Connectivity technologies for IoT

Northstream

Full Report
Updated Edition, 2018

Commissioned by

telenor | connexion

Executive summary

Selecting the most suitable **connectivity technology** is one of the critical decisions that enterprises need to make in their IoT launch strategy as connectivity is an important component in an end-to-end IoT solution. This decision can impact the success of the service as a poor choice can result in inferior performance or higher cost in the short-term, and in the long-term it can hinder scalability or necessitate an expensive swap if the technology is not sufficiently future proof.

There are a range of technologies available for IoT such as traditional cellular (2G/3G/4G), Low Power Wide Area, Wi-Fi, Bluetooth and more. Every use case has specific needs, which translate into certain technology requirements that determine the choice of most suitable connectivity technology. Our analysis identifies and groups these technology requirements into three categories – technical, commercial and ecosystem related, thus providing a structured approach enterprises can use to analyze their requirements:

- Technical requirements – coverage, energy efficiency, data rate, other features relevant to specific applications (bidirectional communication, mobility, localization);
- Commercial requirements – quality of service, cost, security, scalability;
- Ecosystem requirements – future proofness, global reach and interoperability.

No single technology or solution is ideally suited to serve all potential IoT use cases and certain technologies will coexist alongside, as complementing rather than competing standards. Currently, there are also various actors within these technologies that are aiming to establish their market dominance and ecosystem. The current fragmentation is not sustainable for the industry in the long run and leaders will emerge.

According to our analysis, for IoT deployments in remote/wide areas, LoRa, NB-IoT and LTE-M are good complements and together will address a large share of this market. LoRa's dynamic open ecosystem is ideal for private networks with customized deployment, while NB-IoT and LTE-M are backed by major mobile operators offering standardized connectivity with global reach. Other proprietary technologies, like Sigfox, may address certain niche segments but their future proofness is to be time tested. For applications requiring high data rate, the most suitable technology options are either LTE, Wi-Fi or BLE, depending on the scope of the IoT deployments. For local short range applications, the choice of connectivity technology is less obvious and often the interfaces and implementation of platform and application layers become more crucial. From around 2020 onwards, 5G networks will also start to be commercially available, bringing improved capabilities to address both massive and critical communication use cases.

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

Copyright © 2018 Northstream AB

1. Introduction

The Internet of Things[1] (IoT) is transforming many industries and will create value for both businesses and their customers. This paper aims to provide a structured approach enterprises can use to analyze 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. 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 decrease costs in internal production processes and 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.**

After defining both the strategic and financial objectives and impact, enterprises can proceed to identifying technology requirements and selecting the most suitable technologies and vendors. As illustrated in Figure 1, deploying IoT entails securing an end-to-end technology solution that includes hardware (device, components), connectivity technology, platform and applications (software), often brought together with the help of a system integrator/technology consultancy.

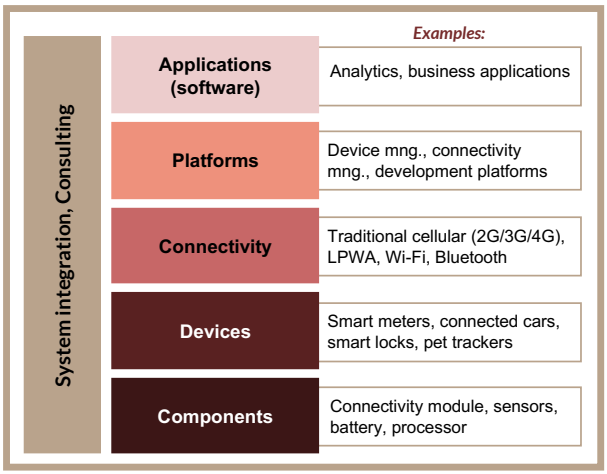

Figure 1. Main components of an end-to-end IoT solution

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

[1] IoT is hereby used as a term that includes all connected devices, both connected directly to the internet but also deployed in a closed network.

Copyright © 2018 Northstream AB

Every use case has specific characteristics and needs 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 example, enterprises may have products which are:

- Simple sensors that deliver small amounts of non-sensitive data with low requirements for security, but need for low cost to deploy and manage a large number of devices in close proximity;
- (Part of) sophisticated machines that need to report data and be monitored, upgraded and maintained remotely, with the need for high level of security and to be future-proof for 5-10 years, while potentially operating in places hard to access.

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.

1.2 THE IMPORTANCE OF CHOOSING THE RIGHT CONNECTIVITY TECHNOLOGY

Selecting the right connectivity technology (and vendor) can impact the outcome both in the short and long-term and therefore 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 number increases or necessitate an expensive swap if the technology does not prove sufficiently futureproof to support the long lifecycles of some products.

There are currently a range of technologies available for IoT based on both licensed and unlicensed spectrum, and respectively actors that are aiming to build their market dominance and a strong ecosystem. The current fragmentation is not viable for the industry in the long-run. We believe that certain connectivity technologies (or players) will emerge as leaders in their category, however, no single technology or solution is ideally suited to serve all potential IoT use cases. A number of technologies (and vendors) will 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. ■

Copyright © 2018 Northstream AB

2. Connectivity technologies for IoT

Traditionally, the IoT landscape or rather the machine-to-machine (M2M) communication has been dominated by radio technologies such as ZigBee, Bluetooth and Wi-Fi for **short range** local area networks, and **traditional cellular** such as GSM (2G), UMTS (3G), and LTE (4G) for wide area networks. In the near future 5G will be also added to the latter. Many of these technologies, especially Wi-Fi and 2G/3G/4G were originally designed for consumer and business voice and data services.

A number of new radio technologies have emerged recently to connect things that were too expensive or too remote to be connected previously. These newcomers characterized by their low power consumption and wide coverage are generally known as Low Power Wide Area (LPWA) technologies. We divide them into two main categories. The first one is **proprietary LPWA** such as Sigfox, LoRa, Ingenu, which operate on unlicensed spectrum; they are typically deployed by non-telecom actors but can be also deployed by telecom operators. The second one is 3GPP[2] standardized LPWA (for simplicity often referred to as "**cellular LPWA**") such as NB-IoT and LTE-M, which are operator managed networks and operate on licensed spectrum. These technologies were specifically developed to provide a cellular option that addresses the needs of IoT; they were standardized in 2016 and deployments started in 2017.

To choose the right option for a specific IoT application when facing such a diverse selection of technologies, requires understanding of technology from many different aspects. 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.

