CHEMICAL ENGINEERING TRANSACTIONS
VOL. 33, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Enrico Zio, Piero Baraldi

ISBN 978-88-95608-24-2; **ISSN** 1974-9791
DOI: 10.3303/CET1333082

IEC 61508: Effect of Test Policy on the Probability of Failure on Demand of Safety Instrumented Systems

Sergio Contini[a], Sabrina Copelli*[a], Massimo Raboni [a], Vincenzo Torretta [a], Carlo Sala Cattaneo [b], Renato Rota [b]

[a] Università degli Studi dell'Insubria - Dip. di Scienza e Alta Tecnologia, Via G.B. Vico 46 - 21100 Varese - Italy
[b] Politecnico di Milano - Dip. di Chimica, Materiali e Ingegneria Chimica "G. Natta", Via Mancinelli 7 - 20131 Milano - Italy
sabrina.copelli@uninsubria.it

Standard IEC 61508 provides probabilistic equations for determining the Average Probability of Failure on Demand (PFD_{avg}) and the Average Probability of Failure per Hour (PFH_{avg}) for some architectures of Safety Instrumented Systems (SIS) under the hypothesis of equal redundant components, taking into account Common Cause Failures (CCF), Detection Coverage (DC) and Proof Test Coverage (PTC) parameters. Surprisingly, IEC standard does not mention the testing policy aspects of SIS redundant components. However, from a close examination of the probabilistic equations, it is possible to recognize that the simultaneous/sequential testing policy has been implicitly assumed.
This paper describes the conditions under which the staggered testing policy - which is better than all the others in case of independent tested components - can be advantageously applied to reduce PFD_{avg} when CCF, DC and PTC parameters are taken into account.

1. Introduction

In 2010, the International Electro-technical Commission issued the second edition of the standard IEC 61508 on the unavailability and failure frequency of safety-related functions containing electrical/electronic/programmable electronic components. The standard defines, among other features, qualitative and quantitative methods to determine, for Safety Instrumented Systems, the Average Probability of Failure on Demand (for low demand mode of operation) and the Average Probability of Failure per Hour (for high demand or continuous mode of operation). Low/high demand mode refers to the frequency at which the SIS is called to operate with respect to the test frequency.
In order to get a scale of performance of a SIS, the concept of Safety Integrity Level (SIL) was introduced. Particularly, such a concept concerns the probability that a Safety Instrumented System performs satisfactorily the required safety functions under stated conditions and for a given period of time. Four SIL levels, which are expressed in terms of PFD_{avg} and PFH_{avg}, are defined in the standard. Table 1 shows the SIL levels for the two previously cited modes of operations (that is, low and high/continuous). Each level entails clearly defined design, construction and operational procedures, aiming at assuring the adequate level of quality and reliability of the safety function components.
The failure type of a safety system component can be "safe" or "danger". Fail safe failures cause spurious trips which put the plant in a safe condition. Dangerous failures prevent the safety system to correctly act on demand leading to dangerous situations. The total failure rate λ of a component is given by the following equation:

$$\lambda = \lambda_D + \lambda_S \quad (1)$$

where λ_D and λ_S are respectively the dangerous (subscript D) and safe (subscript S) failure rates. In this paper we deal with dangerous failures only. Particularly, dangerous failure rate λ_D can be then subdivided into λ_{DD} and λ_{DU}, where the second subscript D means detected and U undetected.

Please cite this article as: Contini S., Copelli S., Raboni M., Torretta V., Sala Cattaneo C., Rota R., 2013, Iec 61508: effect of test policy on the probability of failure on demand of safety instrumented systems, Chemical Engineering Transactions, 33, 487-492
DOI: 10.3303/CET1333082

Table 1: Intervals of SIL levels in IEC 61508.

SIL	Low-demand mode PFD_{avg}	High or continuous demand mode PFH_{avg}
4	$\geq 1.0 \cdot 10^{-5}$ to $< 1.0 \cdot 10^{-4}$	$\geq 1.0 \cdot 10^{-9}$ to $< 1.0 \cdot 10^{-8}$
3	$\geq 1.0 \cdot 10^{-4}$ to $< 1.0 \cdot 10^{-3}$	$\geq 1.0 \cdot 10^{-8}$ to $< 1.0 \cdot 10^{-7}$
2	$\geq 1.0 \cdot 10^{-3}$ to $< 1.0 \cdot 10^{-2}$	$\geq 1.0 \cdot 10^{-7}$ to $< 1.0 \cdot 10^{-6}$
1	$\geq 1.0 \cdot 10^{-2}$ to $< 1.0 \cdot 10^{-1}$	$\geq 1.0 \cdot 10^{-6}$ to $< 1.0 \cdot 10^{-5}$

The Standard considers the use of a diagnostic testing (a feature sometimes provided in programmable electronic components) able to reveal all failures or only a part of them. The fraction of revealed failures is represented by the Detection Coverage parameter, defined as:

$$DC = \lambda_{DD} / \lambda_D \tag{2}$$

Hence, dangerous detected failures are modelled as on-line repairable with the following equation:

$$\lambda_{DD} = \lambda_D \cdot DC \tag{3}$$

whereas dangerous undetected failures are modelled as tested using the complementary expression:

$$\lambda_{DU} = \lambda_D \cdot (1 - DC) \tag{4}$$

SIL level calculation for a safety system is described in the standard IEC 61508 with reference to Reliability Block Diagrams (i.e. a success oriented model) for some koon (k out of n) configurations of equal components as a function of failure rate, λ, repair time, τ, test interval, θ, Common Cause Failure (CCF), beta factor, β, Detection Coverage (DC) and Proof Test Coverage (PTC) parameters. Considered configurations are such that $n < 3$ and $k \leq n$, i.e. from 1oo1 to 3oo3 (Börcsök et al., 2007).

The Detection Coverage DC, as mentioned above, represents the fraction of failures revealed by a self-diagnostic feature of the component whereas the PTC parameter accounts for incomplete tests. Indeed, PTC < 1 means that the periodic test is able to check the working conditions of only a part of the component (e.g. the case of partial stroke testing of valves); the failure of the non tested parts (1-PTC) remains hidden until the end of the mission or the time at which a complete functional test is performed.
As shown by Lundteigen and Rausand (2008) a careful examination of the component and of the testing operation is necessary to define the PTC value.
Innal et al. (2010) and Dutuit et al. (2008) described the implementation of algorithms for calculating PFD_{avg} and PFH_{avg} by means of a fault tree (i.e. a failure oriented model), considering CCF; however, their equations do deal with DC and PTC parameters.
IEC 61508 equations have been implemented in ASTRA 3, the fault tree analyser developed at the Joint Research Centre of the European Commission (Contini et al., 2009; Contini and Matuzas, 2011), with the aim of simplifying the fault tree modelling of any configuration of safety related functions (i.e. not limited to $n \leq 3$) and correctly quantifying PFD_{avg} and PFH_{avg} also in the case of unequal components. This was obtained by defining a new 6-parameters model for tested components, obtained by combining the three fundamental models, namely: a) on-line repairable; b) tested and c) not repairable, weighted by Detection Coverage (DC) and Proof Test Coverage (PTC) parameters. CCF is dealt with using the beta factor method, with the conservative approximation that the beta factor is the same for both revealed and unrevealed failures. In this way the fault tree construction can be significantly simplified and the probabilistic results correctly determined. In brief, ASTRA method determines PFD(t) and PFH(t) functions for any configuration and any number of components, from which the mean and the maximum values are finally determined.
As pointed out by Dutuit et al. (2008), the mean value of the PFD_{avg} is not sufficient to state that the protective system presents a given SIL level. Indeed, the unavailability function has the classical saw-tooth behaviour with peaks that may enter into a worst SIL level region. As an example, let us suppose that, according to PFD_{avg} and PFD_{max} values, we have respectively SIL 2 and SIL 1. In these cases, it is sound to determine the percentage of the mission time the system works in the SIL 1 region.
The testing policy defines the way through which redundant components should be tested to minimise PFD_{avg}. Three types of policies could be applied: Simultaneous, Sequential and Staggered.

