2oo4 architecture, an advanced processing architecture for safety related systems

PROF. DR.-ING. HABIL. JOSEF BÖRCSÖK
DIPL.-ING. EVZUDIN UGLJESA

Rechnerarchitektur und Systemprogrammierung
Universität Kassel
34121 Kassel, Wilhelmshöher Allee 73

HIMA Paul Hildebrandt GmbH + Co KG
68782 Brühl, Albert-Bassermann-Str. 28

GERMANY

www.hima.com

Abstract: - The 2 out of 4-system (2oo4) is an advanced safety architecture. A 2oo4-system is 2-failure safe, this means that at least two of the four channels have to work correctly in order to trigger the safety function. In order to classify the quality of a system different parameters have to be calculated, like the PFD and MTTF. In this paper, equations are indicated for PFD for normal and common-cause-failures. Additionally, the Markov-model for a 2oo4-architecture is introduced and the MTTF-value for this architecture is calculated. The results are high availability and a high reliability.

Key-Words: - 2oo4-Architecture, Availability, IEC/EN 61508, Reliability, Markov-model, MTTF, PFD, SIL

1 Introduction

Modern technical systems, controlling and steering safety relevant processes are becoming more and more complex. There are multifarious reasons for this: On one hand, the demands on high quality performance systems increase while simultaneously the required space for components has to decrease, and on the other hand, it is necessary to offer technically enhanced and safer systems, due to a steadily growth of competitive globalisation, - in order to remain competitive. This applies especially to the field of safety relevant digital processing and automation, in which complex digital circuits are integrated.

Digital processing systems of each size are particularly used for safety related tasks. Such tasks might be the supervising or controlling of vehicles, trains, airplanes or power plants and chemical processing units. Another important and growing application field is the medical field. In each of the indicated sectors failures and errors of the systems would increase the risk for immense damage up to the threat of human lives.

Today’s controlling or application systems used for safety critical missions commonly consist of highly complex single components, implemented either as software or hardware. A hardware and a software model have to be generated, evaluating aspects like reliability and safety of a complex system. Reliability means to function without any failure under all circumstances. Safety here means that the system will not come into a critical state even if a failure occurs. The process’s safe status is referred to as a status of no danger occurring. If a failure occurs the system has to be able to reach the safe status.

The various functional, non-functional and safety-technical demands to the system along with common system characteristics lead to a list of system specific features. This contains:

- Reliability, availability and failure safe operation
- System integrity and data integrity
- Maintenance and system restoring.

In order to have measurable parameters, the widely used parameters “mean time to failure” (MTTF) and “probability of failure on demand” (PFD) were defined. The PFD characterises the quality of a faultless system. The smaller the value is the better the safety of the system. A system’s safety refers to all items in the loop. In automation, a loop among others consists of a safety related system of the following components:

- Computing elements (logic processing devices such as analogue and digital in- outputs, CPU)
- Sensors
- Termination elements such as actuators
Combing all elements of a system in a safety architecture, the system can be classified with a defined safety level, safety integrity level (SIL).

Table 1 shows various classifications of safety systems. The norm IEC 61508 defines two different criteria for the classification of the safety systems into the individual safety levels.

On one hand, a system can be judged by its probability of a dangerous failure, i.e. an error occurs on the demand of a safety function and the system can no longer perform its safety function. IEC 61508 implies that the so called proof check interval lies at

- two years
- ten years.

This probability of failure is defined as “probability of failure on demand” (PFD). It has a dimension of 1 unit.

### Table 1: SIL classification

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Low demand mode of operation</th>
<th>High demand or continuous mode of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>T₁ = 2 years or T₁ = 10 years</td>
<td>T₁ = 1 month or T₁ = 2 months or T₁ = 6 months or T₁ = 1 year</td>
</tr>
<tr>
<td>1</td>
<td>≥ 10⁻² to &lt; 10⁻¹</td>
<td>≥ 10⁻⁶ to &lt; 10⁻⁵</td>
</tr>
<tr>
<td>2</td>
<td>≥ 10⁻³ to &lt; 10⁻²</td>
<td>≥ 10⁻⁷ to &lt; 10⁻⁶</td>
</tr>
<tr>
<td>3</td>
<td>≥ 10⁻⁴ to &lt; 10⁻³</td>
<td>≥ 10⁻⁸ to &lt; 10⁻⁷</td>
</tr>
<tr>
<td>4</td>
<td>≥ 10⁻⁵ to &lt; 10⁻⁴</td>
<td>≥ 10⁻⁹ to &lt; 10⁻⁸</td>
</tr>
</tbody>
</table>

IEC 61508 proposes a second possibility for the classification of a safety system. The probability of an occurring failure on demand leaving the system unable to perform its safety functions is calculated as well. Therefore, a certain period of time is demanded for the proof check interval, either

- one month or
- three months or
- six months or
- one year.

This probability of failure is defined as probability of failure per hour (PFH). Unlike probabilities, it has a dimension of 1/h. Systems demanding a continuous operation are highly significant for industrial systems.

Note that comparing both systems to its PFD or PFH value is only possible within limits, as they refer to different bases.

The probability of a failure on demand has always to be regarded as a statistical term. Even in safety systems, there is no absolute safety given, since these systems may fail on demand.

By long lasting empirical studies on corresponding applications the distribution of a system’s failures can commonly be assumed as follows:

- 15% of computing elements
- 50% of sensors
- 35% of termination elements such as actuators.

The whole system’s failure rate λ is subdivided into safe failures λₛ and dangerous failures λ₅. In addition, safe failures are subdivided into safe undetected failures λₛᵤ and safe detected failures λₛ₅. Whereas dangerous failures are subdivided into dangerous undetected failures λ₅ᵤ and dangerous detected failures λ₅₅. Fig. 1 shows the spreading of failure rates. Failure rates could be specified with the aid of standard specifications.

A system’s quality can be specified by defining its PFD value referred to its accuracy. The smaller this value the better the system is. However, the longer the system runs the higher the PFD value will be. The PFD value is calculated for a period of time called proof check interval T₁. After the maintenance of the system we proceed on the assumption that it works without any failures. Judging and comparing systems is mostly specified by the PFD average value (PFDavg) over a whole proof check interval.

The most known architectures in use for safety systems are the 1oo2- and 2oo3-architectures. 1oo2 and 2oo3 architectures are common for safety-related systems in industry.

In order to meet all requirements for safety the 1oo2-architecture is sufficient. If an (additional) high reliability is required a 2oo3-architecture has to be chosen. In order to take advantage of both systems in industry, a 2oo4-architecture has to be developed. This architecture will be described in the following.

![Fig. 1: Structural Software Creation for Safe Systems](image-url)
2 Description of the 2oo4-architecture for safety-related technology
The 2oo4-system normally contains of four independent channels. The four channels are connected one with another. In order to trigger the safety function at least two of the four channels have to work correctly. Even if two failures in two different channels occur the system can be transmitted into the safe state. It is said: “A 2oo4-system is 2-failure safe”.
A dangerous breakdown of the system is generated if three of the four channels have dangerous failures themselves. Figure 2 shows a reliability block diagram of a 2oo4-architecture. Each single channel contains of an input circle, a safe processing unit and two serial output circles.

In a fault-tree-analysis you can determine the following which causes a system in a dangerous non safety state:
- There is in all four channels a dangerous detectable failure which all have a common cause
- There is in all four channels a dangerous undetectable failure which all have a common cause
- Three of four channels have a dangerous detectable or a dangerous undetectable failure which all have no common cause

Theoretically, a 2oo4-system is immediately transmitted into the safe state if a dangerous failure arises. However, in practice, each failure detection is time consuming. If any more failure occurs in this time, then two failures exist at the moment. However, due to its 2-failure-safety the 2oo4-system can definitively reach the safe state, whereas a 1oo3-system can not.

3 Calculation of probability distributions
You can apply the basic approach for determination of $PFD_{avg}$-equation of a 2oo4-system:

$$P(t) = P_{single} + P_{common cause}$$

$$= 4 \cdot P_1(t) \cdot P_2(t) \cdot P_3(t) + P_{DDC}(t) + P_{DUC}(t)$$  (1)

The index DUC means a dangerous undetected common-cause-failure, whereas DDC accounts for a dangerous detected common-cause failure.

3.1 Calculation of probability of normal failures
As already mentioned, the 2oo4-system is 2-failure tolerant. Before the probability of normal failures for a 2oo4-system are calculated, it should be shown, how the probability for a 1-failure tolerant system is calculated, e. g. a 1oo3-system. If a 1oo3-system should fail with normal failures, the system is within the condition that each of the three channels must have a dangerous failure. If the probability is calculated for this case, then the product is derived from the probability of failure of each channel. The following equation results:

$$P_{normal} = P_1(t) \cdot P_2(t) \cdot P_3(t)$$  (2)

$P(t)$ describes the probability of failure for the $i^{th}$ channel with the failure rate of

$$\lambda = \lambda_{Di}$$  (3)

for a dangerous, normal failure in channel $i$ and the probability of failure

$$P_i(t) = 1 - e^{-\lambda_{Di} \cdot t}$$  (4)

If the equation (4) and (2) are used with the general applicable $PFD_{avg}$ equation
\[ PFD_{\text{avg}}(T) = \frac{1}{T} \int_0^T P(t) \, dt \] (5) 

we get the result

\[
PFD_{\text{avg, normal}}(T) = 1 + \frac{e^{-\lambda_0 T} - 1}{\lambda_0 T} + \frac{e^{-\lambda_0 T} - 1}{\lambda_0 T} - \frac{e^{-\lambda_0 T} - 1}{(\lambda_0 + \lambda_1) T} + \frac{e^{-\lambda_0 T} - 1}{(\lambda_0 + \lambda_1) T} \]

\[
= \frac{e^{-\lambda_0 T} - 1}{\lambda_0 T} + \frac{e^{-\lambda_0 T} - 1}{(\lambda_0 + \lambda_1) T} - \frac{e^{-\lambda_0 T} - 1}{(\lambda_0 + \lambda_1 + \lambda_2) T} + \frac{e^{-\lambda_0 T} - 1}{(\lambda_0 + \lambda_1 + \lambda_2) T} \] (6)

This function can be developed into a power series with help of a Taylor development (exactly MacLaurin series). The condition that the \( PFD_{\text{avg, single}}(T) \) is a continuous function, which has a removable singularity at \( T = 0 \) and thus all derivations at this point exist can be proved, e.g. in [2], [3]. After some calculation, see also [2], [3], we get the result

\[ PFD_{\text{avg, normal}}(T) = \frac{(\lambda_D)^3 \cdot T^3}{4} \] (7)

This is the result for the probability of failure on demand for a 1oo3-system for normal failure. The reader should be aware that the parameter \( T \) is not equivalent to the parameter \( T_1 \) (proof check interval) in the IEC/EN 61508, see [10]. \( T_1 \) is only a part of \( T! \)

For the calculation of the \( PFD_{\text{avg}} \) value for a 2oo4-system in case of normal failures, equation (7) of the 1oo3-system can be used. This equation has to be extended for the factor four as with four channels there are four possibilities that in two channels a failure exist—remember the 2oo4-system is two-failure tolerant.

The probability of failure for the 2oo4-system for normal failures is

\[ PFD_{\text{avg, normal}}(T) = (\lambda_D)^3 \cdot T^3 \] (8)

### 3.2 Calculation of probability of common-cause failures

Now, the failure probability for dangerous undetectable and dangerous detectable common cause failures \( P_{\text{DUC}} \) and \( P_{\text{DDC}} \) is calculated. Common cause failures are those failures that occur in all system channels at the same time and which have a common cause. When determining the \( PFD_{\text{avg}} \) this kind of failure is rated for a multi channel system through the \( \beta \)-factor. One differentiates between the \( \beta \)-factor for dangerous undetectable failures, with the weight \( \beta \), and the \( \beta \)-factor for dangerous detectable failures, with the weight \( \beta_D \). Calculating the common cause part of the total probability, the failure probabilities \( P_{\text{DUC}} \) and \( P_{\text{DDC}} \) have to be added.

\[ P_{\beta}(t) = P_{\text{DUC}}(t) + P_{\text{DDC}}(t) \] (9)

