Consideration of Common Cause Failures in Safety Systems

BÖRCSÖK J.\textsuperscript{1, 2}, HOLUB P.\textsuperscript{1, 2}

\textsuperscript{1} Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel
GERMANY

http://www.uni-kassel.de

\textbf{Abstract:} - Systems in which failure could endanger human life are termed safety-critical. The SIS (Safety Instrumented System) should be designed to meet the required safety integrity level as defined in the safety requirement specification. Moreover, the SIS design should be performed in a way that minimizes the potential for common mode or common cause failures (ccf). The ccf are the biggest part when calculating the probability of failure for redundant safety integrity systems. A ccf can occur, when a random hardware failure leads to a failure of several components. There are several methods to calculate the probability of ccf, which will be shown in this paper. The ccf ratio for the calculation of the overall probability of failure is defined with the beta-factor.

\textbf{Key-Words:} - Common cause failure, Probability of failure on demand, beta-factor-model, multi parameter model, IEC 61508

\section{1 Introduction}

A safety-related system that fulfills functional safety requirements reduces the risk, which comes from the equipment under control (EUC). The danger for people, environment or machine via an EUC will be appraised through a risk analysis, e.g. with the help of a risk graph, a fault tree analysis, a Markov analysis or with a semi-quantitative method such as LOPA (layer of protection analysis). How small the residual risk shall be will be defined, on the one hand, by the organisation itself – at this point each individual will ask himself whether he is ready to accept that risk or not – and, on the other hand, will be influenced by the production availability. The art of the engineer consists then in implementing appropriate safety architectures, which would permit reducing the conflict between the requirements according to high safety, equivalent with small residual risk, and high production availability, which exists in most of the systems implemented up to now.

Fault tolerance is a particular technique that allows building systems that preserve the delivery of their expected service despite the presence of errors caused by faults within the system itself. Redundancies can be classified into four types:

- time redundancy
- hardware redundancy
- software redundancy
- information redundancy

In the case of hardware redundancy the system is provided with more hardware components (e.g. channels) than it would need if the hardware were perfect. Upon failure of a hardware component (or channel) a spare one is switched in. In the case of software redundancy the system may be provided with different versions of tasks. In the case of time redundancies the scheduler has some extra time so that some tasks can be rerun and still meet deadlines. In the case of information redundancies data are coded in such a way that a certain number of bit errors can be detected and/or recovered. A fault tolerant system will only fail if multiple failure events happen.

The optimised safety system offers an architecture having the two following criteria:

- The safety system has a hardware-fault-tolerance of equal or greater to two. It means that the equipment under control EUC- system, will run to a safe state after at least two faults in the safety system has occur. 1 Thereby the production availability will be guarantee.
- In safety systems two independent channels must always exist, which properly function so that, if in one or several channels dangerous failure occur, the EUC system will be driven in a safe state.

These criteria guarantee the safety. The disadvantages of such a redundant structure, which by mono channels structures, with which a very small residual risk can

\textsuperscript{1} A hardware fault tolerance of $N$ means that $N + 1$ faults could cause a loss of the safety function \cite{1}.
definitely be achieved, do not occur according to the construction, are however:

- A higher grade of the design – this will have at a later stage, consequence during the assembling, the commissioning and the maintenance of the system.
- The observance and valuation of an additional failure source, the so-called common cause failure (ccf), during the risk analysis.

This ccf, which by mono-channel structures do not occur according to the construction, constitute for redundant structures the main part of safety integrity systems (SIS) during the calculation of the probability of failure on demand. However, this does not mean, that mono-channel systems, due to the not existing ccf, have a smaller failure probability. On the contrary, through the ccf one part of the failures, which also occur in mono-channel systems, will be evaluated with a weighted factor smaller as one. Should a ccf occurs the whole architecture would be affected. Whereas in mono-channel systems, only single failures (also called normal failures) can occur, failures in a redundant system can be divided in single and ccf, see figure 1 [1], [4]. Another often-used presentation is shown in figure 2. Here both individual channels’ single failures make the failures’ intersection in a redundant system. Those are the ccf [1], [5], [6]. The evaluation of the ccf depends on the chosen model. Hence, in this paper, different models will be presented and the results will be compared with one another after calculating the failure probability.

![Fig. 1. Reliability block diagram for a single channel (left) and a redundant system architecture (right). \( \lambda_1 \) and \( \lambda_1 \) are single failure rates, \( \lambda_2 = \text{ccf rate.} \)](image)

![Fig. 2. Relationship between single failures and ccf in a redundant system [1], [2], [5].](image)

2 Systematic and random failures

In all standard frequently used to functional safety, one finds the classification of failures in systematic and random failures.

A random hardware failure means (according to def. out of [1]) a „failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.” A systematic failure will be in [1] defined as a “failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors”.

Should random hardware failure exist, it is possible to consider the probability with the help of random failure rates and to calculate the probability of failure. Systematic failures exist continuously in a system. They depend on special event, such as function processes and environmental conditions. The occurrence probability cannot be calculated with methods to define the probability but at the most, generally very inexactly and subjective averaged. To guarantee the functional safety, random as well as systematic failures will have to be control or prevent from happening. There, amongst others, a systematic and controlled developed process will be used as well as the use of guaranteed safety principles during the design and the realisation. Failure tolerance, automatic fault detection and the ability when acknowledging a failure to react are part of it.

As long as one deals with hardware failures [1], [2], [3] synonym concepts, such as physical failure, independent failure [2] or aging failure [3] can be found in the Norms. For the concept common cause failure, it will be a bit more complicated. Generally assumed is the fact that dependent failures are ccf. Depending on the cause of a ccf, a ccf can present a systematic failure [1], [2], [3] as well as a random hardware failure [1], [2]. To the ccf as systematic failures belong stress failure [3], design failure [1], [2], [3] and interaction failure [1], [2], [3]. Here attention should be paid to the fact that the stress failure in [1] and [2] can be caused through physical failure and thereby belong to the random hardware failures. Hence, in [1] and [2] the ccf caused though stress can be calculated with the help of a random hardware failure rate. Should however ccf exist in form of design failures or interaction failures, then they will be detected via the life-cycle-management system, which is in [1], one of the central points during the evaluation of functional safety. In order to calculate design or interaction failures In [2] and [3], one will introduce an additional parameter for the systematic failure rates. This parameter can however only be averaged after long-time experience and the results are thus not always comparable, if the relevant data are unknown! For the random hardware failure rate however exist worldwide.
databank with comparable values, see [14] - [17], whereupon attention must also be paid for environmental conditions whose values account. Mentionable is, that in [3] the stress failures can also be calculated with the help of random hardware failure rate. In the following models the relevant data, which are the cause of ccf physical failures, and that therefore the probability of failure of ccf can be calculated with the help of random hardware failure rates.

3 Models of CCF
The different models can be distinguished and separated into categories according to the number of parameters:

- **Single-parameter:** $\beta$-factor model which produces conservative results for high redundancy systems
- **Multi-parameter:** provides a more realistic assessment of ccf frequencies for redundancy levels higher than two.

or into categories depending on how multiple failures occur:

- **Shock models:** the binomial failure rate model which assumes that the system is subject to a common cause ‘shock’ at a certain rate. The common cause failure frequency is the product of the shock rate and the conditional probability of failure, given a shock.
- **Non-shock models**
  - Direct: use the probabilities of common events directly (Basic parameter model)
  - Indirect: estimate probabilities of common cause events through the use of other parameters.

3.1 Basic parameter model
This model makes use of the rare events approximation

$$P(S) = P(A_I) \cdot P(B_I) + P(A_I) \cdot P(C_I) + P(B_I) \cdot P(C_I) + P(C_{AB}) + P(C_{AC})$$

under the following assumptions:

- The probability of similar events involving similar types of components are the same
- Symmetry assumption: the probability of failure of any given basic event within a common cause component group depends only on the number and not on the specific components in that basic event.

$$P(A_I) = P(B_I) = P(C_I) = Q_I$$
$$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2$$
$$P(C_{ABC}) = Q_3$$

(2)

$$Q_I = Q_I + 2 \cdot Q_2 + Q_3$$
$$Q_S = 3 \cdot Q_1^2 + 3 \cdot Q_2 + Q_3$$

This equation is calculated for a 2oo3-system.

$$Q_I = \sum_{k=1}^{m} \left( \frac{m!}{k! (m-k)!} \right) Q_k$$

(3)

Ideally, the $Q_k$ values can be calculated from data. Unfortunately, all data are normally not available. Other models have been developed that put less stringent requirements on the data. This is only done at the expense of making additional assumptions that address the incompleteness of the data.

3.2 Beta factor model
It models dependent failures of two types:
- intercomponent physical interactions and
- human interactions.

The model assumes that $Q_o$, the total probability failure for each component, can be expanded into an independent, $Q_I$, and a dependent, $Q_m$ contribution; where $m$ is the number of components in the common cause group (in other words, the common cause failure is such to fail all $m$ components in the group). All $Q_k$’s are then 0 except $Q_I$ and $Q_m$:

$$Q_I = Q_I + Q_m$$

(4)

A parameter $\beta$ is defined as the fraction of the total failure probability attributable to dependent failures:

$$\beta = \frac{Q_m}{Q_I} = \frac{Q_m}{(Q_I + Q_m)}$$

$$\Rightarrow Q_m = \beta \cdot Q_I$$

$$\Rightarrow Q_I = (1 - \beta) \cdot Q_t$$

(5)

For a system with 2 out of 3 logic:

$$Q_S = 3 \cdot (1 - \beta)^2 \cdot Q_t^2 + \beta \cdot Q_t$$

(6)

For a system with more than two units, the $\beta$-factor model does not provide a distinction between different numbers of multiple failures. Thus, simplification can lead to conservative predictions when it is assumed that all units fail when a common-cause failure occurs. The
strength of the \( \beta \)-factor model lies in its direct use of field data and its flexibility. The total component failure probability \( Q_t \) and \( \beta \) have to be estimated. For time distributions of failure probabilities:

\[
\beta = Q_m / Q_t = (1 - \exp(-\lambda_m \cdot t))/(1 - \exp(-\lambda_t \cdot t)) \approx \lambda_m / \lambda_t
\]  

(7)

3.3 Multiple Greek letters model

The following equation allows to compute the probability of common cause failures of order \( k \) (if \( m - 1 \) parameters):

\[
Q_k = \frac{1}{m-1} \left( \frac{k}{k-1} \right) \cdot \left( 1 - \rho_{k+1} \right) \cdot Q_t
\]  

(8)

\( \rho_2 = \beta \): conditional probability of the failure of at least one additional component, given that one has failed

\( \rho_3 = \gamma \): conditional probability of the failure of at least one additional component, given that two have failed

\( \rho_4 = \delta \): conditional probability of the failure of at least one additional component, given that three have failed.

3.4 \( \alpha \)-factor model

The following equation with \( m \) parameters hold:

\[
\alpha_k^{(m)} = \frac{m \cdot Q_k^{(m)}}{\sum_{k=1}^{m} \left( \frac{m}{k} \right) \cdot Q_k^{(m)}}
\]  

(9)

with normalization:

\[
\sum_{k=1}^{m} \alpha_k^{(m)} = 1
\]  

(10)

The equation becomes

\[
Q_k^{(m)} = \frac{k}{m-1} \cdot \frac{\alpha_k^{(m)}}{\alpha_1} \cdot Q_t
\]  

(11)

with \( k = 1, 2, \ldots m \) and

\[
Q_t = \sum_{k=1}^{m} k \cdot \alpha_k
\]  

(12)

