# A Snapshot of Methods and Tools to Assess Safety Integrity Levels of High Integrity Protection Systems

Yves DUTUIT
Université Bordeaux-1 / LAPS
351, cours de la Libération
33405 Talence cedex, France

Antoine RAUZY
CNRS / IML
163, avenue de Luminy
13288 Marseille cedex 09, France

Jean-Pierre SIGNORET
TOTAL / CSTJF
Avenue Larribau
64018- Pau cedex, France

**Abstract**

In the oil industry, High Integrity Protection Systems tend to replace traditional safety systems. In this article, we give a snapshot of the methods and tools we designed to evaluate efficiently Safety Integrity Levels of High Integrity Protection Systems, as required by IEC 61508 and 61511 standards.

IEC 61508 and 61511 standards provide rigorous processes to build the safety of Safety Instrumented Systems. They are very efficient from an organizational point of view. However, difficulties arise with definitions and probabilistic calculations. To overcome these difficulties, we extended existing methods and tools. We present here these extensions by means of simple examples. We focus on the treatment of High Integrity Protection Systems working in low demand mode (i.e. with less than one demand per year according to the standards), i.e. systems like High Integrity Pressure Protection Systems. We give some indications for safety systems working in continuous mode. We draw some practical conclusions from the various experiments we performed. First, fault trees, when properly used, are very efficient for low demand safety systems. Second, multi-phase Markov processes provide accurate results, even if only very small systems are tractable with this approach. Finally, behavioral modeling coupled with Monte Carlo simulation on Petri nets is both efficient and accurate. From our point of view, these approaches are simpler to handle than the informative formulae proposed in the present issue of IEC 61508 and 61511 standards.

## 1. Introduction

In the oil industry, traditional protection systems defined in API 14C [1] tend to be replaced by Safety Instrumented Systems (SIS), like the so-called High Integrity Protection Systems (HIPS). To comply with IEC 61508 [2] and IEC 61511 [3] standards, Safety Integrity Levels (SIL) of these SIS must be calculated. IEC 61508 and 61511 standards distinguish two kinds of SIS: SIS working in low demand mode, which are assumed to have less than one demand per year and SIS working in high (or continuous) demand mode (the others). In the oil industry, there are mainly three kinds of HIPS:

- Topside HIPS that are easily tested and maintained,
- Sub-sea HIPS that are difficult to test and to maintain,
- Preventive HIPS.

According to the standards, topside and sub-sea HIPS belong to the low demand mode category, while preventive HIPS belong to the continuous mode category.

IEC 61508 and 61511 standards provide rigorous processes to build SIS. They are very efficient from an organizational point of view. However, some difficulties arise when using them to assess SIL [4] [5] [6]. These difficulties are often ignored by practitioners. They stand in the following issues.

- The taxonomy and definitions of failures,
- The way tests and maintenance procedures are handled,
- The concept of Safe Failure Fraction (SFF),
- The calculations of Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH).

In order to solve these difficulties, we extended a set of existing probabilistic methods and tools: Fault Trees, multi-phase Markov processes and Petri nets or high level models coupled with Monte Carlo simulation. Each of these approaches has its own merits and drawbacks. From our experiments, we are able to draw a number of conclusions:

- Fault trees, when properly used, are very efficient for low demand safety systems.
- Multi-phase Markov processes provide interesting results, even if only very small systems are tractable with this approach.
- Petri nets or high level models coupled with Monte Carlo simulation are efficient and accurate.

From our point of view, these approaches are simpler to handle than the informative formulae proposed in the present issue of IEC 61508 and IEC 61511 standards. We present them here by means of simple examples. We focus on High Integrity Protection Systems working in low demand mode. We give also some indications for safety systems working in continuous modes of operation. The contribution of this article is twofold. First, we attempt to clarify the underlying mathematical concepts of the IEC 61508 and IEC 61511 standards. Second, we present a number of methods and tools we designed in order to overcome the difficulties raised by the evaluation of safety integrity level of safety instrumented systems.

The remainder of this article is organized as follows. Section 2 recalls some classical definitions. Section 3 discusses the vocabulary and definitions of IEC 61508 and IEC 61511 standards. Section 4 discusses the formula given by the standards for the analysis of a single component. Finally, section 5 presents the different approaches we are using to assess SIL of HIPS.

## 2. Classical definitions

In this section, we recall some classical definitions, taken mainly from [7].

Let *S* denote the system under study. Let *T* denote the date of the first failure of *S*. *T* is a random variable. It is called the lifetime of *S*. We assume that components of *S* were as good as new at time *0* and that they are as good as new after a repair.

Reliability $R_S(t)$ and unreliability $F_S(t)$: the reliability of *S* at *t* is the probability that *S* experiences no failure during time interval *[0,t]*, given it was working at *0*. Formally,

$$R_S(t) \overset{def}{=} \Pr\{t < T\}$$

The unreliability, or cumulative distribution function $F_S(t)$, is just the complement to 1 of the reliability.

$$F_S(t) \overset{def}{=} \Pr\{t \geq T\} = 1 - R_S(t)$$

Failure density $f_S(t)$: The failure density refers to the probability density function of *T*. It is the derivative of $F_S(f)$:

$$f_S(t) \overset{def}{=} \frac{d\ F_S(t)}{dt}$$

For sufficiently small *δt's, fS(t).δt* expresses the probability that the system fails between *t* and *t+δt*, given it was working at time *0*.

Failure rate *$r_S(t)$*: the failure rate or hazard rate is the probability the system fails for the first time per unit of time at age *t*. Formally,

$$r_S(t) \overset{def}{=} \lim_{dt \to 0} \frac{\Pr\{\,the\ system\ \ fails\ between\ t\ and\ t + dt / C\,\}}{dt}$$

where *C* denotes the event "the system experienced no failure during the time interval *[0,t]*". It is easy to derive the following property from the definitions.

$$R_S(t) = \exp\left[-\int_0^t r_S(u)\,du\right]$$

Availability *$A_S(t)$* and unavailability *$Q_S(t)$*: the availability of *S* at *t* is the probability that *S* is working at *t*, given it was working at *0*.

$$A_S(t) \overset{def}{=} \Pr\{\,S\ is\ working\ at\ t\,\}$$

The unavailability is just the complement to 1 of the availability.

$$Q_S(t) \overset{def}{=} 1 - A_S(t)$$

Conditional failure intensity *$\lambda_S(t)$*: the conditional failure intensity refers to the probability that the system fails per unit time at time *t*, given it was working at time *0* and it is working at time *t*. Formally,

$$\lambda_S(t) \overset{def}{=} \lim_{\delta t \to 0} \frac{\Pr\{\ the\ system\ \ fails\ between\ t\ and\ t + \delta t / D\,\}}{\delta t}$$

where *D* denotes the event "the system *S* was working at time *0* and is working at time *t*". The conditional failure intensity is sometimes called Vesely rate. *$\lambda_S(t)$* is an indicator of how the system is likely to fail.

Unconditional failure intensity $w_S(t)$: the unconditional failure intensity refers to the probability that the system fails per unit of time at time *t*, given it was working at time *0*. Formally,

$$w_S(t) \overset{def}{=} \lim_{\delta t \to 0} \frac{\Pr\{\, the\ system\ fails\ between\ t\ and\ t + \delta t / E \,\}}{\delta t}$$

where *E* denotes the event "the system was working at time *0*".

In reference [7], it is shown that the following property holds.

$$\lambda_S(t) = \frac{w_S(t)}{A_S(t)}$$

The above equation provides an actual mean to assess the conditional failure intensity from a fault tree model.

## 3. Vocabulary and Definitions of the Standard

In this section, we discuss the vocabulary and the definitions of IEC 61508 and 61511 standards.

### 3.1. Failure taxonomy

In IEC 61508 and 61511 standards, failures are classified according to two dimensions: dangerous as opposed as safe and detected as opposed as undetected. This is slightly different from the usual failure taxonomy:

- safe versus unsafe,
- revealed versus hidden,
- Time dependent versus on demand.

Terms dangerous and unsafe play similar roles. They describe failures tending to inhibit the safety function. However, in IEC 61508 and 61511 standards, safe failures are defined as not dangerous failures. This definition is different from the conventional one which considers safe failures as failures tending to anticipate the safety action.

The distinction "detected versus undetected" is similar to "revealed versus hidden". The problem is that practitioners reading IEC 61508 and 61511 standards superficially may infer incorrectly that terms revealed and safe can be assimilated. A dangerous detected failure remains indeed dangerous until something is done to make it safe, like reconfiguring the HIPS or stopping the installation.

IEC 61508 and 61511 standards do not distinguish explicitly time dependent (i.e. failures with a probability increasing with time) and on demand failures (i.e. failures occurring due to the demand itself). Only the formers are actually considered by the standards. The latter's are completely ignored. Even worse, they are hidden behind the term Probability of Failure on Demand (see below) which encompasses time dependent failures occurring during test intervals. In our opinion, this is a big problem as on demand failures are likely to arise each time a demand (including proof tests) produces a change in the states of some items (e.g. the rupture of the spring of a relay, the blockage of a valve, ...). This kind of failures cannot be detected by any test.

### 3.2. Low demand versus continuous demand modes

IEC 61508 and 61511 standards identify two modes of functioning: SIS working in low demand modes of operation, and SIS working in high demand or continuous modes. These two kinds of modes are arbitrarily split according to the demand frequency (lower or higher than once per year). The calculation of the average value (PFDavg) of the so-called Probability of Failure on Demand (PFD) is required for those in the first category. The calculation of the so-called Probability of Failure per Hour (PFH) is required for those in the second category.

IEC 61508 and 61511 standards do not define (even informally) the notion of PFD. Only two notes provide some information about it:

- Note 4 (IEC 61508-1; p65): “The parameter in table 3 for high demand or continuous mode of operation, probability of a failure per hour, is sometimes referred as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour” .

- Note 5 (IEC 61508-1; p65): "… Determine the required probability of failure of the safety function during the mission time and divide this by the mission time, to give a required probability of failure par hour".

The mode of operation should be determined by comparing demand and proof test frequencies:

- When the demand frequency is low compared to the test frequency, a failure occurring during the test interval is likely to be detected and repaired before the occurrence of a demand. Therefore the HIPS behaves almost independently from the protected installation. An accident happens if the HIPS is unable to respond (i.e. unavailable) when a demand occurs. The concept of PFD is therefore identical to the traditional concept of unavailability.
- As the frequency of demand increases (compared to the frequency of tests), the probability that the failure of the HIPS is detected and repaired decreases. It even reaches 0 in genuine continuous mode. In this case, the HIPS and the protected installation become strongly linked together. If the HIPS is the only protection system of the operation process, an accident is likely to happen as soon as the former experiences its first failure (i.e. is unreliable).

According to the recommendations of note 4 and 5 cited above, the PFH for a system S and a mission time T can be interpreted as follows.

$$PFH_S(T) = \frac{F_S(T)}{T} = \frac{1 - R_S(T)}{T} = \frac{1 - \exp\left(-\int_0^T \lambda_S(t)\, dt\right)}{T} = \frac{1 - \exp\left(-\lambda_S^{avg}(T).\, T\right)}{T}$$

If $\lambda_S^{avg}.\, T \ll 1$, then the PFH can be approximated as follows.

$$PFH_S(T) \approx \frac{\lambda_S^{avg}(T).\, T}{T} = \lambda_S^{avg}(T)$$

When the system is made of completely and quickly repairable components with constant failure and repair rates (i.e. dangerous detected failures), $\lambda_S(T)$ and therefore $\lambda_S{}^{avg}(T)$ reach quickly an asymptotic constant value $\lambda_S^{as}$. Then, when $PHS_S(T) << 1$, the following equality holds.

$$PFH_S(T) \approx \lambda_S^{as} = \frac{1}{MTTF}$$

To summarize the above developments, we can say that:

- Except the use of a new (and somehow inaccurate) name for a classical concept, the framework of IEC 61508 and 61511 standards raises no problem for the low demand mode: a classical approach may be used.
- For the high demand or continuous mode however, IEC 61508 and 61511 standards introduce a rather unusual parameter.

We think that it is preferable to come back to sound probabilistic concepts of unavailability and reliability when assessing the SIL of HIPS.

The values of the PFDavg and PFH are used to evaluate the Safety Integrity Level are shown in Table 1 and Table 2, as extracted from IEC 61508. Inequalities of Table 1 can be understood as follows. A system which operates in low demand mode is said SIL4 if its PFDavg is between $10^{-5}$ and $10^{-4}$, it is said SIL3 if its PFDavg is between $10^{-4}$ and $10^{-3}$ and so on. Similarly, inequalities of Table 2 can be understood as follows. A system which operates in high demand mode is said SIL4 if its PFH is between $10^{-9}$ and $10^{-8}$, it is said SIL3 if its PFH is between $10^{-8}$ and $10^{-7}$ and so on. Only 4 levels are defined in the standard from the worst level (SIL1) to the best level (SIL4).

## 4. Formula given by the Standards for the Analysis of a Single Component

In this section, we discuss the formula given by IEC 61508 and 61511 standards for the analysis of a single component. We show the drawbacks of a too restrictive approach.

### 4.1. Formula for a Single Component

For a single component with a dangerous undetected failure rate $\lambda$, a repair rate $\mu$ and a test interval $\tau$, IEC 61508 part 6 gives the following formula for the average value of the PFD:

$$\text{PFDavg} \approx \lambda\tau/2 + \lambda/\mu$$

This approximation is shortened very often into the traditional and widely used simple formula PFDavg $\approx \lambda\tau/2$. This latter approximation is valid only when the equipment under control is stopped during both tests and maintenance. Unfortunately, this underlying hypothesis is almost never valid for actual industrial systems. Applying the approximation beyond its application range may lead to non conservative results. In fact, a lot of other parameters have to be taken into consideration to properly model components as actually used in industry, including:

- The probability $\gamma$ of on demand failure,
- The test staggering $\theta$,
- The test duration $\pi$.

With the above parameters, PFDavg becomes:

$$\text{PFDavg} \approx \lambda\tau/2 + \lambda/\mu + \gamma/(\mu.\tau) + \pi/\tau$$

The above approximation is indeed much more complex than the formula given by the standards! The staggering of tests, which has no effect on the PFDavg of a single component, has, on the contrary, a strong systemic impact when redundancy is implemented. Other parameters may be considered like test coverage or human errors. Therefore a thorough analysis of the component is needed to identify which parameters to handle according to the actual study.

### 4.2. Limits of the concept of PFDavg

PFDavg is helpful to design the overall average safety of HIPS. However, it is not really a good measure of the actual risk. A HIPS can spread over several SIL zones through the time. As an illustration, consider the curve of PFD(t) pictured Figure 1. According to PFDavg point of view, the HIPS is SIL3. However, 30% of the time is spent in SIL2 (bold line), which is indeed very significant. The situation is even worse after the 1st test as 44% of the time is spent in SIL2 rather than in SIL3. Therefore, it is of utmost importance to evaluate PFD(t) and PFDmax in addition to PFDavg.

### 4.3. Importance of a thorough analysis of tests

The curve pictured Figure 2 illustrates what happens when a test is performed. The jump $\gamma$ is the probability of failure due to the test itself, i.e. the genuine on demand failure. $\pi$ is the test duration. At the end of the test, the component is either available or unavailable (when a failure has been revealed). The competition between these two situations gives the decreasing part of the curve. The PFD reaches its minimum for the Mean Time To Repair (MTTR = $1/\mu$). After, it increases again, as shown Figure 1.

Figure 2 illustrates the case where the safety function of the component under study remains available during the tests. If it is unavailable (e.g. isolated during tests), PFD(t) is equal to 1 all over the duration $\pi$. The unavailability is taken into account in the second formula of the previous section by the contribution $\pi/\tau$. This ratio is often the main contributor to PFDavg. Unfortunately, this important fact is forgotten in the formula given by the IEC 61508 standard.

## 5. Models and tools

### 5.1. Formulae versus models

Part 6 of IEC 61508 standards provides a list of formulae to assess the PFDavg in some particular cases. Unfortunately, the method used to establish these formulae is not described. This would be acceptable if part 6 was considered only as informative and if its content was not intended to cope with all problems encountered. Unfortunately many users apply it as if it was normative, i.e.

prescriptive. Even worse, some software packages have been developed based on these sole formulae. Someone who ignores the underlying hypotheses may use these software packages and get erroneous and dangerous results.

Three years ago, we noticed that the SIL studies from Total’s contractors were very poor and diagnosed that the common cause was IEC 61508 part 6. Therefore, we decided to develop a sound methodology based on method and tools in use since the early eighties:

- Fault trees which are widely used by most of the practitioners,
- Multi-phase Markov processes which are used less frequently by the practitioners,
- Petri nets or high level models coupled with Monte Carlo simulation which solve most of the difficulties encountered.

## 5.2. Fault Trees

Most of oil industry HIPS are HIPPS (High Integrity Pressure Protection Systems). They operate in low demand mode. For these HIPS, the Fault Tree (FT) approach seems to be the good tool for SIL calculations. With a warning however: combining the PFDavg's of individual components through a FT does not provide the PFDavg of the top event. Unfortunately, some FT commercial software packages apply formulae like the one given in the previous section to calculate PFDavg of basic events and then use these quantities to assess the PFDavg of the system under study. Their results are increasingly non conservative when fault tolerance increases and higher SIL's are targeted.

When failures are (reasonably) independent, the top event PFD(t) can be estimated by using the instantaneous unavailability PFDi(t) of basic events (as shown in reference [8]). PFDavg can be obtained by summing the PFD(t) over the relevant period [0,T].

