Introduction in safety bus systems

PROF. DR.-ING. HABIL. JOSEF BÖRCSÖK
HIMA Paul Hildebrandt GmbH + Co KG
68782 Brühl, Albert-Bassermann-Str. 28
GERMANY
j.boercsoek@hima.com

Abstract: - Modern distributed control systems are connected via bus systems, and need effective and uninterrupted communication between all bus stations. Therefore it is necessary that these communications are fault tolerant and safe. Especially for safety related systems additional safety layers are required to fulfil these requirements. In a safety related application it is important to understand that the safe protocol cannot alone fulfil this requirement without two safe hardware ends (source node and destination node). Only the conjunction between safety related protocol and safety related hardware nodes can fulfil the requirements for safety related bus systems.

Key-Words: - Protocol, Safety, Safety-bus, Functional-safety

1 Basics of functional safety

1.1 Fundamental considerations

At safety related devices, which are controlled by a microprocessor, random component faults are often not the cause for a failure. Rather there are special conditions during the operation, which the programmer had not considered. A further possibility of errors is caused by the system maintenance, since effects of changes are not directly apparent in the program.

Thus it can be determined that in applications, which are based on a microprocessor, errors in the development phase are made, which can lead much later in the operation phase to a dangerous situation. For this reason measures must be taken against such errors in the development phase of a safety device.

The standards DIN V VDE 0801 and IEC 61508 differentiate therefore on one hand measures for fault avoidance and on the other hand measures for fault control. The first measure will be taken by the manufacturer and a test organisation (TÜV) in the course of the planning phase, development-, installation and change process, so that these errors are not made at all, or can be detected and corrected during the process. The measures for fault control included hardware and software modules. These detect arising errors during the operation and cause as result appropriate safety-related reactions of the computer system.

1.2 Measure combinations for fault avoidance

Particularly in complex systems thus errors can only be fought effectively, if procedures in the design, development and maintenance phase are structured. The aim is to avoid errors from the very beginning. Such a strategy is carried out by a whole number of constructive, analytic and testing measures along the safety life cycle.

In the standard IEC 61508 the respective phases of the safety life cycle are described by fundamental requirements for each phase. The parts 2 and 3 of the IEC 61508 contain details for the implementation of electrical, electronic and programmable electronic (PES) systems.

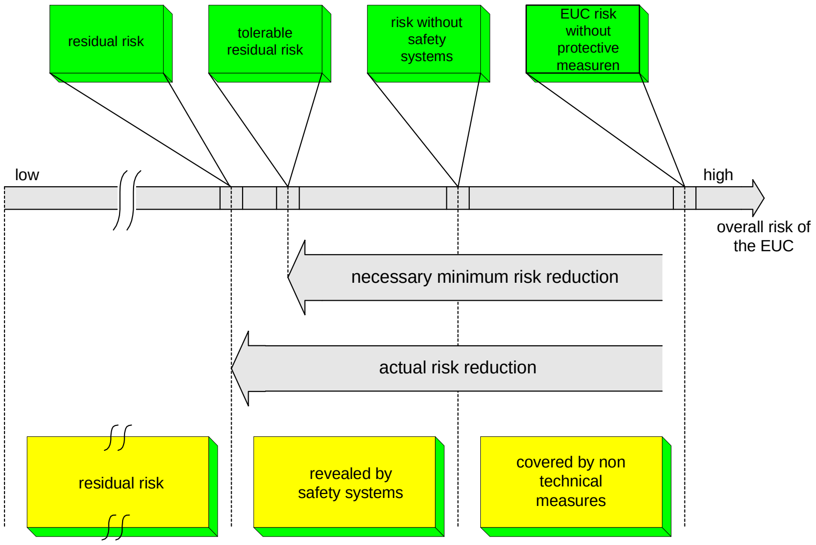
residual risk
tolerable residual risk
risk without safety systems
EUC risk without protective measuren
low
high
overall risk of the EUC
necessary minimum risk reduction
actual risk reduction
residual risk
revealed by safety systems
covered by non technical measures

Fig. 1: Minimizing the risk by technical equipments

Thereby concrete measures are assigned to each phase for the realization of a complex safety device for fault avoidance. These measures are contained in the annex A and B of the parts 2 and 3, scaled according to their effectiveness, and described in detail in part 7. The basic idea of the safety life cycle is based on the fact that particularly in complex systems, the functional safety can be ensured only parallel to the development over the entire life cycle of the system. German test institutes e. g. the Technischer Überwachungsverein (TÜV) take at certification of computer controlled systems already for a long time this path. An acceptance by such a test institute begins with the so-called development-accompanying examination in the product requirement specifications phase, that is already a very early phase. The examination accompanies the development, the operation as well as the modification and maintenance of the system. The safety-referred reliability of complex safety systems can be only ensured, if constructional, analytic and testing measures are combined.

The measures vary in their expenditure thereby depending upon the minimizing of the risk, which can be ensured by the safety function.

Fig. 1 shows the concept of the risk reduction by technical equipments. The required safety level is achieved by suitable measures whether technical or not technical, the risk of a hazardous machine or respectively a plant is reduced to an acceptable residual risk. If that is the case, then this machine or plant is considered as safe. But the question arises how is this acceptable residual risk defined. In Germany it is generally accepted, that the tolerable residual risk can be not absolutely specified. The necessary risk reduction of technical equipments can only be determined based on analogy by arguments from the past. That means, that the expense for the risk reduction of a plant or a machine with cyclic human access, in which for example irreversible injuries can occur as for instance the loss of a hand or similar, there is a very substantial expense for fault avoidance and fault control to be done.

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

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

A dimension for the risk reduction represents the so-called Safety Integrity Level (SIL) to the standard IEC 61508. This SIL can be compared at least for the fault avoiding measures with the categories of the EN 954, part of 1 and the requirement classes (AK) of the DIN V VDE 0801 and DIN V 19521, which is to be seen in Table 1.

1.3 Measure combinations for fault control

A comparison of the three above schemata of categorization of the risk reduction is for the named measures for control of faults not to be achieved by fixed correlation. In all standards for functional safety it can be read, that the safety-relevant reliability of a complex system can be achieved by building up redundancy as well as technical or nontechnical measures for fault detection of the safety system’s subsystems. However, it is not sufficient, to develop a complex system, which is 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. The control of faults means in this context, that based on redundancy it either does not lead to the failure of the safety equipment or it is diagnosed so early that the safety equipment can be repaired. A further important factor for the evaluation of a safety system is, apart from redundancy and fault detection, the reliability of the component.

This 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, what is to be seen in Table 2.

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

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

In the former national and in the European standards necessary risk reduction is not quantified. They specify structures and the effectiveness of fault detection mechanism, so that the risk reduction of technical equipments can be classified. 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 coherence can only be established if the relevant structures are described more precise and the single-channel subsystems have assigned failure rates. Prerequisites for the relevant system structures:
General prerequisites:

- The switch-off of the drive causes the machine in to the safe state.
- The safety system itself does not initiate a dangerous/hazardous situation. In 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.

Examples self-test with an estimation of the effectiveness can be found in the appendix A of IEC 61508, part 2. The effectiveness of a test results from the kind of the failures that are detected by the test.
Besides the described measures to control random faults the national and international standards describe measures for the control of systematic failures. These effect supplementary to the measures at faults 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.

1.4 Consequences for the design of safety related communication systems

For the introduction of complex systems to the safety technology particularly experiences are necessary during the entire life cycle of this complex product. Safe communication systems are as well complex systems as the transmitters and receivers of safety-relevant information.

Therefore the design of safe communication system prerequisites the necessary measures for risk reduction of the fault avoidance and fault control. However safe communication over a bus alone does not ensure that the transferred safety-relevant function is also safe. The information must be produced safely and processed safely. It is nevertheless possible by the development of safe complex electronic systems to include bus systems into the safety system. This requires however further qualitative and quantitative requirements, which are described more exactly in the following sections.

2 Fundamental requirements of bus systems for the safety systems

2.1 Functional requirements of the process

There are branches in the process industry, in which requirements in the range of the machinery and plants are partly far beyond basic requirements of the process control. This is mainly caused of fast processes in the machinery.
Within the range of metalworking like the automobile production, manually fed presses are used with press controllers, which control via a light curtain, depending from the users action, the workflow. The press bear, which presses the raw material into the form, reverses at interference into the press, and protects the user against heavy harm or even from death. A control, which protects the user against dangerous situations, has to fulfil relatively small response times within the range of 10 milliseconds.

Thus to the fast machinery process the speed is to be added with which a person can intervene in the hazardous area. The protection fields of light curtains and laser-scanners or also ESPE (Electro Sensitive Protective Equipment), must be dimensioned with consideration of these two dynamics of machine and user with certain additional safety margins. In the standard EN 999 [1] guidelines for such protection fields are set up, response time of a ESPE is to be calculated directly proportionally, i. e. is the response time high, it forces the light curtains installed farther away from the dangerous area. The demand rate of the protection device depends for example on the possible failure of the machine, as well as the frequency that can be expected, such a dangerous situation occurs.

The mode of operation of a hazardous system is operated in accordance in the IEC 61508 in high demand mode. Other branches differ in the instrumentation of the control system, a functional control system is superseded by a safety control system. This monitoring PES is usually used 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 as well applies 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.

It remains stated that the demand rate to a safety system is generally high and the response times are by 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 limitations.

The statements made so far basically concern controllers and their bus systems within the range of the sensor and actuator. At complex machines the transmission of large data amounts plays an important role: for example at machine tools safety relevant parameters must be transferred to the processing safety system. Besides it is possible to exchange complete or parts of application programs via bus systems.

With transmissions of middle to large messages it is conceivable to manage an adjustment of the sensor technology on a certain machine situation, i. e. the position of a robot arm has influence on the sensor for person detection. So you can imagine in the future that the protection fields of laser scanner can be reconfigured without interruption of the workflow in few 100 milliseconds with high dynamics. Due to the large messages, this transferring means a high demand to the bus system. A controller inclusive safety related bus system, which is universal applicable, is an important economic aspect, which must be designed for the respective application. Table 3 shows the requirements to a desirable universal system:

Table 3: Overview about the requirements of process to bus systems

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 an application dependent risk evaluation with consideration of the appropriate standards.			

2.2 Qualitative measures against transfer failures

2.2.1 General

Fig. 2 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 (IC), which converts parallel or serial incoming messages into a serial, bus-specific transmission protocol on a two-wire line.

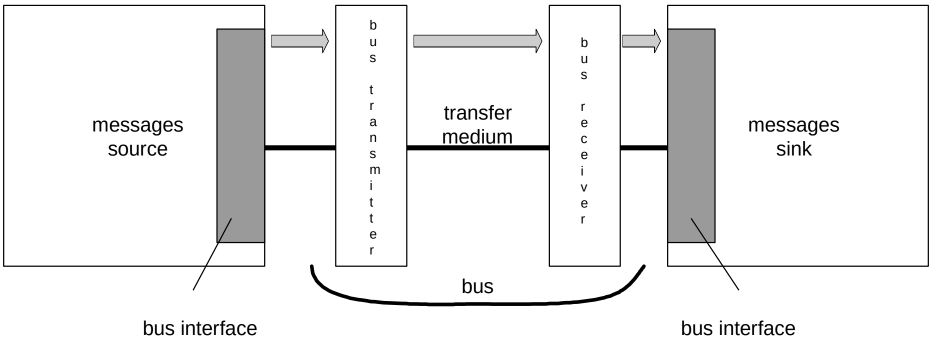

Fig. 2: Schematic of a simple bus system

The protocol receiver component converts the detailed incoming messages for the information sink into a useful signal. The bus system is formed out of the 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.

A conventional wiring cannot be replaced by a simply commercial bus system, without realizing certain failure detection measures. It will probably function physically, however the necessary and required measure of risk reduction is not reached. The reasons supply the following arguments:

- The interface between bus protocol controller and processing unit of the controller are in the case of a failure not automatically safe against short-circuit, interruption etc.
- While the timing behaviour of conventional wiring is usually sufficiently fast, in serial bus systems it can come to delays.
- The addressing of the participants is fixed with conventional wiring by the electrical structure and/or connection diagram. Bus systems are able to bring flexibility inside the system, with the assistance of protocol components, however this brings in potential of faults.
- A bus can be regarded due to different characteristics as a storage medium of information. During an incorrect transmission the system is able to send the data repeatedly to the receiver. This functionality can stress a certain time, which causes a potential danger in the safety communication, because for example process data can have already lost their 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 it is impossible to interfere between non safety-relevant and safety-relevant parts in the precondition by a correct wiring. With open bus systems however both control parts (safety related and non safety related systems) and additional merged participants have 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 against to a signal distortion. With bus systems however there are electromagnetic disturbances, which have an influence on the signals.

These above not completely listed problems of bus systems, can be controlled by measures in the bus or using commercial bus systems in the processing unit of the safety related participants. Thus a functional safety level is reached in combination with increasing of the flexibility and the efficiency.

2.2.2 Variety of terms

This section deals with terms, which are used by many specialists within the range of the bus systems as synonymous. In particular terms, as for example telegram, protocol, message, information or frameworks, into its sense are completely different interpreted. For this reason the most important terms, which are used again and again, are briefly described.

2.2.3 Definition of message and reaction time

A message consists of the transferred process data (the actual information) and the address (the information, to which sink the message should be send). The process data and the addresses are combined into the data of the message. Thus with the consistency check of a message the data and also the addressing with is checked.

A further check is concerned with that correct receiving of the data; this is information for data protection, which contains a checksum of the message. Mostly used is the CRC check, which calculates via a mathematical algorithm a checksum over the complete message. This checksum can be calculated by the receiver from the message data and be compared with the sent checksum.

address	process data	data protection	etc.

Fig. 3: Definition of a message

The reaction time is defined as the time starting at the electrical recognition of a safety relevant demand up to the execution on the actuators, which initiate the safe state (regarding the electrical side). In Table 3 the reaction times are listed, there is a substantial characteristic for the application of a bus system in a special application. The reaction time depends on the data transmission rate of the bus system and on the processing in the safety related controller.

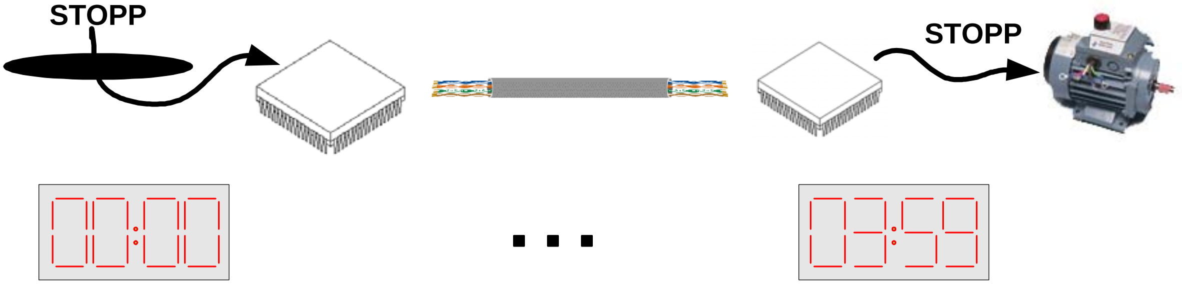

Fig. 4: Definition of reaction time

2.2.4 Embedding of commercial bus systems into the total controller

How already mentioned previously, it is not sufficient to replace simply a conventional wiring by a commercial bus system. The bus system’s safety controller must be able to detect failures, and ensure by plausibility checks a correct data communication. In this sense is a safety-relevant controller, the control device for the medium, the protocol circuits and the bus interface.

Fig. 5 shows an OSI model for the safety related communication, the so-called safety layer, which is not present in the hardware commercial bus system, but in the safety application.

First, the data are handed over to the safety interface, this layer add further data to authenticity and for data protection. In this packed condition the data will transmitted to the lower not safety related transmission layer.

Statement to the commercial bus system:

1. It makes no contribution to safety or no contribution to necessary risk reduction.
2. The contribution is too small, so that one cannot use it without additional measures.

To point 1.)

It is to mention that the entire risk reduction by additional measures is to be realized in the safety controller. Thus the complicated proof is saved, how good the quality of a commercial bus system supports to risk reduction.

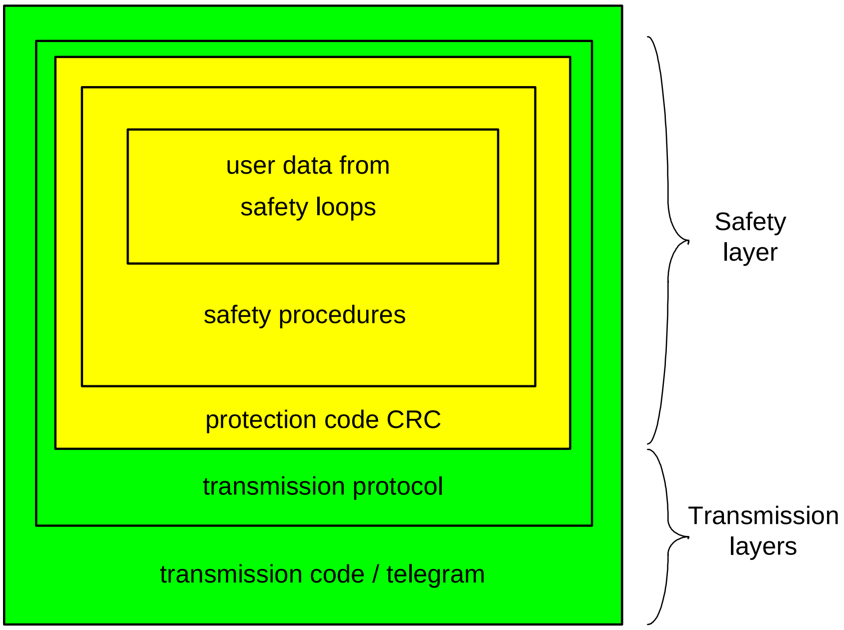

Fig. 5: OSI-model for safety engineering

2.2.5 Transfer failures in bus system

As previously mentioned transmission failures can occur in any situation.

Table 4 shows, the influences of different faults to the transmission.

Surely the list of influences is incomplete, but it demonstrates impressively, that the different influences (systematic failures, random hardware failures or environmental influences) have to only six communication faults to be considered.

An exact examination of the various hardware and software errors shows, that the errors always cause the same small amount of transmission errors of bus systems. It has to be mentioned, that in respect of data corruption of the address fields in the messages are regarded as transmitted data.

Transmission errors are of great importance in safety-related systems. The first transmission error shown in

Table 4 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 loss of a whole message due to an error, which causes deletion of the message.

Furthermore the 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.

2.3 Qualitative control of faults

Several methods are known which can be used against the transmission errors mentioned in the previous section. These methods are subject of the following section. The proper methods against transmission errors are often already integrated in commercial bus systems in one or the other way. But these methods are solely implemented in very highly integrated complex integrated circuit. Malfunction / faults of these components cannot be detected with the required reliability. Today, these commercial protocol chips are not manufactured according to the requirements of the international standards for safety-related systems like IEC 61508. The measures have to be implemented comprehensible traceable, testable and fault-tolerant, which means that they normally have to be implemented inside the safety-related control system as mentioned in section 2.2.4.

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 errors retransmission, loss, insertion and wrong sequence can be detected by this method.

Table 4: Causes of transmission errors

	Failures					
Causes of failures	**Repetition**	**Loss**	**Insertion**	**Wrong sequences**	**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	•		•			

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. In this case, 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 successful reception of a message, the receiver sends an acknowledgement for 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 errors loss, insertion and data corruption can be detected. Usage of identification for sender and receiver is also possible. The sender and receiver identify each other by recognizing 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 crossover and in that way tested for correct transmission. Detected differences represent an error. By 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 in 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 summarized in a short form in Table 5. 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 according to 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.

Table 5: Causes of transmission errors

	Measures per message							
Errors	**Sequential number**	**Time marks**	**Time expectation**	**Receive-acknowledge-ment**	**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								

2.4 Quantitative measures against transmission errors

In the preceding section the requirements were qualitatively described to the safety bus system. There is at least one measure against each transfer error, which must be realized in safe technology. Using the quantitative approach of the error controlling measures specified above a key feature is the data protection, since it represents a widespread tool in the information technology to detect errors. However each mechanism mentioned at least theoretically can increase the so-called data integrity. At some (mathematical) expenditure 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 partly vary regarding their fault tolerance. For improvement information sources and information sinks the appropriate standard the IEC 61508 is to be used. The bus participants are normally designed compliant to SIL 2 and SIL 3 (IEC 61508), in a suitable redundant system configuration.

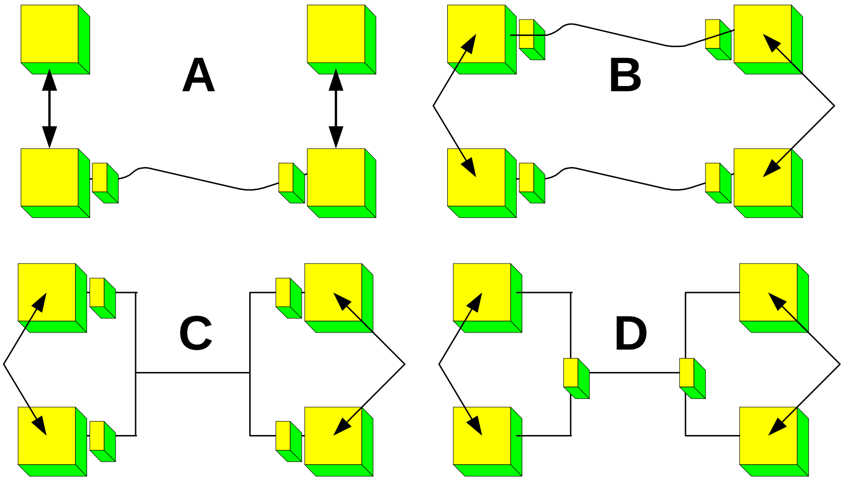

Fig. 6: Architectures of bus-systems for safety technology

2.4.1 Architecture models for the bus binding

The node for bus connection is present with Model A only at a single channel of the controller. The second channel of this model can send 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.