3.5 Binominal failure rate (BFR) model

Consider a system composed of \( m \) identical components. Each component can fail at random times, independently of each other, with failure rate \( \lambda \). Furthermore, a common cause shock can hit the system with occurrence rate \( \mu \). Whenever a shock occurs, each of the \( m \) individual components may fail with probability \( p \), independent of the states of the other components. The term “binomial” failure rate is used because the number \( I \) of individual components failing. As a consequence, the shock is therefore binomially distributed with parameters \( m \) and \( p \):

\[
p(I = i) = \binom{m}{i} \cdot p^i \cdot (1 - p)^{m-i}
\]  

(13)

with \( i = 0, 1, \ldots, m \).

Two conditions are further assumed:

- Shocks and individual failures occur independently of each other
- All failures are immediately discovered and repaired, with negligible repair time

The assumption that a component fails independently is often not satisfied, in practice. The problem can, be remedied by defining one fraction of the shocks as being “lethal shocks”, namely shocks that automatically cause all the components to fail (\( p = 2 \)). If all the shocks are lethal, one is back to the \( \beta \)-factor model. Observe that the case \( p = 1 \) corresponds to the situation that there is no built-in protection against these shocks. The BFR model differs from the \( \beta \)-factor model in that it distinguishes between the numbers of multiple-unit failures in a system with more than two units:

\[
\lambda_i = m\lambda + \mu \left( \binom{m}{i} p^i \cdot (1 - p)^{m-i} \right)
\]  

Failure rate of one unit

\[
\lambda_i = m\lambda + \mu \left( \binom{m}{i} \right)
\]  

Failure rate of \( i \) units, \( i = 2, \ldots, m \)

(14)

Three parameters \( \lambda, \mu \) and \( p \) need to be estimated.
4 Basic Beta-Factor Model

The Basic Beta-Factor Model, which has already been introduced in 1974 by K. N. Fleming [7], describes the correlation between the independent, random hardware failures and the dependent failure, of the ccf, in a redundant system. Thereby the following data are relevant:

- The redundant system consists of identically constructed redundant components.
- The ccf finds its origins in a physical failure, which can be described with a method of probability, the random hardware failure rate.

The calculated values for the \( \beta \)-factor averages ca. over 0 and 25 % [5], [18]. Once the \( \beta \)-factor has been defined, then the ratio of the independent failure \( \lambda_i \) divided by

\[
\lambda_i = (1 - \beta) \cdot \lambda
\]  

and the ratio for ccf \( \lambda_{CCF} \) divided by

\[
\lambda_{CCF} = \beta \cdot \lambda
\]

with

\[
\lambda = \lambda_i + \lambda_{CCF}
\]

will be determined.

The general valid equation for the failure probability will be calculated for \( n \) redundant channel out of the sum of the failure probabilities \( PFD_{single} \) for single failure and \( PFD_{CCF} \) for ccf:

\[
PFD = PFD_{single} + PFD_{CCF} = \left[ (1 - \beta) \cdot \lambda \cdot t \right]^n + \beta \cdot \lambda \cdot t^n
\]

A derivation of this equation can be found for example in [6]. Should for example a 1oo3-system with \( n = 3 \) redundant components exists, then the diagram calculated in figure 5 will be obtained. Thereby is assumed that the beta-factor varies between 0 and 1.0, a basic failure rate from \( \lambda = 1E-07 \) 1/h and a time interval \( t \), that averages between 1 and 10 years.