The simultaneous testing policy means that all components are put off-line and tested every θ hours; during the test the safety function is not available.
With the sequential testing policy the components are tested every θ hours, but one after the other in such a way that only one component at a time is put off-line for testing.
In the staggered testing policy components are tested regularly in an overlapping sequence; i.e. given k tested components in parallel, each component is tested every θ hours, but the time between two tests is θ/k hours. As an example, if k=3 and θ=3,000 h, the first component is tested at 1000 h, the second at 2000 h, the third at 3000 h, the first again at 4,000 h, and so on.
Surprisingly, IEC 61508 standard does not discuss the type of testing policy of redundant components and, consequently, it does not give any recommendation about the policy to apply. However, from the equations described in that report, it is possible to argue that the simultaneous/sequential policy was implicitly adopted. Since the sequential policy is always better than the simultaneous one, in the following the latter will be no more considered.
ASTRA implementation of the IEC standard allows studying the effect on PFD_{avg} of different testing policies of redundant components.
The aim of this paper has been to compare, with the use of ASTRA, the effects of sequential and staggered testing policies on both PFD_{avg} and PFD_{max} and outline the conditions under which the latter may be more conveniently applied with respect to the former. This study has been performed on some redundant configurations of SIS made up by components characterised by CCF, DC and PTC parameters.
The content of this paper assumes that the reader is familiar with the basis of the system reliability theory (Rausand and Høyland, 2003; Smith and Simpson, 2011), the calculation methods of the IEC 61508 standard (Hokstad and Cornelliussen, 2004; Langeron et al., 2008) and the safety applied to systems and instruments, for which the literature is very rich (see e.g. Lundteigen et al., 2009; Necci et al., 2012; MacDonald, 2003).

2. Test policies of redundant components

When a repairable component presents unrevealed dangerous faults, it has to be periodically tested to verify whether it will be working properly on demand. After the test, if the component is found failed, it is immediately repaired.
A safety function is implemented by sensors, logic solver and actuators. The times at which components are tested have an impact on the on-demand unavailability of the safety function. This section discusses the types of applicable test policies and their impact on functional safety.
Any koon failure logic is modelled as a series of n!/[k!(n-k)]! parallel configurations each one made up by k components. For instance, a 2oo3 logic is represented as a series of 3 subsystems each one made up by 2 components in parallel.
The mean unavailability of each component is given by the sum of three contributions: Q_1, the mean unavailability due to unrevealed failures between tests (mean duration: θ/2); Q_2, the unavailability due to test (mean duration: γ); and Q_3 the unavailability due to repair (mean duration: τ).
Conservative approximated equations for determining the three contributions to the mean unavailability of a generic parallel of k equal components are provided in Table 2. Equations are based on the following assumptions: $\lambda\,\theta < 0.1$; $\tau+\gamma \ll \theta$; test perfect (no human error during test).

Table 2: Contribution to PFD_{avg} for sequential and staggered testing policies (λ represents the dangerous failure rate λ_{DD}).

Unavailability contribution	Sequential	Staggered	Staggered / Sequential (Reduction Factor, RF)
Q_1 between tests	$Q_1 = \frac{1}{k+1}\lambda^k\ \theta^k$	$Q_1 = \frac{k!\,(k+3)}{4\,k^k\ (k+1)}\lambda^k\ \theta^k$	$\frac{k!\,(k+3)}{4\,k^k}$
Q_2 due to test	$Q_2 = \lambda^{k-1}\ \theta^{k-2}\ \gamma$	$Q_2 = \frac{(k-1)!}{k^{k-2}}\lambda^{k-1}\ \theta^{k-2}\ \gamma$	$\frac{(k-1)!}{k^{k-2}}$
Q_3 due to repair	$Q_3 = \lambda^k\ \theta^{k-1}\ \tau$	$Q_3 = \frac{(k-1)!}{k^{k-2}}\lambda^k\ \theta^{k-1}\ \tau$	$\frac{(k-1)!}{k^{k-2}}$

The policy that gives the greater unavailability reduction is the staggered one, as shown by the reduction factor (RF) expression in the last column of Table 2. Table 3 shows the numerical values of the RF for parallel redundant configurations made up by k components ($2 \le k \le 5$). RF represents the maximum difference on mean unavailability between staggered and sequential policies.

