THE ULTIMATE GUIDE TO

Wireless Connectivity for Massive Scale IoT Deployments

BEHRTECH

Table of Contents

Introduction

The Internet of Things (IoT) is taking worldwide industrial and commercial sectors by storm. According to the 2019 IoT report by PwC, 93% of surveyed executives believe the benefits of IoT outweigh its risks and 70% reported to have planned or ongoing IoT initiatives in place. IoT refers to vast networks of physical objects that can autonomously communicate information about their current status and surroundings. By uncovering asset, process and workforce insights at unprecedented granularity, IoT empowers businesses of all sizes to pinpoint previously invisible bottlenecks and optimize their operations in numerous ways.

Pervasive wireless connectivity is a major driving force behind the IoT revolution and a fundamental building block in its architecture. The use of connectivity isn't simply about getting a message to its destination; it's about doing so in a scalable, secure and cost-effective fashion. Selecting the right technology is paramount to the long-term success of your IoT project and various factors must be considered from the get-go in devising a functional and future-proof wireless infrastructure. Needless to say, this can be an overwhelming endeavor, especially for companies with little or no background in M2M communication technologies.

Regardless of where you currently are in your IoT journey, this e-book will help you gain a better understanding of the current wireless landscape and how different technologies might fit into your IoT strategy. It also takes a closer look at Low Power Wide Area Networks (LPWAN) – a newer wireless family that addresses the unique needs of massive-scale industrial and commercial IoT networks. Last but not least, it explores some of the most important considerations when building a versatile wireless architecture.

Wireless Connectivity at a Glance

Why Wireless Connectivity for IoT

Given its significant benefits in terms of reliability, minimal latency and security, wired communications has been the backbone of industrial control and automation systems. Nevertheless, as the new wave of IoT applications arises, we quickly see wired solutions reaching their limits.

Trenching cables is inherently cumbersome, capital- and labor-intensive, not to mention the fact that damage to wiring brings the risk of production downtime. Due to the plethora of proprietary wiring protocols, any additions or modifications to the architecture is deemed costly and could even entail a “rip-and-replace” of cables and conduits. The bulky and expensive wired infrastructure thus limits the number of connected endpoints and is highly constrained in terms of range and network capacity.

In direct comparison, wireless networks require far fewer hardware components, and less installation and maintenance costs. As there aren’t any physical cables involved, sensors can be easily attached to mobile assets to tap into a new host of operational data. On top of that, wireless networks make data collection in hard-to-access and hazardous environments possible and can flexibly expand to meet your changing business needs.

The central value around IoT is the unprecedented visibility into existing processes, equipment and production environment that empowers strategic decision-making. Think of applications used for asset maintenance, facility management and worker safety. As opposed to high-bandwidth, time-sensitive communications, many IoT sensor networks send small-sized telemetry data periodically or only when abnormalities are identified. Of even greater importance is their ability to connect vast numbers of distributed field assets and devices to bring granular business insights. With this in mind, wireless connectivity is often the better option to bring your physical “things” online.

Common Wireless Requirements in Industrial and Commercial IoT

Due to their mission-critical nature, requirements related to industrial and commercial IoT wireless applications are more complex and stringent than their consumer counterparts. Below we outline five key considerations to bear in mind.

Reliable Coverage and Deep Building Penetration

Manufacturing plants, constructed using steel, present a hostile environment for radio propagation due to its rebar structure and a high density of large mechanical and electronic equipment. Other industrial campuses such as open-pit and underground mines are often located in areas with challenging topography characterized by hills, extreme depths or severe bends and corners. Even in high-rise commercial buildings, walls and other physical obstructions will attenuate radio signals and prevent successful data reception.

Low Power Consumption

As many industrial assets are located nowhere near a power supply, sensing devices must be able to operate on independent batteries. Low power consumption of the radio link is crucial to minimize the cost and hassle of battery replacement and/or recharge.

Resilience Against Existing and Future Radio Interference

The majority of existing wireless technologies operate in the license-free Industrial, Scientific and Medical (ISM) frequency bands. Given the explosive number of connected devices and rapidly growing wireless deployments in the license-free spectrum, you want to look for a robust technology that is purpose-built to withstand co-channel interference from other systems. This ensures your critical data is always delivered when it's needed the most.

High Network Capacity and Scalability

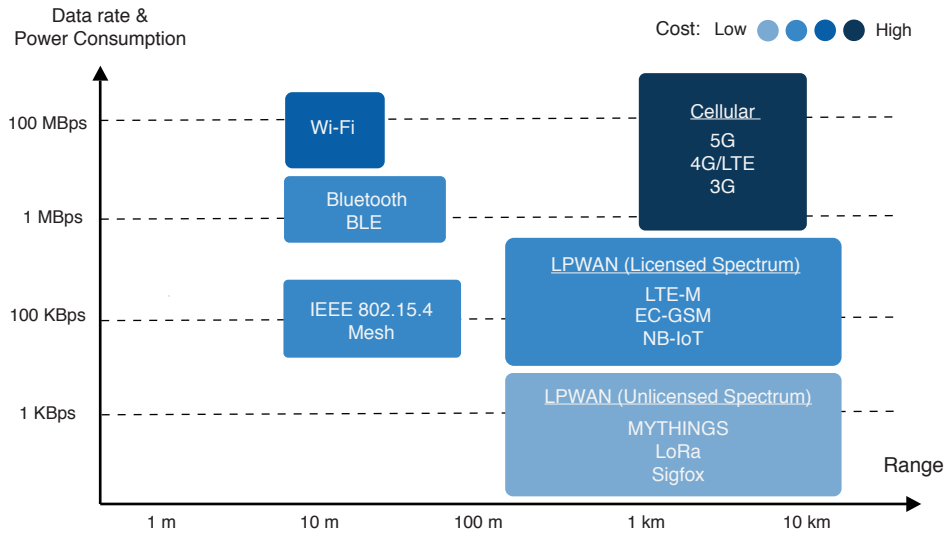
A scalable wireless architecture can help you to address multiple applications while in tandem, enabling seamless future network expansion. This lowers upfront investment and simplifies the management of your IoT architecture to accelerate the return on investment. Increasing the number of endpoints should never come at the cost of other important factors like reliable message delivery and ease of deployment.

Security and Data Privacy

An IoT network is only as secure as its wireless link. With every breach taking a heavy toll on finance and reputation, security and data privacy are top priorities for any company looking to deploy a wireless solution. The fact that many legacy industrial control systems have limited, or outdated security features further intensifies these challenges. In this context, robust cryptographic schemes for end-to-end data protection are crucial, and you might want to consider a privately managed network for complete data authority and ownership.

Navigating the IoT Landscape: 5 Wireless Families You Should Know

Given the bewildering range of wireless solutions available in the market today, choosing the right technology is no easy task. While the requirements we have briefly discussed serve as a useful baseline, the list is far from exhaustive and can vary depending on the use cases. With that said, let's look into the most prominent wireless families in the market today.



QUICK TIP

When evaluating different wireless options, it's important to have a clear vision of the business case you want to address and the operational objectives you are trying to accomplish with your IoT initiative. Equally important is to consider not only existing needs, but also future requirements that might arise. Will the network scale to thousands or even tens of thousands of devices? Will you need to connect mobile assets? What happens if you want to employ new, more power optimized hardware models (e.g. transceiver chipset)?

Only then can you explore the pros and cons of each technology against your specific considerations to identify the best match for your future-proof IoT architecture.

1. Cellular

Well-established in the consumer mobile market, cellular networks offer reliable broadband communication to support voice calls and video streaming. The latest cellular standard – 5G, has garnered a great deal of excitement. Compared to previous generations, 5G introduces significant improvements including ultra-reliable low-latency communications (URLLC) and better mobility support.

On the flip side, cellular networks – including 5G carry very high power consumption and expensive data plans. As such, they aren't viable for most IoT applications powered by battery-operated sensor networks. Instead, the cellular family is a better fit in use cases like connected cars and fleet management. For example, in-car infotainment, traffic routing, advanced driver assistance systems (ADAS) alongside fleet telematics and tracking services are able to rely on the high bandwidth and trans-region availability of cellular connectivity.

With high-speed mobility support and ultra-low latency, 5G is deemed to be a dominant catalyst for other emerging tech trends like augmented/virtual reality and autonomous vehicles. The technology is also expected to play a vital role in telehealth innovations, future public safety and mission-critical communications and certain industrial automation use cases.

DID YOU KNOW?

While telco service operators have offered early 5G networks in several countries since mid-2019, 3GPP Release 16 and with it, the "full 5G vision", won't arrive until late 2020. With that said, the 5G roll-out will span over the next few years and devices supporting full features are further down the road.

5G comes in three categories: ultra-reliable low latency, extreme mobile broadband, massive machine-type communication.

Millimeter-wave used in 5G URLLC enables extremely high data speed at the cost of drastically reduced range and network footprint. Thus, its availability is mostly limited to dense urban areas, leaving a big question over its application for industrial automation.

2. Wi-Fi

There is little need to explain Wi-Fi (also known as Wireless Local Area Networks), given its critical role in providing high-throughput data transfer for both enterprise and home environments. However, in the IoT space, Wi-Fi's inherent limitations in terms of coverage, scalability and power consumption make the technology much less prevalent.

Given the high energy requirements and a limited range (less than 100 meters), Wi-Fi is a less feasible solution for large networks of battery powered IoT sensors, especially in industrial IoT and smart building scenarios. Instead, it's more suitable for devices that can be easily connected to a power outlet like smart home gadgets and appliances, digital signs or security cameras. Self-interference is also a real challenge in Wi-Fi networks, given that an increase in the number of end devices can quickly degrade connection quality.

Wi-Fi 6, the newest Wi-Fi generation, brings greatly enhanced system bandwidth (i.e. <9.6 Gbps) to improve data throughput per user in congested environments. With this, the standard is poised to level up public Wi-Fi infrastructure and transform the customer experience with new digital mobile services in retail, hospitality and mass entertainment sectors. Also, in-car networks for infotainment and on-board diagnostics is expected to be a game-changing use case for Wi-Fi 6. However, development will likely take more time.

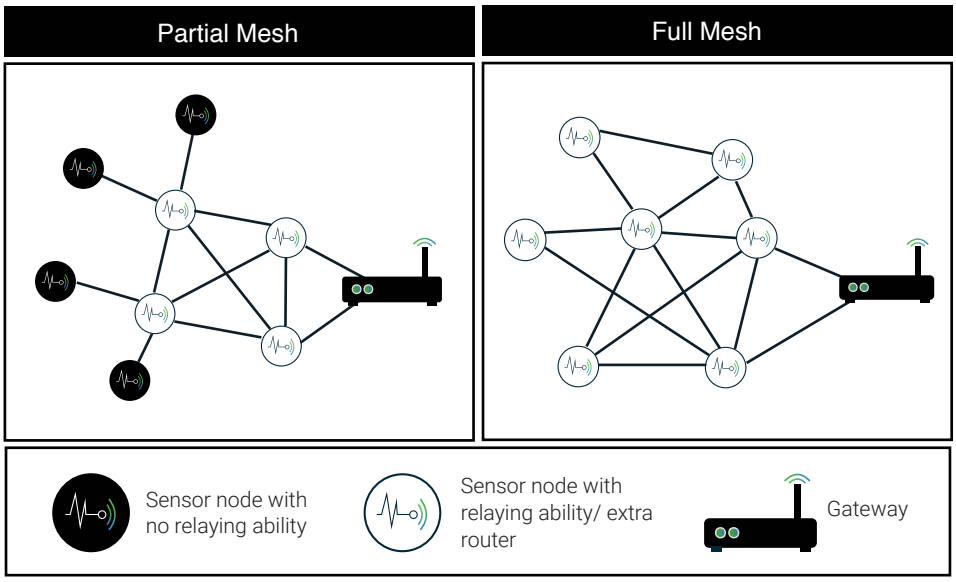
DID YOU KNOW?

Rather than enabling a single device with lightning speed, Wi-Fi 6 aims to support more endpoints per router concurrently, without compromising data throughput per device. In doing so, the router employs multiple antennas, and the total used spectrum is divided into a much larger number of sub-channels for simultaneous data streams from multiple devices.

3. IEEE 802.15.4 Mesh Protocols

IEEE 802.15.4 is a radio standard, defining physical and medium access control (MAC) layers in low-rate Wireless Personal Area Networks. By reducing the data rate to a maximum of 250 kbit/s, IEEE 802.15.4 solutions aim to deliver a low power alternative to traditional wireless options. Common technologies based on IEEE 802.15.4 specifications include WirelessHART, ISA-100.11a, and Zigbee.

The physical range of IEEE 802.15.4 protocols is often limited to between 10 and 100 meters. As such, these protocols must resort to a mesh topology, wherein a signal hops through multiple devices until it reaches the gateway, in order to improve the overall network footprint. In full mesh networks like WirelessHART, all sensor nodes have the routing ability to relay data from other nodes. In partial mesh networks like Zigbee or ISA-100.11a, only selected nodes can act as routers.



While it helps to extend coverage, mesh topology is not power efficient and requires complex configuration and management, particularly when the network scales to a few hundreds of devices. For this reason, mesh solutions are best-suited for medium-range applications where nodes are evenly distributed near each other. For example, WirelessHART and

ISA-100.11a an ideal alternative to expensive wired networks in certain industrial automation and control scenarios. Similarly, Zigbee can greatly complement Wi-Fi to enable home automation use cases like smart lighting, water and energy monitoring or security sensor networks.

DID YOU KNOW?

Though the IEEE 802.15.4 standard allows for operations in different license-free industrial, scientific, and medical (ISM) bands, solutions built on this standard are mostly tuned for the globally available 2.4 GHz band.

The 2.4 GHz channels are widely used among legacy radio systems including Wi-Fi hubs, Bluetooth devices, RF lighting, industrial heaters, and welding equipment. Therefore, companies will need to accurately assess how saturated these channels are before adding another system to the field.

4. Bluetooth/ BLE

Also categorized as Wireless Personal Area Networks, Bluetooth is a short-range communication technology well-positioned in the consumer marketplace. Bluetooth Classic was originally intended for point-to-point or point-to-multi-point (up to seven slave nodes) data exchange among consumer devices. Optimized for power consumption by drastically reducing data rates, Bluetooth Low-Energy (BLE) was later introduced to address small-scale Consumer IoT applications.

BLE-enabled devices are often used in conjunction with electronic devices, typically smartphones that serve as a hub for transferring data to the cloud. Nowadays, BLE is widely integrated into fitness and medical wearables (e.g. smartwatches, glucose meters, pulse oximeters, etc.) as well as Smart Home devices (e.g. door locks), where data is conveniently communicated to and visualized on smartphones.

The release of the Bluetooth Mesh specification in 2017 aimed to enable a more scalable deployment of BLE devices, particularly in retail contexts. Providing versatile indoor localization features, BLE beacon networks have been used to unlock new service innovations like in-store navigation, personalized promotions, and content delivery.

DID YOU KNOW?

Built upon the BLE specifications, Bluetooth 5.0 offers an energy-efficient option to stream audio and send large data files without quickly draining the device battery in a matter of few hours.

If speed isn't a top requirement, Bluetooth 5.0 also gives devices the ability to communicate at low data rates in exchange for a much-improved range of up to 200 meters.

Bluetooth 5.1 and 5.2, the two latest derivatives of the fifth Bluetooth generation, include innovative direction-finding techniques for highly precise indoor localization.

5. Low Power Wide Area Networks (LPWAN)

Geared for low-bandwidth, low computing end nodes, the newer Low Power Wide Area Networks (LPWAN) offer highly power-efficient and affordable IoT connectivity in vast, structurally dense environments. No current wireless classes can beat LPWAN when it comes to battery life, device and connectivity costs, and ease of implementation. As the name implies, LPWAN nodes are designed to operate on independent batteries for years, rather than days as with other wireless solutions. They can also transmit over many kilometers while providing deep penetration capability to connect devices at hard-to-reach indoor and underground locations.

Due to this unique combination of features, LPWAN has established itself as a prime driver of massive, latency-tolerant sensors network in industrial IoT, smart building and smart city sectors. While there is a plethora of LPWAN protocols available today, it is important to look at the distinct advantages of standard-based technologies. Given the explosive growth of IoT connected devices, Quality-of-Service, scalability and interoperability will be cardinal criteria in your wireless decision.

3GPP-based standards like NB-IoT and LTE-M, along with MYTHINGS – a connectivity solution based on the latest ETSI open standard for low-throughput networks, have emerged as alternatives to proprietary technologies (e.g. LoRa, Sigfox, etc.) and specifically address these requirements.

In terms of applications, NB-IoT and other carrier-based LPWAN standards will be a core pillar of future smart city networks. Leveraging existing cellular infrastructure, these managed networks provide extensive coverage in urban areas, while removing infrastructure expenses. On the other hand, for industrial deployments where data security and ownership are supreme, privately deployed solutions like MYTHINGS will rise as a preferred option. As an aside, industrial facilities are often located in remote regions that are poorly serviced by network operators.

DID YOU KNOW?

A main challenge among legacy LPWANs is the persistent trade-off between Quality-of-Service and power consumption. Technologies that can transcend this trade-off are poised to deliver an unmatched competitive advantage.

Industrial alliances have been established around certain proprietary solutions to promote standard development. Note that these efforts do not ratify the viability of the technology and in fact, do not cover the whole network stack such as in the case of the LoRa Alliance.

Wireless IoT Cheat Sheet: An Overview of Technology-Application Compatibility

Key IoT Verticals	LPWAN	Cellular	Mesh	BLE	Wi-Fi
Industrial IoT	●	○	○		
Smart Metering	●				
Smart City	●				
Smart Building	●		○	○	
Smart Home			●	●	●
Wearables	○			●	
Connected Car		●			○
Connected Health		●		●	
Smart Retail		○		●	●
Asset Tracking	●	●			
Smart Agriculture	●				

● Highly applicable ○ Moderately applicable

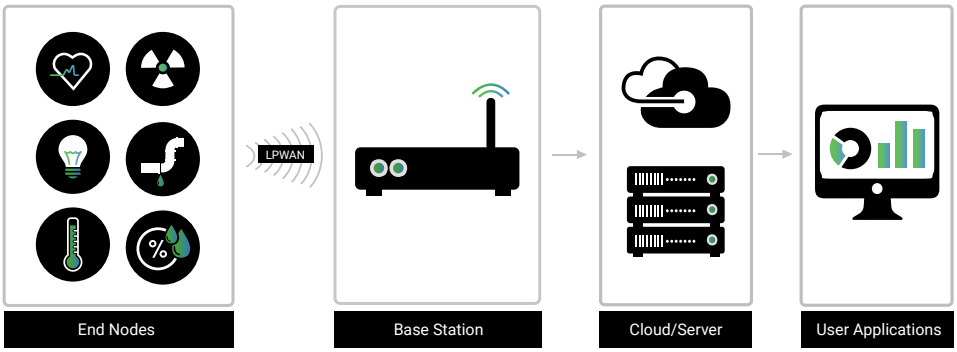
Final Takeaway

To quickly sum up this chapter, we've seen that no wireless solution is a silver bullet for all IoT applications. Having said that, when it comes to telemetry-based remote monitoring use cases fuelled by vast, battery-operated sensor networks, LPWAN is the most versatile option. LPWAN technologies overcome the pitfalls in range, power and cost faced by traditional cellular and short-range solutions (e.g. Wi-Fi, Bluetooth). Compared to mesh networks, LPWAN is also much easier to deploy thanks to the star topology, so you can avoid the hassle of network planning and management. For those looking to get a better grasp of this wireless family, in the next chapter, we'll walk through its technical underpinnings and how major technologies compare.

II

A Deep Dive into LPWAN for Massive-Scale IoT

As previously mentioned, LPWANs employ a star topology in which a base station or gateway collects data from numerous remote, distributed end nodes. Except for cellular LPWAN (i.e. NB-IoT), the connection between end nodes and the base station is non-TCP/IP to avoid hefty packet headers. After receiving and demodulating messages, the base station relays them to the backend server through a standard TCP/IP backhaul link (e.g. Ethernet, cellular, etc.). For public LPWAN services, data must be routed through the network operators' server before reaching the end user's applications. Conversely, in privately managed LPWANs, data can be directly transferred to the user's preferred backend for complete data privacy and control.



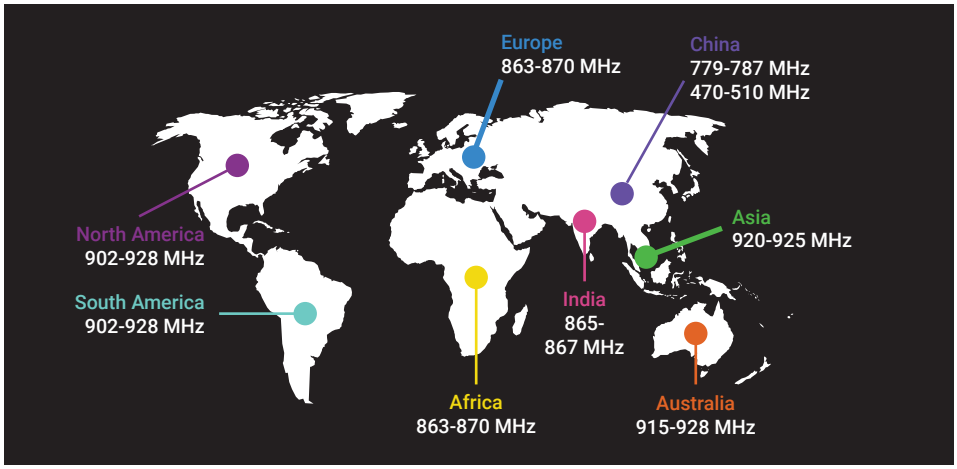
The appeal of LPWANs exists within their two signature features: long range and low power consumption. While Wi-Fi and Bluetooth are limited to less than a hundred meters at best, LPWANs can communicate up to 15 km in rural areas and up to 5 km in urban, structurally dense areas. On top of that, LPWAN's simple, small-footprint transceiver design minimizes cost and power consumption on the end node side. The idea is to leave the heavy lifting to the base station and keep the data frame as short as possible.

Two Key Qualities of LPWAN

1. Long Range

Radio range is often measured in terms of receiver sensitivity – the lowest signal power for which a message can be detected and demodulated. In LPWANs, receiver sensitivity can reach -130 dBm, as compared to a moderate -70 dBm sensitivity in Bluetooth. This high receiver sensitivity is typically achieved by reducing the signal bandwidth and thus experienced noise levels (i.e. (Ultra-)Narrow Band) or adding processing gain (i.e. Spread Spectrum); both come at the cost of lower data rates.

