Sophisticated Calculation of the 1oo4-architecture for Safety-related Systems Conforming to IEC61508

A Hayek1, M Al Bokhaiti, M H Schwarz and J Boercsoek
Institute of Computer Architecture and System Programming
University of Kassel, Wilhelmshoher Allee 71, 34121 Kassel, Germany
E-mail: hayek@uni-kassel.de

Abstract. With the publication and enforcement of the standard IEC 61508 of safety related systems, recent system architectures have been presented and evaluated. Among a number of techniques and measures to the evaluation of safety integrity level (SIL) for safety-related systems, several measures such as reliability block diagrams and Markov models are used to analyze the probability of failure on demand (PFD) and mean time to failure (MTTF) which conform to IEC 61508. The current paper deals with the quantitative analysis of the novel 1oo4-architecture (one out of four) presented in recent work. Therefore sophisticated calculations for the required parameters are introduced. The provided 1oo4-architecture represents an advanced safety architecture based on on-chip redundancy, which is 3-failure safe. This means that at least one of the four channels have to work correctly in order to trigger the safety function.

1. Introduction
The design process of system architectures to control a safety related system in any technical field requires several aspects which have to be taken into account such as: system complexity, functional safety, reliability and availability. The standard IEC 61508 provides several measures and design methodologies as well as system architectures, which treat these aspects [1]. Basically, the key factor of enhancing reliability, safety and availability of a given system is the use of system redundancy and diagnosis elements. However, nowadays almost only approved architectures with the lowermost redundancy are used in safety-related systems such as the 1oo2-, 1oo3- and the 2oo3-architectures. There are various reasons for this: First, higher redundancy leads to more complex systems with increasing system costs and power consumption, which are two key factors for designing such systems. Second, the use of higher redundancy leads to more complex design issues such as synchronization and connectivity operations, which require additional components and highest verification and validation efforts. However, with the on-going miniaturization of semiconductor structures those reasons can be neglected. Nowadays a complete safety-related system can be integrated into a single silicon chip, which in turn reduces number of components, design area, cost and power consumption. Additionally, due to the intra-chip communication, a highest synchronization and connectivity operations can be achieved. Furthermore, a high testability can be achieved due to various sophisticated EDA-tools for verification and validation of electronic chips. Now the standards

1 To whom any correspondence should be addressed.
of designing a safety-related system with on-chip redundancy are available within the framework of IEC 61508 standard [2].

On the basis of the presented arguments, a concept for the realization of a safety controller based on a quadruple redundancy (1oo4-architecture) for use in steer-by-wire applications has been presented [3]. The benefits of this architecture are higher safety and higher reliability. In order to insert a higher availability to the proposed architecture a concept of degradability is introduced. Once a system failure is detected the failed system component will be excluded and the controller will be degraded to a 1oo3-architecture and so on to a 1oo2-architecture. However, this paper presents the proposed 1oo4-architecture as well as the sophisticated calculations of the required safety parameters. Section 2 briefly explains the necessary background on safety-related systems. In section 3 the proposed 1oo4-architecture is introduced. In section 4 the calculations of the probability distribution are presented. For that a fault-tree analysis and the calculation of the average probability of failure on demand (PFDavg) of the target architecture are introduced. In section 5 the Markov model of the 1oo4-architecture is presented, from which the mean time of failure (MTTF) is deduced. Section 6 includes the conclusion as well as a short analysis about the presented architecture.

2. Survey on safety related systems

Today’s control systems, which are used for safety critical applications, consist commonly of highly complex single components. These components can be implemented either as software or hardware. The generated hardware and software models of the complex system have to be evaluated with respect to different aspects like reliability and safety. Reliability is a mean for ensuring a function without any failure under all circumstances. Safety here means that the system will not get into a critical state even if a failure occurs. The process’s safe status refers to the status of no danger. If a failure occurs the system has to be able to reach the safe status.

The various functional, non-functional and safety-technical demands of 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) characterize the quality of a faultless system. The failure rate is the main parameter needed for the calculation of these parameters. The whole system’s failure rate \( \lambda \) is subdivided into safe failures and dangerous failures. In addition, safe failures are subdivided into safe undetected failures and safe detected failures. Whereas, dangerous failures are subdivided into dangerous undetected failures and dangerous detected failures. Figure 1 shows the distribution of failure rates. Failure rates could be specified with the aid of standard specifications.

![Figure 1. Failure rate distribution.](image-url)
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

Combining all elements of a system in a safety architecture, the system can be classified with a defined safety level, the so called safety integrity level (SIL). Table 1 shows various classifications of safety systems. The standard IEC 61508 defines two different criteria to classify safety systems into the individual safety levels.

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 the so called proof check interval $T_1$ as defined in table 1. This probability of failure is defined as “probability of failure on demand” (PFD). It has a dimension of 1 unit.

The standard IEC 61508 proposes a second possibility to classify a safety system. The probability that a failure occurs and leaves 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 (see table 1). The probability of failure is defined as probability of failure per hour (PFH). Unlike probabilities, it has a dimension of 1/h. Systems demanding continuous operations are highly significant for industrial systems. 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.

| Safety Integrity Level | Low demand mode of operation | High demand or continuous mode of operation |
|------------------------|-------------------------------|------------------------------------------|
|                        | $T_1 = 2$ years or $T_1 = 10$ years | $T_1 = 1$ month or $T_1 = 2$ months or $T_1 = 6$ months or $T_1 = 1$ year |
| 1                      | $10^{-2}$ to $10^{-1}$        | $10^{-6}$ to $10^{-5}$                  |
| 2                      | $10^{-3}$ to $10^{-2}$        | $10^{-7}$ to $10^{-6}$                  |
| 3                      | $10^{-4}$ to $10^{-3}$        | $10^{-8}$ to $10^{-7}$                  |
| 4                      | $10^{-5}$ to $10^{-4}$        | $10^{-9}$ to $10^{-8}$                  |

A system’s quality can be specified by defining its PFD value which is referred to its accuracy. The smaller this value is, the better the system is. The PFD value is calculated for a period of time called proof check interval $T_1$. After the maintenance of the system, we can assume that it will work without any failures. Judging and comparing systems is mostly specified by the PFD average value ($PFD_{AVG}$) over a whole proof check interval. The most known architectures are the 1oo2-, 1oo3- and 2oo3-architectures, which 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 availability is required a 2oo3-architecture has to be chosen. In order to take advantage of both systems in industry, a 2oo4-architecture has been developed [4, 5]. The 1oo4-architecture presented in the following section achieves a higher safety and reliability level. The degradability concept enhances the proposed architecture with higher availability.
3. 1oo4-architecture for safety related systems

The 1oo4-architecture is a safety architecture that normally consists of four independent channels. The four channels are interlinked in a way where only one channel is needed to resolve the safety function in order to carry out the safety function correctly. In figure 2 the block diagram of the 1oo4-architecture is given. A dangerous breakdown of the system is generated if three of the four channels have dangerous failures themselves. From the fault-tree-analysis [6], we can determine when the system can go to the dangerous non safety state:

- in each channel of the four channels there is a dangerous detectable failure due to a common cause
- in each channel of the four channels there is a dangerous undetectable failure which has a common cause
- in each channel of the four channels there is a dangerous detectable or a dangerous undetectable failure which all have no common cause.

Figure 2. Block diagram of the 1oo4-architecture.

Theoretically, the 1oo4-architecture is immediately transferred from the operation state into the safe state if a dangerous failure arises. However, due to its 3-failure-safety the 1oo4-archirctecture can definitively reach the safe state in contrast to a 2oo3-architecture. When a dangerous failure occurs then the faulty channel is switched off. Therefore, the 1oo4-architecture degrades to a 1oo3-architecture. In this new system it is still possible that another failure emerges. The system is in a defined state and it decides to go into the safe state. In 1oo2-architecture one of the two channels has to work correctly.
4. PFD-Calculation

In this paper the mathematical and statistical calculations for the safety analysis of the 1oo4-architecture has been evaluated. The measurement of the safety performance of the system in relation to the freedom of failures has been introduced through the average PFD calculation. Mathematically the average “Probability of Failure on Demand” (PFDavg) of the system is given by the arithmetic mean of the “probability of failure” {P(t)} in the interval [0, T]. The probability of failure of the ith channel P_i(t) is calculated using the following equation:

\[ P_i(t) = 1 - R_i(t) \]  \hspace{1cm} (1)

Where the reliability \( R_i(t) \) of ith channel is given by:

\[ R_i(t) = e^{-\lambda_i t} \]  \hspace{1cm} (2)

Under the condition:

\[ \lambda_i = \lambda_{Di} + \lambda_{Si} = \text{const.} \]  \hspace{1cm} (3)

Where:
- \( \lambda_i \): is the overall failure rate of the ith element
- \( \lambda_{Si} \): is the safe failure rate of the ith element
- \( \lambda_{Di} \): is the dangerous failure rate of the ith element

For the calculation of the average “probability of failure on demand” (PFDavg), only the value of \( \lambda_{Di} \) is required. As shown in figure 3, the 1oo4-architecture can fail dangerously in the following cases:

- A dangerous detected (DD) failure occurs in all channels as a result of a common cause failure

[Figure 3. Fault-tree-diagram of the 1oo4-architecture.]
• A dangerous undetected (DU) failure occurs in all channels as a result of common cause failure.
• In each channel either a (DD or DU) failure occurs as a result of non-common cause failure.

Therefore the total probability of failure is given by:

\[ P(t) = P_1(t) \cdot P_2(t) \cdot P_3(t) \cdot P_4(t) + P_{DUC}(t) + P_{DDC}(t) \]  
(4)

Where:
• \( P_1(t) = 1 - e^{-\lambda_{D1}t} \)
• \( P_2(t) = 1 - e^{-\lambda_{D2}t} \)
• \( P_3(t) = 1 - e^{-\lambda_{D3}t} \)
• \( P_4(t) = 1 - e^{-\lambda_{D4}t} \)
• \( P_{DUC}(t) = 1 - e^{-\lambda_{DU}t} \)
• \( P_{DDC}(t) = 1 - e^{-\lambda_{DD}t} \)

As it is shown in equation (4) the probability of failure \( P(t) \) comes from two types of failures. The first type is the failure due to a single failure in each channel either detected or undetected. The second type is the common cause failure due to “dangerous undetected” (DU) failure and “dangerous detected” (DD) failure. The average Probability of Failure on Demand \( PFD_{avg} \) is given by:

\[ PFD_{avg}(T) = \frac{1}{T} \int_0^T P(T)dt \]  
(5)

To calculate the \( PFD_{avg} \), first we do the calculation for the single failures and second for the common cause failures and then add the two result to find the “Probability of Failure on Demand” for the overall 1oo4-architecture (\( PFD_{avg,1oo4} \)).

4.1. Single failures
The probability of failure for dangerous undetected and dangerous detected failures for the 1oo4-architecture can be calculated as follows:

\[ P_{single}(t) = P_1(t) \cdot P_2(t) \cdot P_3(t) \cdot P_4(t) \]  
(6)

Compared to the common cause failures, the failures to be considered here are characterized as single failures. \( P(t) \) describes the probability of failure for the \( i \)th channel with failure rate of \( \lambda = \lambda_{D1} \) for dangerous single failure as it is given by equation (4). The probability of failure due to single failure will be as following:

\[
\begin{align*}
P_{single}(t) &= (1 - e^{-\lambda_{D1}t}) \cdot (1 - e^{-\lambda_{D2}t}) \cdot (1 - e^{-\lambda_{D3}t}) \cdot (1 - e^{-\lambda_{D4}t}) \\
&= (1 - e^{-\lambda_{D1}t} - e^{-\lambda_{D2}t} + e^{-(\lambda_{D1}+\lambda_{D2})t}) \cdot (1 - e^{-\lambda_{D3}t} - e^{-\lambda_{D4}t} + e^{-(\lambda_{D3}+\lambda_{D4})t}) \\
&= 1 - e^{-\lambda_{D1}t} - e^{-\lambda_{D2}t} - e^{-\lambda_{D3}t} - e^{-\lambda_{D4}t} + e^{-(\lambda_{D1}+\lambda_{D2})t} + e^{-(\lambda_{D3}+\lambda_{D4})t} \\
&\quad + e^{-(\lambda_{D1}+\lambda_{D3})t} + e^{-(\lambda_{D1}+\lambda_{D4})t} + e^{-(\lambda_{D2}+\lambda_{D3})t} + e^{-(\lambda_{D2}+\lambda_{D4})t} \\
&\quad + e^{-(\lambda_{D3}+\lambda_{D4})t} - e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D3})t} - e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D4})t} \\
&\quad - e^{-(\lambda_{D1}+\lambda_{D3}+\lambda_{D4})t} - e^{-(\lambda_{D2}+\lambda_{D3}+\lambda_{D4})t} + e^{-(\lambda_{D1}+\lambda_{D2}+\lambda_{D3}+\lambda_{D4})t}
\end{align*}
\]  
(7)
The function can be developed into a series with the help of MacLaurin series. In the case of 1oo4-architecture, to calculate the PFDavg it is sufficient to develop the first six terms plus the corresponding remaining terms $R_{6A}$, $R_{6B}$, $R_{6C}$, and $R_{6D}$, but only the first six terms will contribute to the result. The notation of the remaining terms can be described as:

- $R_{6A}$ is the sixth order remaining term which belongs to the exponential functions with the failure rate $\lambda = \lambda_{D1}, \lambda_{D2}, \lambda_{D3}$.
- $R_{6B}$ is the sixth order remaining term which belongs to the exponential functions with the failure rate $\lambda = \lambda_{D1} + \lambda_{D2}, \lambda_{D1}$.
- $R_{6C}$ is the sixth order remaining term which belongs to the exponential functions with failure rate $\lambda = \lambda_{D1} + \lambda_{D2}, \lambda_{D1} + \lambda_{D2}$.
- $R_{6D}$ is the sixth order remaining term which belongs to the exponential function with failure rate $\lambda = \lambda_{D1} + \lambda_{D2} + \lambda_{D3}$.

The remaining previous terms converges at $T = 0$ to the zero value and they are very small compared to the six terms when building the limit value at $T = 0$. The power series with six terms and remainder for the function $f(t) = e^{-\lambda t}$ will be as following:

$$
e^{-\lambda t} = 1 - \lambda \cdot T + \frac{\lambda^2 \cdot T^2}{2} - \frac{\lambda^3 \cdot T^3}{6} + \frac{\lambda^4 \cdot T^4}{24} - \frac{\lambda^5 \cdot T^5}{120} + R_6$$

Every exponential function in equation (8) should be replaced by the above series with the exception of the remainder term with:

$$\lim_{T \to 0} (R_{6A}) = \lim_{T \to 0} (R_{6B}) = \lim_{T \to 0} (R_{6C}) = \lim_{T \to 0} (R_{6D}) = 0$$

$$\therefore PFD_{avg, single}(T) = \frac{1 - \lambda_{D1} \cdot T + \frac{\lambda_{D1} \cdot T^2}{2} - \frac{\lambda_{D1} \cdot T^3}{6} + \frac{\lambda_{D1} \cdot T^4}{24} - \frac{\lambda_{D1} \cdot T^5}{120} + R_6}{\lambda_{D1} \cdot T}$$
The previous equation can be further simplified to get the PFD\textsubscript{avg,single}(T) of 1004-architecture which will be as following:

\[
PFD\textsubscript{avg,single}(T) = \frac{24\lambda_D}{120} \lambda_D^2 \lambda_D^2 \lambda_D^2 \lambda_D^4 T^4
\]  

(11)

If the failure rates of the redundant channels are equal \((\lambda_D = \lambda_{D1} = \lambda_{D2} = \lambda_{D3} = \lambda_{D4})\) then:

\[
\therefore PFD\textsubscript{avg,single}(T) = \frac{24\lambda_D^4}{120} T^4
\]  

(12)

With
\[
\frac{T_4}{120} = t_{CE} \cdot t_{GE} \cdot t_{SE}
\]  

(13)

Where (see [4]):

- \(t_{CE}\): channel equivalent mean down time.
- \(t_{GE}\): group equivalent mean down time.
- \(t_{SE}\): system equivalent mean down time.