The calculation shows – as it can also be seen in figure 5 – that it is necessary to take the ccf into consideration, as well as the fact that the \( PFD_{ccf} \)-ratio is clearly bigger than the \( PFD_{single} \). A \( \beta = 0.0 \) means, that an ideal redundant exist, in which no ccf occur. This is unrealistic in practice! However, if one give \( \beta = 1.0 \) in eq. 4, one obtains the probability of failure for a 1oo1-system. Therefore, as a comparison, the upper curve (\( \beta = 1 \)) shows how, despite ccf, the introduction of a redundant system improves the \( PFD \)-value. Eq. 18 shows, that the \( PFD \)-value for ccf does not depend on the amount of redundant components. The graph in figure 4 underneath is therewith generally valid for redundant architecture, see figure 3.
dangerous undetected and a beta-factor both norms, of safe and dangerous failure rates. To the reason why in this model both a beta-factor dangerous undetected random hardware failure. This is which a ccf can occur via dangerous detected as well as undetected. Both standards describe a ccf-model, in be detected, the other part remains dangerous related system, then one part of the dangerous failure can automatic diagnostics tests be implemented in the safety-dangerous failure rates are relevant [19]. Should calculate the probability of failure only the latter formula given in the standards.

The correlation between these two beta-factors can be calculated via a checklist with variables and the dangerous detected failures is required. Both beta-factors and ISA TR84.00.02 different places, which could lead during a wrong application to far too optimistic results.

The basis failure rate \( \lambda_D \) consists, in accordance with both norms, of safe and dangerous failure rates. To calculate the probability of failure only the latter dangerous failure rates are relevant [19]. Should automatic diagnostics tests be implemented in the safety-related system, then one part of the dangerous failure can be detected, the other part remains dangerous undetected. Both standards describe a ccf-model, in which a ccf can occur via dangerous detected as well as dangerous undetected random hardware failure. This is the reason why in this model both a beta-factor \( \beta_D \) for the dangerous undetected and a beta-factor \( \beta_0 \) for the dangerous detected failures is required. Both beta-factors can be calculated via a checklist with variables and the formula given in the standards.

The correlation between these two beta-factors should be shown as an example for a 1oo2-system. The equation for the probability of failure of a 1oo2-system is (derivation see [5]):

\[
P(t) = P_1(t) \cdot P_2(t) + P_{DUC}(t) + P_{DDC}(t) \tag{19}
\]

Thereby the product for both single failure probabilities \( P_1 \) and \( P_2 \) is the probability of failure of independent single faults for the system. Both additive terms \( P_{DUC} \) and \( P_{DDC} \) make the ccf-ratio.

As for the simple basic beta-model the ccf-ratio is also here for the probability of failure the clearly bigger term and – at least by the logic solver of a safety-related system – at least twice as big as the probability of failure of the single fault. The \( PFD_{avg} \)-equation for the ccf-ratio via dangerous undetected failures is [1], [2], [5]:

\[
PFD_{avg, \beta_{DU}} = \beta_D \cdot \lambda_D \cdot (T_1 + MTTR) \tag{20}
\]

and for the ccf-ratio via dangerous detected failures:

\[
PFD_{avg, \beta_{DD}} = \beta_D \cdot \lambda_D \cdot MTTR \tag{21}
\]

Eq. 20 describes the probability of failure for dangerous undetected failures during the Interval \( [T_1 + MTTR] \), i.e. in the span of time of the proof test interval \( T_1 \) and the mean time to repair \( MTTR \) eq. 21, however, describes that during the mean time to repair \( MTTR \) – within this time a system’s redundancy is not given and herewith intersections’ comparisons of test values via equipment diagnosis are not possible – also a safety related risk occurs via the dangerous detected failure. As a consequence, a probability of failure for the safety related system occurs. Both equations (20) and (21) apply in accordance with [1] and [2] not only for a 1oo2-architecture, but also for any redundant architecture.

Figure 5 presents the \( PFD \)-value for ccf, which is the result of the sum of equations (21) and (22). In order to compare figure 4 with 5, the same values for the failure rate \( \lambda_D \) and the interval (now described as proof test interval \( T_1 \)) have been chosen. \( MTTR \) is assumed with 8 h. For both beta-factors \( \beta \) and \( \beta_D \) the following values will be used (presented in pairs: \((0.2 \// 0.1)\) and \((1.0 \// 1.0)\)). The \( DC \)-value, which is described by the diagnostic coverage, has the value 90 %.

Table 2: \( C_{Moos}^n \)-factor for different architectures according [3], a summary.

