Principles of Safety Networks – Part II

BÖRCSÖK J. UGLJESA E. HOLUB P.
Computer architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel,
GERMANY

http://www.rs.eecs.uni-kassel.de

Abstract: This paper is the second part of principles of safety networks. In the first part the requirements and specifications were detailed to be considered and fulfilled to design safety bus systems. The second part introduces data integrity in more detail and compares mathematically different architectures of safety-bus-systems.

Key-Words: Protocol, Safety, Safety-bus, Functional-safety, Data integrity, Markov model

1 Introduction

Part I and part II of the paper principles of safety networks give a detailed overview of the requirements and specifications for the design and implementation of safety bus systems following the standard of IEC 61508. Whilst the first part gives more a practical overview of the design and aspects to be considered, the second part explains in more detail data integrity and evaluates mathematically different architectures of safety bus systems, introduced in part I.

2 Data integrity

For the qualitative estimation of safety relevant procedures of the data protection, the standard IEC 61508 is applied (IEC/EN 61508). Although this standard makes neither qualitative nor quantitative preconditions for the evaluation of transmission errors, it is still applicable because of the requirements of the probability of failure by the hardware design. In a safety-related controller a random hardware fault leads finally to a random failure, which can lead to a transmission error. [1,2,3]

If transmission errors are regarded similar to the random hardware faults, the probabilities of failures on demanded in the IEC 61508 [8] can be applied to the transmission errors as shown in Table 1. A comparison of different definitions of the Safety Integrity Level are presented in Table 3.

### Table 1: Definition of Safety Integrity Level According to IEC 61508

<table>
<thead>
<tr>
<th>SIL</th>
<th>Low demand mode of operation (Average probability of failure to perform its design function on demand)</th>
<th>High demand or continuous mode of operation (Probability of a dangerous failure per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$\geq 10^{-9}$ to $&lt; 10^{-8}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
<td>$\geq 10^{-10}$ to $&lt; 10^{-9}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
<td>$\geq 10^{-12}$ to $&lt; 10^{-11}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
<td>$\geq 10^{-14}$ to $&lt; 10^{-13}$</td>
</tr>
</tbody>
</table>

Note: The exact times are to be determined by an application dependent risk evaluation with consideration of the appropriate standards.

### Table 2: Overview about the requirements of process to bus systems

<table>
<thead>
<tr>
<th>Application / Operation mode</th>
<th>Reaction time</th>
<th>Typical amount of data</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor / Actuator Low demand mode</td>
<td>$\leq 150$ ms</td>
<td>$= 1$ Byte</td>
<td>Safety off</td>
</tr>
<tr>
<td>Sensor/Actuator High demand mode</td>
<td>$\leq 150$ ms</td>
<td>$= 1$ Byte</td>
<td>Admittance protection Laser scanner</td>
</tr>
<tr>
<td>Sensor / Actuator High demand mode</td>
<td>$\leq 10 - 100$ ms</td>
<td>$= 1$ Byte</td>
<td>Finger protection Light barriers</td>
</tr>
<tr>
<td>Sensor / Actuator Low demand mode “offline”</td>
<td>As long as needed</td>
<td>some megabyte</td>
<td>Software update</td>
</tr>
<tr>
<td>Sensor / Actuator High demand mode “offline”</td>
<td>Tolerance time of the process $\leq 100$ ms</td>
<td>some kilobyte</td>
<td>Switching of protection areas of laser scanners within the reaction time</td>
</tr>
</tbody>
</table>

The requirements indicated in Part I of the paper *Principles Safety Networks* demand among other things for a universal safety system that the mode of operation is either continuous or high demand mode. Table 1 and Table 2 shows the values for these modes of operation according the IEC 61508.[1, 2, 3]

As already mentioned in the first part, 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 for transmission errors, in order that the probability of a dangerous fault of the system can be calculated. Methods for bus systems are partially very complex, so that some preconditions have to be 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 is only an approximated value. 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 [1].

Using the appropriate bus architecture and the data protection mechanism approach it turned out that those are sufficient for quantification. In the following, for a function of the bus architecture, different calculation methods are described, which have the failure rate \( \Lambda \) (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, which is concerned with normal distributed probabilities of bit error and white noise. It is assumed that during the transmission of information the probability, that a bit is falsified, is normal distributed, which is generally called bit error probability \( p \). [1]

The approach with longer messages is to be regarded as worst case. Table 4 shows examples of the bit error probability \( p \). It will be shown that \( p \) strongly influences the failure rate of the bus system. Without proof the calculation has to be based on the worst value \( p = 10^{-2} \).

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

Table 3: Definition of the Safety Integrity Level of IEC 61508

<table>
<thead>
<tr>
<th>Probability of bit failures ( p )</th>
<th>Transmission medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>( &gt; 10^3 )</td>
<td>Transmission path</td>
</tr>
<tr>
<td>( 10^4 )</td>
<td>Unscreened data line</td>
</tr>
<tr>
<td>( 10^5 )</td>
<td>Screened twisted-pair telephone circuit</td>
</tr>
<tr>
<td>( 10^6 ) - ( 10^7 )</td>
<td>Digital telephone circuit (ISDN)</td>
</tr>
<tr>
<td>( 10^9 )</td>
<td>Coaxial cable in local defined application</td>
</tr>
<tr>
<td>( 10^{12} )</td>
<td>Fibre optic cable</td>
</tr>
</tbody>
</table>

Table 4: Examples of probabilities of bit failures depending of the transmission medium

First a message with only one bit is regarded with safety-relevant information [3]. It is assumed that the bus system structure is designed without backup processing methods. It will now be demonstrated 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 results in:

\[
U = p \cdot v = 10^{-2} / s
\]  

(1)

This result can be interpreted 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 an unchanged \( v = 100/s \) is:

\[
U_{\text{red}} = p' \cdot v = 10^{-6} / s
\]  

(2)

Computing the reciprocal of the previous result can be understood as 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 depends not only 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 combinatorial analysis according to the amount of regarded single bit errors.
The residual error probability is

\[ R(p) = \sum_{e=d}^{n} A_{n,e} p^e (1 - p)^{(n-e)} \tag{3} \]

with the binomial coefficient

\[ A_{n,e} = \binom{n}{e} = \frac{n!}{e! (n-e)!} \tag{4} \]

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 \( d \).

### 3 Methods for calculating the residual error probability

First the data protection for the models A and D is regarded [1], with which the backup processing of the transmission layer are not considered, as shown in Figure 1.

In this scenario, the commercial bus system is regarded to be not safe. Consequently, all measures have to taken for data protection in the safety related controller. The remaining error rate \( \Lambda \) 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. Furthermore the number of \( m \) of the participants in a safety function is to be considered. Bus systems are freely configurable and it is assumed that the maximum extent of participants on the safety bus system is taken into account. Finally \( m \) participants and \( m-1 \) messages are transferred on the network.

The rate normalized on one hour results in the equation below

\[ \Lambda(R,V,m,p) = 3600 \cdot R(p) \cdot v \cdot 100 \cdot (m-1) \tag{5} \]

The arising value can be compared with Table 2. Afterwards, the parameters \( \Lambda \) and \( R(p) \) must be varied depending upon the required SIL (Table 1).

Now, the data protection for the models B and C (Fig.1) is considered, where the individual channel of the transmission layers is not regarded as safety related. It results that the qualitative requirement of the two-channel hardware is related to the bus nodes with the combined quantitative computation of \( \Lambda \). 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 a sufficient measure against coincidental hardware errors in the bus protocol device. 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, and an accumulation by errors can be managed.

The consequence of redundant bus nodes is also a redundant transmission of messages. All messages are consequently transmitted twice and examined and compared. The transmission only fails if the redundant message has exactly the same errors as first message. 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

\[ R_{red}(p) = R^2 \tag{6} \]

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

The data protection for the models A and D is described next, where the bus system has a segment 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. Consequently, bus nodes are often realized as single-channel systems. Unfortunately, the calculation method 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 overhead does not exceed 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-proof evaluations have to be done and/or the hardware reliability $\lambda$ 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 allocated to three substantial transition probabilities.

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

$\Lambda_{HW}$ corresponds to the rate of the hardware faults, which are caused by hardware failures in the transmission layer a message is falsified. Failures can only be detected by 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 has to be known. Therefore, $\Lambda_{HW}$ 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. $\Lambda_{HW}$ can be calculated as follows:

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

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

$$\lambda_{HW} = \frac{1}{MTTF} \quad (9)$$

An improvement of $\Lambda_{HW}$ can be achieved, if $\lambda_{HW}$ is regarded more exactly. It has to be distinguished between the actual communication partners and the other bus participants. This fraction varies because of different mechanisms in the components involved and uninvolved. The mechanism of a falsification by hardware errors within the components involved ($x_1$) is different than the mechanism of the destruction of a message by uninvolved components ($x_2$). Thus the fractions $x_1$ and $x_2$ of the dangerous failures differ. $x_1$ can be estimated by a failure mode and effect analysis (FMEA). It applies now:

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

Where $\Lambda_{HWF}$ stands for the hardware probability of failure of the two actual communicating safety-relevant participants, $\Lambda_{HWS}$ for the hardware probability of failure. $x_1$ stands for the part of the dangerous errors by the components uninvolved, $x_2$ for the segment 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 by the middle branch in Figure 2. The correct function of the bus protocol component is assumed 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 $f_{WS}$ with which messages on a bus system are disturbed. To EMI applies:

$$\Lambda_{EMI} = f_{W} \cdot R_{UB} \cdot R_{US}$$  \hspace{1cm} (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 Figure 2 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 separated, the probability increases since it has to deal 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 with, for example, with 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 increase can be determined and after a certain time $T$, the system can be brought into the safe state. $R_{fW}$ 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:

$$\Lambda_{TC} = R_{UB} \cdot \frac{k}{T}$$  \hspace{1cm} (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.

4 Summary

This paper comprises the mathematical description for the paper principles of safety networks –Part I. It detailed data integrity following the IEC-61508 and specified mathematically different model architectures for safety bus systems.

References: