CHEMICAL ENGINEERING TRANSACTIONS

VOL. 48, 2016

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Eddy de Rademaeker, Peter Schmelzer
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-39-6; **ISSN** 2283-9216

DOI: 10.3303/CET1648107

PFD Calculation Considering Imperfect Proof Tests

Thomas Gabriel*[a], Andreas Hildebrandt[b], Udo Menck[c],

[a]Bayer Technology Services GmbH, OSS-PPS-MTS, Chempark Leverkusen, B407, 51368 Leverkusen, Germany
[b]Pepperl+Fuchs GmbH, Lilienthalstraße 200, 68307 Mannheim, Germany
[c]Dow Deutschland Anlagengesellschaft mbH, Werk Stade, Bützflether Sand, 21683 Stade, Germany
thomas.gabriel@bayer.com

The current state of the art in process and plant safety for the process industries with means of process control technology (PCT) follows the concepts of functional safety as denoted in IEC 61511-1 (2003). Target of the standard is to provide suitable means for ensuring safety integrity of PCT safety functions throughout their entire lifecycle.

Each PCT safety function gets rated with a SIL (safety integrity level) as a measure for the process risk that any particular measure covers. The higher the SIL the higher the requirements towards safety related availability.

Among other requirements, IEC 61511-1 provides two criteria that depend on the target SIL and are tailored towards handling of systematic and random failures preventing a PCT safety function from executing its intended safety function upon demand:

- The minimum required hardware fault tolerance (HFT) criterion demands a minimum degree of redundancy in order to compensate for systematic failures, like design flaws, that could not be eliminated by the safety management system.
- For random hardware failures the average PFD (Probability of Failure on Demand) is to be calculated. It is a probabilistic criterion that is impacted by hardware failure rates, degree of redundancy, diagnostic means, as well as the maintenance strategy.

IEC 61508-6 (2010) (part 6 of the related framework standard to IEC 61511) provides an overview of suitable mathematical methods that could be used to obtain the PFD. However, since most of the approaches tend to generate large and complex system descriptions (e.g. Markov technique) a set of simplified calculation formulae is also provided. From these, a large set of publications have been generated, providing even further simplified PFD calculation approaches, e.g. US ISA TR84.00.02 pt. 2 (2002) or German VDI/VDE 2180 pt. 4 (2010). Simplified equations allow for PFD calculation without the need for elaborate and time-consuming probabilistic models that require well-trained reliability engineers.

A typical disadvantage of available simplified equations is their lack of consideration of imperfect proof tests: While a 100 % test of PCT safety equipment is not feasible in many cases, the related mathematical representation would often become too complex to be presented as a closed equation.

In order to overcome these shortcomings, the current revision of German VDI/VDE and NAMUR PCT safety standards will address said topic by including a set of advanced PFD calculation formulae.

These come for the most common (diverse redundancy) architectures (1oo1, 1oo2, 2oo3, …) and allow for the consideration of individual imperfect proof tests per channel. They can further be combined with partial tests (also with individual proof test coverage per channel).

Together with the equations, recommendations on achievable proof test coverages for both, proof tests and partial tests, will be included.

1. Equation fundamentals, 1oo2 system example

According to IEC 61508-6 (2010), the safety related unavailability of a 1oo2 redundant system (following MooN notation) can be expressed by an equation as given in Eq(1).

Please cite this article as: Gabriel T., Menck U., Hildebrandt A., 2016, Pfd formulae considering imperfect proof tests, Chemical Engineering Transactions, 48, 637-642 DOI:10.3303/CET1648107

$$\begin{aligned} t_{CE} &= \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_\beta}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR,\ t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_\beta}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \\ PFD &= 2\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_\beta}{2} + MRT\right). \end{aligned} \tag{1}$$

In order to avoid confusion with channel subindices introduced later in this paper, the proof test interval T_1, as defined in IEC 61508-6 (2010), Table B.1, is referred to as T_β.

Eq(1) is based on the assumption that all DU failures get revealed during proof tests at multiples of T_β and repaired within MRT. This assumption is overly optimistic for many applications, as in-process calibration or actively induced process upsets for testing purposes are often times not feasible or even dangerous. Furthermore, the equation is based on identical failure rates for both channels. Typically, the larger failure rate is then used for the parameterization of Eq(1). This leads to strong conservatisms in case of significantly differing device failure rates.

