A Fuzzy Probabilistic Approach for Determining Safety Integrity Level

Mohamed Sallak, Christophe Simon, and Jean-Francois Aubry

***Abstract*—The process industry has always been faced with the difficult task of determining the required integrity of safeguarding systems such as Safety Instrumented Systems (SISs). The ANSI/ISA S84.01-1996 and IEC 61508 safety standards provide guidelines for the design, installation, operation, maintenance, and test of SIS. However, in the field, there is a considerable lack of understanding of how to apply these standards to both determine and achieve the required safety integrity level (SIL) for SIS. Moreover, in certain situations, the SIL evaluation is further complicated due to the uncertainty on reliability parameters of SIS components. This paper proposes a new approach to evaluate the "confidence" of the SIL determination when there is an uncertainty about failure rates of SIS components. This approach is based on the use of failure rates and fuzzy probabilities to evaluate the SIS failure probability on demand and the SIL of the SIS. Furthermore, we provide guidance on reducing the SIL uncertainty based on fuzzy probabilistic importance measures.**

***Index Terms*—Failure rates, fuzzy probabilistic importance measure, fuzzy probabilities, safety instrumented systems (SISs), safety integrity level (SIL), uncertainty.**

I. Introduction

THE process industry tends to be technically complex and has the potential to inflict serious harm to persons and property if the trip cannot avoid harm or during a spurious trip (i.e., the safety function is carried out without a demand from the process). In spite of the application of a wide variety of safeguarding measures, many accidents still happen. Experiences gained from these accidents have led to the application of a variety of technical and non-technical layers of protection, such as safety instrumented systems (SISs). The SIS consists of instrumentation or controls that are implemented for the purpose of mitigating a risk or bringing the process to a safe state in the case of a process failure. Risk in process industry is defined as a measure of human injury, environmental damage or economic loss in terms of both the incident likelihood and the magnitude of the injury, damage, or loss [1]. A SIS is used for any process in which a process hazards analysis (PHA) has determined that the mechanical integrity of the process equipment, the process control, and other protective equipments are insufficient to mitigate the potential risk.

Manuscript received June 16, 2006; revised May 11, 2007.

M. Sallak and J.-F. Aubry are with the Research Center of Automatic Control, Nancy University, CNRS, 54516 Vandoeuvre les Nancy Cedex, France.

C. Simon is with the Research Center of Automatic Control, Nancy University, CNRS, 54509 Vandoeuvre les Nancy, France.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TFUZZ.2007.903328

The ANSI/ISA S84.01-1996 [2] and IEC 61508 [3] safety standards provide guidelines for the design, installation, operation, maintenance, and test of SIS. However, in the field there is a considerable lack of understanding of how to apply these standards to both determine and achieve the required SIL. Thus, determining SIL for a SIS and its validation are very important for compliance with the ANSI/ISA S84.01-1996 [2] and IEC 61508 [3] standards. The SIL of a SIS is defined by its probability to fail on demand (PFD). The PFD represents the probability that the SIS will fail such that it cannot respond to a potentially dangerous condition. $\mathrm{PFD}_{\mathrm{avg}}$ is a term used to describe the average probability of failure on demand. It depends on the period of exploitation of SIS equipments. $\mathrm{PFD}_{\mathrm{avg}}$ will not reach a steady state value if any periodic inspection, test, and repair are done [4]. According to safety standards [2], [3] $\mathrm{PFD}_{\mathrm{avg}}$ is an appropriate metric for measuring the effectiveness of a SIS if it is assumed that the potentially dangerous condition is independent from equipment failures in the SIS.

In the process industry, the operating conditions and environments can change for the same SIS component. The most desirable information is to have sufficient plant specific data about component failures to evaluate their failure rates. Due to the lower solicitation of SIS in plant, SIS components have not been operating long enough to provide statistical valid failure data, and for new plant it is not possible to collect in-house failure data [5], [6]. Laboratory data and generic data are often used to provide failure data of SIS components [4], [7], [8]. Point values from these data origins are generally used to obtain an estimation of the failure rates of SIS components.

However, measuring and collecting failure data have uncertainty associated with them, and borrowing data from laboratory and generic data sources involves uncertainty as well. As mentioned by Kletz [9], failure data can deviate by a factor of 3 or 4, and a factor of 10 is not unusual. Wang *et al.* [5] discussed the impact of data uncertainty in determining the PFD of SIS. However, they do not propose a methodology to treat this problem. They just underlined that more work is needed to examine and justify the uncertainty about determining the PFD of SIS in these cases.

The probabilistic approaches combined with Monte Carlo simulation [3], [10]–[14] which evaluate the PFD of SIS from the failure probabilities of its components might be inappropriate, since most of the available failure rates data are point values without information about the probability distributions of theses failure data. Some reliability databases [15]–[17] provide upper bounds, lower bounds, and error factors of failure rate data for safety components. Fuzzy methods can use advantageously these uncertainty parameters to evaluate the

failure rates of components, and then to determine the failure probabilities of SIS components and the PFD of SIS.

The purpose of this paper is to present a new approach to evaluate the "confidence" of the SIL determination, when there is an uncertainty about failure rates of SIS components. This approach is based on the use of failure rates and fuzzy probabilities to evaluate the fuzzy SIS PFD (SIS probability to fail on demand), and the SIL of the SIS. Furthermore, we provide guidance on reducing the uncertainty of determining SIL based on fuzzy probabilistic importance measures which are used to identify the SIS critical components. Then we modify the SIS configuration for reducing the SIL uncertainty accordingly to the critical components.

This paper is organized as follows. Section II briefly describes the procedure to achieve the safety target level of the process, and reviews the risk analysis techniques that can be used to comply with ANSI/ISA S84.01-1996 [2] and IEC 61508 [3] safety standards. In Section III, we introduce the fuzzy probabilistic approach to determine the SIL of the SIS and evaluate the SIL uncertainty. Moreover, the fuzzy probabilistic importance measure to reduce uncertainty is presented. Section IV concerns an example from the technical report ISA-TR84.00.02-2002 [11] which illustrates the use of the proposed approach and compares it to the conventional probabilistic approach. Then, the reduction of the SIL uncertainty is achieved by computing the fuzzy probabilistic importance measures and modifying the configuration of the SIS critical components accordingly. Finally, some concluding remarks and perspectives are given in Section V.

II. Procedure to Achieve the Safety Target Level of the Process

This section focuses on qualitative and quantitative techniques that can be used to evaluate the risk associated to a process. After the risk has been evaluated, we have to identify the necessary safety instrumented function (SIF) (i.e., a function that is a single set of actions that protects against a single specific risk). Then we have to implement it on a SIS in order to achieve the desired safety level for the process, and verify that the SIS configuration meet the required SIL. All these steps are required in order to comply with the ANSI/ISA S84.01-1996 [2] and IEC 61508 [3] standards.

A. Performance-Based Safety Standards

During the last years, great emphasis has been placed on improving technological risk management in the process industry. Process industry refers to those processes involved, but not limited to the production, generation, manufacture, treatment of oil, gas, wood, metals, food, plastics, petrochemicals, chemicals, steam, electric power, pharmaceutical, and waste material. These efforts have resulted particularly in the development of two performance-based safety standards from the Instrument Society of America (ISA) ANSI/ISA S84.01-1996 [2] and the International Electrotechnical Commission (IEC) IEC 61508 [3].

