Simplified vs rigorous techniques for safety integrity level verification in safety instrumented systems including proof test coverage

A. Gubert[1], J. Basco[2], D. Serral[2]
[1]Univ. Rovira i Virgilli, ETSEQ, Av. Països Catalans, 26-43007 Tarragona, Spain.
[2]Basell Poliolefinas Iberica SL, Ctra. Nacional 340, Km 1156, 43006 Tarragona, Spain.
e-mail: andreugubert@gmail.com

Abstract
Safety Integrity Level (SIL) verification is a matter of major importance in process industries. During SIL verification it is required the calculation of the average Probability of Failure on Demand (PFD_{avg}) of Safety Instrumented System (SIS). ISA and IEC standards give recommendations for the design of SIS and provide simplified equations for the calculation of PFD_{avg}. Several other probabilistic analysis techniques are used for this purpose, such as Fault Tree Analysis (FTA) and Markov Analysis (MA). In addition, dedicated software like Exida's exSILentia^{TM} is frequently used for SIL verification. A comparison of the aforementioned techniques is performed by the direct application to a set of SIS of a petrochemical plant. Afterwards, Proof Test Coverage (PTC) factor is introduced to assess the effect of imperfect proof tests on final PFD_{avg} and a similar comparison of techniques is made. A case study is performed to proof that simplified equations are highly accurate and PTC influence should not be ignored. Finally, recommendations of best practices in SIL verification exercise are given.

Keywords
Safety instrumented systems; SIL verification; Proof test coverage

INTRODUCTION

Ensuring the safety and integrity of assets is of great importance in the Chemical Process Industries (CPI). Safety Instrumented Systems (SIS) are layers of protection installed to prevent or mitigate the risk of a hazardous event. ISA TR84 (2002) and IEC 61508 (2003) provide guidelines for the design of SIS and specify functional safety requirements for its safety life cycle. A critical step in the life cycle of SIS is the validation of its safety integrity level (SIL). SIL provides the order of magnitude in which the risk is reduced by the application of the SIS.

Validation of the SIL comprises the fulfilling of three conditions. First, architectural constraints refer to the requirement to dispose of a sufficiently robust SIS in terms of architecture, which is expressed by its subsystem's Hardware Fault Tolerance (HFT). Second, systematic capability requirement refers to the systematic safety integrity of the elements alone, which is affected by its systematic failures. Finally, the average Probability of Failure on Demand (PFD_{avg}) of the SIS is required to be lower than a threshold value. PFD_{avg} quantifies the safety unavailability of the SIS and its calculation is of strong interest for SIS designers.

A SIS is commonly divided into three subsystems: sensor elements, logic solver and final elements. The calculation of PFD_{avg} is normally accounted by the contribution of these three parts to the SIS. Therefore, the PFD_{avg} of the subsystems are commonly determined alone to later be added up. Each of the subsystems of a SIS is arranged in such a way that can be defined by its MooN architecture, where N represents the total number of elements in the subsystem and M indicates the number of elements required to perform the safety function. Thus, it is always true that $M \leq N$ and that for the subsystem to fail, M-N+1 elements should fail. In other words, the subsystem can tolerate M-N failures while still being operable, which is the definition of HFT.

Several techniques are commonly used for the computation of PFD_{avg}, such as simplified equations, Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), Markov Analysis (MA) and hybrid methods. It was concluded by Oliveira et al. 2010 that ISA equations provided in its technical report ISA-TR84.00.02-Part 2 are conceptually more solid than those of IEC 61508-Part 6. The first ones, ISA equations, are the focus of this paper. The technical report of ISA advises that the simplified equations provided should only be used for 1oo1, 1oo2, 1oo3, 2oo2, 2oo3 and 2oo4 voting architectures and that for more complex ones, MA and FTA should be used. Hauge et al. 2006 of SINTEF propose an adjustment in simplified equations for MooN architectures up to 6oo6. In common practice is rarely dealt with more complex architectures. Another limitation of simplified equations relies on their use of the linear approximation to the exponential and should not be utilized for resulting PFD_{avg} greater than 0.1. In these cases, the approximation returns increasingly higher values than the exponential function.