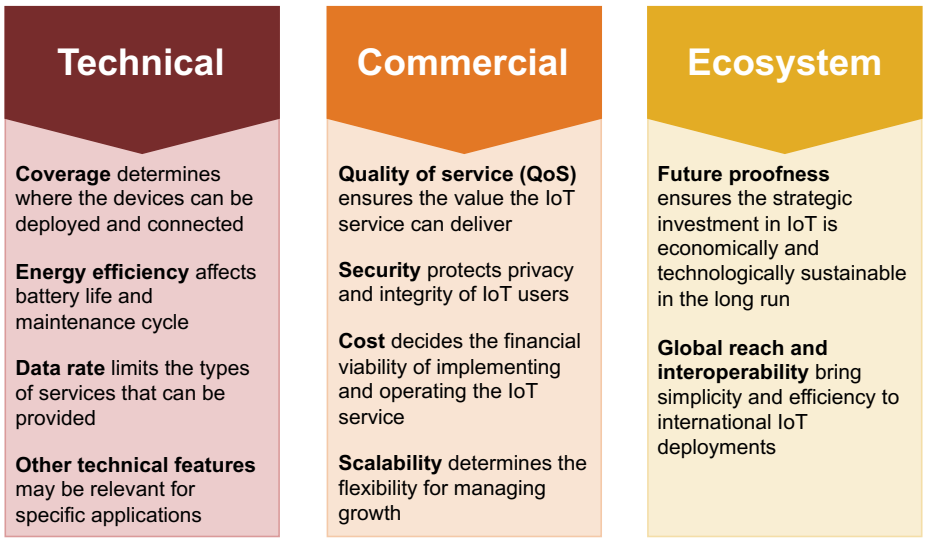

Figure 2: Connectivity technology requirements

[2] 3GPP is the industry group specifying wireless networking standards.

Copyright © 2018 Northstream AB

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 they are conflicting objectives that every radio technology has to make tradeoffs with.

Coverage

All IoT applications need good coverage to connect the 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, is a typical example of wide area solution with excellent coverage 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 signaling protocol and reducing the amount of overhead to the bare minimum, thus allowing longer battery life.

Data rate

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.

Wi-Fi and cellular networks 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 short range. In contrast, most LPWA technologies have much lower data rate and lower energy consumption as they employ more robust modulation scheme and run on commodity-priced micro-controllers with limited bandwidth.

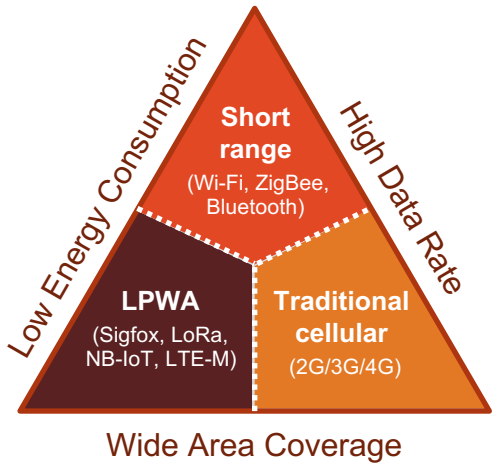

Figure 3: Design constraints on the technical level

As illustrated in Figure 3, traditional cellular technology emphasizes on data rate and range with complex designs optimized 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, including NB-IoT, sacrifice data rate for superior battery life and coverage.

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.

Bidirectional communication – for some applications it is sufficient to have only unidirectional communication (uplink only) for the end device to report data to an access point or a gateway. A bidirectional link, however, is necessary for the end device to receive data from the access point. This can improve the reliability of data transfers through handshaking and security through authentication exchanges. Most of the technologies discussed here support bidirectional communication but some such as Sigfox in our view have inadequate downlink bandwidth to support features like over-the-air-software updates.

Copyright © 2018 Northstream AB

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.

Localization – 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 localization 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 localization capability as the algorithm is getting more sophisticated.

COMMERCIAL REQUIREMENTS

Understanding the technical requirements is only the first step in selecting the most suitable IoT connectivity technology. Depending on the IoT business model, tradeoffs often must be made among quality of service, cost and scalability, which impact the commercial aspect of the enterprise's product or service.

Quality of Service (QoS)

The QoS requirement can vary significantly for different IoT applications, ranging from delay-tolerant metering applications to mission-critical remote control systems that require both high reliability and low latency. While there are connectivity suppliers for almost every technology who can provide operational support with certain degrees of QoS assurance, typically solutions that are enabled by licensed spectrum can provide higher degrees of QoS. In cellular networks, SLAs are commonly used as the tool by major actors to guarantee certain levels of quality 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 QoS assurance as they are subject to potential interferences from other uncoordinated technologies and networks. Regulatory requirements can in some cases (for example, utilities) also mandate certain SLAs that can impact the choice of connectivity technology.

Security

With respect to security for IoT applications, better security in connectivity typically requires more processing power for data encryption/decryption and identification/authentication. This processing comes along with yet another concern that is the size of overhead data associated with IoT information. Many proprietary LPWA technologies provide only rudimentary security as they are limited by the simplicity of device and protocol. Cellular networks rely on Subscriber Identify Modules (SIM) as the basis for the authentication, security, and privacy mechanisms. Wi-Fi and Bluetooth Low Energy (BLE) also have employed advanced encryption mechanisms. In more advanced applications, security is also done in the higher levels of the technology stack, however that can drive further overhead.

Cost

The cost for IoT connectivity technology is comprised of the connectivity module cost and the connection 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 sub-$5 LPWA modules to more expensive LTE modules due to their more pricey hardware and IP royalties. It is expected that the price of the latter has potential for further reduction as the deployment volume increases.

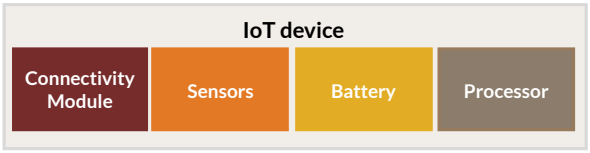

Figure 4: Main cost components of an IoT device

The connection cost can be the subscription cost if connectivity is provided by a network operator, or the network cost if the enterprise owns its private network. In either case, the connection cost is ultimately driven by the cost for deploying, operating and maintaining the IoT network, and understanding those cost drivers is useful since the cost will directly or indirectly need to be paid by the enterprise.

