FUNCTIONAL SAFETY SOLUTIONS

# Safety protocols go wireless

Comparison of industrial safety protocols and their performance in wireless networks

# Comparison of safety protocols and their performance in wireless networks

## INTRODUCTION

### UNTANGLING SAFETY FUNCTIONS

For decades, safety functions had been hard-wired in factory automation systems. Dedicated wires carrying safety signals had been proven in use and catered for deterministic reactions. Over the last ten to fifteen years, fieldbus technologies have been finding their ways into automation systems, allowing for more flexibility in machine and application building. Along with this, the safety signals had also been successively integrated into conventional fieldbus infrastructure. Still transferred via fixed network wires, the new freedom of communication over fieldbus enabled much more flexibility in the overall application of safety functions. While factory automation devices had been tied to the factory basement, safety functions had been, too. All the design of safe data communication via fieldbus networks was done assuming robust, reliable and fixed networks.

As the wheels of automation literally started to turn faster, factory automation components became more and more agile. A growing armada of mobile machines are deployed in warehouses and factory floors. The age of mobile robots in factory automation has placed new requirements on safe data communication. New methods had to be found to untangle the safety functions from the wired networks, enabling communication with a central control unit, but also among each other in a constantly moving environment. Safety over wireless technologies is therefore the key for the new freedom of mobile machines.

The most widely used and known wireless communication technology is the Wireless LAN (WLAN or Wi-Fi) as described in the IEEE802.11. Regular updates of this standard address the increasing amount of networking devices, data latency, roaming delays, or the data throughput in these networks. It's a trend that shows how the initially much slower wireless technologies are looking to catch up with the proven, high-bandwidth, wired network technologies.

However, all of these advances in wireless communication can easily be undone if poorly suited transmission protocols – safe and non-safe ones- are deployed over the wireless medium. This white paper therefore focuses on the usability of various standard safety protocols in a wireless environment.

**CONTENTS**


- Untangling safety functions 2
- Wireless application scenario 3
- Properties of safety protocols 3
- Conclusions 6
- Safety protocols in a wireless env. 7
- Unidirectional safety data transmission 7
  CIP Safety (8), PROFIsafe (8), OPC UA Safety (9)
- Bidirectional safety data transmission 9
  CIP Safety (10), PROFIsafe (12), OPC UA Safety (12)
- Conclusion / References 13

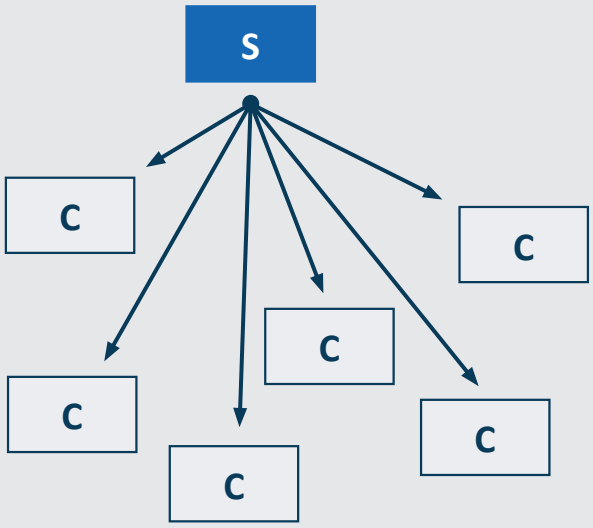


*Figure 1: Single server, multiple clients communication relationship*

### WIRELESS APPLICATION SCENARIO

In a typical scenario, there are several clients C, which can be mobile machines that communicate with a central controller, or more generically, a server S over long distances (see Figure 1).

The use of mobile machines in factories or warehouses creates additional hazards in the work environment. This makes the use of safety functions inevitable. For example, a safety emergency stop signal must be sent from a central server to specific mobile machine clients. Fast-moving mobile machines require high data rates, low latency, and fast roaming. Therefore, this white paper focuses on Wi-Fi (802.11) networks, which meet these requirements better than other wireless technologies such as Bluetooth.

Despite ongoing technological advances, the fundamental problems of a wireless network remain. Using the air as "shared medium", sensitivity to interference and susceptibility to congestion have an adverse effect on communication. This places increased demands on the transmission protocols used, the safety protocol especially. In the following, therefore, the essential properties of known safety protocols are presented first.

