White Paper

Trusted Wireless 2.0 – Basics and practical applications

Author:
MEng Frank Hakemeyer
fhakemeyer@phoenixcontact.com

ION03-17,000.PR5

Table of contents

Overview

The use of wireless technologies for industrial automation is becoming increasingly popular. This is partly due to the fact that wireless networking of remote system parts or mobile units is becoming more and more important. Additionally industrial wireless technologies have clearly proven their advantages and their reliability and have addressed any misconceptions over the past years.

This document refers specifically to the Trusted Wireless 2.0 technology and its application in the field of automation. The main focus will be on the description of the technological properties which are of particular interest for industrial applications. The relationships that exist between technology and practical application will be explained and delimitations to other wireless technologies will be shown.

First and foremost, this white paper addresses industrial users of factory or system automation as well as of the infrastructure. Moreover, it is also aimed at all readers who are interested in the technical concepts of industrial wireless data transmission.

Use of wireless technologies in automation technology

Year by year, more wireless technologies are used in automation technology. Users benefit from this, as wireless solutions offer a higher degree of mobility and flexibility. Often it is the cost saving from the elimination of cable installation which is the reason for the use of a wireless system.

The automation industry focuses mainly on wireless technologies, which can be used practically worldwide and function in license-free frequency bands. Due to national frequency regulation, there are only a few frequency bands which meet this criteria. ISM (Industrial-Scientific-Medical) bands can be used without a license, but only the 2.4-GHz band is distributed nearly worldwide. Thus, the majority of wireless technologies in automation technology use this band.

Thanks to the large bandwidth of 83MHz, a high data throughput and/or the parallel operation of multiple wireless systems in the 2.4 GHz ISM band is possible. The bandwidth of the low-frequency bands is considerably smaller and is between a few hundred kHz and 26 MHz. However, the propagation and the properties of material penetration of these ISM bands are considerably better (see Fig. 1), which makes longer ranges and wireless paths without a line of sight possible.

Thus, Trusted Wireless 2.0 is available for ISM bands 868 MHz (Europe), 900 MHz (America and Australia) and 2.4 GHz (worldwide). In this way, requirements can also be met for ranges over 5 km and in unfavorable ambient conditions. Here it is always essential to correctly apply the advantages of the selected wireless system.

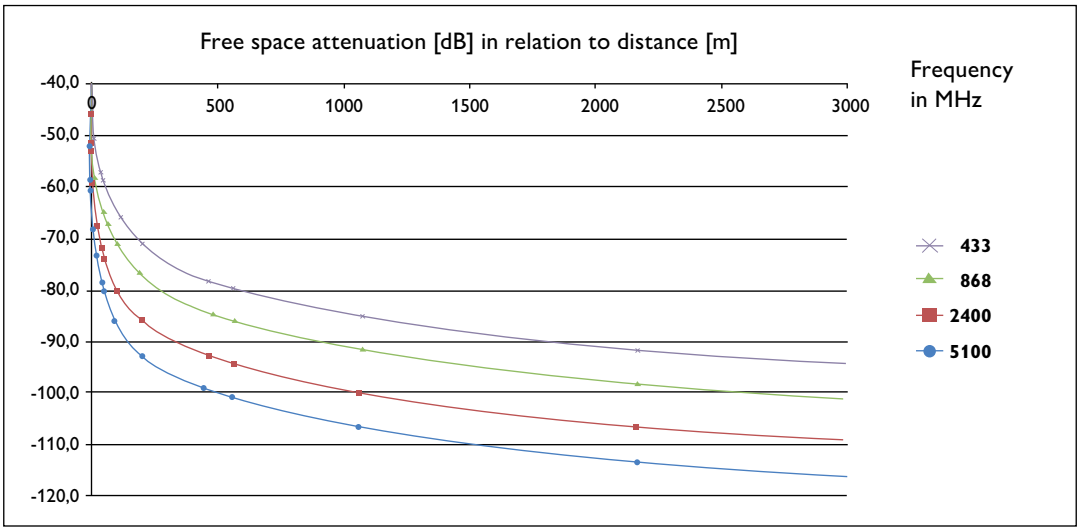

Figure 1

The free space attenuation increases in proportion to the frequency

In the following, the description of the wireless technology Trusted Wireless 2.0 will refer to familiar wireless technologies from the consumer and IT world. Since Bluetooth and WLAN are now also used in industrial environments, this white paper will focus particularly on the differences between these technologies. In addition, there is already a wireless technology specially developed for process technology, WirelessHART, which is also used for comparison.

Since wireless technologies in the sub-GHz band cannot be compared with wireless technologies in the 2.4 GHz band, familiar Low Power systems from the sub-GHz band are used here for comparison.

Areas of application for Trusted Wireless **2.0**

Trusted Wireless 2.0 is a wireless technology developed specially for industrial use. It is particularly suitable for sensor-actuator information covering cable infrastructure is from one. It is used to up small to medium-sized data quantities, over larger distances of hundreds meters to several kilometers.

The main features of Trusted Wireless 2.0 are

- Robust communication thanks to FHSS
- Automatic and manual coexistence mechanisms
- Secure communication due to encryption (AES 128 Bit) and integrity check
- Long range thanks to high receiver sensitivity and variable data transmission rates
- Flexible networks with automatic connection management
- Distributed network maintenance makes things easier and faster
- Extensive diagnostic properties
- Adaptability to the desired application

These features are explained in more detail in the following.