Analogue, these failure probabilities can be derived for a 1oo1-system with \( \lambda_{\text{D,1oo1}} = \beta \cdot \lambda_{\text{DU}} \) respectively \( \lambda_{\text{D,1oo1}} = \beta \cdot \lambda_{\text{DD}} \). A random common cause failure represents a 1oo1 function block! Therefore, it is possible to apply the derived \( PFD_{\text{avg}} \) equation of the 1oo1-system for the calculation of probability of common cause failure, see [2], [3]. The general solution for the probability failure results in

\[ PFD_{\text{avg}} = \frac{\lambda_D \cdot T}{2} \] (10)

Since there are two common cause failure modes, \( \lambda_{\text{DUC}} = \beta \cdot \lambda_{\text{DU}} \) and \( \lambda_{\text{DDC}} = \beta_D \cdot \lambda_{\text{DD}} \), and with the two assumptions that

- a dangerous undetected common cause failure occurs within the time period \( T_1 + \text{MTTR} \) (\( T_1 \) means the proof time interval, \( \text{MTTR} \) means the mean time to repair) and
- a dangerous detected common cause failure occurs within the repair time \( \text{MTTR} \),

the \( PFD_{\text{avg}} \) value for common cause failures can be calculated as

\[ PFD_{\text{avg, } \beta} = \frac{\beta_D \cdot \lambda_{\text{DU}}}{2} (T_1 + \text{MTTR}) + \frac{\beta \cdot \lambda_{\text{DU}}}{2} \cdot \text{MTTR} \] (11)

### 3.3 \( PFD_{\text{avg}} \)-equation for a 2oo4-system

The \( PFD_{\text{avg}} \) equation of a 2oo4-system is taking into account the normal failures, equation (8), and the common cause failure, equation (11), is therefore:

\[ PFD_{\text{avg}} = (\lambda_D)^3 \cdot T^3 + \frac{\beta_D \cdot \lambda_{\text{DU}}}{2} (T_1 + \text{MTTR}) + \frac{\beta \cdot \lambda_{\text{DU}}}{2} \cdot \text{MTTR} \] (12)

The probability of a common cause failure is the same in a 1oo2-, 2oo3- and in a 2oo4-system. If the probability of a normal failure in a 2oo4-system is compared with the probability of a 2oo3-system, then the probability in a 2oo4-system is several dimensions smaller than in a 2oo3-system. This can be recognized in figure 3. The values are calculated for a proof-test-interval of \( T_1 = 10 \) years and are applied in industrial logic solver modules.
4 Markov-model of a 2oo4-architecture

Basically, the Markov-model is of a 2oo4-“Single-Board System” accomplished with conventional calculation methods. The single transitions are shown in figure 4. A 2oo4-system possesses four error levels.

The state 0 represents the accuracy in all of the 4 channels. State 1 is the safe state in which the system evolves if a safe failure occurs. The transition rate from state 0 to state 1 is $4 \cdot \lambda_{S}$, because in each of the four channels is a safe failure possible. On the basis of state 3 of the 2oo4 model the authors will describe the different transitions. The same issues exist for all other states.

In state 3 one of the four channels is operating with a failure. The occurring failure is dangerous and is not recognised by the failure diagnostics. The transition rate between the states 0 and 3 has the value $4 \cdot \lambda_{DD}$, as in one of the three channels a dangerous undetected failure can exist. No transition possibility exists for the system from state 3 into safe state 1 because the failure cannot be recognised within the test interval $\tau_{Test} = 1/\mu_{0}$. From state 3 a transition takes place into state 5 respectively 6 if a failure occurs in the until then still failure-free channels. The system can only change to state 0 again, where the system is failure free, after $\tau_{LT}$ if during the total lifetime of the system in state 3 no further failures occur. In praxis this means: After time $\tau_{LT}$ the total system is exchanged.

If the second failure in state 3 is a dangerous detected failure then a transition takes place into state 5. The transition rate is $3 \cdot \lambda_{DD}$.

The following two cases can be differentiated if a common cause failure occurs in a 2oo4-system:

- The common failure cause leads to dangerous detected failures. Then a transition exists from state 0 directly into the state 11. The transition rate is $\beta_{D} \cdot \lambda_{DD}$.

- The common failure cause leads to dangerous undetected failures. Then a transition exists from state 0 directly into the state 14. The transition rate is $\beta \cdot \lambda_{DU}$.

