Abstract: - This paper describes the requirements and specifications to be considered and fulfilled to design safety bus systems. 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 alone cannot 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 Introduction
This paper outlines the requirements for designing safety bus systems. It starts with an introduction to safety in general and to safety bus systems in particular. It discusses state of the art measures of fault avoidance and fault control. In the second section, it details the requirements of safety bus systems and discusses amongst others the qualitative measure against transfer failures, the qualitative control of faults and transmission errors as well as external influences. It finally concludes with a short summary.

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 [1,7]. 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 later in the operation phase to a dangerous situation [1]. For this reason measures have to be taken against such errors in the development phase of a safety device. The standards DIN-V-VDE0801 and IEC61508 [4,8] 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 avoided, or can be detected and corrected during the process [1]. The measures for fault control included hardware and software modules. These arising errors detected during operation, cause as a result appropriate safety-related reactions of the computer system [3].

1.2 Measure combinations for fault avoidance
Particularly in complex systems, thus errors can only be reduced effectively, if procedures in the design, development and maintenance phase are structured [1,2]. 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 [8] 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 [8] contain details for the implementation of electrical, electronic and programmable electronic (PES) systems. Thereby, precise measures are assigned to each phase for the realisation of a complex safety device for fault avoidance. 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. National test institutes e. g. the Technischer Überwachungsverein (TÜV) takes this path at certification of computer controlled systems already for a long time [1]. 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 only be ensured, if constructional, analytical 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 [1,3].
The design of safe communication systems for the control of systematic failures. These two measures can be helpful to detect disturbances in the functional software in time, which are caused either by unexpected 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. 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.
2. Fundamental requirements of bus systems for the safety systems

2.1 Functional requirements of the process

In process industry, in which requirements are 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 the workflow via a light curtain, depending from the users’ action. 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), has to be dimensioned with consideration of these two dynamics of machine and user with certain additional safety margins. In the standard EN 999 [1] guidelines such protection fields are set up. Response time of an ESPE is to be calculated directly proportionally, i.e. the response time high, it forces the light curtains installed further away from the dangerous area. The demand rate of the protection device depends for example on the possible failure of the machine and the frequency that can be expected for such a dangerous situation to occur. The mode of operation of a hazardous system is operated in accordance to 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 [8] in a low demand mode. In addition, with processes with a response time of some 100ms a low demand mode is completely sufficient. This applies to safety systems, which are under complete control of human being, e.g. vehicles or machine which can be brought into a safe state by the emergency stop within a time range of 100ms. It remains stated that the demand rate to a safety system is generally high and the response times are by 50 to 150ms, 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. It can imagined that in the future the protection fields of laser scanner can be reconfigured without interruption of the workflow in few 100ms with high dynamics.

2.2 Qualitative measures against transfer failures

Figure 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.

![Schematic of a simple bus system](image)

The protocol receiver component converts the 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 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 provide flexibility inside the system, with the assistance of protocol components. However, this introduces 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.
- 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.

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. However, electromagnetic disturbances have an influence on the signals of bus systems.

2.3 Embedding of commercial bus systems into the total controller
It is not sufficient to replace simply a conventional wiring by a commercial bus system [1,2,3]. The bus system’s safety controller has to be able to detect failures, and ensure by plausibility checks a correct data communication. In this sense, a safety-relevant controller is the control device for the medium, the protocol circuits and the bus interface. Figure 3 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. The data is handed over to the safety interface; this layer adds further data to authenticity and for data protection. In this packed condition the data is transmitted to the lower not safety related transmission layer. The entire risk reduction by additional measures is to be realized in the safety controller.

![Fig. 3: OSI-model for safety engineering](image)

2.4 Qualitative control of faults
Several methods [1,8] are established and can be used against transmission errors. 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. These commercial protocol chips [1] are still 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. 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. 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 checks whether the time between two messages exceeds a given limit. In this case, the receiver has to expect that an error has occurred and operations, which could lead to dangerous situations, have to be stopped. Time expectation can be used to detect a transmission error delay and is mandatory for every safety-related bus system since it is an equivalent to the quiescent current principle.

A different method is the acknowledgement of a transmission. After successful reception of a message, the receiver sends an acknowledgement for the received message. 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 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 [8], provided that the time expectation method is always implemented. The protocol used for safety-related transmission via bus systems has to be modified accordingly.

2.5 Quantitative measures against transmission errors

In the preceding section the requirements were qualitatively described for a safety bus system. There is at least one measure against each transfer error, which has to 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.

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.

2.6 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 also be transmitted to a transmission error. If random hardware faults are similar regarded as transmission errors, the probabilities of failures on demanded in the IEC 61508 [8] can be applied to the transmission errors. The IEC 61508 [8] regards the 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 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. A complete calculation of the data integrity level for each model, presented in the last section, is detailed in part II of this paper and in Electronic Safety Systems [1].

2.7 Extern influences

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 1 the minimum requirements [1,8].

<table>
<thead>
<tr>
<th>Perf. criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>The bus system must work intended during and after the disturbing influence.</td>
</tr>
<tr>
<td>B</td>
<td>The bus system must work after the disturbing influence intended. Bus communication is automatically again taken up after disturbing influence.</td>
</tr>
<tr>
<td>C</td>
<td>The safety related introduce participant the safe condition. Communication failed. All safety-related participants remain in the safe condition. The re-establishment of the correct enterprise takes place via setters.</td>
</tr>
</tbody>
</table>

Table 1: Performance criteria

2.7.1 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 1. Disturbances are subdivided in conducted disturbances, electromagnetic interference and electrostatic influence. In field bus systems, all three disturbances 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 [1,8].

2.7.2 Mechanical and climatic influences
Beside EMC other influences in the field operation are considered such as shock, vibration, temperature and humidity. The bus systems are not different from other safety-relevant systems in this aspect. Table 2 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. Additionally, the existing relevant standards have to be observed [1,8].

<table>
<thead>
<tr>
<th>Range of application I:</th>
<th>None increased demands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range of application II:</td>
<td>Average environmental technical or operating conditioned influences are to be expected, the assembly place protects the installation against strong influence.</td>
</tr>
<tr>
<td>Range of application III:</td>
<td>One proceeds from hard environmental technical or operating conditioned influences. That is particularly for process near installations of sensors and actuators the case.</td>
</tr>
<tr>
<td>Range of application IV:</td>
<td>It is concerns with the external area. In addition to range of application III are considering stricter requirements (e. g. lightning protection).</td>
</tr>
</tbody>
</table>

Table 2: Range of different applications

3 Summary/Conclusion
This paper has detailed the principles of safety bus systems, which have to be considered and applied in order to design a safety bus for process industries and to get the system finally certified by a national institution. It started with the fundamentals of safety. It introduced the measures for fault avoidance and fault control. It focused on the requirements of bus systems which have to be designed for safety systems. The paper detailed the requirements of international standards for safety related systems such as the IEC 61508 and introduced the concepts of safety layers and different architectures of safety bus systems. It briefly established data integrity and finally examined extern influences to be taken into considerations for designing a safety bus system.

References: