

EMPOWERING ENGINEERS TO BUILD THE FUTURE



Farnell

AN AVNET COMPANY

EXPERT ADVICE

ISSUE 2

LEADING EDGE WIRELESS CONNECTIVITY

RADIO
COMMUNICATIONS +
SOLUTION

MASTERING
ANTENNA
DESIGN

ZIGBEE
VS.
BLUETOOTH

5G ANTENNA
AND CONNECTOR
DESIGN

SECURING
CONNECTED
DEVICES

PREFACE

Welcome to our meticulously curated edition of Expert Advice "Leading Edge - Wireless Connectivity." We acknowledge design engineers' pivotal role in shaping the future in today's fast-paced technological landscape, where precision meets innovation. This edition addresses the intricate challenges professionals like you face in wireless connectivity.

The demand for seamless wireless solutions is at an all-time high, reshaping industries and transforming our lives. With the escalating need for interconnected devices, your expertise in optimising wireless solutions has become indispensable. Design engineers are now tasked with creating robust and adaptable wireless solutions amidst ever-changing technologies.

This edition explores the challenges, innovations, and solutions defining your domain. Dive into mastering antenna design, navigate the complexities of choosing between Zigbee and Bluetooth, discover strategies for overcoming obstacles in 5G antenna and connector design, learn to integrate the most suitable radio communications solutions, and gain insights into securing connected devices.

Each article is meticulously crafted, offering practical insights, in-depth analyses, and real-world solutions tailored to your daily hurdles. We understand the importance of staying ahead of technology trends and strive to equip you with the knowledge needed to excel in your field.

We invite you to engage deeply, ponder the facts, contemplate the reasons, and draw inspiration from the solutions provided. We are confident that the knowledge within these pages will empower you, inspire innovation, and strengthen your expertise in the dynamic field of wireless connectivity.

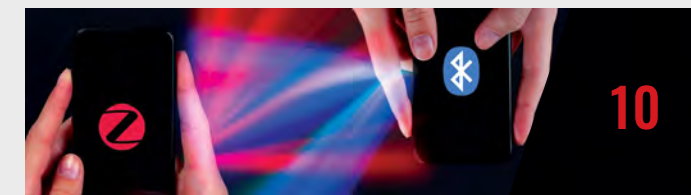


Cliff Ortmeier, Editor
Email: editor-TJ@element14.com

CONTENTS



MASTERING ANTENNA DESIGN



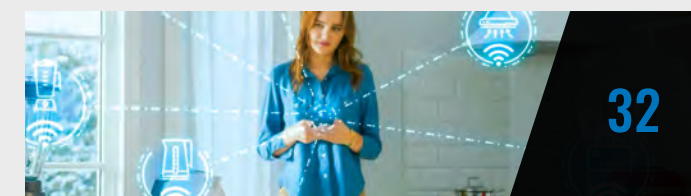
ZIGBEE VS. BLUETOOTH



5G ANTENNA AND CONNECTOR DESIGN



RADIO COMMUNICATIONS SOLUTION



SECURING CONNECTED DEVICES

Editor-in-chief: Cliff Ortmeier,
Managing Editor: Ankur Tomar

©Premier Farnell. All rights reserved. No portion of this publication, whether in whole or in part, can be reproduced without the express written consent of Premier Farnell. All other registered and/or unregistered trademarks displayed in this publication constitute the intellectual property of their respective holders. Errors and omissions in the printing of this magazine shall not be the responsibility of Premier Farnell. Premier Farnell reserves the right to make such corrections as may be necessary to the prices contained herein.



Scan QR code to register
and to access all issues of
Expert Advice



MASTERING ANTENNA DESIGN: OPTIMIZE WIRELESS CONNECTIVITY

Antennas are an essential component of every wireless communication system. The efficiency and effectiveness of antennas is critical to the success of any wireless communication system.

As the need for seamless wireless communication expands, it becomes essential to understand the complexities of antenna design and the elements that contribute to optimal performance.

Wireless connectivity has become an indispensable aspect of our daily lives, linking gadgets and allowing communication across long distances.

Wireless communication, on the other hand, has various drawbacks, including limited range, prolonged data transfer, and signal interference. A good antenna is an effective wireless communication option. An antenna's design impacts how successfully it can broadcast and receive signals.

Engineers can design better-working antennas by considering factors such as radiation pattern, impedance matching, frequency range, and polarisation. These factors influence the range of antennas, increase the speed of data transfer, and make signals stronger.

This article will dive into how antenna design concerns affect wireless connectivity. We will go through the aspects that influence antenna design, operation, and type. We will also go through antenna selection and design considerations.

Fundamentals of Antenna

An antenna consists of a conductor that is exposed in space. An antenna is formed when the length of the conductor is a specific ratio or multiple of the wavelength of the signal. As the electrical energy provided to an antenna is radiated into free space, this phenomenon is known as "resonance."

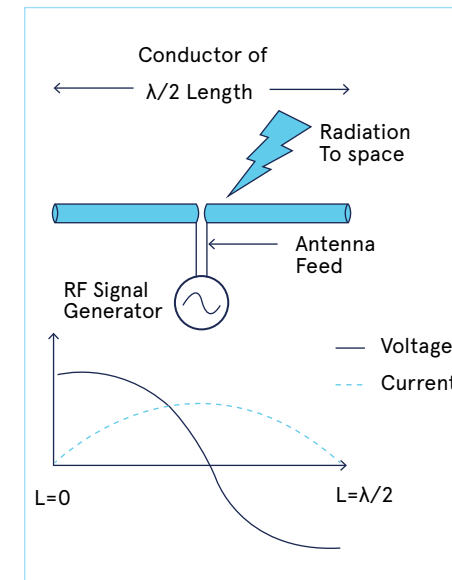


Figure 1: . Dipole Antenna Basic

In figure 1, the wavelength of the electric signal (λ) is twice the size of the metal part. The antenna receives the signal from the signal generator through a transmission line called the "antenna feed".

The figure shows the current and voltage form along the metal part when the wavelength is twice the length. This type of antenna is termed a dipole antenna.

However, on printed circuit boards, most antennas work equally well by using a metal a quarter of the wavelength ($\lambda/4$) and arranged in a specific way.

Types of Antennas

Any conductor of length $\lambda/4$ exposed in free space over a ground plane with an appropriate feed can be an effective antenna, as explained in the preceding section. The antenna can be as long as a car's FM antenna or as small as a trace on a beacon, depending upon the wavelength. For use with 2.4-GHz applications. In this section, we will look at some of the most common types of antennas:

1. Monopole Antenna

The Monopole antenna is an unbalanced antenna with a single-quarter wavelength element. It is made up of a single conductor suspended above a conducting surface, usually the ground plane. Vertically polarised monopole antennas feature a half-omnidirectional radiating pattern. They are frequently employed in mobile devices, cellular base stations, and other applications where space is limited.

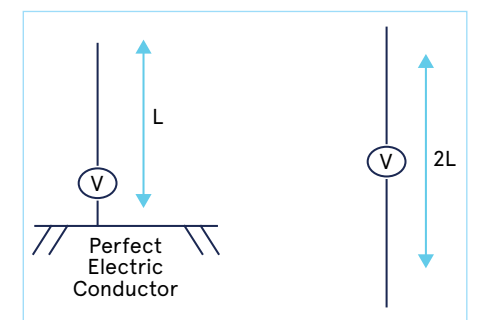


Figure 2 : Monopole Antenna

2. Dipole Antenna

The Dipole antenna consists of two physical elements, each of which is a quarter wavelength. The directivity is the same as the Monopole, but the use of two physical quarter wavelength elements instead of one, with support from a ground plane reflection results in a potential gain of up to 3dB over the Monopole in some configurations. They are extensively utilised in mobile devices, cellular base stations, and other applications where space is constrained.

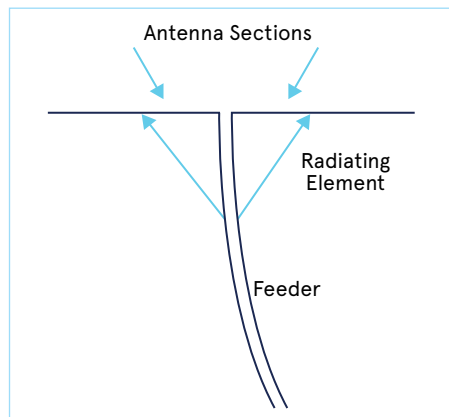


Figure 3 : Dipole Antenna

3. Loop Antenna

Due to its simplicity and ease of construction, loop antennas resemble both dipole and monopole antennas in terms of their features.

Loop antennas come in a variety of shapes, including circular, elliptical, and rectangular, etc. The configuration of the loop antenna has little bearing on its basic properties.

They have a frequency of about 3GHz and are commonly employed in communication networks. In microwave bands, these antennas can also be utilised as electromagnetic field probes.

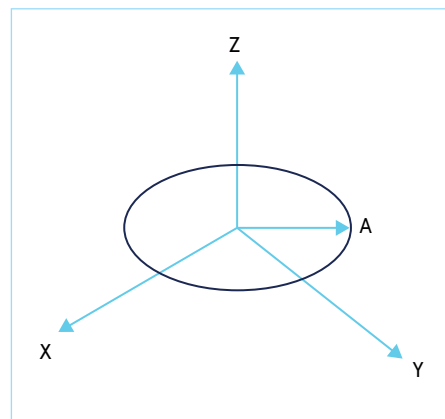


Figure 4: Loop Antenna

4. PCB Antenna

This is a trace drawn on the PCB. Depending upon the antenna type and space limits, this can be a straight trace, an inverted F-type trace, a meandering trace, a circular trace, or a wiggled curve. In a PCB antenna, the antenna becomes a two-dimensional (2D) structure in the same plane as the PCB; see Figure 5.

There are guidelines that must be observed whilst the 3D antenna exposed in free space is transported to the PCB plane as a 2D PCB trace.

A PCB antenna requires greater PCB space, has a less efficiency than a wire antenna, but is less expensive. It is simple to manufacture and provides an adequate wireless range for a BLE application.



Figure 5. PCB Antenna

5. Chip Antenna

This is an antenna in the shape of a tiny form-factor IC with a conductor packed within. When there isn't enough room to print a PCB antenna or support a 3D wire antenna, this is useful. Figure 6 depicts a Bluetooth module with a chip antenna. The size of the antenna and module in relation to a one-cent coin is shown below.

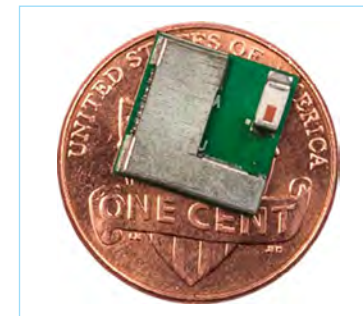
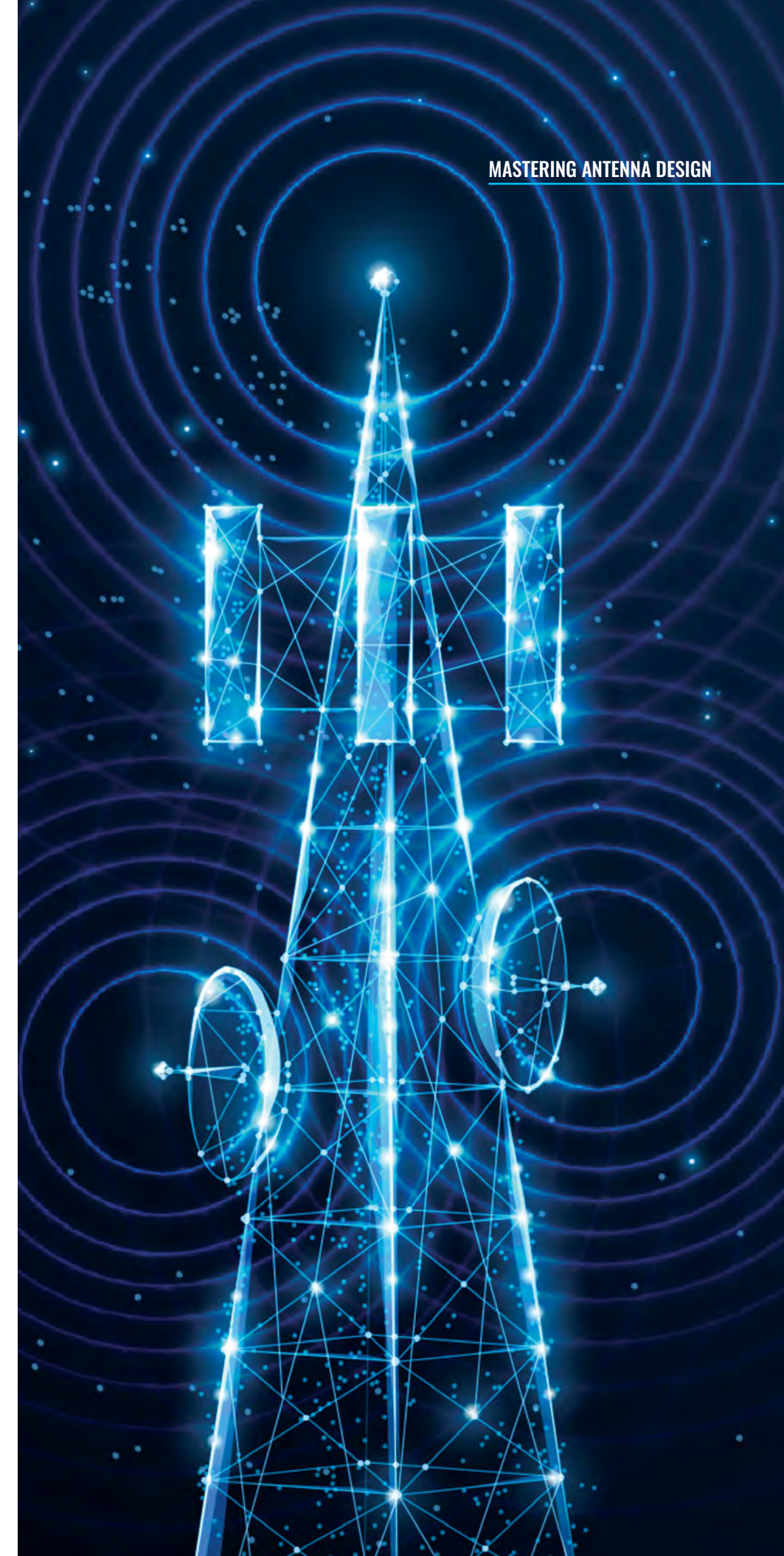


Figure 6. BLE Module (10 mm × 10 mm) with Chip Antenna



Choosing an Antenna and Antenna Design Considerations

There are various key characteristics to consider when developing an antenna for wireless connectivity. These characteristics contribute to the antenna's performance and efficiency in transmitting and receiving signals. Here are some key antenna parameters to consider:

Gain

In contrast to an isotropic antenna, which radiates uniformly in all directions, gain indicates the radiation in the direction of interest. This is expressed in decibels (dB)—how intense the radiation field is in compared to an ideal isotropic antenna.

Bandwidth

The frequency response of an antenna is indicated by its bandwidth. It denotes how well the antenna is matched to the 50Ω transmission line across the whole spectrum of interest, which for BLE applications is between 2.40 GHz and 2.48 GHz.

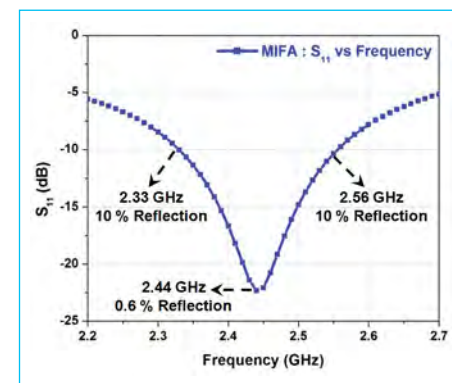


Figure 7. Bandwidth

Return loss

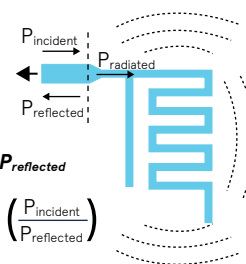
An antenna's return loss indicates how well it is matched to the 50Ω transmission line (TL), illustrated as a signal feed in Figure 8. The normal TL characteristic impedance is 50Ω; however, it might be a different number. Return loss (Equation 1) specifies how much of the incident power is reflected by the antenna owing to a mismatch.

When precisely aligned, an ideal antenna will radiate the entire energy without any reflection. The antenna is perfectly matched to the TL if the return loss is infinite, as shown in Figure 7. S11 is the inverse of return loss in dB. In most circumstances, a return loss of 10 dB (equal to S11 -10 dB) is deemed enough. The return loss (dB) is proportional to the power reflected by the antenna (percent). A return loss of 10 dB indicates that 90% of the incident power is utilised by the antenna for radiation.

Equation 1

$$\text{Return Loss (dB)} = 10 \log \left(\frac{P_{\text{incident}}}{P_{\text{reflected}}} \right)$$

Transmission line leading to the matching network and PSoC/PROC BLE



$$P_{\text{radiated}} = P_{\text{incident}} - P_{\text{reflected}}$$

$$\text{Return Loss (dB)} = 10 \log \left(\frac{P_{\text{incident}}}{P_{\text{reflected}}} \right)$$

Figure 8: Return Loss

S ₁₁ (dB)	Return Loss (dB)	P _{reflected} /P _{incident} (%)	P _{radiated} /P _{incident} (%)
-20	20	1	99
-10	10	10	90
-3	3	50	50
-1	1	79	21

Table 1. Return Loss and Power Reflected from Antenna

Radiation efficiency

A portion of the non-reflected power (see Figure 8) is dissipated in the antenna as heat or thermal loss. The dielectric loss in the FR4 substrate and the conductor loss in the copper trace cause thermal loss. This data is referred to as radiation efficiency.

A radiation efficiency of 100% means that all non-reflected power is radiated to free space. The heat loss on a small-form-factor PCB is low.

Radiation pattern

The radiation pattern reveals the directional feature of radiation, that is, which directions have more, and which have less radiation. This information aids in appropriately orienting the antenna in an application. In the plane perpendicular to the antenna axis, an isotropic dipole antenna radiates equally in all directions. Most antennas, however, vary from this optimal behavior.

Figure 9 depicts the radiation pattern of a PCB antenna as an example. Each data point shows RF field intensity as measured by the receiver's received signal strength indicator (RSSI). Because the antenna is not isotropic, the contours are not quite round, as predicted.

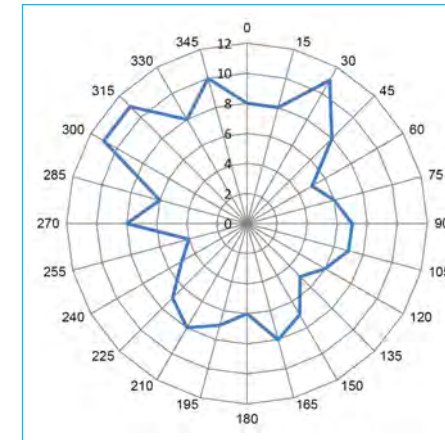


Figure 9. Radiation Pattern

Size and form factor

The physical size and shape of the antenna are crucial factors to consider, particularly in space-constrained applications. To accomplish the necessary size and shape while keeping high performance, miniaturisation techniques and alternative antenna topologies can be used.

Interference and noise

When designing an antenna, consider variables such as interference and noise sources that may impair signal quality. Filtering and shielding are two antenna design strategies that can assist reduce the impact of external interference.

Conclusion

As more products become wirelessly connected, antenna design recommendations will become increasingly crucial for PCB and industrial designs. To prevent costly delays and changes in architecture that may have a substantial influence on time-to-market and development costs, antenna design must be thoroughly considered early in the development cycle.

Farnell has partnered with many different suppliers catering to a wide range of Antenna portfolios for wireless connectivity, such as Antennas, Antennas - RFID, RF Antennas, WiFi Antenna, NFC Antenna, Antennas - Dual Band Chip and Antennas - Single Band Chip.

High-Speed Solutions

Explore our range of high-performance antennas designed for IoT excellence.

[Click here](#)

ZIGBEE VS. BLUETOOTH: CHOOSING THE IDEAL EDGE DEVICE MESH PROTOCOL

Most IoT applications are grouped around four functions: sensing, communication, computing, and actuation. The Internet of Things (IoT) uses these applications to connect companies' assets to their operating systems.



However, it is impossible for a single device to support all four capabilities. Older systems thus used end devices for environmental sensing, gateways for communication and network needs, and the centralised cloud-like server did the computation.

The system then sent the generated information to selected devices that acted as executors. However, such a centralised computing system failed to satisfy the exacting needs of time-critical and compute-intensive applications.

The shortcomings of the centralised computing system have led to edge devices adopting new management systems. These systems enable real-time response and management of critical assets in highly distributed environments.

Edge device mesh networking involves connecting multiple edge devices to create a mesh network that provides high reliability, flexibility, and scalability. However, a key challenge is to choose the correct protocol when setting up an edge device mesh network. It is vital to select one that fits your specific needs.

Two popular protocols for edge device mesh networking are Zigbee and Bluetooth. Each protocol has its advantages and disadvantages. Ultimately, the choice between Zigbee and Bluetooth will depend upon the specific application needs and the devices used.

The correct protocol enables the network to run smoothly and achieve the desired outcome. This article will explain why choosing the proper edge device mesh networking protocol is crucial.

Zigbee

Zigbee is a globally accepted open standard that allows low-power, low-bandwidth wireless mesh networking at an affordable cost. The Zigbee protocol facilitates data transmission over extremely long distances. These messages reach their destination by hopping through the intermediary radio nodes. The 2.4 GHz frequency range allows license-free communication up to a range of 100 meters.



3 Zigbee Mesh Kit



ONsemi Strata enabled



Digi Xbee 2.4GHz



USB Dongle

Advantages of the Zigbee Protocol

Zigbee can help to create substantial mesh networks that can exceed the reach of a single radio. The mesh network can configure itself automatically (self-forming) and is self-healing. By self-healing, Zigbee can dynamically reconfigure itself to restore functionality if any nodes are removed or disabled. The interoperable standard of Zigbee allows seamless communication amongst devices from various manufacturers, leading to its widespread adoption in home automation and industrial IoT.

Zigbee comes with tough security measures, such as support for AES-128 encryption that safeguards the data when it is exchanged amongst devices. Zigbee provides superior scalability and can accommodate up to 65,000 devices in a single network.

Limitations of the Zigbee Protocol

The Zigbee nodes that “hop” or route messages inside the Zigbee mesh network must have power. This is typical with most mesh networks. Although end devices can participate inside the mesh, they cannot extend it. These devices conserve battery life through intermittent sleep. The Zigbee nodes do not favour the IP addressing method.

Instead, the nodes install gateway devices to establish connectivity with cloud and internet services. Platforms such as Android, iOS, and Windows do not currently support Zigbee. An additional gateway is required to connect them to Zigbee, making it a complex process. The higher latency of the mesh network must be considered in light of the mesh’s noticeably greater reliability and effective range.

Bluetooth

Bluetooth is used in personal area networks (PAN). Bluetooth Special Interest Group (SIG) develops and manages this wireless networking protocol. The Bluetooth protocol implements a master/client architecture where, in a small personal-area network, a master device can connect up to seven client devices. The specially designed Bluetooth Classic can transmit high-throughput data at 2 Mbps and maintain long battery life. The SIG ensures compatibility amongst various device manufacturers.

Bluetooth Mesh is a recent protocol that includes routing and network formation standards to extend simple point-to-point BLE and establish mesh networks. Such networks can use nodes as relays to expand beyond the range possible by a single device. Despite being similar in architecture and function to Zigbee, Bluetooth Mesh has many differences. Although a Bluetooth network can theoretically accommodate over 32,000 nodes, practical considerations such as bandwidth restrict it to a few hundred devices.

Advantages of using Bluetooth

Bluetooth can transfer streaming audio or video content or large files due to its high data transfer speeds, reaching 2 Mbps. In addition, Bluetooth has AES-128 encryption support and other excellent security features. Mesh networks enabled through Bluetooth technology are not restricted by the range of a single radio node.

This is possible as a single node can route and forward messages to destinations beyond their nominal range, creating extensive physical networks. Since Bluetooth Mesh is built on BLE, it inherits the many advantages of that protocol, like low energy use, beaconing support, and good security. BT Mesh networks are self-repairing and autonomous, and like Zigbee, with sleep support for end devices engaged in a store-and-forward parent/child relationship.

Limitations of the Bluetooth Protocol

Bluetooth Mesh is a new protocol with ongoing modification and improvements. Support for this protocol is limited, and original equipment manufacturers (OEMs), handheld devices, and gateways may not be completely compliant. When compared with Zigbee, Bluetooth Mesh has a lower level of scalability. Bluetooth Mesh can support a maximum of 32,000 devices per single network.

Bluetooth Mesh follows the “managed flood” protocol in network design. This protocol simplifies network design, but there are trade-offs: power usage and efficiency are sacrificed. Devices routed in Bluetooth Mesh must be mains powered as routers cannot sleep like Zigbee nodes.

Interactions of BT Mesh routers with the Internet and cloud servers must pass via border routers or fixed gateways, as IP addressing is not used. Mesh networks must have higher latency since messages must “hop” through several nodes to reach their destination. Applications thus must tolerate slower response times. This slowness is a trade-off for the bigger mesh network scale.

Comparison between Zigbee and Bluetooth

Range, Scalability & Mesh network size

Bluetooth Mesh and Zigbee do not need a license to work in the 2.4GHz spectrum. However, many devices have BLE and, by extension, Bluetooth Mesh capability. Conversely, a Zigbee mesh network requires a communication gateway with smartphones and other devices.

Bluetooth Mesh and Zigbee networks share similar conditional range limits between nodes – 10 meters to 100 meters. Zigbee can support a higher number of nodes in a mesh. The theoretical limit of Bluetooth Mesh is 32,000 nodes, whilst it is 65,000 nodes for Zigbee. This implies that a Zigbee mesh network—theoretically—can cover twice the area of Bluetooth Mesh. In practice, the network size will be limited by other concerns.

Power consumption and sleep modes

Engineers must consider power consumption. This is specifically applicable to battery-powered nodes. The Bluetooth Mesh and Zigbee nodes that act as routers must be active if these nodes transfer data across the mesh. End devices in both protocols can sleep when they are non-participants in the mesh. Bluetooth Mesh nodes need less power than Zigbee nodes when active.

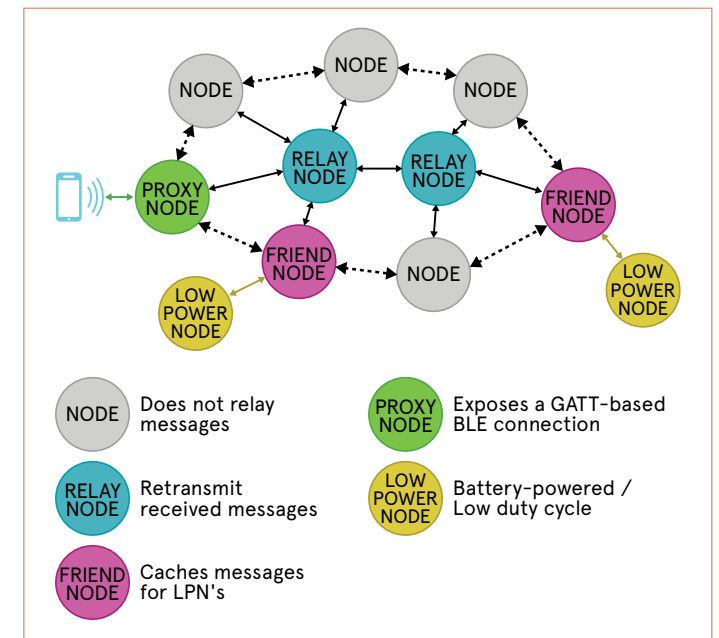


Figure: End devices can sleep without participating in the mesh. (Source: STMicroelectronics)

Data Rates

Bluetooth Mesh, at first glance, seems to have an advantage over Zigbee when it comes to the data rate of each network. BT Mesh has an air data rate of 1Mbps, and Zigbee's is 250Kbps. However, making decisions solely on the basis of air data rate is not recommended as data is relayed between many nodes, and the efficiency of data transfer depends upon the path it takes through the mesh network.

The architecture of a mesh network can vary even if the same protocol is used. The architecture depends on various factors such as the nodes' physical location and the network's configurable logical structure.

For example, if the end devices have to sleep, a Zigbee network can use many router nodes close to the end device nodes' clusters. There can be fewer router nodes if power consumption is a negligible concern.

Security

Both Zigbee and Bluetooth offers support for AES-128 encryption. With this, they have robust security features. However, Zigbee has a higher level of security compared to Bluetooth.

Comparison Chart: Bluetooth v/s ZigBee

	ZigBee	Bluetooth
Network Type	Local Area Network (LAN)	Personal Area Network (PAN)
Range	291 meters	77 meters
Frequency	Around 2.4GHz	2.4GHz to 2.483 GHz
Operating System	Not currently compatible	Android, iOS, Windows and OS X
Throughput	250 kbps	270 kbps
Cell Nodes	Has almost 65000 cell nodes	Maximum 8 cell nodes
RF Channels	Has only 16 RF Channels	Has 79 RF Channels

Topology	Mesh only	Mesh and Star
Modulation	Uses GFSK, BPSK and QPSK modulation techniques	Uses GFSK modulation technique
Transmit Power	100mW	10mW

Use cases

Zigbee finds use in various industries:

1. Home automation: Smart homes use Zigbee control security systems, lighting, thermostats, and security systems.
2. Industrial automation: Manufacturing plants use Zigbee in industrial automation for monitoring and controlling processes.
3. Healthcare: Healthcare applications, including remote patient monitoring, medical adherence, and tracking medical equipment, uses Zigbee.

Bluetooth finds use in many industries.

1. Healthcare: Many healthcare applications that monitor vital signs, track medical equipment, and monitor remote patients use Bluetooth.
2. Consumer electronics: Wireless headphones, speakers, and other audio devices generally use Bluetooth
3. Retail: Bluetooth is used in retail applications that use indoor location-based services, and proximity marketing use Bluetooth.
4. Automotive: Cars that offer hands-free calling, audio streaming, and other features use Bluetooth

Conclusion

Bluetooth Mesh and Zigbee networks share more similarities than distinctions. Both are excellent options; you do not have to choose between them. Modern hardware, such as STMicroelectronics' STMWB55 series of SoCs, supports Zigbee and Bluetooth Mesh networks.

Several factors must be considered when comparing Bluetooth and Zigbee for mesh networking on edge devices. Zigbee is better suited for larger networks and low-power applications.

It offers better scalability and security but with trade-offs such as limited range and slower data transfer rate. Conversely, Bluetooth is suitable for smaller networks and high-speed data transfers. It provides lower scalability, with a shorter range and high-power consumption.

The choice between Zigbee and Bluetooth for edge device mesh networking requires consideration of power consumption, scalability, range, and security. The protocol must also be compatible with the devices to be used in the network.

Farnell has partnered with many different suppliers catering to a wide range of edge device mesh networking components portfolio, such as Internet of Things, IoT Solutions Kits, Wireless Modules & Adaptors, Communications & Networking Modules, Bluetooth Modules & Adaptors, Zigbee Modules / XBee, WLAN Modules & USB Adaptors, Industrial Wireless, RF / Wireless Development Kits, and Networking - Wireless Products.



Wireless Connectivity Solutions

Experience Seamless Connectivity with our wide selection of Wireless Modules and Development platforms!

Modules

DevKits

Modules

DevKits

Modules

DevKits



molex

Visit Molex 

OVERCOMING THE CHALLENGES OF 5G ANTENNA AND CONNECTOR DESIGN

This article looks at the challenges of designing antennas, connectors and associated RF equipment to meet the demands of 5G, including both sub-6GHz and mmWave components.

After discussing the general challenges of signal propagation and signal integrity, it covers the implications of these for both infrastructure cell and user equipment. Finally, it focuses on more detailed design considerations, with some suggested solutions from antenna and RF connectivity specialist Molex.

Over the past few years, the telecommunications industry has shifted from the connected era—with a heavy focus on connected or “smart” devices—to the data era, where the information acquired through connected devices can be used to deliver services to improve lives. The transition from 3G and 4G connectivity to LTE was the first step in enabling a significantly large amount of data to be transferred over the network. Soon, 5G connectivity will boost data processing rates even more and open a world in which data can be used in the workplace, cities and home life.

However, these unprecedented data rates inevitably mean high radio frequencies – and handling these high frequencies is creating design challenges, not just for the antennas, but also for the associated electronic equipment distributed throughout the 5G network infrastructure.

The high frequency RF conundrum

On a top-down basis, the industry is currently moving forward with a compromise on wavelength and frequency; the Non-Standalone (NSA) New Radio (NR) air interface continues to support 3G and 4G as well as 5G at sub-6GHz frequencies. However, the long-term goal for 5G communications is to use a combination of sub-6GHz and millimetre wavelength (mmWave) frequency spectra between, approximately 24GHz – 100GHz. The fundamental conundrum for radio designers is that as frequency rises, wavelengths shorten. This poses challenges, especially for antenna design.

One obvious consequence is that mobile carriers need more base stations, closer to their end users. But even with plenty of base stations, signal propagation can be a problem. mmWave frequencies travel only short distances – say a few hundred meters or a kilometre at best – before they attenuate due to absorption loss associated with atmosphere, weather conditions, building materials and foliage, and other obstacles. The human body can also contribute to losses.

Accordingly, 5G deployments involve trade-offs. Higher mmWave frequencies support increased data throughput, but signal propagation becomes vulnerable. Phenomena encountered by engineers include: multipath (communications break-up); path loss; and packet loss. As a result, there is an urgent need for a proliferating variety of new base-stations and small cells – including femto, macro, nano, and pico cells.

The essential core component of these base-stations and cells is an antenna array, comprising multiple antennas, for both reception and transmission. This technique, which is not new, is known as MIMO (Multiple Input, Multiple Output).

MIMO is a response to how a signal breaks up into multiple paths, typically when it enters a building and tries to navigate through doors, windows, elevator shafts and other obstacles, creating signal reflections in the process. MIMO solves this multipath issue by using multiple antennas to maintain coherent data transmission. On a large scale, this is called “Massive MIMO”. Molex expects sub-6GHz communications to utilize 4 x 4 MIMO, and mmWave 5G to use 2 x 2 MIMO.

Traditionally, radio waves propagate rather like a stone dropped into water. If the antenna is the stone, by analogy, normally the radio waves will spread out as ripples in a circular fashion.

In the case of mmWave 5G, though, the higher frequencies introduce a high degree of directionality to RF propagation. Accordingly, antenna design becomes all-important to benefit from this near ‘line-of-sight’ propagation whenever possible. MIMO, in fact, when applied in really clever antenna designs, can not only mitigate multipath, but also possibly use “massive MIMO” techniques for ‘beam forming’ and ‘beam steering’, turning directionality to the advantage of the user – see Fig.1.

Beam forming allows signal propagation in very narrow paths; beam steering techniques ensure that mmWave signals can find a low-attenuation path towards the desired User Equipment (UE) location. Additionally, beam tracking is used to shift these directed beams as user equipment like mobile phones change positions as users move.

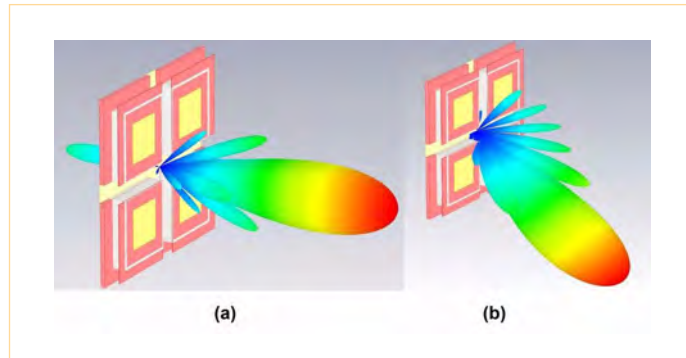


Figure 2: Molex 5G mmWave RF Flex-to-Board Connectors

Signal integrity and interference

While excellent antenna design is critical, as shown above, there are many further challenges; when dealing with weak signals, every fraction of a dB counts. The feeds, traces, and connections that go into the antenna must all be designed with high end-to-end signal integrity (SI) in mind. Molex 5G mmWave RF Flex-to-Board connectors are one example of the type of components needed – See Fig.2. They offer excellent signal integrity performance for high-speed, extreme RF applications, along with the robust mating features and PCB real-estate space savings needed in compact 5G mobile and other communication devices.



Fig.3: Molex combo antennas

Implications across the 5G network – for cells and user devices

Designing 5G networks has implications for both the cells and the user devices:

Cell sites: In addition to the increase in data and speeds anticipated by 5G, small cell sites are being designed to use even less power than the current 4G infrastructure does. 5G cell sites are expected to reduce the amount of always-on signal transmissions common in lower-frequency connections. This will allow 5G cells to switch to “sleep mode,” potentially reducing energy consumption by up to 10 times compared with current idle systems.

Additionally, 5G devices are typically packed with many other RF technologies including Wi-Fi, Bluetooth, UWB, and NFC. Any leakage from the mmWave system can potentially affect the other frequency bands. Given that higher-frequency signals are inherently more prone to leakage, this risk should not be underestimated.

However, component solutions are available to mitigate the design effort and space constraints involved with accommodating multiple technologies. For example, Fig. 3 shows some Molex combo antennas, which offer expanded frequency ranges to handle a combination of multiple wireless communication protocols, while also delivering long-range connectivity, high-power efficiency, a compact form factor and easy integration. Combo GPS/Cellular and Combo Wi-Fi/GNSS antennas are available.

Similarly, the use of multiple input, multiple output (MIMO) architecture – which allows 5G carriers to precisely point the signal from the cell site to the intended receiver – results in an optimal signal for the receiver (rather than transmission at high power in all directions). As a result, less energy is transmitted for each receiver, and the cell site can transmit to other receivers in various directions at the same frequencies, allowing for unprecedented flexibility.

User devices: The evolution in network infrastructure is just one side of the 5G deployment. Device manufacturers must prepare now to leverage the benefits of 5G by defining optimal RF device designs, regardless of the network structure. As with the cell sites, these designs will have to implement a completely different – and more complex – approach.

Since it involves a higher frequency, mmWave deployment requires chipsets for mobile devices to include all the key RF components on the same integrated circuit, including antennas. On the interconnect side, tolerances on mmWave connectors must be precisely tuned.

Device manufacturers will have to decide what parts of the 5G network they want each device to use. Existing RF electronics and antennas will suffice for simple, low-bandwidth devices, such as many IoT products. However, high-performance smartphones and 5G access routers will be best supported by using existing lower frequencies (sub-6 GHz) or optimized RF electronics for mmWave (>30 GHz) and additional mmWave antennas.

More detailed design considerations

Antenna placement and tailored design optimise the radiation patterns of mobile devices: The quality of RF performance with 5G antennas placed on or near the printed circuit board depends on how well the antenna is integrated into the product. However, at 5G’s relatively lower frequency sub-6 GHz bands, antenna placement is only part of the performance equation. There is a strong relationship between the antenna and the mobile device’s internal configuration in determining the overall resonance performance of that device’s wireless communications. Given user preference for thin mobile devices, antenna engineers have needed to consider the physical design, material selections, and internal component configurations when tuning the antenna design.

At mmWave frequencies, though, the interaction between the antenna and the phone body is of less concern. Instead, the challenge is that the covering over the antenna, be it metal, glass, or even plastic is no longer electrically thin and can have negative impacts on the radiating performance of the underlying antenna. Also, the placement of the antenna with respect to the device user’s hand will influence mmWave transmission and reception.

Here design engineers are looking at how to couple tailored antenna design and unique antenna placement along with slot-based design or frequency selective surface design principles which can be employed successfully to optimise the radiation patterns of mobile devices antennas. Additionally, the use of multiple antennas on a user device is required to overcome beam propagation loss in non-ideal directions.