## PROPERTIES OF SAFETY PROTOCOLS

The protocols used in the IT world differ in the areas of application for which they were originally intended. A protocol for transmitting video streams must have different properties than a protocol for controlling a robot in production. In this paper, however, we only consider protocols for the area of safety applications. These protocols are similar but differ significantly in terms of their applicability in the wireless area, for which they were not originally intended. Like all protocols, safety protocols also have a hierarchical structure (Fig. 2). Each safety protocol has a different number and complexity of layers. Certain intermediate layers (e.g. the encapsulation protocol layer of EtherNet/IP) are omitted in some of the protocols.

The individual layers fulfill different tasks. The top layer represents the safety layer. The underlying layers form the transmission protocol via the so-called black channel. The tasks of the layers can include, for example, monitoring the transmission process and the connection or routing packets. With each additional layer, however, the packet size and thus the data volume also increase.

The most common safety protocols (listed in figure 2) are based on different communication models. In a client-server model, communication is done using a request-response sequence. Data is sent in both directions with the same frequency.

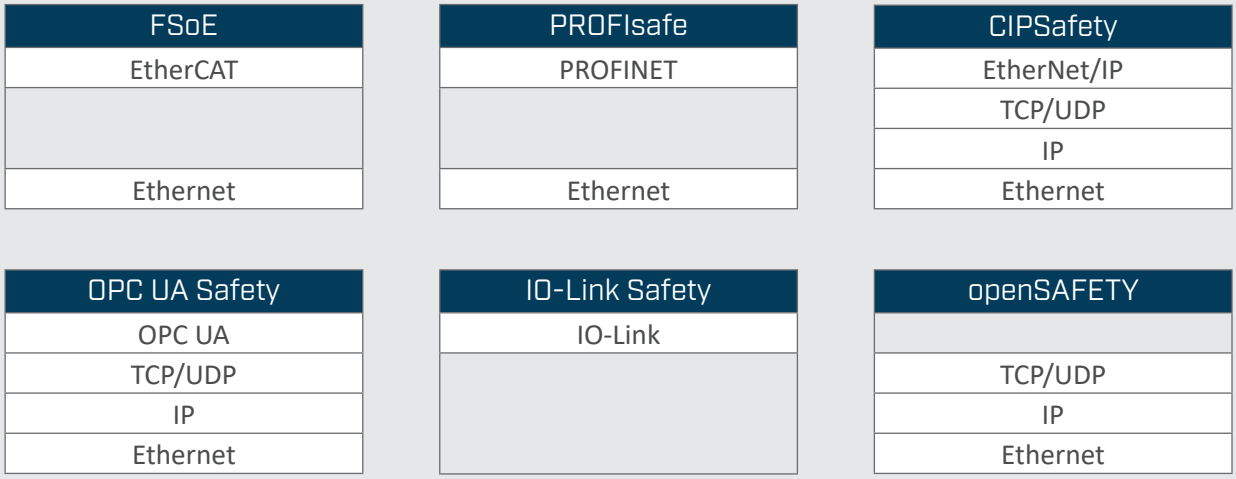


*Figure 2: Layer stack of selected safety protocols*

In a producer-consumer model, data is transmitted without a prior request. In principle, the transmission is only in one direction. This corresponds to a data stream.

In most safety protocols, the communication participants are in a master-slave relationship. The connection is established by a central master through which data exchange takes place. Direct communication between slaves is not supported. This limits the producer-consumer model. The data produced by a slave must be consumed by another slave via the master.

Normally in safety applications, it is more important that the latest data is received than that all data is received. For example, it would make no sense to repeat the lost position value of a position encoder if the position encoder has already sent out a new position value. It would also make little sense to repeat an emergency stop signal if it is sent periodically anyway. From the point of view of the transmission protocol, confirmations and repetitions of messages can then be omitted. Another advantage of the producer-consumer model is that the number of consumers is not limited. A producer can have multiple consumers. This is even supported with some protocols in that the producer only has to send the data once, but the data can be processed by several consumers.

There are also different methods  for the way in which data is transmitted:

**Connections**
Some protocols use separate connections for the different transmission directions. Although this allows, for example, several consumers to receive the same produced data, however, if data is transmitted bidirectionally between stations, two individual connections must be maintained.

**Transmission types**
With a periodic transmission, it does not matter whether the data changes or not. In contrast, with change-of-state connections, data is only transmitted if it has changed. However, since a sign of life for the connection must be sent regularly for safety reasons, periodic transmission is required in addition to a status change transmission. In such a case, the application typically determines how often the connection alive shall be sent for a stable connection.

**Data priority**
In addition to process data, protocols also transmit administrative data. The transmission of administrative data is usually not that time critical. For this reason, some protocols offer the option of giving the process data a higher priority during transmission. This is an example of a Quality of Service.

The different properties of known safety protocols are compared in a table below. The abbreviations used have the following meaning:

- **CM** (Communication Model)
  Variants here are a client-server relationship based on request-response communication or a producer-consumer relationship, in which a consumer receives the data without first asking for it.
- **SC** (Separate Connections)
  Separate Connections used for bi-directional user data transfer.
- **SD** (Shared Data)
  Shared use of the user data. The user data is only sent once via the physical medium but is received and processed by several network participants.
- **FC** (Flow Control)
  It prevents data loss due to buffer overflow. At least one of the layers requires acknowledgment of sent frames over the communication medium.
- **RT** (Re-transmission)
  On at least one of the layers, unacknowledged or lost frames are retransmitted.
- **QoS** (Quality of Service)
  In the form of a prioritization of messages on the communication channel.
- **PE** (Protocol Efficiency)
  Relation of framing data (header/trailer) to actual application data.

| Protocol | CM | SC | SD | FC | RT | QoS | PE |
|---|---|---|---|---|---|---|---|
| **OPC UA Safety** | Client-Server | ✓ | ✗ | ✓ | ✓ | ✗ | - - |
| **CIP Safety** | Producer-Consumer 1:1 up to 1:15 | ✓ | ✓ | ✗ | ✓ | ✓ | - |
| **FSoE** | Client-Server | ✗ | ✗ | ✓ | ✗ | ✗ | + |
| **PROFIsafe** | Client-Server | ✗ | ✗ | ✓ | ✓ | ✓ | + |

*Table 1: Properties of selected safety protocols*

*✗ = no, ✓ = yes, + = more efficient, - = less efficient, -- = much less efficient*

## Conclusions

**SC:** OPC UA Safety and CIP Safety use two independent bidirectional connections when transferring user data between two stations in both directions. This results in a total of four transmit messages to exchange the user data in both directions. PROFIsafe and FSoE, in contrast, use only one bidirectional connection for this kind of user data transfer. Thus, only two messages are needed in total for the user data exchange in both directions.

**SD:** CIP Safety is the only protocol that allows the same data to be evaluated simultaneously by multiple recipients using multicasts. However, the number of recipients is limited to a maximum of 15.

**FC:** In a request-response communication, the response message represents the acknowledgment that the request has been received. The absence of a response is time-monitored. Only one request message may be pending for acknowledgement in a request-response communication corresponding to a flow control with window size 1.
With CIP Safety being producer-consumer based, the safety layer monitors the connection by periodically transmitting confirmation packets in the opposite direction to the user data transmission. However, these confirmation packets are not used for flow control of user data packets.

**RT:** The retransmission of messages only take place with protocols that use TCP/IP for the transmission of management frames. Process data, on the other hand, is never retransmitted.
The OPC UA Safety and CIP Safety protocols have many layers, even when transferring process data. One of these layers is IP, which enables routing of process data through various networks including wireless. One drawback of the many layers is that the ratio of user data to administration data is less favorable than with other protocols.

## SAFETY PROTOCOLS IN A WIRELESS ENVIRONMENT

A few typical application scenarios with different safety protocols are presented below. FSoE is not considered here, as the EtherCAT transport layer is unsuitable for wireless transmission. The examples serve to give an idea of the data volume and the differences between the various protocols. Therefore, an optimal environment is assumed.

For example, the 802.11 retransmissions that frequently occur are neglected as well as non-safety communication on the wireless media. It is assumed that the full bandwidth of an access point is available and used for the transmission of the safety process data.

