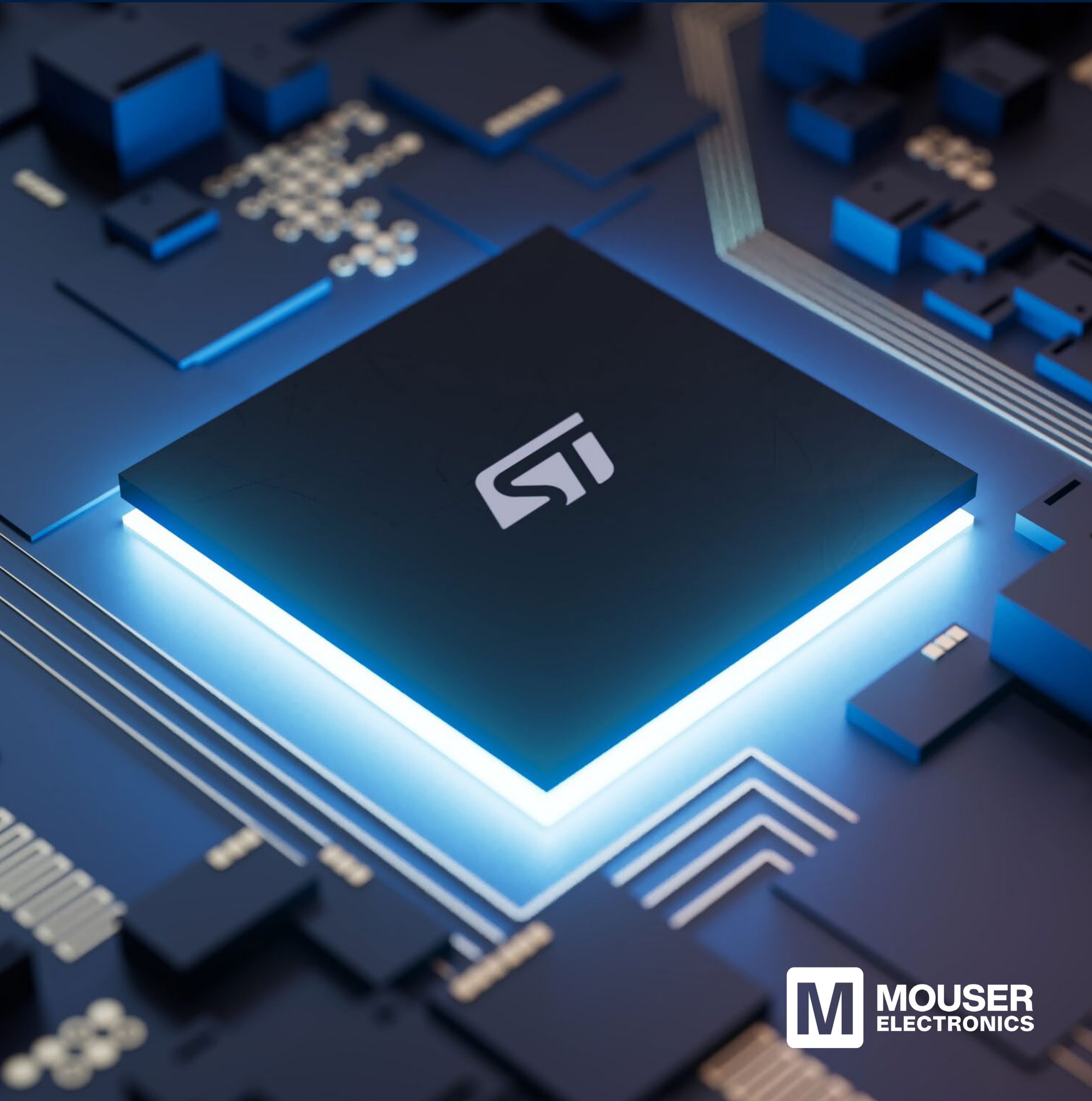
Beyond the Wires:

Exploring Bluetooth and LoRaWAN Connectivity



Contents

Connect with Mouser

Change Is in the Air

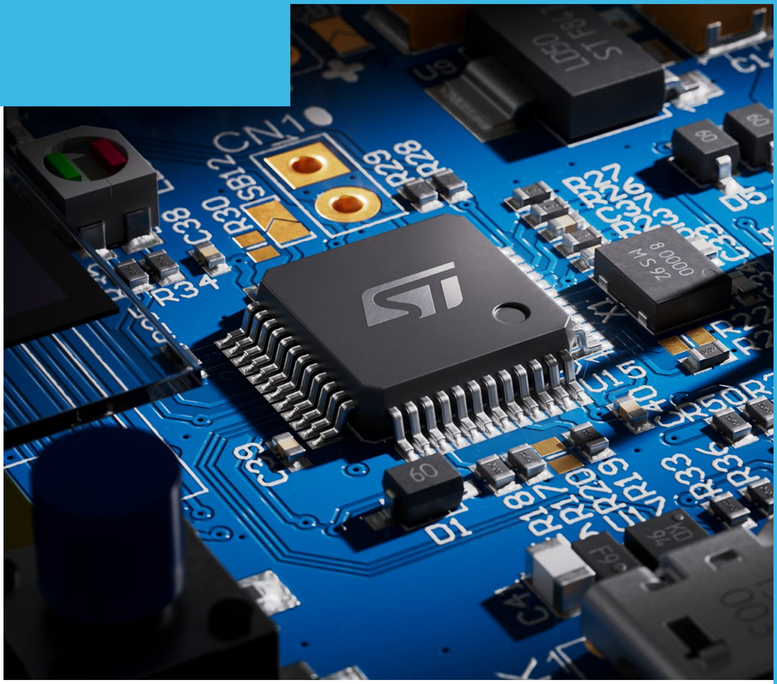
By Benoit Rodrigues, Wireless MCU Division General Manager, STMicroelectronics

We are in a profound technological revolution that will touch the lives of nearly every person on earth. No, we don't mean artificial intelligence. We are describing advances in wireless machine-to-machine networks: the spreading web of communications links that are drawing together the physical things in our world—machines, motors, sensors, processors, and the internet—into networks that will change lives.

The change is happening today. Highways and railroads are sprouting sensor networks to boost safety, streamline maintenance, and optimize traffic. Farms are becoming integrated, automated crop-growing systems. Cities and towns are deploying networks to manage energy, congestion, and safety. Public spaces—concert halls, sports arenas, airports, and train stations—are installing networks to deliver tailored, high-quality audio to each of their users. Individual dwellings are linking sensors and smart appliances to create safe, luxurious, energy-efficient living.

The foundation for all these changes is wireless networking between things. None of these use cases can be achieved with wired networks. And these wireless networks have some requirements in common.

Most nodes must operate on very little energy. And most require low cost—dollars, not hundreds of dollars. And many of these networks will be responsible for lives, health, and property; they must be secure. Finally, many of the organizations that are designing these wireless networks are application experts, not SoC designers or software platform developers. They must be able to start with proven silicon and software stacks, off the shelf.



There are also some major differences in requirements among these use cases. Some network links may have to carry tens of megabytes per second, while others will relay only a few bytes per day. Some entire networks will fit in a small apartment, while others may span an urban core and reach beyond into suburbs or countryside.

Increasingly, sophisticated industry standards—such as *Bluetooth*® Low Energy or LoRaWAN®—define wireless networks that can meet requirements across this wide space. But standards alone don't make systems. It is our role at STMicroelectronics not just to participate in standards bodies but also to implement these standards in our families of wireless microcontroller chips and modules and to create reference software stacks for real-world use cases.

In this eBook, you will find chapters on many use cases, from remote sensor networks to smart cities and homes, from agriculture to public entertainment. We will discuss special requirements for security, private networks, long range, and much more. We will emphasize applications, user experiences, and system requirements.

Please read and enjoy!

Secure IoT Connectivity: Design to Meet Forthcoming Cybersecurity Legislation

Nathalie Vallespin, Product Line Manager Connectivity STM32, STMicroelectronics

IoT technologies make it possible to detect, monitor, measure, track, and control almost anything, almost anywhere, bringing new opportunities to create innovative services. IoT applications can significantly improve access to high-quality healthcare, enhance comfort and convenience in everyday life, help to manage infrastructures and resources efficiently, and enable businesses to improve safety and productivity. On the other hand, many IoT devices handle data that should be kept private, such as network-access credentials, personal information like health data or financial details, intellectual property, and intelligence about business assets.

As IoT devices have become more ubiquitous and pivotal in running everything, from home security cameras to smart cities and the smart grid, security specifications and standards have evolved, credible certifications have emerged, and best practices have been defined that are appropriate to their needs and work within the typical constraints on power, processing, and memory. Prominent examples include the Security Evaluation Standard for IoT Platforms (SESIP) created by GlobalPlatform—a technical association of industry experts—as well as the PSA Certified security framework and evaluation scheme created by a consortium including Arm, software developers, and well-known independent testing organizations.

Historically, the rewards for producing demonstrably secure equipment have been reputational: highly regarded products and services win market share. But changes are afoot.

New regulations are coming forward in territories worldwide that oblige device makers and solution developers to implement proper security. It’s a great opportunity for responsible product developers to encourage greater adoption of IoT technologies in consumer and industrial markets by delivering superior security solutions.

Toughening Security Stance

New European legislation, in effect now and due to become enforceable by August 2025, mandates compliance with sections of Article 3.3 of the Radio Equipment Directive (RED) that cover cybersecurity. Specifically, these are sections 3.3d, e, and f. Section 3.3d calls for features to prevent harming communication networks or disrupting services. Section 3.3e covers personal data and privacy protection and requires measures to prevent access or transmission of personal data. Section 3.3f focuses on fraud prevention through features such as user authentication controls to protect electronic payments and monetary transfers. The legislation applies to devices that can communicate over the internet, whether directly or via other equipment, and equipment that may expose sensitive personal data.

End users’ attitudes towards device security are also changing. The PSA Certified 2022 Security Report noted that consumers have become more likely to check for security than to focus only on cost and features.

Creating Compliant Devices

To meet market expectations and to comply with tougher incoming legislation, device manufacturers need to ensure that the platforms and ecosystems powering their development can enable them to certify their products successfully.

ST's latest STM32 wireless microcontrollers (MCUs) are at the heart of next-generation devices that must satisfy legislation such as EU RED and U.S. Cyber Trust Mark. In fact, this product is already certifiable according to SESIP Level 3.

Designers using ST wireless MCUs, such as the STM32WBA5 series, can take advantage of hardware features built into the silicon when creating wireless IoT devices. Security starts with the Arm® Cortex®-M33 core—designed with Arm's TrustZone® architecture that allows an isolated secure area—running on a secure operating system and preventing access by non-secure software. TrustZone ensures security begins from the lowest level, the physical layer, which includes securing the boot and firmware update processes.

STM32WBA5 Multiprotocol Wireless Radio MCU

Learn More ⟶

Moreover, the MCUs are compliant with the Arm Trusted Base System Architecture (TBSA), which requires hardware features including a root of trust (RoT), protected keystore, random number generator to support cryptography, and hardware cryptographic acceleration. These components ensure the correct security properties and can be maintained without compromising real-time application performance. The STM32WBA5 MCUs include a secure AES coprocessor and public key accelerator (PKA), both incorporating resistance to differential power analysis (DPA), and a HASH hardware accelerator.

The MCUs also support secure firmware updates for over-the-air or local updating of the firmware image, in addition to lifecycle management to keep deployed devices protected as cyber threats evolve. In addition, STM32WBA5 MCUs incorporate a secure firmware install (SFI) mechanism that allows secure and counted installation of OEM firmware in untrusted production environments, such as a contract manufacturer, for anti-cloning and IP protection. Readout protection and debug unlock with password assist lifecycle management. The peripherals, memories, and I/Os are securable, while the peripheral and memory privileges are configurable to limit access to the MCU's security-sensitive resources. There are also protection mechanisms for embedded flash memory and SRAM.

These wireless MCUs offer active tamper detection and protection against physical attacks, with internal monitoring capable of erasing secret data if an attack is detected. This helps meet requirements for point-of-sales applications.

Secure Device Development

Of course, developers need help to marshal these features, and here is where the STM32 ecosystem comes in. While STM32Cube resources provide software tools and libraries to aid development, ST has also created the STM32Trust framework that helps navigate the security requirements and resources available to reach the desired security assurance level. STM32Trust security functions are conceived to ensure IP protection, data protection, secure connectivity, and system integrity. It guides developers to solutions such as ST's X-CUBE-SBSFU software for implementing secure boot and secure firmware updates, as well as the Trusted Package Creator software to encrypt binaries for SFI.

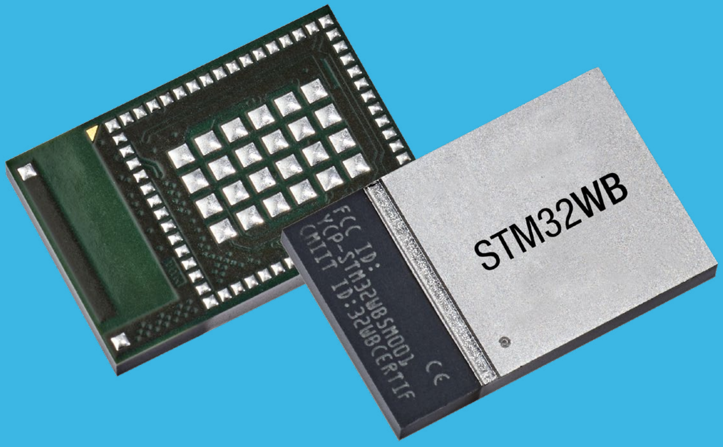
With integrated *Bluetooth*® Low Energy 5.4 and 802.15.4 radio, STM32WBA5 wireless MCUs—and similar STM32WL sub-1GHz MCUs for longer-range communication—simplify and accelerate development of wireless IoT devices. Leveraging their hardware security features and the curated resources provided by STM32Trust, developers can confidently implement cyber protection that meets the latest industry standards and regulations on security and privacy.

ST@EW2023: STM32WBA - 2.4GHz wireless microcontroller with SESIP Level 3 security V3

Wireless Integrated MCU SoC or Module?

JJ DeLisle for Mouser Electronics

Explore the advantages of wireless MCU SoCs versus wireless modules in IoT applications, focusing on integration, cost, and design flexibility.



Internet of Things (IoT) solutions are steadily growing in diversity and capability. This growth in the volume of products, as well as the wide range of requirements, is leading to a burgeoning selection of microcontroller unit (MCU) system-on-chip (SoC) solutions with integrated wireless capabilities to offer an all-in-one solution alongside an equally expanding array of wireless module solutions. Though relevant for virtually all commonly used frequencies and a growing number of unlicensed and licensed frequencies extending to over 100GHz, the most common IoT wireless device operating frequency ranges are sub-1GHz (sub-GHz) and the 2.4GHz ISM band.

The 2.4GHz ISM band includes protocols and standards such as *Bluetooth*®, Zigbee, Thread, Matter, and other open and proprietary IoT wireless standards. Sub-GHz frequency bands are more complicated and vary based on regions. Typically, the most popular sub-GHz bands are around 920MHz and 433MHz. However, there are region-specific bands available in the sub-GHz region. For example, North America and Australia share 915MHz; Europe uses 868MHz; China, 470MHz and 779MHz; and Japan, 426Mhz and 920MHz. Many sub-GHz IoT applications make use of IEEE 802.15.4, which is a technical standard that defines the operation of low-rate wireless personal area networks (LR-WPAN), suited to the limited data rates but relatively efficient and long-range capabilities of sub-GHz communications. LoRa is another popular wireless standard for sub-GHz applications.

Benefits of MCU SoCs with Integrated Wireless

A wireless MCU SoC is an IC that fully integrates an MCU and a radio interface. These SoCs can offer all-in-one processing, programmability, and I/O interfaces for wireless communications in a single chip. Such single-chip solutions with these features can significantly reduce PCB footprint, overall product size/weight, and cost—as long as the design team understands the necessary wireless circuitry to achieve a certifiable wireless communication solution.

Benefits of Wireless Modules

A wireless module is a device—often pre-certified—that offers a complete wireless communications, transceiver, or sensor unit. This speeds up time to market by saving on certification costs, removing the need for RF knowledge, and reducing BOM complexity and purchasing burden. The basic makeup of a wireless module is typically a radio transceiver built to accommodate specific protocols (but usually with some flexibility), an MCU, antennas, and software stack. The antennas may be external, or the wireless module may have optional ports for external antenna connections.

Wireless modules are usually straightforward to integrate into a design and pair with a compatible main MCU to offer a complete IoT solution. With a wireless module, the design team doesn't need to worry about developing a certification- and regulation-passing wireless communications circuit, which can dramatically reduce costs and development time. Additionally, product line diversity can be achieved by using different wireless modules—or even the same wireless module with different programming—to operate with various wireless standards.

Wireless Modules vs. Wireless MCUs for 2.4GHz and Sub-GHz IoT Applications

With both 2.4GHz and sub-GHz frequency ranges well-suited for most IoT applications, there are many approaches and product options for designing IoT solutions in these ranges. Some groups choose to go with a wireless MCU SoC and design their wireless communication circuit instead of selecting a prebuilt wireless module. However, to make a wireless MCU solution viable, a design group needs RF design/engineering expertise, lab equipment, RF sourcing expertise, RF PCB design skills, and antenna design and fabrication capability, and the entire solution would then need to be separately certified. On the other hand, a wireless module is a drop-in solution that can alleviate the need for additional development work aside from software development for programming the module.

Conclusion

For a given application, there are a variety of factors to keep in mind when selecting between wireless MCUs and wireless modules. Wireless modules have higher per-chip costs than wireless MCU SoCs. Depending on the production volume of an IoT product, designers may incorporate a wireless MCU with a low per-unit cost where the RF design and development costs would be divided among a large number of parts. This could result in a lower cost of production than a wireless module, which may also not be available at specific volumes desired, depending on the supply chain for the part.

STM32WB1MMC BLUETOOTH® Low Energy Module

Learn More ⟶

> “With a wireless module, the design team doesn't need to worry about developing a certification- and regulation-passing wireless communications circuit.

Discovery Kit with STM32WB5MMG MCU

Learn More ⟶

Smart Home Trends Benefit Developers and Users

JJ DeLisle for Mouser Electronics

The smart home ecosystem is evolving with the integration of Matter, advancements in mesh networking, and the advent of multi-protocol scenarios.

This past year has seen many changes in the smart home ecosystem. As Matter matures and more devices adopt the unifying standard, the accelerating growth of smart home devices and users leads to a more dynamic Internet of Things (IoT) landscape. A few interesting trends and discussion topics in IoT and the smart home are on the rise, including multi-protocol scenarios, mesh networking, the Matter ecosystem, and future smart home technologies.

The Promise of Matter

The original goal of Matter, which started as Project CHIP (Connected Home over IP), was for the major players in the smart home industry to converge on a unified application layer standard for connected devices for the home. In this way, Matter was designed to make it easier for manufacturers to create secure and reliable smart home products that are easier for developers and certainly much more streamlined for end users. Moreover, Matter solutions are intended to be interoperable with major smart home ecosystems, such as Google Assistant, Apple HomeKit, and Amazon Alexa.

Matter-certified devices that use Thread for the transport layer, along with Wi-Fi® and Ethernet, must also include *Bluetooth*® Low Energy capability for commissioning smart home devices, as Bluetooth Low Energy is instrumental in adding new devices to the network. The Matter protocol is positioned below the device application layer and above the transmission control protocol (TCP) layer, connecting the IP layer in the communications stack.