Figure 3 illustrates a very simple system made of 3 identical components working in two out of three (2oo3) [2]. Only the dangerous undetected failure rates ($\lambda$) and test intervals ($\tau$) have been modeled because it is enough to enlight two important conclusions:

- The difference between PFDavg and the maximum PFD is large (2.5 times),

- The equivalent failure rate of the system is not constant between tests.

In Figure 3, the three components are tested at the same time but it is interesting to see what happens when tests are staggered.

As shown Figure 4, staggering the tests makes PFDavg and PFDmax decrease. This is due to two complementary effects:

- The maximum decreases because the tests are more homogeneously distributed along the time.
- The average decreases because the common cause failures (CCF) test frequency has been multiplied by three.

Therefore, staggering the tests is the best way to improve PFDavg (i.e. SIL), to decrease the spreading of the saw-tooth curve and to reduce the impact of common cause failures. This very important characteristic is not mentioned in the IEC standards.

### 5.3. Multi-Phase Markov Processes

Multi-Phase Markov processes are the simplest way to obtain the saw tooth curves of individual components.  It is illustrated Figure 5.

This model represents a single component with a failure rate λ, a repair rate μ and a probability γ to fail because of the test. The principle is very simple:

- Between tests the component behaves like a 3 states Markov process.
- When a test is performed, the component jumps may change immediately of state according to a transition matrix describing the effect of the test.

With this simple example, we just intended to illustrate the principle of the method.  Multi-phase Markov processes and transition matrices may be more sophisticated than those of Figure 5.  When the test has some positive duration, several phases must be distinguished (during and between tests).

Analytical formulae for PFD(t) can be derived from such models. These formulae can be used in turn into FT models.

Multi-phase Markov processes give accurate results. Unfortunately, they cannot be used for complex systems because of the combinatorial explosion of the number of states and phases. Consider for instance the typical simple architecture for a HIPS working in low demand mode of operation presented Figure 6. The corresponding multi-phase Markov process has dozens of phases and thousands of states. This size remains tractable, but constructing such a model by hand would be much too error prone. An interesting alternative approach consists in generating it from a higher level description. We designed the following treatment chain.

1. Model the system in the high level description language AltaRica [9],
2. Generate automatically of the multi-phase Markov process from the AltaRica model,
3. Assess the multi-phase Markov process (see [10] for a presentation of assessment algorithms),
4. Draw the saw tooth curve.

Figure 7 illustrates the results obtained on the simple HIPS of Figure 6 processed in this way.

We checked the results given by a fault tree model for the simple HIPS of Figure 6 against those given by the multi-phase Markov process. This experiment reinforces the conclusion that, when usable, the fault tree approach provides a very good, if not the best, engineering solution for SIL calculations. Note that reliability parameters used to draw this curve have been chosen to obtain a *nice* saw-tooth curve rather than to calculate the SIL of an actual HIPS.

The above results are focused on low demand mode of operation (unavailability/PFD) but multi-phase Markov processes are also efficient to model continuous mode of operation (unreliability/PFH) or special maintenance policies like repair at the second failure (e.g. encountered when dealing with subsea HIPS). Although its interest is mainly theoretical (because of the exponential blow-up of the size of the models), it provides sound results based on sound mathematical bases. It should be used to validate approximated models.

### 5.4. Behavioral models coupled with Monte Carlo simulation

When analytical methods fail to provide results, Monte Carlo simulation can be used instead. This approach implies to build a model behaving as closely as possible to the actual system. In the early eighties, after a thorough survey of potential models, we have chosen the so-called stochastic Petri nets [11] [12] as a modeling formalism. We have used them for twenty five years. More recently, we participated to the development of the AltaRica language [9]. This language has been published to be used freely.

Behavioral models have been mainly used for production availability calculations (RAM studies) but they also prove to be very efficient for SIL calculations. Figure 8 illustrates a Petri net (PN) modeling a subsea sensor periodically tested by a support vessel. The present time state of the sensor is represented by the location of the token in the various places (represented by circles). It is currently running (W):

- from this state the sensor may fail by itself (λ) or by a common cause failure (message ?DCC received from another sub PN),
- when failed, it enters in a waiting-for-detection state (Wait),
- the failure is detected only when a rig reaches the location above the subsea platform and performs a test: a token arrives in the place (Rig),
- when the failure is detected, it has to wait to be repaired until a rig is available to do that (message ?StR),
- Then, the repair is started (R) and, when finished, the sensor becomes available again (W).