Robust communication thanks to FHSS

Every user would like to have "reliable" and "robust" communication for his or her application, though these are rather subjective criteria. Requirements of real characteristics such as availability, latency, determinism and data throughput, which play an important role for the user depending on the application, are referred to as objective.

However, it is important to know and be able to classify the real application requirements. The available wireless technologies have different key aspects and performances and have to be selected according to the application requirements.

It is also vital to know which factors impede the "reliability" of a wireless path and how the different wireless technologies deal with these problems.

There are two major factors that can influence a wireless connection. Firstly, 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 is caused by the free space attenuation and especially by reflections.

Disturbance of the wireless signal by other wireless systems or electromagnetic interference

In the 2.4 GHz band, 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 are otherwise problematic, do not disturb the upper MHz or GHz band. Their high-energy emissions are instead in the kilohertz and megahertz band.

Usually, other wireless systems are the cause for disturbances of these wireless systems. There are two completely different approaches to deal with this problem: the Direct Sequence Spread Spectrum (DSSS) and the Frequency Hopping Spread Spectrum (FHSS).

With the DSSS, the useful signal to be transmitted passes through a spreading code generator,

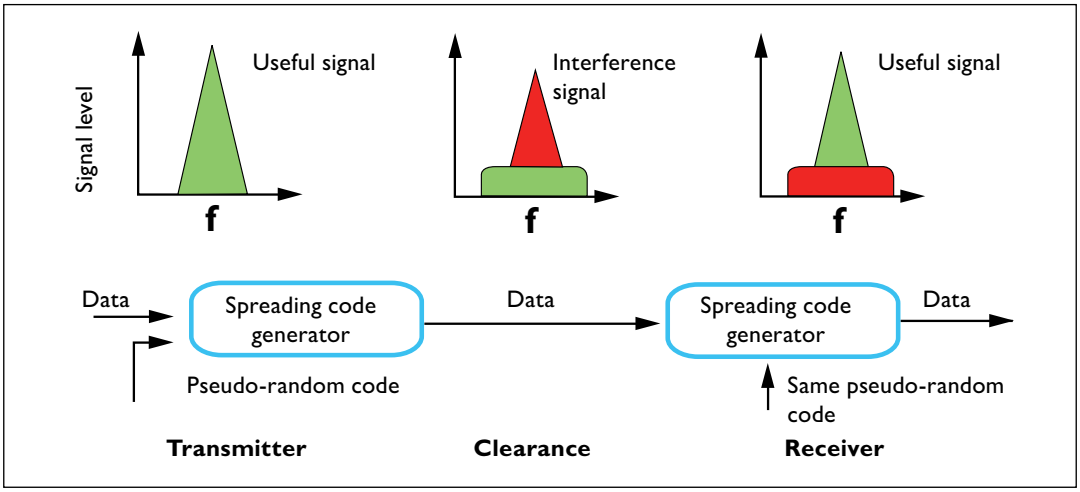

Figure 2a
Diagram of the DSS procedure

which transforms the narrow band interference signal with high amplitude into a broadband signal with lower amplitude (see Fig. 2a). Together with the useful signal, the incoming narrow band interference signal with high amplitude passes the same spreading code generator in the receiver. This way, the wide-band useful signal with low amplitude is converted again into a narrow band signal with high amplitude and simultaneously, the interference signal is transformed into a wide-band noise. One benefit of this procedure is the possible transmission with a very high data rate. The disadvantage is the fixed transmission frequency as well as the fact that this procedure is only useful up to a certain interference signal level. If this level is exceeded, the receiver cannot make a distinction between the useful signal and the interference signal.

With the FHSS, many different individual frequencies are hopped through in a pseudo-random

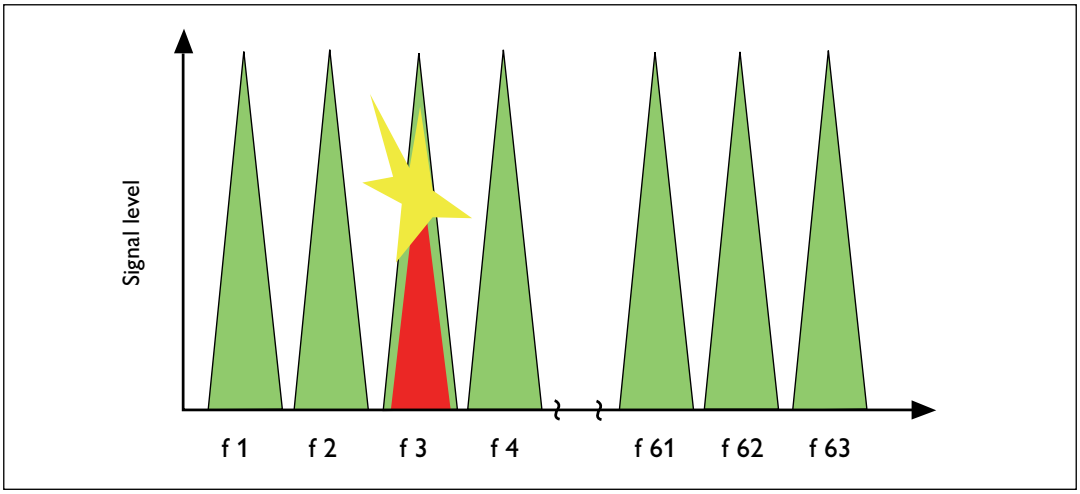

Figure 2b
Diagram of the FHSS procedure

pattern. In this way, an interference signal only blocks one or a few neighboring individual frequencies – no matter how high the level. The transmission can be implemented without interferences using the remaining frequencies.

