

Safety bus systems

Prof. Dr.-Ing. Josef Börcsök, HIMA Paul Hildebrandt GmbH + Co KG, Germany

Abstract

Modern distributed control systems are connected via bus systems, which need effective and uninterrupted communication between all subscribers. Therefore it is necessary for these communications to be fault tolerant and safe. For safety related systems, additional safety layers are required to fulfil these requirements. In a safety related application it is important to understand that a safe protocol alone cannot fulfil this requirement without two safe source and destination hardware nodes. Only the marriage of safety related protocol and safety related hardware nodes can fulfil the requirements for safety related bus systems.

1 Basics of functional safety

For nearly 20 years, great effort has been made in developing National, European und International standards for control engineering. In the early 1980s the International Electrotechnical Commission (IEC) and the German Institute of Standardization (DIN) investigated the fundamental requirements for protective systems using measurement and control techniques.

The IEC was mainly concerned with computer technology. DIN was concerned with risk assessment (DIN V 19250), the general requirements for protective devices (DIN V 19251) and computers in systems with safety tasks (DIN V VDE 0801). In 1989, these German standards were integrated into the European standards e. g. the EN 1050 for risk assessment and the EN 954-1 in scalable requirements to safety-relevant parts of controllers. Later in 1991, development continued by the IEC toward a holistic standard encapsulating full lifecycle concepts titled “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems” (IEC 61508). This is now an Australian Standard.

With safety related microprocessor based systems, random component faults are not the main contributor to a failure. The main contributor is the specification on how the system should operate, which is implemented by the engineer or the programmer. The next major contributor is modifications after commissioning operation and maintenance, since the intent of the original design and safety engineering is often not understood by the end user. Measures must be taken to prevent or minimise such errors in the development/design phase of a safety system.

For the original manufacturer of safety related systems, the standards DIN V VDE 0801 and IEC 61508 differentiate between measures for **fault avoidance** during the development stage and **fault control** by of the final product. Fault avoidance in design of the electronics is applied by the manufacturer and verified by a test organisation such as the German test institute Technischer Überwachungsverein (TÜV). These measures are applied in the course of the planning, development, and manufacture such that errors may be detected and corrected. The measures for fault control are part of the system hardware and software functionality and result in an appropriate safety-related action.

In complex systems, errors can only be managed effectively with rigorous procedures for the design, development and maintenance phases. The aim is to avoid errors from the very beginning and use

constructive and analytical processes along with testing and verification throughout the entire safety life cycle.

In the standard IEC 61508 the respective phases of the safety life cycle are described by fundamental requirements for each phase. Parts 2 and 3 of the standard contain guidelines for the implementation of electrical, electronic and programmable electronic (PES) systems. These guidelines if followed allow for the “realisation” of a complex safety system with an acceptable degree of fault avoidance. These measures are contained in the annex A and B of parts 2 and 3, scaled according to their effectiveness, and described in detail in part 7.

The concept of the safety life cycle is founded on the fact that in complex systems, functional safety can be ensured by verification over the entire life cycle of the system. German test institutes such as the TÜV have applied this approach for many years when certifying microprocessor based systems for safety related applications. An acceptance by such a test institute begins with the so-called “development-accompanying examination” in the product requirement specification/concept phase. The examination continues with the design phase, the operation phase as well as the modification and maintenance phases of the system.

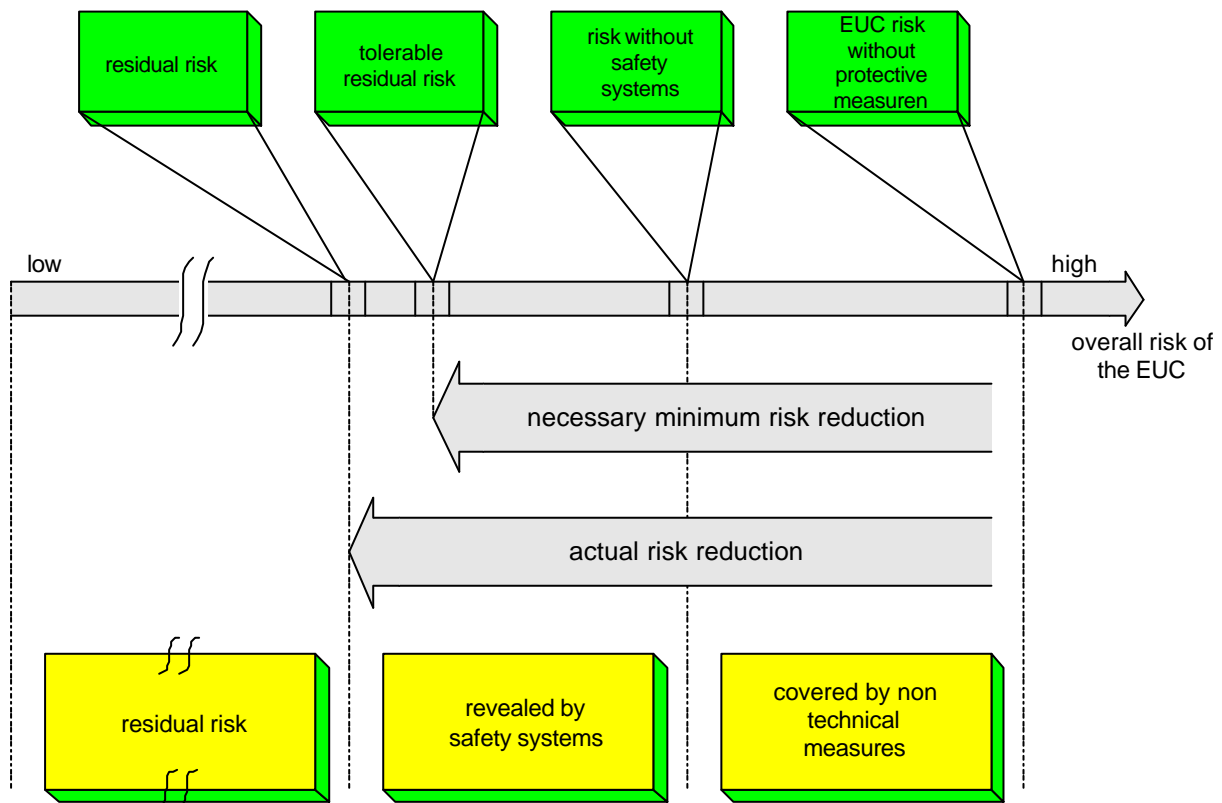


Figure 1: Risk minimisation model for Plant and Equipment.

The safety related reliability of complex safety systems can be only achieved with the application of rigorous and analytic processes incorporating continual verification and testing. The extent of these measures varies depending upon the necessary risk minimisation necessary by the safety function. Figure 1 shows the concept of risk reduction. Required risk reduction is achieved by a combination of technical and non

technical methods, with the result that the remaining (residual) risk of the hazardous plant or equipment is reduced to an acceptable level.

The question remains, how is this acceptable residual risk defined? In Germany it is generally accepted that the tolerable residual risk cannot be absolutely specified. The necessary risk reduction of technical equipment can only be determined based on analogy against experience. Plant and equipment that has a continual human presence in its vicinity which has the capacity for loss of life or limb, may require substantial fault avoidance and fault control. Figures 2 and 3 demonstrate the processes used by manufacturers and test institutes for fault avoidance. A measurement of the degree of risk reduction is the so-called Safety Integrity Level (SIL) as identified in the standard AS 61508. The SIL identified in AS 61508 can be approximated against the categories of the EN 954, part of 1 and the requirement classes (AK) of the DIN V VDE 0801 and DIN V 19521, as shown in table 1.