ISA-TR84.00.02-Part 3 provides guidance on the application of FTA for SIL verification. An approximation of this technique is proposed and contrasted in this paper. This approximation reduces computational effort in comparison with fully developed FTA technique.

MA is a method in which the unavailability of a system is analyzed by representing the system in the different (failure) states it can be in. MA is widely studied and simplified in numerous efforts (Goble et al. 2005, Bukowski et al. 1995). It is commonly accepted as the most rigorous technique for SIL verification. ISA-TR84.00.02-Part 4 gives recommendations on its application to redundant systems.

The comparison of techniques conducted in the first part of this paper only takes into account Dangerous Undetected (DU) failures thus dismissing Dangerous Detected (DD) ones, since their contribution to PFD_{avg} is minimal with reasonably fast repair rates. For instance, Mean Time To Repair (MTTR) is commonly taken 8 hours in industry but even with MTTR values of 24 hours, DD effect on PFD_{avg} is insignificant. Nevertheless, this assumption is not kept in MA since it enhances the model of repairs.

Most of the literature available ignores the influence of Proof test coverage (PTC), thus considering that proof tests are perfect and therefore are capable to detect all failures present. This assumption is difficult to sustain and leads to over confident results of PFD_{avg}. Fernandez et al. 2012 proposes the introduction of this factor into simplified equations by dividing dangerous undetected failures into two parts. One part is affected and restored during proof tests while the other is not, thus constantly increases. This approach is adopted and derived to any MooN architecture in a second part of this paper.

Several SIL calculation programs e.g. exSILentia^{TM} and FSC SafeCalc^{TM}, are commonly used during SIF validation. These offer key advantages as containing reliability databases; providing more architecture possibilities than simplified equations (although approximation techniques are used for more complex than 4oo4 architectures); or offer reuse and reporting options. On the other hand, their acquisition is expensive and require of a considerable learning period. Software exSILentia^{TM} is utilized in this work in order to check the results obtained with the mentioned techniques.

This paper is structured in six sections in the following way. After this brief introduction, terminology used in this paper is presented in next section. Application of SIL verification to a set of SIS of an existing plant is explained latter, and a comparison of techniques (SE, FTA, MA and exSILentia^{TM}) is drawn. In a similar manner, in next section, proof test coverage is introduced in simplified equations and results are verified with exSILentia^{TM} software. A case study about SIL verification is developed then to illustrate the application of simplified equations with proof test coverage. Last section concludes the paper with final comments.

TERMINOLOGY

The abbreviations used in this paper are summarized in Table 1, as well as the variables used in the mathematical expressions of the case study.

Table 1. Abbreviations and nomenclature.

SIS	Safety Instrumented System	β	Beta Factor for CCF
SIF	Safety Instrumented Function	TI	Proof Test Interval
SIL	Safety Integrity Level	LT	Lifetime
PFD	Probability of Failure on Demand	MooN	M out of N architecture
HFT	Hardware Fault Tolerance	C_{MooN}	Modification factor of β
CCF	Common Cause Failure	PTC	Proof Test Coverage
SE	Simplified Equations	$\lambda_{DU,PT}$	Dangerous undetected failure rate, pressure transmitter
RBD	Reliability Block Diagrams	$\lambda_{DU,TT}$	Dangerous undetected failure rate, temperature transmitter
FTA	Fault Tree Analysis	$\lambda_{DU,LS}$	Dangerous undetected failure rate, logic solver
MA	Markov Analysis	$\lambda_{DU,V}$	Dangerous undetected failure rate, valves

NUMERICAL COMPARISON OF TECHNIQUES

Techniques explained in the introduction are compared in this section. These are simplified equations, FTA (average after logic approximation and average before logic standard methodology) and MA. They are developed according to ISA-TR84.00.02-Part 2, Part 3 and Part 4 respectively.

The exercise of SIL verification is applied to a set of SIFs in two existing polypropylene plants. Architectures of sensor elements and final elements are shown in table 2. Logic Solver is voted 1oo1 for all SIF. A complex SIF with highly redundant components is explained in the case study.

It should be remarked that the comparison possible is between techniques (horizontally in Table 2) and not between different SIFs given that they present different architectures, as well as diverse equipment failure rates. However, a slightly relation is observed between higher architectures, e.g. 8oo8, and relative error of simplified equations.

The following assumptions were made:

- Failure rates are constant along time.
- Proof Test interval is one year (8760 h).
- All the channels in a voted group have the same failure rate.
- Common cause failures are modeled with the single beta mode, where β=5%.
- Independent failures and common cause failures cannot occur in the same unit of time.

Table 2. Comparison of PFD$_{avg}$ results from applied techniques without Proof Test Coverage.

SIF	Arch. Sensors	Arch. Final elements	ISA Simplified Equations	FTA approx.	FTA	Markov Analysis	exSILentia^{TM}
1	1oo1	1oo1	1.86E-03	1.86E-03	1.86E-03	1.81E-03	1.86E-03
2	1oo1	1oo1	7.58E-03	7.55E-03	7.55E-03	7.29E-03	7.78E-03
3	1oo1	1oo1	2.76E-03	2.76E-03	2.76E-03	2.68E-03	2.76E-03
4	1oo1	1oo1	7.46E-03	7.42E-03	7.42E-03	7.16E-03	7.55E-03
5	1oo2	1oo1	1.39E-03	1.39E-03	1.39E-03	1.36E-03	1.40E-03
6	1oo2	1oo1	1.39E-03	1.39E-03	1.39E-03	1.36E-03	1.40E-03
7	1oo2	1oo1	1.45E-03	1.45E-03	1.45E-03	1.41E-03	1.46E-03
8	1oo2	1oo1	6.42E-03	6.40E-03	6.40E-03	6.21E-03	6.42E-03
9	1oo2	1oo1	6.42E-03	6.40E-03	6.40E-03	6.21E-03	6.42E-03
10	1oo2	1oo1	1.12E-03	1.10E-03	1.11E-03	1.05E-03	1.14E-03
11	1oo2	1oo1	6.41E-03	6.38E-03	6.38E-03	6.22E-03	6.40E-03
12	1oo3	1oo1+1oo1	7.72E-03	7.69E-03	7.69E-03	7.44E-03	7.69E-03