If disturbances become worse, only the data throughput is reduced in the FHSS system. In the DSSS system, however, transmission might be blocked completely.

In the 2.4 GHz band, Trusted Wireless 2.0 uses a Frequency Hopping Spread Spectrum (FHSS) with up to 440 possible individual frequencies, with the devices using a selection of up to 127 channels. In the 868 MHz and 900 MHz frequency band, the procedure is also employed. Due to the smaller bandwidths in the frequency bands, the number of available channels is correspondingly smaller. 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 (black-listing) 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 is weakened due to different external influences. The main factors are reflections occurring during the propagation of the radio wave. The signal travels from the transmitter to the receiver on many different paths via these reflections (multipath fading). The time the signals need for this vary since, depending on the reflection path, the distances the signals have to travel vary. This means that the signal reaches the receiver in a different phase relation. Therefore, many different individual signals are superposed in different phase relations at all times.

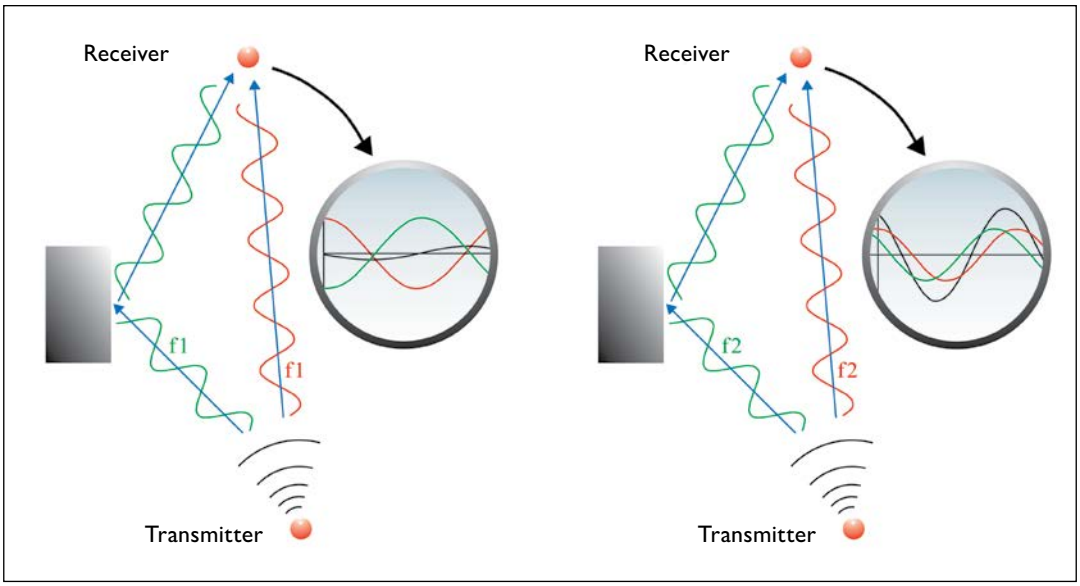

Figure 3
Weakening of the signal on f1 and amplification of the signal on f2

This can result in a weakening (destructive interference) or amplification (constructive interference) of the signal (Fig. 3), dependent upon the constellation of the phase relations at the receiver.

Important: If the transmission frequency – and thus the wavelength – changes under constant ambient conditions (reflection situation), the reflection signals and the situation of the superposed signals at the receiver change, too. Therefore, a particularly unfavorable constellation might occur on an f1 frequency of a wireless system, causing the receiver to receive an extremely weak or insufficient signal. Under the same ambient conditions, however, an amplification of the signal might occur on another frequency. This is a considerable advantage of a frequency hopping system (FHSS), which constantly changes the transmission frequency and therefore automatically prevents this physical problem.

The Trusted Wireless 2.0 wireless technology use many individual transmitting frequencies within the respective frequency band (see FHSS). The distances between the frequency bands are selected so that the wavelength variation is large enough to create a significant signal yield. This ensures reliable transmission which is not appreciably affected by signal fading.

In other words: if – depending on the multipath fading – the transmission is not possible on one frequency, the signal on the next frequency is strong enough for easy reception.

Automatic and manual coexistence mechanisms

Due to the increasing use of ISM bands, the co-existence mechanisms of a wireless system are becoming more and more important for long-term problem-free usage.

Example of a incoming mechanism, is listen-before-talk (LBT for short). With LBT, first the strength of the receiver signal is measured. The RSSI Signal (Receive-Signal-Strength-Indicator) is determined. This value provides – regardless of the sending technology employed – a measurement of whether another wireless-system is already sending. Depending on the strength of the RSSI signal, the mechanism decides whether it is possible to use the medium or not.

The disadvantage of this process is that it has a higher latency period in comparison with a fixed Duty Cycle (see below). Especially when the 2.4 GHz band is used in an industrial environment or in public places since here, in addition to the installed WLAN and Bluetooth systems, all private devices may represent a wireless system to be taken into account.