Short range networks like Wi-Fi have low cost per access point, but they require dense deployment, fixed broadband access, configuration and maintenance that drive up the cost for providing a wider coverage. Proprietary LPWA networks in contrast may require the least investment for providing a national coverage 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. Traditional cellular networks have in most places excellent existing coverage and cellular LPWA can be implemented on top with only marginal cost. While telecom operators can charge a premium for better QoS of their cellular LPWA networks (compared to proprietary LPWA), LPWA technologies in general have a lower total cost than traditional cellular options. However, the cost of traditional cellular connectivity has been decreasing during the past years, specifically in the EU, boosting high-data use case cases such as connected cars.

Copyright © 2018 Northstream AB

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 large volume with sustained growth. Centralized 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 impose restriction on their scalability in the long run.

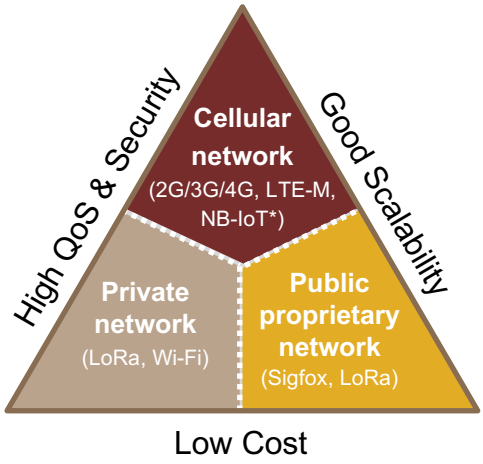

Figure 5: Trade-offs on the commercial level

As illustrated in Figure 5, cellular networks have the necessary scale and capability for delivering high QoS, security and scalability but will typically charge a premium (*LPWA networks such as NB-IoT and LTE-M, however, have a lower price point than traditional 2G/3G/4G). On the other hand, proprietary LPWA networks that are deployed as public network, such as Sigfox, can offer cost-effective and scalable solutions but with limited QoS. Enterprises can directly purchase capacity from these 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 customized private network. Deploying a private network by either the enterprise itself or a system integrator could be a cost efficient solution to meet specific requirements and provide more control of the network, but it is difficult to scale up and replicate globally.

ECOSYSTEM REQUIREMENTS

Future proofness

The future proofness of a technology encompasses longevity to assure its availability in the future, as well as long-term economic viability, derived from long-term cost reduction potential.

Technology longevity is a crucial consideration for IoT applications with logistical and cost challenges for replacing deployed devices. Understanding the strategic intention of key stakeholders backing the technology can help predict future direction of its development. For instance, Ingenu and Sigfox are companies funded by venture capital, whose commitment and ability to provide long-term service continuity are yet to be time tested. Furthermore, an open standard approach adopted by the likes of LoRa promises a better sustainability than technologies with closed systems. The latter poses a risk for single point of failure while the former creates 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 industry-wide cooperation but also promotes heavy competition in the commercialization among numerous vendors and service providers. Proprietary LPWA technologies had an earlier commercial launch than cellular LPWA solutions NB-IoT and LTE-M, but their ecosystems are still developing. Telecom operators have been hedging on different LPWA technologies to meet the short-term market demand. Fragmentation will continue until some technologies emerge as more dominant, regional differences will likely also appear as a result of government stimulus and endorsement from specific service providers.

Global reach and interoperability

Global companies need global solutions in order to achieve economies of scale and avoid having different technologies and network operators for each single market, but also because 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 a market of larger volume and global competition, both of which help to drive the cost down.

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

Many proprietary LPWA technologies have a stronger regional presence in either the U.S. or Europe. They often have to make a trade-off between global reach and interoperability. An open

Copyright © 2018 Northstream AB

standard approach, as in the case of LoRa, creates a vibrant ecosystem encouraging innovation and wide adoption globally, but it leaves too much room for proprietary variants that will not be able to communicate to each other. On the other end of the spectrum, a closed standard approach as in the case of Sigfox ensures the interoperability but restricts the ecosystem scale and reach. Another challenge faced by emerging LPWA technologies is the fragmented regional regulations in sub-1GHz unlicensed spectrum – low-cost devices and simple protocols might not be capable of detecting and adhering to the appropriate regional requirements.

The cellular industry has created global standards and cellular networks currently offer the best global reach. Adding to that, NB-IoT and LTE-M are being deployed by international operators in harmonized cellular band to offer global reach.

2.2 CELLULAR LPWA TECHNOLOGIES (NB-IOT, LTE-M)

Cellular LPWA technologies have presented new opportunities to address emerging use cases and deserve some special attention. Since the specifications for the cellular alternatives NB-IoT and LTE-M were first released in 2016, the number of networks and connections has grown at a steady rate. In mid-2018, there were over 50 commercial NB-IoT and LTE-M networks launched[3] and many operators are planning for upcoming deployments. In fact, the launch of cellular LPWA technologies fits naturally to operators' ongoing network modernization process, as these IoT features can be activated with little to no cost once the network is being upgraded with equipment of recent generation.

Over the past couple of years, most mobile network operators have tended to choose deploying one of these technologies and some regional trends have emerged – the major North American operators AT&T and Verizon opted to start with LTE-M; while Asia, in particular China, has been focused on NB-IoT. In Europe, the landscape has been somewhat mixed – large operators such as Vodafone and Deutsche Telekom have backed NB-IoT for their initial deployments, however LTE-M has been also gaining footprint with launches by Orange, KPN and Telenor.

These early regional differences do not mean that enterprises need to choose one technology over the other – both NB-IoT and LTE-M are on the path towards global footprint and most operators will be deploying both technologies in parallel from 2019. Therefore, enterprises will be able to choose depending on the needs of their use cases.

While NB-IoT and LTE-M are both designed to address LPWA use cases and serve the same overall market, there are some differences, and each performs better in specific use cases. LTE-M has higher data speeds – maximum uplink and downlink data rate of 1 Mbps, while NB-IoT reaches only about 200 Kbps for the downlink and 20 Kbps for the uplink. LTE-M also has lower latency – between 15 and 20 milliseconds, compared to 1.6 to 10 seconds for NB-IoT, which makes it the only one of the two appropriate for real-time applications. Another important consideration and difference is that LTE-M has support for voice functionality via Voice-over-LTE (VoLTE) and therefore can be used for applications that require some human interaction, such as certain connected health, alarms and security, and automotive applications. LTE-M has also better support for mobility because it manages the hand-over between cell towers much like LTE. For example, when a vehicle moves between two points and is crossing several different network cells, a LTE-M device would have smooth handover and would not drop the connection, while an NB-IoT device joins a single base station and would have to re-establish a new connection after reaching a new network cell. In general, LTE-M is very well suited for applications within transportation, logistics, home security, connected health, smart grid, wearables, industrial asset management.