13	1oo2	1oo2	7.41E-04	7.24E-04	7.42E-04	7.02E-04	7.31E-04
14	1oo1	2oo2	1.14E-02	1.13E-02	1.13E-02	1.09E-02	1.15E-02
15	1oo1	2oo2	1.38E-02	1.37E-02	1.37E-02	1.31E-02	1.38E-02
16	1oo1	2oo2	1.38E-02	1.37E-02	1.37E-02	1.31E-02	1.35E-02
17	1oo2	2oo2	1.28E-02	1.27E-02	1.27E-02	1.22E-02	1.27E-02
18	1oo2	2oo2	2.71E-03	2.70E-03	2.70E-03	2.63E-03	2.65E-03
19	1oo2	2oo2	2.65E-03	2.65E-03	2.65E-03	2.66E-03	2.60E-03
20	1oo2	2x(1oo2)	9.37E-04	8.70E-04	9.06E-04	8.23E-04	8.06E-04
21	1oo2	2x(1oo2)	1.11E-03	1.09E-03	1.11E-03	9.72E-04	1.11E-03
22	1oo1	3oo3	4.07E-03	4.06E-03	4.06E-03	3.94E-03	3.89E-03
23	1oo2	3oo3	1.91E-02	1.89E-02	1.89E-02	1.80E-02	1.90E-02
24	1oo2	3oo3	1.91E-02	1.89E-02	1.89E-02	1.80E-02	1.90E-02
25	1oo2	3oo3	1.91E-02	1.89E-02	1.89E-02	1.80E-02	1.90E-02
26	1oo2	3oo3	1.91E-02	1.89E-02	1.89E-02	1.80E-02	1.90E-02
27	1oo2	3x(1oo2)+1oo1	8.84E-03	8.77E-03	8.80E-03	7.96E-03	8.63E-03
28	1oo2	3x(1oo2)+1oo1	8.76E-03	8.75E-03	8.80E-03	8.30E-03	8.63E-03
29	1oo2	3x(1oo2)+1oo1	8.83E-03	8.74E-03	8.81E-03	7.97E-03	8.60E-03
30	1oo2	3x(1oo2)+1oo1	8.74E-03	8.74E-03	8.80E-03	8.30E-03	8.60E-03
31	1oo2	3x(1oo2)+1oo1	8.84E-03	8.77E-03	8.80E-03	7.96E-03	8.63E-03
32	1oo2	3x(1oo2)+1oo1	8.76E-03	8.75E-03	8.80E-03	8.30E-03	8.63E-03
33	*1oo2+4oo5	3x(1oo2)+1oo1	9.10E-03	8.83E-03	8.91E-03	8.33E-03	8.73E-03
34	1oo2+4oo5	3x(1oo2)+1oo1	9.01E-03	8.83E-03	8.91E-03	8.33E-03	8.73E-03
35	1oo2	5x(1oo2)	1.91E-03	1.76E-03	1.83E-03	1.77E-03	1.61E-03
36	1oo1	8oo8	5.12E-02	4.96E-02	4.95E-02	4.69E-02	4.96E-02
37	1oo1	8oo8	5.93E-02	5.72E-02	5.66E-02	5.43E-02	5.48E-02
38	1oo2	8oo8	5.09E-02	4.93E-02	4.93E-02	4.59E-02	4.93E-02
39	1oo2	8oo8	5.85E-02	5.66E-02	5.65E-02	5.18E-02	5.40E-02
40	1oo2+2oo3	8oo8	5.09E-02	5.03E-02	5.07E-02	4.59E-02	4.94E-02
41	1oo2+2oo3	8oo8	5.86E-02	5.83E-02	5.83E-02	5.17E-02	5.38E-02
42	2oo3	8oo8	5.13E-02	4.96E-02	4.96E-02	4.73E-02	4.98E-02
43	2oo3	8oo8	5.13E-02	4.96E-02	4.96E-02	4.73E-02	4.98E-02