In unfavorable cases, LBT may bring about settings which benefit other wireless systems or even interferers of wireless operation. For this reason, in all frequency bands Trusted Wireless 2.0 employs the Duty Cycle mechanisms specified in the ISM regulations.

Depending on the ISM band, there are various co-existence mechanisms which legally regulate media access. This includes, for example, the prescribed Duty Cycle in the 868 MHz range. Here it is legally stipulated that a wireless system must either carry out LBT (see above) or only transmit 10% of the time. This mechanism makes it possible for a wireless system to not block an entire frequency band, thereby blocking weaker transmitters, such as garage door openers or baby phones.

A frequency hopping spread spectrum is also an effective co-existence mechanism which makes it possible to operate multiple systems in the same frequency band. Since the systems constantly and pseudo-randomly change their frequency, collisions only occur occasionally and last only for one communication cycle.

However, interference from coexisting systems with the indicated mechanisms cannot be eliminated but only made less likely.

This is why it is installed in the environment practice today in many automation applications to plan the wireless systems employed in the system. This means different wireless products and technologies are used for different applications. In order to give these products the best possible access to the medium and to have as little reciprocal influence as possible, one should plan the employed spectrum accordingly. This particularly applies to the 2.4 GHz band, since most commercial wireless systems operate there.

A WLAN channel, for example, uses 20 MHz bandwidth according to IEEE 802.11b. If several WLAN systems are needed in a system, they should use different WLAN channels. Since the WLAN channels are arranged in an overlapping manner, when the systems are in the immediate vicinity, channels should be searched for which do not overlap, such as channels 1, 6 and 13. If a Bluetooth or Trusted Wireless System is additionally used, these frequency bands of the WLAN system should be hidden (black-listing). In Fig. 4, one sees the spectrum of the active Frequency Hopping System (for example, Bluetooth) and the three WLAN channels which have been kept open.

It becomes increasingly important that the frequency band used for the different systems is well-planned and the technology must allow for the blacklisting of frequency ranges. Trusted Wireless 2.0 is able to blacklist frequency ranges and therefore allows the coexistence with other systems

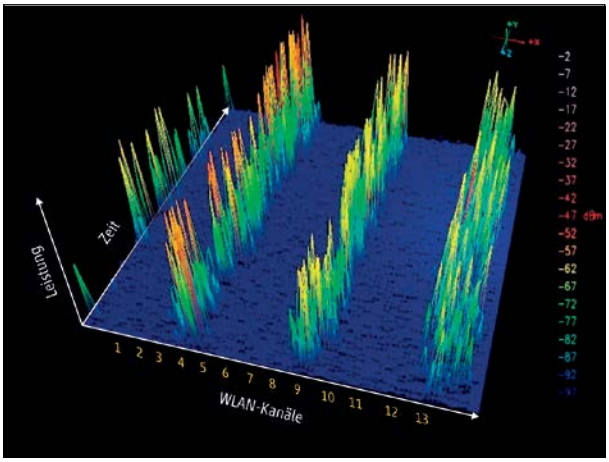

Figure 4
Spectrum of the active Frequency Hopping System and the three WLAN channels which have been kept open

to be planned. For this, frequency hopping patterns are recalculated according to the blacklisted areas.

With Trusted Wireless 2.0, several aspects are taken into account during the creation of the frequency hopping patterns. Firstly, the above-mentioned consideration of the black-listing areas and also the previously mentioned minimum hopping distance for the largest possible frequency or wavelength variation to compensate the multi-path fadings.

The third aspect is the grouping of frequencies in RF bands. An RF band is a group of frequencies made up of individual frequencies from the entire frequency range. Different RF bands use completely different frequencies. If two Trusted Wireless Networks are operated using two different RF bands in a spatial environment, these two networks will never collide. In the 2.4 GHz and 900 MHz band, Trusted Wireless 2.0 has 8 different RF bands. 2 RF bands are available in the 868 MHz band.

In addition, with the targeted use of Trusted Wireless in different frequency bands, a frequency band which has already been used to capacity can be avoided.

Secure communication due to encryption and integrity check

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

With the widely distributed wireless technologies Bluetooth and Wireless LAN, the problem is that the communication interface is accessible for everyone, i.e. every available Bluetooth or WLAN wireless product fundamentally permits a connection with the industrially employed network. The potential danger is especially high with the WLAN interface, since it extremely common in the PC environment and very vulnerable to hacker attacks.

Thanks to its closed technology, an industrial wireless path with Trusted Wireless 2.0 is, in principle, much better protected against possible attacks. Moreover, the frequency hopping method makes spying on the protocol much harder.

But Trusted Wireless 2.0 also has two genuine security mechanisms, an encryption of all transmitted information in accordance with the Advanced Encryption Standard (AES), as well as a user data integrity check described in accordance with RFC3610.

The encryption according to AES ensures that theoretically captured data packets are not "understood", i.e. the content cannot be interpreted. The 128-bit key is calculated from an assigned password (Pre-Shared Key) and must be known to all participants.

The authentication of transmitted data packets is as least as important as the integrity check. The simplest method to attack a wireless path is to listen into a message and possibly to change

it and feed it back. Therefore, it must be ensured that the source of the message, the transmitter, is an authenticated transmitter. For this, the messages have a continuous code, which must not be repeated. This consecutive code is selected for Trusted Wireless 2.0 in such a way that an attacker would have to wait 1,000 years before the code repeats.