Category (EN 954-1)	Requirement class (DIN V 19250)	SIL (IEC 61508)	description
B	1	-	Control Systems according the state of the art/proven in use
2	2/3	1	Test
3	4	2	Single fault tolerance with partial fault detection
4	5/6	3	Self monitoring
-	7/8	4	Not relevant for machine protection

Table 1: Qualitative relationship between fault avoidance measures according to the separate standards

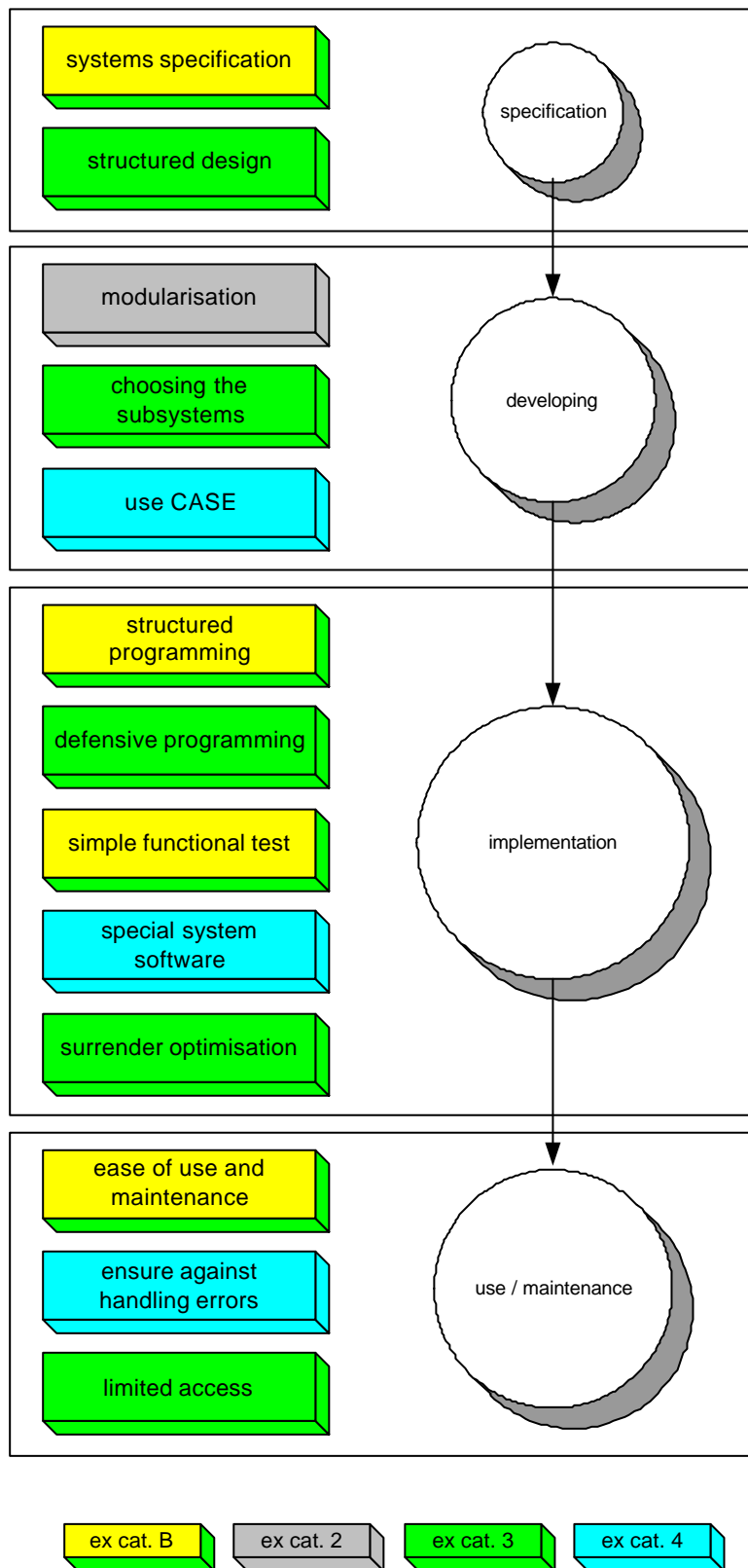


Figure 2: Fault avoidance measures of manufacturers

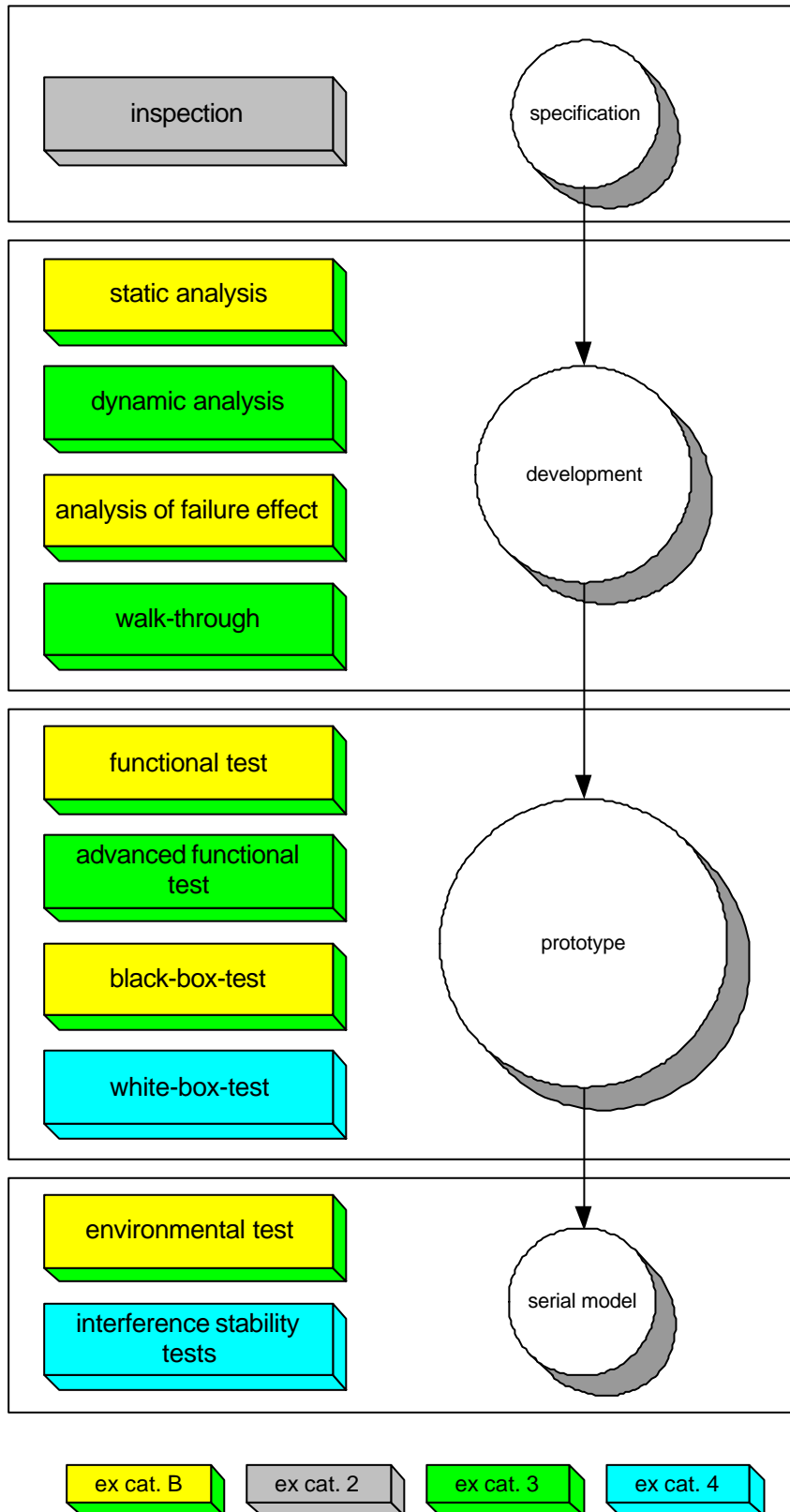


Figure 3: Fault avoidance measures of test institute

2 The basis of Fault Control

It can be seen from the three schematics above that risk reduction is a function of architecture and the methods used in fault avoidance varies accordingly. All standards for functional safety identify safety related reliability of a complex system as a function of redundancy as well as technical or non technical measures for fault detection of its subsystems.

However, it is not possible to develop a complex system completely free of faults. The system's risk reduction can be impaired by random failures of single components. These random failures are unavoidable, thus they have to be controlled. To put "the control of faults" into context means (1) with redundancy the fault does not lead to the failure of the safety equipments ability to function; or (2) the fault is diagnosed sufficiently early that the safety equipment can be repaired in a satisfactory time period. A further important factor for the evaluation of a safety system in addition to redundancy and fault detection is the reliability of the component.

The necessary risk reduction for a safety function based on reliability data of electronic components can be expressed mathematically. The Safety Integrity level (SIL) is defined as probability of failure to perform the safety function on demand or respectively the probability of failure per hour, according to the standard IEC 61508, as shown in table 2.

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	10^{-5} to $< 10^{-4}$	10^{-9} to $< 10^{-8}$
3	10^{-4} to $< 10^{-3}$	10^{-8} to $< 10^{-7}$
2	10^{-3} to $< 10^{-2}$	10^{-7} to $< 10^{-6}$
1	10^{-2} to $< 10^{-1}$	10^{-6} to $< 10^{-5}$

Table 2: Definition of the Safety Integrity Level from IEC 61508

It is important, that the reliability of components is not predefined. That is why requirement classes, categories and SILs for the aspect to the fault control cannot be assigned directly each other. A correlation can only be established if the relevant structures are described more precisely and the single-channel subsystems have assigned failure rates. Table 3 shows the relationship for structures of electronic safety systems, used as protective system for machinery in the category B, category 2, category 3 and category 4 as protective system.

SIL	System architecture (Controller structure)	Mean Time To Failure MTF (Years)	CCF â (%)	Diagnostic coverage per channel (%)	Category
		In/Processing/Out		In/Processing/Out	
-	Single channel PE, single channel PE I/O	15/15/30	-	0/0/0	B
	Single channel PE, single channel I, Ext. WD (t / nt)	15/15/30	-	0/60/0	B
	Dual channel PE, dual channel I/O, 1oo2	15/15/30	5	0/0/0	inapplicable
1	Single channel PE, single channel I, Ext.	15/15/30	-	100/60/100	2

	WD (t / nt)				
	Single channel PE, single channel I, Ext. WD (t / nt)	7,5/15/10	-	100/60/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	5	100/60/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	10	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	45/15/60	10	100/90/100	3
2	Dual channel PE, single channel I, Ext. WD (t)	15/15/30	-	100/90/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	1	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	30/30/60	5	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	7,5/15/10	1	100/99/100	4
3	Single channel PE, single channel I, Ext. WD (t)	30/30/60	-	100/99/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	45/45/90	1	100/99/100	4

Caption:	
WD(t/nt):	Watchdog timer and associated switch-off path tested/untested
WD(t):	Watchdog timer and associated switch-off path tested
I/O:	Input/Output
PE:	Programmable electronics
Cat.:	Category
1oo2:	Dual channel safety-related structure
CCF:	Common cause failure
IPC:	Comparison between the channels
Conditions for single-channel systems:	
<ul style="list-style-type: none"> • All test rates: 1/ (15 minutes) • The demand rates: 1/ (24 hours) • The repair rates: 1/ (8 hours) • The life span: 10 years • The MTTF of the watchdog timer: 100 years • The MTTF of the switching of paths is as a normal switching of paths 	
Conditions for two-canal systems:	
<ul style="list-style-type: none"> • All test rates: 1/ (24 hours) • The demand rates: 10/ hour • The repair rates: 1/ (8 hours) • The life span: 10 years 	

Table 3: Context between controller architectures and SILs

Description of the input parameters	Parameter
MTTF of sensors, PE-devices and PLC	15 years
MTTF of a shut down path of actuators	30 years
MTTF of Watchdogs	100 years
Lifetime operating	10 years
Repair rate (after a fault detection or a dangerous event)	1/(8 hours)
All test rates of single channel systems	1/(15 minutes)
All test rates of multi channel systems	1/(10 seconds)
All demand mode of single channel systems	1/(24 hours)
All demand mode of multi channel systems	1/(10 seconds)

Table 4: Input parameter for the calculation of typical controller structures

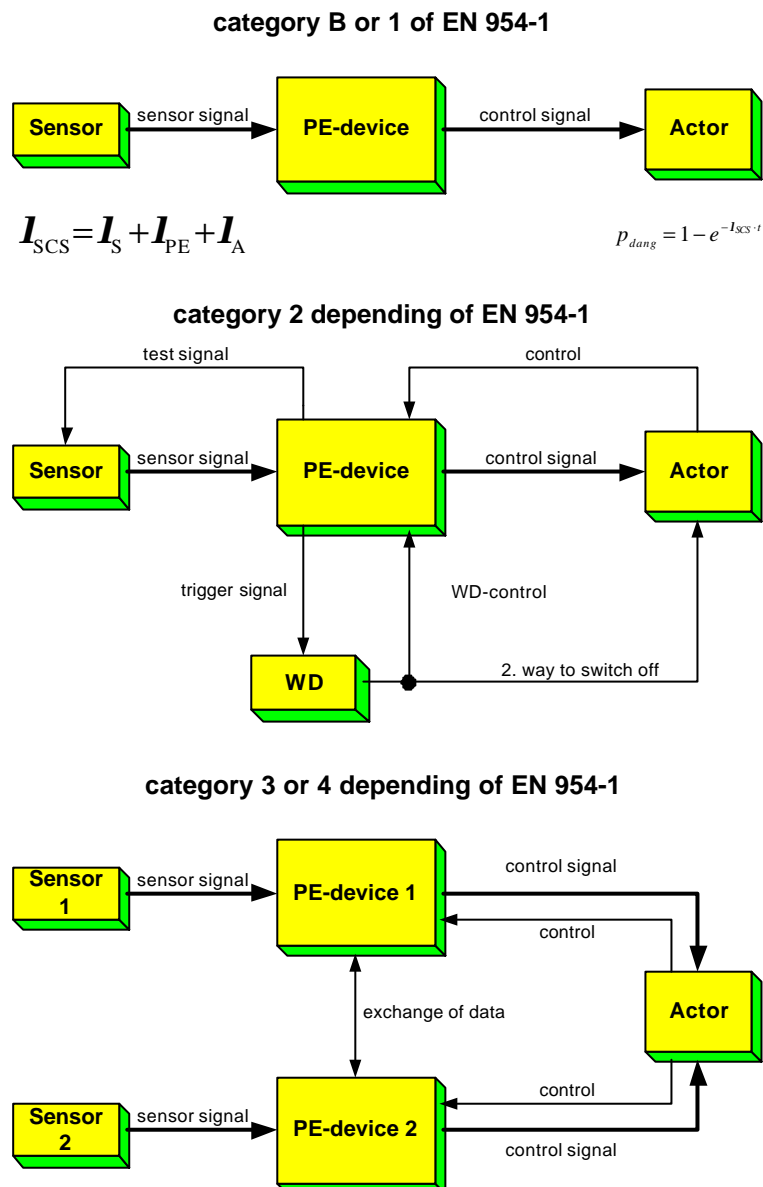


Figure 4: Overview of system architectures as shown in table 3.

The SIL calculation is based on the architectures shown in figure 4 and the initial parameters from table 4. Given an operating lifetime of 10 years an average probability of failure is calculated. For the individual structures in machine protection usual conditions are accepted.

Prerequisites for the relevant system structures:

- The switch-off of the drive causes the machine to the safe state.
- The safety system itself does not initiate a dangerous/hazardous situation. In the worst case a dangerous failure hinders the safety system in executing the safety functions.
- When faults are detected, the safety system will be repaired. After repair the system is regarded 100 % functional safe.

The necessity of automatic tests to detect failures is shown in table 3. Examples of self-test with an estimation of the effectiveness can be found in the appendix A of IEC 61508, part 2. The following tables (table 5 and table 6) show in context the relative effectiveness in relation to diagnostic coverage.

Component	Requirements for diagnostic coverage or safe failure fraction claimed		
	low (60 %)	medium (90 %)	high (99 %)
Electromechanical devices	Does not energize or de-energize welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or deenergize Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent) No positive opening (for position switches this failure not assumed if they are built and tested according to EN 60947-5-1, or equivalent)
Discrete Hardware			DC-fault model, drift, oscillation
Digital I/O	Stuck-at	DC-fault model	
Analogue I/O	Stuck-at	DC-fault model, drift, oscillation	DC-fault model, drift, oscillation
Power supply	Stuck-at	DC-fault model, drift, oscillation	DC-fault model, drift, oscillation
Bus			
General	Stuck-at of the addresses	Violation of timing conditions / time out	Violation of timing conditions / time out
Memory management unit (MMU)	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
Direct memory access (DMA)	No or continuous access	DC fault model for data and addresses Wrong access time	All faults which affect data in the memory Wrong data or addresses Wrong access time
Bus-arbitration	Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration
CPU			
Register, internal RAM	Stuck-at for data and Addresses	DC fault model for data and addresses	DC fault model for data and addresses Dynamic cross-over for memory cells No, wrong or multiple addressing
Coding and execution including flag register	Wrong coding or no execution	Wrong coding or wrong execution	No definite failure assumption
Address calculation	Stuck-at	DC fault model	No definite failure assumption

Program counter, stack pointer	Stuck-at	DC fault model	DC fault model
Interrupt handling	No or continuous interrupts	No or continuous interrupts Cross-over of interrupts	No or continuous interrupts Cross-over of interrupts
Invariable memory	Stuck-at for data and addresses	DC fault model for data and addresses	All faults which affect data in the memory
Variable memory	Stuck-at for data and addresses	DC fault model for data and addresses Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	DC fault model for data and addresses Dynamic cross-over for memory cells No, wrong or multiple addressing Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher
Clock (quartz)	Sub- or super harmonic	Sub- or super harmonic	Sub- or super harmonic
Communication and mass storage	Wrong data or addresses No transmission	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence
Sensors	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation
Final elements	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation
<p>Remark:</p> <ol style="list-style-type: none"> 1. Bus arbitration is the mechanism to determine, which device controls the bus. 2. Stuck-at is a failure category, which shows a constant “0” or “1“ on the pins of the component. 3. The DC-fault model incorporates the following modes: <ol style="list-style-type: none"> a. Stuck-at b. Line break c. High impedance outputs d. Short circuit between signal lines. 			