Matter comprises six functional layers—data model, interaction model, action framing, security, message framing/routing, and IP framing/transport management—and acts as an interoperable application layer solution. The transport management layer of Matter handles the link to individual protocols, such as Wi-Fi and Thread.

Multi-Protocol Scenario for Enhanced User Experience

Thread is a protocol based on IEEE 802.15.4, designed to be a low-power wireless IP protocol that enables the development of mesh networks with an array of advanced features. Unfortunately, a Thread-based device cannot communicate with a device based on Wi-Fi (which is based on IEEE 802.11). To overcome this, some chipset manufacturers are incorporating Bluetooth Low Energy alongside Thread or Wi-Fi so that the multi-protocol capable devices can seamlessly function in a Matter smart home environment. Such devices can address end devices and border routers within the Matter ecosystem. For end users, regardless of whether their smart home network is Wi-Fi or Thread, Bluetooth Low Energy can be used for commissioning. These new multi-protocol devices can readily be added to the network with direct integration within an existing Matter network.

The Power of Mesh for IoT in the Home

Wireless mesh networking is an extraordinary feature for enhancing the reliability and reach of an IoT network, including for smart home applications. In a wireless mesh network, nodes within range of each other receive the messages sent by the other nodes; based on the needs of the network, each node that receives a message can then relay that message to other nodes within range. Mesh networking allows multiple paths for a message to reach a destination node. Well-designed mesh networks will automatically optimize the most reliable paths for a message to reach its destination, accounting for the dynamic nature of wireless communications. The more nodes within range of each other in a mesh network, the more reliable the network can be.

This reliability is a huge advantage in a smart home scenario where devices may be scattered across a relatively large area, with some regions experiencing poor reception due to aspects of the home structure or different elevations within the home. Modern mesh networking technologies, such as Thread, can even be self-healing. Self-healing is when a mesh network automatically reconfigures and optimizes paths between nodes automatically after any nodes are removed or change position. This is key for smart home applications where nodes may be frequently moved, added, or removed.

Unlocking the Potential of Zigbee, Open Thread, and Matter

Zigbee and Thread are the dominant wireless mesh networking solutions for smart home technology. While Thread works intrinsically with Matter, Zigbee does not. However, connecting Zigbee devices to a Matter network is possible through a Matter bridge. Many smart home devices use Zigbee for networking and communication. A Matter/Zigbee bridge means that Matter and Zigbee networks can work together within a smart home, bridging non-Matter smart home technology with the Matter-based smart home technology as a seamless network. This bridge also allows end users to diversify their smart home offerings to include devices that weren't traditionally compatible with each other, better customizing their smart home experience to their liking. These factors dramatically reduce the barrier to entry for many potential smart home device users and make it easier for developers familiar with a given networking technology to continue to develop with that technology and still see their products viable in the smart home.

Mastering The Matter Ecosystem

There are three types of Matter network devices: gateways, border routers, and end devices. Gateways support remote access to Matter devices with an internet connection. Matter bridges enable connection and communication of the Matter network to other non-Matter wireless networks. Bridges are instrumental in connecting Matter-incompatible devices with Matter-compatible nodes and networks. Some devices can be upgraded via software to become Matter compatible, but this varies by manufacturer. Many legacy devices may not receive such software upgrades, which makes Matter bridges essential for smart homes with legacy devices. A border router is a device that connects Thread devices to a smart home Wi-Fi or Ethernet network, allowing for communication between devices that can connect to the Wi-Fi network but do not have a Thread radio, such as a smartphone or tablet.

Matter uses AES-CCM encryption with 128-bit keys for end-to-end encryption of every message sent between devices. This means a Matter message is encrypted before transmission and can only be decrypted by the intended recipient through the network. This level of encryption works from Matter-compatible devices to other Matter-compatible devices and through gateways and bridges. Matter uses public key infrastructure (PKI) with certificates to authenticate devices and encrypt the transmissions. Each Matter device is issued a unique certificate with its public key and information used to identify the device. These certificates are assigned by a trusted certificate authority (CA) that verifies the identity of each device that has approval to participate in the network. Matter uses a hierarchical trust model with a Matter root CA that assigns certificates to intermediate CAs and issues certificates to the network devices. For two Matter devices to communicate, they first must share their certificates and determine if they have permission to communicate. Then, they use their public keys to establish and share a secret key that is then used to encrypt all the transmission between devices. These security methods help to prevent man-in-the-middle attacks.

Conclusion

The Matter standard continues to be updated with support for more device types. These developments indicate that the future smart home will grow more diverse as more device manufacturers embrace IoT solutions in their product lines and new manufacturers attempt to carve out niches in the smart home. With the growing integration of artificial intelligence (AI) and machine learning (ML) in IoT networks, more AI/ML will inevitably find its way into the smart home beyond the capabilities of smart speakers connected to automated assistant services.

With greater security and seamless communication among smart home devices, end-user confidence in smart home technology is rising. A more capable smart home networking infrastructure is also integral to the increased adoption of in-home robotic solutions. These new solutions could lead to coordinated in-home robotic services that are much more advanced and useful than today's robotic vacuums.

Unmuting the World with Bluetooth LE Audio Auracast

Ozcan Yurt, Staff Applications Engineer, Microcontrollers, Americas, STMicroelectronics

In its 1,000-plus pages of documents, the *Bluetooth®* LE Audio specifications cover a huge range of functions that together define a new way for Bluetooth to support audio—and, ultimately, new ways for users to live in the audible world.

Building Blocks

Key to this audio revolution are new elements introduced in the Bluetooth LE Audio specifications: a new audio codec, an isochronous streaming data mode, broadcast capability, and multi-profile by design. Working together, these elements will change the way audio consumers relate to the sources around them.

Fundamental to LE Audio is a new audio codec, LC3. Compared to the default SBC compression in Bluetooth Classic, LC3 offers additional bit rates (down to 16kbps), optional greater sample resolution, lower latency, remediation for lost or corrupted packets, and lower overall power consumption. And LC3 outscores SBC on stereo listening tests, even when comparing 160kbps LC3 against 345kbps SBC.

Isochronous streaming is another fundamental advance. This capability allows audio packets to be time-synchronized when they are played. So, for example, audio being streamed separately to two earbuds will stay in synch to deliver a correct stereo experience. There are actually two isochronous streaming modes in LE Audio: Connected Isochronous Streams (CIS), in which the source establishes a point-to-point connection to a sink, and Broadcast Isochronous Streams (BIS), in which any number of compliant devices may choose to accept a time-synchronized stream.

CIS is used to provide True Wireless Stereo (TWS). In Bluetooth Classic, there is generally one link from the source to one wireless earbud or speaker, and then a link from that device to the second earbud or speaker. With two CIS links, the source can connect to both earbuds directly, keeping the two synchronized (**Figure 1**).

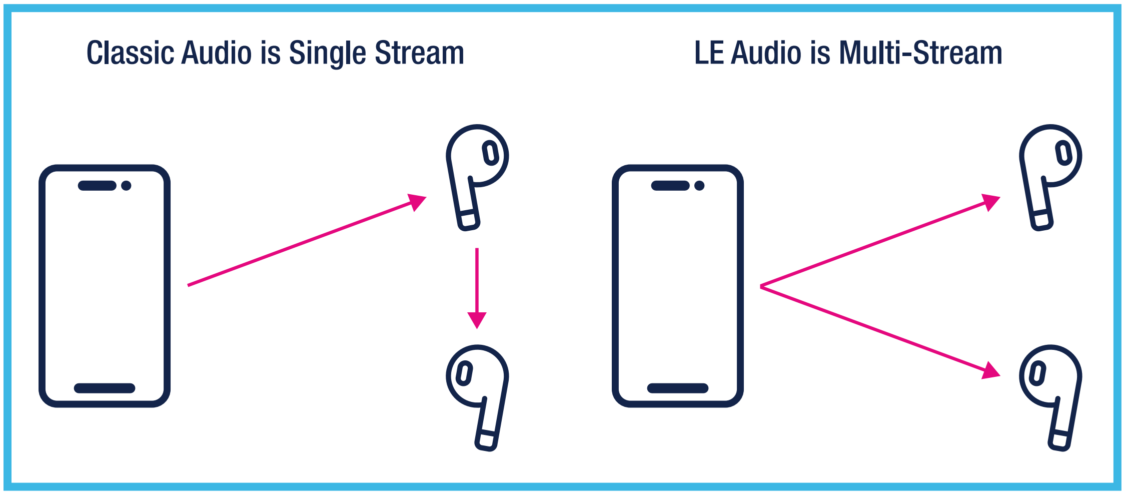


Figure 1: *True Wireless Stereo (TWS) comparison of current audio vs. LE Audio (Source: Mouser Electronics)*

BIS can be used to broadcast gate announcements at an airport terminal, or music to attendees at a concert, among many other use cases. BIS is the mode underlying the audio broadcasting capabilities that the Bluetooth organization has branded as Auracast™ (**Figure 2**).

Inherent with BIS/CIS is the ability of both sources and sinks to handle multiple channels simultaneously. This ensures that an earbud user could be listening to music from their smartphone and monitoring public-address announcements at the same time.

Now, let's take a closer look at broadcast mode. Under Bluetooth Classic, connections are 1:1—one source connected to one sink. Bluetooth LE Audio allows a source to simply broadcast streams of packets to whoever might be listening. This ability of a source to simply broadcast content, allowing users to subscribe if they wish, opens new categories of use cases, from individuals sharing content with each other to delivering messages or music in crowded public spaces. Bluetooth SIG has branded a collection of these capabilities as Auracast.