Antenna-tuning techniques improve transmitted power efficiency and, therefore, battery life: Device manufacturers have increasingly turned to the skills and experience of radio frequency engineers, seeking out best RF design practices for optimally tuning the antenna to each device to enhance wireless performance. Antenna-tuning techniques include aperture tuning – where the electrical length of the antenna is calibrated to match its resonance more closely to the required frequency band, and impedance tuning – where the impedance of the antenna is correlated with the RF frontend.

Both techniques can improve gain over a wider bandwidth and improve battery life, as a tuned antenna draws less current than an untuned antenna to deliver the same amount of transmitted power. This is a crucial factor when it comes to meeting consumer expectations around the performance of next-generation 5G mobile phones.

Highly designed connectors protect against unwanted signals, maintain signal integrity and shield against Electromagnetic Interference (EMI): High frequency 5G signals also introduce further considerations around interconnections, board traces, cable assemblies, and connectors. Sending millions of bits across a series of components at speeds dictated by 5G standards inside consumer-grade products presents significant challenges.

Connectors must be carefully designed and manufactured to minimise any impedance variations along the transmission line. External signals can also pose a threat. Therefore, connectors must sufficiently protect the system from electromagnetic interference and capacitive pickup, which becomes increasingly difficult at higher speeds.

5G connectors must also fit into the tiny spaces afforded by modern mobile devices. Stacked connectors allow for densely populated flexible and rigid circuit boards – see Fig.4. Despite the stringent physical constraints, 5G electronics must still meet demanding requirements for scattering parameters, such as voltage standing wave ratio and insertion loss. Well-designed connectors can minimize reflections, degradation, and distortion of the signal while reducing physical footprint, and can be adequately shielded to effectively cut down on EMI.



Fig. 4: Molex SlimStack Board-to-Board Connectors, 0.635mm Pitch, floating series, feature a best-in-class floating connector range with various circuit sizes and stacking heights while offering space savings, design flexibility and a simplified assembly process

Transmission line effects: In addition to managing the challenges of the air interface and associated antennas, extremely high-frequency 5G signals also introduce further challenges for monolithic microwave integrated circuits (MMICs), chip-to-package interconnections, board traces, cable assemblies and connectors. Propagation of signals at gigahertz frequencies causes cables and traces to behave as transmission lines rather than simple wires. The current and voltage vary in magnitude and phase over the length of a transmission line.

Transmission lines can introduce difficult-to-troubleshoot errors if not handled correctly during design. If trace lengths are longer than one-fourth of the signal wavelength, the transmission-line effects must be considered during design. Additionally, at those lengths, there are antenna effects that could have impacts, such as electromagnetic interference and crosstalk; designers must also allow for these.

Connectors can also introduce challenges to achieving an effective and efficient mmWave-based system. Component designers must contend with requirements that constrain the geometry, size and material selection of connectors while still having to match the characteristic impedance of the entire transmission line.

Impedance matching is crucial to reducing signal reflection and achieving maximum power transfer. This, in turn, maximises the amount of energy radiated by the antenna to generate the strongest wireless signal possible for the receivers.

In such situations, inserting devices into a transmission line can cause insertion loss, which means a loss of signal power. If the power transmitted to the load before insertion is P_T and the power received by the load after insertion is P_R , then the insertion loss in decibels is given by

$$IL(dB) = 10 \log_{10} P_T / P_R$$

It is very challenging to meet required specifications such as those pertaining to insertion loss, return loss, power, IMD (passive intermodulation) and temperature stability in a small isolator and circulator package.

However, by combining their experience with their patented technologies, Molex can provide isolators and circulators as small as 6mm while meeting customer requirements, in high production volumes – See Fig.5.



Fig. 5: Molex isolator/circulator

Power handling is very dependent on the circulator's mechanical design and ferrite material properties. Using high power increases temperature and, therefore, degrades performance. Molex engineers select raw materials with appropriate properties, including the required operating temperature range.

Low IMD is very important in systems and is not easily achieved in smaller devices. It usually requires larger isolators and circulators and thicker dimensions. Proper design through applying Molex expertise, along with optimised materials and dimensions selection, results in acceptable IMD and harmonics performance with frequency bandwidth suitable for meeting customer expectations.

5G connectors must also be able to handle significantly higher power than previous generations (15A+ instantaneous current draw is possible in certain situations). Molex PowerWize high-voltage, high-current wire-to-board/wire-to-busbar connectors – see Fig.6 – are offered in two sizes, 6.00 mm and 8.00 mm, suitable for applications requiring up to 1,000 V and 190 A. Additionally, the headers can be mounted on either printed circuit boards or busbars.



Fig. 6: Molex PowerWize high-voltage, high-current connectors

Conclusion

The challenge for design engineers is to create new 5G products which are suitable for mass production while meeting customer expectations. This means selecting the most appropriate 5G components and correctly incorporating them into highly sensitive environments, while also ensuring accurate testing.

Molex is highly invested in 5G research and development, providing a broad range of optical, copper, RF connectivity, antenna, networking, testing, and computing solutions. Through investment in state-of-the-art manufacturing equipment and new higher frequency RF test chambers, Molex enables the development of cost-effective, best-in-class products that help their customers bring 5G ideas and technology to market, faster.

Explore more about Molex Wireless Infrastructure Solutions & Technology

[Click here](#) 



High-Speed Solutions

Fast and reliable connectivity solutions for 5G, data center, and beyond.

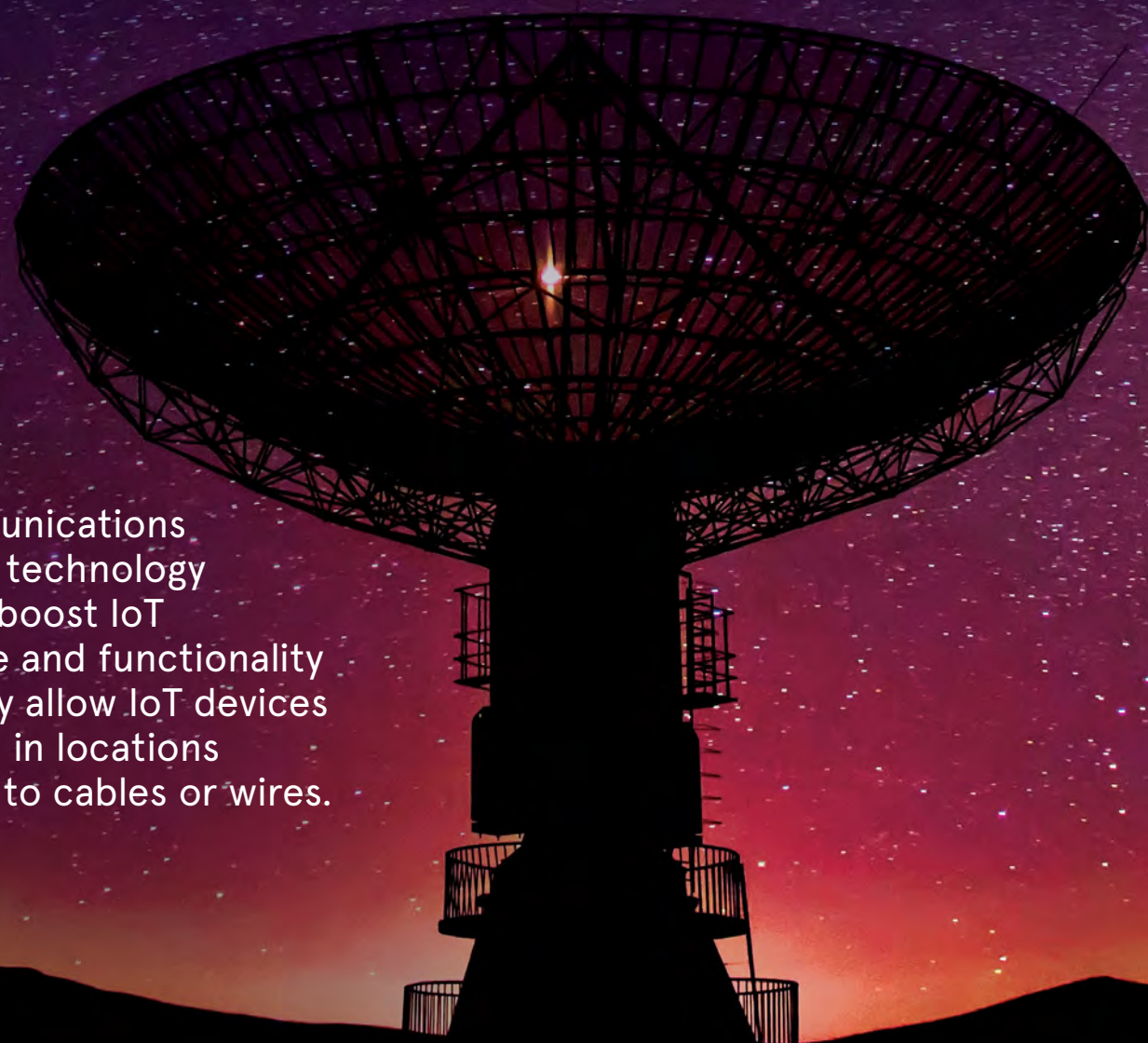
[Click here](#) 

HOW TO ADD THE RIGHT RADIO COMMUNICATIONS SOLUTION TO YOUR PRODUCT DESIGN



Visit Würth Elektronik [↗](#)

Radio communications and wireless technology significantly boost IoT performance and functionality because they allow IoT devices to be placed in locations inaccessible to cables or wires.



This is critical for mobile applications from smart watches and phones, through warehouse robots, to vehicles of all types, but it equally allows IoT solutions for a wider range of fixed applications, including remote monitoring and control systems.

However, adding wireless connectivity to an OEM product is not straightforward, because there are so many factors involved. Although the situation can be mitigated by buying in ready-to-use radio modules and antennas, decisions must still be made about the radio technology to be used, and assembling a matched configuration of modules, antennas, software and firmware – as well as on choosing the supplier that can best integrate all these components into an efficient, reliable, and adequately certified solution.

This article shows how Würth Elektronik has developed an ecosphere of radio modules with support products and services, which allows engineers to rapidly add radio capability to their products, or change to a different radio protocol, using a simple plug 'n' play approach.

We start with a brief overview of radio communications fundamentals, and then of practical considerations, including modular approach advantages, range estimation, and meeting global certification requirements.

Then we review some of the most popular radio protocols, and the Würth Elektronik radio module solutions available for each.