NB-IoT on the other hand excels in other areas – it has long range, offers excellent penetration in underground and indoor settings and can support longer battery life (in excess of 10 years). 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. For example, NB-IoT is optimal for remote environmental sensors that need to send regular updates from a fixed location while optimizing battery life.

The device cost is also an important consideration for enterprises – NB-IoT and LTE-M modules have been more expensive than respective modules for proprietary LPWA technologies due to their later launch but are coming down in price. There is also an expectation in the industry that China will play an important role in driving down the cost of chipsets and modules for NB-IoT due to ambitious plans for massive-scale deployment. The Chinese government has set a goal to connect 600 million devices to NB-IoT networks by 2020. It is also important to note that the subscription cost for cellular LPWA is lower than for traditional cellular technologies (such as 2G/3G/4G), which makes them an attractive option for addressing the needs of use cases with a very sensitive business case.

Roaming capability on cellular LPWA networks is also an important consideration, especially for use cases such as logistics tracking, which may involve containers crossing multiple national borders. The number of spectrum bands and protocols a particular device needs to support affects its cost. Therefore, cooperation between mobile network operators to align on the deployment architecture and the spectrum bands for deploying LPWA networks, is important. Industry bodies such as the GSMA are working to deliver guidance and facilitate standardization work. In mid-2018, the first

[3] Source: GSMA

Copyright © 2018 Northstream AB

international roaming trial in Europe using licensed NB-IoT technology was successfully completed, which paves the way for delivering international coverage and service continuity.

Historically, many IoT applications have been using 2G connectivity technology as 2G networks have been widely available, have a mature ecosystem and can support voice. However, as a new generation of mobile technology, 5G, is coming up on the horizon, mobile operators are facing the need to reduce complexity in managing their networks and free up spectrum and resources. Therefore, many operators are planning the sunset of their 2G and 3G networks in the next 5-10 years. For example in Europe, Telenor Norway has announced plans to shut down their 3G network in 2020 and 2G network in 2025; T-Mobile Netherlands is working on shutting down their 2G network by 2020; some operators in Asia (e.g. in Singapore, Taiwan, Japan) and US (e.g. AT&T) have already even shut down 2G networks. Enterprises may wonder which one among the cellular technologies would then be the most natural choice instead of 2G/3G. For enterprises that want to connect their products today using cellular and need a technology with longevity of at least 10 years, NB-IoT and LTE-M would likely be the best alternative. LTE-M, in particular is a good candidate to replace 2G/3G in many automotive use cases (such as fleet management, vehicle telematics) thanks to its support for voice and mobility. Connected cars are also increasingly adopting LTE to support infotainment services requiring high bandwidth.

2.3 ASSESSMENT OF LEADING CONNECTIVITY TECHNOLOGIES

While there is no single technology that can best serve all use cases, only few connectivity technologies can emerge as the dominant options in each category. For IoT deployments in remote/wide areas, LoRa and NB-IoT/LTE-M are good complements to each other and together will address a large share of this market. LoRa's dynamic open ecosystem is ideal for private networks with customized deployment, while NB-IoT is backed by major mobile operators offering standardized connectivity with global reach. Other proprietary technologies, like Sigfox, may address certain niche segments but with uncertain future proofness. For applications requiring high data rate, the most promising technology options are either LTE or Wi-Fi, depending on the scope of the IoT deployments. For local short-range applications, the choice of connectivity technology is less obvious and often the interfaces and implementation of platform and application layers become more crucial.

The key strengths and weaknesses of the three main types of technologies – traditional cellular, LPWA and short range – are summarized in Figure 6. Table 1 compares a number of the leading IoT connectivity technologies from the perspective of the different considerations discussed in the previous section. ■

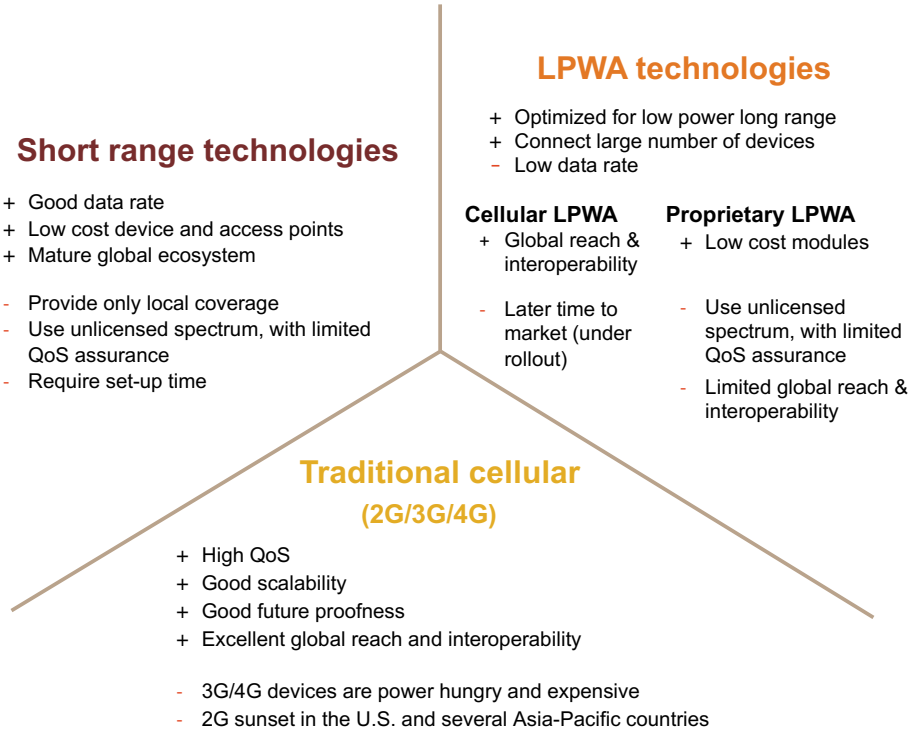

Figure 6. Key strengths and weaknesses of different types of connectivity technologies

