Estimation and Evaluation of Common Cause Failures

BÖRCSÖK J.
Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel, Germany
j.boercsoek@uni-kassel.de

HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Str. 28, 68782 Brühl
j.boercsoek@hima.com

SCHAEFER, S.
Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel, Germany
schaefer@uni-kassel.de

UGLJESA, E.
Computer Architecture and System Programming
University of Kassel
Wilhelmshöher Allee 73, 34121 Kassel, Germany
e.ugljesa@uni-kassel.de

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

***Abstract*— Success of many modern applications is highly dependent on the correct functioning of complex computer based systems. In some cases, failures in these systems may cause serious consequences in terms of loss of human life. 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 (safety requirement allocation). Moreover, the SIS design should be performed in a way that minimizes the potential for common mode or common cause failures (CCF). A CCF occurs when a single fault result in the corresponding failure of multiple components. Thus, CCFs can result in the SIS failing to function when there is a process demand. Consequently, CCFs have to be identified during the design process and the potential impact on the SIS functionality have to be understood. This paper gives details about the estimation and evaluation of common failures and assesses a 1oo2 system. It is a survey paper that presents the newest developments in common cause failure analysis.**

Keywords-β-factor, common cause failure, 1oo2-system, PFD

I. INTRODUCTION

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 [1,3,6]:

hardware redundancy	software redundancy
time 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 [2,5,7,8]. 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 the data is coded in such a way that a certain number of bit errors can be detected and/or recovered [2,6,7]. A fault tolerant system will only fail if multiple failure events happen.

II. COMMON CAUSE EVENTS

The introduction of redundancies makes the work of safety engineers more difficult, since redundancies bring with them a new class of events named common cause events [6,7,8]. Common cause events affect safety analysis so that the measurable likelihood of a minimal cut, a minimal cut set (MCS) is defined as the smallest combination of error that will lead to a failure of the system, set is bigger than the product of the likelihood of each single event in the minimal cut set considered alone [4,7,8]. Common cause events make it useless to increase the number of redundant channels beyond a certain limit. If engineers were able to build redundant systems with independent redundant channels, there would not be the need of Common Cause Failure (CCF) analysis. In addition, engineers would be able to reach the aimed level of safety (and reliability) by increasing the level of redundancy [7]. Unfortunately, it is practically impossible to build independent redundant channels and the contribution of common cause events have to be evaluated to assure that safety and reliability requirements are met in fault tolerant systems [6,7]. The easiest way to consider common cause failures is to work on minimal cut sets. Events in a minimal cut set may represent the same failure mode in different components (i.e. common mode) or

Second International Conference on Systems (ICONS'07)
0-7695-2807-4/07 $20.00

different failure modes. They can be generated by the same cause (i.e. common cause) or by different causes [7].

However, the issue for the purpose of this paper is that, when all the events in a minimal cut set arise simultaneously by the same root cause, the fault tolerant system fails as if the events in the minimal cut set had arisen randomly. The likelihood that a minimal cut set occurs because of a common cause failure is usually extremely small. However, it is always greater than the likelihood of the minimal cut set to be happened randomly. Purpose of common cause failure analysis is to evaluate this likelihood and to help improving the design. Without considering common cause events, the likelihood of critical minimal cut sets for fault tolerant systems would be underestimated [2,6].

A. *Common cause failure analysis*

Common cause failure events are not usually considered as independent events occurring within a system, but as influences on the system from some source that are common to redundant components, resulting in some abnormal output states.

Common mode failures are a subset of common cause failures, whilst dependent failures encompass both common cause and cascade failures [2,6,7]. Cascade failures include all dependent failures that are not common cause failures (Fig. 1). These are multiple failures initiated by the failure of one component in the system (chain reaction or domino effect). When several components share a common load, failure of one component may lead to an increased load on the remaining ones and, thus, to an increased likelihood of failure. Common Cause Failures are multiple failures which are a direct result of a common or shared root cause. The root cause [2,6,7] may be

- extreme environmental conditions
- failure of a piece of hardware external to the system
- or a human error.

The root cause is not a failure of another component in the system. Operation and maintenance errors are often reported to be root cause failures (carelessness, maladjustment, erroneous procedures). We define "multiplicity" of the common cause failure as the number of components that fail due to that common cause [6,7].

The failures of a system are considered to arise from two causes:

- random hardware failures
- systematic failures.

Random hardware failures are assumed to occur randomly in time for any component and to result in a failure of a channel within a system of which the component forms part. Thus the probability of such failures concurrently affecting parallel channels is low compared to the probability of a single channel failing. This probability can be calculated using well-established techniques. Common cause failures which result from a single cause, may affect more than one channel. These may result from a systematic fault or an external stress leading to an early random hardware failure. Because common cause failures are likely to affect more than one channel in a multi-channel system, the probability of common cause failure is likely to be the dominant factor in determining the overall probability of failure of a multi-channel system.

Dependent failure (DF)	The likelihood of a set of events, the probability of which cannot be expressed as simple product of the unconditional failure probabilities of the individual events.
Common cause failure (CCF)	This is a specific type of dependent failure that arises in redundant components where simultaneous (or near simultaneous) multiple failures result in different channels from a single shared cause.
Common mode failure (CMF)	This term is reserved for common-cause failures in which multiple items fail in the same mode.
Cascade failure (CF)	These are all those dependent failures that are not Common Cause, i.e. they do not affect redundant components.
Further: The term "Dependent failure" as defined above is designed to cover all definitions of failures that are not independent. From this definition of dependent failure it is clear that an independent failure is one where the failure of a set of events is expressible as simple product of individual event unconditional failure probabilities.	

Figure 1. definitions of dependent, common cause, common mode and cascade failures

III. QUANTITATIVE EVALUATION OF COMMON CAUSE FAILURES

In some cases, it may be necessary to consider the impact of potential common cause failures on the SIS performance. In such cases, the potential common cause failures will need to be considered in the systems quantitative performance evaluation. There are two approaches for addressing CCF

- the explicit model and the
- implicit model by approximation method.

Multiple failure events, for which no clear root cause event can be identified, can be modeled using implicit, parametric models.

A. *Explicit method*

The explicit model is used for common cause failure sources that are specific and well understood. These specific sources of common cause failure are modeled as explicit basic events during an evaluation using fault tree analysis.

The failure rates for these events are estimated using internal data, published data (where available), or a conservative failure rate estimate [6,7]. It involves the identification and treatment of specific root causes of dependent failures at the system level, in the event- and fault-tree logic.

B. *Implicit methods*

The different models can be distinguished and separated into categories according to the number of parameters [6,7]:

- Single-parameter: β-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: the probabilities of common events are used directly (Basic parameter model)
  - Indirect: the probabilities of common cause events are estimated through the use of other parameters.

1) Basic parameter model

This model makes use of the rare events approximation 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.

According to this the probability of failure of a 2oo3 system, with the components A, B, and C where $P(X_I)$ is the probability of failure for component X and $P(C_{XY})$ is the probability of a common failure of the components X and Y, is:

$$\left.\begin{array}{c} P(A_I)=P(B_I)=P(C_I)=Q_1 \\ P(C_{AB})=P(C_{AC})=P(C_{BC})=Q_2 \\ P(C_{ABC})=Q_3 \end{array}\right\} \begin{array}{l} Q_t = Q_1 + 2\cdot Q_2 + Q_3 \\ Q_S = 3\cdot Q_1^{\,2} + 3\cdot Q_2 + Q_3 \end{array} \quad (1)$$

Whereas Q_S is the probability of failure of the system and Q_t is the total probability of failure for each component. The general formula to calculate Q_t, with m as the total number of components and k as the actual component, is:

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} \cdot Q_k \quad (2)$$

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

2) β-factor model

It models dependent failures of two types:

- intercomponent physical interactions and
- human interactions.

The model assumes that Q_t 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:

$$Q_t = Q_I + Q_m \quad (3)$$

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

$$\begin{aligned} \beta &= \frac{Q_m}{Q_t} = \frac{Q_m}{Q_I + Q_m} \quad (4) \\ &\Rightarrow Q_m = \beta \cdot Q_t \\ &\Rightarrow Q_I = (1-\beta)\cdot Q_t \end{aligned}$$

For a system with 2oo3 logic:

$$Q_S = 3\cdot(1-\beta)^2 \cdot {Q_t}^2 + \beta \cdot Q_t \quad (5)$$

For a system with more than two units, the β-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 β-factor model lies in its direct use of field data and its flexibility. The total component failure probability Q_t and β have to be estimated. For time distributions of failure probabilities, with the corresponding failure rates λ, this gives:

$$\beta = \frac{Q_m}{Q_t} = \frac{(1-\exp(-\lambda_m \cdot t))}{(1-\exp(-\lambda_t \cdot t))} \approx \frac{\lambda_m}{\lambda_t} \quad (6)$$

3) Multiple Greek letters model

The following equation allows to compute the probability of common cause failures of order k with m - *1* parameters:

$$Q_k = \frac{1}{\binom{m-1}{k-1}} \cdot \left(\prod_{i=1}^{k}\right) \cdot (1-\rho_{k+1}) \cdot Q_t \quad (7)$$

$\rho_2 = \beta$ = 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.

4) α-factor model

The following equation with m parameters hold:

$$\alpha_k^{(m)} = \frac{\binom{m}{k} \cdot Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} \cdot Q_k^{(m)}} \quad (8)$$

with normalization:

$$\sum_{k=1}^{m} \alpha_k^{(m)} = 1 \quad (9)$$

The equation becomes

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \cdot \frac{\alpha_k^{(m)}}{\alpha_t} \cdot Q_t \quad (10)$$

with

$$\text{k=1,2,…m and } Q_t = \sum_{k=1}^{m} k \cdot \alpha_k \quad (11)$$

5) Binomial failure rate (BFR) model

Here we consider a system composed of m identical components. Each component can fail at random times, independently of each other, with failure rate λ. Furthermore, a common cause shock can hit the system with occurrence rate μ. 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 of the shock is binomially distributed with parameters m and p::

$$p(I=i)=\binom{m}{i}\cdot p^{i}\cdot(1-p)^{m-i} \tag{12}$$

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 = 1). If all the shocks are lethal, one is back to the β-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 β-factor model in that it distinguishes between the numbers of multiple-unit failures in a system with more than two units:

$$\lambda_1 = m\lambda + \mu\left[\binom{m}{1}p(1-p)^{m-1}\right]$$ Failure rate of **one** unit

Total contribution due to independent failures

Rate of single-unit failures from common cause shocks

$$\lambda_i = m\lambda + \mu\left[\binom{m}{i}p^{i}(1-p)^{m-i}\right]$$ Failure rate of **i** units, i=2,...,m

Three parameters, λ, μ and p need to be estimated.

IV. BETA-FACTOR

The susceptibility of a system to common stressors is normally measured by the so-called "beta"-factor (β-factor).

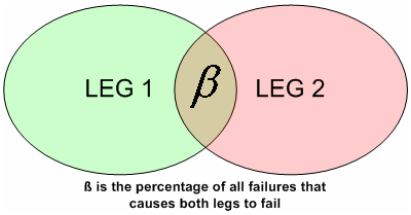

Figure 2. Dual system with one β-factor

The range of the β-factor is from 0 to 0.25 (0 means: no common cause failure). It is defined as the percentage of all failures in one leg of a multiple channel system that will cause two or more legs to fail due to a common stressor. A dual system shows just one β-factor, as seen in Fig. 2. The β-factor is the percentage of all failures that causes both legs to fail. Systems in triplicate or higher show a number of subfactors. For example a triple redundant PLC-system distinguishes 4 common cause factors:

- 3 combinations of legs giving β_1, β_2 and β_3.
- β_0 indicates the single stressor that causes all legs to fail.

The stressors defining β_1, β_2 and β_3 are probably due to systematic failures (design), while β_0 originates most likely from an environmental stressor. For practical safety integrity calculations all β-factors are often combined into one value. The formulas mostly used are also based on one β-factor, using the assumption that all legs of a redundant system will fail due to a single common cause. The determination of the β-factor is rather difficult and mostly based on an analysis by experts and quite a number of discussions and assumptions. In spite of the division among the experts all publications have one opinion in common:

With an order of a magnitude reduction in safety integrity, common-cause is very significant. The approximation method is the more commonly used approach to the quantitative evaluation of common cause failures. In the application of this method, typically called the β-factor method, the likelihood of a common cause failure is related to the random failure rate for the device. This method makes it possible to evaluate CCFs without identifying the specific sources of dependent failures and their associated probability. The β-factor can be estimated as follows:

- Identify the total failure rate for the device from published or internal data
- Review the failure modes to determine the portion that is expected to have a common cause affect
- Calculate/estimate the percentage of the failure rate that can be associated with CCF (β-factor)
- Use the β-factor to calculate the dependent and independent failure rates for the device.

The β-factor can range from nearly 0 up to 25 %, depending upon the device and the particular common cause issues under consideration. The estimation of the β-factor can be accomplished through either quantitative or qualitative methods. Plant experience can be used to calculate a β-factor for a particular device, when good maintenance and inspection records are available. In such instances, the following equation can be used:

$$\beta = \frac{m}{n+m} \tag{13}$$

With

n = number of events where only a single component failed

m = number of devices which failed in a set of events where multiple similar components have failed.

In instances where sufficient plant data is not available, qualitative methods can be used to estimate the β-factor. A number of published sources provide limited guidance on the selection of the β-factor based upon expert judgment.

A. *Impact of the β-factor on safety integrity*

There are several quantitative models to predict the effect of common cause failures of a safety system. The most simple is called the "β-model". This model is based on the same formulas as mentioned in the previous section but includes the β-factor based on a common stressor effecting all legs of a redundant PLC at the same time. Derived from ISA-TR84.02 [4] and including the β-factor, the formulas can be written as shown in Tab. I:

TABLE I. PROBABILITY OF FAILURE ON DEMAND (PFD)-FORMULAS WITH CCF

Safety system	**PFD_{avg}**
1002D	$1/3 \cdot ((1-\beta)\cdot \lambda_{DU} \cdot T)^2 + 1/2 \cdot \beta \cdot \lambda_{DU} \cdot T$
2oo3	$((1-\beta)\cdot \lambda_{DU} \cdot T)^2 + 1/2 \cdot \beta \cdot \lambda_{DU} \cdot T$
2oo4	$((1-\beta)\cdot \lambda_{DU} \cdot T)^2 + 1/2 \cdot \beta \cdot \lambda_{DU} \cdot T$

Tab. I presents the probability of failure on demand (PFD), whereas λ_{DU} stands for the failure rate caused by dangerous undetectable errors and T is the elapsed time of the system, of the most used PLC architectures, being the 1oo2D, 2oo3 and the 2oo4. It clearly shows the formulas exist of two parts.

- The left part gives the effect due to the used redundant architecture.
- The right part of the formula is identical with the formula of a single PLC and indicates the effect of the β-factor on the PFD_{avg}.

The higher the β-factor is the more significant the effect.

Published opinions of experts put the β-factor in the range of 0.1 % to 10 % for hardware failures. Especially, parts placed outside of the safety loops are sensitive to common environmental stressors and are subject to high β-factors. For example: Typical values for final elements are at 10 %.

Fig. 3 shows how the PFD_{avg} deteriorates as β goes higher. This is quite understandable, regarding the value of the β-factor and its dominant effect on the results of the formulas. Comparing the calculation result of a 1oo2D architecture (PFD_{avg} = 2.56E-5) with $\beta = 0$ with a calculation with $\beta = 10$ % (PFD_{avg} = 3.0E-4), the PFD_{avg} is deteriorated with a factor of 10!

B. *1oo2 system*

The 1oo2 system consists of two independent channels. In order to carry out the safety function correctly both channels are connected with each other in a way that only one channel is sufficient to activate the safety function. Therefore, a 1oo2 system will fail dangerously if both channels have failed dangerously. The failure probability of a 1oo2 system can be determined with the fault tree.

The equation for the probability of failure is then

$$P(t) = P_1(t) \cdot P_2(t) + P_{DUC}(t) + P_{DDC}(t) \tag{14}$$

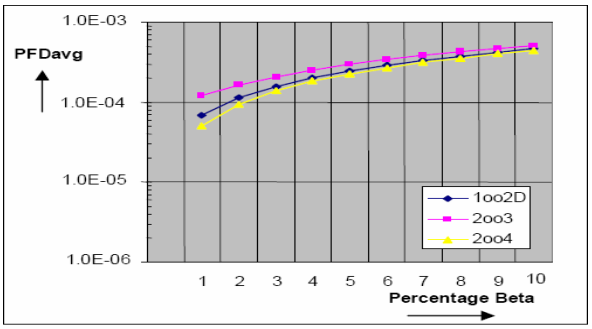

Figure 3. PFD_{avg} for different architectures

with

$$P_1(t) = 1 - e^{-\lambda_{D1} \cdot t} \tag{15}$$

$$P_2(t) = 1 - e^{-\lambda_{D2} \cdot t} \tag{16}$$

$$P_{DDC}(t) = 1 - e^{-\beta_D \cdot \lambda_{DD} \cdot t} \tag{17}$$

Next, the failure probability is calculated for dangerous undetectable and dangerous detectable common cause failures P_{DUC} and P_{DDC}. When determining the PFD_{avg} the common cause failure is rated for a multi channel system according to the equation:

$$P_\beta(t) = P_{DUC}(t) + P_{DDC}(t) \tag{18}$$

For a 1oo1 system these probabilities of failure can be derived with

$$\lambda_{D,1oo1} = \beta \cdot \lambda_{DU} \tag{19}$$

respectively, with β_D the factor for all dangerous errors and λ_{DD} the failure rate of the dangerous detectable errors:

$$\lambda_{D,1oo1} = \beta_D \cdot \lambda_{DD} \tag{20}$$

A random common cause failure represents a 1oo1 function block. Therefore, it is possible to apply for the calculation of probability of common cause failure the derived PFD_{avg} equation of the 1oo1 system. The general solution for the probability failure results in

$$\begin{aligned} PFD_{avg,\,\beta\ faulttree} &= \beta \cdot \lambda_{DU}\left(T_1 + MTTR'\right) \\ &\quad + \beta_D \cdot \lambda_{DD} \cdot MTTR' \\ &= \lambda_D \cdot \tilde{t}_{CE,\beta} \end{aligned} \tag{21}$$

From the fault tree of the 1oo2 system, it is possible to derive the equation for the common cause failures. The PFD_{avg} equation consists of the probability that a dangerous undetected common cause failure occurs within the time period T_1 + *MTTR'* (mean time to repair):

$$PFD_{avg,\,\lambda_{DU},\beta} = \beta \cdot \lambda_{DU}\left(T_1 + MTTR'\right) \tag{22}$$

and of the probability that a dangerous detected common cause failure occurs within the repair time *MTTR'*:):

$$PFD_{avg,\lambda_{DD},\beta} = \beta_D \cdot \lambda_{DD} \cdot MTTR' \tag{23}$$

with the variable

$$\tilde{t}_{CE,\beta} = \beta \cdot \frac{\lambda_{DU}}{\lambda_D} \cdot \left(T_1 + MTTR'\right) + \beta_D \cdot \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR' \tag{24}$$

With

$$\tilde{t}_{CE,\beta} = T \tag{25}$$

this results in

$$\begin{aligned} PFD_{avg,\beta} &= \frac{\lambda_D}{2} \cdot \tilde{t}_{CE,\beta} \\ &= \frac{\lambda_D}{2} \cdot \left[\beta \cdot \frac{\lambda_{DU}}{\lambda_D} \cdot (T_1 + MTTR') \right. \\ &\quad \left. + \beta_D \cdot \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR' \right] \\ &= \left[\beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + \frac{MTTR'}{2} \right) \right. \\ &\quad \left. + \beta_D \cdot \lambda_{DD} \cdot \frac{MTTR'}{2} \right] \end{aligned} \tag{26}$$

With the assumption that

$$\frac{T_1}{2} >> \frac{MTTR'}{2} \approx MTTR' = MTTR \tag{27}$$

it is possible to calculate the PFD_{avg} value for common cause failures as

$$\begin{aligned} PFD_{avg,\beta} &= \left[\beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) \right. \\ &\quad \left. + \beta_D \cdot \lambda_{DD} \cdot MTTR \right] \\ &= \lambda_D \cdot \left[\beta \cdot \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) \right. \\ &\quad \left. + \beta_D \cdot \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \right] \\ &= \lambda_D \cdot t_{CE,\beta} \end{aligned} \tag{28}$$

with

$$t_{CE,\beta} = \beta \cdot \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \beta_D \cdot \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{29}$$

The PFD_{avg} equation for a 1oo2 system is calculated as follows, by adding to the probability of a single failure the part of the common cause failure:

$$\begin{aligned} PFD_{avg,\beta} &= 2 \cdot ((1-\beta) \cdot \lambda_{DU} + (1-\beta_D) \cdot \lambda_{DD})^2 \cdot t_{CE} \cdot t_{GE} \\ &\quad + \left[\beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) \right. \\ &\quad \left. + \beta_D \cdot \lambda_{DD} \cdot MTTR \right] \end{aligned} \tag{30}$$

The PFD_{avg} value of a 1oo2 system is identical to the corresponding formula from IEC 61508 [2].

V. CONCLUSION

A fault-tolerant safety system built especially for critical applications can provide many benefits for safety protection and other critical system applications. However, most safety analyses done in the past have ignored the effects of common-cause. This report has shown that the safety level of a system can degrade by more than an order of magnitude when the common cause factor is considered. It also means that a higher degree of redundancy does not provide better performance evidently. The β-factor really is a critical parameter. In a pragmatic way, its assessment is conceivable. However, assumptions on which the assessment is based are still very disputable. A reduction of common-cause failures is achieved through a number of mechanisms

- Physical separation of redundant units: The worst implementation has redundant circuits on the same circuit board. The best implementation allows redundant circuits to be located in different cabinets.
- Diversity: The worst implementation has identical hardware (and software) in redundant units. The best implementation uses diverse components that respond differently to a common stressor.
- Robustness of hardware (and software): Other important parameters include the overall ruggedness of the system (and the use of a systematic audited software development process).

The right implementation of these three items allows the decrease of the β-factor to an acceptable level.

REFERENCES

[1] G. T. Edwards and I. A. Watson, "A Study of Common Mode Failures", SRD-R-146, UK Atomic Energy Authority, Safety and Relia. Dir., 1979.

[2] IEC/EN 61508, "International Standard: 61508 Functional safety of electrical electronic programmable electronic safety related systems Part1-Part7", Geneva, Int. Elec. Com. 1999-2002

[3] S. Hauge, P. Hokstad, H. Langseth, K. Øien, "Reliability prediction method for safety instrumented systems", PDS method handbook, SINTEF (Norwegen), 2006

[4] ISA-TR84.00.02-2002, Parts 1-5, "Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques", 2002.

[5] A. C. Brombacher, "Reliability of mechanical products", NL, 1996

[6] J. Börcsök, "Electronic safety systems", Hüthig Verlag, 2004

[7] J. Börcsök, "Functional safety", Hüthig Verlag, 2006, in press

[8] W. M. Gobel, "Control systems safety evaluation and reliability", 1998

[9] R. J. Tiezema, "Eliminating the Unexpected", Part 2: Safety Assessment, May 1995 GTI IA, NL

0-7695-2807-4/07 $20.00 © 2007 IEEE