SINTEF

Safe Cooperating Cyber-Physical Systems
using Wireless Communication

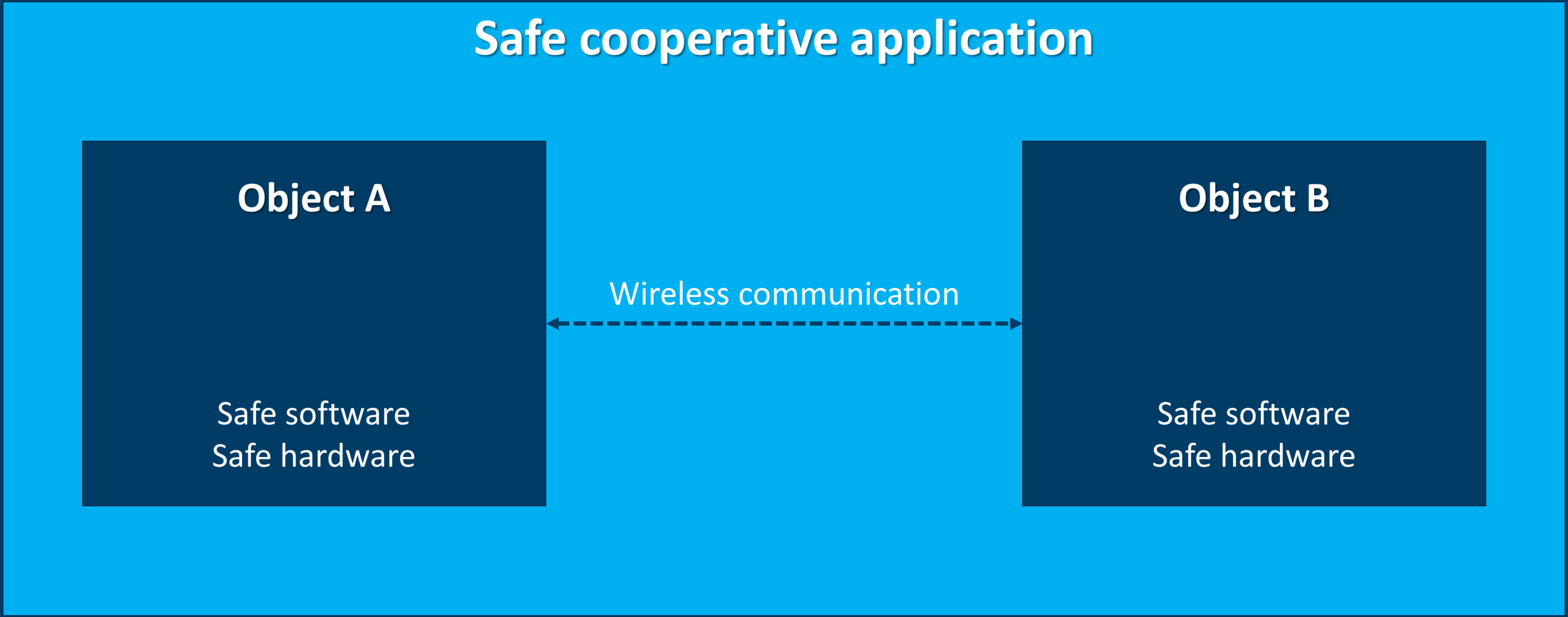
SafeCOP

WP3: Safe Communication

Stockholm, August 29, 2018

Stig Petersen, SINTEF Digital
stig.petersen@sintef.no

SafeCOP Concept



Safe cooperative application

Object A

Safe software
Safe hardware

Wireless communication

Object B

Safe software
Safe hardware

Contents

Information Security

Functional Safety

Safe Wireless Communication

Protocol Development

Information Security

Practice of preventing unauthorized access, use, modification, recording or destruction of information.

Information security protects against malicious threats (hacking, eavesdropping, …)

There are two main concepts used to ensure information security:

- Integrity
- Confidentiality

Integrity

Integrity ensures that information has not been modified in an unauthorized or undetected manner.

Mechanisms for integrity include access control, checksums, and cryptography.

In medieval times, wax seals were used to authenticate official letters, and as proof against tampering.

Prince of Wales signet ring

Confidentiality

Confidentiality ensures that information is not made available or disclosed to unauthorized parties.

Cryptography is used to secure communication in the presence of third parties.

Other techniques for confidentiality include user ID / passwords, biometric verification, and security tokens.

Cryptography

(Greek: secret writing)

Prior to the computer era, cryptography focused on encrypting text, making it unreadable unless the cipher code was known.

The encryption typically consisted of substituting letters.

Julius Caesar used encrypted communication with his generals.

VdihFRS

Modern Cryptography

The computer era moved cryptography from letters and languages to bits and bytes.

Modern cryptography is based on advanced mathematics.

Messages are encrypted and decrypted using digital keys.

Proper management and distribution of digital keys is important to ensure information security.

Contents

Information Security

Functional Safety

Safe Wireless Communication

Protocol Development

Functional Safety

Safety can be defined as the freedom from unacceptable risk of harm to humans, either directly or indirectly as a result of damage to property or to the environment.

Safety can be achieved through various barriers:
Physical barriers, work processes, training and education, monitoring and control systems, emergency response.

Functional safety are barriers in the shape of electrical and programmable systems which must operate correctly in order to ensure safe operation.

Functional Safety

Functional safety can be achieved by adhering to international safety standards.
Safety requirements for different domains are regulated by authorities.

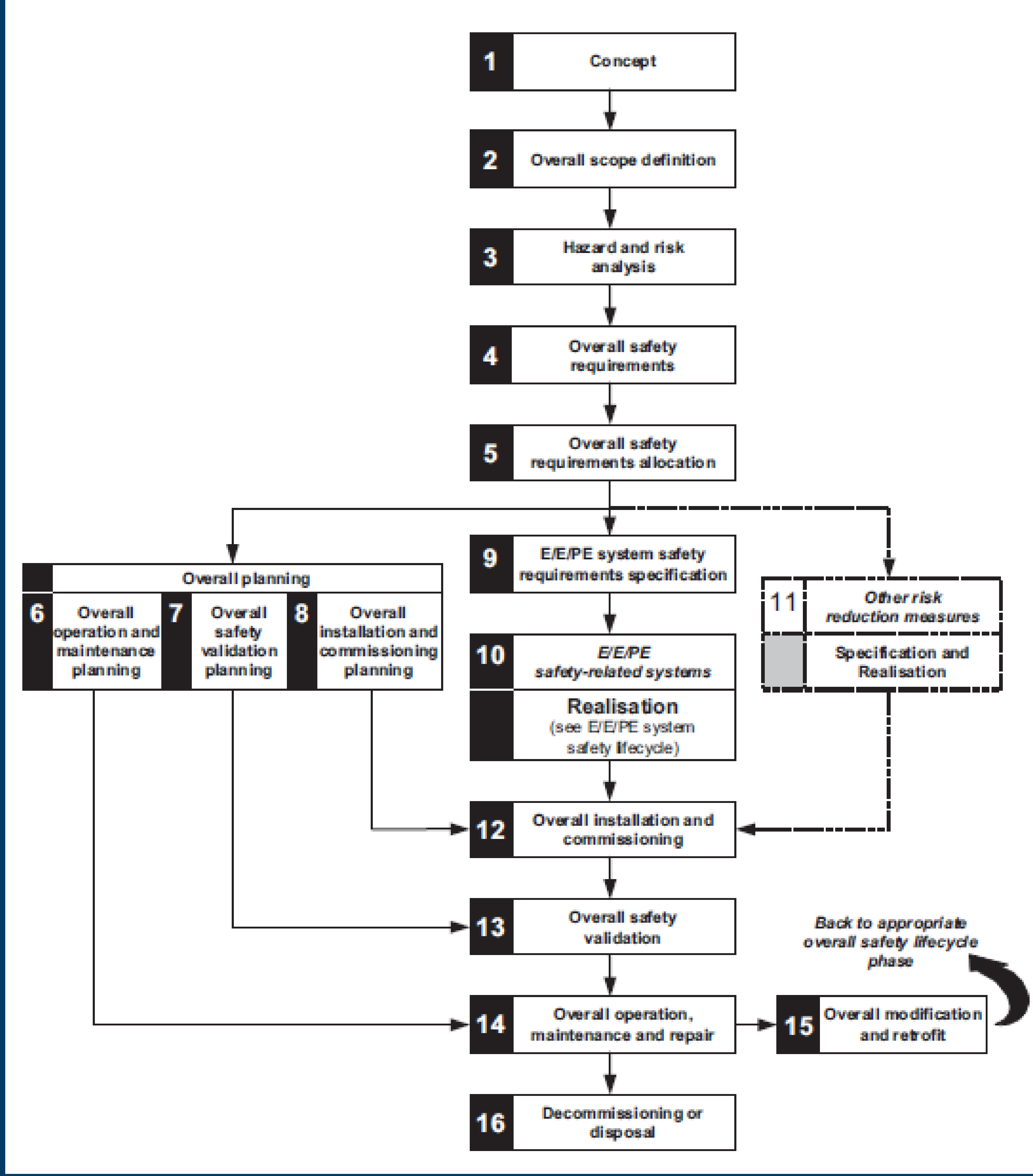
• IEC 61508	Main (generic) standard for safety
• ISO 26262	Automotive
• ISO 13849-1	Machinery
• IEC 62061	Machines
• IEC 60601	Medical
• IEC 61511 series	Process industry
• IEC 60880 and IEC 61513	Nuclear industry
• DO 178C	Avionics
• EN 5012x series	Railway domain
• …	

Functional Safety: Life cycle management

Functional safety requirements governs the entire life cycle of a safety system, from concept and specification, through design and development, to maintenance and decommissioning.

Developing a safety system is much more complex, time consuming and costly than a similar non-safety system.

With functional safety, the perspective is changed from developing technology that works, to developing technology that does not fail.


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation
(see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal

Security and Safety

Security

- Protection from external malicious threats

Safety

- Preventing accidents from internal random faults and failures
- Preventing accidents despite external malicious threats

Security and Safety: Worlds Collide

Security

- Frequent patching to software and firmware to combat new threats

Safety

- Preferably no changes to systems after deployment
- Modifications to safety systems require time consuming re-certification

Contents

Information Security

Functional Safety

Safe and Secure Communication

Protocol Development

Safe communication

A communication system is considered as part of a safety system if the application involves transmission of information between different locations.

For a communication system to be safe, it must be proven and certified according to domain-specific safety standards.

Certification of safe communication systems

According to IEC 61508, a safe communication system can be achieved by:

I. Design, implementation and validation of the entire communication channel according to relevant safety standard.

II. Part of the communication channel is not designed, implemented or validated according to relevant safety standard.

Method II is called the black-channel principle.

I. Certification of the entire system

There are two approaches to certification of an entire communication system:

A. The communication system is under the control of the designer of the safety system.

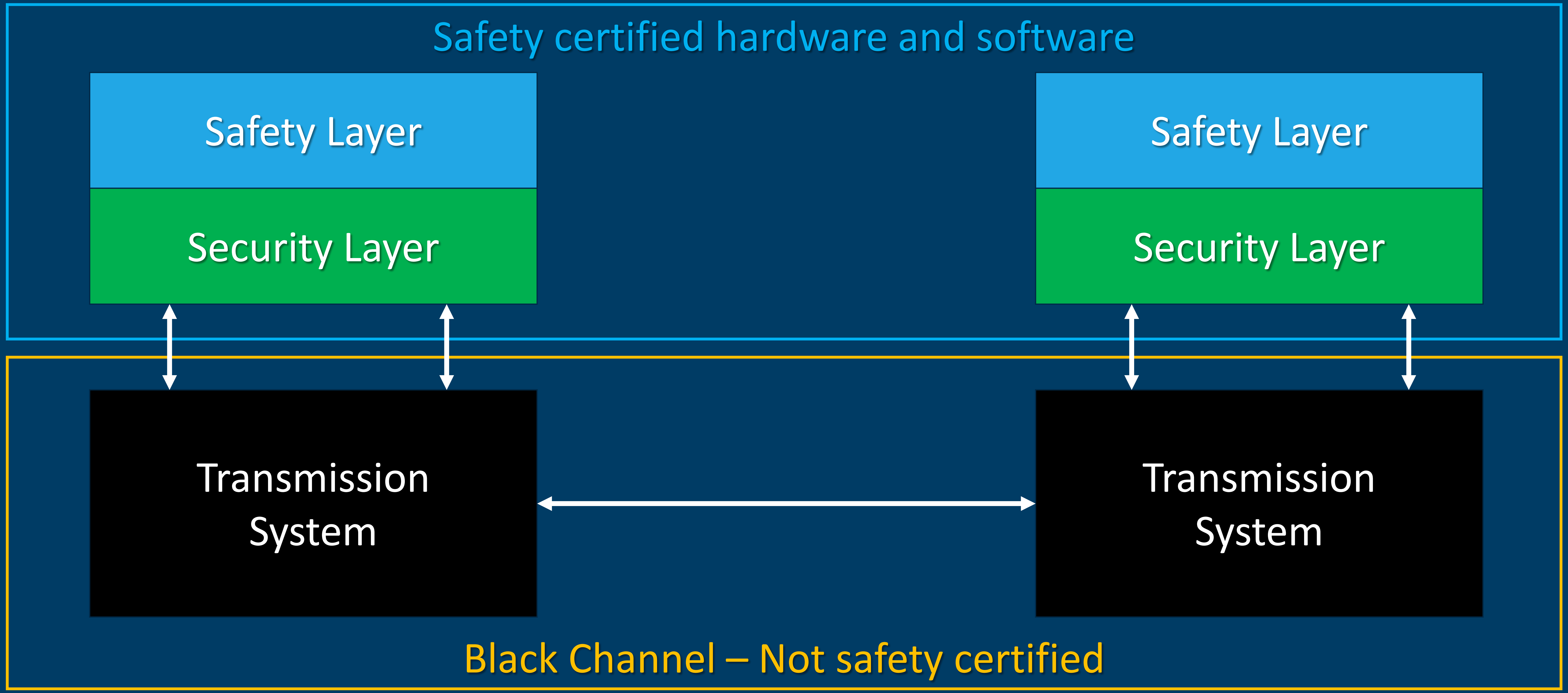
B. The communication system is not under the control of the designer, but it is designed, implemented and validated by a third party.

These two approaches are often not practically or financially feasible.

Approach A requires the safety system owner to build a communication system from scratch.
Approach B requires a third party vendor to go through the rigorous process of safety certifying a product.

II. The black channel principle

The black channel principle is based on applying end-to-end safety and security. This bypasses the need for a safety certified transmission system.



Safety certified hardware and software

Safety Layer

Security Layer

Safety Layer

Security Layer

Transmission System

Transmission System

Black Channel – Not safety certified

Generic standards for safe communication

Inadequate handling of information security

IEC 61784-3: Industrial communication networks

Functional safety fieldbuses

ISO 26262-5: Automotive applications

Product development at the hardware level (Annex D)

EN 50159: Railway applications

Safety-related communication in transmission systems

IEC 61508: Functional safety for electrical/electronic/programmable electronic systems

Refers to IEC 61784-3 and EN 50159 for how to handle safe communication.

Specific protocols for safe communication

IEC 61784-3-3: PROFISafe
SIL3 certified functional safety fieldbuses implemented on top of PROFINET.
Inadequate handling of information security, and potential issues related to patents.

AUTOSAR – Overview of Functional Safety Measures in AUTOSAR
ISO26262-based functional safety considerations (including communication) for automotive industries.

openSAFETY
SIL3 certified open source safe communication protocol for industrial fieldbus communication.
Inadequate handling of information security.

SafetyNET p
SIL3 certified Ethernet-based fieldbus protocol for automation.

Contents

Information Security

Functional Safety

Safe and Secure Communication

Protocol Development

Safety Specification for Communication

Based on evaluations of safe communication standards, EN 50159 is chosen as the foundation for the development of the UC1 and UC2 safe communication protocol.

EN 50159 is mature and well written, and covers all aspects of open and closed communication due to the mobile nature of railways.

The (main) generic standard for functional safety, IEC 61508, refers to EN 50159 for matters pertaining to safe communication.

(IEC 61508 also refers to IEC 61784-3, but it has inadequate handling of security)

EN 50159 Categories

Category 1 **Closed – need not consider information security**

Communication systems under the control of the designer, and fixed during their lifetime.

Category 2

Communication systems partially unknown or not fixed, but unauthorized access can be excluded.

Category 3 **Open – must consider information security**

Communication systems which are not under the control of the designer, and unauthorized access has to be considered.

Wireless communication is always considered a Category 3 system.

Safe communication observations

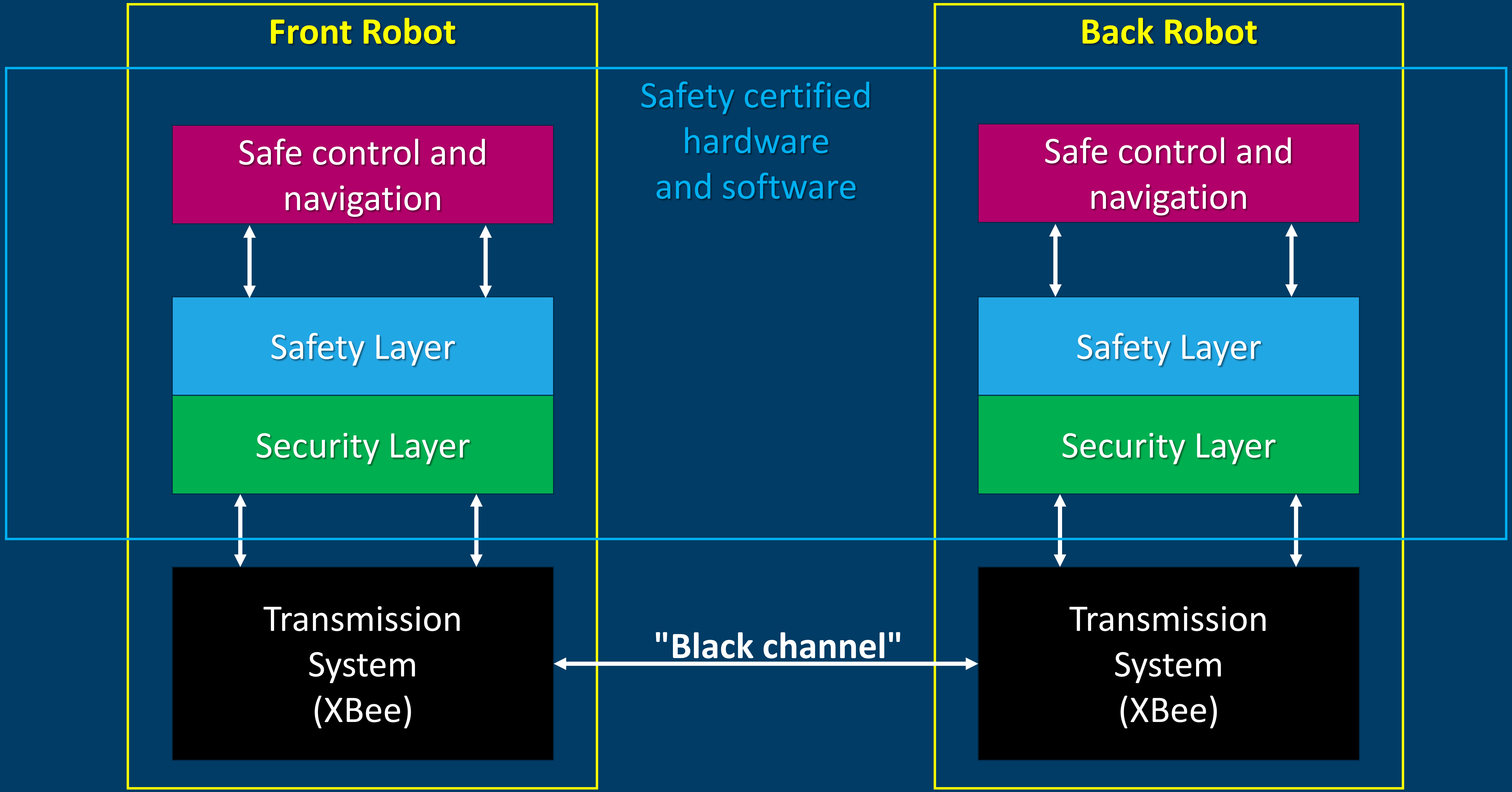
The safety application must consider the following issues:

The safety application is required to have one or more fail-to-safe mechanisms.
E.g. process shutdown, emergency brake, safe-to-shore, evasive maneuvering …