Copyright © 2018 Northstream AB

Considerations	Traditional Cellular			Cellular LPWA		Proprietary LPWA			Short Range		
	2G	3G	4G	LTE-M	NB-IoT	SigFox	LoRa	Ingenu	Wi-Fi low power	ZigBee 3.0	Bluetooth LE
Outdoor coverage	>10km	>10km	>10km	>10km	>15km	>15km	>10km	>15km	<1km	<300m	<100m
Indoor coverage	High	Medium	Medium	Medium	High	High	High	Very low	Very high	Medium	Low
Energy efficiency	2-5 years	<10 days	<10 days	>10 years	>10 years	10-20 years	10-20 years	10-20 years	6-12 months	6-12 months	6-12 months
Typical uplink data rate	50 kbps	1 Mbps	10 Mbps	1 Mbps	20 kbps	100 bps	25 kbps	50 kbps	1 Mbps	250 kbps	1 Mbps
Bidirectional communication	Yes	Yes	Yes	Yes	Yes	Limited downlink	Yes in Class A	Yes	Yes	Yes	Yes
Mobility	Very high	Very high	Very high	Very high	High	Very low	Low	Medium	Medium	Low	Very low
Localization	Yes	Yes	Yes	Yes	n/a	No	Limited accuracy	n/a	Yes	Yes	yes
QoS & security	Very high	Very high	Very high	Very high	High	Very low	Low	Low	Medium	Medium	Medium
Connectivity cost	Medium	High	Very high	High	Medium	Very Low	Low	Low	Medium	Medium	Medium
Scalability	High	High	High	High	Very high	High	High	High	Low	Low	Very low
Future proofness	Medium	Medium	Very high	High	Very high	Low	High	Low	Medium	High	High
Global reach & interoperability	Very high	Very high	Very high	High	High	Medium	Low	Very low	Low	Medium	High

Table 1. Main technologies for IoT[4]

[4] The data points in this table are collected from official reference sources, including 3GPP standards for cellular technologies, company websites for proprietary LPWA technologies, IEEE 802 standards for Wi-Fi, ZigBee and Bluetooth. "n/a" is used in the table where official information was not available.

Copyright © 2018 Northstream AB

3. Application areas and technology mapping

This section discusses the needs of some example application areas with respect to the technical, commercial and ecosystem requirements introduced in the previous section to illustrate how these needs determine the choice of connectivity technology for each area (or use case within). A summary is provided in Table 2.

An application area is usually not homogenous and there can be differences in development stage across markets. As a result the discussion on needs may differ to some extent. Markets that are new to IoT have the advantage of being able to learn from best practices in more developed regions and benefit especially from partners that provide both technology and experience. Developing markets typically start with the more basic applications and therefore may not have as high initial requirements but can develop fast to more advanced applications.

Application area	Technical requirements							Commercial requirements			Ecosystem requirements		Suitable connectivity technologies
	Indoor coverage	Wide area coverage	Energy efficiency	High data rate	Bidirectional comm.	Mobility	Localization	QoS & security	Low cost	Scalability	Future proofness	Global reach & interoperability	
Automotive	L	H	L	H	H	H	M	H	L	H	H	H	Cellular
Smart cities	L M	M	H	L	L M	L	L	L	H	H	M	L	LPWA, Wi-Fi
Safety and security	H	M	L	L H	H	L	L	H	L	M	M	L	Cellular, LPWA
Industrial manufacturing	H	L	L	M	M H	L	L	H	M	L M	M H	L	Wi-Fi, Cellular
Fleet and logistics	M	H	L	L	L	H	H	M	L M	M	M	H	Cellular, LPWA
Asset management	H	H	L	L	L M	L	M	L	M	L	H	H	Cellular, LPWA
Agriculture and environment	L	H	H	L	L	L	L	L	H	H	M	L	LPWA
Smart meters	H	H	H	L	M	L	L	L	M	M H	H	L	Cellular, LPWA
Wearables	H	L	L	L	L M	L	L	M	H	L	L	L	Bluetooth, ZigBee

L = Low, M = Medium, H = High

Table 2. Application areas, typical requirements and suitable connectivity technologies

Copyright © 2018 Northstream AB

AUTOMOTIVE

The connected car provides vehicle owners and car manufacturers with great amounts of data about driving behavior, car performance, need for maintenance and more. The connected car market is set for fast growth in the next decade, as in-vehicle wireless connectivity is rapidly expanding from luxury brands and models to the mid-market segment and onwards. Gartner Research has forecast that about one in five vehicles on the road worldwide will have some form of wireless network connection by 2020, amounting to more than 250 million connected vehicles in service.

For a connected car with embedded connectivity (where both the connectivity and intelligence are built directly into the vehicle), there is a wide range of requirements that have determined cellular as the most suitable technology. To begin with, a key feature of vehicles is mobility, which translates into the need for reliable coverage while in motion and regardless of location – both national coverage in urban and rural areas, as well as global reach (roaming capability) to provide continuous connectivity when driving across borders.

Connected cars have a need for high QoS – both in terms of reliability of the network to ensure the faultless operation of features such as voice calls, remote access to car functions, real-time navigation, automatic crash notification and roadside assistance. In addition, security is a major consideration given the nature of personal data collected and strict safety requirements. Connected cars have also demands for high data rate in order to support infotainment services for streaming of music and video. Such services offered by third-party service providers are proliferating and driving the need for higher data rate.

From a technology ecosystem perspective, another major requirement is longevity – the product development cycles for new vehicles can be three to five years, followed by a lifespan of seven to ten years. These long lifecycles mean that it is necessary to rely on a connectivity technology and solutions that have long-term commitment by technology vendors and operators and support over the air software updates. With the GSMA embedded SIM Specification, automakers are able to remotely provision connectivity over the air to vehicles with an operator of their choice and connect vehicles with local operators, regardless of where the cars are manufactured.

Currently, only cellular technology can fulfill all the above-mentioned key requirements, which is why connected cars rely on cellular networks (2G/3G/4G) and will continue to do so for the foreseeable future. Generation shifts within cellular will present new opportunities. 5G networks, which will become commercially available from around 2020, will offer a range of benefits including higher speed and lower latency and will play a role in enabling autonomous vehicles and vehicle-to-everything (V2X) communication.

The evolution of mobile network technology will also impact eCall. Since April 2018, all new cars sold in the European Union are required to have the emergency call system, eCall, which automatically dials the emergency services' 112 number after an accident. The current eCall is based on circuit switched emergency call in 2G and 3G networks. However, there is no circuit switched calling in packet-switched (i.e. IP-based) networks like 4G LTE and 5G. One can use Circuit Switched FallBack (CSFB) – a protocol whereby voice and SMS services are delivered to LTE devices through the use of 2G (GSM) or another circuit-switched network. However, as operators are preparing for the advent of 5G, many are planning the sunset of their 2G and/or 3G networks. Therefore, the intention is that the Next Generation eCall architecture will use Internet Multimedia System (IMS) emergency calling in 4G networks, which will also bring expanded capabilities to transfer video. The full deployment of the Next Generation eCall may take 5-10 years and that combined with the long lifespan of cars means that the issue of how eCall migration will be managed requires planning and close cooperation between standardization bodies, operators and automakers. Regulatory requirements will also play a role and impact the choice of solution used in different countries.