For typical safety applications within the process industry scope of IEC 61511-1 (2003) the contribution of dangerous detected (DD) failures to the PFD is negligible, as the failure detection time is typically much smaller than the actual repair time ($MTTR \approx MRT$) and usually $T_\beta \gg MRT$. With this assumption, Eq(1) simplifies to

$$\begin{aligned} t_{CE} &= \frac{T_\beta}{2},\ t_{GE} = \frac{T_\beta}{3} \\ PFD &= 2\big((1-\beta)\lambda_{DU}\big)^2 t_{CE} t_{GE} + \beta \lambda_{DU} \frac{T_\beta}{2}. \end{aligned} \tag{2}$$

In this form, the equation still has the shortcomings as described above. However, from Eq(2) a significant improvement can be achieved by applying a restructuring notation together with an extension to diversely instrumented channels, following Hildebrandt (2007):

$$\begin{aligned} P_{K,1} &= (1-\beta)\lambda_{DU,1}\frac{T_\beta}{2},\ P_{K,2} = (1-\beta)\lambda_{DU,2}\frac{T_\beta}{2} \\ PFD &= (1-\beta)\big(P_{K,1}\lambda_{DU,2} + P_{K,2}\lambda_{DU,1}\big)\frac{T_\beta}{3} + \beta\left(\frac{T_1}{2}\min\{\lambda_{DU,1}, \lambda_{DU,2}\}\right). \end{aligned} \tag{3}$$

$\lambda_{DU,1}$ and $\lambda_{DU,2}$ refer to the respective channel's individual failure rate. The Beta model as implemented here deviates from Hildebrandt (2007), following a policy that for $\beta = 1$ the effective common-cause failure rate must not be larger than the smaller of the two contributing channel failure rates.

The last extension enabling for imperfect proof testing is made based on the suggested equation in IEC 61508-6 (2010), section B.3.2.5, and results in the final set of equations for a 1oo2 system as denoted in Eq(4):

Configuration channel 1:	**Configuration channel 2:**
$\lambda_{\alpha,1} = PTC_{A,1} \cdot \lambda_{DU,1}$	$\lambda_{\alpha,2} = PTC_{A,2} \cdot \lambda_{DU,2}$
$\lambda_{\beta,1} = \big(PTC_{B,1} - PTC_{A,1}\big)\lambda_{DU,1}$	$\lambda_{\beta,2} = \big(PTC_{B,2} - PTC_{A,2}\big)\lambda_{DU,2}$
$\lambda_{\gamma,1} = \big(1 - PTC_{B,1}\big)\lambda_{DU,1}$	$\lambda_{\gamma,2} = \big(1 - PTC_{B,2}\big)\lambda_{DU,2}$

Averages for common-cause contribution:

$$\begin{aligned} PTC_{A,avg} &= \frac{PTC_{A,1} + PTC_{A,2}}{2} \\ PTC_{B,avg} &= \frac{PTC_{B,1} + PTC_{B,2}}{2} \\ \lambda_{\alpha,avg} &= PTC_{A,avg} \cdot \min\{\lambda_{DU,1}, \lambda_{DU,2}\} \\ \lambda_{\beta,avg} &= \big(PTC_{B,avg} - PTC_{A,avg}\big) \cdot \min\{\lambda_{DU,1}, \lambda_{DU,2}\} \\ \lambda_{\gamma,avg} &= \big(1 - PTC_{B,avg}\big) \cdot \min\{\lambda_{DU,1}, \lambda_{DU,2}\} \end{aligned} \tag{4}$$

PFD calculation:

$$\begin{aligned} P_{K1} &= (1-\beta)\left[\lambda_{\alpha,1}\frac{T_\alpha}{2} + \lambda_{\beta,1}\frac{T_\beta}{2} + \lambda_{\gamma,1}\frac{T_\gamma}{2}\right] \\ P_{K2} &= (1-\beta)\left[\lambda_{\alpha,2}\frac{T_\alpha}{2} + \lambda_{\beta,2}\frac{T_\beta}{2} + \lambda_{\gamma,2}\frac{T_\gamma}{2}\right] \\ PFD &= (1-\beta)\left[\big(P_{K1}\lambda_{\alpha,2} + P_{K2}\lambda_{\alpha,1}\big)\frac{T_\alpha}{3} + \big(P_{K1}\lambda_{\beta,2} + P_{K2}\lambda_{\beta,1}\big)\frac{T_\beta}{3} + \big(P_{K1}\lambda_{\gamma,2} + P_{K2}\lambda_{\gamma,1}\big)\frac{T_\gamma}{3}\right] \\ &\quad + \beta\left(\frac{T_\alpha}{2}\lambda_{\alpha,avg} + \frac{T_\beta}{2}\lambda_{\beta,avg} + \frac{T_\gamma}{2}\lambda_{\gamma,avg}\right). \end{aligned}$$

The equation comes along with a set of boundary conditions:

$$T_\alpha \leq T_\beta \leq T_\gamma \tag{5}$$

$$T_\beta = j \cdot T_\alpha; T_\gamma = k \cdot T_\beta; j,k \in \mathbb{N} \tag{6}$$

$$PTC_{A,n} \leq PTC_{B,n} \text{ for } n \in \{1{,}2\} \tag{7}$$

The underlying maintenance strategy consists of a staggered system of three different proof test module elements.

2. Maintenance model

As denoted in Figure 1, each of the proof test module elements α, β, γ is executed after equidistant intervals T_α, T_β, or T_γ, each revealing a fraction λ_α, λ_β, or λ_γ of the channel failure rate λ_{DU} (see Figure 2). Because of Eq(6) multiple proof test module elements have to be executed at the same time at certain multiples of the intervals. These combinations of proof test module elements thus form the three different possible modules A, B, and C. In practice, module B and C will not just consist of the individual proof test plans of the underlying elements, but provide a single combined test plan, incorporating the respective elements' features.

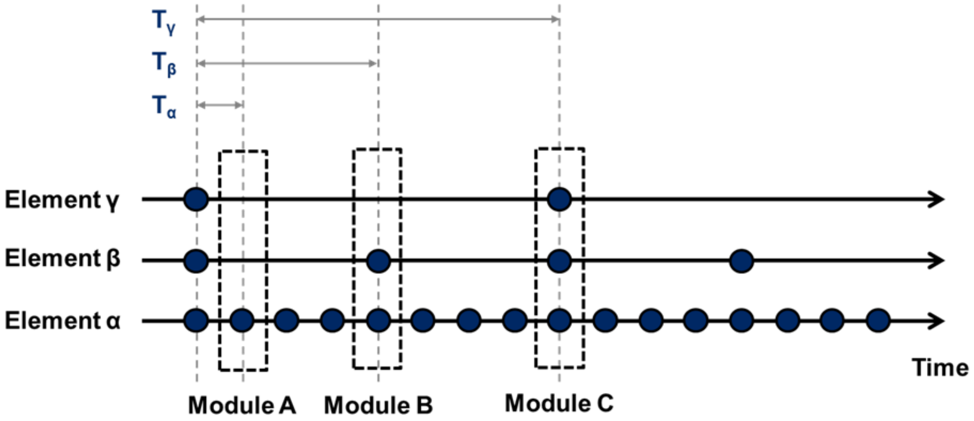

Figure 1: The maintenance model applied throughout the paper consists of three different proof test module elements α, β, and γ. All of these are executed with equidistant intervals. The intervals are chosen in a way that at multiples of T_α, T_β, and T_γ, multiple proof test module elements are executed simultaneously, forming test modules A, B, and C.

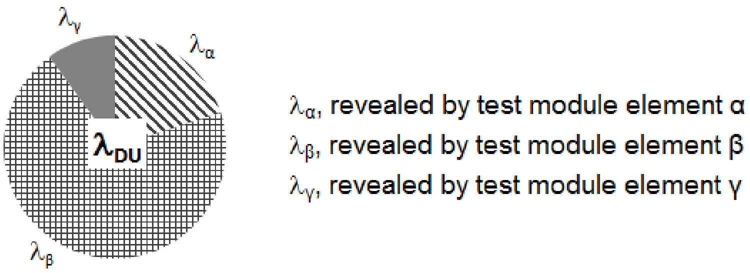

Figure 2: Dangerous undetected failures within a channel can only be revealed by means of testing. The maintenance strategy applied throughout this paper is based on three different test module elements, each capable of revealing a certain fraction of DU failures. When all three test module elements are performed at once, all DU failures potentially contained in a channel are found.

As $\lambda_\alpha + \lambda_\beta + \lambda_\gamma = \lambda_{DU}$ (see Figure 2), it becomes immediately clear, that after execution of module C every T_γ all potential DU failures get revealed from the system. In real world examples this can be achieved by either performing very high quality proof tests (e.g. dismounting and calibration/overhauling in workshop), or replacing devices with new ones. Typical reasonable values lie between 15 and 20 years. In worst case scenarios the value corresponds to the plant's mission time (~30 years to 40 years). Both strategies, high quality testing and replacing, mathematically result in the requirement of module C to entirely remove DU failures from the considered channel.

Module B is related to the proof test activities executed every T_β. The interval corresponds to T_1 in IEC 61508-6 (2010). Typical values in the process industry range from 1 to 3 years up to 5 years for petrochemical plants. From figure 1 and Figure 2 it can be derived that module B combines the proof test procedures of elements α and β, the revealed fraction of DU failures at multiples of T_β thus corresponds to $\lambda_\alpha + \lambda_\beta$.

$$PTC_{B,n} = \frac{\lambda_{\alpha,n} + \lambda_{\beta,n}}{\lambda_{DU,n}} \tag{8}$$

Following Eq(8), the proof test coverage related to module B can be defined for every single channel $n\epsilon\{1,2\}$. It is utilized in Eq(4). Consequently, module C describes a maintenance activity that is executed every T_α and only reveals a small portion of DU failures from the channel:

$$PTC_{A,n} = \frac{\lambda_{\alpha,n}}{\lambda_{DU,n}} \tag{9}$$

Typical applications for this type of proof test activity are partial stroke tests, or partial tests of sensors (e.g. plausibility check of sensor signal, test buttons, …). Selecting $PTC_{A,n} = 0$ mathematically results in not performing a partial test on the system under consideration.

Notice that for very small T_α the partial test interval gets in the same range as MRT and thus leads to a probably negligible PFD contribution (see considerations made for derivation of Eq(2)).

Due to the introduction of the failure rates λ_α, λ_β, λ_γ according to Figure 2, together with the definitions for the proof test coverages in Eq(8) and Eq(9), it has to be made sure that $PTC_{B,n} > PTC_{A,n}$. A partial test at T_α is thus always less efficient than a regular proof test at T_β.

3. Further PFD equations

Based on the equation fundamentals from chapter 1 together with the explanation of the underlying maintenance strategy from chapter 2 further PFD calculation equations can be provided. All of them share the same properties:

- Diverse redundancy (where applicable)
- Channel individual proof test coverages (between 0 and 100 %) for
    - partial test (interval T_α) and
    - regular proof tests (interval T_β)

Channel indices and module names correspond to the notation used before.

3.1 PFD for 1oo1 system

Configuration channel 1:

$$\lambda_{\alpha,1} = PTC_{A,1} \cdot \lambda_{DU,1}$$
$$\lambda_{\beta,1} = (PTC_{B,1} - PTC_{A,1})\lambda_{DU,1}$$
$$\lambda_{\gamma,1} = (1 - PTC_{B,1})\lambda_{DU,1} \tag{10}$$

PFD calculation:

$$PFD = \lambda_{\alpha,1}\frac{T_\alpha}{2} + \lambda_{\beta,1}\frac{T_\beta}{2} + \lambda_{\gamma,1}\frac{T_\gamma}{2}$$

3.2 PFD for 2oo3 system

Configuration channel 1:

$$\lambda_{\alpha,1} = PTC_{A,1} \cdot \lambda_{DU,1}$$
$$\lambda_{\beta,1} = \left(PTC_{B,1} - PTC_{A,1}\right)\lambda_{DU,1}$$
$$\lambda_{\gamma,1} = \left(1 - PTC_{B,1}\right)\lambda_{DU,1}$$

Configuration channel 2:

$$\lambda_{\alpha,2} = PTC_{A,2} \cdot \lambda_{DU,2}$$
$$\lambda_{\beta,2} = \left(PTC_{B,2} - PTC_{A,2}\right)\lambda_{DU,2}$$
$$\lambda_{\gamma,2} = \left(1 - PTC_{B,2}\right)\lambda_{DU,2}$$

Configuration channel 3:

$$\lambda_{\alpha,3} = PTC_{A,3} \cdot \lambda_{DU,3}$$
$$\lambda_{\beta,3} = \left(PTC_{B,3} - PTC_{A,3}\right)\lambda_{DU,3}$$
$$\lambda_{\gamma,3} = \left(1 - PTC_{B,3}\right)\lambda_{DU,3}$$

Averages for common-cause contribution:

$$PTC_{A,avg} = \frac{PTC_{A,1}+PTC_{A,2}+PTC_{A,3}}{3}$$

$$PTC_{B,avg} = \frac{PTC_{B,1}+PTC_{B,2}+PTC_{B,3}}{3}$$

$$\lambda_{\alpha,avg} = PTC_{A,avg} \cdot \min\left\{\lambda_{DU,1}, \lambda_{DU,2}, \lambda_{DU,3}\right\}$$

$$\lambda_{\beta,avg} = \left(PTC_{B,avg} - PTC_{A,avg}\right) \cdot \min\left\{\lambda_{DU,1}, \lambda_{DU,2}, \lambda_{DU,3}\right\} \tag{11}$$

$$\lambda_{\gamma,avg} = \left(1 - PTC_{B,avg}\right) \cdot \min\left\{\lambda_{DU,1}, \lambda_{DU,2}, \lambda_{DU,3}\right\}$$

PFD calculation:

$$P_{K,12} = \left(1-\frac{3}{2}\beta\right)\left[\left(\lambda_{\alpha,1}\frac{T_\alpha}{2} + \lambda_{\beta,1}\frac{T_\beta}{2} + \lambda_{\gamma,1}\frac{T_\gamma}{2}\right) + \left(\lambda_{\alpha,2}\frac{T_\alpha}{2} + \lambda_{\beta,2}\frac{T_\beta}{2} + \lambda_{\gamma,2}\frac{T_\gamma}{2}\right)\right]$$
$$P_{K,23} = \left(1-\frac{3}{2}\beta\right)\left[\left(\lambda_{\alpha,2}\frac{T_\alpha}{2} + \lambda_{\beta,2}\frac{T_\beta}{2} + \lambda_{\gamma,2}\frac{T_\gamma}{2}\right) + \left(\lambda_{\alpha,3}\frac{T_\alpha}{2} + \lambda_{\beta,3}\frac{T_\beta}{2} + \lambda_{\gamma,3}\frac{T_\gamma}{2}\right)\right]$$
$$P_{K,13} = \left(1-\frac{3}{2}\beta\right)\left[\left(\lambda_{\alpha,1}\frac{T_\alpha}{2} + \lambda_{\beta,1}\frac{T_\beta}{2} + \lambda_{\gamma,1}\frac{T_\gamma}{2}\right) + \left(\lambda_{\alpha,3}\frac{T_\alpha}{2} + \lambda_{\beta,3}\frac{T_\beta}{2} + \lambda_{\gamma,3}\frac{T_\gamma}{2}\right)\right]$$

$$PFD = \left(1-\frac{3}{2}\beta\right)\left[\left(P_{K,23}\lambda_{\alpha,1} + P_{K,13}\lambda_{\alpha,2} + P_{K,12}\lambda_{\alpha,3}\right)\frac{T_\alpha}{3} + \left(P_{K,23}\lambda_{\beta,1} + P_{K,13}\lambda_{\beta,2} + P_{K,12}\lambda_{\beta,3}\right)\frac{T_\beta}{3} + \left(P_{K,23}\lambda_{\gamma,1} + P_{K,13}\lambda_{\gamma,2} + P_{K,12}\lambda_{\gamma,3}\right)\frac{T_\gamma}{3}\right] + \frac{3}{2}\beta\left(\frac{T_\alpha}{2}\lambda_{TD,avg} + \frac{T_\beta}{2}\lambda_{T1,avg} + \frac{T_\gamma}{2}\lambda_{TM,avg}\right)$$

Eq(11) follows IEC 61508-6 (2010), Table D.5, for the modification of β in case of a voting algorithm other than 1oo2.

4. Current German standardization activities

Following IEC 61511 (2010), which is currently under revision (as of September 2015), many national follow-up standards also undergo regular maintenance. While VDI/VDE 2180 pt. 4 (2010) covers simplified PFD calculation formulae assuming 100 % proof test coverage, the new release will contain different sets of equations for various maintenance strategies, including an approach as provided in this paper. The release of the new VDI/VDE 2180 will be synchronized with IEC 61511.

An important question has not been touched throughout chapters 1 to 3: how to chose $PTC_{A,n}$ and $PTC_{B,n}$ for a given setup?

While some manufacturers provide their safety manuals with suitable proof test instructions and related proof test coverages, the availability of this kind of data is still very low, especially on final element side. A frequently discussed question is related to the proof test coverage of a regular proof test of a valve, including visual external inspection and functional test, but without internal inspection (or leakage test). It can easily be shown that this value has significant consequences for state-of-the-art safety systems in the process industries.

Therefore, the new release of the current NAMUR NE 106 (2007) will provide conservative, but reasonable, PTC bands for generic proof test activities, including partial and full stroke tests for valves, as well as multiple approaches for sensors. Release is expected together with the new VDI/VDE 2180 pt. 4.

5. Conclusions

The advanced PFD calculation equations provided in this paper close an important gap for reliability engineers working in the process industries. They enable for the consideration of diversely instrumented safety systems and bring a more realistic approach towards proof test strategies including imperfect proof tests. While the formulae therefore overcome the shortcomings of simplified equations as provided by many current standards they remain simple enough to allow for an implementation in any spreadsheet program across any company. This effect is significant as it enables engineers to integrate the required reliability considerations in already existing tool landscapes, databases, and workflows, without the need to maintain interfaces to professional standalone reliability software

Symbols and abbreviations

Table 1: Symbols

Symbol	Description	Comment
β	Common-cause factor	See also IEC 61508-6 (2010), Table B.1
λ_{DD}	Failure rate for dangerous detected failures	Related to dangerous channel failures that can be automatically revealed by internal diagnostic means; see also IEC 61508-6 (2010), Table B.1
λ_{DU}	Failure rate for dangerous undetected failures	Related to dangerous passive channel failures that can only be revealed by means of a test as part of the maintenance strategy; see also IEC 61508-6 (2010), Table B.1
$\lambda_{DU,n}$	DU failure rate for the *n*-th channel of a voted group	$n \epsilon \{1,2\}$ for a 1oo2 group; $n \epsilon \{1,2,3\}$ for a 2oo3 group
$\min\{\cdot\}$	Minimum function	Delivers the minimum value contained in the specified set
PFD	Probability of Failure on Demand	Safety related unavailability; throughout the paper PFD refers to the averaged probability of failure on demand rather than $PFD(t)$; see also IEC 61508-6 (2010), Table B.1
PTC	Proof Test Coverage	Denotes the fraction of dangerous passive channel failures that can be revealed with a specific test procedure; see also IEC 61508-6 (2010), Table B.1
$PTC_{m,n}$	Proof Test Coverage related to the *m*-th test module of the *n*-th channel	$n \epsilon \{1,2\}$ for a 1oo2 group; $n \epsilon \{1,2,3\}$ for a 2oo3 group; $m \epsilon \{1,2\}$ for the maintenance model presented in this paper
T_α	Partial test interval	
T_β	Proof test interval	Corresponds to T_1 in IEC 61508-6 (2010), Table B.1; renamed here in order to avoid confusion with channel subindices
T_γ	Mission time interval	

Table 2: Abbreviations

Symbol	Description	Comment
HFT	Hardware Fault Tolerance	See IEC 61511 (2003), section 11.4
MooN	M-out-of-N	The voting architecture notion following IEC 61511 (2003), section 3.2.45
MRT	Mean Repair Time	See also IEC 61508-6 (2010), Table B.1
MTTR	Mean Time to Restauration	See also IEC 61508-6 (2010), Table B.1
PCT	Process Control Technology	
SIL	Safety Integrity Level	SIL$\epsilon\{1,2,3,4\}$; target quality level for a safety instrumented function as introduced by IEC 61511 (2003); imposes target values for the PFD, as well as for the minimum required failure tolerance for a MooN group

References

Hildebrandt A., 2007, Berechnung der “Probability of Failure on Demand” (PFD) einer heterogenen 1-aus-2-Struktur in Anlehnung an die EN 61508, atp – Automatisierungstechnische Praxis 10-2007, 73-80.

IEC 61508-6, 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

IEC 61511-1, 2003, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

ISA TR84.00.02 pt. 2 (2002), Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations

NAMUR NE 106 (2007), Test Intervals of Safety Instrumented Systems

VDI/VDE 2180 pt. 4 (2010), Safeguarding of industrial process plants by means of process control engineering – Verification of the hardware safety integrity of safety instrumented systems