In addition to special modulation techniques, the use of sub-GHz frequency bands in most LPWAN solutions, instead of the popular 2.4 GHz band, further improves range and penetration capability. As the wavelength is inversely proportional to free space path loss, the long radio waves in sub-GHz systems can travel over long distances. Compared to 2.4 GHz signals, they can also penetrate through walls, trees and other structures along the propagation path much better, while bending around solid obstacles.



2. Low Power

QUICK TIP

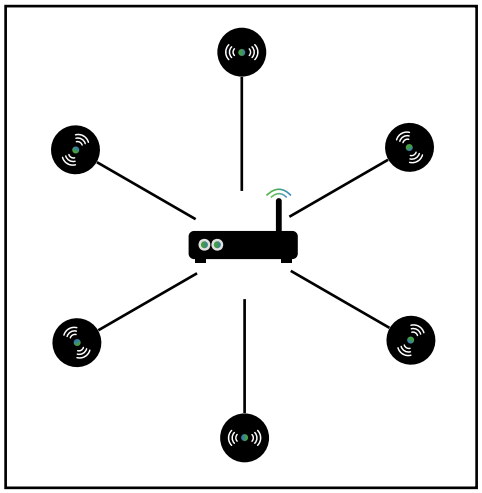
It's important to note that power efficiency can drastically vary among LPWAN technologies. This is because transmission time or on-air radio time of each message is very different across systems. Since transmission is technically the most energy consuming activity, short on-air time allows the transceiver to turn off faster to further reduce power consumption.

LPWAN systems adopt multiple approaches to optimize power efficiency, giving many years of battery life on end nodes. First, when not actively transmitting, the transceivers are put into deep "sleep" mode whereby very minimal power is consumed. In bi-directional communications, a listening schedule is defined so that the device is "awake" only at predefined times or shortly after an uplink is sent to receive the downlink message.

Secondly, many LPWAN technologies employ a lightweight asynchronous protocol at the Medium Access Control layer to minimize data overhead. Pure ALOHA ,a very simple random access protocol, is a common choice.

> ***What's pure ALOHA?***
> *In pure ALOHA, a node accesses the channel and transmits a message whenever data is available. There is no time-slotted coordination, no carrier sensing, and even acknowledgment of received messages is often bypassed to further reduce the power footprint. Note that the significant power benefit comes at the expense of network performance since uncoordinated transmissions increase the chances of message collision and data loss. The use of pure ALOHA without effective contention-resolving mechanisms is an underlying cause for Quality-of-Service and scalability issues among many LPWAN solutions like LoRa and Sigfox.*

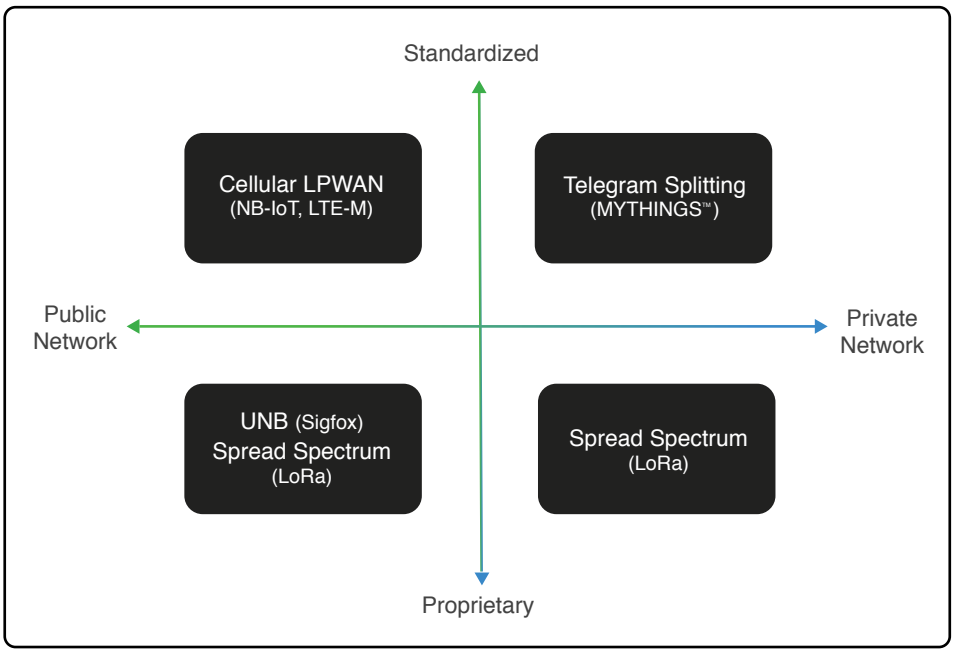
Star Topology



Finally, the one-hop star topology introduces considerable power benefits. As discussed previously, while certain mesh solutions have been implemented for battery-operated, industrial sensor networks, they consume more power than an LPWAN solution by orders of magnitude. This is because, in a multi-hop mesh topology, devices must spend extra energy listening for and relaying messages from other devices. On the other hand, a star network allows devices to "turn off" and stay in sleep mode most of the time.

LPWAN Technology Comparison

If we take a look at the underlying technology, LPWAN solutions can be broadly grouped into four main types: cellular LPWAN, Ultra-Narrowband (UNB), Spread Spectrum, and Telegram Splitting. Among these four, cellular LPWAN is the only category that operates in the licensed spectrum, while the latter three mostly leverage the license-free ISM frequency bands.



1. Cellular LPWAN (Licensed Spectrum)

Pros

- High data rate
- High QoS and scalability
- Proven, standardized technology

Cons

- Shorter battery life due to complex synchronous communications and large data rates
- No mobile communication supported (NB-IoT)
- Unpredictable technology sunsetting
- Dependence on operators' network footprint

LTE-M and NB-IoT are the two leading variants of cellular LPWAN. Both employ a narrowband approach, wherein the received signal bandwidth and data rates are reduced to improve range and building penetration ability. Compared to LTE, their transmission power and technical design complexity are also drastically reduced to achieve low-cost, low-power qualities. NB-IoT, however, uses a much smaller system bandwidth (200 kHz) than LTE-M (1.4 MHz) and thus is a better choice for underground and indoor applications.

Due to the fact that they operate in the licensed spectrum, cellular LPWAN solutions offer great Quality-of-Service advantages, as there is no co-channel interference from external systems. Additionally, they employ time and frequency synchronization alongside handshaking for very high transmission reliability and network scalability. That being said, these mechanisms come at the cost of power efficiency due to the required data overhead [1]. Besides consuming extra energy, handshaking makes the battery life of a node unpredictable, since it's difficult to decide how many times the process needs to be repeated for each transmission.

Compared to its unlicensed counterparts, cellular LPWAN provides relatively higher peak data rates (i.e. > 1 Mbit/s for LTE-M and 250 kbit/s for NB-IoT), which further increases power budget requirements. Available as

managed connectivity services from telecom providers, coverage at remote locations might not be guaranteed, and network longevity is at stake due to the unforeseeable technology sunsetting. If your IoT end nodes are mobile, NB-IoT is not a good choice as it's mostly designed for stationary devices.

Given their pros and cons, cellular LPWAN options are best suited for higher data rate IoT use cases and in smart city scenarios where telecom infrastructure is mature. On the other hand, they aren't optimal for applications where ultra-low power is at a high priority. The same goes for deployments in remote locations and those that require the supported communications network to sustain over several decades.

2. Ultra-Narrowband – UNB (License-free Spectrum)

Pros

- Extensive range (very high link budget)
- High spectrum efficiency

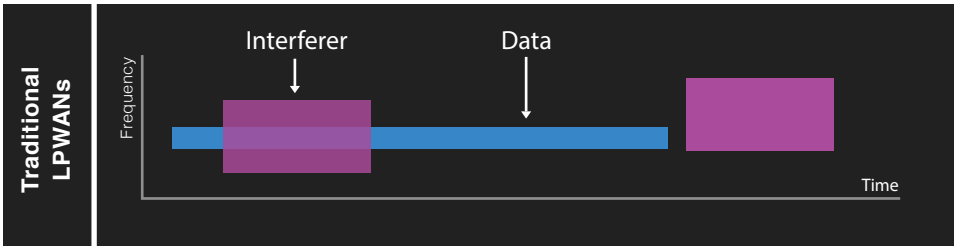
Cons

- Extremely low data rate

  Prone to interference and data loss
- Limited payload size and number of daily transmitted messages
- More power usage due to long on-air time
- Limited mobility support
- Proprietary technology

To minimize the noise level and optimize receiver sensitivity, Ultra-Narrowband solutions contract the signal bandwidth to as small as 100 Hz. Besides extensive range and excellent penetration, the UNB approach allows for high spectral efficiency as each signal occupies very minimal channel bandwidth. High spectral efficiency means that more messages can fit into an assigned frequency band without overlapping with each other, thereby improving overall system capacity and scalability. Sigfox and Telensa are representatives of UNB-based LPWAN technologies.

Ultra-narrow band signals, however, introduce very low data rates which translate into long on-air radio time. For example, systems like Sigfox feature a 100 Hz signal bandwidth and a data rate of 100 bps (EU mode). So, every Sigfox transmission of 12-byte user data (with a total message size of 26 bytes) lasts for as long as 2 seconds. This presents several challenges. First, long on-air time inevitably requires more power usage as the transceiver needs to be active for a longer period. Second, under EU duty cycle regulations (i.e. 1%) imposed by ETSI, a device operating in the 868 MHz band can "speak" for only 36 seconds per hour. As such, the more time each transmission must be on-air, the fewer total messages are allowed to be sent. In the USA, FCC regulations limit the frequency occupation time of each message to 0.4 seconds, requiring a different network design with a higher data rate and shorter overall network range.



Long on-air time makes UNB signals highly susceptible to interference

Another issue with long on-air time is impaired Quality-of-Service. Coupled with asynchronous communications, longer time in the air interface exposes a message to a higher chance of data collision, especially in a crowded license-free spectrum with heavy radio traffic from multiple co-existing systems. Some solutions send the same data multiple times in an attempt to improve message reception. However, this measure proves to be counter-productive, as it increases the total on-air time and energy usage per unique payload, while further limiting effective data amounts that can be sent per hour.

Another drawback of UNB networks is its sensitivity to multipath fading caused by Doppler effects in mobile end devices or those situated close to fast-moving objects (e.g. near a highway) [2]. To avoid packet errors due to Doppler shifts, UNB nodes should be stationary or moving only at minimal speeds.

3. Spread Spectrum (License-free Spectrum)

Pros

- Flexible data rate based on SF choice
- Existing ecosystem and industry support (LoRaWAN)
- Medium mobility support (> 40 km/h)

Cons

- Proprietary and hardware-driven
- Scalability and QoS problems due to low spectrum efficiency and long on-air time
- Complex network management

Another common LPWAN modulation technique, Spread Spectrum overcomes the very slow data rate and Doppler fading issues experienced by UNB solutions to a certain extent. In Spread Spectrum, a narrowband signal continuously changes frequency, resulting in a frequency ramp that occupies a much wider channel bandwidth. More bandwidth use essentially comes with higher experienced noise levels. As such, processing gain is added to improve the Signal-to-Noise ratio and overall system range. The Spreading Factor (SF) signifies the level of processing gain with higher SF enabling longer range at a lower data rate.

Compared to UNB, Spread Spectrum signals are more resilient to multipath fading in mobile devices. Chirp Spread Spectrum (CSS) implemented in LoRa technology is a representative variant of this modulation scheme. A recent study shows that CSS systems can effectively support mobile nodes at a speed of up to 40 km/h [3].

On the flip side, the biggest limitation of Spread Spectrum solutions is their inefficient use of the spectrum resource, since more bandwidth is required to transmit only a small amount of data. This induces bad co-existing behavior and serious scalability problems. In the limited sub-GHz radio spectrum, high wideband data traffic combined with uncoordinated transmissions in pure ALOHA can cause message overlays and eventually packet errors. This challenge is further intensified in long-range applications using a high spreading factor, due to the low data rate and thus, longer on-air time of messages [4].

The use of different spreading factors and bandwidth combinations (i.e. orthogonality) and a higher number of base stations are common approaches to mitigate this issue. However, tuning each base station to a different frequency entails complex network management and requires radio system expertise.

4. Telegram Splitting (License-free Spectrum)

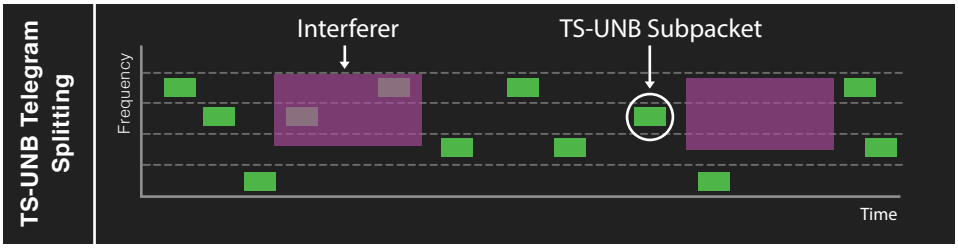
Pros

- Very high interference immunity for excellent QoS and scalability
- Power optimized design
- Unparalleled mobility support
- Proven, standardized technology

Cons

- New emerging ecosystem
- Relatively low date rate

Telegram Splitting is the latest and thus far, the only standardized LPWAN technology in the licensed-free spectrum. Introducing a new radio transmission approach for UNB signals, this technology aims to eliminate the trade-off between Quality-of-Service and power efficiency commonly faced in other LPWAN solutions. MYTHINGS by BehrTech is the only solution that implements Telegram Splitting and fully complies with the ETSI TS 103 357 standard.



Short on-air time of sub-packets in Telegram Splitting minimizes packet collision and data loss.

Telegram Splitting systems feature a data rate of 512 bit/s. At the physical layer, the technology divides an ultra-narrowband telegram into multiple equal-sized sub-packets, each of which is randomly sent at a different time and carrier frequency. As each sub-packet has a much smaller size than the original telegram, its on-air time is drastically reduced to only 16 milliseconds. As an example, the accumulated on-air time of a 24-byte

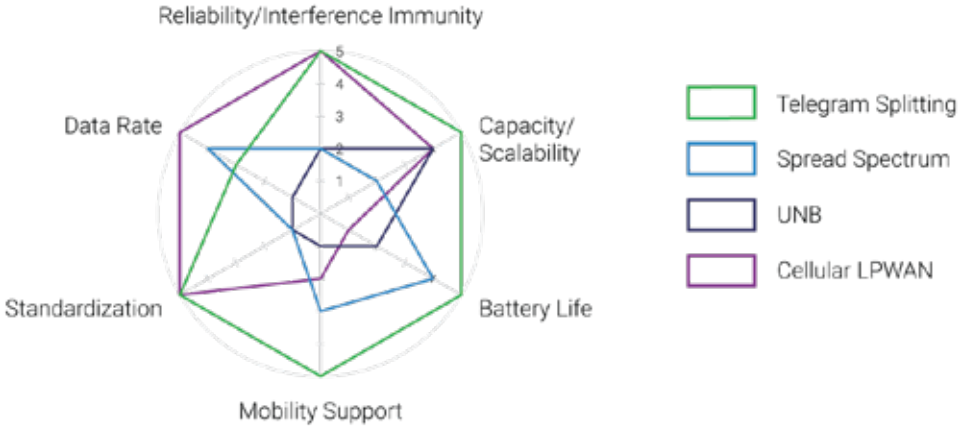
message with 10-byte user data is only 390 milliseconds. Short on-air time combined with the random distribution of sub-packets over time and frequency significantly mitigates their risk of being hit by interferers. On top of that, Forward Error Correction (FEC) built into the protocol ensures that even if 50% of sub-packets are lost, the full message can be retrieved at the base station.

As such, although asynchronous communication is used for its ultra-low power benefits, short on-air time and FEC resolve collision issues to deliver very high interference immunity and system capacity. Specifically, a single base station can handle more than one million messages a day as specified in the ETSI TS 103 357 standard [5]. Also, in an Industrial IoT-equivalent scenario, Telegram Splitting has been proved to drastically outperform Chirp Spread Spectrum in LoRa in terms of message deliverability and network reliability [6].

In addition to Quality-of-Service, the characteristics of Telegram Splitting, also offer great power benefits. After the transmission of each sub-packet, there is a much longer transmission-free period in which the node goes into "sleep mode". Short on-air time and longer off-air time minimize power consumption while giving the battery time to recover, which in turn substantially extends battery life.

The short on-air time of sub-packets coupled with coherent demodulation additionally diminish Doppler fading effects. And, even if some sub-packets suffer from deep fades, FEC ensures that message detection and retrieval are minimally affected. With this, Telegram Splitting systems can connect end nodes moving at up 120 km/h [5] – a feature not available in previous LPWAN technologies.

The following figure compares the four major LPWAN technology types in different network criteria.



The Importance of Standardization

Standardization is one of the core pillars in a robust and vibrant IoT ecosystem. A standardized technology provides a rigorous and transparent technical framework to fuel both vertical and horizontal interoperability. Given its significance, we want to clarify what makes a standard-based technology and why it matters for the end user.

The Official Definition of Standard

In the LPWAN realm, we have seen many industrial alliances established around proprietary solutions to promote standard development. However, these efforts do not ratify the viability of the technology and more notably, might not cover the whole network stack. It's common that only the MAC layer is made open, while the physical layer remains entirely proprietary, as in the case of the LoRa Alliance (i.e. LoRaWAN is the MAC layer and LoRa is the proprietary physical layer by Semtech). By making (part of) the technical specifications publicly available on a royalty-basis, many LPWAN vendors attempt to claim their technologies as "open standards." Nevertheless, this is not really the case.

Strictly speaking, an industry standard – must undergo a stringent evaluation process by an established Standards Development Organization (SDO). This guarantees the quality and credibility of the technology. Dominant global SDO examples include ETSI, IEEE, IETF, 3GPP, etc. So far, there have been only two camps of LPWAN technologies that have succeeded in standardization efforts and are endorsed by formal standard organizations. One is cellular LPWAN that implements 3GPP standards, and the other is the Telegram Splitting technology based on the newly released ETSI standard on Low Throughput Networks – TS 103 357.

Key User Benefits

From an IoT adopter's perspective, standardized communication solutions offer the following significant benefits:

Guaranteed Quality and Credibility: Standardization ensures that products and solutions are fit for their intended purposes. In other words,

communication technologies that adhere to rigorous standards deliver high Quality-of-Service, robustness against interferences and industry-grade security to ensure reliable and secure transmission of massive IoT sensor data at the edge.

Interoperability and Innovation Flexibility: Standard-based protocols can be programmed on various commodity, off-the-shelf hardware (i.e. chipsets, gateways) to support multi-vendor solutions and interconnection of heterogeneous devices. Besides promoting long term interoperability, standardization helps end users avoid commercial risks of vendor lock-in, whereby a single supplier retains total control over functionality design and future product/technology innovation.

Global Scalability: Industrial users with worldwide operations want to adopt IoT connectivity that can be implemented across their global facilities. Standardized solutions function universally and help minimize installation complexity, thereby safeguarding long-term investment.

Final Takeaway

As we have seen, not all LPWAN technologies are created equal. Existing solutions can be categorized based on their operating frequency (license vs license-free) and the underlying technology. While the LPWAN landscape might seem overwhelming at first sight, it isn't so hard to decide which technology is the right fit, once you understand your key network criteria. In industrial and commercial scenarios with their extremely low tolerance for message error, it's critical to look at solutions purpose-built for Quality-of-Service and scalability while not compromising other requirements like power consumption and mobility support. Concurrently, a standard-based technology fortifies long-term industry support while accelerating the development of a vibrant ecosystem.

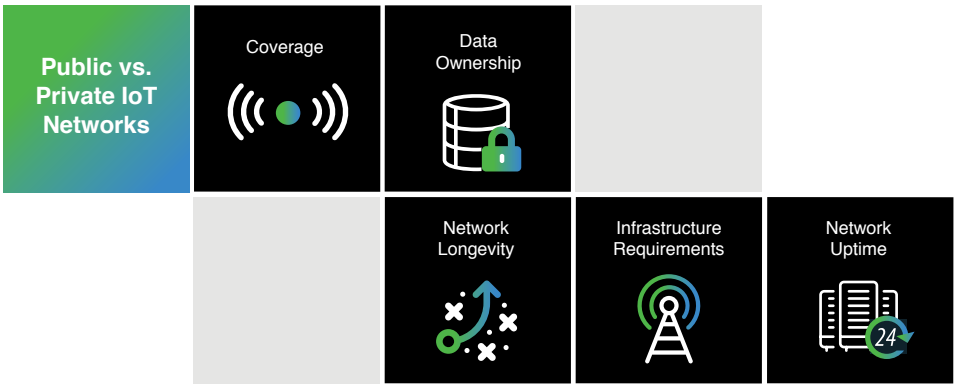
IV

Wireless Design Considerations

Now that we've walked through the most prominent wireless options in the market, it's time to give some thought to what the wireless architecture should look like. This chapter explores some of the most important considerations when designing a functional and future-proof wireless network.

1. Public vs Private Network

Public connectivity services are provided and managed by a mobile carrier or third-party operator, while a private network is locally built and managed for dedicated data communications on your premises. Both have pros and cons and again, the decision should be tied to the use case in question. Below are five key differentiation factors to examine before making up your mind.



Global vs Campus Coverage

One common selling point of many IoT network operators is their self-proclaimed global and nationwide footprint, alongside cross-region roaming ability. However, there's indeed a big difference between "absolute" and "relative" footprint, with the latter resonating more with reality. While the promise of ubiquitous connectivity might hold true in urban, densely inhabited areas, public coverage still remains inconsistent or absent

altogether in many remote industrial areas. As soon as a node gets close to a network's edge, its reliability is not guaranteed. Depending on your use cases, indoor and underground coverage might also be in question. In direct comparison, a private IoT network can't offer trans-region connectivity for applications like commercial fleet telematics. Nevertheless, when it comes to a campus-style deployment, it gives you the best chance to tailor network coverage to your specific needs.

Data Privacy and Ownership

Data ownership is among the leading concerns plaguing IoT implementations in industrial contexts. In a recent webcast from Deloitte, the "lack of ownership/ governance to drive security and privacy" landed second place as the top 10 IIoT cyber and privacy risks. The problem with a public network is that no matter what your IoT architecture looks like, your data must be routed through the operator's backend before reaching the end server or application platform. If keeping data on-premises is at the top of your list, you're probably better off with a private solution.