Table 5: Faults or failures to be detected during operation or to be analyzed in the derivation of safe failure fraction

Component	Low diagnostic coverage	Medium diagnostic coverage	High diagnostic coverage
CPU	total less than 70 %	total less than 90 %	
register, internal RAM	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
coding and execution including flag register	50 % - 60 %	75 % - 95 %	-
address calculation	50 % - 70 %	85 % - 98 %	-
program counter, stack pointer	40 % - 60 %	60 % - 90 %	85 % - 98 %
Bus			
memory management unit	50 %	70 %	90 % - 99 %
bus-arbitration	50 %	70 %	90 % - 99 %
Interrupt handling	40 % - 60 %	60 % - 90 %	85 % - 98 %
Clock (quartz)	50 %	-	95 % - 99 %
Program flow monitoring			
temporal	40 % - 60 %	60 % - 80 %	-
logical	40 % - 60 %	60 % - 90 %	-
temporal and logical	-	65 % - 90 %	90 % - 98 %
Invariable memory	50 % - 70 %	99 %	99,99 %
Variable memory	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Discrete hardware			
digital I/O	70 %	90 %	99 %
analogue I/O	50 % - 60 %	70 % - 85 %	99 %
power supply	50 % - 60 %	70 % - 85 %	99 %
Communication and mass storage	90 %	99,9 %	99,99 %
Electromechanical devices	90 %	99 %	99,9 %
Sensors	50 % - 70 %	70 % - 85 %	99 %
Final elements	50 % - 70 %	70 % - 85 %	99 %

Table 6: Diagnostic coverage and effectiveness for different subsystems

Besides the described measures to control random faults the German and International standards describe measures for the control of systematic failures. These measures are supplementary to the measures of fault avoidance. Examples are: plausibility testing and program monitoring by an external watchdog. These two measures can be helpful to detect disturbances in the functional software in time, which are caused either by programming failures or by unexpectedly strong electromagnetic influences on the systems memory.

The implementation of networking and bus systems as safety technology also requires the same consideration of the entire life cycle as discussed earlier. Safe communication systems are complex systems consisting of transmitters and receivers of safety-relevant information. The design of a safe communication system therefore requires the same prerequisites for risk reduction, fault avoidance and fault control.

It is important to note however, that safe communication over a bus alone does not ensure that the transferred safety-relevant function is also safe. The information must be produced and processed safely. It is nevertheless possible with the development of safe complex electronic systems to include bus systems into the safety system. This requires further qualitative and quantitative requirements, which are described in the following sections.

3 Fundamental requirements of safe bus systems

In industry there can be a wide range of plant and equipment with requirements far beyond that of normal process control, such as machinery control where reaction times are very fast.

If you take automobile production for example, there are manually fed presses that have press controllers which use a light curtain to detect human intrusion. Should the light curtain be penetrated the press bear which presses the raw material into the form must stop in sufficient time to protect the user from harm. Such control has to be fulfilled in a relatively small response time, such as 10 milliseconds.

Thus to the fast machinery process, not only does the speed of response have to consider the machinery but it also has to allow for the speed at which a person can intervene into the hazardous area. The protection field provided by light curtains, laser-scanners or ESPE (Electro Sensitive Protective Equipment), must be engineered with consideration of the dynamics of machine and user with additional safety margins.

In the standard EN 999, the guidelines for such protection fields are identified and the response time of an ESPE determines the distance a light curtain is installed from the dangerous area. The mode of operation of a hazardous system is operated in accordance in the IEC 61508 in high demand mode.

Other industries differ in that the instrumentation of the control system, is completely separate to the safety control system. This monitoring PES implements the required shutdown functions in seldom cases of failure in the functional controller. The mode of operation of such a monitoring PES is according to IEC 61805 in a low demand mode. In addition, with processes with a response time of some 100 milliseconds a low demand mode is completely sufficient. This applies also to safety systems, which are under complete control of human being, e. g. vehicles or machine which can be brought by the emergency stop into a safe state in a time range of 100 milliseconds.

The demand rate of a safety system is generally high if the response times are 50 to 150 milliseconds, and it usually operates in high demand mode. These data refer to universal controllers (PES) and/or bus systems, which can be used within the machinery and plants without limitation.

The discussion until now has been in relation to controllers and their bus systems within the range of the sensor and actuator. With complex machines, the transmission of a large amount of data plays an important role with many safety relevant parameters being transferred to the processing safety system. In some instances it may be required to exchange complete or parts of application programs via the bus systems.

With transmissions of middle to large quantities of data, it is conceivable to make operational adjustments to the field device parameters in real time under certain machine situations. As an example, if the position of a robot arm has an influence on the sensor positioning for personnel detection, it may be possible to adjust the sensor position based on robot arm position. Possibilities for the future include dynamic reconfiguration of various elements of the safety control system in real time without interruption to the operation of the plant and equipment. Such possibilities may lead to new efficiencies and savings in operations not conceivable with conventional I/O.

Due to the large quantity of data required to be transferred, a bus system needs to be capable of a very high baud rate. It is also an important economic consideration that a universally applicable safety related bus

system should be based on open standards. The following table 7 shows the requirements to a desirable universal system:

Application / Operation mode	Reaction time	Typical amount of data	Example
Sensor / Actuator Low demand mode	≤ 150 ms	~1 Byte	Safety off
Sensor / Actuator High demand mode	≤ 150 ms	~1 Byte	Admittance protection Laser scanner
Sensor / Actuator High demand mode	≤ 10-100 ms	~1 Byte	Finger protection Light barriers
Sensor / Actuator Low demand mode "offline"	As long as needed	some megabyte	Software update
Sensor / Actuator High demand mode "offline"	Tolerance time of the process ≤ 100 ms	some kilobyte	Switching of protection areas of laser scanners within the reaction time
Note: The exact times are to be determined by a application dependent risk evaluation with consideration of the appropriate standards.			

Table 7: Overview of the requirements of the process to the bus systems

3.1 Qualitative measures against transfer failures

Figure 5 shows a circuit diagram of a simple bus system. The intelligent source sends a message via an interface to a protocol component. Usually this is a commercial integrated circuit, which converts parallel or serial incoming messages into a serial, bus-specific transmission protocol on a two-wire cable. The protocol receiver component converts the detailed incoming messages into a useful signal. The bus system consists of a transmitter and/or bus receiver and the transmitting media. For economic reasons, all presented bus systems work with functionally “proven in use” standard components and protocols.

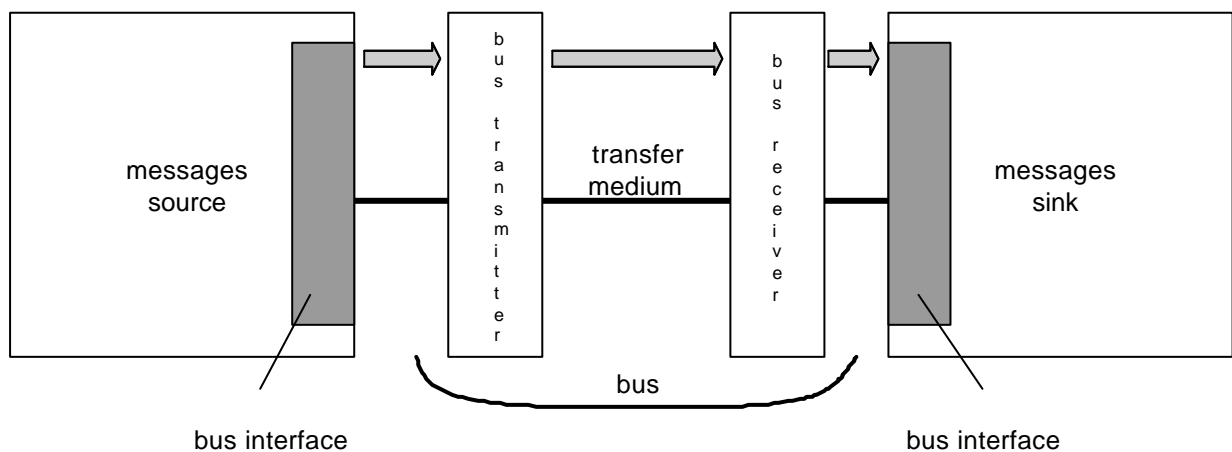


Figure 5: Schematic of a simple bus system.

Conventional proven safety I/O cannot be replaced by a simple commercial bus system without the addition of failure detection technology. Without failure detection technology the bus system will probably function physically, however the necessary and required measure of risk reduction will not be reached. Following are some important considerations for bus system in safety related applications:

- The interface between bus protocol controller and processing unit of the controller may not automatically safe against short-circuit, interruption etc.
- While the timing behaviour of conventional wiring is usually sufficiently fast, in serial bus systems delays may be possible.
- With conventional wiring participant addressing is fixed by the electrical structure and/or connection diagram. Bus systems are able to bring flexibility inside the system, with the addition of protocol considerations there is greater potential for faults.
- A bus can be regarded due to its characteristics as a storage media for information. During an incorrect transmission the system may send the data repeatedly to the receiver. This functionality can stress at a certain time, causing a potential danger in the safety communication. In such an instance the data in transmission could have already lost its validity.
- A conventional control system is usually wired 1 to 1. Additional parts of a controller are usually inserted by means of additional connections, thus with the correct physical wiring there is no interference between non safety-relevant and safety-relevant elements. With open bus systems however both control parts (safety related and non safety related systems) and additional merged participants have a direct influence on the safety-relevant signals using the bus.
- Using the quiescent current principle the signal coordination for each connection is unique. Therefore hard-wired control parts are to a large extent insensitive to signal distortion. With bus systems however there are electromagnetic disturbances, which have an influence on the signals.

Although the above considerations are not a complete list of possible problems of a safety related bus system, it is possible to control these with bus fault avoidance technology . This is the case even with commercial bus systems that interconnect safety related participants. Thus a functional safety level is possible in combination with the flexibility and the efficiency of commercially available “off the shelf” components.

3.1.1 Definition of terms

This section deals with terms, which are used within this subject area that are often confused or misused. Words such as telegram, protocol, message, information or frameworks, are often differently interpreted. For this reason the most important terms, which are used in this paper, are briefly described:

3.1.2 Message and reaction time

A message consists of the transferred process data (the actual information) and the address (the location where information, to which sink the message should be sent). The process data and the addresses are combined into the data of the message. A consistency check is carried out on the process data and the address. An additional check is carried out on the process performed to confirm the correct data has been

received; this ensures data protection and utilises a checksum of the message. The most commonly used is the CRC check, which calculates a checksum via a mathematical algorithm over the complete message. This checksum is separately calculated by the receiver from the message data and then compared with the sent checksum for verification.

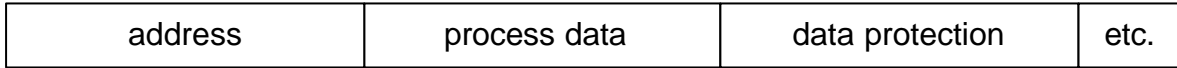


Figure 6: Definition of a message

The reaction time is defined as the time from electrical recognition of a safety demand to the actuators full operation to the safe state,.. With the reaction times given in table 7 a bus system can be a substantial component where reaction times are critical. The reaction time depends on the data transmission rate of the bus system and on the processing in the safety related controller.

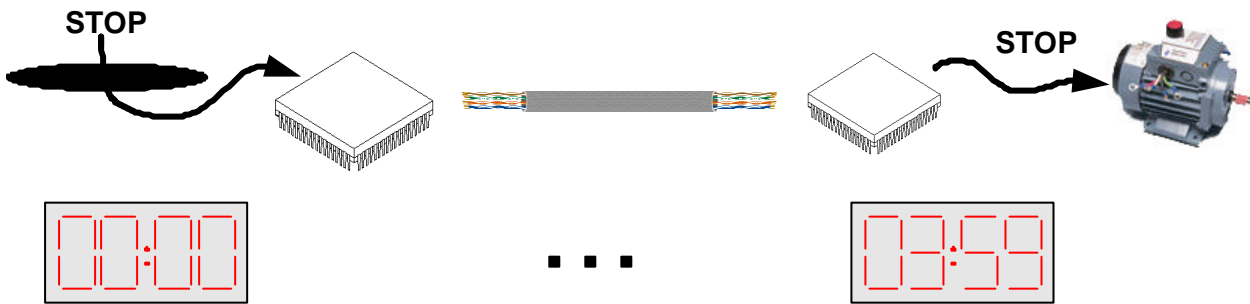


Figure 7: Definition of reaction time

Embedding of commercial bus systems into the total controller. As mentioned previously, it is not sufficient to simply replace conventional wiring by a commercial bus system. The bus system's safety controller must be capable of detecting failures, and ensuring correct data communication by plausibility checks. In this sense a safety-relevant controller is the control device for the medium, protocol circuits and the interface.

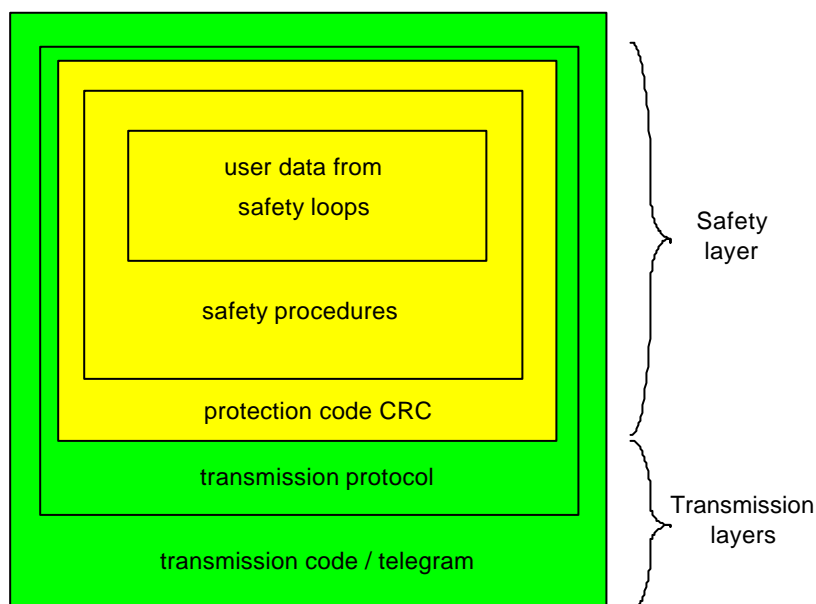


Figure 8: OSI-model for safety engineering

Figure 8 shows the OSI model for safety related communication. It shows the so-called safety layer is present in the safety application and not in the hardware of commercial bus system. First, the data is handed over to the safety interface, this layer adds additional data for authenticity and for data protection. Once in this packed condition the data will be transmitted to the lower non safety related transmission layer.

Statement in regards to the commercial bus system:

1. It makes no contribution to safety or contribution to necessary risk reduction.
2. The contribution is too small, thus it cannot be used without additional measures.

point 1.) It is important to note that the entire risk reduction by additional measures is to be realized in the safety controller. Therefore it is not necessary to use a complicated proof for the good quality of a commercial bus system that is supporting the risk reduction.

3.1.3 Transfer failures in bus system

As previously mentioned transmission failures can occur in any situation. Table 8 shows, the influences of different faults.

Causes of faults	Failures					
	Repetition	Loss	Insertion	Wrong sequence	Data falsification	Delay
Systematic error HW, SW	•	•	•	•	•	•
Crosstalk		•	•		•	
Cable break		•			•	•
Wrong aerial arrangement		•			•	
Cabling error		•	•		•	•
Accidental error	•	•	•	•	•	•
Aging	•		•	•	•	•
Use not calibrated instruments	•	•	•	•	•	•
Use of wrong HW	•	•	•	•	•	•
Insertion		•		•	•	•
Electromagnetic fields		•			•	
Human error	•	•	•	•	•	•
Temperature		•			•	
Magnetic storm		•			•	•
Fire		•			•	•
Earthquake		•			•	•
Flash		•			•	•

Net overcharge		•				•
Tapping	•	•	•	•	•	•
Destroyed HW		•			•	•
Unauthorized software changing	•	•	•	•	•	•
Transmission of unauthorized messages	•		•			

Table 8: Causes of transmission errors

The above list is not comprehensive however it demonstrates that the different influences (systematic failures, random hardware failures or environmental influences) can be classified into six categories. An exact examination of the various hardware and software errors shows that the errors always cause the same type of transmission failures in a bus system. With respect to data corruption, the address fields of the messages are also regarded as transmitted data.

Transmission errors are of great importance to safety-related systems. The first transmission error shown in table 8 is the repetition of a message which disturbs the receiver because an outdated message is repeated at the wrong time. Another transmission error is the deletion of a whole message due to an error. Furthermore an insertion may take place, in which a message is inserted due to an error. In a wrong sequence error, the chronological order of the messages is altered due to an error. The transmission error data corruption causes an unnoticed corruption of a message. The transmission error delay describes a message which is not transmitted within the required response time.

3.2 Qualitative control of faults

Several known methods can be used to combat the transmission errors mentioned in the previous section. These methods are the subject of the following section. Most of the methods used to combat transmission errors are already integrated into commercial bus systems. However these methods are normally implemented in very highly integrated and complex networks.

Malfunction/faults of these components cannot be detected with the required safety related reliability. The commercial protocol chips are not manufactured according to the requirements of the international standards for safety-related systems such as IEC 61508. The measures have to be comprehensively implemented, traceable, testable and fault-tolerant. On this basis they would normally have to be implemented inside the safety-related control system.

The following methods can be used to control transmission errors. One method is the sequence number. This number is contained in an additional data field of the message and is incremented from message to message in a defined way. Since the number of the next message is known by the receiver the number of an incoming message solely has to be compared to the expected sequence number. The transmission error's retransmission, loss, insertion and wrong sequence can be detected by this method.

Another method is to add time stamps to each message. A time stamp contains the time at which the sender creates a message for transmission. Using time stamps the transmission errors retransmission, wrong sequence and delay can be detected. Using the time expectation the receiver tests whether the time between

two messages exceeds a given limit. If the time limits were exceeded the receiver has to expect that an error has occurred and movements, which could lead to dangerous situations, have to be stopped. Time expectation can be used to detect the transmission error delay and is mandatory for every safety-related bus system since it is an equivalent to the quiescent current principle.

Another method is the acknowledgement of a transmission. After the successful reception of a message, the receiver sends an acknowledgement of the received message to the sender. Using an echo, the message can be repeated and the sender is able to check whether the message has been transmitted correctly. In this case, the transmission error's loss, insertion and data corruption can be detected.

Use of identification for sender and receiver is also possible. The sender and receiver identify each other by recognising a specified identifier added to the message. This method detects insertions into a message by a non-authorized sender. The method redundancy with cross-comparison assumes that sender and receiver have two communication channels. The received messages are compared for crossover and therefore test for correct transmission. Detected differences represent an error. Using this kind of redundancy in the hardware, the transmission errors retransmission, loss, insertion and wrong sequence are detected.

Data protection is a method in which the data content of a message is tested for correct transmission at the receiver. The data protection is usually inserted into the message and is performed to detect data corruption. Data protection contains for example cyclic redundancy check (CRC-check), hamming code and redundant data transmission.

The methods described above are summarised in a short form in table 9. To improve the efficiency of a bus system to a safety-related level, a mark has to appear in each row of the table. The methods have to be entirely implemented inside the safety-related processing units from sender to receiver. The methods have to be implemented according to the required SIL as defined in IEC 61508, provided that the time expectation method is always implemented. The protocol used for safety-related transmission via bus systems has to be modified accordingly.

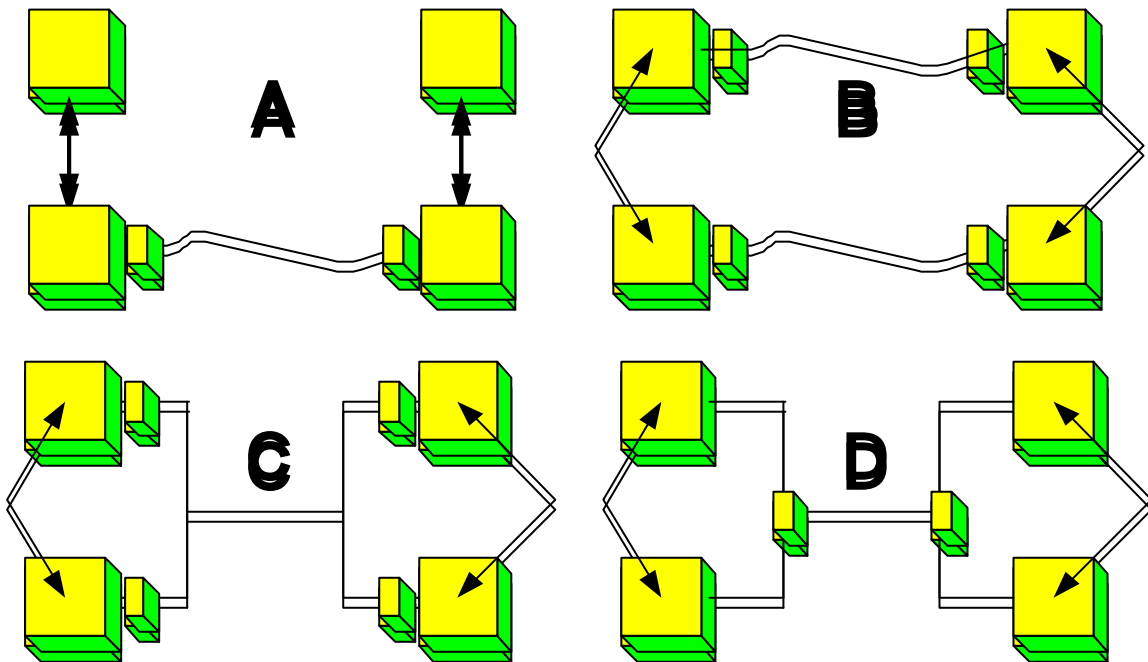
Errors	Measures per message							
	sequential number	Time marks	Time expectation	Receive-acknowledge	Recognition for transmitter and receiver	Data safety	Redundancy with cross comparison	Difference. of SI and NSI messages
Repeating	.	.					.	
Loss	.			.			.	
Insertion	
Wrong Sequence	.	.					.	
Data falsification				.		.	Only for serial busses	
Delay		.	.					
Coupling of SI- and NSI-messages				.	.			.
SI: Safety related NSI: Not safety related								

Table 9: Methods for control of faults

3.3 Quantitative measures against transmission errors

In the preceding section the requirements were qualitatively described for the safety bus system. There is at least one method that must be used in safe technology for each transfer error type. However each mechanism mentioned theoretically increases the so-called data integrity. With some mathematics it can be shown, that the quantitative calculation of the data, integrity depends on the relevant structure.

Four structure models are pointed out for the bus connection. These models vary depending their fault tolerance. The bus participants are normally designed compliant to SIL 2 and SIL 3 (IEC 61508), in a suitable redundant system configuration.



3.3.1 Architecture of bus systems for safety technology

Figure 9: Architectures of bus-systems for safety technology

The bus connection node is present with Model A only at a single channel of the controller. The second channel of this model can transmit only over the other channel messages. Link layers (ISO/OSI model) can be present in one channel or in each channel. The transport layer is only single.

Model B describes a completely redundant system, in which safeguard and transmission layers are designed in a dual configuration. At first sight this model appears too complex for a new installation, however for existing installations it represents a possible solution. Particularly large machines and manufacturing plants generally contain several bus systems, which may be used under certain circumstances for the safety communication.

Model C is similar to Model B, however it has only a single-channel transmission medium. Apart from the transmission medium safeguarding and transmission layers are present in both channels.

Model D has two-canal link layers, which can only access the transmission layer only via a single-channel transmission layer. Data can be sent either in one or in two telegrams.

3.3.2 Data integrity

For the qualitative estimation of the data protection standard IEC 61508 can be applied. Although this standard makes neither qualitative nor quantitative prerequisites for the evaluation of transmission errors, it is applicable because of the requirement associated with the probability of hardware failure. In a safety-related controller a random hardware fault leads finally to a random failure, which is identified as a transmission error. If one regards transmission errors similar to the random hardware faults, the probabilities of failures on demand in IEC 61508 can be applied to these errors. The requirements indicated at the beginning of the chapter require a universal safety system that has a continuous or high demand mode of operation. Table 2 from the previous chapter shows the mode of operation values according the IEC 61508.

As already mentioned in the previous chapter, IEC 61508 considers probability of failure of the complete hardware / system according to a quantitative model. A similar model has to be set up for transmission errors, so that the probability of a fail to danger system fault of the system can be calculated. Methods for bus systems are very complex, thus some assumptions are made, which guarantee that a bus system supplies only a contribution of 1 % to the failure of the safety function. Deviating from this 1 % is possible, since it concerns only an approximate value. Such deviating is possible, if a complete quantification of a controller including the transmission is required. Qualitative measures for fault control from one of the previous sections contribute to the decrease of the probability of failure.

Using the appropriate bus architecture and data protection mechanisms method is a good quantification approach. In the following bus architecture, different methods for calculation are described. These have a failure rate Λ (lambda) as initial value. The failure rate is the number of the safety relevant transmission errors per hour. All models use the approach of Gauss, with a focus on normal distributed probabilities of bit error and white noise. During transmission of information thus the probability that a false bit, is distributed is generally called bit error probability p.

A worst case scenario is the approach with longer messages. Table 10 shows examples of the bit error probability p. This shows that p influences failure rate of the bus system. Without proof of bit error probability the calculation has to be based on the worst value $p = 10^{-2}$.

Probability of bit failures p	Transmission medium
$>10^{-3}$	Transmission path
10^{-4}	Unscreened data line
10^{-5}	Screened twisted-pair telephone circuit
$10^{-6} - 10^{-7}$	Digital telephone circuit (ISDN)
10^{-9}	Coaxial cable in local defined application

10^{-12}	Fibre optic cable
------------	-------------------

Table 10: Examples of probabilities of bit failures depending of the transmission medium

Initially a safety relevant information message with only one bit is considered. The bus system is considered after that, still without backup processing. Simple redundancy does not promise always success. If the signal is transferred over unscreened twisted-pair cable, i. e. the bit error probability is 10^{-4} and the data transmission rate lies at $v = 100/s$. Thus the rate of transfer errors without redundancy amounts to:

$$U = p \cdot v = 10^{-2} / s \quad (1)$$

This means that one transmission error occurs approximately every 100 seconds. Assuming independence of probabilities, the probability of two corrupted bits (redundancy) is given by $p = 10^{-8}$. In this case the amount of transmission errors at unchanged $v = 100/s$ is:

$$U_{red} = p' \cdot v = 10^{-6} / s \quad (2)$$

Computing the reciprocal one transmission error can occur each 11.6 days, which is certainly intolerable. Should this be the case more methods for reduction of the single bit error probability are necessary.

The integrity of a message not only depends on the single bit error probability but also the possibility of corruption of a whole message, as a result the residual error probability is important. This error probability is the summation of the single bit error probabilities, which also depends on the summation of regarded single bit errors.

The residual error probability is:

$$R(p) = \sum_{e=d}^n A_{n,e} p^e (1-p)^{(n-e)} \quad (3)$$

with the binomial coefficient:

$$A_{n,e} = \binom{n}{e} = \frac{n!}{e!(n-e)!} \quad (4)$$

where 'n' is the message length, 'p' is single bit error probability and 'd' the hamming distance of the data protection method implemented in the controller. When no data protection methods are implemented, d is set to 1. A better data protection method results from a higher value for d.

3.3.3 Methods for calculating the residual error probability

Initially the data protection for the models A and D is considered, with the backup processing of the transmission layer not being considered. This is a 'non safe' commercial bus system. Thus data protection

must be implemented in the safety related controller. The remaining error rate \ddot{E} results from the residual error probability $R(p)$ of the supervising safeguarding processor, the data transmission rate n of the safety-relevant messages and the 1 %-rule. Beyond that the number 'm' of participants in a safety function must be also considered. Bus systems are freely configurable and thus the maximum extent of participants on the safety bus system must be assumed. With 'm' participants $m-1$ messages will be transferred.

The rate normalized for one hour results in the equation below:

$$\Lambda(R, V, m, p) = 3600 \cdot R(p) \cdot v \cdot 100 \cdot (m - 1) \quad (5)$$

The calculated value can be compared now with table 2. Afterwards the parameters \ddot{E} and $R(p)$ must be varied depending upon required SIL.

Now the data protection for the models B and C is to be considered. It should be noted that the individual channel of the transmission layers is not regarded as being safety related. Thus the qualitative requirement of the two-channel hardware related to the bus nodes with the combined quantitative computation of \ddot{E} needs to be regarded. The individual transmission layer is not regarded as safe. However the combination of redundant bus nodes with cross-wise comparison of the messages in the safety application is regarded as sufficient measure against coincidental hardware errors in the bus protocol device. Therefore in this model the data protection of the commercial bus system is utilised fully. Should only one node the data protection mechanism fail, the flagging of the error is only possible over one comparator. This is not sufficient to fulfil the requirements of the category 4 of EN 954-1. For the requirements of the category 3 it is sufficient. Bus systems like CAN bus guarantee integrity because of their structure where each message is verified in separate hardware.

The consequence of redundant bus nodes is redundant transmission of messages. All messages are thus transmitted twice and examined over the comparator. It is possible to say, that transmission fails only when the redundant message has the same errors. The probability of message falsification on the bus system is given by the residual error probability R_{KOM} .

The disturbance of both messages can be regarded as random, so that the residual error probability of the redundant system $R_{red}(p)$ is given by:

$$R_{red}(p) = R^2 \quad (6)$$

The parameter 'R' is used for the representation of the single probabilities. With this, the calculation of Λ is possible and with variation of parameters 'v' and 'm', the required SIL can be achieved.

Next the data protection for the models A and D is described, in this model the bus system has a portion of safety, which applies for example to field bus systems. Normally field busses are different to sensor-actuator-busses which have applications on the system level. These require larger arithmetic performances or shorter response times, whereby the amount of data is constant. Bus protocol devices are very expensive. Thus bus nodes often realized as single-channel. Unfortunately the method of calculating this is complicated. IEC 61508 uses Markov-Models for calculation. A condition for this is that it requires a reliable commercial bus system, so that additional expenditure is not required. Based on the transmission quality of the commercial bus system, the requirement for reaching a certain category or a SIL must be realized in the safety controller. For the protocol devices proof evaluations have to be available and/or the hardware reliability \ddot{e} of the protocol device is to be included into the calculation.

Depending on IEC 62280 (EN 50159-1) the Markov analysis of this model can be attributed to three substantial transition probabilities.

The protocol device can be caused to fail in three different ways, see figure 10. Transmission hardware can fail, so that one message or several messages are falsified. Additionally bit errors can occur because of electromagnetic influences (EMI), which are not recognized by the data communication equipment. Finally each message may be passed from the data communication equipment on to the safety system, because only bus-checker failed. From table 2 one can select at the required SIL an appropriate target value for Λ , Λ_{target} . The calculated error rate results from the individual transitions $\Lambda_{HW}, \Lambda_{EMI}, \Lambda_{TC}$ in this simplified Markov model, which is shown in figure 10. The result is the remaining error rate with the 1 %-rule is :

$$\Lambda_{SYS} = \Lambda_{HW} + \Lambda_{EMI} + \Lambda_{TC} < \frac{\Lambda_{target}}{100} \quad (7)$$

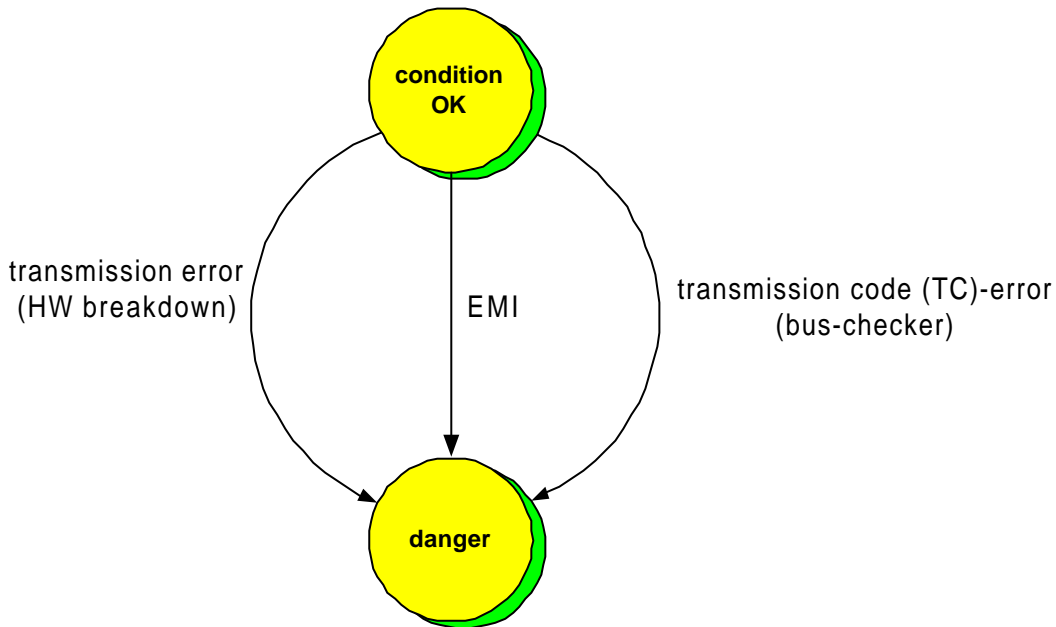


Figure 10: Markov-Model for single-channel bus nodes and additional supervising data integrity