SMART CITIES

The objective of smart cities is to improve the quality of life and public services, traffic and safety as well as conserve limited resources and monitor the condition of vital infrastructure. Therefore, there is a wide variety of use cases within this area, some of the most discussed being smart parking, waste management, street lighting, noise monitoring and many more.

What many of these use cases have in common are the key needs for good coverage in urban areas, long battery life (10+ years) and low cost of the solution and connectivity, which can enable cities to justify the investment of public funds. In addition, although each of the connected devices may be sending small amounts of data, the magnitude of smart cities means that tens of thousands of devices may be connecting to a single access point/ base station and will need to often transmit data simultaneously, thus placing demands for network scalability, especially as new devices are constantly added.

The combination of above requirements is best satisfied by LPWA technologies. Proprietary LPWA technologies such as LoRa and Sigfox have had the advantage of an earlier commercial launch and are offering good cost efficiency. Since these proprietary technologies are using unlicensed spectrum, they may face some potential scalability challenges in the long run as more networks and billions of devices are deployed using the same unlicensed band, but in the short to medium run, they are capable of meeting requirements. With the commercial launch of cellular LPWA technologies such as NB-IoT and LTE-M, the technology alternatives have expanded, as they bring comparable benefits plus the extra advantages of better quality of service, reliability and security, as well as better support for over-the-air (OTA) firmware upgrades. The latter is a very important capability to ensure that devices with long lifetimes remain secure and relevant.

Wi-Fi networks are another suitable alternative, especially for use cases like smart parking, which entail connecting sensors within an indoor parking garage.

Copyright © 2018 Northstream AB

ASSET MANAGEMENT

Connected assets offer benefits both to the businesses that own them and the businesses that manufacture them. In this application area we include a wide range of mostly fixed assets – water pumps, vending machines, elevators, ice cream machines, lawn mowers and similar. If companies have better insights into how their assets are working, they can improve efficiency and avoid downtime through predictive rather than reactive maintenance. If businesses that manufacture such assets can receive data on how their products are used, they can offer better service and maintenance, supply spare parts faster, develop new (value added) services or even entirely transform business models (e.g. from product to as-a-service).

Most of these assets are used indoors and can often be in dispersed locations in urban areas (e.g. vending machines) but also in rural areas (e.g. water pumps). Therefore, they have the need for reliable (indoor) coverage at low cost. For many businesses global reach is also needed so that a single type of device can fit each machine produced to be sold anywhere in the world. Assets would send small amounts of data more or less frequently, but high data rate is not a requirement. Depending on the type of asset, quality of service guaranteed by SLAs can be important. Cellular networks such as 2G offer good coverage and telecom operators can provide global reach. LPWA networks can also serve many use cases in this application area, especially when cost is a deciding factor, thus allowing to connect even assets of lesser value.

CASE STUDY: CARPIGIANI GROUP

This case study is provided by Telenor Connexion

About the company and its IoT challenges

Carpigiani is a market-leader in the production of machines for gourmet gelato, better known as Italian-style ice cream. Carpigiani was founded in 1946 by the Carpigiani brothers, and quickly established itself as the market leader in the production of machines for gourmet gelato. During the 1960s and 1970s, Carpigiani began to expand globally.

The Italy-based company manufactures over 10,000 ice cream machines per year, of which over 80% are being exported around the world. Customers span from small ice cream shops to large global fast-food brands and the installed base of machines exceeds hundreds of thousands.

The company was early in seeing the benefits of connecting its products and started the process in the late 90's.

Main reasons for being connected

- **Cut cost of aftermarket service within the warranty period.**
- **Long lifespan of machines calls for an efficient way to do upgrades and maintenance.**
  By monitoring the lifecycle of the machine based on actual use, not time, customers reduce the risk of downtime. The system schedules the substitution of critical parts only when necessary and based on the quantity of ice cream produced.
- **Increase the efficiency of machines.**
  Connectivity enabled the company to offer a remote monitoring system, Teorema, by which the efficiency of each machine is improved. The data generated is used to comprehensively examine the state of the equipment and to provide the customer with a diverse range of service options, including predictive maintenance and cost reductions such as decreased downtime, less waste, compliance with hygiene & safety regulation, energy savings.
- **Allow to perform field tests for improvement and new machines.**

All the above became especially important when the company started to expand worldwide with machines installed in many countries.

Key connectivity needs and technology choice

The first steps of the project were undertaken in the late '90s, when only few technologies were available. Carpigiani started with the powerline technology, but faced challenges such as difficulties to access firewalls where the machines were installed.

The company then switched to cellular technology and the first big deployment of the system took place in early 2008. At first the connectivity was provided via a local network provider, but when the company started expanding out of Italy it was no longer possible to work with a local operator. At that time (2010) the cooperation with Telenor Connexion started.

The machines were not mobile and only needed to transmit small data volumes. Therefore, the critical requirements on connectivity were:

- Global reach and standard connectivity
- Reliability and accessibility

Carpigiani tried several different technologies but cellular technology has proven most suitable to meet the company's requirements.

Copyright © 2018 Northstream AB

INDUSTRIAL MANUFACTURING

Industry 4.0 is a collective term that in recent years has come to signify the transformation that IoT brings to the world of industrial production. Sensor technology and connectivity make it possible to create smart factories in which machines can connect and self-organize, optimizing the production process based on real-time data. Smart factories can even be connected into one production network to form a global factory. Companies such as ABB and Harley Davidson have already reaped benefits from transforming their manufacturing process through IoT.

Industrial manufacturing use cases need connectivity that offers good indoor coverage, often in industrial regions, and high reliability since every interruption of service can be very costly. In addition, many of the machines are in close proximity to each other and multiple sensors send frequently data, thus requiring high bandwidth at low cost. In many factories, there are old machines that were not initially designed to be connected and thus need to be retrofitted with sensors and connectivity, which means that the network fabric must be adaptable to a mix of both legacy and new machines and be able to scale up easily as new machines are being connected.

Wi-Fi networks have a lot of advantages in meeting the needs above, offering good indoor coverage and high capacity at low connectivity cost (after the initial investment in setting-up the network). It is also relatively easy to retrofit legacy machines with sensor nodes with Wi-Fi connectivity. Cellular technologies such as 2G/GPRS 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.