Figure 9 shows an example of enhanced generalized stochastic Petri nets using predicates (i.e. any formula which is true or false) and assertions (i.e. formulae used to update variables during the simulation) as implemented in the software package. Again, this implements a very fast algorithm improved over the past 20 years and allows very efficient Monte Carlo simulations.

By using sub Petri nets (e.g. like Figure 8) it is rather easy to build step by step the whole Petri net modeling the behavior of a safety instrumented system.

Monte Carlo simulation is not able to provide smooth curves like those obtained in analytical ways (fault trees, multi-phase Markov processes) but anyway, Figure 10 and Figure 7, which both result from the assessment of the system pictured Figure 6, are rather similar. The 90% confidence bounds of the simulation which have been represented show that the Monte Carlo simulation may be rather accurate for such SIL calculations. It has to be noted that this curve has only been drawn to assess the maximum PFD(t). PFDavg can be straightforwardly calculated just by estimating the time spent in the failed state. This gives in general the same results as fault-trees and multi-phase Markov processes.

Even if the above approach is very powerful, some analysts unfortunately remain reluctant to handle Petri nets (especially when they think that using a few formulae is sufficient to do the job!). This is why we have adapted a tool developed sometime ago to hide Petri nets behind reliability block diagram (RBD). This is achieved by using libraries of pre-established sub models [13]. Therefore, a specific library for periodically tested components has been developed and the principle of SIL calculations became very simple:

- Building a model like the RBD on Figure 6,
- Attributing the relevant sub PN model to each module by picking it from the library,
- Launching the calculations to obtain the results.

The equivalent Petri Net is automatically generated and calculated. It is not necessary to have heard about PN to use this tool but it is strongly recommended to understand what is done! Anyway, it is always possible to analyze the generated PN if needed. Used on the simple HIPS presented Figure 6, this leads exactly to the same results as those on Figure 10.

When using such models, unavailability, reliability, PFD and PFH may be calculated in the same run. Therefore they are adapted both for low demand and continuous mode of operation.

To finish this presentation, it is worth to notice that Monte-Carlo simulation can be applied to AltaRica Data-Flow descriptions as well. The same AltaRica Data-Flow description can be actually used to:

- generate a fault tree,
- generate a multi-phase Markov process,
- perform a Monte-Carlo simulation.

## 6. Conclusion

Problems encountered when achieving SIL calculations as required by IEC 61508 and IEC 61511 standards may be easily solved by making the link with the conventional reliability field which has developed, over the last 30 or 40 years, sound definitions for reliability parameters, accurate failure taxonomy and very efficient methods, tools and algorithms. This is rather easy for low demand mode HIPS and a little bit more complicated for continuous mode HIPS.

We adopted this philosophy and adapted conventional reliability software packages to SIL calculations. This has been achieved with fault trees and Markov processes on analytical calculations side and with behavioral models (Petri nets and AltaRica Data-Flow) on the Monte Carlo simulations side. This constitutes a powerful set of tools able to manage any SIL calculation of oil production systems on sound mathematical bases.

An important conclusion is that using these methods and tools makes it possible for analyst to focus his work, i.e. on the analysis of the HIPS itself rather on the probabilistic calculations. This avoids spending time to establish complicated and error prone formulae. Therefore, in most of the cases, it is easier to perform rigorous calculations in this way than applying *ad-hoc* formulae like those proposed in the standards.

Studies performed in this way are also easier to verify. This is why we have begun to disseminate the above approaches and why we advocate their use.

# 7. References

[1] API RP 14C: Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms. American Petroleum Institute (2001)

[2] IEC 61508: "Functional safety of electric/ electronic/ programmable electronic safety-related systems. Parts 1-7". (1998, 2000)

[3] IEC 61511: "Functional safety. Safety Instrumented systems for the process sector. Parts 1-3". (2003)

[4] Signoret, J-P: "Managing risks in HIPS by making SIL calculations effective". Proceedings of the seminar IQPC2006, Aberdeen, Great Britain, (2006).

[5] Dutuit,Y., Innal, F., Rauzy, A., Signoret, J-P: "An attempt to understand better and apply some recommendations of IEC 61508 standard". Published in the proceedings of the international seminar ESREIDA, Trondheim, Norway (2006).

[6] Signoret J.-P. "High Integrity Protection Systems HIPS: Methods and Tools for Efficient Safety Integrity Levels Analysis and Calculations". Proceedings of the Offshore Technology Conference, Houston, USA 2007

[7] Y. Dutuit & A. Rauzy. Approximate estimation of system reliability via fault trees. Reliability Engineering and System Safety, Volume 87, Issue 2, pp 163-172, 2005.

[8] Rauzy, A., Dutuit, Y., Signoret, J-P: "Assessment of safety integrity levels with fault trees". Published in the proceedings of the international conference ESREL, Estoril, Portugal (2006).

[9] M. Boiteau, Y. Dutuit, A. Rauzy and J.-P. Signoret, The AltaRica Data-Flow Language in Use: Assessment of Production Availability of a MultiStates System, *Reliability Engineering and System Safety*, Vol. 91, pp 747-755, Elsevier.

[10] A. Rauzy. An Experimental Study on Six Algorithms to Compute Transient Solutions of Large Markov Systems. *Reliability Engineering and System Safety*. vol 86, n°1, pp 105-115.

Elsevier. 2004

[11] Signoret, J-P: "Modeling the behavior of complex industrial systems with stochastic Petri nets". Published in the proceedings of the international conference ESREL 1998, Trondheim, Norway. (1998)

[12] Dutuit,Y., Signoret, J-P: "Tutorial on dynamic system modeling by using stochastic Petri nets and Monte Carlo simulation". Presented at the international conferences Konbin03, Gdansk, Poland and ESREL 2003, Maastricht, the Netherland. (2003)

[13] Signoret, J-P, Chabot, J-L, Hutinet, T.: "Hiding a stochastic Petri net behind a reliability block diagram". Published in the proceedings of the international conference ESREL, Lyon, France (2002)

