

THE ULTIMATE GUIDE TO IOT



INDEX

Introduction	3
What you need to know about connectivity	4
01 Solution requirements	6
Mobility and access to power	7
Networks	12
Software	17
02 Price issues	19
Pay-per-unit or “pooled” data traffic	20
03 Examples of applications	22
Energy and electricity plants	23
Transport and logistics	23
Agriculture	24
Micromobility	24
Retail trade	25
The healthcare sector	25
Smart cities	26

INTRODUCTION



The opportunity

“The Internet of Things” (IoT) is well on its way to making cars, electricity meters, trackers, sensors, homes and even whole cities smarter. Numerous companies are already using IoT to create completely new solutions, or to upgrade existing products – and thus far we have only begun to scratch the surface of what this technology can do.

The challenge

If an IoT solution has problems with unreliable coverage, demanding administration or weak security, it doesn't matter if it is ten times better than your competitor's version. In the same way, there is no point having a system that features innovative AI which converts raw data into an excellent decision making basis if the solution does not feed reliable data into the system. Without a strong connection to the outside world, even the best IoT device has nothing to offer.

The solution

Choose an experienced connectivity provider with the right tools, the right expertise and the capacity to prepare an ideal, tailor-made solution that can help your IoT service take the world by storm.



What you need to know about connectivity

An IoT project consists of a huge number of choices, which can have a major impact on the end result; an IoT solution is never stronger than the weakest link in this chain of elements. It is therefore important to be familiar with all these elements so that you can avoid the common pitfalls on the journey from concept development to final, implemented solution.

In this document, we will be taking a look at the advantages and drawbacks of different aspects of connectivity for an IoT solution, different cost aspects you need to be aware of, and which benefits different software and administration tools can provide.

- **Solution requirements**
Access to power, connectivity, bandwidth and latency, for example
- **Networks**
Different types of SIM card, different networks, available protocols and properties of different networks
- **Software**
Secure integration with different cloud services, the importance of testing and development, requirements on administration tools
- **Price issues**
“Pooled” data traffic versus Pay-per-unit
- **Examples of applications**



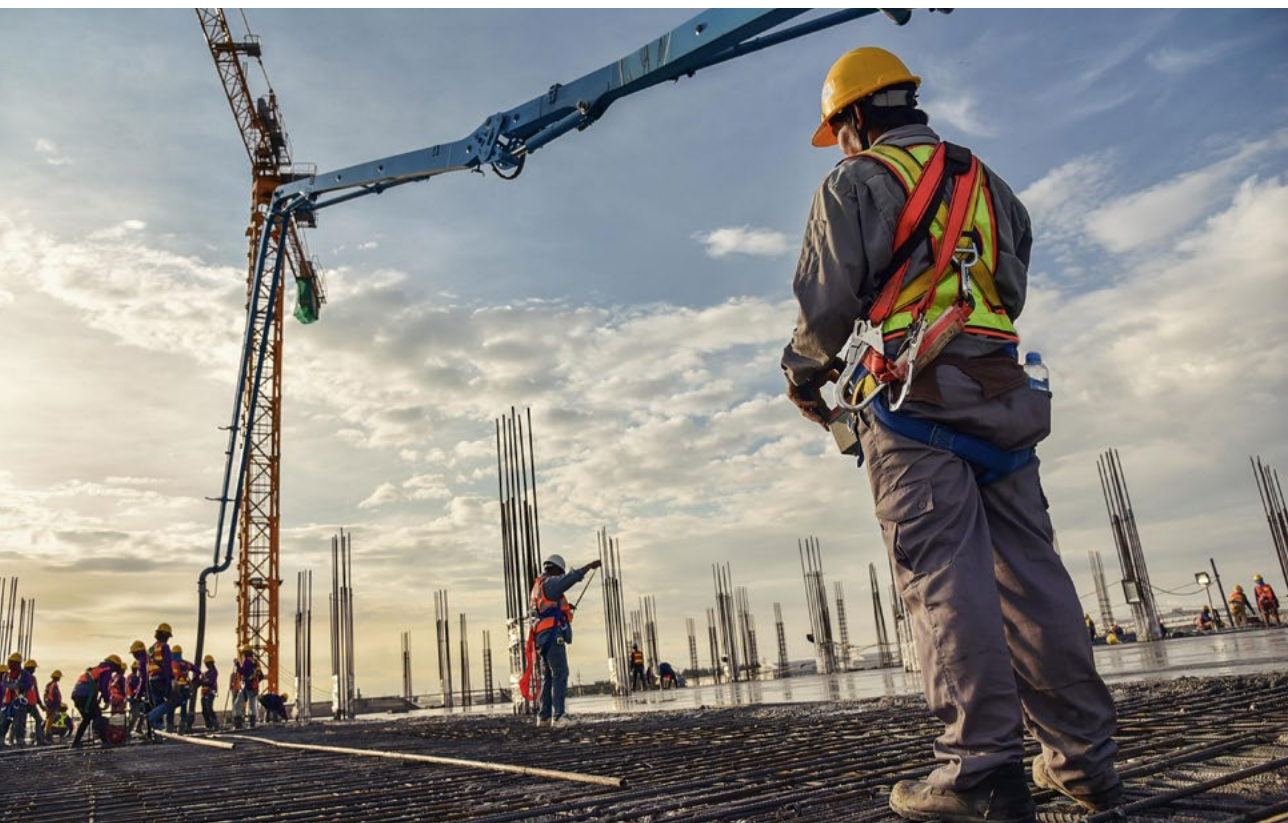
There are more
than **400 active IoT**
platforms worldwide

Source

01

SOLUTION REQUIREMENTS

IoT devices can deal with a range of problems and challenges, and every potential application has different requirements. In this chapter, we will look at some of these requirements and focus on how they can help determine which connectivity solution is best for you.



Mobility and access to power

Maintenance as you go

IoT projects often comprise a large number of devices that need to last a really long time, and which can be difficult to access once they have been positioned. IoT solutions can have a service life of at least a decade, so it is incredibly important to ensure that the devices feature a robust design, and that they are painstakingly tested in the field prior to large-scale roll-out.

It can be expensive to gamble on technologies that fail to catch on, and which therefore cease to be backed by support or are phased out entirely. This is one of many reasons why modern mobile network standards are a good, safe choice. It can be extremely expensive or difficult in practice if at some point you need to switch SIM cards in a device, and for elevated flexibility it is a good idea to choose devices that support rewritable SIM cards (eUICC).

These cards can be updated or changed “over the air”, which means you avoid the trap of becoming “locked into” a specific network provider.

Energy and power supply

A key issue has to do with where and how the IoT devices in the system are to be positioned. Should they be located in a place where it is easy to connect them to the power grid – like the smart energy meters we have all now had installed in our electricity panels at home?

Or could it be possible to connect them to the power grid so that they only need to draw minimal energy in order to ensure long battery life – like the parking sensors in the ground? Or, again, will the device be moved around a lot, thus requiring a regular, if low, supply of current, even though a power supply in and of itself may be readily available – like electric city scooters?

Connectivity and data traffic requirements

Another issue has to do with the demands the solution places on the device's data traffic: How much data will the device be transferring, and how high does the data speed need to be? What are the demands on uptime? And so on.

Bandwidth gives an indication of how much data a device can send and receive at the same time. For the vast majority of IoT applications, a couple of kilobits per second (kbps) is sufficient. A reading from a smart electricity meter, a position report from a driving log application, or instructions to an electric vehicle charger – all these require only the sporadic transfer of small volumes of data. If the application has to transfer speech, on the other hand, a bandwidth of around 100 kbps is essential.

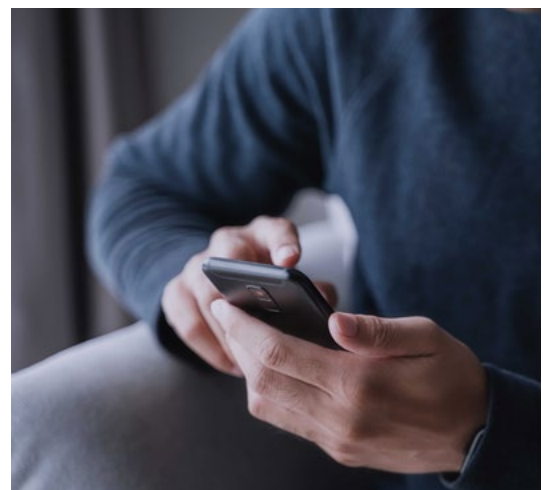
The bandwidth is also affected by the signal strength. For real time applications, it is essential that data can be transferred with minimal delay (latency) and without excessive variation (jitter). The 5G network can actually support applications that demand a delay of no higher than millisecond level, but most IoT applications can handle some degree of delay and jitter, depending on the application area and the protocols utilised.

The need for seamless mobility is a separate requirement. If your IoT device needs a continuous session/connection while it moves around between the coverage areas of different base stations, the unit must use technology such as LTE-M or 4G/5G. On the other hand, many IoT applications do not need this kind of continuous data session and can easily work with NB-IoT, for instance.

Uptime

Some solutions and application areas place stringent requirements on uptime and availability. Mobile data communication typically supports uptime of at least 99.9 per cent, and for solutions with even tougher demands, it is worth considering a solid option for back-up communication. An alternative may be to support multiple mobile technologies or to have access to other networks. Whatever you choose, you need a provider with a strong support set-up, and who provides ongoing, reliable information about possible error situations.

Minimising downtime is critical for suppliers of communication services. You will therefore need mobile platforms, preferably with duplex lines for power and fibre. Ideally, you would want the backbone of your system to have redundant data centres and a secondary backup location. In this way, your information will always be protected, even in the face of external influences such as water damage, fire or power outages.





A poor network connection can prove costly

A bad choice of network connection can make the difference between a successful product and a disastrous launch. The following example highlights the need to think carefully about the area of application – and to complete a solid, comprehensive pilot phase – before roll-out:

In order to boost efficiency, work smarter and care for the environment, a recycling company chose to launch a smart refuse container that automatically alerts the collection centre when it starts to fill up. The objective was to set the filling level for the containers, the time since they were last emptied, weather data and other factors as data points in an algorithm that could optimise the collection routes.

After a lengthy test period, the solution was rolled out city-wide, but then around ten per cent of the refuse containers surprisingly failed

to report their data as planned. It was then discovered that some households had placed their containers in their underground garages where 2G signals could not reach them. Nor was the operator able to offer satisfactory reporting for responsible troubleshooting. In this case, a solution based on NB-IoT would have been a much better choice, because it would have provided much better communication with the refuse containers – along with much longer battery life.

The example shows how important it is to choose a communication provider who specialises in IoT and therefore has the experience to highlight such possible problems early in the project. The provider must also have tools that make it easy to troubleshoot and deal with such problems as do arise.



Security

The threat landscape in the field of cyber-security is constantly developing. This means you need a partner who has a strong security management system, who carefully and systematically keeps track of the risk level, and who complies with the sector recommendations for security.

There are many different aspects to consider: Handling security keys for encrypted communication, setting up routers, monitoring the systems, regular reinforcement of the core network, procedures for dealing with and following up on security incidents, and much more besides.

The mobile network features a number of built-in security mechanisms, but the project should nevertheless consider the need for additional end-to-end encryption from the IoT device to the application server. In cases where the users make stringent demands on the integrity of the

solution, as in the majority of mission-critical solutions, this is an understandably self-evident requirement.

Ideally, you should work with a provider who can keep subscribers and IoT devices separated in an isolated APN so as to enhance the security of the IoT network. In combination with a fully functional VPN, this will also prevent unauthorised persons from gaining access to the data, as well as ensuring that no-one can manipulate the information as it moves through the system. This also provides stronger protection against cyberattacks.

The issue of whether this is an actual need should be assessed in consultation with an IT specialist who has experience from similar applications, who knows how you can best ensure this interacts smoothly with the communication technology, and who understands how the underlying components can be aligned to ensure a holistic, well-functioning solution.