***** SIF developed in the case study.

Introduction of proof test coverage

Proof test coverage is introduced in simplified equations to assess its effect on PFD_{avg}. Study time is set to 10 years, which is the lifetime (LT) of equipment considered. For sensors PTC is 80% and for valves 60, 90 and 95%. These values are chosen depending on the historical failures corded in the plant. While 90 and 95% PTC factors for valves are required to be justified with more exhaustive proof test, other values of PTC are quite conservative for sensors and valves.

Table 3. Comparison of PFD_{avg} results from applied techniques with Proof Test Coverage.

SIF	Arch. Sensors	Arch. Final elements	PTC of Sensors (%)	PTC of Final elements (%)	Simplified Equations**	exSILentia^{TM}
1	1oo1	1oo1	80	65	6.84E-03	6.93E-03
2	1oo1	1oo1	80	65	2.97E-02	2.98E-02
3	1oo1	1oo1	80	65	9.44E-03	9.44E-03
4	1oo1	1oo1	80	65	2.94E-02	2.91E-02
5	1oo2	1oo1	80	65	5.59E-03	5.65E-03
6	1oo2	1oo1	80	65	5.59E-03	5.65E-03
7	1oo2	1oo1	80	65	5.78E-03	5.85E-03
8	1oo2	1oo1	80	65	2.65E-02	2.61E-02
9	1oo2	1oo1	80	65	2.65E-02	2.61E-02
10	1oo2	1oo1	80	65	5.87E-03	6.75E-03
11	1oo2	1oo1	80	65	2.64E-02	2.60E-02
12	1oo3	1oo1+1oo1	80	65	3.19E-02	3.13E-02
13	1oo2	1oo2	80	65	3.89E-03	4.36E-03
14	1oo1	2oo2	80	65	4.57E-02	4.48E-02
15	1oo1	2oo2	80	65	5.57E-02	5.42E-02
16	1oo1	2oo2	80	65	5.57E-02	5.29E-02
17	1oo2	2oo2	80	65	5.29E-02	5.12E-02
18	1oo2	2oo2	80	65	1.10E-02	1.08E-02
19	1oo2	2oo2	80	65	1.10E-02	1.12E-02
20	1oo2	2x(1oo2)	80	65	4.83E-03	4.85E-03
21	1oo2	2x(1oo2)	80	65	5.84E-03	6.70E-03
22	1oo1	3oo3	80	65	1.66E-02	1.58E-02
23	1oo2	3oo3	80	65	7.92E-02	7.55E-02
24	1oo2	3oo3	80	65	7.92E-02	7.55E-02
25	1oo2	3oo3	80	65	7.92E-02	7.55E-02
26	1oo2	3oo3	80	65	7.92E-02	7.55E-02
27	1oo2	3x(1oo2)+1oo1	80	65	3.82E-02	3.73E-02
28	1oo2	3x(1oo2)+1oo1	80	65	3.89E-02	3.73E-02
29	1oo2	3x(1oo2)+1oo1	80	65	3.82E-02	3.72E-02
30	1oo2	3x(1oo2)+1oo1	80	65	3.82E-02	3.72E-02
31	1oo2	3x(1oo2)+1oo1	80	65	3.82E-02	3.73E-02
32	1oo2	3x(1oo2)+1oo1	80	65	3.82E-02	3.73E-02
33	*****1oo2+4oo5	3x(1oo2)+1oo1	80	65	3.89E-02	3.76E-02
34	1oo2+4oo5	3x(1oo2)+1oo1	80	65	3.89E-02	3.76E-02
35	1oo2	5x(1oo2)	80	65	9.42E-03	9.93E-03
36	1oo1	8oo8	80	90	9.75E-02	9.10E-02
37	1oo1	8oo8	80	95	8.58E-02	7.84E-02
38	1oo2	8oo8	80	90	9.66E-02	9.01E-02
39	1oo2	8oo8	80	95	8.48E-02	7.70E-02
40	1oo2+2oo3	8oo8	80	90	9.68E-02	9.03E-02
41	1oo2+2oo3	8oo8	80	95	8.51E-02	7.68E-02
42	2oo3	8oo8	80	90	9.71E-02	9.07E-02
43	2oo3	8oo8	80	90	9.71E-02	9.07E-02

***** SIF developed in the case study.

******Simplified Equations from ISA modified to introduce the PTC factor.

Comparison of PFD_{avg} results

From the first part, presented in Table 2, the accuracy of simplified equations is reasonable high since the results just differ from exSILentia^{TM} between 0 and 10% for most cases. In all cases MA provided lower values of the average PFD_{avg}, therefore being simplified equations more conservative. Such conclusion is favorable given that simplified equations are much faster to implement and at the same time provide conservativeness regarding safety. The average after logic approximation used in FTA present minimal differences in respect with the average before logic standard methodology. Therefore, its usage is recommended instead of the standard FTA approach.

In the second part, presented in Table 3, PTC was introduced and PFD_{avg} results incremented by a factor of 4 to 5, demonstrating that the effect of this parameter cannot be ignored. Differences between simplified equations and the software in this case are in the same range, 0 to 10%.

CASE STUDY

In this section, a case study is performed to better illustrate the procedure followed to calculate PFD_{avg} in last section, where proof test coverage factor was introduced in ISA Equations This study is based in the work of one of the authors, Gubert, A 2015. An approach to incorporate this factor in simplified equations is proposed by Fernandez et al. 2012. However, only equations for 1oo1 and oo2 architectures are given. The same approach is followed for more complex architectures. In addition, this case study proposes a derived equation for a subsystem of sensors voted 4oo5 based on Hauge et al. 2006 of SINTEF, which takes into account independent failures with a combinatorial expression and the C_{MooN} factor to adjust common cause failures for complex architectures. Results are then verified with SIL verification *software* exSILentia^{TM}.

Application to a plant SIF

Studied SIF is composed by two pressure transmitters voted 1oo2, five temperature transmitters voted 4oo5, a 1oo1 logic solver, one valves voted 1oo1 and three legs composed by two valves voted 1oo2. Figure 1 shows the representation of the SIF.

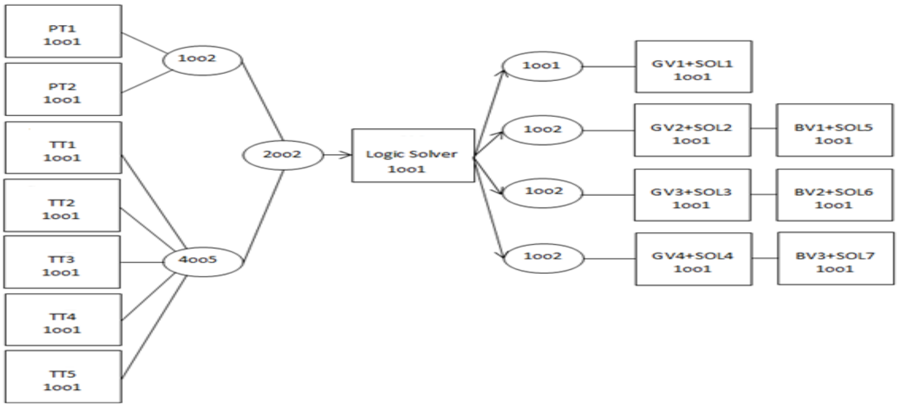

Figure 1. Representation of SIF *(PT: pressure transmitter; TT: temperature transmitter; GV: glove valve; BV: ball valve; SOL: solenoid valve).*

The parameters used both in simplified equations and exSILentia^{TM} for PFD_{avg} results comparison are set as shown in Table 4.

Table 4. Data used in the PFD_{avg} calculation.

Parameter	Value	Parameter	Value
β	0.05	$\lambda_{DU,PT}(h^{-1})$	1.46E-7
TI (h)	8760	$\lambda_{DU,TT}(h^{-1})$	2.86E-7
LT (h)	87600	$\lambda_{DU,LS}(h^{-1})$	1.27E-8
$PTC_{sensors}$ (%)	80	$\lambda_{DU,V}(h^{-1})$	1.70E-6
PTC_{valves} (%)	65	C_{4oo5}	3.7

The expression for 1oo2 systems, applied to pressure transmitters and valves, is shown in Eq. (1) below:

$$PFD_{avg,1oo2} = \left[\left((1-\beta)\lambda_{DU}\right)^2 \frac{(TI\,PTC)^2}{3}\right] + \left[\left((1-\beta)\lambda_{DU}\right)^2 \frac{\left(LT(1-PTC)\right)^2}{3}\right] + \left[\beta\lambda_{DU}\frac{TI\,PTC}{2}\right] + \left[\beta\lambda_{DU}\frac{LT\,(1-PTC)}{2}\right] \tag{1}$$

The general equation for any MooN architecture is applied to temperature transmitters, as shown in Eq. (2) and (3):

$$PFD_{avg,MooN} = \frac{N!}{(N-M+2)!(M-1)!}\left[\left((1-\beta)\lambda_{DU}\,TI\,PTC\right)^{N-M+1}\right] + \frac{N!}{(N-M+2)!(M-1)!}\left[\left((1-\beta)\lambda_{DU}TI\,PTC\right)^{N-M+1}\right] + C_{MooN}\left[\beta\lambda_{DU}\frac{TI\,PTC}{2}\right] + C_{MooN}\left[\beta\lambda_{DU}\frac{LT\,(1-PTC)}{2}\right] \tag{2}$$