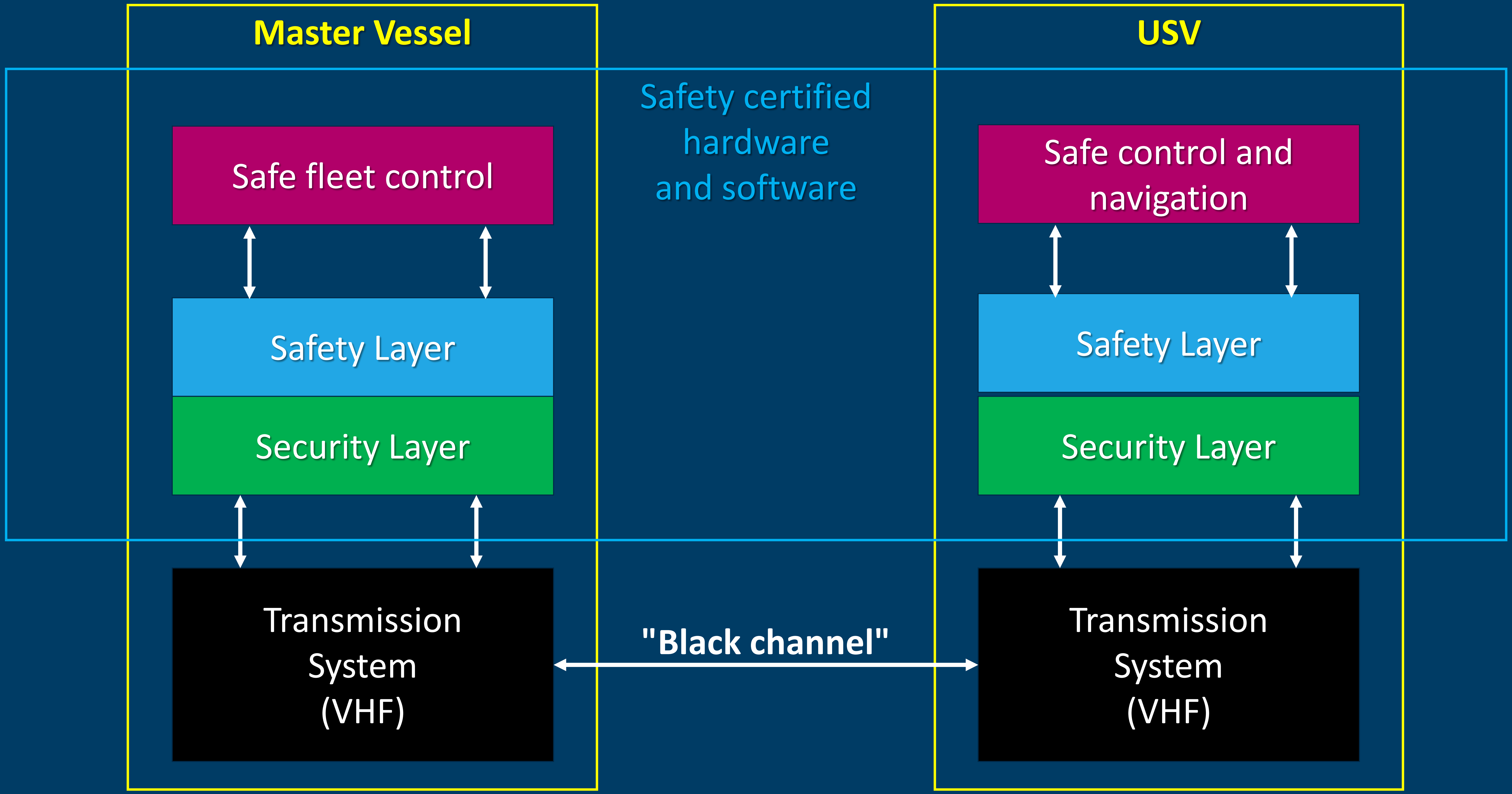
Detected loss of safety-related communication can initiate a fail-to-safe event.
E.g. the communication link suffers from noise, interference, jamming, hacking, …

The safety application may be financially unviable due to frequent fail-to-safe events.
E.g. due to poor communication performance or malicious attacks.

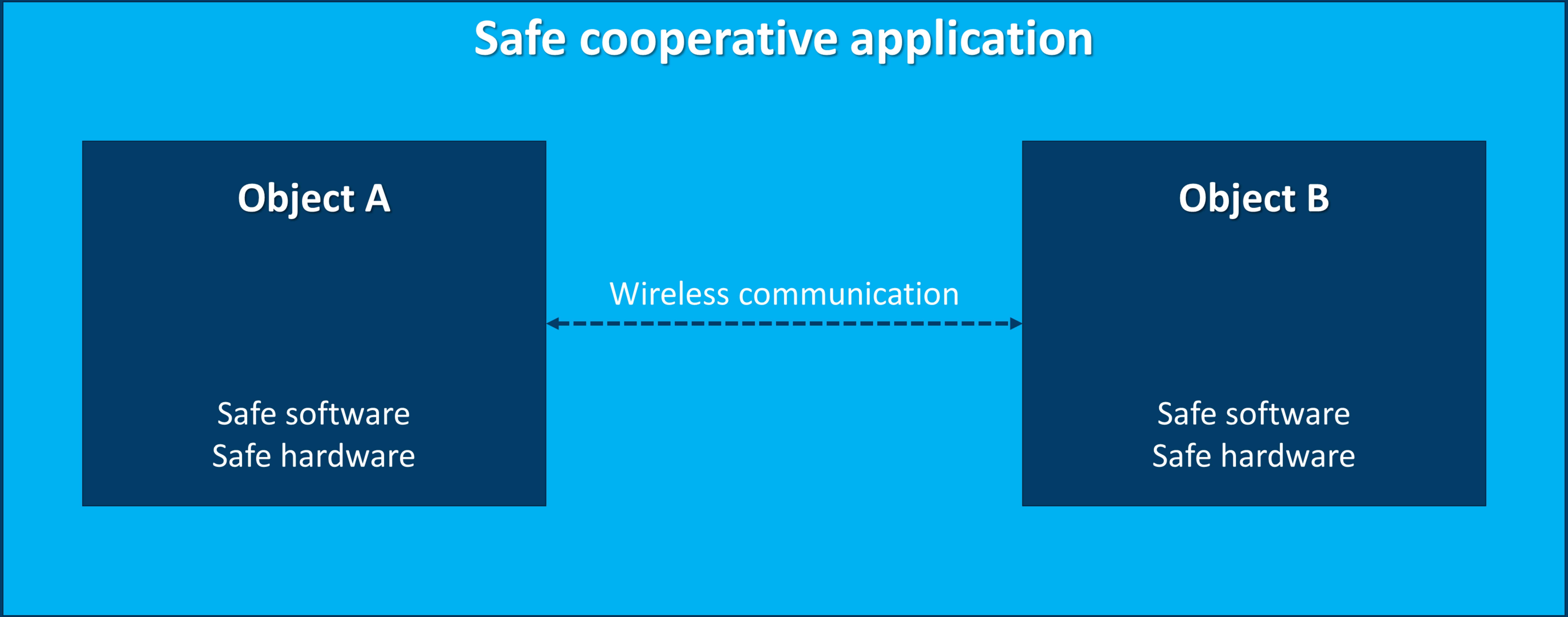
EN 50159 Architecture for Use Case 1


Front Robot
Back Robot
Safety certified hardware and software
Safe control and navigation
Safety Layer
Security Layer
Transmission System (XBee)
Safe control and navigation
Safety Layer
Security Layer
Transmission System (XBee)
"Black channel"

EN 50159 Architecture for Use Case 2



SafeCOP Concept



Safe cooperative application

Object A

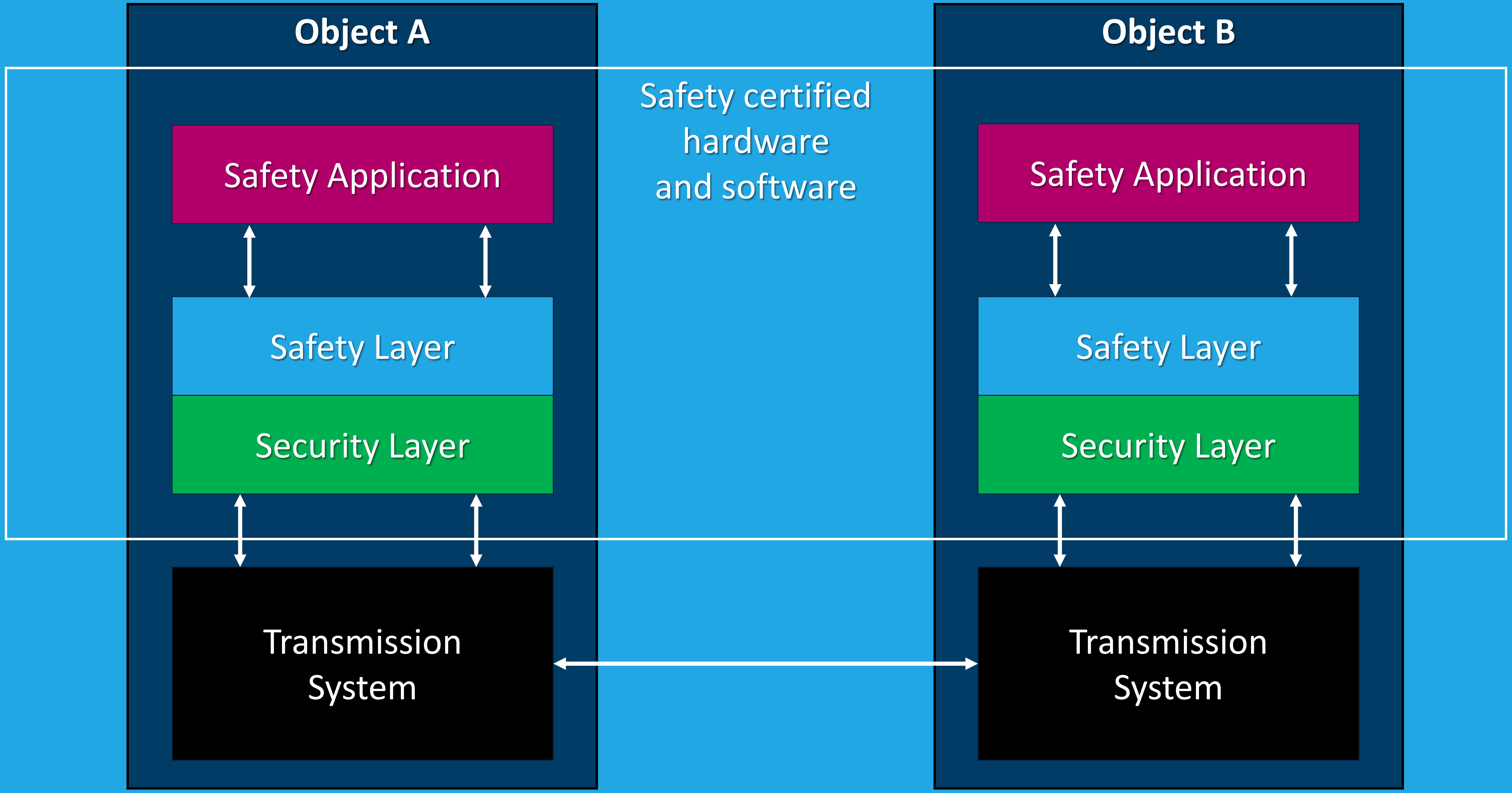
Safe software
Safe hardware

Wireless communication

Object B

Safe software
Safe hardware

Safe cooperative application



EN 50159 Threats to Communication

A communication system can be subjected to a multitude of threats:

Random events

- Broken wires
- Antenna misalignment
- Performance loss
- HW failure
- Human error
- Maintenance error
- Fading
- Fire
- Lightning
- Solar radiation
- …

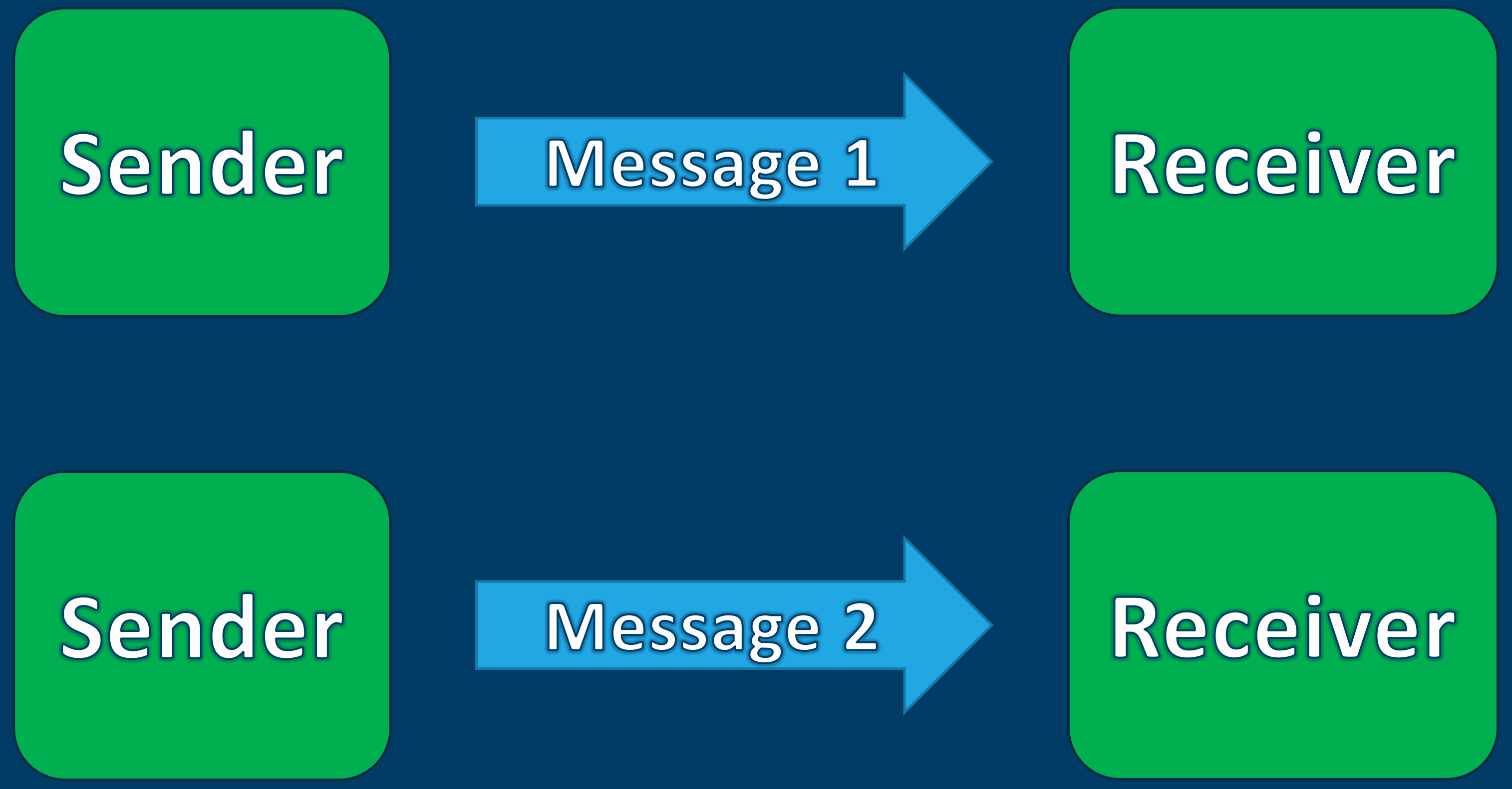
Deliberately caused events

- Wire-tapping
- Damage to HW
- Unauthorized change to HW
- Unauthorized change to SW
- Monitoring of channels
- Transmission of unauthorized messages
- Jamming
- …

EN 50159 Threats to Communication

All random or intentional threats to a communication system will lead to one of the following basic message errors:

- Repetition
- Deletion
- Insertion
- Re-sequence
- Corruption
- Delay
- Masquerade



EN 50159 Defenses

The threats to the communication system have the following defenses:

- Sequence number
- Time stamp
- Time-out
- Source and destination identifiers
- Feedback message
- Safety code
- Identification procedure
- Cryptographic techniques

EN 50159 Certification

The safety case for the safe communication protocol must provide evidence for how the implementation of the different defenses are able to combat the threats to the communication system.

The strength and complexity of the defenses will depend on the safety integrity level (SIL) of the safety system.

A properly designed and implemented safety protocol can achieve functional safety certification.

EN 50159 Implementation

EN 50159 provides specific requirements for the seven defense mechanisms.

The designer of the protocol still has freedom of operation on how to actually implement the defenses according to the stated requirements.

The implemented defenses need to take into account:

- The level of risk identified for each threat
- The safety integrity level (SIL) of the data and process

Defense: Sequence Number

The sequence number is a running number associated with each message exchange between a sender and a receiver.

The following must be considered in relation to the SIL and nature of the process:

- The length of the sequence number
- Functionality for initialization and roll-over
- Functionality for recovery following interruption of the message flow

Defense: Time Stamp

In some applications it might be beneficial to apply a time stamp to transmitted data.

If time stamp is applied in the protocol, the following must be considered:

- 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

Defense: Time-out

In some applications the sender can check the delay between message transmission and the reception of an acknowledgement (ACK).

In cyclic communication the receiver can check the delay between consecutive messages.

If time-out is applied in the protocol, the following must be considered:

- The acceptable delay
- The accuracy of the time-out.

Defense: Source and destination ID

Source and destination IDs are used to verify a valid sender of information.

A separate source and destination ID must be included in the safety layer, regardless of the presence of ID mechanisms in the transmission system.

Defense: Feedback message

A feedback message can be sent from the receiver to the sender if a back channel is available.

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.

Defense: 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.

Defense: Safety code

Safety codes are used in communication systems to detect and/or correct bit errors.

Safety 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 to detect potential message corruption.

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.

Defense: Cryptographic techniques

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

There are three different solutions for cryptographic techniques that can be used by the safety-related communication:

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.

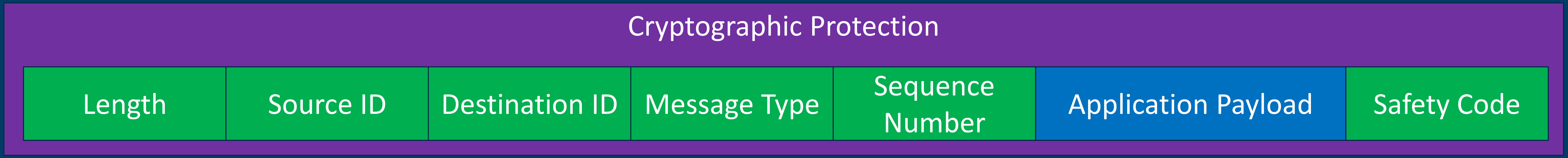
Defense: Cryptographic techniques (2)

The safety case must demonstrate the appropriateness of the solution with regards to:

- Technical choice of cryptographic technique
- Technical choice of cryptographic architecture
- Relevant management activities (e.g. production, storage and distribution of cryptographic keys).

Reasonable assumption shall be described about the nature, motivation, and financial and technical means of potential attackers. Expected technical developments and social developments that are expected in the life time of the safety equipment must also be considered when selecting the cryptographic technique

WP3 Protocol for Safe Communication

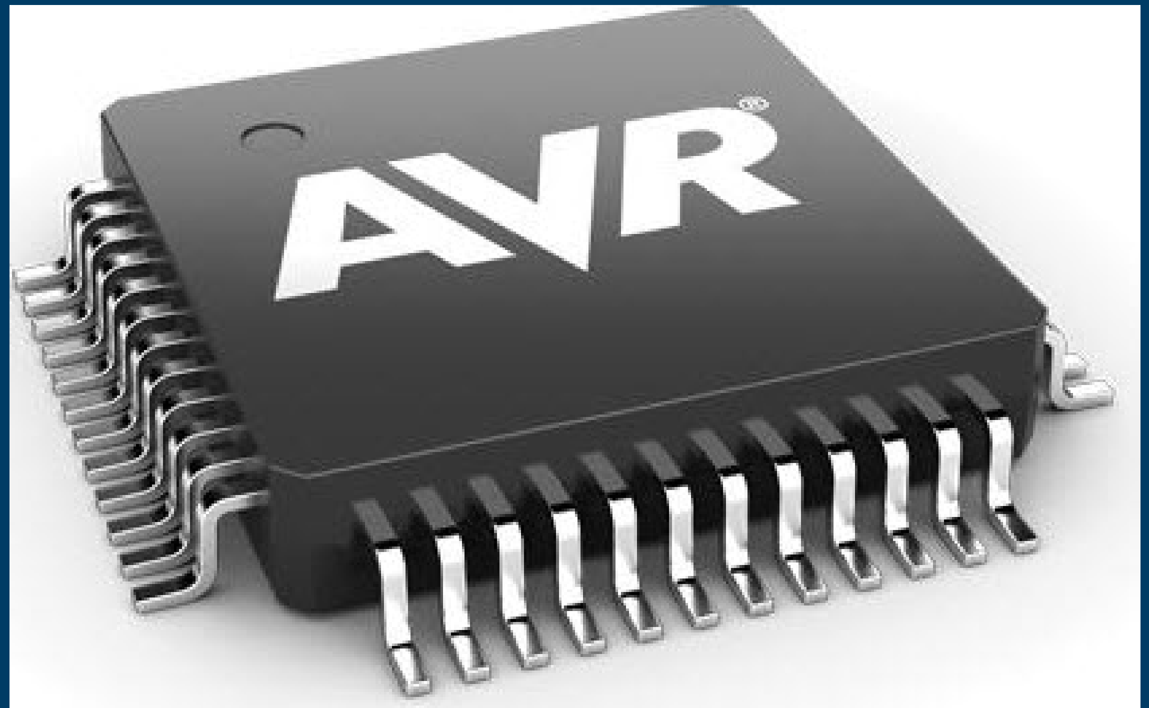


Cryptographic Protection						
Length	Source ID	Destination ID	Message Type	Sequence Number	Application Payload	Safety Code

Additional functionality includes:

- **Feedback message**
  All exchanged messages are verified by an ACK (acknowledgment).
- **Time-out**
  Application "safety time". A time-out will trigger fail-safe if no ACK is received.
- **Time stamp**
  Data may be time stamped (application dependent).
- **Identification and authentication procedures**
  Devices must have clearly defined identification and authentication procedures.

Application-specific considerations



Single MCU (Micro-Controller Unit) architecture

The safety protocol is implemented on the same MCU as the safety application.

Need functionality for memory handling, timing / capacity, concurrency and interrupts.

Dual MCU architecture

The safety protocol is implemented on a dedicated MCU.

Need a safe communication protocol for the connection between the two MCUs.
Solves many of the issues with single MCU architecture, but requires more hardware.

Application-specific considerations (2)

Handling of sequence numbers

The running sequence number can be generated and managed by either the safety application or the safety protocol.

Handling of time-out

The time-out functionality can be managed by either the safety application or the safety protocol.

Status reporting

The safety protocol can report some or all discovered errors to the safety application.

Application-specific considerations (3)

Transmission system (black channel)

The transmission system can be dedicated for the safety protocol, or shared with non-safe communication.

Any potential multiple access issues for a shared system must be handled adequately.

Transmission systems on a separate MCU often has a single API input, e.g. UART or I2C.

Safety certification

All hardware and software must be designed and implemented according to IEC 61508.

Contents

Information Security

Functional Safety

Safe Wireless Communication

Protocol Development

Conclusions

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.

IEC 61508 refers to either IEC 61784-3 or EN 50159 for safe communication perspectives.

As IEC 61784-3 is known to have weaknesses regarding information security, EN 50159 is the natural choice for detailed requirements and implementation guidelines for SafeCOP.

Conclusions (2)

EN 50159 suggests achieving safe communication by applying a safety and security layer on each end node, also known as the black channel principle.

The black channel principle allows the transmission system to be unsafe, i.e. it does not have to be safety certified.

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.

Conclusions (3)

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.

The implementation must be according to the requirements stated in IEC 61508, addressing specification, design, construction, installation, acceptance, operation, maintenance, modification and extension phases of safety systems, as well as procedures relating to electronic hardware components.

Creating a generic safe communication protocol is unfeasible due to the close dependencies and integration to the safety application and the transmission system.

SINTEF

Technology for a better society