norden
Nordic Innovation Centre

NT TECHNICAL REPORT

TR 605
Approved 2007-03

VALIDATION OF SAFETY-RELATED WIRELESS MACHINE CONTROL SYSTEMS

Timo Malm, Jacques Hérard, Jørgen Bøegh & Maarit Kivipuro

NORDTEST
a Nordic Innovation Centre brand

Nordic Innovation Centre
Stensberggata 25
NO-0170 OSLO
Norway

Telephone +47 47 61 44 00
Fax +47 22 56 55 65
info@nordicinnovation.net
www.nordicinnovation.net

ISSN 0283-7234

NT TECHN REPORT 605
Approved 2007-03

Authors:
Timo Malm[1)],
Maarit Kivipuro[1)],
Jacques Hérard[2)] &
Jørgen Bøegh[3)]

Institution:
[1)]VTT Technical Research Centre of Finland
[2)]SP Swedish National Testing and Research Institute
[3)]DELTA Danish Electronics, Light & Acoustics

Nordic Innovation Centre project number:
04143

Title:

Validation of Safety-related Wireless Machine Control Systems

Abstract:

Wireless technologies are spreading also to safety-related applications. Wireless communication is realised by sending messages bit by bit from transmitter to receiver (serial mode communication). This resembles quite much the method used in field buses. There are already several field buses, which are validated to be used in safety-related applications. Many similar risks are relevant also in wireless communication systems, but wireless systems introduce also some new risks and the probability of failures is often higher than in wired systems. When all the risks or threats are considered, safety requirements determined, adequate measures are applied to minimise risks and the system is validated, wireless communication can be relevant possibility in safety-related machinery applications.

Technical Group:
Safety and Reliability

ISSN:	**Language:**	**Pages:**
0283-7234	English	57 p. + 7 appendices

Key Words:
Safety, wireless communication, control system, machinery

Distributed by:
Nordic Innovation Centre
Stensberggata 25
NO-0170 Oslo
Norway

Report Internet address:
info@nordicinnovation.net
www.nordicinnovation.net

Participants:

Finland

VTT Technical Research Centre of Finland
Timo Malm, Senior research scientist
P.O. Box 1300, FI-33101 Tampere, Finland
Tel. +35820 722 3224
Fax. +35820 722 3499

VTT Technical Research Centre of Finland
Maarit Kivipuro
Research Scientist

Sweden

SP Swedish National Testing and Research Institute
Jacques Hérard
Research Scientist

Denmark

DELTA Danish Electronics, Light & Acoustics
Jørgen Bøegh,
Project manager

Executive summary

Purpose of this project was:

- To develop a validation method for safety-related wireless machine controls. The target group was machine builders.
- To find the most common and critical new risks that wireless communication creates in comparison with the risks caused by field buses.
- To find protective measures against the risks and to create methods how to validate the system and protective measures.
- To help machine builders to choose an existing wireless communication system (COTS). When machine builder understands the safety principles it is easier to recognize defects and possibly add some features.

The study has achieved this aim by:

- Utilising results from former Nordtest (Nordic Innovation Centre) projects related to field buses, standards IEC 61508, IEC 62061 and many standard proposals.
- Describing safety principles of communication systems.
- Creating a model for fault propagation in a communication system. The model shows how basic faults lead to message errors and furthermore to system failures.
- Introducing risks related to wireless communication.
- Explaining examples of protective methods against the risks.
- Describing the safety principles.
- Describing the design process of a safety-related communication system.
- Describing validation process of the communication system.

Method

In the study first the existing information about field buses was gathered. In field buses the messages are put through a single channel bit by bit in the same way as in wireless communication. There are also new risks related to wireless communication and such risks were found from literature and in discussions. The design and validation methods were based on methods presented in standards. The design and validation methods need to be credible and credibility is achieved by using standardised methods. Standardized methods are more or less proven in use and this is important in safety-related systems. Protective measures are gathered mainly from the information given by manufactures and protocol specifications.

Main results of the study:

- Wireless communication can be as safe as wired communication. However, more precautions are needed since bit error probability is higher and access to the system is easier.
- The message correctness is the key to the safety. This includes: integrity, authenticity, timeliness and sequencing. Protective measures are needed also to achieve low bit error probability, but the measures do not substitute the measures needed to ensure the messages.
- Systematic methods in design and validation are needed.
- Safety requirement specification is important to remember since major part of design errors are related to safety requirement specification.

Conclusions:

- Wireless communication is becoming more and more common. There are already some safety-related wireless applications. Many of them are related to existing safety buses (field buses designed for safety applications). These wireless links

are becoming common feature in the field buses. Wireless links are becoming common also in many kind of moving working machines.

- The knowledge of the safety of field buses was the basis for the project. There are a lot of similarities in risks and protective measures of wireless systems and field buses. There are also some differences. The designer of wireless system must always consider lost communication, bit errors and access to the system. Risks related to power consumption economy (e.g. sleeping nodes), relaying nodes and unique machine addresses are specific for wireless systems.
- When the limitations of wireless communication are kept in mind, wireless communication is a useful solution for safety-related applications, where wireless properties are needed.
- The target group of this project is machine builders. Wireless technologies are spreading to new applications and it is important to know the possibilities and limitations of the technology. The technology is developing rapidly and new communication protocols are published frequently. This means that one needs to know the basics in order to be able to apply the knowledge to new protocols. Some information of the report may look detailed for machine builders, but it is important to understand the safety principles in choosing commercial systems and adding some features to them. The machine builders are usually not so much developing communication and control systems, but they are applying them in machines. This means that when buying commercial control systems they decide, which technology is going to prosper and this requires lot of knowledge.

Recommendations for continued studies:

- Study for practical use of new principles in safety critical applications. The control systems are developing rapidly. New features of control systems need to be applied also in safety systems. There is a contradiction since safety-related systems should be to some extent proven in use. This is a challenge for pioneers of technology. There is a need to help the pioneers, who want to use modern technology. Also the application can be new although the technology can be mature. This means consideration of new risks.
- Study of design and validation principles for software in safety critical applications. Software is getting bigger and bigger role in safety systems. The current validation systems rely very much on testing and good design practices. There is a standard family for safety-related programmable control systems (IEC 61508), but the means to detect errors are weak. The systems are getting larger and they have more connections to other systems. Although the design and validation methods have developed a lot, in general, the safety of control systems is not getting much better. This is also a reliability issue since the more components and connections a system has the more probable errors are. There is an increasing need to better the reliability and safety of programmable control systems.

Table of Contents

Preface

The project is a joint project between VTT Technical Research Centre of Finland, SP Swedish National testing and Research Institute and DELTA Danish Electronics, Light & Acoustics. It started at the beginning of 2005 and it ended at the end of 2006. The main intention of this report is to help machine builders to choose and design a safety-related wireless communication system. Also a machine builder needs a lot of information about the communication principles in order to be able choose the most suitable system. Some communication protocols are described in this report briefly, but new protocols and new versions of protocols are introduced frequently. Chapters 2-5 contain information about a survey of safety-related wireless communication systems in machinery, risks related to wireless communication and safety lifecycle, which is the base for design. All of these subjects are needed mainly before the actual design phase. Chapter 6 contains information about defensive methods and validation. These issues are needed during the actual design and validation phase.

Definitions

Black channel: communication channel without available evidence of design or validation according to IEC 61508 [14]

Byzantine error: A Byzantine error occurs if a number of receivers receive different (conflicting) values about a real-time entity at some point in time. Some or all of these values are incorrect. [22]

Common cause failure: Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure.[13]

Communicating processes: Communicating processes can be described as a set of concurrent processes that access common variables or that respond to signals or parameters received from other processes. [28]

Communication system: arrangement of hardware, software and propagation media to allow the transfer of messages from application to another. [20]

Concurrency: In systems containing two or more computers, independent processing entities can execute simultaneously on separate processors. The concept of two or more processes operating simultaneously leads to the notion of concurrency. Processes can operate with true concurrency if their executions overlap in time on separate processors. If the processes share one processor, they operate with apparent concurrency. No distinction shall be done in this work, between true and apparent concurrency. [28]

COTS: Commercial Off The Shelf**.** Generally available component (software or hardware) to be moved from one system to another. [29]

Dependability: The dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable [1].
Alternative definition: Trustworthiness of a computer system such that reliance can justifiably be placed in the service it delivers. The service delivered by a system is its behaviour, as its users perceive it; a user is another system (human or physical), which interacts with the former. [24]

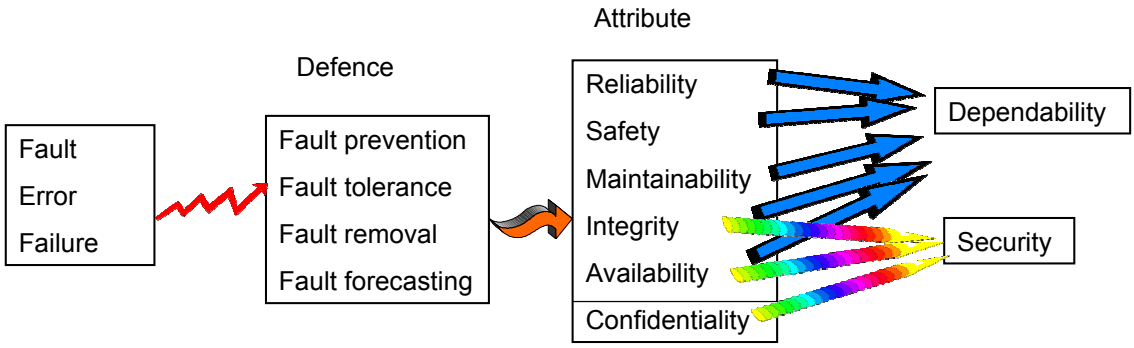


Figure 1.Some ways how to reach dependability. To reach security, also confidentiality must be considered.

In the figure the following terms are used [1]:

Availability: readiness for correct service;
Reliability: continuity of correct service;
Safety: absence of catastrophic consequences
Integrity: absence of improper system alterations;
Maintainability: ability to undergo modifications, and repairs.
Prevention of development faults is a process, which includes development methodologies, both for software (e.g., information hiding, modularization, use of strongly-typed programming languages) and hardware (e.g., design rules).
Fault tolerance is carried out via error detection and system recovery.
Fault removal during the development phase of a system life-cycle consists of three steps: verification, diagnosis, correction.
Fault forecasting is conducted by performing an evaluation of the system behaviour with respect to fault.

Diversify: Different means of performing a required function. Example Diversity may be achieved by different physical methods or different design approaches. [13]

E/E/PE: Electrical/electronic/programmable electronic. [8]

E/E/PES: Electrical/electronic/programmable electronic system. [8]

Error: Part of a system state that is liable to lead to a subsequent failure. It is a manifestation of a fault in the system. [24]

EUC: Equipment under control

Event-triggered system: A real-time computer system is event-triggered (ET) if all communication and processing activities are triggered by an event other than a clock tick. [22]

Fail active: The ability of a system to recover and continue execution after the occurrence of a failure. [22]

Fail halt: The ability of a system to stop after the occurrence of a failure.

Fail-operational (FO): The ability of a system to continue to deliver service in degraded mode and with known safety risks after the occurrence of a failure. [22]

Fail-safe (FS): The ability of a system to reach a safe state after the occurrence of a failure. [9]

Fail-silent: A subsystem is fail-silent if it either produces a correct result or no result at all. [22]

Fail soft: The ability of a system to enter a safe state and continue to deliver service in degraded mode after the occurrence of a failure. [9]

Fail passive: The ability of a system to close down after the occurrence of a failure. [9]

Fail stop: The ability of a system to signal a failure and then stop after the occurrence of a failure. [9]

Fault, error and failure

The basic concepts for dependable computer-based systems are fault, error and failure. Since long they are defined and established in research on fault-tolerant computer systems. In certain respects the terminology differs from the standards for software engineering and for reliability. This is quite natural as the prime interest when studying dependable systems is the handling of defects in a computer-based system

A *fault* is an impairment that exists in the system or in the usage of a system. A fault can be a design defect, an illegal input or a hardware failure. Normally a fault is dormant and if never activated it will never affect the behaviour of the system. Users can perceive a system as perfectly reliable if the faults never are activated and the system always behaves as expected and specified. If a fault is activated it will cause an *error* in the system, which means that the status of the system deviates from the designer's intention. If this erroneous state affects the external behaviour the system fails in giving service according to specification and we have a *failure*.

Faults are always hidden. Only errors can be detected as they in other engineering disciplines can be quantified. Once an error is detected we can:

- confine it, so the damage will not spread,
- diagnose it, so we know what measures to take to and
- treat it, so we can restore the system to its normal state.
- If we do not succeed in error detection and recovery, the error may propagate over the system boundary and cause a failure.

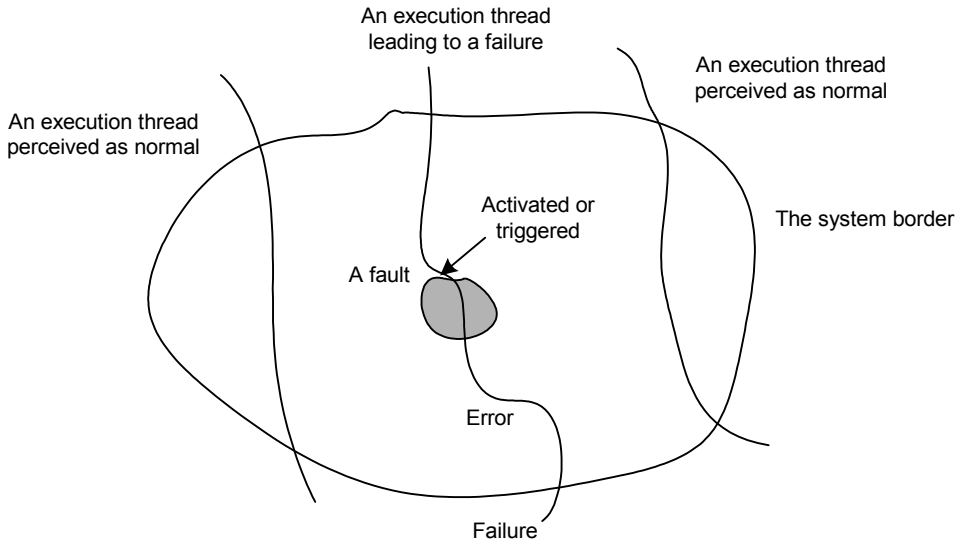


Figure 2. The fundamental fault – error – failure chain.

The notion of fault, error and failure is recursive. A failure in a component of a system is a fault on the next higher level. A failure in an integrated circuit may cause an output signal to be stuck at zero, which is a fault in circuit board. A programmer's failure in writing correct source code for a program results in a fault in the running program. [1]

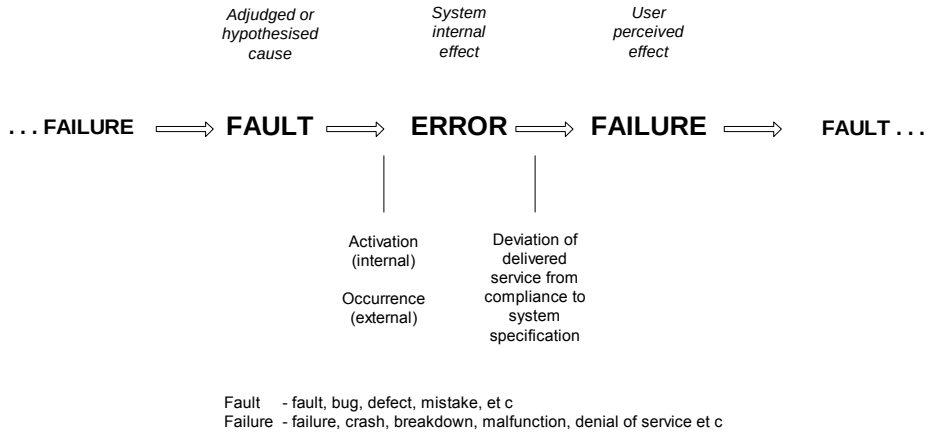


Figure 3. The hierarchical relationship between failure and fault.

Alternative definitions used in hardware technology:
Fault: state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. A fault is often the result of a failure of the item itself, but may exist without prior failure.
Failure: termination of the ability of an item to perform a required function. After a failure, the item has a fault. “Failure” is an event, as distinguished from “fault”, which is a state. The concept as defined does not apply to items consisting of software only. [IEC 60050–191:1990, 04-01] [6].

Fault-tolerance: Ability of a functional unit to continue to perform a required function in the presence of faults or errors. [13]

Firm deadline: A deadline for a result is firm if the result has no utility after the deadline has passed. [22]

FMEA: Failure mode and effects analysis. [18]

FTA: Fault tree analysis. [9]

Functional safety: Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities. [8]

Grey channel: communication channel with some evidence of design or validation according to IEC 61508, but not sufficient for the desired integrity level [14].

Hard deadline: A deadline for a result is hard if a failure can cause loss of the safety function(s) in case the deadline is missed. [22].

Hard real-time system: A real-time computer system that must meet at least one hard deadline. [22]

Hazard: A hazard is an undesirable condition that has the potential to cause or contribute to an accident. [22]

HazOp studies: Hazard and operability studies [13].

Jitter: The jitter is the difference between the maximum and the minimum duration of an action (processing action, communication action). [22]

Maintainability (of a machine): Ability of machine to be maintained in a state which enables it to fulfil its function under conditions of intended use, or restored into such a state, the necessary actions (maintenance) being carried out according to specified practices and using specified means. [5]

Real-time system: A real-time computer system is a computer system in which the correctness of the system behaviour depends not only on the logical results of the computations, but also on the physical time when the results are produced. [22]

Reliability: Dependability with respect to the continuity of service. Measure of continuous correct service delivery. Measure of the time to failure. [24]

Risk: A risk is combination of the probability of occurrence of harm and the severity of that harm [5].

Safety: Dependability with respect to the non-occurrence of dangerous failures. Measure of continuous delivery of either correct service or incorrect service after benign failure.

Safety case: A safety case is a combination of a sound set of arguments supported by analytical and experimental evidence substantiating the safety of a given system. [22]

Safety communication layer: communication layer that includes all the necessary measures to ensure safe transmission of data in accordance with requirements of IEC 61508

Safety-critical system: A system where a failure can cause damage on persons, property or the environment. In [22] this is synonymous with hard real-time computer system.

Safety integrity: The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. [13]

Safety integrity level (SIL): Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [13]

Safety lifecycle: Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all the safety-related systems are no longer available for use. [13]

Safety-related system: A system that:

- implements the required safety functions necessary to achieve a safe state for the equipment under control, EUC, or to maintain a safe state for the EUC; and
- is intended to achieve, on its own or with other safety-related systems, the necessary level of safety integrity for the implementation of the required safety

functions.
[13]

Safety-related control function (SRCF): control function with a specified integrity level (to be implemented by a SRECS) that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s)

Security: Dependability with respect to the prevention of unauthorized access and/or handling of information. [24]

Soft deadline: A deadline for a result is soft if the result has utility even after the deadline has passed. [22]

Soft real-time system: A real-time computer system that is not concerned with any hard deadline. [22]

Software isolation: Software isolation is method that separates COTS software from other software. The method can be based on software or hardware.

SRCF: Safety-related control function.

SRECS: Safety-related electronic control system

SRS: Safety requirements specification

Synchronisation: The mechanism used to satisfy the timing constraints of two communicating processes and the protection of access to shared data. [28]

System: A system is a collection of object, called parts, which are correlated in some way. [23]

Time-triggered system: A real-time computer system is time-triggered (TT) if all communication and processing activities are initiated at predetermined points in time at an a priori designated tick of a clock. [22]

Threat: A potential violation of access protection including safety of a communication system.

Trap Door: A trap door is a link to another part of a program which is unknown to the program developer and which may introduce an extra risk.

Voter: A voter is a unit that detects and masks errors by accepting a number of independently computed input messages, and delivers an output message that is based on the analysis of the inputs. [22]

White channel: communication channel in which all hardware and software components are designed, implemented and validated according to IEC 61508 [14].

1 Introduction

The control systems performing safety functions of machinery have developed a lot during the past decade. During early 1980's the safety functions were realised, usually, by using relays with guided contacts. Some years later came safety relays, which were compact packages containing safety circuits inside. In the middle of 1990's safety logics were approved for safety applications in machinery. Some few years later came safety buses. This meant that serial mode communication can be made as safe as simple wiring. It was possible to use programmable electronics in machinery because the validation methods developed and they became credible. Now there is an increasing need to use wireless technology also for safety purposes. There are already some applications, but after some years there will be more applications available. Figure 4 shows the timeline of safety-related machinery control systems.

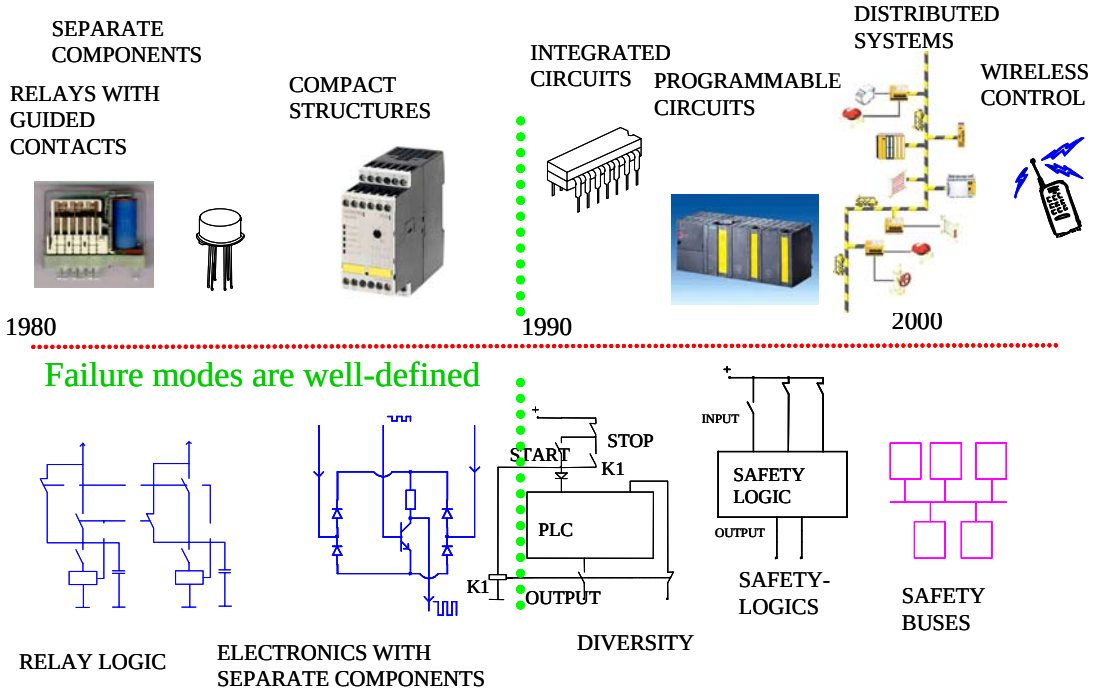


Figure 4. The development of safety-related machinery control systems.

Wireless technologies have been used for several decades for machine control, but safety-related applications are still rare. In safety sense, wireless communication can be compared to field buses. They both offer quick throughput via a single channel. The communication is realised by using serial mode communication, i.e. bits are sent one after another. This technology can minimise the costs by minimising needed wires and in wireless technology wires are not needed at all. In these technologies fairly expensive transmitters and receivers are needed. Now, the price of electronics is going down in comparison with cables and therefore technologies minimising the amount of the cables are getting more common.

Basically, by using different frequencies and modulation techniques air provides huge possibilities to put through messages quickly. However, all frequencies are already determined for a specific use. For most frequencies the user needs also a license. As a result, only a few frequencies with limited bandwidth are available for machine control. On e point is that now very high frequencies are available as technologies have developed and very quicker signals can be manipulated. Also new modulating technologies can pack the messages or make more immune to interfering frequencies.

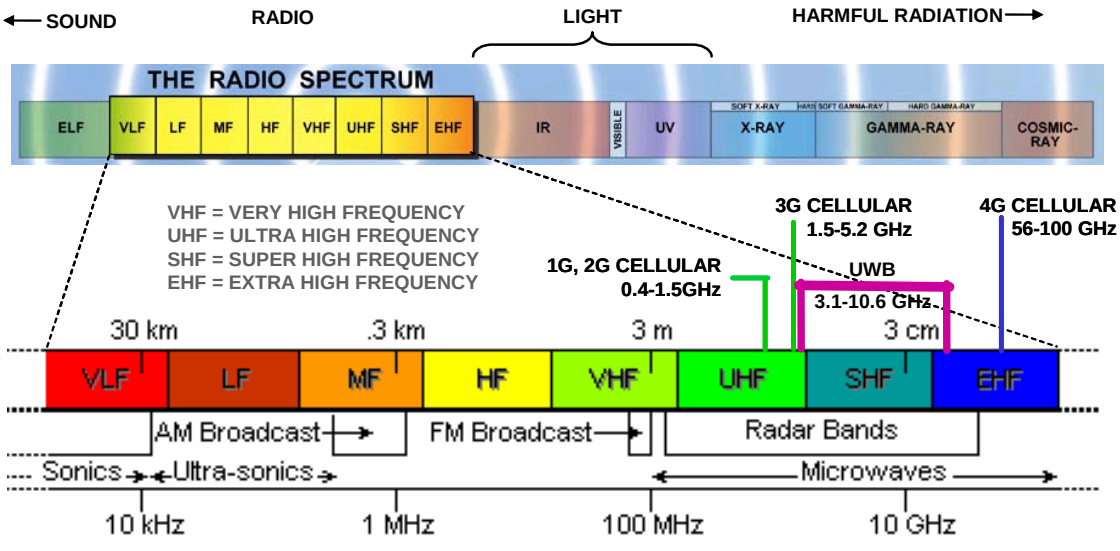


Figure 5. Spectrum of radio frequencies [28].

Wireless communication has got some challenges, which are now more or less solved, but some challenge still exists.

- Radio frequencies are sensitive to interferences. Now, higher frequencies, which do not have so much interference, are available and there are also modulation technologies, which are not so sensitive to interferences.
- Communication rate has been low compared to cables, but the same technologies, which are against interferences, are useful also in increasing communication rates.
- Security has been one problem, because the radio band is easy to access. There are now several features, which minimise the security fears. Encryption key can be fairly long (e.g. 128 bits≈ $3 \cdot 10^{38}$ possibilities), which prevents well accidental intrusions. The modulating techniques can be application specific and wrong technique do not interfere much the communication. The used operation range in common techniques, as WLAN (100 m), Bluetooth (10 m) and ZigBee (up to 300 m), is fairly short.
- Too much and many radio signals may contaminate the environment. This would make radio communication difficult and it may cause some symptoms to nature and persons. The devices, which spreading now are very low power applications and the range is very short. Also EMC directive aims to decrease unnecessary radio signals and interference.

Ethernet inventor Bob Metcalfe mentioned that the networks value increases as its number of connection points increases. This is one advantage wireless communication can offer. [20]

2 Wireless control technology survey

Most now extensively spreading communication techniques (e.g. Bluetooth, WLAN and ZigBee) apply 2.4 GHz wave band. The frequency is licence free in most countries, which is the main reason for its popularity. It allows also quick communication rates. Now, the frequency may become locally quite crowded, since more and more devices applying the frequency are appearing.

The 2.4 GHz frequency is so high that ordinary electrical devices do not cause interference. One point is that water absorbing frequency is quite close to it and therefore microwave ovens apply it. Because of the absorbing effect moisture at the air or rain decreases operation range remarkably.

Frequency hopping spread spectrum radio technology (FHSS) describes (according to IEEE 802.11) means how to tackle reliability and security problems. Basically, in radio transmission the signal is modulated either in amplitude, phase and/or frequency shift to impress the data information onto the carrier wave. In FHSS technology several carrier waves are applied sequentially. The frequency hops from one to another according to a predefined order known by both the transmitter and receiver. E.g. Bluetooth signal can hop from one frequency to another 1600 times per second, while the message length is less than 625 µs. If data is lost during one frequency, the data is retransmitted by using the next frequency. If a specific frequency has a lot of interference, which cause lost data, the frequency can be removed from frequency list. A master node is controlling this exactly scheduled system. [1]

Direct signal spread spectrum technology (DSSS) describes how signal actually spreads to wide band width. This is realised with a high-speed digital bit stream called pseudo-random numerical sequence (PRN) and a XOR gate function. When the RF carrier is modulated with the high-speed digital stream, the result is a spreading RF energy across the frequency band. Transmitter and receiver, which have the same PRN code, can communicate with each other. Therefore many users can use the same frequency at the same time if they have different PRN codes. [27]

FHSS and DSSS have their own means against radio frequency interference and they both have their own advantages. If there is narrow band interference, it may make some frequencies the FHSS is using useless. Only the frequencies not interfered, are applicable. This can cause at least smaller message throughput. For DSSS narrow band interference is not very critical, but the combined (average) noise through the band determines the result (signal-to-noise ratio).

One safety issue related to advanced wireless nets is their self-managing capabilities. Many networks can detect new members and take them as new members to the network. Some networks can relay messages to the final receiver. In these advanced networks, no person knows the exact route the message uses or the exact time it reaches the receiver. This can be critical in some applications. Then one should consider a deterministic wireless communication system instead of a flexible self-organising system. [20]

Figure 6 shows examples of some wireless protocols, which are already at use or which are expected to have products available soon.

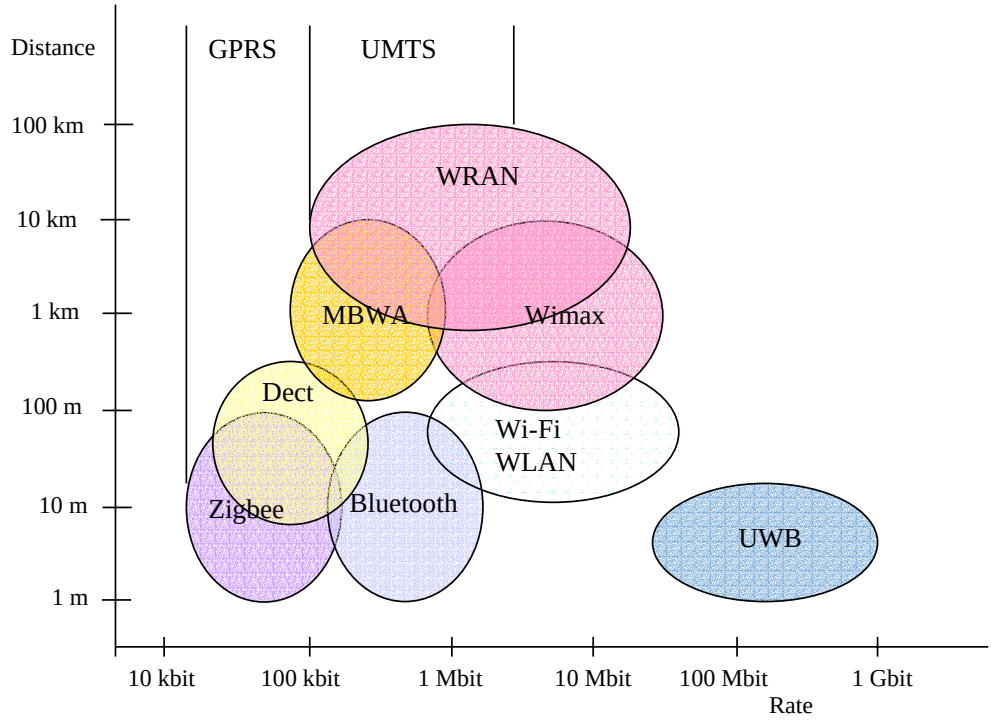


Figure 6. Wireless protocols, their communication speed and operation range.[32]

2.1 Wireless technology

2.1.1 History

At 1971 University of Hawaii made AlohaNet, which was the first wireless computer network. At 1990 AT&T released WaveLAN, which already used Direct Sequence Spread Spectrum (DSSS). The similar technology is used in WLAN.

Nowadays, there are several standards, which define wireless communication and typically the standards evolve continuously. At year 1999 standard IEEE 802.11a defined the basic WLAN. At year 2005 the version IEEE 802.11v is being made. One basic rule in this development has been that there must be a backwards compatibility. At year 2000 there were also some other protocols (HomeRF and HiperLAN), but so far WLAN has been most successful for short range Ethernet-like wireless applications. [22]

2.1.2 Bluetooth

It was Ericsson Mobile Communications that started the development of the Bluetooth technology in 1994. In 1998 a group of companies formed a Bluetooth SIG that would work together to define and promote the Bluetooth specification. The founding members were Ericsson, Nokia, Intel, IBM and Toshiba. Version 1.0 of the Bluetooth specification was released in 1999.

Bluetooth offers digital transmission of both voice and data in the globally available, licence free 2.4 GHz band. It avoids interference and noise from other devices operating in the same frequency band by using the spread spectrum technique called frequency hopping. The communication chances the transmitting/receiving frequency 1600 times per second; using 79 different frequencies between 2400 - 2483.5 MHz.

Bluetooth uses also adaptive power control and short data packets. It normally has a range of 10 - 100 meters. Bluetooth provides a bandwidth of 1Mbit/s at the physical layer.

A Bluetooth connection always has a master and a slave. A Bluetooth network consists of a point-to-point and point-to-multipoint networks called piconets. All the devices in same piconet follow the same frequency hopping and timing rules defined by the piconet master. Bluetooth supports up to 8 devices (1 master, 7 slaves) in a piconet. Two or more piconets can be linked together to create a scatter net, where some members participate in more than one piconet. However, they can only send and receive data in one piconet at the time. Such devices spend a few time slots in one piconet and then few time slots in another piconet etc.

Components are low-cost, small, easy available and consume little energy. Bluetooth focuses on connectivity between large packet user devices, such as laptops, phones, and major peripherals.

2.1.3 WLAN

In 1999 IEEE ratified the specification for IEEE 802.11b, also known as Wi-Fi. IEEE 802.11b defines the physical layer and media access control (MAC) sublayer for communications across shared, wireless local area network (WLAN).

Peer-to-peer (or ad-hoc) mode
This mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points.
This is typically used by two PCs to connect to one another, so that one can share the other's Internet connection for example.

Infrastructure mode
This mode of wireless networking bridges a wireless network to a wired Ethernet network. Infrastructure mode wireless also supports central connection points for WLAN clients. A wireless access point is required for infrastructure mode wireless networking, which serves as the central WLAN communication station.
This is typically used by a stand-alone base-station (such as a Broadband/ADSL connection box).

At the physical layer, IEEE 802.11b operates at the radio frequency 2.45 GHz with a maximum bit rate of 11 Mbps. It uses the direct sequence spread spectrum (DSSS) transmission technique.

2.1.4 ZigBee

ZigBee, pioneered by Philips Semiconductors, is based on the standard IEEE 802.15.4, which was published in 2003. The specification of version 1.0 was released at the end of 2004 by ZigBee Alliance (over 100 companies).

The standard supports 2.4 GHz (worldwide), 868 MHz (Europe) and 915 MHz (Americas) unlicensed radio bands with range up to 75 meters. A ZigBee network is capable of supporting up to 254 client nodes plus one full functional device (master).

At 2.4 GHz there are total of 16 different channels available, and the maximum data rate is 250kbit/s. For 915MHz there are 10 channels with a maximum data rate of 40kbit/s supported; whereas at 868MHz there is only one channel that can support

data transfer at up to 20kbit/s. Data is transferred as packets with a maximum size of just 128 bytes.

The modulation techniques also vary according to the band in use. Although direct sequence spread spectrum (DSSS) is used in all cases, the 868 and 915MHz bands are based on binary phase shift keying (BPSK), whereas the 2.4 GHz band uses offset quadrature phase shift keying (O-QPSK). [30]

ZigBee supports three kinds of network topologies: star, mesh and cluster tree network. The star topology resembles Bluetooth's piconets and has the advantage of being simple to manage. Mesh networks are more like ad hoc networks and offer better reliability because there might be multiple paths between any two nodes. If interference is present in one section, then another can be used. Cluster tree networks are essentially a combination of the former cases.

Components are low-cost, very small and consume very little energy. ZigBee is designed to provide highly efficient connectivity between small packet devices.

2.1.5 RFID

RFID technology is usually used to mark objects and the identification number is read when needed. The same technology can be used also for controlling access, safety devices and functions in cases, where common safety devices are not useful. The technology is not as reliable as most other communication means and therefore some precautions may be needed.

2.1.6 Other existing protocols

ABB has developed WISA (Wireless Interface for Sensors) protocol, which can receive signals from up to 120 switches. Some safety devices and buses can have a fixed point to point communication link in there specification. These communication links offer the same integrity as their wired links.

New communication technologies (standards) are presented often as components get better and faster. However, there are no free frequencies and therefore the current frequencies need to be used.

Table 1 shows properties of some common wireless protocols. Some protocols are new and there are not yet any devices available. Table show that there is a standard for each protocol and there are lot of versions for e.g. WLAN. Some protocols in the table are meant only for telephone use.

Table 1. Wireless protocols and their properties.[32]

Protocol	Speed	Number of participants	Distance	Frequency	Standard	Observations
Bluetooth	1 Mbit/s	8	100 m	2.4 GHz	IEEE802.15.1	
UWB	1 GHz	128	10 m	3.1-4.9 GHz	IEEE802.15.3	
ZigBee	20-266 kbit/s	65000	100 m	868 MHz, 2.4 GHz	IEEE802.15.4	
WLAN (WiFi a)	54 Mbit/s	65000	25 m	5 GHz	IEEE802.11a	
WLAN (WiFi b)	11 Mbit/s	65000	100 m	2.4 GHz	IEEE802.11b	
WLAN (WiFi g)	54 Mbit/s	65000	50 m	2.4 GHz	IEEE802.11g	
WLAN (WiFi h)	11 Mbit/s	65000	70 m	5 GHz	IEEE802.11h	
Dect	384 kbit/s	10-1000	300 m	1.88-1-90 GHz	ETSI Dect	Telephone
Wimax	40 Mbit/s	no limits	10 km	3.3-3.8 GHz, 5.7-5.8 GHz	IEEE 802.16	Products expected
MBWA	1 Mbit/s	no limits	10 km	3.5 GHz	IEEE 802.20	Under development
WRAN	18 Mbit/s	no limits	100 km	1 GHz	IEEE 802.22	Under development
SMS			world		ETSI	Mobile telephone
GPRS	9-160 kbit		world		ETSI	Mobile telephone
3G/UMTS	2 Mbit/s		world		ETSI	Mobile telephone

2.2 Classification of wireless communication systems

Here wireless communication, which is used in machinery, is classified according to communication activities; i.e. one/two-way communication, one/many receivers, straight communication between transmitters or relayed transmission. Safety is here also an issue in classification, since each class have some specific risks. In this way we get the following possibilities:

- one receiver (one-way communication), no feedback,
- many receivers (one-way communication), no feedback
- transmitter sends signal to a device and it sends back its number (e.g. RFID),
- straight well-defined two-way communication between two nodes,
- wireless network in which the communication is between master and devices,
- wireless self-organising network, in which the signal can be relayed from sender to receiver.

The different possible topologies in wireless networks are not considered here thoroughly. The wireless networks are divided to only two kinds of networks. The border between these two classes is a little bit flexible.

<u>One-way communication to a machine (Figure 7)</u>
One-way communication to a machine is used typically in remote control. The operator can see that the machine operates as it should. The operator can do safety measures if the machine operates wrongly. Wireless remote controller has been used e.g. in bridge

cranes for over two decades. The applications are not extremely critical and the machine stops if there is no acceptable signal.

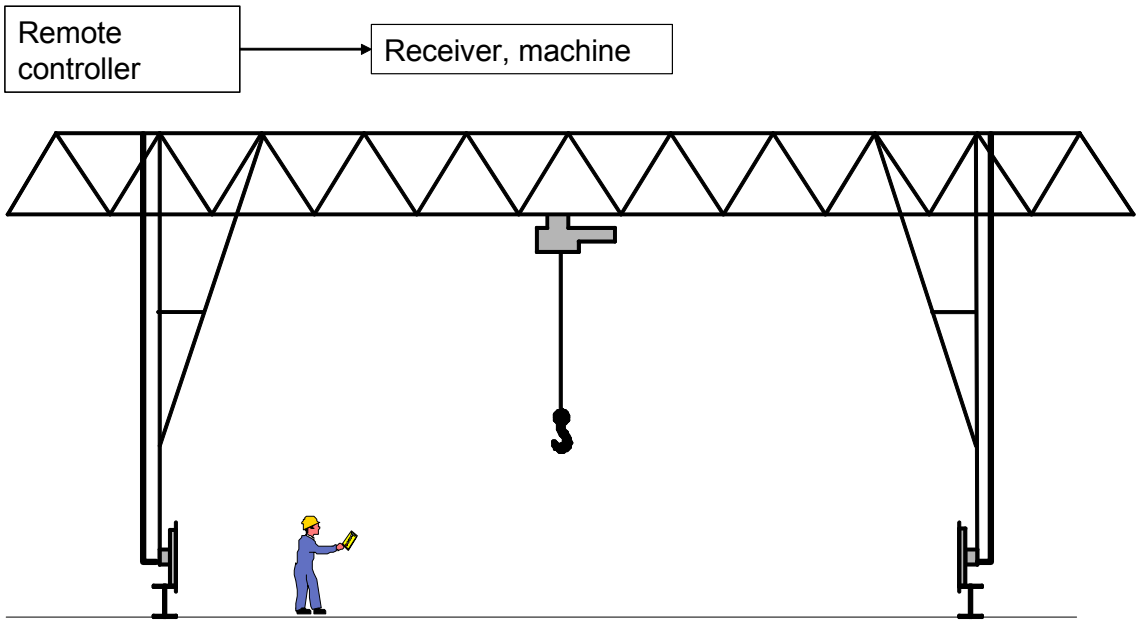


Figure 7. Describes how remote controller sends one-way signal to a crane.

One-way-communication to several machines (Figure 8)

One-way communication to several machines is used e.g. when emergency signal need to be sent to nearby machines. The signal stops all nearby machines. The signal is not called emergency stopping, since the current standards do not allow it (EN 60204-1), however, the function can be similar. After the signal all machines need to be started individually. The signal is not always considered a pure safety measure, but an additional measure to stop quickly machines to avoid a possible emergency situation.

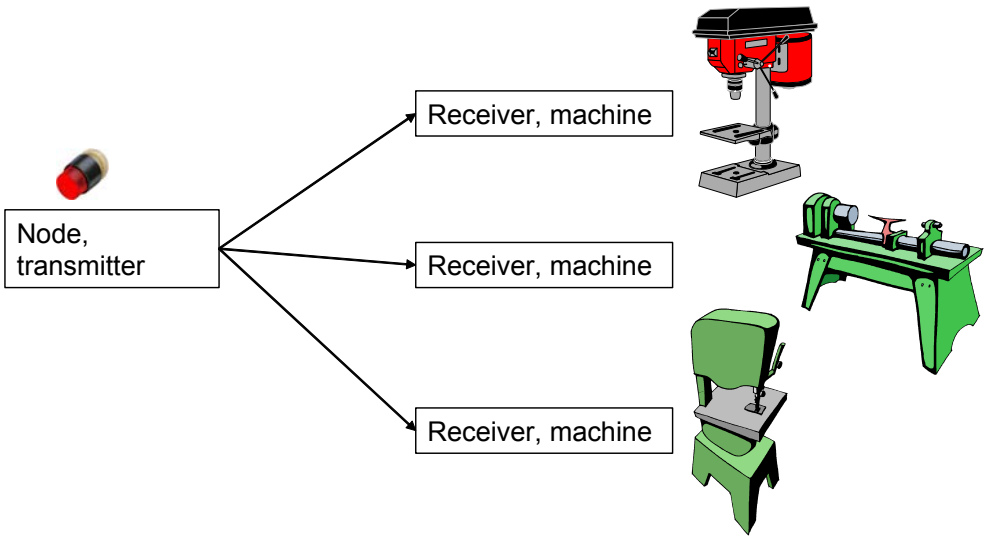


Figure 8. Describes how one signal (e.g. stopping) is sent to all nearby machines.

Two-way communication between two specified nodes (Figure 9)

Two-way communication between two nodes or devices can be highly complex and well-defined or quite simple. In many new applications a tag is mounted to a machine, device or product and it is read by a transmitter/receiver device. In this RFID technology the tag is fairly simple device, which can be either passive or active type.

Passive tag is able to send only its identification number without any modification. Active tag is able to send back its memory and it is possible to modify the memory contents. The applications can be battery-operated or the tags may get their energy from received signal. The distances are from millimetres to several meters.

Two-way communication between nodes can be realised so that a wire is replaced by radio modem communication. All signals coming via wire to one node is sent to the opposite node wirelessly. The signals can be well-controlled and there are also such commercial safety-related applications.

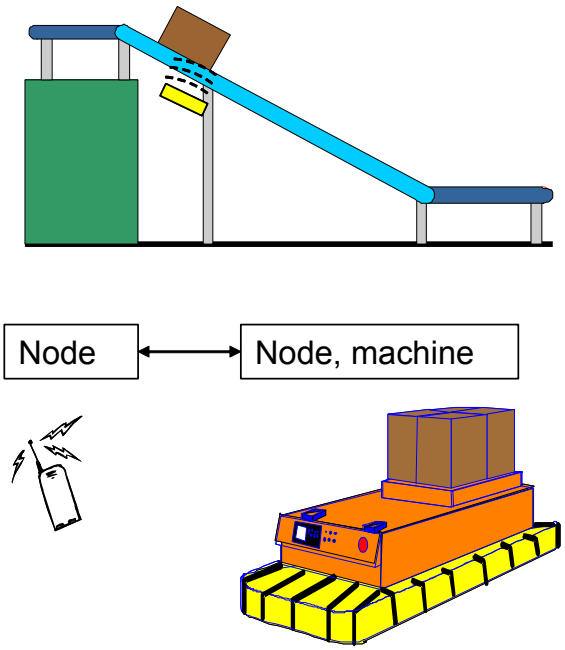


Figure 9. Describes how a wire is replaced by wireless connection. Communication is two-way based. Above a tag in the box is detected by a detector below the conveyor. Below an AGV is controlled with a radio modem.

Wireless network with a master node (Figure 10)

Wireless network with a master node can be well-defined or flexible networks. In well-defined network only predefined members can join the network. In flexible networks all new members, which use an acceptable protocol are accepted to join the network. Bluetooth is a typical this kind of network.

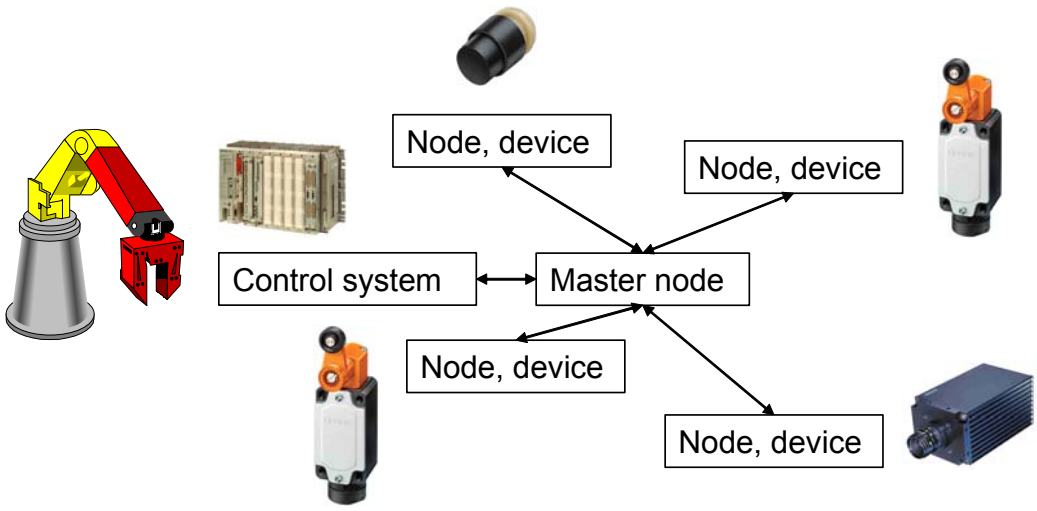


Figure 10. Describes all communication is realised through a master node.

