TRUSTED WIRELESS COEXISTENCE

Coexistence of Trusted Wireless 2.0 and WLAN

Application note
106903_en_00

Table of contents

WARNING:
This application note does **not** replace the device-specific documents.
Please follow the safety notes in the associated package slips and data sheets.

Make sure you always use the latest documentation.
It can be downloaded at phoenixcontact.net/products.

PHOENIX CONTACT
INSPIRING INNOVATIONS

1 Wireless systems in parallel operation

If wireless systems are operated in close proximity, there is a chance that they will have a negative impact on one another. Radio-frequency interference can only occur if the following three factors apply:

– Same place
– Same time
– Same frequency

With radio-frequency interference, it can take longer to transmit a data telegram fully and correctly. This transmission time is measured by interfaces, e.g., from the moment a sensor triggers to the time the telegram becomes available in a fieldbus. By measuring over a long period of time, you can assess whether the radio-frequency interference is still permissible. The tolerable transmission times depend on the application. When sending sensor measurement data, a longer transmission time can be tolerated. However, when controlling a machine, the transmission time must be very short.

Coexistence is a state in which several wireless systems can operate without trouble despite radio-frequency interference. Coexistence depends on the level of interference immunity of the wireless systems used and the frequencies that they use.

Also observe the following documents on the subject of coexistence:

– **IEC 62657-2**: Industrial communication networks – Wireless communication networks, part 2: Coexistence management
– **VDI/VDE directive 2185:** Radio based communication in industrial automation

2 Planning coexistence

The license-free, globally available 2.4 GHz ISM band has a high bandwidth and is not affected by typical industrial sources of interference. It is therefore not just used for domestic and office applications, but also increasingly in automation technology. Different standards, such as WLAN and Bluetooth, as well as proprietary solutions such as Trusted Wireless 2.0 use the 2.4 GHz band.

As wireless solutions are being used more and more frequently, radio frequencies are falling into short supply, particularly in large companies. For this reason, their use must be planned professionally. To do this, different departments have to work together closely.

Figure 1 Wireless systems in factory automation

2.1 Avoiding radio-frequency interference by decoupling the frequency range

The assigned frequency is dictated by the wireless technology and its settings.

Static frequency systems have an allocated frequency range (e.g., WLAN, channels 1 ... 13).

Dynamic frequency systems occupy the entire frequency band uniformly (e.g., Bluetooth, Trusted Wireless 2.0).

- Static frequency systems can easily be decoupled from one another in that it is possible to assign different frequency ranges.
- Dynamic frequency systems must not be decoupled from one another. They constantly hop between the frequencies in different patterns. In the event of a collision, transmission is repeated on another frequency.
- If static frequency and dynamic frequency systems are used at the same time, a blacklist can be defined for the dynamic frequency systems. The dynamic frequency systems then avoid the frequencies occupied by the static system.

For WLAN networks with large quantities of data and high temporal allocation, it is advisable to avoid the 5 GHz band.

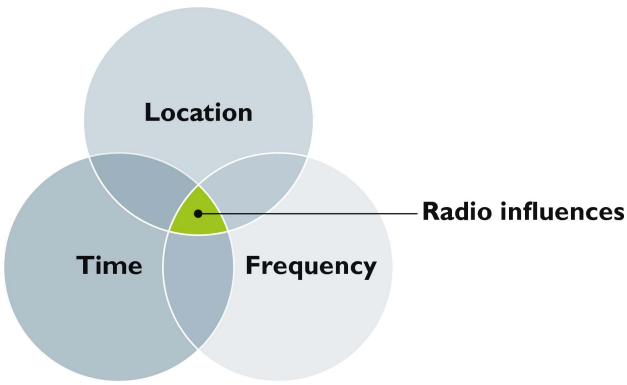


Figure 2 Radio-frequency interference

3 Coexistence of Trusted Wireless 2.0 and WLAN

Phoenix Contact has developed Trusted Wireless 2.0 technology specifically for industrial applications.

