Review of Mathematical Inconsistencies in the Practices to Assess SIL of SIS – Toward a Novel Approach for Risk Reduction

Laurent Cauffriez

Review of Mathematical Inconsistencies in the Practices to Assess SIL of SIS – Toward a Novel Approach for Risk Reduction

Laurent Cauffriez

Univ. Polytechnique Hauts-de- France, CNRS, UMR 8201 – LAMIH – Laboratoire d'Automatique de Mécanique d'Informatique Industrielle et Humaines, F-59313 Valenciennes, France. E-mail: laurent.cauffriez@uphf.fr

A review of the literature has highlighted that there are many approximations and ambiguities in practices for assessing Safety Integrity Level (SIL) of Safety Instrumented Systems (SIS). The aim of this paper is to make at first a review of mathematical inconsistencies in the practices for assessing SIL. Secondly, it introduces an unambiguous approach for risk reduction based on a discrete time approach. Thirdly, it proposes a predictive model to quantify the average number of failures that a SIS will experience during its life cycle. Finally, to the ends of validation, a comparison is made between the results obtained by applying the proposed novel approach, the formulas given in the IEC61508 standard and Monte Carlo simulations.

Keywords: Predictive model, Bernoulli experiment, Odds on, Probability of Failure, Safety Integrity Level, Safety Instrumented System, Risk reduction, IEC 61508, Monte Carlo simulations, Truncation of the failures distribution.

1. Introduction

IEC61508 standard introduces the notion of PFDaverage (average probability to fail dangerously on demand) to determine the SIL level of Safety Instrumented Systems IEC61508 (2010). This notion is nowadays widely used by engineers and scientists who are inventing models more and more complicated using well-known formalisms e.g. Markov models Langeron et al. (2008); Mechri et al. (2015), Reliability block diagram Guo and Yang (2007), Cause-consequence diagrams Beugin et al. (2007), Stochastic Petri Nets Cacheux et al. (2013); Signoret et al. (2013); Aubry et al. (2016), Fault Tree models Dutuit et al. (2008), analytical expressions Chebila and Innal (2015) and fuzzy probabilistic approach Sallak et al. (2008). However, a review of the literature highlights that there are many approximations and ambiguities in practices for assessing SIL of SIS. Hereinafter a number of considerations about those mathematical inconsistencies are introduced.

(i) A look at SIL values given in IEC61508 (2010) points out that the average probability to fail dangerously on demand (in abbreviated form PFDaverage) belongs to $[10^{-5},10^{-1}]$ for SIL ranging from 4 to 1. Therefore, the average probability to survive is very high and ranges between 0.99999 to 0.9. You must then expect that a safety instrumented system fails, fortunately, very rarely during its lifecycle.

(ii) From a mathematical point of view, the notion of "average" implies numerous failure events to be able to assess the average and the standard deviation around this latter. If for low SIL values (i.e. SIL1 and 2) the average can be reached because of "numerous" failure events, it is difficult to reach the average in the case of high SIL values. Indeed, for high SIL, you must face rare events since the SIS fails sporadically due to its high reliability. E.g. for SIL3 and SIL4, a majority of testing periods will experience no failure and the SIS will survive at age T1, T1 being the length of the testing period.

(iii) Please note that the assessment of PFD and PFDaverage is experimentally possible only for testing periods that experience a failure. Indeed, testing periods that do not experience a failure contribute to the assessment of the average probability to survive.

(iv) The "tooth curve behavior" introduced by Dutuit et al. (2008); Rausand (2014) shows a SIS unavailability for all the test periods. This modeling approach for the failures process of SIS seems a little surprising. Indeed, during the lifecycle of a SIS, there must be inevitably numerous periods for which the SIS is available and a minority of periods for which the SIS experiments a failure due to the high reliability of this latter.

(v) Due to the periodic testing of length T1, the failure distribution must be right truncated. This mathematical point is not sufficiently highlighted in the literature as well as industrial practices. Indeed, a discrete time approach must be used instead of a continuous time as described in Cauffriez (2015). The equation for the failure density function of a right-truncated exponential distribution was published in Al-Athari (2008).

(vi) In common practice for reliability studies, the mean of Time To Failures i.e. the expected value of the exponential distribution is equal to $1/\lambda$. However, IEC61508 standard claims that the mean time to failure must be equal to T1/2 for a 1oo1 SIS. This observation leads to the following question: "How to generate with a Monte Carlo simulation Time To Failures (TTF) within the time

Proceedings of the 29th European Safety and Reliability Conference.
Edited by Michael Beer and Enrico Zio

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0 esrel2019-paper_91

interval between two tests for a SIS having a small constant failure rate and therefore a great exponential mean value?". Indeed, as failure rates are very low and testing periods are short, you have inevitably $1/\lambda >> T1/2$. Therefore, a criterion to verify if a model of a SIS failure process is accurate or not, is to check that Time To Failures tend toward the value of T1/2 as introduced in the IEC61508 standard for a 1oo1 SIS (and not to the value of $1/\lambda$). Considering this criterion, you have no option but to truncate the failure distribution and, to use a discrete time approach to model the failure process of a SIS. Unfortunately, continuous Markov chains and stochastic Petri nets are defined mathematically for a complete failure distribution and not for a truncated one.