The number of IoT devices is expected to increase to **29.4 billion** by 2030

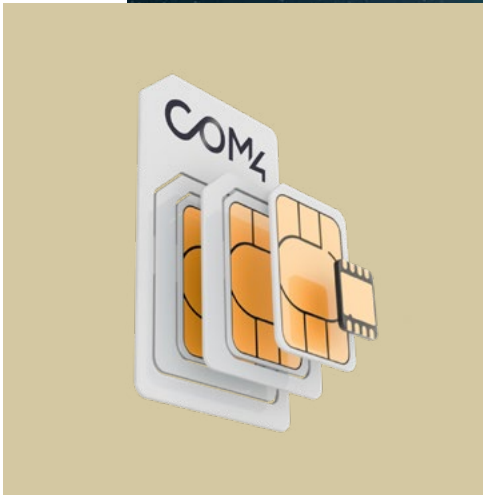
Source



Networks

In theory – and depending on the area of application – IoT devices can communicate over everything from wireless networks in the unlicensed spectrum, to satellites in geostationary orbit. However, none of the innumerable standards and technologies on the market has as broad a user base or as large a global apparatus as the mobile networks.

Let us take a look at the different components in a mobile network, starting with the source: the increasingly tiny parts that identify each and every device and connect it with the network.



Different types of SIM card

If you can remember when GSM telephones became commonplace in the 1990s, you may also remember how amazingly easy it became to switch both mobile phone number and network provider, simply by replacing a little card in your phone. When SIM cards first appeared on the market in 1991, they measured 83 x 53 mm – around the same size as a credit card. Since then, the plastic around the chip itself has been progressively shorn away. The mini-SIM hit the market in 1996, measuring just 25 x 15 mm; then came the micro-SIM in 2003 (15 x 10 mm). The next version was the nano-SIM which many people now use, and which measures a tiny 12.3 x 8.8 mm.

Development didn't stop there, however. 2016 saw the launch of the embedded SIM, or "eSIM" as it is also known. These cards (called Embedded Universal Integrated Circuit Card, or eUICC for short) are soldered into the device's circuit board and can be over-written "over the air". This means that an administrator can switch network operator or change other information directly from a central device, in roughly the same way that software in modern cars can be upgraded without having to enter the car physically and make a manual alteration.

But even this wasn't small enough, and the integrated SIM "iSIM" appeared in 2022. This technology is likewise eUICC-compatible and is built directly into the chipset in the mobile device, where it takes up barely a square millimetre of space.

Thirty years of technological development has thus reduced the size of the SIM card by a factor of at least 4,500, approximately

the same as if someone had succeeded in shrinking the distance between Oslo and Trondheim in Norway (approx. 500 km) to a shade over 100 metres. The result is a SIM solution that takes up little space, demands little energy but still provides full freedom to switch network operator at any time – a completely "agnostic" connectivity solution, in other words. This opens the door to remarkable flexibility in the development of IoT devices.

Communication protocols

Your choice of communication protocol can affect the solution. The MQTT protocol is extremely widespread in the field of IoT and many LTE-M modems support it. The major providers of cloud services also use solutions based on MQTT communication. For NB-IoT-based solutions, where low power consumption is particularly relevant, and where it is likewise important to be aware that potentially difficult coverage conditions may produce higher latency, MQTT-based communication over TCP can be a challenge. In such cases, communication over UDP – such as CoAP – may be a better option.

Communication modules

It is important to choose a connectivity provider that offers broad support for different types of modules and equipment – especially from established manufacturers such as Advantech, Quectel, Nordic Semiconductor and U-Blox, to name but a few. A provider backed by reliable, innovative technology partners can assure the flexibility and the options you need to develop holistic solutions with the potential to succeed in today's tough arena of digital competition.

There is no mobile technology that is universally “right” to use; it depends on the actual requirements in the use case.

Different networks and available protocols – and their properties

A variety of mobile technologies are in use around the world, and it can prove useful to enter into a dialogue about your specific needs with an IoT connectivity provider, particularly in a phase where you are testing different technologies with a view to ensuring that you choose the right solution for your project.

In this context, it is relevant to note that there is no mobile technology that is universally “right” to use; it depends on the actual requirements in the use case. That said, there are a number of “rules of thumb” that provide a decent starting point:

4G or 5G are solid choices if you need significant bandwidth (i.e. above Mbps level) or real-time communication (such as 5G ultra-low latency use cases), but you need to weigh this against factors such as cost, available power supply options, necessary signal strength and geographical area of application.

2G is currently being phased out in a number of countries, so it is not recommended to base new modules on this technology, even though it may be an advantage for the module to support 2G if there is a chance that it may be used in countries that have not yet rolled out the desired technology.

NB-IoT or LTE-M solutions may be a good option for projects that require moderate bandwidth. They need little power, are simple to implement and feature excellent properties for linking up with signals that come from underground installations, for example. This translates into low unit costs and marginal space requirements.

There are some minor differences between these technologies that can make a major difference to the end product. NB-IoT is best for devices that require minimal bandwidth, extremely high penetration strength and truly miserly power consumption. LTE-M, on the other hand, supports seamless mobility, requires slightly more bandwidth and features SMS support. In order to optimise power consumption even further and to simplify data communication, Non-IP Data Delivery (NIDD) can also be used for NB-IoT. In this case, devices will not run on a conventional IP stack but will use simpler mechanisms for data transfer in the mobile network.


For NB-IoT – and, to some extent, LTE-M – it is worth considering the geographical spread of roaming support at present, as well as the anticipated roll-out over the coming years. If the device is to be used in areas without LTE-M/NB-IoT support, it may be a good idea to consider 2G as a fall-back solution.



Properties of different networks

The choice of technology thus depends on the demands made by the solution with regard to aspects including signal strength, bandwidth, real-time requirements, seamless mobility, available infrastructure and so on. In addition, requirements or limitations in a given area of the solution may well affect choices and opportunities in other areas. Volume, size and, in particular, support for future hardware updates will also play a role.

In many IoT projects, the capacity for scaling is a key property. In such cases, it is worth noting that both NB-IoT and LTE-M support 5G requirements for 100,000 devices per square kilometre for massive IoT roll-out.



The value of the IoT
market surpassed **USD
1,000 billion** in 2022

Source



Software

Let there be no doubt, then, that the choice of network is a key decision, but in no way is it the only aspect to consider. It is crucial to ensure that the data are supplied in a secure, efficient and reliable manner, but it is just as important that both the data and the devices that transmit them can be administrated in a user-friendly, cost-optimal way. Here are four key factors that must be included in the assessment:

Integration with cloud services

Thus far, we have focused on how important it is to be able to collect data securely from the IoT devices and transport them safely to a server for secure data storage. At present, it is increasingly common for data to be stored in the cloud, and this means that your solution needs a seamless bridge between your IoT devices and the cloud service you select.

For this reason, it will be important for you to choose a connectivity partner that offers scalable, reliable, secure and standardised integrations with the key cloud platforms – as a minimum, Amazon AWS, Google Cloud and Microsoft Azure, to start with the most commonly used.

A professional connectivity provider will have dedicated connections to the solutions from these suppliers, and will be able to transport your data over private lines, outside the publicly accessible internet. This translates into better control of bandwidth, security and reliability, and allows you to concentrate on what really matters: developing your business.

The importance of testing and development

As we mentioned previously, it is often demanding to gain physical access to IoT devices once they have been placed in position. During the pilot phase (and, under certain circumstances, after the solution has been launched) it is therefore essential to use a good, solid test tool that helps you to verify that the solution will function as intended, or to collect as much information as possible to assist you in your troubleshooting process if it does not.

A good connectivity provider will have tested and verified hundreds of routers, chipsets and other hardware units in order to build up competence that you can then benefit from in your project. Such providers will also have a test environment in which you can simulate how your solution reacts to various error scenarios from the mobile network, measure whether the connectivity has been implemented correctly, and test the power consumption of the devices against the target for power-economical solutions.

All in all, a “precautionary” approach of this kind can save you vast amounts of time and money by eliminating numerous errors and issues prior to an actual implementation.

A good administration tool makes it easy to keep control over costs

Requirements for an administration tool

A good IoT solution demands effective, streamlined tools that make it easy to administrate subscribers and to scale the handling of devices in a user-friendly manner – both for you and for users of your solution.

A robust administration tool makes it simple to keep control of costs, regardless of whether it has to do with switching subscription solution or pausing certain subscriptions when necessary. Location-based services are also important, because they can make things easy for administrators and superusers in customers' organisations to maintain an overview of where their devices are at all times.

At the same time, a SIM administration platform will facilitate administration and follow-up on SIM activity for all your devices at a given location. Irrespective of whether you need to make adjustments for a single user, a group of users or all users at the same time, you need a dynamic tool that makes this simple, seamless and effective. This translates into efficiency in the development, distribution and operation of fleets of IoT devices.

