicensed band. But in the short to medium run, it can meet the outlined requirements. As use cases are advancing with more sensitive data requiring higher reliability and security, NB-IoT and LTE-M have also become suitable alternatives.

Healthcare

Increasing cost pressure from a rise in chronic diseases and more tailored patient treatments are driving healthcare IoT deployments. Major use cases range from chronic disease management to patient data transmission from medical devices.

Chronic disease management improves patient experience and treatment through continuous tracking of critical patient data. In remote monitoring cases, patients' medical data is constantly collected and transmitted to the treating doctor. Patients experience a better treatment while the number of visits to healthcare facilities is minimised.

Within healthcare facilities, monitoring use cases enable the transmission of data obtained from medical equipment. Instead of being read out manually by healthcare personnel it can now be transmitted, centralised, and stored in patient records.

Within elderly care homes, monitoring refers to an improved tracking of residents. Fall detectors, geofencing and bed sensors inform personnel of incidents where residents have fallen, are wandering or are unable to get out of bed.

Healthcare IoT deployments require high indoor coverage and energy efficiency to ensure device reliability for an extended time period and high security due to the sensitivity of patient data. NB-IoT is a suitable technology for remote monitoring, and local monitoring within elderly care homes. NB IoT is relatively cost efficient while also ensuring high reliability and data security. For transmission of medical equipment data or asset tracking within healthcare facilities, Bluetooth Low Energy would be more suitable given high-cost sensitivity and otherwise less complex use case requirements.

Manufacturing & Resources

Industrial IoT (IIoT) refers to the application of sensors and connected devices in manufacturing and industrial settings. The growth in Industrial IoT has been driven by cost pressure, the need for optimised output and reduced energy cost as well as increasing awareness for worker safety and wellbeing.

Some of the main use cases within this area are:

- Process automation and facilities management – sensor devices collect data on all relevant aspects of the manufacturing process – ranging from factory temperature and energy consumption to machinery condition and process efficiency. This can help to ensure the quality of resources and products and get deep visibility in the production process.
- Predictive maintenance – data analytics on equipment condition enables companies to predict when their machines may break down and take pre-emptive action to avoid costly downtime.
- Supply chain optimization – real-time visibility on the flow of goods along the supply chain and the availability of materials allows to improve efficiency and make better decisions.

Manufacturing use cases have been historically dominated by wired connections. However, wireless technology has been gradually increasing its share not only in greenfield but also in brownfield settings where older machines are being retrofitted. The network needs to be adaptable to a mix of both legacy and new machines and be able to scale up easily as new machines are being connected.

Industrial manufacturing use cases require connectivity with good indoor coverage, often in industrial regions, high device density and low cost. Machines are often in close proximity to each other with a high number of sensors and frequent data submission.

LoRa, Sigfox and Wi-SUN are common technologies offering good indoor coverage, reliability, and low operating cost (after the initial investment in setting up the network). Cellular technologies can also be a suitable alternative for companies within industrial manufacturing, eliminating the need to set up and maintain private Wi-Fi networks and providing high quality of service through SLAs.

Major industrial companies, especially in Germany where spectrum has been released, have even turned to private networks to address needs for greater reliability and scalability.

Physical Security

Rising concerns for public, employee and private safety and security drive the market for various IoT security use cases. These range from indoor camera surveillance for public and private properties to intruder detection and safety alarms to indicate fire or gas and water leakage.

Intrusion detection has faced some challenges as the high number of false alarms entailed high cost for service providers. These shortcomings are overcome by an increase in the number of sensors, better calibration and remote monitoring which reduce false alarms. Growth in the indoor surveillance market is mainly driven by increasing density and scale of camera instalments and rising price levels through greater capabilities. Both energy efficiency and analytics have improved substantially through advanced features such as edge processing and AI image recognition capabilities.

Security use cases have varying requirements, especially with regards to the data rate. Video surveillance, for example, has demands for high data rate, coverage, and bandwidth as streaming video entails significant data traffic. In addition, quality of service and reliability need to be very high to ensure uninterrupted real-time operation. High security requirements lead to heavy processing needs for data encryption and decryption. 4G and 5G satisfy those needs. Bandwidth consumption can be a challenge for 4G depending on the scale of camera deployments. Wi-Fi networks are a less pricy option to facilitate surveillance use cases with high bandwidth requirements, exhibit however greater vulnerability to cyber-attacks.

Security and safety alarms in turn send infrequent, small data packages and require good indoor coverage, cost efficiency, reliability, and security. NB-IoT and LTE-M are suitable options to provide more robust connectivity in case the primary broadband connection fails.

Utilities

Smart meters for electricity, water and gas are the main use cases within utilities. Smart electricity meters constitute the largest utilities IoT application to date. They require frequent communication but low energy efficiency due to access to continuous power supply.

Most electricity meter deployments have been on cellular technology, meeting the requirements for coverage, reliability, and longevity of the technology (meters can have a lifespan of up to 15 years). However, as water and gas meters see increasing growth, LoRa and Wi-SUN will be the most common technologies with the ability to penetrate devices that are located underground, low energy requirements and low cost.

4. Future outlook

As illustrated in the previous section, different application areas and use cases have different connectivity requirements that determine the most suitable choice of connectivity technology.

Use cases and thus needs will however change over time and the requirements of future IoT applications remain to be seen.

5G Redcap

The latest generation cellular technology that was added to the IoT connectivity stack was 5G. It was designed for three initial use cases:

- eMBB (enhanced Mobile Broadband) – provides higher data rates and improved latency to serve newer application such as 4K media, AR and VR.
- uRLLC (ultra-Reliable Low Latency Communication) – delivers the best performance when it comes to latency, network reliability, and security.
- mMTC (massive Machine Type Communication) – offers ultra-low power consumption and enhanced in-building coverage for environments with larger number of connected devices, for example, industrial IoT setups such as smart factories.

However, in between these extreme capabilities, there are many use cases for which ultralow latency isn't essential but reasonable throughput is needed to ensure data flows for next-generation applications can be supported. Example of such use cases are wireless industrial sensors, video surveillance, smart grids, and smart wearable technology. To address these lower requirements and thus reduce device complexity and cost, 5G Reduced Capability (RedCap) also called 5G NR-Light was introduced as a new standard in mid-2022. It fills an essential gap in the 5G family to provide a transition path to 5G for applications currently utilizing LTE

Cat 1 or Cat 4. When comparing RedCap with LTE Cat 1 or Cat 4, the main benefits concern higher peak data rate, lower latency than LTE Cat 4, and power consumption improvements.

Many operators first launch the non-standalone (NSA) version of 5G, that is anchored in 4G, before then moving to the standalone (SA) version that supports the full capabilities. Redcap supports only standalone 5G networks. The first 5G RedCap chipsets will be available in 2023 and 2024, and commercial RedCap devices will follow suit. The timeline for migrating from LTE Cat 1 or Cat 4 to 5G RedCap depends on the application, its lifespan, and targeted geographic region for deployment. Likely, mobile network operators in the US and some APAC countries will be the first to roll out RedCap, prompting an earlier transition phase and an eventual lifecycle end for LTE networks. Applications with long lifespan of ten years or more, would also benefit from evaluating a transition to 5G RedCap sooner rather than later.

Private Networks

During the past years, private networks have experienced significant growth, which is expected to continue. While enterprises were initially using proprietary technologies, the share of cellular has been increasing. In mid-2022, almost 40% of the private networks worldwide were either 5G or a mix of 5G and LTE[6] .

The early adopters of private 5G networks have been primarily large enterprises looking to provide secure and highly reliable connectivity for critical infrastructure such as airports, manufacturing facilities and warehouses or oil refineries. Other enterprises will opt for a dedicated cellular deployment, primarily to tackle challenging radio environments that cannot be addressed by LPWA or other existing public networks. In those cases, MNOs or network equipment vendors could deploy and operate such private networks on behalf of the enterprise, solving the coverage issue and taking over the job of managing and operating the network.

Opening 5G Networks to Application Developers

As 5G networks are commercially rolled out globally, there is an opportunity to expose 5G network capabilities to developers through APIs and SDKs in order to drive adoption and innovation. Through these APIs, enterprises can get easier access to the network performance specifically needed for their individual use case. For example, super low latency for mobile gaming or location services for connected vehicles. To make this possible, mobile network operators will need to cooperate in order to harmonize the exposure of APIs in 5G networks and adopt new business models such as resell of enhanced APIs or through subscriptions, moving away from the traditional approaches based on minutes and data use . The efforts to orchestrate this new approach are still in early stages but if successful will make 5G even more attractive and bring opportunity for enterprises to bring to market new services more easily.

[6] Source: GSMA
[7] Source: Ericsson

5. Concluding words from Telenor IoT

Enterprises seeking to implement IoT solutions should carefully evaluate their specific use cases and connectivity requirements to select the most suitable IoT connectivity technology. No single technology is a one-size-fits-all solution. It is important to select the right partner that can guide in making an informed decision. As businesses navigate the evolving landscape of IoT, having a trusted and experienced partner like Telenor IoT by your side can provide the necessary expertise and support to ensure successful implementations and long-term value.

Traditional cellular technologies such as 2G have served IoT cases for many years, providing global coverage with excellent roaming capabilities and support for mobility. As 2G networks are being sunset in many countries to make room for the new generations of cellular networks, the options for enterprises are not shrinking but rather expanding as new technologies tailored to the needs of IoT have been introduced. LTE-M has emerged as a strong and viable option for many use cases, thanks to its capabilities to support the data rate and mobility needed by many applications such as fleet management, while providing sufficient battery life.

For applications requiring a high data rate, the most suitable cellular technology options are either 4G or 5G, depending on the scope of the IoT deployments. 5G is addressing the needs of use cases with high and complex requirements. LTE Cat-1 and in the near future 5G RedCap are well suited for the needs of the medium speed use cases.

Advancements in connectivity technology present new opportunities. Exposing 5G network capabilities to developers through APIs can help foster innovation and drive adoption. Incorporating edge computing

solutions into IoT infrastructure can enable enterprises to reap benefits such as reduced response times and improved data privacy. For enterprises that want a high degree of control over the network in a contained environment (such as mines), private networks can be an alternative to a public network.

Staying up to date with the latest IoT connectivity technologies is vital for enterprises to ensure they are using the most suitable technology for their needs. Continuously evaluating emerging technologies and their potential applications allows businesses to adapt and maintain a competitive edge. With Telenor IoT's comprehensive portfolio of IoT solutions and deep industry expertise, enterprises can navigate the dynamic IoT landscape with confidence and maximize the potential of their IoT deployments.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.
Visit us at www.accenture.com.

Telenor Connexion

Telenor IoT is the portfolio of IoT solutions from Telenor Group, one of the world's major mobile operators. With more than 20 years' experience of providing global IoT connectivity, cloud services and expert support to companies of all sizes, Telenor is one of the world's most advanced IoT solution providers. Telenor IoT manages international IoT deployments for global customers in some 200 countries and today operates more than 20 million connected devices to enterprises such as Volvo, Scania, Hitachi, Verisure Securitas Direct and Husqvarna. The IoT solutions are offered to national customers in the Nordics through the local Telenor operations in each country, and on a global level through Telenor Connexion, Telenor's specialized unit that provides IoT solutions for large, international enterprises who need a customized offer with advanced support.

iot.telenor.com

sales@telenorconnexion.com