Table 3: Maximum reduction factors RF

k	Between tests	Due to test	Due to repair
2	0.625	1	1
3	0.333	0.66	0.66
4	0.164	0.375	0.375
5	0.077	0.192	0.192

IEC 61508 documentation does not explicitly state the type policy, even if, from PFD_{avg} equations, it is possible to see that the sequential one is implicitly considered. Hence, nothing is said about the staggered testing type.
A question arises about the staggered testing: "under which conditions, could it be advantageously applied to safety instrumented systems when the contribution of CCF, DC and PTC are considered in calculating PFD_{avg} and PFD_{max}?".
The current section answers the above question showing the comparison between sequential and staggered testing policies on a test case analysed by means of ASTRA (Contini and Matuzas, 2011), in which IEC equations are implemented as a 6-parameters model. All considerations that follow are based only on probabilistic results and do not account for the costs associated with the two test policies.
Table 4 provides PFD_{avg} and PFD_{max} values for three redundant configurations in the hypothesis that each component has no diagnostic capability (DC = 0), the test is able to detect all failure conditions (PTC = 1) and CCF is ignored. Each component is characterized by: λ = 5.0e-6 h^{-1}; τ = 8 h; and θ = 4380 h.

Table 4: Δ% reduction on PFD_{avg} and PFD_{max} for kook when CCF=no; DC= 0; PTC=1.

Degree of Redundancy	PFD_{avg} Sequential	PFD_{avg} Staggered	Δ%	PFD_{max} Sequential	PFD_{max} Staggered	Δ%
2oo2:F	$1.62 \cdot 10^{-4}$	$1.02 \cdot 10^{-4}$	37.5	$4.71 \cdot 10^{-4}$	$2.35 \cdot 10^{-4}$	50.0
3oo3:F	$2.70 \cdot 10^{-6}$	$8.58 \cdot 10^{-7}$	68.2	$1.02 \cdot 10^{-5}$	$2.29 \cdot 10^{-6}$	77.5
4oo4:F	$4.85 \cdot 10^{-8}$	$7.89 \cdot 10^{-9}$	83.7	$2.22 \cdot 10^{-7}$	$2.11 \cdot 10^{-8}$	90.5

The measure of the convenience of applying the staggered policy instead of the sequential one is represented by the Δ% value, defined as:

$$\Delta\% = (1 - \frac{Staggered}{Sequential})100 = (1 - RF)100 \quad (5)$$

The greater is the redundancy degree, the lower are PFD_{avg} and PFD_{max} and the greater is Δ% difference. Note that the relative percentage difference Δ% is larger for PFD_{max}, i.e. the staggered testing has also an important reduction effect on the maximum unavailability value.
As mentioned before the Δ% values are the maximum achievable ones under the hypotheses of equal components and negligible test and repair contributions; under these conditions it can also be proved that Δ% does not depend on λ and θ.
The Δ% unavailability reduction in Table 4 will be lowered when DC and PTC parameters are introduced.
If the status of k equal components is continuously monitored, or when their failure is immediately revealed, then safety will be influenced by the DC parameter. In particular if DC = 100% all components behave as on-line repairable, i.e. there is no need of testing them. In this case Δ% = 0. On the contrary, if DC = 0% all components are modeled as purely tested, which means that the maximum difference is that provided in Table 4. For a given k it can be analytically proved that Δ% is independent on the failure rate, whereas it slightly increases as the test interval θ increases.
Table 5 provides the PFD_{avg} and PFD_{max} for different DC% values for two redundant configurations: 2oo2:F and 3oo3:F. Table 6 provides ASTRA results for 2oo2:F and 3oo3:F parallel configurations with different values of the PTC parameter.
As it can be seen, the staggered policy is better than the sequential one provided that DC< 90%. For DC values greater than 90% the advantage rapidly decreases, due to the fact that on-line repairable behaviour of components gives the major contributor to PFD(t). At DC = 100% only the repairable contribution is present, i.e. testing contribution is zero. The maximum Δ% value is obtained with PTC = 1; for different kook configurations this value is that one provided by Table 4. The minimum value Δ% = 0 is obtained with PTC = 0, which corresponds to a situation in which all components are not repairable.
As it can be seen from Table 6 the practical advantage of the staggered testing is with PTC = 1. It can be analytically proved that Δ% is independent from the failure rate, whereas it depends on the test interval.

Table 5: Δ% reduction on PFD_{avg} and PFD_{max} when CCF=no; DC ≥ 0; PTC=1.

DC	Redundancy Degree	PFD_{avg} Sequential	PFD_{avg} Staggered	Δ%	PFD_{max} Sequential	PFD_{max} Staggered	Δ%
0 %	2oo2:F	$1.62 \cdot 10^{-4}$	$1.02 \cdot 10^{-4}$	37.0	$4.71 \cdot 10^{-4}$	$2.37 \cdot 10^{-4}$	49.7
30 %		$8.00 \cdot 10^{-5}$	$5.03 \cdot 10^{-5}$	37.1	$2.33 \cdot 10^{-4}$	$1.17 \cdot 10^{-4}$	49.8
60 %		$2.64 \cdot 10^{-5}$	$1.66 \cdot 10^{-5}$	37.1	$7.67 \cdot 10^{-5}$	$3.86 \cdot 10^{-5}$	49.7
90 %		$1.71 \cdot 10^{-6}$	$1.11 \cdot 10^{-6}$	35.1	$4.96 \cdot 10^{-6}$	$2.53 \cdot 10^{-6}$	49.0
99 %		$2.67 \cdot 10^{-8}$	$2.04 \cdot 10^{-8}$	26.6	$6.71 \cdot 10^{-8}$	$3.84 \cdot 10^{-8}$	42.8
100 %		$1.59 \cdot 10^{-9}$	$1.59 \cdot 10^{-9}$	0.0	$1.59 \cdot 10^{-9}$	$1.59 \cdot 10^{-9}$	0.0
0 %	3oo3:F	$2.70 \cdot 10^{-6}$	$8.58 \cdot 10^{-7}$	68.2	$1.02 \cdot 10^{-5}$	$2.29 \cdot 10^{-6}$	77.5
30 %		$9.39 \cdot 10^{-7}$	$2.97 \cdot 10^{-7}$	68.3	$3.55 \cdot 10^{-6}$	$7.95 \cdot 10^{-7}$	77.6
60 %		$1.78 \cdot 10^{-7}$	$5.67 \cdot 10^{-8}$	68.1	$6.72 \cdot 10^{-7}$	$1.51 \cdot 10^{-7}$	77.5
90 %		$2.96 \cdot 10^{-9}$	$9.90 \cdot 10^{-10}$	66.5	$1.10 \cdot 10^{-8}$	$2.56 \cdot 10^{-9}$	76.7
99 %		$5.31 \cdot 10^{-12}$	$2.96 \cdot 10^{-12}$	44.2	$1.74 \cdot 10^{-11}$	$5.42 \cdot 10^{-12}$	68.8
100 %		$6.39 \cdot 10^{-14}$	$6.39 \cdot 10^{-14}$	0.0	$6.39 \cdot 10^{-14}$	$6.39 \cdot 10^{-14}$	0-0

Table 6: Δ% reduction on PFD_{avg} and PFD_{max} when CCF= no; DC = 0; PTC ≤ 1.

PTC	Redundancy	PFD_{avg} Sequential	PFD_{avg} Staggered	Δ%	PFD_{max} Sequential	PFD_{max} Staggered	Δ%
1	2oo2:F	$1.62 \cdot 10^{-4}$	$1.00 \cdot 10^{-4}$	38.3	$4.71 \cdot 10^{-4}$	$2.37 \cdot 10^{-4}$	49.7
0.9		$2.40 \cdot 10^{-4}$	$2.01 \cdot 10^{-4}$	16.25	$8.08 \cdot 10^{-4}$	$5.59 \cdot 10^{-4}$	30.8
0.7		$5.77 \cdot 10^{-4}$	$5.51 \cdot 10^{-4}$	4.67	$1.84 \cdot 10^{-3}$	$1.61 \cdot 10^{-3}$	12.5
0.5		$1.13 \cdot 10^{-3}$	$1.11 \cdot 10^{-3}$	1.77	$3.45 \cdot 10^{-3}$	$3.29 \cdot 10^{-3}$	4.64
1	3oo3:F	$2.70 \cdot 10^{-6}$	$8.40 \cdot 10^{-7}$	68.9	$1.02 \cdot 10^{-5}$	$2.29 \cdot 10^{-6}$	77.5
0.9		$4.85 \cdot 10^{-6}$	$2.96 \cdot 10^{-6}$	39.0	$2.29 \cdot 10^{-5}$	$1.08 \cdot 10^{-5}$	52.8
0.7		$1.72 \cdot 10^{-5}$	$1.55 \cdot 10^{-5}$	9.9	$7.29 \cdot 10^{-5}$	$5.07 \cdot 10^{-5}$	30.5
0.5		$4.82 \cdot 10^{-5}$	$4.69 \cdot 10^{-5}$	2.7	$2.02 \cdot 10^{-4}$	$1.84 \cdot 10^{-4}$	8.9

Finally Table 7 provides PFD_{avg} and PFD_{max} values for 2oo2:F and 3oo3:F architectures with the beta factor ranging between 1 % and 20 %. Increasing the CCF contribution to system failure obviously increases both PFD_{avg} and PFD_{max}, independently on the adopted policy. However the Δ% values remain constant, meaning that the CCF has no influence on the relative difference between sequential and staggered policies. As described in the IEC 61508 report, this is due to the fact that the event describing the CCF is tested each time a component is tested. Consequently, in case of staggered testing, the CCF event is tested k times during the test interval θ, whereas according to the sequential testing this occurs only once. It can be proved that for kook configurations Δ% is about 1/k. Hence for 4oo4 and 5oo5 configurations the Δ% values are respectively about 0.75 and 0.8. From what has been shown, the following general considerations can be drawn, which are applicable also to other configurations with different data:

- The staggered testing reduces PFD when components are purely tested (DC=0, PTC=1) and independent (no CCF); compared with the sequential policy the maximum gain is approximately equal to 37 % for n = 2; 68 % for n = 3; 83 % for n = 4, and 92 % for n=5. This gain is independent from failure rate and test interval values.
- When redundant components have auto-testing capability the staggered testing is practically convenient only if DC ≤ 90 %, i.e. if unrevealed faults are greater than 10 %. Hence it is necessary to perform a detailed Failure Mode and Effect Analysis (FMEA) of the components.
- When the proof test is not complete (PTC<1), there is no practical advantage of using the staggered policy.
- When CCF is of concern the staggered testing is useful, independently of β values. The gain Δ% is approximately equal to 50 % for n = 2; 66 % for n = 3; 75 % for n = 4; and 80 % for n=5.

Table 7: Δ% reduction on PFD_{avg} and PFD_{max} when CCF=yes; DC=0; PTC=1.

CCF β	Redundancy (k)	PFD_{avg} Sequential	PFD_{avg} Staggered	Δ%	PFD_{max} Sequential	PFD_{max} Staggered	Δ%
1 %	2oo2:F	$2.68 \cdot 10^{-4}$	$1.51 \cdot 10^{-4}$	43.6	$6.81 \cdot 10^{-4}$	$3.42 \cdot 10^{-4}$	49.7
5 %		$6.94 \cdot 10^{-4}$	$3.62 \cdot 10^{-4}$	47.3	$1.52 \cdot 10^{-3}$	$7.63 \cdot 10^{-4}$	49.0
10 %		$1.23 \cdot 10^{-3}$	$6.37 \cdot 10^{-4}$	49.0	$2.57 \cdot 10^{-3}$	$1.29 \cdot 10^{-3}$	49.8
20 %		$2.29 \cdot 10^{-3}$	$1.16 \cdot 10^{-3}$	49.3	$4.68 \cdot 10^{-3}$	$2.35 \cdot 10^{-3}$	49.9
1 %	3oo3:F	$1.12 \cdot 10^{-4}$	$3.73 \cdot 10^{-5}$	66.7	$2.29 \cdot 10^{-4}$	$7.56 \cdot 10^{-5}$	66.7
5 %		$5.49 \cdot 10^{-4}$	$1.83 \cdot 10^{-4}$	66.6	$1.10 \cdot 10^{-3}$	$3.69 \cdot 10^{-4}$	66.5
10 %		$1.09 \cdot 10^{-3}$	$3.66 \cdot 10^{-4}$	66.4	$2.20 \cdot 10^{-3}$	$7.35 \cdot 10^{-4}$	66.6
20 %		$8.70 \cdot 10^{-3}$	$2.91 \cdot 10^{-3}$	66.5	$1.74 \cdot 10^{-2}$	$5.85 \cdot 10^{-3}$	66.4

Summarising, from the pure probabilistic point of view, it can be stated that the staggered testing policy can be advantageously applied to redundant components, with or without CCF, provided that the proof test is complete i.e. PTC = 1, and the detection coverage DC < 90 %.

3. Conclusions

All components of a safety instrumented system need to be periodically tested when not all their failure modes can be revealed at the time of their occurrence. Two testing policies have been considered and compared: sequential and staggered. Even if the standard does not explicitly specify the policy considered, it is possible to infer that the proposed equations are based on the sequential one. Consequently some questions arise about the staggered policy: e.g., “Under which conditions, it could be conveniently applied? Which could be its advantages and limitations?”.

The paper gives answer to these questions by outlining the conditions on CCF, DC and PTC parameters under which the staggered policy can be applied to reduce PFD_{avg}. Moreover, the study also considers the maximum unavailability PFD_{max}, even if this is not considered by the standard, because its value allows the analyst to verify to what extent PFD_{avg} and PFD_{max} belong to different SIL levels.

References

Börcsök J., Machmur D., 2007, Influence of partial stroke tests and diagnostic measures of the proof test interval, Risk, Reliability and Societal Safety, Taylor & Francis Group, London, United Kingdom.

Contini S., Fabbri L., Matuzas V., 2009, JRC Scientific and Technical Reports, EUR 23825 EN: Concurrent Importance and Sensitivity Analysis applied to multiple Fault Trees, JRC, Ispra, Italy.

Contini S., Matuzas V., 2011, JRC Scientific and Technical Reports, EUR 25052 EN: ASTRA 3.x Theoretical manual, JRC, Ispra, Italy.

Dutuit Y., Innal F., Rauzy A., Signoret J.P., 2008, Probabilistic assessment in relationship with Safety Integrity Levels by using Fault Trees, Reliab. Eng. Syst. Safe. 93, 1867-1876.

Hokstad P., Corneliussen K., 2004, Loss of safety assessment and the IEC 61508 standard, Reliab. Eng. Syst. Safe. 83, 111-120.

IEC 61508, 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems”, Parts 1 to 7, Edition 2, International Electrotechnical Commission, Geneva, Switzerland.

Innal F., Dutuit Y., Rauzy A., Signoret J.P., 2010. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems, J. Risk Reliab. 224, 75-86.

Langeron Y., Barros A., Grall A., Bérenguer C., 2008, Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules, J. Loss Prev. Proc. Ind. 21, 437-449.

Lundteigen M.A., Rausand M., 2008, Partial stroke testing of process shutdown valves: how to determine the test coverage, J. Loss Prev. Proc. Ind. 21, 579-588.

Lundteigen M.A., Rausand M., Bouwer Utne I., 2009, Integrating RAMS engineering and management with the safety life cycle of IEC 61508, Reliab. Eng. Syst. Safe. 94, 1894-1903.

MacDonald D., 2003, Practical Industrial Safety, Risk Assessment and Shutdown Systems, Elsevier, Amsterdam, the Netherlands.

Necci A., Antonioni G., Renni E., Cozzani V., Borghettib A., Nucci C.A., Krausmann E., 2012, Equipment failure probability due to the impact of lightning, Chem. Eng. Trans. 26, 129-134.

Rausand M., Høyland A., 2003, System Reliability Theory – Models, Statistical Methods and Applications, Second Edition, John Wiley & Sons, Hoboken, USA.

Smith D. J., K. Simpson G. L., 2011, Safety Critical Systems Handbook, Third Edition, Elsevier, Amsterdam, The Netherlands.