Comparison of PFD calculation

Prof. Dr.-Ing. habil. Josef Börcsök

Prof. Dr.-Ing. habil. Josef Börcsök is vice president of R&D at HIMA Paul Hildebrandt GmbH + Co KG, Industrial Automation. He is working for many years on the field of safety technology and he is member of different committees of DKE. He is doing lectures for many years on universities and colleges with the topics automatic technologies, computer architectures and safety computer architectures.

Address:
HIMA Paul Hildebrandt GmbH + Co KG
Albert-Bassermann-Str. 28
D-68782 Brühl near Mannheim
Tel. +49-6202 709 270
E-Mail: j.boercsoek@hima.com

Keywords

IEC/EN 61508, ISA-TR84.0.02, normal failure, common cause failures, 1oo1-system, safety related 1oo2-system, safety related 2oo3-system, safety integrity levels (SIL), SIL-requirement, probability of failure on demand (PFD), probability of failure per hour (PFH), safe failure fraction (*SFF*), type A subsystem, type B subsystem, hardware fault tolerance, diagnostic coverage factor (*DC*), proof-test interval, loop calculation

Abstract

Safety systems are be used in a wide range of technical application. Beside the availability of such systems the safety aspects, e. g. PFD and PFH figures, must be observed. Especially the calculation of these figures requires the use of standards. Worldwide are standards available for this calculation. The newest standard is IEC 61508. This standard is worldwide accepted. Another standard, which is used since years, is ISA-TR84.0.02. In this standard a safety calculation can be performed without using MTTR and common cause failure. Since the introduction of the standard IEC 61508 a lot of discussion concerning the PFD-number appears in the industry. The reason for that discussion is the way of calculation this numbers. This contribution will compare both calculation-methods.

Introduction

In the process industry is the use of safety related controllers and systems increasing by regulative measures. For the validation of applications of those systems specific figures of the failure rates are used. VDE 0801 part 1 to 7 "Functional safety, Safety related systems" has been recently the state of the art for national and international standards (also known IEC 65A/179/CDV, Draft IEC1508). It describes the procedures and the calculations of complex electronics and microcomputers for safety related applications. After the introduction of the IEC/EN 61508, a common national and international standard was created that describes/specifies generic safety related systems.

Today in various publications exist different ways of calculating the PFD-figures and availability-figures. Some parts of them are based on the ISA-TR84.0.02 (1998) and the therein described equations.

To get reasonable analysis related to the safety and the probability of failure rates, it is required to do the comparisons on the same base.

Basically there is a differentiation in the failure analysis between safe and dangerous failures.
Further more the safe failures are differentiate in

- safe detectable
- safe undetectable.

Safe failures are failures, which have no effect to the safety function of the system, either detected nor undetected.
At dangerous failures this situations is not valid. These failures lead at their occurrence to a dangerous situations in the application, that can lead under certain circumstances up to massive risk for human life. These failures are differentiate as well in

- dangerous detectable
- dangerous undetectable.

When the safety related system is designed properly the system reaches the safe state at detectable dangerous failures. For this cases the safety related system is able to bring the complete system or the plant in the safe state.

The critical state is caused by the undetectable dangerous failures. In their occurrence there is no possibility in any safety related systems to detect them. They can exist in the systems until the systems will be shut down. Or in the worst case they can be present without possibility to be detected and any knowledge of the user up to the system hazard.

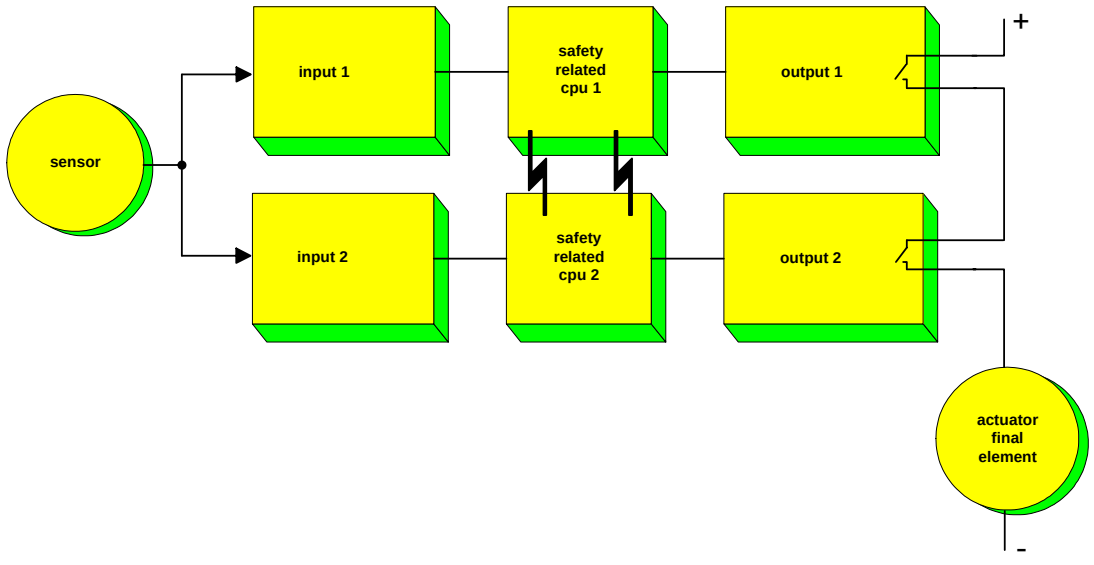

Figure 1: Safety related 1oo2-system

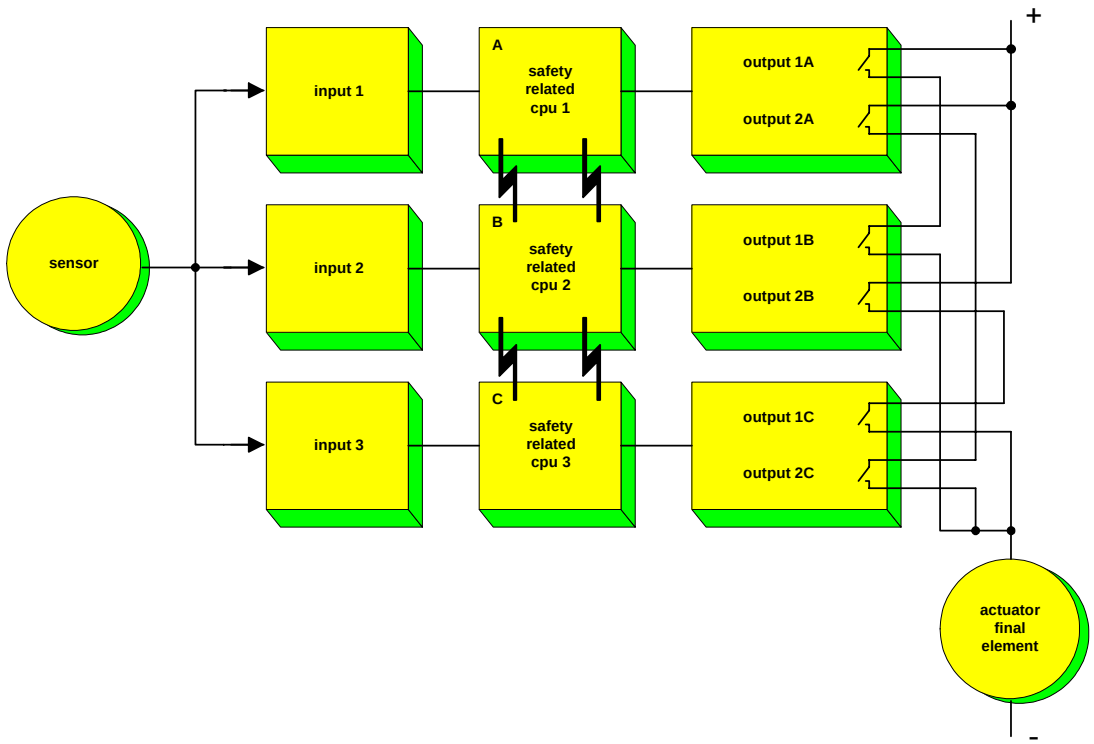

Figure 2: Safety related 2oo3-system

SIL-requirements according to IEC/EN 61508 and ISA-TR84.0.02 (1998)

The following tables show the fundamental requirements of the different safety integrity levels (SIL) according to IEC/EN 61508 and ISA-TR84.0.02 (1998).

Table 1: SIL for systems operating in low and high demand or continuous mode of operation according to IEC/EN 61508

Safety integrity level (SIL)	**Low demand mode of operation** (average probability of failure to perform its design function on demand)	**High demand or continuous mode of operation** (probability of dangerous failure per hour)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Table 2: SIL according to ISA-TR84.0.02 (1998)

Safety integrity level (SIL)	**demand mode of operation** (probability of failure on demand average)	
3	$\geq 10^{-4}$ to $<10^{-3}$	
2	$\geq 10^{-3}$ to $<10^{-2}$	
1	$\geq 10^{-2}$ to $<10^{-1}$	

In principle the statement can be derived from the tables that the probabilities of failures are specified in the same ranges.

Advanced considerations of PFD-values according to IEC/EN 61508

Part 2 of this standard specifies the hardware requirements. Further the safety life cycle of the hardware is there defined, also the architecture constraints for type A (for these subsystems the behavior is in the case of an error well known), as well as type B subsystems (for these subsystems the behavior is in the case of an error not completely known), and at least the required safe failure fraction (*SFF*).

Table 3: Type A subsystems and type B subsystems

Safe failure fraction	Type A			Type B		
	Hardware fault tolerance			Hardware fault tolerance		
	0 fault	1 fault	2 faults	0 fault	1 fault	2 faults
< 60 %	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60 % - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % - < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Calculation of *PFD*-values according to IEC/EN 61508

Part 6 besides the parts 2 and 3 of the IEC/EN 61508 represents one of the central parts for the development of safety related systems. Detailed information are given for the quantitative calculations of safety related systems. For example there are shown block diagrams and formulas to calculate the *PFD* values. As well there are tables to determine the β factor as well as equations for the calculation of the diagnostic coverage (*DC*) and safe failure fraction (*SFF*). Further tables are presented with calculated *PFD* values for all system configurations demonstrated in this standard with variants of all relevant parameters. The equations for the *PFD* values of different systems are here presented exemplarily:

Equation to quantify a 1oo1-System:

$$\begin{aligned} PFD_{G,1oo1} &= (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \\ &= \lambda_D \cdot t_{CE} \\ &= \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) + \lambda_{DD} \cdot MTTR \end{aligned} \quad (1)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (2)$$

Equation to quantify a 1oo2-System:

$$\begin{aligned} PFD_{G,1oo2} = 2 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \right)^2 \cdot t_{CE} \cdot t_{GE} \\ + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right) \end{aligned} \quad (3)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (4)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (5)$$

Equation to quantify a 2oo3-System:

$$PFD_{G,2oo3} = 6 \cdot \left((1-\beta_D)\cdot \lambda_{DD} + (1-\beta)\cdot \lambda_{DU}\right)^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right) \quad (6)$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (7)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (8)$$

Two further more important indicators for safety related systems are represented by the safe failure fraction (*SFF*) and the diagnostic coverage factor (*DC*). The *SFF* is calculated by the equation:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \quad (9)$$

The *DC* factor can be determined by the equation:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (10)$$

The *SFF* represents the ratio of non safety critical failures and the *DC* factor describes the fraction of dangerous failures which are detected by automatic diagnostic tests. The individual factors in these equations have the following meaning:

β	The fraction of undetected failures that have a common cause
β_D	The fraction of those failures that are detected by the diagnostic tests, the fraction that have a common cause
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal 0,5 λ (assumes 50 % dangerous failures and 50 % safe failures)
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)
MTTR	Mean time to restoration (hour)
PFD_G	Average probability of failure on demand for the group of voted channels
T_1	Proof-test interval (h)
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)

The standard shows exemplary the procedure with the determination of hardware failures. At first basics and assumptions are specified establishing the calculations. There are in principle several methods for the analysis of the safety integrity of safety related systems. The most frequent applied methods are the reliability block diagrams and the Markov models. Both methods correctly applied supply almost equivalent results. The Markov models represent the more exact, although more difficult method, delivering accurate values with more complex systems.

A further characteristic value of the average probability of a failure for a system or a loop is the PFD_{sys}. This value is calculated adding the average probabilities of the individual systems.

$$PFD_{sys} = PFD_s + PFD_L + PFD_{FE} \quad (11)$$

In order to determine the average probability of failures for each subsystem the following information must be present:

- the system architecture
- the diagnostic coverage of each channel
- the failure rate per hour for each channel
- the factors β and β_D for the failures with common cause.

In the last list the term common cause factor is introduced. The β-factor is introduced as ratio of the probability of failures with a common cause to the probability of random dangerous failures. The next example shall show this:

The factors are specified as follows:

β_D	=	common cause-factor of detectable failures
β	=	common cause-factor of undetectable failures
T_1	=	Proof-test interval
MTTR	=	Mean time to restoration

with following values:

β_D	=	1 %
β	=	2 %
T_1	=	3 years
MTTR	=	8 hours

With these assumptions the PFD-calculations can be executed.

PFD-calculation according to ISA-TR84.0.02 (1998)

In order to compare directly the equations for the PFD-calculations, the ISA-equations are listed below. Basically there are two different methods for calculating: with and without common cause factor.

Equations to quantify a 1oo1, 1oo2 and 2oo3-system according to ISA-TR84.0.02 (1998). Remark: The first equation is with consideration of the common-cause failure and *MTTR*. The second equation is the simplified equation.

1oo1-system

$$PFD_{avg} = \lambda^{DU} \cdot \frac{TI}{2}$$

$$PFD_{avg} = \lambda^{DU} \cdot \frac{TI}{2}$$

The factors in this configuration have the meaning:

λ^{DU}	=	dangerous undetectable failure rate
TI	=	time interval between manual functional tests of the component

1oo2-system

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^2 \cdot \frac{TI^2}{3}\right] + \left[\lambda^{DU} \cdot \lambda^{DD} \cdot MTTR \cdot TI\right] + \left[\beta \cdot \lambda^{DU} \cdot \frac{TI}{2}\right]$$

$$PFD_{avg} = \frac{\left(\lambda^{DU}\right)^2 \cdot TI^2}{3}$$

The factors in this configuration have the meaning:

λ^{DD}	=	dangerous detectable failure rate
λ^{DU}	=	dangerous undetectable failure rate
β	=	percentage of failures that impact more than one channel of a redundant system (common cause)
TI	=	time interval between manual functional tests of the component
MTTR	=	mean time to repair

2oo3-system

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^2 \cdot TI^2\right] + \left[3\lambda^{DU} \cdot \lambda^{DD} \cdot MTTR \cdot TI\right] + \left[\beta \cdot \lambda^{DU} \cdot \frac{TI}{2}\right]$$

$$PFD_{avg} = \left(\lambda^{DU}\right)^2 \cdot TI^2$$

The factors in this configuration have the meaning as for the 1oo2-system:

λ^{DD}	=	dangerous detectable failure rate
λ^{DU}	=	dangerous undetectable failure rate
β	=	percentage of failures that impact more than one channel of a redundant system (common cause)
TI	=	time interval between manual functional tests of the component
MTTR	=	mean time to repair

Comparison between IEC 61508 and ISA-TR84.0.02 (1998)

Seeing the differences between IEC 61508 and ISA-TR84.0.02 (1998) in the following items are to be considered.

In the ISA-standard there is no consideration of the safe failure fraction (*SFF*). The diagnostic coverage factor (*DC*) is defined in a different way, IEC is more detailed. In addition the beta factor β is considered only for the failure rate λ_{DU}.

The part of failures of λ_{DD} during the repair time (*MTTR*) caused by common-cause failures is not calculated.

In a 1oo1-architecture the ISA standard does not consider the parts of failure rates caused by λ_{DD}.

In a case of a huge *DC* factor it is possible that the IEC 61508 standard shows worse values than the ISA standard. In the IEC the term

$\lambda_{DD} \cdot MTTR$.

is considered.

This means for redundant systems like 1oo2 or 2oo3 with a high *DC* factor (assumption: > 99,9) and a high *MTTR* compared with *TI*, it is possible that the IEC term shows worse values than the ISA standard. In the IEC the term $\beta_D \cdot \lambda_{DD} \cdot MTTR$

is taken into account.

The above mentioned points are serious because depending on chosen system configuration they create the need for additional hard- and software measures in safety systems.

Comparison of the results

Basically both calculation methods show possibilities to calculate the probability of failure. To clarify the comparison a fictive module is considered.

Following values are applied for the fictive module:

Fictive module	λ_b [1/h]	*MTTF* [years]	λ_S [1/h]	λ_D [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	*MTTR* [h]	β_D	β
	1,700E-07	671,50	8,500E-08	8,500E-08	8,415E-08	8,500E-10	8	0,01	0,02

Additional fixed parameters:
Diagnostic coverage factor *DC* = 99 %
Safety relevant factor *S* = 50 %

Please observe: The scale on the y-axis is logarithmic.

PFD-calculation for a 1oo1-system

Diagram of the different *PFD*-values for a 1oo1-system:

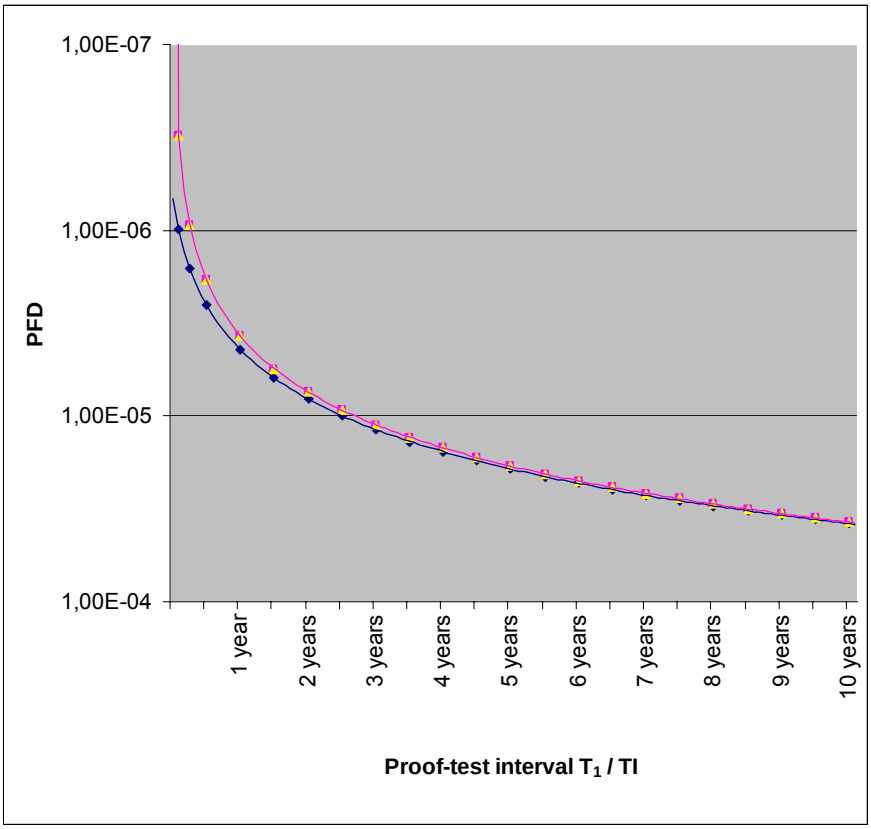

Figure 3: *PFD*-diagram for a 1oo1-system with *DC* = 99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Table 4: *PFD*-values for a 1oo1-system with *DC* = 99 %

Proof-test interval T_1 / *TI*	IEC 61508: PFD_{1oo1} [1]	ISA TR 84.0.02: PFD_{1oo1} with *MTTR* and cc [1]	ISA TR 84.0.02: PFD_{1oo1} without *MTTR* and cc [1]
1 month	9,902500E-07	3,102500E-07	3,102500E-07
3 months	1,610750E-06	9,307500E-07	9,307500E-07
6 months	2,541500E-06	1,861500E-06	1,861500E-06
1 year	4,403000E-06	3,723000E-06	3,723000E-06
2 years	8,126000E-06	7,446000E-06	7,446000E-06
3 years	1,184900E-05	1,116900E-05	1,116900E-05
4 years	1,557200E-05	1,489200E-05	1,489200E-05
5 years	1,929500E-05	1,861500E-05	1,861500E-05
6 years	2,301800E-05	2,233800E-05	2,233800E-05
7 years	2,674100E-05	2,606100E-05	2,606100E-05
8 years	3,046400E-05	2,978400E-05	2,978400E-05
9 years	3,418700E-05	3,350700E-05	3,350700E-05
10 years	3,791000E-05	3,723000E-05	3,723000E-05

At a 1oo1-system both ISA-graphs are identical because in this system configuration no common cause failure exists.

The *PFD* values based on IEC and ISA are in the same magnitude, see figure 3. Dramatic chances occur at low T_1/*TI* and vary high *DC*-factor, see figure 4, e. g. *DC* = 99,99 %.

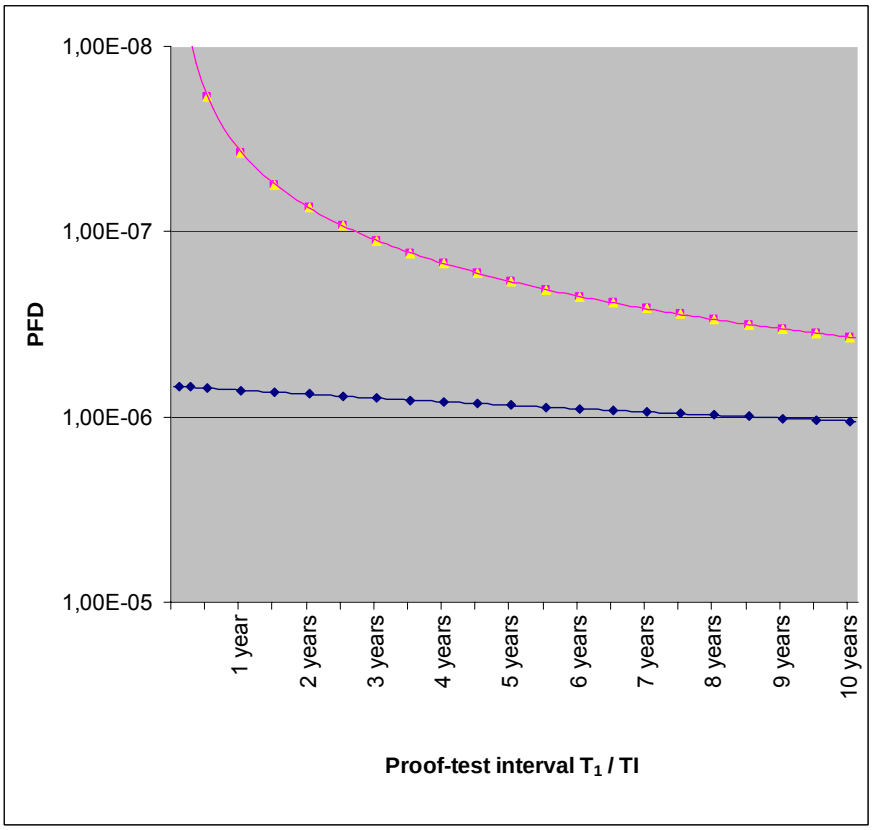

Figure 4: *PFD*-diagram for a 1oo1-system with *DC* = 99,99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Table 5: *PFD*-values for a 1oo1-system with *DC* = 99,99 %

Proof-test interval T_1 / *TI*	IEC 61508: PFD_{1oo1} [1]	ISA TR 84.0.02: PFD_{1oo1} with *MTTR* and cc [1]	ISA TR 84.0.02: PFD_{1oo1} without *MTTR* and cc [1]
1 month	6,831025E-07	3,102500E-09	3,102500E-09
3 months	6,893075E-07	9,307500E-09	9,307500E-09
6 months	6,986150E-07	1,861500E-08	1,861500E-08
1 year	7,172300E-07	3,723000E-08	3,723000E-08
2 years	7,544600E-07	7,446000E-08	7,446000E-08
3 years	7,916900E-07	1,116900E-07	1,116900E-07
4 years	8,289200E-07	1,489200E-07	1,489200E-07
5 years	8,661500E-07	1,861500E-07	1,861500E-07
6 years	9,033800E-07	2,233800E-07	2,233800E-07
7 years	9,406100E-07	2,606100E-07	2,606100E-07
8 years	9,778400E-07	2,978400E-07	2,978400E-07
9 years	1,015070E-06	3,350700E-07	3,350700E-07
10 years	1,052300E-06	3,723000E-07	3,723000E-07

PFD-calculation for a 1oo2-system

Diagram of the different *PFD*-values for a 1oo2-system:

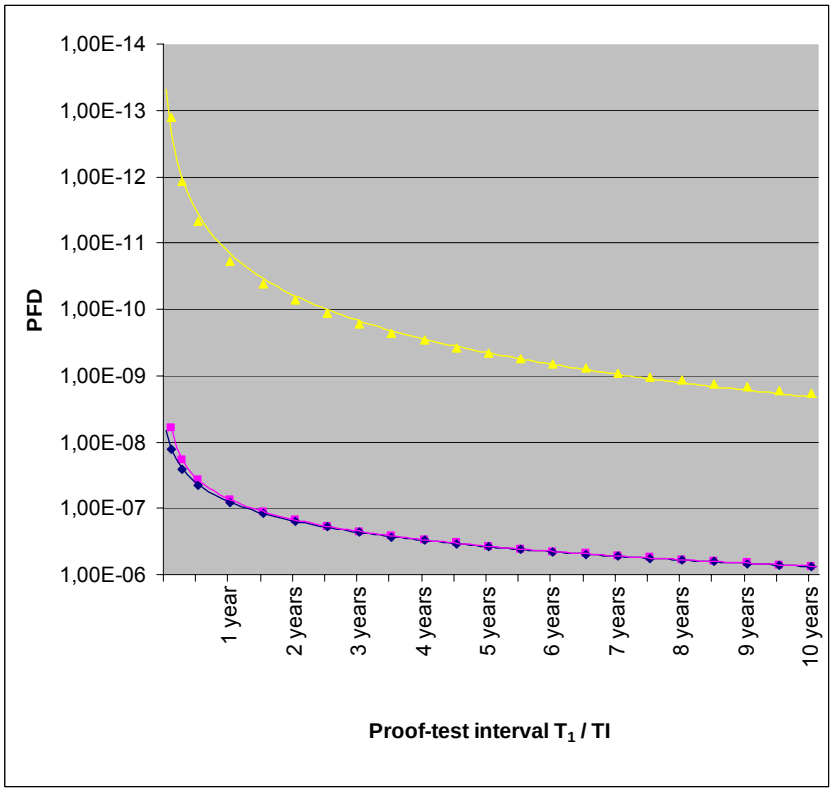

Figure 5: *PFD*-diagram for a 1oo2-system with *DC* = 99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Table 6: *PFD*-values for a 1oo2-system with *DC* = 99 %

Proof-test interval T_1 / *TI*	IEC 61508: PFD_{1oo2} [1]	ISA TR 84.0.02: PFD_{1oo2} with *MTTR* and cc [1]	ISA TR 84.0.02: PFD_{1oo2} without *MTTR* and cc [1]
1 month	1,307472E-08	6,205546E-09	1,283401E-13
3 months	2,548711E-08	1,861741E-08	1,155061E-12
6 months	4,410757E-08	3,723713E-08	4,620243E-12
1 year	8,135528E-08	7,448349E-08	1,848097E-11
2 years	1,558779E-07	1,490039E-07	7,392389E-11
3 years	2,304367E-07	2,235614E-07	1,663287E-10
4 years	3,050317E-07	2,981557E-07	2,956956E-10
5 years	3,796630E-07	3,727871E-07	4,620243E-10
6 years	4,543305E-07	4,474554E-07	6,653150E-10
7 years	5,290342E-07	5,221607E-07	9,055676E-10
8 years	6,037741E-07	5,969029E-07	1,182782E-09
9 years	6,785502E-07	6,716821E-07	1,496959E-09
10 years	7,533626E-07	7,464982E-07	1,848097E-09

At a 1oo2-system the ISA-graph is under consideration of the *MTTR* and the common-cause failure three to four magnitudes bigger, at low *T1/TI* and *DC* = 99 %, than the ISA-graph without consideration of these two parameters, see figure 5. The deviation between the two graphs increases the higher the *DC*-factor becomes, see figure 6.

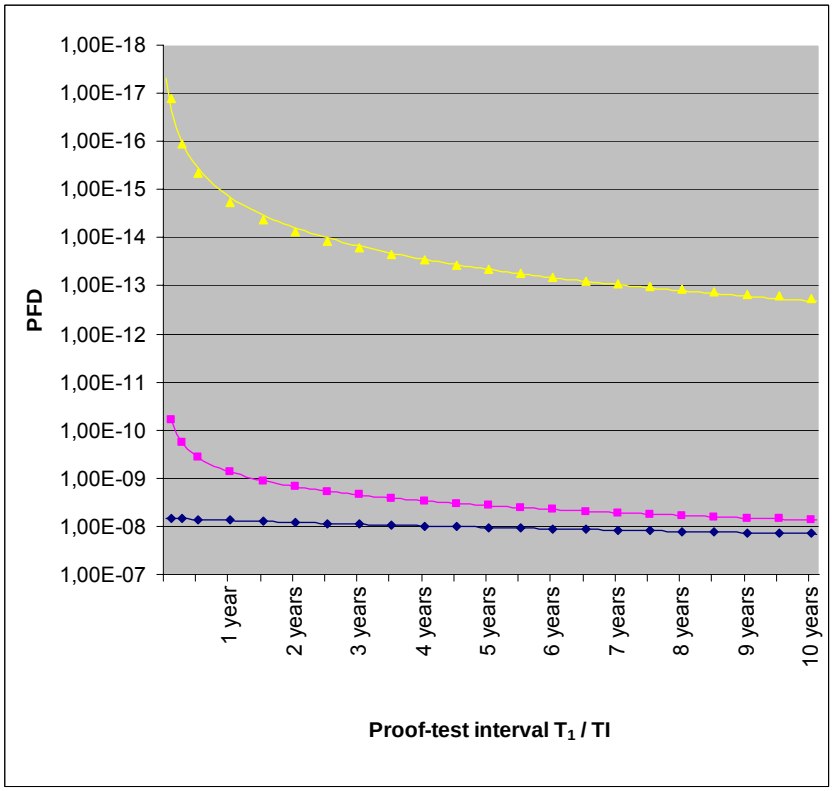

Figure 6: *PFD*-diagram for a 1oo2-system with *DC* = 99,99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Comparing the ISA and the IEC graph under consideration of *MTTR* and common-cause-failure with *DC* = 99 %, see figure 5, both graphs are to be found in the same magnitude. With increasing the *DC*-factor, *DC* = 99,99 %, see figure 6, these both graphs deviate at low T_1/TI by two magnitudes from each other. The reason for this deviation results mainly in the case that in the IEC the part of failures of λ_{DD} is considered during the repair time *MTTR* caused by common-cause-failures by the term $\beta_D \cdot \lambda_{DD} \cdot MTTR$.

Table 7: *PFD*-values for a 1oo2-system with *DC* = 99,99 %

Proof-test interval T_1 / *TI*	IEC 61508: PFD_{1oo2} [1]	ISA TR 84.0.02: PFD_{1oo2} with *MTTR* and cc [1]	ISA TR 84.0.02: PFD_{1oo2} without *MTTR* and cc [1]
1 month	6,863643E-09	6,205423E-11	1,283401E-17
3 months	6,987757E-09	1,861628E-10	1,155061E-16
6 months	7,173928E-09	3,723258E-10	4,620243E-16
1 year	7,546271E-09	7,446525E-10	1,848097E-15
2 years	8,290959E-09	1,489309E-09	7,392389E-15
3 years	9,035651E-09	2,233969E-09	1,663287E-14
4 years	9,780346E-09	2,978632E-09	2,956956E-14
5 years	1,052505E-08	3,723299E-09	4,620243E-14
6 years	1,126975E-08	4,467970E-09	6,653150E-14
7 years	1,201445E-08	5,212645E-09	9,055676E-14
8 years	1,275916E-08	5,957323E-09	1,182782E-13
9 years	1,350388E-08	6,702005E-09	1,496959E-13
10 years	1,424859E-08	7,446691E-09	1,848097E-13

PFD-calculation for a 2oo3-system

Diagram of the different *PFD*-values for a 2oo3-system:

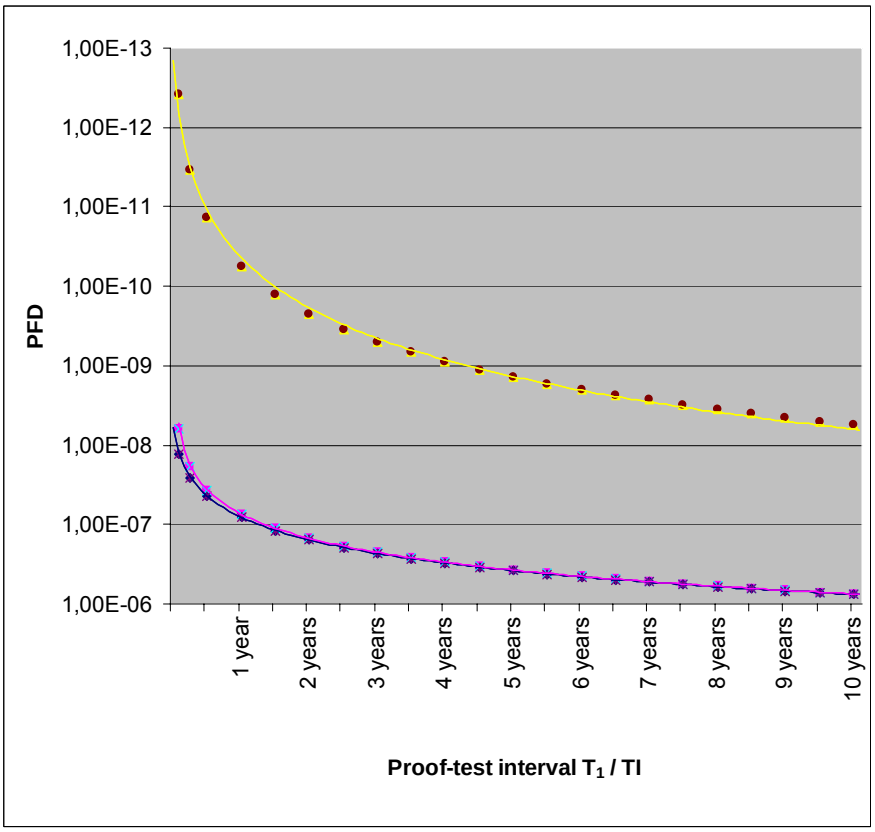

Figure 7: *PFD*-diagram for a 2oo3-system with *DC* = 99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Table 8: *PFD*-values for a 2oo3-system with *DC* = 99 %

	IEC 61508:	ISA TR 84.0.02:	ISA TR 84.0.02:
Proof-test interval *T_1 / TI*	***PFD_{2oo3}* [1]**	***PFD_{2oo3}* with *MTTR* and cc [1]**	***PFD_{2oo3}* without *MTTR* and cc [1]**
1 month	1,307816E-08	6,206638E-09	3,850203E-13
3 months	2,549532E-08	1,862222E-08	3,465182E-12
6 months	4,412670E-08	3,725138E-08	1,386073E-11
1 year	8,140985E-08	7,453048E-08	5,544292E-11
2 years	1,560576E-07	1,491718E-07	2,217717E-10
3 years	2,308141E-07	2,239241E-07	4,989862E-10
4 years	3,056792E-07	2,987872E-07	8,870867E-10
5 years	3,806530E-07	3,737613E-07	1,386073E-09
6 years	4,557354E-07	4,488462E-07	1,995945E-09
7 years	5,309265E-07	5,240420E-07	2,716703E-09
8 years	6,062262E-07	5,993487E-07	3,548347E-09
9 years	6,816346E-07	6,747662E-07	4,490876E-09
10 years	7,571517E-07	7,502947E-07	5,544292E-09

General:

The difference between the *PFD*-values of a 1oo2 and a 2oo3 architecture is marginal, thereby it is not important, using the equations from the ISA or the IEC standard.

Reason:

The difference of both architectures mathematically depends on the different weighting of the single faults, thereby at the 2oo3 architecture the single faults are weighted stronger.

At a 2oo3-system the ISA-graph is under consideration of the *MTTR* and the common-cause failure three to four magnitudes bigger, at low *T1/TI* and *DC* = 99 %, than the ISA-graph without consideration of these two parameters, see figure 7. The deviation between the two graphs increases the higher the *DC*-factor becomes, see figure 8.

Comparing the ISA and the IEC graph under consideration of *MTTR* and common-cause-failure with *DC* = 99 %, see figure 7, both graphs are to be found in the same magnitude. With increasing the *DC*-factor, *DC* = 99,99 %, see figure 8, these both graphs deviate at low T_1/TI by two magnitudes from each other. The reason for this deviation results mainly in the case that in the IEC the part of failures of λ_{DD} is considered during the repair time *MTTR* caused by common-cause-failures by the term $\beta_D \cdot \lambda_{DD} \cdot MTTR$.

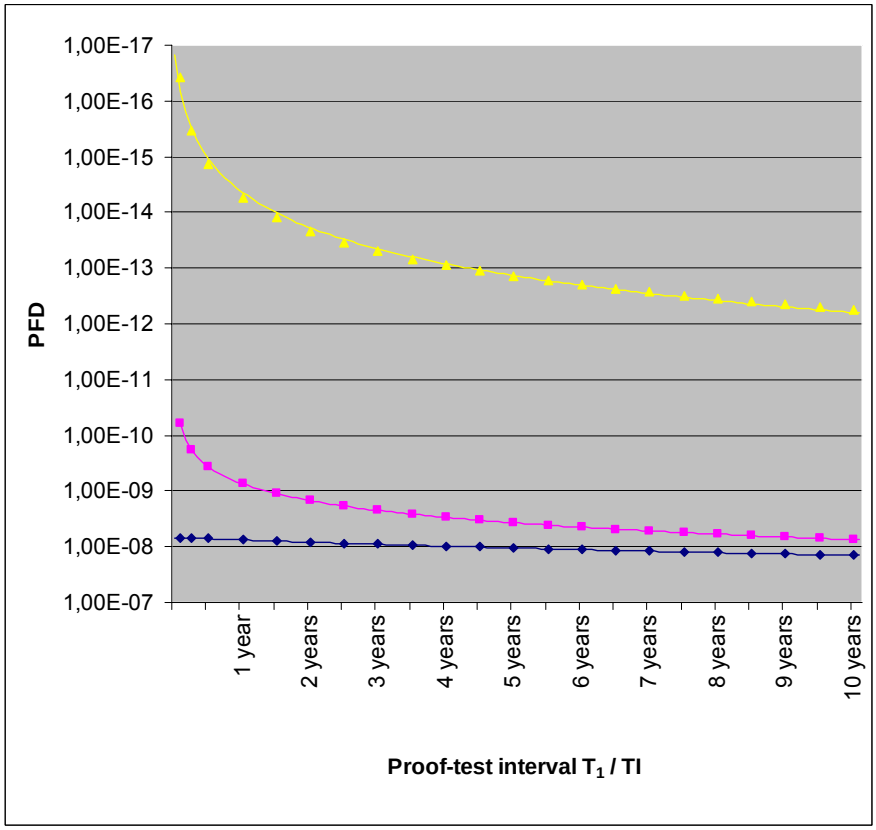

Figure 8: *PFD*-diagram for a 2oo3-system with *DC* = 99,99 %

Legend:

according to IEC 61508, with *MTTR* and common-cause-failure

according to ISA standard, with *MTTR* and common-cause-failure

according to ISA standard, without *MTTR* and without common-cause-failure

Table 9: *PFD*-values for a 2oo3-system with *DC* = 99,99 %

Proof-test interval T_1 / *TI*	IEC 61508: PFD_{2oo3} [1]	ISA TR 84.0.02: PFD_{2oo3} with *MTTR* and cc [1]	ISA TR 84.0.02: PFD_{2oo3} without *MTTR* and cc [1]
1 month	6,865470E-09	6,206270E-11	3,850202E-17
3 months	6,989612E-09	1,861883E-10	3,465182E-16
6 months	7,175825E-09	3,723773E-10	1,386073E-15
1 year	7,548253E-09	7,447574E-10	5,544292E-15
2 years	8,293117E-09	1,489526E-09	2,217717E-14
3 years	9,037992E-09	2,234306E-09	4,989862E-14
4 years	9,782879E-09	2,979096E-09	8,870867E-14
5 years	1,052778E-08	3,723898E-09	1,386073E-13
6 years	1,127268E-08	4,468711E-09	1,995945E-13
7 years	1,201760E-08	5,213535E-09	2,716703E-13
8 years	1,276253E-08	5,958370E-09	3,548347E-13
9 years	1,350747E-08	6,703216E-09	4,490876E-13
10 years	1,425242E-08	7,448073E-09	5,544292E-13

Summary

This short comparison demonstrates the difficulty of the direct comparing between PFD-values that are generated by means of different procedure. In fact using both standards the quantitative values are to be found in the same ranges as long as not the simplified calculations of the ISA-standard are applied. Although the parameters are different leading to these calculations. For example at the ISA standard there are no definitions regarding SFF- / DC-factor. A further criterion is the non existing of the differentiation between type A and Type B subsystems, that has remarkable influence on the structure and on the integrity level of the system. Also there is no differentiation in the ISA standard between β and β_D , here is only considered the better factor for the failure rate λ_{DU}. Further more a difference is the consideration of the part of failures of λ_{DD} during the repair time caused by common-cause-failure. This is not considered in the ISA-standard.

In the IEC 61508 all these factors are considered comparing to the ISA-standard. These consideration increases the demand in safety measures in Hard- and Software in the system. A so designed system is at all more suitable qualified for a safety related application.

In a summary it can be stated that based on the fact that IEC 61508 has an universal application approach and not only applies to the pure safety calculation of systems, this new standard for the functional safety will open a wide spectrum of applications. The approach of the IEC-standard follows the goal and succeeded according to the author's opinion in creating a generic standard for safety related applications.

For the certification of already used complex systems it is necessary to proof the conformity to the standard. Both standards tolerate as all standards do certain latitude at the different integrity levels. It can be stated that e. g. a system certification according to SIL3 represents not necessarily a decision criterion to a complete system. In fact the described system fulfills the requirements of the safety integrity level but it is necessary to keep the prerequisites in mind written down in the so-called certification reports. Generally the limitations of the certified system or plant are to be found in this document.

Literature

[1] IEC/EN 61508: International Standard 61508 Functional Safety: Safety-Related System. Geneva, International Electrotechnical Commission

[2] ISA-TR84.0.02 (1998) Technical Report; Safety Instrumented Systems (SIS) – Safety Integrity Level (SIL) Evaluation Techniques. Instrument Society of America

[3] *Börcsök, J.*: Internationale-/Europa Norm 61508, Vortrag bei der VD-Tagung der HIMA GmbH + Co KG, 2002

[4] *Börcsök, J.*: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen, 2002

[5] *Börcsök, J.*: Sicherheits-Rechnerarchitekturen Teil 1 und 2, Vorlesung Universität Kassel 2000/2001

[6] *Börcsök, J.*: Echtzeit-Betriebssysteme für sicherheitsgerichtete Realzeitrechner, Vorlesung Universität Kassel 2001/2002

[7] VDE 0801 part 1 to 7: Functional safety, Safety related systems, IEC 65A/179/CDV, Draft IEC1508, part 6, p. 26f, August 1998.

[8] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR- Schutzeinrichtungen. Beuth Verlag Berlin 1998

[9] DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben. Beuth Verlag

[10] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung. 12/2001