Substituting M=4 and N=5 in Eq. (2), one obtains:

$$PFD_{avg,4oo5} = \frac{5!}{(5-4+2)!(4-1)!}\left[\left((1-\beta)\lambda_{DU}\,TI\,PTC\right)^{5-4+1}\right] + \frac{5!}{(5-4+2)!(4-1)!}\left[\left((1-\beta)\lambda_{DU}TI\,PTC\right)^{5-4+1}\right] + C_{4oo5}\left[\beta\lambda_{DU}\frac{TI\,PTC}{2}\right] + C_{4oo5}\left[\beta\lambda_{DU}\frac{LT\,(1-PTC)}{2}\right] \tag{3}$$

For the logic solver and the valve voted 1oo1, Eq. (4) is used:

$$PFD_{avg,1oo1} = \left[\lambda^{DU}\cdot\frac{TI{\cdot}PTC}{2}\right] + \left[\lambda^{DU}\cdot\frac{LT{\cdot}(1-PTC)}{2}\right] \tag{4}$$

Results

Numerical results are summarized in Table 5.

Table 5. Comparison of PFD$_{avg}$ results from simplified equations and exSILentia^{TM}

Subsystem legs	Simplified equations	exSILentia^{TM}
1oo2 pressure transmitters 4oo5 temperature transmitters	9.18E-5 7.36E-4	1.60E-4 3.06E-4
Total Sensor elements	**8.28E-4**	**4.66E-4**
1oo1 logic solver	**4.93E-5**	**4.69E-5**
1oo1 valve 1oo2 valves (each of the 3 legs)	3.09E-2 2.39E-3	3.00E-2 2.35E-3
Total Final elements	**3.81E-2**	**3.71E-2**
Total SIF	**3.89E-2**	**3.76E-2**

FINAL COMMENTS

Simplified equations have been proved to provide enough accuracy either when proof tests were considered perfect and when PTC was introduced. In addition, its conservativeness is favorable for SIL verification. On the contrary, MA might be advised in some applications where PFD$_{avg}$ should be calculated with more precision. When comparing with exSILentia^{TM}, simplified equations also present high accuracy. Therefore, in terms of precision, simplified equations are recommended over any other SIL verification technique. However, in some cases exSILentia^{TM} software might be advisable: when reliability data is not available; when the user deals with complex architectures or when actualization of SIF and report making occur constantly.

The effect of PTC has been proved to be huge and therefore its implementation in SIL verification techniques is encouraged as further research.

From the case study might be concluded that the adjustment made by Hauge et al. (2010) of SINTEF for 4oo5 architectures might require of further adjustment. Nevertheless, a clear conclusion cannot be drawn since the approach of exSILentia^{TM} for this architecture is an approximation not well explained by the developers.

References

ISA-TR84.00.02-2002 *Safety Instrumented Functions (SIF). Safety Integrity Level (SIL) Evaluation Techniques Parts 1-5*. Instrumentation, Systems and Automation Society, Research Triangle Park, NC, USA (2002).

IEC 61511. *Functional Safety-Safety Instrumented Systems for the process industry sector, Parts 1-3*. International Electrotechnical Comission,Geneva, Switzerland (2003).

Oliveira LF, Abramovitch RN. *Extension of ISA TR84.00.02 PFD equations to KooN architectures.* Reliability Engineering and System Safety 95 *(2010) 707-715.*

Hauge S, Hokstad P, Langseth H,et al*. Reliability prediction method for safety instrumented systems, PDS method handbook.* SINTEF, Norway, (2006).

Goble W, Cheddie H. *Safety Instrumented Systems verification: practical probabilistic calculations*. USA, ISA (2005).

Bukowski J, Goble W. *Using Markov models for safety analysis of programmable electronic systems*, ISA Trans (1995).

Gubert A. *A new approach for the SIL verification of the Safety Instrumented Systems of a petrochemical plant*. Master Science Thesis (2015).

Fernandez I, Camacho A, Gasco C, Macías AM, Martín MA, Reyes G, Rivas J. *Sistemas Instrumentados de Seguridad y Análisis SIL, Seguridad Funcional en Instalaciones de Procesos*. ISA. (2012).