Features

- Frequency ranges:
  - 2400 MHz ... 2483.5 MHz
  - 869.4 MHz ... 869.65 MHz
  - 902 MHz ... 928 MHz
- Transmission power: 0 dBm ... 20 dBm, depends on the data rate, can be set via software (in Europe 0 dBm ... 19 dBm)
- Possible data rates: 16 kbps, 125 kbps, 250 kbps
- Robust communication thanks to the frequency-hopping spread spectrum with up to 127 channels
- Automatic and manual mechanisms for coexistence with other systems transmitting in the same frequency band
- Secure data encryption and authentication
- Long range thanks to high receiver sensitivity and variable data transmission speed
- Flexible network structure with automatic connection management
- Distributed network management
- Comprehensive diagnostics options

Frequency-hopping spread spectrum (FHSS) method

In the license-free 2.4 GHz frequency band, Trusted Wireless 2.0 uses the frequency-hopping spread spectrum (FHSS) method. This method uses a selection of up to 127 channels from the entire spectrum of the frequency band. The wireless module “hops” between these channels on the basis of a pseudo-random pattern. This results in more robust and more reliable communication.

Blacklisting

Blacklisting means that certain frequencies can be hidden selectively. This method allows you to operate several WLAN systems in parallel with Trusted Wireless 2.0 systems without any interference or performance limitations.

3.1 Investigation into coexistence

In 2014, the Institut für Automation und Kommunikation (ikaf) in Madgeburg, Germany looked at how Trusted Wireless 2.0 and WLAN affect one another. In addition, it recorded spectrograms of the frequency band as well as histograms of the packet runtime.

Procedure:

1. Both wireless systems were operated individually.
2. The wireless systems were operated in parallel with their respective factory settings.
3. The coexistence mechanisms were set in the most effective way possible using wireless network planning.

These observations were implemented both with the WLAN system as the interferer and with the Trusted Wireless 2.0 system as the interferer.

3.2 Test set-up

Two wireless systems were operated in parallel on the 2.4 GHz ISM band in a hall. The institute looked at the following:

– Influence of a WLAN system on a Trusted Wireless system
– Influence of a Trusted Wireless system on a WLAN system

The operating behavior was examined based on the transmission times. The 95th percentile (P95) was used for the statistical analysis of the measurement results. 95% of all measured values are smaller than or the same as the P95 value.

Distances (see Figure 3):

WLAN access point (AP) ... WLAN clients (Cl)	8 meters
WLAN access point (AP) ... Consumer 01	1 meter
WLAN client 01 ... Producer	3 meters
WLAN clients 02, 03, 04 (Cl) ... Consumer 01	7.8 meters

In the test set-up, the distances are small, as a set-up of this type is most critical with respect to coexistence. The level of performance drops quadratically with the distance.