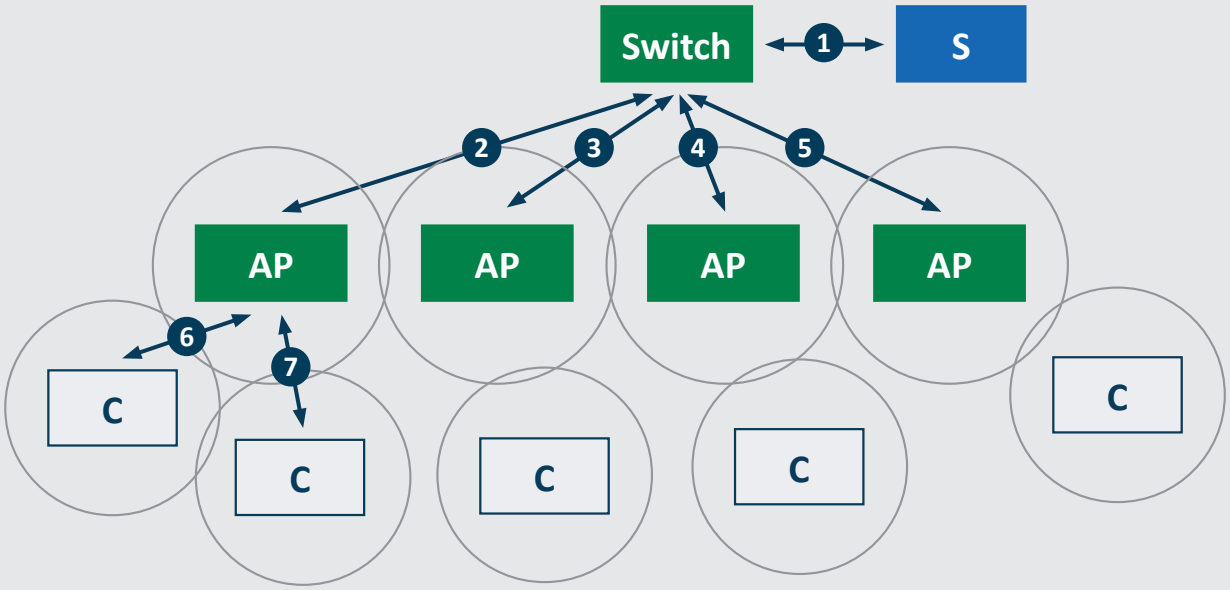


*Figure 3: Wireless network for unidirectional transmission*

### Unidirectional safety data transmission

The figure above shows a wireless LAN consisting of access points (AP), clients (C), server (S), and switch. The APs bridge wireless 802.11 and wired Ethernet. They are connected via a central switch to the server (see Figure 3).

In this example, a safety emergency stop signal is transmitted from the server (PLC) to the clients. By nature of the emergency stop signal, this safety process data is transmitted unidirectionally at a high data rate to achieve quick, safe reaction times.

**CIP Safety**

Because CIP Safety only supports at most 15 consuming clients for a multicast safety connection, we assume that all CIP Safety connections are singlecast and thus each client shall use an individual communication channel to the server. Given **n** clients, n consuming singlecast safety connections are established. As a result, **n** bidirectional EtherNet/IP connections and thus n UDP/IP connections are maintained.

With **m** Access Points and an equal distribution of the clients to the APs, the wireless communication channel (6),(7) between the clients and a single AP transmits **2 n/m** 802.11 frames sequentially per process data cycle.

The wired channels (2)-(5) between an AP and the switch each transmit **2 n/m** Ethernet frames. The wire (1) between switch and server transmits **2 n** Ethernet frames.

Example: n=100 n/m=20-> m=5-> there are 40 802.11 frames per radio cell and cycle. With a frame size of 70 bytes (most of which are framing bytes) and a net throughput rate of 20 Mbps (Anybus Wireless Bridge from HMS [AWB3000]), a cycle time of about 1 ms can be achieved.

The confirmation messages can be transmitted at a lower rate than the user data. In this case, the amount of data within a radio cell is reduced accordingly. **The cycle time can in theory approach 0.6 ms.**

What has not been taken into account so far are the additional acyclic frames for establishing the CIP Safety connections required in case of broken connections.