But broadcast raises an issue with the way to handle data integrity. Bluetooth Classic assumes every data transaction must be lossless. If a packet is dropped or corrupted, the source device will repeat the transmission until it receives a positive acknowledgment. Broadcast is inherently unidirectional, so acknowledgments are not possible. Rather than waiting for an acknowledgment, broadcast mode will continue on, depending on LC3's packet loss concealment (PLC) algorithm in the receiving device to reconstruct the missing data so that the loss is inaudible. It is also possible for broadcast mode to do multiple retransmissions to ensure that a wide variety of receiving devices in different reception environments get a usable copy of the data.

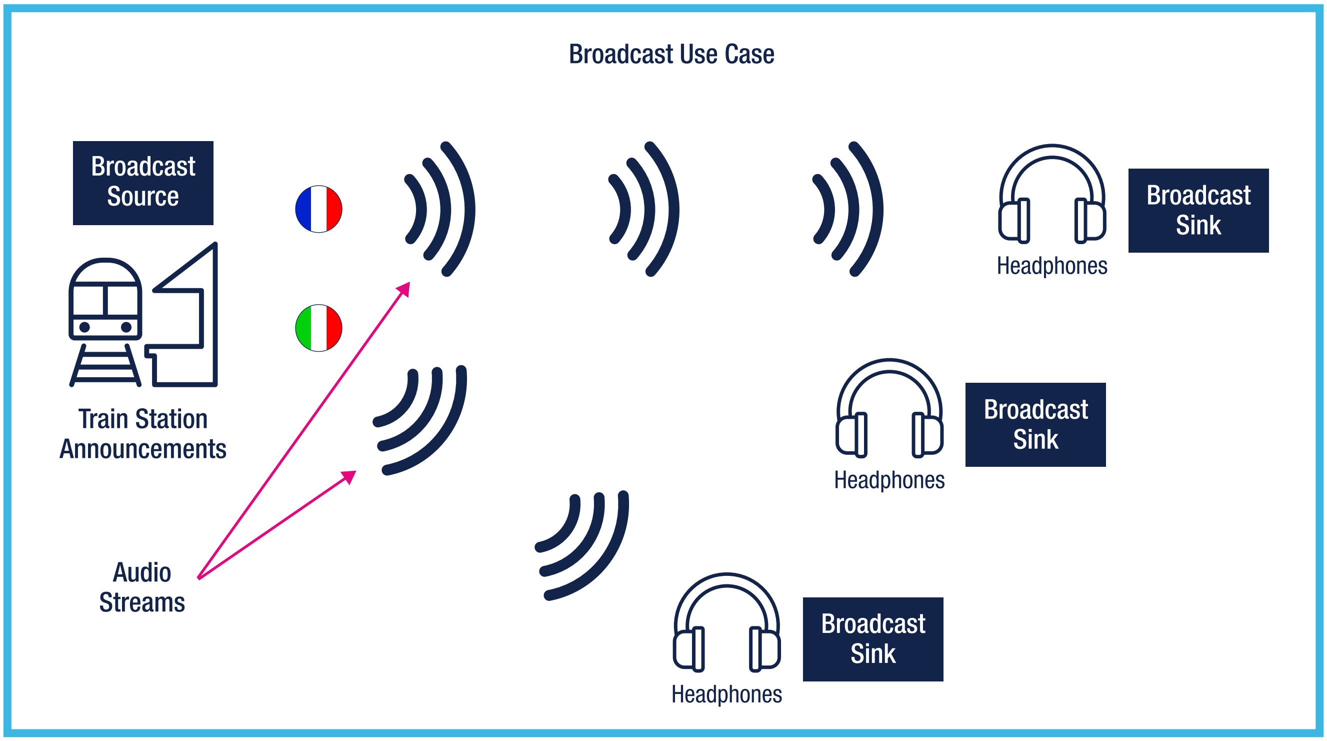
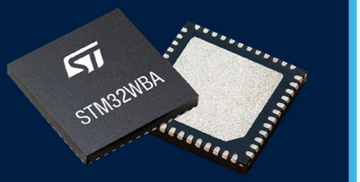
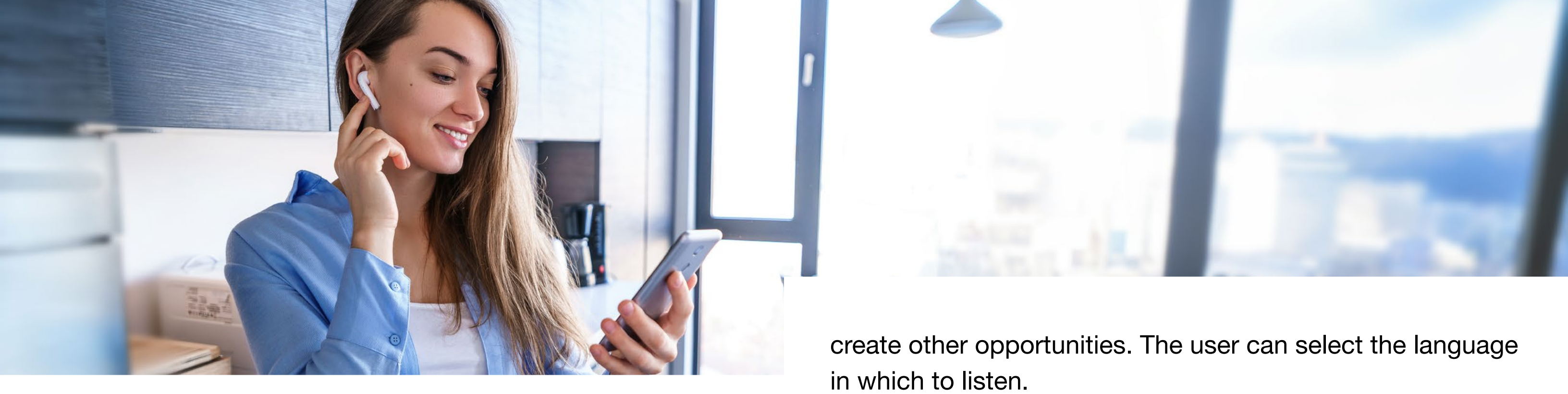


Figure 2: *Example of a broadcast use case. (Source: Mouser Electronics)*





Use Cases

These elements work together to change lives. Starting at a personal level, LE Audio can enable hearing aids whose sophisticated electronics can be packaged outside the earbuds. Bidirectional CIS links and the LC3 codec would allow low-latency, synchronized connections between in-ear microphones, sophisticated external signal processing, and earbuds. And the ability to handle multiple channels means users can—finally—actually hear telephone conversations, broadcast public-address announcements, and the TV at the local bar through additional CIS and BIS links to the earbuds.

The case is similar for wireless stereo. In Bluetooth Classic, audio is daisy-chained from handset to earbud to earbud, requiring an additional radio and antenna in the relaying earbud, and hence additional power consumption. Then, getting the two earbuds synchronized requires proprietary algorithms that limit interoperability. With LE Audio, the handset can connect isochronously to each earbud in parallel, and users get the sound quality of LC3, with the CIS connections synchronized in time.

BIS opens up many more possibilities. An earbud user can share her music without having to lend an earbud. Nearby friends can simply opt-in to her broadcast directly with their handsets. In those impossible-to-hear places like gyms or sports bars with a dozen TV screens, users can select a broadcast stream from a particular screen and actually enjoy it—no muted TVs, no battle of the little TV speakers. At concerts, attendees can receive a broadcast directly from the mixing board and actually hear the music at near-studio quality; perhaps they can select from among different mixes. Videos or live events with multiple-language broadcasts create other opportunities. The user can select the language in which to listen.

What It Takes

Implementation of these features is not trivial. The LC3 codec, required for LE Audio to ensure interoperability, may require less memory than an SBC codec. But it may also require careful coding and more processing performance.

The functions that make multiple broadcasts or connected streams possible—Isochronous Channels (ISOC) and Enhanced Attribute Protocol (EATT)—are options to Bluetooth LE. They reside in the controller link layer and in the host stack, respectively. Extended advertising, which is required to establish BIS channels, also adds to the controller workload. Altogether, the needs of codecs, host and controller tasks, the audio framework, top-level profiles, and applications will dictate high CPU performance in a SoC, but at low power.

Device design for Bluetooth LE Audio and Auracast will need special attention when choosing the right wireless microcontroller. The design needs hardware that can handle all the necessary functions of the target product while meeting requirements such as performance, power, latency, memory, cost, time-to-market, driver/middleware/library support, and longevity. But that effort will open whole new audio experiences for users.

ST at CES 2024 — Bluetooth LE Auracast™ Broadcast Audio ▶

Connectivity with Bluetooth Low Energy

From Industrial Applications to Consumer and Personal Electronics Devices

Kamel Kholti, Product Marketing Manager STM32 Wireless MCU, STMicroelectronics

The Keys to Bluetooth Low Energy Success

Bluetooth® Low Energy is a critical technology in the Internet of Things (IoT) spectrum and has important attributes that have contributed to its success. These include properties such as low power consumption, suitable range and data rate, native security features, an acceptably compact memory footprint, affordability, and support built-in to every smartphone.

Initially conceived as a standardized, wireless communication protocol for short-range point-to-point data exchange between devices, early Bluetooth generations presented a wireless alternative to RS-232 data cables. The first official Bluetooth specification (version 1.0), released in 1999, enabled mobile users to cut the cables to accessories such as a telephone headset and enjoy hands-free experiences. Other contemporary use cases included file sharing between devices and wirelessly connecting computer peripherals, including keyboard and mouse.

The addition of the Bluetooth Low Energy radio option, included in the Bluetooth 4.0 specification that arrived in 2010, changed all that. Not only designed for very low power, as the name suggests, Bluetooth Low Energy also supports additional communication topologies, making the technology suitable for connecting large-scale device networks and moving from wired to wireless networks.