And they are given by:

\[
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left( T_1 + \frac{T_2}{2} \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}
\]  

(14)

\[
t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left( T_1 + \frac{T_2}{3} \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}
\]  

(15)

\[
t_{SE} = \frac{\lambda_{DU}}{\lambda_D} \left( T_1 + \frac{T_2 + T_3}{4} \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}
\]  

(16)

Where:

- \(\lambda_D\): Dangerous failure rate.
- \(\lambda_{DU}\): Dangerous undetected failure rate.
- \(\lambda_{DD}\): Dangerous Detected failure rate.
- \(T_i\): Time interval.
- \(\text{MTTR}\): Mean Time to Failure.

Equation (12) can be rewritten as:

\[
PFD_{\text{avg single}}(T) = 24 \cdot \lambda_D \cdot t_{CE} \cdot t_{GE} \cdot t_{SE}
\]  

(17)

It is also possible to write for \(\lambda_D\):

\[
\lambda_D = (1 - \beta_D) \cdot \lambda_{DD} + (1 - \beta) \cdot \lambda_{DU}
\]  

(18)

With

\[
\lambda_D = \lambda_{DD} + \lambda_{DU}
\]  

(19)

Where:

- \(\beta\)- factor qualifies the effect of failures with a common cause.
- \(\beta_D\)- factor for detected dangerous failures that have a common cause.
If we substitute the value of $\lambda_3$ as it is given in equation (18), then the average probability of failure on demand of 1oo4-architecture due to single failures is given as:

$$PFD_{\text{avg single}}(T) = 24 \cdot [(1 - \beta_D) \cdot \lambda_{DD} + (1 - \beta) \cdot \lambda_{DU}]^4 \cdot \hat{t}_{CE} \cdot \hat{t}_{GE} \cdot \hat{t}_{SE}$$  \hspace{1cm} (20)

4.2. Common-cause failures

In the same manner we can calculate the PFD_{avg} for common cause failures which will be as following [4]:

$$PFD_{\text{avg} \beta} = \lambda_D \cdot t_{CE \beta} = \beta \cdot \lambda_{DU} \cdot \left[ \frac{T_1}{2} + \text{MTTR} \right] + \beta_D \cdot \lambda_{DD} \cdot \text{MTTR}$$ \hspace{1cm} (21)

Where $t_{CE \beta}$ is the channel equivalent mean down time and is given by:

$$t_{CE \beta} = \beta \cdot \frac{\lambda_{DU}}{\lambda_D} \left[ \frac{T_1}{2} + \text{MTTR} \right] + \beta_D \cdot \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}$$ \hspace{1cm} (22)

Where:

- $\lambda_D$: Dangerous failure rate.
- $\lambda_{DU}$: Dangerous undetected failure rate.
- $\lambda_{DD}$: Dangerous Detected failure rate.
- $T_1$: Time interval.

By adding equations (20) and (21), then we can calculate the PFD_{avg} for the 1oo4-architecture.

$$PFD_{\text{avg} \ 1oo4} = 24 \cdot [(1 - \beta_D) \cdot \lambda_{DD} + (1 - \beta) \cdot \lambda_{DU}]^4 \cdot \hat{t}_{CE} \cdot \hat{t}_{GE} \cdot \hat{t}_{SE} + \beta \cdot \lambda_{DU} \cdot \left[ \frac{T_1}{2} + \text{MTTR} \right] + \beta_D \cdot \lambda_{DD} \cdot \text{MTTR}$$ \hspace{1cm} (23)

5. MTTF-calculation

5.1. Markov Model

As we have seen in the fault tree diagram in figure 3, the 1oo4-architecture has fourteen failure combinations. Each combination can be represented as a system state, so we have fourteen states. If we add to the previous states the safe state which is the de-energized state, and the start state (no failure), then the total number of states for the 1oo4-architecture will be sixteen states. The system will transfer from one state to another according to the failure type of its channels. This kind of transformation depends only on the current state of the system. In other words the future state of the system is independent of the past states given the current state. The previous transition method satisfies the Markov property which states that the next outcome of the experiment depends only on the current outcome. Therefore the 1oo4-architecture states can be considered as a Markov chain where the transition probability from state $j$ to state $k$ after a time period of $dt$ is given by:

$$P(S_j \rightarrow S_k) = P_{jk} = \lambda_{jk} \cdot dt$$ \hspace{1cm} (24)
Where: $\lambda_{jk} \geq 0$.