TABLE I
Definition of SIL for Low and High Demand Modes

Solicitation	Low Demand	High Demand
SIL	PFD_{avg}	Failures/hour
1	$[10^{-2}, 10^{-1}]$	$[10^{-6}, 10^{-5}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-7}, 10^{-6}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-8}, 10^{-7}]$
4	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

B. Safety Instrumented System (SIS)

The SIS is a system composed of sensors, logic solver and final elements for the purpose of taking the process to a safe state when predetermined conditions are violated. The safety performance of the SIS is defined in terms of SIL, which is defined by its $\mathrm{PFD}_{\mathrm{avg}}$. The $\mathrm{PFD}_{\mathrm{avg}}$ value is obtained by combining the average failure probabilities of system components. This combination is a function of the SIS configuration, the proof test interval, the common causes failures, and the inspection and maintenance policies. The ANSI/ISA S84.01-1996 [2], IEC 61508 [3], and ISA-TR84.00.02-2002 [11] recommend several techniques to determine the $\mathrm{PFD}_{\mathrm{avg}}$ value. For safety functions with a low demand rate (for example anti-lock braking), and safety functions with a high demand rate or operate continuously (for example normal braking), the standards recommend values presented in Table I. In the next section, we will use these PFD values for the SIL evaluation.

C. Compliance With ANSI/ISA S84.01-1996 and IEC 61508 Standards

The overall objective of these standards is to identify the required safety functions, establish their SIL and implement them on a SIS in order to achieve the desired safety level for the process. The basic steps required to comply with are the following.

- Identify the safety target level of the process;
- Evaluate the hazardous events that pose a risk higher than the safety target level;
- Determine the safety functions that must be implemented on a SIS to achieve the safety target level;
- Implement the safety functions on a SIS and evaluate its SIL;
- Install, test, and commission the SIS;
- Verify that the installed SIS does reduce the process risk to satisfy the safety target level.

The standards [2], [3] offer three methods of determining SIL requirements:

- qualitative methods;
- semi-quantitative methods;
- quantitative methods.

1) Qualitative Methods: In qualitative methods, the risk concept of likelihood and consequence is used even though no explicit quantification is required. There are several techniques published in the literature [2], [3], [11]. The risk graph method is the widely used. It provides a SIL correlation based on the following four factors [3]:

- consequence (C);
- frequency and exposure time (F);
- possibility of avoiding the hazardous event (P);
- probability of the unwanted occurrence (W).

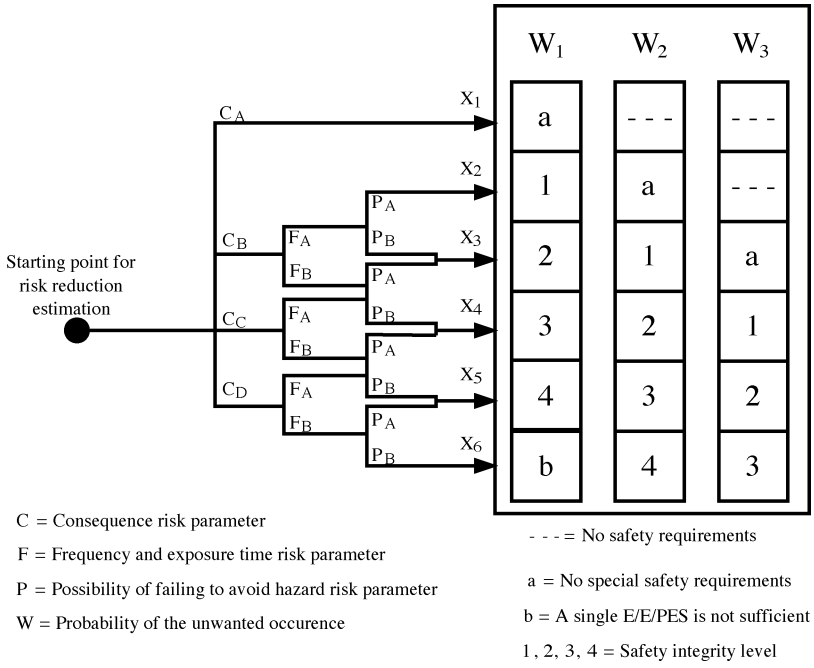

Fig. 1. Example risk graph.

This method is a qualitative technique that requires tools to be developed to ensure that the four parameters listed above are properly chosen. It focuses most of the evaluation on an individual person's risk. The four factors are evaluated from the point of view of a theoretical person being in the incident impact zone. The probability of the unwanted occurrence W is based on the likelihood of the event, which should be evaluated without taking into account any existing SIS. If a frequency is involved in the evaluation of risk graph, the outcome W is expressed as well in terms of a frequency or an expected frequency. For this method, the likelihood and consequences are determined by considering the independent protection layers during the assessment. Independence of protection layers can be guaranteed if the performance is unaffected by the failure of another protection layer or by the conditions that caused another protection layer to fail. The protection layers must also be independent of the initiating cause of failure. Once these factors are determined, the risk graph is used to determine the minimum risk reduction level and associated SIL. An example risk graph is shown in Fig. 1.

2) Semi-Quantitative Methods: A semi-quantitative approach can be used to assess process risk [10], [18]. It allows a traceable path of how the accident scenario develops and comprises the following steps:

- identify the accident scenarios;
- identify the basic events that comprise each accident scenario. Basic events that involved failure or success of safety systems are also taken into account;
- assign a typical likelihood of occurrence for each event;
- estimate the likelihood (approximate range of occurrence) of an accident scenario;
- perform consequence analysis to understand the severity of the accident scenario consequences;
- assign the rate for the severity of the consequences;
- evaluate the risk as a combination of the likelihood and the consequences.

3) Quantitative Methods: The quantitative approach to SIL assignment is the most rigorous technique to use. The SIL is assigned by determining the process demand or incident likelihood quantitatively. The potential causes of the incident are modeled using a quantitative risk assessment technique [11], [12]. The quantitative technique is often used when there is a very limited information database about the process. So, the quantitative determination of likelihood is extremely difficult. The method does require a thorough understanding of the potential causes of the event and an estimated probability of each potential cause. The technical report ISA-TR84.00.02-2002 [11] presents three quantitative methods:

- simplified equations;
- fault tree analysis (FTA);
- Markov modeling.

The simplified equation technique involves determining the average failure probability of the field sensors (FS), logic solvers (LS), and final elements (FE). Once the individual failure probabilities for each input, logic solver and output are known, these probabilities are summed to compute the SIS PFD.

Fault trees analysis can be actually used as either a quantitative or a semi-quantitative method for modeling the SIS. Fault tree symbols are used to show the failure logic of the SIS. The graphical technique of fault tree analysis allows easy visualization of failure paths. Since the actual failure logic is modeled, diverse technologies, complex voting strategies and interdependent relationships can be evaluated. However, fault tree analysis is not suitable to SIS that have time dependent failures. Therefore, Markov approaches can be used to model the SIS and evaluate the SIS PFD.

4) Discussion: The qualitative technique is simple and the limited resources required for its execution make it a useful

screening tool to identify safety areas concerned. The drawback is the dependence on the expertise level of the practitioners. Particularly, consistency may be a problem. The semi-quantitative technique does provide a more systematic approach to assess risk than qualitative methods. The quantitative technique is resource intensive but does provide benefits that are not provided in the other two approaches. The most significant disadvantage of this technique is the need of credible data. In this work, we consider some imprecise information about failure rates of SIS components. Also, it becomes interesting to investigate the use of a quantitative method like FTA, with an integration of the uncertainty involving a fuzzy set approach.

III. Determining SIL via a Fuzzy Probabilistic Fault Tree Analysis

To determine SIL, the technical report ISA-TR84.00.02-2002 [11] recommends the use of fault tree analysis in SIL2 and SIL3 SIS applications. The conventional fault tree analysis which is based on the probabilistic approach has been used extensively in the past [12]–[14]. However, in order to use upper and lower bounds of failure probabilities of SIS components provided by some reliability databases [15]–[17], we propose to use fuzzy fault trees which provide an interesting tool for representing and analyzing these failure probabilities.

The pioneering work on fuzzy fault tree analysis belongs to Tanaka *et al.* [19]. They treated basic events probabilities as trapezoidal fuzzy numbers and applied the fuzzy extension principle to compute the top event probability. Singer [20] analyzed fuzzy reliability by using $L-R$ fuzzy numbers. He considered the relative frequencies of basic events as fuzzy numbers and used possibility instead of probability measures. However, these approaches cannot be applied to a fault tree with repeated events. In order to deal with repeated basic events, Soman and Misra [21] provided a simple method for fuzzy FTA based on the α-cut method, also known as resolution identity. Other results on fuzzy FTA are reported in [22]–[27].

Our approach is to quantitatively evaluate the performances of a SIS. But, as mentioned previously, studies are under uncertainty. The goal of the paper is to take into account these uncertainties in the evaluation. So, we investigate the use of fuzzy set theory to determine the SIL of the SIS.

A. Fuzzy Numbers

Let x be a continuous variable restricted to a distribution function $\mu(x) \in [0,1]$, which satisfy the following assumptions:

- $\mu(x)$ is a piecewise continuous;
- $\mu(x)$ is a convex fuzzy set;
- $\mu(x)$ is a normal fuzzy set.

A fuzzy set which satisfies these requirements is called a fuzzy number.

Obviously, computational efficiency is important in any practical application of fuzzy numbers. But, the operation implied in the extension principle requires extensive computation. From the previous studies made by Kaufman and Gupta [28], it is shown that the computational effort with operation on fuzzy numbers can be reduced by composing the membership functions into α-levels and by conducting mathematical operations on these intervals [29], [30].

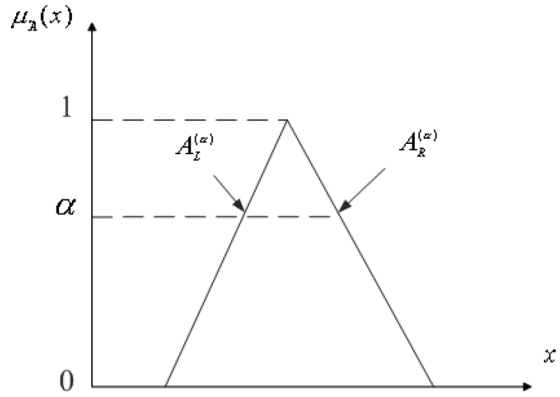

Fig. 2. Bounds points for α-level set interval of $\mu_{\widetilde{A}}(x)$.

For any fuzzy number $\widetilde{A}$ which has the membership function $\mu_{\widetilde{A}}(x)$, an interval bounded by two points at each α-level ($0 \leq \alpha \leq 1$) can be obtained using the α-cut method. The symbols $A_L^{(\alpha)}$ and $A_R^{(\alpha)}$ have been used in this paper to represent the $\mu_{\widetilde{A}}(x)$ left-end-point and right-end-point of this interval.

As it is shown in Fig. 2, we can express a fuzzy number $\widetilde{A}$, using the following form:

$$\widetilde{A} \rightarrow \left[A_L^{(\alpha)}, A_R^{(\alpha)}\right], \quad 0 \leq \alpha \leq 1.$$

The wider the support of the membership function, the higher the uncertainty. The higher the value of α, the higher the confidence in the parameter represented by the fuzzy number [31]. For each α-level of the fuzzy number which represents a parameter, the model is run to determine the minimum and maximum possible values of the output. This information is then directly used to construct the corresponding membership function of the output which is used as a measure of uncertainty. If the output is monotonic with respect to the dependent fuzzy numbers, the process is rather simple since only two simulations will be enough for each α-level (one for each boundary). Otherwise, optimization routines have to be carried out to determine the minimum and maximum values of the output for each α-level.

B. Fuzzy Probabilities

A fuzzy probability, i.e., a fuzzy set defined in probability space, is represented by a fuzzy number between 0 and 1 assigned to the probability of an event occurrence [19], [26], [32].

One can choose depending upon the suitability different types of membership function for fuzzy probability; the more confident portion is given value 1 and other portions are given values between [0,1]. Our goal is to use fuzzy probabilities to describe occurrence probabilities of events. To this end, we follow the standard approach proposed by Soman and Misra [21] to describe the probabilities of various unions, intersections, and complements of these events occurrences.

C. Fuzzy Probabilistic Fault Tree Analysis

In this paper, the fault tree analysis is based on fuzzy set theory. So, we can allocate a degree of uncertainty to each value of the failure probability. The fuzzy probability of system failure

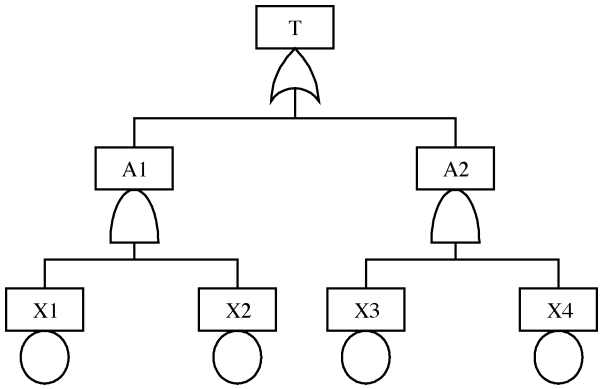

Fig. 3. Fault tree example.

(top event occurrence) is determined from the fuzzy probabilities of components failure.

For example, in the fault tree shown in Fig. 3, if we assume that the events X_i are independent, and have low failure probabilities (rare-event approximation), the fuzzy probability of top event occurrence can be expressed by

$$\widetilde{P}_T(y) = sup_{\{y=p_{A1}+p_{A2}\}} \min\left\{\widetilde{P}_{A_1}(p_{A1}), \widetilde{P}_{A_2}(p_{A2})\right\}$$

where

$$\widetilde{P}_{A1}(y) = sup_{\{y=p_1p_2\}} \min\left\{\widetilde{P}_{X_1}(p_1), \widetilde{P}_{X_2}(p_2)\right\}$$
$$\widetilde{P}_{A2}(y) = sup_{\{y=p_3p_4\}} \min\left\{\widetilde{P}_{X_3}(p_3), \widetilde{P}_{X_4}(p_4)\right\}$$

where $\widetilde{P}_T$ is the fuzzy probability of system failure (top event occurrence), and $\widetilde{P}_{X_i}$ is the fuzzy probability of a component failure.

D. Fuzzy Probabilistic Importance Measure

The methods to evaluate the relative influence of components availability on reliability or availability of the entire system provide useful information about the importance of these elements. Many measures are available in conventional probabilistic approaches [33]–[35]. These measures are based on the evaluation of the contribution of components failure probabilities to the system failure probability. However, probabilistic importance measures are not suitable for the fuzzy approach proposed in this paper, because they are defined for crisp values or probability distributions. Therefore, fuzzy importance measures were introduced by Furuta and Shiraishi [36]. They have proposed a fuzzy importance measure equivalent to structural importance. Liang and Wang [37] proposed a fuzzy importance index based on a ranking method of triangular fuzzy numbers with maximizing and minimizing sets. Guimarees *et al.* [38] proposed a fuzzy importance measure based on the Euclidian distance between two fuzzy sets.

Here, we introduce a fuzzy probabilistic importance measure γ_i defined by [39]

$$\gamma_i = \mathrm{defuz}(\widetilde{\gamma}_i) \tag{1}$$

where defuz is the center of area method of defuzzification used to obtain a crisp value from the fuzzy probability $\widetilde{\gamma}_i$ which is given by

$$\widetilde{\gamma}_i = \widetilde{P} - \widetilde{P}^i \tag{2}$$

where $\widetilde{P}$ is the fuzzy probability of system failure when the component i is available (the failure probability of the component i is equal to 0), and $\widetilde{P}^i$ is the fuzzy probability of system failure when the component i is not available (the failure probability of the component i is equal to 1).

IV. Application Example

A. Process

In order to illustrate the approach proposed in this paper, let us consider a process composed of a pressurized vessel containing volatile flammable liquid. The example process is defined in the technical report ISA-TR84.00.02-2002 [11]. The engineered systems available are the following.

- An independent pressure transmitter to initiate a high pressure alarm and alert the operator to take an appropriate action to stop inflow of material;
- In case the operator fails to respond, a pressure relief valve releases material in the environment and thus reduces the vessel pressure and prevents its failure.

The safety target level for the vessel is: no release to the atmosphere with a frequency of occurrence greater than 10^{-3} in one year. A hazard and operability (HAZOP) analysis was performed to evaluate hazardous events that have the potential to release material in the environment. The results of HAZOP study identify that an overpressure condition could result in a release of flammable material in the environment, and a risk analysis technique indicates that the safety function required to protect against the overpressure condition needs a SIL2.

As a SIS is used to perform the safety target level for the vessel, our goal is to evaluate its $\mathrm{PFD}_{\mathrm{avg}}$, and make certain that this SIS meets the SIL2. The example process with the implemented SIS (see Fig. 4), the schematic SIS configuration (see Fig. 5), and the reliability data (failure probabilities of components which are computed from the failure rates) are defined in the technical report ISA-TR84.00.02-2002 [11]. The error factor values of failure probabilities were chosen between 1.1 and 1.7 which is very realistic according to Kletz [9]. A fuzzy probabilistic fault tree analysis is used to evaluate the SIL of the SIS by determining its $\mathrm{PFD}_{\mathrm{avg}}$. The results will be compared to those obtained by a conventional probabilistic fault tree analysis. Finally, we provide guidance on reducing the SIL uncertainty based on a fuzzy probabilistic importance measure.

B. Uncertainty Fault Tree Analysis

Fault tree analysis consists of two major parts: construction and evaluation. Here, we are only concerned with the evaluation of occurrence probability of fault tree top event. The fault tree model of SIS failure on demand is shown in Fig. 6.

First, we propose to compare fuzzy probabilistic and conventional probabilistic approaches to evaluate the SIS PFD from the components failure probabilities.

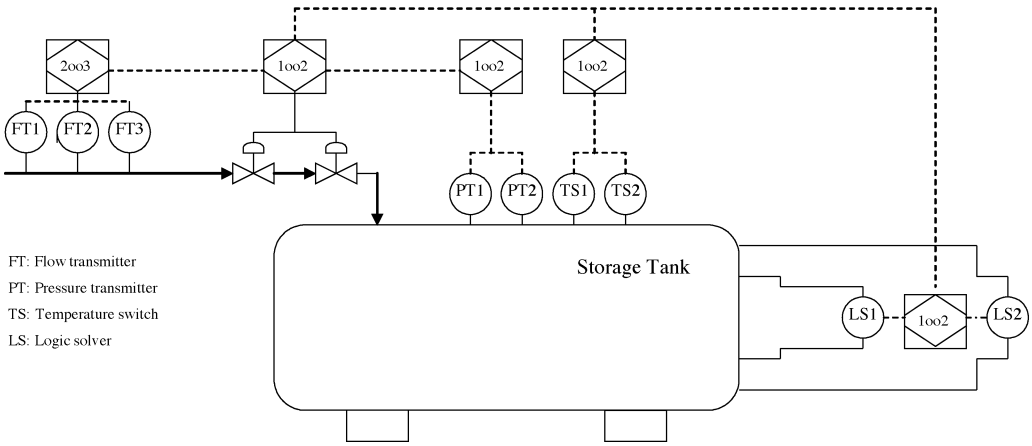

Fig. 4. Process diagram of the example [11].

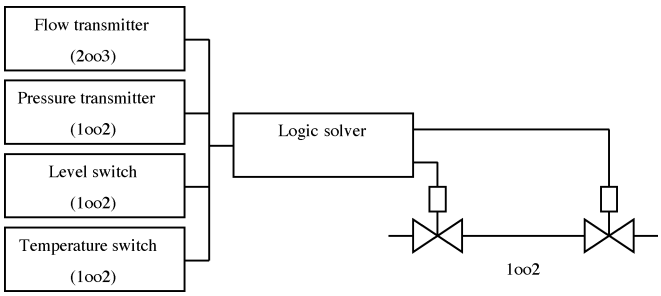

Fig. 5. Schematic SIS configuration of the example [11].

1) Assumptions:

- The basic events of the fault tree are independent.
- The failure probabilities represent the average failure probabilities per year.
- The failure probabilities of SIS components are computed from their failure rates.

2) Fuzzy Probabilistic Approach: In the proposed method, the uncertainty of components failure probabilities is treated by taking fuzzy probabilities. The failure probabilities of SIS components are computed from their failure rates. Fig. 7 provides representation of a fuzzy probability of a component failure. The parameter a_i is the lower bound, the parameter m_i is the modal value, and the parameter b_i is the upper bound for each fuzzy probability of components failure. These parameters are given in Table II. We choose the triangular shapes because of their mathematical simplicity. However, our approach can be applied for any shape (trapezoidal, peak, normal, ...).

In the fault tree shown in Fig. 6, there are 11 minimal cut-sets (cf. Table III). Since basic events have low failure probabilities, we can use the rare-event approximation. Then, we determine the fuzzy probability of the top event occurrence (fuzzy SIS PFD) from the fuzzy probabilities of components failure. Fig. 8 gives the fuzzy probability of the top event occurrence (fuzzy SIS PFD). Table IV gives lower and upper bound values obtained in each α-level.

3) Conventional Probabilistic Approach: The present probabilistic approach to determine the SIS PFD consists in treating the components failure probabilities as random variables represented by a specified distributions (log-normal, normal, log-uniform...). In this paper, the uncertainty of each failure probability will be represented by a log-triangular distribution which is defined by a median m_i and an error factor e_i ($e_i = b_i/m_i = m_i/a_i$) [37] given in Table V. We choose a log-triangular distribution because it is similar to the triangular shape used in the fuzzy probabilistic approach. The log-triangular probability distribution of components failure is shown in Fig. 9. The software FAULT TREE + developed by the ISOGRAPH Company has been used for generating minimal cut-sets and top event failure probability estimation. It uses Monte Carlo sampling simulations to repeatedly sample components failure probabilities from the appropriate distributions, calculate and record the top event failure probability. Fig. 10 gives the frequency distribution of the top event occurrence probability (SIS PFD).

C. Comparison Between the Two Approaches

In order to do a comparison between the fuzzy probabilistic and the conventional probabilistic approaches, we use three measures for each approach.

In the fuzzy probabilistic approach, we use the following measures.

- Modal value: The peak of the fuzzy SIS PFD is called the modal value. This value is the element with the highest confidence in the fuzzy SIS PFD. In this example, the modal value is the 1.4×10^{-2} which corresponds to SIL1;
- Average index: We use the index proposed by Yager [40] which is defined by

$$I(PFD) = \int_0^1 \frac{1}{2} \left(\mathrm{PFD}_L^{\alpha} + \mathrm{PFD}_R^{\alpha}\right) d\alpha \tag{3}$$

  where PFD_L^{α} and PFD_R^{α} represent the left-end-point and the right-end-point of the interval corresponding to the α-level. We choose this index because it is assumed that we have an unbiased approach to making a decision. In this study, the average index is 1.39×10^{-2} which corresponds to SIL1;
- Knowledge interval: The knowledge interval is obtained by the 0-level of the fuzzy SIS PFD. It represents the maximum interval within where a true value may exist. In this

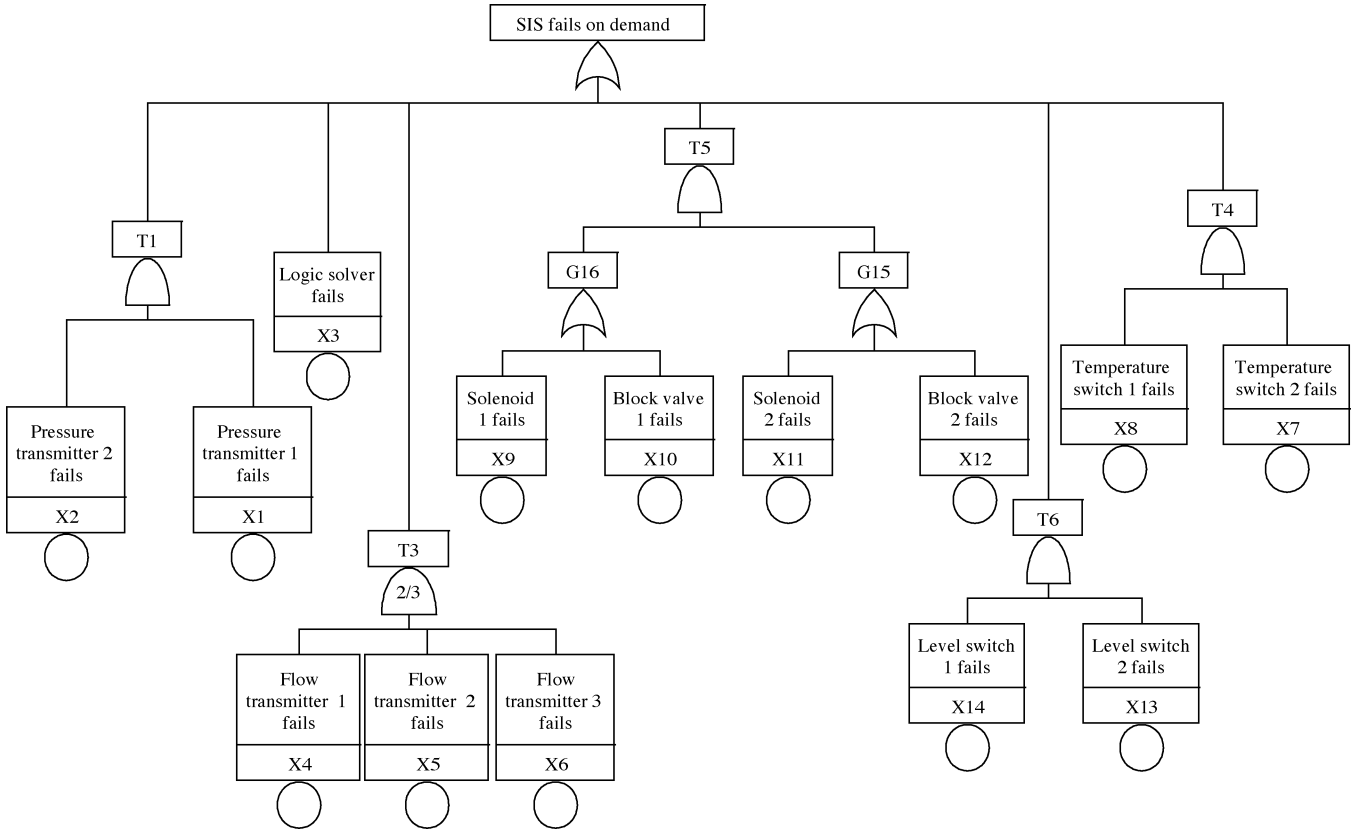

Fig. 6. Fault tree of the example.

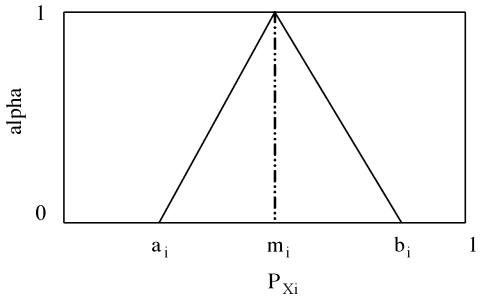

Fig. 7. Fuzzy probability of a component failure.

TABLE II
PARAMETERS OF FUZZY PROBABILITIES

SIS components	$a_i(\times 10^{-2})$	$m_i(\times 10^{-2})$	$b_i(\times 10^{-2})$
X1, X2: Pressure transmitters	2.13	3.2	4.8
X3: Logic solver	0.5	0.6	0.72
X4, X5, X6: Flow transmitters	1.31	1.7	2.21
X9, X11: Solenoids valves	1.65	2.8	4.76
X7, X8: Temperature switches	3.64	4	4.4
X10, X12: Block valves	1.65	2.8	4.76
X13, X14: Level switches	3.07	3.99	5.19

example, the knowledge interval is $[8.62 \times 10^{-3}, 2.42 \times 10^{-2}]$ which falls into SIL1 or SIL2.

In the conventional probabilistic approach, we use the following three measures.

- Median: The median is the value that each result has a 50% probability of exceeding. In this example, frequency $(\mathrm{PFD}_{50\%}) = 1.405 \times 10^{-2}$ which corresponds to SIL1. The modal value in the fuzzy probabilistic approach can be compared to the median value in the conventional probabilistic approach;
- Mean: The mean value is defined by

$$\mathrm{PFD}_{\mathrm{avg}} = \sum_{i=1}^{n} \text{frequency}\,(\mathrm{PFD}_i).\mathrm{PFD}_i = 1.428 \times 10^{-2} \tag{4}$$

where n represents the number of samples of Monte Carlo simulations. The average index in the fuzzy probabilistic approach can be compared to the mean value in the conventional probabilistic approach.
- Maximum and minimum values: These values can be compared to the knowledge interval, and they are given by

TABLE III
FAULT TREE MINIMAL CUT-SETS

Minimal Cut-sets
$C_1 = \{X3\}$
$C_2 = \{X1, X2\}$
$C_3 = \{X10, X11\}$
$C_4 = \{X10, X12\}$
$C_5 = \{X13, X14\}$
$C_6 = \{X4, X5\}$
$C_7 = \{X4, X6\}$
$C_8 = \{X5, X6\}$
$C_9 = \{X7, X8\}$
$C_{10} = \{X9, X11\}$
$C_{11} = \{X9, X12\}$

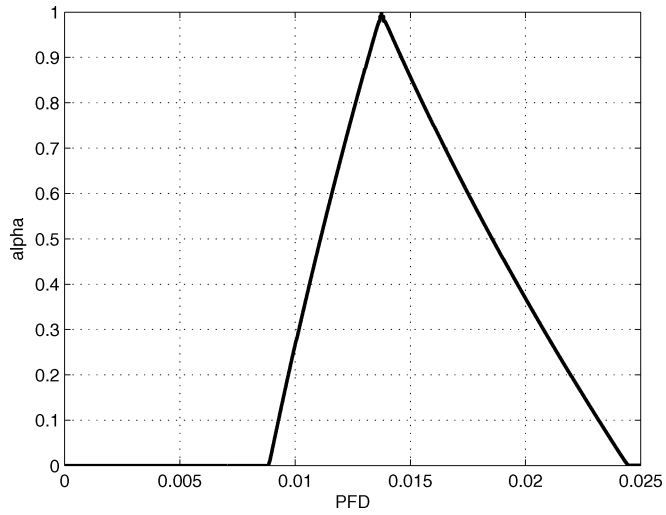

Fig. 8. Fuzzy SIS PFD.

TABLE IV
LOWER AND UPPER BOUND VALUES FOR FUZZY SIS PFD

$\alpha-$level	Lower bound($\times 10^{-2}$)	Upper bound($\times 10^{-2}$)
0	0.862	2.42
0.1	0.914	2.37
0.2	0.972	2.24
0.3	1.03	2.18
0.4	1.11	1.91
0.5	1.17	1.78
0.6	1.23	1.72
0.7	1.26	1.65
0.8	1.32	1.60
0.9	1.36	1.46
1	1.4	1.4

TABLE V
UNCERTAINTY PARAMETERS OF COMPONENTS FAILURE PROBABILITIES

SIS components	$m_i(\times 10^{-2})$	e_i
X1, X2: Pressure transmitters	3.2	1.5
X3: Logic solver	0.6	1.2
X4, X5, X6: Flow transmitters	1.7	1.3
X9, X11: Solenoids valves	2.8	1.7
X7, X8: Temperature switches	4	1.1
X10, X12: Block valves	2.8	1.7
X13, X14: Level switches	3.99	1.3

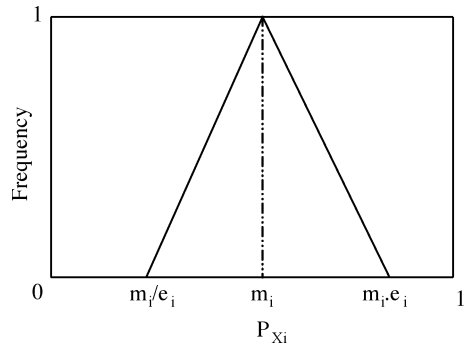

Fig. 9. Frequency probability distribution of a component failure.

— Minimum value $(5\%) = 1.124 \times 10^{-3}$ which corresponds to SIL2;
— Maximum value $(95\%) = 1.589 \times 10^{-2}$ which corresponds to SIL1.

This study shows that the differences between results obtained using either approach with respect to two measures (modal value vs. median and average index vs. mean) are very small, and the SIL obtained in each approach is the same. The width of the support defined by the knowledge interval in the fuzzy approach is higher than the width of the support in the minimum and maximum values in the conventional probabilistic approach. However, in the conventional probabilistic approach the obtained probability values can lie anywhere between 0 and 1.

D. Fuzzy Probabilistic Importance Measures

According to the results above, we have to reduce the uncertainty about determining the SIL of the SIS. That is why, we propose to compute the importance of SIS components. We use the fuzzy probabilistic importance measure γ_i defined in (1). The fuzzy probability $\widetilde{\gamma}_i$ is given by

$$\widetilde{\gamma}_i = \widetilde{\mathrm{PFD}} - \widetilde{\mathrm{PFD}}^{\,i} \tag{5}$$

where $\widetilde{\mathrm{PFD}}$ is the fuzzy SIS PFD when the component i is available (the failure probability of the component i is equal to 0), and $\widetilde{\mathrm{PFD}}^{\,i}$ is the fuzzy SIS PFD when the component i is not available (the failure probability of the component i is equal to 1).

The results of fuzzy probabilistic importance measures calculations for SIS components are summarized in Fig. 11. We note that the most critical component to system failure is related to the logic solver with an importance value of 0.99. The relatively higher value of $\gamma_{\mathrm{LogicSolver}}$ indicates that a small variation in the logic solver configuration causes a relatively greater change in the estimate of the SIS PFD and may be caused a significant change in the SIL of the SIS. These results allow us to make effort on the logic solver configuration to reduce uncertainty.

E. Reducing Uncertainty

We aim to reduce uncertainty about determining the SIL. That's why we modify the SIS configuration. Since, the fuzzy probabilistic importance measures have identified the logic solver as the most critical component in the SIS, we propose to modify the logic solver configuration. We add another logic solver in the SIS in order to evaluate the impact of this change on the SIL uncertainty. Then we have two possible configurations: the $1oo2$ (i.e., the SIS will fail if the two logic solvers fail), and the $2oo2$ (i.e., the SIS will fail if one of the two logic solvers fails). We compute the fuzzy SIS PFD of each SIS configuration (cf. Fig. 12). The $2oo2$ voting configuration is superior to others voting configurations ($1oo1$ and $1oo2$) for reducing the SIL uncertainty. In the $2oo2$ voting configuration, we are certain that the SIL is 1.

The benefit of this method is providing to the decision-maker a good picture of reducing the SIL uncertainty, by modifying the configuration of the most critical components, or trying to reduce the uncertainty about these components reliability parameters. Other considerations, such as components availability, and maintenance policies, could also drive the decision towards reducing the SIL uncertainty and achieving the required SIL.

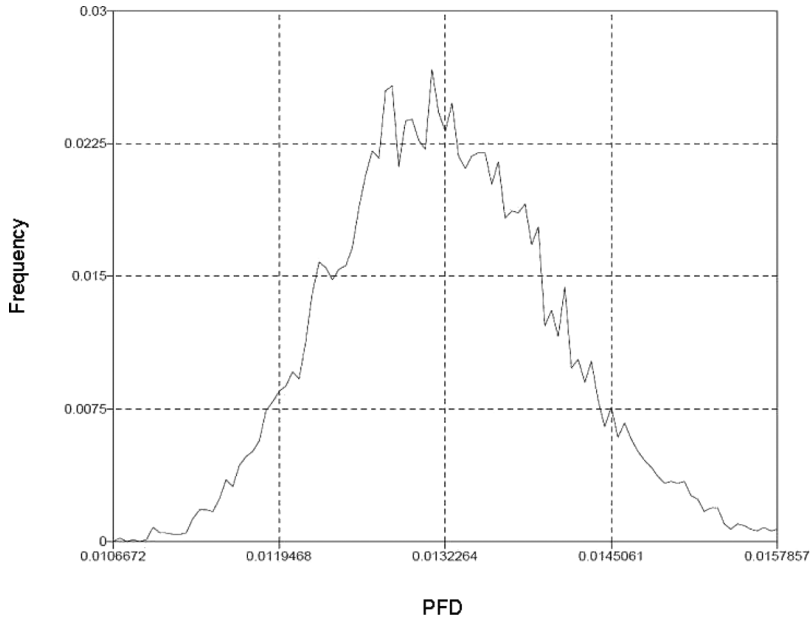

Fig. 10. Frequency probability distribution of SIS PFD.

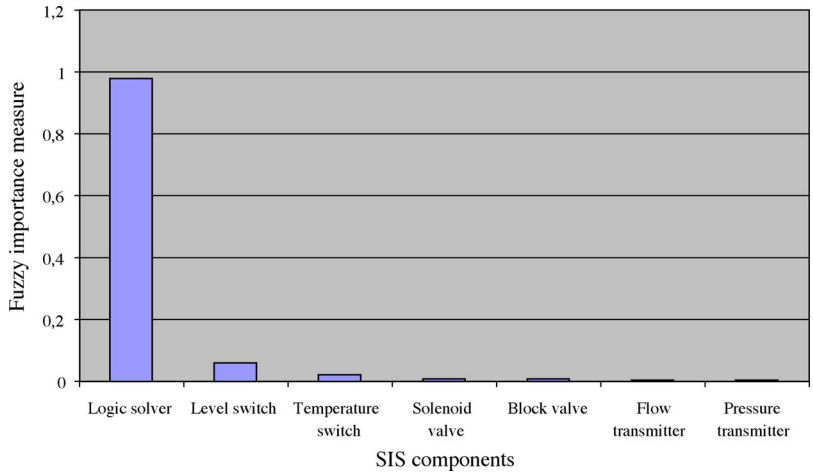

Fig. 11. Fuzzy probabilistic importance measures.

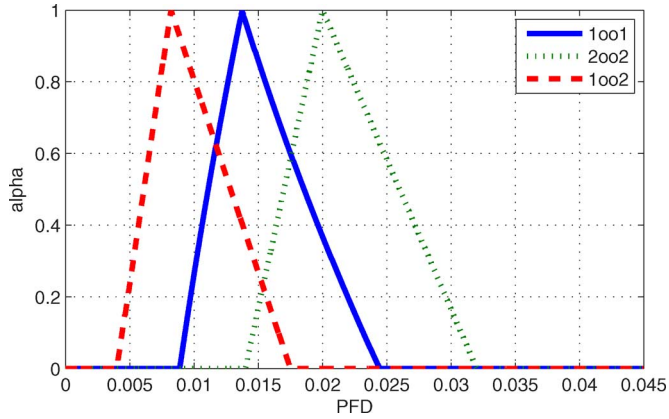

Fig. 12. Fuzzy SIS PFD as a function of SIS configurations.

V. Conclusion

Evaluating the SIL of SISs is crucial to achieve the safety target level of the process. However, the uncertainty of reliability parameters of SIS components is not taken into account in the methods proposed by safety standards [2], [3]. In this paper, we have proposed a fuzzy probabilistic approach to evaluate the SIL of the SIS, when there is an uncertainty about the components failure probabilities. This approach is based on the use of fuzzy probabilities to evaluate the SIS PFD and the SIL of the SIS. To demonstrate the efficiency of our approach, we have applied it to a process example from the technical report ISA-TR84.00.02-2002 [11], and compared it to a conventional probabilistic approach. The results justify the effectiveness of the proposed methodology in evaluating the SIL of the SIS. Moreover, the approach we proposed offers a guidance on reducing the SIL uncertainty based on a fuzzy probabilistic importance measure which is used to identify the SIS critical components. These critical components are then used to modify the SIS configuration for reducing the SIL uncertainty. It is interesting as further research to incorporate the issues of maintenance and repair strategies into the fuzzy probabilistic approach in order to perform the tradeoff between the maintenance cost and the required SIL for the SIS.

REFERENCES

[1] *"Guidelines for Chemical Process Quantitative Risk Analysis,"* 2nd ed. Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE), 2000.

[2] *Application of Safety Instrumented Systems for the Process Control Industry*, ANSI/ISA S84.01-1996, Instrumentation Society of America Std., 1996.

[3] *Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems*, IEC 61508, International Electrotechnical Commission Std., 1998.

[4] W. M. Goble and H. Cheddie, Safety Instrumented Systems Verification: Practical Probabilistic Calculations ISA, 2005.

[5] Y. Wang, H. H. West, and M. S. Mannan, "The impact of data uncertainty in determining safety integrity level," *Process Safety Environ. Protection*, vol. 82, pp. 393–397, 2004.

[6] A. Villemeur*, Reliability, Availability, Maintainability and Safety Assessment: Methods and Techniques.*, A. Cartier and L. M. C. , Eds. New York: Wiley, 1992, T. from French Edition.

[7] S. Hauge, H. Langseth, and T. Onshus*, Reliability Data for Safety Instrumented Systems, PDS Data Handbook*. The Netherlands: SINTEF, 2006.

[8] *Safety Equipment Reliability Handbook*, 2nd ed. Sellersville, PA: Exida, 2005.

[9] T. A. Kletz*, HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards*, 4th ed. New York: Institution of Chemical Engineers, 1999.

[10] *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, IEC 61511, International Electrotechnical Commission Std., 2000.

[11] *Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation techniques*, ISA-TR84.00.02-2002, International Electrotechnical Commission Std., 2002.

[12] A. E. Summers, "Viewpoint on ISA TR84.00.02: Simplified methods and fault tree analysis," *ISA Trans.*, vol. 39, pp. 125–131, 2002.

[13] L. Beckman, "Expanding the applicability of ISA TR84.02 in the field," *ISA Trans.*, vol. 39, pp. 357–361, 2000.

[14] P. Stavrianidis and K. Bhimavarapu, "Safety instrumented functions and safety integrity levels (SIL)," *ISA Transactions*, vol. 37, pp. 337–351, 1998.

[15] *IEEE Guide To The Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipement Reliability Data for Nuclear-Power Generating Station*, IEEE-Std-500, IEEE, 1984.

[16] *"Guidelines for Process Equipment Reliability Data With Data Tables,"* CCPS, 1991, Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE).

[17] *"Offshore Reliability Data Handbook,"* 4th ed. Offshore Reliability Data (OREDA), 2002.

[18] L. Moore, K. Bhimavarapu, and P. Stavrianidis, *"Performance Based Safety Standards: An Integrated Risk Assessment Program,"* Instrumentation Society of America, 1997, Tech. Rep..

[19] H. Tanaka, L. T. Fan, F. S. Lai, and K. Toguchi, "Fault tree analysis by fuzzy probability," *IEEE Trans. Reliab.*, vol. 32, pp. 453–457, 1983.

[20] D. Singer, "A fuzzy set approach to fault tree and reliability analysis," *Fuzzy Sets Syst.*, vol. 34, pp. 145–155, 1990.

[21] K. P. Soman and K. B. Misra, "Fuzzy fault tree analysis using resolution identity," *J. Fuzzy Math.*, vol. 1, pp. 193–212, 1993.

[22] Z. J. Pan and Y. C. Tai, "Variance importance of system components by Monte Carlo," *IEEE Trans. Reliab.*, vol. 37, pp. 521–523, 1998.

[23] H. Z. Huang, X. Tong, and M. J. Zuo, "Posbist fault tree analysis of coherent systems," *Reliab. Eng. Syst. Safety*, vol. 84, pp. 141–148, 2004.

[24] J. Feng and M. D. Wu, "The Profust fault tree and its analysis," *J. Nat. Univ. Defense Tech.*, vol. 23, pp. 85–88, 2001.

[25] C. Lin and M. Wang, "Hybrid fault tree analysis using fuzzy sets," *Reliab. Eng. System Safety*, vol. 58, pp. 205–213, 1997.

[26] F. A. Siontorou, "A theory of independent fuzzy probability for system reliability," *IEEE Trans. Instrum. Meas.*, vol. 53, pp. 301–310, 2003.

[27] M. Sallak, C. Simon, and J.-F. Aubry, "Evaluating safety integrity level in presence of uncertainty," presented at the 4th Int. Conf. on Safety Reliability KONBiN 2006, Krakow, Poland, May 30–Jun. 2 2006.

[28] A. Kaufman and M. M. Gupta*, Introduction to Fuzzy Arithmetic Theory and Application*. New York: Van Nostrand Reinhold, 1991.

[29] H. Kwakernaak, "Fuzzy random variables i," *Inform. Sci.*, vol. 15, p. 129, 1978.

[30] M. L. Puri and D. A. Ralescu, "Fuzzy random variables," *J. Math. Anal. Appl.*, vol. 114, p. 409422, 1986.

[31] H. X. Li and V. C. Yen*, Fuzzy Sets and Fuzzy Decision-Making*. Boca Raton, FL: CRC Press, 1995.

[32] J. Dunyak, "A theory of independent fuzzy probability for system reliability," *IEEE Trans. Fuzzy Syst.*, vol. 7, pp. 286–294, 1999.

[33] Z. W. Birnbaum, "On the importance of different components in a multicomponent system," in *Multivariate Analysis II*, P. R. Krishnaiah, Ed. New York: Academic, 1969.

[34] H. E. Lambert, "Measures of importance of events and cut sets in fault trees," *Reliab. Fault Tree Analysis*, pp. 77–100, 1975.

[35] S. Beeson and J. D. Andrews, "Importance measures for noncoherent system analysis," *IEEE Trans. Reliab.*, vol. 52, pp. 301–310, 2003.

[36] H. Furuta and N. Shiraishi, "Fuzzy importance in fault tree analysis," *Fuzzy Sets and Systems*, vol. 12, pp. 205–213, 1984.

[37] G. Liang and M. Wang, "Fuzzy fault tree analysis using failure possibility," *Microelectron. Reliab.*, vol. 33, pp. 583–597, 1993.

[38] A. C. F. Guimarees and N. F. F. Ebecken, "Fuzzyfta: A fuzzy fault tree system for uncertainty analysis," *Ann. Nucl. Energy*, vol. 26, pp. 523–532, 1999.

[39] M. Sallak, C. Simon, and J.-F. Aubry, "On the use of a new possibilist importance measure to reduce safety integrity level uncertainty," presented at the 4th Int. Conf. on Safety and Reliability KONBiN 2006, Krakow, Poland, May 30–Jun. 2 2006.

[40] R. R. Yager, "A procedure for ordering fuzzy subsets of the unit interval," *Inf. Sci.*, vol. 24, p. 143, 1981.

Mohamed Sallak received the M.S. degree from the Ecole Nationale Superieure d'Electricite et de Mecanique, an engineering high school of the Institut National Polytechnique de Lorraine, in France, in 2003. He is currently working toward the Ph.D. degree in the field of design and dependability assessment of automatic control systems at the Research Center for Automatic Control, Nancy, France.

His research interests include applying fuzzy set theory to evaluate reliability of safety related systems under uncertainty.

Christophe Simon received the M.S. degree in metrology, control systems, and electrotechnic and the Ph.D. degree both from the University Henri Poincari—Nancy 1, France, in 1991 and 1996, respectively.

In 1999, he joined the Department of Quality, Industrial Logistic and Organization, IUT Epinal, University of Nancy 2, France, as an Assistant Professor, where, since 2002, he has been Head of the department. In 1992, he joined the Research Center for Automatic Control, Nancy, France. His research area concerns reliability and systems safety, pattern recognition, fuzzy logic, possibility theory and evidence theory.

Dr. Simon is a member of French Association of Electrical, Electronic and System Control Association (Club EEA).

Jean-Francois Aubry is a Full Professor at the Ecole Nationale Superieure d'Electricite et de Mecanique, an engineering high school of the Institut National Polytechnique de Lorraine, Lorraine, France, where he is in charge of discrete event systems and reliability, availability, maintainability, and safety courses. He is also a Research Director at the Research Centre for Automatic Control (CRAN), a CNRS labeled laboratory, where he works especially on the design and dependability assessment of automatic control systems and particularly safety instrumented systems. Since 1998, he has also been the Head of the "Institut de Surete Industrielle" (a federative institute of the four Universities in Lorraine) for research and training in the field of quality, safety, dependability, and environmental impact of industrial activity.