WHITE PAPER

MAY 2023

1

Trusted Wireless: Wireless technologies in industrial automation

Created by: I/O & Networks Industrial Electronics Division – Daniel Fenton, Associate Product Manager, Wireless Phoenix Contact USA, dfenton@phoenixcontact.com

Wireless technologies in industrial automation

Year after year, more industrial applications are using wireless technologies. Users benefit from this as wireless solutions offer a higher degree of mobility and flexibility. Reasons to use wireless vary, from reducing the cost of an installation either upfront or in employee time spent recording data, or reducing time to start up an installation.

The frequency bands commonly used in factory and process automation industries are typically the so-called ISM (industrial, scientific, and medical) bands. In North and South America, the popular 900 MHz is used, and globally 2.4 GHz is often used. As these bands do not require licenses, they are frequently utilized by different organizations. As a consequence, many different systems may be operating in the same radio bands within a geographic area, and this means that coexistence, the ability for different radio networks to work in the area, is one of the vital properties of wireless technologies.

Because the 2.4 GHz ISM band is used globally, users deal with heavier congestion than with the 900 MHz band, although there is more bandwidth available in the 2.4 GHz band. However, the conditions for

INSIDE

Wireless technologies in industrial automation 1
Areas of application for Trusted Wireless 2
Rugged communication thanks to FHSS 2
Disturbances of the wireless signal 3
Automatic and manual coexistence mechanisms 4
Secure communication thanks to encryption and authentication 4
Flexible networks with automatic connection management 4
Distributed network maintenance – faster and easier 5
Extensive diagnostic properties 5
Adjustable to the desired application 5
Glossary 6

U003950B

PHOENIX CONTACT • P.O. Box 4100 • Harrisburg, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Website: www.phoenixcontact.com

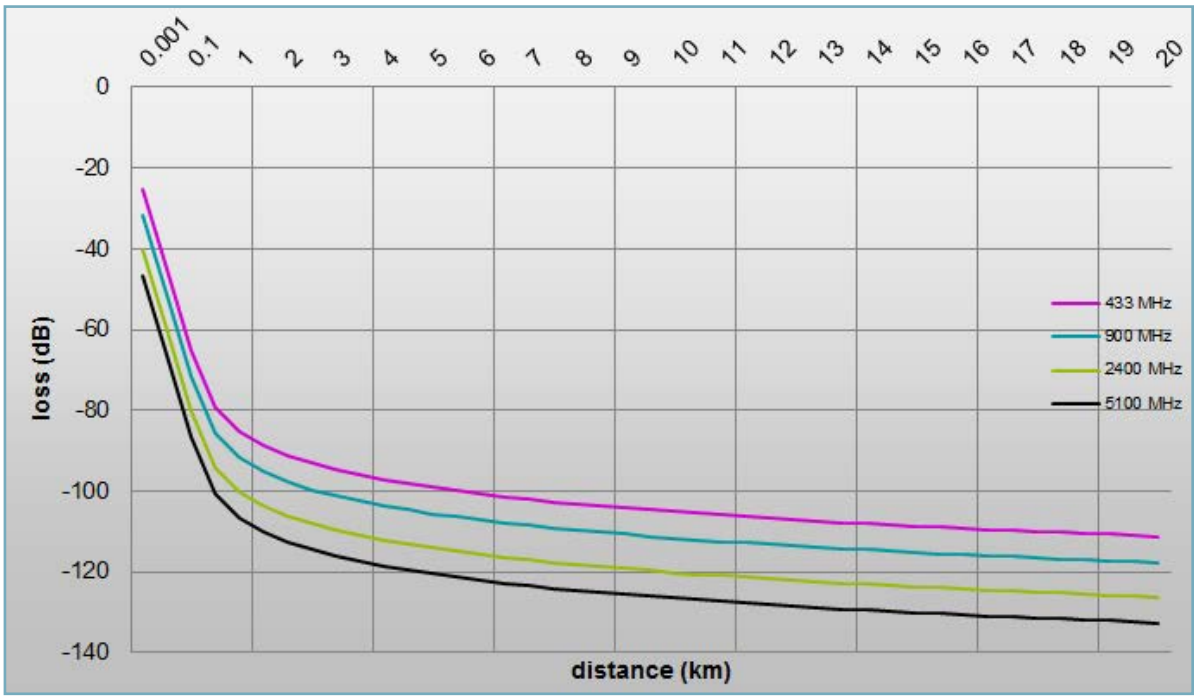

Figure 1: The free space attenuation increases in proportion to the frequency

the attenuation of electromagnetic waves are better in lower frequency ranges (Figure 1). Therefore, higher frequencies will have reduced range. The free space attenuation depends logarithmically on the transmission frequency. This means that if one halves the transmission frequency (e.g., from 868 MHz to 433 MHz), the free space attenuation reduces by 6 dB for the same distance.

With a decrease in free space attenuation of 6 dB, the range will potentially double with the transmission power staying the same. Thus, it is possible to overcome longer ranges with lower frequencies.

Areas of application for Trusted Wireless

Trusted Wireless, a wireless technology developed especially for industrial use and the technology that is used in the Radioline platform, is particularly suited for the transmission of analog and digital I/O without wires or for the transmission of small or medium data amounts – even over large distances from a few hundred meters to several kilometers/miles.

The main features of Trusted Wireless include:

- Rugged communication with Frequency Hopping Spread Spectrum add (FHSS)
- Secure communication using 128-bit AES encryption and authentication
- Long range due to high receiver sensitivity, variable data transmission rates, and high transmission power (100 mW for 2.4 GHz, 1 W for 900 MHz)
- Flexible network structures: point-to-point, star, repeater
- Extensive diagnostic features

Rugged communication thanks to FHSS

Every user wants a reliable and rugged communication connection for their application. However, the concepts of "reliable" and "rugged" are inherently subjective. Usually, these are expressions of perceived latency, determinism, data throughput, and the tendency of a network to lose connectivity in a given setting. All of these are important and need to be taken into account.

Two major factors can influence the perceived reliability of a wireless connection: first, the disturbance of the wireless signal by other electromagnetic waves, triggered by other wireless systems or unwanted emissions of other electric devices (EMC disturbances); secondly, "fading," which occurs because of free space attenuation, but most especially by reflections.

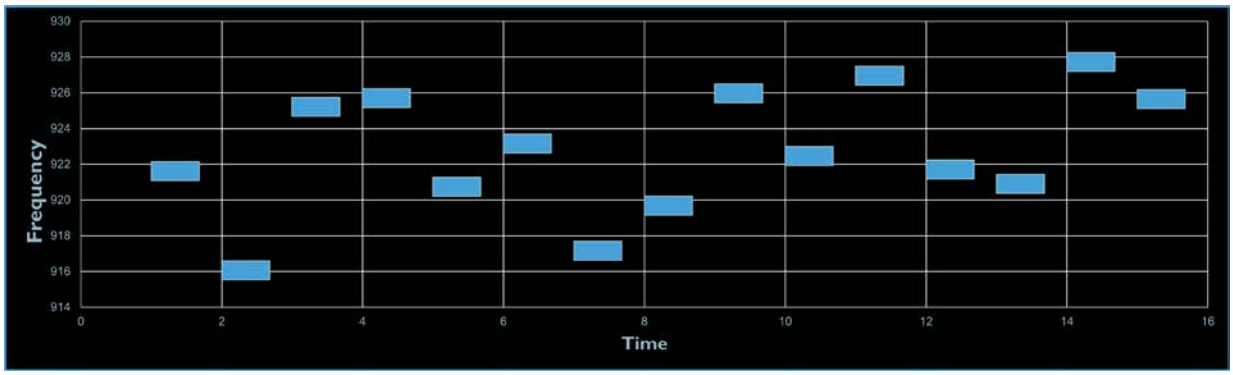

Figure 2: Frequency hopping moves in a pattern across a range of frequencies to avoid interference in communication.

Higher receiver sensitivity and adjustable data rates for increased range

For industrial wireless applications, the range plays a vital role, especially for outdoor applications. Four key aspects of a radio system determine range, and users can easily find them on any data sheet: the operating frequency, as discussed previously, the transmitter power output, the receiver sensitivity, and the RF data rate.

A regulating authority, such as the FCC, limits the transmitter output power, and in practice, companies find it relatively simple to design an RF transmitter that meets the regulatory requirements. A radio device may have a transmitter power level lower than the maximum allowable level for a purpose, such as packaging and heating restrictions.

Conversely, it is much more difficult to design a high-quality RF receiver. The defining specification of a receiver is sensitivity, which is a measure of the smallest (lowest) signal that the receiver can "hear" and understand.

A more sensitive receiver can detect a lower signal, which results in longer range. Designing a good receiver requires careful selection of components such as a low noise amplifier or "preamplifier" to boost the incoming signal, as well as good filters to eliminate undesired interference.

Receiver sensitivity can be further increased by reducing the data rate. If a transmission uses a low data rate, every bit transmits with the transmission power P for a longer time than at a high data rate.

A higher energy per bit results in a higher system gain. This shows in the increased receiver sensitivity. A four-times-lower data rate results in a system gain of about 6 dBm, which effectively doubles the range of a radio link.

Trusted Wireless offers different, adjustable data rates. Thus, depending on the application requirements, the range can be many times longer than the ranges of common Bluetooth and WLAN systems.

A reliable wireless connection should also always operate with a minimum system reserve or fade margin of 10-15 dB.

With Trusted Wireless technology, wireless links stretching over several miles/kilometers are possible, depending on the data rate and antenna installation used. When using the 2.4 GHz system, Phoenix Contact recommends its use for applications less than 1 km and using the 900 MHz system for longer links.

Disturbances of the wireless signal

Disturbance caused by other wireless systems or EMC disturbances

In the 900 MHz and 2.4 GHz bands, wireless systems benefit from the fact that EMC disturbances caused by general industrial applications do not reach this high-frequency range. Frequency converters, ballasts, and other EMC-producing devices, which usually pose a problem, do not disturb the GHz band. Their energy transmissions play a role for frequencies in the kHz and MHz area.

In the 2.4 GHz and 900 MHz spectrum, disturbances are typically related to other wireless system coexisting in the same spectrum. Two completely different approaches help to deal with this problem: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). Since Trusted Wireless utilizes FHSS, this paper will focus on that approach.

With FHSS, many different individual frequencies or channels are utilized in a pseudo-random pattern. This way,

PHOENIX CONTACT • P.O. Box 4100 • Harrisburg, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Website: www.phoenixcontact.com

an interference signal only blocks one or a few neighboring individual frequencies, so at least some portion of the communication continues.

If disturbances worsen, only the data throughput is reduced in the FHSS system. This is an important advantage over DSSS, as the same issue results in communication being completely blocked.

The number of frequencies used within the pseudo-random hopping pattern depends on further settings and mechanisms such as the exclusion of certain frequency ranges (blocklisting) for the coexistence management, or the use of several frequency groups (RF bands) to optimize the parallel operation.

Disturbance of the wireless signal caused by fading. Fading means that the signal weakens due to different external influences. Reflections occurring during the propagation of the radio wave factor into signal fading.

The Trusted Wireless technology uses many individual transmission channels within both the 900 MHz (26 MHz of bandwidth) and 2.4 GHz (83 MHz of bandwidth) ISM bands. Thus, the extensive change in wavelength significantly improves the signal and enhances the possibility of a reliable transmission on that particular channel. In other words: if the transmission cannot happen on one channel, the signal strength on the next channel allows for easy reception.

Automatic and manual coexistence mechanisms

For many industrial applications, planning of the wireless systems is recommended before deployment.

If a 2.4 GHz Trusted Wireless system is co-located with a WLAN network, the user should blocklist the frequency ranges of the WLAN channel. Similarly, in the 900 MHz band, if interference is detected during the planning phase, a 900 MHz Trusted Wireless system should blacklist those frequencies. With the proliferation of wireless in industrial applications, users have discovered an increasing importance in carefully planning the frequency band used for the different systems and ensuring the technology allows the blacklisting of frequency ranges.

Trusted Wireless has the ability to blacklist frequency ranges and therefore allows planning the coexistence with other systems. For this, the system recalculates frequency hopping patterns according to the blacklisted areas.

Secure communication thanks to encryption and authentication

Security plays an important role in the wireless transmission technology. As information propagates through the unprotected air, security strategies have to prevent unauthorized access.

Trusted Wireless has two real security mechanisms: the encryption of all transmitted information according to the Advanced Encryption Standard (AES,) as well as an authentication of the data in accordance with RFC 3610.

AES Encryption makes sure that hackers cannot extract the content of theoretically captured data packets. A designated password (pre-shared key) generates the 128-bit key, and all network devices must recognize this password.

The importance of the authentication of transmitted data packets rates as highly as encryption. The simplest method of attacking a wireless system: listen to a message, change it and feed it back into the network. Therefore, the source of the message must come from a guaranteed source, such as an authenticated transmitter. For this, the messages have a continuous code, which must not repeat. The code for Trusted Wireless was chosen in such a way that an attacker would have to wait more than 1,000 years before the code repeats.

Flexible networks with automatic connection management

As already mentioned, there are special requirements to ensure the reliability of wireless networks in an industrial environment. The right network structure can considerably improve this reliability.

Trusted Wireless has store-and-forward repeater functionality, and the network can heal itself if a link breaks, i.e., build up/find an alternative connection path (self-healing network).

This automatic self-healing implementation occurs within milliseconds or seconds after losing a link, depending on the data rate. Users sometimes refer to this self-healing capability as a mesh network, although definitions of a mesh network vary.

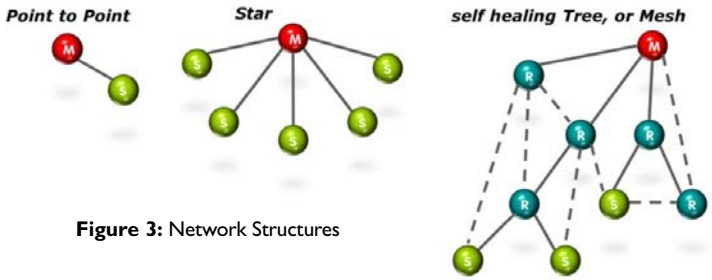

Figure 3: Network Structures

A Trusted Wireless wireless network can therefore operate in all network formations (see Figure 3)

Due to the high receiver sensitivity of Trusted Wireless, sometimes a node does not connect to the nearest node but to another one farther away. Due to this, Trusted Wireless offers the possibility to do a parent-blocklisting. With this method, users specifically exclude nodes from acting as possible repeaters. For every node, the system can "forbid" other nodes (parent-blacklisting) or "allow" (parent-white-listing) as repeaters. By default, the system permits all repeaters as possible nodes.

Distributed network maintenance – faster and easier

In order to operate a wireless network – independent of the data volume transmitted – individual wireless nodes must have internal communication capabilities. In this context, the process for adding a new node to the network (joining), as well as the management of already existing nodes, plays an important role.

Trusted Wireless uses a patented, distributed approach. Here, the implementation of the entire network management occurs within the parent-child zone. This means that a parent (either a base station or repeater) takes care of its children and, if necessary, also integrates new nodes into its zone. This information does not have to transmit all the way to the central manager and back, which in turn reduces the message traffic in the network and considerably accelerates the entire process.

Extensive diagnostic properties

For industrial wireless network operations, the consequences of non-availability far exceed those of private-sector, home applications. Users wish to have greater access to network information, and diagnostics provide the vital information that users want on the state of their wireless networks.

Trusted Wireless offers a wide range of diagnostic information, such as network structure and channel statistics.

The node table contains information on the directly connected nodes, their properties (master to base station, repeater, remote station) their connection quality (RSSI signal), the network depth and the list of permitted or prohibited parents.

The channel table contains information on the radio frequencies used, for example, on the noise level (current and maximum), the channel blocking rate and the packet error rate.

Users can query all diagnostic information remotely and give an exact overview of the network and its environment. This also allows for targeted optimization measures.

Adjustable to the desired application

Trusted Wireless, a wireless technology developed especially for industrial use, was based on the requirements of industrial infrastructure applications and closes the gap between specific sensor networks such as WirelessHART and the high-speed technology WLAN.

Characterized by its particularly good adaptability to the desired industrial application, Trusted Wireless offers a high degree of reliability, ruggedness, security and flexibility.

PHOENIX CONTACT • P.O. Box 4100 • Harrisburg, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Website: www.phoenixcontact.com

Glossary

AES	Advanced Encryption Standard
DSSS	Direct Sequence Spread Spectrum
EMC	Electromagnetic compatibility
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
ISM band	Industrial, Scientific, and Medical band
LBT	Listen Before Talk
LOS	Line of sight
NLOS	Non-line-of-sight OTA Over-the-Air
P/C zone	Parent-Child zone
R & TTE	Radio and Telecommunications Terminal Equipment
RF band	Radio frequency band
RFC	Request for Comments
RSSI	Receive Signal Strength Indicator
WLAN	Wireless Local Area Network

ABOUT PHOENIX CONTACT

Phoenix Contact is a global market leader based in Germany. Phoenix Contact produces future-oriented components, systems, and solutions for electrical controls, networking, and automation. With a worldwide network reaching across more than 100 countries, and with over 20,300 employees, Phoenix Contact maintains close relationships with its customers, which is essential for shared success. The company's wide variety of products makes it easy for engineers to implement the latest technology in various applications and industries. Phoenix Contact focuses on the fields of energy, infrastructure, process, and factory automation.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com, call** technical service at **800-322-3225,** or email **info@phoenixcontact.com**.

PHOENIX CONTACT • P.O. Box 4100 • Harrisburg, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
Website: www.phoenixcontact.com