FLEET MANAGEMENT AND LOGISTICS

This application area includes a variety of use cases for tracking and management of moving assets – trucks, shipping containers, construction equipment vehicles etc. Connected solutions in fleet management allow to monitor vehicle location, optimize route planning, perform remote vehicle diagnostics and analyze driving behavior. The resulting benefits are that businesses can improve operations and delivery time, prevent theft and save fuel.

The main connectivity requirements for this type of solutions are about reliable coverage – both in urban and rural areas as well as global reach (roaming capability) to provide continuous connectivity when assets travel across countries. Other requirements include also localization capability for tracking location, quality of service to ensure that assets do not “go dark”, and longevity of the technology as some of the assets (like vehicles) have production and life cycles spanning over a decade. The latter also means that the devices have SIMs and modules that are future proof and support bidirectional communication for over-the-air updates to avoid the need for costly swapping out in the field.

Typically, cellular networks, especially 2G/GPRS have been best suited and most commonly used for tracking large moving assets. As network operators are increasingly shifting traffic to their 3G and 4G networks (and some operators even plan to shut down their 2G networks), the faster networks offer expanded benefits that can enable new services – such as video streaming, new productivity tools etc.

Apart from the large assets, there is a whole category of lower value assets like packages, luggage and other items that are to a great extent still unconnected and tracked only by scanning bar codes. LPWA networks can make it economically feasible to track such a large number of widely dispersed objects through sensors that can send location and other status updates. LPWA networks can also be suitable for creating sophisticated integrated solutions that serve large docksides and warehouses.

WEARABLES

This consumer application area includes devices attached to the human body (also called wearables), such as smart watches, connected shoes and clothing, fitness and healthcare devices. Their purpose is to measure and collect data on human activity – exercise, sleep, heart rate, blood pressure and many more in order to improve wellness, health and productivity.

What these devices have in common is that their use is tightly connected to the use of a smartphone, which is already wirelessly connected, as well as the need to work out of the box and at virtually no extra cost since consumers do not appear willing to pay for separate connectivity for their wearables. Therefore, for a majority of these devices Bluetooth is a natural choice since it provides the necessary short-range connectivity at no cost.

SMART METERS

Smart meters are used in electricity, water and gas. Smart electricity meters in particular require frequent communication. This has been the most developed use case to date, because it offers good cost savings and since electricity meters have access to continuous power supply battery life is not an issue. For electricity meter deployments traditional cellular technology has been widely used, meeting well the requirements for coverage, reliability and longevity of the technology (meters can have a lifespan of up to 15 years). With the advent of LPWA options, NB-IoT and class-C LoRa (which has the lowest latency among all the LoRa class end devices) can be used. For smart grid applications that have higher requirements for latency and speed (to enable real-time grid monitoring), LTE-M is a good fit.

Water and gas meters on the other hand are often located underground and in more inaccessible places (e.g. sensors placed in sewers), without access to electricity supply and thus requiring very long battery life. These use cases are hard to address with traditional cellular systems but LPWA solves both of the above challenges. NB-IoT technology is very suitable for water-metering applications, which have some of the most extreme coverage requirements underground.

Copyright © 2018 Northstream AB

CASE STUDY: INTELLIGENT SHIPPING CONTAINERS
This case study is provided by Telenor Connexion

About the company and its IoT challenges

China International Marine Containers (Group) Ltd. (CIMC) is one of the world's largest makers of shipping containers. In order to find new solutions to long-standing problems in shipping and logistics, CIMC established its CIMC Hitech subsidiary to develop and deploy intelligent technologies to be integrated into the parent company's products.

Shipping containers with sensors and tracking devices can be tracked anywhere in the world, as can the status of their contents. With these connected solutions, CIMC Hitech is helping their customers simplify processes and lower operational costs.

Main reasons for being connected

- Enable global traceability of shipping containers and their contents
- Lead shipping and logistics into Industry 4.0
- Differentiate in a highly consolidated vertical
- Provide connected solutions that boost efficiency and decrease costs

Key connectivity needs and technology choice

In order for CIMC's containers to transmit data in near-real time, they need to be constantly connected, on sea and on land. That means the only viable choice is to connect over mobile (cellular) networks.

With lifecycles that span more than a decade, CIMC's shipping containers needed future-proof SIM cards and modules. This meant CIMC Hitech needed an IoT connectivity technology provider that could guarantee longevity, stability and reliability.

The critical requirements for the connectivity solution were:

- Global reach and standard connectivity
- Reliability and accessibility
- Future proof connectivity and device management

After evaluating several suppliers, CIMC Hitech chose Telenor Connexion Global Connectivity, using a single SIM card solution regardless of the country in which connectivity is needed. With help of AuEase, Telenor Connexion's partner in China, CIMC Hitech offers an end-to-end, one-stop, smart logistics solution to end customers. This CIMC Hitech solution covers business innovation, pre-sales technical support and product life cycle management.

Copyright © 2018 Northstream AB

SAFETY AND SECURITY

Connected safety and security includes a wide range of use cases ranging from video surveillance in both public setting and on private properties, security alarms to prevent intruders, as well as safety alarms to signal events such as fire, gas or water leakage.

These use cases can have varying requirements. 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 operation in real time. Security for the data transmission is often highly important, which entails the need for heavy processing for encryption and decryption of data. These requirements are very well served by cellular networks such as 4G LTE (but also 3G) that can provide a high rate of data transmission. Although LTE networks have high capacity, bandwidth consumption can be a challenge for LTE if a large number of cameras need to be served – this challenge though can be mitigated with careful system design for efficient scheduling, camera placement etc. Wi-Fi networks can be another technology option for supporting video surveillance applications and have the benefit of lower cost and ability to manage the high bandwidth requirements but have a disadvantage in terms of security as they are more vulnerable to hacking attacks.

Security and safety alarms send small amounts of data, often infrequently, but have requirements for high reliability, security, indoor coverage and low cost. Cellular 2G/GPRS networks fulfill these conditions and are typically used to provide wireless connection between the on-site control panel and the central monitoring station. The needs of safety and security alarms are also very well served by LPWA networks, especially if the alarms are used for buildings in remote areas. Sigfox has, for example, made deployments in home security, where they provide back-up connectivity to create a more robust system in case the building's primary broadband connection fails or the burglars use GSM jammers. NB-IoT and LTE-M can also serve very well the needs of safety and security alarms.

AGRICULTURE AND ENVIRONMENT

Sensors can be used in agriculture to monitor environmental conditions such as solar intensity, the temperature and humidity of soil and air, thus defining the optimum time and location for irrigation, fertilization etc., resulting in more efficient use of agricultural land and resources and improving the quality of produce. Another use case is tracking the location and health of domesticated and wild animals. Environmental agencies can also use sensors to monitor weather conditions.