(vii) According to the author's knowledge, a majority of commercial software implement Monte Carlo algorithms working $\forall\ t \in [0, +\infty[$ and inversing therefore the whole distribution of failures. However, for SIL studies, Time To Failures must belong to [0, T1]. Therefore, a specific Monte Carlo algorithm must be developed by implementing a truncation of the failure distribution. This can be summarized as follows: $\forall\ t \in [0,T1]$, $F(t) \in [0,F(T1)]$. Therefore, for any random variable $U \in [0, F(T1)]$, it exists $t \in [0,T1]$ such as $t=F^{-1}(t)$, F^{-1} being the inverse function of the failure distribution F(t). Please note that F(T1) is the maximal probability to fail and is equal to $F(T1)=F(T1)-F(0)=1-e^{-\lambda T1}$.

(viii) The formulas given in the standard for the PFDaverage point out that the PFDaverage for the 2oo2 architecture is twice the PFD of 1oo1 architecture. Indeed, $PFD2oo2=2\cdot\lambda DU\cdot T1/2$ whereas $PFD1oo1=\lambda DU\cdot T1/2$. Therefore, for a given pair of λDU and T1 (for comparison purposes), the 2oo2 architecture appears to be less reliable than a 1oo1 SIS with the risk that the SIL is lower for a 2oo2 SIS than for a 1oo1 SIS as the PFDaverage is higher. However, a 2oo2 architecture contributes to a better safety thanks to the duplication of the channels for the EUC.

(ix) There are side effects applying those above formulas that can be explained simply with an example. Let be a 1oo1 SIS whose PFDaverage tends toward the lower level of SIL1, i.e. 10^{-1}. If this 1oo1 SIS is combined with another one to build a 2oo2 SIS, the PFDaverage of the 2oo2 SIS tends toward $2\cdot10^{-1}$ according the PFD formulas given in the previous remark point. A side effect appears because the PFDaverage of the 2oo2 SIS is outside the interval $[10^{-2},10^{-1}]$ defining a SIL1 and should be of SIL0. Such side effects appear when the evaluation of the SIL focuses on the average probability of failure without considering the standard deviation around the average. Fortunately, the SIS designer of a 2oo2 architecture can select lower test intervals and/or reduce the failure rate to meet the required SIL.

(x) Please note that for architectures 1oo2 or 2oo3, two channels must experience a failure during the same test period to lead to a SIS failure. Therefore, the periodic tests of the channels must be synchronous to agree with the mathematical equations given in IEC61508 standard. This modelling point must be more highlighted.

(xi) In fact, approximations and ambiguities, like the linearization of the exponential distribution and the sum of PFDaverage, are due to the continuous time modelling approach chosen and developed in the standard.

In the context of the previous considerations, a novel approach to assess the SIL of SIS without any approximations and ambiguities is proposed in the next paragraph. This approach relies on the maximal probability of failure over the test period instead of the notion of PFDaverage. As the goal of this work is to model only the failure process of SIS, the repair process is not considered in this paper.

2. Proposition of a Discrete Time approach for SIL level assessment

In order to assess SIL of SIS, it is proposed in this paper to transpose Table 1 of SIL given in IEC61508 (2010) into a table that gives the SIL according to the maximal probability of failure over [0,T1], i.e. at age T1. This transposition is very easy to do with the help of Eq. (1) given in the standard for a 1oo1 SIS. Indeed, Eq. (1) can be transformed into Eq. (2). By applying the mathematical property of the exponential function given in Eq. (3), Eq. (2) produces Eq. (4). Table 2 presents the resulting table for assessing SIL according to the novel proposed approach. With this approach, a SIS designer can calculate the probability of failure at age T1 with Eq. (4) and compare this probability with the values given in Table 2 to identify the SIL of a 1oo1 SIS.

$$\mathrm{PFDaverage} = 1 - e^{-(\lambda \cdot T1/2)} \quad (1)$$

$$p = 1 - (1 - \mathrm{PFDaverage})^2 = 1 - e^{-(\lambda \cdot T1/2)^2} \quad (2)$$

$$e^{-\lambda \cdot T1} = e^{-(\lambda \cdot T1/2)^2} \quad (3)$$

$$p = pmax = 1 - e^{-\lambda \cdot T1} \quad (4)$$

Table 1. Safety Integrity Level based on average probability of failure according to IEC61508.

SIL	PFDaverage
4	$[10^{-5}, 10^{-4}[$
3	$[10^{-4}, 10^{-3}[$
2	$[10^{-3}, 10^{-2}[$
1	$[10^{-2}, 10^{-1}[$

Table 2. Safety Integrity Level based on the maximal probability of failure at age T1 according to the novel proposed approach.

SIL	pMax
4	$[1.99999 \cdot 10^{-5}, 1.9999 \cdot 10^{-4}[$
3	$[1.9999 \cdot 10^{-4}, 1.999 \cdot 10^{-3}[$
2	$[1.999 \cdot 10^{-3}, 1.99 \cdot 10^{-2}[$
1	$[1.99 \cdot 10^{-2}, 1.9 \cdot 10^{-1}[$

3. SIL assessment of multi-channel SIS architectures

One advantage of the novel approach proposed in this paper is that SIL can be quantified by applying conventional reliability studies. This property is demonstrated in the next paragraph.

3.1 *Case of 1oo1 architecture*

For a 1oo1 SIS, the SIL level is simply assessed by calculating F(T1) (See Eq. (5)) for a given pair (λ,T1) and by comparing the value of F(T1) to the values given in Table 2.

Please note that for a 1oo1 SIS, Zhang (2003) demonstrates that the MTTF i.e. the average of the Time To Failures (TTF) is roughly equal to the half of the testing period.

$$F_{1oo1}(T1) = F(T1) - F(0) = 1 - e^{-\lambda \cdot T1} \quad (5)$$

$$R_{1oo1}(T1) = e^{-\lambda \cdot T1} \quad (6)$$

3.2 *Case of 2oo2 architecture*

As a 2oo2 SIS fails as soon as one of both channels fails, a series system model is relevant for reliability calculation of this architecture. For two entities in series, each with a constant failure rate λ, the probability to fail and to survive over [0,T1] is given by equations (7) and (8). It is to be observed that, likewise a 1oo1 architecture, the MTTF of a 2oo2 SIS is roughly equal to T1/2.

$$F_{2oo2}(T1) = F(T1) - F(0) = 1 - e^{-2\lambda \cdot T1} \quad (7)$$

$$R_{2oo2}(T1) = e^{-2\lambda \cdot T1} \quad (8)$$

3.3 *Case of 1oo2 architecture*

For two entities in parallel, each with a constant failure rate λ, the unreliability of the entire SIS is equal to the product of the unreliability of each channel (Please see Eq. (9)). The probability to survive is given by Eq. (10) for 1oo2 SIS.

$$F_{1oo2}(T1) = F(T1) - F(0) = (1 - e^{-\lambda T1})^2 \quad (9)$$

$$R_{1oo2}(t) = 1 - (1 - R(T1))^2 = 2e^{-\lambda \cdot T1} - e^{-2\lambda \cdot T1} \quad (10)$$

For the MTTF of a 1oo2 architecture, both channels must experience a failure during the same *ith* period of test. Therefore, the designer has to expect a value strictly greater than T1/2 due to the active redundancy of channels 1 and 2. It can be demonstrated by simulation or by a theoretical approach that the value of the MTTF for a 1oo2 SIS is roughly equals to 2T1/3 (see Eq. (11)).

$$MTTF\_1oo2_{th} = Max(ti\_Channel\_1; ti\_Channel\_2) \approx 2T1/3 \quad (11)$$

where Max is the mathematical Maximum function.

3.4 *Case of 2oo3 architecture*

For three entities in a 2 out of 3 configuration, each entity with a constant failure rate λ, the probability to fail and to survive for the system is given by Eq. (12) and (13) applying binomial distribution.

$$F_{2oo3}(T1) = 1 - 3 \cdot R^2(T1) \cdot (1 - R(T1)) - R^3(T1) = 1 - 3e^{-2\lambda \cdot T1} + 2e^{-3\lambda \cdot T1} \quad (12)$$

$$R_{2oo3}(T1) = 3 \cdot R^2(T1) - 2R^3(T1) = 3e^{-2\lambda \cdot T1} - 2e^{-3\lambda \cdot T1} \quad (13)$$

Concerning the MTTF of a 2oo3 architecture (see Eq. (14)), the designer has to expect a value strictly greater than T1/2 due to the redundancy of 2 out of 3 channels. This value is roughly equal to 2T1/3 alike the case of a 1oo2 architecture.

$$MTTF\_2oo3_{ith} = \min(Max(ti\_Channel\_1; ti\_Channel\_2), Max(ti\_Channel\_1; ti\_Channel\_3), Max(ti\_Channel\_2; ti\_Channel\_3)) \quad (14)$$

where min and Max are respectively the mathematical minimum and Maximum functions.

To compare the architectures among them, a case study is plotted in Fig. 1 and consists in

assessing the probability to fail for a value of λ equals to 10^{-3} h^{-1} and ∀ t∈ [0,300] hours.

Looking at Fig. 1 reveals that a 2oo2 SIS is less reliable than a 1oo1, a 1oo1 is less reliable than a 2oo3, a 2oo3 is less reliable than a 1oo2. As the mission of SIS is to achieve a safe state for the Equipment Under Control (EUC), please note that architectures 1oo2 and 2oo3 are more fault tolerant as they continue to work even if a safety channel fails, whereas the safety function is lost as soon as a channel fails for 1oo1 and 2oo2 SIS.

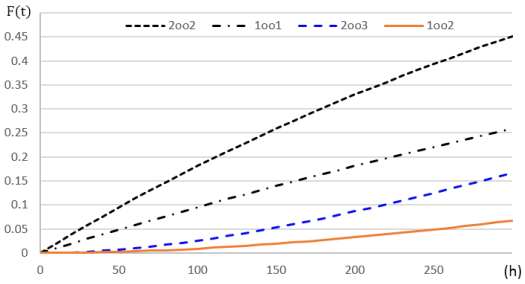

Fig. 1. Comparison between each kind of architectures for a λ value equal to 10^{-3} h^{-1}.

4. Proposition of a Predictive Model to assess SIL level of SIS

For a SIS architecture, one can see that the outcome of the periodic test is one of the following:

- either a failure appears within the current test interval [0, T1],
- or no failure appears within the current test interval [0, T1], i.e. the SIS survives at time T1.

This is the exact definition of a Bernoulli experiment. The application of the Bernoulli experiment to model the failure process of a 1oo1 SIS is given in Fig. 2 according to Cauffriez (2017).

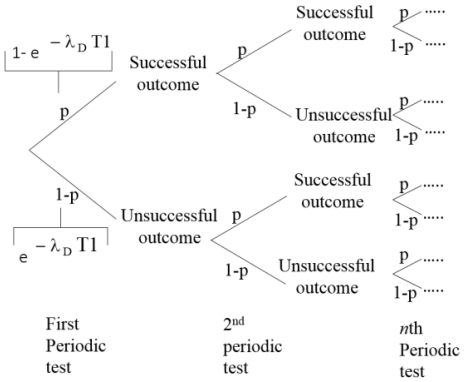

Fig. 2. Bernoulli experiment to model 1oo1 SIS failures.

For the first periodic test, there is a probability *1-p* that the SIS experiences no failures and survives at age T1 (Unsuccessful outcome: "No failure of SIS") and a probability *p* that the SIS fails within [0,T1] (Successful outcome: "Failure of SIS"). This is also true for the second periodic test, for the third periodic test, and so on until the *nth* periodic test. A Bernoulli experiment is therefore performed at several separate times so that the probability of success *p* remains the same from trial to trial. This concatenation of the Bernoulli experiment defines a so-called sequence of Bernoulli trials Hsu (1997); Alston et al (2013).

To characterize a SIS failure process, a predictive model is proposed in this paper. This predictive model calculates the expectation of a sequence of Bernoulli trials as described hereafter. Let a random variable X be the number of successes for an infinite sequence of Bernoulli trials. Let *n* be the first *n* trials.

(i) The expected value or expectation (measure of the center of the distribution) of random variable X is given by Eq. (15)

$$E(X) = n \cdot p \tag{15}$$

(ii) The standard deviation is defined as:

$$\sigma X = \sqrt{n \cdot p \cdot (1-p)} \tag{16}$$

(iii) Odds on favor (Of) of a Success, i.e. a failure of the SIS for SIL studies, is equal to Eq. (17) according to Walsh (2012).

$$Of = \frac{p}{1-p} \tag{17}$$

(iv) For a very large population of trials, i.e. for $n \to +\infty$, the probability *p* that trials result in success is given by Eq. (18)

$$\frac{Successful\ outcome}{n} \to p \quad \text{as } n \to +\infty \tag{18}$$

To enhance the approach in IEC 61508 for studying SIL, it is proposed in this paper to use the notion of odds as defined by Walsh (2012). Table 3 gives the odds on favor of a SIS failure (O*f*) compared to some probabilities of failure. For example, in Table 3, p=10^{-1} gives the odds value of 1:9. Therefore, the designer of the SIS has to expect 1 Successful outcome, i.e. "X=1, a failure of the SIS appears within the current interval [0,T1]" against 9 unsuccessful outcomes, i.e. "X=0, no failure of the SIS appears within the current interval [0,T1]. One can see in Table 4 that the SIS fails less than once per year only for *p* equals 10^{-4} and 10^{-5} for a SIS working time corresponding to 1 year, 10 years, 100 years assuming that the test period T1 is equal to 8 hours.

Table 3. Odds on favor of a SIS failure for some probability of failure at age T1.

p	$Of = \frac{p}{1-p}$
10^{-5}	1:99999
10^{-4}	1:9999
10^{-3}	1:999
10^{-2}	1:99
10^{-1}	1:9

Table 4. Expected theoretical value of random variable X for 1oo1 SIS with a periodic test of 8 hours.

	1 year n=1095	10 years n=10950	100 years n=1095000
p	*E(X)*	*E(X)*	*E(X)*
10^{-5}	0,01095	0,1095	1,095
10^{-4}	0,1095	1,095	10,95
10^{-3}	1,095	10,95	109,5
10^{-2}	10,95	109,5	1095
10^{-1}	109,5	1095	10950

The advantage of applying Bernoulli trials is that the designer is able to predict as an average the number of times a SIS will experience a failure during its lifecycle or its working time. Table 5 illustrates the notion of Odds according to SIL levels. In column 2 of Table 5, $2 \cdot 10^{-1}$ to $2 \cdot 10^{-5}$ are the round off values for pMax given in Table 2 to make easier the assessment of the odds O*f*.

Table 5. SIL assessment considering pMax and the notion of Odds on a SIS failure.

SIL	pMax	$Of = \frac{p}{1-p}$
4	$[2 \cdot 10^{-5}, 2 \cdot 10^{-4}[$	[1:49999, 1:4999[
3	$[2 \cdot 10^{-4}, 2 \cdot 10^{-3}[$	[1:4999, 1:499[
2	$[2 \cdot 10^{-3}, 2 \cdot 10^{-2}[$	[1:499, 1:49[
1	$[2 \cdot 10^{-2}, 2 \cdot 10^{-1}[$	[1:49, 1:4[

To summarize the proposed method in this paper for risk reduction, a SIL can be easily determined by calculating the probability to fail at age T1 using equations (5), (7), (9), (12) depending on the kind of architecture (1oo1, 2oo2, 1oo2, 2oo3) and by comparing the obtained value to pMax given in Table 5. As a bonus, the designer is able to predict the number of times the SIL fails during its lifecycle by assessing the expectation of the sequence of Bernoulli trials using Eq.(15). Moreover, Eq.(17) gives the odds in favor a failure i.e. the relative probability that the SIS will experience a failure during a test period.

Please note that Eq.(15) to Eq.(17) constitute the predictive model proposed in this paper to assess SIL of SIS.

5. Experimental simulation

5.1 *Remind on the need to truncate the failure distribution for Monte Carlo simulation*

Fig. 3 illustrates the need to truncate the failure distribution for Monte Carlo distribution. Due to the periodic testing of SIS, the lifecycle of the SIS must be decomposed into sliding time windows of length T1. At the beginning of a new testing period, the SIS is assumed to be as good as new until a failure occurs within $[(k-1)\cdot T1 , k\cdot T1]$, $\forall k \in [1, N]$.

This modelling point is not sufficiently highlighted in the literature. It is also important to insist on the fact that a specific Monte Carlo algorithm must be implemented to build relevant model of the failure process of SIS.

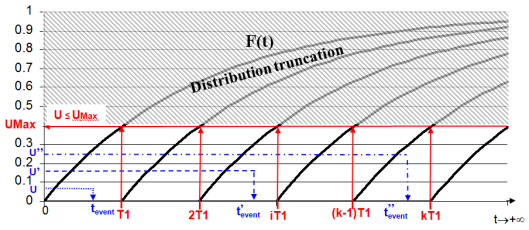

Fig. 3. Need to truncate the failure distribution for Monte Carlo simulation according to Cauffriez (2015).

5.2 *Examples of irrelevant/relevant Monte Carlo simulations*

To illustrate the previous remarks, Monte Carlo simulation results with a scan of the entireness of the exponential failure distribution are given in Fig. 4. Indeed, inversing the failure distribution for $t \in [0,+\infty[$ is the common practice for reliability studies. For the simulation given in Fig.4, the value of λ and T1 equals respectively to 10^{-1} h^{-1} and 2 hours. As it can be observed, Time To Failures (TTF) are greater than T1 with a MTTF value roughly equals to $1/\lambda$. Therefore this modeling approach cannot be applied to systems that are tested periodically as the TTF and the MTTF must belong to the interval [0,T1] and not to $[0,+\infty[$.

In Fig. 5, the failure distribution is truncated to age T1. As it can be observed, Time To Failures and MTTF belong to interval [0, T1]. The simulation gives a MTTF around the value of T1/2. This modeling approach for the TTF is the good one to satisfy the criterion of the half of the testing period given in the introduction. Please, see remark (vi). However, one can see that the system fails for all the testing periods. This is impossible due to the high average reliability R of a safety system which relies between [0.9, 0.99999] according to IEC61508.

Finally, in Fig. 6 the failure distribution is truncated to age T1 and a TTF is generated only if the system experiences a failure before age T1. This approach is based on Bernoulli trials theory as described in this paper. The outcome of the periodic testing is in one of two mutually exclusive ways: "either a failure appears within actual test interval [0,T1]" with probability *p* or "no failure appears within actual test interval [0,T1]" with probability *1-p*. This modeling approach for the failure process of a SIS is the right one as a minority of testing periods experience a failure due to the SIS high reliability.

