New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems

F Innal[1], Y Dutuit[2]*, A Rauzy[3], and **J-P Signoret[4]**
[1]Université de Batna, Batna, Algeria
[2]IMS/LAPS, Université Bordeaux I, Talence, France
[3]DASSAULT Systèmes, Suresnes, France
[4]TOTAL/CSTJF, Pau, France

The manuscript was received on 14 September 2009 and was accepted after revision for publication on 3 December 2009.

DOI: 10.1243/1748006XJRR278

Abstract: The aim of this paper is to give a new insight into some fundamental concepts of the IEC 61508 standard. First, low and high or continuous demand modes of operation of safety instrumented systems are examined by analysing their official definitions given in the IEC 61508 and IEC 61511 standards. In this context, the paper proposes a new criterion for distinguishing these two modes of operation. A study allowing the determination of accident frequency is also presented, where the system under study consists of one element under control and its associated safety instrumented system. Second, the relationship between the average probabilities of failure on demand and the risk reduction factor is studied. It is shown that the commonly used approach (the standard approach) may lead to an optimistic value for the risk reduction factor. Finally, the paper clarifies the nature of the probability of failure per hour of a safety instrumented system and proposes different ways to compute this in the general case, based on fault tree, Markov model, and Petri nets approaches.

Keywords: IEC 61508 standard, safety instrumented system, probability of failure per hour, fault tree, piecewise Markovian models, Petri nets with predicates

1 INTRODUCTION

Risk management approaches are aimed primarily at reducing the current risk, generated by a given application, to an acceptable or tolerable level and to maintain that level over time. This reduction is often achieved by the interposition of successive layers of protection between the hazard source (an industrial process, for example) and potential targets such as mankind, property, and the environment. The typology of these layers covers a wide variety and is increasingly supplemented by an extra layer, known as the safety instrumented system (SIS). A SIS has the function to detect the occurrence of a dangerous situation that could lead to an accident and then to implement a whole set of reactions necessary to the setting in safety of the monitored system, and this to be achieved within a specified time.

These SISs have sparked (and continue to arouse) growing interest from their effective or potential users and, of course, from equipment manufacturers. Their importance within these different communities lies in the different standards relating to them, published over the last few years, whether of general application, such as IEC 61508 [**1**], or sector-based application, such as IEC 61511 [**2**] for process industries. One of the particular characteristics of the IEC 61508 standard is that it uses a global safety life cycle model as a technical framework to process systematically the activities to be carried out, so as to ensure the required performance level (qualitative and quantitative) of safety functions that the SIS must implement to meet a given safety target (tolerable risk). These activities range from the initial safety specifications phase, based on a risk analysis approach, to the decommissioning of the SIS, and

**Corresponding author: IMS/LAPS, University of Bordeaux, 351, cours de la Libération, Talence 33405, France.*
email: yves.dutuit@iut.u-bordeaux1.fr

include design, installation, operation, and maintenance [**1**]. The performance of the SIS with respect to its assigned safety function is defined in terms of safety integrity levels (SILs). According to the IEC 61508 standard, the SIL is closely linked to the operating modes of the SIS: low demand and high or continuous demand modes of operation. It then defines four safety integrity levels which are identified with the average probability of failure on demand of the SIS (PFD_{avg}) for the low demand mode, and with its probability of dangerous failure per hour (PFH) for the high or continuous demand mode of operation. These concepts will be detailed in the current paper.

Standard IEC 61508 provides a formalized and rigorous approach to determining the required SIL levels, and it is interesting from this organizational point of view, but there are significant disadvantages regarding its applicability. These disadvantages arise particularly from the sometimes vague and ambiguous character of the statement of certain concepts and major definitions in this standard. The current paper aims to clarify the situation by presenting some innovative (in the authors' opinion) contributions, which were initially presented in the first-named author's doctoral thesis [**3**].

The remainder of this paper is organized as follows. Section 2 presents a study of the two modes of operation of a SIS and introduces a new criterion that helps to distinguish them without ambiguity. This has never been previously achieved, to the authors' knowledge. It also proposes a generic model involving both low and high or continuous demand modes of operation. This model is used to illustrate the relationship between the accident frequency of a system controlled by a SIS and the PFD_{avg} or the PFH of the SIS. Moreover, this model shows, for the first time in a scientific journal, that any given SIS can lead to an accident through two different failure modes, respectively, related to each of its two modes of operation. Section 3 describes the relation between the risk reduction factor (RRF) and the PFD_{avg} and, once again for the first time in a scientific journal, shows that the whole RRF obtained with the combination of several layers of protection is not equal to the product of the respective RRFs. Section 4 is devoted to the notion of PFH. More precisely, its nature is clearly defined and three procedures for its calculation are described and applied to a 'one out of two' (1oo2) system. Finally, section 5 offers a summary and the conclusion of this work.

2 THE TWO MODES OF OPERATION OF A SIS

According to the IEC 61508 standard, the demand on a SIS to achieve its implemented function can be either low (low demand mode) or high or continuous (high or continuous demand mode). These two modes of operation, as defined in the normative documents, are quite ambiguous and imprecise. To help to remove this ambiguity, this section primarily focuses on the meaning of these two modes of operation. First, the definitions given in the reference documents, IEC 61508 and IEC 61511 standards, should be recalled in order to open the debate.

2.1 Official definitions

Project on IEC 61508 standard [**4**]:

(a) *low demand mode* corresponds to the case where the demand frequency is lower than the proof-test frequency;
(b) *high or continuous mode* corresponds to the case where the demand frequency is significantly higher than the proof-test frequency.

Current IEC 61508 standard [**1**]:

(a) *low demand mode* is where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-tests frequency;
(b) *high or continuous demand mode* is where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-tests frequency.

Current IEC 61511 standard [**2**]:

(a) *demand mode* is where a specified action (for example, closing a valve) is taken in response to process conditions or other demands; in the event of a dangerous failure of the safety instrumented function a potential hazard only occurs when there is a failure in the process or the BPCS (basic process control system);
(b) *continuous mode* is where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it.

2.2 Comments

In relation to the definitions given in the provisional version, one can remark on the disymmetrical nature of their duality: the expression (simply) 'less than' is used for the low demand mode, while the expression 'significantly greater' appears in the definition relating to high or continuous demand mode. Furthermore, how should the adverb 'significantly' be interpreted? Does it indicate a factor of 2, 3, 5, 10, or more ? Finally, is the reference to the frequency of the proof tests sufficient or relevant to be able to discriminate the two modes of operation in all cases? In fact, a SIS assuring a safety function is made up of at

least three subassemblies (sensors, logic unit, actuators) characterized by proof-test frequencies that are often different. In these conditions, what is the frequency of the proof tests to be considered?

By comparison, in the current version of the IEC 61508 standard, the conditions affecting the frequency of the demand, which define the two modes of operation, are clearly expressed in dual forms of each other. This is an advantage from the point of view of definition uniformity. The other side of the coin is that these two definitions refer to a threshold value (annual demand frequency equal to 1) and a ratio of frequencies equal to 2, given without any justification. What is the origin of this and do they really have universal value; in other words are they valuable for all cases that we are likely to meet?

The IEC 61511 standard, on the other hand, sets the occurrence conditions for a potential hazard (accident) to such an extent that it defines the modes of operation. It stands out, however, that the low demand mode is characterized by the fact that an accident can occur if a demand emanating from the process or the BPCS appears while the SIS is already unavailable, whereas for the high or continuous demand mode, the occurrence of an accident can result from the SIS failure. The point of view expressed in this standard is interesting, because it brings to light that the characteristic of the SIS involved in the demand mode (low demand) is its availability, whereas its reliability is linked to the continuous mode.

The review of the different definitions for the low demand and high or continuous demand modes did not provide a satisfactory answer to the question raised: is there a clear definition for each of these two modes, based on a specific and discriminating criterion? An attempt to answer this question is presented in the next subsection.

2.3 A discriminating criterion

As the demand is omnipresent in the three definitions given above, it is sensible to integrate it into the behavioural model for the studied SIS, as is done by several authors [**4**, **5**]. They all chose a Markov model. The same approach is used in the present paper, although more explicitly. In fact, each subassembly of a SIS can undergo undetectable failures, which can only therefore be discovered and repaired during proof tests following their occurrence (hidden failures). The behaviour of this type of periodically tested system, monitored over several test periods, cannot be correctly reported by a classic Markov model. This requires the use of a multiphase (piecewise) Markov model [**5**, **6**], which can be approximated using a classical Markov model by calculating return rates from its partial or total failure states [**3**].

The current authors' demonstration is based on a generic model of a SIS equipped with the simplest of architectures, the 1oo1 architecture. The corresponding multiphase Markov model and its classical approximation are represented in Fig. 1. The classical Markov model of the SIS incorporating the demand of the controlled process is depicted in Fig. 2. The unavailability states KO(DU) and KO(DD) from the model in Fig. 1 have been added (state 3) in Fig. 2.

1. Each state of the model in Fig. 2 is identified by three labels. The upper label indicates the state of the SIS: OK stands for working state and KO stands for failed state. The median label indicates the state of the equipment under control (EUC). The nominal state is denoted by OK. The shutdown state is denoted by STOP. Finally, the accident state is denoted by ACCIDENT. The lower label is just an index of the state.
2. The parameter λ_d denotes the demand rate, while λ_D is the sum of the dangerous failures rates which are detected (λ_{DD}) and undetected (λ_{DU}).

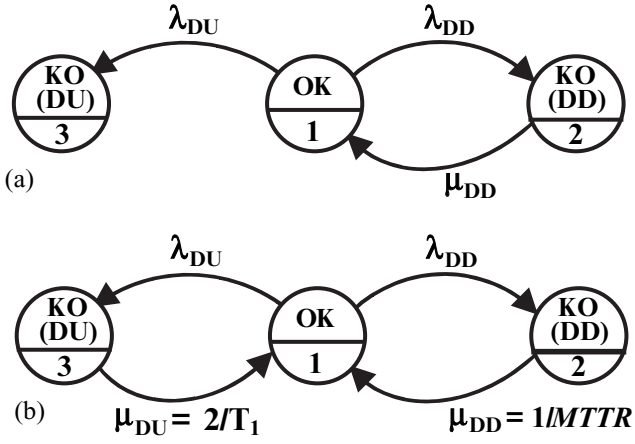


Fig. 1 (a) Multiphase Markov model of a SIS with 1oo1 architecture; (b) its 'approximated' Markov model

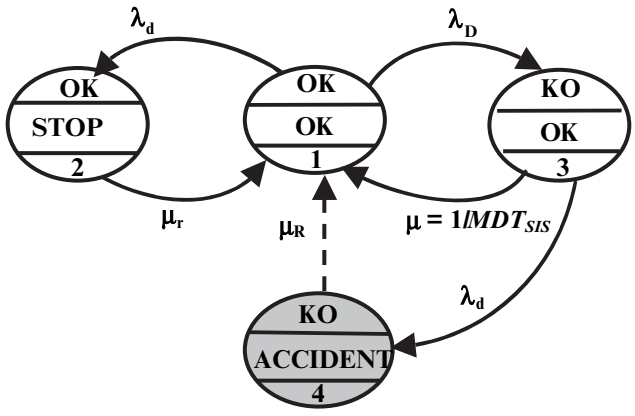


Fig. 2 'Approximated' Markov model for a SIS (1oo1) integrating the demand

3. The value μ_r is the inverse of the mean time required to restart the EUC after it has been stopped (shutdown) by the SIS reacting to a demand, while μ is the inverse of the mean time of SIS unavailability (MDT_{SIS}), following a detected or undetected failure.
4. The value allocated to μ_R is very large (immediate transition) to mask the time spent after an accident (state 4), see reference [**3**] for further explanation. It refers to the so-called renewal transition [**7**].

It is shown in reference [**3**] that the average behaviour, over an important observation period, of a given system modelled by a multiphase Markov graph can be approximated in a valid way by its asymptotic behaviour resulting from the corresponding approached Markov model, for which the return rates from the failure states have already been determined. This makes it possible to compute the average value of the accident frequency named w_{acc}

$$w_{acc} = p_3(\infty) \cdot \lambda_d = p_1(\infty) \cdot \frac{\lambda_D}{\lambda_d + \mu} \cdot \lambda_d \qquad (1)$$

$p_1(\infty)\lambda_D$ is the average value w_{SIS} of the failure frequency of the SIS. Therefore, the following equality holds

$$w_{acc} = \frac{\lambda_d}{(\lambda_d + \mu)} \cdot w_{SIS} \qquad (2)$$

Two extreme configurations can be deduced from equation (2) and are described below.

The first extreme configuration can be outlined as follows. If $\lambda_d \gg \mu$, then it is the continuous mode of operation. In this case, equation (2) reduces to

$$w_{acc} = w_{SIS} \qquad (3)$$

The above equality indicates that an accident occurs as soon as the SIS fails. This complies with the statement of the condition given in the IEC 61511-1 standard. Moreover, by considering λ_d as an approximation of the demand frequency w_d, the condition ($\lambda_d \gg \mu$) can be rewritten as follows

$$w_d = \frac{1}{T_d} \gg \mu = \frac{1}{MDT_{SIS}} \qquad (4)$$

where T_d (named T_1 in the IEC 61508) is the mean duration between two successive demands.

For the 1oo1 architecture the MDT, owing to both detected (λ_{DD}) and undetected (λ_{DD}) dangerous failures, is expressed as follows [**1**, **3**]

$$MDT_{SIS} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR \qquad (5)$$

Nevertheless, detected dangerous failures can be easily monitored. Consequently, in practice, the occurrence of the accident is largely due to undetected dangerous failures. Detected dangerous failures are then considered as not being actually dangerous, thereby restricting λ_D to λ_{DU}. Hence, the equality (5) is reduced to

$$MDT_{SIS} \approx \frac{T_1}{2} + MTTR \approx \frac{T_1}{2} \qquad (6)$$

Jointly taking into account equations (4) and (6) leads to

$$w_d \gg \frac{2}{T_1} = 2 \cdot w_{PT} \qquad (7)$$

where w_{PT} denotes the frequency of the proof tests.

Therefore, for the specific case of the 1oo1 architecture, the condition defining the high or continuous demand mode of operation is found, which is given in the current IEC 61508 standard. The origin of factor 2 which is evoked there, and which is also mentioned in note 2 attached to the definition given in Part 1 of the IEC 61511 standard, can also be understood.

However, it is important to remember that equation (7) has only been established for the 1oo1 architecture. For the 1oo2 architecture, for example, factor 2 is replaced by factor 3 ($T_1/3$ is approximately the mean downtime related to two consecutive undetected failures). Furthermore, if the term T_1 is also found in the 1oo2 architecture and all the other *KooN* configurations, this is for the simple reason that all the components of this kind of architecture are identical and are tested simultaneously on the same dates. This is not the case for components belonging to the different subsystems making up a SIS. As the explicit reference to factor 2 and a unique proof-test period T_1 are only valid for the 1oo1 architecture, they should not figure in the definition of the continuous demand and the low demand modes of operation.

The second extreme configuration is now described. If $\lambda_d \ll \mu$, then it is the low demand mode of operation. In this case, equation (1) gives

$$w_{acc} = p_3(\infty)\,\lambda_d \approx PFD_{avg}\lambda_d \approx PFD_{avg}\, w_d \qquad (8)$$

because it is now accepted and recognized that the PFD_{avg} corresponds to the average value of the SIS unavailability, which can be approximated by its asymptotic unavailability $p_3(\infty)$.

The above considerations show that the expected criterion suitable for distinguishing between the two, or even three, modes of operation regardless of the SIS architecture being studied is obtained by

comparing the product $w_d \times MDT_{SIS}$ with the unity (see Table 1).

2.4 A generic model for the accident frequency

Low and high demand modes of operation are considered separately in the IEC 61508 standard. Furthermore, the EUC is put instantaneously into a safe state after the occurrence of a demand, if the SIS is available. This point of view is simplistic, because any SIS can be successively in both of the two modes if a certain latency of the demand after occurrence is assumed. As an illustration, consider a shutdown valve, which has to close when an overpressure occurs in an upstream part of a pipe. The considered SIS is working in accordance with low demand mode until the overpressure arises but, after that and until the overpressure is exhausted, the SIS works under continuous mode of operation to preserve the pipe against this overpressure. In this state, any inappropriate opening of the shutdown valve can lead to an accident. This general configuration, which extends the previous one (Fig. 2), is shown in Fig. 3.

The meaning of all the states and parameters used in this new model remains the same as in the previous one. Here μ_d stands for the inverse of the mean latency time of the demand, and state 2 is the demand state.

In the following, the accident frequency w_{acc} is determined by using the critical working states approach [**8**]

Table 1 A discriminatory criterion of the different demand modes for a SIS

Modes of operation	Conditions
Low demand	$w_d \times MDT_{SIS} < 1$
High demand	$w_d \times MDT_{SIS} \geqslant 1$
Continuous demand	$w_d \times MDT_{SIS} \gg 1$

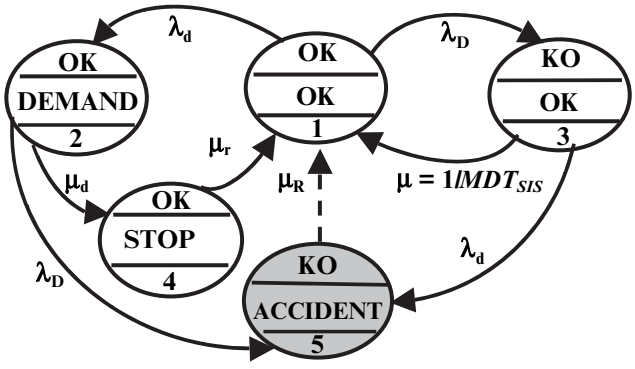


Fig. 3 An extended generic Markovian model incorporating process demand

$$
\begin{aligned}
w_{acc} &= \frac{1}{T}\int_0^T w_{acc}(t)\,dt \\
&= \frac{1}{T}\int_0^T (p_3(t)\lambda_d + p_2(t)\lambda_D)\,dt \\
&= \frac{\lambda_d}{T}\int_0^T p_3(t)\,dt + \frac{\lambda_D}{T}\int_0^T p_2(t)\,dt
\end{aligned} \tag{9}
$$

As before, the mean values of the probabilities can be approximated by their asymptotic values

$$w_{acc} \approx \lambda_d\, p_3(\infty) + \lambda_D\, p_2(\infty) \tag{10}$$

By explaining $p_2(\infty)$ and $p_3(\infty)$, by making the realistic hypothesis that $p_2(\infty) \approx 1$, equality (10) becomes

$$w_{acc} \approx \frac{\lambda_D}{(\lambda_d + \mu)}\lambda_d + \frac{\lambda_d}{(\lambda_D + \mu_d)}\lambda_D \tag{11}$$

Because $\lambda_d \ll \mu$ and $1/\mu_d << 1/\lambda_D$, equality (11) can be reduced

$$w_{acc} \approx \frac{\lambda_D}{\mu}\lambda_d + \frac{\lambda_d}{\mu_d}\lambda_D \tag{12}$$

Moreover λ_D/μ and λ_d/μ_d express respectively the average value of the PFD of the SIS and the average value of the probability of demand, i.e. PFD_{SIS} and p (demand), when λ_D and λ_d respectively approximate the PFH of the SIS, PFH_{SIS}, and the demand frequency w_d.

Under the above conditions, equation (12) can be rewritten as follows

$$w_{acc} \approx PFD_{SIS}\, w_d + PFH_{SIS}\, p(\text{demand}) \tag{13}$$

Here are the two extreme cases of the SIS mode of operation.

1. *Low demand mode*. In this case, $p(\text{demand}) \approx 0$ and equation (13) is reduced to

$$w_{acc} = PFD_{SIS}\, w_d \tag{14}$$

   This corresponds to the following chronological sequence: failure of the SIS followed by the occurrence of the demand.
2. *Continuous demand mode*. This time $p(\text{demand}) = 1$. Now this demand emanates from the EUC, which is continuously outside its nominal state, meaning unavailable to all intents and purposes ($A_{EUC} = 0$). In these conditions $w_d = \lambda_{EUC} A_{EUC} = 0$, and equation (13) is reduced to

$$w_{acc} \approx PFH_{SIS} \tag{15}$$

   This corresponds to the following chronological sequence: sustainable presence of the demand followed by the occurrence of the SIS failure.

The equalities (14) and (15), which return to equalities (3) and (8), reflect only specific cases. An exhaustive analysis of the behaviour of any SIS should conclude that a SIS is as likely to fail before or after the occurrence of a demand and that each of these two mutually exclusive configurations can lead to the undesired event (accident). In more concise terms, the frequency of this accident must be calculated based on the formula (13), in which the SIS failure modes to be taken into consideration to calculate the PFD_{SIS} and the PFH_{SIS} are different.

3 PFD_{avg} AND RISK REDUCTION FACTOR (RRF)

For a SIS working in low demand, IEC 61508 and IEC 61511 standards establish the relationship between the PFD_{avg} and the RRF by means of the following equality

$$w_{acc} \approx \mathrm{PFD}_{avg}\, w_d \Leftrightarrow \frac{w_d}{w_{acc}} = \frac{1}{\mathrm{PFD}_{avg}} = \mathrm{RRF} \tag{16}$$

In accordance to the above relation, the IEC 61511 standard provides a table that indicates the RRF corresponding to each SIL zone (see Table 2).

It is worth noticing that the equation (16), which partially returns to equation (8), is correct, regardless of the protection system in question, whether it is reduced to a single layer or not. In the latter case, however, it is imperative to consider all the protection layers together. That protection technique, aimed at reducing the risk by interposing several layers of protection between the initiating event (demand) emanating from the monitored process and the target to protect, is examined in detail in Annex F of the IEC 61511-3 standard under the title of LOPA (layer of protection analysis). It has been frequently presented, commented upon, implemented, but too often, unfortunately, without retaining a degree detachment [**9**, **10**]. In fact, in the case of an association (parallel assembly in reliability terms) of several independent protection layers (IPLs), it has been established that the risk reduction factor RRF_S provided by this association is the same as the product of the individual factors RRF_i for the layers making them up. So

Table 2 Relation between RRF and SIL in low demand mode

SIL	PFD_{avg}	RRF
4	$\geqslant 10^{-5}$ to $< 10^{-4}$	10000 to 100 000
3	$\geqslant 10^{-4}$ to $< 10^{-3}$	1000 to 10 000
2	$\geqslant 10^{-3}$ to $< 10^{-2}$	100 to 1000
1	$\geqslant 10^{-2}$ to $< 10^{-1}$	10 to 100

$$\mathrm{RRF_S} = \prod_{i=1}^{n} \mathrm{RRF}_i = \prod_{i=1}^{n} \frac{1}{\mathrm{PFD}_i} \tag{17}$$

In other words, the PFD_S for the assembly is equal to the product of the PFD_i for the constitutional layers

$$\mathrm{PFD_S} = \prod_{i=1}^{n} \mathrm{PFD}_i \tag{18}$$

This is clearly false, if one remembers that average values are being considered. In order to illustrate this problem, a system that consists of a simple association of two protection layers is considered (see Fig. 4).

For the sake of simplicity, assume that the first layer is a SIS with a 1oo1 architecture and the second layer is a relief valve. Assume, moreover, that the accident occurs only if both layers fail. The parameters of interest for the SIS and the relief valve respectively are (λ_{DU1}, λ_{DD1}, MTTR, T_1) and (λ_{DU2}, MTTR, $T_2 = 2T_1$), where T_i ($i = 1, 2$) is the proof-test interval. First, the standard approach to compute the global RRF is applied. Then, the correct approach is used.

3.1 Standard approach

On the basis of Fig. 4, the following can be written

$$\begin{aligned}\frac{1}{\mathrm{RRF_{std}}} &= \frac{1}{(\mathrm{RRF_1\,RRF_2})} = \mathrm{PFD_1\,PFD_2} \\ &= \left[\lambda_{DU1}\left(\frac{T_1}{2} + \mathrm{MTTR}\right) + \lambda_{DD1}\,\mathrm{MTTR}\right] \\ &\quad \times \lambda_{DU2}\left(\frac{T_2}{2} + \mathrm{MTTR}\right)\end{aligned} \tag{19}$$

The title 'std' refers to 'standard'.

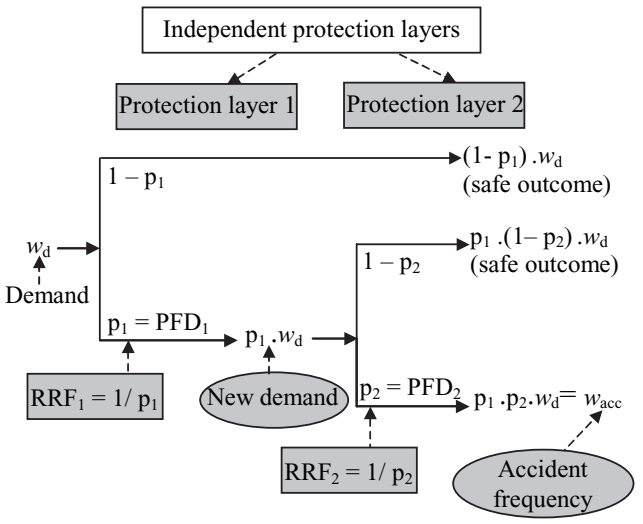


Fig. 4 Risk reduction carried out according to the standard by associating two protection layers

Taking into account the respective values for T_1, T_2, and MTTR, a good approximation of equation (19) is given below

$$\frac{1}{\mathrm{RRF_{std}}} = (\lambda_{\mathrm{DU1}}\,\frac{T_1}{2})\,(\lambda_{\mathrm{DU2}}\,\frac{T_2}{2}) = \frac{\lambda_{\mathrm{DU1}}\,\lambda_{\mathrm{DU2}}\,T_1^2}{2} \tag{20}$$

3.2 Correct approach

The previous approach is erroneous because the whole $\mathrm{PFD_{avg}}$ of the SIS made up of two layers is clearly not equal to the simple product of their individual $\mathrm{PFD_{avg}}$ values. The approach that the present authors recommend requires considering the two protection layers together and therefore calculating the overall $\mathrm{PFD_{avg}}$ as follows

$$\mathrm{PFD_{avg}} = \frac{1}{T_2}\int_0^{T_2} \mathrm{PFD_1}(t)\;\mathrm{PFD_2}(t)\,\mathrm{d}t \tag{21}$$

By approximating $\mathrm{PFD_1}(t)$ and $\mathrm{PFD_2}(t)$ by $\lambda_{\mathrm{DU1}}t$ and $\lambda_{\mathrm{DU2}}t$ respectively over their first interval between tests, and by $\lambda_{\mathrm{DU1}}.\,(t - T_1)$ and $\lambda_{\mathrm{DU2}}t$ over the second interval, the following is obtained

$$\mathrm{PFD_{avg}} = \frac{\lambda_{\mathrm{DU1}}\,\lambda_{\mathrm{DU2}}}{2T_1}\left[\int_0^{T_1} t^2\,\mathrm{d}t + \int_{T_1}^{2T_1} (t - T_1)\,t\,\mathrm{d}t\right] \tag{22}$$

So, after solving

$$\mathrm{PFD_{avg}} = \frac{7}{12}\,\lambda_{\mathrm{DU1}}\,\lambda_{\mathrm{DU2}}\,T_1^2 = \frac{1}{\mathrm{RRF_{ex}}} \tag{23}$$

where 'ex' refers to 'exact'. Comparing equations (20) and (23) leads to

$$\frac{\mathrm{RRF_{ex}}}{\mathrm{RRF_{std}}} = \frac{7}{6} \approx 1.17 \tag{24}$$

This last result shows that the standard approach leads to an (in the present case, slightly) optimistic value for the RRF, and therefore it is non-conservative. This may not be acceptable from a safety point of view. The standard approach is erroneous, because the average value of the product of mathematical functions (PFD(t) here) is not equal to the product of the average values for these functions. Moreover, it should be explained that the 'exact' method is valid regardless of whether the different protection layers are independent or not.

4 THE TRUE NATURE OF THE PFH

4.1 Preliminary remarks

The $\mathrm{PFD_{avg}}$ of a SIS is now widely recognized as its average unavailability, but the nature of the probability of failure per hour (PFH) is still not clearly defined either in the IEC 61508 standard, or in the general literature. To highlight this lack of definition, the reader can check Part 4 of the IEC 61508 standard, which is entirely devoted to definitions and abbreviations, and gives no definition of the PFH! Note 4 of paragraph 7.6.2.9 of the IEC 61508-1 is the only place where a so-called definition is given: 'The parameter in Table 3 for high demand or continuous mode of operation, probability of a dangerous failure per hour, is sometimes referred as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour'. This definition is ambiguous, however, because it gives the wrong impression that a failure frequency and a failure rate are equivalent ideas. Two ways of calculating it, also not equivalent, are also explicitly mentioned, in two other volumes.

1. The calculation procedure described in paragraph B.3.1 of the IEC 61508-6 standard is quoted in full: 'the overall probability of a dangerous failure (understood per hour) for a safety function of a E/E/PE safety related system is determined by calculating the dangerous failure rates for all the sub-systems assuring the safety function and by adding these individual values'.
2. Note 5 located at the foot of page 64 of the IEC 61508–1 standard states that to obtain this probability, for a defined mission time during which no repair can take place, one must determine the failure probability of the safety function during the mission time and divide this probability by the mission time.

Table 3 Variables used in the Petri nets model

Domain	Name	Definition/initial value
Real	LDDIN	(LAMBDA*0.5)*(1-BETAD)*DC
Real	LDUIN	(LAMBDA*0.5)*(1-BETA)*(1-DC)
Real	LDDCD	(LAMBDA*0.5)*BETAD*DC
Real	LDDCU	(LAMBDA*0.5)*BETA*(1-DC)
Real	BETA	—---------
Real	DC	—---------
Real	LAMBDA	—---------
Real	BETAD	BETA*0.5
Boolean	A_KO	False
Boolean	B_;KO	False
Boolean	CCF_DD	False
Boolean	CCF_DU	False
Boolean	TEST	False
Real	1oo2_KO	#1==0&#11==0

Examination of the above procedures raises the following points. The first procedure does not take into account the real architecture of the studied SIS, as it is assimilated in all cases into a generalized series architecture. This leads to an overestimation of the 'equivalent' failure rate for the overall system and consequently an underestimation of its reliability, which is conservative but penalizing.

The second procedure lacks rigour in its statement. What is 'the probability of the safety function failing during the mission time'? That could be, at most, perceived as an average unavailability. It seems more likely, or even certain, that the authors of this statement were thinking about the distribution function $F(t)$, which is only the unreliability of the SIS assuring the safety function ('... no repair can take place ...').

These pseudo-definitions will now be examined in order to converge on to an acceptable definition.

4.2 Is PFH an average failure rate?

From Note 5 mentioned above, it appears that PFH can be expressed as follows

$$\text{PFH} = \frac{\text{probability of failure of a SIS during } T}{T} \tag{25}$$

If the probability of the SIS failing to perform the safety function, during the mission time T, actually designated its unreliability $F(T)$, equation (25) becomes

$$\text{PFH} = \frac{F(T)}{T} \tag{26}$$

This formulation can arouse surprise because it seems that it is sufficient to calculate the PFH value over a long duration T to obtain a low, or even very low, value and therefore very advantageous for this probability, as $F(T)$ was limited from above by the unit, the ratio $F(T)/T$ tends towards zero when T increases. Can this dead-end be avoided by explaining $F(T)$ as shown below? The following paragraph demonstrates that this is not possible.

$$\text{PFH} = \frac{1 - R(T)}{T} = \frac{1 - \exp\left(-\int_0^T \lambda(t)\mathrm{d}t\right)}{T} = \frac{1 - \exp\left(-\lambda_{\text{avg}} T\right)}{T} \tag{27}$$

If, furthermore, $\lambda_{\text{avg}}\, T \ll 1$, which is presumably the case in practice, the preceding expression is simplified

$$\text{PFH} \approx \frac{\lambda_{\text{avg}} T}{T} = \lambda_{\text{avg}}(0,\ T) \tag{28}$$

The probability of failure per hour could therefore be assimilated to the average value of the failure rate $\lambda(t)$, calculated over the duration T, called average failure rate. Another disadvantage of this formulation lies in the fact that $\lambda(t)$ is expressed by an indeterminate form when t increases sufficiently, as shown by the following well-known expression

$$\lambda(t) = \frac{-[\mathrm{d}R(t)/\mathrm{d}t]}{R(t)} \tag{29}$$

Calculating λ_{avg} no longer makes any sense. This allows the question set as the title to this paragraph to be answered with a 'No'. Another interpretation of PFH is then required.

4.3 Is PFH an average density function?

Equation (26) can be rewritten as follows

$$\text{PFH} = \frac{F(T)}{T} = \frac{1}{T}\int_0^T f(t)\mathrm{d}t = f_{\text{avg}}(0,\ T) \tag{30}$$

The PFH for an entity can be considered as the average value of its probability density, calculated over a given period T. As for the preceding case, the value of f_{avg} obviously depends on the duration T over which it is calculated, but it is different on two points: obtaining it is not subject to satisfying a condition ($\lambda_{\text{avg}}\, T \ll 1$) and its limit is defined. The problem is that this limit is nil when the duration T becomes very large. As it is not conceivable to have a null PFH, nor can the interpretation according to which this PFH would be the average value of a probability density be validated. Once again, another interpretation is needed.

4.4 Is PFH an average failure intensity?

The common problem with the two previous attempts to define the PFH lies in the fact that they are only related to the reliability of the SIS. It seems more relevant to choose another indicator, which is able to take into account the successive failures and repairs of this system. Two other parameters, with a similar nature to the preceding ones, are suitable for that: the conditional failure intensity $\lambda^{\text{v}}(t)$ (Vesely's rate), and the unconditional failure intensity $w(t)$ (failure frequency [**11**]). Their definitions are given below.

$$\lambda^{\text{v}}(t) = \lim_{\mathrm{d}t\to\infty} \frac{\text{prob (C fails between } t \text{ and } t + \mathrm{d}t/A\,)}{\mathrm{d}t} \tag{31}$$

where A denotes the event 'component C was working at time $t = 0$ and is working at time t'.

$$w(t) = \lim_{\mathrm{d}t\to\infty} \frac{\text{prob (C fails between } t \text{ and } t+\mathrm{d}t/B)}{\mathrm{d}t} \tag{32}$$

where B denotes the event 'component C was working at time $t = 0$'.

Moreover, these two formal definitions are consistent with the following formulae giving their average values

$$w_{\text{avg}} = \frac{1}{T}\int_0^T w(t)\,\mathrm{d}t = \frac{W(0,\,T)}{T} \tag{33}$$

where $W(0, T)$ is the expected number of SIS failures occuring over the period T. The ratio $W(0,T)/T$, calculated over a high mission time, can be assimilated to the mean time between two consecutive failures, i.e. the so-called MTBF.

$$\lambda^{\text{v}}_{\text{avg}} = \frac{1}{T}\int_0^T \lambda^{\text{v}}(t)\,\mathrm{d}t \approx \frac{W(0,\,T)}{TF} \tag{34}$$

where TF is the cumulated duration that the SIS has been working over duration T. This last equation is just an approximation and is only acceptable in a stationary regime ($\lambda^{\text{v}}_{\text{avg}} = 1/\text{MUT}$).

Which, between $w(t)$ or $\lambda^{\text{v}}(t)$, is the most suitable term to represent the PFH, via the average value? It seems undeniable to the present authors that the PFH is the average failure frequency or the average unconditional failure intensity w_{avg}. This assertion is justified by the following considerations.

1. $w(t)$ is identified at $f(t)$ in the cases of non-repairable entities.
2. The PFH is intimately associated with the 'continuous demand' mode of operation for which a failure in the SIS automatically leads to an undesired event emanating from the monitored process, in the absence of other layers of protection. This simultaneity appears in the relationship (3), which identifies the SIS's failure frequency with that of the undesired event (the accident): $w_{\text{acc}} = w_{\text{SIS}}$.
3. The examination of the definition of $w(t)$ and $\lambda^{\text{v}}(t)$ and the way of obtaining their average values over a duration T, reinforce the authors' conviction. In fact, what interests the people in charge of the process is finding out the average number of accidents that could arise over a specified duration, which is often the system's lifetime (T); this of course encompasses both production periods (TF) and downtimes.

4.5 How to compute the PFH (w_{avg})?

The analytical formulae proposed in Annex B of the IEC 61508-6 standard make quite restrictive assumptions. They cannot be easily extended beyond these hypotheses [**3**]. On the other hand, holistic models, such as fault trees, Markov chains, and stochastic Petri nets, can be used to compute the PFH in the general case. It is worth noticing that these holistic models also provide the PFD_{avg} of the studied SIS (see references [**3**] and [**12**] for further detail).

4.5.1 Fault tree model

The PFH(t) for a system S, meaning its unconditional failure intensity $w_{\text{S}}(t)$ is obtained, using the fault tree approach, on the basis of the so-called critical working states method [**8**]. To do this, for each of its components c_i, it is possible to calculate their own unconditional failure intensity $w_i(t)$ and their Birnbaum importance factor $I_{\text{B}}(S,\, c_i)$. Their respective products are then added together [**13**, **14**], making

$$w_{\text{S}}(t) = \sum_i I_{\text{B}}(S,\ c_i)\, w_i(t) \tag{35}$$

PFH is then deduced by applying the first equality of the equation (33).

4.5.2 Markov model

The method used is, as before, the critical working states method, but this time applied to a Markov model (multiphase or its corresponding classical model). The expression for the PFH(t) is then as follows [**8**]

$$\text{PFH}(t) = w_{\text{S}}(t) = \sum_{i\in M_{\text{C}}} \Lambda_i p_i(t) \tag{36}$$

where M_{C} denotes the set of the critical working states and Λ_i the sum of the failure rates removing the critical working state i and finishing in a failed state. The average value of PFH(t) over the period T is directly deduced from equation (36)

$$\begin{aligned}\text{PFH} &= \frac{1}{T}\int_0^T \left(\sum_{i\in M_{\text{C}}} \Lambda_i p_i(t)\right)\mathrm{d}t \\ &= \frac{1}{T}\sum_{i\in M_{\text{C}}}\left(\Lambda_i \int_0^T p_i(t)\,\mathrm{d}t\right) \\ &= \frac{1}{T}\sum_{i\in M_{\text{C}}} \Lambda_i\, \text{CST}_i\,[0,\ T]\end{aligned} \tag{37}$$

and finally

$$\text{PFH} = \sum_{i\in M_{\text{C}}} \Lambda_i\, \text{APS}_i\,[0,\ T] \tag{38}$$

where $\text{CST}_i\ [0,\ T]$ and $\text{APS}_i\ [0,\ T]$ denote respectively the cumulative sojourn time in the critical working state i, over the period T, and the average probability of sojourn in this state over the same period.

4.5.3 Petri net model

When the Petri net approach is used, w_{avg}, and then PFH, are obtained by estimating the expected number of firing $W(0, T)$ of transitions leading directly to any place related to a system failed state, and dividing it by the mission time T, according to the second part of the equation (33).

4.6 An illustrative example

4.6.1 The models used

To illustrate the ability of the three above models to compute the PFH, each of them is applied to a simple 1oo2 architecture. Fault tree, multiphase Markov, and Petri nets models are depicted in Figs 5 to 7 respectively.

The fault tree model does not need any particular comment. The multiphases Markov model, however, requires some explanations.

1. This model shows that common cause failures (CCF), transitions $\beta_D \lambda_{DD}$ and $\beta \lambda_{DU}$, must be not considered independently from individual failures.
2. The values of the state probabilities at the beginning (b_i) of the period i are computed from those obtained at the end of the period $i - 1$, by means of the matrix pictured in Fig. 6.

The Petri nets model of Fig. 7 is rather hard to understand without any explanation. An explicit description of the main features of this kind of model is outside the scope of this paper. However, some explanations related to the syntax used are given below:

#i (i is an integer > 0) is the marking of the place number i on the network
jets indicates the number of tokens
e1|e2 is the OR logic for *e1* and *e2*, which are Boolean expressions
e1&e2 is the AND logic for *e1* and *e2*, which are Boolean expressions
!! introduces a list of variables assignments; these assignments take place when the transition is launched
?? specifies a list of conditions that must be verified for the transition to be valid
drc δ is Dirac's law of duration δ
exp λ is the exponential law with the rate λ.

The Boolean and real variables used, which greatly improve the ability of Petri nets to capture any aspect of the behaviour of studied systems, are grouped in Table 3.

4.6.2 Numerical results

Some results, calculated over 10 years, obtained from the three models and those given in Table B.13 of Annex B of the IEC 61508-6 standard are presented in Table 4, with the reliability parameters of interest: T_1 (proof-tests interval) = 8760 h, λ (overall failure rate), DC (diagnostic coverage), β (proportion of dangerous undetected common cause failures), β_D (proportion of dangerous detected common cause failures), MTTR = 8 h.

A brief examination of Table 4 shows very good agreement between the results obtained from the three holistic models, which are increasingly closer to the standard values. It also shows that the latter are not systematically greater than those obtained from

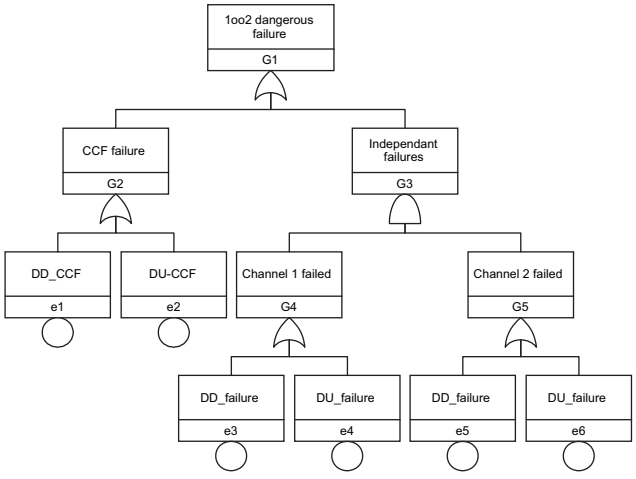
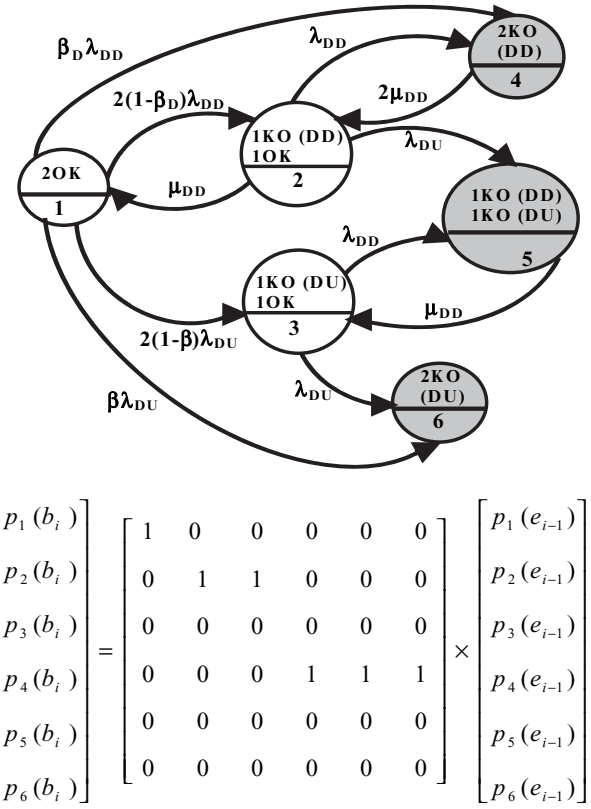


Fig. 5 Fault tree model related to the 1oo2 architecture



$$\begin{bmatrix} p_1(b_i) \\ p_2(b_i) \\ p_3(b_i) \\ p_4(b_i) \\ p_5(b_i) \\ p_6(b_i) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} p_1(e_{i-1}) \\ p_2(e_{i-1}) \\ p_3(e_{i-1}) \\ p_4(e_{i-1}) \\ p_5(e_{i-1}) \\ p_6(e_{i-1}) \end{bmatrix}$$

Fig. 6 Multiphase Markov model related to the 1oo2 architecture

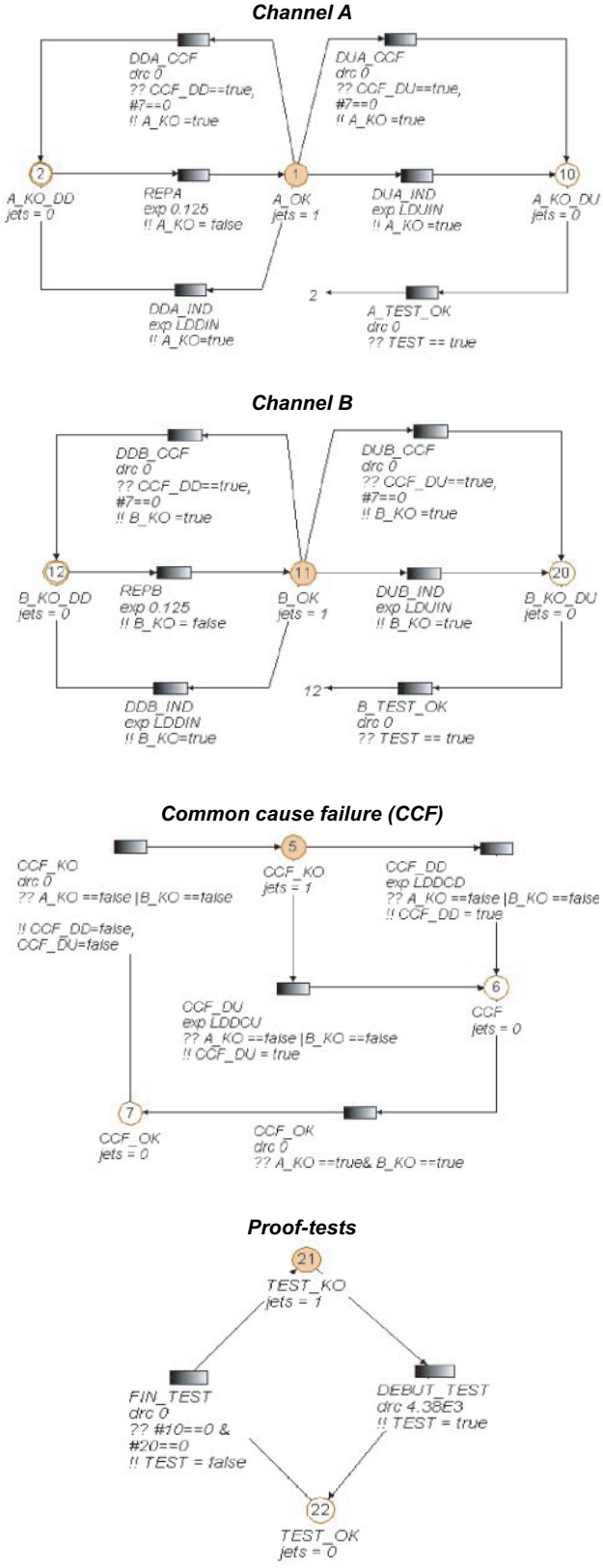


Fig. 7 Petri net models related to the 1oo2 architecture

the holistic models used (not systematically conservative), conversely to what has been observed for the case of PFD_{avg} [**3**].

Table 4 Numerical results obtained from holistic models and from the IEC 61508-6 standard

Failure rate λ (h^{-1}) (LAMBDA in Table 3) $= 5.0\times10^{-6}$				
Approaches				
IEC 61508	DC (%)	0	$\beta = 2\beta_D = 10\%$	2.90×10^{-7}
			$\beta = 2\beta_D = 20\%$	5.40×10^{-7}
		60	$\beta = 2\beta_D = 10\%$	1.90×10^{-7}
			$\beta = 2\beta_D = 20\%$	3.70×10^{-7}
		90	$\beta = 2\beta_D = 10\%$	1.40×10^{-7}
			$\beta = 2\beta_D = 20\%$	2.80×10^{-7}
Fault tree model	DC (%)	0	$\beta = 2\beta_D = 10\%$	2.93×10^{-7}
			$\beta = 2\beta_D = 20\%$	5.33×10^{-7}
		60	$\beta = 2\beta_D = 10\%$	1.93×10^{-7}
			$\beta = 2\beta_D = 20\%$	3.65×10^{-7}
		90	$\beta = 2\beta_D = 10\%$	1.42×10^{-7}
			$\beta = 2\beta_D = 20\%$	2.79×10^{-7}
Multiphase Markov model	DC (%)	0	$\beta = 2\beta_D = 10\%$	2.93×10^{-7}
			$\beta = 2\beta_D = 20\%$	5.33×10^{-7}
		60	$\beta = 2\beta_D = 10\%$	1.93×10^{-7}
			$\beta = 2\beta_D = 20\%$	3.65×10^{-7}
		90	$\beta = 2\beta_D = 10\%$	1.42×10^{-7}
			$\beta = 2\beta_D = 20\%$	2.79×10^{-7}
Petri nets model (10^6 trials)	DC (%)	0	$\beta = \beta_D = 10\%$	2.97×10^{-7}
			$\beta = \beta_D = 20\%$	5.37×10^{-7}
		60	$\beta = \beta_D = 10\%$	1.91×10^{-7}
			$\beta = \beta_D = 20\%$	3.66×10^{-7}
		90	$\beta = \beta_D = 10\%$	1.46×10^{-7}
			$\beta = \beta_D = 20\%$	2.81×10^{-7}

5 CONCLUSION

This paper summarizes some qualitative and quantitative results from recent advanced work [**3**] on several topics related to the IEC 61508 standard. New insights have been given regarding some of the main definitions and concepts of this standard, in order to highlight any ambiguity regarding their comprehension before implementing or using them. First, this clarification has concerned the definitions of low demand and high demand or continuous mode of operation and has proposed a new criterion to distinguish them. This criterion is based on the confrontation between two perfectly defined amounts: the demand frequency from the EUC (w_d) and the mean downtime of the associated SIS (MDT_{SIS}). Then, the relationship between the whole RRF obtained by associating several layers of protection and the combination of their individual PFD_{avg} has been studied. The result is that the commonly used approach is not conservative. Finally, this paper showed that the PFH can be identified with the average unconditional failure intensity (w_{avg}) of the SIS. In this regard, three procedures for calculating the PFH have been proposed and applied to a 1oo2 system.

The authors hope that this contribution will provide the reader with a better understanding of the IEC 61508 standard (Part 6, in particular). Some important concepts, however, such as safe failure fraction

(architectural constraints) and spurious failures (their impact on the PFD_{avg} and on the EUC availability), have not been discussed here. This will be the subject of a forthcoming publication.

REFERENCES

1 IEC 61508 standard: Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, 1998–2000 (International Electrotechnical Commission, Geneva, Switzerland).

2 IEC 61511 standard: Functional safety – safety instrumented systems for the process industry sector, Parts 1 to 3, 2003 (International Electrotechnical Commission, Geneva, Switzerland).

3 **Innal, F.** *Contribution to modelling safety instrumented systems and to assessing their performance – Critical analysis of IEC 61508 standard*. PhD thesis, Université Bordeaux-1, France, 2008 (English version available from the author).

4 **Misumi, Y.** and **Sato, Y.** Estimation of average hazardous-event frequency for allocation of safety-integrity levels. *Reliability Engng Syst. Safety*, 1999, **66**(N2), 135–144.

5 **Bukowski, J. V.** Incorporating process demand into models for assessment of safety system performance. In Proceedings of the RAMS'06 Symposium, Newport Beach, California, USA, 2006, pp. 577–581.

6 **Innal, F., Dutuit, Y., Rauzy, A.,** and **Signoret, J. P.** An attempt to better understand and to better apply some of recommendations of IEC 61508 standard. In Proceedings of the 30th ESReDA Seminar on *Reliability of safety critical systems*, SINTEF/NTU, Trondheim, Norway, 7–8 June 2007, pp. 1–16 (JRC, Ispra, Italy).

7 **Yoshimura, I.** and **Sato, Y.** Safety achieved by the safe failure fraction (SFF) in IEC 61508. *IEEE Trans. Reliability*, 2008, **57**, 662–669.

8 **Vesely, W. E.** A time-dependent methodology for fault tree evaluation. *Nucl. Engng Des.*, 1970, **13**, 337–360.

9 **Dowell, A. M.** Layer of protection analysis for determining safety integrity level. *ISA Trans.*, 1998, **37**, 155–165.

10 **Marszal, E. M.** An example of layer of protection: Analysis using the PROBE tool, 2000. Available from www.exida.com.

11 **Kumamoto, H.** and **Henley, E. J.** *Probabilistic risk assessment and management for engineers and scientists*, 1996 (IEEE Press, Piscataway, New Jersey).

12 **Dutuit, Y., Rauzy, A.,** and **Signoret, J.-P.** A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. *Proc. IMechE, Part O: J. Risk and Reliability*, 2008, **222**(O3), 371–379. DOI: 10.1243/1748006XJRR147.

13 **Cocozza-Thivent, C.** *Processes stochastiques et fiabilité des systèmes*, 1997 (Springer, Berlin).

14 **Dutuit, Y.** and **Rauzy, A.** Approximate estimation of system reliability via fault trees. *Reliability Engng Syst. Safety*, 2005, **87**(N2), 163–172.

APPENDIX

Notation

APS_i [0, T]	average probability of sojourn in the critical working state i, over the period T
BPCS	basic process control system
CCF	common cause failure
CST_i [0, T]	cumulative sojourn time in the critical working state i, over the period T
DC	diagnostic coverage
E/E/PE	electrical/electronic/programmable electronic safety-related systems (SIS)
f_{avg}	average probability density
$I_B(S, c_i)$	Birnbaum importance factor of component c_i
IPL	independent protection layer
*K*oo*N*	*K* out of *N*
LOPA	layer of protection analysis
MDT	mean downtime
MTBF	mean time between failure
MTTR	mean time to repair
MUT	mean uptime
PFD_{avg}	average probability of failure on demand
PFH	probability of dangerous failure per hour
RFF	risk reduction factor
SIL	safety integrity level
SIS	safety instrumented system
T	SIS mission time
T_1	proof-test frequency
TF	cumulated duration that the SIS has been working over duration T
w	unconditional failure intensity (failure frequency)
w_{acc}	average accident frequency
w_{avg}	average unconditional failure intensity (average failure frequency)
w_d	demand frequency
w_{PT}	proof-tests frequency
w_{SIS}	average SIS failure frequency
$W(0, T)$	expected number of SIS failures over its mission time T
λ_{avg}	average failure rate
λ_d	demand rate
λ_D	dangerous failure rate
λ_{DD}	detected dangerous failure rate
λ_{DU}	undetected dangerous failure rate
λ^v	conditional failure intensity (Vesely's rate)
λ^v_{avg}	average conditional failure intensity (Vesely's rate)
μ	inverse of the SIS mean downtime (MDT_{SIS})
μ_d	inverse of the mean latency time of the demand
μ_r	inverse of the mean time required to restart the EUC after its shutdown