In cases where it is necessary to be able to pinpoint and rectify faults in previously positioned devices, you need access to real-time data and ongoing status updates, as well as to detailed historical data. Not only will this make it simple to keep the devices operating, but this volume of data is also a precondition for the ability to use AI for predictive maintenance (where relevant).

Another key factor is to choose a solution that allows the IoT service you are developing to be integrated seamlessly with companies' internal systems. This can contribute significantly to making the IoT functionality a value-boosting development of both new and existing products and services.

The life cycle of the devices

In the same way as almost all other technology, IoT devices cannot live for ever. However, robust administration tools will help them both cost less while they are still operating, and continue to operate for longer than would otherwise have been possible. For this, you need a platform that enables you seamlessly to activate, modify and suspend SIMs, at the same time as providing you with full control of data consumption: per device, per customer and in total.

When a good administration solution is combined with a market-leading test solution, this can, for example, make it more likely that it will be possible to implement a potentially life-extending upgrade of the IoT devices, without the risk of costly service interruptions for customers. All this can contribute to enhancing value and profitability from your IoT solution, at the same time as it extends the service life of the devices and makes them more sustainable.

02 PRICE ISSUES



Pay-per-unit or “pooled” data traffic

It is a precondition for all IoT solutions that the data reach their destination, but you naturally want to keep the network costs at a manageable level. This means that you need flexibility in the cost structure, such that you can adapt it to the unique requirements of your IoT project. In this regard, there are least three models you need to bear in mind:

Pay-as-you-go

This is a variable model where you pay for what you actually use, without being tied to a set volume of data. It can be a relevant solution during the development or establishment phase of a new service.

Data package

A data package model contains different levels of data consumption during a set period. In return for an obligation to maintain a given level, you are offered lower costs per data unit

transferred. A decent connectivity partner will nevertheless provide tools that give you cost control and flexibility – for example, through automatic, progressive adaptation of the data volume as your needs develop.

Data pool

This is a model where, rather than a given data quota per SIM card, you work with a general “pool” for all the SIM cards in your solution, paying only for average consumption per card. This means that you are less vulnerable to fluctuations in data consumption from device to device, and should trigger volume discounts for your solutions. Not all connectivity providers offer a data pool scheme, but it is absolutely worth seeking out.

McKinsey estimates that approximately **65 percent** of the value from IoT devices will stem from the B2B segment

Source

03 **EXAMPLES OF APPLICATIONS**



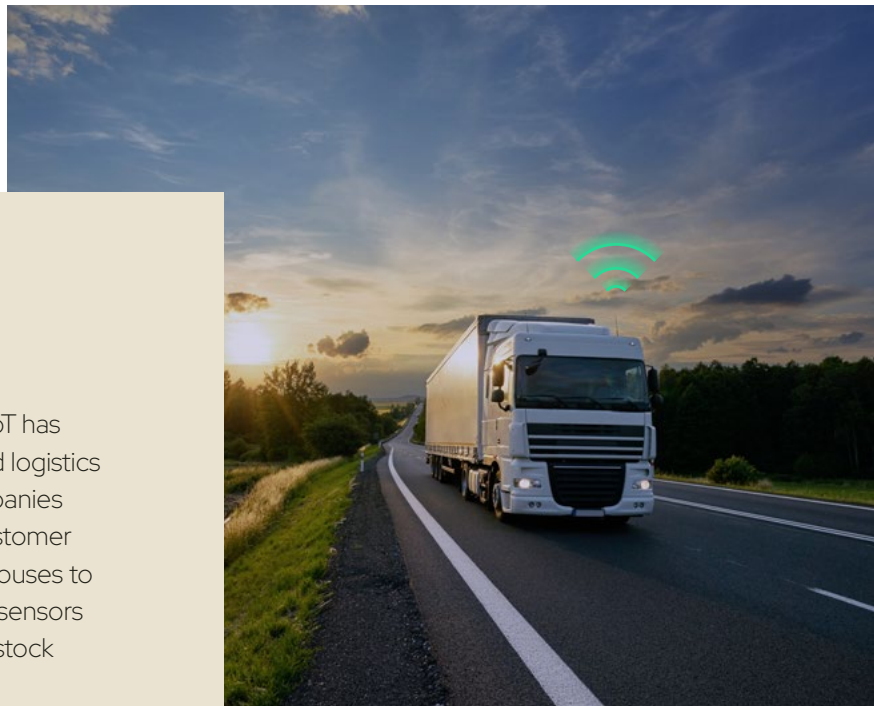
Energy and electricity plants

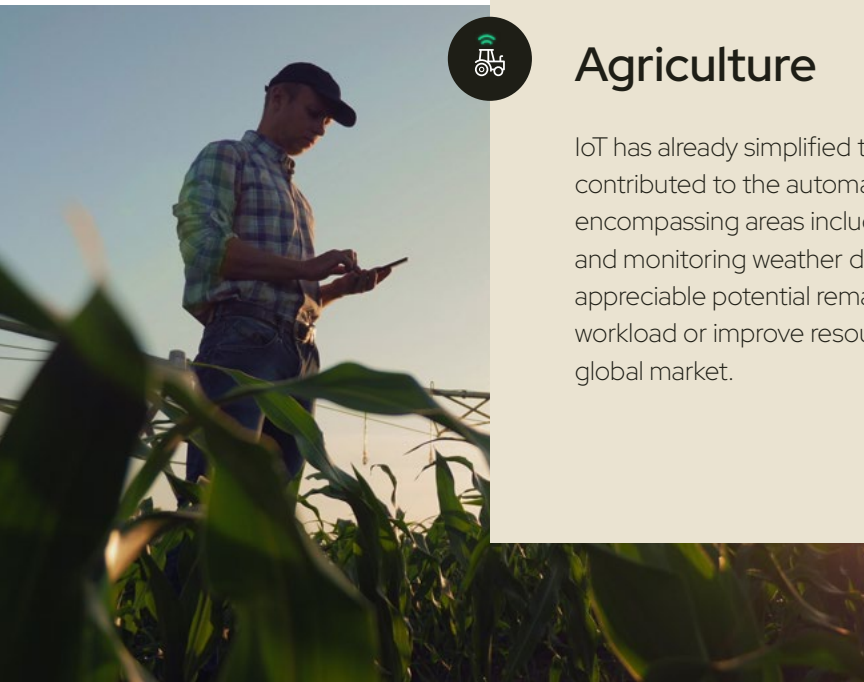
Simpler administration of energy production and power supply is an IoT area of application with which most people in Norway are familiar, given that remote reading equipment has been installed in all Norwegian homes in recent years. This serves as inspiration far beyond the energy sector: similar solutions can also prove beneficial in water supply systems and other public services.



Transport and logistics

The broad spectrum of areas of application for IoT has influenced the development of the transport and logistics sector over a period of years. It has helped companies operate more efficiently, cut costs and boost customer satisfaction. Linking vehicles, cargoes and warehouses to real-time data from positioning devices or other sensors enables enterprises to optimise routes, improve stock management and ensure timely delivery.





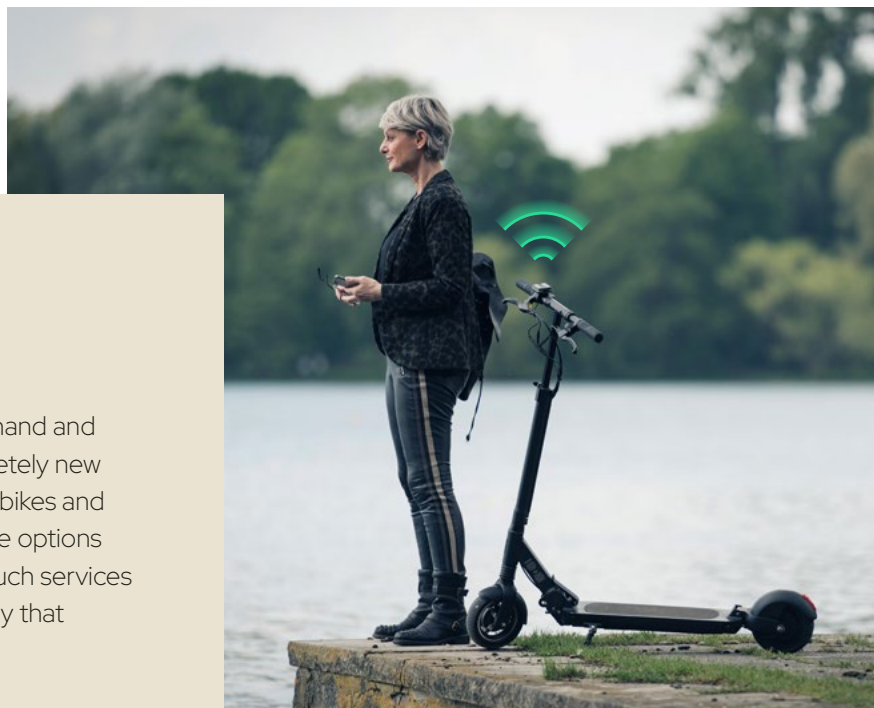
Agriculture

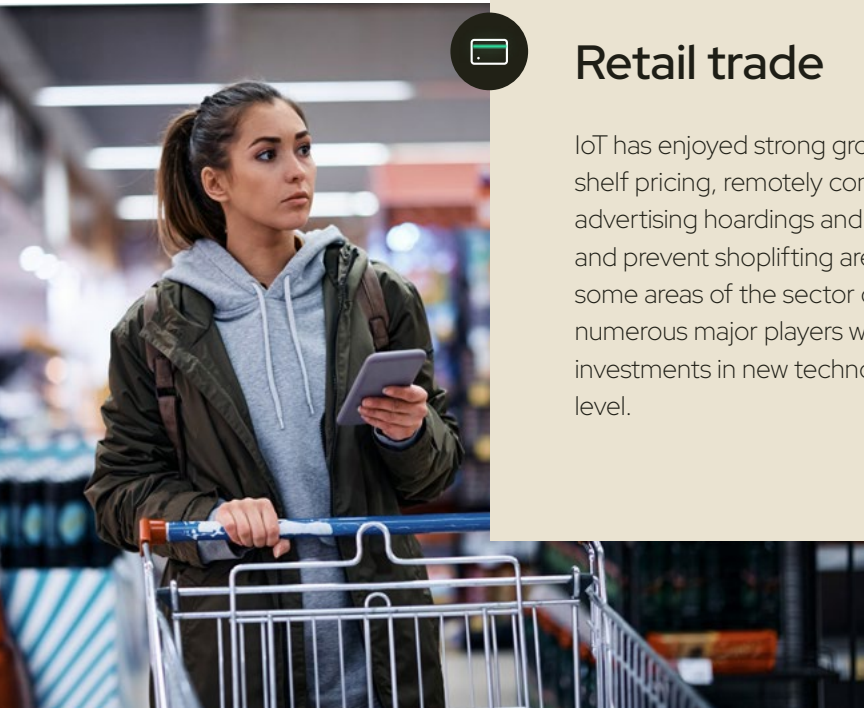
IoT has already simplified the monitoring of livestock and contributed to the automation of farming operations, encompassing areas including planting, irrigation, harvesting and monitoring weather data and other conditions. That said, appreciable potential remains for services that can help cut workload or improve resource utilisation, so this is a promising global market.



Micromobility

In recent years, the expansion of IoT on the one hand and smartphones on the other has generated completely new markets, such as those for electric scooters, city bikes and other services that offer the general public simple options for making their way around urban areas. Many such services have proved to be highly lucrative, and it is unlikely that development in this field will stop any time soon.





Retail trade

IoT has enjoyed strong growth in the retail sector: dynamic shelf pricing, remotely controlled campaigns on digital advertising hoardings and item tags that monitor expiry dates and prevent shoplifting are just some examples. Even though some areas of the sector operate with tight margins, there are numerous major players with the capacity to shoulder exciting investments in new technology – especially at international level.



The healthcare sector

The health and care sector is facing huge challenges in the immediate future, and the sector has long since realised that these cannot be overcome without appreciable focus on technology. This may take the form of remote healthcare, where patients are issued with sensors, meters and other equipment to submit data for closer examination by doctors at a central location, or digital services which otherwise assist care providers at hospitals and other treatment centres.





Smart cities

Recent years have witnessed growing acceptance that IoT can be used to make cities smarter. This can encompass everything from remotely controlled street lighting, refuse containers that send messages themselves when they are almost full, smart traffic lights, or signs that display the wait time for the next tram or bus. Nevertheless, there is still plenty of room to use technology to achieve higher efficiency and to improve resource utilisation so as to give taxpayers more for their money.



COM4