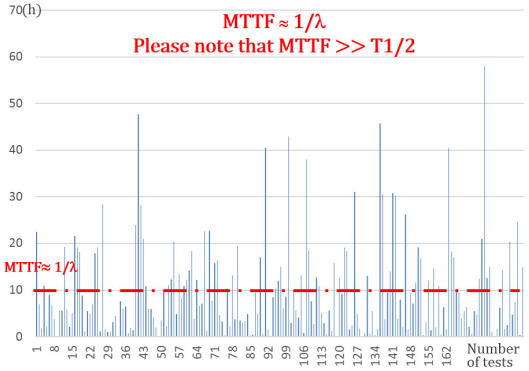

Fig. 4. Monte Carlo simulation results with a scan of the entireness of the exponential failure distribution.

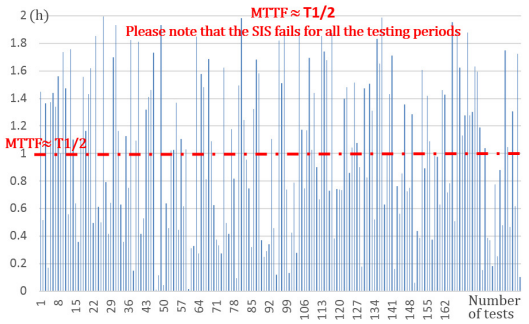

Fig. 5. Monte Carlo simulation results with a truncation of the failure distribution to age T1.

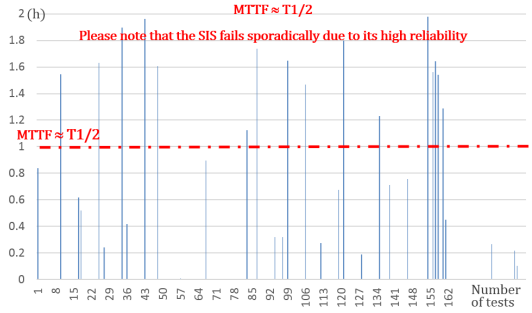

Fig. 6. Monte Carlo simulation results with a Bernoulli trials modelling and a truncation of the failure distribution to age T1.

5.3 *Consequences for the assessment of PFDaverage*

In order to understand why a discrete time approach is needed in practice, let's have a look on Fig. 4. You can see that time to failures exceed the length of the periodic test i.e. T1=2 hours. Moreover, the MTTF tend toward the value of $1/\lambda$=10 hours as the Monte Carlo algorithm scan the entireness of the failure distribution. Therefore, $F(t)\rightarrow 0$ for $t\rightarrow+\infty$ and the probability to fail for the mean value of time to failures obtained by simulation is equal to $F(t=MTTF)= 1-e^{-(\lambda\cdot MTTF)}=1-e^{-1}=0.63$. This value is of course an erroneous one for SIL studies. Whereas, for the time to failures obtained with a truncation of the failure distribution as given in Fig. 5, the mean value of the time to failures obtained experimentally tend toward the value of T1/2. Therefore, $F(t)\rightarrow F(T1)$ for $t\rightarrow T1$ and the probability to fail for the mean value of time to failures obtained by simulation is equal to $F(t=T1/2)=1-e^{-(\lambda\cdot T1/2)}=0.095$. This value is the right one for SIL studies as the mean time to failures converge to the expected value of T1/2.

5.4 *Experimental results applying Monte Carlo simulations for SIL studies*

To demonstrate the powerfulness of the predictive model, equations (5), (15), (16), (17) are applied for a 1oo1 SIS having a periodic test of length 8 hours and a probability to fail over [0,T1] equals to $7.99\cdot10^{-5}$, $7.99\cdot10^{-4}$, $7.96\cdot10^{-3}$, $7.68\cdot10^{-2}$ i.e. for a λ value respectively equals to 10^{-5}, 10^{-4}, 10^{-3} and 10^{-2} h^{-1}.

Table 6 gives the expected number of failures E(X) for a use of 20 years i.e. 21900 testing periods of 8 hours (column 2), the standard deviation (column 3), odds on favor of a SIS failure (column 4), and SIL according to the novel approach proposed in this paper i.e. the maximal probability to fail over [0,T1] applying Table 5. Please see column 5 of Table 6.

Table 6. Odds on favor a failure for periodic testing T1 of length 8 hours. Case of a 1oo1 SIS.

p	E(X)	±σx	Of	SIL
$7.99\ 10^{-5}$	1.75	1.32	1:12499	4
$7,99\ 10^{-4}$	17.5	4.18	1:1249	3
$7,96\ 10^{-3}$	174.5	13.15	1:124	2
$7,68\ 10^{-2}$	1683.7	39.42	1:12	1

Table 7. Monte Carlo simulation results for periodic testing T1 of length 8 hours. Case of 1oo1 SIS.

p	Number of failures	TTF Min (h)	TTF Max (h)	Mean of TTF (h)
$7.99\ 10^{-5}$	2	1.059	3.404	2.231
$7,99\ 10^{-4}$	18	0.1095	6.782	3.731
$7,96\ 10^{-3}$	166	0.0037	7.903	4.010
$7,68\ 10^{-2}$	1740	0.0070	7.995	4.003

Table 7 gives the results for a Monte Carlo simulation of 20-years. If you compare the number of times the SIS fails over the whole duration of the simulation with the expectation to fail given by the predictive model (see Column 2, Table 6 and Table 7), you observe that experimental results converge to the theoretical ones considering the standard deviation around the average. Experimental and theoretical results confirm the assertion that the SIS failure concerns a reduced set of testing periods during its lifecycle.

Please note that the SIS fails less than once per year only for p equals $7.99 \cdot 10^{-4}$ and $7.99 \cdot 10^{-5}$ i.e. for SIL 3 and 4. Therefore, the notion of high and low demand mode of IEC61508 depends also on the probability to fail of the Equipment Under Control (EUC) and is not only due to the probability to fail of the safety system. The problem at stake is finding the probability that the EUC fails knowing that the SIS is already in a failed state. Finding the solution of this problem may require the application of Bayesian probabilities.

One another point to be observed in column 5 of Table 7 is that the mean of TTF tends to the value of T1/2 only for SIL1 and 2. This observation allows to validate the truncation of the failure distribution for the simulation of Monte Carlo since the mean of TTF tends toward the value of T1/2 and not to the value of $1/\lambda$. Please note that for high SIL i.e. for a probability to fail p less or equal to 10^{-4}, simulation results do not converge to T1/2 because of rare failure events despite the simulation of 20 years.

One advantage of the predictive model proposed in this paper is that the SIS designer is able to quantify the relative probability that the SIS will experience a failure during a test interval with the notion of Odds on. A look at Of in Table 6 shows that the SIS designer has to expect, as an average, 1 test period experiencing a failure against 12 periods of test with no failure i.e. an odds equals to 1:12 for SIL 1. Likewise, looking at Table 6, the odds in favor a SIS failure are equal to 1 against 124 for SIL2, 1 against 1249 for SIL3 and 1 against 12499 for SIL4.

6. Validation by comparison between experimental and theoretical results

To the ends of validation, a comparison is made between the SIL values assessed with

i) the formula of PFDaverage given in the IEC61508 standard,
ii) the predictive model according to the novel approach proposed in this paper,
iii) simulation results.

This comparison was done for a λ value respectively equals to 10^{-5}, 10^{-4}, 10^{-3} and 10^{-2} h^{-1} and a period of test of length 8 hours.

i) Concerning a validation applying the IEC61508 standard, the PFDaverage is calculated according equation (1) i.e. $PFDaverage=1-e^{-\lambda \cdot (T1/2)}$ and the probability obtained is compared to the ones given in Table 1 according to the standard. For the chosen values of λ, it comes a PFDaverage equals respectively to $3.99 \cdot 10^{-5}$, $3.99 \cdot 10^{-4}$, $3.98 \cdot 10^{-3}$, $3.84 \cdot 10^{-2}$ and a SIL value respectively equals to 4, 3, 2 and 1.

ii) Concerning a validation applying the predictive model, equation (4) is applied i.e. $p=pMax=1-e^{-\lambda \cdot T1}$ and the probability obtained is compared to the ones given in Table 5 according to the novel proposed approach. For the chosen values of λ, it comes a pMax value respectively equals to $7.99 \cdot 10^{-5}$, $7.99 \cdot 10^{-4}$, $7.96 \cdot 10^{-3}$, $7.68 \cdot 10^{-2}$ and a SIL value respectively equals to 4, 3, 2, 1. Please note a ratio of two between pMax and PFDaverage given in above paragraph i). This property is sufficient to validate the novel approach proposed in this paper which recommend the use of Table 5 for SIL assessment.

iii) Concerning a validation based on simulation, the probability to fail $F(t)= 1-e^{-\lambda \cdot t}$ is assessed using the mean of TTF generated by the Monte Carlo simulation (See column 5 of Table 7) and compare the probability obtained to the ones given in Table 1 according IEC61508. For the chosen values of λ, the simulation gives respectively a mean of TTFs equal to 2.231 h, 3.731 h, to 4.010 h, 4.003 h and a SIL value respectively equals to 4, 3, 2, 1.

Table 8 summarizes and compares the SIL values obtained applying the three methods to the ends of validation. As you can see the same value of SIL is obtained for all cases.

