SAFE COOPERATING CYBER-PHYSICAL SYSTEMS USING WIRELESS COMMUNICATION

Report type	**Deliverable D3.3**
Report name	**Wireless Safety Layer**
Dissemination level	PU
Report status:	Final
Version number:	1.0
Date of preparation:	2018.03.31

Authors

Contributors

SINTEF

Revision chart and history log

Version	Date	Reason
0.1	2017.10.01	First draft of document structure
0.2	2018.03.16	First draft for review
0.3		Updated draft
0.4		Final review among the partners
1.0	2018.03.31	Final release

Table of contents

Abbreviations

Abbreviation	Description
CO-CPS	Cooperative Cyber-Physical Systems
UC1	SafeCOP Use Case 1 on hospital beds.
UC2	SafeCOP Use Case 2 on collaborative bathymetry.
SIL	Safety Integrity Level

1. Purpose

The purpose of this document is to describe an approach to safe communication for cooperative cyber-physical systems (CO-CPS). The deliverable aims to provide a comprehensive overview and suggested safety requirements for how to achieve safe communication over a wireless transmission channel for selected use cases of the SafeCOP project.

The content of this document is safety-related, but not domain specific, and can be used for various applications. Most of the work inspired by IEC 61508 [1] and EN 50159 [2].

2. Introduction to safe communication

The SafeCOP project addresses collaborative cyber-physical systems (CO-CPS) applied in safety-related applications. S*afety* can be defined as freedom from unacceptable risk of harm to humans, either directly through injury or death, or indirectly as a result of damage to equipment, property or the environment [1]. Safe operation can be achieved through various methods and mechanisms, typically categorized as *barriers*. Traditionally, a barrier is a component that restricts physical access to an area in order to mitigate risk. However, in modern approaches to safety, e.g. as found in the petroleum industry [3], a barrier is defined as a measure whose function is to offer protection in failure, hazard and accident situations. The barrier element may be of a technical, organizational or operational nature. In this regard, technical barriers are often subject to *functional safety* requirements, which are barriers in the shape of electrical, electronical and programmable systems which must operate correctly in order to ensure safe operation [1]. Depending on the nature and criticality of the operations, relevant authorities designate a certain *safety integrity level* (SIL) to each technical barrier which shall govern the barrier's entire lifecycle (i.e. concept, design, implementation, deployment, operation, maintenance, decommissioning) [1]. Some examples of technical safety barriers include process emergency shut-down systems, fire and gas detection, anti-lock braking, airbags and railway signaling. Functional safety is achieved by adhering to safety standards for the operational domain as exemplified in Table 1.

Table 1 Examples of safety standards for different domains

Standard	Domain
IEC 61508	Generic standard for functional safety
ISO 26262	Automotive
ISO 13849-1	Machinery
IEC 62061	Machines
IEC 60601	Medical
IEC 61511	Process industries
IEC 60880	Nuclear industry
IEC 61513	Nuclear industry
DO 178C	Avionics
EN 5012x	Railway

If a safety system involves communication between different locations, the communication system is considered an integral part of the safety system. For such a communication system to be safe, it must be proven and certified according to a safety standard. In some domains, specific safety standards for safe communication have been developed (e.g. IEC 61784-3 [4] for industrial automation and EN 50159/IEC 62280 for railway signaling), while other domains cover principles for safe communication in the main safety standards (e.g. ISO 26262-5 for automotive applications).

3. Safe communication for SafeCOP

The SafeCOP-project addresses safety-related CO-CPSs using wireless communication. The basic concept consists of two or more safety objects that collaborate to solve a safety function, as shown in Figure 1. Wireless communication is the selected technology for safe information exchange between the safety objects. For the work in this deliverable, SafeCOP Use Case 1 (UC1) and Use Case 2 (UC2) are selected as example applications for acquiring concepts and requirements for safe communication. UC1 consists of two robots collaborating to move a hospital bed, while the goal of UC2 is to perform bathymetry with a fleet of collaborating autonomous boats.

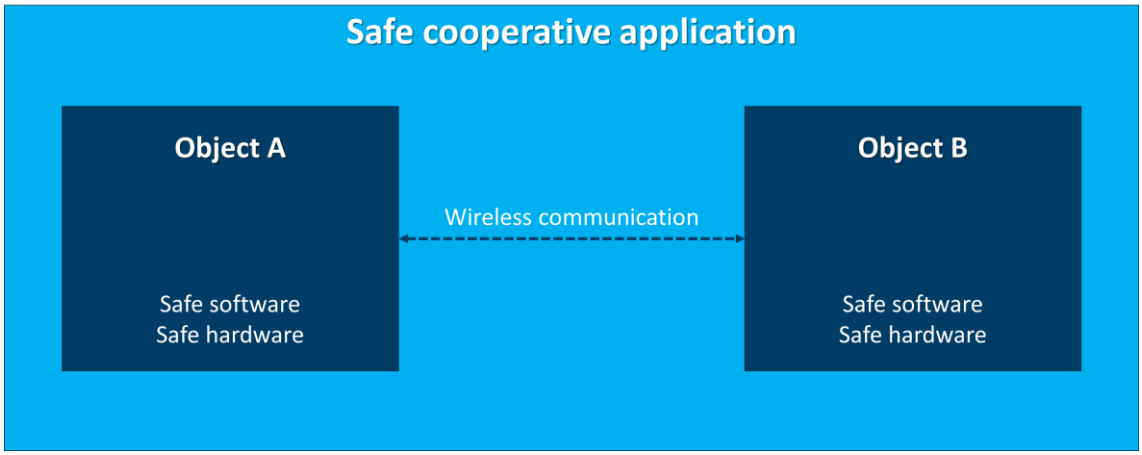

Figure 1 Simplified SafeCOP concept with collaborative safety using wireless communication

As mentioned in *Section 2*, a communication system is considered as an integral part of a safety system if the application involves transmission of information between different locations. In the SafeCOP concept, wireless communication is by definition an integral part of the safety system, and must thus be certified as safe according to relevant safety standards. For UC1 (robots) and UC2 (boats) there are no formal regulations or directives in place regulating the required safety certification of the system, including communication. At the time of writing, there is also no known initiatives addressing the development and implementation of specific safety standards for these two domains. However, as other domain specific safety standards all inherit concepts and methods from the generic safety specification, IEC 61508, it is reasonable to assume that this will also be the case for any future safety regulations for UC1 and UC2. IEC 61508 will thus be used as the foundation for developing the safe communication protocol and methods for these two SafeCOP use-cases. Further details on how IEC 61508 addresses the issue of achieving safe communication is presented in the following section.

4. Safe communication according to IEC 61508

IEC 61508 states that when a safety function relies on communication in its implementation, the failure measure of the communication process shall be estimated. The estimation must consider transmission errors (e.g. repetition and deletion) as well as random errors.

IEC 61508 defines two different methods for achieving safe communication:

I. Design, implementation and validation of the *entire* communication channel according to IEC 61508 *and* either IEC 61784-3 or IEC 62280/EN 50159.
II. Part of the communication channel is *not* designed, implemented or validated according to IEC 61508. The measures necessary to ensure failure performance of the communication system shall be implemented in accordance with either IEC 61784-3 or IEC 62280/EN 50159.

For reference, IEC 61784-3 is a standard for (wired) functional safety fieldbuses, while IEC 62280 is a standard for safety-related communication in transmission systems for railway signaling. IEC 62280 is also known as EN 50159, and will be referenced under this designation in the remainder of this document.

For Method I, called the *white channel* principle, there are two approaches that can be followed:

A. The communication system is under the control of the designer of the safety system.
B. The communication system is not under the control of the designer, but it is designed, implemented and validated by a third-party vendor.

These approaches have some practical considerations which may limit their applicability in safety system development projects. For *approach A*, it requires the safety system designer to be able to design and implement an entire communication system from scratch, an expertise which might not be readily available in all organizations. Examples of safety systems designed after *approach A* may be mission-critical space missions, military and weapon systems. For *approach B*, on the other hand, it requires a third-party communication system vendor to go through the rigorous, time-consuming and costly process of safety-certifying a communication solution. In addition, due to the close coupling between the communication system and the safety processes, the third-party vendor must preferably be tightly integrated into the design and implementation team.

Method II for achieving safe communication is often referred to as the *black channel* principle. It involves applying safety (and security when needed) on an end-to-end basis, thereby bypassing the need for a safety certified communication system.

For the SafeCOP project it is out of scope to develop a new white-channel communication protocol for safe wireless communication. It is also difficult to find a relevant safety-certified wireless communication protocol from a third-party vendor, which rules out Method I for achieving safe communication. Method II, the black channel principle, is thus selected as the main approach to achieving safe communication for UC1 and UC2. This implies designing, implementing and validating the hardware and software of the end-to-end safety functionality illustrated in Figure 3 according to IEC 61508, while the communication aspects of the black channel solution must be developed according to either IEC 61784-3 or EN 50159. To select the most appropriate and suitable safe communication protocol for the SafeCOP-project, an analysis of both specifications has been performed, as described in the following two sections of this document.

5. Safe communication according to IEC 61784-3

The IEC 61784-3 for industrial communication networks defines common principles for use in the transmission of safety-relevant messages among participants within a distributed fieldbus network in accordance with the requirements of IEC 61508 for functional safety. The principles are based on the *black channel* approach as defined in IEC 61508, with the goal of addressing various industrial applications such as process control, manufacturing automation and machinery. See Figure 2 for an example configuration of a functional safety fieldbus communication network based on the black channel principle. Here, only the Safety Communication Layer needs to be safety certified, the rest of the communication system is considered as part of the black channel.

While IEC 61784-3 addresses various failure modes of the communication channels (e.g. message repetition, deletion, delay and insertion), it does not adequately cover threats related to information security. It refers to IEC 61784-4 for profile specific security mechanisms, and to

IEC 62443 for common security mechanism, but there are no further claims to how these security mechanisms might be validated and certified. However, this can be explained from a historical perspective. IEC 61784-3 addresses industrial fieldbus communication which are wired technologies used for factory and process automation. In the typical usage scenario, these solutions can be considered as segregated *closed* communication systems, with no connections to other systems or to the Internet. External threats to the system from people with malicious intent can be disregarded, as the wires themselves also deployed in protected production areas with physical access restrictions and access control. In this context, there is no need for information security mechanisms. The term *open* communication system, defined as a system that is subject to threats from external malicious source, is not defined in the specification. A further limitation to the use of IEC 61784-3 is related to the claim that compliance to the standard might involve the use of various patents related to fieldbus communication technologies [4].

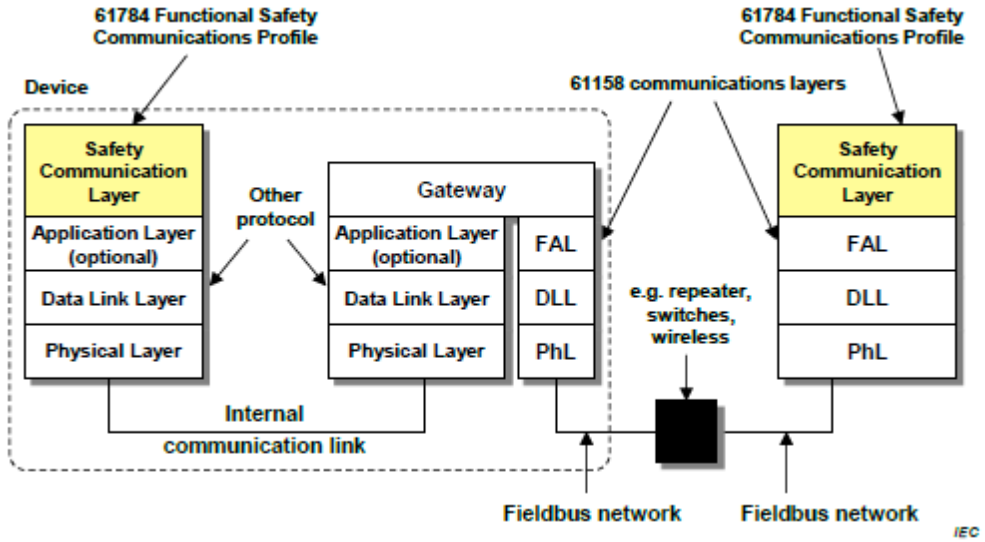

Figure 2 Example fieldbus functional safety communication system [4]

A practical example of the shortcomings of IEC 61784-3 with regards to security, as well as potential patent and licensing issues, can be found in IEC 61784-3-3, better known as PROFISafe. PROFISafe is a SIL3 certified safety communication protocol based on the black channel principle. Due to patent and licensing rights enforced by its creator, Siemens, it is required to use PROFINET as the underlying protocol for safe communication with PROFISafe. In addition, it has been proven that PROFISafe has major flaws in its implementation of information security, leading to it being vulnerable to attacks [5]. Despite these flaws, PROFISafe has been used as the protocol of choice for the world's first wireless SIL2-certified infrared hydrocarbon gas detector for use in process automation [6]. The gas detectors are battery operated, and uses ISA100.11a as a wireless transmission system. From a system point-of-view, the safety controller and the gas detector are considered the end-points, and PROFISafe is used as the safety protocol for the end-to-end communication. The black channel consists of both a wired PROFINET configuration between the safety controller and an ISA100.11a gateway (as required by Siemens lisencing), and a wireless ISA100.11a mesh network between the ISA100.11a gateway and the ISA100.11a-enabled gas detector. The PROFISafe messages are encapsulated in a PROFINET message by the safety controller, and then "unwrapped" from PROFINET and encapsulated into an ISA100.11a message by the gateway before transmitted to the gas detector. However, this solution does not consider end-to-end security, and relies on inherent security mechanisms in ISA100.11a and PROFINET as protection against attacks from external malicious sources.

Based on the abovementioned weaknesses, IEC 61784-3 is not considered as a suitable safety communication protocol for SafeCOP UC1 and UC2. However, it is worth noting that IEC61784-

3-3, better known as PROFISafe, has been used as a safety protocol for a wireless SIL2 application, and lessons learned from this process is highly relevant for SafeCOP.

6. Safe communication according to EN 50159

If a safety-related electronic system in a railway application involves the transfer of information between different locations, EN 50159 states that the end-to-end communication must be safe in accordance with EN 50129 [7]. Note that the transmission system itself does not need to be safe, nor satisfy any particular preconditions. From a safety point-of-view, the transmission system is simply considered not trusted, or not fully trusted. However, the particular safety requirements for the end-to-end communication depend on the nature and characteristics of the transmission system.

To reduce the complexity of safety certification, EN 50159 classifies transmission systems into three categories:

- **Category 1:** Systems which are under the control of the designer and fixed during their lifetime.
- **Category 2:** Systems which are partly unknown or not fixed, however unauthorized access can be excluded.
- **Category 3:** Systems which are not under the control of the designer, and where unauthorized access has to be considered.

Category 1 and 2 type communication systems are often referred to as *closed*, defined as a transmission system with well-known and fixed properties and consisting of a fixed number or fixed maximum number of participants. The risk of unauthorized access to a closed transmissions system is considered negligible. Similarly, category 3 transmission system are referred to as *open*, defined as a having an unknown number of participants, as well as unknown, variable and non-trusted properties. An open transmission system will always have the potential for unauthorized access. Thus, an important distinction between the two types of systems is the need for information security to protect against malicious attacks on open communication channels.

Architecture

EN 50159 defines safety requirements for safe communication between safety-related equipment using a transmission system. The transmission system can be either closed or open. Furthermore, both safety-related and non-safety-related equipment can be connected to the transmission system.

The reference architecture as defined by EN 50159 divides the safety-related communication system into the following components:

I. Safety-related transmission functions incorporated in the safety-related equipment.
II. Safety-related cryptographic techniques that protect the safety-related message.
III. A non-safety related, open or closed transmission system that may itself include transmission protection function and/or protection functions.

The transmission system is used for unknown telecommunication services and has the potential for unauthorized access. For open communication systems it is necessary to include cryptographic techniques as described in component II above.

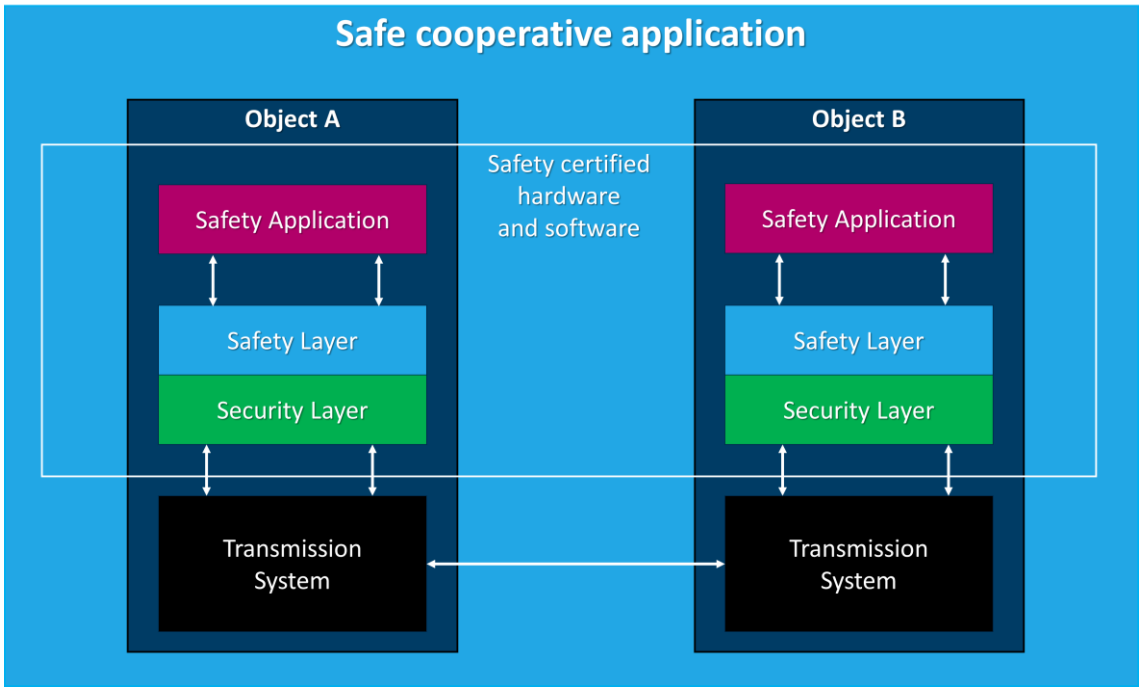

Figure 3 Safe end-to-end communication using the black channel principle

For category 3 open communication systems, EN 50159 proposes an end-to-end safety approach using the black channel principle. The transmission system is considered as unsafe, and safety and security mechanisms are implemented as separate layers in each end node in the communication, as illustrated in Figure 3. The purpose of the safety layer is to detect hazardous faults and failures, while the security layer protects the communication from threats from external parties with malicious intents. The safety and security layers are closely integrated with the safety application.

The main hazard to safety-related communication is the failure to obtain a valid message at the receiving end of the communication path. Hazardous events can be categorized into either random or deliberate events. Examples of random events include [2]:

- Broken wires
- Cabling error
- Antenna misalignment
- Performance loss
- Random HW failure
- Electromagnetic interference
- Thermal noise
- Fire
- Lightning
- Solar radiation
- …

Examples of deliberately caused events include [2]:

- Wire-tapping and eavesdropping
- Damage to HW
- Unauthorized change to SW
- Transmission of unauthorized messages
- Jamming

- …

Some of these events are specific to *wired* transmission systems (e.g. broken wires and wire-tapping), while others are relevant only for *wireless* transmission systems (e.g. antenna misalignment and jamming). However, regardless of the nature and origin of the failure event and whether or not it is a wired or wireless transmission system, the basic message errors can be simplified into one of the following seven threats [2]:

1) Repetition
2) Deletion
3) Insertion
4) Resequencing
5) Corruption
6) Delay
7) Masquerade

To reduce the risks associated with these threats, a set of defenses have been identified [2]:

a) Sequence number
b) Time stamp
c) Time-out
d) Source and destination ID
e) Feedback message
f) Identification procedure
g) Safety code
h) Cryptographic techniques

Each of these defenses can provide protection against one or more of the seven identified threats to the communication system. In the safety case[1] for the safety system it shall be demonstrated that there is at least one corresponding defense or combination of defenses for each defined threat. The correlation between threats and defenses is shown in Table 2. As mentioned previously, this threat and defense matrix applied both to wired and wireless transmission systems.

