Monte Carlo Analysis and Fuzzy Sets for Uncertainty Propagation in SIS Performance Assessment

Fares Innal, Yves Dutuit, Mourad Chebila

***Abstract*—**The object of this work is the probabilistic performance evaluation of safety instrumented systems (SIS), i.e. the average probability of dangerous failure on demand (PFD_{avg}) and the average frequency of failure (PFH), taking into account the uncertainties related to the different parameters that come into play: failure rate (λ), common cause failure proportion (β), diagnostic coverage (DC)... This leads to an accurate and safe assessment of the safety integrity level (SIL) inherent to the safety function performed by such systems. This aim is in keeping with the requirement of the IEC 61508 standard with respect to handling uncertainty. To do this, we propose an approach that combines (1) Monte Carlo simulation and (2) fuzzy sets. Indeed, the first method is appropriate where representative statistical data are available (using pdf of the relating parameters), while the latter applies in the case characterized by vague and subjective information (using membership function). The proposed approach is fully supported with a suitable computer code.

***Keywords*—**Fuzzy sets, Monte Carlo simulation, Safety instrumented system, Safety integrity level.

I. Introduction

NOWADAYS, most of industrial processes, especially the characteristic parameters of their behavior, are constantly monitored by devices qualified as safety instrumented systems (SIS). A SIS is conventionally made up of three main subsystems: sensing elements (S) elements, logic solvers (LS) and final elements (FE). The primary objective assigned to such systems is to detect the occurrence of a hazardous situation, when predetermined conditions are violated such as set points for pressure, temperature, level, etc., that could lead to an accident and then implement a set of necessary reactions to take the system under control to a safe state. In this context, the IEC 61508 [1] has been developed as a performance-based standard to define the requirements for SIS regarding the necessary risk reduction. To characterize these requirements, the IEC 61508 uses the concept of safety integrity level (SIL), which is therefore a measure of the confidence with which the SIS can be expected to perform its safety function [2]. Actually, the SIL relies both on quantitative and qualitative measures. Note that qualitative measures are beyond the scope of this paper. Quantitative measures depend on the number of times the SIS is called to achieve the safety function. According to this statement, IEC 61508 defines two modes of operations: (1) *Low demand mode* (SIS is called upon at a low frequency) for which the relevant performance indicator is the average probability of dangerous failure on demand (PFD_{avg}), and (2) *High or continuous mode* (frequent use of the SIS) where the indicator of interest is the average frequency of a dangerous failure (PFH: Probability of Failure per Hour).

The accordance between SIL levels and the above indicators is presented in Table I [1].

TABLE I
RELATION BETWEEN SIL LEVELS AND SIS PERFORMANCE INDICATORS (PFD_{avg} AND PFH)

SIL	PFD_{avg}	PFH (h^{-1})
4	10^{-5} to < 10^{-4}	10^{-9} to < 10^{-8}
3	10^{-4} to < 10^{-3}	10^{-8} to < 10^{-7}
2	10^{-3} to < 10^{-2}	10^{-7} to < 10^{-6}
1	10^{-2} to < 10^{-1}	10^{-6} to < 10^{-5}

In a previous work [3], the authors have proposed general analytical formulations for PFD_{avg} and PFH which provide a general case of those given on the IEC 61508. The process allowing the establishment of these formulations will not be given in this paper. They are simply recalled hereafter:

$$PFD_{avg}^{KooN} = A_N^{N-K+1}\ \lambda_{Dind}^{N-K+1} \cdot \prod_{i=1}^{N-K+1} MDT_{1ooi} + \lambda_{DU}^{CCF} \cdot \left(T_1/2 + MTTR\right) + \lambda_{DD}^{CCF} \cdot MTTR \tag{1}$$

$$PFH^{KooN} = A_N^{N-K+1}\ \lambda_{Dind}^{N-K+1} \cdot \prod_{i=1}^{N-K} MDT_{1ooi} + \lambda_{DU}^{CCF} + \lambda_{DD}^{CCF} \tag{2}$$

where:

- KooN: K out of N architecture which represents each subsystem constituting the SIS (S, LS, FE).
- $A_n^p = \frac{n!}{(n-p)!}$.
- λ_{Dind} =$(1-\beta)\lambda_{DU}$ + $(1-\beta_D)\lambda_{DD}$: independent dangerous failure rate.
- λ_{DD} (= $DC.\lambda_D$) and λ_{DU} (= $(1-DC).\lambda_D$) are respectively detected and undetected dangerous failure rates.
- *DC*: Diagnostic Coverage. It represents capability for on-line detection of dangerous failures.
- *β and β_D* are common cause failure (*CCF*) proportion for respectively detected and undetected dangerous failures.

F. Innal is with the Laboratory of Research in Industrial Prevention (LRIP), Health and Occupational Safety Institute, University of Batna, Batna 05000 Algeria (corresponding author phone: (00213) 669920488; e-mail: innal.fares@hotmail.fr).

M. Chebila (e-mail: hsemourad@gmail.com).

Y. Dutuit was with Bordeaux-1 University, Bordeaux, 33405, France. He is now with TOTAL Professors Associate (TPS), Gradignan, 33170 France (e-mail: yves.dutuit@sfr.fr).

- $\lambda_{DD}^{CCF} = \beta_D\, \lambda_{DD}$: detected dangerous common cause failure rate. $\lambda_{DU}^{CCF} = \beta\, \lambda_{DD}$: undetected dangerous common cause failure rate.
- *MTTR*: mean time to repair a detected failure.
- $MDT_{\ 1ooi} = \dfrac{\lambda_{DU}}{\lambda_{DD}+\lambda_{DU}} \cdot \left(T_1/(i+1)+MTTR\right) + \dfrac{\lambda_{DD}}{\lambda_{DD}+\lambda_{DU}} \cdot MTTR$ is the mean down time for 1oo*i* architecture.
- T_1: proof-test interval.

For the entire *SIS*, based on the rare events approximation, PFD_{avg}^{SIS} and PFH_{SIS} are given by the following formulae:

$$PFD_{avg}^{SIS} \approx PFD_{avg}^{S} + PFD_{avg}^{LS} + PFD_{avg}^{FE} \tag{3}$$

$$PFH_{SIS} \approx PFH_S + PFH_{LS} + PFH_{FE} \tag{4}$$

Now, the question is where to find quality reliability data, namely: λ_D, *DC*, β, β_D and *MTTR*. It is worth noticing that these parameters may be subject to uncertainty, especially since SIS are highly reliable systems and produce weak historical failure data [4], [5]. Furthermore, the recourse to generic reliability data may introduce uncertainty due to lack of relevance with respect to the system under study [6]. The data shortcomings also induce a strong dependency on the analyst's judgments and may significantly affect the results [7]. Those facts may lead to an inaccurate (even erroneous) SIL level, which could have a great impact on the actual safety of the system under control by increasing the risk of making wrong decision. We stress that this paper deals with the so-called epistemic (state-of-knowledge) uncertainties. For more detail about uncertainty classification, one may refer to [8].

To overcome the underlying difficulties, beside the necessary PFD_{avg} and PFH calculation, the IEC 61508 imposes completing it with a second procedure which may be carried out by two quite different ways called Route 1_H (deterministic) and Route 2_H (probabilistic). Both ways enable us the determination of the maximum SIL that can be claimed (Claimed SIL) for the safety function. They will be explained further in the current document. Route 2_H, introduced at the second version of the IEC 61508 [9], is based on uncertainty propagation. Therefore, it is in keeping with the main goal of this paper. Of course, the uncertainty propagation shows how the uncertainty of input parameters (failure rate, for example) spreads onto the output of the model at hand (in our case: PFD_{avg} and PFH).

For uncertainty propagation many approaches have been developed. Monte Carlo sampling is the most commonly used approach for that purpose, where data uncertainty processing is based on a sampling carried according to a given probability density function (pdf). Even though, within the framework of reliability engineering and risk assessment, a large related work has been achieved, Monte Carlo analysis applied to the SIL calculation still limited. For example and not exclusive, we may note Rouvroye's Ph.D. thesis [10] in which a Monte Carlo analysis were applied to Markov model for the computation of the time dependent probability of failure on demand (PFD(*t*)). Also, Mechri [11] modeled the imperfect knowledge related to the common cause failure proportion (β) by a uniform and triangular probability distribution laws.

An alternative is the use of fuzzy numbers [12] which seems to be appropriate when addressing highly uncertain conditions, i.e. where the statistical data are not sufficient [13]. For this reason, it is suited when data arising from human subjectivity are involved [6]. Many studies have been carried out on the application of fuzzy sets theory to dependability methods [4]. In connection with the treatment of uncertainty in assessing PFD_{avg}, one can note the work of Sallak [4] who proposed the modeling of failure rate with a fuzzy number using the fault tree approach. Furthermore, Mechri [11] has replaced the point-values of common cause failure proportion (β) and diagnostic coverage (DC) by fuzzy numbers using both Fault tree and Markov chains.

The remainder of this article is organized as follow. Section II presents the IEC 61508 approach for uncertainty treatment, i.e. Route 1_H and Route 2_H. In Section III, Monte Carlo and Fuzzy sets principles are briefly described and applied separately to an illustrative example. Section IV is devoted to the presentation of a combined approach using Monte Carlo and Fuzzy sets to deal with different levels of uncertainty. Finally, Section V gives some concluding remarks and research perspectives.

II. Treatment of Uncertainty According to IEC 61508 Standard

As already mentioned, according to the IEC 61508 standard, the computation of PFD_{avg} or PFH is necessary but not sufficient. Indeed, the standard stipulates that additional requirements have to be fulfilled by implementing one of two possible routes: (1) Route 1_H based on hardware fault tolerance (HFT) and safe failure fraction (SFF) concepts, and (2) Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels. Let us look at these two procedures.

A. Route 1_H: Architectural Constraints

In the first edition of the IEC 61508 [1], this procedure was the exclusive way to deal with uncertainty. It is based on two tables (each one concern a specified type of components: A or B which are gathered in this paper (Table II)). Therein, the maximum claimed SIL is expressed in terms of the safe failure fraction (SFF), element type (A or B) and hardware fault tolerance (HFT). A HFT of M means that M+1 is the minimum number of faults that could cause a loss of the safety function. A KooN architecture tolerates N–K failures (faults); e.g. 2oo3 system tolerates 1 fault. Type A element must satisfy the following three conditions: all failure modes are well defined, the behavior under fault conditions can be completely determined and there is sufficient reliable failure data. Otherwise, the element is of type B. The SFF = $(\lambda_\text{S}+ \lambda_\text{DD})/(\lambda_\text{S}+ \lambda_\text{D})$, where λ_S is the safe failures rate (failures which could anticipate the safety function without a demand condition). The SFF at a first view characterize the "safe" behavior under failures of the element at hand (fail-safe), i.e. the higher the SFF, the higher the degree of confidence in this element.

TABLE II
MAXIMUM ALLOWABLE SIL FOR A SAFETY FUNCTION CARRIED OUT BY A TYPE A (RESP. B) ELEMENT OR SUBSYSTEM

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL 1 (Not Allowed)	SIL 2 (SIL 1)	SIL 3 (SIL 2)
60 % - < 90 %	SIL 2 (SIL 1)	SIL 3 (SIL 2)	SIL 4 (SIL 3)
90 % - < 99 %	SIL 3 (SIL 2)	SIL 4 (SIL 3)	SIL 4 (SIL 4)
≥ 99 %	SIL 3 (SIL 3)	SIL 4 (SIL 4)	SIL 4 (SIL 4)

In order to illustrate the route 1_H procedure, let us consider a SIS which must assure a safety function with a required safety integrity level equal to 3 (SIL 3). This imposes that each subsystem of the SIS has at least this SIL: S (e.g. with 1oo2 voting logic, SFF = 70%, type A); LS (e.g. 1oo1, SFF = 99%, type B); FE (e.g. 2oo3, SFF= 50%, type A). From Table II, it can be seen by inspection that the maximum allowable SILs for the above subsystems are respectively: SIL 3, SIL 3 and SIL 2. As a result, the SIS does not meet the required SIL, due to the SIL 2 of the FE subsystem (even if its PFD_{avg} would be in the range of SIL 3). To improve this subsystem, we may change its voting logic from 2oo3 to 1oo3 (redundancy improvement) or use elements with a higher SFF (e.g. 60%) (element improvement). These two improvements could compensate any possible underestimation of failures rates used in PFD_{avg} and PFH calculations. One can conclude that the Route 1_H procedure prevents from selecting a design fully based on a quantitative assessment. It may therefore be interpreted as mistrust to the PFD_{avg} and PFH, as already stated in [14].

However, the SFF, which is the key parameter of that procedure, is based on some failures rates used in the PFD_{avg} and PFH calculations. So, is it a relevant parameter? We are going to attempt to answer this question in the following.

The objective of Route 1_H is to obtain a sufficiently robust architecture. We are not answering the chosen objective, but the fact that we must resort to the SFF to attain it. Let us actually consider two components C_1 and C_2, for which the reliability characteristics are: C_1 (λ_{1S} = 5.4E–7h^{-1}; $\lambda_{1D} = \lambda_{1DU}$ = 6 E–8h^{-1}; T_1 = 4380h; type A), C_2 (λ_{2S} = 5 E–8h^{-1}; $\lambda_{2D} = \lambda_{2DU}$ = 5 E–8h^{-1}; T_2 = 4380h; type A).

Assuming, for a single element, that $PFD_{avgi} \approx T_i/2$, we can easily calculate their respective PFD_{avg}: PFD_{avg1} = 1.3E–4 and PFD_{avg2} = 1.1E–4. Table tells us that these values correspond to a SIL 3. We can now calculate their SFF and obtain: SFF_{C1}= 90% and SFF_{C2} = 50%.

By consulting Table II, the SIL 3 is validated for component C_1, but the claimed SIL for component C_2 is limited to level 2 (SIL 2). This latter is therefore more restricted, more penalised by its SFF than C_1 is, whilst it is slightly higher from a safety point of view ($\lambda_{2D} < \lambda_{1D}$), and 10 times better from an availability point of view ($\lambda_{2S} < \lambda_{1S}$).

The preceding example does not argue in favour of using the SFF and therefore the Route 1_H. We still think that the SFF of any entity is representative neither of its safety, nor its availability. So what use is it? An alternative is to consider the second procedure: Route 2_H. It is explained hereafter.

B. Route 2_H: Uncertainty Propagation

From the description of Route 1_H, one can easily see that the standard does not explicitly handle uncertainty related to parameters used in quantitative assessments of the SIS performances. It only expresses doubts about the quantitative results, where many decision processes require that uncertainty be treated explicitly. Moreover, these doubts concern only failure rates of individual components without taking into account common cause failures that may jeopardize the system redundancy, such as the concept of HFT would be meaningless.

Contrary to Route 1_H, Route 2_H principle is in keeping with uncertainty propagation philosophy, even some minimum HFT requirements still maintained. Beside these requirements, the IEC 61508 [9] stipulates that "*If Route 2_H is selected, then the reliability data uncertainties shall be taken into account when calculating the target failure measure (i.e. PFD_{avg} or PFH) and the system shall be improved until there is a confidence greater than 90 % that the target failure measure is achieved*".

Depending on route 2_H, the uncertainties on reliability data are modeled using probability distributions according to a given law (Uniform, Lognormal, etc.). Hence, a Monte Carlo sampling allows taking into account their effects on the output measures (PFD_{avg} or PFH). However, output measures themselves become random variables (X) and their distributions may cover more than one SIL zone. Therefore, the objective is to demonstrate that the obtained value for PFD_{avg} or PFH of the SIS performing a specified safety function belongs "almost surely" (i.e. with probability of 90%) to the required SIL zone. Different ways to fulfill this objective are presented in the next sections.

Compliance with IEC 61508 shall become a principal step in quantitative risk assessment (QRA) process. Also, uncertainty propagation is a paramount within the framework of QRA to validate and give credit to the obtained results [15]. This being the case, one could understand that Route 2_H is in accordance with that statement which confirm its supremacy regarding Route 1_H.

The next section presents the Monte Carlo approach in more detail. A second approach, Fuzzy sets, will also be presented.

III. MONTE CARLO AND FUZZY SETS PRINCIPLES

A. Monte Carlo (MC) Simulation

Monte Carlo simulation method is generally used to perform uncertainty analysis. This is because this technique has become the industry standard for propagating uncertainties [7]. It provides an efficient way for this purpose. We give hereafter, in connection with SIS performance indicators, its main steps.

- Construct a probability density function (pdf) for each input parameter (pdf reflects state of knowledge about the value of the parameter). In our developed approach, all parameters may be considered: λ_D, DC, β, β_D, MTTR and T_1 (for S, LS and FE). Moreover, therein, seven different probability distributions are implemented: Uniform, Triangular, Normal, Lognormal, Chi-square, Beta and Gamma.
- Generate one set of input parameters by using random numbers (uniformly distributed between 0 and 1) according to pdfs assigned to those parameters.
- Quantify the output function (PFD_{avg} or PFH) using the above set of random values. The obtained value is a realization of a random variable (X).
- Repeat steps 2 to 3 n times (until a sufficient number, e.g. 1000) producing n independent output values. These n output values represent a random sample from the probability distribution (empirical distribution) of the output function.
- Generate statistics from the obtained sample for the output result: mean ($\bar{X}$: PFD_{avg} or PFH), standard deviation σ, confidence interval (percentiles), etc.

The confidence on the obtained SIL according to the value of PFD_{avg} or PFH may be established by checking that the upper limit of the confidence interval ($X_{90\%}$ (or $X_{95\%}$)) is encompassed in the corresponding SIL zone. Also, a direct measure is the evaluation of the cumulated density function (cdf) at the upper bound of the required SIL (noted SIL_{RU}):

$$F\,(SIL_{RU}) = p(X \leq SIL_{RU}) \tag{5}$$

where F is the cdf of the distribution: normal $(X, \sigma/\sqrt{n})$.

An illustration of the Monte Carlo approach is made on a hypothetical SIS. Assume a SIS working in low (resp. high) demand mode. The subsystem S is made up of three pressure transmitters connected according to 1oo3 voting logic. If a condition of high pressure should occur, it is detected at least by one pressure transmitter which send a signal to the subsystem LS. This latter, composed of two programmable logic controllers (1oo2), commands the closure of five shutdown valves (resp. monitors control valves) (subsystem FE). The working of two valves is required. The related reliability characteristics are given in Table III. These characteristics are only given for an illustrative purpose and assumed to be in the range of the available data. 1E+4 iterations have been performed. The obtained results are summarized in Table IV, while the histograms for PFD_{avg} and PFH are presented on Fig. 1.

The review of Table IV allows to the safety function of the SIS at hand a SIL 2 (in case of low demand) and SIL 1 (in case of high demand). This statement is valid with a probability higher than 95%, because the 95th percentiles are included in the related SIL zones. This probability is exactly: $p(X \leq SIL_{RU} = 1E{-}2) = 1$.