With these underlying features, Bluetooth Low Energy is well-adapted to diverse IoT applications, particularly smart-home devices and smart industrial sensors deployed in factories or remote locations. Its low power consumption meets the needs of small, battery-operated devices, making it a natural choice for wearables such as fitness trackers, smartwatches, and personal health devices (PHDs).

The Bluetooth SIG continues to extend Bluetooth Low Energy with new features such as the generic health sensor (GHS) profile, which standardizes the way sensor data is uploaded from PHDs into electronic health record (EHR) systems. This facilitates interoperability between PHDs, personal health gateways, and EHR systems, extending the scope for remote patient monitoring by lowering system costs and stimulating the development of a wider range of suitable PHDs.

Bluetooth 5.0, introduced in 2016, brought further enhancements, including improved coexistence with other wireless technologies, increased data transfer speeds, and extended range. Bluetooth Long Range, which uses a coded physical layer (PHY), permits reliable communication over long distances and at low power for specific use cases. Bluetooth 5.1 introduced direction-finding features that enable precise location capabilities. There is also Bluetooth LE Audio, which intends to replace the Bluetooth Classic introduced with Bluetooth 5.2. This permits efficient audio streaming to enhance applications like hearing aids and wireless audio devices in the IoT ecosystem. The latest specifications, Bluetooth 5.3 and 5.4, continue the evolution, adding more technologies and use cases.

Making the Right Choices

Bluetooth Low Energy is an excellent choice for connecting small IoT devices for a wide variety of medical, industrial, and consumer applications, including wearables like smartwatches and smart-home devices that require reliable

connectivity without wires. It offers affordability, low power consumption, flexibility, a wide variety of profiles that simplify implementation, and unlicensed operation in the 2.4GHz frequency band. The Bluetooth SIG is committed to the future of the technology and continues to introduce improvements such as new and valuable profiles. There is also a large pool of expertise, including test houses and software developers.

When it comes to product development, choosing the right place to start is important and can influence the performance and cost of the end product, as well as the time to market and future flexibility to scale and adapt the design to meet evolving market demands.

There are many options, and one of the first considerations regards hardware design and the skills available to complete the RF system. RF design is notoriously difficult, mainly due to antenna matching, and circuit layout, in particular, is known to be time-consuming and demands considerable specialist expertise to get right. Engineers may be working with an existing product built for wired communication using a standard such as USB, challenged to upgrade to wireless for greater user freedom and convenience. Its heart may already contain an STM32 microcontroller, as this is one of the world's most popular Arm® Cortex®-M MCU families. So, the team could be heavily invested in code, tools, and hardware for STM32 development.

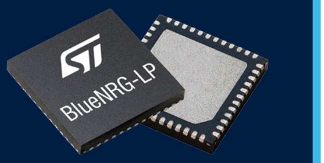
STMicroelectronics has made it possible to sidestep many of the hardware design issues and continue working within the STM32 ecosystem by introducing the STM32WB and STM32WBA series of wireless system-on-chips (SoCs). Using these devices also connects developers with the ST community and online resources, including wiki pages, training materials, application notes, and code samples, which help developers reach their project goals.

ST's Wireless Microcontrollers Simplify Development

The STM32WB and STM32WBA series SoCs combine a microcontroller capable of running the Bluetooth communication stack and the application code while also integrating a Bluetooth Low Energy radio on the same silicon. Also, ST can provide an STM32WB or STM32WBA companion chip that integrates the impedance matching and filtering circuitry needed to connect the antenna, helping avoid additional RF-circuit design challenges.

In some use cases, it is critical to ensure that both the radio link and the application can ensure real-time performance. Examples include certain types of medical monitors or motor drives. To address this, the STM32WB55 SoCs comprise dual-core SoCs conceived to handle such situations. They contain an Arm Cortex-M0+ core dedicated to the radio layer, while an Arm Cortex-M4 with floating-point unit and DSP extensions handles application processing. A memory protection unit (MPU) enhances application security, and the microcontroller contains mechanisms for managing shared and exclusive resources between the two cores.

To provide another example, applicable to wearables applications, the STM32WBA52 allows up to +10dBm output power to facilitate connecting to the device even if it is far from the consumer. This MCU is an ultra-low-power platform that leverages ST's 40nm process technology and contains an Arm Cortex-M33 processor running at 100MHz, which ensures high performance.



Even Faster Time to Market

While these SoCs help users overcome many design and integration challenges, creating a solution using these devices calls for resources that some organizations may not have or be able to access. For these situations, a module such as the STM32WB5MMG integrates the wireless SoC with all the external components needed for the radio system, including the antenna, matching and filtering network, and timing crystals. The module is then certified in accordance with regional legislations such as FCC, CE, and RoHS, in addition to being certified according to the Bluetooth SIG requirements. This approach eliminates many hardware design headaches and saves certification costs for product developers, helping accelerate time to market for the end product.

Using either of these approaches allows access to the STM32Cube ecosystem, which includes code samples, middleware, and tools to assist software development. Available resources include the STM32CubeMX MCU configurator, which also provides utilities for clock configuration and power estimation, and the STM32CubeMonRF radio performance tester for STM32WB and STM32WBA devices. It provides help to build test scripts, control the STM32WB and STM32WBA SoC, and visualize performance to help developers reach their desired targets.

Ahead of forthcoming European and US legislation on cyber resilience, ST's Bluetooth SoCs are ready to demonstrate compliance, including certification according to the demanding GlobalPlatform Security Evaluation Standard for IoT Platforms (SESIP) Level 3 specifications.

Aided by the extensive choice of wireless SoCs, modules, and development tools, and with the assurance of leading-edge security compliance, product developers can leverage the strengths that have made Bluetooth Low Energy such a success in their next-generation IoT products.

CES 2023: Advanced Bluetooth® LE features Bluetooth LE Power Control

Challenges of Multi-Connectivity Asset Tracking

Private Network Concepts Using the STM32WL

Antonio Mascioli, Senior Principal Application Engineer, STMicroelectronics

The STMicroelectronics STM32WL (**Figure 1**) is a system-on-chip (SoC) designed for long-range wireless applications consisting of a general-purpose microcontroller and sub-GHz radio. Along with these core components, the SoC also includes up to 43 general-purpose input/output (GPIO) pins and various power management/optimization features, as well as embedded security hardware functions. For security, the SoC supports AES hardware encryption, read/write protection, ST's Secure Key Management Services (SKMS), secure hardware isolation, and secure boot and firmware update capabilities.

The STM32WL is supported by a robust development ecosystem—anchored by the STM32WL55 Nucleo board and the STM32Cube Ecosystem—which provides a consistent set of hardware and software development tools. The ecosystem provides preconfigured software examples, drivers, and a full set of middleware and radio stacks. It also has a dynamic and active developer community, which is a critical component for any development ecosystem to facilitate rapid learning, problem solving, and, ultimately, innovation.

The radio stack provided with the STM32WL, through the STM32Cube Ecosystem, allows the SoC to support the Long-Range Wide Area Networking (LoRaWAN) protocol, along with multiple modulation schemes that include Gaussian Frequency-Shift Keying (GFSK) and Binary Phase Shift Keying (BPSK). BPSK modulation is only available on the Transmit side. Given its ability to transmit small data payloads over long distances at ultra-low power, LoRaWAN is ideal for Internet of Things (IoT) applications such as transmission of sensor data (e.g., a thermostat reporting room temperature). However, LoRaWAN may not be suitable for other types of IoT applications that require higher bandwidth. The requirement to always communicate back to a gateway and server location introduces technical challenges that the LoRaWAN network was not designed for.

Utilizing the STM32Cube ecosystem, the following project provides an example of how powerful this ecosystem and the customizability of the STM32WL truly are—especially when its capabilities are used to deliver new feature sets to address expanded use cases.

In this project, we use the STM32WL's customizability and GFSK capability to address use cases in smaller, centralized networks that can be expanded as required, such as monitoring and integrating various sensors within a warehouse configuration. In this case, the private network

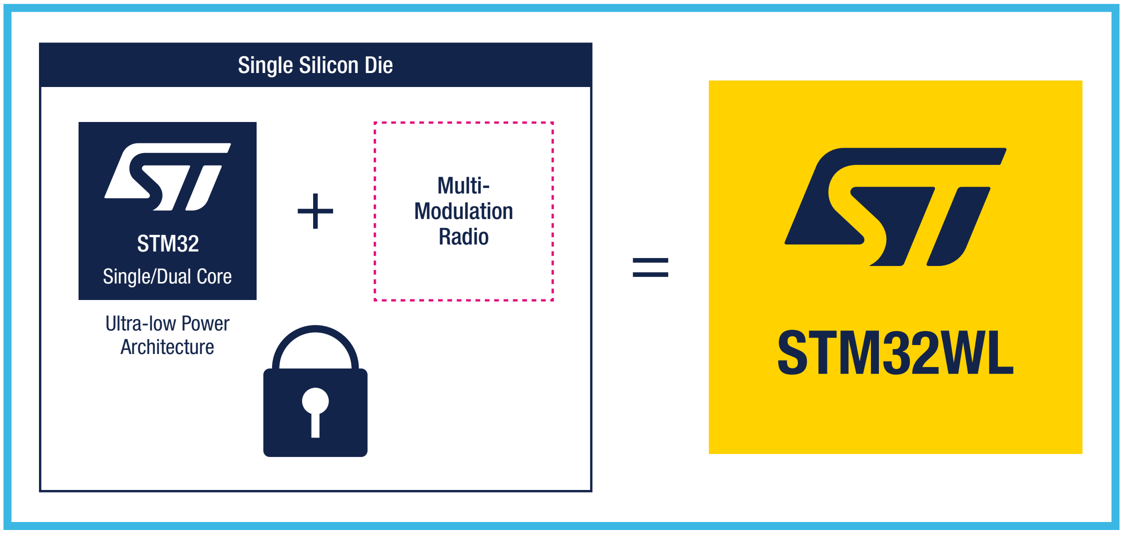


Figure 1: *High-level block diagram of STMicroelectronics' STM32WL MCU. (Source: STMicroelectronics)*

allows for internal security, rapid response times to events, and the eventual backhaul to an internet connection through a secured hub. In addition, the network can easily be expanded to accommodate many nodes that may be in a physically close area. The key contribution of this topology is that it is private and controls a specific function.

To address these use cases, the STM32WL is used as the basis of a new network architecture that delivers an expanded-footprint, mobility-capable private network using GFSK modulation. The keys to delivering this successfully are the implementation of a hub-node architecture (**Figure 2**) and the ability of the hubs and nodes to operate in peer-to-peer mode. Compared with a typical LoRaWAN network, the distribution of nodes is tightly controlled over a much shorter distribution distance profile, allowing hubs and nodes to interact with each other.

In this architecture, general nodes (as opposed to relay nodes, which will be discussed later) are associated with one hub, thus creating a network of devices. A general node is typically a device that hosts sensors and/or GPS

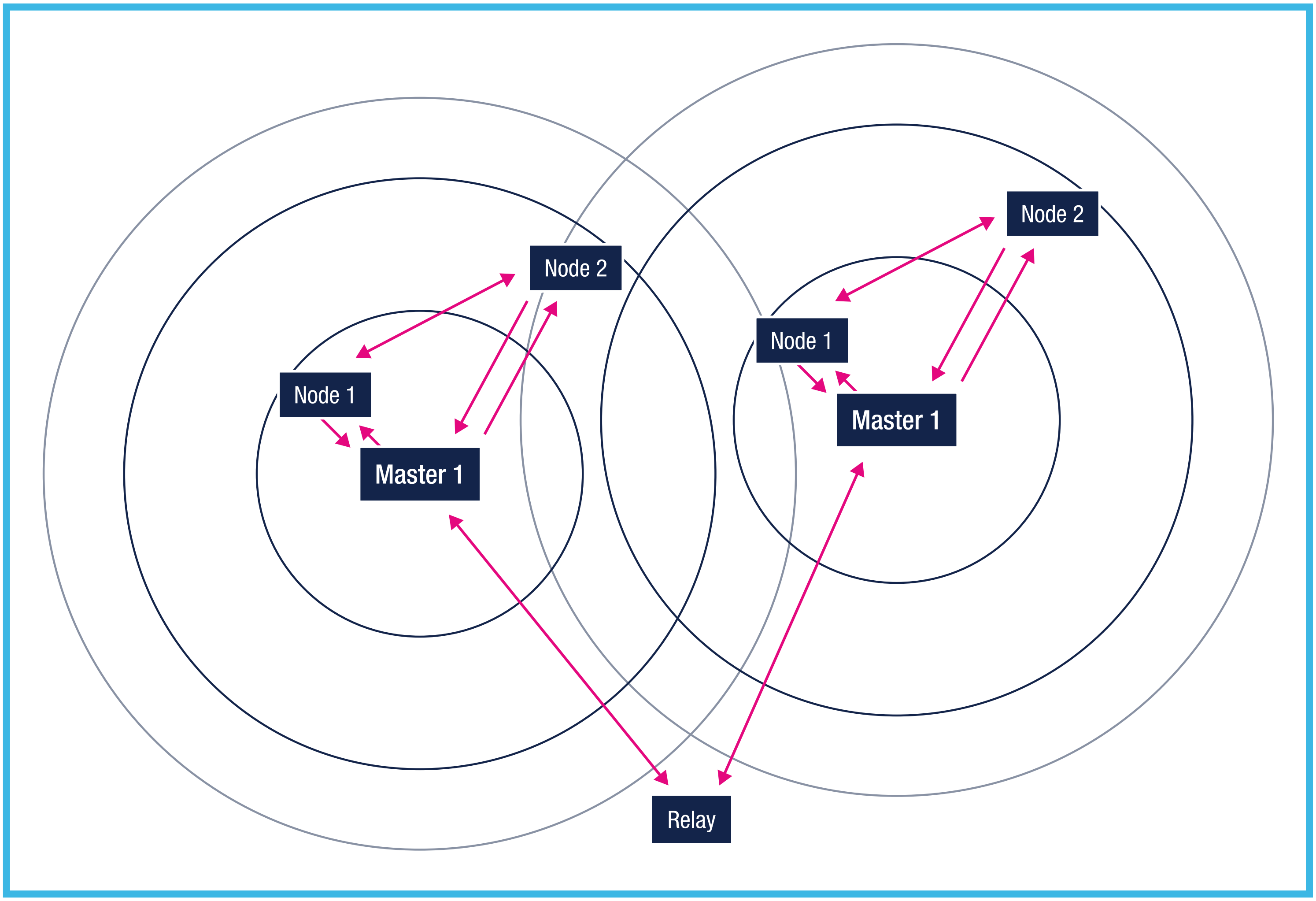


Figure 2: *Typical multi-node and network extension model. (Source: STMicroelectronics)*

receivers connected to an STM32WL—especially for applications like non-stationary asset tracking. A hub is also an STM32WL-based device, but it is configured as a master that controls baud rate, modulation type, and power to optimize link performance. More important, however, is that the hub controls the time slot generation and frequency-hopping configuration needed to meet FCC requirements and sets the communication timetable between itself, other hubs, and other nodes. Thus, each node or associated hub is completely aware of the communication time slot and frequency structure. Broadcasting this information to all elements of the network allows for a highly efficient network structure. The network topology decision to broadcast the information *a priori* to all network elements promotes higher bandwidths, frequency, and time re-use.

The first enhancement that helps with network expandability is that each general node can also communicate with other general nodes in a peer-to-peer mode, essentially performing as a mesh network and extending the footprint of the network. As previously discussed, the main hub analyzes the time slot structure and broadcasts a connection table, where nodes may communicate within an unused sector of a time slot.

A second enhancement in this architecture is that each general node can also join additional networks controlled by other hubs where those networks' coverage areas overlap, further extending the network footprint. Consequently, small local area wireless networks can be expanded by adding other local area wireless networks. The networks may operate in an overlapping manner or, if separated due to distance or obstructions blocking the wireless signals, may be connected using relay nodes. These relay nodes, as opposed to general nodes, are specialized nodes capable of connecting two or more hubs to overcome distance or physical barriers.

A third enhancement further leverages the ability of nodes to interact with other hubs by ensuring that timing is tightly controlled between hubs, allowing for mobility at pedestrian speeds as the node moves from one hub's coverage area into another's. This new architecture enhancement takes advantage of the STM32WL's GFSK modulation support, its TimeServer function (which allows each time slot to be precisely set between hubs and nodes), and its inherent customizability. It does this through a frequency-hopped, time-division multiplexing (TDM) communications protocol (**Figure 3**).

Along with mobility, the structured time slot patterns and broadcast information allow nodes to enter stop or sleep

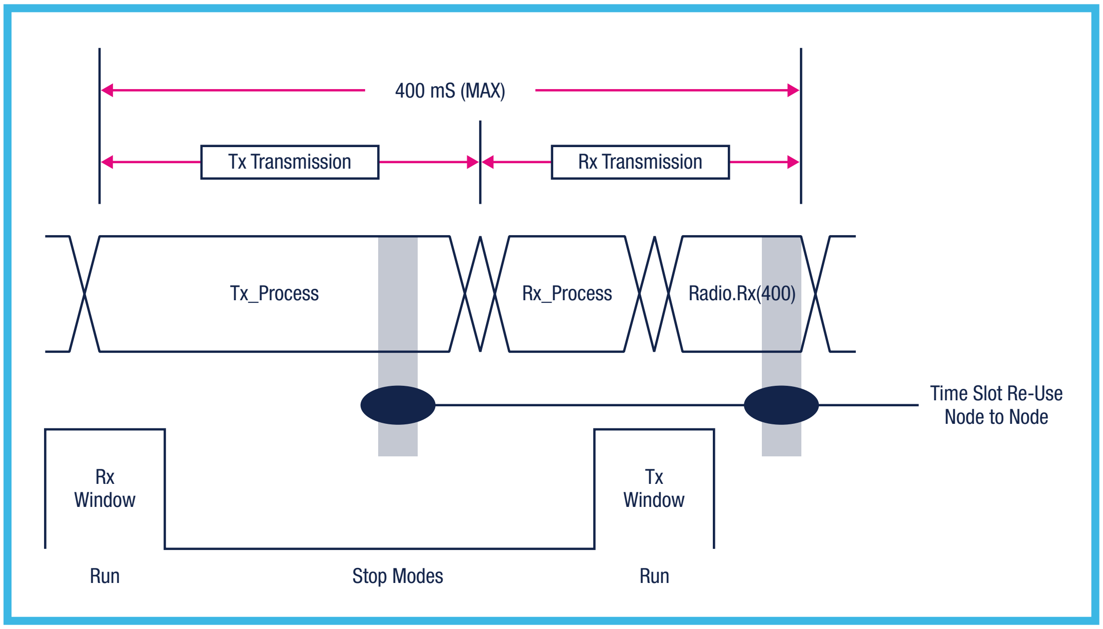


Figure 3: *Single time slot transaction summary, including node-to-node events. (Source: STMicroelectronics)*

modes at known, specific time intervals, thus minimizing power consumption from a battery-operated system. Additionally, they establish a mechanism by which layer 2 messaging may be facilitated between hubs and nodes. This allows for broadcast and control messages that enable hubs to facilitate initial discovery and connection with the nodes. Layer 2 messaging also enables the hubs to adjust modulation schemes and node transmit power based on signal quality indicators as reported by the nodes, thereby optimizing throughput versus power as appropriate for a given RF environment.

This power and modulation scheme control allows the network architecture to maintain low-power operation while still facilitating higher bandwidth than what LoRaWAN can provide. The higher bandwidth is delivered through a larger payload capacity as well as through control of the modulation schemes and the ability of the hub to direct the node to transmit at higher power levels as necessary. The typical baud rate for a node can range from 25kbps to 250kbps per time slot connection, depending upon the channel characteristics. Clearly, it is not meant to do what cellular communications can do with gigabit speeds; but the faster throughput, as well as two-way communications, expands the STM32WL's addressable applications and can be used to complement standard LoRaWAN network implementations. Dedicated, faster monitoring methods are easily integrated into an existing LoRa network as an option for long range backhaul.

While generally applicable for ultra-low-power, long-range wireless applications, the STM32WL has the elements needed to be modified for more. The project in this article is just one example of how the STM32WL's inherent capabilities, along with its customizability, can be leveraged to deliver a solution that expands the applicability of the already capable SoC. While an extremely experienced principal engineer customized the STM32WL to deliver the expanded network architecture for the project in this article, the robust development ecosystem supporting the SoC—from the preconfigured software stacks and embedded software resources to development tools and the highly engaged developer community—enables engineers of various levels to try creating their own transformative solutions.

> “While generally applicable for ultra-low-power, long-range wireless applications, the STM32WL has the elements needed to be modified for more.

Harnessing Wide Area Networks for Farming Efficiency

Anicet Giaimo, LPWAN Product Marketing Manager, Wireless Microcontrollers, STMicroelectronics

Smart farming is a data-driven concept that can potentially overcome several challenges associated with rearing livestock and growing crops. The growing world population needs to be fed, although access to land and the nutrients needed for plant and animal growth are restricted.

Farming businesses everywhere are under pressure to survive financially, even in economic areas that can provide subsidies, and must do everything possible to maximize their yield. Conversely, concern about the unwanted effects of pesticides and fertilizers, as well as antibiotics to protect animal health, is driving a desire to reduce or eliminate these human-engineered aids to farming.

Smart farming offers a different kind of technical assistance that is predicated on providing farmers with high-value information to help maximize yield and minimize reliance on chemicals and pharmaceuticals.

Timing is everything for farmers: Spotting when conditions are right to sow seeds, when the crop is optimal for harvesting, and identifying plant or animal health problems as early as possible is key. Smart farms can provide that guidance, in real time, by capturing data that contains the raw information. IoT technologies make it possible to deploy and connect sensors anywhere relevant indicators can be monitored, even inside animals, and gather the data into applications to generate actionable insights.

Smart Farming in Action

Given that farms typically exist in rural locations and can cover areas equivalent to many thousands of acres, connectivity needs to be wireless and, in many cases, must be effective over distances of up to several kilometers. Providing power to sensors and infrastructure is another concern; batteries and energy harvesting are obvious candidates, although the equipment must be designed for minimal energy demand to have a practicable operating lifetime. And then there are environmental hazards to consider—farming lifestyles are hard, so the tech can expect to live outdoors, through rain and snow, from deep sub-zero to equatorial summer temperatures, and endure exposure to all kinds of substances, including chemicals, oils, and animal waste.

Wireless technology also facilitates placing sensors in locations that are difficult to monitor frequently, giving insights that would be impractical to capture using conventional techniques. Is there a more extreme example than inside an animal? ST has helped to develop swallowable sensors for cattle farming, using its STM32WL wireless system-on-chip (SoC) to collect physiological data from individual animals. Regularly monitoring signs such as water intake, body temperature, and digestive pH can show when a cow is in heat, becoming sick, or if other health issues need attention. This knowledge can help farmers reduce breeding costs by increasing the likelihood of fertilization. It can also reduce their use of antibiotics by allowing a targeted approach that contrasts with practices that preemptively add the drugs to food provided for all cattle.

The STM32WL integrates a multiprotocol radio with a 32-bit Arm® Cortex®-M microcontroller (MCU) to host the application, which contributes to achieving an extremely robust sensor able to withstand its operating environment. The radio complies with the LoRaWAN® physical layer requirements specified by the LoRa Alliance®, also supporting Sigfox™, WM-BUS, mioty®, and other protocols. The associated STM32CubeWL software package provides resources, including LoRaWAN and Sigfox stacks, low-layer APIs, and sample application code.

In another application, these long-range wireless MCUs are helping smart, connected rubber-tree-tapping robots in Asia to detect the right conditions for collecting sap, thus preserving the condition of the harvest and the tree. ST helped redesign the robots' existing radio communication subsystem, which had been found to be vulnerable to interference by other signals in the local area. LoRa modulation is highly resistant to interference yet operates in a license-free sub-1GHz frequency band available anywhere in the world. LoRa networks are also established worldwide and accessible through locally appointed service providers at a reasonable cost per connection.

One further characteristic of the STM32WL, valuable in smart farming applications, is the low-power MCU technologies that allow sensors to operate for long periods from a minimal energy supply. This could be a single-cell battery or, in the case of the Silvanet wildfire sensors created by ST customer Dryad, an energy harvesting system like a small solar panel. Silvanet sensors can be installed in remote locations where there is no convenient power infrastructure and can operate maintenance-free for up to about 15 years. Arrays of these sensors, connected using LoRa wireless, provide an early warning of forest fires and help minimize their effects, which can be catastrophic in so many ways, including the destruction of wildlife, animal habitats, economic assets, and farmland.

Developing with Wireless MCUs

The STM32WL portfolio provides flexible options to help product developers accelerate time to market, optimize the engineering and per-unit costs of their products, and support scalability in the future. The STM32WL5M module is a 10mm × 10mm system-in-package (SiP) that contains an STM32WL5 wireless MCU with frequency-control crystals, an ST IPD intelligent passive device containing RF matching filters needed to connect the antenna, and a transmit/receive switch already integrated. It comes ready to use, pre-certified for connection to LoRaWAN and Sigfox networks, and supported in the STM32CubeMX ecosystem. Users can also optionally select the STSAFE-A110 secure element, a drop-in authentication solution powered by a state-of-the-art secure MCU with cryptographic accelerators, secure key storage, and ready for pre-loading with Sigfox or LoRaWAN LPWAN security credentials.

Sensor Integration

The STEVAL-ASTRA1B reference design, built around the STM32WL5 SoC, provides a fast and simple way to build complete wireless sensors suitable for smart

agriculture applications and asset tracking such as livestock monitoring, as well as fleet management and logistics. This reference design also contains the STM32WB5MMG 2.4GHz *Bluetooth*® Low Energy module for short-range communication and an optional STSAFE-A110 secure element.

This reference design comes with comprehensive software, firmware libraries, tools, a battery, and an antenna, all conveniently housed in a plastic case, ready to start experimenting. The kit embeds a complete set of MEMS environmental and motion sensors. These include the LIS2DTW12 digital output dual motion and temperature sensor, LSM6DSO32X inertial module with 3D accelerometer and 3D gyroscope, STTS22H ultra-low-power high-accuracy temperature sensor, and LPS22HH barometric pressure sensor. The Teseo-LIV3F GNSS module is also integrated to provide outdoor positioning data, as well as the ST25DV64K dynamic NFC/RFID tag IC that simplifies product marking and contactless reading.

This development kit represents a sensor-to-cloud proof of concept available through dedicated mobile applications for setting up and monitoring the tracker using Bluetooth Low Energy and a web-based cloud dashboard accessible using a myST account for remote monitoring.

Together, the SoCs, modules, and STEVAL-ASTRA1B reference design provide several options to short-cut hardware development and overcome the complex RF design challenges to help keep developers' projects on track. In addition, ST's long-range wireless MCUs and modules also come with the STM32Cube ecosystem and manufacturer support to optimize and fine-tune the application. It's a smart way to deliver powerful solutions for smart farming.

STEVAL-ASTRA1B from the box to the cloud in a few minutes

STEVAL-ASTRA1B Asset Tracking Evaluation Board

Learn More ⟶

Interconnecting the Smart, Safe, Sustainable City

**Filippo Colaianni, Technical Marketing Manager,
IoT & Connectivity, STMicroelectronics**

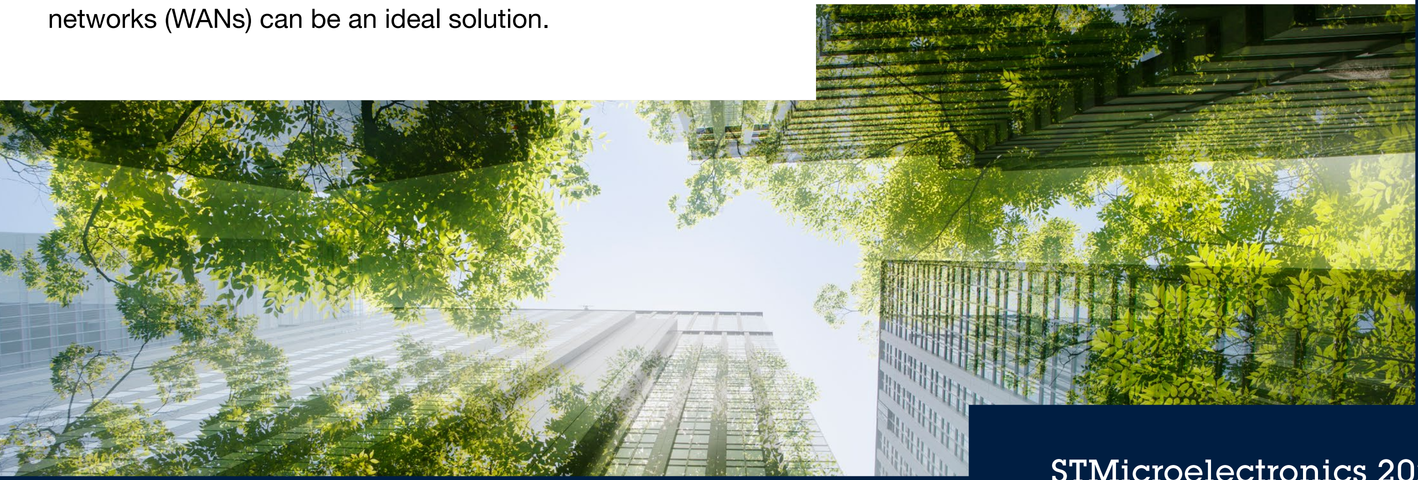
Smart cities aren't just dreamscapes. Today, a significant number of smart-city initiatives promise to manage energy, ease traffic flow, improve safety, track assets, and generally boost the quality of life for residents. These initiatives rely on a number of technological advances, especially communications infrastructure that links sensors and computing resources into coherent networks.

Such networks can control, for example, street lighting, minimizing energy consumption and maintenance cost. They can link smart meters to energy distributors as well as consumers, so distributors of electricity, gas, and water can optimize them. This network can be used to monitor and track chemical and noise pollution. And they can interrogate stress and vibration sensors on critical infrastructure so city engineers will know continuously the health of their buildings, bridges, and roads.

A challenge common to all these applications is connectivity. Many of the sensor systems required must have long unattended operating lives, often disconnected from both physical networks and the electrical grid. They must communicate over long distances with very low energy consumption and high reliability. Fortunately, most will not require high sustained data rates. So low-power, wide-area networks (WANs) can be an ideal solution.

Of the low-power WAN architectures available today, Semtech's Long Range (LoRa) technology is perhaps the most promising. Based on chirped spread-spectrum modulation that spreads the transmitted signal across a wide frequency band, LoRa achieves ranges up to 3–5km in urban settings—and three times that for unobstructed line of sight—at very low energy per bit, with high data integrity and high resistance to interference. Recognizing that much of the data that moves around in a smart-city WAN will be sensitive, LoRA offers secure transmission with AES-128 encryption.

LoRaWAN, an open standard developed by the LoRa Alliance, builds data-link and network layers on top of LoRa, creating a star-of-stars network topology. This topology allows for enormous networks with potentially millions of connections. A new gateway concept allows the topology to reach beyond urban cores into remote areas.

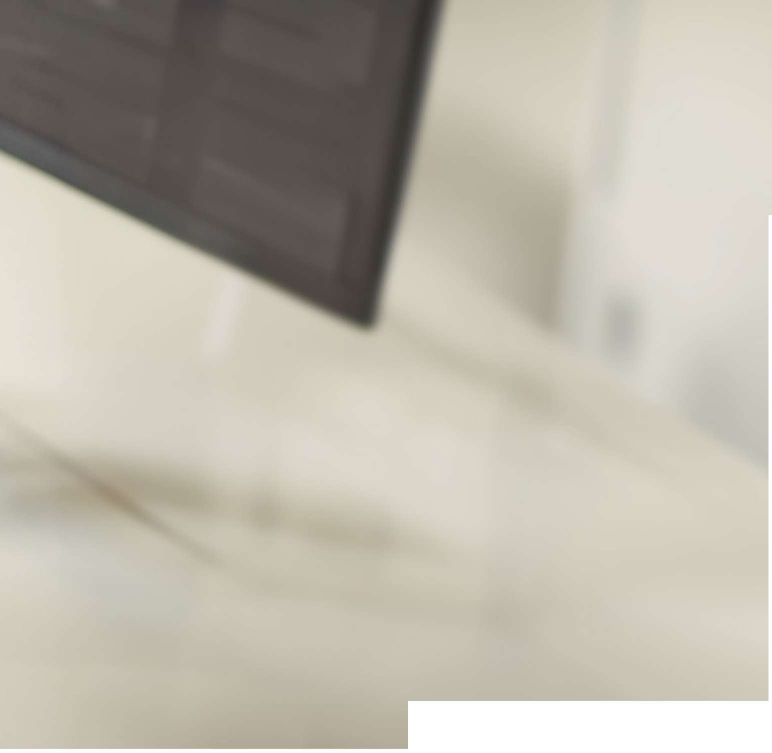


The building blocks for these urban networks are already appearing. Today, STMicroelectronics offers the STM32WL wireless microcontroller, the first MCU in the industry with an embedded LoRa transceiver. This device is available in chipset or module form, and in evaluation boards such as the STEVAL-ASTRA1B. This board includes LoRa, *Bluetooth*®, and NFC, as well as a GNSS positioning module and MEMS sensors (including temperature and pressure sensors, an accelerometer, and a gyroscope), making it ideal for asset tracking and monitoring. A full solution (**Figure 1**) includes the STAssetTracking mobile app for configuration and real-time monitoring via Bluetooth Low Energy, and a web-based cloud dashboard, the DSH-ASSETTRACKING, for remote real-time monitoring.

Similarly, for infrastructure monitoring applications, STMicroelectronics offers a reference design, STDES-CBMLoRaBLE. It features Bluetooth Low Energy and LoRa connectivity, an integral vibrometer and inclinometer, and dedicated algorithms for vibration analysis and tilt monitoring.

This last solution allows users to monitor assets and infrastructure using long-distance connectivity, thanks to a web-based cloud interface based on AWS, the DSH-PREDMNT. Through this interface, users can visualize device information in the cloud, anytime and anywhere.

LoRaWAN has emerged as one of the most promising technologies for implementing the industrial Internet of Things (IIoT) in smart cities. STMicroelectronics is accelerating the deployment of these concepts with products and reference designs that are ready for proof-of-concept demonstration and field testing—today.



> “LoRaWAN has emerged as one of the most promising technologies for implementing the IIoT in smart cities.

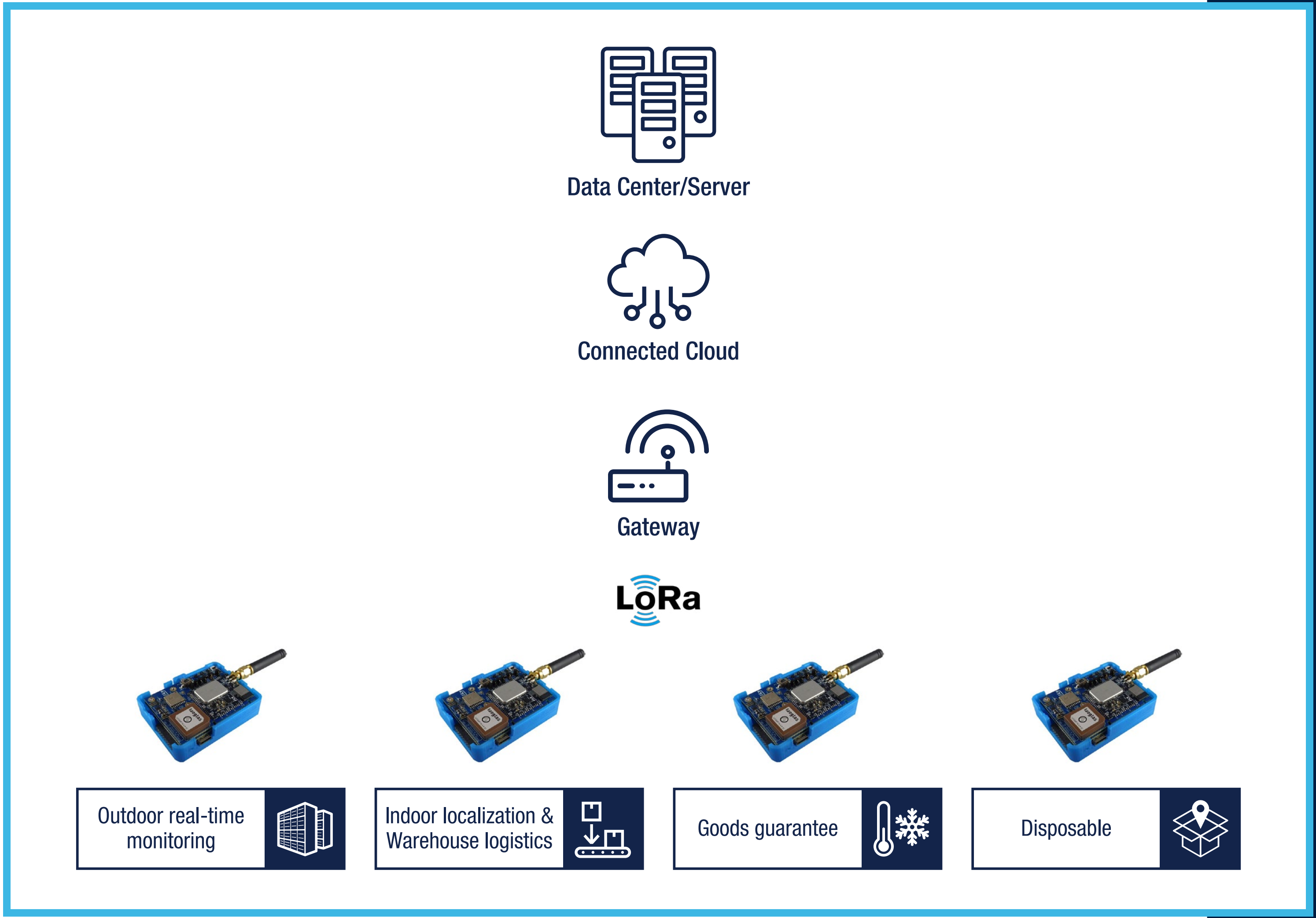

Data Center/Server
Connected Cloud
Gateway
LoRa
Outdoor real-time monitoring
Indoor localization & Warehouse logistics
Goods guarantee
Disposable

Figure 1: *LoRa network with STEVAL-ASTRA1B asset tracking. (Source: Mouser Electronics)*

Mouser stocks the widest selection of the newest products

mouser.com/st

Worldwide leading authorized distributor of
semiconductors and electronic components

MOUSER
ELECTRONICS