Table 2 Threats and defenses matrix

Threats	Defenses							
	Sequence number	Time stamp	Time-out	Source and destination ID	Feedback message	Identification procedure	Safety code	Cryptographic techniques
Repetition	X	X						
Deletion	X							
Insertion	X			X	X	X		
Resequencing	X	X						
Corruption							X	X
Delay		X	X					
Masquerade					X	X		X

Seen in relation to the safe end-to-end communication architecture using the black channel principle as depicted in Figure 3, the defenses *Identification procedure* and *Cryptographic techniques* are only relevant for open communication systems where unauthorized access must be considered. These two defenses are thus the content of the *Security Layer*, while the other defenses reside in the *Safety Layer*.

[1] *Safety case* is in EN 50159 defined as a documented demonstration that the product complies with the specified safety requirements.

Requirements for communication defenses in EN 50159

Safety systems using an open or closed transmission system must provide adequate defenses against all identified threats to communication. The requirements for the defenses needed for the safety application shall take into account the following [2]:

- The level, frequency and consequence of the risks identified for each threat
- The safety integrity level of the data and process involved in the communication

Furthermore, EN 50159 states that the defenses shall be implemented according to the requirements stated in EN 50129, addressing specification, design, construction, installation, acceptance, operation, maintenance and modification/extension phases of safety systems, as well as procedures relating to electronic hardware components. The defenses shall also be functionally independent from the layers used in the non-trusted communication system.

EN 50159 provides an overview of the specific requirements for each of the defenses, to be used in the argumentation in the safety case:

a) Sequence number

The sequence number is a running number that is incremented for each message exchange between a given transmitter and receiver. It is used to check if the messages arrive in correct order. Depending on the nature of the safety process and its safety integrity level, the safety case must demonstrate the appropriateness of the sequence number in relation to its length and mechanisms for initialization, wrap-around and recovery after message interruption.

b) Time stamp

For some safety applications, it might be beneficial to tag sensor data with a time stamp. This is especially important if there is a risk for a deviation between the time of origin of the data and the time the data is used for decision making at the receiver. This is especially important for transmission systems with significant delay or variable delay.

If time stamp is applied in the safety protocol, the following aspects must be considered [2]:

- The value and accuracy of the time increment
- The size of the timer
- The absolute value of the timer
- Synchronization of timers in different devices in the network
- Time delay between information origin and application of the time stamp
- Time delay between checking the time stamp and using the information

c) Time-out

A time-out is used to check if the delay between messages exceeds a predefined threshold. If the threshold is exceeded, an error in the transmission system shall be assumed. For safety-related communication, the threshold is often associated with the safety time of the safety application.

When using time-out as a defense mechanism for safety-related communication, the safety case shall demonstrate the appropriateness of the acceptable delay and the accuracy of the time-out in relation to the nature and safety integrity level of the safety application.

d) Source and destination ID

For transmission networks with multiple participants, a measure for checking the source of received information is necessary to achieve safe communication. A message may include a unique ID for either the source (transmitter) or the destination (receiver), or for both source and destination. The source and/or destination IDs shall be included in the safety layer

regardless of the presence of ID mechanisms in the transmission system.

Depending on the nature of the safety process and its safety integrity level, the safety case must demonstrate the appropriateness of the source and/or destination IDs in relation to the uniqueness of the IDs and the size of the ID data field.

e) Feedback message
For transmission systems with the availability of a back channel, a feedback message can be sent from the receiver of a safety-critical message to the sender. The feedback message may contain information about content in the original message, additional data added by the receiver, or additional data for safety or security purposes.