TABLE III
RELIABILITY CHARACTERISTICS FOR THE SIS ELEMENTS

Parameters	Subsystem S: 1oo3	Subsystem LS: 1oo2	Subsystem FE: 2oo5
λ_D	Logn. (–12.5, 0.557)	Trian. (5E–7, 1E–5, 3.67E–6)	Trian. (3E–6, 1E–5, 5.33E–6)
DC	Unif. (0.6, 0.8)	Unif. (0.95, 0.99)	Trian. (0.2,0.5, 0.3)
β	Beta (2.33, 4.66) with $0.15 \leq x \leq 0.30$	Unif. (0.01, 0.1)	Unif. (0.1, 0.2)
β_D	Gam. (3.70, 0.027)	Unif. (0.005, 0.05)	Unif. (0.1, 0.2)
$MTTR$	Logn. (2.43, 0.21)	Logn. (2.047, 0.4)	Logn. (2.85, 0.34)
T_1	Constant (4380)	Constant (8760)	Constant (2190)

TABLE IV
OBTAINED RESULTS FROM MC APPROACH

Elements	PFD_{avg}	PFH
S	5.722E–4	5.605E–7
LS	3.642E–5	1.416E–7
FE	6.870E–4	9.157E–7

SIS	Mean = 1.296E–3
	σ= 4.407E–4
	$PFD_{05\%}$ = 1.288E–3
	$PFD_{95\%}$ = 1.303E–3
		Mean = 1.618E–6
		σ= 4.738E–7
		$PFH_{05\%}$ = 1.610E–6
		$PFH_{95\%}$ = 1.626E–6

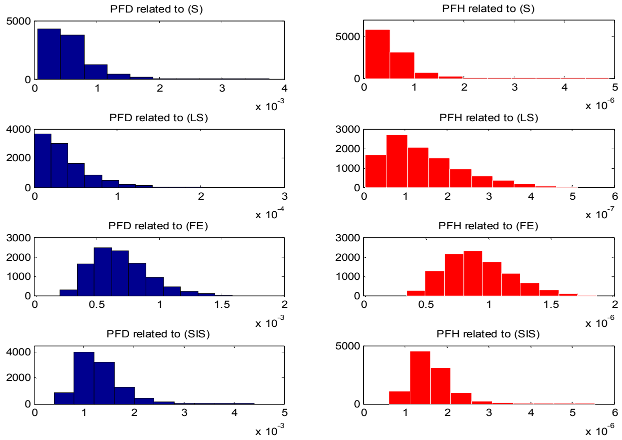


Fig. 1 Histograms related to PFD_{avg} and PFH

B. Fuzzy Sets

The fuzzy set theory started to be developed at the decade of 1960 by Zadeh [12], intending to treat the nebulous aspect of the information. Therefore, it offers an alternative to deal with parameters uncertainties and is an efficient tool for applications where no sharp boundaries (or problem definitions) are possible. It allows using imprecise and approximate data that are typically met in probabilistic assessment. Especially, this approach is suitable when data are affected with high degree of subjectivity and vagueness [6]. Being less restrictive, it may be considered more suitable for treating information provided by human beings than other theories [16]. Of course, when no (or poor) statistical data are available, the use of Monte Carlo simulation becomes meaningless, although possible using some distributions, e.g. Uniform.

A fuzzy set A is a subset from the universe of discourse Ω, whose boundaries are progressive rather than abrupt. Mathematically, such a set is characterized by a membership function μ_A, which assigns to each x belonging to Ω a grade of membership ranging between zero (non-membership) and one (total membership). In that way:

$$A = \left\{x,\ \mu_A(x) \middle| x \in \Omega \text{ and } \mu_A : \Omega \to [0,\ 1]\right\} \qquad (6)$$

In safety and reliability analysis, the membership function is defined by the typical convex functions of triangular, trapezoidal and Gaussian type. Only triangular and trapezoidal functions are implemented in this work. Trapezoidal fuzzy number can be denoted by the fourtuple point (a, m_1, m_2, b), see Fig. 2. It expresses the idea that the evaluation is "*around of*". Mathematically, the corresponding membership function is written as:

$$\mu_A(x) = \begin{cases} \dfrac{x-a}{(m_1 - a)} & \text{if} \quad a \le x \le m_1 \\ 1 & \text{if} \quad m_1 \le x \le m_2 \\ \dfrac{b-x}{b-m_2} & \text{if} \quad m_2 \le x \le b \\ 0 & \text{otherwise} \end{cases} \qquad (7)$$

Triangular fuzzy number is a special case of the trapezoidal one: when $m_1 = m_2$. It expresses the idea that the evaluation is "*close to*". The classical number is encountered when the evaluation is "*exactly*": $a = m_1 = m_2 = b$ (crisp function). To simplify the mathematical operations on fuzzy numbers, a fuzzy number is often represented by its cuts of level α, named α-cuts and noted $A(\alpha)$ [17]: 0 1

$$\forall \alpha \in [0,\ 1],\ A(\alpha) = \left\{x \in R \middle| \mu_A(x) \ge \alpha\right\} \qquad (8)$$

α-cuts represent therefore horizontal slices in a fuzzy set that produce non-fuzzy ones: intervals $[A_L^{(\alpha)}, A_R^{(\alpha)}]$ (Fig. 2).

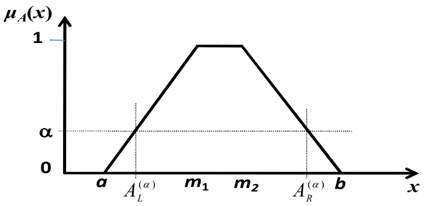


Fig. 2 α-cuts concept

Consider two fuzzy numbers A and B. Based on interval arithmetic, the following expressions are established.

$$\begin{cases} A \to [A_L^{(\alpha)},\ A_R^{(\alpha)}], \quad B \to [B_L^{(\alpha)},\ B_R^{(\alpha)}] \\ C = A + B \to [C_L^{(\alpha)},\ C_R^{(\alpha)}] = [A_L^{(\alpha)} + B_L^{(\alpha)},\ A_R^{(\alpha)} + B_R^{(\alpha)}] \\ C = A - B \to [C_L^{(\alpha)},\ C_R^{(\alpha)}] = [A_L^{(\alpha)} - B_R^{(\alpha)},\ A_R^{(\alpha)} - B_L^{(\alpha)}] \\ C = A \cdot B \to [A_L^{(\alpha)},\ A_R^{(\alpha)}] \cdot [B_L^{(\alpha)},\ B_R^{(\alpha)}] = [C_L^{(\alpha)},\ C_R^{(\alpha)}]: \\ \begin{cases} C_L^{(\alpha)} = \min(A_L^{(\alpha)} \cdot B_L^{(\alpha)}, A_L^{(\alpha)} \cdot B_R^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}, A_R^{(\alpha)} \cdot B_R^{(\alpha)}) \\ C_R^{(\alpha)} = \max(A_L^{(\alpha)} \cdot B_L^{(\alpha)}, A_L^{(\alpha)} \cdot B_R^{(\alpha)}, A_R^{(\alpha)} \cdot B_L^{(\alpha)}, A_R^{(\alpha)} \cdot B_R^{(\alpha)}) \end{cases} \\ C = A / B \to [C_L^{(\alpha)},\ C_R^{(\alpha)}] = [A_L^{(\alpha)},\ A_R^{(\alpha)}] \cdot [1/B_R^{(\alpha)}, 1/B_L^{(\alpha)}] \end{cases} \qquad (9)$$

After fuzzy arithmetic operations, the result is a fuzzy number which further needs to be translated into a crisp value. Defuzzification is an inverse transformation which maps the output from the fuzzy domain back into the crisp domain. Several methods exist for the defuzzification process: centre of area, centre of maximum, mean of maximum, smallest of maximum, largest of maximum and centre of gravity COG (weighted average or centroid). The COG method is the most used and provides a conservative value:

$$A_{COG} = \int_x x \cdot \mu_A(x)\,\mathrm{d}x \Big/ \int_x \mu_A(x)\,\mathrm{d}x \qquad (10)$$

TABLE V
FUZZY CHARACTERISTICS FOR THE SIS ELEMENTS

Parameters	Subsystem S: 1oo3	Subsystem LS: 1oo2	Subsystem FE: 2oo5
λ_D	(1.48E–6, 4.35E–6, 9.26E–6)	(5E–7, 3.67E–6, 1E–5)	(3E–6, 5.33E–6, 1E–5)
DC	(0.6, 0.7, 0.8)	(0.95, 0.97, 0.99)	(0.2, 0.3, 0.4, 0.5)
β	(0.15, 0.2, 0.25, 0.3)	(0.01, 0.055, 0.1)	(0.1, 0.15, 0.2)
β_D	(0.07, 0.1, 0.15)	(0.005, 0.0275, 0.05)	(0.1, 0.15 ,0.2)
MTTR	(8, 12 ,16)	(5, 9, 15)	(8,18, 30)
T_1	4380	8760	2190

TABLE VI
OBTAINED RESULTS FROM FUZZY SETS APPROACH

Elements	PFD$_{avg}$ (COG)			PFH (COG)	
S	1E-3			9.327E-7	
LS	6.920E-4			3.792E-7	
FE	8.182E-4			1.138E-6	
SIS	α	$PFD_L^{(\alpha)}$	$PFD_R^{(\alpha)}$	$PFH_L^{(\alpha)}$	$PFH_R^{(\alpha)}$
	0.0	3E-4	8.2E-3	3.19E-7	6.523E-6
	0.1	3E-4	5.1E-3	3.86E-7	5.429E-6
	0.2	4E-4	4.1E-3	4.62E-7	4.716E-6
	0.3	4E-4	3.5E-3	5.46E-7	4.153E-6
	0.4	5E-4	3.1E-3	6.38E-7	3.672E-6
	0.5	6E-4	2.7E-3	7.39E-7	3.246E-6
	0.6	7E-4	2.4E-3	8.50E-7	2.860E-6
	0.7	8E-4	2.1E-3	9.70E-7	2.508E-6
	0.8	9E-4	1.8E-3	1.10E-6	2.186E-6
	0.9	1E-3	1.6E-3	1.241E-6	1.890E-6
	1.0	1.1E-3	1.4E-3	1.393E-6	1.618E-6
	PFD$_{avg}$ = 2.3E-3			PFH = 2.418E-6	

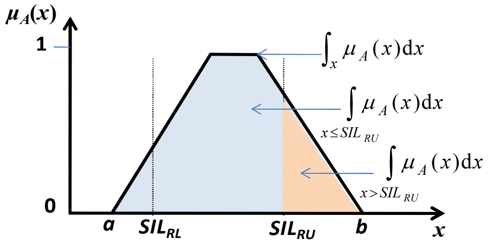

$\mu_A(x)$
1
0
$\int_x \mu_A(x)\mathrm{d}x$
$\int_{x\le SIL_{RU}} \mu_A(x)\mathrm{d}x$
$\int_{x> SIL_{RU}} \mu_A(x)\mathrm{d}x$
a
SIL_{RL}
SIL_{RU}
b
x

Fig. 3 Alternative approach

For illustration, assume a SIS with uncertain parameter values as gathered in Table V. We have kept the same range of variation used in the previous example, in order to compare the results. Using the above principles and relations, the obtained shape related to the SIS fuzzy PFD$_{avg}$ and PFH are depicted in Fig. 3, while the results are gathered on Table VI.

The resulted uncertainty is more important than that obtained using MC simulation: PFD$_{avg}$(α = 0) = [3E–4, 8.2E–3] and PFH(α = 0) = [3.19E–7, 6.523E–6]. The crisp values derived using the COG methods are: PFD$_{avg}$ = 2.3E–3 and PFH = 2.4184E–6h^{-1}. However, the 1-cuts are very close to confidence intervals given by MC simulation: PFD$_{avg}$(α =1) = [1.1E–3, 1.4E–3] and PFH(α = 1) = [1.393E–6, 1.618E–6]. 1-cuts mean that the corresponding intervals belong to the fuzzy number of interest (PFD$_{avg}$ or PFH) with confidence of 100 %. It is obvious that fuzzy sets provide a wide range of uncertainty compared to Monte Carlo simulation, because the formalism is adapted for handling highly uncertain information which leads to high uncertain result.

Also, it is clear that the possibility to reach the range of variation defined by the 0-cuts is very low. In the other hand, 1-cuts intervals do not tack into account different values with high degree of membership (0.9, 0.8, etc.). To remedy to this problematic situation, the analyst may choose an arbitrary interval with for example α = 0.6 and compare the upper limit of that interval to the upper limit of the required SIL zone. However, what value for α the analyst does tack?

To avoid any extra uncertainty due to the choice of α, we propose an alternative based on the following equation, where $p_F(A \le \mathrm{SIL}_{RU})$ express the compliance probability of the fuzzy number A (PFD$_{avg}$ or PFH) with the required SIL (see Fig. 3).

$$p_F(A \le SIL_{RU}) = \int_{x\le SIL_{RU}} \mu_A(x)\mathrm{d}x \Big/ \int_x \mu_A(x)\mathrm{d}x \qquad (11)$$

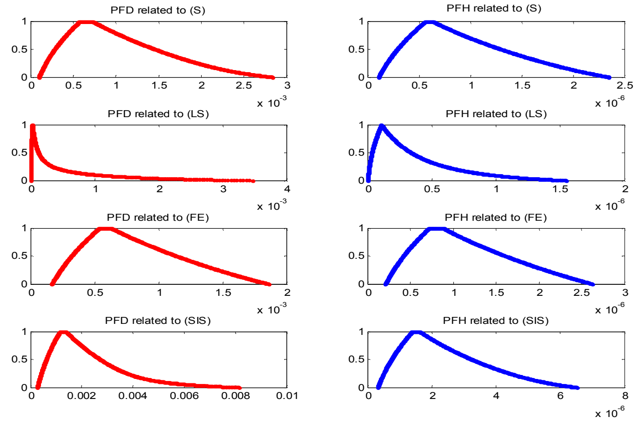


Fig. 4 Curves related to PFD$_{avg}$ and PFH

In the case of the preceding example, applying (11) results in: p_F (PFD$_{avg}$ ≤ 1E–2) = 1, p_F (PFD$_{avg}$ ≤ 1E–3) = 0.151, p_F (PFH ≤ 1E–5) = 1; p_F (PFH ≤ 1E–6) = 0.102. Therefore, the conclusions issued from MC simulation are confirmed: SIL2 for low demand and SIL1 for high demand mode. Despite this agreement between the two approaches, the purpose of this work is not comparing them, but it is their combining to cover different kinds of uncertainties inherent to parameters used to compute the SIS metrics. This is the object of the next section.

IV. Combining Monte Carlo and Fuzzy Sets

In the previous sections, it is noticed that Monte Carlo simulation is a suitable tool to tackle uncertainties when historical data are significant. In the contrary case, i.e. where the provided data are vague and highly subjective, fuzzy sets offers a more effective way to deal with uncertainty.

In practice, those two kinds of uncertainty may be encountered simultaneously. Indeed, for example, a significant historical data may exist for failure rates inherent to proven in use SIS element. Nevertheless, that may not be the case regarding common cause failures of the same element. In addition, data could be available for one subsystem and not available for another one. For example, in the case of new technologies SIS elements (which are generally very complex and highly reliable), no pertinent reliability data exist. This is true for failure rates and it is still more for common causes and diagnostic coverage.

The present paper does not discuss further the gathering and the evaluation of uncertainties of input parameters, but the proposed approach start with these uncertain parameters supposed well defined.

This approach enables one to carry out uncertainty propagation using both Monte Carlo simulation and fuzzy sets. Fig. 5 shows its overall process which is described hereafter. This process is fully automated within a computer code developed under the MATLAB environment.

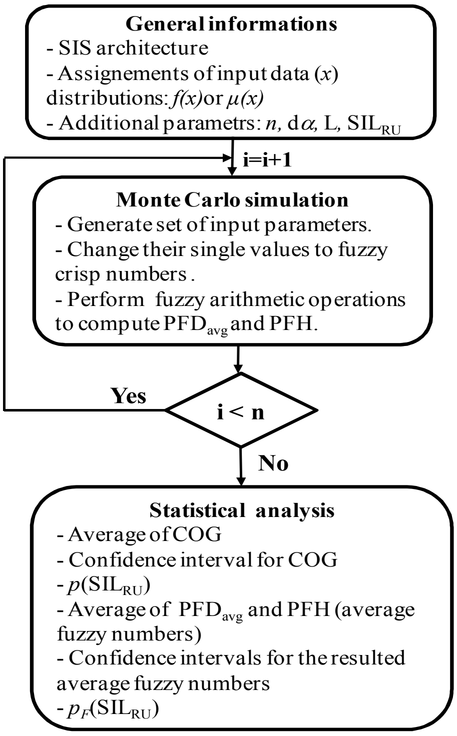

General informations
- SIS architecture
- Assignements of input data (x) distributions: $f(x)$ or $\mu(x)$
- Additional parametrs: n, dα, L, SIL_{RU}
i=i+1
Monte Carlo simulation
- Generate set of input parameters.
- Change their single values to fuzzy crisp numbers.
- Perform fuzzy arithmetic operations to compute PFD_{avg} and PFH.
Yes
i < n
No
Statistical analysis
- Average of COG
- Confidence interval for COG
- $p(SIL_{RU})$
- Average of PFD_{avg} and PFH (average fuzzy numbers)
- Confidence intervals for the resulted average fuzzy numbers
- $p_F(SIL_{RU})$

Fig. 5 Overall process for combining MC and fuzzy sets

A. General Information

The first step of the proposed approach is the assignment of all input data needed for the calculation procedure, including: K and N for the three subsystems of the SIS, probability distributions and/or membership functions for uncertain parameters. The constant law related to Monte Carlo simulation is presented as a fuzzy number in order to easily handle fuzzy representations: crisp value a = [a, a, a, a]. Additional inputs are also required such as *n* (number of Monte Carlo iterations), required SIL upper bounds (SIL_{RU}) for PFD_{avg} and PFH, confidence level L (to compute confidence intervals) and dα which represents the increment for α-cuts (the smaller dα, the more accurate the results).

B. Monte Carlo Simulation

The main idea for the proposed procedure is a Monte Carlo simulation driven by Fuzzy arithmetic. In fact, if at least one parameter is considered as fuzzy number, all resulted amounts are also fuzzy numbers. Once the first step is fulfilled, a Monte Carlo sampling is performed. To deal with uncertainties specified as fuzzy numbers, each input parameter issued from the sampling (described by a pdf) is changed to a crisp number a = [a, a, a, a]. Hence, arithmetic operations may tack place to evaluate PFD_{avg} and PFH, of course they are expressed as fuzzy numbers and entirely defined by their α-cuts.

At the end of this step, the results are stored in two matrixes (for PFD_{avg} and PFH); each line represents the obtained value for the corresponding iteration (*A* stands for PFD_{avg} or PFH):

$$A=\begin{bmatrix} A_{L_1}^{(\alpha_1=0)},\ldots,A_{L_1}^{(\alpha_{(1/d\alpha)+1}=1)},A_{R_1}^{(\alpha_{(1/d\alpha)+2}=1)},\ldots,\ A_{R_1}^{(\alpha_{2(1/d\alpha)+2}=0)} \\ \vdots \\ A_{L_n}^{(\alpha_1=0)},\ldots,A_{L_n}^{(\alpha_{(1/d\alpha)+1}=1)},A_{R_n}^{(\alpha_{(1/d\alpha)+2}=1)},\ldots,\ A_{R_n}^{(\alpha_{2(1/d\alpha)+2}=0)} \end{bmatrix} \quad (12)$$

C. Statistical Analysis

The first computed metrics are the centre of gravity (COG) related to each fuzzy number (each line of the matrixes) and the average of the obtained COGs. Each COG is evaluated according to a discretization (with respect to dα) of (10). Therefore, the average of COGs can be deduced:

$$A_{COG}^{avg}=\sum_{i=1}^{n}A_{COG}^{i}/n \quad (13)$$

In addition, confidence intervals at a given level (L) are provided:

$$\left[A_{COG}^{avg}-E\cdot(\sigma/\sqrt{n}),A_{COG}^{avg}+E\cdot(\sigma/\sqrt{n})\right]=[\,A_{COG_L}^{avg}\;,A_{COG_U}^{avg}\;] \quad (14)$$

where $E=\sqrt{2}\cdot erfinv(L)$ (e.g. for L = 0.9, E = 1.6449).

The probability $p(A_{COG} \leq SIL_{RU})$ is also given:

$$p(A_{COG}\leq SIL_{RU})=F(SIL_{RU})=normcdf(SIL_{RU},A_{COG}^{avg},\sigma/\sqrt{n}) \quad (15)$$

where, *normcdf* (x, μ, σ) computes the normal cdf at the value x using the corresponding mean μ and standard deviation σ.

Furthermore, from the matrix given by (12), the average fuzzy number is computed according to (16).

$$A_{avg}^{F}=\begin{bmatrix}\dfrac{\sum_{i=1}^{n}A_{L_i}^{(\alpha_1=0)}}{n},\ldots,\dfrac{\sum_{i=1}^{n}A_{L_i}^{(\alpha_{(1/d\alpha)+1}=1)}}{n},\dfrac{\sum_{i=1}^{n}A_{R_i}^{(\alpha_{(1/d\alpha)+2}=1)}}{n},\ldots,\dfrac{\sum_{i=1}^{n}A_{R_i}^{(\alpha_{2(1/d\alpha)+2}=0)}}{n}\end{bmatrix} \quad (16)$$

It is obvious now to establish a confidence interval for the resulted average fuzzy number: upper and lower bounds which are also fuzzy numbers. For this purpose, the following procedure is proposed. Its starting point is that the mean of elements associated to each colon of the matrix *A* follow a normal distribution. This being the case, each colon may be characterized by a mean (those given by (16)) and a standard deviation. Therefore, for each elements of the vector given by (16), lower and upper bonds may be computed at a given confidence level. By doing so, the upper bound (resp. lower Bound) of the confidence interval for the average fuzzy number A_{avg}^{F} could be specified by these individual upper bounds (resp. lower bounds), see Fig. 6. Their corresponding COGs are respectively noted $A_U^F\,(COG)$ and $A_L^F\,(COG)$.

Moreover, the compliance probability of the average fuzzy number A_{avg}^{F} with the required SIL, p_F (A_{avg}^{F} $\leq SIL_{RU}$), is computed according to a discretization of (11).

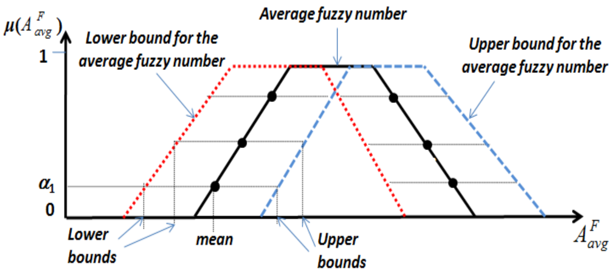


Fig. 6 Confidence interval for the average fuzzy number

D. Illustrative Example

In order to illustrate the application of the proposed procedure, the reliability characteristics of the new SIS are mixed from Tables III and V (see Table VII). Results are grouped on Table III, while Fig. 7 depicts average fuzzy numbers corresponding to the SIS and its subsystems. Fig. 8 presents the histograms related to the SIS COGs. Fig. 9 maps the confidence intervals for the SIS average fuzzy number.

TABLE VII
RELIABILITY CHARACTERISTICS FOR THE SIS ELEMENTS

Parameters	S	LS	FE
λ_D	Logn. (–12.5, 0.557)	(5E–7, 3.67E-6, 1E–5)	Trian. (3E–6, 1E–5, 5.33E–6)
DC	(0.6, 0.7, 0.8)	(0.95, 0.97, 0.99)	(0.2, 0.3, 0.4, 0.5)
β	(0.15, 0.2, 0.25, 0.3)	(0.01, 0.055, 0.1)	(0.1, 0.15, 0.2)
β_D	Gam. (3.70, 0.027)	(0.005, 0.0275, 0.05)	(0.1, 0.15 ,0.2)
MTTR	Logn. (2.43, 0.21)	Logn. (2.047, 0.4)	Logn. (2.85, 0.34)
T_1	Constant (4380)	Constant (8760)	Constant (2190)

TABLE VIII
OBTAINED RESULTS FROM THE COMBINED APPROACH

n = 5000; dα = 0.001; L= 90%

Metrics	PFD$_{avg}$	PFH

A_{COG}^{avg}	Mean= 2.40E–3
	Std = 1.1365E–5
		Mean = 1.912E–6
		Std = 6.67E–9

[$A_{COG_L}^{avg}$, $A_{COG_U}^{avg}$]	[2.381E–3, 2.420E–3]	[1.902E–6, 1.923E–6]
$A_{avg}^{F}(COG)$	2.40E–3	1.912E–6
[$A_L^F(COG)$, $A_U^F(COG)$]	[2.381E–3, 2.420E–3]	[1.902E–6, 1.923E–6]
$p\,(A_{COG} \leq$ SIL$_{RU}$)	p($A_{COG} \leq$ 1E–2) = 1 p($A_{COG} \leq$ 1E–3) = 0	p($A_{COG} \leq$ 1E–5) = 1 p($A_{COG} \leq$ 1E–6) = 0
p_F($A_{avg}^{F} \leq$ SIL$_{RU}$)	p_F(A_{avg}^{F} $\leq$ 1E–2) = 1	p_F(A_{avg}^{F} $\leq$ 1E–5) = 1
	p_F(A_{avg}^{F} $\leq$ 1E–3) = 2.2E-3	p_F(A_{avg}^{F} $\leq$ 1E–6) = 2.04E-2