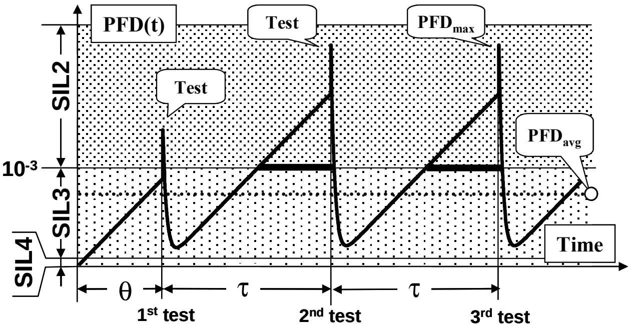

**Figure 1. PFD(t) of a single component**

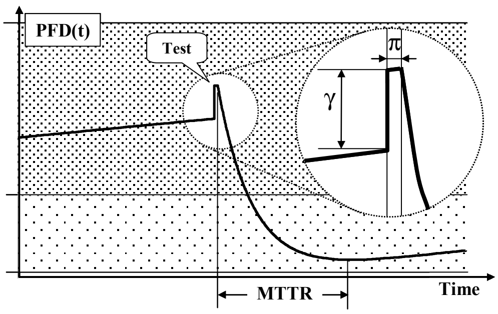

**Figure 2. Detail of the test zone**

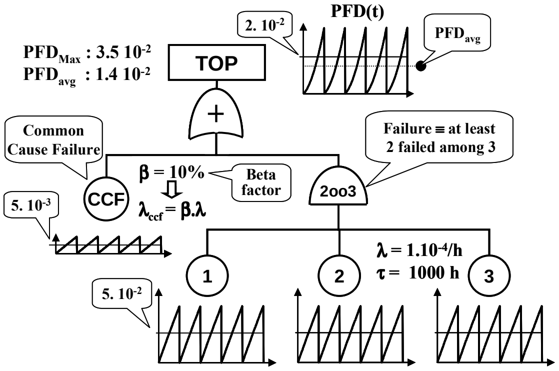

**Figure 3. Example of simple Fault tree**

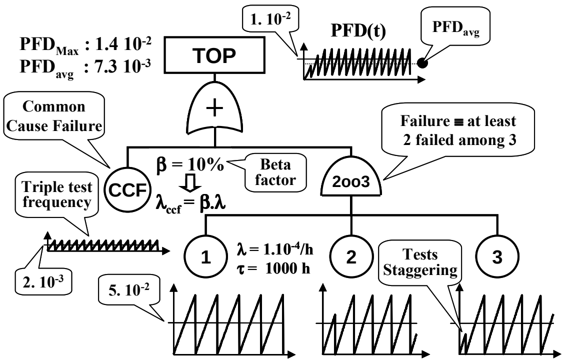

Figure 4. Effects of Test Staggering

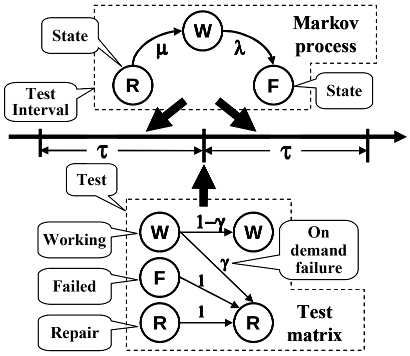

Figure 5.  Multi-Phases Markov Model

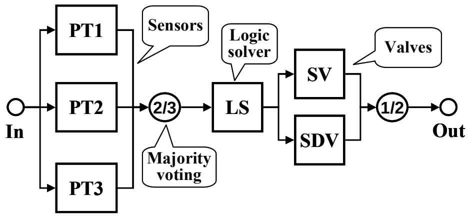

Figure 6. A Simple HIPS

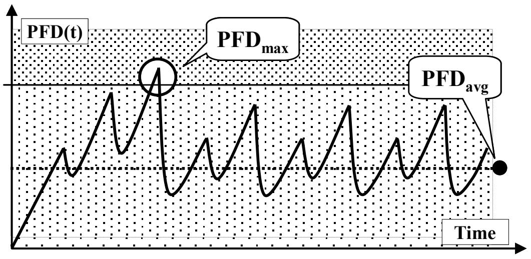

**Figure 7. A Simple HIPS (continued)**

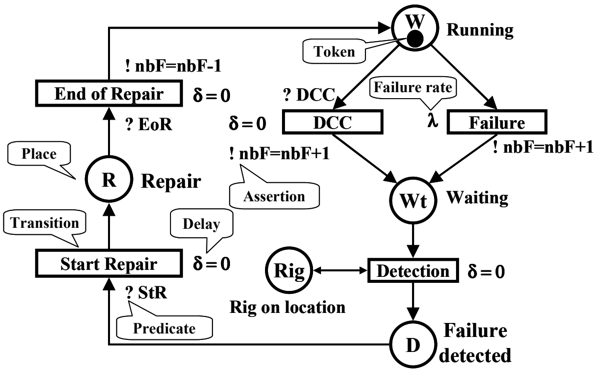

**Figure 8. PN of a subsea sensor**

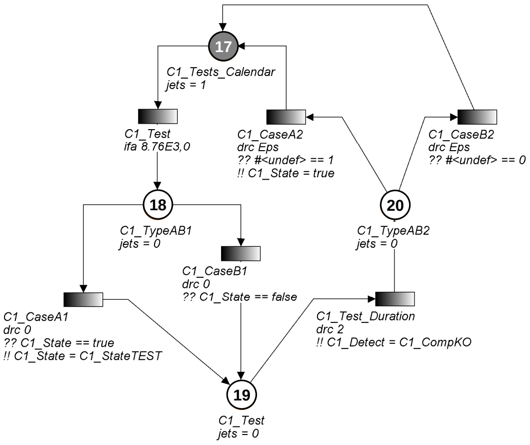

**Figure 9. PN with predicates and assertions**

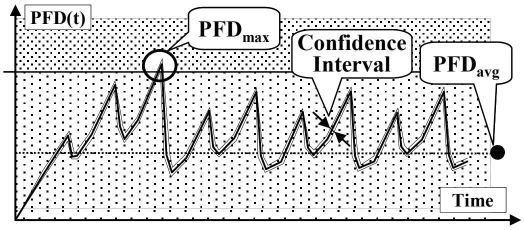

Figure 10. Results from Monte Carlo Simulation

Table 1. Safety Integrity Level: Probability of Failure on Demand

| Demand mode of operation | |
|---|---|
| Safety Integrity Level (SIL) | Target average probability of failure on demand (PFDavg) |
| 4 | $\leq 10^{-5}$ PFD$_{avg}$$<10^{-4}$ |
| 3 | $\leq 10^{-4}$ PFD$_{avg}$$<10^{-3}$ |
| 2 | $\leq 10^{-3}$ PFD$_{avg}$$<10^{-2}$ |
| 1 | $\leq 10^{-2}$ PFD$_{avg}$$<10^{-1}$ |

Table 2. Safety Integrity Level: frequency of dangerous failure of the safety instrumented function

| Safety Integrity Level (SIL) | Target frequency of dangerous failures to perform the safety instrumented function (per hour) |
|---|---|
| 4 | $\leq 10^{-9}$ PFH$<10^{-8}$ |
| 3 | $\leq 10^{-8}$ PFH$<10^{-7}$ |
| 2 | $\leq 10^{-7}$ PFH$<10^{-6}$ |
| 1 | $\leq 10^{-6}$ PFH$<10^{-5}$ |

## Table of Figures

## Table of Tables