The feedback message on its own does not provide a defense against any specific threat, but it is used as an enabler for other defense mechanisms.

f) Identification procedure
In *open* transmission systems there is always a risk of messages from unknown, non-safety-related users being confused with information originating from legitimate sources. To defend against this threat, the safety-related process can implement a suitable identification procedure to authenticate participants in the safety-related communication.

Note that this defense is only relevant for category 3 transmission systems.

g) Safety code
Transmission codes are used in transmission systems to *detect* bit errors, and in the case of forward error correcting codes (FEC) to improve transmission quality by also *correcting* bit errors. Unfortunately, transmission codes are prone to failures due to hardware faults, systematic errors and external influences, and can as such not be trusted from a safety point-of-view. It is therefore necessary to implement a safety code in the safety layer (ref. Figure 3) to detect potential message corruption.

When using a safety code as a defense mechanism for safety-related communication, the safety case shall demonstrate the appropriateness of the capability of the safety code for detection of random as well as expected systematic types of message corruption, in relation to the nature and safety integrity level of the safety application. In addition, the safety code must be different from the transmission code used by the transmission system. This can be achieved by using different algorithms, or by using different configuration parameters (e.g. polynomials) for the same algorithms. Furthermore, the safety code must be able to detect and act on typical transmission faults and errors [2]:

- Interrupted transmission line
- All bits set to logical 0
- All bits set to logical 1
- Message inversion
- Synchronization error for serial transmission
- Random errors
- Burst errors
- Systematic errors
- Combination of the above errors

h) Cryptographic techniques
Cryptographic techniques are defense mechanisms for *open* transmission systems where there are risks of malicious attacks from unauthorized participants of the network. This defense is

then aimed at protecting the safety-related communication against potential threats from unauthorized transmitters within the transmission network. There are three different solutions for cryptographic techniques that can be used by the safety-related communication [2]:

1. Using a safety code that also provides cryptographic protection.
2. Enciphering of the message after the safety code has been applied.
3. Adding a cryptographic code to the safety code.

Depending on the nature of the safety process and its safety integrity level, the safety case must demonstrate the appropriateness of the solution with regards to technical choice of cryptographic technique, technical choice of cryptographic architecture and relevant management activities (e.g. production, storage and distribution of cryptographic keys). In this regard, reasonable assumption shall be described about the nature, motivation, and financial and technical means of potential attackers. Expected technical developments (e.g. increased computational power of computers) and social developments (e.g. economic conflicts and worsening of vandalism) that are expected in the life time of the safety equipment must also be considered when selecting the cryptographic technique.

Note that this defense is only relevant for category 3 transmission systems.

7. Implementation of safety-related end-to-end communication

As described in the previous sections, the generic standard for functional safety, IEC 61508, refers to either IEC 61784-3 or EN 50159 for issues related to safe communication. However, IEC 61784-3 has some open questions related to licensing and patents, in addition to weaknesses related to security mechanisms for open transmission systems. EN 50159, on the other hand, addresses both open and closed transmission systems, including wireless transmission systems. On this background, it is thus recommended to use principles from EN 50159 as the foundation for the safe communication protocol for SafeCOP.

EN 50159 defines a set of requirements for defenses necessary as protection against threats to the transmission system used as the carrier for safety-related communication. The standard suggests using end-to-end communication to ensure safety, where the transmission system is regarded as a black channel, as illustrated in Figure 3. The safety layer is responsible for defenses against random and systematic faults and failures, while the security layer protects against deliberate threats from external sources with malicious intent. Note that for *closed* transmission systems where unauthorized access can be disregarded, the security layer is not required. However, this is of little relevance to SafeCOP, as wireless communication is always considered an *open* transmission system.

For matters related to actual implementation of the defenses of the safety and security layers, EN 50159 does not offer any guidelines or recommendations. These aspects are considered out of scope for the standard, and it is left to the system designer to demonstrate compliance to EN 50159 in the safety case of the safety system. As a result, there is a large degree of freedom in how to design and implement end-to-end safety-critical communication. This includes choice of distribution of responsibilities between the safety layer and the safety application, e.g. whether is it relevant for the safety application to be aware of potential errors, faults, failures and attacks in the transmission system. Furthermore, depending on the nature of the safety application, parts of the defense mechanisms may be integrated with the safety process itself. This could contribute to optimization of the performance of the safety-related communication through enhanced knowledge of the performance of the communication and transmission systems.