Fundamentals of radio communication

There are five main key facts for consideration:

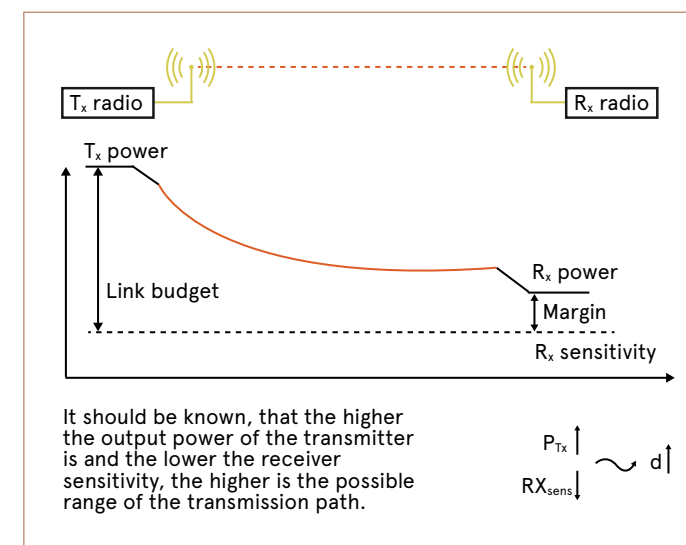
1. Signal Transmission
2. Link Budget
3. Duty Cycle
4. Access
5. Integration of Radio Technology

1. Signal transmission

For transmission, the signal modulates either the amplitude or the frequency of a (mostly) sinusoidal, constant amplitude carrier wave. The modulated wave is radiated by an antenna and detected by a receiving antenna. The signal can be extracted by demodulation in the receiver.

2. Link budget

A link budget is an account of all of the power gains and losses that a communication signal experiences in a telecommunication system; from a transmitter, through a medium (free space, cable, waveguide, fibre, etc.) to the receiver. It is an equation giving the received power from the transmitter power, after the attenuation of the transmitted signal due to propagation, as well as the antenna gains and feedline and other losses and amplifications of the signal in the receiver or any repeaters it passes through.



Power [dBm]	Power [watt]
- 120 dBm	1 fW
- 110 dBm	0.01 pW
- 100 dBm	0.1 pW
- 90 dBm	1 pW
-80 dBm	10 pW
-70 dBm	100 pW
-60 dBm	1 nW
- 50 dBm	10nW
- 40 dBm	100 nW
- 30 dBm	1 μW
- 20 dBm	10 μW
- 10 dBm	100 μW
- 1 dBm	794 μW
0 dBm	1 mW
1 dBm	1.26 mW
10 dBm	10 mW
20 dBm	100 mW
30 dBm	1 W
40 dBm	10 W

Fig.1: Link budget illustration

3. Duty cycle

A duty cycle or power cycle is the fraction of one period in which a signal or system is active. Duty cycle is commonly expressed as a percentage or ratio.

4. Polite Spectrum Access – listen before talk

When an application uses polite spectrum access, the duty cycle restrictions are relaxed. Polite spectrum access encompasses two aspects: Listen Before Talk (LBT) and Adaptive Frequency Agility (AFA).

5. Integration of Radio Technology

Certification is one of the last steps before a product with integrated wireless technology can be launched on the market. Manufacturers of products with integrated RF-technology may only market these with the necessary certification. Fig.2 shows the three options available for integrating wireless technology.

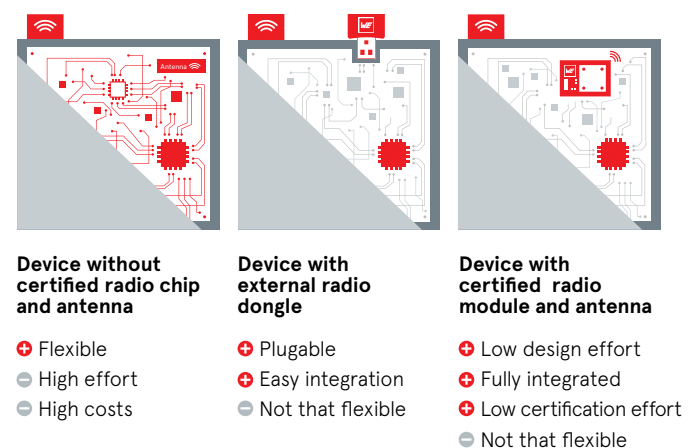


Fig.2: Three options for integrating wireless technology

Practical solutions for adding radio capability to an OEM product

Figure 2 shows the three options available for integrating wireless technology into an OEM product. We now look at some practical considerations for achieving technically and commercially successful integration, including:

- **Why using a radio module is the best approach**
- **How to estimate range**
- **Certification and conformity considerations**

Why use a radio module?

To fully appreciate the advantages of using Würth Elektronik modules, it is important to understand that they comprise complete hardware, firmware and software solutions.

The ready-to-use hardware modules are based on powerful RF-chips and support for integrated or external antenna. The firmware comprises the WE-ProWare Radio Stack (described later) and conformity certifications for Europe, North America, Japan and, in some cases, China.

The software element includes Plug & Play PC-Software for easy evaluation, testing and updating, and mobile apps for easy evaluation and testing. Design libraries are available for fast Altium and Eagle PCB design. A Software Development Kit (C-Files) is provided for comfortable coding of the HOST-controller system.

The availability of these components as an integrated solution will have a significant impact on reducing development and certification cost, time, risk, resource and expertise requirements. Above all, the radio modules allow users to bring their products to market months earlier than would otherwise be possible – or switch rapidly to a different radio protocol on demand.

Range estimation

Engineers who have elected to base their designs on radio modules can use Würth Elektronik eiSos's free Range Estimator, available at www.we-online.com/redexpert. With this tool, modules can be sorted and selected by their attributes. While simplified equations only yield approximate results, experience shows that these results provide reliable estimates of transmission range, if applied correctly.

Below is a path loss calculation that estimates the range of a radio link in a free space environment, using the Friis Transmission for Free Space model. A two-ray ground reflection model is also available.

This model assumes that the emitted power is radiated equally in every direction (isotropic) and calculates the power loss only allowing for the decreasing power density of the wavefront with increasing distance to the origin, without any reflection, absorption or attenuation.

Range calculation using Friis transmission for free space model

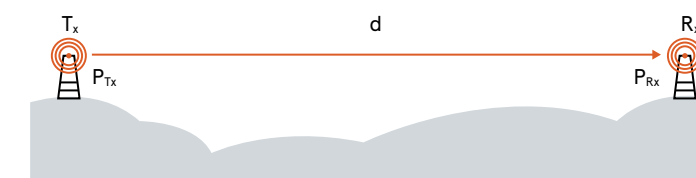


Fig.3: Free space model

Character	Description	Unit
λ	wavelength of the signal	[m]
2RPL	path losses of the 2-ray ground reflection model	[dB]
C	speed of light in vacuum (299 792 458)	[m/s]
d	distance from transmitter to receiver	[m]
f	frequency of the signal	[m]
hT	height of the transmitter antenna over ground	[m]
hRx	height of the receiver antenna over ground	[m]
FSPL	path losses of the free space model	[dB]
LM	link margin (safety to ensure a received signal)	[dB]
PTx	total power emitted by the transmitting antenna	[W] or [dBm]
PRx	total power received by the receiving antenna	[W] or [dBm]
Rx sens	sensitivity of the receiving RF module	[dB]

$$P_{Rx} = \left(\frac{\lambda}{4\pi d}\right)^2 * P_{Tx}$$

this leads to the space path loss

$$FSPL = \frac{P_{Tx}}{P_{Rx}} = \left(\frac{4\pi d}{\lambda}\right)^2 = \left(\frac{4\pi df}{c}\right)^2$$

expressed in decibel this means,

$$FSPL [dB] = 10 \log_{10}\left(\frac{4\pi df}{c}\right)^2$$

$$FSPL [dB] = 20 \log_{10}\left(\frac{4\pi df}{c}\right)$$

$$FSPL [dB] = 20 \log_{10}\left(\frac{4\pi}{c}\right) + 20\log_{10}(d) + 20\log_{10}(f)$$

To determine the maximum range of a Würth Elektronik eiSos RF-module, the path losses of the transmission are equalled to the ratio of the received power to the emitted power:

$$FSPL[dB] = \frac{P_{Tx}}{P_{Rx}} = P_{Tx}[dBm] - P_{Rx}[dBm]$$

$$20 \log_{10}\left(\frac{4\pi}{c}\right) + 20\log_{10}(d) + 20\log_{10}(f) = P_{Tx}[dBm] - P_{Rx}[dBm] - L_M[dB]$$

$$d=10^{\frac{P_{Tx}[dBm] - P_{Rx}[dBm] - L_M[dB] - 20\log_{10}\left(\frac{4\pi}{c}\right) - 20\log_{10}(f)}{20}}$$

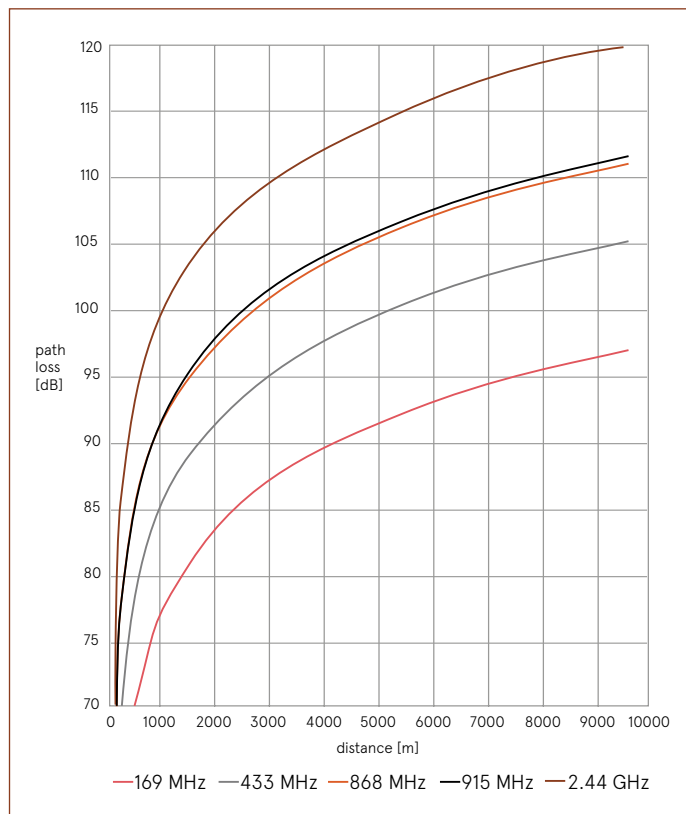


Fig.4: Path losses for different frequencies

Certification and conformity

A product that is to be launched globally must meet the certification or conformity criteria of each country where it is marketed. This is to prove that the product complies with regulations, laws, norms, standards, and other requirements. There is no worldwide certification applicable to all countries.

