Available online at www.sciencedirect.com
ScienceDirect
Journal of Loss Prevention in the Process Industries 21 (2008) 437–449
Journal of Loss Prevention in the process industries
www.elsevier.com/locate/jlp

# Combination of safety integrity levels (SILs): A study of IEC61508 merging rules

Yves Langeron*, Anne Barros, Antoine Grall, Christophe Bérenguer

*Université de Technologie de Troyes, Institut Charles Delaunay, FRE CNRS 2848, System Modelling and Dependability Group, 12, rue Marie Curie, BP 2060-10010 Troyes cedex, France*

Received 16 October 2007; received in revised form 8 February 2008; accepted 8 February 2008

**Abstract**

The role of a safety system is to provide a safety-related function in order to monitor and maintain the safety of any equipment under its control. The safety analysis of such systems is of prime importance to avoid catastrophic consequences or even the loss of human life. In general, the various hazards that any equipment may encounter are considered without any safety functions. Later on, each hazard is studied using methods such as the risk matrix to quantify the associated risk. These methods determine which safety integrity level (SIL) needs to be implemented in order to reduce this risk to a tolerable one. Once this safety target is evaluated, an architecture is chosen during the design phase of the safety system. The standard IEC61508 states the requirements for safety systems to verify if the implemented functions reach these targets. For instance, Part 2 suggests a non-prescriptive method to merge different safety subsystems in order to achieve one with a higher SIL than those supplied by these subsystems. During the design of a SIS, the SIL selection is a very critical phase because often this system is the last line of protection against hazardous events. Even if this method is just informative, using it as a guide to follow may be an easy shortcut to label products with a dedicated safety degree. This merging method seems not to be based on an analytical method and for this reason the present paper investigates its robustness by starting from a multiphase Markovian approach. It consists in dividing the study window time of a system in phases in which a Markovian modelling is available. This method is then applied to two tudy cases given in the standard to illustrate the use of this merging method.


*Keywords:* IEC61508; Multiphase Markovian modelling; Probability of failure on demand (PFD); Safety integrity level (SIL)

## 1. Introduction

Safety Instrumented Systems (SIS) have become more and more a subject of study because of their contribution to many technical applications. For instance, a SIS may be an air-bag system, a smoke detector or a breaking system to stop a dangerous motion. The role of a SIS is to provide a safety-related function in order to monitor and maintain the safety of any equipment under its control (EUC). At initial stage of safety analysis, the potential hazards are considered. Each hazard is studied with quantitative and/or qualitative methods to capture the associated risk. These methods output which safety integrity level (SIL) needs to be implemented in order to reduce the risk to a tolerable one. For instance, the risk matrix method belongs to the quantitative tools while risk graph belongs to the qualitative ones when information like hazardous occurrence frequency is quite difficult to obtain (Marszal, Fuller, & Shah, 1999). Once this safety target is established, an architecture needs to be considered during the design phase of a SIS.

In this way, it becomes very important to verify the quality of a SIS in terms of reliability and to assess its performances notably to verify if the implemented safety functions can fulfill the safety targets defined above. The standard IEC61508 (IEC61508, 2002) is a generic one that states the requirements for safety systems and is common to several industries. For instance, starting from this standard, the process industry has developed its own sector specific one (IEC61511, 2003). In IEC61508, a safety system is mentioned as E/E/PE safety-related system (for Electrical/Electronic/

*Corresponding author. Tel.: +33 3 25 71 56 91; fax: +33 3 25 71 56 49.
*E-mail address:* yves.langeron@utt.fr (Y. Langeron).

0950-4230/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2008.02.003

**Nomenclature**

| | |
|---|---|
| DC | diagnostic coverage for dangerous failures |
| EUC | equipment under control |
| HFT | hardware fault tolerance |
| SFF | safe failure fraction |
| SIF | safety instrumented function |
| SIL | safety integrity level |
| SIS | safety instrumented system |
| PFD | probability of failure on demand (average unavailability) |
| KooN | SIS where K out of N channels have to function in order to perform its SIF |
| N | number of inspections |
| $\Lambda$ | transition rate matrix of the Markov model |
| $W_i^{IR}$ | inspection and repair matrix of the subsystem $i$ |
| $\pi(t)$ | probability of each Markov state at time $t$ |
| $f^{\mathrm{T}}$ | column vector used to only retrieve the states relating to unavailability |

Programmable Electronic) while in IEC61511 the acronym SIS is preferred for Safety Instrumented System. Although this paper studies some requirements of IEC61508, the acronym SIS is used for simplicity.

To ensure this safety mission, a SIS is submitted to diagnostic self-tests and also to periodic inspections. According to this standard (IEC61508-4 definition 3.6.7 and 3.6.8), a SIS may have two kinds of failure modes. The first one is a dangerous failure which has the potential to put the safety-related system in a hazardous or fail-to-function state. This is the case of a hidden failure not detected by an on-line test. This failure is supposed to be detected at the next inspection date. The second one is a safe failure which has not this potential even if the standard seems to give a limited focus to the behavior of this kind of failures (Langeron, Barros, Grall, & Bérenguer, 2007; Lundteigen & Rausand, 2007a). An example may be a safety shutdown valve when it fails to reopen.

Whatever the failure mode is, some failures are detected by on-line tests and others only during the inspection phases. The first ones are called detected failures, the others undetected. Thus, for both failure modes, the following rates assumed to be constant are defined:

- $\lambda_{DU}$: dangerous undetected failure rate.
- $\lambda_{DD}$: dangerous detected failure rate.
- $\lambda_{SU}$: safe undetected failure rate.
- $\lambda_{SD}$: safe detected failure rate.
- $\lambda_S$: safe failure rate $\lambda_S = \lambda_{SU} + \lambda_{SD}$.
- $\lambda_D$: dangerous failure rate $\lambda_D = \lambda_{DU} + \lambda_{DD}$.
- $\mu_{DD}$: repair rate of a dangerous failure when detected.

In addition, the standard introduces the diagnostic coverage to quantify the on-line tests efficiency to detect dangerous failures with the following definition:

$$DC = \lambda_{DD}/\lambda_D, \quad \lambda_{DU} = (1 - DC)\lambda_D, \quad \lambda_{DD} = DC\lambda_D.$$

In the aim to capture the complete behavior of a SIS, the standard gives two main measures that are the probability of failure on demand (PFD) and the safe failure fraction (SFF). The first one enables to quantify a safety integrity level (SIL) when only the dangerous random hardware failures are considered. The second measure is used to quantify the impact of the safe failures. At the design stage of a SIS, starting from PFD and SFF, the part 2 of the standard (Section 7.4.3) suggests to use merging rules to combine different subsystems with different SILs in order to get a better SIS; that is to say with a higher SIL. In Schäbe (2003), the qualitative study of several examples of simple SISs shows that general rules as the ones suggested in this standard may become quickly inconsistent notably because the inspection intervals and the design rules are not considered.

The aim of this paper is to study in an analytical way the robustness of these merging rules; it is organized as follows:

- Section 2 presents the manner to quantify PFD and SFF and the way they are used by the merging rules through two study cases given in the standard. The first one concerns a simple series structure while the second one stands for a system with redundancy.
- Section 3 defines the mathematical framework to model different architectures. First of all, a multiphase Markovian approach is used to formalize the probability of each potential state that a SIS may have. Later, this formalism enables one to generalize the expression of PFD which is applied to three models. The first one is a basic SIS (elementary channel) where the potential imperfection and the frequency of on-line tests are illustrated. A second model is proposed for a system composed of two elementary channels allowing the study of series and parallel structures. The last model concerns the second study case of the standard with some assumptions in order to reduce its complexity.
- Before concluding on the robustness of the merging rules, Section 4 presents some numerical results of the possible SIL values of the previous models. These results are compared with the ones suggested in the standard.

## 2. Safety integrity requirements

### 2.1. Probability of failure on demand

The first measure to capture the behavior of a SIS is PFD for probability of failure on demand. PFD concerns

Table 1
SIL levels for a low frequency demand of the SIF

| SIL | PFD |
|---|---|
| 4 | $\geqslant 10^{-5}$ to $<10^{-4}$ |
| 3 | $\geqslant 10^{-4}$ to $<10^{-3}$ |
| 2 | $\geqslant 10^{-3}$ to $<10^{-2}$ |
| 1 | $\geqslant 10^{-2}$ to $<10^{-1}$ |

Table 2
Architectural constraints

| SFF | Hardware fault tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| <60% | 1(na) | 2(1) | 3(2) |
| 60% − 90% | 2(1) | 3(2) | 4(3) |
| 90% − <99% | 3(2) | 4(3) | 4(4) |
| ⩾99% | 3(3) | 4(4) | 4(4) |

SIL levels for SIS type A and (type B) complexity.
na: not allowed.

only the dangerous random hardware failures and is used to define a safety integrity level (SIL). SIL is a discrete level (61508-1 Section 7.6 Tables 2–3) that specifies the ability of a SIS to fulfill its SIF on demand. As can be seen in Table 1 in the case of a low frequency demand of the safety function, each SIL represents a bounded interval for this probability. The way to quantify PFD mainly depends on the interpretation given to this measure (Bukowski & Goble, 1995; Bukowski, Rouvroye, & Goble, 2002). Some consider PFD as the average value of the unreliability function over an inspection period and others as a steady state unavailability. In the latter case, a continuous Markovian approach is used rendering the behavior of a SIS continuous in time by creating fictitious repair rates (Zhang, Long, & Sato, 2003). Note that using this method enables one to obtain the same analytical expressions for some models of the standard (1oo1, 1oo2, 2oo3…). Even if these quantifying methods lead to the same numerical results, PFD should be considered as the average value of the unavailability function over a given period of time (Lindqvist & Amundrustad, 1998; Rausand & Høyland, 2004) based upon a Markovian study for its high modelling power (Rouvroye & van den Bliek, 2002). This latter approach is used here to gain more insight into the behavior of the merging rules and to investigate their robustness even if it may become very costly for complex systems. In such a case, the study of the time dependent unavailability may be achieved with specialized software based upon e.g. Monte Carlo simulations and Petri nets[1] (Dutuit, Châtelet, Signoret, & Thomas, 1997).

### 2.2. Safe failure fraction

The second measure to characterize a SIS is SFF, for safe failure fraction. SFF considers the fraction of failures not leading to dangerous ones (Lundteigen & Rausand, 2006) and is defined by

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}. \quad (1)$$

A reliability engineer may use SFF with two approaches. First, SFF can be applied to obtain a type of architecture for a given SIL. Secondly, SFF can be applied to quantify the maximum expected SIL for a given architecture. These two ways of using SFF lie on two major keys. The first one concerns the hardware fault tolerance (HFT) given by assessing the voting of the hardware architecture. The second one is the type of SIS, more precisely the kind of complexity. The standard defines a type A that stands for a low complexity system and B for a high complexity one. A low complexity is characterized by the fact that all failure modes of the SIS are well known, its failed behaviors are clearly known and there exists feedback reliability data allowing the quantification of the dangerous failure rates. A high complexity is present when at least one of these three points is not covered. Thus, starting from SFF, HFT and the type of SIS a reliability engineer can use the rule of Table 2 to evaluate the SIL level. For instance, with a 1oo2 SIS A and a SFF of 50%, the maximum expected SIL is SIL2. On the other hand, for a system A, a SFF of 50% and a desired SIL2, the recommended architecture is with a HFT of 1 (for instance 1oo2).

### 2.3. Merging rules

The standard (Part 2, Section 7.4.3) proposes the following merging method to easily achieve a SIS starting from safety subsystems with different SILs. The desired goal is to obtain a better SIS; i.e with a higher SIL. This section of the standard belongs to the phase *Design and Development in the safety lifecycle of E/E/PE* (see Part 2: Table 1 and Fig. 2 (block 9.3)).

The best SIL for a system composed of different elementary subsystems may be achieved in four steps:

- *Step* 1: Define the safety integrity level of each subsystem following the rule in Table 2 with the values of SFF and HFT.
- *Step* 2: Design some intuitive combinations from these subsystems.
- *Step* 3: Use the following merging rules to determine the SIL of each combination
  - Series merging rule: for a series structure, the SIL is summarized by the lowest SILs of the subsystems composing the structure.
  - Parallel merging rule: the SIL of a parallel structure is given by the SIL of the subsystem with the highest SIL. In the case of its failure, the SIF is then ensured

[1] Aralia workshop software package; MOCA-RP.

by an other SIS of this structure. In order to take into account of this backup possibility, the standard considers that the HFT of the former SIS needs to be increased by one which moves it to the next higher SIL as shown in Table 2.

- Step 4: Repeat from step 2 until the entire architecture is reduced to one block to get the best SIL for the complete system.

To highlight the use of the above method, the standard (see IEC61508 part 2) proposes two study cases.

The first one (see Fig. 1) is a simple series structure composed of three SISs. Assuming that the first step is realized, the obvious combination is to reduce this SIS to an equivalent one for which the SIL is determined with the series merging rule which finally gives to the complete system a safety integrity level of SIL1.

The second one (see Fig. 2) is the case of a system composed of subsystems in redundancy. Here, there are two series structures in parallel. This redundancy is then terminated with a final subsystem. Assuming that the first step is realized, the first evident combination is to reduce the subsystems A and B to one block (A and B) whose SIL is given by the series merging rule. The equivalent safety integrity level becomes SIL2. The other evident combination is to reduce the subsystems C and D to one block (C and D) with the same series merging rule which gives an equivalent safety integrity level of SIL1. The next combination is to reduce the redundancy formed with the previous blocks to one (A and B + C and D) using the parallel merging rule. An equivalent safety integrity level of SIL3 is then achieved. At this stage, the whole system can be summarized by this block (A and B + C and D) and the final subsystem E. The last combination is to reduce these two subsystems to one block applying the series merging rule resulting finally in a safety integrity level of SIL2 for the complete system.

This merging method is very easy to apply but seems to be empirical. For this reason, the aim of the next section is to define a mathematical framework to investigate its quality for different architectures.

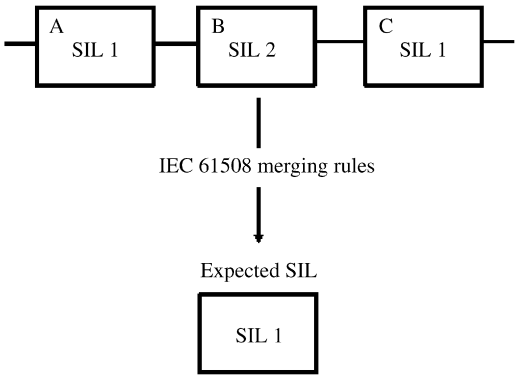


Fig. 1. Study case I. SIF composed of only one series structure.

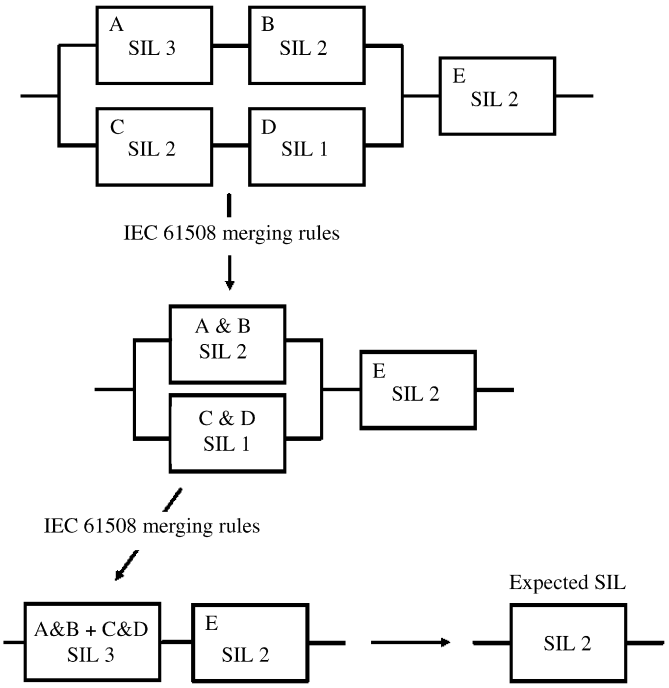


Fig. 2. Study case II. SIF composed of several channels.

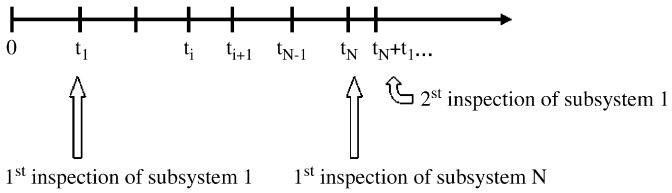


Fig. 3. Staggered tests chronology of a SIS composed of $N$ subsystems.

## 3. Mathematical modelling framework

In this section, a multiphase Markovian approach is used to capture the probabilistic behavior of a SIS composed of various subsystems and submitted to a staggered tests policy. This general case enables one to obtain the analytical expression of PFD when it is considered as the average unavailability. Then, this multiphase method is applied to three Markov models. The first one concerns a basic SIS (elementary channel), the second one a SIS with two channels (series and parallel structures) and the last one stands for the second study case of the standard (Fig. 2).

### 3.1. Multiphase Markov modelling

The general case of a safety instrumented system composed of $N$ subsystems is considered here. This system is submitted to a staggered tests policy. Each subsystem is periodically inspected with a period $t_N$ as illustrated in Fig. 3.

In a classical Markov modelling approach, the Kolmogorov equation for the whole system is

$$\pi(t)' = \pi(t).\Lambda \tag{2}$$

assuming that $\Lambda$ stands for the transition rate matrix of the Markov model and $\pi(t)$ for the probability of each state at time $t$. From a modelling point of view, the implementation of a staggered tests policy introduces in some sense a dependence to the past which can seems contradictory with Markovian assumptions of memorylessness (Becker, Camarinopoulos, & Ohlmeyer, 1994) and makes the analysis of such maintained system more complex (Bondavalli et al., 2000). However, this dependence is only limited to fixed-time points (which delimit *phases* i.e. disjoints periods of system operational life) and the proposed multiphase approach can explicitly take into account these discontinuities. A classical Markov model is associated to each phase and these discontinuities are accommodated by a mapping procedure at the transition time from one phase to the next. This procedure linearly redistributes the states probabilities at the beginning of each phase $i$ through a multiplication by an inspection and repair matrix $W_i^{IR}$ such as $\pi(t_i^+) = \pi(t_i)W_i^{IR}$; $\pi(t)$ is thus piecewise constructed (Bukowski, 2001; Châtelet, Bérenguer, & Grall, 1997).

We have then for the successive maintenance phases:

- for the phase $[0, t_1]$

  $\pi(t) = \pi(0)e^{\Lambda t}$;

- for the phase $[t_1, t_2]$

  $\pi(t) = \pi(t_1^+)e^{\Lambda(t-t_1^+)}$

  the inspection and repair time is supposed to be negligible that leads the previous relation to the following one:

  $\pi(t) = \pi(t_1^+)e^{\Lambda(t-t_1)}$

  with

  $\pi(t_1^+) = \pi(t_1)W_1^{IR}$

  and

  $\pi(t_1) = \pi(0)e^{\Lambda t_1}$

  so,

  $\pi(t_1^+) = \pi(0)e^{\Lambda t_1}W_1^{IR}$

  then

  $\pi(t) = \pi(0)e^{\Lambda t_1}W_1^{IR}e^{\Lambda(t-t_1)}$

- for the phase $[t_2, t_3]$

  $\pi(t) = \pi(t_2^+)e^{\Lambda(t-t_2)}$

  $\pi(t_2^+) = \pi(0)e^{\Lambda t_1}W_1^{IR}e^{\Lambda(t_2-t_1)}W_2^{IR}$,

  $\pi(t) = \pi(0)e^{\Lambda t_1}W_1^{IR}e^{\Lambda(t_2-t_1)}W_2^{IR}e^{\Lambda(t-t_2)}$

- for the phase $[t_i, t_{i+1}]$

  $\pi(t) = \pi(t_i^+)e^{\Lambda(t-t_i)}$

  $\pi(t) = \pi(0)e^{\Lambda t_1}W_1^{IR}e^{\Lambda(t_2-t_1)}W_2^{IR} \times \ldots \times e^{\Lambda(t_i-t_{i-1})}W_i^{IR}e^{\Lambda(t-t_i)}$.

As seen above, the repair time is assumed to be negligible. Note that this repair time refers to the time required to repair a failure when it has been detected during a periodic inspection. This repair time is often supposed to be very small in front of the period $t_N$ and then it can be neglected. For instance, a typical value is 8 h while $t_N = \{730\,\text{h}, 2190\,\text{h}, 4380\,\text{h}, \ldots, 87600\,\text{h}\}$ (see part 6 Annex B Table B.1). If it is not the case because e.g. of difficult access to some SIS parts, a more realistic modelling would include an additional phase in the multiphase Markov model to integrate the behavior of the system during the repair process (Dieulle, Bérenguer, & Châtelet, 2000). This point is however not covered in this paper.

### 3.2. PFD expression

As suggested previously in Section 2, the probability of failure on demand should be considered as the average unavailability over a given period of time. The system is periodically inspected and repaired, so the unavailability is periodic and the chosen period of time is obviously $t_N$.

Thus,

$$PFD(t) = \pi(t)f^{\mathrm{T}} \tag{3}$$

$f^{\mathrm{T}}$ is a column vector solely composed of 1 and 0 elements allowing to sum the state probabilities concerned by unavailability.

$$PFD = \frac{1}{t_N}\int_{t_1}^{t_N+t_1} PFD(t)\,\mathrm{d}t \tag{4}$$

- for the phase $[t_1, t_2]$

  $$\int_{t_1}^{t_2} \pi(t)f^{\mathrm{T}}\,\mathrm{d}t = \pi(0)e^{\Lambda t_1}W_1^{IR}\int_{t_1}^{t_2} e^{\Lambda(t-t_1)}\,\mathrm{d}t f^{\mathrm{T}}$$

  with

  $$e^{\Lambda t} = \sum_{k=0}^{n}\frac{\Lambda^k}{k!}t^k \qquad \int_a^b e^{\Lambda t}\mathrm{d}t = \lim_{n\to\infty}\sum_{k=0}^{n}\frac{\Lambda^k}{k!}\left[\frac{t^{k+1}}{k+1}\right]_a^b$$

  $$\int_{t_1}^{t_2} PFD(t)\,\mathrm{d}t = \lim_{n\to\infty}\pi(0)e^{\Lambda t_1}W_1^{IR}\sum_{k=0}^{n}\frac{\Lambda^k}{k!}\frac{(t_2-t_1)^{k+1}}{k+1}f^{\mathrm{T}}$$

- for the phase $[t_2, t_3]$

  $$\int_{t_2}^{t_3} PFD(t)\,\mathrm{d}t = \lim_{n\to\infty}\pi(0)e^{\Lambda t_1}W_1^{IR}e^{\Lambda(t_2-t_1)}W_2^{IR} \times \sum_{k=0}^{n}\frac{\Lambda^k}{k!}\frac{(t_3-t_2)^{k+1}}{k+1}f^{\mathrm{T}}.$$

The relation (4) may be generalized for a system composed of $N$ subsystems with the following one:

$$PFD = \lim_{n\to\infty}\frac{1}{t_N}\pi(0)\sum_{j=1}^{N}\left(\prod_{i=1}^{j}\mathrm{e}^{\Lambda(t_i-t_{i-1})}W_i^{IR}\right)\times\left(\sum_{k=0}^{n}\frac{\Lambda^k}{k!}\frac{(t_{j+1}-t_j)^{k+1}}{k+1}\right)f^{\mathrm{T}}\quad\text{with } t_0=0. \tag{5}$$

Three remarks may be done about the relation (5):

- the average unavailability may be portioned with the vector $f^{\mathrm{T}}$ in order to highlight different Markov state classes due to different kind of failures. For instance those leading to a loss of production, those to a loss of safety, etc. …,
- the system architecture is summarized with $\Lambda$ and $f^{\mathrm{T}}$,
- $W_i^{IR}$ can take into account some maintenance policy imperfections.

### 3.3. Application: 1oo1 architecture

The first and basic SIS proposed in the standard is the 1oo1 architecture. This one is an elementary channel described by the reliability block diagram in Fig. 4. This is a series structure with two *components*; each one stands for a type of failure. The first one is for a dormant failure, the second one for a failure detected by on-line tests. This SIS is functioning if and only if its two components are functioning.

The Markov model for this system between two periodic inspections is represented in Fig. 5 as suggested in Signoret and Dutuit (2006). This model considers dangerous failures with one absorbing state induced by undetected failures (*KO DU*) and one repairable state induced by detected failures (*KO DD*).

The transition rate matrix $\Lambda$ for this model is

$$\Lambda = \begin{pmatrix} -\lambda_D & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Starting with initial conditions $\pi(0) = [1\,0\,0]$ and in order to ensure its safety mission, this SIS is submitted to on-line tests according to an inspection and repair matrix $W^{on}$ such as

$$\mathscr{W}^{on} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and also to periodic inspections with a period time $T$ according to an inspection and repair matrix $W^{p}$ such as

$$\mathscr{W}^{p} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

assuming perfect inspections and repairs.

The chronology of these different inspections is summarized in Fig. 6.

Applying the relation (5), it follows

$$PFD = \lim_{n\to\infty}\frac{1}{T}\pi(0)\left\{\left[\sum_{j=1}^{l-1}\left(\prod_{i=1}^{j}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\right]+\left[\left(\prod_{i=1}^{l-1}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\mathrm{e}^{\Lambda\Delta t}W^{p}\right]\right\}\left(\sum_{k=0}^{n}\frac{\Lambda^k}{k!}\frac{\Delta t^{k+1}}{k+1}\right)f^{\mathrm{T}} \tag{6}$$

with $f^{\mathrm{T}} = [0\,1\,1]$ (see Appendix for details). The above relation (6) seems to be far from the one proposed in the standard (see IEC-61508 part 6) which gives for a 1oo1 system under some assumptions:

$$PFD = \lambda_{DU}\left(\frac{T}{2}+\frac{1}{\mu_{DD}}\right)+\frac{\lambda_{DD}}{\mu_{DD}}. \tag{7}$$

However, as can be seen in Table 3, the PFD results obtained from the relations (6) and (7) are nearly the same with the following data: $\lambda_D = 2.5\times10^{-5}$, $\mu_{DD} = \frac{1}{8}$, $T = 4380\,\mathrm{h}$, $l = 100$, $DC \in \{0\%, 60\%, 90\%\}$.

But, even if this latter relation is certainly ready and easy to use for a reliability practitioner, it does not allow to handle the behavior of this SIS. On the contrary, the


Fig. 4. 1oo1 reliability block diagram.

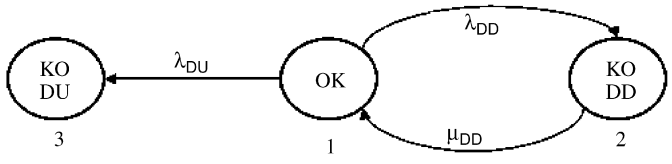


Fig. 5. 1oo1 state diagram. Component level.

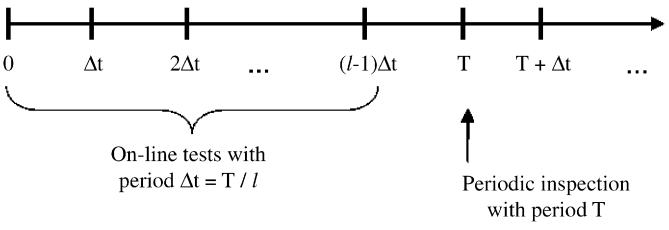


Fig. 6. Inspections chronology of a 1oo1 architecture.

Table 3
1oo1

| DC | IEC (7) | Relation (6) |
|---|---|---|
| 0% | $5.50\times10^{-2}$ | $5.28\times10^{-2}$ |
| 60% | $2.20\times10^{-2}$ | $2.16\times10^{-2}$ |
| 90% | $5.70\times10^{-3}$ | $5.57\times10^{-3}$ |

PFD values according to the relations (6) and (7).

multiphase approach can draw up the shape of the time dependent unavailability with the effect of on-line tests (see Fig. 7), the impact of their frequency $l$ (see Fig. 8) or the impact of their potential imperfection $r$ (see Fig. 9) according to the following matrix

$$\mathscr{W}^{on} = \begin{pmatrix} 1 & 0 & 0 \\ 1-r & r & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In the next sections, two Markov models are suggested for a SIS with two channels and for the second study case of the standard. Without loss of generality, the on-line tests of each subsystem are not considered in order to not overload the analytical expressions for PFD. For instance, this assumption leads the expression (7) of an elementary channel to the following and well-known one:

$$PFD \approx \lambda_D \frac{T}{2}. \quad (8)$$

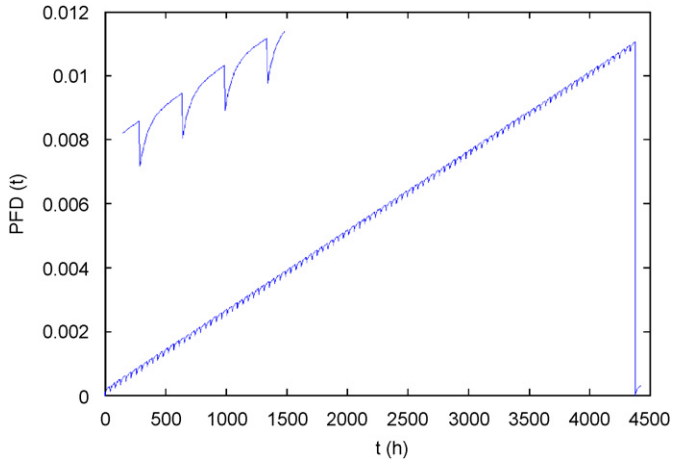


Fig. 7. 1oo1. Time dependent unavailability for $DC = 90\%$ and in the top left a zoom on PFD(t).

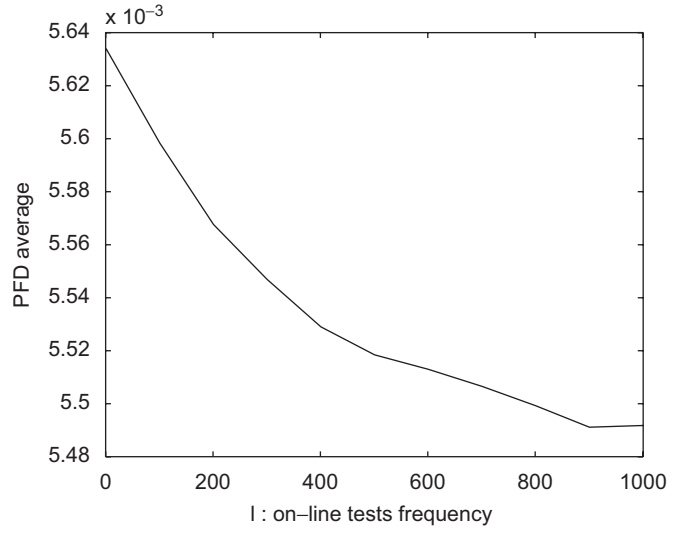


Fig. 8. 1oo1. Impact of the on-line tests frequency $l$ on PFD.

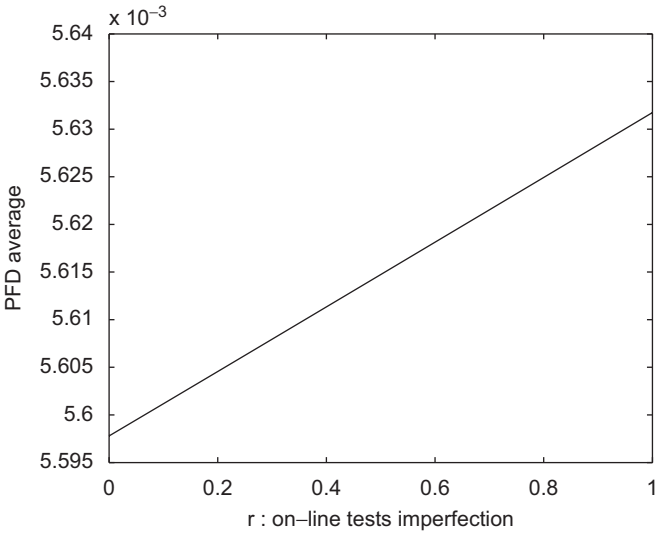


Fig. 9. 1oo1. Impact of the on-line tests imperfection $r$ on PFD.

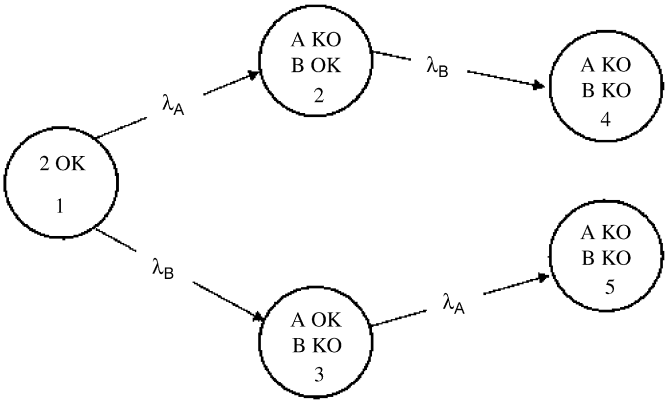


Fig. 10. State diagram of a SIS composed of two channels. Channel level.

### 3.4. Markov model for a SIS with two channels

To consider a safety instrumented system composed of two channels A and B, the Markov model described in Fig. 10 is proposed (Rouvroye & Wiegerinck, 2006). This model enables to study two kind of structures (series and parallel), and then the respective merging rules.

In the case of a parallel structure, the model contains one nominal state (state 1), two degraded states (states 2 and 3) and finally two identical critical states (states 4 and 5); the corresponding vector $f^{\mathrm{T}}$ is [0 0 0 1 1].

In the case of a series structure, the model contains one nominal state (*state 1*) and four critical states (states 2,3,4 and 5); the corresponding vector $f^{\mathrm{T}}$ is [0 1 1 1 1].

Note that this kind of modelling (i.e. without merging states 4 and 5) enables to distinguish which channel fails before the other and then is well adapted to a staggered tests policy. The channel A is supposed to be inspected at time $t_1$ with an inspection and repair matrix $W_1^{IR}$ while the

channel B is inspected at time $t_2$ with an inspection and repair matrix $W_2^{IR}$. Both channels are periodically inspected with the same period $t_2$ and initial conditions $\pi(0) = [1\,0\,0\,0\,0]$.

The redistribution of probabilities after the first test and repair $W_1^{IR}$ is given by

$$\mathscr{W}_1^{IR} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

while the redistribution of probabilities after the second test and repair $W_2^{IR}$ belongs to

$$\mathscr{W}_2^{IR} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

For instance, before the first test and repair if the system belongs to the state 3, it remains in the same one after this inspection because this state is not concerned by the repair of channel A. In the same way, if the system belongs to the state 4 or 5, it leaves this one to state 3 after the inspection of channel A.

Applying the relation (5), the probability of failure on demand for both potential structures becomes

$$PFD = \lim_{n\to\infty} \frac{1}{t_2}\pi(0)\mathrm{e}^{\Lambda t_1} W_1^{IR}\left\{\left(\sum_{i=0}^{n}\frac{\Lambda^i}{i!}\frac{(t_2-t_1)^{i+1}}{i+1}\right) + \mathrm{e}^{\Lambda(t_2-t_1)} W_2^{IR}\left(\sum_{i=0}^{n}\frac{\Lambda^i}{i!}\frac{t_1^{i+1}}{i+1}\right)\right\} f^{\mathrm{T}}. \quad (9)$$

### 3.5. Markov model for the second study case

The Markov model of the second study case (see Fig. 2) proposed in the standard to illustrate the use of merging rules is described in Fig. 11. This model is achieved with the following assumptions in order to reduce its complexity:

- the subsystems A and B compose the channel 1 and are both inspected with an inspection and repair matrix $W_1^{IR}$,
- the subsystems C and D compose the channel 2 and are both inspected with an inspection and repair matrix $W_2^{IR}$,
- the subsystem E composes the last channel 3 and is inspected with an inspection and repair matrix $W_3^{IR}$,
- the common cause failures are not taken into account,
- all channels are periodically inspected.

It is also assumed that the dangerous failures cannot be detected by on-line tests (i.e the diagnostic coverage

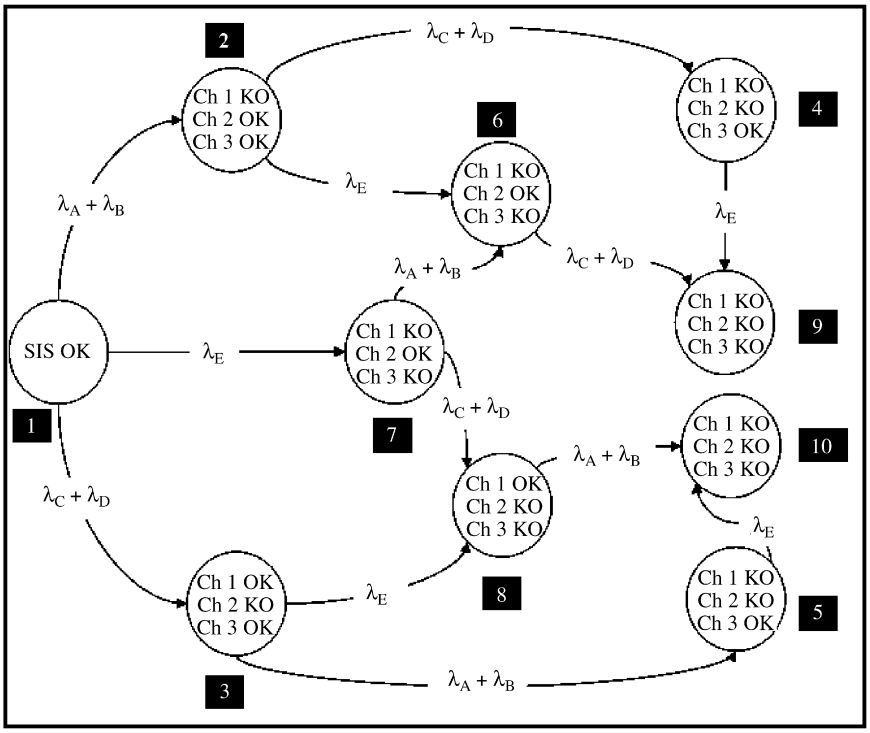


Fig. 11. Study case II. State diagram. Channel level.

$DC = 0\%$) which is a pessimistic case. Moreover, as mentioned in the standard, the safe failures have not the potential to put the SIS in a hazardous or fail-to-function state. For this reason, the failure rates concern only dangerous failures. Finally, the inspections are supposed to be perfect.

The state numbered 1 represents the nominal one where the SIF is available all the time. The states numbered 2 and 3 are degraded ones because some parts are failed but the SIF is nevertheless available while the states numbered from 4 to 10 are dangerous failed ones.

The inspection and repair matrices $W_1^{IR}$, $W_2^{IR}$ and $W_3^{IR}$ are not described here but are based on the same principle as the one used in Section 3.4. Finally, according to the inspections chronology described in Fig. 3, if the channel 1 is inspected at $t_1$, the channel 2 at $t_2$ and channel 3 at $t_3$ the relation (5) gives for PFD

$$PFD = \lim_{n\to\infty} \frac{1}{t_3}\pi(0)\mathrm{e}^{\Lambda t_1} W_1^{IR}\left\{\left(\sum_{i=0}^{n}\frac{\Lambda^i}{i!}\frac{(t_2-t_1)^{i+1}}{i+1}\right) + \mathrm{e}^{\Lambda(t_2-t_1)} W_2^{IR}\left[\left(\sum_{i=0}^{n}\frac{\Lambda^i}{i!}\frac{(t_3-t_2)^{i+1}}{i+1}\right) + \mathrm{e}^{\Lambda(t_3-t_2)} W_3^{IR}\left(\sum_{i=0}^{n}\frac{\Lambda^i}{i!}\frac{t_1^{i+1}}{i+1}\right)\right]\right\} f^{\mathrm{T}}. \quad (10)$$

## 4. Numerical results

The previous section has shown that a multiphase Markovian approach enables to handle the probabilistic behavior of a SIS even if it leads to complex analytical expressions for PFD. In the present section, the models suggested for a SIS composed of two channels and the one for the second study case of the standard are tested to consider the possible SIL values of each system. The obtained results are compared with the expected values given in the standard by both series and parallel merging rules.

### 4.1. Data

All numerical tests are done with Matlab and a period of one year 8760 h that is representative of values used in the standard. The series expansion of matrix exponentials is done with a 20th order allowing a numerical convergence of results.

To use the proposed models with simulations, the SIL value of each safety subsystem needs to be chosen. As described in Section 2, a SIL level summarizes a bounded interval of the average unavailability. Then, according to Table 1, $SIL_1^-$ corresponds to the lower bound ($PFD = 0.01$) and $SIL_1^+$ to the higher bound ($PFD < 0.1$) and so on for the other SILs. Starting from these values, the relation (8) enables to approximate the corresponding failure rates for basic systems . For instance, the dangerous failure rate of a basic SIS with a $SIL_1^-$ periodically inspected every $8760h$ is nearly $2.28 \times 10^{-6}$. The obtained approximated failure rates are used to construct the transition rate matrix $\Lambda$.

### 4.2. SIS with two channels

The channel B is inspected every $t_2 = 8760$ h while the channel A is inspected with a date $t_1$ varying from 24 to 8760 h. Two types of configuration are studied with the SIL values of Table 4. The first configuration (1st conf.) stands for the channels A and B with a safety integrity level of $SIL_1$ while the second configuration (2nd conf.) stands for a channel A of $SIL_1$ and a channel B of $SIL_2$.

For each configuration, three combinations of SIL values are tested on two architectures (series and parallel structures) leading finally to realize 12 numerical tests.

Table 4
SIL values of channels A and B for two configurations

| | | | |
|---|---|---|---|
| 1st conf. $SIL_1$ and $SIL_1$ | | | |
| $SIL_A$ | $SIL_1^-$ | $SIL_1^-$ | $SIL_1^+$ |
| $SIL_B$ | $SIL_1^-$ | $SIL_1^+$ | $SIL_1^+$ |
| 2nd conf. $SIL_1$ and $SIL_2$ | | | |
| $SIL_A$ | $SIL_1^+$ | $SIL_1^+$ | $SIL_1^-$ |
| $SIL_B$ | $SIL_2^+$ | $SIL_2^-$ | $SIL_2^+$ |

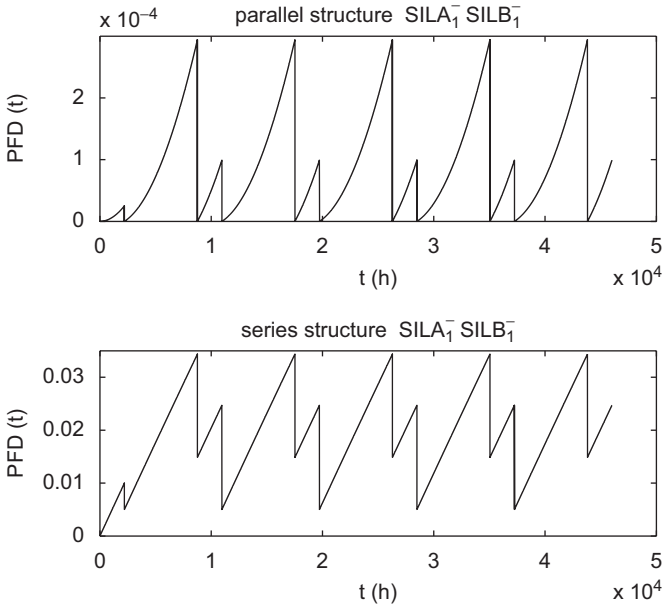


Fig. 12. Example of the time dependent unavailability of a SIS composed of two channels A and B for series and parallel structures. Each channel has a $SIL_1^-$ value. A is inspected at $t_1 = 2200$ h while B is inspected at $t_2 = 8760$ h.

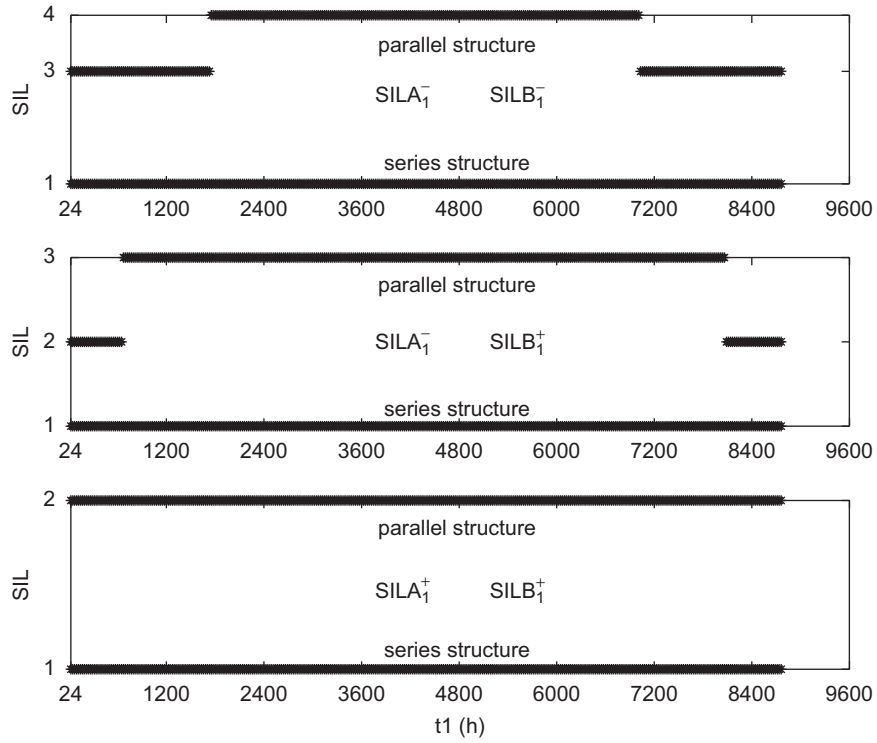


Fig. 13. SIS composed of two channels A and B (first configuration). Evolution of the SIL value versus the inspection date $t_1$ of channel A. Series and Parallel structures.

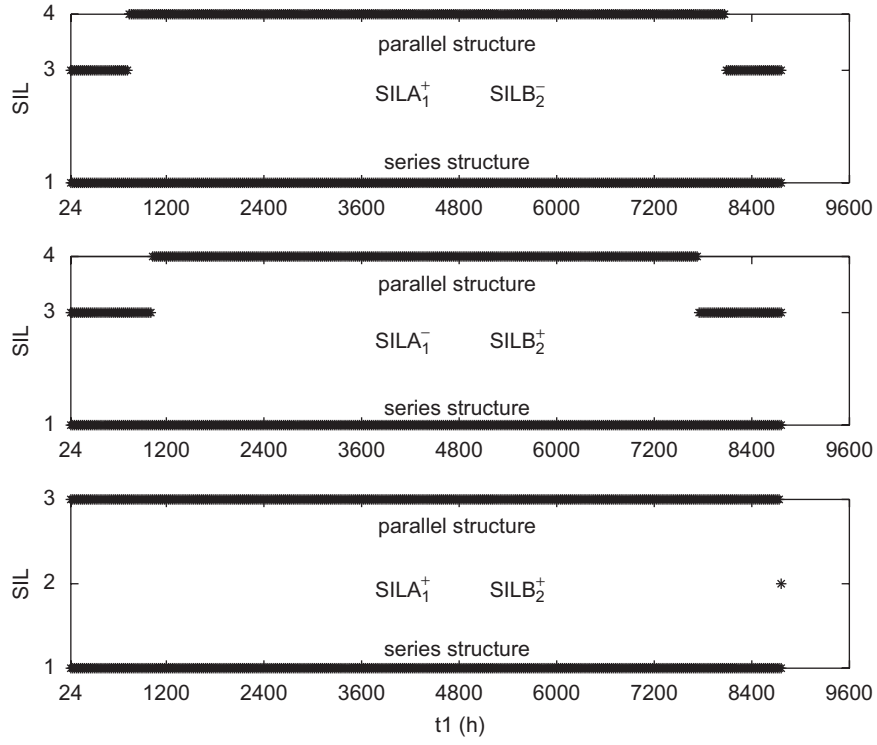


Fig. 14. SIS composed of two channels A and B (second configuration). Evolution of the SIL value versus the inspection date $t_1$ of channel A. Series and Parallel structures.

For each configuration, the time dependent unavailability is implemented according to Eq. (3) as can be seen in Fig. 12. The probability of failure on demand is implemented according to the relation (9) which gives the results in Fig. 13 for the first configuration and those for the second one in Fig. 14.

From these results, we can draw the following comments:

- whatever the type of configuration, the kind of SIL values and the value of the inspection date $t_1$ are, the merging rule for a series structure composed of two subsystems is always verified. That is to say the equivalent SIL for the complete system is equal to the lowest of both. For both configurations, the expected SIL level from the series merging rule is SIL1 and this result is verified with the multiphase approach,
- on the other hand, it can be seen that the merging rule for a parallel structure is not always verified. Normally, according to the standard the equivalent SIL is SIL2 for the first configuration and SIL3 for the second one. These SILs seem to be reached when the SIL values of the subsystems are close to the higher bound $SIL^+$ except for one point which presents a SIL2 (see the third subplot in Fig. 14). But in many cases the maximum expected SIL value is higher than the one mentioned in the standard. On the tested example, the parallel merging rule gives conservative results.

### 4.3. Standard second study case

According to the Markov model suggested in Section 3.5, the subsystems A and B compose the channel 1 ($Ch_1$), the subsystems C and D the channel 2 ($Ch_2$) and finally the subsystem E the channel 3 ($Ch_3$). Two types of configuration are studied with the SIL values of Table 5.

These configurations are tested with the different inspection chronologies of Table 6 based upon the dates $t_1$, $t_2$ and $t_3$ which implies a simple circular permutation of the matrices $W_i^{IR}$ in the relation (10). The dates $t_1$ and $t_2$ are varying from 24 to 8760 h while $t_3 = 8760$ h regarding the following inequality

$t_1 \leqslant t_2 \leqslant t_3$,

An example of PFD evolution is described in Fig. 15 for the second configuration and the first case. The plots of Figs. 16 and 17 summarize the possible SIL values of the whole system for each configuration as a function of $t_1$ and $t_2$.

Table 5
Study case II

| SIS | 1st conf. | 2nd conf. |
|---|---|---|
| $SIS_A$ | $SIL_3^-$ | $SIL_3^+$ |
| $SIS_B$ | $SIL_2^-$ | $SIL_2^+$ |
| $SIS_C$ | $SIL_2^-$ | $SIL_2^+$ |
| $SIS_D$ | $SIL_1^-$ | $SIL_1^+$ |
| $SIS_E$ | $SIL_2^-$ | $SIL_2^+$ |

SIL values of each subsystem and for two configurations.

Table 6
Study case II

| Case | Inspection dates | | |
|---|---|---|---|
| | $t_1$ | $t_2$ | $t_3$ |
| 1 | $Ch_1$ | $Ch_2$ | $Ch_3$ |
| 2 | $Ch_1$ | $Ch_3$ | $Ch_2$ |
| 3 | $Ch_2$ | $Ch_1$ | $Ch_3$ |
| 4 | $Ch_2$ | $Ch_3$ | $Ch_1$ |
| 5 | $Ch_3$ | $Ch_1$ | $Ch_2$ |
| 6 | $Ch_3$ | $Ch_2$ | $Ch_1$ |

Inspection scenarios for each channel $Ch_i$.

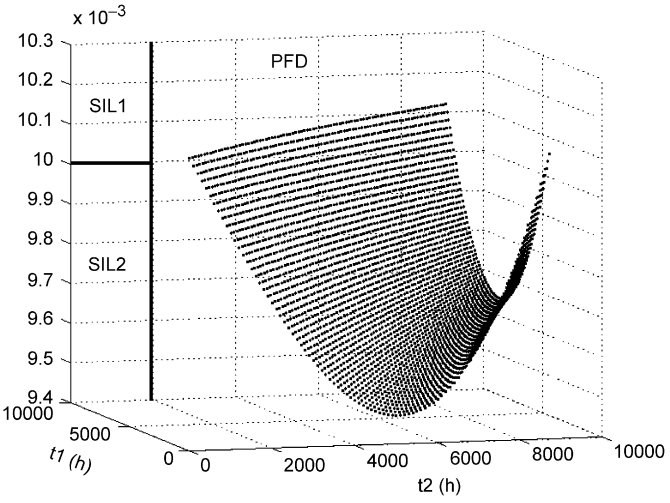


Fig. 15. Study case II. PFD map for the 2nd configuration—case 1.

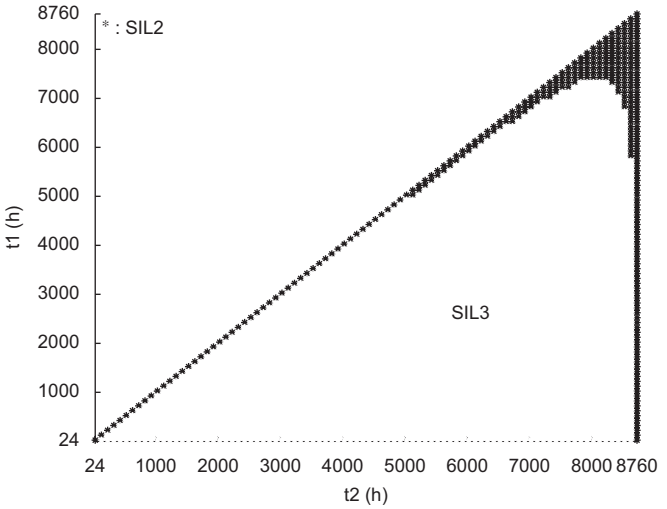


Fig. 16. Study case II. SIL map for the 1st configuration - cases 2,4.

From these results, we can draw the following comments:

- for this study case, the expected SIL is SIL2 (see Section 2.3). The numerical results show that this level is the

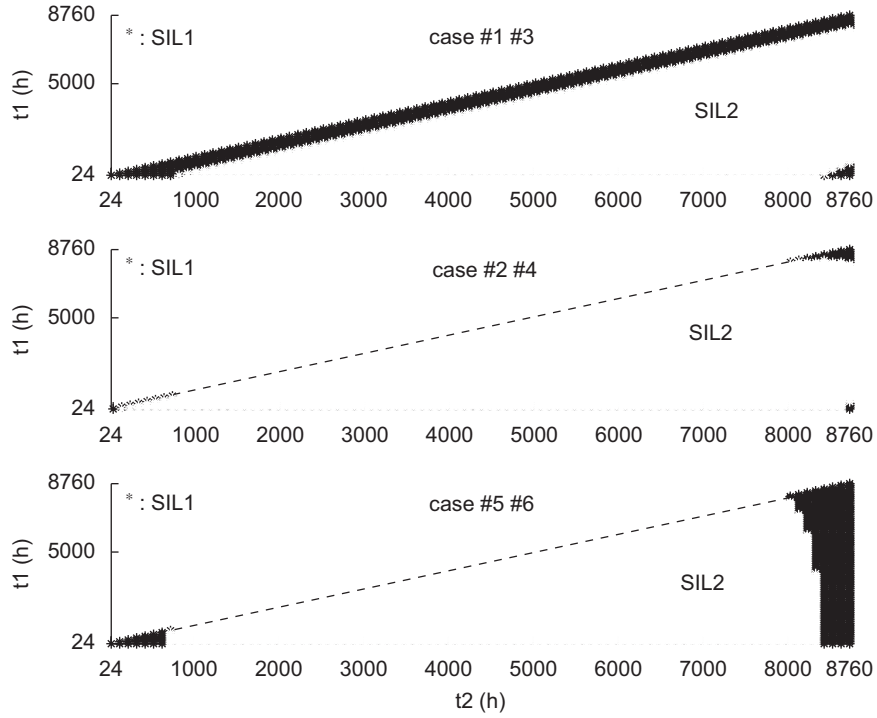


Fig. 17. Study case II. SIL map for the 2nd configuration.

lowest one that may be obtained for the first configuration. Moreover as can be seen in Fig. 16, in most cases a SIL3 is obtained instead of a SIL2 as expected,

- on the other hand, it can be seen for the second configuration in Fig. 17 that the expected SIL (SIL2) is here the highest one obtainable. This result (SIL2) is observed for most of values of the couple $(t_1, t_2)$. However, in some cases the resulting SIL value is SIL1 whatever the inspection scenario is. For this configuration, the merging rules do not give conservative results which obviously can be a problem in a safety point of view.

## 5. Conclusion

This paper has shown that the method based upon both series and parallel merging rules suggested by the IEC61508 standard is really easy to apply but yet it does not lie on a robust approach. A multiphase Markovian study has highlighted that these merging rules do not take into account (i) the inspection dates and (ii) the value of the corresponding PFD $(SIL_i^+, SIL_i^-)$ of the different safety subsystems. The SIL values expected from the standard are in some cases higher than the exact results obtained from the proposed Markovian approach. These rules give conservative results in many cases but because some scenarios which present a weakness of security exist, they have to remain and to be considered as just informative. They can be used to give a first impression of the safety integrity of an entire system composed of different subsystems.

In many ways, an in-depth study of the safety integrity of a SIS is more suitable. Thus, the suggested Markovian approach may be a way to reach this goal by allowing the generalization of the PFD expression but limited to a reasonably sized system where only the dangerous failures are concerned. If systematic software failures, human errors or common cause failures (Lundteigen & Rausand, 2007b) are to be studied, then additional models need to be designed. To consider these failures a first approach may be the PDS method (Hokstad & Corneliussen, 2002).

Finally, as mentioned in Kosmowski and Sliwinski (2005), this paper confirms that the standard evaluating method is in some cases too rough and needs to be refined if one wants to avoid inconsistency or non-conservative results.