A further observation about the black channel principle is the distinction between the *safety requirements* and the *performance* of the transmission system. A pervasive misconception is that

the transmission system must be *reliable* in order to be *safe*, but this is not the case. Safety and reliability are two different properties, and one does not necessarily imply the other [8]. A system can be reliable but unsafe, and a system can be safe but unreliable. This is also the case for end-to-end safe communication. A reliable transmission system can be unsafe if the safety and security layers are not implemented in a safe manner, while an unreliable transmission system can be safe if the safety and security layers work as intended. However, it is worth noting that a prerequisite for the safe but unreliable transmission system is the existence of a *safe state* that the system can enter if the safety layer detects any errors in the exchange of safe messages.

8. Summary and conclusions

The goal of this document is to describe requirements and methods for achieving safe communication over the wireless transmission systems used by the CO-CPS safety-applications in the SafeCOP project. To limit the scope of work, UC1 and UC2 has been used as reference use cases. UC1 addresses two robots collaborating to move a hospital bed, while UC2 addresses autonomous boats in fleet formation used for bathymetry applications. Common for both UC1 and UC2 is that they operate in domains which have limited maturity when it comes to functional safety, as there are no formal regulations enforced by authorities. This is expected to change in the near future, as authorities realize the need for controlling and governing autonomous applications with high risks for accidents and hazardous situations. On this background, the generic standard for functional safety, IEC 61508, is chosen as the reference for functional safety for safe communication in SafeCOP.

IEC 61508 addresses functional safety for electrical, electronic and programmable electronic systems, and most domain specific safety standards typically inherit their properties from IEC 61508, with some minor modifications. When it comes to safe communication, IEC 61508 refers to either IEC 61784-3 (functional safety fieldbus communication for industrial automation applications), or EN 50159 addressing safe communication for railway transmission systems. As IEC 61784-3 is known to have weaknesses regarding information security, which is needed when using a wireless transmission system for safe communication, EN 50159 is the natural choice for detailed requirements and implementation guidelines for SafeCOP UC1 and UC2.

EN 50159 suggests achieving safe communication by applying a safety and security layer on each end node, also known as the black channel principle. This allows the transmission system to be unsafe, i.e. it does not have to be safety certified. With this approach, the transmission system used for safe end-to-end communication can basically be of any type and format, as safety requirements are handled by the safety and security layers.

The practical implementation of a safety-related end-to-end communication systems is out of scope of EN 50159, and is left to the designer of the safety system. However, the defenses shall be implemented according to the requirements stated in EN 50129, addressing specification, design, construction, installation, acceptance, operation, maintenance, modification and extension phases of safety systems, as well as procedures relating to electronic hardware components.

References

[1] IEC 61508, *Functional safety for electrical/electronic/programmable electronic systems*, 2005.
[2] EN 50159, *Railway applications. Communication, signaling and processing systems. Safety-related communication in transmission systems*, 2010.
[3] "*Principles for barrier management in the petroleum industry – Barrier Memorandum 2017*", Petroleum Safety Authority of Norway, 2017.
[4] IEC 61784-3, *Industrial communication networks – Functional safety fieldbuses*, 2016.
[5] J. Åkerberg and M. Björkman, "*Exploring Network Security in PROFIsafe*", Proceedings of the 28th International Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009.
[6] W. Ikram et al., "*Towards the Development of a SIL Compliant Wireless Hydrocarbon Leakage Detection System*", Proceedings of the International Conference on Emerging Technologies and Factory Automation, Cagliari, Italy, Sept. 10-13, 2013, pp. 1-8.
[7] EN 50129, *Railway applications. Communication, signaling and processing systems. Safety related electronic systems for signaling*, 2003.
[8] N. Levinson, "*Engineering a Safer World – Systems Thinking Applied to Safety*", MIT Press, ISBN 978-0-262-01662-9, 2011.