Wireless self-organising networks (Figure 11)
Wireless self-organising networks can well-defined or they may accept new members, which use acceptable protocol. If the receiver of a message is not straight reachable, the network tries to establish connection via other nodes. The routes can even change if a better route is possible. The operator does not necessarily know the used route. Typical this kind of communication protocol is ZigBee.

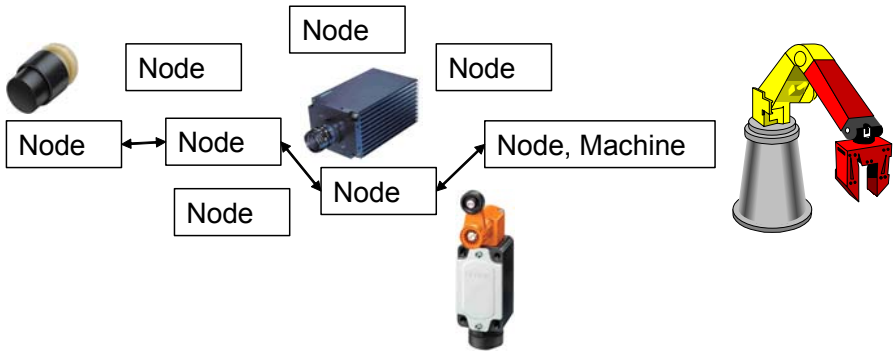


Figure 11. Describes how two-way communication can be realised through several nodes.

2.3 Characteristics of wireless systems

There are some characteristics, which make the wireless communication somewhat different from wired systems. The communication rate in wireless systems is usually slower than in wired systems. This is one reason why the messages are often shorter. Another reason is often high bit error rate. Typically, transient errors cause bit errors. The bit error rate depends on the distance and the environment. These factors can be challenging to designers. The advantages of wireless systems are related the mobility of the system. The nodes can move freely while communicating and it is also quick to install a new network.

2.4 Wireless communication system as part of a complete system

The current section addresses the development of safety-related functions involving wireless communication as an integrated part of a machine control system. Safety functions are specified on the basis of the results of the risk and hazard analysis. The risks and hazards associated with wireless technology depend both on the type of EUC and the operational environment. Such information is suitably provided in the first development phase of the safety lifecycle of the control system.

Section 2.2 of this report presents a classification of the communication models that are commonly applied. The communication models described earlier address exclusively wireless systems. In practice communication systems are hybrid systems that combine wireless and wired communication technology.

As shown in Figure 12 the overall safety function integrates safety sub-functions which are realised by sub-systems and components, in our case: sensor, communication system, logic solving and actuator. The communication system is an integrated part of the safety-related function. In the earlier crane example of section 2.2 the wireless communication system is limited to the exchange of signals between the remote controller and the receiver. Data exchange between the receiver, the logic solver and the actuator uses wired-communication technology. Thus the overall safety–related function in such equipment depends on a hybrid communication system. The block diagram of Figure 12 below presents the general description of an overall safety function.

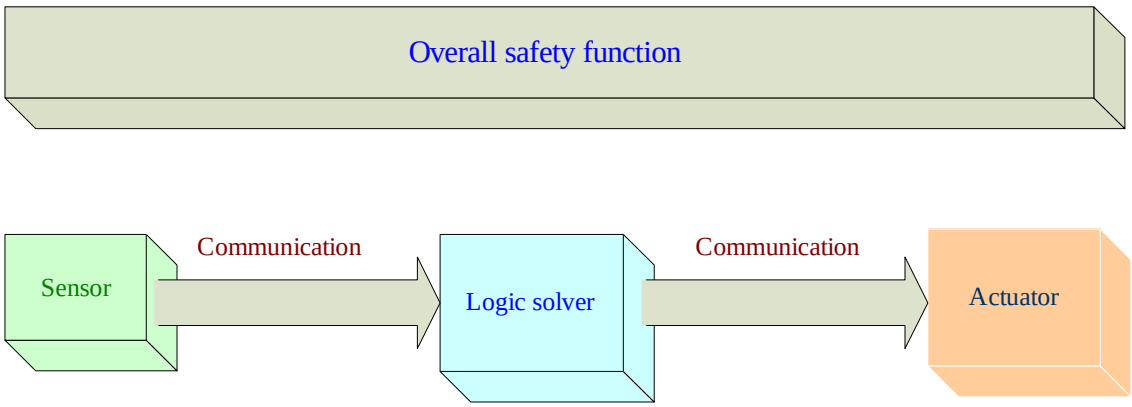


Figure 12. Safety communication as a part of an overall safety function

Depending on the technology used for the implementation of the sub-functions, an overall safety function may coincide to one of the three combinations showed in Figure 13 below.

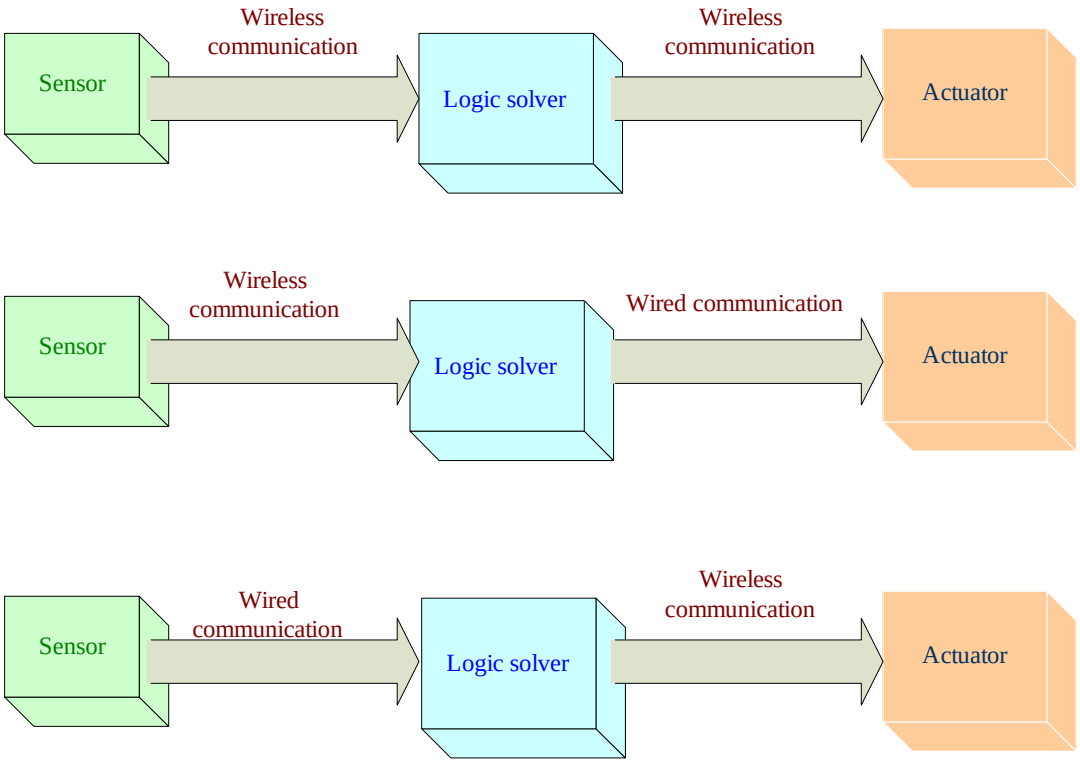


Figure 13 Implementation of communication sub-systems

Similarly an industrial network configuration is presented in Figure 14 below. The safety-related sub-system might use solutions ranging from data-oriented communication like wireless LANs (WLANs), wireless personal area networks [WPANs (Bluetooth)] and wireless sensor networks.

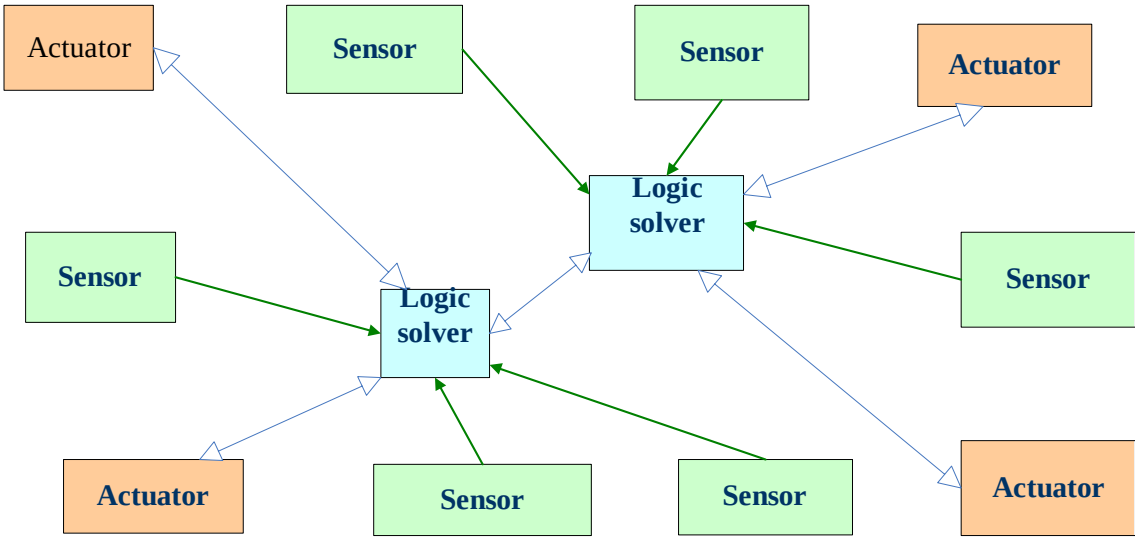


Figure 14. Safety communication as part of an overall safety function in industrial environment

The block models presented in Figure 12 are the basic elements of the context diagrams for the EUC. The complete functionality will be specified in the following development phases of the safety lifecycle.

3 Safety lifecycle

Basically the principles for the development of safety-related systems treated in the IEC 61508 are directly applicable for the development of wireless control systems. In this special work, safety issues are entirely focussed on wireless communication and therefore the need to emphasize the development of system safety within the framework of communication. The safety sub-functions which are part of the safety communication layer shall comply with the requirements of IEC 61508 for the specified safety integrity level of the overall safety functions. This raises certain questions, such as, the allocation of error detection and correction mechanisms, as well as the suitability of certain communication technologies to fulfil the specified safety integrity level.

This chapter shows only a reduced safety lifecycle as described in IEC 61508. Some phases are described in other chapters of this report. The wireless communication is only part of a complete system during the development of which the other development phases are realised.

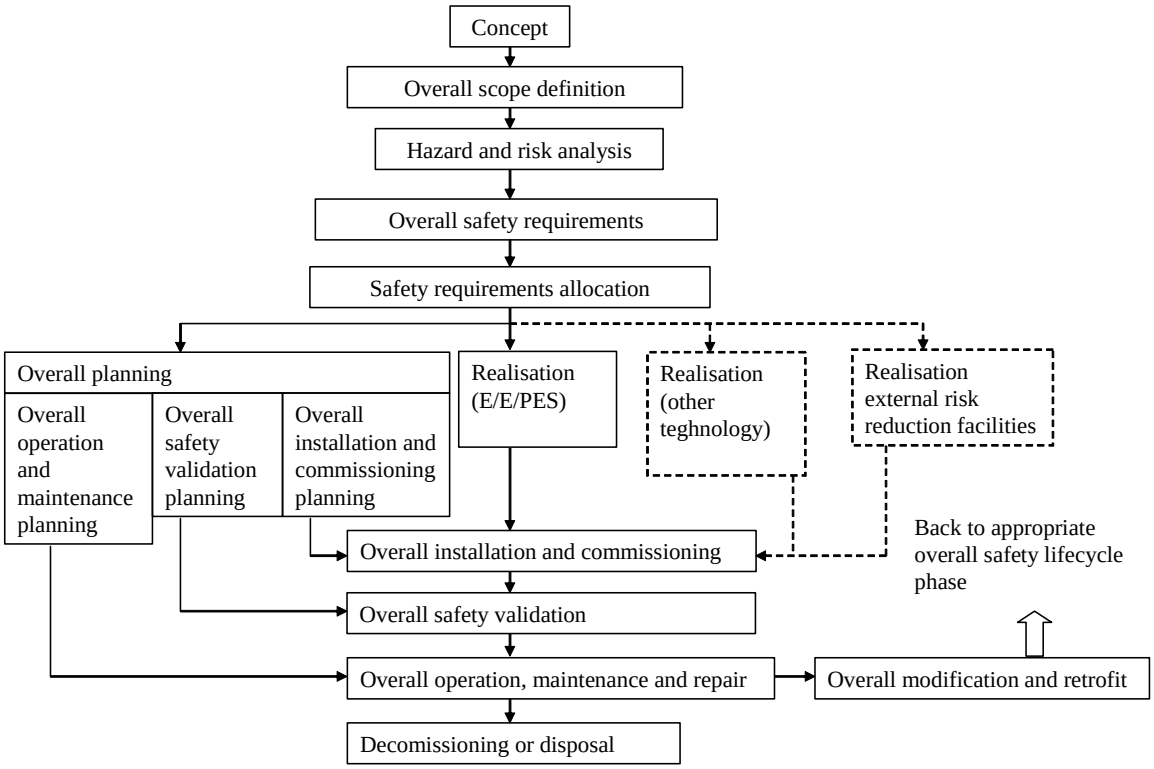


Figure 15. Safety lifecycle.

3.1 Concept

Any information that contributes to ensure an appropriate level of understanding of the current system shall be available. Known restrictions resulting from combination with other equipment or particularities that affect operational performance shall be considered when describing the expected context of use of the current system.
Besides the functional specification set for the EUC, the environmental conditions and further information regarding communication requirements such as amount of transmitting data, frequency of transmission, size of data packets, power consumption etc, shall be provided.

The information accumulated so far is an indispensable input to the risk and hazard analysis. It should be clear in which conditions and by whom the system will be operated.

- EUC with single point of communication characterised by limited number of operational modes and reduced physical extension and velocity of moving parts.
- EUC with several nodes for control of coordinated functions
- EUC using multiple points of communication
- EUC using half duplex communication technique
- EUC using simplex communication technique
- EUC using COTS technology

The objective of this phase is not to detect faults but rather to address safety issues at such an early stage as possible. Is e.g. information concerning the plausible mechanisms for transmission of data available?

The open-loop architecture does not provide feedback from the receiver to the transmitter and thus require the implementation of additional safety features must to make the transmission system robust.

The closed-loop architecture, on the contrary, is a transmission concept that provides the transmitter with feedback information for eventual monitoring and control of possible impairments.

The functional model that is used in this work enables a hierarchic description of control systems and provides the fundament for more detailed analysis. The following diagram (Figure 16) represents the system top level or context diagram.

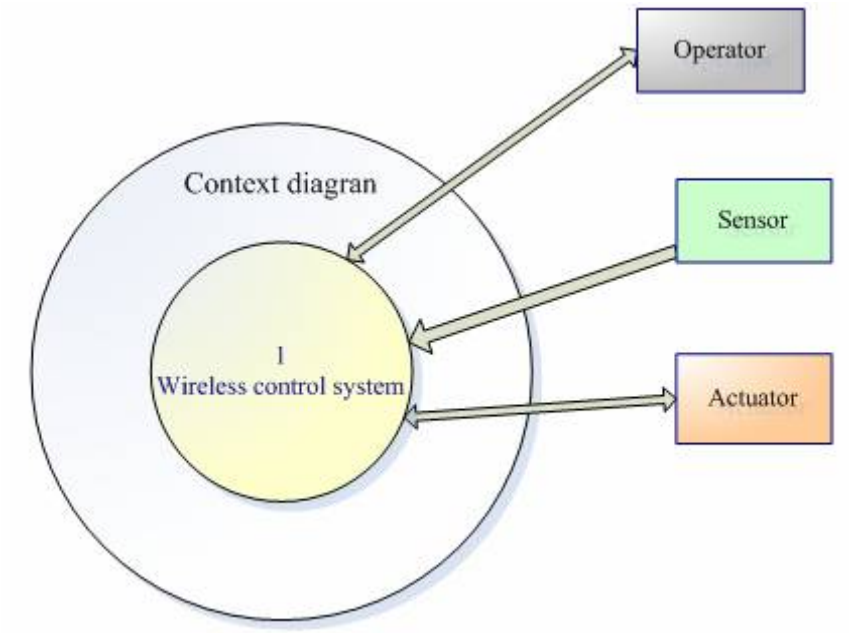


Figure 16. Context diagram.

The context diagram that illustrates the basic functionality and describes the operating environment of the control system provides some understanding of the data flow taking place between the major components of the EUC.

The next step consists of specifying more in detail the complete functionality of the EUC in order to settle the overall scope definition. The arrows in the diagram (Figure 17) show the data flow between components and the arrow-heads indicate the direction of the data flow. The components represented by bubbles are equivalent to processes. That will be developed under the design process.

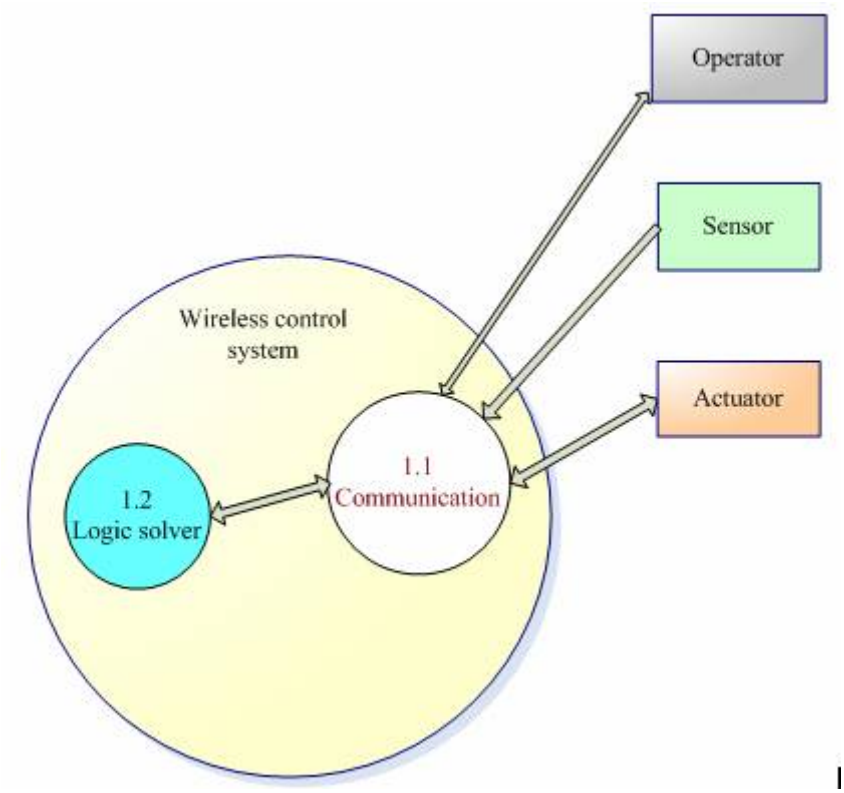


Figure 17. Data flow diagram.

3.2 Overall scope definition

The overall scope definition determines the boundary of the EUC and the EUC control system. The overall scope definition specifies the scope of the hazard and risk analysis. The emphasis shall naturally reflect the impact of the communication system on the initiation of the safety-related functions.

3.3 Hazard and risk analysis

The standard IEC 62061 provides requirements and recommendations for hazard and risk analysis. Hazard and risk analysis contains elements of risk estimation, risk evaluation and risk reduction option analysis. The primary purpose of hazard analysis

is to classify hazards and/or hazardous situations for appropriate further treatment. It acts as a screening technique reducing the number of specific risks, which have to undergo the full process of risk estimation. For complex systems the number of specific risks can be large and evaluation of each one becomes impracticable. In many situations there are established methods for the hazard and risk control of the hazards inherent in the technology, construction and operation of the system. This provides a relatively straightforward way of achieving a satisfactory outcome to the risk assessment process.

However it is unlikely that all hazardous situations can be dealt with in this way and even when established methods are used, detailed risk estimation and evaluation may need to be employed for the specification of certain aspects, for example the allocation of the SIL to safety-related control functions.

HazOp is the most commonly used method for risk and hazard analysis. It is a systematic brain storming process and can be applied for both software and hardware.

In the IEC 62061 standard the hazard and risk analysis is divided into five steps:

System limits
Information on the intended use, space and time limits of the system shall be obtained. This should include:

- a definition of the phases of system life such as operation and maintenance;
- a description of the system particularly in the form of any drawings and diagrams which are available such as isometric, functional, block, flow, graphical etc. - a general arrangement drawing is particularly useful;
- the functional specification of the system and any supporting information, such as technical sales information/sales brochures, video, film or photographs of the machinery;
- the user manual or instructions for use;
- the accident history of similar system (wherever it is available).

Hazard identification
Information on hazards, which are generated, or which can be generated, by the system, shall be obtained. This shall also include hazards associated with operation of the control system(s) used for productive function(s) of the system.

Activity identification and analysis
Each activity carried out by persons, involving use of the system, including foreseeable misuse, shall be identified. For each activity the following information shall be determined or estimated, and recorded:

- training/skill level of person(s) performing the activity;
- activity performed; Each human activity associated with each mode of use should be identified; in particular the presence of a person(s) during each mode of use of the system. In particular activities and interventions associated with non-routine modes of use (for example, fault finding) need to be identified. It is important to determine the probable sequence(s) of activities, including misuse that could be carried out in order to resolve an intermittent malfunction mal-function within for example, a sensor, control system, power control element, and other operative part, on a system.
- status and mode of machine; this could include i) setting (or adjustment); ii) teaching/programming; iii) process change-over; iv) operation (this includes start-up and shut-down of the machine); v) cleaning; vi) maintenance; vii) fault finding.
- duration of activity;
- frequency of activity;

- environmental conditions; this could include temperature, noise level, location (indoor or outdoor),and light level;
- whether use of personal protective equipment (PPE) is specified in the instructions for use of the system;
- whether other persons are expected to be in the vicinity of the system.

Where the information is unavailable or estimates are of necessity unreliable because the circumstances of use are not well defined, the most unfavourable combination(s) from a safety viewpoint shall be assumed.

Estimates of the possibility of defeating or circumventing protective measures

The possibility of defeating or circumventing the proposed protective measures, and the incentives to do so, shall be analysed from a study of the system, its limits and the activities associated with it, and shall be documented.

Risk estimation and evaluation

For each hazard and activity identified, the risk arising from a hazardous situation should be estimated and evaluated. It is particular important to carry out risk estimation when:

- the system can cause harm and the protection is incomplete. A guard provides protection against ejected material up to a maximum energy value. There is a finite probability that this energy value is exceeded
- there are no relevant international standards for the measures used, or where they exist they have nor been followed
- the effectiveness of the risk reduction depends substantially upon correct human behaviour
- no protection is provided.

The methods used to reduce risk should be recorded.