## Appendix

The system considered here is a 1oo1 SIS submitted to on-line tests and periodic inspections described in Fig. 6. These tests and inspections have to be studied as phases in the aim to evaluate their impact before formalizing PFD. Then,

- for the phase $[0, \Delta t]$:

$$\pi(t) = \pi(0)e^{\lambda t};$$

- for the phase $[\Delta t, 2\Delta t]$:

$$\pi(t) = \pi(\Delta t^+)e^{\lambda(t-\Delta t)},$$

$$\pi(\Delta t^{+}) = \pi(0)\mathrm{e}^{\Lambda\Delta t}W^{on},$$
$$\pi(t) = \pi(0)\mathrm{e}^{\Lambda\Delta t}W^{on}\mathrm{e}^{\Lambda(t-\Delta t)};$$

- for the phase $[2\Delta t, 3\Delta t]$:

$$\pi(t) = \pi(0)\mathrm{e}^{\Lambda\Delta t}W^{on}\mathrm{e}^{\Lambda\Delta t}W^{on}\mathrm{e}^{\Lambda(t-2\Delta t)};$$

- and so on until the phase $[(l-1)\Delta t, l\Delta t]$, i.e. $[(l-1)\Delta t, T]$ concerning the impact of on-line tests:

$$\pi(t) = \pi(0)\left(\prod_{i=1}^{l-1}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\mathrm{e}^{\Lambda(t-(l-1)\Delta t)};$$

- finally the phase $[l\Delta t, (l+1)\Delta t]$, i.e. $[T, T+\Delta t]$ concerning the impact of the periodic inspection:

$$\pi(t) = \pi(0)\left(\prod_{i=1}^{l-1}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\mathrm{e}^{\Lambda\Delta t}W^{p}\mathrm{e}^{\Lambda(t-l\Delta t)}.$$

With

$$PFD(t) = \pi(t)f^{\mathrm{T}},$$

$$PFD = \frac{1}{T}\int_{\Delta t}^{T+\Delta t} PFD(t)\,\mathrm{d}t.$$

Whatever the phase $m$ is

$$\int_{m\Delta t}^{(m+1)\Delta t}\mathrm{e}^{\Lambda(t-m\Delta t)}\,\mathrm{d}t = \lim_{n\to\infty}\sum_{k=0}^{n}\frac{\Lambda^{k}}{k!}\frac{\Delta t^{k+1}}{k+1}$$

and finally, summing all the integrals of the different phases from $\Delta t$ to $T+\Delta t$, the PFD relation for a 1oo1 system becomes

$$PFD = \lim_{n\to\infty}\frac{1}{T}\pi(0)\left\{\left[\sum_{j=1}^{l-1}\left(\prod_{i=1}^{j}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\right] + \left[\left(\prod_{i=1}^{l-1}\mathrm{e}^{\Lambda\Delta t}W^{on}\right)\mathrm{e}^{\Lambda\Delta t}W^{p}\right]\right\}\left(\sum_{k=0}^{n}\frac{\Lambda^{k}}{k!}\frac{\Delta t^{k+1}}{k+1}\right)f^{\mathrm{T}}.$$

## References


Becker, G., Camarinopoulos, L., & Ohlmeyer, W. (1994). Discontinuities in homogeneous markov processes and their use in modelling technical systems under inspections. *Microlectronics Reliability*, *34*(5), 771–788.

Bondavalli, A., Mura, I., Chiaradonna, S., Filippini, R., Poli, S., & Sandrini, F. (2000). DEEM: A tool for the dependability modeling and evaluation of multiple phased systems. *Proceedings of international conference on dependable systems and networks*, *DSN 2000* (pp. 231–236). Los Alamtos, CA, USA: IEEE Computer Society Press.

Bukowski, J. (2001). Modeling and analysing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Transactions on Reliability*, *50*(3), 321–329.

Bukowski, J., & Goble, W. (1995). Using markov models for safety analysis of programmable electronic systems. *ISA Transactions*, *34*, 193–198.

Bukowski, J., Rouvroye, J., & Goble, W. (2002). What is pfdavg? Available on the ⟨www.exida.com⟩ free article web page.

Châtelet, E., Bérenguer, C., & Grall, A. (1997). Reliability evaluation of systems subject to partial renewals for preventive maintenance. In C. Guedes Soares (Ed.), *European conference on safety and reliability—ESREL'97*, Lisbon, Portugal (vol. 3, pp. 1767–1774). ISBN 0-08-042835-5.

Dieulle, L., Bérenguer, C., & Châtelet, E. (2000). Evaluation of preventive maintenance policies using multiphased Markov models. In M. Nikulin, & N. Limnios (Eds.), *Proceedings of second international conference on mathematical methods in reliability—methodology, practice and inference*, Bordeaux, France (pp. 343–346), July 4–7, 2000.

Dutuit, Y., Châtelet, E., Signoret, J.-P., & Thomas, P. (1997). Dependability modelling and evaluation by using stochastic Petri nets: Application to two test cases. *Reliability Engineering and System Safety*, *55*(2), 117–124.

Hokstad, P., & Corneliussen, K. (2002). *PDS data handbook*, 2002 Edition. Reliability data for safety instrumented systems SINTEF. ISBN: 82-14-02707-1

IEC61508 (March 2002). *IEC61508 Electric/Electronic/Programmable Electronic safety-related systems, parts 1–7*. Technical report, International Electrotechnical Commission.

IEC61511 (January 2003). *IEC61511 safety instrumented systems for the process industry sector, parts 1–3*. Technical report, International Electrotechnical Commission.

Kosmowski, K. T., & Sliwinski, M. (2005). Methodology for functional safety assessment. In K. Kolowrocki (Ed.), *European conference on safety and reliability—ESREL'05 Gdynia-Sopot-Gdansk*, Poland (vol. 2, pp. 1173–1180). ISBN 0-415-38340-4.

Langeron, Y., Barros, A., Grall, A., & Bérenguer, C. (2007). Safe failures impact on safety instrumented systems. In T. Aven & J. E. Vinnem (Eds.) *European conference on safety and reliability—ESREL'07*, Stavanger, Norway (vol. 1, pp. 641–648). ISBN 978-0-415-44786-7.

Lindqvist, B., & Amundrustad, H. (1998). Markov models for periodically tested components. In S. Lydersen, G. K. Hansen, & H. A. Sandtorv (Eds.), *European conference on safety and reliability—ESREL'98*, Trondheim, Norway (vol. 1, pp. 191–197). ISBN 90 5410 966 1.

Lundteigen, M., & Rausand, M. (2006). Assessment of hardware safety integrity requirements. *30th ESReDA Seminar*, Trondheim, Norway (pp. 185–198). June 7–8, 2006. ISBN 978-92-79-06574-3.

Lundteigen, M., & Rausand, M. (2007a). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering and System Safety*, *Available online 2 August 2007*, doi:10.1016/j.ress.2007.07.004.

Lundteigen, M., & Rausand, M. (2007b). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, *20*(3), 218–229.

Marszal, E. M., Fuller, B. A., & Shah, J. N. (1999). Comparison of safety integrity level selection methods and utilization of risk based approaches. *Process Safety Progress*, *18*(4), 189–194.

Rausand, M., & Høyland, A. (2004). *System reliability theory—models statistical methods and applications* (Second ed.). NY: Wiley series.

Rouvroye, J., & van den Bliek, E. (2002). Comparing safety analysis techniques. *Reliability Engineering and System Safety*, *75*(3), 289–294.

Rouvroye, J. L., & Wiegerinck, J. A. (2006). Minimizing costs while meeting safety requirements: Modeling deterministic staggered tests using standard Markov models for SIL calculations. *ISA Transactions*, *45*(4), 611–621.

Schäbe, H. (2003). Apportionment of safety integrity levels in complex electronically controlled systems. In Bedford & van Gelder (Eds.), *European conference on safety and reliability—ESREL'03*, Maastricht, The Netherlands (pp. 1395–1400). ISBN 90-5809-551-7.

Signoret, J.-P., & Dutuit, Y. (2006). An attempt to better understand and to better apply some of the recommendations of IEC 61508 standard. *30th ESReDA Seminar*, Trondheim, Norway (pp. 1–16), June 7–8, 2006. ISBN 978-92-79-06574-3.

Zhang, T., Long, W., & Sato, Y. (2003). Availability of systems with self-diagnostic components—applying Markov model to IEC 61508-6. *Reliability Engineering and System Safety*, *80*(2), 133–141.