**PROFIsafe**

PROFIsafe uses bidirectional connections regardless of the process data transfer directions. This means, in case of a unidirectional process, data flows half of the Request-Response communication messages are sent empty (without process data). Given n clients, **n** consuming singlecast safety connections are established by the server (Master). As a result, **n** bidirectional PROFINET connections and thus **n** Ethernet connections are maintained.

The distribution of clients and data volume to the radio cells is the same as in the example for CIP Safety above.

Example: n=100, n/m=20-> m=5-> there are 40 802.11 frames per radio cell and cycle. With a frame size of 33 bytes (most of which are framing bytes) and a net throughput rate of 20 Mbps (Anybus Wireless Bridge from HMS [AWB3000]), **a theoretical cycle time of about 0.5 ms can be achieved.**

The data volume of PROFIsafe is almost the same as that of CIP Safety. The disadvantage of PROFIsafe, that packets are sent with the same cycle time in the opposite direction of the user data transmission, is offset by the advantage that PROFIsafe uses less framing data than CIP Safety.

### OPC UA Safety

Like PROFIsafe, OPC UA Safety uses bidirectional messages for each data connection regardless of the application data transmission direction. This means two messages are involved to transmit one safety user data packet. In case of unidirectional data communication OPC UA Safety sends half of the request-response messages without process data, just like PROFIsafe. However, the overhead of framing bytes is higher than with PROFIsafe.

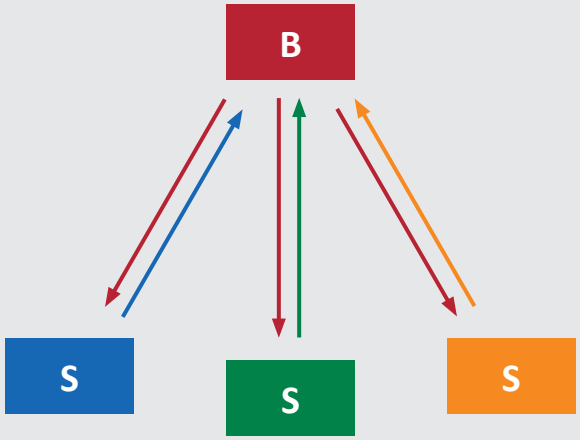


*Figure 5: Data communication via broker*

### Bidirectional safety data transmission

In this scenario, data is to be exchanged between the stations (S) of a wireless network using bidirectional connections. So, data is to be transmitted from each station to each station (see Figure 4).

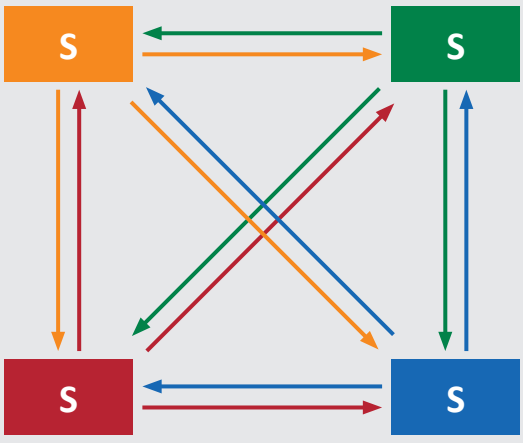


*Figure 4: Fully meshed bidirectional data transfer*

This leads to a very high volume of data. A central data "broker" can be used to reduce this volume of data (see Figure 5). With the broker concept, there is only one bidirectional connection between each station and the broker, which reduces the overall number of necessary connections for the user data transfer.

Another advantage of this central instance is that the network can be configured centrally and the connection to the stations can be established by a central instance (e.g. the broker B itself). This reduces the performance demands on the stations S.

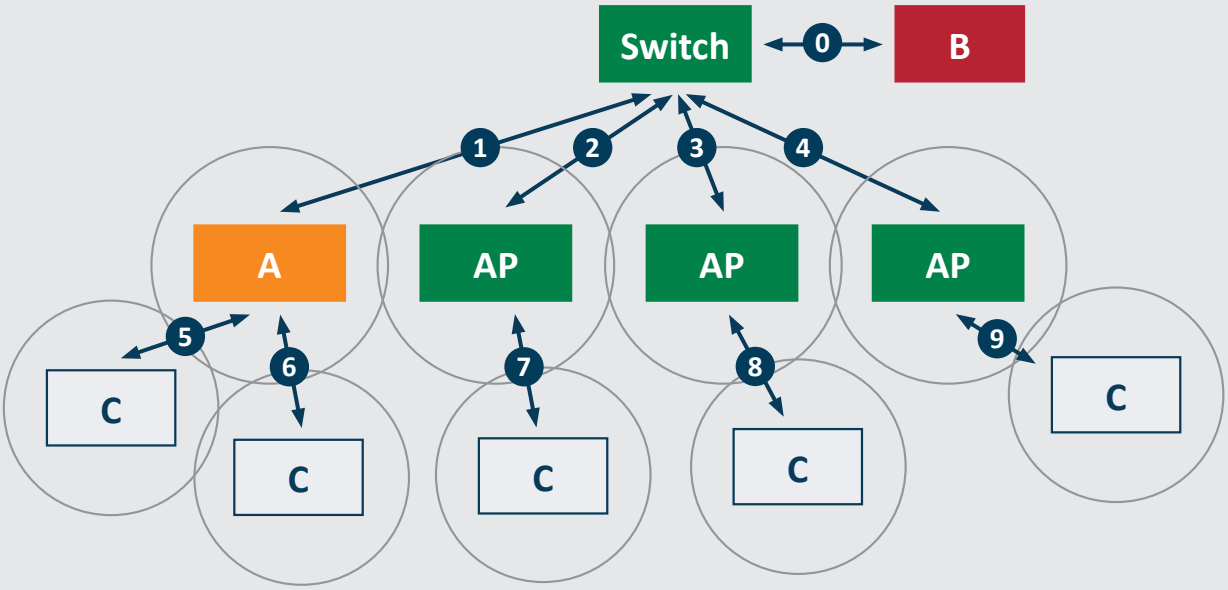


*Figure 6: Wireless network for bidirectional data exchange*

Figure 6 shows a wireless LAN consisting of access points (AP), clients (C), controller (B) and switch. In this example, the stations are meant to share safe application data among each other, such as their 4-byte position values. This kind of data exchange can be realized by using a central controller, a data "broker" B. This broker collects all data from the clients and is able to send the collected data out to all relevant clients again. So, in a first step, the broker B collects the position values of all clients C. Then it assembles a process image with all collected position values and transmits this to all clients. Depending on the maximum supported packet size of the safety protocol, this process image must be split into several smaller safety frames by the broker.

**CIP Safety**

We assume again that all CIP Safety connections are singlecast. With n clients, n producing singlecast safety connections are established for the data transmission from the clients to the broker and n producing singlecast safety connections are established for the data transmission from the broker to the clients (Figure 7).

As a result, **2n** bidirectional EtherNet/IP connections and thus **2n** UDP/IP connections are maintained. The process data is transmitted with a high frame rate. In the following, we assume that the frames that are transmitted in the opposite direction to the process data have a significantly lower transmission rate. Therefore, these frames were not considered here.

Each client sends only a single frame to the broker (this is the positive effect of the broker approach). With m access points and an equal distribution of the clients to the APs, all n/m clients of the radio cell A send their IP frame to the broker. This requires n/m 802.11 frames (5), (6).

The broker collects the safety data of all clients and sends them to all clients in a number of safety packets. Each AP therefore receives c*n/m IP frames, where c is the number of frames into which the broker's process image data is split. These will be converted to c*n/m 802.11 frames.

Thus, within a radio cell (c+1)*n/m 802.11 frames are transmitted per process data cycle.

Example n=100, n/m=20-> m=5, the broker wants to send approx. 400 bytes-> these bytes are transmitted with two CIP Safety frames due to the CIP Safety user data limit of 250 bytes per packet-> c=2. Every CIP Safety packet transports the user data and its complement. There are 60 802.11 frames per radio cell and cycle. With a number of 400 bytes received from the broker plus framing bytes including the complement, a frame size of approx. 80 bytes transmitted by the clients to report their safe application data and a net throughput rate of 20 Mbps (Anybus Wireless Bridge from HMS [AWB3000]), **a theoretical cycle time of about 8 ms can be achieved**. This is the update rate of the complete safety process image. The split transmission of the process data reduces the effective cycle time of the packages by about two times . The broker must therefore open safety connections with a cycle time of about 4 ms.

The confirmation messages in the opposite direction of the process data were not taken into account here. However, the administration effort for a bidirectional transmission is twice as high as for a unidirectional connection.

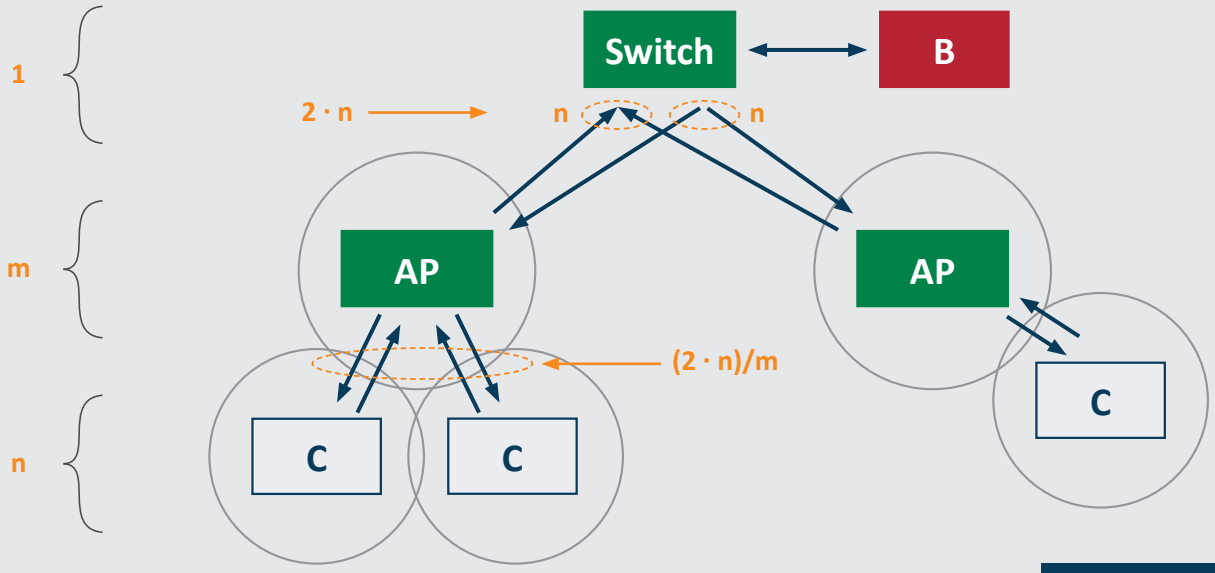


*Figure 7: Message count with bi-directional data exchange for CIP Safety*

**PROFIsafe**

PROFIsafe uses bidirectional connections for the process data transfer. Given n clients n singlecast safety connections are established. As a result, **n** Ethernet connections are maintained (see Figure 8).
PROFIsafe only supports a maximum of 123 bytes of process data per frame. The splitting factor is greater than with CIP Safety. In addition, all frames must be confirmed. This results in a significantly higher number of frames per cell to transfer the safety data process image.

Example n=100, n/m=20-> m=5, the broker wants to send approx. 400 bytes-> these bytes are transmitted with four PROFIsafe frames due to the PROFIsafe user data limit of 123 bytes per packet-> c=4. We assume that the clients send their position values with the response frames of the received broker frames. There are 80 received 802.11 frames and 80 transmitted response frames per radio cell and cycle. With a number of 400 bytes  received from the broker plus framing bytes, a frame size of approx. 30 bytes transmitted by the clients and a net throughput rate of 20 Mbps (Anybus Wireless Bridge from HMS [AWB3000]), **a theoretical cycle time of about 5ms can be achieved**. This is the update rate of the safety process data image. The split transmission of the process data image reduces the required cycle time of the packages by about four times. The broker must therefore open safety connections with a cycle time of about 1ms.

The result is better than that of CIP Safety. However, it must be taken into account that 802.11 has to send more acknowledgment frames due to the higher number of PROFIsafe messages.

**OPC UA Safety**

Like CIP Safety, OPC UA Safety uses two bidirectional connections to transfer user data in both directions between two nodes. In total four messages are involved in the transmission of user data in this example. However, the messages involved must always be transmitted with the same cycle time for each transmission direction of a user data packet. In contrast, CIP Safety allows a different cycle time for the messages involved in a bi-directional data exchange. In addition, the overhead for framing bytes is higher with OPC UA Safety than with CIP Safety and PROFIsafe.

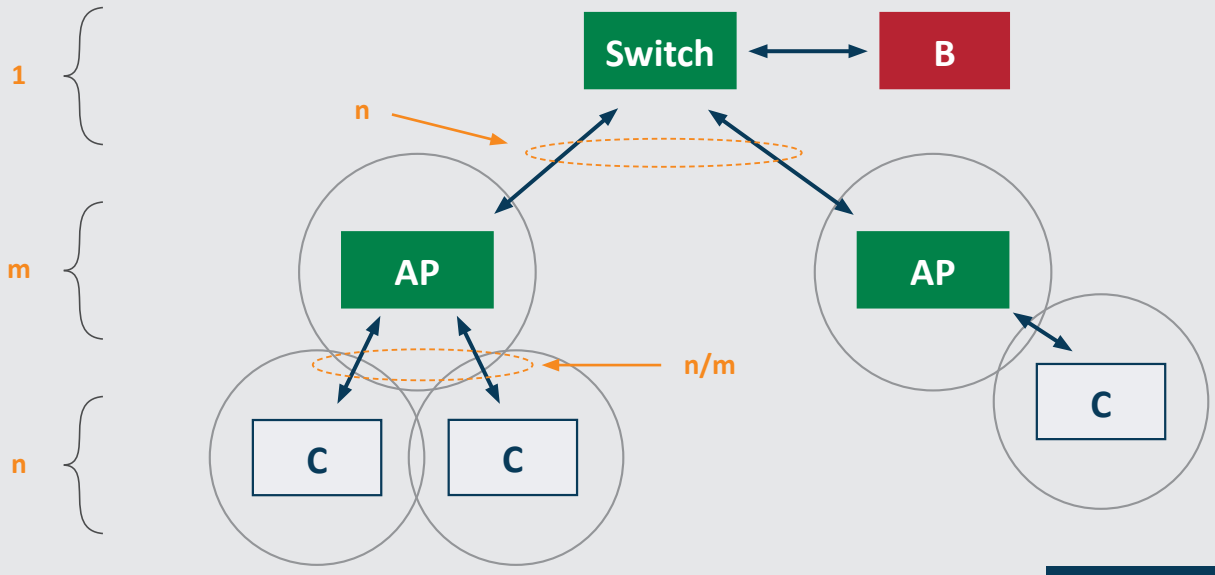


*Figure 8: Message count with bi-directional data exchange for PROFIsafe*

## Conclusion

The safety protocols presented here all have their advantages and disadvantages. The advantages of CIP Safety lie in the weighting of process data and monitoring data. Added to this is the routing capability of the process data due to the use of standard IP-layer. Some disadvantages are the doubling of the user data, the extensive framing information and the management of two connections for bidirectional data transmission. The explicit connection management of CIP Safety also leads to an increased data traffic when establishing the connection e.g. when dropping a connection, due to a disturbed wireless connection.

PROFIsafe has a lower overhead of framing information but require the transmission of data in both directions with the same frequency. Routing is also not supported due to the lack of the IP addressing layer.

All protocols allow the timeout parameters to be adjusted to the generally larger latencies caused by the wireless medium.

To achieve the maximum performance and stability of a safety wireless network, a set of parameters and architectural decisions is to be considered. As shown above, application data relations do also influence the achievable communication cycle times depending on the used safety protocol.

The cycle times of the examples given above are of theoretical nature to show the general impact of the safety protocols themselves as well as the data communication directions. In essence, the full wireless bandwidth is not used for the safe data exchange, and re-transmissions due to temporarily bad wireless connections must also be considered. Real-life networks with CIP Safety or PROFIsafe over wireless typically use cycle times that are 10 to 100 times higher than the theoretically possible ones to obtain a stable safety data connection.

## References

[1] OPC UA Safety: Functional Safety Communication with OPC UA, Version 1, September 2022, https://opcfoundation.org/wp-content/uploads/2022/09/OPCF-OPCUA-Safety-EN.pdf

[2] OPC UA Online Reference, Part 15 Safety, https://reference.opcfoundation.org/Safety/docs/#5

[3] HMS, Whitepaper, Wireless technologies for industrial communication, https://www.anybus.com/products/wireless-solutions/wireless-wp