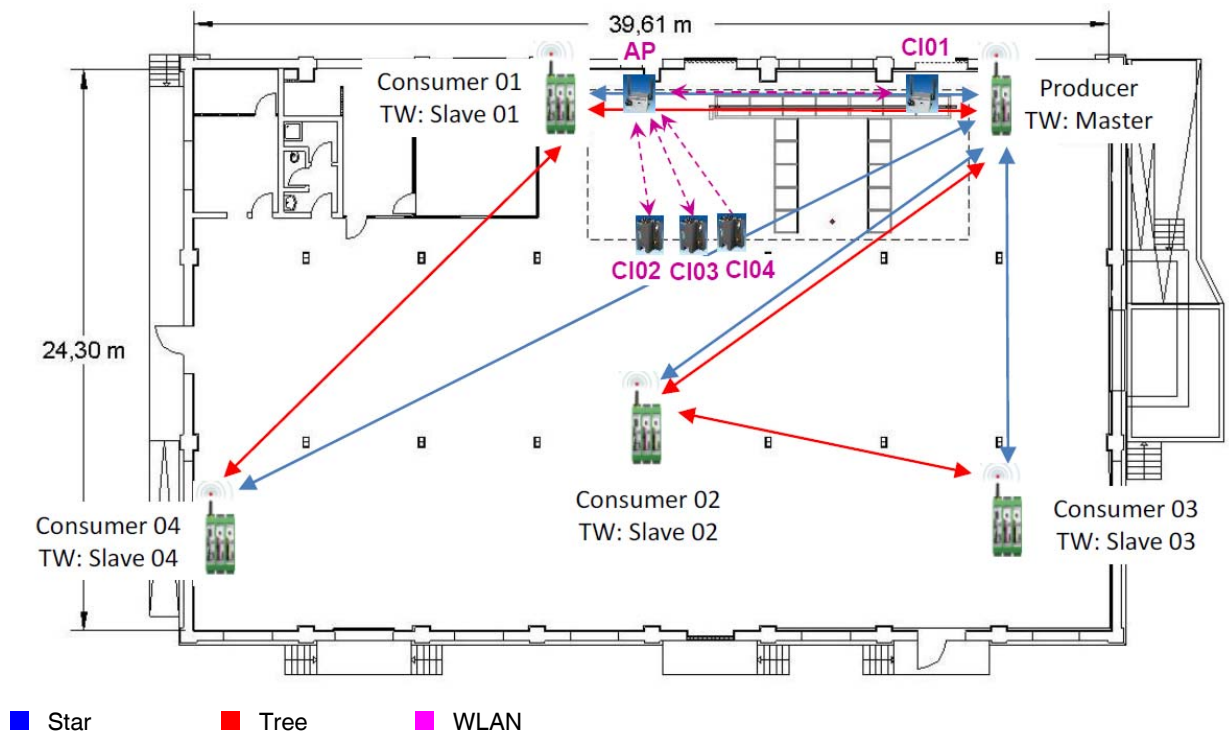
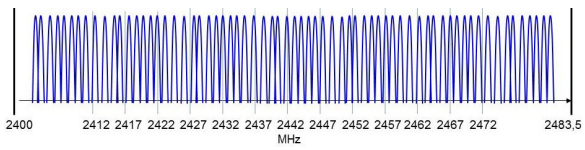
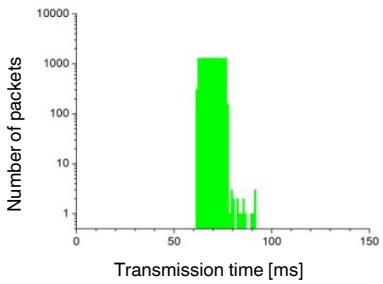
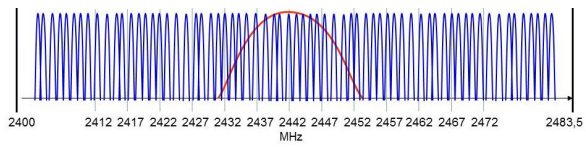
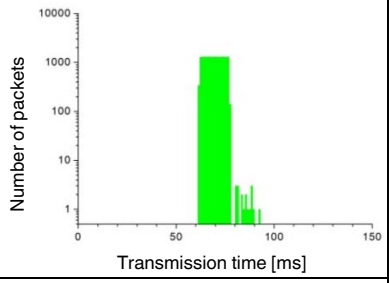
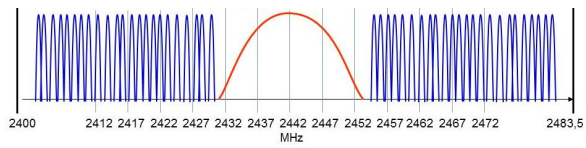
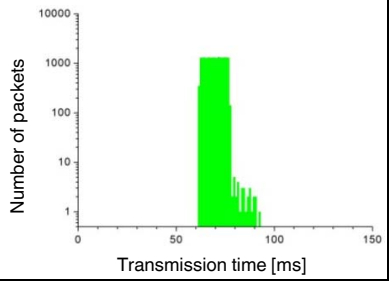


Figure 3 Test set-up

3.3 Measurement results

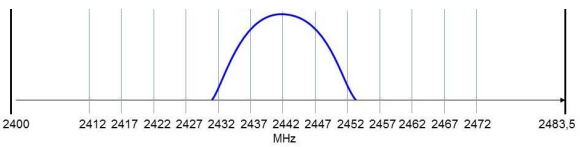
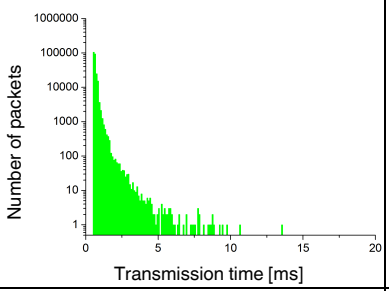
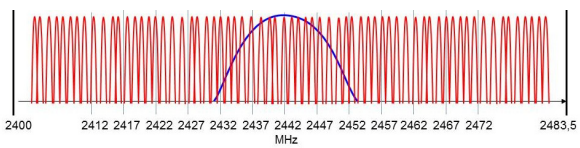
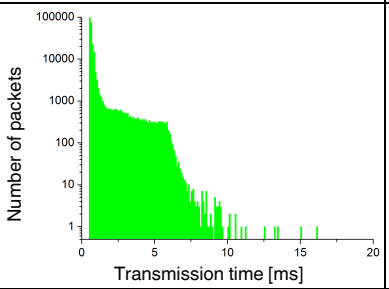
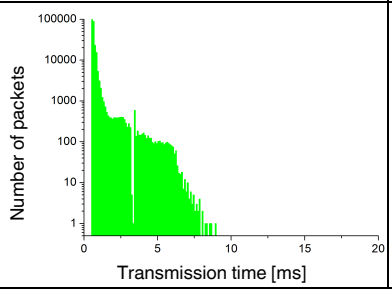
Influence of a WLAN system on a Trusted Wireless 2.0 system

- The narrow-band input filter of the Trusted Wireless system filters the interference signal and therefore reduces radio-frequency interference.
- The transmission time remains constant.
- The Trusted Wireless network is not affected by WLAN.

Influence of a WLAN system on a Trusted Wireless 2.0 system		Transmission time [ms]		
Test system (Trusted Wireless) Interferer (WLAN)		Mini-mum	Maxi-mum	P95
Without interferer				
		61.6	91.5	76.3
With interferer, without blacklisting				
		61.6	92.3	76.4
With interferer, with blacklisting				
		61.6	92.3	76.3

Influence of a Trusted Wireless 2.0 system on a WLAN system

- The wide-band WLAN receiver processes the energy from the Trusted Wireless interferer.
- Without blacklisting, the interference is clearly noticeable.
- If blacklisting is active, the transmission time remains more or less constant.
- Frequency planning with blacklisting prevents interference from Trusted Wireless 2.0.

Influence of a Trusted Wireless 2.0 system on a WLAN system		Transmission time [ms]		
■ Test system (WLAN) ■ Interferer (Trusted Wireless)		Mini-mum	Maxi-mum	P95
Without interferer				
		0.5	9.7	0.9
With interferer, without blacklisting				
		0.5	16.1	2.8
With interferer, with blacklisting				
		0.5	8.9	1.2

3.4 Conclusion of the investigation

The measurement results show that it is possible to operate different wireless systems on the 2.4 GHz band in parallel without any problems. The narrow-band radio technology Trusted Wireless 2.0 is highly insensitive to interference. It is not affected by WLAN.

Wireless network planning in line with IEC 62657-2 and VDI/VDE directive 2185 prevents other wireless systems from affecting the WLAN system. If blacklisting is activated in the Trusted Wireless devices, the wide-band WLAN system is also not affected.

If you plan the wireless network accordingly and use the coexistence mechanisms available, you can be sure that different wireless systems will be able to operate in harmony.

You can find more information on the ZVEI homepage by searching for “wireless system coexistence in automation technology”.