Long range thanks to high receiver sensitivity and variable data transmission rates

For industrial wireless applications, the range plays a vital role, especially for outdoor applications. However, also in systems where no long ranges have to be overcome, a good receiver sensitivity offers a high system reserve for transmission in harsh conditions, e.g., with NLOS (non-line-of-sight). Essentially, the receiver sensitivity depends on the quality of the switching circuits and the transmission speed. Trusted Wireless 2.0 uses high-quality components for the transmission and reception levels and reaches a good sensitivity due to an additional pre-amplification.

Still much greater is the additional increase of sensitivity from variable data rates. If a lower data rate is used on the air transmission path, each individual information (each bit) is transmitted for a longer time with transmission power P. The energy per bit [EBit = P • tBit] is thus four times lower with a data rate that is four times higher (Fig. 6).

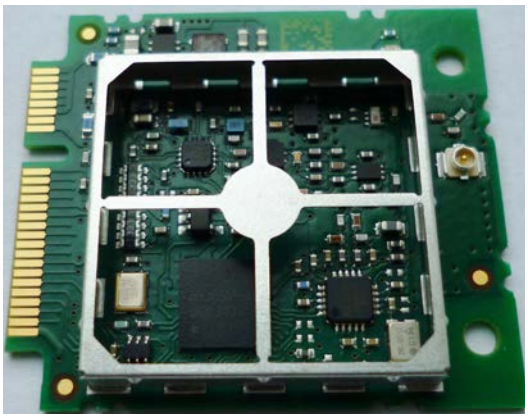

Figure 5
High-quality components for good receiver sensitivity

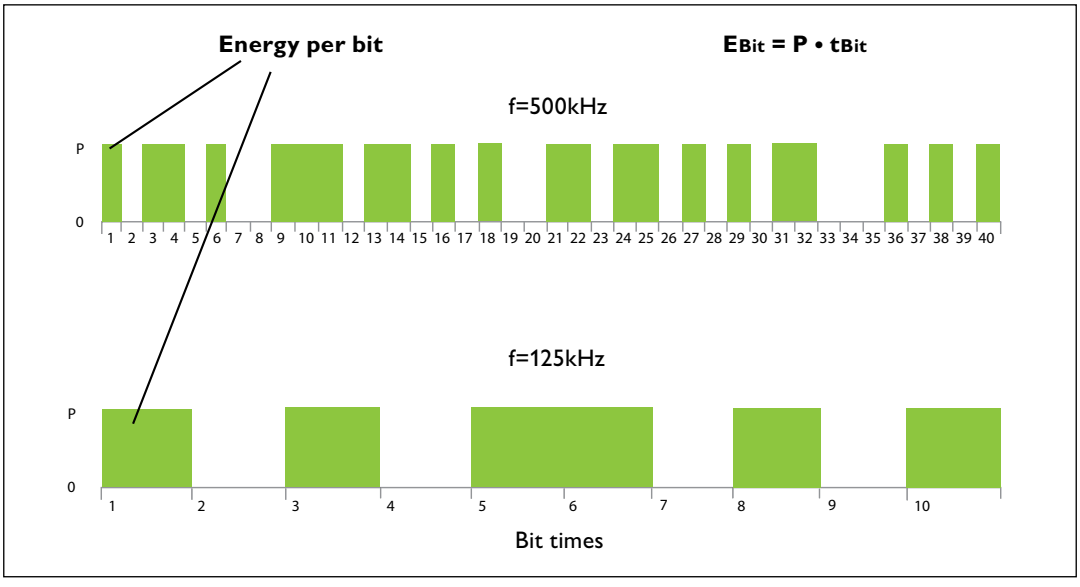

Figure 6
The lower the data rate, the higher the energy per bit

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. Since the range of a system doubles each 6 dB, the range of a 125 kHz system is about twice as long as that of a 500 kHz system.

Trusted Wireless 2.0 offers various adjustable data rates. In this way, depending on the application requirements, the range can be maximized and is thus much greater than the ranges of common Bluetooth and WLAN systems.

The wireless technology Trusted Wireless 2.0 offers the following receiver sensitivities:

OTA data rate in kbps	Typical receiver sensitivity in dBm	Possible distance that can be overcome with LOS and a system reserve of 12 dB	ISM band	Max. EIRP in dBm
250	-93	1 km	2.4 GHz	20
125	-96	3 km	2.4 GHz	20
16	-106	5 km	2.4 GHz	20
500	-95	8 km	900 MHz	30
250	-102	18 km	900 MHz	30
125	-105	24 km	900 MHz	30
16	-112	32 km	900 MHz	30
120	-103	8 km	868 MHz	27
60	-104	10 km	868 MHz	27
19.2	-111	18 km	868 MHz	27
9.6	-114	20 km	868 MHz	27
1.2	-122	25 km	868 MHz	27

* The transmission power in the 2.4 GHz band in Europe depends on the data rate and is <19 dBm for Trusted Wireless 2.0.

Table 1:

Comparison of receiver sensitivity and range in the respective systems.

In order to determine the surmountable clearance, the receiver sensitivity must be taken into account along with the transmission power. To determine the link budget, the cable attenuations of the antenna installation and sometimes the antenna gain must also be taken into account. A safe wireless connection should also always be operated with a system reserve of 10-15 dB.

With the Trusted Wireless 2.0 technology, transmission within the kilometer range is possible – in the event of line of sight and depending on the data rate and antenna installation used.

Flexible networks with automatic connection management

As already mentioned, there are special requirements for the reliability of wireless networks in an industrial environment. The right network structure can considerably improve this reliability. Bluetooth uses only point-to-point connections and a master can manage up to seven of them simultaneously. This way, up to seven Bluetooth slaves can be operated with one Bluetooth master.

A WLAN access point functions in a star structure with a sensible number of less than 20 clients. Neither technology supports repeater functions. The expansions of these networks are therefore smaller and there is no possibility to use alternative wireless connections. Trusted Wireless 2.0 has repeater functions and the network is able to heal itself after a connection abort

(self-healing network), i.e. build up or find an alternative connection path. This self-healing is implemented automatically within almost no time (within milliseconds or seconds, depending on the data rate).

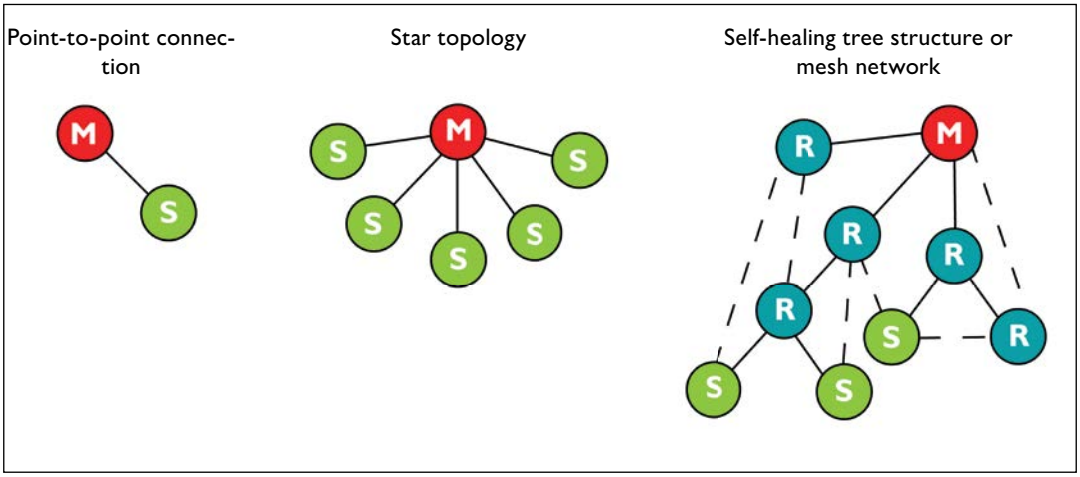

Figure 8
Possible network structures with Trusted Wireless 2.0

As, due to these multiple communication paths, small meshes form between the nodes in the network, this kind of wireless network is also called mesh network. A Trusted Wireless 2.0 wireless network can therefore be operated in all network formations.

In actual networks, it may occur that, due to the high receiver sensitivity of Trusted Wireless 2.0, a node does not connect to the nearest node, but instead to a distant one. Therefore, Trusted Wireless 2.0 offers the option of carrying out what is called parent-black-listing. In this process, targeted nodes are excluded as possible repeaters. Each node can thus become "forbidden" to other nodes as a repeater (parent black-listing) or "allowed" (parent white-listing). In the basic settings, all repeaters are allowed as possible nodes.

Network optimization procedures can be carried out with this functionality. Additionally, in this way network structures, such as chains, can be set up if desired. In Fig. 9, nodes 1, 2 or 3 could be good connections for node 5. Nodes 4, 6 and 9, however, are not good repeaters and can be excluded via parent-black-listing.

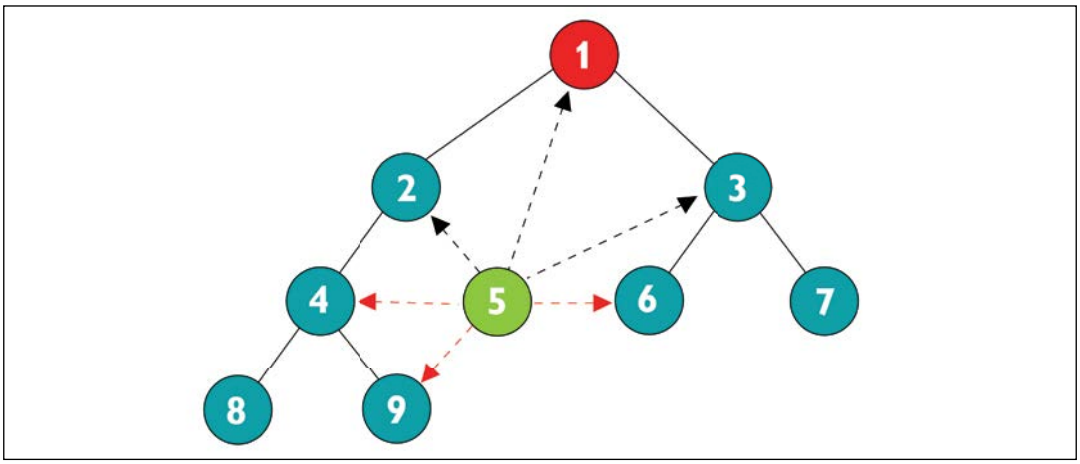

Figure 9
Parent-black-listing for node 5 should contain nodes 4, 6 and 9

Distributed network maintenance makes things easier and faster

Internal communication between the individual wireless nodes is necessary to operate a wireless network - independent of the data volume to be transmitted. In this context, the process for adding a new node to the network (joining) as well as the cyclic management of already existing nodes play an important role.

Wireless networks such as Zigbee and WirelessHART follow a central approach with the use of a central control function, known as the Manager. This results in all network management messages having to be initiated in the Manager and transported through the network to the destination nodes. Responses also travel the entire path. This principle causes considerable communication traffic in the wireless network.

Trusted Wireless 2.0, however, uses a decentralized approach. Here the entire network management is processed with the Parent-Child Zone. This means a parent takes care of its children and integrates a new node in its zone if necessary. The information does not always have to be passed up and down to the central Manager, thus reducing communication traffic in the network and also greatly accelerating the whole process.

This has a positive effect on the network formation speed. If in a centrally managed network, the power supply for the manager fails and it therefore loses the information on the relation of the nodes, a reformation takes a long time. With WirelessHART this may take several minutes, depending on the number of nodes.

With Trusted Wireless 2.0, though, these processes can run in parallel in the individual branches of the network tree (Fig. 10, P/C zone 2.1 and 2.2) because they take place within the parent-child zone. This considerably accelerates the reformation of the wireless network.

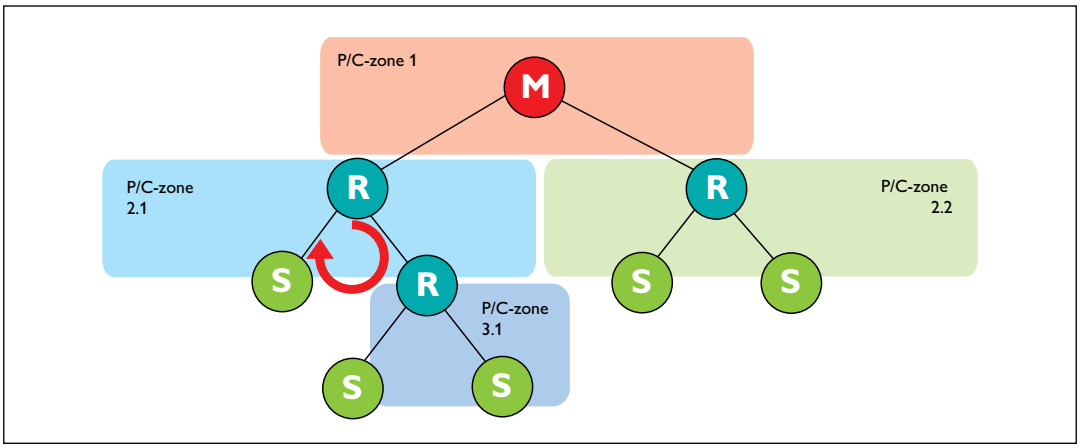

Figure 10

Distributed network management in the parent-child zone (P/C zone)

Extensive diagnostic properties

The operation of an industrial wireless network differs substantially from home applications. The consequences of non-availability are far more critical than in the private domain. This is one of the reasons why users want to have more information on the state of their wireless network. "Diagnostics" thus become very important.

Trusted Wireless 2.0 offers a wide range of diagnostic information. Thus in each node, a node table and a channel table are saved. The node table contains information on the directly connected nodes, their properties (master, repeater, slave), 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. All diagnostic information can be remotely requested via the wireless network to provide the operator with an accurate picture of the network and its environment. This allows targeted optimization measures to be carried out.

Adaptability to the desired application

Trusted Wireless 2.0 is a wireless technology developed specifically for industrial use. It is based on the requirements of industrial infrastructure applications and closes the gap between specific sensor networks such as WirelessHART and the high-speed technology WirelessLAN. Trusted Wireless 2.0 is characterized by its particularly good adaptability to the desired industrial application and offers a high degree of reliability, robustness, safety and flexibility. The following figure shows a comparison of Trusted Wireless 2.0 and other wireless technologies in the 2.4 GHz band.

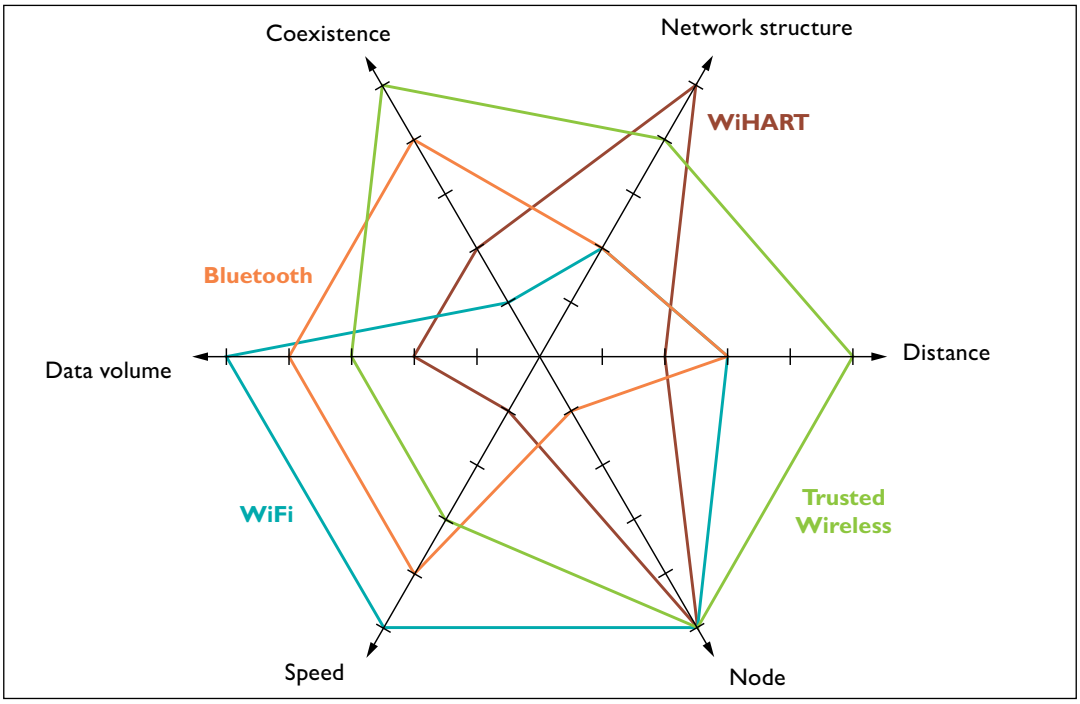

Figure 11

Comparison of various wireless technologies in the 2.4 GHz band

In addition, Trusted Wireless 2.0 represents a private alternative to the provider-dependent Low Power WAN networks in
the 868 and 900-MHz-ISM band. Compared with Sigfox, LoRa and other providers in this segment, Trusted Wireless 2.0 stands out for its considerably higher data rate and flexibility. Thanks to its unique diagnostic depth, its long range and its complete access to its own network, large networks without data limits can be set up whose availability is independent of network distribution or carriers. The following illustration presents a comparison between the technological properties of Trusted Wireless 2.0 and those of other wireless systems in the 868 and 900-MHz-ISM band.

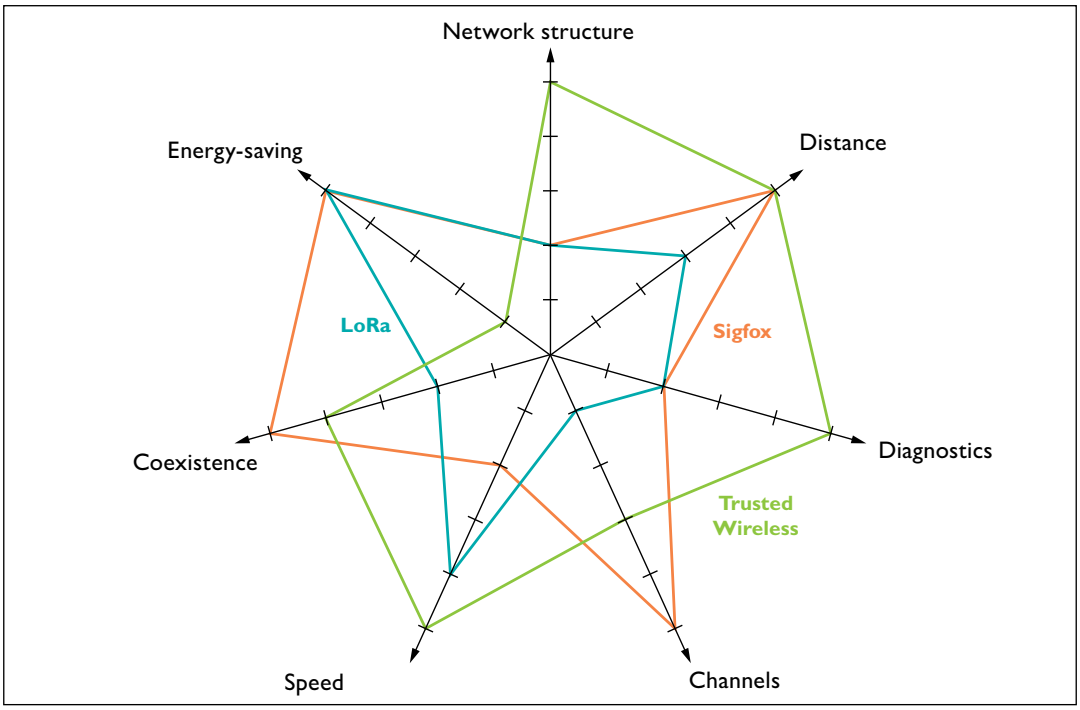

Figure 12

Comparison of various wireless technologies in the 868 and 900 MHz-ISM band

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 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 (Standardization document of the Internet Research and Development group, for example, for the definition of protocols and services)
RSSI	Receive Signal Strength Indicator
WLAN	Wireless Local Area Network

In dialog with customers and partners worldwide

Phoenix Contact is a globally active market leader based in Germany. Our group is synonym for future-oriented components, systems, and solutions in the fields of electrical engineering, electronics, and automation. A global network across more than 100 countries, and 15,000 employees ensures close proximity to our customers, which we believe is particularly important.

The wide variety of our innovative products makes it easy for our customers to find future-oriented solutions for different applications and industries. We especially focus on the fields of energy, infrastructure, process and factory automation.

PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Germany
Phone: + 49 5235 3-00
Fax: + 49 5235 3-41200
phoenixcontact.net

PHOENIX CONTACT