In model B it describes a completely redundant system, in which safeguard and transmission layers are designed dual. At first sight this model appears too complex in a new installation, in existing machine concepts however it represents quite a possible way. Particularly large machines and manufacturing plants already often contain several bus systems, which can be used under certain circumstances for the safety communication.

Model C essentially corresponds to Model B, has however only a single-channel transmission medium. Safeguard and transmission layers are, apart from the transmission medium, present in both channels.

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

2.4.2 Data integrity

For the qualitative estimation from safety relevant procedures of the data protection in the following the standard IEC 61508 is applied. Although this standard makes neither qualitative nor quantitative prerequisites for the evaluation of transmission errors, it is applicable because of the requirement to the probability of failure by the hardware. In a safety-related controller a random hardware fault leads finally to a random failure, which can be transmitted also to a transmission error.

If one regards transmission errors similar to the random hardware faults, the probabilities of failures on demanded in the IEC 61508 can be applied to the transmission errors. The requirements indicated at the beginning of the chapter require among other things for a universal safety system that the mode of operation in continuous or high demand mode. Table 2 from the previous chapter shows the values for this mode of operation according the IEC 61508.

As already mentions in the previous chapter, the IEC 61508 regards the probability of failure of the complete hardware / system according to a quantitative model. A similar model has to be set up now for transmission errors, so that the probability of a dangerous fault of the system can be calculated. Methods for bus systems are partially very complex, so that some prerequisites 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 here. Such deviating is possible, if a complete quantification of a controller is possible including transmission system. The 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 the data protection mechanisms approach turned out to be a good for quantification. In the following as a function of the bus architecture, different methods for calculation are described, which have the 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, who is concerned with normal distributed probabilities of bit error and white noise. During the transmission of information thus the probability, that a bit is falsified, is normal distributed, which is generally called bit error probability *p*.

The approach with longer messages is to be regarded as worst case. Table 6 shows examples of the bit error probability *p*. It will be shown that p influences failure rate of the bus system strongly. Without proof the calculation has to be based on the worst value $p = 10^{-2}$.

Table 6: Examples of probabilities of bit failures depending of the transmission medium

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

First a message with only one bit is regarded with safety-relevant information. The bus system is laid out beyond that still without backup processing. It will now be shown that a simple redundancy does not promise always success. It is transferred over unscreened twisted-pair cable, i. e. the bit error probability is at 10^{-4} and the data transmission rate lies at $v = 100/s$. Then the rate of transfer errors without redundancy amounts to:

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

This means that one transmission error occurs at 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:

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

Computing the reciprocal one can see that one transmission error can occur each 11,6 days, which is certainly intolerable. This leads to the fact that 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. Especially the probability of corruption of a whole message, the so-called residual error probability is important.

This error probability is the summation of the single bit error probabilities, which also depends on the combinatoric according to the amount of regarded single bit errors.

The residual error probability is

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

with the binomial coefficient

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

where *n* is the message length, *p* is the single bit error probability and *d* is the hamming distance of the data protection method implemented in the controller.

For the case no data protection methods are implemented, *d* is set to 1. A better data protection method results in a higher value for *d*.

2.4.3 Methods for calculating the residual error probability

First the data protection for the models A and D is regarded, with which the backup processing of the transmission layer are not considered. Here is the commercial bus system regarded to be not safe. Thus all measures must take place for data protection in the safety related controller. The remaining error rate Λ results from the residual error probability *R(p)* of the supervising safeguarding processing, the data transmission rate n of the safety-relevant messages and the 1 %-rule. Beyond that the number of m of the participants in a safety function is to be regarded also. Bus systems are freely configurable and assume here the maximum extent of participants on the safety bus system. With *m* participants *m*-1 messages will be transferred.

The rate normalized on one hour results in the equation below

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

The arising value can be compared now with Table 2. Afterwards the parameters Λ and *R(p)* must be varied depending upon required SIL.