For example, the CE mark is required in Europe, and FCC certification in North America.

All Würth Elektronik radio modules are either certified and/or declared for conformity. This simplifies their approval process within the end-application significantly.

Radio technologies

A large number of radio technologies and protocols are available for a wide range of applications. Below, we look at some of the most popular:

Cellular

LTE (Long Term Evolution) is a cellular communication standard, which operates in licensed spectrum. LTE is also referred to as fourth generation ("4G") cellular communication technology. The standards for LTE are defined by 3rd Generation Partnership Project (3GPP). 3GPP is a worldwide standards organisation that develops protocols/standards for cellular telecommunications.

LPWAN cellular technologies are for low-power, low transmitting speeds, low-cost module and devices with low data usage per month, and wide area coverage. Existing cellular technologies were not designed to handle low power applications, hence cellular LPWAN technologies cover scenarios where existing mobile network technology is not suitable.

These cellular LPWANs refer to low power wide area networks (LPWAN) in licensed spectra. 3GPP specified LTE-M (LTE-MTC) and NB-IoT (Narrow-Band IoT) to address the fast-expanding market for low power wide area network (LPWAN) connectivity.

Multiple IoT connectivity options are available, which can be broadly categorised into two types:

- **Short range wireless connectivity solutions in unlicensed spectrum**
- **Long range wireless connectivity solutions in licensed spectrum**

Würth Elektronik solution: Cellular module

The Adastrea-I is a dual-mode LTE-M/NB-IoT cellular module, which supports international multi-regional coverage. The module will select NB-IoT where LTE-M coverage is not available, and vice versa.

Fig.5 shows the module's key features.

Adrastea-I
LTE-M / NB-IoT Cellular Module

Characteristics

	Small form factor		Security & encryption
	Long range / worldwide coverage		Multi-band support

Fig.5: Adrastea-I LTE-M/NB-IoT cellular module

An integrated ARM Cortex-M4 MCU is provided exclusively for customer application firmware; this reduces cost, size, and power consumption. The integrated MCU also enables positioning, through GPS and GLONASS satellite systems. This allows GNSS positioning for asset management applications where infrequent position updates are required.

Bluetooth

Bluetooth Classic was released in 1998; from Release 4.0 in 2010, Bluetooth Low Energy (BLE) was added. Key differences between Classic and BLE include:

- Classic Bluetooth operates on 79 frequency channels, whereas BLE uses only 40.
- Classic Bluetooth has a higher throughput and can send larger data files than BLE, but it also consumes more energy.
- Classic Bluetooth can only connect to seven other devices, while BLE has no theoretical limit.
- BLE stays in sleep mode until users initiate a connection, and hops between frequencies at a different rate, helping save more power.


Industrial and IoT applications need easy connections between field devices and mobile phones or tablets. As the field devices do not need displays, significant cost savings are possible. Typical BLE applications include door control, service interface, light, roller shutter, and heart rate monitor.

Bluetooth Mesh was released in 2017.

Würth Elektronik offers their Proteus modules for Bluetooth 5.1; the Proteus-e Slim-version and their fastest, Proteus-III/ Proteus-III SPI.

**OUR SLIM-VERSION:
BLUETOOTH® LOW ENERGY 5.1**

Proteus-e
Bluetooth® LE 5.1 Module




Characteristics

- Security & encryption
- Miniaturized design
- Cost effective
- Smart antenna selection

Fig. 6: Proteus-e slim-version BLE 5.1 module

**OUR FASTEST:
BLUETOOTH® LOW ENERGY 5.1**

Proteus-III / Proteus-III SPI
Bluetooth® Low Energy 5.1
Standard with 2 MBit PHY and
Coded PHY (long range)



Characteristics

- Security & encryption
- High throughput
- Long range / worldwide coverage
- Smart antenna selection

Fig.7: Proteus-III/ Proteus-III SPI BLE 5.1 module

Wi-Fi


Wi-Fi (wireless fidelity) is a specification for ensuring interoperability, based on the IEEE 802.11 family of standards, which are commonly used for local area device networking and Internet access. Wi-Fi's wavebands have relatively high absorption and work best in line-of-sight use. Many common obstructions such as walls, pillars, home appliances, etc. may greatly reduce range, but this also helps minimise interference between different networks in crowded environments. An access point (or hotspot) often has a range of about 20 metres indoors while some modern access points claim up to a 150-metre range outdoors.

Wi-Fi networks can operate in two modes. In the infrastructure mode, an access point acts as a central entity serving several connected clients. To connect to such a Wi-Fi network, a user typically needs the network name (the SSID) and a password. The password is used to encrypt Wi-Fi packets to block eavesdroppers. The Wi-Fi direct mode offers a point-to-point connection without the need for a dedicated central entity.

Würth Elektronik offers their Calypso fully-featured standalone Wi-Fi IEEE 802.11 b/g/n 2.4 GHz module as shown in Fig. 8.

**OUR NETWORKER:
WI-FI 2.4 GHZ**

Calypso
Fully featured
standalone Wi-Fi
module IEEE 802.11
b/g/n, 2.4 GHz



Characteristics

- Security & encryption
- Global availability 2.4 GHz licence free band
- Smart antenna selection

Fig.8: Calypso IEEE 802.11 b/g/n 2.4GHz Wi-Fi module

The module provides a good basis for secure end applications, with secure boot and secure storage for user data. Other features include low power operation, smart antenna selection, firmware over the air update (FOTA) and provisioning.

Connectivity possibilities include HTTP, Multicast DNS, SSL and TL51.2 support, and MQTT client on module.

Proprietary radio as BLE alternative

There are several advantages to using Proprietary Radio as a BLE alternative:

- Connection only with manufacturer-authorized devices
- Security aspect as a benefit for end customers
- Closed communication is "invisible" for Smart devices
- Higher throughput possible – no effort with large Bluetooth overhead
- Saving Bluetooth Listing costs
- Business model to build the whole chain as user experience
- Binding the end customer to the product with additional accessories using the same communications

All Wireless Connectivity RF Modules have the WE-ProWare radio stack pre-loaded: Würth Elektronik modules' added value is the fully-included WE-ProWare operating system. Communication functions are configured with simple AT commands. Designers can easily swap between radio channels and protocols to simplify new market entry.

WE-ProWare can connect to external peripherals using numerous interfaces, such as UART or digital and analogue I/O. Network topologies it supports include:

- Point to Point
- Point to Multipoint
- Peer to Peer
- Mesh
- Multi-hop

Würth Elektronik's strongest proprietary 868 MHz modules are the Tarvos-III and Thebe-II, as shown in Fig. 9.

**OUR STRONGEST:
PROPRIETARY 868 MHZ**




<p>Tarvos-III Long range radio module 868 MHz</p> 	<p>Thebe-II Long range radio module 868 MHz</p> 
<p>Characteristics</p> <ul style="list-style-type: none"> Long range 10 / 20 km Small size Mesh High penetration 	

Fig.9: Tarvos-III and Thebe-II proprietary 868 MHz modules

**OUR SMALLEST:
PROPRIETARY 2.4 GHZ**

Thyone-I
Proprietary radio
module 2.4 GHz



Characteristics

- Long life battery driven application with sleep current = 0.4 µA
- Global availability 2.4 GHz licence free band
- Mesh
- Nano SIM size

Fig.10: Thyone-I proprietary 2.4 GHz module

Combined proprietary 2.4 GHz and Bluetooth Low Energy 5.1

The Würth Elektronik Setebos-I combines Bluetooth® Low Energy 5.1 Standard and a Proprietary 2.4 GHz radio module. It contains both the Thyone-I and Proteus-III modules.

OUR COMBINED: PROPRIETARY 2.4 GHZ & BLUETOOTH® LOW ENERGY 5.1

Setebos-I

Bluetooth® Low Energy 5.1 Standard & Proprietary radio module 2.4 GHz



Characteristics

- Security & encryption
- High throughput
- Long range
- Smart antenna selection
- Long life battery driven application with sleep current = 0.4 µA
- Global availability 2.4 GHz licence free band
- Mesh
- Nano SIM size

Fig.11: Setebos-I combined proprietary 2.4 GHz and Bluetooth Low Energy 5.1 module

Mesh

A Mesh is a network of multiple interconnected devices. All nodes interconnect directly with no need of a master controller. In general, there are more connection paths between the source and the target. The information is passed from one node to another. Bluetooth Mesh and Wirepas Mesh are two established protocols.

Bluetooth Mesh: Bluetooth released a Mesh Version in 2017. It is not strictly part of the Bluetooth standard. It uses Bluetooth Low Energy link layer and radio and prefers Bluetooth 5.0 or newer due to long advertising packets. As a flooding Mesh it includes time to live (TTL) in the messages. Security is approved by application key and network key.

Wirepas Mesh is a connectivity protocol for radio modules, optimised for large scale and energy efficient 2.4 GHz wireless mesh networks. This innovative technology can be used to create large IoT networks, for example using battery-powered sensors, in which each node also functions as a router.

An asynchronous flooding mesh is integrated into Würth Elektronik Thyone-I, Tarvos-III, Thebe-II, Thelesto-III, Themisto-I & Setebos-I modules. These are suited for applications using small/medium size mesh networks (much traffic due to flooding technique), or where current consumption does not play a role (always on RX or TX).

Würth Elektronik also offers their Thetis-I 2.4 GHz Radio Module with Wirepas Mesh protocol. The Wirepas Mesh grows organically and has automated interference avoidance, so one network can handle multiple use cases and thousands of assets.

OUR MESHED: WIREPAS 2.4 GHZ

Thetis-I

Radio Module 2.4 GHz with Wirepas Mesh protocol



Characteristics

- Security & encryption
- Mesh
- Long life battery driven application with sleep current = 0.4 µA
- Smart antenna selection

Fig.12: Thetis-I Wirepas Mesh module

Wireless M-Bus

Wireless Meter Bus (wM-Bus) is the extension of the Meter Bus (M-Bus) with a wireless protocol and role scheme for handling communication over a standardised wireless communication interface between meters and data loggers – so called smart meter gateways (SMGW). This scheme is specified by the European standard EN 13757 and its sub-standards. This standard was introduced to allow automated measuring and processing of data, track resource usage, and optimise provisioning to create an “Advanced Metering Infrastructure” (AMI).

The Würth Elektronik Wireless M-Bus Analyzer is a tool for receiving and parsing wireless M-Bus telegrams that comply with EN 13757-4:2013 transmitted by “meter” or “other” devices. It is excellent for analysing errors and M-Bus devices’ RF range. Thanks to the simplified representation and an integrated logging function, data can also be analysed at a later time.

Available modules include Mimas-I, Metis-I, and Metis-II.

Build your own firmware (BYOFw)

With Würth Elektronik’s portfolio of BYOFw modules like Ophelia-I, customers can receive a radio module in a hardware-only version, allowing them to develop and flash their own firmware for the transceiver chipset.

GNSS

GNSS (Global Navigation Satellite System) provides positioning and time synchronisation capabilities to unlimited numbers of users worldwide. The system is based on signals from the following four satellite constellations – see Fig.13.

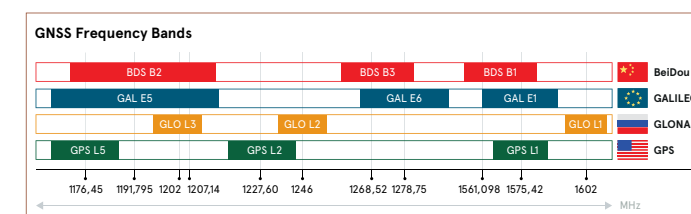




Fig.13: GNSS frequency bands and satellite constellations


Fig. 14 shows Würth Elektronik’s range of GNSS radio modules.




Elara-I



Elara-II




Erinome-I



Erinome-II


Characteristics




Smallest GNSS module (Elara Series)

001101
010100
101101

NMEA + OSP protocol



High update rate



Multi constellation

Fig.14: Choice of GNSS radio modules

Conclusion

Committing today to tomorrow’s wireless technology seems impossible. Würth Elektronik offers freedom to use one radio module footprint for multiple radio modules to expand applications with different radio protocols at any time without any layout changes. It is a single quality-proven hardware base that eliminates enormous future re-design costs today.

Explore more about Würth Elektronik Wireless Connectivity & Sensors

[Click here](#)

SECURING CONNECTED DEVICES: CHALLENGES & SOLUTIONS

In today's technologically advanced world, connected devices have become integral to our daily lives.

Connected devices, also known as Internet of Things (IoT) devices, offer seamless connectivity and automation in anything from smartphones and smart TVs to smart household appliances and industrial machinery.

These devices have sensors, processors, and network connectivity, allowing them to collect and transmit data to perform various functions. The increasing number of linked devices has resulted in various advantages, including enhanced effectiveness, convenience, and productivity. However, ensuring their security has become essential with an increasing number of technologically advanced devices.

Securing connected devices is essential for safeguarding user privacy, protecting key infrastructure, and maintaining consumer and business competence. This article will look at the security challenges connected devices encounter in wireless and wired connectivity networks and effective solutions for mitigating these threats.

Importance of Security in Connected Devices

- **Data Security and Privacy:** Connected devices collect and transmit sensitive personal and organisational data, such as personally identifiable information (PII), financial data, and proprietary business information. Without strong security safeguards in place, this data is vulnerable to unauthorised access, theft, and abuse, resulting in privacy violations and financial losses.

- **Physical Security and Safety:** Connected devices are being incorporated into key infrastructures such as healthcare systems, transportation networks, and industrial control systems. Any security breach in these devices can potentially threaten human lives, interrupt services, or cause substantial physical damage.
- **Reputation and Trust:** Security breaches involving connected devices can have serious ramifications for manufacturers, service providers, and customers. Data breaches, malware infections, and unauthorised access may erode consumer trust and harm a brand's reputation, resulting in financial losses and lower customer engagement.

Security challenges in connected devices

Despite increasing awareness of safety risks, various obstacles remain in connected devices. Understanding these issues is critical for building viable solutions. Here are some examples of common security challenges:

- **Lack of standardisation:** One of the major safety concerns in IoT is a lack of standardisation. Ensuring compatibility and interoperability is difficult. With so many devices, protocols, and platforms. This can result in vulnerabilities that attackers can exploit.

- **Insufficient authentication and authorisation:** Another key issue confronting IoT is the prevalence of weak or insufficient authentication techniques in connected devices. Many devices continue to utilise default credentials or weak passwords, exposing them to unauthorised access. Inadequate authorisation methods exacerbate the situation by enabling unauthorised users access to critical functions.
- **Vulnerabilities in software and firmware:** IoT devices are frequently powered by embedded systems with limited resources, making them challenging to protect. This can result in vulnerabilities that attackers can exploit. Furthermore, embedded systems frequently include specialised hardware and software, which might provide extra issues when it comes to security.
- **Physical security risks:** IoT devices have significant physical security challenges since they are frequently small and simple to conceal, leaving them vulnerable to physical assaults. Tampering, theft, or destruction of an IoT device are examples of physical attacks. This can lead to unauthorised access to sensitive data, system outages, and data loss.

Solutions for security challenges

A multi-layered approach is necessary to handle security challenges in connected devices successfully. Here are some solutions that can significantly enhance the security of connected devices.

Standardisation and regulation

- Developing and implementing industry standards for IoT devices, protocols, and platforms can aid in ensuring compatibility and interoperability. This might include device security standards, data privacy standards, and communication protocols.
- IoT device and platform certification can assist verify that they accomplish certain safety criteria. This may help organisations gain trust in the security of the devices they use, as well as identify devices that may be more vulnerable to attack.
- Using a secure gateway may assist ensure that all network devices communicate securely. A secure gateway, for example, may be used to encrypt communications, authenticate devices, and monitor network traffic for unusual activities. This can help reduce the risk of attacks and improve network security overall.

Strong authentication and authorisation mechanisms

- Implementing strong methods of authentication, such as two-factor authentication, to ensure that only authorised users have access to the device can support.
- Using a secure gateway will ensure that all network devices communicate securely.
- Using Public Key Infrastructure (PKI) can help ensure the authenticity of all network devices. And secure data transfer technologies such as Transport Layer Security (TLS).

Regular software and firmware updates

- Using safe IoT app development practises such as threat modelling and code reviews may assist assure software security. Organisations may assist to lower the risk of attacks and improve the security of their IoT devices by adding these practises into the development process.
- Using secure boot and secure firmware update protocols can assist to ensure that reliable software is running on the device. Secure firmware update techniques may verify that the device is running the most recent firmware version, as well as that any upgrades are genuine and have not been tampered with.

Implementation of physical security measures

- Using secure network protocols such as VPN and HTTPS will help ensure secure information transmission. Virtual Private Networks (VPNs) may be used to encrypt connections between IoT devices and the internet, making data interception more difficult.

HTTPS, on the other hand, may be used to encrypt communications between web servers and clients, adding a further level of protection to web enabled IoT devices.

- Using network segmentation may help reduce the impact of a network assault. To limit the scope of an attack, network segmentation involves separating a network into smaller sub-networks, or segments. An organisation, for example, may segment its network such that all IoT devices are on a distinct segment from the rest of the network.
- Since the attacker can only access the segment retaining the IoT devices rather than the entire network, this will help in limiting the impact of an attack on IoT devices.

Visit uk.farnell.com/it-and-ot-in-industrial-iot-applications to know more about IoT in industrial-connected devices.

Best practices for connected device security

- 1. Password management:** Encouraging users to use strong and unique passwords, as well as changing passwords on a regular basis, is essential. Utilising password managers and enabling two-factor authentication improves device security significantly.
- 2. Network security:** It is critical to maintain strong network security. This includes employing strong encryption methods such as WPA2/WPA3, segmenting networks, implementing firewalls, and monitoring network traffic on a regular basis to detect any irregularities or unauthorised access attempts.
- 3. Encryption:** Implementing end-to-end encryption for data transport and storage ensures that sensitive information remains secure even if intercepted. Both data in transit and data at rest on linked devices should be encrypted.
- 4. Regular auditing and monitoring:** Regular auditing and monitoring operations enable organisations to proactively detect and respond to possible security issues. Analysing device logs, monitoring network traffic, and employing intrusion detection systems all contribute to the continued security of linked devices.

Conclusion

As the number of connected devices diversifies, it becomes increasingly important to prioritise their security. The risks involved with compromised devices can have serious ramifications for people, businesses, and society.

We may mitigate these risks and fully utilise the promise of connected devices by recognising security concerns and developing effective solutions. Manufacturers, developers, and end users must work together to create a secure and resilient ecosystem for connected devices, assuring a safer and more trustworthy digital future.

Farnell has partnered with many different suppliers catering to a wide range of edge device mesh networking components portfolio, such as Internet of Things, IoT Solutions Kits, Wireless Modules & Adaptors, Communications & Networking Modules, Bluetooth Modules & Adaptors, Zigbee Modules / XBee, WLAN Modules & USB Adaptors, Industrial Wireless, RF/Wireless Development Kits, and Networking - Wireless Products.

Explore the widest range of Security solutions for the connected world

[Click here](#) 



OPTIGA embedded security solutions

State-of-the-art answers to today's embedded security challenges with OPTIGA™ Trust.

[Click here](#) 

TECHNICAL RESOURCES CENTRE

Learn innovations,
Stay informed,
Be inspired

A comprehensive selection of products framed into design situations, latest news and trends, design tools and resources to enable you to move from block diagram concept to solution for your vertical segment applications.

[LEARN MORE](#)



Explore our expanding library of:



Whitepapers



Articles



How To's



Webinars



Podcast