What these use cases have in common is the need for coverage in rural/remote areas, low cost and ability to support devices that are geographically dispersed and send occasionally small amounts of data. For tracking livestock, reliable localization is also important. Once the devices are deployed across large remote areas, they are expected to need minimum maintenance and operate for long periods of time without access to power supply. Therefore, long battery life but also future-proofness of the technology are essential.

This area is one of the most suitable for LPWA technologies – Sigfox and LoRa in particular are best fit for this application. NB-IoT is also suitable in theory, however, many agricultural farms are remote and do not have LTE cellular coverage, which is a limiting factor for using NB-IoT in the near future.

Copyright © 2018 Northstream AB

4. Future outlook

As illustrated in the previous section, different application areas and use cases have different needs that determine the most suitable choice of technology. At the same time, these needs may change over time and new use cases will appear. Therefore, what the requirements of future IoT applications will be is not completely clear.

Using a single connectivity technology has advantages but some enterprises will face situations where multiple technologies need to be used in parallel, either because they serve different applications that are part of a larger system, or because they serve the same application but in different environments/geographies where network availability differs. In those cases, cloud platforms as the middle layer of integration can become an important means for navigating complexity and allowing to unify the data collected and present it through the same interface. This may mitigate certain future risks but can present other challenges as it entails considerable transformation and integration efforts. Therefore, the choice of connectivity technology still remains an important decision that can have long-lasting implications.

4.1 5G AND IOT

5G has been garnering increasing attention as the next generation of mobile technology. 5G will be at first very much focused on Enhanced Mobile Broadband (mainly for the consumer segment) as a primary application but will bring architectural changes and new features that give operators better flexibility to address the diverse requirements of future IoT applications. More specifically, 5G will support:

- Network slicing that creates 'private-like' networks for different IoT applications with separated billing and service provisions;
- Ultra-low latency (less than 1ms) high reliability communication for mission-critical applications;
- Multiple access technology coexistence that integrates devices deployed in different environments (for example in Wi-Fi, fixed line and cellular networks) into a unified network layer and thus allows to serve diverse use cases;
- Network support for massive increases in data traffic;
- Faster speeds – as high as 10Gbps.

With these technology improvements, 5G is designed to serve both what are referred to as "Massive" and "Critical Communications" IoT use cases. Massive IoT entails large numbers of low cost devices (usually sensors) that have an ultra-long battery life and transmit a small amount of data to the cloud – therefore, they require low bandwidth and are not latency critical. Typical application areas are agriculture, smart cities, utilities, logistics.

One of the common questions is 'how will the cellular LPWA networks (NB-IoT, LTE-M) relate to 5G in the future?' NB-IoT and LTE-M have been already designed to address most of the requirements that will apply to Massive IoT in the 5G context. NB-IoT and LTE-M are 3GPP standards that will fulfil the long-term 5G LPWA requirements and are **both set to coexist alongside other components of 5G**. The 3GPP has agreed that the LPWA use cases will continue to be addressed by evolving NB-IoT and LTE-M as part of the 5G specifications.[5] The 3GPP is also investigating options for the 5G core network to support NB-IoT and LTE-M radio access network. Therefore, enterprises looking to deploy LPWA use cases today and considering NB-IoT and/or LTE-M need not be worried about the longevity of these technologies and need not wait for the advent of 5G.

[5] GSMA, Mobile IoT in the 5G Future, 2018

Copyright © 2018 Northstream AB

Critical Communications use cases, on the other hand, have very stringent requirements for reliability and latency in order to enable real-time control and automation in various fields. Example application areas are in healthcare (remote surgery that allows a surgeon to use a VR headset and special glove to control a robot arm that would perform an operation in another location), autonomous cars (that can communicate with other cars and surrounding road infrastructure), industrial automation (remote control of heavy machinery and real-time factory monitoring). These types of applications will need the capabilities of 5G, however, these emerging use cases will need a number of years to mature. It is safe to predict that there will be also many new use cases, still to be identified, that will require 5G.

When will 5G be commercially available? The first phase of 5G standards were completed in mid-2018, which starts the roadmaps for commercialization of network equipment, chipsets and devices. Commercial devices can typically lag the standardization by 12-18 months, which means they are expected in late 2019. Therefore, 2018 and 2019 can be viewed as a "trial" phase for 5G, during which operators conduct trials and prepare their networks. Early commercial operations will start around 2020 primarily in hotspots in urban areas, and wider commercial adoption is expected from 2023 onwards. Different regions and countries will also have different timelines, with some Asian countries (such as Japan, South Korea, China) and the US being among the early adopters, while Europe is slightly behind.

In conclusion, 5G will certainly provide new opportunities within IoT but due to the deployment timeline, it will play a very limited role in the next 3 years. In the meantime, the latest cellular IoT technologies NB-IoT and LTE-M will continue their evolution and eventually become a pillar in future 5G networks. Therefore, enterprises that have identified specific IoT opportunities can proceed with the technologies available as they will remain relevant and coexist with 5G. ■

Copyright © 2018 Northstream AB

ABOUT THIS PAPER

This white paper was written by Northstream with the aim to provide an objective and independent view on IoT connectivity technologies.

While the white paper was commissioned by Telenor Connexion, all opinions expressed are entirely Northstream's and do not necessarily represent the opinions of Telenor Connexion.

ABOUT TELENOR CONNEXION

Telenor Connexion designs and operates Internet of Things (IoT) solutions. Building on almost 20 years of experience Telenor Connexion provides reliable IoT solutions to a number of global customers such as Volvo, Scania, Hitachi, Verisure Securitas Direct and Husqvarna. Headquarters and tech centre are located in Sweden and the company has regional offices in UK, Germany, US and Japan. Telenor Connexion is wholly owned by Telenor Group, one of the world's major mobile operators.

www.telenorconnexion.com

ABOUT NORTHSTREAM

Northstream is a boutique consulting firm dedicated to serve domestic and international clients. We have put our competence, passion and efforts at the intersection of business and mobile technologies, providing strategies handcrafted for each client's unique business and competitive dynamics. We are proud to say that we come highly recommended by many of the most successful players in the ecosystem of a connected world. We typically work with:

- Business strategy development and planning
- Technology and product assessment
- Strategic sourcing of systems and services
- Reorganization and transformation
- Market analysis and due diligence

Northstream was founded in 1998, and is fully owned and controlled by people active in the company.

www.northstream.se

Copyright © 2018 Northstream AB