Now the data protection for the models B and C is regarded, with which the individual channel of the transmission layers is not regarded as safety related. It becomes the qualitative requirement of the two-channel hardware related to the bus nodes with the combined quantitative computation of Λ. The individual transmission layer is not regarded sufficiently 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. That is in this model the data protection of the commercial bus system is completely used. If only one node the data protection mechanism fails, an uncovering of the error is only possible over one comparator, which 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 the CAN bus guarantee because of their structure that other participants examine each message in a separate hardware, an accumulation by errors can be managed.

The consequence of redundant bus nodes is also a 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 exact the same errors. The probability of message falsification is given by the residual error probability R_{KOM} of the used bus system.

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

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

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

Next the data protection for the models A and D is described, with which the bus system has a portion of safety, which applies for example to field bus systems. Normally field busses are contrary to sensor-actuator-busses equipped on system level with applications, which require larger arithmetic performances or shorter response times, whereby the amount of data is constant.

In a fact bus protocol devices are very expensive. Thus bus nodes often realized as single-channel. Unfortunately the method of calculating is getting more complicated. The IEC 61508 uses the Markov-Models for calculation. A condition for this is a reliable commercial bus system, so that the additional expenditure does not blow up the framework. Based on the transmission quality of the commercial bus system, the remainder for reaching a certain category or a certain SIL is to be realized in the safety controller. For the protocol devices proofs evaluations have to be done and/or the hardware reliability λ 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.

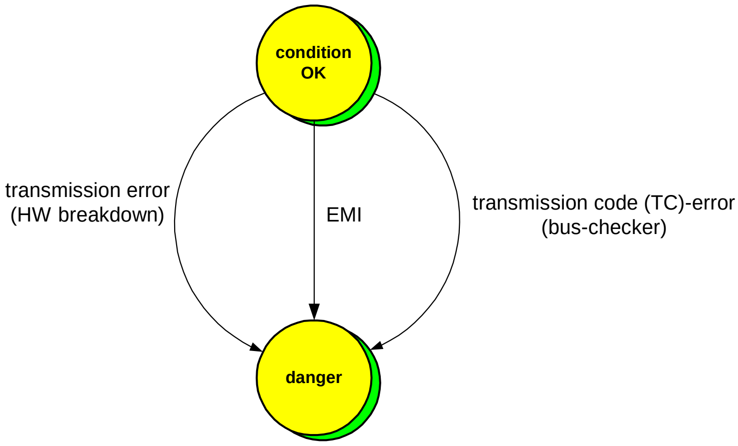
condition OK
transmission error (HW breakdown)
EMI
transmission code (TC)-error (bus-checker)
danger

Fig. 7: Markov-Model for single-channel bus nodes and additional supervising data integrity

The protocol device can fail in three different causes of failure, see Fig. 7. First of all the transmission hardware can fail, so that one message or several messages are falsified. Further it can come to bit falsifications because of electromagnetic influences (EMI), which are not recognized by the data communication equipment. Finally each message is passed from the data communication equipment on to the safety system, because only the bus-checker failed. From Table 2 one can select at required SIL the appropriate target value for Λ, $\Lambda_{t\,arg\,et}$. The remaining error rate results from the individual transitions Λ_{HW}, Λ_{EMI}, Λ_{TC} in this simplified Markov model, which is shown in Fig. 7. The result is the remaining error rate with the 1 %-rule:

$$\Lambda_{SYS} = \Lambda_{HW} + \Lambda_{EMI} + \Lambda_{TC} < \frac{\Lambda_{t\,arg\,et}}{100} . \qquad (7)$$

Λ_{HW} corresponds to the rate of the hardware faults, which caused by hardware failures in the transmission layer a message is falsified.

Failures can only be detected by 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:

$$\Lambda_{HW} = \lambda_{HW} \cdot R_{US} . \qquad (8)$$

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

$$\lambda_{HW} = 1/\,MTTF . \qquad (9)$$

An improvement of Λ_{HW} can be achieved, if λ_{HW} is regarded more exactly. It is distinguished between the actual communication partners and the other bus participants. This fraction varies because of different mechanisms in components involved and uninvolved. The mechanism of a falsification by hardware errors within the components involved (x1) is another than the mechanism of 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). It applies now:

$$\Lambda_{HW} = \left(x_1 \cdot \lambda_{HWF} + x_2 \cdot \lambda_{HWS}\right) \cdot R_{US} . \qquad (10)$$

Thereby stands Λ_{HWF} for the hardware probability of failure of the two actual communicating safety-relevant participants, Λ_{HWS} for the hardware probability of failure maximally x 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 described in Fig. 7 by the middle branch. It is assumed here the correct function of the bus protocol component and the additional data protection mechanisms in the application. That means, that 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 that 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. To EMI applies:

$$\Lambda_{EMI} = f_W \cdot R_{UB} \cdot R_{US} . \qquad (11)$$

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 described in Fig. 7 by the right branch. Under this condition the additional mechanism will work as the only error detection. Since this last specified mechanism is now completely alone on itself, the probability rises that it is confronted with incorrect messages. There is either a certain probability that messages arrive falsified at the safe application or the probability that the error is recognized in the safety controller. In case of failure of the mechanism on the bus therefore the frequency such detected errors will increase, that can be determined for example by a permanent measurement by means of counters and timer. If the frequency is well-known, with which the functional standard data safeguard mechanism detects the failures in the additional data protection mechanism 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 at a small fraction k of the hardware faults. Thus arises for the critical failure of standard protocols:

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

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 introduces the safe condition.

2.5 Extern influences

Of course, as well as all safety-related controllers, also bus systems have to withstand the expected operating and environmental demands. Particularly in the safety technology is environmental compatibility important. Certain insensitivity is required by safety systems for the maintaining operation (high availability), the principal purpose is that a safety-relevant controller never fails to danger also 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). These criteria show in Table 7 the minimum requirements.

Table 7: Performance criteria for the behaviour of safety related bus systems by environment demands

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.

2.5.1 Electromagnetic influences

The standard IEC 61000-6-2 shows only noise immunity for the electromagnetic compatibility (EMC) as minimum requirement. The standard required further performance criteria, which were adapted in Table 7 for the bus systems.

We differentiate disturbances in conducted disturbances, electromagnetic interference and electrostatic influence. In field bus systems all three have an influence on the transmission reliability. Bit errors or burst errors are caused for example by single disturbances pulses.

Field bus systems can use to possibilities to tolerate electromagnetic disturbances or to react safety related. In this aspect they differ from other modern controllers. The first possibility is the passive screening e. g. by EMC filtering and special wiring. The second possibility is an active tolerance e. g. by detection of disturbed messages and block replications and retransmissions. The availability of the system does not suffer, if this measure is possible within the demanded reaction time.

In the case of strong and longer persisting disturbance the bus system will change into its safe condition.

Normally by a combination of these two measures a very good protection from EMC influences is guaranteed, which provides both safety and availability.

Disturbances can impair however apart from the direct influence of the transmission of messages also the safe function of electronics devices. For instance a destruction of the entire bus protocol circuit or other important components as the safe guarding mechanism (at redundant system a common cause failure) are to be considered. These influences must be likewise considered with field bus systems.

2.5.2 Mechanical and climatic influences

Beside EMC other influences in the field operation are to be considered such as shock, vibration, temperature and humidity. The bus systems are not different from other safety-relevant systems in this aspect. Table 8 shows four different application areas with different severity levels for mechanical examinations.

It is advised that a safety related bus system is only applicable within the specified environment. Also the existing relevant standards are to be observed.

Table 8: Range of different applications

Range of application I: None increased demands
Range of application II: Average environmental technical or operating conditioned influences are to be expected, the assembly place protect the installation against strong influence. Note: It is to be noted that cabinets are set up also at exposed places and so they can exist also in the range of application III or IV.
Range of application III: One proceeds from hard environmental technical or operating conditioned influences. That is particularly for process near installations of sensors and actuators the case. Electrical fitting spaces also exposed and fall under this range of application.
Range of application IV: It concerns the external area. In addition to range of application III are considering harder requirements (e. g. lightning protection).

References:

[1] *IEC/EN 61508: International Standard 61508 Functional safety: Safety-related System*, Geneva, International Electrotechnical Commission

[2] Börcsök, J.: *Elektronic Safety Systems*, Hüthig publishing company, 2004.

[3] Börcsök, J.: *Safety related Bus-Systems*, Presentation within the conference Foundation Fieldbus End Users Council Australia Incorporated, Australia 2003

[4] Börcsök, J.: *Principles of Safety Related Bus-System and Protocols*, Presentation within the FF-SIS – Meeting in Hannover 2004

[5] *DIN VDE 0801: Funktionale Sicherheit, sicherheitsbezogenener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES)*, (*IEC 65A/255/CDV:* 1998), Page: 27f, August 1998

[6] *DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen*, Beuth publishing company, Berlin 1998

[7] *DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben*, Beuth publishing company

[8] *IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung*, 12/2001