Λ_{HW} corresponds to the rate of the hardware faults, which are caused by hardware failures in the transmission layer, hence a message is falsified. Failures can only be detected by any still functional data protection mechanisms in the safe application. In this case the maximum error probability R_{US} , which depends on the bit error probability, of these mechanisms must be known. Therefore Λ_{HW} consists of either of the probability that the hardware of the bus protocol components fails and / or of the residual error probability of the safety transmission mechanism in the safety application. Λ_{HW} calculates itself as follows:

$$\Lambda_{HW} = \mathbf{I}_{HW} \cdot R_{US} \quad (8)$$

\mathbf{I}_{HW} is thereby the sum of all failure rates of the bus protocol components of the safety-relevant participants per hour. In this model per IEC 61508 a direct linear connection between \mathbf{I}_{HW} and the average actual working time up to the failure (MTTF = Mean Time To Failures) can be established.

$$\mathbf{I}_{HW} = 1/\text{MTTF} \quad (9)$$

An improvement of Λ_{HW} can be achieved, if \mathbf{I}_{HW} is accurately defined. This is done by distinguishing between the actual communication partners and any other bus participants. This fraction varies because of the different mechanisms in components involved and uninvolved. The mechanism of an inaccurate assumption of hardware errors within the equipment involved (x1). Another is the destruction of a message by indifferent components (x2). Thus the fractions x1 and x2 of the dangerous failures differ. x1 can be estimated by a failure mode and effect analysis (FMEA). The following formulae applies :

$$\Lambda_{HW} = (x_1 \cdot \mathbf{I}_{HWF} + x_2 \cdot \mathbf{I}_{HWS}) \cdot R_{US} \quad (10)$$

\mathbf{I}_{HWF} stands for the hardware probability of failure of the two actual communicating safety-relevant participants, \mathbf{I}_{HWS} for the hardware probability of failure maximum x the actual not communicating safety-relevant participant. x1 stands for the portion of the dangerous errors by the components uninvolved, x2 for the portion of the dangerous errors by the indifferent components. x1 and x2 are in the range between 0 and 100 %. R_{US} is the maximum residual error probability for the safety measures in the application.

Transient transmission errors by external influences such as EMI are detailed in figure 10. It is assumed that bus protocol component and the additional data protection mechanisms in the application operate correctly. Thus the residual error probability of commercial protocols and the residual error probability of the additional data protection mechanism are to be considered. These two probabilities can be multiplied with each other only if they are independent. Thus the data protection mechanisms of the bus and of the safe application must be independent from each other and must be proven approximately by simulation or consideration of the mathematical limit value. A further parameter is the frequency f_w , with which messages on a bus system are disturbed. The following formulae is relevant to EMI :

$$\Lambda_{EMI} = f_w \cdot R_{UB} \cdot R_{US} \quad (11)$$

R_{UB} designates the residual error probability of the commercial bus system and R_{US} the maximum residual error probability of the data protection in the safe application.

Hardware faults of standard data safeguarding mechanisms in the bus protocol component are detailed in figure 10. Under this condition the bus checker will work as the only error detection. Since this last specified mechanism is independent, the probability rises that it may be confronted with incorrect messages. There is either a probability that messages arrive falsified at the safe application or the error is recognized in the safety controller. In case of failure of the bus checker the frequency such detected errors will increase. This can be determined for example by permanent measurement utilising counters and timer. If the frequency of detected errors, with which the functional standard data safeguard mechanism is available and failures of the

bus checker are recognized, a rise can be determined and after a certain time T the system can be brought into the safe state. R_{HW} considers already general hardware faults. It is assumed that the bus protocol component is still able to send and receive but the data protection is defective. It is only realistic to allocate a small fraction k to the hardware faults. Thus the formulae for the critical failure of standard protocols is as follows:

$$\Lambda_{TC} = R_{UB} \cdot \frac{k}{T} \quad (12)$$

k is the relationship of the hardware faults of the standard data safeguard mechanism to the entire hardware faults of the bus protocol component and should be set in the case of doubt to 1. T is the time interval, in which a well-defined maximum number of falsified messages on the transmission system may not be exceeded, without the safe guarding layer introducing a safe condition.

3.4 External influences

Of course, as well as all safety-related controllers, bus systems have to withstand the expected operating and environmental demands. Less emphasis is required by safety systems for the maintaining operation (high availability). The principal purpose is that a safety-relevant controller never fails to danger under the influence of usual disturbances and environmental conditions.

Criteria are specified for environmental checks, which demand a fixed behaviour of a bus system under disturbances (vibration, EMC). The minimum criteria are detailed in table 11. It is advised that safety related bus systems are only installed within the specified environment. Also the existing relevant standards are to be observed.

Performance criteria	Description
A	The bus system must work intended during and after the disturbing influence.
B	The bus system must work after the disturbing influence intended. With exceeding of the time Out time because of disturbing influence the safety-relevant participants must introduce the safe condition. Restarting is to be realized application-dependently automatic or by explicit release. Bus communication is automatically again taken up after disturbing influence.
C	The safety related introduce participant the safe condition. Communication failed. All safety-relevant participants remain in the safe condition. The re-establishment of the correct enterprise takes place via setters.

Table 11: Environmental demands performance criteria for the behaviour of safety related bus systems

Literature

- [1] DIN V VDE 0801: Principles for computers in safety-related systems, with appendix A1. Beuth Verlag Berlin 1990 and 1994.
- [2] EN 954-1: 1997-03; Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Beuth Verlag Berlin 1997.
- [3] EN 999: 1998-12; Safety of machinery – The positioning of protective equipment in respect of approach speed of parts of the human body. Beuth Verlag Berlin 1998.
- [4] EN 1050: 1997-01; Safety of machinery – Principles for risk assessment. Beuth Verlag Berlin 1997.
- [5] EN 50159-1: Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems“. Beuth Verlag Berlin 2001.
- [6] IEC 61000-6-2: Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments. VDE Verlag 1999.
- [7] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 – 7. IEC Verlag Genf 1999.
- [8] Börcsök, J.: Netzwerke im industriellen Einsatz. Grundlagen, Konzepte, Protokolle. VDE-Verlag 2002.
- [9] Börcsök, J.: Internationale-/Europa Norm 61508, Vortrag bei der VD-Tagung der HIMA GmbH + Co KG, 2002
- [10] Börcsök, J.: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen, 2002
- [11] Börcsök, J.: Sicherheits-Rechnerarchitekturen Teil 1 und 2, Vorlesung Universität Kassel 2000/2001
- [12] Börcsök, J.: Echtzeit-Betriebssysteme für sicherheitsgerichtete Realzeitrechner, Vorlesung Universität Kassel 2001/2002
- [13] Gerdson, P.: Digitale Übertragungstechnik. Teubner-Verlag 1983.
- [14] Kriesel, W.; Heimbold, T.; Telschow, D.: Bustechnologien für die Automation-Vernetzung, Auswahl und Anwendung von Kommunikationssystemen. 2. Aufl. Hüthig Verlag Heidelberg 2000.
- [15] Phoenix Contact (Hrsg.): Grundkurs Sensor-Aktor-Feldbustechnik. Vogel-Verlag Würzburg 1997.
- [16] Reinert, D.; Schaefer, M.: Sichere Bussysteme für die Automation. Hüthig Verlag Heidelberg 2000.
- [17] Schnell, G. Bussysteme in der Automatisierungstechnik. 3. Aufl. Vieweg-Verlag 1999.
- [18] Vorschlag eines Grundsatzes für die Prüfung und Zertifizierung von „Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten“, Stand 28.05.2000. Erhältlich bei Berufsgenossenschaft für Feinmechanik und Elektrotechnik, 50962 Köln.

Prof. Dr.-Ing. Josef Börcsök is Executive Vice President of Research + Development at HIMA GmbH + Co KG Industrie-Automatisierung. He has been working for many years in the field of safety related technology. He is member in different Institution of DKE. At universities he holds lectures in computer science, network techniques and safety computer architectures.

Address: HIMA GmbH + Co KG, Albert-Bassermann-Str. 28, D-68782 Brühl near Mannheim, Tel. (0049-6202) 709-270, E-Mail: j.boercsoek@hima.com