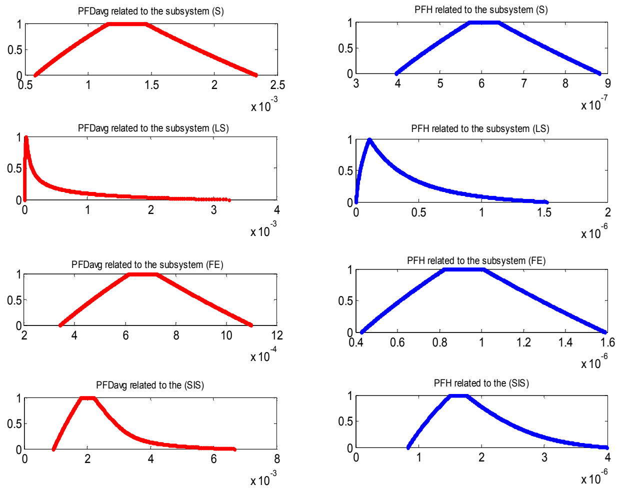


Fig. 7 Average fuzzy numbers related to PFD$_{avg}$ and PFH

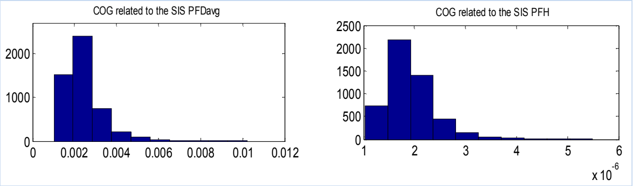
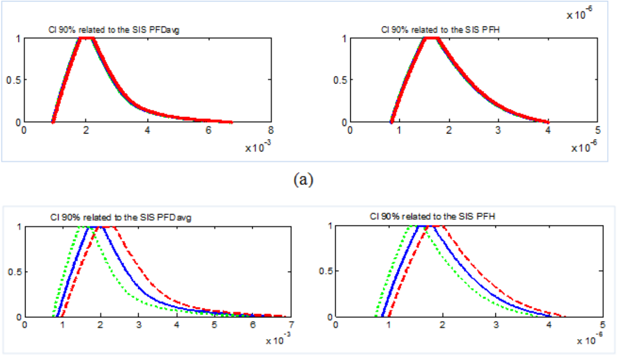


Fig. 8 Histograms for COGs related to the SIS PFD$_{avg}$ and PFH



(a)

(b)

Fig. 9 The SIS PFD$_{avg}$ and PFH confidence intervals for (a) n = 1E+4 and (b) n = 20

Inspection of Table VIII allows, once again, SIL 2 (PFD$_{avg}$) and SIL 1 (PFH) for the safety function implemented in the considered SIS. The main resulting statement, on one hand, is that the average center of gravity (A_{COG}^{avg}) has the same value that the centre of gravity related to the average fuzzy number $A_{avg}^{F}(COG)$, whatever the number of iterations n (MC trials). The same conclusion is made for the confidence intervals:

$$[\ A_{COG_L}^{avg}\ ,\ A_{COG_U}^{avg}\ ] = [\ A_L^F(COG), A_U^F(COG)\ ]$$

At Fig. 9 (a), the mean fuzzy numbers and their respective lower and upper bonds curves are superimposed due to their very close values. Fig 9 (b), where n = 20, shows separated curves.

In addition, the fact that $p_F(A^F_{avg} \le \mathrm{SIL}_{\mathrm{RU}})$ is slightly greater than $p\,(A_{COG} \le \mathrm{SIL}_{\mathrm{RU}}) = 0$ (for $\mathrm{SIL}_{\mathrm{RU}}$= 1E–3 and 1E–6) is due to the spreads of the average fuzzy numbers (Fig. 7) which are slightly higher (toward $\mathrm{SIL}_{\mathrm{RU}}$) than those of the corresponding COGs distributions (Fig. 8).

V. Conclusion

The IEC 61508 standard require to consider uncertainties related to safety instrumented systems' reliability parameters when assessing their performances. This requirement may be carried out by two quite different ways called respectively Route 1_{H} (deterministic) and Route 2_{H} (probabilistic). In this paper we have demonstrated, on the basis of a simple example, that Route 1_{H} is not suitable to handle uncertainty in an effective manner. Furthermore, with respect to Route 2_{H} principle, we have proposed an approach which combines Monte Carlo sampling and fuzzy sets, in order to deal with different degrees of uncertainty: Monte Carlo method is used when a sufficient statistical data are available, while fuzzy sets method is more adapted when data are affected with high degree of subjectivity and vagueness.

In a future work, a sensitivity analysis will be carried out. In this context, new indicators for sensitivity analysis will be introduced regarding the proposed approach.

References

[1] IEC 61508 standard, *Functional safety of electrical/electronic /programmable electronic safety-related systems. Parts 1 to 7*, International Electrotechnical Commission, Geneva, Switzerland, 2010.

[2] Y. Dutuit, F. Innal, A. Rauzy, and J-P. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using fault trees," *Reliability Engineering and System Safety*, vol. 93, pp. 1867–1876, 2008.

[3] F. Innal, "Contribution to modelling safety instrumented systems and to assessing their performance-Critical analysis of IEC 61508 standard," Ph.D. dissertation, University of Bordeaux, France, 2008.

[4] M. Sallak, "Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception: Application aux Systèmes Instrumentés de Sécurité," Ph.D. dissertation, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2007.

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

[6] U. Hauptmanns, "The impact of reliability data on probabilistic safety calculations," *Journal of Loss Prevention in the Process Industries*, vol. 21 (1), pp. 38–49, Jan. 2008.

[7] NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. NASA Office of Safety and Mission Assurance,Washington, 2002.

[8] T. Aven. *Foundations of Risk Analysis - A Knowledge and Decision-oriented Perspective*. Chichester: Wiley, 2003.

[9] IEC 61508 standard, *Functional safety of electrical/electronic/ programmable electronic safety-related systems. Parts 1 to 7*, International Electrotechnical Commission, Geneva, Switzerland, 1998-2000.

[10] J. L Rouvroye, "Enhanced Markov Analysis as a method to assess safety in the process industry," Ph.D. dissertation, Technische Universiteit, Eindhoven, Netherlands, 2001.

[11] W. Mechri, "Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis," Ph.D. dissertation, Université de Tunis El Manar, Ecole Nationale d'Ingénieurs de Tunis, Tunisia, 2011.

[12] L. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, pp. 338–353, 1965.

[13] K. B Misra, and G. G Weber, "A new method for fuzzy fault tree analysis" *Microelectronics and Reliability*, vol. 29(2), pp. 195–216, 1989.

[14] M. A. Lundteigen, "Safety instrumented systems in the oil and gas industry," Ph.D. dissertation, Department of Production and Quality Engineering, Trondheim, Norway, 2009.

[15] T. Bedford, and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, Cambridge, 2003.

[16] C. E Kim, Y. J Ju, and M. Gens, "Multilevel fault tree analysis using fuzzy numbers" *Computers & Operations Research*, vol. 23(7), pp. 695–703, 1996.

[17] D. Dubois, L. Foulloy, G. Mauris, and H. Prade, "Probability-possibility transformations, triangular fuzzy sets, and probabilistic inequalities," *Reliable computing,* vol. 10, pp. 273–297, 2004.

Fares Innal is an Associate Professor with the Health and Occupational Safety Institute at the University of Batna in Algeria. He received a Ph.D. degree in reliability engineering from Bordeaux-1 University in 2008 (France). His current research interests concern dependability modeling including: safety instrumented systems, multi-state systems, probabilistic risk assessment, Monte Carlo simulation and uncertainty propagation.