If $\lambda_{jk} = 0$, then the transition from state $j$ to state $k$ is impossible. In this case the system doesn’t change its state within the time interval $dt$. The transition probability is this case will be defined as:

$$P(S_j \to S_j) = P_{jj} = 1 - \sum_{k=1}^{n} \lambda_{jk} \cdot dt$$  \hspace{1cm} (25)$$

Where: $j = 0,1,2,\ldots,n$; $k = 0,1,2,\ldots,n$; $k \neq j$

The summation in equation (25) can be described as:

$$\sum_{k=1}^{n} \lambda_{jk} = \lambda_{jj}$$  \hspace{1cm} (26)$$

Where: $j = 0,1,2,\ldots,n$; $k = 0,1,2,\ldots,n$; $k \neq j$

$$\therefore P(S_j \to S_j) = P_{jj} = 1 - \lambda_{jj}$$  \hspace{1cm} (27)$$

Where: $j = 0,1,2,\ldots,n$; $k = 0,1,2,\ldots,n$; $k \neq j$

The state space $S$ of the 1oo4-architecture is a finite space and consists of sixteen possible states.

$$S \triangleq \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$$

The transition probabilities can be collected in a matrix called transition matrix $P$.

$$P = \begin{bmatrix} P_{00} & P_{01} & \cdots & P_{015} \\ P_{10} & P_{11} & \cdots & P_{115} \\ \vdots & \vdots & \ddots & \vdots \\ P_{150} & P_{151} & \cdots & P_{1515} \end{bmatrix} = \begin{bmatrix} 1 - \lambda_{00} \cdot dt & \lambda_{01} \cdot dt & \cdots & \lambda_{015} \cdot dt \\ \lambda_{10} \cdot dt & 1 - \lambda_{11} \cdot dt & \cdots & \lambda_{115} \cdot dt \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{150} \cdot dt & \lambda_{151} \cdot dt & \cdots & 1 - \lambda_{1515} \cdot dt \end{bmatrix}$$  \hspace{1cm} (28)$$

The previous state space with the transition probabilities between them can be represented by a very convenient short-hand visual representation called the state transition diagram of the Markov chain. Figure 4 shows the state transition diagram of the 1oo4-architecture.
As we have seen in the previous figure, at state 0 all the channels are working properly without failures. State 1 is the de-energized state which is called safe state. The system transfers from state 0 to state 1 if a safe failure occurs. The transition rate will be \( 4\lambda_s \), because each channel of the 1oo4-architecture will face a safe failure with a transition rate equal to \( \lambda_s \).

In the case of a dangerous detected failure, the system will transfer to a new state, where the transition rate depends on the number of channels which are still working properly without failures. For the first, second, third, and fourth dangerous failures occurrence, the transition rate will be \( 4\lambda_{DD} \), \( 3\lambda_{DD} \), \( 2\lambda_{DD} \), and \( \lambda_{DD} \) respectively. In those states with a dangerous detected failure the system have two possibilities:

- The first one is the ability to detect the failure within the test interval \( \tau_{test} \). If this happens, then the system will transfer from the current state to the safe state “state 1”. The transition rate in this case will be given by:

\[
\mu_0 = \frac{1}{\tau_{test}}
\]  

- The second possibility is the possibility of occurrence a further dangerous failure before the detection of the previous failure. If this happens, then the system will transfer to a new state. The transition to the new state will depend on the failure type either dangerous detected or dangerous undetected.

In case of a dangerous undetected failure, the system will transfer to a new state where the transition rate depends on the number of channels which are still working properly without failures. For the first, second, third and fourth dangerous failure occurrence, the transition rate will be \( 4\lambda_{DU} \), \( 3\lambda_{DU} \), \( 2\lambda_{DU} \), and \( \lambda_{DU} \) respectively. In those states with a dangerous undetected failure the system have also two possibilities:
• The first one is the ability to work with the remaining operating channels if there is no additional failure within the lifetime $\tau_{LT}$. The system will return to the state 0 after lifetime $\tau_{LT}$ with a transition probability given by:

$$\mu_{LT} = \frac{1}{\tau_{LT}}$$  \hfill (30)

• The second possibility is the possibility of occurrence an additional dangerous failure within the lifetime $\tau_{LT}$. In this case the system will transfer to a new state according to the failure type.

In case of common cause dangerous detected failures which affect all the channels, the system will transfer directly from state 0 to state 11. The transition rate in this case is equal to $\beta \cdot \lambda_{DD}$, where $\beta$ is the weighted factor of detected dangerous failures that have a common cause. The system can transfer to the safe state if the failures are detected within the test interval $\tau_{test}$. The transition rate is then equal to $\mu_0$. If common cause dangerous undetected failures affect the system, then the system will transfer directly from state 0 to state 15. The transition rate in this case is equal to $\beta \cdot \lambda_{DU}$. In this case the system can be returned to the state 0 only after lifetime $\tau_{LT}$.

5.2. MTTF Calculation

From the Markov model of the 1oo4-architecture, the following probability of failure matrix exists:

$$P = \begin{bmatrix} P_1 & P_2 \\ P_3 & P_4 \end{bmatrix}$$  \hfill (31)

$$P_2 = \begin{bmatrix}
1 - A_1 \cdot \text{dt} & 4 \cdot \lambda_4 \cdot \text{dt} & 4 \cdot \lambda_{DD} \cdot \text{dt} & 4 \cdot \lambda_{DU} \cdot \text{dt} & 0 & 0 & 0 & 0 \\
\mu_8 \cdot \text{dt} & 1 - \mu_8 \cdot \text{dt} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mu_5 \cdot \text{dt} & 1 - A_2 \cdot \text{dt} & 0 & 3 \cdot \lambda_{DD} \cdot \text{dt} & 3 \cdot \lambda_{DU} \cdot \text{dt} & 0 & 0 \\
\mu_{LT} \cdot \text{dt} & 0 & 0 & 1 - A_3 \cdot \text{dt} & 0 & 3 \cdot \lambda_{DD} \cdot \text{dt} & 3 \cdot \lambda_{DU} \cdot \text{dt} & 0 \\
0 & \mu_6 \cdot \text{dt} & 0 & 0 & 1 - A_4 \cdot \text{dt} & 0 & 0 & 2 \cdot \lambda_{DU} \cdot \text{dt} \\
\mu_{LT} \cdot \text{dt} & 0 & 0 & 0 & 0 & 1 - A_5 \cdot \text{dt} & 0 & 0 \\
0 & \mu_7 \cdot \text{dt} & 0 & 0 & 0 & 0 & 1 - A_6 \cdot \text{dt} & 0 \\
0 & \mu_9 \cdot \text{dt} & 0 & 0 & 0 & 0 & 0 & 1 - A_7 \cdot \text{dt}
\end{bmatrix}$$  \hfill (32)

Where:

- $A_1 = 4 \cdot \lambda_4 + 4 \cdot \lambda_{DD} + 4 \cdot \lambda_{DU} + \beta D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU}$
- $A_2 = \mu_0 + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU}$
- $A_3 = \mu_{LT} + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU}$
- $A_4 = \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$
- $A_5 = \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$
- $A_6 = \mu_{LT} + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$
- $A_7 = \mu_0 + \lambda_{DD} + \lambda_{DU}$
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 1oo4-architecture in the states 0, 2, 3, 4, 5, 6, 7, 8, 9, and 10. The states 1, 11, 12, 13, 14, and 15 are not considered during the MTTF calculation, because they are absorbing states. The Q matrix results from the:

- 1st row with the elements in the 1st, 3rd, 4th, 5th, 6th, 7th, 8th, 9th, 10th, and 11th columns.
- 3rd row with the elements in the same previous columns.
- 4th, 5th, 6th, 7th, 8th, 9th, 10th, and 11th rows with the elements of the previously mentioned columns.

For the considered Markov model applies \( \tau_{LT} = \infty \)

\[ \therefore \mu_{LT} = \frac{1}{\tau_{LT}} = 0 \]
Therefore the Q-matrix has the following form:

\[
Q = \begin{pmatrix}
1 - A_{c, dt} & 4 \cdot \beta_{D} \cdot dt & 4 \cdot \lambda_{D} \cdot dt & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 - A_{d, dt} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 - A_{e, dt} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\]

\[
M = I - Q = \begin{pmatrix}
A_{1} & -4 \cdot \lambda_{D} & -4 \cdot \lambda_{D} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & A_{2} & -3 \cdot \lambda_{D} & -3 \cdot \lambda_{D} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & A_{3} & 0 & -3 \cdot \lambda_{D} & -3 \cdot \lambda_{D} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & A_{4} & 0 & 0 & -2 \cdot \lambda_{D} & -2 \cdot \lambda_{D} & 0 \\
0 & 0 & 0 & 0 & 0 & A_{5} & 0 & 0 & -2 \cdot \lambda_{D} & -2 \cdot \lambda_{D} \\
0 & 0 & 0 & 0 & 0 & 0 & A_{6} & 0 & 0 & -2 \cdot \lambda_{D} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{7} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{8} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{9} \\
\end{pmatrix}
\]

In order to derive the MTTF value, we need to compose the so called N-matrix. The N-matrix is the inverse of the M-matrix \( N = M^{-1} \)

\[
N = \begin{pmatrix}
0 & \frac{1}{A_{1}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{A_{2}} & 0 & 2 \cdot \lambda_{D} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \frac{1}{A_{3}} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{A_{4}} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{A_{5}} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{A_{6}} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{A_{7}} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\]

The MTTF value is the mean value of the time interval between two successive failures. Let’s assume that the starting state is state 0, which is the state of failure free operation. The elements of the N-matrix are time dependent values. If we want to calculate the MTTF value, then we can simply sum the elements of the first row. The MTTF value of the 1004-architecture will be:

\[
MTTF_{1004} = \frac{1}{A_{1}} + \frac{4 \cdot \lambda_{D}}{A_{1} \cdot A_{2}} + \frac{4 \cdot \lambda_{D}}{A_{1} \cdot A_{3}} + \frac{12 \cdot \lambda_{D}^{2}}{A_{1} \cdot A_{2} \cdot A_{4} \cdot A_{5} \cdot A_{6} \cdot A_{7}} + \frac{24 \cdot \lambda_{D}}{A_{1} \cdot A_{2} \cdot A_{3} \cdot A_{4} \cdot A_{5} \cdot A_{6} \cdot A_{7}}
\]

6. Conclusion and future prospects

In this paper the 1004-architecture for safety-related systems and the calculation of its parameters were presented. The proposed architecture is targeted to be used in automotive applications and can also be targeted to be used in computer systems where higher safety, reliability and availability are required.
Such computer systems are applied where human life need to be protected and/or saved, either in material handling, energy production/distribution, process industry, pipelines, petrochemical, 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 for the processes which has to be monitored. Future safety control systems must support us, either in recording and analyzing data, or by perform the necessary operations according to the recorded data to avoid hazards.

Advanced safety architectures like the introduced 1oo4-architecture have to be utilized in order to guarantee the required safety. The degradable 1oo4-architecture combines the safety feature of the 1oo2- and 1oo3-architectures and the availability feature of the 2oo3- and 2oo4-architectures. So, we will get higher reliability and at the same time higher safety than what we have gotten in today’s systems. While the probability of common cause failure is equal in all system models, the probability of a single failure in the 1oo4-architecture is several times smaller than those values which we got in the mentioned architectures. Due to the degradable concept the 1oo4-architecture, it also offers a high availability.

References

[1] IEC Commission 2001 *Functional Safety of electrical/electronic/programmable/ electronic safety-related systems-IEC 61508 part 1-7*, (Geneva: CENELEC)

[2] IEC Commission 2010 *Functional Safety of electrical/electronic/programmable/ electronic safety-related systems-IEC 61508 part 1-7*, (Geneva: CENELEC)

[3] Boercsoek J, M H Schwarz, E Ugljesa, P Holub and A Hayek 2011 *High-Availability Controller Concept for Steering Systems: The Degradable Safety Controller* (Tenerife: WSEAS Conference)

[4] Boercsoek J 2007 *Electronic Safety System, Hardware Concepts, Models and Calculation* 2nd Ed. (Heidelberg: Huethig Verlag)

[5] Boercsoek J 2007 *Functional Safety: Basic Principles of Safety-Related Systems* (Heidelberg: Huethig Verlag)

[6] Vesley W E et al. 2011 *Fault Tree Handbook. Nuclear Regulatory Commission NUREG–0492* http://www.nrc.gov/reading-rm/doc/collections/nuregs/staff/sr0492/sr0492.pdf