

Microwaves & RF[®]

LIBRARY

LEADING LPWAN TECHNOLOGIES

A compendium of articles from the Editors of *Microwaves & RF*

LEADING LPWAN TECHNOLOGIES

A compendium of articles from the Editors of *Microwaves & RF*



DAVID MALINIAK
Technology Editor
Microwaves & RF

INTRODUCTION

The Internet of Things (IoT) that's become ubiquitous in modern life has its better-known aspects, mostly those related to consumer use cases such as smart homes, offices, and buildings. It sure is handy to be able to lock doors, adjust thermostats, and turn lights on or off from remote locations using a smartphone app.

However, a less glamorous, but perhaps more important, realm for the IoT is in industrial and infrastructure applications,

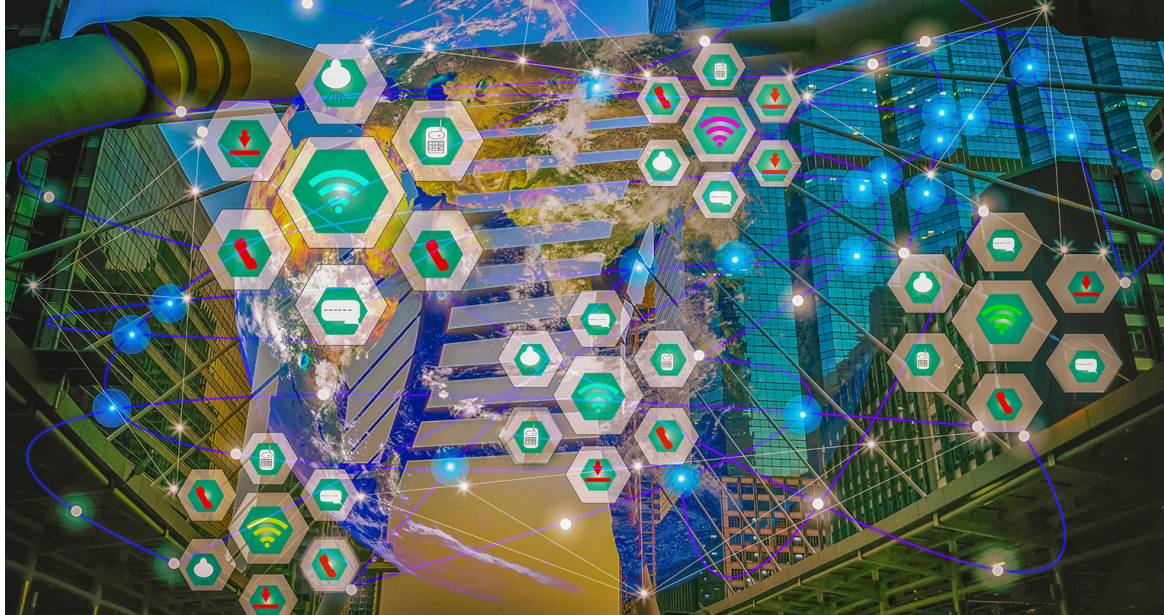
and that's where low-power wireless technologies take center stage. Low-power wide-area network (LPWAN) technologies are the glue holding together a network of sensors, ferrying low-bit-rate data (usually 50 kb/s per channel) over relatively long ranges (10 km or more in rural settings).

Among the chief benefits of LPWAN for the IoT is that devices, or nodes, on the network can operate reliably for as long as 10 to 15 years on a single battery. You might find such devices in applications like smart meters, smart cities, smart agriculture, or asset management use cases. Some of the network protocols that dominate the LPWAN landscape include LoRaWAN, LTE-M, NB-IoT, and ZigBee.

In this eBook, you'll find a collection of informative articles that will jumpstart your knowledge base on LPWAN technologies and use cases. They'll get you up to speed on some of the basics as well as provide some comparisons between various technologies.



CHAPTER 1: THE 4 BUILDING BLOCKS FOR LORA NETWORKS	2
CHAPTER 2: LPWANs HELP REALIZE SUPPLY-CHAIN MONITORING'S POTENTIAL	7
CHAPTER 3: UNDERSTANDING THE UNDERLYING SENSOR AND WIRELESS TECHNOLOGIES IN IIOT APPS.....	11
CHAPTER 4: WHAT'S THE DIFFERENCE BETWEEN BLUETOOTH AND UWB FOR HIGH-SPEED DATA AND MULTIMEDIA?	19
CHAPTER 5: WHAT'S THE DIFFERENCE BETWEEN BLUETOOTH LOW ENERGY, UWB, AND NFC FOR KEYLESS ENTRY?	23



CHAPTER 1:

The 4 Building Blocks for LoRa Networks

RAMYA KOTA, Product Line Manager, Wireless Solutions Group, Microchip Technology

This article introduces the four main elements of LoRa network architecture and discusses some of the most common challenges faced by designers while developing LoRa end-nodes. How can regulatory certified LoRa modules help overcome such challenges?

Long-range (LoRa) technology is extending the reach of the Internet of Things (IoT) by combining long-range wireless connectivity with low-power performance. From smart cities to smart agriculture to supply-chain tracking, LoRa is an ideal choice to create flexible IoT networks that can operate in both urban and rural environments. But how easy is it really to develop a new LoRa solution or migrate to one?

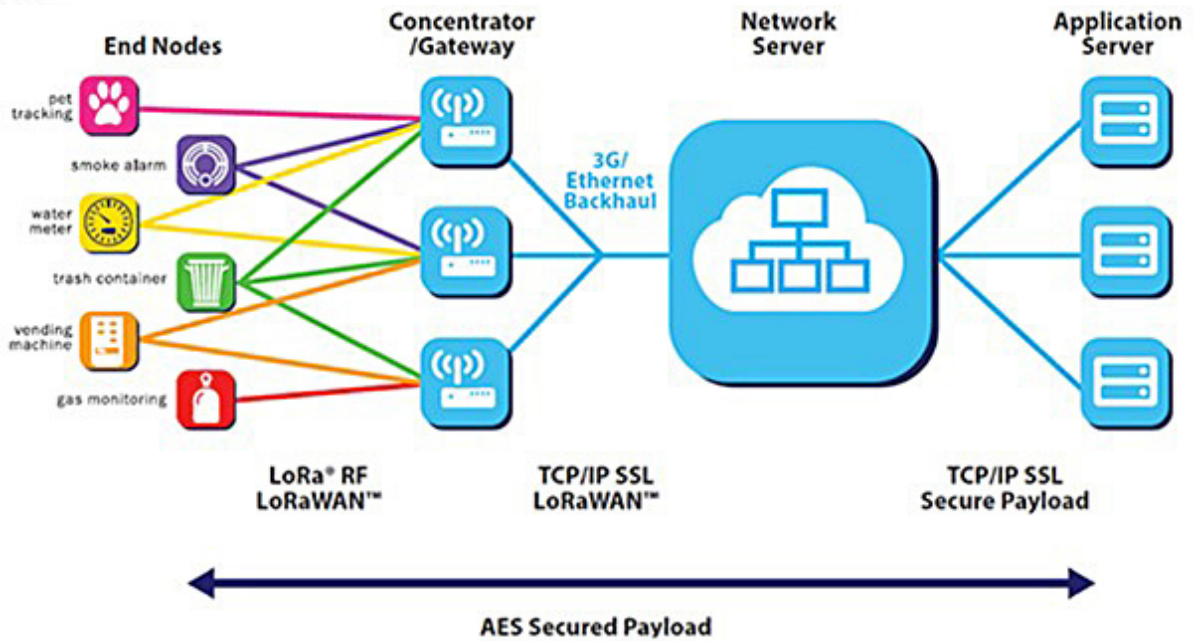
Understanding a new wireless technology and choosing the right solution for your application can be exhausting. Wireless radio-frequency (RF) design usually requires in-depth RF expertise and adds significant development time for designers.

LoRaWAN Network Architecture

LoRa is a wireless modulation technique or physical layer that allows low-power end-devices to communicate over long range. LoRaWAN—a wireless networking protocol that acts as a media-access-control (MAC) layer—is implemented on top of the LoRa physical layer. The LoRaWAN specification details the communication protocol and network architecture and is meant to provide secure communication of end-devices and interoperability within the network.

The LoRa network has four elements (**Fig. 1**):

1. *End-nodes* are elements of the LoRa ecosystem that gather sensor data and transmit/receive the data. They're generally remotely connected and are battery-powered.
2. *The gateway* is a transparent bridge between the end-nodes and network server. Typically, end-nodes use LoRaWAN to connect to the gateway, while the gateway uses high-bandwidth networks such as Wi-Fi, Ethernet, or cellular to connect to the networks.
3. A *network server* connects to multiple gateways. It gathers data from the gateways



1. These are the four main elements of the LoRa network (Source: LoRa Alliance)

and filters out duplicate messages, decides which gateway should respond to end-node messages, and adapts data rates to extend battery life of end-nodes.

4. *The application server* collects data from end-nodes and controls the actions of the end-node devices.

Let's take a closer look at LoRa end-nodes and the challenges in designing them.

Common Challenges in Designing LoRa End-Nodes

End-nodes are simple objects, such as sensors and actuators. Typically, they comprise the “things” within the Internet of Things (IoT). In the LoRaWAN ecosystem, an end-node communicates to the network server through one or many gateways.

LoRa end-nodes are typically low-cost battery-powered applications that need to be power-efficient. Depending on the development time, target costs, power consumption, and RF expertise available, several options are available to build LoRa end-nodes. Before researching those options, let's look at some of the most common challenges that designers face when designing end-nodes. They include:

RF Design

As with any wireless design, significant RF design expertise is needed when designing LoRa end-nodes. When using LoRa systems-on-chip/systems-in-package (SoCs/SiPs), the end-node device developer is responsible for the entire RF design, including schematics, bill of materials (BOM), PCB layout, antenna tuning, and other RF hardware.

Even with the best documentation and application design guides, RF design isn't always easy. It not only requires in-depth RF expertise, but also adds up significant development



time for designers. Furthermore, debugging RF designs most often requires special equipment, adding further to the development costs.

To overcome the RF design challenges, some suppliers offer SoCs/SiPs that are supported by excellent documentation, regulatory certified reference designs, and detailed chip-down design packages. However, for the shortest development time and reduced risk, an RF optimized, tested, and certified LoRa module is almost always the best choice. These modules can provide a complete solution as a single component reducing design risk and development times.

Regulatory Compliance and Certifications

LoRa/sub-GHz radios typically operate in the ISM license-free band. The frequencies vary depending on the region, making it challenging for hardware and software designers. Diligent care must be taken to design a fully compliant solution while keeping the BOM costs minimal. Also, RF regulatory requirements are constantly changing. Thus, keeping up with the regulatory changes, re-testing the devices, and re-certifying for compliance can cost several thousands of dollars—as well as engineering time—for end-node developer companies, money and time that could otherwise be spent on new projects.

Using a certified LoRa module solves this issue easily; the module manufacturer takes care of keeping up with the regulatory requirements and re-certifying modules to the latest specifications. All of these costs and time spent on regulatory compliance can be completely avoided by choosing a regulatory certified LoRa module.

Multi-Region Operation

LoRa devices support several frequencies, depending on the region. Often end-node manufacturers release their end-products in one major region first. Once the demand ramps up, companies investigate expanding the same design in other regions. Having a single SKU that supports multiple regions allows for seamless migration and expansion of the end-product into different countries and regions. A regulatory certified LoRa module that works for multiple frequency bands is ideal for this type of product expansion.

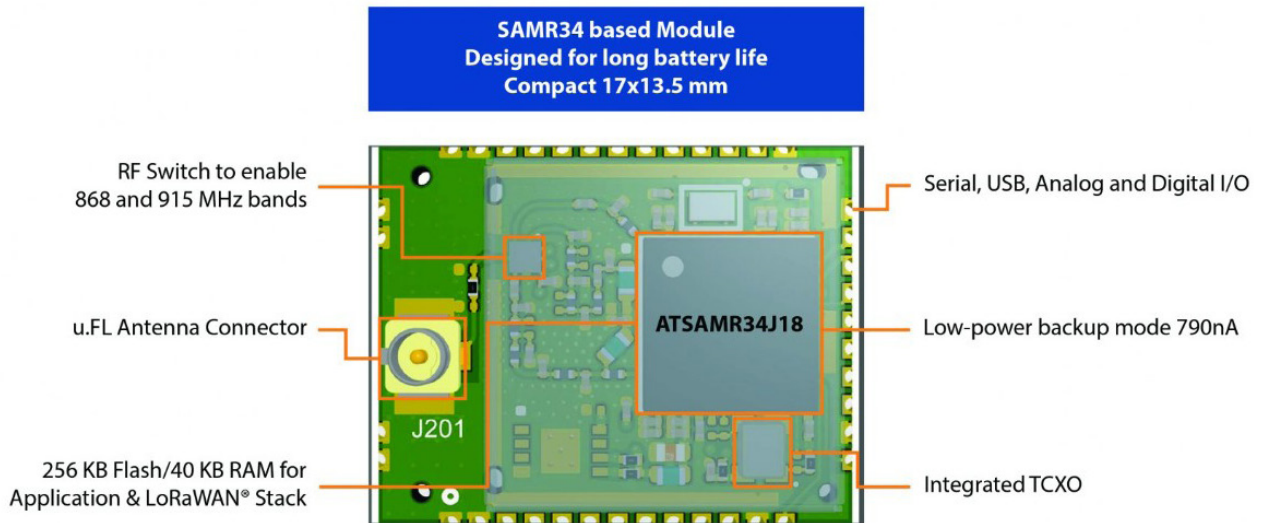
Robust Software

Generally, LoRa modules integrate the whole LoRaWAN stack inside the module. The end-node developer only needs to implement the initialization and communication to the module. With LoRa SoCs/SiPs and with standalone LoRa modules, the stack must either be provided by the manufacturer, or the developer must develop its own stack if no stack is provided.

To minimize software development, it's recommended to choose LoRa modules/ICs that are supported by the manufacturer's LoRaWAN stack. Proven LoRaWAN stacks from manufacturers ensure interoperability of end-nodes with major LoRaWAN networks and gateways, enabling end-nodes to work across different networks with reduced risk.

Migration Path from Modules to SoCs

Many companies start their prototypes and initial production runs with certified modules to reduce risk and get their products faster into market. Once their product starts to ramp up, companies may decide to move to LoRa SoCs/ICs for increased flexibility or lower BOM costs. The migration isn't always easy, so it's very important to consider standalone



2. Shown is the block diagram for the WLR089U0 LoRa module.

modules that allow for simple software migration between the modules and ICs. Also, it's essential to choose suppliers that sell both modules and SoCs; therefore, the development platform, software migration, and support structure remain the same.

Regulatory Certified LoRa Modules Simplify LoRa End-Node Designs

LoRa modules consist of all required radio components along with LoRaWAN stack and RF circuitry, thus helping accelerate development of LoRaWAN end-devices. Since the RF development and the certification are implemented by the module manufacturer, any changes in certification specifications or component replacements are completely handled by the manufacturer, saving tons of development time as well as re-certification costs for end-device manufacturers.

Standalone LoRa modules with highly integrated LoRa ICs provide enough memory to run the application code along with the LoRaWAN stack. This eliminates the need for an external microcontroller, saving board space and system costs. **Figures 2** and **3** show a simple example of such a standalone module.

The [WLR089U0](#) module based on the SAM R34/35 family of ICs from [Microchip Technology](#) is a compact module with 256 kB of flash and 40 kB of RAM, making it well-suited for space-constrained applications. Also, the module includes an integrated RF switch, enabling multi-band operation and allowing the same module to be used across multiple geographies, facilitating market expansion for end-products. The WLR089U0 also is supported by Microchip's LoRaWAN stack and proprietary peer-to-peer software, easing



3. The WLR089U0 LoRa module is based on Microchip Technology's SAM R34/35 family of ICs.




the software development for end-users developing LoRa applications.

Because the modules are based on the SAM R34/35 ICs, the migration path from modules to ICs and vice versa also is much simpler. Choosing such a module helps overcome all of the common design challenges while developing LoRa end-nodes, easing the entire design process.

Conclusion

Developing LoRa end-nodes can be complex and time-consuming. Highly integrated, certified LoRa modules provide an easy and proven approach to overcome the complex challenges involved in designing these end-nodes. Reliable software, larger memory, integrated RF switches, and regulatory certifications are some of the key features to look for in LoRa modules. Choosing a highly certified LoRa module not only helps simplify the design process, but also enables end-node developers to successfully differentiate their products and release them to market faster.

to view this article online,  [click here](#)

 [BACK TO TABLE OF CONTENTS](#)



CHAPTER 2:

LPWANs Help Realize Supply-Chain Monitoring's Potential

PIERRE GELPÍ, Logistics Marketing Group Chair, LoRa Alliance,
and LoRa Business Development Director, Semtech

IoT is enabling a new era of end-to-end supply-chain monitoring and actionable analytics. Low-power, wide-area networks provide the connectivity to make this possible.

Real-time, transparent, and seamless tracking of assets, both indoors and out, while optimizing logistics and supply chains, has long been the focus of innovative companies around the globe. Internet of Things (IoT) technology is on the cusp of ushering in a whole new era of end-to-end supply-chain monitoring and actionable analytics. In particular, the recent emergence of low-power, wide-area networks (LPWANs) is driving this transition.

As the volume of goods transported globally continues to rise, organizations face greater complexity but also more opportunities to optimize their supply chains. The Council of Supply Chain Management Professionals' annual State of Logistics report found that in 2017 in the U.S. alone, total spending on logistics rose to a record of nearly \$1.5 trillion. That's up 6.2% from the year before, and totaling about \$250 billion more than companies spent on logistics in 2008.

Analyst firm Berg Insight reports that the number of active tracking devices deployed for cargo-loading units, including trailers, intermodal containers, rail freight wagons, air cargo containers, cargo boxes, and pallets, reached 6.1 million worldwide in 2018. Growing at a compound annual growth rate (CAGR) of 27.3%, this number is expected to reach 20.4 million by 2023.

The highly diverse supply chain spans a wide range of different attributes and requirements, requiring intercontinental and global solutions. Routine activity encompasses everything from the shipping of large products from factories to distributors and customers to the minutiae of ensuring the tiniest parts arrive punctually at just-in-time production lines.

Supply-chain management also is at the heart of the retail sector: Ensuring stock is available and swiftly dispatched to customers or stores is integral to ensuring the right



equipment is in the right place and in the right condition to enable the activities of many other industries.

As economies combat the COVID-19 pandemic, it will take even greater visibility into supply chains to enable factories that depend on just-in-time delivery of goods to reopen and adapt to new operational requirements.

Supply-Chain Management Demands Greater Visibility

Because traditional patterns can no longer be relied on, facilitating decision-making by providing timely data that can be analyzed and acted upon is a vital capability for manufacturers, retailers, and distributors. Deloitte's "Global Chief Procurement Officer Study 2018" found that only 6% of organizations have full visibility into their supply chain, and 65% of organizations have poor or no visibility beyond their tier-1 suppliers.

To gain further knowledge of their supply chains, organizations need connectivity to freight transport down to the individual package or parcel. Besides being cost-effective, connectivity must be set up rapidly, flexibly, and simply so that networks can be turned on, moved, or switched off as required. In addition, there must be a vibrant developer ecosystem to create the devices and applications around the connectivity that enable data to be gathered and analyzed to deliver actionable insights.

LPWAN Technology Transforms Supply-Chain Management

LPWANs enable low-cost wireless connectivity that makes it viable to add connectivity to lower-value assets as well as traditionally tracked equipment like trucks, shipping containers, and rail freight. The price point means individual lower-value items (or

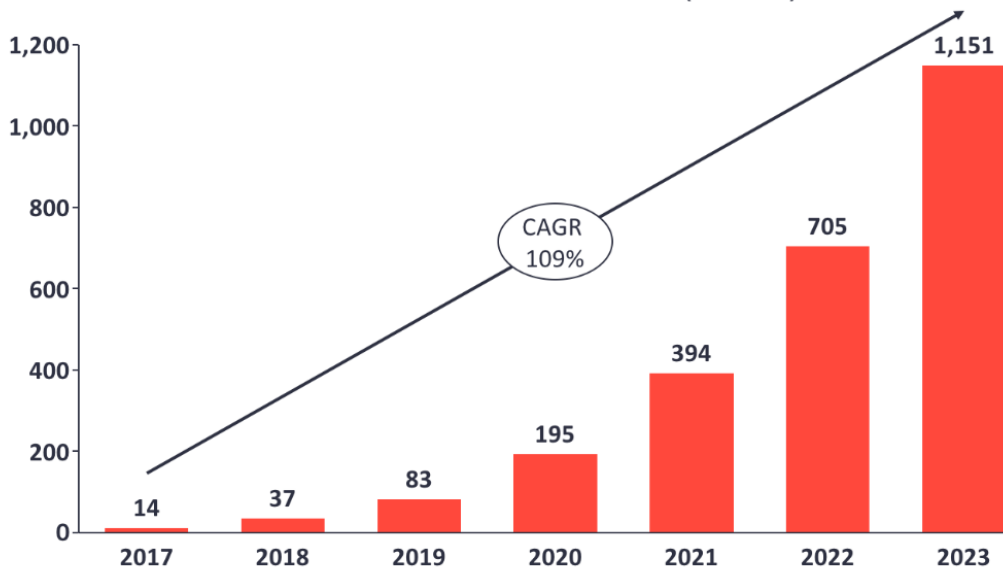
packages of them) can be tracked at a sustainable cost and at enormous volume. In such scenarios, LPWANs can communicate important data for analysis that yields actionable insights into the location, condition, and predicted arrival time of assets.

In **Figure 1**, analyst firm IoT Analytics projects LPWAN connections will exceed one billion in 2023. In contrast to short-range solutions such as Bluetooth and Zigbee, which provide a good solution for hyper-local tracking and tracing of assets, LPWAN connectivity can be enabled many miles from the nearest gateway, thereby covering large industrial sites.



Global LPWAN Market Size 2017-2023

Global LPWAN Market Size in # of connected devices (millions)



1. Projections assert that the number of LPWAN connections will exceed one billion in 2023.

(Source: IoT Analytics)



Cellular solutions, which are near-ubiquitous, are more complex to manage globally. They require roaming agreements between multiple providers and often necessitate adoption of multiple technologies across the GSMA stack of protocols. 4G and 5G are not fully rolled out and, where available, remain relatively costly solutions for low-value asset tracking both in terms of connectivity and module cost.

Satellite solutions offer excellent global coverage and are ideal for tracking higher-value, larger assets. In these cases, the higher cost of satellite connectivity makes sense and the larger device size, including antennas, can be more easily accommodated. An example might be a truck or a shipping container. However, for smaller packages, the power requirements, antenna size, and cost make satellite-based approaches unsuitable.

LPWAN Isn't One-Size-Fits-All

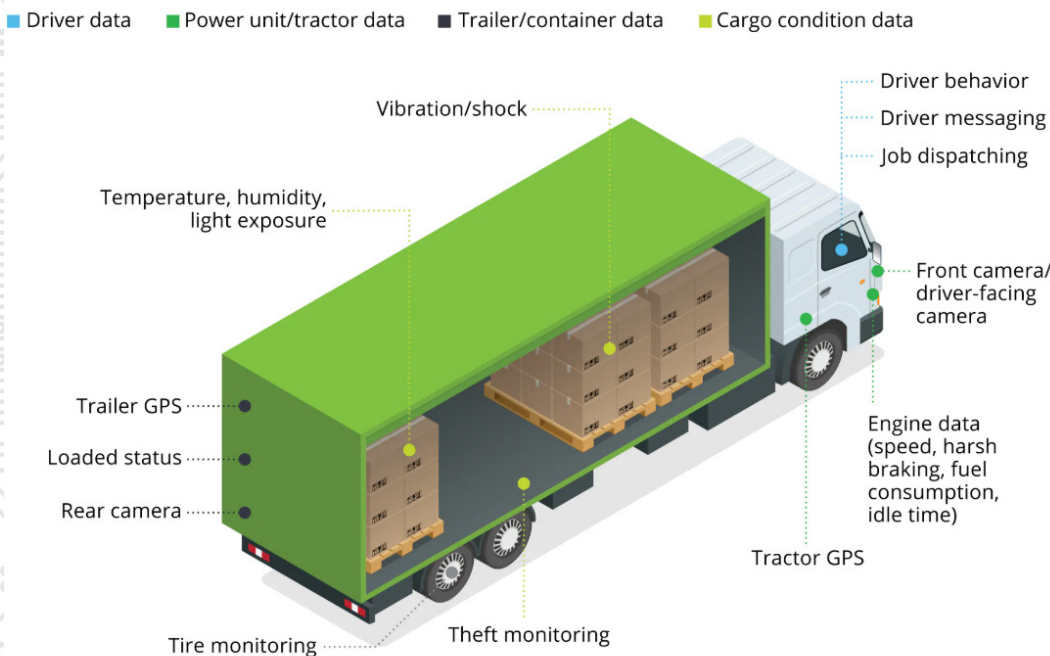
The LPWAN tag describes a number of different technologies that have low-power, wide-area attributes. This field is becoming increasingly crowded with options such as narrowband IoT (NB-IoT), Sigfox, and LoRaWAN, each of which must be carefully evaluated for the application at hand.

LoRaWAN specifically is an excellent fit because it brings together competitive cost with the capability to handle extremely high device density at a given site. Think of a logistics facility with the tens of thousands of containers, assets, and parcels that traverse it daily. The ability to have deep indoor coverage, which is vital inside the large warehouses that form the core of international logistics, some of which involve underground capacity, is extremely valuable. LoRaWAN can penetrate these large buildings, ensuring uninterrupted asset tracking.

At these facilities, LoRaWAN offers the option of public or private networks, which is attractive to large site operators because it can drive economies, assure performance, and is perceived to be highly secure. In either type of deployment, it's worth noting LoRaWAN's mature security, which has been developed over many years.

A further strength of LoRaWAN devices is their typically very long battery life. It makes them ideal for multiple long journeys, such as for the months involved in intercontinental shipping, or for more complex applications like daily updates on the location and status of a truck (Fig. 2).

An IoT-enabled fleet vehicle



2. Shown are the typical connected devices that feed supply-chain management from an IoT-enabled fleet vehicle. (Source: Deloitte)



Asset tracking isn't performed in controlled environments and logistics, and by its nature involves shock, vibration, temperature extremes, and other factors otherwise not present in smooth, non-mobile environments. LoRaWAN is rugged, so it can continue to operate in most extreme situations.

How LoRaWAN Delivers Supply-Chain Benefits

LoRaWAN provider Semtech has supplied a car manufacturer with connected racks used in the vehicle-manufacturing process. These racks, which typically have an active life of 10 years, are used to transport key components such as gearboxes from their point of manufacture to the assembly plant. These racks cost about €500 and manufacturers use hundreds of thousands of them. Approximately 10% are replaced each year, resulting in €10 million in operating expenditures.

Semtech also has supplied Pallet Alliance, a provider of pallet-management programs for multi-site organizations, with its IntelliPallet, an IoT-based pallet-monitoring platform. The platform integrates location and environmental sensors into wooden pallets, which comprise more than 90% of the worldwide palletized shipping market. The flexible LoRaWAN-based platform offers customized tracking capabilities, including entry and exit notifications from a geo-fenced area, stationary time and arrival/departure from designated hubs, and environmental monitoring for factors including temperature, humidity, and motion.

Another LoRaWAN supply-chain example can be found at United States Cold Storage (USCS), a provider of public refrigerated warehousing (PRW) and logistics services. The company wanted to offer enhanced visibility into shipments of perishable goods as part of its integrated third-party logistics service offering.

LoRaWAN network operator Senet and NanoThings—a developer of long-range, temperature-tracking smart labels and a platform to monitor temperature and manage cold chains with inter-company communication—have partnered to combine the affordability and small form factor of NanoThings' NanoTags with LoRaWAN network connectivity to address USCS's needs. The partners provide customers with autonomous temperature monitoring and touchpoint tracking that could transform how data on perishable goods is collected and used throughout the retail supply chain.

The Connected Supply Chain of the Future

LoRaWAN and other LPWA technologies imbue supply-chain management with the power to continuously connect items in transit and cost-effectively monitor them globally for the lifespan of the device. These capabilities have the potential to radically transform the industry. To date, visibility has been obtained by tracking large assets such as shipping containers, trucks, or rail wagons. LPWANs open the next stage of opportunity by enabling connectivity down to the individual item to be viable.

This isn't a high-bandwidth, multimedia experience. Rather, it's the simple transmission of data, robustly and securely, that can feed supply-chain management systems with a flow of accurate data that informs important decisions. Its value will be proved in increased efficiency, greater accuracy, and fewer failures because of lost assets or spoiled goods.

to view this article online,  [click here](#)

 [BACK TO TABLE OF CONTENTS](#)



CHAPTER 3:

Understanding the Underlying Sensor and Wireless Technologies in IIoT Apps

TINU OZA, Product Manager, L-com

This article details some of the more common industrial IoT applications that utilize wireless sensor technology to control, monitor, and report on critical processes and control functions.

From the connected home and smart wearables to Industry 4.0 and smart-city applications, wireless sensor networks (WSNs) permeate nearly every conceivable application. They bring automation to simple manual tasks with remotely controlled actuators and monitoring/tracking environments with evolving microelectromechanical-systems (MEMS) sensors. These relatively simple, energy-constrained devices reveal a massive potential in data collection and data analytics to better assess human, machine, and even plant systems.

In industrial IoT (IIoT), short-range wireless solutions, cellular, and low-power wide-area networks (LPWANs) can be leveraged to support the various sensor nodes. The choice of industrial communications depends on whether the process is time-critical with the need for real-time data or is non-time critical with either frequent or infrequent transmissions. Depending on the industrial application at hand, there are numerous IIoT use cases in which many sensor technologies and/or communication protocols may be brought to bear (Fig. 1).

Process Monitoring

Process monitoring is likely to be the largest application for industrial WSNs (IWSNs) as it requires the placement and tracking of thousands to tens of thousands of sensor nodes over vast distances. This centralized method of tracking industry operations is what leads to realizing predictive maintenance strategies that systematically minimize factory downtime and save on operational overhead.



IIoT Use Case	Applications	Potential Technologies	Potential Protocols
Process Monitoring/ Predictive Maintenance	Machine health monitoring (precision CNC, conveyor belt)	Temp Sensor Camera Humidity Sensor Pressure Sensor Level Sensor Gas Sensor Proximity Sensor Acoustic Sensor Chemical Sensor Accelerometer	LPWAN WirelessHART ISA 100.11a Cellular Zigbee
	Asset Monitoring (hydraulic hose, pipeline, wellhead, steam trap, corrosion/ structural integrity, seismic monitoring, tank level)		
	Remote visualization (force sensors, laser measurement devices, cameras)		
Facility Management	Health and Safety Monitoring (emissions/toxin)	Gas Sensor Chemical Sensor	WiFi Cellular Bluetooth
	Environmental Monitoring/Control (lighting, HVAC, smart metering)	Light Sensor IR Sensor Camera	ISA100.11a WirelessHART LPWAN
	Perimeter Security		
Inventory Management	Asset Tracking (RTLS)	Bluetooth beacons RFID Camera IR Sensor	Bluetooth WiFi UWB
Fleet Management	Delivery truck tracking, passenger car tracking, route development	GPS Module	Cellular LPWAN NB-IoT LTE-M1

Machine-Health Use Cases and Common Sensor Types

Hyper-specialized equipment is leveraged all over IIoT because monitoring common faults is critical to maintain optimal performance of machine equipment. For instance, while a high-end computer-numerical-control (CNC) system can perform precision machining on a massive scale, it can encounter the common faults of spindle unbalance.

Should such a fault occur, the mass unbalance in the spindle system can cause the machine tool to vibrate, ultimately degrading machine accuracy and potentially causing further machine damage if left unrepaired.¹ Typically, the bearings within the spindle are analyzed for vibrations as they allow the shaft to stay in place while rotation occurs—uncharacteristic vibrations would therefore be apparent with these components.

Accelerometers are able to monitor and detect such machine-tool failures by collecting vibration data. Ultrasonic and acoustic emission sensors can detect damage within the bearings of the spindle before any noticeable vibrations occur by discerning the ultrasonic acoustic emissions resulting from metal degradation. Armed with knowledge of the nominal thermal operation, temperature sensors can also note temperature anomalies in various critical components within the machine. An inductive current sensor would detect variations in the current consumed by the electrical motor, too, and similarly detect anomalies.

¹ Depending on the industrial application at hand, there are numerous IIoT use cases in which many sensor technologies and/or communication protocols may be brought to bear.



These same principles can be applied to any large machine that includes a large electric motor. Cranes, for instance, are often used in manufacturing facilities to move large, heavy equipment from passenger cars to airplanes. Pulleys and electric motors will be found in conveyor belts that are leveraged in a broad array of applications including coal mining, food processing, and chemical segregation. Accelerometers, temperature sensors, and inductive current sensors are all useful in adequate monitoring of such machines.²

Asset-Monitoring Use Cases and Common Sensor Types

Oil and gas manufacturers monitor assets such as pipelines over vast distances. In this application, leaks and ruptures are avoided at all costs to prevent the potential loss of life and damage to the environment. Pipelines have several significant failure modes, including construction/manufacturing defects; damage during installation; corrosion; and earth forces such as earthquakes, land slips, and extreme weather-related incidents.³

External accelerometers can monitor the pipeline’s flow rate by tracking flow-induced vibrations. Crack monitoring can be accomplished through ultrasonic detection or transverse magnetic-flux leakage. Failures due to corrosion can be prevented through several sensors with technologies like RFID and fiber optics. Seismic sensors can provide a subsurface map for offshore drilling rigs, improving rig efficiency.

In chemical, food, and pharmaceutical processing facilities, mixing tanks rotate chemicals and ingredients that are added in precise values. Sensors placed at key locations on these tanks measure parameters such as temperature, humidity, pressure, pH value, and fill level, thus ensuring optimal plant operational procedures with little to no manual intervention.

Table 1

Wireless Technologies Used in IIoT

Parameters	Operating Frequency	Maximum Range	Throughput	Latency	Bandwidth	Battery life	Device #
WirelessHART	2.4 GHz	~200m	250 kbps	10-50 ms	3 MHz	several years	30,000
ISA 100.11a	2.4 GHz	~200m	250 kbps	~ 100 ms	5 MHz	several years	unlimited
LoRa	915 MHz (US), 868 MHz (Eur), 433 MHz (Asia)	5-20km	0.3-50 kbps	-	7.8-500 kHz	10+ years	50,000
NB-IoT (LTE Cat NB2)	Cellular bands	1- 10 km	159 kbps	1.6-10s (NB1)	180 kHz	10+ years	100,000
LTE-M2 (LTE Cat M2)	Cellular bands	>11 km (M1)	4 Mbps (DL), 7 Mbps (UL)	10-15ms (M1)	5 MHz	-	>>100,000
Sigfox	868 MHz, 902 MHz	>50km	100-600 bps	-	100-600 Hz	10+ years	-
Bluetooth 5 Low Energy	2.4 GHz	<200 m (PtP), <1.5km (mesh)	1 to 3 Mbps	<3ms	~ 2 MHz	-	32,767
WiFi	2.4, 3.6, 4.9, 5, 5.9 GHz	< 300 ft	>54 Mbps	1-3ms	~22 MHz	-	-

- 802.15.4-based
- LPWAN
- Popular Protocols



IIoT protocols for process monitoring vary greatly depending on the application. **Table 1** lists some commonly used IIoT protocols and some of their respective key parameters. Oftentimes, WSNs monitor machine health within a facility that, when compared to some asset-monitoring applications such as tracking pipeline health, is contained within a relatively small area.

In cases where small payloads of data are transmitted infrequently, LPWANs such as LoRa, Sigfox, and NB-IIoT offer narrowband modulation schemes at sub-gigahertz frequencies—two qualities that increase signal range. The LPWANs are known not only for large transmission distances, but also for long battery lifetimes beyond 10 years and one-to-many architectures in which thousands of devices can be wirelessly connected to a gateway (when sensor nodes can be deployed on the scale of tens of thousands, energy-harvesting techniques and battery lifetime are critical considerations).

However, LPWAN protocols are often asynchronous with unscheduled transmissions. Thus, they're susceptible to data collisions at high network capacities. This would not be ideal for time-critical IIoT applications that require deterministic and reliable transmissions with a low bit error rate (BER). Industry-specific wireless networks such as WirelessHART and ISA100.11a are based on IEEE 802.15.4, low-rate wireless personal-area networks (LR-WPANs). With a maximum range of 200 meters, these offer up to a 250-kb/s throughput and latencies of 10 to 100 ms for more real-time communication on critical processes.

Health and Safety

Monitoring the environmental conditions with the respective intelligent alarm installations is essential in protecting industrial workers and maintaining smooth operations. This often involves the use of gas/chemical-based sensor nodes around areas of particular risk.

In the oil and gas industry, tracking highly combustible methane leaks is paramount in preventing any potential explosions around wellheads. Steam traps leverage a huge range of manufacturing facilities to filter out condensate from air without letting steam escape. A faulty steam trap would fail to remove water droplets from steam, causing water to accumulate and rupture steam lines, leading to expensive downtime and safety hazards.

Acoustic sensors and temperature sensors have been used to monitor the behavior of these critical components to prevent any costly failures. Underground mines are notorious for hazardous safety conditions; environmental parameters such as carbon-monoxide emissions, methane emissions, and airflow are actively monitored to ensure a safe working environment.

Reliable and deterministic protocols are necessary for these applications, often calling for WirelessHART or ISA100.11a communications within the facility. While these protocols may consume more power on sensor nodes than other WSN technologies such as Bluetooth Low Energy (BLE) or LPWANs, the ability to perform real-time analysis and control on data is critical to ensure adequate safety measures.

Both WirelessHART and ISA100.11a were specifically designed for industrial applications. WirelessHART is the wireless alternative to the existing HART technologies and ISA100.11a was developed by the International Society of Automation (ISA) to support multiple protocols already used in industrial applications, including HART, Modbus, Foundation Fieldbus, and Profibus. Both networks support star and mesh networking with bidirectional communication from the host to the sensor node.⁴



Asset Tracking with RTLS

Compared to outdoor tracking systems that rely on GPS and typically yield an accuracy around 10 m, indoor position systems (IPSs) such as real-time location systems (RTLSs) can achieve accuracies on par or lower without the major consideration of satellite signals penetrating factory walls. **Table 2** below lists some of the more commonly used RTLSs.

Table 2
RTLS Technologies

RTLS Technology	Accuracy	Real-time Tracking	Range
Bluetooth	1m to 4m	Yes	~75m
WiFi	5m to 15m	Yes	~50m
UWB	sub-meter	Yes	~50m
Passive RFID	<1 m	No	~50m

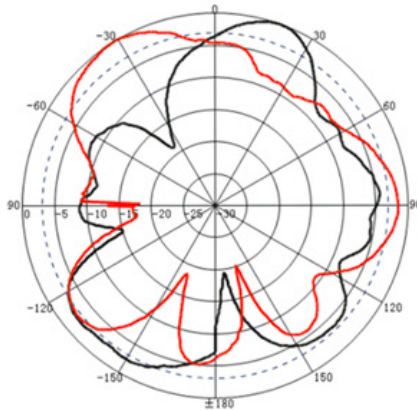
Such IPSs can be applied on the plant floor to actively track moving indoor equipment like forklifts and actively track inventory in transport within a facility. Outdoor environments, e.g. truck yards, can leverage RTLSs to monitor and manage truck movement by assigning docks and tracking loading/unloading of cargo.

Indoor positioning systems will employ either a trilateration or a fingerprinting localization method, depending on the wireless protocol in use. Trilateration uses estimated distances to calculate the likeliest coordinates of an object. The fingerprinting method compares current signal characteristics with a previously catalogued set of signal characteristics obtained from fingerprint locations—implementing this is often more technically involved. The movement of a sensor can then be obtained by comparing the online measurements with the “fingerprint.” For brevity, this section will cover two popular RTLS protocols: Bluetooth and Ultra-wideband (UWB).

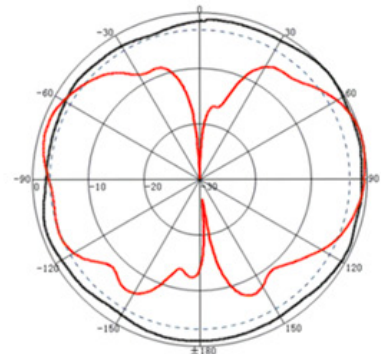
Leveraging a UWB system for RTLS

Ultra-wideband (UWB) technology essentially sends a burst of energy of extremely short duration ($< \text{ns}$), resulting in a broadband signal. Sending out wideband bursts of energy would typically be a power-hungry process. However, a UWB system can be engineered to produce a low probability of detection (LPD) RF signature with a low energy density that doesn’t interfere with neighboring equipment.

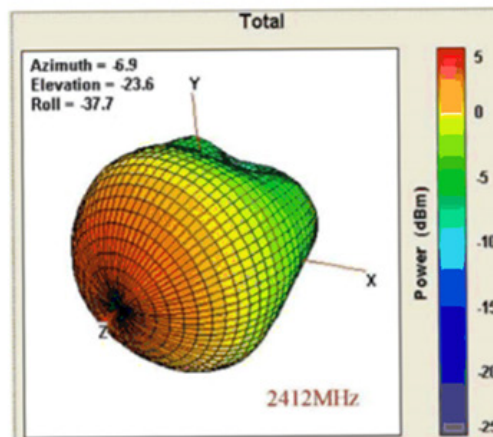
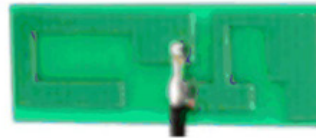
For RTLS applications, the short pulses in UWB modulation allow for precise delay estimates, ultimately yielding position/location data. Typically, UWB technology leverages time-of-arrival (ToA) and time-difference-of-arrival (TDoA) information generated by tags that emit low-power UWB pulses which are received by the sensors or UWB readers. Those pulses are used to determine the precise 3D location for a tag with centimeter accuracy. However, precise time synchronization is needed between the UWB readers



Radiation Pattern at 2.4 GHz
Gain: 5.64 dBi



Radiation Pattern at 2.4 GHz
Gain: 3.87 dBi



Radiation Pattern at 2.412 GHz
Gain: 2.5 dBi

2. Bluetooth PCB antennas with an omnidirectional radiation pattern are often suitable due to the 360-degree beam coverage over the factory floor.



within a network to successfully gain location data.

The UWB frequencies have frequency allocations between 3.1 and 10.6 GHz. Typically, a planar monopole antenna is employed in these applications due to their omnidirectional radiation pattern and ability to yield stable input impedance over the large frequency bandwidth. Because of their performance into the X-band and the fact that trace dimensions grow smaller at higher frequencies, these antennas offer a small form-factor solution that can be printed on the same PCB holding the transmitter/receiver.⁵

Bluetooth Beacons

While already a prolific short-range protocol, BLE modules are utilized in RTLS applications by delivering Bluetooth beacons to disseminate localized content. These beacons can act as proximity sensors by broadcasting low-energy signals with packets of data at predetermined intervals of time (>100 ms).

Distances are calculated with received signal-strength indicator (RSSI) readings, ultimately extrapolating distances between nodes based on the mathematical relationship between the strength of the received signal and the propagation of an RF signal through space.⁶ This creates a live map of inventory outfitted with unique IDs and BLE tags with actively updated location data. Because most smart devices are Bluetooth-enabled (i.e., smartphone, tablet, laptop), this can potentially eliminate the need for custom hardware, leading to dramatic cost savings.

While BLE does support mesh topologies with bidirectional communications, BLE beacons generally support one-way communications and are therefore limited to star topologies. In such configurations, beacons connect to a Bluetooth-enabled device/router and relay information to the cloud, typically via cellular or Wi-Fi.

As alluded to earlier, many of these beacons can include multi-protocol SoCs with a sub-gigahertz, long-range wireless network to control/monitor factory environments with smart lighting or HVAC control. The large window for the advertising packet can allow for the sub-gigahertz radio to be in a receiving state, obtaining non-frequent and unpredictable packets of information from distant locations within the facility.

Typically, BLE beacon designs will involve a 2.4-GHz PCB antenna combined with a vendor-specific Bluetooth chip. In some cases, the Bluetooth chip will have an integrated chip antenna. If the board employed a sub-gigahertz frequency protocol, a PCB antenna would not be viable as it would be too large.

As stated earlier, BLE typically uses trilateration (RSSI) to determine location areas. In this case, an omnidirectional radiation pattern is often suitable due to the 360-degree beam coverage over the factory floor, so long as the antenna matches the transmitter's impedance for maximum signal transfer and range (**Fig. 2**). However, a TDoA algorithm can be implemented, calculating either two angles from a singular beacon signal, or three angles from two beacon signals. In this case, a 3D map can potentially be created with the use of the complex mapping and placement of BLE beacons outfitted with more sophisticated antenna arrays.⁷

Fleet Management

Industrial fleet management can vary with passenger cars, tractor trailers, railways, airplanes, ships, and heavy equipment. Trucks alone account for 70% of the goods transported in the United States, making tracking logistics such as repairs, replacements,



and scheduled maintenance all the more important to prevent poor fleet operation. Typically, the cellular infrastructure is used for applications that transcend plant-wide boundaries. However, in the case of localized equipment such as heavy equipment operation within a mine, LPWANs can be considered.

Fleet telematics can communicate with 2G, 3G, and 4G infrastructures or IoT-specific cellular alternatives such as NB-IoT or LTE-M1. Sensor nodes can consist of GPS modules, gyroscopes, level sensors, and accelerometers. Where the GPS provides location data, the accelerometer offers the orientation of the vehicle, and the level sensor measures fuel in real time. More complex systems are also utilized for fleet management; autonomous mining trucks have been in operation since 2008, outfitted with over 200 sensors, a GPS receiver, and radar guidance system.²

Summary

An array of sensors and communication protocols can serve industrial networks depending on the required level of reliability, latency, and flexibility. Process monitoring and health and safety applications often require real-time communications with IEEE 802.15.4-based protocols (e.g. ISA100.11a, WirelessHART), while some asset-monitoring applications can benefit from the long range offered by LPWAN applications.

Indoor asset-tracking applications have specific localization systems with ToA- or RSSI-based algorithms for accuracy. Fleet-management systems, on the other hand, can rely on GPS for location data but must transfer all sensor data to a centralized point via either cellular backhaul. They can even benefit from LPWAN if the fleet is based in a restrictive geographic location.

References

1. Wang, Zhan, et al. "Optimization and Experiment of Mass Compensation Strategy for Built-In Mechanical On-Line Dynamic Balancing System." *Applied Sciences*, vol. 10, no. 4, 2020, p. 1464., doi:10.3390/app10041464.
2. Zhou, C et al. "Industrial Internet of Things: (IIoT) applications in underground coal mines." *Mining engineering* vol. 69,12 (2017): 50-56. doi:10.19150/me.7919
3. Kishawy, H. and Gabbar, H., 2010. Review of pipeline integrity management practices. *International Journal of Pressure Vessels and Piping*, 87(7), pp.373-380.
4. Peter M (2017) Industrial wireless mesh network architectures. L-com Global Connectivity. https://www.l-com.com/images/downloadables/white-papers/wp_wireless-industrial-mesh-networks.pdf
5. Y. Lu, Y. Huang, H. T. Chattha and P. Cao, "Reducing Ground-Plane Effects on UWB Monopole Antennas," *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 147-150, 2011, doi: 10.1109/LAWP.2011.2119459.
6. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura and A. A. F. Loureiro, "Localization systems for wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 6-12, December 2007, doi: 10.1109/MWC.2007.4407221.
7. https://www.bluetooth.com/wp-content/uploads/Files/developer/1903_RDF_Technical_Overview_FINAL.pdf

to view this article online,  [click here](#)

 [BACK TO TABLE OF CONTENTS](#)



CHAPTER 4:

What's the Difference Between Bluetooth and UWB for High-Speed Data and Multimedia?

DR. FREDERIC NABKI, Co-Founder and CTO, SPARK Microsystems

For nearly 20 years, Bluetooth has dominated as the short-range technology for wirelessly connected devices. But UWB's latency and power-efficiency advantages position it as a compelling alternative with faster, freer dataflow and low power consumption.

Bluetooth and ultra-wideband (UWB) short-range wireless technologies both rose to prominence at the turn of the century, and their development paths have been driven by the unrelenting need to reduce power consumption and extend battery life for an endless proliferation of wirelessly connected devices.

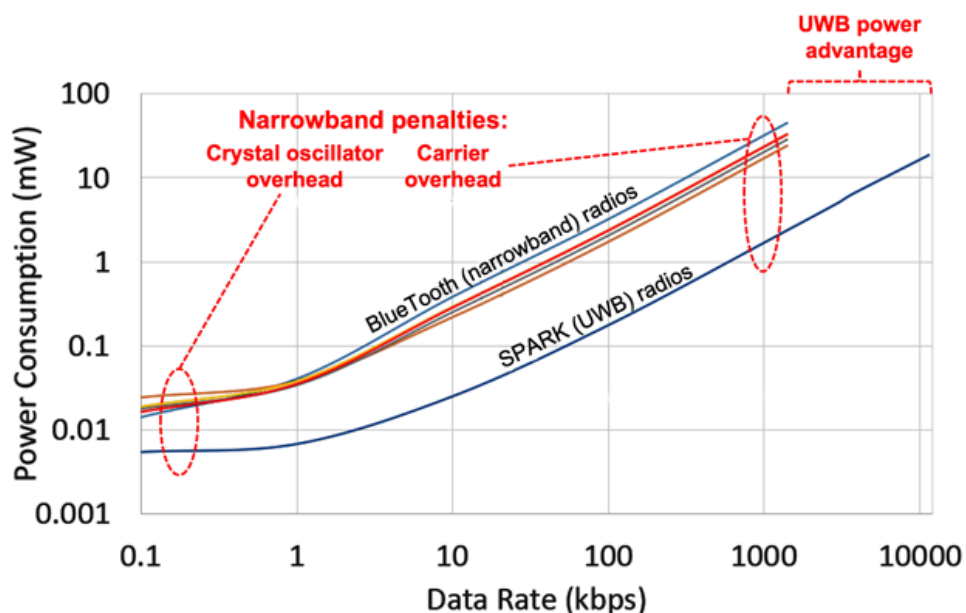
Bluetooth Low Energy (BLE) was ratified in 2006 to address the early power-consumption deficiencies of Bluetooth. More recently, Bluetooth 5.2 added features to reduce consumption for targeted applications like audio. However, these modifications are strictly incremental. Fundamentally, reductions in power consumption are physically limited by the Bluetooth architecture—a carrier-based transceiver will always require a significant amount of power to start, stabilize, and maintain its RF oscillator.

The **figure** on the next page shows the two significant power penalties inherent to all narrowband radio architectures, including Bluetooth.

First, crystal oscillator overhead (*lower left*) cripples low data-rate performance. Bluetooth uses a ~20-MHz crystal oscillator, which requires a few milliwatts to power. When efficiently optimized, UWB radios can operate with impulses that don't require a high-frequency crystal oscillator and can be designed to operate with a low timing power-consumption overhead. Much depends on the UWB optimization technique, though, so this is an area that should draw scrutiny.

Many of today's UWB technology implementations must in fact use higher-frequency crystal oscillators than what's required for BLE. Meanwhile, advanced UWB implementations can utilize crystal oscillators down to 32-kHz timing.

Second, the modulated carrier overhead (*upper middle in the chart above*) penalizes



These are the two significant power penalties inherent to all narrowband radio architectures, including Bluetooth.

high data-rate performance. Transmitting a large amount of data over a narrow bandwidth channel such as that used in Bluetooth radios requires lots of time and power.

Large amounts of data can be transmitted with UWB far more quickly because it's spread across a wide bandwidth, keeping the transmitter on for a much shorter duration and significantly reducing power consumption. This means for the same amount of consumed power, UWB can transmit much more data (*far upper right*).

This owes to the time-frequency duality, well encapsulated by the Fourier transform. In simple terms, this duality states that if you have an infinitely long periodic time signal, it will have an infinitely small bandwidth. On the other hand, if you have an infinitely short impulse signal, it will have an infinitely large bandwidth. In other words, you can trade time for bandwidth.

Ultra-wideband enjoys a clear inherent advantage over narrowband given its allocation and support over a large portion of radio spectrum. A UWB signal is defined as a signal having a spectrum larger than 500 MHz. In the United States, the Federal Communications Commission (FCC) in 2002 authorized the unlicensed use of UWB in the frequency range from 3.1 to 10.6 GHz.

UWB systems use short-duration (i.e., nanosecond timescale) electromagnetic pulses for high-speed transmission and reception of data over large bandwidths. They also have a very low duty cycle, which is defined as the ratio of the time that an impulse is present to the total transmission time.

Bluetooth vs. UWB for Positioning

After two decades of maturation, Bluetooth today is nearly ubiquitous in the battery-powered wireless-device market, spanning smartphones/tablets, earphones/headsets, gaming peripherals, IoT sensors, and more. For wireless apps that could get by with high



latency and highly compressed audio signals, Bluetooth has delivered an acceptable user experience for some wireless apps. However, it could be argued that Bluetooth has reached its point of diminishing returns.

Today, UWB is emerging as a compelling successor to Bluetooth/BLE for the next generation of low-power short-range wireless applications. Consumer electronics manufacturers like Apple, Samsung, and others sure to follow are leveraging UWB spectrum for the delivery of electromagnetic impulses for applications like positioning for object/asset tracking, as exemplified by Apple's AirTags. This is a narrow application of UWB's technology potential, but nonetheless an effective one.

In this capacity, UWB measures time of flight (ToF): an impulse is sent from one device to another, and we measure the time it took from transmit to receive. The distance between objects is determined accordingly, and this can be measured with picosecond accuracy with UWB chips. Leveraging onboard antennas, measurements are then able to be correlated to determine a signal's angle of arrival, and UWB "tagged" objects can consequently be located with accuracy down to a mere 10 cm.

Bluetooth technology comes nowhere close to matching this precision, as it utilizes received signal strength (RSS) to measure spatial distance. RSS is a very simple technique to implement and can be used by any wireless transceiver, which explains why it's so widely used. However, it's severely limited in its accuracy: The perceived distance between two immobile objects will change according to obstacles in their direct path, and BLE typically achieves positioning accuracy only to within several meters.

Positioning technology enabled with UWB—while extremely accurate—is exceedingly complex from a design perspective and therefore extremely power hungry. As a result, UWB chips used today for object tracking are actually less power-efficient than Bluetooth chips/radios by as much as 10X. So, while UWB is well-suited for positioning, it's a power-intensive application by nature and at the end of the day, there's no device-level power benefit delivered with UWB.

UWB for High-Speed Data and Multimedia Communication

The aforementioned time-frequency duality expresses how time and bandwidth are interchangeable. If one wants to compress in time a wireless transmission, it requires more frequency bandwidth. This property can be used to increase the accuracy of positioning and ranging, but these capabilities represent a mere sliver of UWB's potential.

Another very interesting capability enabled by the time-frequency duality is that it can reduce the latency in systems. This has huge implications for untold short-range wireless applications into the future.

Impulses delivered over ultra-wide bandwidth ensure extremely low latency—these signals can be sent in microseconds with UWB, whereas Bluetooth would take milliseconds. The end result is ultra-efficient wireless data communication. What's more, UWB implementations have demonstrated at least 10X less power consumption than BLE for non-positioning applications.

Bluetooth's latency penalties will only persist for applications like gaming, audio, and IoT, which is the chief reason why wired connectivity has lingered so stubbornly for peripherals and sensors used in these applications. We welcome the freedom of mobility that wireless affords us, but historically it's cost us quite a bit in terms of latency/delays, signal degradation, and battery drain.



Gaming

Forgaming, speed is everything when it comes to outperforming one's opponents, and latency is therefore a major concern among die-hard gamers. When gamers press the mouse button, they want an instantaneous response, but Bluetooth can only deliver response speeds of 20 to 30 ms at best.

Leveraging UWB connectivity, SPARK has demonstrated sub-0.2-ms latency for UWB wireless gaming peripherals, and the company is well along the path to achieving sub-0.1 ms. This is far beyond what Bluetooth can do, and it's even faster than what many commercially available USB-wired mice can deliver today.

Audio

For audio, since Bluetooth is limited to a very narrow bandwidth, audio data compression must be applied to squeeze an otherwise bulky audio signal through a narrow pipe, which degrades the signal. Bluetooth codecs are inherently lossy in that lots of source audio data is stripped away. CD-quality audio is achieved with a 1,411-kb/s data rate—a Bluetooth codec renders that down to about 300 kb/s to be able to fit the audio stream within Bluetooth's limited data-rate capabilities.


UWB enables 10X more data throughput than BLE; thus, there's no need to compress the audio signal for wireless delivery to your UWB headset. This ensures that the sound stage one can hear with UWB headsets is considerably more detailed than what's possible with Bluetooth today, and exactly faithful to the audio source. These benefits extend to live music performance as well—UWB liberates performing musicians from cumbersome cables without sacrificing latency, allowing for wireless live performances.

IoT

The battery life of wireless sensors and devices is insufficient today for many IoT applications, leading to overly frequent recharge cycles, limited connectivity, and bulky batteries and/or costly maintenance. In addition, long latency makes wireless inadequate in applications requiring real-time sensing and communications.

With UWB, huge volumes of sensor data can be delivered with 60X lower latency and 40X better energy efficiency than legacy Bluetooth. This is hugely beneficial not only to IoT applications, but also to the myriad smart building, smart city, and AI-guided applications on the horizon that will require ultra-high-speed communication among sprawling networks of battery-powered wireless sensors.

Bluetooth technology is well-entrenched today and has served us reasonably well for the last two decades. However, UWB's stark latency and power-efficiency advantages position it as a compelling alternative for any wireless application requiring more data to flow faster and more freely with minimal power consumption. Everywhere Bluetooth resides today—across untold commercial and industrial applications, from our earphones to the edge—UWB can potentially reside tomorrow.

to view this article online,  [click here](#)

 [BACK TO TABLE OF CONTENTS](#)



CHAPTER 5:

What's the Difference Between Bluetooth Low Energy, UWB, and NFC for Keyless Entry?

JOSEPH SFEIR, Director of Business Development, LitePoint

Automotive keyless entry brings convenience, but this feature gives hackers a new way to unlock or steal cars. Learn about the communication protocols involved and how UWB can make this more secure.

With the COVID-19 pandemic shelter in place and significant numbers of employees now working from home, consumers are driving less and, unfortunately, seeing an increase in auto theft. In fact, with cars left unattended for longer periods of time, the Associated Press reported in May 2020 that major cities like New York City and Los Angeles have seen an increase in auto theft.

Even before this “new normal” we’re experiencing in the age of COVID-19, the National Insurance Crime Bureau (NICB) reported that 209 vehicles, on average, were stolen each day across the U.S. due to drivers forgetting key fobs in their vehicles, making for easy theft.

While leaving key fobs behind is an unfortunate mistake leaving drivers vulnerable to theft, another vulnerability is making car thefts easier—smart keys and smartphone car access.

While keyless entry is a standard on many cars sold today, the feature isn’t totally secure. For all of the convenience smart keys and smartphone access brings to drivers, it has given hackers a new way to unlock or steal cars through the wireless protocols that enable the entry. This is because current wireless protocols used for access are susceptible to criminals hijacking a car key’s signal.

Three communication protocols are involved in enabling a smart key or smartphone for unlocking a vehicle: Bluetooth Low Energy, ultra-wideband (UWB), and near-field communication (NFC), the latter mostly used as a backup. The three communication protocols, however, aren’t equal in terms of access security.



Bluetooth Low Energy

For quite some time, Bluetooth Low Energy (BLE) has been used in vehicles to unlock/lock the car and connect multimedia applications—to pair a smartphone with the multimedia console for voice calls or music streaming applications.

BLE is one of the communication technologies used for smart key or smartphone wireless access when approaching a car. In newer car keys, BLE communication is mainly used to track the approach of a driver beyond the 10-meter distance, while also preparing for UWB authentication. By using data packets, BLE relies on the measurement of signal strength to evaluate the distance of a driver.

Unfortunately, despite a certain degree of encryption, BLE can be subjected to jamming and relay or man-in-the-middle attacks. During a relay attack, the communication from the valid key is spoofed by a hacker by amplifying its signal strength and tricking the receiver into believing that the key is nearby. If a hacker can sniff and replay the data exchange between key and car, it's possible to unlock the car and steal it.

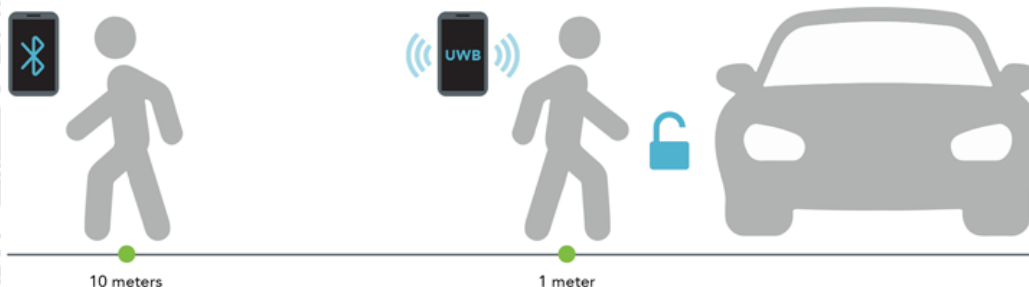
UWB

Ultra-wideband, based on IEEE802.15.4z, is a newer technology standard that can be employed in wireless entry systems to prevent distance manipulation attacks—short UWB pulses are used for precise and secure time-of-flight (ToF) and angle-of-arrival (AoA) measurements. ToF measures the propagation time that it takes for the RF signal to travel between the transmitter and receiver. AoA measures the angle of an incoming signal using multiple antennas. Positions can be determined by having multiple angles, multiple distances, or a combination of the two.

With UWB, once the two devices (in this case, the smart key/smartphone and car) is within proximity, they begin ranging and calculating the distance with a centimeter level of precision between them. The smart key/smartphone can lock or unlock the vehicle when it's within, for example, two meters of the vehicle, depending on the direction of movement (moving away or towards).

Unlike BLE, UWB is based on time, not signal strength. Therefore, a relay attack will not work on UWB, as the attack will add latency to the transmission and indicate that the key is actually far away from the receiver. In addition, adding a Scrambled Time Sequence (STS) into the UWB frame—an “encrypted” measure of a timestamp—prevents preamble insertion attacks and allows for even more accurate distance measurements. **Figure 1** shows BLE and UWB distance for automotive access.

Automatically locks and unlocks as driver approaches or departs vehicle



1. Shown is the Bluetooth Low Energy and UWB distance for automotive access.

The new technical features enabled by UWB combined with a smartphone can enable not only safer access, but also new services such as locating your vehicle in a parking garage.

Redundancy with NFC

NFC provides the same locking and unlocking capability as UWB or BLE,



but NFC is mainly used as a redundant system in the event the smart key's or smartphone's battery runs out. Redundancy in automotive applications is very important because a user doesn't want to be in a position of not being able to unlock the car.

When an NFC passive device is brought within the near field of an active device (the car), the passive device "wakes" and communicates with the active device to perform an action, like unlocking the door.

While NFC is a much simpler communication protocol and therefore doesn't have the same security benefits as UWB, it's an excellent backup system for UWB because it's very low power and requires much less battery from the device being used. In some cases, the smart key or smartphone may have a capability built in to recognize the level of power supply that's available at a specific moment and select which communication protocol should be used to unlock the vehicle. It is, however, a less convenient solution than UWB because the car key needs to be held on an active part of the car.

Conclusion

All three technologies may be available in different smart keys and smartphones for enabling keyless vehicle entry. The comparison chart in **Figure 2** summarizes the key technical aspects of each communication protocol.

	UWB	Bluetooth LE	NFC
Accuracy	up to +/- 10 cm	1-5 meters	Centimeters
Reliability	Resilient to multipath and interference	Sensitive to multipath and interference	no multipath
Range	70-250m	25-100m	<1m
Data Rate	up to 27 Mbps	Up to 2 Mbps	Up to 424 Kbps
Security	Difficult to jam as UWB signal are made by fast impulse (2ns), supports scrambled timestamp sequence (STS)	Sensitive to Relay attack and jamming	Sensitive to Relay attack
Latency	Typ<1ms	Typ>3s	Typ>1s
Chip cost	~ >\$5	~ \$2	~ \$0.25

2. The chart compares the important technical aspects of each communication protocol.

While a UWB chip is more expensive than BLE, the wireless protocol provides significantly greater security in ensuring that only the driver obtains automotive access. Successful deployments of UWB-enabled smart keys or smartphones will depend on the accuracy of their fine ranging capabilities, making test compliance verification and performance validation imperative to successful implementation.

to view this article online,  [click here](#)

 [BACK TO TABLE OF CONTENTS](#)