The risk assessment is carried out by analysing the combinations of:

- the severity of the hazard
- the probability of the hazard, which is a function of
    - the frequency and duration of the exposure to the hazard
    - the probability of occurrence of a hazardous event
    - the technical and human possibilities to avoid or limit the consequences

In the standard errors are classified according to the following:

- Error of omission: Failure to perform an action, absence of response
- Error of time: Action performed but not at or within proper time
- Extraneous act: Unnecessary action not required by procedure or training
- Transposition: Correct action on wrong unit , system, train or component
- Error of selection: Incorrect selection control
- Error of sequence: Performance of correct actions in wrong order if this is significant for success of the task
- Miscommunication: Failure to communicate or receive information correctly
- Qualitative errors: By excess or default (perform action incompletely)
- Other: Anything else

For each identified error there are a number of aspects, which should be considered:

- hazard(s) the human error would expose the operator or any bystanders to;
- range of consequences, from most usual to worst, likely to result from the hazard being realized;
- factors that could increase or decrease the likelihood of the error occurring;
- actions/factors that could increase the risk of harm;
- those actions/factors that could decrease the risk of harm, including existing safeguards which will protect against the error being made, or the hazard thus exposed causing harm;

- suggested safeguards required to protect against the error being made or the hazard thus exposed causing harm;
- any other actions that need to be carried out, and by whom.

The analysis will usually lead to new requirements for the system. In addition, the required SIL level will be important for the analysis and derivation of additional requirements.

The standard IEC 61508 defines SIL 1 up to SIL 4, where SIL 4 corresponds to the most severe demands. A safety function that fulfils SIL 4 has a very low probability of not working correct and is developed with very great care. In situations with lower risks it is acceptable to choose a safety function that is more economic to use.

Therefore, the same device, machine or vehicle can have safety functions with different SIL demands. If all safety functions are controlled by the same control system the highest SIL requirement will be the guiding one, i.e. the control system must be designed for the highest SIL. In certain cases, however, it can be good economy to not design the safety functions better than they need to be.

The safety levels are defined by means of the probability for fault (see below table) but this is only part of the contents of this standard. Great importance is also attached to methods in order to avoid design faults and methods in order to deal with faults that occur during operation. The table of Figure 18 differentiates continuous mode of operation and low demand mode of operation.

SIL	Low demand mode of operation Average probability of failure to perform its design function on demand	High demand or continuous mode of operation Probability of a dangerous failure per hour
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Figure 18 Safety integrity levels. Currently, in machinery SIL 4 and low demand mode are not applicable.

3.4 Overall safety requirements

The objective of a safety-related control function (SRCF) is to provide the adequate risk reduction pointed out by the risk assessment. Consequently the safety requirements specification (SRS) for the SRCF is a determining factor to ensure its adequate design and realisation. For each SRCF the communication requirements are specified so that the overall safety requirements are fulfilled. The requirements specification for each selected SRCF shall comprise the following:

a. Functional requirements specification
b. Safety integrity requirements specification

3.4.1 Functional requirements specification

A defined safety-related functional requirement specification shall be produced addressing in detail:

- Safety-related functions which are to be implemented
- External interfaces
- Human-machine interface
- System-internal interfaces
- Initialisation procedures
- Actions in case of power failure or re-start-up
- Assumed operational conditions, including data value range, automatic start-up, normal operation and shutdown
- Required performance characteristics such as response times, accuracy and similar internal self tests (hardware and software) and the actions in case of detected faults
- General conditions (development platform, tools, programming language, version) of the software
- Environmental conditions

In addition to the requirements listed above, following information shall be provided:

- Machine operating mode where the SRCF shall be active
- Machine operating mode where the SRCF shall be disabled
- Priority in relation to simultaneously active functions
- Frequency of operation
- Response time of the SRCF.

Any particular requirements for stopping performance should be specified by the installation designer.

The response time of the control system and the parameters listed below play a central role in the description of the SRCF:

- Interface to other machine functions
- Response time to the input device
- Response time to the output device
- Description of the current SRCF
- Description of fault reaction function and any constraints
- Description of operating environment
- Test and associated facility
- Rate of operating cycles
- Rate of duty cycle.

3.4.2 Safety integrity requirements

Safety integrity is a measure of a SRCF' ability to perform the required safety function within a required period of time. The safety integrity calculation is a function of:

- Failure rate of the components involved
- Proof test interval
- Diagnostic coverage
- Common cause failure
- Safe failure fraction
- Architecture.

It is considered that SIL 3 is appropriate for the highest risk applications in machinery. This corresponds to a 10^{-3} probability of dangerous failure per year.
The safety integrity requirements for each SRCF are specified in terms of a SIL in accordance with the target failure values of Figure 18 above.

The software, program design or functional specification design shall be subject to effective configuration management and change control. During development, effective procedures shall confirm that changes in requirements, specification, design, etc. are adequately documented and that the impact of all changes is analysed to confirm that the specification process remains traceable throughout the design development.
The design development shall be protected from unauthorised change, and its precise configuration (e.g. list of modules, version number) shall be recorded accurately.

When considering the requirements for a particular function, the whole system must be considered. An important aspect that must be considered is the extent to which the human operator is needed to accomplish a specific task.

The SRS is an important document for the designer and for personal dealing with the validation process. Validation personnel have often no detailed knowledge about the design of the SRCF and therefore, the SRS must cover all safety aspects for the actual SRCF. During the validation phase the SRS is used as a reference to check that the safety requirements are implemented in the SRCF.

3.4.3 Information to be available for each SRCF

The safety requirements specification is carried out after SIL determination in the safety lifecycle. In order to create a comprehensive SRS it is important that the required information is accessible to the personnel involved with the SRS set up.

Risk assessment document
Documentation on risk assessment shall describe the procedure that has been followed and the results that have been achieved. This documentation shall include the following information, when relevant:

a) the machinery for which the assessment has been made (for example: specifications, limits, intended use)
- any relevant assumptions that have been made (for example: loads, strengths, safety factors)

b) the hazards identified

- the hazardous situations identified
- the hazardous events considered in the assessment

c) the information on which risk assessment was based

- the data used and the sources (for example: accident that have occurred, experiences gained from risk reduction applied to similar machinery)
- the uncertainty associated with the data used and its impact on the risk assessment

d) the objectives to be achieved by protective measures
e) the protective measures implemented to eliminate identified hazards or to reduce risk (for example: from Standards or other specifications)
f) residual risks associated with the machinery
g) the result of the final risk evaluation
h) any forms completed during the assessment such as the one given in Figure 33 of Annex A

EUC characteristics
Applicable in industrial environments, the cycle time is the time required to generate a given movement pattern.

In a machine, the reaction of moving parts to critical control signals shall be adapted to the safety functions. The measurement of how quickly stopping or starting such a movement pattern takes place is a prerequisite for the set up of the SRCF requirements specification. Such data is obtained with good precision from executed operations with the current equipment. Depending on the conditions of operation, (load, and type of material being processed) the various results obtained establish the current time cycle range.

Safety response times

- Failure detection time
- Safety message delivery time
- Safety response time

The control requirements for initiating and maintaining certain stop modes are important and are application specific. It is necessary to specify stopping performance in terms of time or distance and to provide information concerning inertia and speed-torque characteristics of the parts involved.

3.5 Realisation

In realisation phase the system is designed according to specifications. The system may contain subsystems, which need to be designed according safety lifecycle in miniature size. Typically, COTS parts are applied in design phase. This contains both hardware and software. In COTS components all the lower level layers (according to OSI model) are covered by COTS and the designer need to concentrate on the application layer. After designing the system it need to be realised according to the plans. Usually, subsystems are processed separately so that each subsystem include own lifecycle phases. During the realisation phase all subsystems are implemented to operate together.

4 The risks of wireless communication

4.1 Risks

A wireless system is characterised by being physically disconnected and depending on radio communication between different parts of the system. These characteristics have some obvious advantages, but also some disadvantages. The disadvantages are mainly related to new safety and security related issues where new risks are introduced.

Table 2 Basic wireless communication threats and their consequences.

Basic threats	Consequences
The transmission fades because the distance between sender and receiver increases	Signal level is low. Bit error rate increases. Data is corrupted or lost.
The signal fades because of obstacles	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signal fades because of environment conditions	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances	Signal level is low. Bit error rate increases. Data is corrupted or lost. Inserted new messages.
Two or more signals interfere with each other and cause proper signal for another receiver	Bit error rate is high and therefore an acceptable transient signal can be initiated.
Receiver is too sensitive.	Signal is generated out from noise. Short message can appear.
Poor capability of a relaying station.	The signal can be delayed e.g. due to heavy traffic or extra signal processing in relaying stations.
The nodes understand the network state or configuration differently at the same time.	Consistency and stability problems especially when nodes are moving. Radio B can hear radio C and A, but radio A cannot hear radio C. This may cause confusion
Nearby wireless network is using similar communication protocol.	One node is substituted intentionally or unintentionally with another node
Security; intentional penetration to wireless network	New messages may be inserted
Systematic failure, characteristics of wireless communication is not considered	Almost any of the above mentioned consequences may result
Sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower power consumption i.e. longer battery life.	There is no communication through a sleeping node until the node awakes.

4.1.1 Transmission failures

Repetition: This means that the same message is sent repeatedly. This can mean that the transmitter is unable to send new information or it sends so much information that it fills the whole transmission media and no other communication is possible. Repetition is usually a systematic failure, which cannot be neglected in any communication system.

Deletion: This means that the transmission media is not able to function or there is disturbance so that sometimes the message cannot be received. Deletion can be caused by various kinds of events or errors and it is one of the most common error types and it cannot be neglected in any communication system. Usually detected corruption in a message leads to deletion.

Insertion: This means that a message is received unintentionally. Insertion happens usually when a receiver gets an additional message, which is interpreted to have correct address.

Incorrect sequence: This means that the messages are received in an incorrect order. This may cause a cancelling of a safety function. Incorrect sequence happens usually when the message can travel via two ways from receiver to sender and one way is slower than the other.

Message corruption: This means that data are changed in the message. Corruption can be caused by various kinds of events, errors or electromagnetic interference, which causes one or some bits of the message to change their value.

Delay: This means that data is received correctly, but too late. Delay can be caused by interference or overloaded media.

Erroneous addressing (masquerade): This means that a message is not what it pretends to be. Masquerade is usually caused by misrouting of a correct message or by an unauthorized message (e.g. a malicious message).

4.1.2 Communication system faults

Crash: The system lose its state and halts permanently
Omission: The system gives no response to stimuli, it may later return to normal behaviour
Timing: The system reacts either too early or too late
Computation (Corrupted data): The system provides wrong results
Byzantine: The system behaves in a totally arbitrary manner
Unauthorized access to the system: The access can be unintentional or malicious.

The following table analyses each of the identified wireless system properties. Faults or lack of protective mechanisms may cause one or more of these properties to appear as transmission failures. A transmission failure eventually manifests itself as a system failure. The table provides the most common types of transmission failure for each of the wireless system properties mentioned.

Table 3 Wireless system properties and corresponding transmission failures.

	Transmission failures						
Specific wireless system properties	Repetition	Deletion	Insertion	Sequence	Corruption	Delay	Masquerade
The transmission fades because the distance between sender and receiver increases		X			X		
The signal fades because of obstacles		X			X		
Transmission signal fades because of environment conditions		X			X		
Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances		X				X	
Two or more signals interfere with each other and cause proper signal for another receiver			X				
Receiver is too sensitive.			X		X		
The nodes understand the network state or configuration differently at the same time.							
Nearby wireless network is using similar communication protocol.			X				X
Security; intentional penetration to wireless network	X		X	X			X
Poor capability of a relaying station.						X	
Reconfiguration of transmission path in networks consisting of relaying nodes may affect the correct sequence of sent signals.				X		X	
Systematic failure, characteristics of wireless communication is not considered	X	X	X	X	X	X	X
Sleeping nodes in low power networks.		X				X	

The risk of interference is relatively high because wireless devices typically apply unlicensed communication frequency bands. Even with different technologies there may be interference.

If only one wireless system is used in an area then the risk is reduced. However, it may not be possible to enforce such restrictions. For example, there may be more than one wireless control system in the same place or the wireless control system is used in a place where it is not possible to prevent others to use wireless devices. One important issue is the possible range of the communication. Bluetooth has a range of 10-100 meters.

For example, a collision between Bluetooth and 802.11b occurs when these systems transmit on overlapping frequencies. When 802.11b packets overlap with Bluetooth transmission, the probability of collision is in the order of 50%, which may cause considerable delay. In case of overlap the performance of 802.11b suffers more from Bluetooth transmission than vice versa. This is because Bluetooth transmits short packages using frequency hopping at 1600 hops per second. This hopping process is repeated rapidly across the entire frequency band and hence it spends less time on a frequency channel. In contrast, 802.11b is based on direct sequence spread spectrum that transmits data on a statically allocated carrier frequency.

4.2 Fault models

Each message error occurs because of some kind of basic threat or fault. Without this basic threat all messages would be correct. The basic threats include among others design and modification errors, HW failures and transient faults. To tackle these basic threats system need to be robust, reliable and protected against unauthorized modifications. Furthermore, if all messages are correct and delivered correctly, the communication system would perform perfectly. Unfortunately, message errors occur and error handling mechanisms are needed to avoid further damages. Usually faulty messages are deleted and new messages are delivered and then depending on required response time some other safety functions may be executed. If the message errors are bad enough the communication system fails operate according the specifications. Usually, communication is interrupted because there are not enough acceptable messages. In worst case, the message errors are not detected and the communication system delivers corrupted information, it operates against the specifications or it accepts unauthorized messages. Figure 19 shows how basic threats can lead to message error, which furthermore may lead to communication system threat. The threats and errors are described in previous chapter.

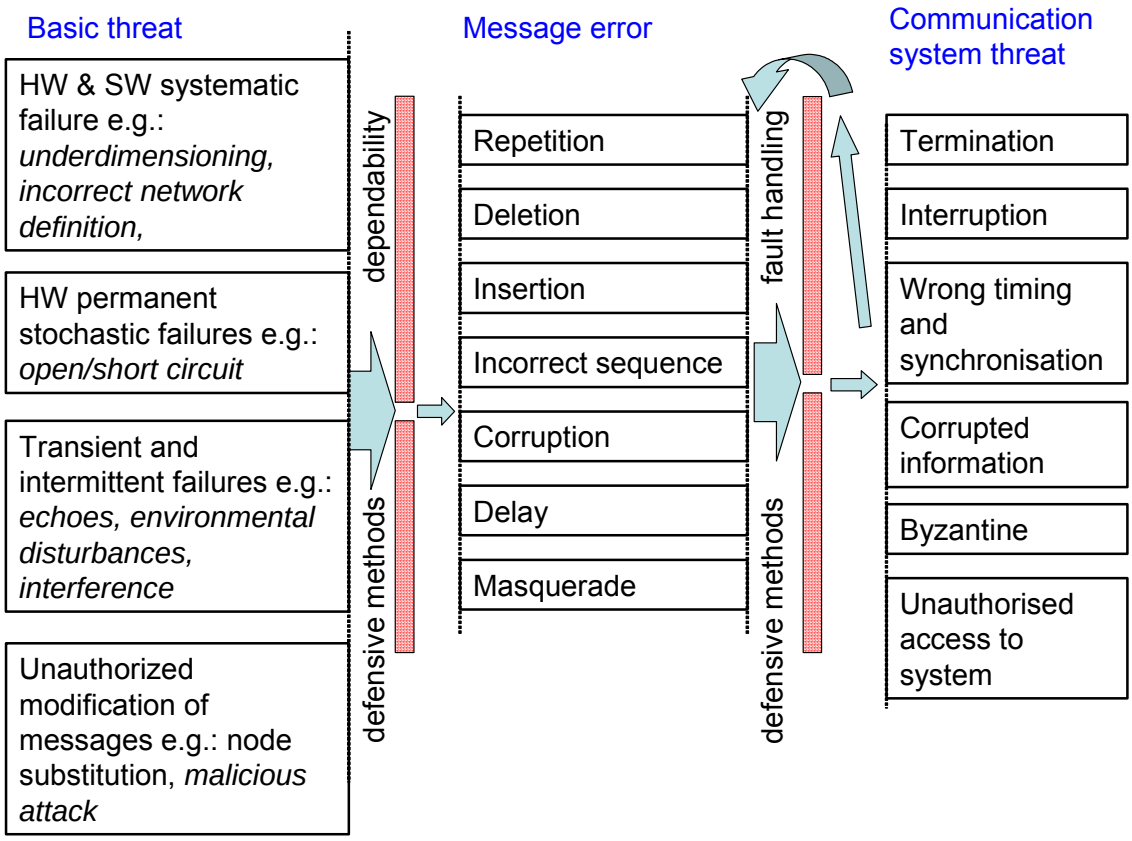


Figure 19. Fault model for wireless communication.

5 Safety principles for wireless machine control systems

Depending on the current architecture: open-loop or closed-loop, adopted for data and signal transmission over the wireless channel; many mechanisms have been developed to increase their dependability and increase their robustness.

5.1 Defensive methods

5.1.1 Basic threats

Systematic failure
Systematic failures are caused by an inadequate design. It may appear immediately or later in a specific situation. Systematic failures are for instance such as underdimensioning, incorrect network definition and antennas misalignment etc. Poor safety requirement specifications cause most of the systematic failures. Systematic failures can be prevented by design principles, systematic methods during the whole lifecycle and validation.

Stochastic failures
Stochastic failures are component failures such as open circuit and short circuits. Defensive methods against stochastic failures are for instance using more reliable components, using redundancy and using protective components against overvoltage, overcurrent etc. Choose equipment and shields which are suitable for the environment; in hostile environment shielded components in cabinets. Preventive maintenance is worthwhile.

Transient and intermittent failures
It is possible to decrease the amount of transient and intermittent failures by using good antennas, interference free frequencies, wideband transmissions capable to detect poor S/N ratio (signal/noise) transmissions, reasonable communication rates and good isolation in signal processing components. Also reasonable worst case response time may help to keep messages going on without error handling procedures. However, when transmission distance increases, obstacles come between emitter and receiver, another transmitter interferes or the environment is otherwise bad for transmission, then the transient failures become probable. It is not correct to trust that transient failures are not possible in wireless systems.

Unauthorized modification
There are two types of unauthorized modifications: system modification and message modification.

The defences against message modification are mainly encryption schemes and error correcting codes. Both are described in section 5.3

System modifications can be either hardware modifications or software modifications. Modifications can be prevented by preventing unauthorized access to the system or elements of the system. For example, the system could be placed in a secure area or it could be encapsulated in a secure box.

Software modifications can also be partly prevented by restricting access. However, this may be more difficult in practice.

Software modifications may be detected by applying checksums or other similar techniques. This means that regularly a checksum of the software is calculated and compared with the checksum of the unmodified software. In case of any discrepancy the original software must be reloaded. This method can detect most software modifications, of course depending on the chosen checksum algorithm. Checksum algorithms are usually similar to algorithms used for hash functions. Such functions have the property that they distribute the values in the input domain evenly on the output domain. In addition such functions should aim at ensuring that if two values in the input domain are close then their respective values in the output domain are far from each other. The size of the output domain of the function indicates the probability for detecting a modification.

5.1.2 Message threats

Many standards, such as, IEC 61508-2, IEC 61784-3 and IEC 62280-1, consider the message-related errors (threat) most essential with respect to safety. One reason is that there are effective means to tackle message-related errors. Furthermore if the message authenticity, integrity, timeliness and sequence were correct, there would not be any problems with communication. The standards state 7 basic errors and in safety-related communication there must be at least one defensive method against each threat. There is no single method, which could tackle all the threats and therefore several methods are needed. Figure 20 shows some examples of defensive methods and how they can tackle the threats, when used effectively.

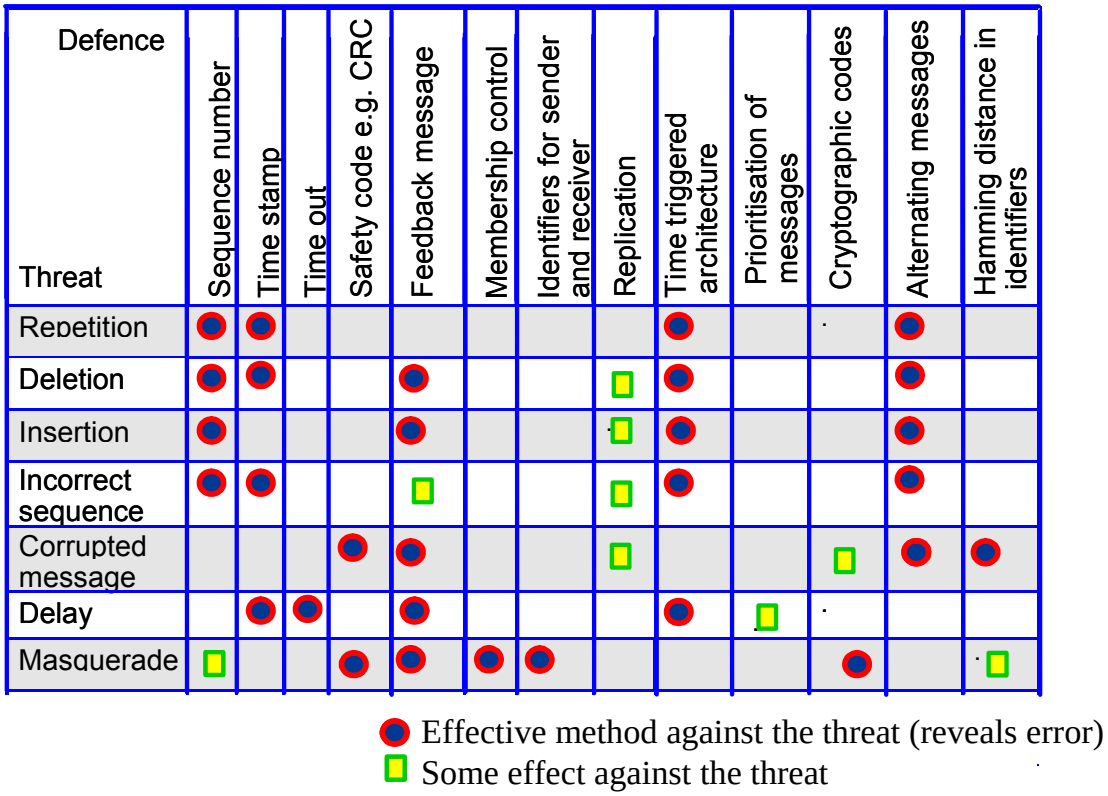


Figure 20. Message-related threats and examples of decencies against them.

Certain type of defensive method can be effective or poor depending on the chosen effectiveness. Here are observations of some defensive methods:
Safety code. The most simple safety code is parity bit it can detect all single bit errors and 50 % of random messages. It is not sufficient to be used for safety purposes as the

only method. Cyclic redundancy checks (CRC) can detect usually all few bit errors (depending on CRC code and message length) and probability not to detect random message bit error is for 16 bit CRC 2^{-16}. In safety-related communication usually 32 bit CRC or checksum is used.

Feedback messages. Feedback messages may contain many kind of information at it affects the effectiveness of the method. If feedback message contains time stamp the transmitter will know when it was received and delays are revealed. If the feedback message contains safety code, the transmitter can calculate if the message were correctly received.

Message replication. Message can be repeated in order to be sure that the message was correctly received. The method is often quite slow since the entire message is repeated. Yet, if the same bit is incorrect in both messages, the information is incorrect.

Alternating messages. It is possible to convert some or all of the bits in a message. This will reveal missing or extra message. It is also possible to pick up acceptable messages from a predefined table. It makes possible to ensure also the integrity of the message, because only certain data is acceptable. This method is used when the messages are very short.

Hamming distance in message parts. Hamming distance in message parts means that only certain predefined identifiers, address codes and messages are allowed. If e.g. one or two bits change in the message an acceptable message will not appear.

Timing information. The message may contain time stamp or sequence number, which shows when the message was sent. If the time stamp is short (e.g. one bit), also the probability of an undetected error increases. The timing information can also mean simply utilization of the receivers clock (nothing in the message). If no acceptable messages are received during certain period of time an error handling sequence is started.

More about the methods are described in “Methods for Verification & Validation of time-triggered embedded systems” [10].

5.1.3 System threats

Basically system threats are a consequence of basic or message threat. The threats cannot be totally avoided. It is possible to reduce the threats by using redundancy in system level. In practice e.g. the following kind of means need to be applied:

- All or part of the communication system is duplicated; this is related to system architecture.
- Correct functioning of the system is monitored. If needed a proper error handling procedure is initiated.
- The system (SW and HW) is designed according to systematic method (see safety lifecycle Figure 15).

5.2 Security issues to support safety

Cryptographic techniques are primarily used in security critical applications. However, there may also be useful applications of cryptographic techniques in safety critical systems. For wireless systems it is obvious to investigate cryptographic techniques for transmission of signals between control and system.

The basic idea of cryptography is to provide algorithms that make it impossible to read a message for anyone but the sender and the intended receiver. Most cryptographic systems apply a key as part of the process, where the key is input to the encryption and decryption algorithm (see Figure 21 and Figure 22).

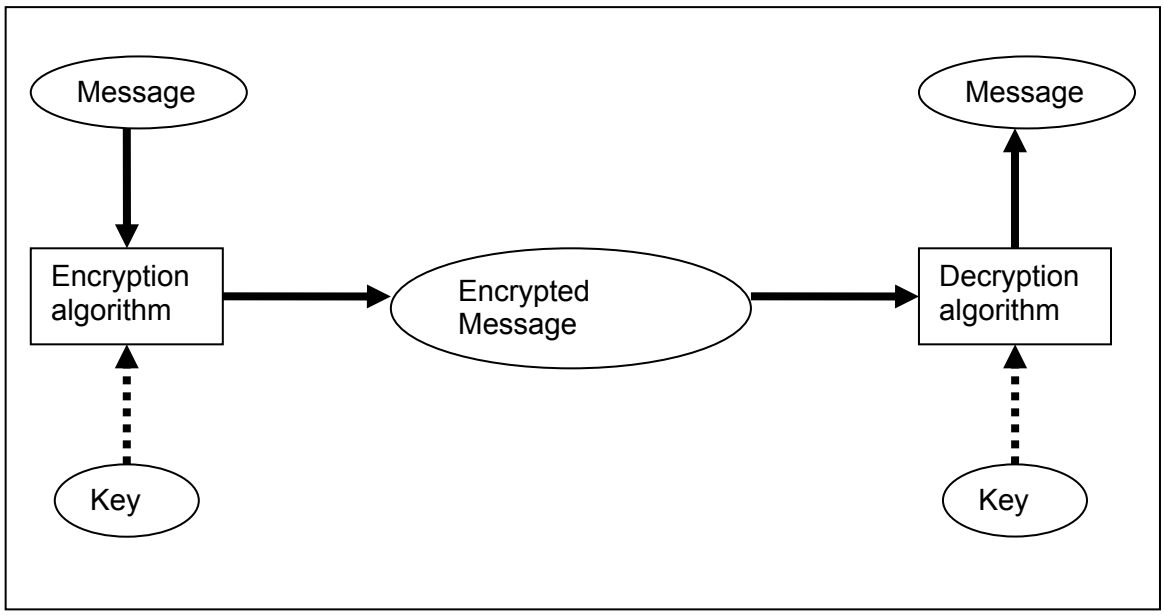


Figure 21. A cryptographic system.

The following very simple example can illustrate the general principle.

Key = 10011100
Message = 00110011

Encryption algorithm = bitwise addition <+>
Decryption algorithm = bitwise addition <+>

Encrypted message = message <+> key = 00110011 <+> 10011100 = 10101111

Decrypted message = encrypted message <+> key = 10101111 <+> 10011100

Figure 22. Example of encryption and decryption.

There are basically two types of cryptographic systems: symmetric and asymmetric cryptographic systems. A symmetric cryptographic system applies the same key for encryption and decryption. An asymmetric cryptographic system applies different keys for encryption and decryption.

For a cryptographic system to work as intended something must be kept secret for everybody except the sender and the intended receiver. In most systems the key is the secret part, whereas the encryption/decryption algorithm is public. When analyzing the strength of a cryptographic system it is usually assumed that the algorithm is known.

Some asymmetric cryptographic systems, known as public key systems, makes the encryption key publicly available, but keeps the decryption key secret. This scheme makes it possible for parties to communicate secretly without having to exchange keys in advance. Public key cryptosystems are usually based on mathematical functions with the property that the inverse function is very difficult to calculate. For example, it is easy to calculate the product of some prime numbers, but it is difficult to find the prime factors of a large number. Generally private key systems (symmetric cryptographic systems) are more efficient than public key systems.

Some cryptographic systems require that the message is divided into fixed length blocks whereas other systems can manage infinitely long strings of text. The DES (Data Encryption Standard) is a well known example of a block system. The DES system was originally published in 1977 by the US National Bureau of Standards and although it is widely believed to include a secret trapdoor, this has never been proved. The DES algorithm is still being used in slightly modified form. The famous Enigma cryptographic system used by the German military during the Second World War is a typical example of a non-block system. The basic principle of this type of system is that an algorithm generates an infinite long sequence of pseudo random numbers with are used to transform the text characters into an unintelligible string of characters.

A symmetric cryptographic system has the property that only senders and receivers knowing the secret key can communicate intelligently. This property can be used in safety critical applications for ensuring that only authorized senders can send messages to a receiver. There are different schemes for implementing this. For example, if a time stamp is attached to a message (command) such that the resulting message is unique. The risk with this scheme is attacks based on replication of messages and the way to reduce this risk is to make messages unique with a time stamp (see Figure 23).

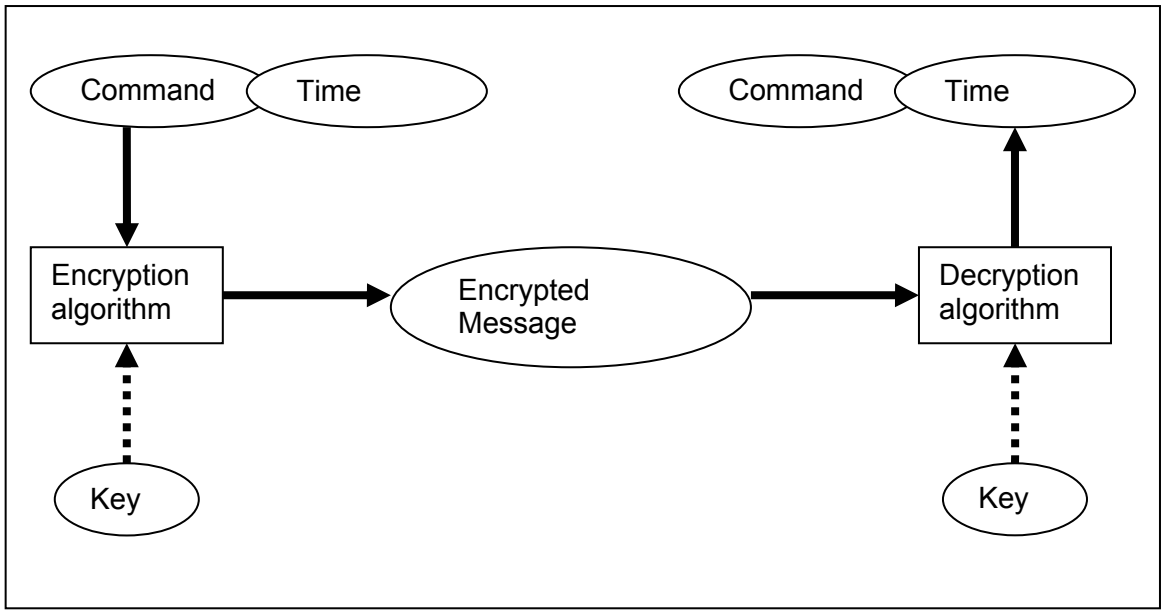


Figure 23. General principle how commands are encrypted and decrypted by using symmetric key.

A problem with this type of scheme is that the encryption makes the communication very sensitive to transmission errors. If the cryptographic algorithm is good is should be expected that a single bit error in the transmission will result in half of the bits in the decrypted message to be wrong. Hence, if problems with transmission errors are not legible then error detection and correction must be applied in addition.

For this type of scheme a block based system seems obvious to use since commands are usually of a fixed length.

An asymmetric cryptographic system can also be applied. For example, a public key cryptographic system can be used in the ‘opposite’ way, such that what is normally the secret key is made publicly available and what is normally the public key is kept secret. The sender then uses his secret key and the receiver uses the corresponding public key. In this way everybody is able to read the message, but only a sender with knowledge about the secret key can prepare the message. In this way the

cryptographic system is used to authenticate the sender and not to secure the message. The authentication scheme ensures that only messages from authorized senders will be accepted. As with other schemes is important to protect against replication of messages. Again this can be done by adding a time stamp to the command, see figure.

The above authentication scheme can be extended with for example a public key encryption scheme, which can ensure confidentiality. Such a double encryption scheme works in the following way: The sender first uses his secret key to ensure authentication. This message is then encrypted using the receiver's public key before transmission. When receiving the message the receiver first applies his private key to encrypt the message and then the public key of the sender to ensure authentication.

It should be noted that there are different possible cryptographic schemes that can be used as sketched here (see Figure 24).

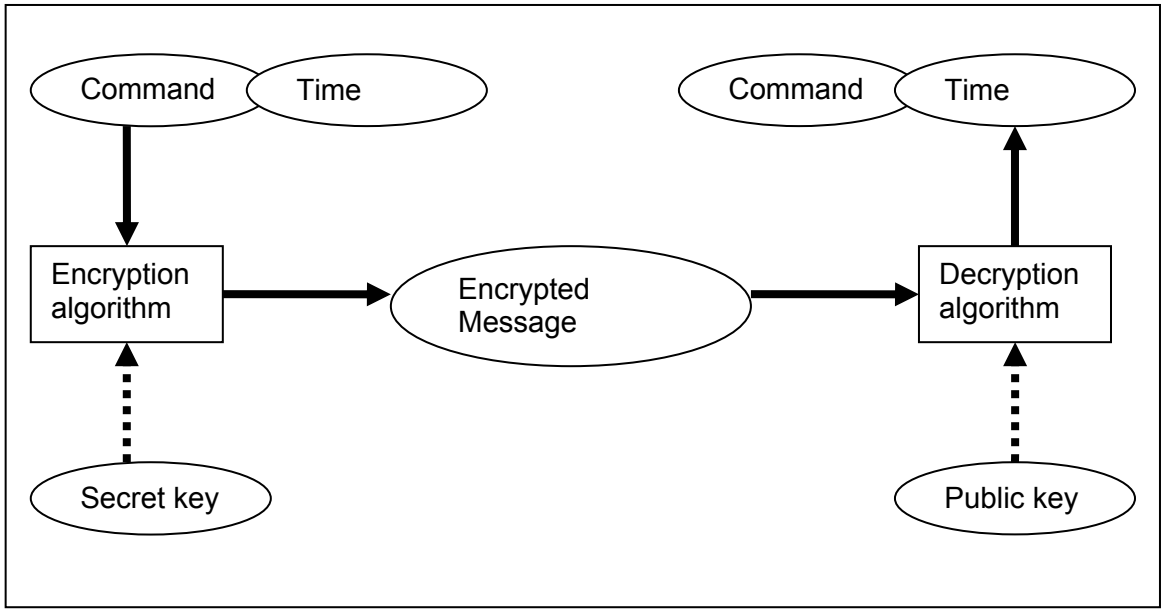


Figure 24. General principle how commands are encrypted and decrypted by using public key.

Generation and distribution of cryptographic keys is called key management. Key management is often a problem area for cryptographic systems. It is very important to pay much attention to this aspect. If secret keys are not kept secret or if they are easy to guess it does not help much to use a very strong cryptographic algorithm. The best way is to generate keys randomly, for example by using random numbers. The second best solution is to use a pseudo random number generator. Manually generated keys will often be easier to guess and should therefore be avoided. Also it is very important to ensure that unauthorized persons or equipment can get access to keys. The weakest point is generally distribution of keys. This aspect has been studied and a number of schemes have been suggested. They are of course involving a cryptographic system. It is assumed that the key distribution cryptographic system is less vulnerable to attacks since it is used entirely to send randomly generated keys. In addition such a system will have less time constraints since key distribution is not time critical.

The frequency of key change also affects security. As mentioned above key distribution is a potential weak part of the security of a system. Frequent key changes may therefore be a potential threat to system security. On the other hand, if the same key is used for a long time it may encourage possible hackers to invest effort in reconstructing

the key since their effort will be paid off over a long time period. So the frequency of key change is a trade off between different aspects. Of course, if a key has been compromised, it should be changed as quickly as possible.

Keys must be stored in a secure way. That means that there must not be physical access to keys by non authorized persons or devices. It will usually be worth considering to only storing keys in encrypted form. This means that if unauthorized persons get access to keys they will not be directly usable, thereby providing an extra layer of security.

In general it must be assumed that longer keys provide more security. This is trivially true if the only way to break a cryptographic system is by exhaustive trial. This is not always the case and makes an analysis of cryptographic systems very difficult. Long keys and complex cryptographic algorithms may often require extensive computational resources. It is therefore necessary to find the right balance between cryptographic strength and computational effort. In safety critical systems it is often a strict requirement that the system reacts quickly to input. If the cryptographic scheme imposes heave computational effort the required response time may not be possible. A risk analysis may be used to solve this problem.

It was already mentioned that a cryptographic system is very vulnerable to transmission errors. A common way to deal with transmission errors is the use of error correcting codes. The idea of error correcting codes is to add extra bits to a message. The additional bits make it possible to detect and correct some transmission errors. The number of additional bits and the detection and correction algorithm used determines how many transmission errors can be detected and corrected.

The simplest scheme adds one extra bit. This bit is used as a parity bit, e.g. the extra bit is set such that the sum of all bits in the message is even. This scheme makes it possible to detect one bit error in a transmission. It is not possible to correct a message and to detect more than one transmission error. This simple parity bit scheme has been extensively used, for example for storing data in computer memory.

Examples of error correcting codes include Hamming codes, Reed-Muller code, and Binary Golay code. These codes have different variants and in addition there are several other error correcting codes. The simplest real error correcting codes can correct one error and detect two errors.

Hamming codes normally refer to a very specific situation with a four bit data and additional three bit. This code can correct single bit errors and detect all single bit and two bit errors. If two bits are not transmitted correctly then the message must be retransmitted. The following small example shows the general principle of an error correcting code (see Figure 25).

The message 1011 is extended with 3 additional bits using a simple linear transformation.

$$\begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&1&1&1 \\ 1&0&1&1 \\ 1&1&0&1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

The transmitted message is 1011010.

A similar linear operation is able to recover one single bit error and to detect two bit errors.

Figure 25. Example of error detecting code.

The choice of error correcting code depends on the probability of transmission errors. As with cryptographic systems the computational effort depends on the properties of the code. The more errors to be detected and corrected the more computational power is required. Error detection and correction codes can be designed to fit specific purposes, such as expected transmission error rate, consequences of accepting erroneous commands, and available computing power. Different codes have different properties with respect to error detection and correction as well as with respect to computational effort required by the sender and the receiver. To give an example, for deep space communication with spacecrafts there will be limited computational power available at the spacecraft and almost unlimited computational power available at the earth station. Therefore a code fulfilling these requirements will be chosen for this application.

General security issues related to wireless communication can be found from publication: “Information Security in Wireless Networks” [25].

6 Validation

6.1 Management of system safety

The realisation of a safety-related wireless machine control systems is the result of technical activities performed by many parts under different phases of the project development. A systematic approach is necessary to ensure that the proper measures are taken at each development stage. It is also important that normative documents that affect the decision of developers and other actors involved in the design are properly updated.

6.1.1 Purpose

The purpose of management of system safety is to establish the realisation of technical activities carried out during the development of safety-related wireless machine control systems according to the principles listed in clause 3 Safety lifecycle of this report. The following is also applicable when modifications are carried out even after installation on an industrial site or plant. Recommendations are presented for defining the control procedures applicable at different phases of system realisation.

Management of system safety in a wireless machine control system shall lay down the general outline in

- identifying the activities related to the tasks mentioned above
- describing the policy and strategy to fulfil the specified functional requirements
- identifying persons, departments and other units and resources that are responsible for carrying out and reviewing each of the activities specifies in clause 3 of this report.
- identifying or establishing the procedures and resources to record and maintain information relevant to the functional safety of a safety-related control systems
- describing the strategy for configuration management
- establishing a verification plan
- establishing a validation plan
- preparing means for follow-up

6.1.2 Management of functional safety

The objective of the management of functional safety is to specify the technical activities necessary for the realisation of the required functional safety of the safety-related control functions. These activities are specified in the different phases of the safety lifecycle of Figure 11 above and are described more in detail with respect to the following tasks.

- requirements specification of safety-related control functions,
- design and integration of the safety-related control system.

The specification of the management and technical activities that are necessary for the achievement of the required functional safety of the wireless machine control system is recapitulated in the functional safety plan and ensured by its fulfilment.

Requirements for the management of functional safety

A functional safety plan shall be drawn and documented for each safety-related wireless machine control system design project. This plan shall include procedures for control of the activities specified.

The extent of the information depends on current factors specific to the current wireless machine control system, such as:

- Size of the project
- Degree of complexity
- Degree of novelty of design and technology
- Degree of standardisation of design features
- Possible consequence(s) in the event of failure

The activities that shall be covered in the safety plan are listed in the following clauses.

Identification of relevant activities

Technical activities that are necessary for the achievement of the required functional safety involve design, integration and validation. Control systems are used either singly or in a network to carry out safety functions on machines, including machines working together in a coordinated manner. The sequence of activities involved in the design and development process of safety-related wireless machine control systems is shown in Figure 27 based on IEC 62061 [16], which describes the workflow of the SRECS design and development process.

Specification of requirements for safety-related functions

The requirements include:
- Compulsory preliminary information
- The functional requirements specification
- The safety integrity requirements specification

Design and integration of the safety-related control system

The activities of this phase include:

- Set-up of general requirements
- Requirements for behaviour of the safety-related control system on detection of a fault
- Requirements for systematic safety integrity
  These requirements include:
  - The requirements for avoidance of systematic hardware failures
  - The requirements for the control of systematic faults
  - The requirements for electromagnetic (EM) immunity
- Selection of safety-related electrical control system
- Safety-related electrical control system design and development

  These requirements define in addition to general requirements:
  - The Design and development process
  - The estimation of the safety integrity achieved by a safety-related control system

Realisation of subsystems
The realisation of subsystems defines in addition to general requirements for subsystem, requirements regarding the:

    - selection of existing (pre-designed) subsystems
    - design and development of subsystems
    - determination of the safety performance of the subsystem
    - architectural constraints on hardware safety integrity of subsystems
    - estimation of safe failure fraction (SFF)
    - probability of dangerous random hardware failures of subsystems
    - systematic safety integrity of subsystems
    - subsystem assembly

- Realisation of diagnostic functions
- Hardware implementation of the safety-related control system
- Software safety requirements specification
- Software design and development
  Software design and development include the following aspects:
    - Embedded software design and development
    - Software parameterisation
    - Application software design and development
- Safety-related electrical control system integration and testing
- General requirements
- Tests to determine systematic safety integrity during system integration
- Safety-related wireless machine control system installation

Information for use of the wireless safety-related machine control system

- Documentation for installation, use and maintenance

A detailed list of the information concerning the use and maintenance of the machine control system shall be provided. The clause 7.2 presented in IEC 62061 [16] is a good support. See also clause 6 of ISO 12100-2 [6] that provides information that should be considered during drafting of accompanying documents.

Validation of the safety-related electrical control system

- General requirements
- Validation of systematic safety integrity

Modification

The different aspects considered in the modification of a safety-related control system are the modification procedure and the configuration management procedures.

Modification procedure
The modification procedure is initiated by a modification request of the control system motivated by, for example:

- Safety requirements specification changed
- Conditions of actual use
- Incident/accident experience
- Change of material processed
- Modification of the machine or of its operating modes

Configuration management procedures
The configuration management procedures shall comply with the functional safety plan and shall take the requirements listed in IEC 62061 [16], clauses 9.3.1 – 9.3.3 under consideration.

Policy and strategy to fulfil the specified functional safety requirements

The policy and strategy for achieving functional safety shall cover the means for evaluating its achievement and the means by which communication within the organisation is realised in order to ensure a culture of safe working.

Strategy to achieve functional safety for the application software

The functional safety planning shall define the strategy for the software procurement, development, integration, verification, validation and modification to the extent required by the safety integrity level of the safety-related control functions.

The strategy shall ensure that following requirements are fulfilled, that their implementation is carried out and documented in accordance with the functional safety plan.

- The software configuration management
- The requirements for software architecture
- The requirements for support tools, user manual and application languages
- The requirements for application software
- The requirements for application code development
- The requirements for application module testing
- The requirements for application software integration testing

Identification of parties involved in carrying out identified activities.

The persons, departments or other units and resources responsible for carrying out and reviewing each of the identified activities are identified. These activities are listed in [12], clauses 5 to 9 and also include, where relevant, licensing authorities or safety regulatory bodies.
Procedures for ensuring that applicable parties are competent to carry out the activities for which they are accountable shall be established. The training experience and qualifications of all persons involved in any overall or software safety lifecycle activity, including any management of functional safety activities should be assessed in relation to the particular application.
The following factors should be considered when assessing the competence of persons to carry their duties:

- Engineering knowledge appropriate for the application area
- Engineering knowledge appropriate for the technology (for example electrical, electronic, programmable electronic, software engineering)
- Safety engineering knowledge appropriate for the technology
- Knowledge of the legal and safety regulatory framework
- The consequences in the event of failure of the EUC safety-related systems; the greater the consequences, the more rigorous should the specification and assessment of competence
- The safety integrity levels of the EUC safety-related systems; the higher the safety integrity levels, the more rigorous the specification and assessment of competence should be
- The novelty of the design, design procedures or application; the newer or more untried the designs, design procedures and application, the more rigorous the specification and assessment of competence should be
- Previous experience and its relevance to the specific duties to be performed and the technology being employed; the greater the required competence levels, the closer the fit should be between the competencies developed from previous experience and those required for the specific duties to be undertaken
- Relevance of qualifications to specific duties to be performed

The training, experience and qualifications of all persons involved in any overall or software safety lifecycle activity should be documented.

Procedures and resources ensuring the functional safety of a safety-related control system

The following should be considered:

- The results of the hazards identification and risks assessment
- The equipment used for safety-related functions together with its safety requirements
- The organisation responsible for maintaining functional safety
- The procedures necessary to achieve and maintain functional safety (including system modifications)

Description of the strategy for configuration management

The procedures for configuration management of the safety-related machine control system during the overall and software safety lifecycle should be specified in particular the following shall be established:

- The stage at which formal configuration control is to be implemented
- The procedures to be used for uniquely identifying all constituent parts of an item (hardware and software)
- The procedures for preventing unauthorised items from entering service

See IEC 62061 [16], Clause 9.3 for detail requirements. Relevant organisational issues such as authorised persons and internal structures of the organisation should be taken into account.

Establishment of a verification plan

The plan shall include:

- Details of when the verification shall take place
- Details of the persons, departments or units who shall carry out the verification
- The selection of verification strategies and techniques
- The selection and utilisation of test equipment
- The selection of verification activities
- Acceptance criteria
- The means to be used for the evaluation of verification results

Set-up of a validation plan

The validation plan shall comprise:

- Details of when the validation shall take place
- Identification of the relevant modes of operation of the machine (e.g. normal operation, setting)
- Requirements against which the safety-related machine control system is to be validated
- The technical strategy for validation, for example analytical methods or statistical tests
- Acceptance criteria
- Actions to be taken in the event of failure to meet the acceptance criteria.

The list of requirements related to the validation of the safety-related wireless machine control system is presented in IEC 62061 [16], Clause 8.

6.1.3 Implementation of the functional safety plan

The functional safety plan shall be implemented to ensure prompt follow-up and satisfactory resolution of issues relevant to a safety-related wireless machine control arising from:

- Activities specified in IEC 62061 [16],, clauses 5 to 9
- Verification activities
- Validation activities

The requirements associated to the implementation of the functional safety plan are considered in IEC 62061 [16], Clause 8.

6.1.4 Documentation

It shall be demonstrated that the requirements have been fulfilled according the specified criteria. Necessary information must be documented in order to perform effectively all the phases of the overall safety lifecycles.
The documentation shall:

- Be accurate and concise
- Be easy to understand by the persons having to make use of it
- Suit the purpose for which it is intended
- Be accessible and maintainable

Documents classification
The designer of the safety-related wireless control system should distinguish between the documentation that is relevant to the user and the documentation that is relevant to its design and construction.

Documents scope
The documents shall have titles or names indicating the scope of the contents.

Configuration management of document items
The documents shall have a revision index (version numbers) to enable the identification of the different versions of the document

As far as management of system safety is concerned, the design and development of safety-related wireless machine control systems is supported by IEC 62061 [16]. For that reason this report refers to the documentation required by this standard.

Figure 26 Information and documentation of a SRECS below summarises the information and documentation to be available, where appropriate.

Information required	Subclause IEC 62061
Functional safety plan	4.2.1
Specification of requirements for SRCFs	5.2
Functional safety requirements specification for SRCFs	5.2.3
Safety integrity requirements specification for SRCFs	5.2.4
SRECS design	6.2.5
Structured design process	6.6.1.2
SRECS design documentation	6.6.1.8
Structure of function blocks	6.6.2.1.1
SRECS architecture	6.6.2.1.5
Subsystem requirements specification	6.6.2.1.7
Subsystem realisation	6.7.2.2
Subsystem architecture (elements & their interrelationships)	6.7.4.3.1.2
Fault exclusions claimed when estimating fault tolerance/SFF	6.7.1.c)/6.7.7.3
Subsystem assembly	6.7.10
Software safety requirements specification	6.10.1
Software based parameterisation	6.11.2.4
Software configuration management items	6.11..3.2.2
Suitability of software development tools	6.11.3.4.1
Documentation of the application program	6.11.3.4.5
Results of application software module testing	6.11.3.7.4
Results of application software integration testing	6.11.3.8.2
Documentation of SRECS integration testing	6.12.1.3
Documentation of SRECS installation	6.13.2.2
Documentation for installation, use and maintenance	7.2
Documentation of SRECS validation testing	8.1.4
Documentation for SRECS configuration management	9.3.1

Figure 26 Information and documentation of a SRECS

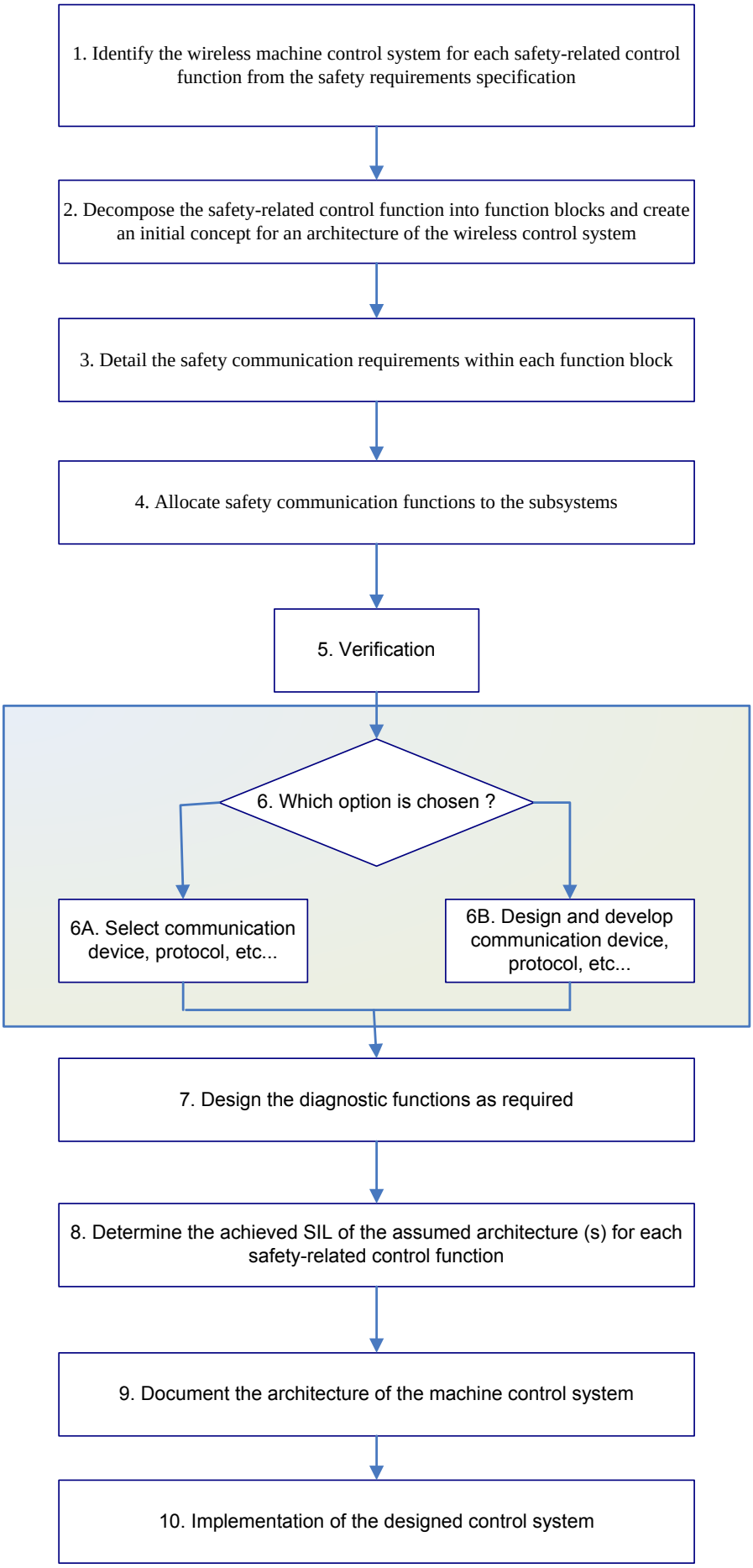


Figure 27. Development flow of a SRECS [16].

6.2 Validation process

When addressing validation of safety-related wireless machine control systems, two major types of control systems emerge. One type of machine control systems supervises the operation of a single machine or device as described in Figure 13 Implementation of communication subsystems (a crane for example).

The other type of control systems supervises the operation of a network configuration of devices or machines as described in Figure 14 Safety communication as part of an overall safety function in industrial environment. The synchronised movements of robots that handle the tasks involved in car body parts manufacturing is such an example.

These two types of wireless control systems (WCSs) are basically constructed with similar components or modules except for the network that ensures the exchange of information between devices (or modules). The wireless network introduces additional complexity compared to the former type and hence demands a more precise description model. Safety and security aspects must be addressed with respect to interaction between system parts/devices.

The validation process aims in both cases to assess the compliance of the safety functions as well as their respective safety integrity level with the safety requirements specification.

The validation is systematically carried out for the assessment of each phase of the overall safety lifecycle.

6.2.1 Concept

The acquired information concerning the EUC and its environment shall be sufficient to enable the other safety lifecycle activities to be carried out satisfactorily. The validation shall emphasise the following considerations:
- The characteristics of the four most common types of wireless networks; Wi-Fi (IEEE 802.11a/b/g) [1)], Wi-Max (IEEE 802.11n), Bluetooth (IEEE 802.15.1), and ZigBee (IEEE 802.15.4) [2)] involve tradeoffs with regard to speed, interoperability, security, coexistence, battery life and building or object penetration.
The physical conditions
The legal requirements and restrictions

6.2.2 Overall scope definition

The boundary of the EUC and the EUC control system shall be specified so that the scope of the hazard and risk analysis for functional hazards can be clearly defined.

6.2.3 Hazard and risk analysis

The methods applied to realise the Hazard and risk analysis are assessed. The description and information relating to the results of this analysis are assessed as well.

6.2.4 Overall safety requirements

The tasks related to the specification of the overall safety requirements and safety integrity requirements for the WCS are analysed to confirm the correspondence between risks and requirements. Risk reduction facilities are addressed.

The following aspects are particularly important when dealing with the operation of a network configuration of devices or machines:

- Monitoring and transmission of control and emergency signals
- Reliability of message delivery
- Transmission delay: the network should deliver the messages carrying critical information within a specified time period.
- Power conservation:
- Coverage for mobile (moving) and fixed modules
- Support for diverse and battery-limited devices adapted to specific parts: it is very likely that modules/devices present diverse characteristics in functionality and for power supply. These devices must be utilised in terms of power and processing resources and must be matched to the spatial and environmental conditions
- Scalability: the key factors are the bit rate, the frequency of monitoring and transmission and the amount of information per module/sensor device. The effective bit rate of an ad hoc network might decrease with a growing distance between devices.

6.2.5 Safety requirements allocation

The safety-related functions and sub-functions are allocated to match the overall safety requirements specification. The communication subsystem performs the safe transmission of safety relevant data/control signals. To ensure e.g. an effective transmission bit rate of safety-related messages within a specified range, a power monitoring device with alarm function might be necessary.

6.2.6 Realisation of safety-related systems

The realisation of safety-related systems is done according to (safety) requirement specifications. The better requirement specification the better realisation. All changes in plans should be considered according to specified procedures.

6.2.7 Evaluation of analysis and design methods

Functional model

Analysis and design tools are necessary in developing real time systems. The functional model mentioned in clause 3.1 Concept is a graphic method for systematic analysis and design of such systems. The major benefit of the functional model is its substantial contribution to each phase of development and also during the validation process. By providing material for system analysis the functional model helps the designers to describe the hierarchy of the system and manage the complexity of the design requirements. The functional model is a perfect tool to describe the hierarchy in the system, thus providing the basics for more detailed analysis. Functional aspects in a system can be analysed from top level via sub-system levels down to components level.

Data flow diagrams (DFDs) are used as one of the primary analysis tools for managing the complexity of the requirements of a real-time system. The DFD describes the data flow between the components of the system. The top level DFD or Context diagram (See Figure 16 Context diagram) illustrates the interfaces between the software system and the various hardware devices.

Formal methods

Formally modelling and analysing a system offers the advantage of ascertaining that it behaves according to specifications and helps developers identify potential problems or misunderstandings.

- The design of protocol mechanisms and transmission schemes
- The combination of these schemes
- The transition to a safe state in the occurrence of critical events that may affect the execution of safety-related operations
- Real-time capabilities

Validation of safety principles

Safety principles are measures and techniques applied to enhance the functional safety of a design. They may be implemented in development work, in documentation, at validation at system design and at detailed design. Requirements are given to use well-tried safety principles when certain behaviour at fault is claimed.

The objective of this validation is to ensure that the software and the hardware design of the control system satisfy the specified requirements for safety with respect to overall functional safety and safety integrity levels. The overall safety function integrates safety transmission sub-functions realised by sub-systems and components such as sensor, communication system, logic solver and actuator. The application/control algorithms of the communication system that performs the safety transmission sub-function shall be robust enough to tolerate potential failures and random faults.

Validation of safety mechanisms

The validation methodology should include the following processes and related documentation:

- Detailed inventory of each device, subsystem and interface
- Identification and selection of the appropriate detailed white-box, black-box or grey-box testing technique for each device, subsystem and interface
- Simulation of safe and reliable system performance
- Re-specification or re-configuration of components to address any deficiencies identified
- Simulation or site-testing to assure avoidance of RF conflicts
- Verification of reliable interoperability of embedded device decision support systems and intelligent alarms, which might also be done with a formal method tool
- Creation of a verification process and documentation package that specifies all tests and results
- Determination and documentation of verification intervals, criteria or both
- Creation of preliminary verification process and documentation for future repairs, upgrades and changes
- Periodic review of validation procedures and documentation
- Update of the model to support validation and problem analysis of future modifications.

The validation process shall consider the environmental conditions in which the system will operate in order to assess the scope definition and the hazard and risk analysis.

The assessment of the safe transmission of safety relevant data includes the analysis of the following aspects:

- The design and evaluation of protocol mechanisms
- The Formulation of appropriate performance measures, benchmark applications and wireless channel models adapted to the current operating environment.

Attention is also given to implemented mechanisms for improving the coexistence of multiple wireless technologies.
Performance of coexisting networks and methods for reducing mutual disturbances between multiple wireless technologies can be used to enhance safety of transmission.

CSMA is e.g. a mechanism for improving the coexistence of multiple communication systems that use the same frequency band. In fact, the goal of the carrier-sensing operation is to avoid interfering with ongoing transmissions.

Applications which do not handle safety-critical functions can coexist with the common and inexpensive WDN devices, especially as available bandwidth continues to increase.

To accommodate these types of multi-user data demands, developers use the simple Collision Sense Method (CSM) to handle multiple simultaneous wireless messages. For many short-burst messages, the CSM strategy causes few visible delays, even for multiple simultaneous users. If one or more users are sending large streams of continuous data, other WDN users might experience noticeably erratic delays in system response.

Although safety-critical data is exchanged between modules, occasional delays can be tolerated within a specified range. However alarms and related information shall be available within strictly specified time intervals. Such safety-critical data delays, distortions, loss or other erratic delivery problems could result in unsafe states.

The checklist in appendix D addresses the main aspects and issues that should be considered for the management of safety and under the validation process.

Evaluation methods

Given a completely new system design and installation, a formal, independent validation process allows proper specification, valid installation acceptance testing and periodic systemic revalidation following major system repairs or changes. In keeping with IEEE software engineering practices, developers can perform a validation process such as this incrementally: first validating individual pieces or modules, then validating subsystems by carefully testing all interface modes and functions. Ultimately, the developer validates the entire system by testing the combination of all subsystems. Manufacturer testing or verification procedures must be considered during this process, but they are rarely site-specific or situation-specific and are often out of date.

The validation methodology should include the following processes and related documentation:

- Detailed inventory of each device, subsystem and interface
- Identification and selection of the appropriate detailed white-box, black-box or grey-box testing technique for each device, subsystem and interface
- Simulation of safe and reliable system performance
- Re-specification or re-configuration of components to address any deficiencies identified
- Simulation or site-testing to assure avoidance of RF conflicts
- Verification of reliable interoperability of embedded device decision support systems and intelligent alarms, which might also be done with a formal method tool
- Creation of a verification process and documentation package that specifies all tests and results
- Determination and documentation of verification intervals, criteria or both
- Creation of preliminary verification process and documentation for future repairs, upgrades and changes
- Periodic review of validation procedures and documentation
- Update of the model to support validation and problem analysis of future modifications.

Any changes – such as repairing a device or upgrading a piece of hardware or software – should be verified and documented by testing critical performance parameters and anticipated critical failure modes such as power interruptions.

6.2.8 Software quality validation

The international standard ISO/IEC 25000 Software engineering – software product quality requirements and evaluation (SQuaRE) is a new series of standards covering software product quality requirements and evaluation. The SQuaRE series of standards are based on previously published standards, in particular ISO/IEC 9126 Software quality characteristics and guidelines for their use, which was originally published in 1991. This standard has become well known in the software community and is frequently referred to. Later ISO/IEC 9126 was supplemented by a series of technical guidelines and a six part standard ISO/IEC 14598 Software product evaluation. As the area of software product quality became more mature the need for a revision and restructuring of these standards became evident and an effort to rewrite and reorganize these standards was initiated and is currently still going on.

The new series of standards were assigned the 25000 - 25099 number series and named SQuaRE. The main part of SQuaRE consists of five divisions according to the Figure 28.

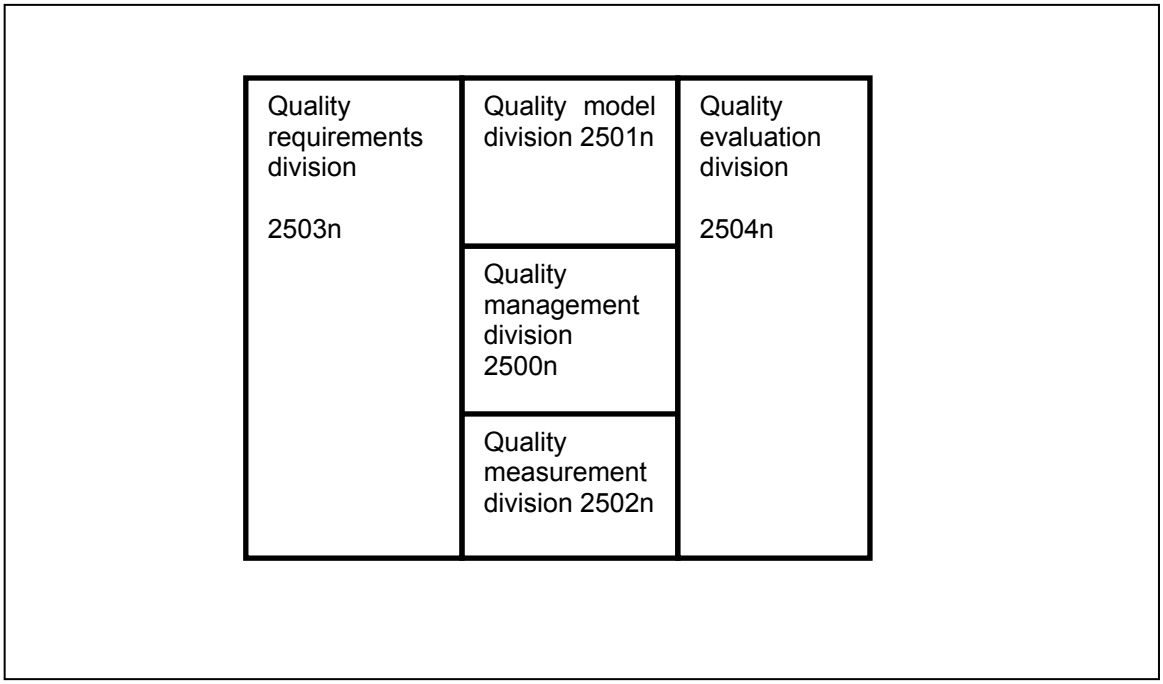


Figure 28. Structure of the 2500 series of standards.

Quality Management Division

The standards that form this division define all common models, terms and definitions referred further by all other standards from SQuaRE series. Referring paths (guidance through SQuaRE documents) and high level practical suggestions in applying proper standards to specific application cases offer help to all types of users. The division provides also requirements and guidance for planning and management supporting functions for software product requirements specification and evaluation. There are two standards in this division.

Quality Model Division

The standards that form this division present detailed quality model and specific characteristics and sub-characteristics for internal and external quality and

characteristics for quality in use are defined together with practical guidance. The internal and external quality characteristics are: functionality, reliability, usability, efficiency, maintainability, and portability. The characteristics for quality in use are: effectiveness, productivity, safety, and satisfaction. This part is based on the ISO/IEC 9126 standard.

Quality Measurement Division

The standards that form this division cover mathematical definitions and guidance for practical measurements applicable to a software product. Examples of measures apply to internal quality, external quality and quality in use. Measurement primitives forming foundations for the latter measures are defined and presented. This part is based on the technical reports supporting the previous ISO/IEC 9126.

Quality Requirements Division

The standards that form this division help specify quality requirements. These quality requirements can be used in the process of quality requirements elicitation for a software product to be developed or as input for an evaluation process. The requirements definition process is mapped to technical processes defined in ISO/IEC 15288 – Information Technology - Life Cycle Management - System Life Cycle Processes. The quality requirements part is new.

Quality Evaluation Division

The standards that form this division provide requirements, recommendations and guidelines for software product evaluation, whether performed by evaluators, acquirers or developers. The support for documenting a measure as an Evaluation Module is also presented. The evaluation process is mapped to technical processes defined in ISO/IEC 15288 – Information Technology - Life Cycle Management - System Life Cycle Processes. This part is based on the ISO/IEC 14598 series of standards. The individual parts of this division focus on evaluation from different perspectives:

- 25040 – Quality evaluation overview and guide: contains general requirements for specification and evaluation of software quality and clarifies the general concepts. Provides a framework for evaluating quality of software product and states the requirements for methods of software product measurement and evaluation (ISO/IEC 9126-1 and 14598-1)

- 25041 - Evaluation modules: defines the structure and content of the documentation to be used to describe an Evaluation Module (ISO/IEC 14598-6)

- 25042 – Process for developers: provides requirements and recommendations for the practical implementation of software product evaluation when the evaluation is conducted in parallel with the development (ISO/IEC 14598-3)

- 25043 – Process for acquirers: contains requirements, recommendations and guidelines for the systematic measurement, assessment and evaluation of software product quality during acquisition of “off-the-shelf” software products, custom software products, or modifications to existing software products (ISO/IEC 12119 and 14598-4)

- 25044 – Process for evaluators: provides requirements and recommendations for the practical implementation of software product evaluation, when several parties need to understand, accept and trust evaluation results (ISO/IEC 14598-5).

ISO/IEC 25050 to 25099 are reserved to be used for SQuaRE extension standards and/or technical reports.

The ISO/IEC 25000 series applies a common software quality lifecycle, which is shown in the Figure 29. It illustrates how requirements and product implementations are related. The model applies three layers:

Quality in use: Here requirements specify the required level of quality from the end user's point of view. These requirements are derived from needs of each context of use. Quality in use requirements are used as the target for validation of the software product by the user. Requirements for quality in use characteristics should be stated in the quality requirements specification using quality in use measures and used as criteria when a product is evaluated.

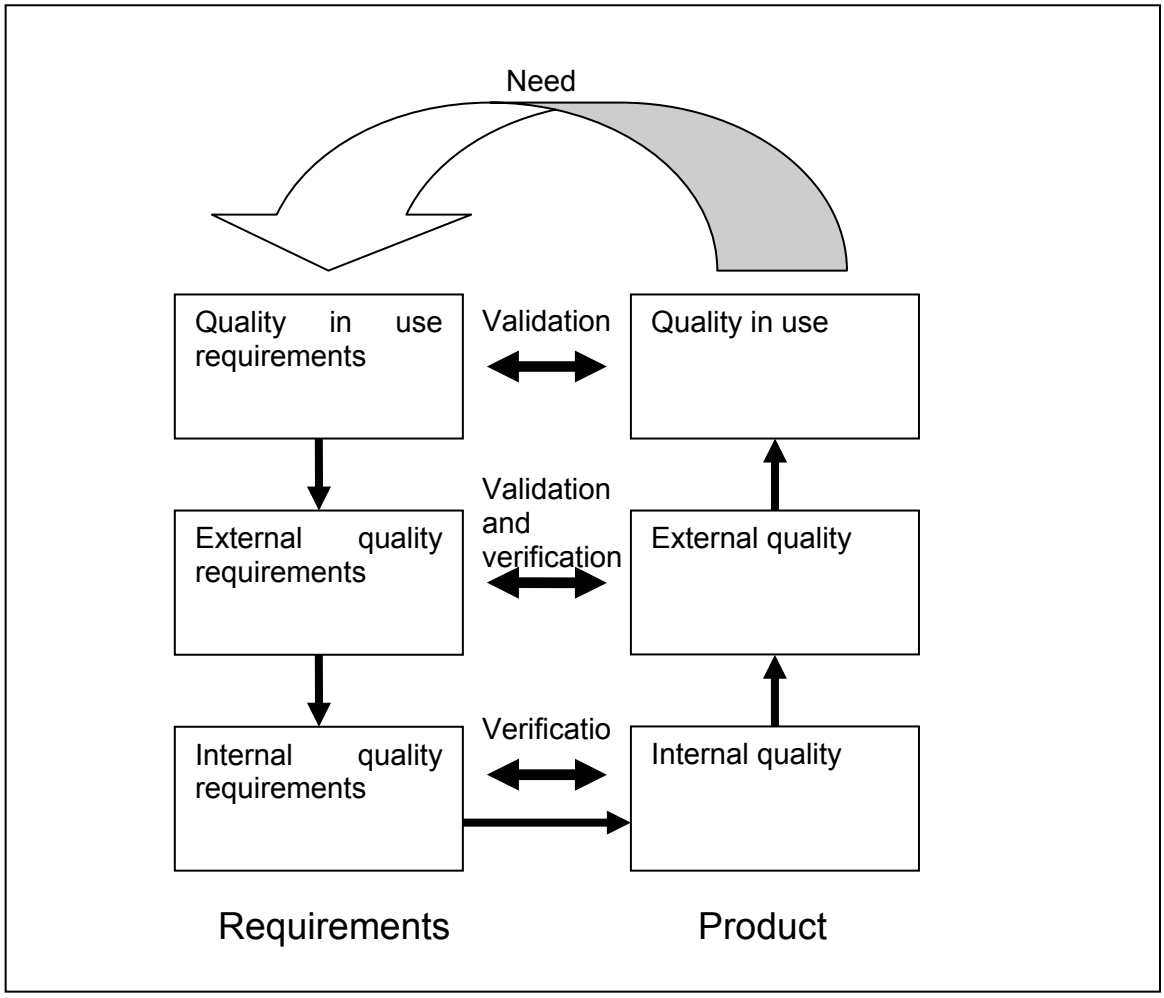


Figure 29. Software quality lifecycle.

External software quality: Here requirements specify the required level of quality from the external view. They include requirements derived from user quality requirements, including quality in use requirements. External software quality requirements are used as the target for technical verification and validation of the software product. Requirements for external software quality characteristics should be stated quantitatively in the quality requirements specification using external measures and used as criteria when a product is evaluated.

Internal software quality: Here requirements specify the level of required quality from the internal view of the product. They include requirements derived from external software quality requirements. Internal software quality requirements are used to specify properties of intermediate software products. Internal software quality requirements may also be applied to deliverable, non-executable software products

such as documentation and manuals. Internal software quality requirements can be used as targets for verification at various stages of development. They can also be used for defining strategies of development and criteria for evaluation and verification during development. This includes the use of additional measures (e.g. for reusability), which are outside of the scope of SQuaRE series of standards. Internal quality requirements should be specified quantitatively in terms of internal measures.

6.3 Validation of defensive methods

It is not possible to say exactly, which method and how effectively it should be applied for each application. In all communication applications, which have safety-related functions and defined safety integrity level some method (or many) against all message-related risks is needed. It is also clear that the higher SIL the better methods against the risks are needed.

Against corruption it is possible to calculate values for probability of dangerous failure. For each SIL there is a corresponding probability of dangerous failure, which gives hints for estimating possibility of corruption. Quite often so called safety budget is used for the estimation. It is estimated that < 1 % of all failures are related to corruption. Corruption takes only 1 % of the safety budget and the rest 99 % is left for other kind of failures. The estimation is on safe side since corruption is quite common. This 1 % assumption means that e.g. for SIL 1 the requirement is 10^{-7} (instead of 10^{-5}).

Some more ideas for validation of defensive methods are presented in “Methods for V&V of time-triggered embedded communication systems” [10].

6.4 COTS

There is no universally accepted definition of COTS or components. A component can be defined as one element of a larger system. A hardware component can be a device as small as a transistor or as large as a disk drive as long as it is part of a larger system. Software components are routines or modules within a larger system.

One possible definition could be: A reusable piece of software in binary form that can be easily integrated with other components with relatively little effort.

The current trend towards the use of COTS can be explained as an attempt to improve productivity and quality in software projects. The assumption is that if a component already is available then it is cheaper to use it compared to develop a similar software product. In addition, if the component is already used in other applications it should have fewer errors and be more reliable. However, this is exactly one of the main problems with COTS: documentation of properties of COTS.

Component suppliers provide information about the functions offered by a component. The level of details vary and sometimes claimed functions does not actually exist, but are only planned for a later version of the component. When looking at quality properties of COTS the situation becomes even more difficult. It is generally very time consuming or even impossible to find any precise information about quality of a component [2].

There are no commonly accepted and widely implemented schemes for evaluation and certification of COTS. Some research activities have suggested approaches to evaluation and certification, including [8] and [3]. Both papers apply the quality model provided in ISO/IEC 25010 (ISO/IEC 9126) and suggest a measurement approach to

defining software quality [4]. This involves defining measures for relevant quality characteristics or sub-characteristics and for each measure a value must be provided. This combination of measure and value represents the quality of the software from a specific point of view.

The measures can be simple like the following examples:

Quality characteristic: Reliability

Attribute: Mean time between failures (MTBF). How frequently does the software fail in operation based on counting the failures occurring during a defined period of operation and computing the average interval between failures?

Measure: $X = T/A$, where T is the sum of the time intervals between consecutive failures (that is, termination of the software's ability to perform a required function) and A is the total number of actually detected failures (those occurring during a specified operation time with a normal operational profile). The measure's scale type is a ratio.

Quality characteristic: Reliability, maturity

Attribute: Estimated residual latent fault density. How many problems still exist that might emerge as future faults based on the number of faults detected during a defined trial period and predicted number of remaining faults using a reliability growth estimation model?

Measure: $X = |P - A| /S$, where P is the number of predicted latent faults in a software product from a reliability growth estimation model, A the number of actually detected faults, and S is the product size (for example, lines of code). The measure's scale type is an absolute.

However, measures can also be very complex. The following example illustrates this without providing any specific details. More details can be found in [3].

Quality characteristic: Functionality, security

Attribute: Security according to ISO/IEC 15408.

Measure: Does the software comply with all requirements in ISO/IEC 15408.

In order to ensure trustworthiness of software quality properties a certification scheme is proposed in [3]. Basically the scheme is based on deriving a number of quality properties from standards. The properties are formulated a software measures as indicated above. The software component supplier claims values of the relevant properties. These values are then checked and certificates are issued by accredited certification bodies. The model of property certification is shown in the Figure 30.

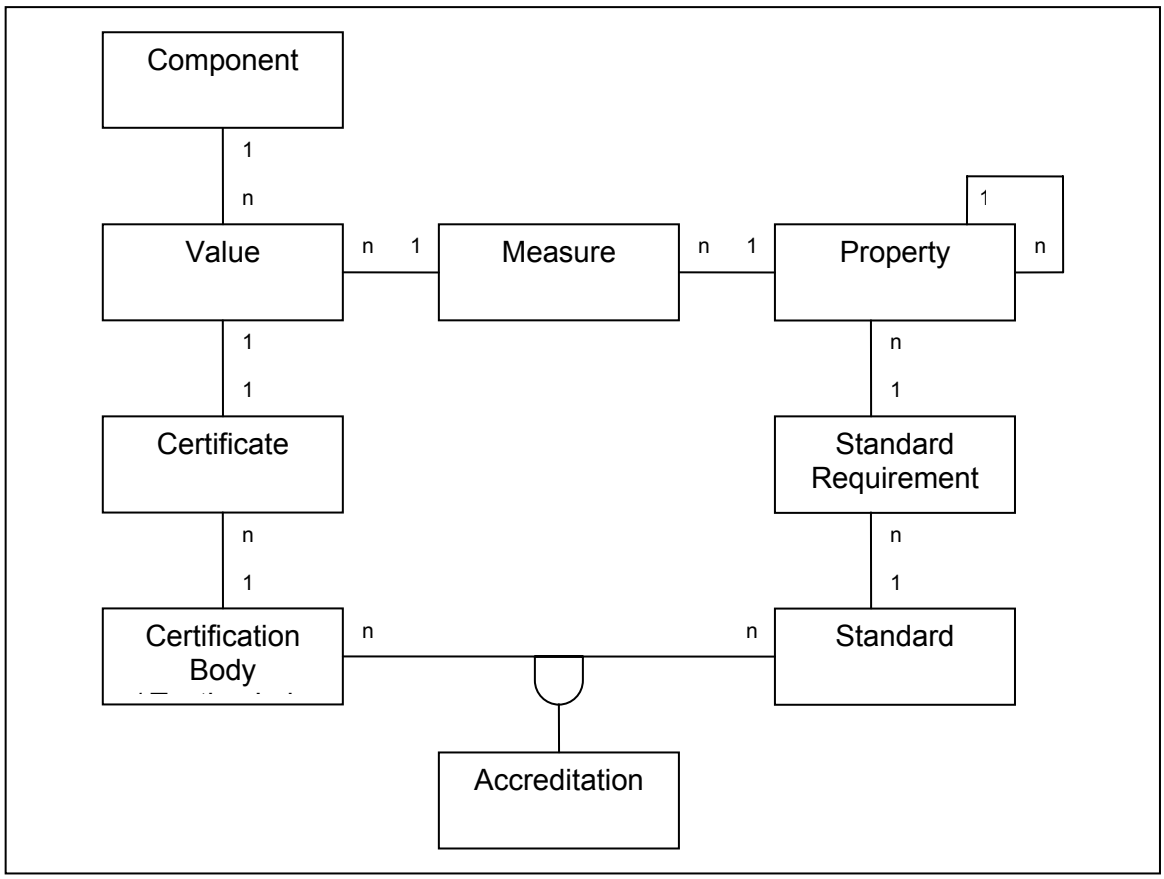


Figure 30. Model of property certification.

Another relevant source of information is the International Standard ISO/IEC 12119 "Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instruction for testing". This standard was recently published in an updated version. The previous version was based on a German scheme for certifying software packages. The standard also applies the ISO/IEC 25010 software quality model.

The standard provides a set of requirements for the COTS product:

- Product description: Must be available, contain the needed information, without inconsistencies and be correct. The description must be uniquely identified and provide necessary information about the COTS supplier and additional services provided. In addition there shall be a description of the quality characteristics defined in ISO/IEC 25010.

- User documentation: The documentation must be complete, correct, consistent, understandable, learnable, and operational.

- Software: The software must have some basic properties following the ISO quality model (all described functions shall be executable and provide the correct results, not lose or corrupt data, provide understandable error messages, screens must be easy to understand and overview, execute within provide response time limits, provide diagnosis for deficiencies, and be installable without disturbing other software products.

- Test documentation: This documentation shall be consistent, and include a minimum set of information.

- Test plan: All quality characteristics and functions mentioned must be tested as well as installation, operational limits, syntax violations, and examples in documentation. Pass/fail criteria and test environment must also be described.

- Test description: This includes test case description, and test procedures.

- Test results: This includes assessment results, execution report that demonstrates that all test cases have been executed according to the test plan, and anomaly report describing all encountered anomalies as well as all corrections provided.

The standard also provides instructions for conformity evaluation. This includes conformity evaluation pre-requisites, evaluation activities, third party evaluation process, conformity evaluation report, and follow up evaluation when a COTS product is evaluated again.

The following table provides a list of verifications that may be used to evaluate the integrity of the COTS software product in a high risk application. The table is based on FAA research report DOT/FAA/AR-02/188.

Feature	Purpose	Verification
Memory protection	Check whether applications are prevented from accessing unauthorized address space.	Run test which attempt to perform, read, and write operations outside their designated address range
Stack overflow protection	Check whether COTS provides facilities to protect against stack overflow.	Test by calling some functions to overflow its stack. Verify that the kernel will suspend the task, or if the task will corrupt the whole system.
Dynamic memory allocation quota	Check if the COTS has resource protection mechanisms to prevent a malicious task from consuming resources unlimitedly	Create task that requests memory in an infinite loop while another task requires very little memory. Verify that the critical task is not corrupted by the COTS.
Fault - tolerance	Verify that the kernel can recover and log the event that preceded the failure	The test of the COTS should be designed to show if fundamental features of the COTS could enable the system designer to build in fault tolerance.
Simultaneous interrupts and interrupt nesting	Determine how long the system needs to respond to two simultaneously occurring interrupts.	Measure the latency to service both high and low priority interrupts. The test should measure the time it takes for the system to respond to two simultaneously occurring interrupts. Verify that interrupt handling is prioritized.
Inclusion of dead or deactivated code	Verify inadvertent execution of dead or deactivated code.	Check for any conditions that may cause the “idle” code to be activated and then test for such condition.

Use of wrappers	Are wrappers used to protect a COTS component within the system or to mask unwanted functionality?	Investigate if COTS components are used in a different context from that of the original design.
COTS Evaluation	Determine the appropriateness of COTS features and their impact to the system design	Quick in-house evaluation and/or prototype
COTS Acquisition Plan	Determine license, lease, maintenance agreements, access to problem reports and potential need for access to source code	Management & COTS vendor signed plan.
CM / SQA Plan for COTS	Determine pedigree of CM and SQA at both in-house and at the COTS vendor's site.	CM/SQA plans signed by management & COTS vendor. Review Problem Reports, insure positive version control of source and object code.
Test Plan for COTS	In-system and out of system testing with COTS product	Verify per system requirements.
COTS Integration Plan	Plan for how the COTS product is to be configured in the system. Special integration software.	Special HW platforms to properly operate COTS, (timing, partitioning, unintended functionality, impact of dead or deactivated code.)
Product Support	Determine the availability of product support.	Evaluate the adequacy of the support systems, (Help menus, operation manuals, product descriptions, help desk
Prior certifications/ qualifications	Service history of the COTS product including any regulatory authority controlled products.	Determine if the service history of the COTS product includes any high criticality applications and investigate the performance in that environment.

7 Discussion

When designing safety-related systems a standardised design method is needed. This is important since credibility is achieved only by using well known methods proven in use. The standards that have been considered here are mainly IEC 61508 and EN 62061. These standards address safety-related control systems, but do not lay stress upon communication. However, the design methods in the standards are also applicable to communication. The methods are based on the so called V-model, which means that systems are defined from upper level down to detail level, designed and then verified, first at detail level and finally the complete system.

The safety of communication is here analysed at three levels: basic, message and system level. At the basic level the risks are related to design, random failures, transient failures and unauthorized modification. Quite many types of threats are well covered, but the detailed messages are not considered. The protection against the threats is related to good design and reliable communication technology. The probability of failures may be reduced substantially if adequate protection is implemented. Basic level failures cause message errors.

Message errors are due to the message being itself erroneous or to transmission interference. Message errors are considered in communication standards as very important with respect to safety. Wrong messages can cause severe damages. Therefore a lot of effort is needed to ensure that the messages are correct. There need to be measures against all seven threats mentioned in communication standards (deletion, repetition, insertion, wrong sequence, corruption, delay and masquerade). If an erroneous message is detected it is normally deleted and the proper error handling procedure is executed.

Undetected message errors can cause damage at system level. The extent of the damage depends on the system and the system architecture. If the system has e.g. a redundant architecture, erroneous outputs can be detected at system level. It is often possible for a machine builder to adapt the system architecture to the specific application while using available commercial communication components. (COTS).

The machine builder usually buys a commercial communication system (COTS), which includes several features to ensure reliability and safety. The machine builder needs to verify that the system is adequate for the intended purpose. COTS with features that do not fulfil the safety requirements of the current system shall not be used. A solution could be to compensate reliability short comings by adding safety features to the application. In wireless communication we cannot ensure reliability since e.g. with increasing distance between transmitter and receiver, errors become more probable and finally the connection is lost. At system level it is possible to e.g. use two transmitters and different frequencies. This helps a little but, again, if distance increases the connection is lost. The duplication of devices helps to minimise the effects of component failure, but does not solve the reliability problem.

Figure 31 shows the basic issues a machine builder needs to consider in a safety-related communication system. Typically, a machine builder buys a commercial communication system, which is meant for a specific application. Some features can be added to the application layer of the system or some devices added to back-up the communication. It is essential in a safety-related system that the risks are identified, the safety measures specified and realised and finally that the system is validated against the safety requirements.

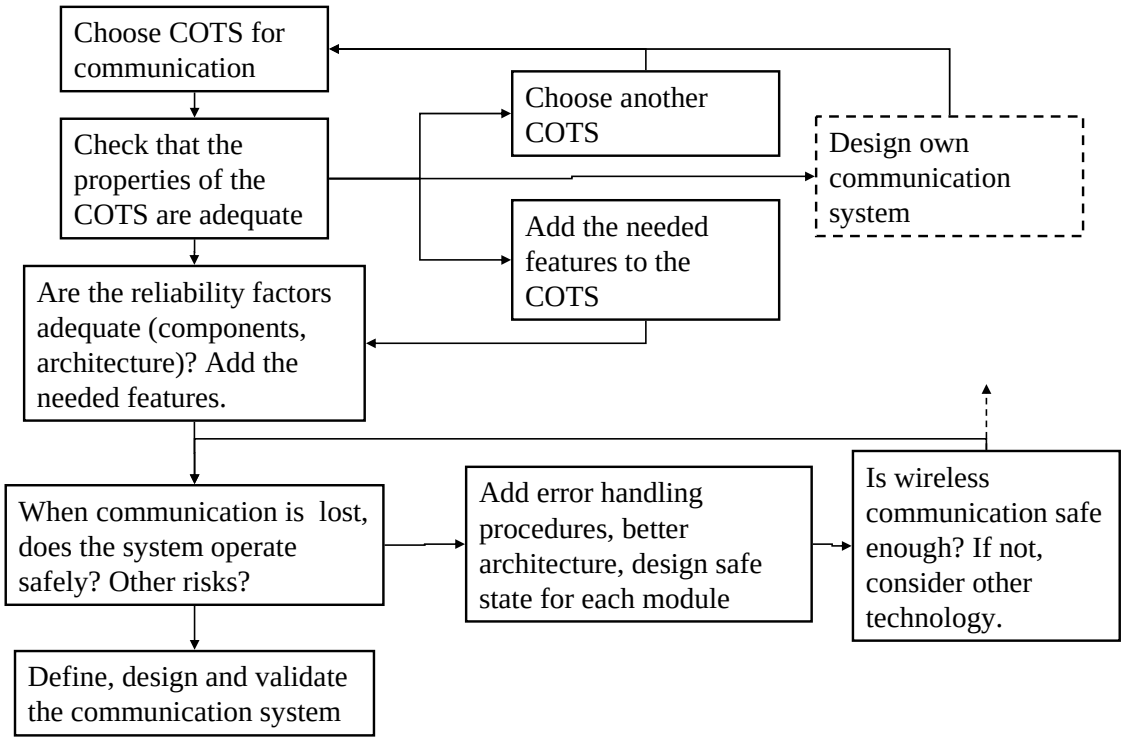


Figure 31. Basic features of the communication system that a machine builder need to consider in a safety-related communication.

8 References

[1] Avizienis, Algirdas; Laprie, Jean-Claude; Randell, Brian; Landwehr, Carl. Basic Concepts and Taxonomy of Dependable and Secure Computing. 2004. Institute for Systems Research TR 2004-47. 36 p.

[2] Bertoa, Manuel F.; Troya, José M.; Vallecillo, Antonio: A Survey on the Quality Information Provided by Software Component Vendors, proceedings of the 7th ECOOP Workshop on Quantitative Approaches in Object-Oriented Software Engineering, Darmstadt, Germany, 2003

[3] Bøegh, Jørgen : Certifying Software Component Attributes, IEEE Software, vol. 23, no. 3, 2006, pp. 74–81

[4] Bøegh, Jørgen; De Panfilis, Stefano;, Kitchenham, Barbara;, Pasquini, Alberto: A Method for Software Quality Planning, Control, and Evaluation, IEEE Software, Vol. 16, Number 2, pp. 69-77, March/April 1999

[5] EN ISO 12100-1 Safety of machinery. Basic concepts, general principles for design. Part 1: Basic terminology, methodology.

[6] EN ISO 12100-2 Safety of machinery. Basic concepts, general principles for design. Part 2: Technical principles.

[7] Forgue, Bruno. Secure wireless networks for industrial applications. Industrial Ethernet Book Issue 19:43. 4 p. http://ethernet.industrial-networking.com/wireless/articledisplay.asp?id=14

[8] Franch, Xavier; Carvallo, Juan Pablo: Using Quality Models in Software package Selection, IEEE Software vol. 20, no. 1, 2003, pp. 34–41]

[9] Handbok för Programvara i säkerhetskritiska tillämpningar, Försvarsmakten, 2002.

[10] Hedberg, J; Söderberg, A.; Malm, T.; Kivipuro, M.; Sivencrona, H. Methods for Verification & Validation of time-triggered embedded systems. NT Technical report 600. 71 p. http://www.nordicinnovation.net/nordtestfiler/rep6001.pdf

[11] IEC 1025 - “Fault tree analysis (FTA)”, IEC international standard, Genève 1990.

[12] IEC 61508-1. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.

[13] IEC 61508– 4. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions.

[14] IEC 61784 Committee draft for voting. 2006. Digital data communication for measurement and control – Part 3: Profiles for functional safety communications in industrial networks [61784-3/Ed 1.0) 45 p.

[15] IEC 61882. 2001. Hazard and operability studies. (HAZOP studies) –Application guide. 122 p.

[16] IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems

[17] IEC 62280-1 Ed. 1.0 b:2002, Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems

[18] IEC 812 - “Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)”, IEC international standard, Genève 1985.

[19] ISO/FDIS 13849-1. Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design. 96 p.

[20] ISO/IEC 7498

[21] Klemba, Keith: Introducing wireless mesh networking. Industrial Ethernet Book Issue 25. 8 p. (17.8.2005) http://ethernet.industrial-networking.com/wireless/articledisplay.asp?id=223

[22] Kopetz, H.: “Design Principles for Distributed Embedded Applications, Kluwer Academic Publishers, 1997.

[23] Langefors, B.: “Theoretical Analysis of Information Systems”, Studentlitteratur, Lund, 1973

[24] Laprie, J. C., (ed.) Dependability: Basic Concepts and Terminology, Springer-Verlag, Wien, 1992.

[25] Lehtonen, S.; Ahonen, P.; Savola, R.; Uusitalo, I.; Karjalainen, K.; Kuusela, E.; Puuperä, R.; Röning, J.; Tokola, T. Information Security in Wireless Networks. Luoti-program publications. 11.12.2006. 88 p. http://www.luoti.fi/material/InfoSec_in_WNetworks_final.pdf
[26] Liao, Raymond; Weiler, Christoph; Bolderel-Ermel, Wolfgang: Demystifying IEEE 802.11 for industrial wireless LAN's. Industrial Ethernet Book Issue 25. 5 p. http://ethernet.industrial-networking.com/wireless/articledisplay.asp?id=225
[27] Marske, Eric P. The Wireless option for industrial Ethernet. Industrial Ethernet Book Issue 16:30. 6 p. http://ethernet.industrial-networking.com/wireless/articledisplay.asp?id=9
[28] Nielsen, Kjell; Shumate, Ken; Designing large real-time systems with ADA. ISBN 0-07-046536-3
[29] NT TECHN REPORT 460 - Safety assessment of systems containing COTS software.
[30] Poole, I. What exactly is ... ZigBee. IEE Communications Engineer 2, No. 4, pp. 44-45.
[31] Shamos, Michael. Wireless Technologies. 2003. Institute for eCommece. 50 p.
[32] Toijer, D. 2006. Så här används trådlösa datanäten. Automation 4/2006 pp. 24–31.
[33] Wiberg, P.-A.; Bilstrup, U., “Wireless technology in industry- Applications and user scenarios,” in Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA ’01), pp. 122-133.
[34] Willig, A.; Matheus, K.; Wolisz, A., Wireless Technology in Industrial Networks. Proceedings of the IEE, Vol. 93, No. 6, June 2005.

Appendix A: Standards related to the safety of communication

Figure 32 shows standards, which are related to functional safety of communication. The figure is from standard (draft) IEC 61784-3 and the mentioned standards are related to machinery or communication. There are also other standards related to e.g. communication and railway applications.

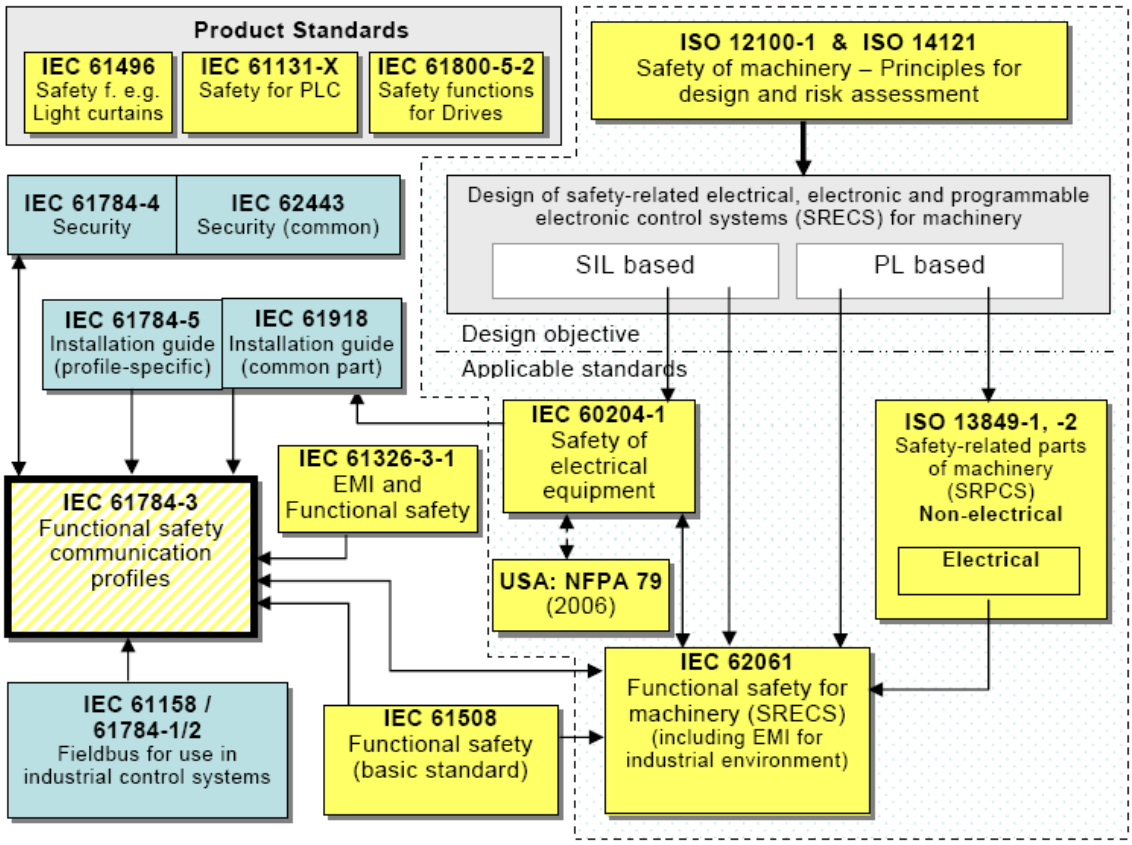


Figure 32. Standards related to functional safety of communication.

Appendix B: Specification of SRCFs (Safety-related control functions)

SRCF No.

Information to be available

Description

Risk assessment

Risk assessment document	

EUC characteristics

Modes of operation	
Cycle time	
Response time	
Environmental conditions	
Interaction of persons	

Information influencing the SRCF

Behaviour of the machine that the SRCF is intended to achieve or prevent	
Interfaces between this SRCF and other SRCFs	
Interfaces between this SRCF and other functions	
Required fault reaction functions	

Functional requirements specification for SRCFs

Machine operating mode where this SRCF shall be active	
Machine operating mode where this SRCF shall be disabled	
Priority in relation to simultaneously active functions	
Frequency of operation	
Response time of this SRCF	
Interface to other machine functions	
Response time of the input device	
Response time of the output device	
Description of this SRCF	
Description of fault reaction function and any constrains	
Description of operating environment	
Test and associated facility	
Rate of operating cycles	
Rate of duty cycle	

Safety integrity requirements specification for the SRCF

SIL	

Figure 33 Form for specification of SRCF

Appendix C: Requirements for safety measures

The overall safety function in a machine control system depends on the safety of communication between safety-related subsystems/modules realising a specific safety function. The requirements listed in the following table shall be fulfilled to ensure and maintain the required safety integrity level for each communication sub-function related to an overall safety function.

Requirement ID	Specification
R1	Safety protection shall be applied to the generation of the data to be transmitted
R2	Safety reaction shall be applied in case of misoperation. This shall be consistent with the safety requirements of the receiver.
R3	Error detection mechanism shall be applied at the receiver and shall be consistent with the safety requirements of the receiver.
R4	The implementation of the safety reaction R2 shall be functionally independent of the nontrusted transmission system.
R5	The residual data error rate of the safety-related transmission system for each information interchange between transmitter and receiver shall be less than a predefined value. This rate shall be compatible with the safety integrity level of each receiver.
R6	The safety integrity level of the safety-related transmission system shall be consistent with the highest safety integrity level of the safety processes.
R7	If the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source identifier to the user data.
R8	Integrity shall be provided by adding a safety code to the user data. The safety process shall not rely on the transmission code generated and checked by integrated circuits being part of the non-trusted transmission system.
R9	The timeliness of user data shall be provided by adding time information (e.g. time stamps, sequence numbers …) to the user data. The time delay which is allowed depends on the application.
R10	If necessary the sequence of messages shall be checked by the safety process.
R11	The safety procedures for the safety-related equipment shall be functionally independent of the procedures used by the non-trusted transmission system. In particular, if both procedures use the same coding mechanism, the parameters (e.g. polynomial) shall be different.
R12	All safety-related equipment shall monitor the performance of the requirements listed in R7, R8, R9 and R10. If the quality of the transmission falls below a level, which is predefined in the system requirement specification then an appropriate safety reaction shall be triggered.
R13	Safety-related and non-safety-related messages shall have different structures achieved by applying a safety code to safety-related messages. This safety code shall be capable of protecting the system to the required safety integrity level (see 5.1) that a non safety-related message changes to a safety-related one.
R14	The safety procedures of the safety-related equipment shall be functionally independent from the procedures used by the non-trusted transmission system and by the non safety-related equipment.

R15	To fulfil the required safety integrity level (see 5.1) it is necessary to detect and act on typical faults of the non-trusted transmission system. The faults to be considered shall at least include: • interrupted transmission line, • all bits logical 0, • all bits logical 1, • message inversion, • synchronization slip (in case of serial transmission).
R16	To fulfil the required safety integrity level (see 5.1) it is necessary to detect and act on typical errors. These errors to be considered shall at least include: • random errors, • burst errors, • systematic errors, for example repeated error patterns, • combinations of the errors listed above.
R17	The safety code shall be functionally independent from the transmission code.
R18	The safety code shall guarantee that the non-trusted transmission system shall be very unlikely to be able to generate a correct safety code word.
NOTE The se requirements are adapted from [17]	

Figure 34 Requirements for safety measures

Appendix D: Checklist for the validation of safety management

No	Requirement	Yes	No	Ref. in this document	Ref. IEC 62061	Comments
1	Has a functional safety plan been drawn up for the design of the SRECS?			6.1	4.2.1	
2	Does the plan identify the relevant activities specified in IEC 62061, clauses 5 to 9?			6.1.1	4.2.1a	
3	Does the plan describe the policy and strategy to fulfil the specified functional safety requirements?			6.1.2	4.2.1b	
4	Does the plan describe the strategy to achieve functional safety for the application software, development, integration, verification and validation?			6.1.3	4.2.1c	
5	Has the responsibility and identification of persons, departments and organisa-tions carrying out design and specification activities and safety management reviewing been established?			6.1.4	4.2.1d	
6	Have the procedures and resources to record and maintain information relevant to the functional safety of the SRECS been identified or established?			6.1.5	4.2.1e	
6.1	Have the results of the hazard identification and risk assessment been considered?			6.1.5	4.2.1e	
6.2	Has the equipment used for safety-related functions together with its safety requirements been considered?			6.1.5	4.2.1e	
6.3	Has the organisation responsible for maintaining functional safety been considered?			6.1.5	4.2.1e	
6.4	Have the procedures necessary to achieve and maintain functional safety (including SRECS) modifications been considered?			6.1.5	4.2.1e	

No	Requirement	Yes	No	Ref. in this document	Ref. IEC 62061	Comments
7	Does the safety plan describe the strategy for configuration management taking into account relevant organisational issues, such as authorised persons and internal structures of the organisation?			6.1.6	4.2.1f	
8	Has a verification plan been established?			6.1.7	4.2.1g	
8.1	Does the established verification plan include details of when the verification shall take place?			6.1.7	4.2.1g	
8.2	Does the established verification plan include details about the persons, departments or units who shall carry the verification?			6.1.7	4.2.1g	
8.3	Does the established verification plan include the selection of verification strategies and techniques?			6.1.7	4.2.1g	
8.4	Does the established verification plan include the selection and utilisation of test equipment?			6.1.7	4.2.1g	
8.5	Does the established verification plan include the selection of verification activities?			6.1.7	4.2.1g	
8.6	Does the established verification plan include the acceptance criteria and the means to be used for the evaluation of verification results?			6.1.7	4.2.1g	
9	Has a validation plan been established?			6.1.8	4.2.1h, 8	
9.1	Does the validation plan include details of when the validation shall take place?			6.1.8	4.2.1h, 8	
9.2	Does the validation plan include an identification of the relevant modes of operation of the machine (e.g. normal operation, setting, etc.)?			6.1.8	4.2.1h, 8	
9.3	Does the validation plan include the requirements against which the SRECS is to be validated?			6.1.8	4.2.1h, 8	

No	Requirement	Yes	No	Ref. in this document	Ref. IEC 62061	Comments
9.4	Does the validation plan include the technical strategy for validation, for example analytical methods or statistical tests?			6.1.8	4.2.1h, 8	
9.5	Does the validation plan include the selection and utilisation of test equipment?			6.1.8	4.2.1h, 8	
9.6	Does the validation plan include the acceptance criteria?			6.1.8	4.2.1h, 8	
9.7	Does the validation plan include actions to be taken in the event of failure to meet the acceptance criteria?			6.1.8	4.2.1h, 8	
10	Does the functional safety plan ensure a prompt follow-up and satisfactory resolution of issues relevant to a SRECS arising from activities specified in IEC 62061, clauses 5 to 9?			6.2	4.2.2, 8	
10.1	Does the functional safety plan ensure a prompt follow-up and satisfactory resolution of issues relevant to a SRECS arising from verification activities?			6.2	4.2.2, 8	
11	Are all documents necessary to perform effectively all the phases of the overall safety lifecycles provided?			6.3	10	

Appendix E: Industrial applications

There will be more and more new wireless application in the industry here some examples of some safety-related wireless communication applications:

- Automine concept (Sandvik Tamrock). In the system automated loaders are controlled via wireless link. Both automated drive and remote control are used.
- Automated straddle carriers (Kalmar Industries). The Straddle carriers are controlled via wireless link. The carriers can carry a container from harbour crane to storage in a controlled area.
- Wireless control of automated guided vehicles (AGVs). Often battery-operated AGVs need wireless control since there are no wires. The distance between antennas (transmitter/receiver) is often short.
- Remote controlled cars in road making. In some methods the car must drive exactly a certain line, which can be seen better from behind the car. Wireless remote control is used to drive the car.
- Wireless remote control of cranes is very common.
- In some cars it is possible to measure tyre pressure, when car is driving. Wireless link is needed from tyre to car body.
- It is possible to get information from gate to machine via wireless link (Schmersal). There is a battery in the gate, solar cell and generator, which produces energy when it is opened. When gate is open the information is sent to the receiver (machine).
- Wireless stopping device is used in various applications. For example, in stone crushing yards, schools

ABB application in Volvo factory

Conventional assembly lines using robotics require frequent maintenance interventions. This is due to the fact that a robot moves the end-effector/griper in very complex patterns exposing the cabling to heavy wear and tear forces. These wires are used internally to transmit commands and performance data, and for the power supply of robot modules. The movement of the robot is also limited by external cabling. It is worth to notice that hanging cables are potential hazards since they can easily get entangled in other automation equipment.

At Volvo Cars Body Components in Olofström Sweden, ABB aimed at replacing the wired communication between the robot controller and the griper by implementing Wireless Interface to Sensors and Actuators (WISA) and powering the end-effector with a contactless power supply. The reliability of wireless communication technology was the first concern and consequently, the behaviour of the system was tested in the following environments:

1) **Industrial environment:** Extreme temperature, vibration, steel constructions, and obstructions. Issues facing wireless communication in such environments are heavy multipath fading, fast/slow fading, coverage quality (due to reflection), and local variations in received power.
2) **EMI:** Electromagnetic Interference from electrical activity such as drives and welding which cause noise in radio frequency bands.
3) **Oth**er **Users** : Occupation of frequencies by other radio users over time (WLAN, Bluetooth, ZigBee, etc)

The WISA system was tested in welding applications and the wireless proximity switches (WPS) were tested in both spot welding and arc welding installations.

Interferences with other wireless devices operating in the same frequency including neighbouring WISA systems ("self interference"), WLANs and Bluetooth band were also a matter of concern. Tests of worst case arrangements where other wireless systems were placed in very close proximity of WISA setups showed only a marginal effect on WISA performance. Very few telegrams had to be retransmitted.

A pilot system of the wireless I/O and a contactless power transfer was installed in Olofstöm in parallel with the existing wired solution and tested extensively. No measurable impact on the wireless communication or contactless power supply could be detected and Volvo decided to switch to full production with the wireless system.

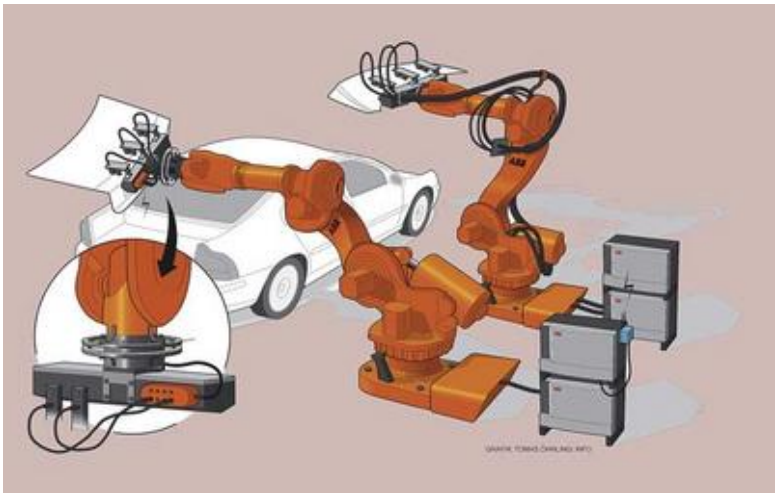
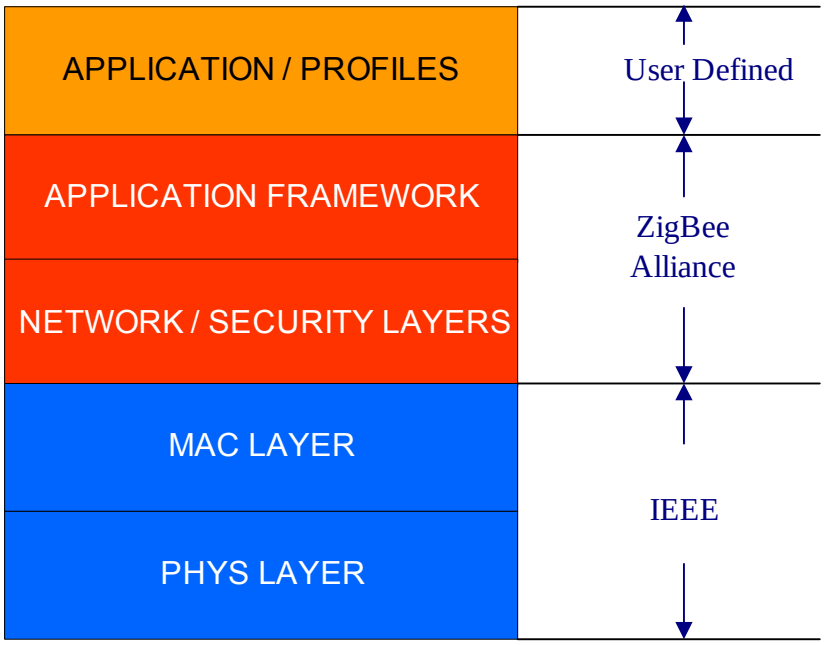


Figure 35. Pilot case in Volvo.

Pilot installation of a wireless I/O and contactless transfer in the production cell for the front wheel house assembly of the Volvo S80, XC70 and V70

Appendix F: More on ZigBee

The characteristics of the physical and MAC layers of a radio networking stack is specified in the IEE 802.15.4 standard. The aim is to meet the requirements for reliability, security, low power and low cost in wireless monitoring and control applications. Included in the Physical layer (PHY) are features like receiver energy detection, link quality indication and clear channel assessment. Packet losses due to errors or collisions, are detected by retransmissions in the MAC layer and then eliminated prior to any slow down that could be initiated by the (TCP).



IEEE 802.15.4 Stack

Range of transmission
The ZigBee-platform implements the RF- and baseband communication functions of the ZigBee device. The range of transmission (10 m – 100 m) depends not only on the frequency at which the network operates, but also whether the network operates indoors or outside. Another factor is the power level at which the items operate, 0 dBm (1 mW, the most common power) or higher. The maximum transmission power 20 dBm (100 mW) requires an amplifier external to the ZigBee chip.

Transmission control protocol (TCP) and packet losses
The MAC layer enables network association and dissociation and has an optional superframe structure with beacons for time synchronisation as well as a guaranteed time slot (GTS) mechanism for high priority communications.
For security purposes, IEEE 802.15.4 provides authentication, encryption and integrity service. The developer can choose between no security, an access control list and encryption with authentication.

Network topology

IEEE 802.15.4 ZigBee specifications enable reliable and secure mesh, star and cluster-tree network topologies.

Star networks are common and provide for very long battery life operation.

In cluster-tree networks, routers move data and control messages through the network using a hierarchical strategy that combines the benefits of high levels of reliability and support for battery-powered nodes.

Mesh or peer to peer networks enable high levels of reliability and scalability by providing more that one path through the network.

Appendix G: Function monitoring using wireless networks – reliability and power management on ZigBee

An industrial plant uses wireless sensor/actuator networks in its production chain, to access relevant machinery for the diagnostic or programming purposes, the localisation and tracking of unfinished parts, the coordination of autonomous transport vehicles and mobile robots. The function monitoring in this environment requires reliable delivery of monitoring messages and power management of diverse battery-operated devices regardless of time- and location-dependent channel quality and signal attenuation.
The current safety-function monitoring addressed:

- the transmission of functional control signals, data and emergency messages (air pressure, temperature of specific parts, air flow, safety-critical dysfunction, abnormal system state, motor activity and vibrations, current location of mobile/moving module) which involves periodic monitoring/transmission for some safety-critical functions and event-driven for others.
- The power conservation (conserve device power while satisfying the reliability requirements of system monitoring)for which the influencing factors are the device range, the available power, the bit rate, the routing protocol and the failure or the uncooperative behaviour of other devices.

Reliability of message delivery and power conservation are somewhat conflicting goals. Four conservation protocols for power management were used:

- Maximum power from current system device and cooperating devices (MP-MCD), for emergency messages. This protocol performs well under low device density, where higher transmitted power is required to reach a neighbouring node.
- Optimal power from current system device and cooperating devices (OP-OCD), for non emergency periodic transmission of routine safety-related signals and to reduce the network traffic.
- Maximum power from current device and optimum from cooperating devices (MP-OCD), for situations involving non-emergency and periodic transmission of functional signals which are not safety-related
- Random power from current system device and cooperating devices (RP-RCD), for comparison between protocols of the worst case scenario.

The power conservation protocols were combined with sleep strategy, involving the saving of transmitted power at the physical layer. Information from network and application layers were utilised to create balance between reliability and power conservation, as illustrated in the following figure.

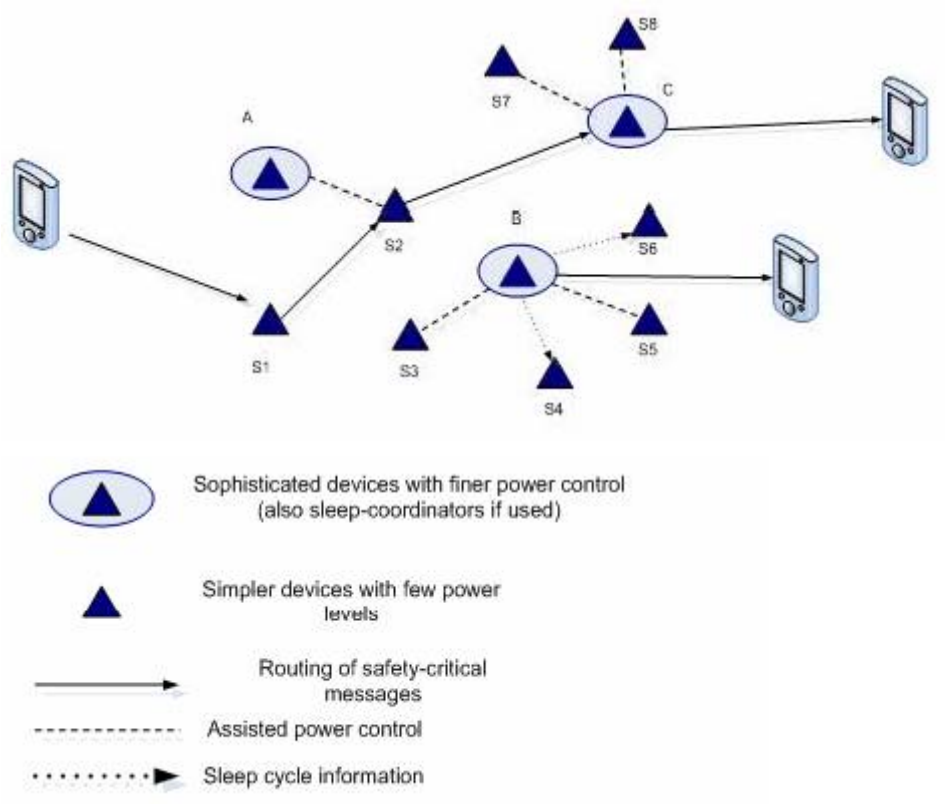


Figure 36. An example of a small wireless network, which has safety related communication and power critical functions.

norden
Nordic Innovation Centre

Return address:
Nordic Innovation Centre,
Stensberggata 25
NO-0170 Oslo, Norway

NORDTEST

NORDTEST is a Nordic Innovation Centre brand offering competence and expertice in the field of harmonizing of norms and methods,a large Nordic net-work of experts, more than 650 recommended Nordic testing methods and 550 published technical reports.

www.nordicinnovation.net

Nordic Innovation Centre

The Nordic Innovation Centre initiates and finances activities that enhance innovation collaboration and develop and maintain a smoothly functioning market in the Nordic region.

The Centre works primarily with small and medium-sized companies (SMEs) in the Nordic countries. Other important partners are those most closely involved with innovation and market surveillance, such as industrial organisations and interest groups, research institutions and public authorities.

The Nordic Innovation Centre is an institution under the Nordic Council of Ministers. Its secretariat is in Oslo.

For more information: **www.nordicinnovation.net**