Infrastructure Requirements

A clear advantage of public IoT networks over private ones is that you can save on upfront infrastructure costs. Depending on the chosen communications technology, investment in gateways, antennas, and repeaters, etc. can be expensive. Besides hardware expenses, labor hours spent setting up and managing the network quickly ramp up with an increase in the required infrastructure. In this context, going for long-range, scalable connectivity is the best way to minimize infrastructure overheads in private solutions.

Network Longevity

Industrial sensors and devices are often designed for long-term use. Once installed, they typically remain there for years, or even decades without the need to be replaced. To ensure a sustainable IoT architecture, it is important to align the network lifecycle with the device lifecycle. Public cellular technologies come and go every decade or so; 2G and 3G networks sunsets are well underway amid increasing LTE prevalence and 5G rollouts.

And, given the backward compatibility gap, this transition isn't as simple as swapping the 3G module for an LTE or 5G one. Technological and regulatory changes that have happened along the way add to the complexity of the migration process, and thus, the disruption time of your industrial network.

Network Uptime

Mission-critical IoT applications call for a highly reliable communications infrastructure, even in times of crisis. Industries that require undisrupted operations strive for nearly 100% network uptime, which is often unrealistic for commercial carriers and other public operators. Every year, natural disasters cause massive outages across public connectivity services. Plus, network uptime is subject to unpredictable disruptions resulted from physical or technical failures of the operator's infrastructure. With a private deployment, you retain full control over network availability at any time.

Summing up, public IoT networks surely have their place in a multitude of consumer and smart city applications. Nevertheless, the undeniable appeal of maximum data authority and control over the network architecture are driving the adoption of privately managed connectivity across industrial verticals.

2. Hybrid Wireless Architecture

In several application scenarios, a single wireless technology might not cut it. Integrating different solutions into the same architecture introduces enhanced value and functionality to cater to the unique requirements in context. Here are two examples in which IoT adopters can benefit from a hybrid solution.

LPWAN and Cellular

For smart city applications in urban areas where cellular infrastructure is omnipresent, having LPWAN and cellular on the same public network pays off in multiple ways. Leveraging the best of both worlds, LPWAN and

cellular can serve a vast spectrum of smart city innovations. For applications requiring only periodical or event-based transmission of small messages, LPWAN is ideal, providing excellent cost and power performance. Examples include smart metering, waste management, intelligent parking, smart lighting, or pollution and disaster management.

On the other hand, for applications demanding high-throughput data streaming, cellular connectivity, especially the upcoming 5G, will be instrumental. Typical examples are surveillance cameras, autonomous drones for security and transportation purposes, connected vehicles and mission-critical voice communications.

LPWAN and Satellite

For IoT applications in harsh, isolated environments such as an offshore oil and gas platform, an integrated LPWAN-satellite hybrid architecture emerges as the most, if not the only viable option to connect granular telemetry networks and forward this data to an onshore backend. While offering seamless and ubiquitous coverage, satellite connectivity mostly pertains to high-bandwidth data communication, alongside the connection of a few critical data points. With this in mind, it is the ideal backhaul option for LPWAN networks at offshore locations where cellular and terrestrial networks are absent.

The architecture works as follows. Data from numerous sensors in the field are collected at a local IoT base station through the LPWAN radio link. The aggregated data is then offloaded to an onshore centralized command center using the satellite link. Marrying LPWAN with satellite systems in this way delivers a solid and cost-effective approach to monitor and manage offshore infrastructures from hundreds of miles afar.

3. Integration into Existing Infrastructures

A wireless IoT network doesn't live in a bubble. Besides connecting standalone assets, a truly versatile wireless solution should be able to interact with legacy, closed-looped automation and control networks to tap into previously siloed operational data. At the same time, it must be able to

interface with and forward data to the preferred backend and applications to derive intelligent insights. This section covers the common challenges and requirements when integrating IoT into an existing infrastructure and what you should look for in a wireless solution to tackle them.

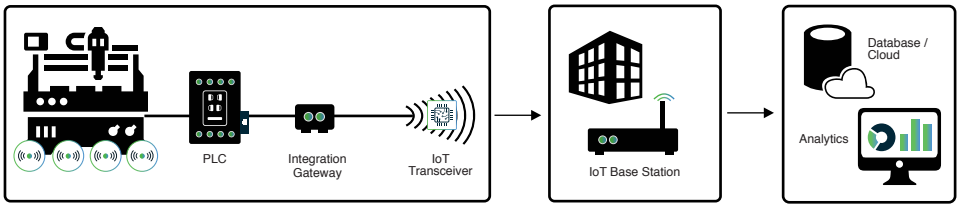
Legacy Control Systems (Operational Technology)

Challenge

Designed in the previous century, legacy assets and systems weren't meant to be connected to the outside world and thus lack effective communication functions. The hassle of integrating IoT solutions with existing operational systems centers around how data is ported across different formats. Many companies struggle to retrofit IoT technologies into legacy equipment such as Programmable Logic Controllers (PLCs) without involving complex, error-prone modifications.

Solution

Plug-and-play IoT connectivity solutions are easing integration tasks with the use of a converter or an integration gateway. On one side, the converter interfaces with brownfield PLCs using automation-specific protocols to gather critical production data. This data is then reformatted and transmitted using reliable, long-range connectivity on the other side. By leveraging such a solution, companies can bypass invasive hardware reprogramming and costly production downtime in a brownfield deployment.



Enterprise IT Systems (Information Technology)

Challenge

Gathering data from legacy operational systems at the edge is only half the battle. Interpreting this data for improved decision making is equally critical. To this end, gathered data needs to be integrated into existing IT infrastructures – whether internal business applications (e.g. enterprise resource planning, building management systems, etc.) or third-party IoT analytics platforms – in a painless and straightforward manner.

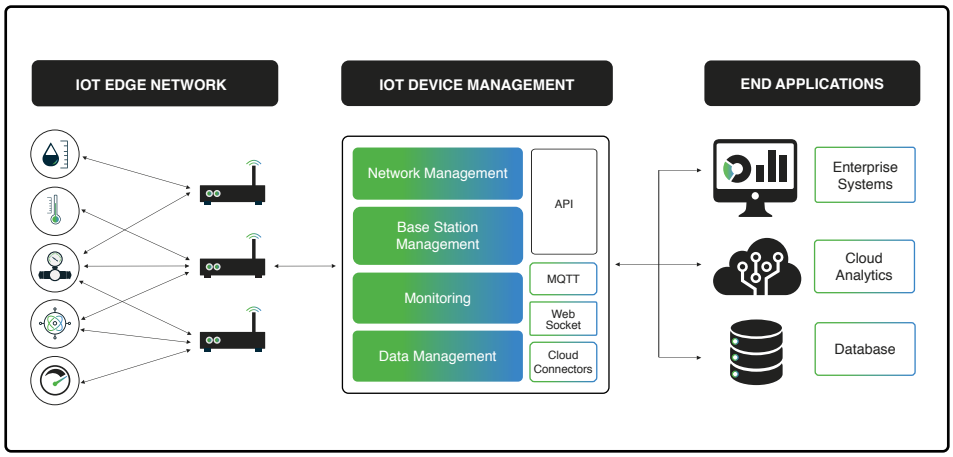
Solution

The device management platform that is specific to each wireless offering is the key to IT integration. As a rule-of-thumb, look for a platform that incorporates embedded Application Program Interfaces (APIs) and native support for open messaging protocols like MQTT.

By establishing the connection between different systems, APIs allow you to use external applications while sticking with your own system and user interface. For example, by interfacing the device management platform with your IT systems using an API, you can execute commands to the IoT devices and network from the convenience of your internal site. Concurrently, MQTT and other open messaging protocols facilitate seamless data transfer to any backend applications and servers of your choice for data analysis and visualization.

4. Device and Network Management

In the last section, we briefly touched on the topic of a device management platform. Given its fundamental, yet often overlooked role in a wireless architecture, it's worth taking a closer look at this IoT component to understand why you need it in the first place.



Simply speaking, a device management platform enables you to perform various network and device administration tasks in a streamlined fashion. When bundled with a connectivity offering, the platform provides everything you need to immediately get the wireless architecture up and running, so

that you can focus on your core expertise. In the IoT data chain, it serves as the bridge between the edge network and downstream IoT applications.

Secure Device On- and Off-boarding

Via a web interface, you can authenticate end nodes and establish secure communications by registering and attaching them to the authorized base station(s) – using their network keys and identification credentials. Only after the onboarding process, is the node permitted to join the network and securely transmit data with network-level encryption.

Streamline Network Monitoring and Troubleshooting

With a single-pane, top-down view of all network traffic, including registered nodes and their status, you can easily monitor and diagnose unexpected issues at both the network- and device-level. For example, if a node intermittently fails to deliver messages, it could mean that the radio traffic is overloaded. On the other hand, if it completely drops out of the network and stops sending messages, there could be a hardware defect or a firmware bug.

Simplify Deployment and Management of Downstream Applications

As mentioned before, an API-driven platform with open interfaces allows for simple integration with any IT backend systems. As such, you can seamlessly deploy and scale IoT applications to adapt to changes in your business requirements – whether adding new devices to the same application or connecting to a new analytics solution. Platforms that offer native cloud connectors also ease data transition to your chosen cloud infrastructure while eliminating duplicated onboarding tasks.

Mitigate Security Risks

A device management platform provides automatic operating-system and security updates from afar, so you can save costs while assuring that remote base stations are best prepared against malicious attempts. On top of that, round-the-clock network monitoring facilitates timely identification of abnormal patterns such as a surge in data traffic that might indicate a breach.

Be aware that there is a great variance in device management platforms depending on your selected wireless option. For example, most don't offer an open architecture with robust APIs and native cloud connectors. On top of that, a platform-agnostic design is an essential factor when examining a device management solution. Such a design maximizes network flexibility and long-term viability by allowing you to deploy the device management tool anywhere you want – whether in a local IoT base station, in an on-premises server, or in a private or public cloud. Equally important, it should provide support for cross-vendor sensors so you can seamlessly integrate new devices in the existing infrastructure along the line.

Security

No IoT conversations are complete without talking about security. Yet, due to its complex nature, many companies might choose to overlook security requirements, while others may try to push it to a later stage of their IoT project. This is a grave mistake, as security isn't and should never be seen as an add-on element in your wireless architecture. Even if you have minimal experience in this realm, the rule of thumb is to opt for a connectivity solution that delivers security by design. This way, you can offload major parts of the security equation while still ensuring your IoT network is well protected.

To help you better grasp the meaning of "security by design", we provide a checklist of some of the most fundamental security features to look for when examining a wireless solution.

End-to-end Data (E2E) Encryption

Encrypting each message with solid cryptographic mechanisms is the foremost condition to safeguard data confidentiality and integrity against eavesdropping during transmission. Data encryption must be applied on any non-IP radio link at the edge (e.g. using AES – Advanced Encryption Standard algorithm), as well as the IP-based connection to the user's backend (typically with TLS – Transport Layer Security protocol).

Device and Message Authentication

To make sure only trusted endpoints can join your IoT network, the wireless protocol must come with rigorous, built-in authentication schemes. Specifically, each device must be assigned with a unique identifier and a network key which are computed to define and validate its identity during the onboarding process, as well as to establish the message authentication code whenever it communicates within the network. With a unique ID in place, each device can also be easily monitored throughout its lifecycle for timely detection of suspicious behaviors.

Message Counter against Replay Attack

A replay attack happens when a valid transmission is maliciously or fraudulently repeated to deceive the receiver into executing wrong actions. The best way to prevent this type of attack is to have a message counter scheme embedded in the wireless protocol. With this, every transmission comes with a unique counter that can't be used again in another transmission.

Jamming Resistant

Jamming is a common type of Denial-of-Service (DoS) attack in wireless networks, where hackers attempt to generate significant radio interference using fake nodes to disrupt intended communications. Here, wireless technology purpose-built for spectrum efficiency and interference immunity is your best bet to be jamming-resistant. Such technology can rule out message errors and data loss even under heavy radio traffic conditions.

Automatic Security Updates

The last thing you want is to expose an IoT base station/gateway that handles millions of daily messages, as an easy target for cyber criminals. Besides firewalls and strong authentication tools, automatic software updates are important to ensure that your base stations are well-armed with the latest security patches to repulse any upcoming breaches.

API/User Authentication

If your wireless network interfaces with external IT applications via API (which in most cases, it does), API authentication is cardinal. Mechanisms like JSON Web Token make sure connection attempts and data requests are only permitted for authorized client servers.

Remember that this is by no means an all-inclusive checklist for IoT security. Instead, it serves as a benchmark for minimum security capabilities that pertain to a wireless network. If a third-party cloud is part of your IoT architecture, there are, of course, other vital considerations to go over.

V

Wrapping Up

While the sheer variety of today's available connectivity offerings can be formidable at first sight, the business cases to be tackled and their specific needs will act as the guiding hand to help you identify the best match. Note that for a future-proof wireless architecture, it's important to consider not only existing requirements but also those that might come up down the road. For example, how much radio traffic will be generated in the near future or can the network grow effectively to support thousands of devices once the need arises?

When it comes to IoT deployments that rely on vast networks of granular, battery-operated IoT sensors amid challenging physical environments, LPWAN emerges as the most pertinent solution. LPWAN has been seen as a crucial catalyst for latency-tolerant industrial and commercial applications like condition monitoring, asset management, smart metering, and environmental monitoring. Nevertheless, even within this wireless family, technologies can greatly vary based on different network criteria. As a general rule, technologies rooted in proven standards offer distinct advantages in terms of Quality-of-Service and long-term interoperability.

Besides the connectivity technology itself, there are other vital factors that constitute a functional, secure and high-performing wireless network. These factors tie the ecosystem and its relevant moving parts to the technology, and they must be incorporated in your wireless decision from the outset. This way, you can select not only the right technology but also the right vendors who will be your partners in the IoT journey.

References

[1] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer. “A comparative study of LPWAN technologies for large-scale IoT deployment, in ICT Express, 2018.

[2] J. Bardyn, T. Melly, O. Seller and N. Sornin, "IoT: The era of LPWAN is starting now," ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference, Lausanne, 2016.

[3] J. Petäjäjärvi, et al., “Performance of a low-power wide area network based on LoRa technology: Doppler robustness, scalability and coverage”, International Journal of Distributed Sensor Networks, 2017.

[4] A. Lavric, “LoRa High-Density Sensors for Internet of Things”, Journal of Sensors, 2019.

[5] European Telecommunications Standards Institute, “Short range devices; Low Throughput Networks (LTN); Protocols for radio interface A”, European Telecommunications Standards Institute, ETSI TS 103 357, 2018.

[6] T. Lauterbach, “MYTHINGS vs LoRa: A comparative study of Quality-of-Service under external interference”, 2019.

BehrTech offers a disruptive wireless connectivity software platform that is purpose-built for massive-scale Industrial Internet of Things (IIoT) networks. At the core of the platform is MIOTY, a new communication technology standardized by ETSI that provides reliable, robust, and scalable connectivity unlike any other technology on the market. With its approach to interoperability, BehrTech makes it easy for end users to retrofit its MYTHINGS platform in any environment and enables partners, system integrators, and VARs to deliver fully-integrated IIoT solutions that enable data-driven decisions to be made.
decisions to be made.

BEHRTECH

www.behrtech.com