In summary we can note the following:

- If state 7 occurs the system immediately switches to state S.
- Failures that bring the 2oo4-system in the states 8, 9, 12, 13, and 15, result in a transition of the system into the safe state 1 after a time, which is smaller than $4 \cdot \tau_{Test}$. The transition rate from these states into state 1 is always equal to $\mu_{0} = 1/\tau_{Test}$.

The states 1, 7, 11, 12, 13, 14 and 15 are absorbing states, that means, this states has only a transition to the safe state or to the state "system fully operational" and no further transitions exist.

In the states 0, 2, 3, 4, 5, 6, 8, 9 and 10 the system is operational. These states have to be taken into account for the MTTF calculation of the 2oo4-systems.
4.1 Calculation of MTTF-value for a 2oo4-system

For the 2oo4 Markov model exists the transition matrix P. This transition matrix is 16 x 16 matrix, see [2], [3], because we have 16 states.

The P matrix is the basis for the Q matrix. The elements of the Q matrix are composed of the respective probability densities, where the corresponding states meet the following criteria:

- System operational
- Non absorbing state.

An operational system is possible for a 2oo4-system in the states 0, 2, 3, 4, 5, 6, 8, 9 and 10. The states 1, 7, 11, 12, 13, 14 and 15 should not be considered during the MTTF calculation, as they are absorbing states.

Therefore, the Q matrix has a 9 x 9 matrix form, see [2], [3].

For the considered Markov model we make the assumption $\tau_{LT}=\infty$. As such applies

$$\mu_{LT} = \frac{1}{\tau_{LT}} = 0.$$  \hspace{1cm} (13)

The next step is to calculate the M-matrix. The M-matrix is presented with the following formula:

$$I - Q = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} dt = M \cdot dt.$$  \hspace{1cm} (14)

For the 2oo4-system the M-matrix is also a 9 x 9 matrix. Now the N-matrix will be calculated. The N-matrix needs to be composed to derive the MTTF value of the system. The N-matrix is the inverse matrix of the M-matrix. The MTTF value describes the mean time between the occurrences of two failures. One assumes state 0 at the start time, i.e. the state in which the system operates failure free. After the inversion the elements of the new matrix represent time dependent values. One needs to sum the first row of the N-matrix in order to derive the MTTF value of the system.

The MTTF term of a 2oo4-system has the following form, see also [2], [3], particularly the parameters $A_1$ to $A_{14}$:

$$MTTF_{2oo4} = \frac{1}{A_1} + 4 \cdot \frac{A_2}{A_1 \cdot A_2} + 4 \cdot \frac{A_{DU}}{A_1 \cdot A_2} + 12 \cdot \frac{A_{DD}}{A_1 \cdot A_2 \cdot A_3} + A_{11} + 12 \cdot \frac{A_{DU}^2}{A_1 \cdot A_2 \cdot A_3} + A_{12} + A_{13} + A_{14}$$  \hspace{1cm} (16)

The great difference of MTTF-values of different architecture is shown in figure 5. These values are also extracted from industry.

5 Conclusion

The more safe 2oo4-architecture is established within high safety class computers nowadays. Such computers will be applied in various fields which require simultaneously both: availability and maximal safety. They are applied where human lives need to be protected and/or saved, either in material handling, energy production/distribution, process industry, pipelines, petrochemical, up and down stream process, in the medical field or industrial power plants.

As already mentioned in the introduction, today’s technical systems will be more and more complex. One will no longer be able to provide appropriate safety in processes which have to be monitored. Future safety control must support him, either in recording and analyzing data, or in operation resulting from this.

Advanced safety architectures like the introduced 2oo4-system have to be utilized in order to guarantee the required safety. The 2oo4-system combines the benefits of the 1oo2- and the 2oo3-system: simultaneously a higher availability and a higher safety than today’s systems. While the probability of a common cause failure is equal in all three system models, the probability of a normal failure in a 2oo4-system is several dimensions smaller than in a 2oo3-system. This is similar for the availability: a 2oo4-system possesses a higher availability than a 2oo3-system, because a 2oo4-system tolerates two failures, and a 2oo3-system only one failure.
References: