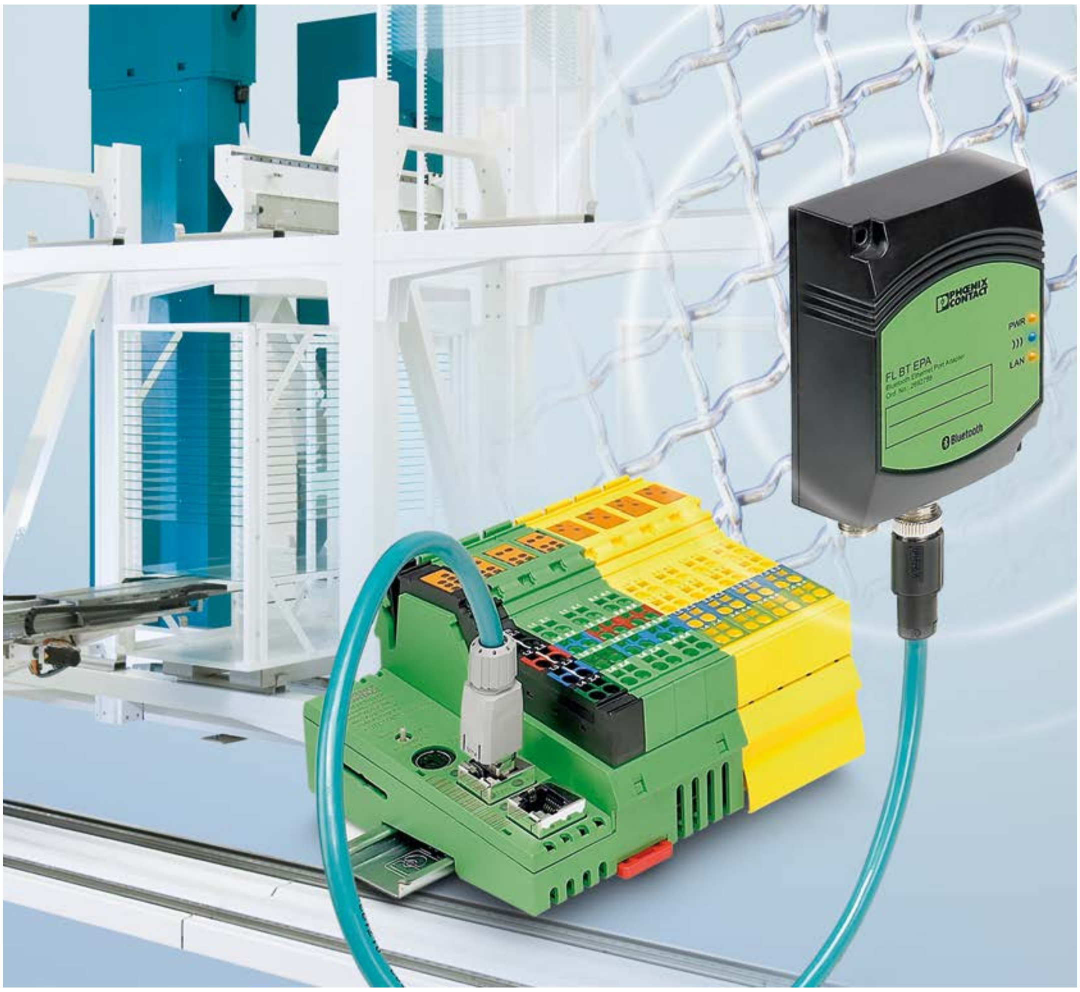

White paper

Functional Safety via Wireless Ethernet

Author:
Jürgen Weczerek
Dipl.-Ing. (FH)
Industrial Electronics
jweczerek@phoenixcontact.com

ION05-15.001.PR5

Table of contents

1 Introduction

Thanks to their flexibility and reliability, wireless solutions are increasingly being used in industrial automation. They serve, for example, to integrate mobile or moving systems into the control network. Yet machine and systems manufacturers expect more than simply high levels of reliability and data security from the wireless solution they use – they also wish to see that their requirements with regard to functional safety are being met. Wireless systems are required to satisfy these complex demands, irrespective of whether they have been developed specifically for industrial applications or are based on standard technologies such as WLAN 802.11 or Bluetooth. In this white paper, you will find out how functionally safe data transmission can be achieved wirelessly with PROFINET and PROFIsafe, as well as with SafetyBridge technology from Phoenix Contact, and also learn what aspects should be taken into account.

2 Safety – and secure wireless transmission

Movement often also means danger. Therefore, the possibility to establish functionally safe, wireless data transmission with moving subsystems is often an essential prerequisite in enabling these systems to be placed in a safe state in an emergency. For the first time, the PROFIBUS user organization (German: PROFIBUS Nutzerorganisation, PNO, set up in 2005) has specified PROFIsafe via PROFINET transmission for wireless communication too. In 2007, the TÜV certification organization and the Institute for Occupational Safety and Health of the German Social Accident Insurance (BGIA) assessed the concept for WLAN 802.11 and Bluetooth again and confirmed its compatibility in accordance with security aspects. The framework conditions required are defined in PROFIsafe profile V.2.4.

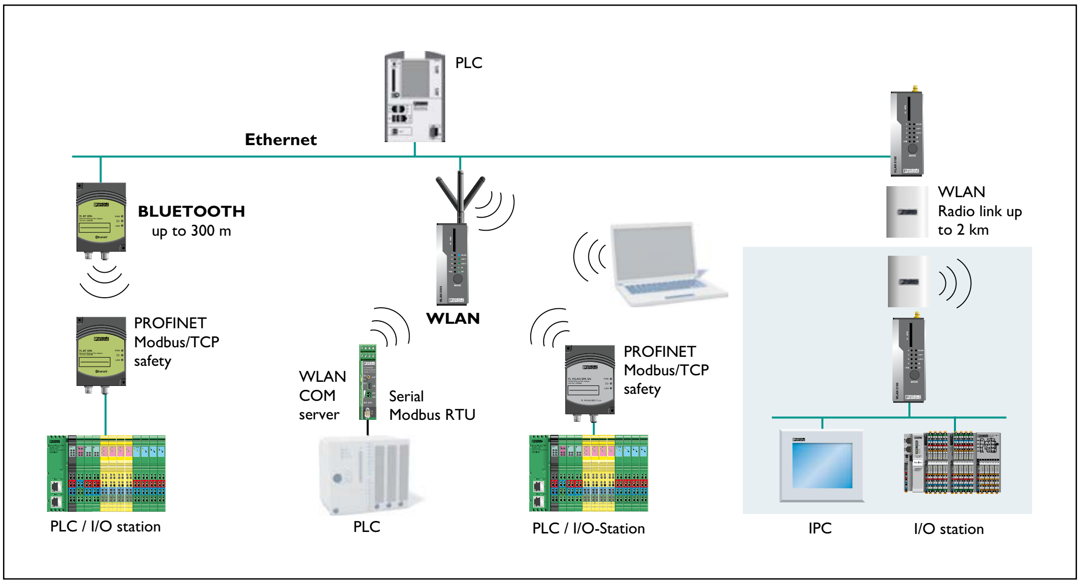

Figure 1

Functionally safe communication between mobile or moving participants is possible via wireless LAN and Bluetooth

3 How safe data transmission works

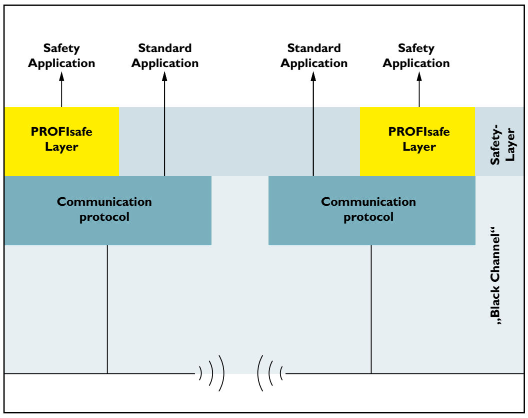

Figure 2
Wireless communication occurs in the black channel and therefore does not have to be validated according to the IEC 61508 series

PROFIsafe and the new SafetyBridge technology from Phoenix Contact can be transmitted safely over Ethernet wireless paths. This is achieved by embedding the safety data of the input module into the standard telegrams of the communication system using an independent safety mechanism. The data is then only unpacked again in the respective safe output module. There, the safety communication stacks check whether an error or an overrun occurred during transmission. If an error is detected, the system is immediately returned to a safe state. The independent, unsafe transmission channel is referred to as the black channel and does not need to be validated in accordance with the IEC 61508 series. This also applies to the network components, such as switches or wireless transmission modules, used in the black channel. The black channel has been defined for an extremely poor bit error rate of 10-2 (IEC 61784-3). This means that 1% or every one hundredth bit can be destroyed. Wireless transmission paths can only be used if excellent error detection measures are in place. Error detection via the safety layer, however, means that the system is switched to a safe, generally unavailable state quickly in the event of errors or overruns. As a result, the use of a robust and reliable wireless transmission method is essential.

4 Data security is compulsory

In contrast to a closed cable network, wireless communication uses a public transmission medium, which is very difficult to restrict in terms of physical space. There is therefore an increased risk of the network being accessed without authorization in order to tamper with the safety system. It was for this reason that emphasis was placed on security requirements when the concept was assessed by TÜV and BGIA. To allow WLAN or Bluetooth to be used for PROFIsafe communication, the corresponding safety measures must be observed. These essentially include safeguards, i.e., the effective encryption of the data transmission, but also the protection of the wireless devices against unauthorized changes to their configuration. A password-protected and safe configuration interface (e.g., HTTPS) is therefore compulsory. Otherwise, there would be the risk that the safety settings for the wireless network could be deactivated without permission or unintentionally, allowing easy and uncontrolled access to the safety network.

5 System availability

A logical mode of operation is crucial when it comes to user acceptance. However, this requires system availability of 100%. This availability depends directly on the error rate of the wireless channel, which must also function extremely robustly and reliably in harsh industrial environments. In addition to the properties of the wireless technology, appropriate planning and installation of the wireless solution is also crucial for ensuring permanent and high-performance wireless communication. What's more, the use of antenna technology that is suitable for the application and its installation in a favorable position is often an important prerequisite for long-term reliable operation.

For high-performance WLAN networks, good planning and the optimum design of the wireless path are crucial. In moving, track-guided systems, for example, it is therefore recommended to use special cable antennas laid along the path and with transmission distances of just a few centimeters.

An extremely robust and reliable wireless technology, Bluetooth, on the other hand, has become firmly established in industrial automation as a wireless small network solution for point-to-point connections, for example. Its extremely high robustness can primarily be attributed to adaptive frequency hopping (AFH). With frequency hopping, the up to 79 transmission channels available for data exchange are switched up to 1600 times a second. If a transmission channel suffers significant interference and the data telegram gets lost, the transmission is repeated on another channel that is not experiencing interference thanks to the automatic repeat request (ARQ) mechanism. Adaptive frequency hopping also detects frequencies that often or permanently suffer interference or frequencies used by other wireless systems, and prevents them from being used automatically. The black channel listing implemented in the industrial Bluetooth devices from Phoenix Contact also allows WLAN channels to be hidden manually, enabling channels to coexist without interference even with a low network load. In addition, the error rate is reduced significantly by an error correction procedure. In the case of forward error correction (FEC), the data is coded redundantly by the transmitter so that the receiver can detect and correct transmission errors. In most cases, it is therefore not necessary to transmit the data that experienced the interference again. This enables reliable and fast communication.

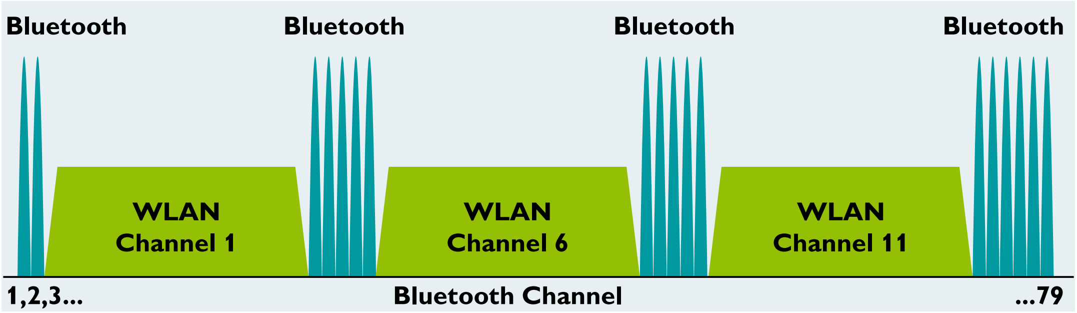

Figure 3

Thanks to AFH and black channel listing, Bluetooth only uses the gaps not used by WLAN and thus avoids interference

6 Planning and installing the wireless connection correctly

It is not just the wireless technology that is the decisive factor when it comes to permanent and high-performance wireless communication – ensuring the appropriate planning and installation for the wireless solution matters too. The use of an antenna that is appropriate to the industrial application and its installation in a favorable position is an important prerequisite. Due to the high losses and sensitivity, the antenna cable between the wireless module and antenna, for example, should be as short as possible. These requirements are often disregarded in practice, however.

When selecting a suitable antenna, it is important to bear in mind that the industrial environment is characterized by reflective metal surfaces. Simple omnidirectional antennas that are usually supplied with wireless components emit a linear radio wave that is polarized either vertically or horizontally. To achieve good reception, the transmitting and receiving antennas must have the same alignment (polarization). If the polarization planes of both antennas are opposed, considerable signal losses will occur. However, the polarization plane changes each time the radio wave is reflected off a metal surface. Even rotating antennas, such as those used on robotic tools, constantly change their polarization plane. To prevent significant fluctuations in the signal strength at the receiver, the use of a circular polarized antenna is recommended. A circular polarized antenna receives a good signal irrespective of the polarization plane, meaning that a good, stable connection can be achieved even in difficult ambient conditions with high levels of reflection.

Ideally, the wireless module and antenna should form a unit and be able to be mounted directly in the field at the best position for wireless reception. Instead of a sensitive antenna cable that significantly reduces performance, only one relatively insensitive Ethernet and energy supply cable needs to be laid. However, this requires the wireless module to have a particularly robust device design. The Ethernet port adapter from Phoenix Contact follows this approach and has been implemented as an active antenna for WLAN and Bluetooth: An industrial wireless module and a circular polarized antenna are integrated into the highly compact and robust housing.

7 Why Bluetooth and WLAN?

In many factory buildings, WLAN is already in use as a wireless add-on to the factory network so that forklift terminals or picking stations can be integrated into the network, for example. As a result, the few available WLAN channels are often already occupied or reserved. The black channel listing implemented in the Bluetooth devices from Phoenix Contact enables frequency ranges of up to three WLAN channels to be manually excluded from use. Bluetooth then makes efficient use of the unused frequency ranges between the WLAN channels, allowing them to coexist without interference. What's more, this enables several Bluetooth networks to be operated in parallel in a very limited amount of space. The last two points in particular are what differentiate the areas of application for Bluetooth technology from those of WLAN. Bluetooth was therefore specified by the PROFIBUS user organization (PNO), just like WLAN, as a wireless communication layer for transparent PROFINET communication and is included in standards IEC 61158-2 and IEC 61784-2.

8 Time response

With a wireless path, in contrast to a cable path, a considerable amount of extra time has to be taken into account. PROFINET offers the advantage here that the update times of each PROFINET device can be set individually. This allows the update time of the devices downstream of the wireless path to be adjusted without affecting the performance of the entire network.
As long as the installation is good, the following key data for a point-to-point wireless path can be applied for the new Bluetooth Ethernet port adapters:

Time response	
PROFINET update time	8 ms
PROFINET timeout time	24 ms
PROFIsafe timeout time:	150 ms

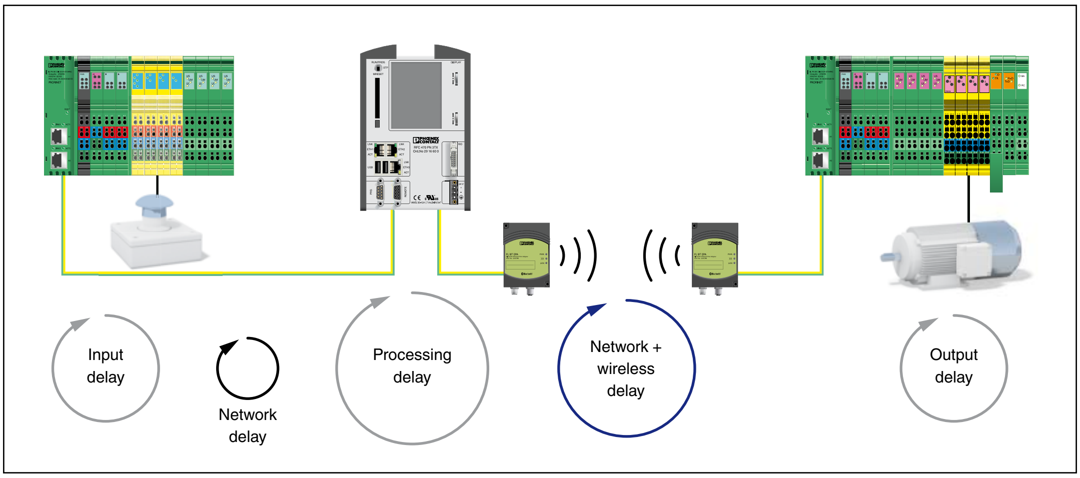

Figure 4

The increased time delays associated with wireless communication must be taken into account at the planning stage under “Bus delay”

9 PROFIsafe vs. SafetyBridge

Unlike PROFIsafe, SafetyBridge technology from Phoenix Contact works independently of the respective network and does not require a safety controller in the network. The safety links are processed directly in the intelligent safe output module. The safe modules can be distributed in the respective network and operated at any point in an I/O station from the Inline automation system. SafetyBridge technology enables all safety-related data signals up to PL e or SIL 3 to be transmitted wirelessly in a safe and reliable manner. This means that cables can simply be replaced with wireless paths without altering the safety characteristics of the safety application.

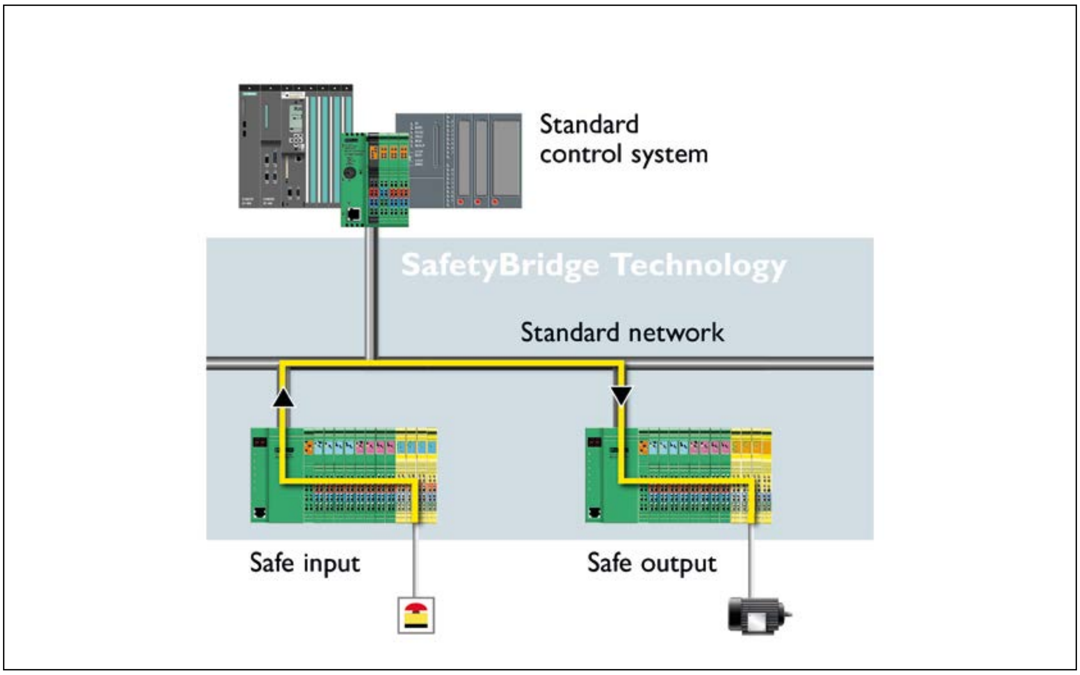

Figure 5

With SafetyBridge technology, safety-related data packets are exchanged between the safe input modules and the output module independently of the network and controller used

10 Conclusion

Doubts concerning the use of wireless communication in industrial automation are unfounded, particularly with respect to functional safety. Technically speaking, wireless communication has no influence on the safety of a machine or system. A certain skepticism regarding the long-term reliability of wireless communication and the associated availability of the machine is completely understandable. However, numerous industrial wireless applications have been running without any problems for many years now and are proof that wireless communication is able to function with optimum availability over the long term. All that is required is a suitable wireless solution for the application and appropriate planning and installation.

PHOENIX CONTACT

Phoenix Contact is a worldwide market leader for components, systems, and solutions in the fields of electrical engineering, electronics, and automation.

Our extensive manufacturing capability means that it is not just screws and plastic and metal parts that are produced in-house, but also highly automated assembly machines. The product range consists of components and system solutions for energy supply including wind and solar energy, device manufacturing and machine building, as well as control cabinet manufacturing.

With a wide range of terminal blocks and special terminal blocks, PCB terminal blocks and connectors, cable connection technology, and installation accessories, we offer innovative components. Electronic interfaces and power supplies, automation systems based on Ethernet and wireless, safety solutions for people, machines, and data, surge protection systems, as well as software programs and tools provide comprehensive systems for installers and operators of systems as well as device manufacturers.

Markets within the automotive industry, renewable energy, and infrastructure are supported by means of consistent solution concepts, ranging from engineering and maintenance to training services, in line with specific needs. Product innovations and specific solutions for individual customer requirements are created in the development facilities at our sites in Germany, China, and the USA. Numerous patents emphasize the fact that many developments from Phoenix Contact are unique. Working closely with universities and scientific institutes, technologies of the future such as E-Mobility and environmental technologies are researched and transformed into marketable products, systems, and solutions.

PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Germany
Phone: + 49 52 35 3-00
Fax: + 49 52 35 3-4 12 00
phoenixcontact.com