Table 8. SIL validation comparing three methods

λ (h^{-1})	T1 (h)	SIL applying IEC 61508	SIL according to the novel proposed approach	SIL according to Monte Carlo simulation results
10^{-5}	8	4	4	4
10^{-4}	8	3	3	3
10^{-3}	8	2	2	2
10^{-2}	8	1	1	1

7. Conclusion

This paper made at first a review of mathematical inconsistencies in the practices for assessing SIL. Secondly, it introduced an unambiguous approach for risk reduction based on a discrete time approach. Thirdly, it proposed a predictive model to quantify the average number of failures that a SIS will experience during its life cycle. Finally, simulation results were given to demonstrate the powerfulness of the proposed model. This novel approach for risk reduction is

more relevant as there are no approximations and ambiguities in the assessment of SIL. It is also simpler to apply because it does not rely on the notion of average probability of failure that often disturbs designers and engineers, especially when architectures must be combined with each other to quantify the SIL of complex architectures. One advantage of the proposed approach is that SIL can be quantified calculating the maximal probability to fail over the testing period and by applying conventional reliability studies.

In order to illustrate the potential of the novel approach for the assessment of safety integrity levels, based on Bernoulli trials theory, the predictive model described in this paper has been also applied to SIL studies for architectures 2oo2, 1oo2, and 2oo3. A thorough validation has been made using Monte-Carlo simulations. The results of those simulations are not presented in this paper because of the recommendation on the length of the paper, they will be published in a future publication.

Acknowledgement

The author would to thank the following institutions for their support: the joint research lab SurferLab funded by European Regional Development Fund (ERDF) and Hauts-de-France region, Univ. Polytechnique Hauts-de-France, Laboratory LAMIH, Systems Manufacturing Academics Resources Technologies S.mart (previously called AIP-Primeca NPdC) and engineering school ENSIAME associated recently with INSA Group.

References

Al-Athari, F.M. (2008). Estimation of the mean of truncated exponential distribution, *Journal of Mathematics and Statistics 4 (4)*:284-288.

Alston, C.-L., K.-L. Mengersen, A.-N. Pettitt (2013). Case Studies in Bayesian Statistical Modelling and Analysis. Wiley Series in Probability and Statistics. J. Wiley & Sons.

Aubry, J.-F., N. Brinzei, M.-H. Mazouni. (2016). Systems Dependability Assessment – Benefits of Petri Net Models, Iste, Wiley.

Beugin, J., D. Renaux, and L. Cauffriez (2007). A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems, *Reliability Engineering & System Safety 92*, 1686–1700.

Cacheux, P.J., S. Collas, Y. Dutuit, C. Folleau, J.P. Signoret and P. Thomas (2013). Assessment of the expected number and frequency of failures of periodically tested systems, *Reliability Engineering & System Safety 118*, 61–70.

Cauffriez, L. (2015). A review of SIL theory and a demonstration on the need to truncate the exponential distribution for the generation of SIS failures: Example for a 1oo1 channel architecture, QUALITA, Nancy, France.

Cauffriez, L. (2017). Modelling of Safety Instrumented Systems by using Bernoulli trials: towards the notion of odds on for SIS failures analysis, *Journal of Physics: Conference Series*, 783 012057.

Chebila, M., F. Innal. (2015). Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH, *Journal of loss Prevention in the process industries 34*, 167-176.

Dutuit, Y., F. Innal, A. Rauzy and J-P. Signoret. (2008). Probabilistic assessments in relationship with safety integrity levels by using fault trees. *Reliability Engineering & System Safety 93*, 1867–1876.

Guo, X. Yang (2007). A simple reliability block diagram method for safety integrity verification", *Reliability Engineering & System Safety 92*, 1267-1273.

Hsu, H. (1997). Theory and Problems of probability, random variables and random processes, Schaum's Outline.

IEC 61508. (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems E/E/PE, Part 2, Int. Electrotechnical Commission.

Langeron, A., A. Barros, A. Grall, C. Bérenguer. (2008). Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules, *Journal of Loss Prevention in the Process Industries 21(4)*, 437–449.

Mechri, W., C. Simon, and K.B. Othman (2015). Switching Markov chains for a holistic modeling of SIS unavailability. *Reliability Engineering and System Safety 133*, 212–222.

Rausand, M. (2014). *Reliability of safety-critical systems: theory & applications*, J. Wiley.

Sallak, M., C. Simon, and J.F. Aubry. (2008). A fuzzy probabilistic approach for determining safety integrity level, *IEEE Trans. on Fuzzy Systems 16(1)*, pp. 239-248

Signoret, J.P., Y. Dutuit, P.J. Cacheux, C. Folleau, S. Collas, and P. Thomas (2013). Make your Petri nets understandable: Reliability block diagrams driven Petri nets, *Reliability Engineering & System Safety 113*, 61–75.

Walsh, J.-B. (2012). Knowing the Odds: An Introduction to Probability. *American Mathematical Society 139*.

Zhang, T., W. Long, and Y. Sato (2003). Availability of systems with self-diagnostic components applying Markov model to IEC61508-6. *Reliability Engineering & System Safety 80*, 133–141.