Modelling of Safety Instrumented Systems by using Bernoulli trials: towards the notion of odds on for SIS failures analysis

Laurent Cauffriez

Modelling of Safety Instrumented Systems by using Bernoulli trials: towards the notion of odds on for SIS failures analysis

IOP Conf. Series: Journal of Physics: Conf. Series **783** (2017) 012057 doi:10.1088/1742-6596/783/1/012057

Modelling of Safety Instrumented Systems by using Bernoulli trials: towards the notion of odds on for SIS failures analysis

Laurent Cauffriez

LAMIH - UMR CNRS 8201
University of Valenciennes
Le Mont Houy, F-59313, Valenciennes Cedex 9, France
laurent.cauffriez@univ-valenciennes.fr

Abstract. This paper deals with the modeling of a random failures process of a Safety Instrumented System (SIS). It aims to identify the expected number of failures for a SIS during its lifecycle. Indeed, the fact that the SIS is a system being tested periodically gives the idea to apply Bernoulli trials to characterize the random failure process of a SIS and thus to verify if the PFD (Probability of Failing Dangerously) experimentally obtained agrees with the theoretical one. Moreover, the notion of "odds on" found in Bernoulli theory allows engineers and scientists determining easily the ratio between “outcomes with success: failure of SIS” and “outcomes with unsuccess: no failure of SIS” and to confirm that SIS failures occur sporadically. A Stochastic P-temporised Petri net is proposed and serves as a reference model for describing the failure process of a 1oo1 SIS architecture. Simulations of this stochastic Petri net demonstrate that, during its lifecycle, the SIS is rarely in a state in which it cannot perform its mission. Experimental results are compared to Bernoulli trials in order to validate the powerfulness of Bernoulli trials for the modeling of the failures process of a SIS. The determination of the expected number of failures for a SIS during its lifecycle opens interesting research perspectives for engineers and scientists by completing the notion of PFD.

1. Introduction

The demand of a Safety Instrumented System (SIS) depends on the failure of the so called Equipment Under Control (EUC) which is *an equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities* [1]. The principle of SIS demand is given in Figure 1. The role of the SIS is to bring the EUC into a safe state when all safety barriers have failed (ultimate safety level) and to do it preventively when the SIS itself fails (integrity of the safety function).

Table 1 gives an overview of possible SIS architectures according to IEC 61508 standards [1]. Please note that for 1oo1 channel, any dangerous failure leads to a failure of the safety function when a demand arises. Two types of intrinsic failures can affect the well functioning of a SIS channel: Dangerous failure and Safe Failure. Dangerous failures are defined by [2] as failures that can provoke accidents because the failed SIS is unable to face a potentially dangerous event for the equipment under control. Safe failures of the SIS denote failures that have no consequence in terms of safety for the equipment under control.

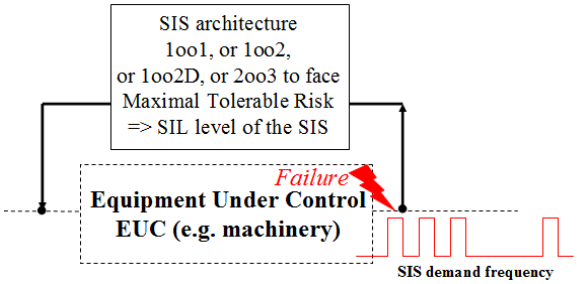
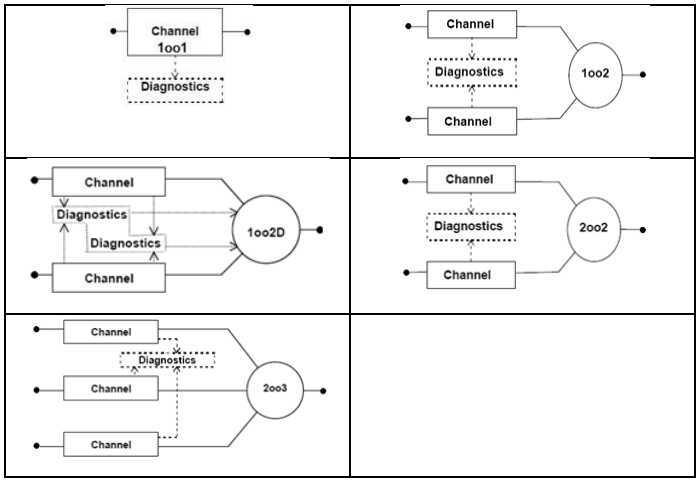


Figure 1. Principle of the demand of SIS

Table 1. Architectures of Safety Instrumented Systems



As a SIS is equipped with a self-diagnostic system, it is thus possible to detect intrinsic failures leading to a specific Safety Integrity Level of the SIS (SIL level of the SIS): the performance of the diagnostic depends on the ability of the diagnosis to care with some type of failures or not.

As described by [2], the tree of figure 2 gives the decomposition of the types of failures λ (λ is usually called failure rate and its unit is h^{-1} or $year^{-1}$). Please note that all the SIL theory developed in IEC 61508 standards make a strong assumption: failure distributions are assumed to be exponential and failure rates are therefore constant regardless of the type of SIS architectures i.e. 1oo1, 1oo2, 1oo2D, 2oo2, 2oo3.

On this point of view, the architecture 1oo1 is the reference for theoretical SIL calculation. For the other types of architectures, SIL levels are usually deduced from the 1oo1 architecture by applying conventional probabilities for events i.e. $P(\overline{Channel1} \cap \overline{Channel2})$ for 1oo2 architecture and, $P(\overline{Channel1} \cup \overline{Channel2})$ for 2oo2 architecture,…

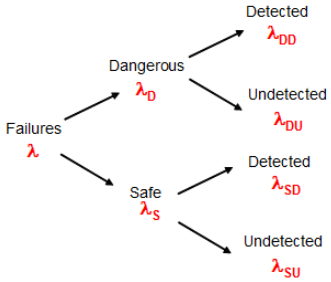


Figure 2. Classification of failures

Markov models [3]-[4], , Reliability block diagram [5], Cause-consequence diagrams [6], Stochastic Petri Nets models [7]-[9], Fault Tree models [10]-[11] or analytical expressions [12] have already

been proposed to assess the SIL level of safety systems architecture. This paper proposes a new and original approach to model the failure process of a SIS based onto Bernoulli trials theory, and aims to complete the notion of PFD given in IEC61508.

2. Reminder on PFDaverage (PFDavg)

The average probability of failing dangerously for the SIS architecture within the test interval [0,τ] is given in equation (1) and represented in figure 3. Applying simplifications proposed by [3] i.e. $ta \approx \frac{\tau}{2}$ and $\lambda D \cdot \frac{\tau}{2} << 1$, equation (1) becomes equation (2) which agrees with the one given in IEC standard 61508-6 for 1oo1 channel architecture. The mean value of time *tc1* for a channel unreliability on interval [0,τ] is equal to equation (3) (see figure 4).

$$PFDavg = 1 - e^{-\lambda D \cdot ta} \tag{1}$$

$$PFDavg = 1 - e^{-\lambda D \cdot \frac{\tau}{2}} \approx \lambda D \cdot \frac{\tau}{2} \tag{2}$$

$$tc1 = \tau - ta \approx \frac{\tau}{2} \tag{3}$$

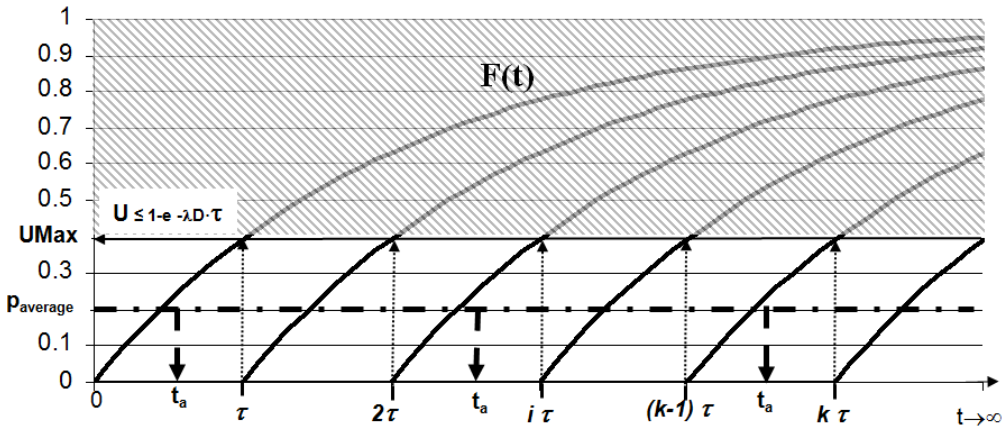


Figure 3. Reminder of PFDavg

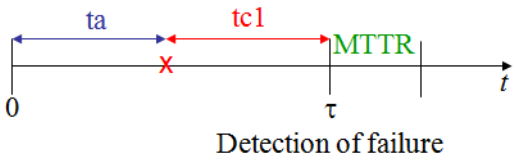


Figure 4. Definition of the mean value of time *tc1* for dangerous failure in [0,τ]

The corresponding value of SIL is found in Table 2 as defined by the standard IEC61508 [1]. A look at probabilities given in Table 2 points out that a dangerous failure occurs very rarely. Indeed, the probability that the SIS has no dangerous failures at age τ (inclusive or exclusive) i.e. that the SIS survives at age τ is very high and belongs to]0.99, 0.99999] according to SIL level 1 (PFD<10^{-1}) and SIL level 4 (PFD≥10^{-5}) of Table 2.

Table 2. Safety Integrity Levels according to PFD

SIL			
4	$10^{-5} \leq$	PFD	$< 10^{-4}$
3	$10^{-4} \leq$	PFD	$< 10^{-3}$
2	$10^{-3} \leq$	PFD	$< 10^{-2}$
1	$10^{-2} \leq$	PFD	$< 10^{-1}$

For reminder, the probability to survive age *t* (inclusive or exclusive) — i.e. the probability of no failure before age *t* — is equal to (4).

$$R(t) = p = e^{-\lambda D \cdot t} \quad (4)$$

Similarly, the probability of failure to age *t* (inclusive or exclusive) is given by (5).

$$F(t) = 1 - p = 1 - e^{-\lambda D \cdot t} \quad (5)$$

Therefore, a SIS can either survive at age τ with probability $p = e^{-\lambda D \cdot \tau}$ or fail dangerously within a test interval with a probability $F(t) = 1 - p = 1 - e^{-\lambda D \cdot t}$ for any $t \in [0, \tau]$. Please note that the maximal probability of failure is achieved at age τ and is equal to $Umax = F(\tau) = 1 - e^{-\lambda D \cdot \tau}$.

On the other hand, it is to be observed that there are two possible outcomes for the periodic test characterizing the failure process of the SIS: either "a failure appears within current test interval [0,τ]" or "no failure appears within current test interval [0,τ]". This observation has given us the idea to use Bernoulli trials for characterizing more deeply the failure behaviour of the SIS during its lifecycle.

3. Proposition of using Bernoulli trials to characterize the process failures of a SIS

3.1 Reminder on Bernoulli experiment and Bernoulli trials

A Bernoulli experiment is a random experiment, the outcome of which can be classified in one of two mutually exclusive ways, say "success" or "unsuccess".
A sequence of Bernoulli trials occurs when a Bernoulli experiment is performed several independent times so that the probability of success, say p, remains the same from trial to trial.
Let a random variable *X* being the number of success for an infinite sequence of Bernoulli trials and *n* being the first *n* trials, then [13]:

i) random variable *X* has a binomial distribution and the probability that exactly *k* successes occur in the first *n* trials is given by $p(X = k) = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$ (6)

ii) the expected value of the random variable *X* is one measure of the "centre" of the distribution and is the average of infinitely many observations on *X*, the expected value is defined as

$$E(X) = \mu_X = np. \quad (7)$$

iii) the variance of the random variable *X* measure its "spread" and is defined as

$$V(X) = np(1-p). \quad (8)$$

iv) the standard deviation σ_X is the positive square root of the variance $\sigma X = \sqrt{np(1-p)}$ (9)

v) odds on favour of success is the ratio of the probability of an event occurring to the probability of its not occurring and is equal to $Of = \frac{p}{1-p} = \frac{Outcomes\ with\ success}{Outcomes\ with\ \ unsuccess}$. (10)

vi) odds against a success is the ratio of the probability of a not occurring event to the probability of its occurring and is equal to $Oa = \frac{1-p}{p} = \frac{Outcomes\ \ with\ unsuccess}{Outcomes\ \ with\ \ success}$. (11)

vii) For a very large population of trials i.e. for $n \to +\infty$, probability *p* that trials result in success is given by $\frac{Outcomes\ with\ \ Success}{n} \to p$ as $n \to +\infty$. (12)

3.2 Bernoulli trials to characterize the process of failures for a SIS

Let a random variable X characterizing the failure process of the SIS. If a parallel is drawn between Bernoulli experiment and SIS testing process, it comes that the outcome of periodic testing of the SIS can be classified as either:

- a success, "X=1, a SIS failure appears within current time interval [0,τ]" with probability $p = 1 - e^{-\lambda D \cdot \tau}$. (13)
- an unsuccess, "X=0, no SIS failure appears within current time interval [0,τ]" with probability $1 - p = e^{-\lambda D \cdot \tau}$. (14)

This way to model the random process of SIS failures thanks to Bernoulli trials is given in figure 5.

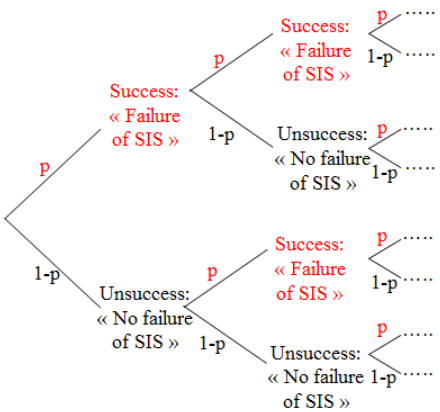


Figure 5. Application of Bernoulli trials to the modelling of SIS failures

A first step of our study is to assess "odds on favour of a failure" O*f* for a SIS according to equation (10). On this point of view, equation (15) gives the definition of "odds on favour of a failure" applied to the modelling of the failure process of a SIS and is obtained by replacing in equation (10) probabilities *p* and *1-p* by respectively $p = 1 - e^{-\lambda D \cdot \tau}$ and $1 - p = e^{-\lambda D \cdot \tau}$.

$$Of = \frac{p}{1-p} = \frac{1 - e^{-\lambda D \cdot \tau}}{e^{-\lambda D \cdot \tau}} \quad (15)$$

The notion of "odds on" seems to be very interesting for the study of SIL levels because it gives the relative probability that the SIS will experience a failure. Moreover, "odds on" depend only on the failure rate λD and test interval τ fixed by the designer.

Table 3 gives a correspondence table between "odds on favour a failure" and SIL levels according IEC61508 standard. As for example, for a odd equals to 1/99 (upper limit of SIL 1), the SIS designer has to expect 1 outcome with success i.e. "X=1, a failure of the SIS appears within current interval $[0,\tau]$" against 99 outcomes with unsuccess "X=0, no failure of the SIS appears within current interval $[0,\tau]$".

Table 3. Odds on favour of failures for a SIS in comparison with SIL levels

SIL	PFD		
4	$10^{-5} \leq$	PFD	$< 10^{-4}$
3	$10^{-4} \leq$	PFD	$< 10^{-3}$
2	$10^{-3} \leq$	PFD	$< 10^{-2}$
1	$10^{-2} \leq$	PFD	$< 10^{-1}$

SIL	Odds on favour a SIS failure		
4	1/99999 $\leq$	Of	$<$ 1/9999
3	1/9999 $\leq$	Of	$<$ 1/999
2	1/999 $\leq$	Of	$<$ 1/99
1	1/99 $\leq$	Of	$<$ 1/9

Another interesting point is that, during a long working time (or during the lifecycle), the SIS is subjected to a total number of N tests whose outcomes are either the system experiences a failure or not. One another advantage of Bernoulli trials is to have, from the beginning of the design, a first approximation of the number of times $\hat{r}$ (equation 16) that the SIS will be subject to a failure for a long working time according to expected value (7) and standard deviation (9).

$$\hat{r} = N \cdot \frac{p}{1-p} = N \cdot \frac{1 - e^{-\lambda D \cdot \tau}}{e^{-\lambda D \cdot \tau}} \tag{16}$$

Please note that this way of assessing the estimated number of failures for a SIS consider that repair duration after a failure detection does not take time. Indeed, a long repair time leads to a reduction of the SIS working time and therefore, in the same proportion, to a reduction of the number of testing periods during its working time. Table 4 gives the expected value $E(X)$ and standard deviation of random variable X characterizing the failure process of a SIS by applying equations (7) and (9) of the Bernoulli theory.

In Table 4, the number of trials n is assessed for a SIS working time expressed in hours and corresponding respectively to 1 year, 10 years, 100 years, 1000 years working time assuming that the test has a period τ equal to 1 hour. One advantage of Table 4 is to give an expected number of times that the SIS will have a failure during its working time: the more the number of testing is important, the more the estimation of SIS failures is good (See column 6).

Looking at Table 4 for $p=10^{-5}$, one can observe that the value of $E(X)$ differs by a factor that is multiple to 10 for column 3 (1 year), 4 (10 years), 5 (100 years) and 6 (1000 years): 0.0876 (1 year), 0.876 (10 years), 8.76 (100 years) and 87.6 (1000 years).

Please note that theory with equation (12) stipulates that the outcomes with success tends toward the probability p if the number of trials n tends to infinity.

Table 4 confirms that, for a long working time, the more the level of SIL is high, the more the probability of failures is low.

Table 4. Theoretical expected value of random variable *X* and standard deviation characterizing the failure process of a SIS

1	2	3	4	5	6
		1 year	10 years	100 years	1000 years
p= P(Failure of SIS)		*n*= 8760	*n*= 87600	*n*= 876000	*n*= 8760000
10^{-5}	*E(X)*	**0.0876**	**0.876**	**8.76**	**87.6**
	σ_X	±0.087	±0.935	±2.959	±9.359
10^{-4}	*E(X)*	**0.876**	**8.76**	**87.6**	**876**
	σ_X	±0.935	±2.959	±9.359	±29.595
10^{-3}	*E(X)*	**8.76**	**87.6**	**876**	**8760**
	σ_X	±2.958	±9.354	±29.582	±93.548
10^{-2}	*E(X)*	**87.6**	**876**	**8 760**	**87 600**
	σ_X	±9.312	±29.448	±93.125	±294.489
10^{-1}	*E(X)*	**876**	**8 760**	**87 600**	**876 000**
	σ_X	±28.078	±88.791	±280.784	±887.918

To conclude this paragraph, it seems that equations (15) and (16) proposed in this paper are sufficient to characterize the failure process of a SIS. Indeed, the notion of "odds on" and the estimation of the expected value of failures that the SIS will experience during its working time (or its lifecycle) seems to complete the notion of PFD.

The target of the next paragraph is to propose a Stochastic P-temporized Petri Net that will serve as reference model for a 1oo1 SIS architecture in order to compare experimental simulation results with the theoretical failure process of a SIS modelled thanks to Bernoulli trials.

4. Proposition of a reference model based onto a Stochastic P-temporized Petri Net for a 1oo1 SIS architecture

For purposes of validation, a reference model based onto a Stochastic P-temporized Petri Net for a 1oo1 SIS architecture is given in figure 6.

The probability to survive during a test interval τ is modelled thanks the left branch of the Petri net given in figure 6. This agrees with equation (14).
The probability to fail during a test interval τ is very low and is modelled thanks the right branch of the Petri net given in figure 6. This agrees with equation (13).

The functioning of Stochastic P-temporized Petri Net given in figure 6 is the following:
Places P1 and P10 are marked at the beginning of the interval $[0,\tau]$. The mark in place P1 moves in place P2 (no failure occurs with a probability $e^{-\lambda D \cdot \tau} = 1 - p$) either in place P3 (a failure occurs with a probability $1 - e^{-\lambda D \cdot \tau} = p.$) If the SIS experiences a failure within $[0,\tau]$ interval, the failure is generated at time $ti \in [0,\tau]$ and place P4 is marked.

After a duration d1 equal to the duration of the periodic test interval $[0,\tau]$, the temporized place P10 is left and place P11 is marked: this models the duration of the testing of the SIS and repair process by making the assumption in this case study that the repair duration is equal to d2=0 hour. The

synchronization between Stochastic P-temporized Petri Nets -a- and -b- of figure 6 is made by the new arrival of the token in place P10.

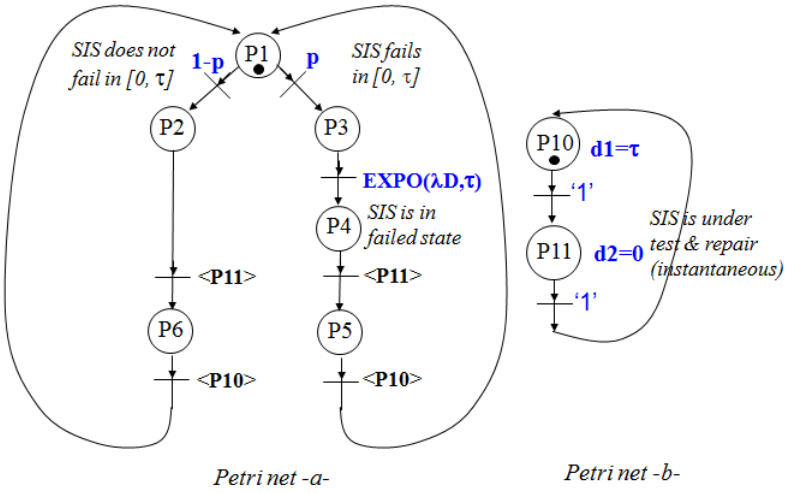


Figure 6. Reference model based onto a Stochastic P-temporized Petri Net for a 1oo1 SIS architecture

Discussion:

1) Please note that the use of a truncated exponential distribution function *EXPO(*λD *,τ)* is absolutely necessary to generate with Monte Carlo algorithm failure events within [0,τ] interval. This crucial modelling point was demonstrated in [14] and is summarized in figure 7: *tevent* ≤τ is equivalent to $Umax \le F(\tau)$ because F(t) is an increasing function i.e. $\forall t \in [0,\tau], \quad F(t) \in [0, 1-e^{-\lambda D \cdot \tau}]$

Therefore F(t) must be truncated to the maximal value $Umax = F(\tau) = 1-e^{-\lambda D \cdot \tau}$ when inverting the distribution function for the simulation of Monte Carlo. This is an essential condition to have statistical results closest to reality. Indeed, this modelling approach decomposes the simulation time *t* into *n* intervals, each interval having a length equals to *τ*.

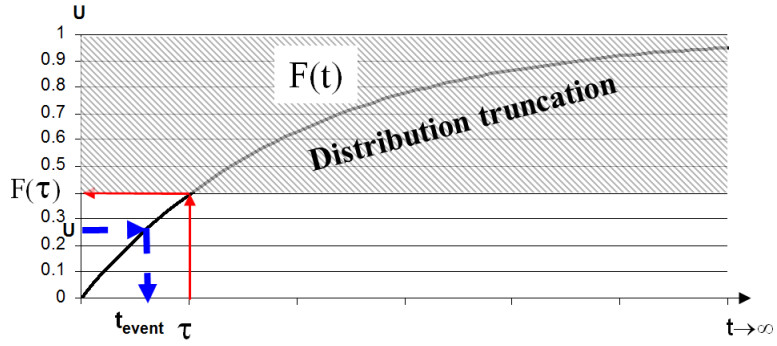


Figure 7. Truncation of failure distribution function F(t) due to periodic testing of SIS

2) This way of modelling the failure process of a SIS is closer to reality in so far as the probability to survive (left branch of Petri net -a-) or to fail (right branch of Petri net -a-) for the SIS is represented. Moreover, successive test intervals are really implemented and are not deduced "a posteriori" using mathematical modulo function "mod" as proposed in [1].

5. Validation of Bernoulli trials approach thorough simulation using Petri net reference model

To implement the Stochastic P-temporised Petri Nets of figure 6, we need a tool which:
1) can generate intermediate reports giving exactly the occurrence of failure events during the whole Monte Carlo simulation in order to verify failures appear within current time interval [nτ, (n+1)τ] with n ∈ [1,N] and N being the highest test number for the simulation.
2) implements the truncation of the failure distribution F(t) described in figure 7.

We have not found such Petri Nets open source software and we have therefore implemented the two proposed Stochastic P-temporised Petri Nets with SIMAN/ARENA discrete event simulation tool. Indeed, this tool allows to define user defined distribution functions and to generate intermediate reports during Monte Carlo simulation.

5.1 First experimental campaign: one year simulation (8760 hours)

During one year simulation, a total of N=8760 tests were observed and r=48 failures were counted. Over the whole Monte Carlo simulation duration i.e. 8760 h, the SIS was in down state during 20.53676887 h and in well functioning state during $\sum_{i=1}^{r} TTFi + (N - r) \cdot \tau = 27.46323113$h+ 8712h=8739.463231 h. An estimator of experimental MTTF can be assessed by using (17)

$$MTTF' = \frac{1}{\lambda'} = \frac{\sum_{i=1}^{r} TTFi + (N - r) \cdot \tau}{r} \quad (17)$$

Therefore, it comes for this simulation MTTF'=182.0721506 h and $\lambda' = 5.492328.10^{-3}$ h^{-1}. These both values agree with input data of the model for λD=5.10^{-3} h^{-1} and τ=1h. Moreover, Table 5 (last raw) shows an experimental PFDavg equal to $2.344380 \cdot 10^{-3}$ and the system is of SIL2.

This experimental PFDavg converges to the theoretical PFDavg according to IEC61508 which is equal to $PFDavg\_IEC61508 = 1 - e^{-\lambda D \cdot \frac{\tau}{2}} = 2.4968776 \cdot 10^{-3}$.
There is a small deviation between the experimental PFD and the theoretical one of $1.52 \cdot 10^{-4}$ due to the simulation approach. Indeed, the mean value to failure for the whole simulation during one year is equal to 0.5721506486 h and is not therefore fully equal to τ/2 as assumed by the theory due to the simulation duration of only one year. The simulation was deliberately limited to 1 year to display in this paper intermediate results such as number of failures and the time to failures.

Applying equation (15) to this case study, we have:

$$Of = \frac{p}{1 - p} = \frac{1 - e^{-\lambda D \cdot \tau}}{e^{-\lambda D \cdot \tau}} = \frac{1 - e^{-0.005 \cdot 1}}{e^{-0.005 \cdot 1}} = 5.012 \cdot 10^{-3} \approx \frac{5}{995} \approx \frac{1}{199}$$

i.e. SIL2 according to our proposed Table 3 giving a correspondance between "odds on" O*f* and SIL levels. Equation (16) gives an estimated value of the number of failures equal to

$\hat{r} = N \cdot \frac{p}{1-p} = N \cdot \frac{1 - e^{-\lambda D \cdot \tau}}{e^{-\lambda D \cdot \tau}} = 43.90$ with a standard deviation σX equals to $\sigma X = \sqrt{np(1-p)} = \sqrt{8760 \cdot e^{-0.005}(1 - e^{-0.005})} = 6.59$. Therefore, it appears that the estimated number of failures with Bernoulli trials is equal to 43.9 ± 6.59 and agrees with experimental results that shows a number of failures of 48 for one year simulation i.e. 8760 tests.

Table 5. Time to failure of SIS within [0,τ] test interval for Petri Net of figure 6

1	2		3	4
Test Number	[0,τ] Test Interval		**TTFi Time To Failure (h)**	**PFDi**
23	22	23	0.840897475	4.195661E-03
96	95	96	0.815554973	4.069472E-03
177	176	177	0.481352907	2.403871E-03
511	510	511	0.013132646	6.566108E-05
706	705	706	0.368733084	1.841967E-03
787	786	787	0.430220239	2.148789E-03
958	957	958	0.498859511	2.491189E-03
961	960	961	0.337026511	1.683714E-03
992	991	992	0.776835878	3.876646E-03
1679	1678	1679	0.519807192	2.595661E-03
1681	1680	1681	0.661869227	3.303876E-03
2307	2306	2307	0.505977449	2.526690E-03
2865	2864	2865	0.861548284	4.298476E-03
2922	2921	2922	0.957011002	4.773625E-03
3025	3024	3025	0.670537633	3.347074E-03
3061	3060	3061	0.943014111	4.703972E-03
3287	3286	3287	0.90349766	4.507300E-03
3461	3460	3461	0.959439348	4.785709E-03
3722	3721	3722	0.848264938	4.232343E-03
3920	3919	3920	0.619847404	3.094439E-03
4183	4182	4183	0.724616967	3.616529E-03
4190	4189	4190	0.499254092	2.493157E-03
4232	4231	4232	0.105261534	5.261692E-04
4382	4381	4382	0.253986804	1.269128E-03
4705	4704	4705	0.918368707	4.581317E-03
4789	4788	4789	0.865380558	4.317555E-03
4833	4832	4833	0.777793087	3.881413E-03
4882	4881	4882	0.62124863	3.101424E-03
5248	5247	5248	0.333491237	1.666067E-03
5303	5302	5303	0.138910404	6.943109E-04
5537	5536	5537	0.206943178	1.034181E-03
5605	5604	5605	0.47362704	2.365333E-03
5659	5658	5659	0.589422393	2.942773E-03
6044	6043	6044	0.440582291	2.200487E-03
6182	6181	6182	0.415179222	2.073743E-03
6222	6221	6222	0.476599278	2.380159E-03
6299	6298	6299	0.144121796	7.203494E-04
6444	6443	6444	0.809779702	4.040713E-03
6602	6601	6602	0.776676663	3.875853E-03
6632	6631	6632	0.921155936	4.595189E-03
7015	7014	7015	0.159845484	7.989081E-04
7181	7180	7181	0.605390804	3.022377E-03
7506	7505	7506	0.157438503	7.868828E-04
7589	7588	7589	0.863700893	4.309193E-03
7647	7646	7647	0.323336046	1.615374E-03

7655	7654	7655	0.546007133	2.726313E-03
7864	7863	7864	0.643066131	3.210167E-03
8226	8225	8226	0.658619149	3.287679E-03
Total of 8760 tests			**Mean value of TTF=** 0.5721506486h **≈ τ/2**	**PFDavg =** 2.855810E-03

5.2 Second experimental campaign to validate Bernoulli trials approach: simulation of 50×1000 years

To validate more deeply the Bernoulli trials approach, five experimental campaigns are processed for 1oo1 architecture. For each campaign, the duration of the Monte Carlo simulation is equal to 1000 years i.e. 8760000h and 50 replications of 1000 years have been processed with input data for the Petri Net of figure 6 equal to τ=1h, d2=0h, and p respectively equal to 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}.

Experimental results are given in Table 6, these results agree with Bernoulli trials approach:
- for p=$10^{-5,}$ the total number of failures 85.42±10.115839 (column 2, raw 1 of Table 6) agrees with the theoretical expected value $E(X) \pm \sigma X = 87.6 \pm 9.3659$ of Table 4.
- the mean value of time to failure *ta* is nearly equal to $\tau/2$ i.e. 0.5h (column 4, Table 6).
- the mean value of time to failures TTF (column 6, Table 6) and the mean time between failures (column 7, Table 6) agree with the Petri net input probability $p = 1 - e^{-\lambda D \cdot \tau}$ (column 1, Table 6).

Table 6. Experimental Mean and standard deviation of the SIS failures

1	2	3	4	5	6	7	8
p	Total number of failures	Minimum value of ta	Mean value of ta	Maximum value of ta	Mean value of TTF	Mean time between failures	Mean number of test intervals between failures
10^{-5}	**85.42** ±10.115839	0.00009458	**0.49900079** ±0.032264	0.99981460	**118653.484** ±123086.377	**129251.6532** ±140754.6694	**129251.6515** ±140754.6343
10^{-4}	**877.18** ±34.856375	0.00004919	**0.50241008** ±0.007729	0.99998673	**10949.0895** ±9945.1393	**9990.92294859** ±411.707434	**9990.91426960** ±411.71604453
10^{-3}	**8751.66** ±91.427591	0.00000299	**0.50039523** ±0.002863	0.99999839	**1201.17544004** ±1143.487393	**1000.93603695** ±10.436939	**1000.93603025** ±10.43694450
10^{-2}	**87539.18** ±307.392237	0.00000003	**0.49932122** ±0.001051	0.99999919	**125.116336** ±125.076263	**100.089623** ±0.409214	**100.0696276** ±0.350987401
10^{-1}	**875881.02** ±678.46812	0.00000002	**0.49129591** ±0.000355	0.999999964	**8.7671654** ±6.630121	**10.00135287** ±7.749970E-03	**10.00134994** ±7.745831E-03

Conclusion

After an introduction, section 2 of the paper gives a reminder on PFDavg according to IEC61508. Section 3 proposes to use Bernoulli trials to characterize the process failure of a SIS during its working time i.e. during its lifecycle. The notion of "odds on" found in Bernoulli trials theory seems to be very interesting because it allows engineers and scientists to determine easily the ratio between "outcomes with failure of SIS" and "outcomes with no failure of SIS" for the whole population of tests of the SIS during its lifecycle. Section 4 proposes a Stochastic P-Temporized Petri net reference model for a 1oo1 SIS architecture, this Petri net helps to simulate the failure process of the SIS thanks to a Monte Carlo simulation. Section 5 makes a validation of the proposed approach by comparing simulation results of Stochastic Petri net with those based onto "odds on" and "expected value" of Bernoulli trials theory. Simulation results point out that expected values of SIS failures computed with Bernoulli trials approach agree with those obtained by Monte Carlo simulation for two experimental campaigns, the first one of one year and the second of 50 replications of thousand years. The ability of Bernoulli trials to characterize the sporadic occurrences of failures for a 1oo1 SIS architecture during its lifecycle was demonstrated in this paper. The main result of this study is to give the relative probability that the SIS will experience a failure in correspondence with SIL levels (see Table 3). Moreover, the introduction of expected value and standard deviation of the random variable characterizing the number of SIS failures for an infinite sequence of tests intervals (Bernoulli trials) complete the notion of PFD and allow to give a new approach to model the safety level of a SIS.

References

[1] IEC 61508-6. Functional safety of electrical/electronic /programmable electronic safety-related systems. NF EN 61508-6. AFNOR Standard, January 2011.
[2] W.M. Goble, Control Systems Safety Evaluation and Reliability (2nd ed.). Research Triangle Park (NC): ISA (The Instrumentation, Systems, and Automation Society), 1998.
[3] T. Zhang, W. Long, Y. Sato, Availability of systems with self-diagnostic components - applying Markov model to IEC 61508-6. Reliability Engineering & System Safety, Vol. 80, pp. 133–141, 2003.
[4] W. Mechri, C. Simon, K.B. Othman, Switching Markov chains for a holistic modeling of SIS unavailability, Reliability Engineering and System Safety, Vol. 133, pp.212–222, 2015.
[5] H. Guo, X. Yang, "A simple reliability block diagram method for safety integrity verification", Reliability Engineering and System Safety, Vol. 92, pp. 1267-1273, 2007.
[6] J. Beugin, D. Renaux, L. Cauffriez, A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems, In Reliability Engineering and System Safety, Vol. 92, pp. 1686–1700, 2007.
[7] P.J. Cacheux, S. Collas, Y. Dutuit, C. Folleau, J.P. Signoret, P. Thomas, Assessment of the expected number and frequency of failures of periodically tested systems, Reliability Engineering and System Safety, Vol. 118, pp. 61–70, 2013.
[8] J.P. Signoret, Y. Dutuit, P.J. Cacheux, C. Folleau, S. Collas, P. Thomas. Make your Petri nets understandable: Reliability block diagrams driven Petri nets, Reliability Engineering and System Safety, Vol. 113, pp. 61–75, 2013.
[9] Y. Liu, M. Rausand, Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems, Reliability Engineering and System Safety, Vol. 145, pp. 366–372, 2016.
[10] F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, Design of complex safety-related systems in accordance with IEC 61508, Reliability, Risk and Safety: Theory and applications, Guedes Soares & Martorell (Eds), Taylor & Francis Group, London, ISBN 978-0-415-55509-8, 2010.
[11] Y. Dutuit, F. Innal, A. Rauzy J-P. Signoret. Probabilistic assessments in relationship with safety integrity levels by using fault trees. Reliability Engineering and System Safety, Vol. 93, pp. 1867–1876, (2008).
[12] M. Chebila, F. Innal, Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH, Vol. 34, 167-176, 2015.
[13] J.B. Walsh, Knowing the Odds: An Introduction to Probability, American Mathematical Society, Vol. 139, ISBN: 978-0-8218-8532-1, 421 pages, 2012.
[14] L. Cauffriez, 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' 2015, Mar 2015, Nancy, France, https://hal.archives-ouvertes.fr/hal-01149814.