Ultra Wideband Wireless Communication for Real-Time Control

by

Daniel M. King and Bradford G. Nickerson

Technical Report TR16-238

May 24, 2016

Faculty of Computer Science
University of New Brunswick
Fredericton, N.B. E3B 5A3
Canada

Phone: (506) 453-4566
Fax: (506) 453-3566
E-mail: fcs@unb.ca
http://www.cs.unb.ca

Contents

List of Abbreviations

ALARP	As Low As Reasonably Practicable
BPM	Burst Position Modulation
BPSK	Binary Phase-Shift Keying
CAP	Contention Access Period
CFP	Contention Free Period
CRC	Cyclic Redundancy Check
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DS-SS	Direct Sequence Spread Spectrum
EIRP	Effective Ssotropically Radiated Power
FCS	Frame Check Sequence
GTS	Guaranteed Time Slot
HART	Highway Addressable Remote Transducer
IC	Integrated Circuit
IR	Impulse Radio
LFSR	Linear Feedback Shift Register
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Media Access Control
O-QPSK	Offset Quadrature Phase-Shift Keying
OD	Ordinary Device
PAN	Personal Area Network
PDU	Protocol Data Unit
PER	Packet Error Rate
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PHR	Physical Header
PLC	Programmable Logic Controller
RD	Root Device
TDMA	Time Division Multiple Access
UWB	Ultra-Wideband

Chapter 1

Industrial Communication Networks

1.1 Control Networks

Many industrial processes use control networks for automating a plant, process, or machine. A common type of control system is a *closed loop* where the controller adjusts the process based on feedback read from sensors. Figure 1.1 shows the schematic for a closed loop control system. A control loop may consist of a single sensor and actuator pair for a simple machine such as a temperature sensor and heating element for a water boiler, to many different sensor and actuator devices for a large automated factory.

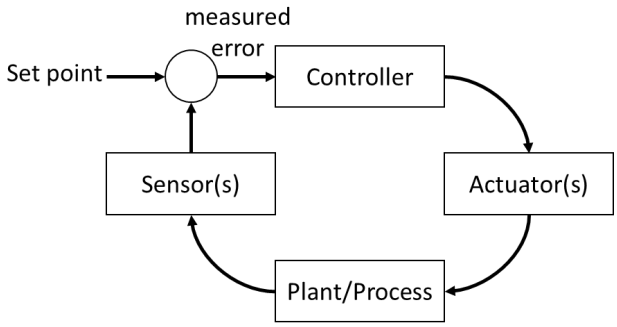


Figure 1.1: A closed control loop.

For larger control systems the sensors and actuators are connected to the controller via a network. Sensors transmit their readings at periodic intervals to the controller, which calculates the necessary adjustments and sends the adjustments to the relevant actuators.

1.2 Plant Hierarchy

Within an industrial plant or factory there is a hierarchy of networks for connecting the various processes and systems for centralized control,shown in Figure 1.2. At the lowest level are individual sensors and actuators connected to a controller at the process level,

such as a programmable logic controller (PLC). These lowest levels of automation are based based on a variety of technologies, such as wired fieldbus or wireless mesh networks. The controllers are connected with PCs and other intelligent devices at the cell level and are closer to computer networks [1].

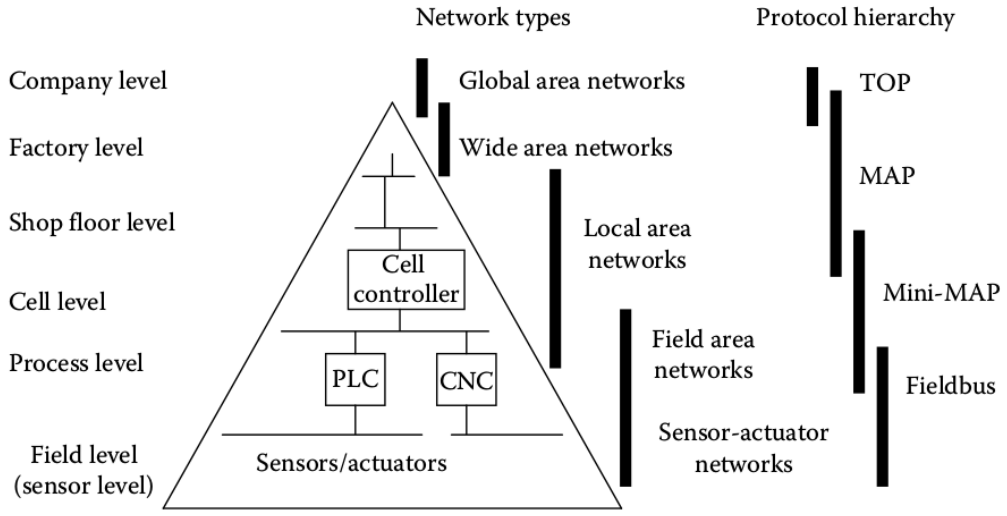


Figure 1.2: Hierarchical network levels in automation and original protocols (from [1]).

1.3 Wired Networks

Wired industrial networks are typically based on a Fieldbus, which consists of a network of several heterogeneous devices such as sensors, actuators, and control devices connected on a common wired bus. The term Fieldbus is the name of collection of protocols and specifications standardized by IEC 61158 [2] and IEC 61784-3 [3].

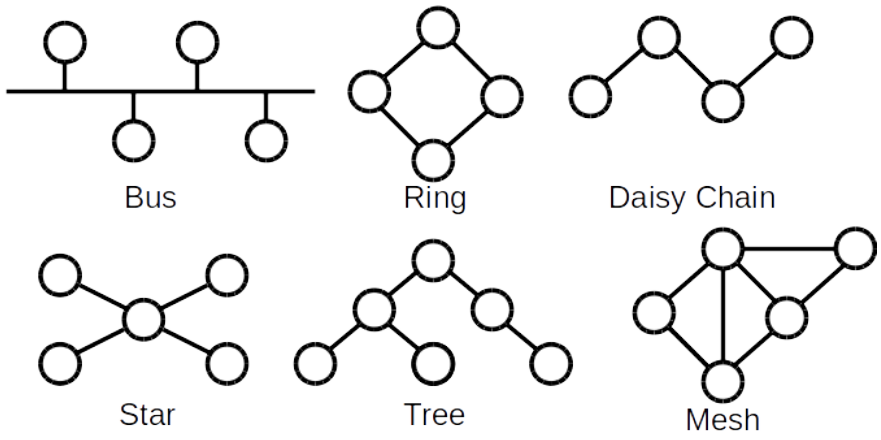


Figure 1.3: Network topologies used in Fieldbus systems.

Fieldbus has existed for 30 years. During this time there have been a variety of fieldbus standards based on different protocols and physical layers, such as RS-485, Ethernet, and optical fiber [4]. Some examples of network topologies used in various fieldbusses are shown in Figure 1.3.

In a bus network there are multiple devices that must share access to the network medium. Sharing access to the medium is handled by the media access control (MAC) layer at the data link layer (DLL) of the OSI model. The MAC layer protocols are usually based on a form of time division multiple access (TDMA), although code division multiple access (CDMA) and frequency division multiple access (FDMA) are also used [1]. Within TDMA there are four strategies:

- *Polling*: the bus master sends a request to a slave device, which then responds with its data. The master then sends a request to the next slave, and so on. This is repeated cyclically.
- *Token-based*: a logical token is passed between devices on the network. Only the device that owns the token is permitted to transmit on the network. The protocol contains mechanisms to manage lost, duplicate, or corrupted tokens.
- *Time slot based*: the bus cycle is divided into fixed-sized time slots, during which one device is permitted to transmit. Slave devices are configured to transmit during a particular time slot. The beginning of the time slot is synchronized by the bus master, after which the slave devices transmit their periodic data during their respective time slot. Aperiodic data may be sent at predetermined periods during the bus cycle outside of the normal periodic data time slots as illustrated in Figure 1.4.
- *Random access*: devices attempt to transmit whenever they have data that they need to send. Contention between devices is mitigated using carrier sense multiple access (CSMA) techniques to detect and avoid collisions.

1.4 Wireless Networks

Wireless networks are becoming more common in industrial automation as a compliment to wired networks. The use of wireless technologies in an industrial context has certain advantages as described by Åckerberg *et al.* [5], such as improved flexibility, scalability, efficiency, and cost reduction.

Although wireless brings several advantages, in some applications electrical power from a mains supply is not feasible, in which case the wireless device is battery powered. The battery lifetime is an additional aspect to consider in such scenarios, as battery lifetimes can range from a few months to 10 years [6, 7] depending on the device, its conditions, and the update frequency.

Another challenge for wireless networks is that they typically experience a higher bit error rate (BER) (e.g. 10^{-2} to 10^{-6}) than wired networks [8]. For comparison, the BER of a

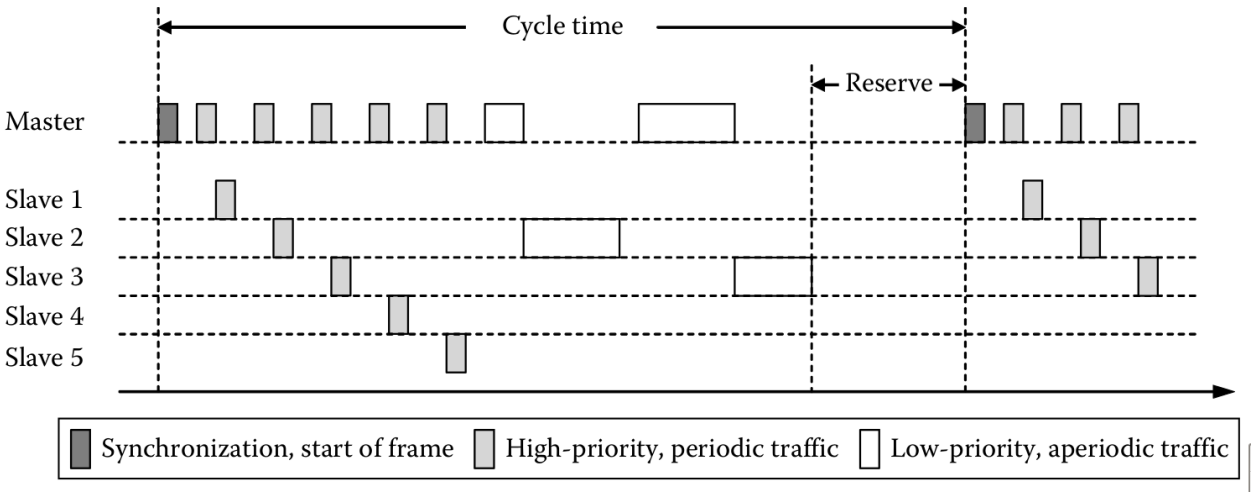


Figure 1.4: PROFIBUS-DP bus cycle (from [1]).

shielded twisted-pair telephone cable is typically 10^{-5}, with a BER of 10^{-12} typical for fiber optic cable [9].

Two major wireless protocols used in industrial automation networks are WirelessHART and ISA100.11a. These protocols are introduced in the following sections.

1.4.1 WirelessHART

WirelessHART is a wireless extension to the highway addressable remote transducer (HART) protocol, a wired protocol. The physical layer of WirelessHART is defined for the 2.4 GHz ISM band, and is based on IEEE 802.15.4-2006 with some modifications to improve reliability in an industrial context [10].

The multiple access technique used in the WirelessHART data link layer is time division multiple access (TDMA). A link between two devices in the network is allocated a *time slot* during which the two devices can communicate. Within the time slot the source sends the data link protocol data unit (DLPDU) and the destination sends back an acknowledgement frame upon successful receipt of the DLPDU. The time slots are grouped together into *superframes* which are continuously repeating, as shown in Figure 1.6. This mechanism provides deterministic communication for the devices in the network, and avoids interference between devices on the network. The use of time slotting differs from wired HART which uses token-based TDMA.

Channel hopping is also used in addition to the TDMA mechanism, where each time slot uses a different wireless channel. The hopping mechanism uses a combination of the absolute time slot index (from the time of network creation) and a channel offset to determine the channel to use for a particular time slot. Channels can be manually blacklisted in the network, which will prevent those channels from being used by the channel hopping mechanism. This can be useful for avoiding interference with crowded channels.

WirelessHART uses a mesh topology at the network level to route messages through the

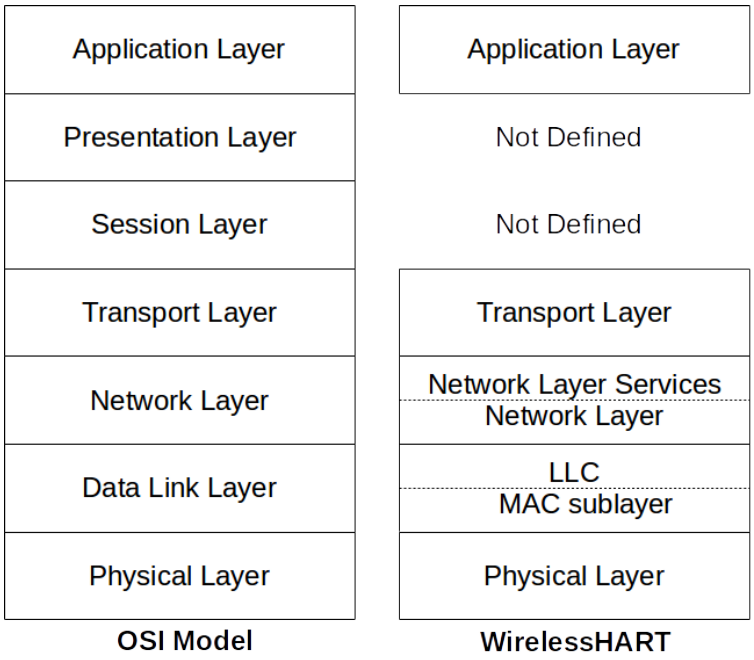


Figure 1.5: The WirelessHART protocol stack (adapted from [11]).

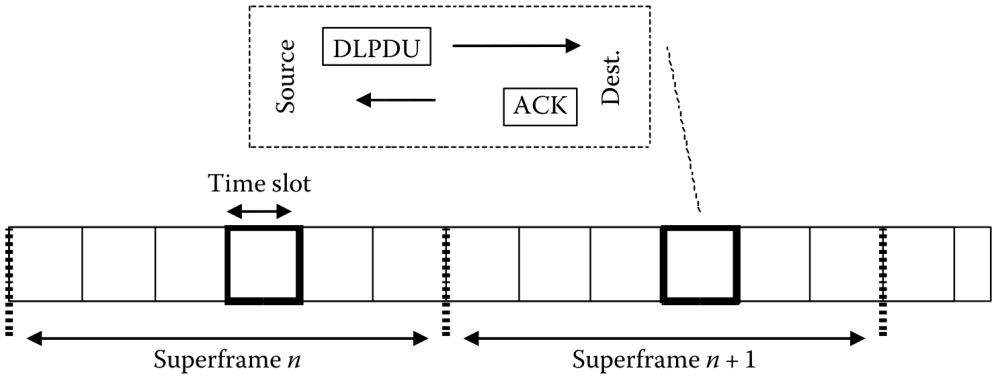


Figure 1.6: The WirelessHART TDMA mechanism (from [10]).

network. The node density of the network can affect the end-to-end delay of messages and the throughput, so the network performance depends on the installation.

Each WirelessHART network has the following elements, as shown in Figure 1.7.

- The *Gateway* bridges the WirelessHART network with the control network.
- The *Network Manager* manages the configuration of the network: allocation of time slots and channel offsets, and monitoring of the network.
- The *Field Devices* are the various sensors and actuators that are connected to the plant.

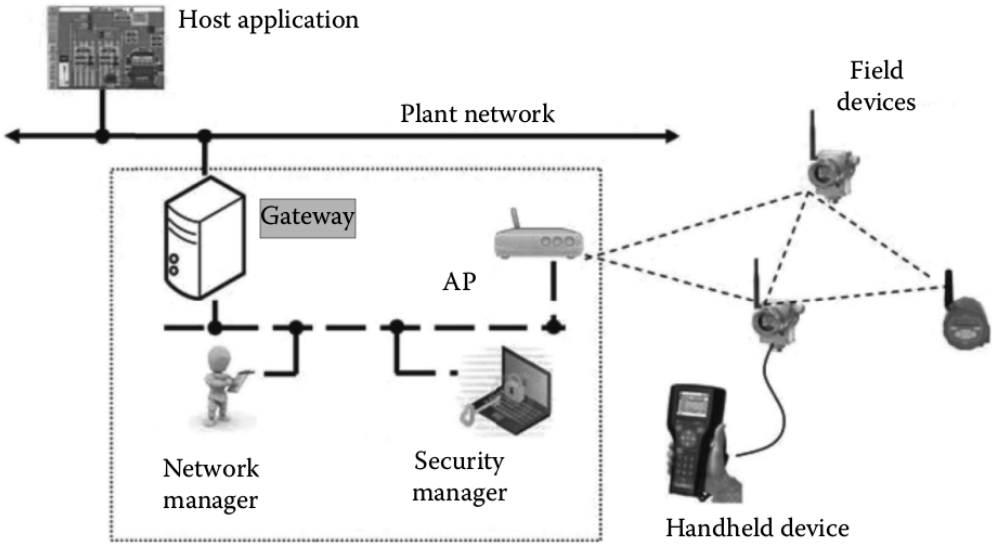


Figure 1.7: A WirelessHART network (from [10]).

- The *Security Manager* handles the distribution of security keys to devices in the network, and controls which devices are allowed to join the network.

The performance of WirelessHART in an industrial environment was investigated by Åckerberg *et al.* in [12]. Their results show an estimated BER of $2.7 \cdot 10^{-4}$ in a close line-of-sight scenario, and $1.2 \cdot 10^{-3}$ at a distance of 42 m non-line-of-sight with many obstacles. The average round trip times of the network in these scenarios is 4.2 ± 1.7 s and 4.8 ± 3.3 s respectively.

1.4.2 ISA100.11a

ISA100.11a is another wireless standard for industrial automation, specified by the ISA100 standards committee. Like WirelessHART, the ISA100.11a physical layer is based on IEEE 802.15.4 in the 2.4 GHz ISM band, with some modifications. The modulation mechanism is direct-sequence spread-spectrum (DS-SS) with offset quadrature phase-shift keying (O-QPSK).

The ISA100.11a protocol stack is shown in Figure 1.8. As with WirelessHART, ISA100.11a does not define presentation or session layers. The data link layer is similarly split into sublayers. In ISA100.11a the data link layer is split into three sublayers. The MAC sublayer is a subset of the MAC layer defined in IEEE 802.15.4, which is also extended by the MAC extension sublayer. The upper data link layer manages the mesh networking, unlike the definition of the data link layer in the OSI model [11].

The data link layer uses the time slotted superframe structure that is common in industrial network protocols. Channel hopping is also with three supported modes: fast hopping, slow hopping, and hybrid hopping. In fast channel hopping the channel is changed after each time slot, whereas in slow channel hopping the same channel is used for a contiguous

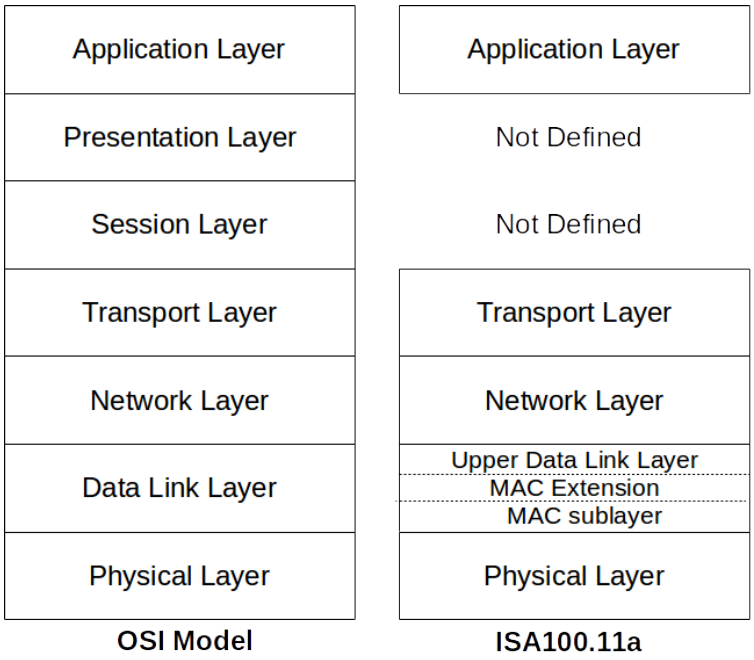


Figure 1.8: The ISA100.11a protocol stack (adapted from [11]).

number of time slots before changing. This is demonstrated in Figure 1.9. Hybrid channel hopping alternates between slow and fast channel hopping for a fixed number of time slots.

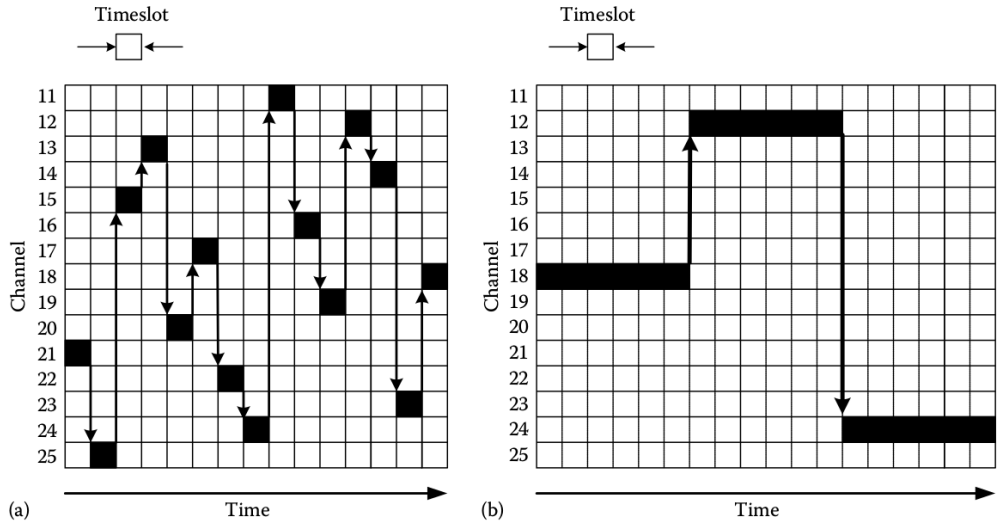


Figure 1.9: Fast (a) and slow (b) channel hopping in ISA100.11a (from [13]).

Whereas WirelessHART requires channels to be blacklisted manually, ISA100.11a can autonomously blacklist channels that experience more noise or interference.

ISA100.11a uses a mesh network topology, where each node in the network implements one or more *roles*. The following roles are defined in ISA100.11a [13] and are shown in

Figure 1.10:

- *I/O devices* are the sensors and actuators that are connected to the plant. These devices do not perform message routing.
- *Routers* are responsible for forwarding and routing messages within the mesh network.
- *Provisioning* devices provision other devices to join the network.
- *Backbone routers* bridge the wireless network with the backbone network and route messages between them.
- The *Gateway* bridges the wireless network with the plant network.
- The *System Manager* manages the network, devices, and communications.
- The *Security Manager* is responsible for ensuring secure communications within the network.
- The *System Time Source* is the master clock and time source for the network.

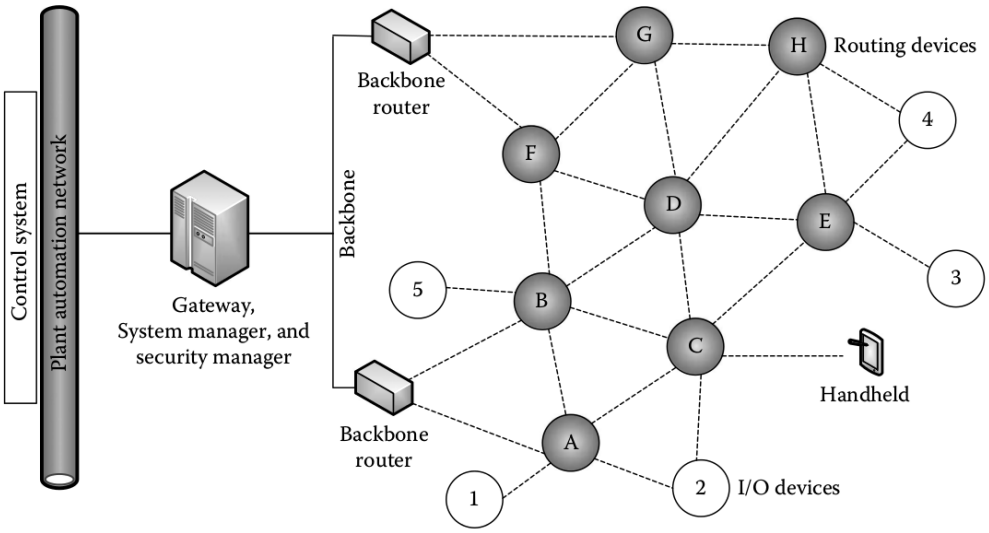


Figure 1.10: An ISA100.11a network (from [13]).

Compared to WirelessHART, ISA100.11a has more configuration options which provides better flexibility. As explained by Petersen and Aakvaag [7]:

> WirelessHART is a rather "simple" specification with very few optional or configurable parameters. ISA100.11a on the other hand, is a complex and comprehensive specification with many configurable and optional parameters found in different stack layers.

In order to manage this complexity ISA100.11a defines various application profiles to allow devices to fulfil various roles. The profiles define which options are used for the profile to permit interoperability between different ISA100.11a devices implementing the same profile. However, even with profiles, full interoperability issues remain a challenge [11].

1.4.3 Comparison

The following table compares WirelessHART and ISA100.11a:

Feature	WirelessHART	ISA100.11a
Physical layer	2.4 GHz based on IEEE 802.15.4 16 channels DS-SS, QPSK	2.4 GHz based on IEEE 802.15.4 14/15 channels (channel 26 is optional) DS-SS, QPSK
Data rate	250 kbps	250 kbps
Range (approx.)	100 m	100 m
Network topology	Mesh	Star, star-mesh, or mesh
Symmetric cryptography	AES-128-CCM	AES-128-CCM
Asymmetric cryptography	None	Optional

Chapter 2

Safety-Critical Communication

2.1 Functional Safety

Functional safety is the management of risk in a system where the failure of the system is unacceptable, for example leading to serious injury or loss of life. IEC 61508 [14] defines safety as the "freedom from unacceptable risk". Many industrial processes such as high-pressure systems, chemical plants, and nuclear power generation are associated with a risk of [15]:

- Loss of life;
- damage to the environment; or
- significant financial damage.

Determining whether a risk is tolerable or unacceptable depends on a variety of factors, such as the amount of injury or death that can occur from a single incident, the degree of controllability over the risk, and the voluntary or involuntary nature of the risk [16]. Ideally, there would be no risk involved, however it is impossible for any system to have zero risk since no system has a zero failure rate and it is impossible to account for every possibility for failure in a system. Many major accidents are caused by a combination of several human and physical factors which are not foreseen by the designers. However, we deal with various risks in every day life, some examples of which are shown in Table 2.1.

Table 2.1: Everday risk of death from various causes (from [16]).

Cause	Accident rate
All causes (mid-life including medical)	1×10^{-3} pa
All accidents	5×10^{-4} pa
Accidents in the home	4×10^{-4} pa
Road traffic accident	6×10^{-5} pa
Natural disasters	2×10^{-6} pa

When designing a safety system the risks must be identified and rated. For risks that are determined to be unacceptable, the risk must be mitigated (e.g. add redundant modules) in order to reduce it to a tolerable level. Ideally, the level of risk would be reduced to as low as possible below the tolerable level. However, reducing the risk to minimal levels normally has a much higher cost than is possible. The principle of establishing whether or not further improvements to risk mitigation are necessary is known as "as low as reasonably practicable" (ALARP).

2.1.1 Standardization

IEC 61508 [14] is a standard for general functional safety, covering the entire system lifecycle, from initial requirements and design through to implementation and testing, deployment, and decommissioning. The previously discussed aspects of risk underly the philosophy of the standard: that there's no such thing as zero risk and that risk should be mitigated ALARP.

IEC 61508 defines six categories for the likelihood of the occurrence of an incident, and four categories of consequences of an incident. These are shown in Tables 2.2 and 2.3.

Table 2.2: IEC 61508 risk categories (adapted from [14, 17]).

Category	Failures per year
Frequent	$> 10^{-3}$
Improbable	10^{-3} to 10^{-4}
Occasional	10^{-4} to 10^{-5}
Remote	10^{-5} to 10^{-6}
Improbable	10^{-6} to 10^{-7}
Incredible	$< 10^{-7}$

Table 2.3: IEC 61508 risk consequence categories (from [14]).

Category	Definition
Catastropic	Many people killed
Critical	Several people killed
Marginal	Major permanent injury to one or more people, or death of one person
Negligible	Minor injury

As a general standard for functional safety, IEC 61508 is the basis of additional industry-specific standards. Some safety standards that are based on IEC 61508 are listed as follows:

- IEC 62304 (Medical devices)
- ISO 26262 (Automotive)
- EN 50128 (Railway software)

- IEC 61513 (Nuclear)
- IEC 62061 (Machinery)

2.1.2 Safety Integrity Levels

The various safety standards have the concept of a safety integrity level (SIL) which defines failure rates for a tolerable level of risk. IEC 61508 [14] defines four SILs (1-4) with SIL 4 as the most dependable and SIL 1 as the least dependable. Each SIL has a set of requirements and objects which must be met during the development of the system in order to meet the acceptable failure rates. For software, these requirements span the software development process to ensure that the risks are successfully identified, understood, and mitigated.

Different safety standards have different SILs, requirements, and objectives. For example, in the DO-178C avionics software standard there are five design assurance levels (DAL) ranging from level A (highest) to level E (lowest). IEC 61508-1 defines four SILs from level 4 (highest) to level 1 (lowest). Although similar, the SIL between the standards do not map directly. For example, the lowest DAL in DO-178C has no effect on the safety of the system and has no additional requirements whereas there is no equivalent SIL in IEC 61508.

The four SILs in IEC 61508 are shown in Table 2.4.

Table 2.4: The IEC 61508 safety integrity levels [14].

SIL	High demand rate Probability of dangerous failure per hour of operation (PFH)	Low demand rate Probability of dangerous failure on demand (PFD)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

Each safety function according to IEC 61508 can have one of two modes of operation depending on the frequency of which the safety function is used. The high demand mode of operation is for safety functions that are used at least once per annum on average, and the low demand mode of operation is for a safety function that is used less than once per annum. A car airbag is an example of a low demand mode device, and a gas sensor is an example of a high demand mode device.

2.2 Functional Safety in Communication

If a communication network is responsible for the transport of safety-related messages then the reliability of the network plays a role in the probability of failure of the safety function. For example, if an emergency stop button is pressed then a message must be sent to the safety host to allow the system to be safely shut down in an acceptable amount of time.

The risk of an error occurring within the network during the transport of the safety-related message must be factored into the overall risk of the system.

There are two classes of errors that can occur within a communication network: *deterministic* and *stochastic* errors. IEC 61784-3 identifies several types of deterministic errors that can occur within a communications network due to an error, fault, or interference [3]:

- *Corruption*: A message is corrupted due to transmission errors or interference.
- *Unintended repetition*: A message is repeated at an incorrect point in time.
- *Incorrect sequence*: Messages arrive at the destination in the incorrect order.
- *Loss*: A message is never received or acknowledged.
- *Unacceptable delay*: A message is delayed beyond an acceptable time window.
- *Insertion*: A message is inserted from an unexpected or unknown source.
- *Masquerade*: A message is inserted from an apparently valid source. This may cause a non-safety related message to be received and processed by a safety-related entity.
- *Addressing*: A safety-related message is sent to the incorrect safety-related entity.

IEC 61784-3 also defines several remedial measures to address these types of errors [3]:

- *Sequence number*: A sequence number is added to each message that are sent between a source and destination. The sequence number changes for each message in a predetermined way (typically by incrementing the sequence number for each message).
- *Time stamp*: Many messages are only valid for a certain period of time. A time stamp is added to each message to allow the receiver to determine whether or not the message is still valid.
- *Time expectation*: The message destination expects a message to be received within a certain period of time. If the message is not received within this time then an error is assumed. Watchdog mechanisms fall into this category.
- *Connection authentication*: Unique source and destination identifiers are added to each message to identify the relevant safety-related entities.
- *Feedback message*: Also known as *aknowledgements*. The receiver of a message sends a feedback message to the source to acknowledge correct receipt of a message.
- *Data integrity assurance*: Redundant data is added to each message to permit detection of data corruption.
- *Redundancy with cross-checking*: A message is sent more than once, possibly using different media and protocols. The receiver cross-checks the messages and if there is a difference then an error is assumed.

The remedial mesaures can address more than one type of deterministic error. The errors addressed for each remedial measure are shown in Table 2.5.

Table 2.5: Deterministic communication errors and their remedial measures (adapted from [3]).

	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity	Redundancy with cross-checking
Corruption					X	X	
Unintended repetition	X	X					X
Incorrect sequence	X	X					X
Loss	X				X		X
Unacceptable delay		X	X				
Insertion	X			X	X		X
Masquerade				X	X		
Addressing				X			

2.2.1 Relationship with IEC 61508 SIL

Stochastic errors such as pertubed bits caused by interference are usually mitigated in the communication protocols using data integrity assurance mechanisms such as a cyclic redundancy check (CRC). CRCs provide good protection against transmission errors such as burst-errors in a network, but CRCs are not guaranteed to detect all possible combinations of pertubed bits. Some combinations of bit errors in a message (including possibly bit errors in the CRC stored in the message) may result in a valid CRC even though an error has occurred. The situation where an error occurs, but is not detected by the error checking mechanisms is known as a *residual error*.

The probability of a residual error is related to the probability of a bit error occurring and the properties of the CRC polynomial. Generally, a residual error is more likely with a higher bit error probability.

The characteristics of the CRC polynomial also play a role in the residual error probability; a CRC polynomial is either *proper* or *improper*. For a proper polynomial the probability

of a residual error occurring approaches, but does not exceed the limit 2^{-r} as the bit error probability increases, where r is the number of bits in the CRC. For an improper polynomial the probability of a residual error may exceed the limit 2^{-r}. This relationship between bit error probability and residual error probability for proper and improper polynomials is shown in Figure 2.1.

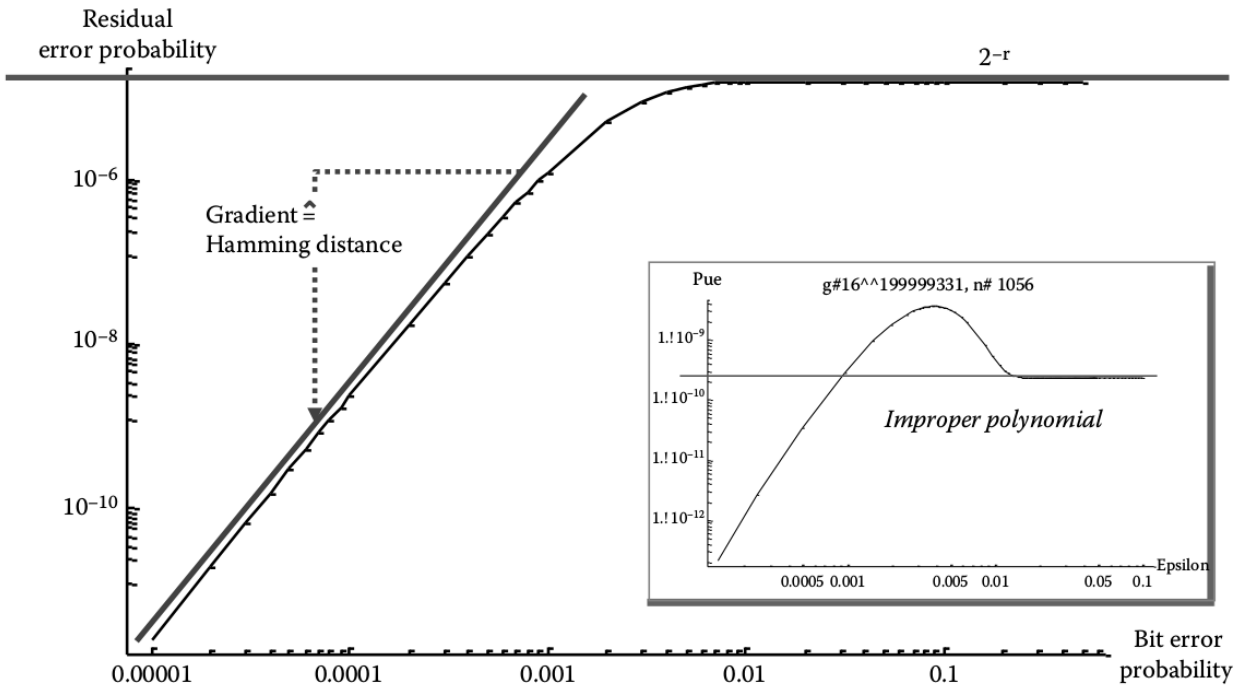


Figure 2.1: Relationship between bit error rate and residual error rate for proper and improper polynomials (from [15]).

The limit on the residual error probability for a proper polynomial used in a safety protocol is important to meet the target SIL. IEC 61784-3 requires that the *residual error rate* of a communication system does not exceed 1% of the target SIL of the safety function, known as the 1% rule. The residual error rate is calculated from the residual error probability with respect to the bit error probability, as shown in Equation 2.1 [3]. The equation items are described in Table 2.6.

$$\wedge_{SL}\ (Pe) = R_{CRC}\ (Pe) \times v \times m \tag{2.1}$$

For example, at SIL 3, the upper limit on the PFH is 10^{-7}. This results in an upper limit for the residual error probability of 10^{-9}.

Since the residual error rate is dependent on the number of devices, m, that receive the safety-related message (including routers and switches), a safety function where many devices receive a safety-related message will require a lower maximum residual error probability to achieve the desired residual error rate. Figure 2.2 shows a safety function with $m = 2$.

Table 2.6: Items for Equation 2.1 (adapted from [3]).

Equation items	Definition
$\wedge_{SL}\ (Pe)$	Residual error rate per hour of the safety communication layer with respect to the bit error probability.
Pe	Bit error probability. Unless a better error probability can be proven, a value of 10^{-2} shall be used.
$R_{CRC}\ (Pe)$	Residual error probability of the CRC with respect to the bit error probability.
v	Maximum number of safety messages per hour.
m	Maximum number of message recipients between the source and destination of the safety function.

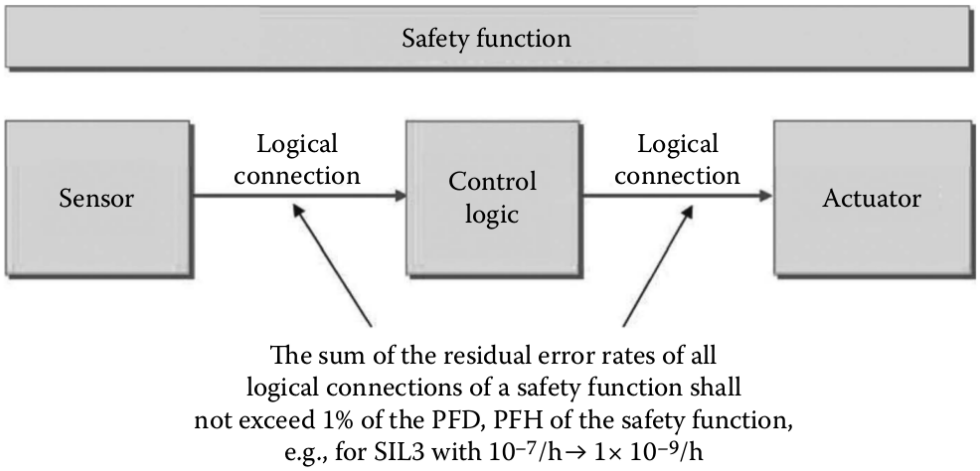


Figure 2.2: The IEC 61784-3 1% rule (from [15]).

2.2.2 PROFIsafe

Although the previously discussed protocols are suitable for normal real-time industrial control, they are not suitable for safety critical applications where there is significant risk [15].

PROFIsafe is an application layer protocol defined in IEC 61784-3-3 [18] which is responsible for the transport of safety-related data within an industrial communication network, and is certifiable up to IEC 61508 SIL 3.

As an application layer protocol PROFIsafe does not specify lower layers of the protocol stack such as the physical and data link layers. Instead, PROFIsafe builds upon the existing PROFIBUS and PROFINET protocols by adding the PROFIsafe application layer above these protocols. With this approach safety devices can be added with minimal changes to existing networks: "what he/she is using, he/she will not be losing" [15]. As a result, PROFIsafe is able to co-exist with other non-safety related functions on the same communication medium, as shown in Figure 2.3.

The protocol layers underneath PROFIsafe are responsible for the transport of the proto-

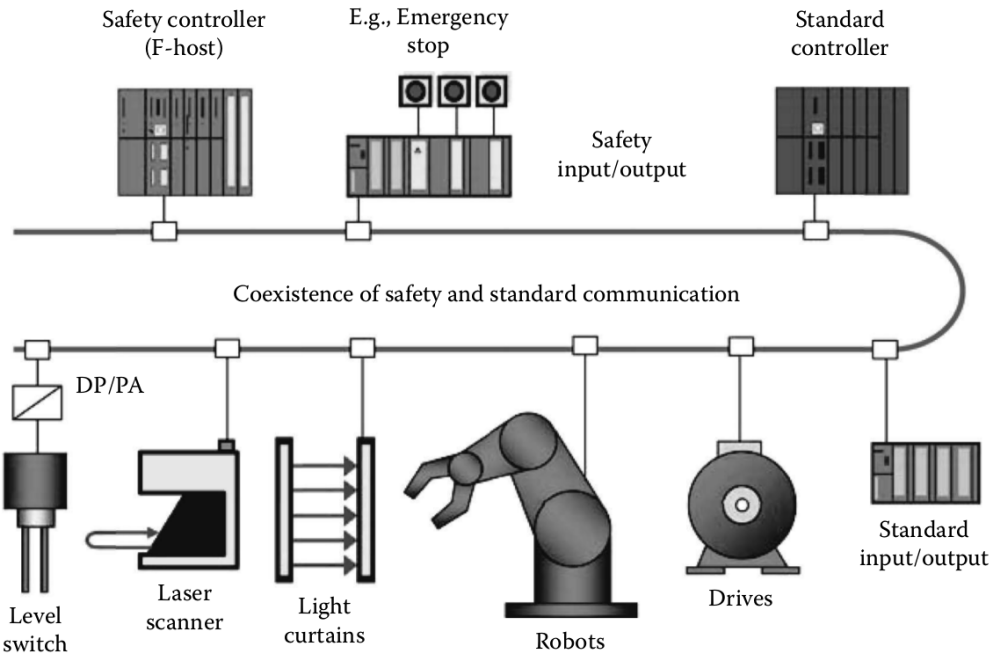


Figure 2.3: The PROFIsafe vision (from [15]).

col data units (PDU) between safety-relevant devices; however, PROFIsafe does not impose additional requirements on the safety or error-checking mechanisms on those layers. Instead, PROFIsafe uses the "black channel" principle (Figure 2.4) where the communication channel between two safety-relevant devices is treated as a black box and is not assumed to be safe. Indeed, PDUs in the black channel may be lost, delayed, or modified during transport.

To ensure the safety of PDUs, PROFIsafe implements the necessary safety measures to meet the requirements for up to IEC 61508 SIL 3.

Although PROFIsafe applies the black channel principle, the residual error rate of the safety layer is dependent on the frequency at which errors occur in the network, including the BER, so the term "grey-channel" [12] is perhaps more appropriate. The fail-safe host monitors the frequency at which detectable errors occur and when the error rate exceeds a certain threshold the system enters a safe state [15]. PROFIsafe messages have a much lower residual error rate, due to the use of two different CRCs [19]; i.e. CRC1 and CRC2.

The process for computing CRC1 and CRC2 are described in IEC 61784-3-3 [18]. The 16-bit CRC1 is computed from the F-Parameters (fail-safe host configuration parameters), including the SIL and watchdog timeout parameters. The CRC1 provides the initial value for the CRC2 computation (24 or 32-bit). The CRC2 is computed over the PROFIsafe frame in reverse byte order. I.e. the MSB of the packet is processed first. This provides better error detection, even if the same CRC polynomial is used within the black channel [18].

PROFIsafe can be successfully used with wireless networks and protocols, such as WirelessHART and PROFINET IO [5, 12]. However, noise and obstacles in industrial environments can cause problems with determinism for wireless communications [12]. To achieve

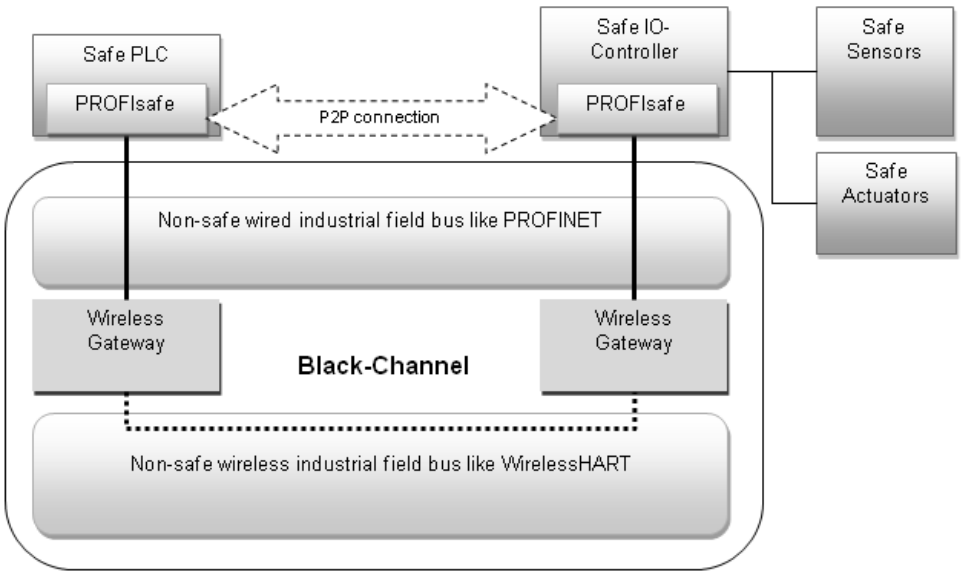


Figure 2.4: The black channel concept (from [5]).

IEC 61508 SIL 3 the BER in a wireless network must not exceed 10^{-2} [12, 3]. PROFIsafe has also been successfully used with ISA100.11a to achieve SIL 2 compliance [20].

2.2.3 SafetyNET p

Other safety protocols do not use the black channel model, but instead define the necessary lower layers of the protocol stack. One such example is *SafetyNET p*, based on industrial Ethernet.

SafetyNET p defines two models of communication based on Ethernet: real-time frame line (RTFL) and real-time frame network (RTFN). RTFL networks are capable of minimum bus cycle times of 62.5 μs with 100 ns jitter [21]. RTFN is suitable where real-time requirements are less strict with a bus cycle time of 1 ms [21].

The RTFL physical network is based on a daisy chain model, shown in Figure 2.5. The root device (RD) initiates the bus cycle by sending an ethernet frame to the first ordinary device (OD). The OD appends its data to the ethernet frame then forwards the frame to the next OD in the chain, which also appends and forwards its data. At the end of the chain the ethernet frame contains the data of all the ODs. The ethernet frame is then transmitted back along the chain through each OD to the RD. Each OD can read any data from that was appended by other OD in the chain as it travels back to the RD.

The protocols for RTFL and RTFN support both cyclic and acyclic data exchanges via two logical channels: the cyclic data channel (CDC) and the message data channel (MDC). Safety-related data is often cyclic so the safety layer is based on the CDC using the black channel model.

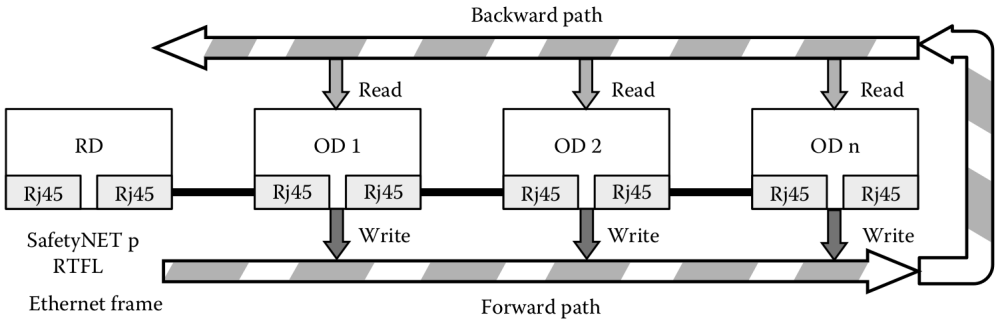


Figure 2.5: SafetyNET p RTFL physical line (from [21]).

2.2.4 CIP-Safety

CIP-Safety is another safety protocol based on the black channel principle, designed as a safety layer on top of the common industrial protocol (CIP) [22]. The common industrial protocol is used in networks such as EtherNet/IP and DeviceNet.

Like PROFIsafe, CIP-Safety implements its own CRC mechanisms to reliably detect bit errors. Data frames in CIP-Safety can have two formats: short format or long format. In both formats a 16-bit CRC is sent for the data along with an additional 16-bit CRC from the inverted (complemented) data [22, 19]. In the long format the frame also contains the inverted data, along with the non-inverted data and the two safety CRCs. The short format does not contain the inverted data alongside the non-inverted data to reduce the overall frame size.

Chapter 3

Ultra Wideband

Ultra-wideband (UWB) radio is the term for radio technology where the aggregate bandwidth is at least 500 MHz when the center frequency f_c is greater than 2.5 GHz, or 20% of the fractional bandwidth when f_c is less than 2.5 GHz, as defined by the Federal Communication Commission (FCC). Under this definition, different radio technologies can be classified as ultra-wideband (such as some OFDM systems). Ultra-wideband radios, however, are commonly based on impulse radio (IR). This chapter focuses on IR as defined by IEEE 802.15.4-2011 [23].

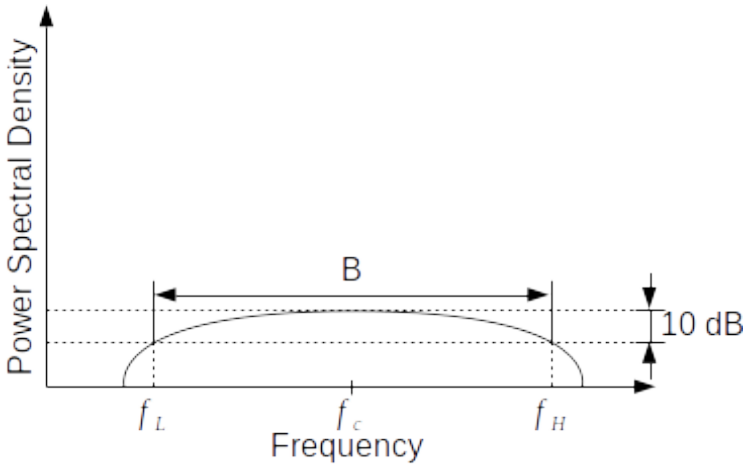


Figure 3.1: Power spectral density of UWB radio (adapted from [24]).

Due to the very wide bandwidth, the power spectral density of UWB signals is very low. This allows UWB signals to share spectrum with other narrowband signals since the energy of a UWB signal at any particular frequency is low enough such that it does not interfere with the narrowband signal [25].

IEEE 802.15.4-2011 [23] specifies physical layers (including UWB) and a media access control (MAC) layer for low-rate wireless personal area networks (LR-WPAN). The MAC layer is further defined in IEEE 802.15.4e-2012 [26].

The IEEE 802.15.4-2011 standard defines three bands of operation for UWB [23]:

- The sub-gigahertz band, occupying the spectrum between 249.6 MHz to 749.6 MHz.
- The low band, occupying the spectrum between 3.1 GHz to 4.8 GHz.
- The high band, occupying the spectrum between 6.0 GHz and 10.6 GHz.

Across the three bands there are fifteen UWB channels specified, shown below in Table 3.1. For each of the bands there is one mandatory channel, and the others are optional. Channel 0 is mandatory for the sub-gigahertz band; channel 3 is mandatory for the low band; and channel 9 is mandatory for the high band [23].

Table 3.1: The UWB channels defined in IEEE 802.15.4-2011 [23]

Channel Number	Center Frequency (MHz)	Bandwidth (MHz)
0	499.2	499.2
1	3494.4	499.2
2	3993.6	499.2
3	4492.8	499.2
4	3993.6	1331.2
5	6489.6	499.2
6	6988.8	499.2
7	6489.6	1081.6
8	7488.0	499.2
9	7987.2	499.2
10	8486.4	499.2
11	7987.2	1331.2
12	8985.6	499.2
13	9484.8	499.2
14	9984.0	499.2
15	9484.8	1354.97

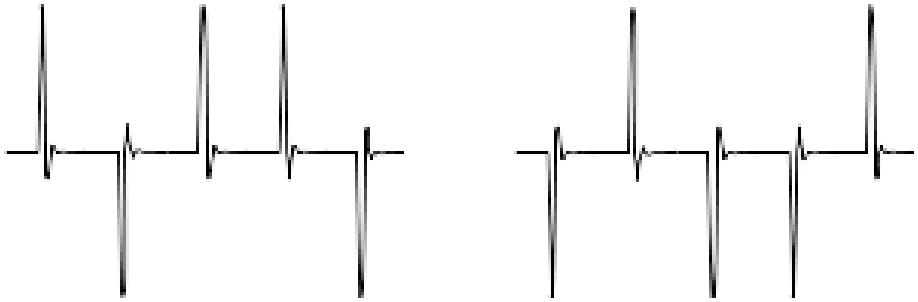
Four standard data rates are supported; i.e. 110 kbps, 850, kbps, 6.81 Mbps and 27.24 Mbps.

3.1 Physical Layer

For each transmitted symbol IEEE 802.15.4 UWB transmits a burst of N_{CPB} UWB chips. The duration of each chip T_c and the number of chips per burst T_{CPB} defines the duration of the burst $T_{burst} = T_c T_{CPB}$. The bursts are modulated using a combination of burst position modulation (BPM) and binary phase-shift keying (BPSK). The combined use of the BPM-BPSK modulation scheme supports sending two bits of information in each symbol: one bit determines the pulse position, and the other bit determines the pulse polarity.

3.1.1 Binary Phase Shift Keying

In the BPSK modulation scheme a data bit is encoded in the polarity of the burst. The burst consists of one or more chips which have a positive or negative polarity as determined by the pseudo-random spreading sequence. The polarity of the burst as a whole is determined by the BPSK modulation bit. An example of a BPSK-modulated burst is shown in Figure 3.2.



(a) Positive burst polarity. (b) Negative burst polarity.

Figure 3.2: BPSK modulation.

The polarity of each chip follows a pseudo-random sequence defined by the spreading mechanism in order to smoothen the spectrum of the transmitted waveform [23]. The spreading mechanism is described in Section 3.1.3.

3.1.2 Burst Position Modulation

The BPM scheme is a time-based modulation scheme. The UWB symbol is transmitted within the duration T_{dsym}, which is separated into two halves $T_{BPM} = T_{dsym}/2$. The BPM bit is encoded by transmitting the UWB burst in one of the two T_{BPM} durations, as shown in Figure 3.3.

IEEE 802.15.4 further divides each T_{BPM} duration into two halves as shown in Figure 3.4. UWB bursts are only transmitted in the first half of the T_{BPM} duration, as the second half acts as a guard interval to mitigate the effects of multipath interference [23].

The T_{BPM} duration is further segmented into multiple possible *burst positions*. In each symbol the UWB burst is transmitted in one of the possible burst positions. The burst position can vary on a symbol-to-symbol basis following a time hopping (TH) code. Out of the possible burst positions in the symbol duration only a subset of burst positions of length N_{hop} are considered for transmitting the burst.

3.1.3 Spreading

The use of TH provides resistance to multi-user interference when each user has their own TH code. The time-varying pseudo-random sequences used for the chip polarity and burst position TH is derived from a linear feedback shift register (LFSR) clocked N_{cpb} times for

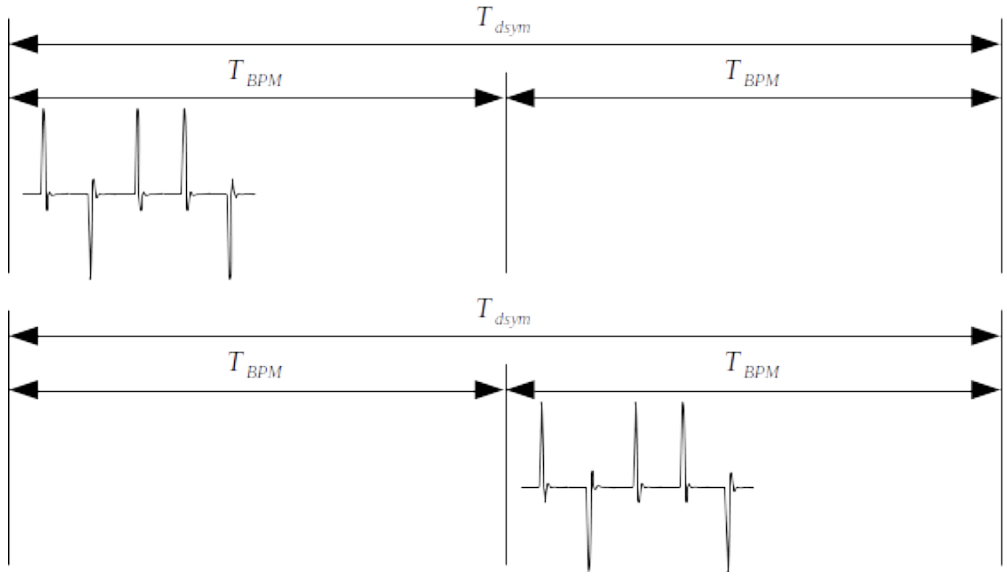


Figure 3.3: UWB burst position modulation.

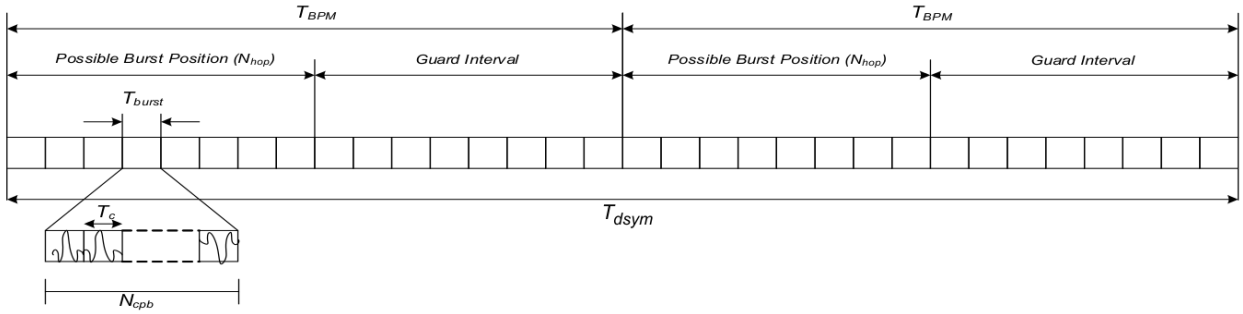


Figure 3.4: IEEE 802.15.4-2011 BPM with time hopping (from [23]).

each symbol. The initial state of the LFSR is determined by the unique preamble code to ensure that the pseudo-random sequence is unique for each user.

The preamble sequence at the beginning of each physical frame transmission consists of a sequence of symbols from the ternary alphabet $-1, 0, +1$, corresponding to a negative-polarity pulse, no pulse, or a positive polarity pulse respectively. The preamble sequence permits the receiver to detect the presence of an UWB frame by its perfect periodic auto-correlation properties. IEEE 802.15.4 defines 8 mandatory ternary codes of length 31, and a further 16 optional codes of length 127. The codes are chosen for each channel to minimize their cross-correlation [23] to reduce multi-user interference.

3.2 Media Access Control Layer

The MAC layer defined in IEEE 802.15.4 is responsible for transmitting and synchronizing beacon frames and reliable data transmission. The MAC organizes the network as a personal area network (PAN) in a star or mesh network topology. Within the PAN there are two types of devices: devices and a coordinator. The coordinator is responsible for managing the PAN; it allows devices to associate and disassociate from the PAN, and transmits the beacon frames to allow the devices to synchronize on the network.

The PDU format of the MAC layer is shown in Figure 3.5 and contains three parts: the MAC header, the payload, and the MAC footer. The header contains information on the frame type, sequence numbering, addressing, and security information. The MAC footer contains a 16-bit frame check sequence (FCS) for error detection. Some fields in the MAC header are variable-length (e.g. address fields may be 2 or 8 octets in length), or may be omitted for some frames.

<table>
<tr><td>Octets: 2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>0/5/6/10/14</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Security Header</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="7">MHR</td><td>MAC Payload</td><td>MFR</td></tr>
</table>

Figure 3.5: IEEE 802.15.4 MAC layer PDU format (from [23]).

The MAC layer uses time slot-based TDMA which is common in industrial communication protocols. The PAN coordinator transmits beacon frames at periodic intervals which mark the start of the *superframe* structure. The layout of a superframe is shown in Figure 3.6. The superframe consists of two parts: the active period and the inactive period. During the inactive period no communication takes place and the coordinator is able to enter a low-power mode. The various durations within the superframe such as the beacon interval and time slot duration are configurable for each PAN.

During the active portion of the superframe there is a contention access period (CAP) and a contention free period (CFP) which are divided into time slots of equal size. During the CAP devices compete for access to the channel based on carrier sense multiple access with collision avoidance (CSMA-CA). Guaranteed access to the channel can be provided to devices during the CFP, where each device has a guaranteed time slot (GTS). Using the CFP for device communication is perhaps more suitable for industrial automation due to the requirement for determinism [6] in industrial networks.

The following frame types are defined for the MAC layer:

- *Beacon* frames are transmitted by the coordinator and synchronize the start of the superframe.

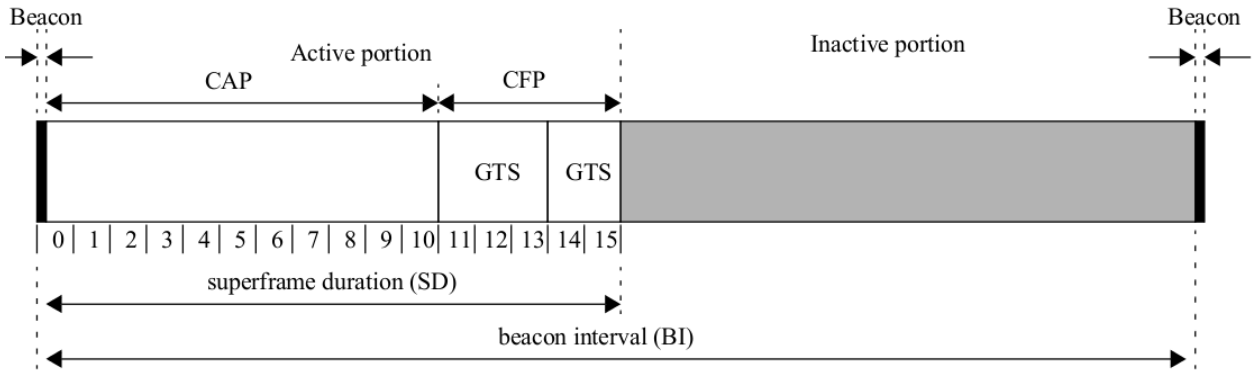


Figure 3.6: The MAC layer superframe structure (from [23]).

- *Data* frames are used to transmit data from any device or coordinator.
- *Acknowledgement* frames are sent in response to the successful receipt of a data or command frame.
- *MAC command* frames provide management of the MAC layer between PAN devices. Device associate and disassociate from the PAN coordinator using MAC command frames.

3.3 Robustness to Interference

Compared to direct-sequence spread-spectrum (DS-SS), UWB has a significant advantage with interference suppression [27]. UWB provides resistance to multipath interference as the time window during which the multipath reflection can overlap with the original pulse is very short. Multipath components can also increase the performance of a RAKE UWB receiver to combine the energy in the multipath components with the original signal [28].

Although UWB has resistance to multipath interference, it is not resistant to intersymbol interference if the multipath reflections are delayed enough to overlap with the next symbol. The burst position modulation scheme employed by the IEEE 802.15.4 UWB physical layer described in Section 3.1.2 employs a guard interval to mitigate against the effects of such interference.

Due to its low power spectral density UWB radio is able to share spectrum with other users [25]. Industry regulators impose limits on UWB radio to avoid interference with narrowband users. In Canada, UWB emissions are regulated by Industry Canada, which limit the effective isotropically radiated power (EIRP) of UWB communication to not exceed -41.3 dBm/MHz [29]. The Industry Canada UWB emission limits for indoor communication systems across all frequencies are shown in Figure 3.7.

UWB receivers are robust in the presence of narrowband interference. As stated by Zhao and Haimovich in [27]:

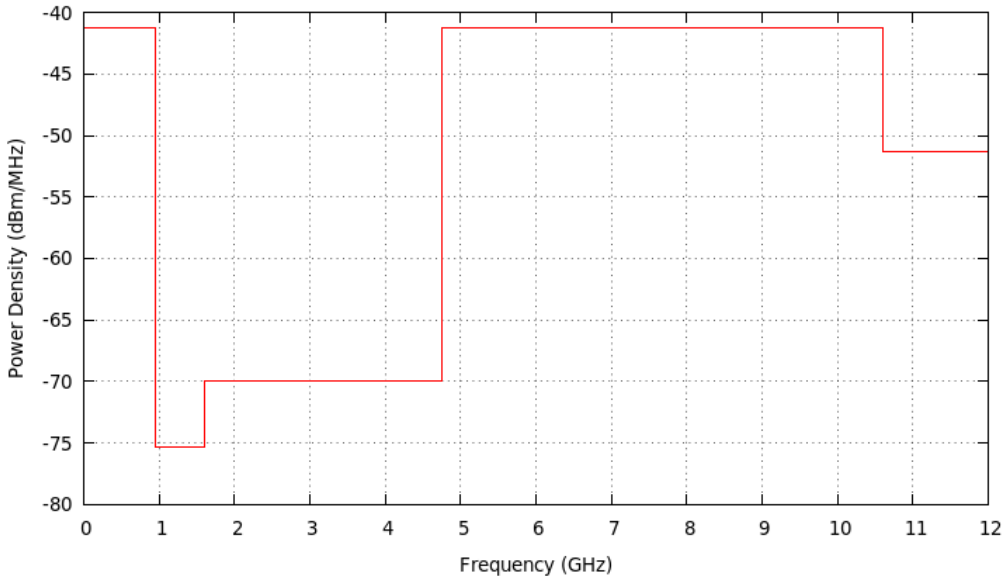


Figure 3.7: Industry Canada UWB average emission limits for indoor communication systems (adapted from [29]).

> "with UWB there are two mechanisms for interference suppression: 1) time windowing over the duration of the short UWB pulse and 2) the cross-correlation at the receiver of the interference with the template results in reduction of a narrowband interference due to the high correlation of the interference at times t and $t \pm T_p$"

where T_p is the pulse width.

3.3.1 Bit Error Rate

The BER performance of UWB is important for reliability of communications, especially if the radio is responsible for transporting safety-related messages as described in Chapter 1.

UWB radio for communication in a multi-user system is able to handle a high node density. Win and Scholtz [30] show that it is possible to achieve a BER of 10^{-5} for over 14,000 nodes at a low data rate of 19.2 kbps. A data rate of 4.77 Mbps can be achieved with 49 users at the same BER of 10^{-5}. These results were obtained from a mathematical model of a digital UWB receiver.

The effect of forward error correction techniques on the UWB BER is studied by Liang *et al.* [31]. They explore the BER of UWB using the residental line-of-sight and industrial non-line-of-sight channel models defined in [32]. Figure 3.8 shows their results for the BER against the energy-to-noise power density E_b/N_0. The results show that with the IEEE 802.15.4 reed-solomon forward error correction, a BER of 10^{-6} with an energy-to-noise power density of 19 dB is achievable in an industrial non-line-of-sight environment defined as channel model 8 (CM8) in [32].

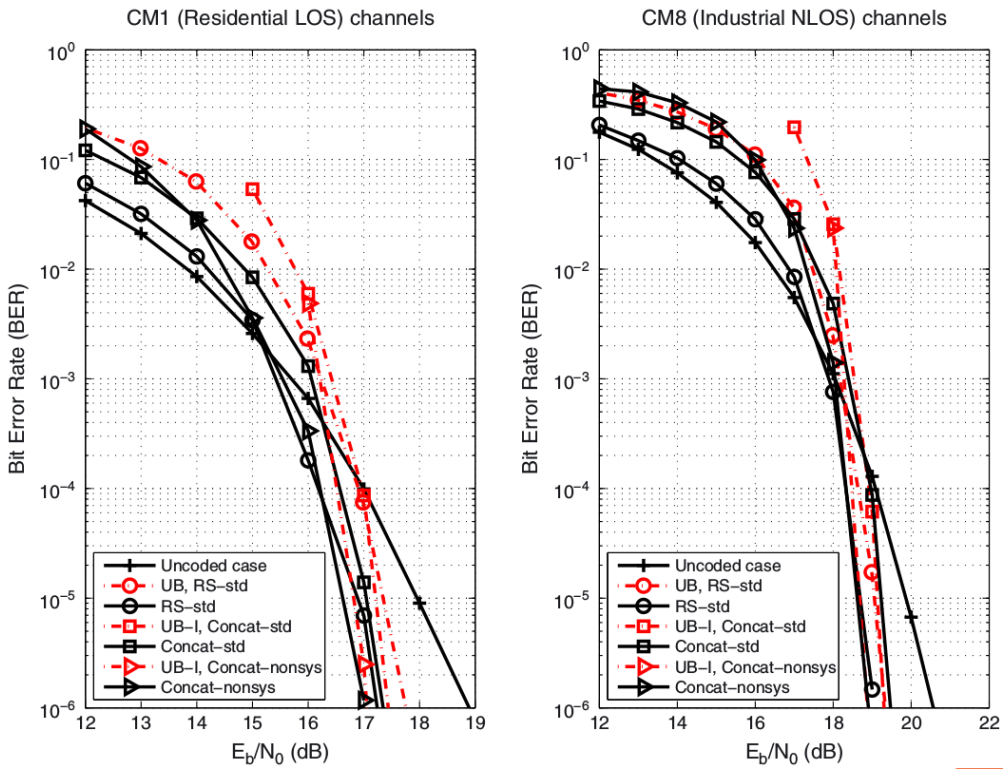


Figure 3.8: Forward error correction techniques and BER in residential and industrial environments (from [31]).

3.4 Error Detection and Correction

IEEE 802.15.4 implements two independent error detection mechanisms on separate parts of the UWB frame. One error detection mechanism in the physical header in the UWB layer, and the other is in the MAC layer.

3.4.1 Physical Layer

The UWB physical layer adds a physical header (PHR) to each transmitted UWB PDU. The PHR is protected using an error correcting code (ECC) which is Hamming block code which is capable of detecting and correcting all single bit errors, and guarantees detecting all combinations of errors two bits errors [23]. This is known as single error correction double error detection (SECDED).

The SECDED ECC protects only the PHR part of the UWB frame. The data part of the frame is protected with a separate mechanism, which is discussed in the next section.

3.4.2 MAC Layer

The MAC layer protects the data content of the PDU with a 16-bit frame check sequence (FCS). This FCS is a 16-bit CRC with the polynomial $x^{16} + x^{12} + x^5 + 1$ [23], which is a proper polynomial for block lengths of 260-1024 bits [33].

The FCS allows the MAC layer to detect (but not correct) transmission errors in the data part of the UWB frame. The FCS is generated by the sender and is transmitted alongside the data in the UWB frame. The receiver recomputes the FCS against the actual received data and compares the calculated FCS against the received FCS. The frame is accepted only if the calculated FCS exactly matches the received FCS.

3.4.3 Implications for SIL

Section 2.2.2 introduces the concept of the black channel in the context of the PROFIsafe protocol. In the black channel model the safety protocol (e.g. PROFIsafe) implements the necessary mechanisms (such as a CRC) to reliably detect data corruption errors. However, CRCs are not guaranteed to detect all possible combinations of bit errors that could occur during transmission.

The probability of an undetected error - known as the residual error rate - is dependent on the probability of a bit error occurring during transmission. As the BER increases, so does the probability of a combination of bit errors occurring which are not detected by the safety layer's CRC check (i.e. an undetected error occurs).

As explained in Section 2.2.2, for a proper CRC polynomial the residual error probability increases monotonically towards the limit 2^{-r} as the BER increases, where r is the bit-length of the CRC [15]. The IEEE 802.15.4e MAC layer utilizes CRC-16-CCITT which is a proper polynomial (as defined in Section 3.4.2) for block lengths of 260-1024 bits [33]. This provides a limit on the residual error rate of $2^{-16} \approx 10^{-4.8}$ using Equation 2.1, assuming a rate of 1 message per hour and 1 receipient of the message. This residual error rate is too high to meet the requirements of even SIL 1 as discussed in Section 2, however, the black channel principle can deliver lower probabilities of residual errors that permit wireless operations at SIL 3.

However, a safety protocol using the black channel model, such as PROFIsafe, implements its own error checking mechanisms, and does not rely on the checks of the underlying protocols in the black channel. Therefore, the CRC checks of the IEEE 802.15.4e MAC layer would be part of the black channel and would not affect the residual error rate of the safety protocol.

3.5 UWB Radio Hardware

The DW1000 is an UWB tranceiver integrated circuit (IC) manufactured by DecaWave, compliant with the IEEE 802.15.4-2011 UWB physical layer and the IEEE 802.15.4e-2012 MAC layer. The tranceiver is capable of operating over distances of up to 60 m at a data rate of 6.8 Mbps or up to 250 m at 110 kbps [34].

The DW1000 supports a subset of the features defined in IEEE 802.15.4; it does not support all UWB channels and data rates. The supported functionality of the DW1000 are [34]:

- Supported channels: 1, 2, 3, 4, 5, and 7.
- Supported bit rates: 110 kbps, 850 kbps, and 6.8 Mbps.

Some MAC features defined in IEEE 802.15.4e are supported by the DW1000. The MAC layer FCS can be automatically checked, and errors can be reported to the host IC. An "auto acknowlegement" feature is also supported which automatically sends a MAC layer acknowledgement frame upon receipt of a frame addressed to the receiver with a correct FCS.

To the best of our knowledge, the DW1000 is the only IEEE 802.15.4-2011 compliant receiver that supports UWB communication in addition to distance measurements.

Chapter 4

Summary and Future Work

4.1 Summary

This report has provided an introduction into industrial control networks, including safety aspects, and ultra-wideband radio for communications. Chapter 1 introduced the wired and wireless technology currently in use in industrial automation. An overview of functional safety and the IEC 61508 standard's safety integrity levels (SIL) for general functional safety are introduced in Chapter 2. Deterministic and stochastic errors in industrial communication networks are introduced, and the relationship between residual errors and SIL is explored. The PROFIsafe protocol is discussed as a safety layer based on the "black channel" principle, which permits using the protocol with different physical media. Åckerberg *et al.* [12] explore the use of PROFIsafe with WirelessHART.

Finally, Chapter 3 introduces IEEE 802.15.4 ultra-wideband (UWB) radio for communication, and describes its properties for communication reliability such as resistance to noise and interference, and bit error rate (BER) performance.

4.2 Future Work

The reliability of wireless networks in industrial control is an important factor in preventing "nuisance trips" or dangerous failures in safety-critical processes. Wireless networks have a higher BER than wired fieldbus systems; reducing the BER would improve the reliability of wireless networks to reduce the likelihood of communication errors. This is particularly important in safety-related systems as too high a BER can prevent the system from achieving the desired SIL. The BER of a network for a safety-related system is limited to a maximum of 10^{-2} [3, 12], although the BER may need to be significantly lower in order to reduce the residual error rate to an acceptable level to reach the desired SIL.

The properties of UWB radio may provide a solution to improve the reliability of wireless industrial control networks. Work by Åckerberg *et al.* [5, 12] has shown that the WirelessHART protocol can be used as the black channel for the PROFIsafe protocol to enable routing of safety-related messages, however they found that non-line-of-sight scenarios

can reduce round trip times to unacceptable levels. Can UWB's resistance to multipath and narrowband interference improve the BER for real-time industrial communication, particularly in non-line-of-sight scenarios? If so, what is the BER performance of UWB compared to existing standards such as WirelessHART?

Furthermore, IEEE 802.15.4e-2012 [26] defines the MAC layer for process control and factory automation. The MAC layer provides deterministic network management via time slot-based TDMA as well as managing security. Can UWB with the IEEE 802.15.4 MAC layer be used as the black channel for a safety layer such as PROFIsafe? Additionally, as the residual error rate of PROFIsafe is reliant on the BER of the underlying network, is the BER of UWB suitable for achieving IEC 61508 SIL 3 with PROFIsafe?

Bibliography

[1] Thilo Sauter. Fieldbus System Fundamentals. In *Industrial communication technology handbook*, chapter 1, pages 1–1 – 1–50. CRC Press, 2014.

[2] IEC. Industrial communication networks - Fieldbus specifications. IEC 61158:2014, Industrial Electromechanical Commission, Geneva, Switzerland, 2014.

[3] IEC. Industrial communication networks – profiles. Part 3, Functional Safety fieldbuses– general rules and profile definitions. IEC 61784-3:2010, Industrial Electromechanical Commission, Geneva, Switzerland, 2010.

[4] J. P. Thomesse. Fieldbus technology in industrial automation. *Proceedings of the IEEE*, 93(6):1073–1101, June 2005.

[5] J. Åkerberg, F. Reichenbach, and M. Björkman. Enabling safety-critical wireless communication using wirelesshart and profisafe. In *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*, pages 1–8, Bilbao, Spain, Sept 2010.

[6] K. Al Agha, M. H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J. B. Viollet. Which wireless technology for industrial wireless sensor networks? the development of ocari technology. *IEEE Transactions on Industrial Electronics*, 56(10):4266–4278, Oct 2009.

[7] Stig Petersen and Niels Aakvaag. Wireless instrumentation for safety critical systems. Technical Report A26762, SINTEF, March 2015. 50 pages.

[8] V. C. Gungor and G. P. Hancke. Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10):4258–4265, Oct 2009.

[9] M. Schäfer. New concepts for safety-related bus systems. In *3rd International Symposium Programmable Electronic Systems in Safety Related Applications*, May 1998.

[10] Alessandra Flammini and Emiliano Sisinni. WirelessHART. In *Industrial communication technology handbook*, chapter 31, pages 31–1 – 31–20. CRC Press, 2014.

[11] S. Petersen and S. Carlsen. WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor. *IEEE Industrial Electronics Magazine*, 5(4):23–34, Dec 2011.

[12] J. Åkerberg, F. Reichenbach, M. Gidlund, and M. Björkman. Measurements on an industrial wireless hart network supporting profisafe: A case study. In *Emerging Technologies Factory Automation (ETFA), 2011 IEEE 16th Conference on*, pages 1–8, Toulouse, France, Sept 2011.

[13] Stig Petersen and Simon Carlsen. ISA100.11a. In *Industrial communication technology handbook*, chapter 32, pages 32–1 – 32–14. CRC Press, 2014.

[14] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508:2010, Industrial Electromechanical Commission, Geneva, Switzerland, 2010.

[15] Wolfgang Stripf and Herbert Barthel. PROFIsafe: Functional Safety with PROFIBUS and PROFINET. In *Industrial communication technology handbook*, chapter 27, pages 27–1 – 27–22. CRC Press, 2014.

[16] David J Smith and Kenneth GL Simpson. *Safey critical systems handbook: a straightfoward guide to functional safety, IEC 61508 (2010 edition) and related standards, including process IEC 61511 and machinery IEC 62061 and ISO 13849*. Elsevier, 2010.

[17] Felix Redmill. An introduction to the safety standard iec 61508. *Journal of the System Safety Society*, 35(1):20–25, First Quarter 1999.

[18] IEC. Industrial communication networks–profiles. Part 3-3, Functional Safety fieldbuses – additional specifications for CPF 3. IEC 61784-3-3:2010, Industrial Electromechanical Commission, Geneva, Switzerland, 2010.

[19] Jun Wu, Zhitao Guan, Ming Zhan, Jianhua Li, and Yuwei Su. Analysis and extension of safety mechanisms for standardized control networks in smart grid. *International Journal of Distributed Sensor Networks*, 2014, 2014.

[20] W. Ikram, N. Jansson, T. Harvei, B. Fismen, J. Svare, N. Aakvaag, S. Petersen, and S. Carlsen. Towards the development of a SIL compliant wireless hydrocarbon leakage detection system. In *2013 IEEE 18th Conference on Emerging Technologies Factory Automation (ETFA)*, pages 1–8, Sept 2013.

[21] Marco Cereia, Jochen Strib, and Reinhard Sperrer. SafetyNET p Protocol. In *Industrial communication technology handbook*, chapter 28, pages 28–1 – 28–24. CRC Press, 2014.

[22] David A. Vasko. CIP Safety: Safety networking for today and beyond. Technical report, ODVA, October 2015.

[23] IEEE Computer Society. *IEEE Std 802.15.4-2011 - IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, September 2011.

[24] Sinan Gezici I. G. Zafer Sahinoglu. *Ultra-wideband Positioning Systems: Theoretical Limits, Ranging Algorithms, and Protocols*. Cambridge University Press, October 2008.

[25] Ruofan Jin, D. Grace, and P. Mitchell. Cognitive Radio for UWB spectrum sharing and power allocation. In *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on*, pages 1001–1005, York, United Kingdom, Sept 2010.

[26] IEEE Computer Society. *IEEE Std 802.15.4e-2012 - IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*, April 2012.

[27] Li Zhao and A. M. Haimovich. Performance of ultra-wideband communications in the presence of interference. *IEEE Journal on Selected Areas in Communications*, 20(9):1684–1691, Dec 2002.

[28] Huaping Liu. Error performance of a pulse amplitude and position modulated ultra-wideband system over lognormal fading channels. *IEEE Communications Letters*, 7(11):531–533, Nov 2003.

[29] Devices Using Ultra-Wideband (UWB) Technology. Technical report, Industry Canada, March 2009.

[30] Moe Z Win, Robert A Scholtz, et al. Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications. *IEEE Transactions on communications*, 48(4):679–689, 2000.

[31] Zhonghua Liang, Xiaodai Dong, T Aaron Gulliver, and Xuewen Liao. Performance of transmitted reference pulse cluster ultra-wideband systems with forward error correction. *International Journal of Communication Systems*, 27(2):265–276, 2014.

[32] Andreas F Molisch, Kannan Balakrishnan, Dajana Cassioli, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal, Juergen Kunisch, Hans Schantz, Ulrich Schuster, et al. Ieee 802.15.4a channel model-final report. *IEEE P802*, 15(04):0662, 2004.

[33] Ts Baicheva, S Dodunekov, and P Kazakov. Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy. *IEE Proceedings-Communications*, 147(5):253–256, 2000.

[34] DecaWave. *DW1000 User Manual*, December 2015. Version 2.07.