SCATTERGOOD & JOHNSON LTD
ELECTRICAL ENGINEERING & FLUID CONTROL DISTRIBUTORS
Est.1899

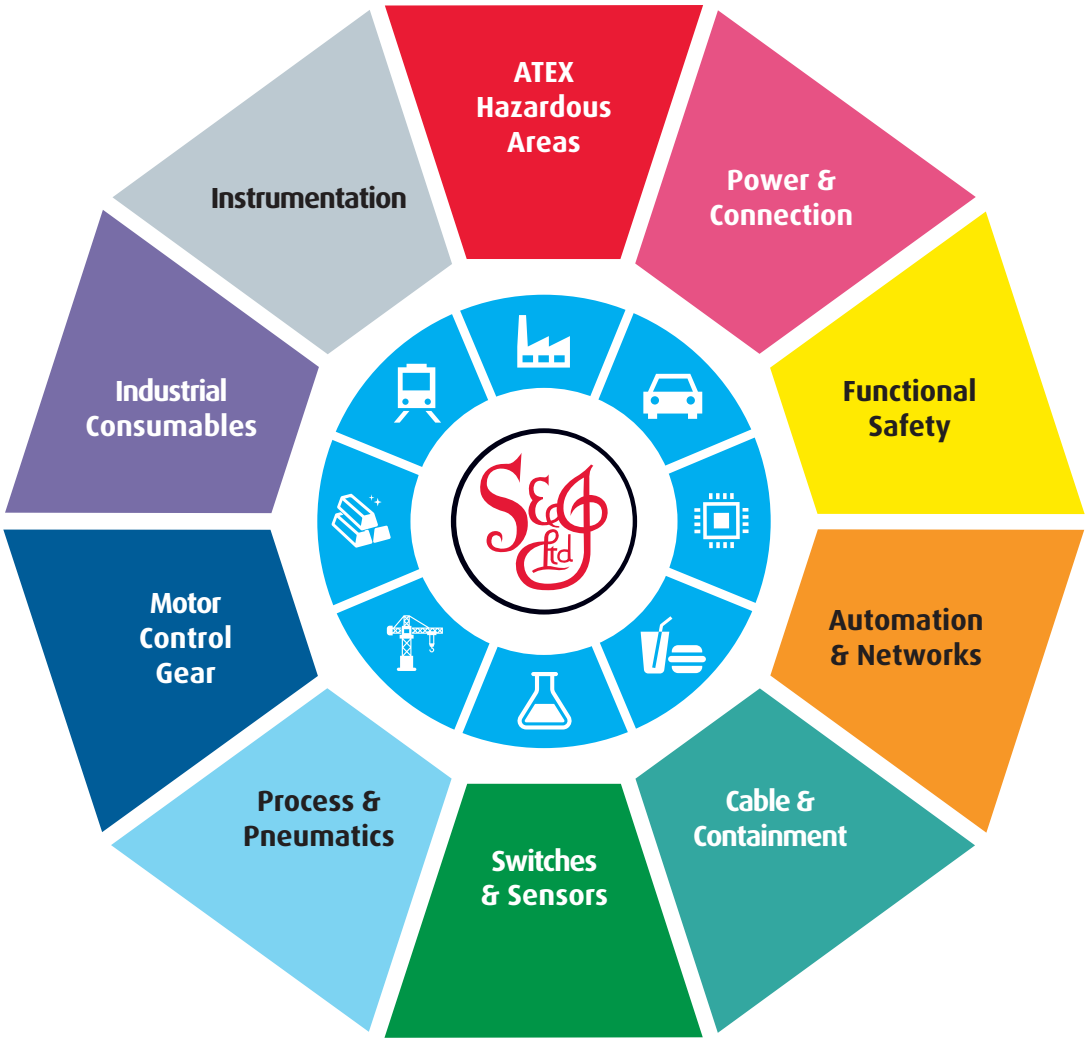
At Scattergood & Johnson Ltd, we pride ourselves on being a technical distributor to specialist industries.

Working with a range of quality product suppliers across a number of specialist markets, we are not your average 'box shifter' - we are your technical and supply chain partner.

We fully support every product we sell - for free! Our internal team and external sales engineers can answer any product or application question, no matter the complexity.

Backing up this technical ability is a range of 50,000+ products available from stock for nationwide next day delivery (same day if required!), or you can collect what you need from any of our trade counters around the UK.

Select your specialist interest below to learn more about how we can help.



Online, In Branch and On the Road - Scattergood & Johnson Ltd, there when you need us.

www.scatts.co.uk