<table>
<thead>
<tr>
<th>( N )</th>
<th>( M )</th>
<th>( M = 1 )</th>
<th>( M = 2 )</th>
<th>( M = 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N = 2 )</td>
<td>( C_{1oo2} = 1.0 )</td>
<td>( \cdots )</td>
<td>( \cdots )</td>
<td></td>
</tr>
<tr>
<td>( N = 3 )</td>
<td>( C_{1oo3} = 0.3 )</td>
<td>( C_{2oo3} = 2.4 )</td>
<td>( \cdots )</td>
<td></td>
</tr>
<tr>
<td>( N = 4 )</td>
<td>( C_{1oo4} = 0.15 )</td>
<td>( C_{2oo4} = 0.75 )</td>
<td>( C_{3oo4} = 4.0 )</td>
<td></td>
</tr>
</tbody>
</table>
The statement for the basic-beta-model, underneath figure 4, also applies for the beta-model in accordance with IEC 61508 and ISA TR84.00.02. Through the determination of the beta-factor in \( \lambda \) and \( \lambda_D \) to determine the ccf, which will be caused through \( \lambda_{DU} \) and \( \lambda_{DP} \), the probability of failure will be reduced depending from the DC-factor compared to the basic beta-model. Should any diagnosis (DC = 0) exist, then both models are identical.

### 6 PDS-Beta-Model PDS

As a basis for the PDS-beta-model – PDS is the Norwegian acronym for „reliability of computer-based safety systems“ – the beta-model is applied in accordance with IEC 61508. The PDS-model, described in details in [3], extended the beta-factor from the IEC to the factor \( C_{MooN} \). \( MooN \) means that at least \( M \) out of \( N \) redundant components have to work properly, in order to perform correctly the safety function. Through this factor, called configuration factor, the influence of the architecture, which has been chosen for a safety system, will be taken into account. In the IEC, there is only one beta value for all architectures and thereby no differences will be made concerning the ccf in a 1oo2, 2oo3 or 2oo4-system. However, the practice [3] has shown that one must distinguish, whether the ccf in two, three or even more components of redundant systems occur. The beta-factor in PDS-beta-model means therefore:

\[
\beta_{MooN} = C_{MooN} \cdot \beta \quad \text{with} \quad (M < N) \quad \text{(22)}
\]

In [3] and [20], the non-trivial derivation is given to define the \( C_{MooN} \)-value. The Parameter \( \beta \) will still be defined with the help of the above-mentioned criteria and checklists. A summary of the values calculated in [3] is given in table 2.

The PFD-equation for ccf considering the configuration factors is then:

\[
PFD_{CCF,PDS} = C_{MooN} \cdot \beta \cdot \lambda \cdot t \quad \text{(23)}
\]

Figure 6 presents the graph of the PFD\(_{CCF}\)-value for the 2oo4-architecture. The values for the 1oo2-system correspond to the values, which have been calculated with the IEC-Beta-model, if the \( \beta_D \)-ratio = 0 is. Because \( C_{2oo3} > C_{1oo2} \) is, the PFD-values for a 2oo3-system are twice as worse. For a 1oo3- and 2oo4-system, it is the contrary: The PFD-value for these systems is better than the PFD-value of a 1oo2-system.

### 7 Conclusion

In this paper, three different beta-models have been compared to one another to calculate the probability of failure of ccf. Compared to the basic beta model, one can also with the IEC/ISA beta model evaluate and calculate the failure of probability, which can be caused through dangerous detected failures. Further, in step with actual practice to calculate the probability of failure for ccf is the PDS-beta model. Here, during the calculation of probabilities of failure, the architecture will be taken into account with the help of the configuration-factors. Thereby ccf, which do not exist in all components but only between single components, can be evaluated. The PDS-beta model does not take into account, that also detected dangerous failures at some precise time, e.g. during the repair-time of redundant systems, can cause a safety critical ccf. Consider these failures in an extended PDS-beta model will be part of another further task.

### References:


