Evaluating Safety Integrity Level in presence of uncertainty

Mohamed Sallak, Christophe Simon, Jean-François Aubry

Evaluating Safety Integrity Level in presence of uncertainty

M. Sallak[a], C. Simon[b], J-F. Aubry[a]

[a]INPL-CRAN UMR 7039,
2, Avenue de la Forêt de Haye,
54506, Vandoeuvre-Les-Nancy, France
mohamed.sallak@ensem.inpl-nancy.fr
jean-francois.aubry@isi.u-nancy.fr

[b]UHP-CRAN UMR 7039,
2, Rue Jean Lamour,
54519, Vandoeuvre-Les-Nancy, France
christophe.simon@esstin.uhp-nancy.fr

Abstract: The safety standards ANSI/ISA S84.01-1996 and IEC 61508 address the application of Safety Instrumented Systems (SIS) to take a process to a safe state when predetermined conditions are violated. A critical aspect of conformance with the standards is the establishment of Safety Integrity Level (SIL) for SIS. This paper presents a fuzzy/possibilist approach for determining the SIL of the SIS in presence of uncertainty.

Key words: ANSI/ISA S84.01-1996; IEC 61508; Safety Instrumented Systems (SIS); Safety Integrity Level (SIL); Fuzzy/Possibilist approach.

1. Introduction

The process industry is obligated to provide and maintain a safe, working environment for their employees. Safety is provided through various safeguards, such as Safety Instrumented Systems (SIS), procedures and training. The SIS consists of instrumentation that is implemented for the purpose of mitigating a risk or bringing the process to a safe state in the event of a process failure. The

ANSI/ISA S84.01-1996 [1] and IEC 61508 [2] 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 of the SIS. Thus, determining SIL for a SIS and its validation is very important for compliance with the ANSI/ISA S84.01-1996 [1] and IEC 61508 [2] standards. The SIL of a SIS is defined by its probability to fail on demand (PFD). There are several probabilistic techniques that can be used to evaluate the SIS PFD (SIS probability to fail on demand) from the reliability parameters of its components ([2], [3], [4]). These reliability parameters have to be estimated based on a large amount of data. However, for SIS it is usually difficult to obtain a sufficient quantity of data due to rare events of SIS components failures. In this case, probabilistic approaches evaluate the failure probabilities of these systems by giving the confidence intervals and errors factors using Monte Carlo simulations ([5], [6]). But, for large systems, this approach is time consuming. Moreover, when we assume probability distributions for both components and SIS failure probabilities, we are introducing an unpredictable uncertainty. Therefore, the probabilistic approaches do not help us very much. Furthermore, the evaluation of the SIL of the SIS rarely considers the uncertainty in the reliability parameters estimation. For reliability researchers, this remains an under-developed research area. Wang et al. [7] discussed the impact of data uncertainty in determining the SIL level. However, they do not propose a methodology to treat this problem.

The purpose of this paper is to present a fuzzy/possibilist approach to determine the SIL of the SIS, when the components failure probabilities are difficult to be precisely estimated. This approach is based on the use of possibility distributions for representing the uncertainty of the SIS components failure probabilities and α-cut method for evaluating the possibility distribution of the SIS PFD and the SIL of the SIS.

2. Determining SIL via a fuzzy/possibilist fault tree analysis

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 average probability to fail on demand (*PFDavg*) over a given time period (cf. Table 1).

Solicitation	Low Demand	High Demand
SIL	PFDavg	Failures/hour
4	$10^{-5} \leq PFDavg \leq 10^{-4}$	$10^{-9} \leq N \leq 10^{-8}$
3	$10^{-4} \leq PFDavg \leq 10^{-3}$	$10^{-8} \leq N \leq 10^{-7}$
2	$10^{-3} \leq PFDavg \leq 10^{-2}$	$10^{-7} \leq N \leq 10^{-6}$
1	$10^{-2} \leq PFDavg \leq 10^{-1}$	$10^{-6} \leq N \leq 10^{-5}$

Table 1. Definition of SIL from IEC 61508

For determining SIL, the technical report ISA-TR84.00.02-2002 [3] 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. Nevertheless, the probabilities of basic events are considered as crisp ones. It is apparently not consistent with practical situations. Because, only by a large amount of tests can these crisp probabilities be concluded. This is not feasible for SIS due to rare events of component failures, and even so, these data are approximate in some degree. Moreover, the failure probabilities are different for different operators and working conditions. Therefore, a reliability analysis method based on fuzzy sets is interesting. The pioneering work on fuzzy fault tree analysis belongs to Tanaka et al. [8]. They treated basic events probabilities as trapezoidal fuzzy numbers and compute the distribution of top event occurrence probability. Other results on fuzzy FTA are reported in [9]. Our goal is to evaluate the reliability of a SIS in presence of uncertainty. So, we investigate the use of both fuzzy sets and possibility theory.

2.1. Fuzzy sets

A fuzzy set initiated by Zadeh [10] is defined as follows:

Definition 1 Let *X be a universal set. Then a fuzzy subset Ã of X is defined by its membership function* $\mu_{\tilde{A}} : X \rightarrow [0,1]$

Which assigns to each element $x \in X$, *a real number* $\mu_{\tilde{A}}(x)$ *in the interval* [0,1], *where the value of* $\mu_{\tilde{A}}(x)$ *at x represents the grade of membership of x in Ã.*

Definition 2 Let *X be a Cartesian product of universes* $X_1, X_2, ...X_r$, *and* $\tilde{A}_1, \tilde{A}_2, ...\tilde{A}_r$ *be r fuzzy sets in* $X_1, X_2, ...X_r$, *respectively. f is a mapping from X to a universe Y. Then, the extension principle allows us to define a fuzzy set* in $\tilde{B}$ *in Y by:*

$$\tilde{B} = \{(y, \mu_{\tilde{B}}(y)) / y = f(x_1, x_2, ...x_r), (x_1, x_2, ...x_r) \in X\}$$

Where:

$$\mu_{\tilde{B}}(y) = \begin{cases} \sup_{(x_1,...,x_r) \in f^{-1}(y)} \min\{\mu_{\tilde{B}}(x_1), ..., \mu_{\tilde{B}}(x_r)\} & if \quad f^{-1}(y) \neq 0 \\ 0 \qquad otherwise. \end{cases}$$

Definition 3 Let *x be a continuous variable restricted to a distribution function* $\mu(x) \in [0,1]$ *which satisfy the following assumptions:*

- *μ(x) is a piecewise continuous;*
- *μ(x) is a convex fuzzy set;*
- *μ(x) is a normal fuzzy set.*

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

The operation implied in the extension principle requires extensive computation. From the previous studies made by Kaufman and Gupta [11], 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. For any fuzzy number

$\tilde{A}$ which has the membership function $\mu_{\tilde{A}}(x)$, an interval bounded by two points at each α-level (0≤α≤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 $\mu_{\tilde{A}}(x)$ left-end-point and the right end-point of this interval. As it is shown in Fig. 1, we can express a fuzzy number $\tilde{A}$, using the following form:

$$\tilde{A} \to [A_L^{(\alpha)}, A_R^{(\alpha)}], \quad 0 \le \alpha \le 1$$

Arithmetic operations on two fuzzy numbers $\tilde{A}$ and $\tilde{B}$ provide the following expressions:

$$\tilde{C} = \tilde{A} + \tilde{B} \to [C_L^{(\alpha)}, C_R^{(\alpha)}] = [A_L^{(\alpha)} + B_L^{(\alpha)}, A_R^{(\alpha)} + B_R^{(\alpha)}]$$

$$\tilde{C} = \tilde{A} - \tilde{B} \to [C_L^{(\alpha)}, C_R^{(\alpha)}] = [A_L^{(\alpha)} - B_L^{(\alpha)}, A_R^{(\alpha)} - B_R^{(\alpha)}]$$

$$\tilde{C} = \tilde{A}.\tilde{B} \to [C_L^{(\alpha)}, C_R^{(\alpha)}] = [\min(A_L^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_L^{(\alpha)}, A_L^{(\alpha)}.B_R^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)}), \max(A_L^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_L^{(\alpha)}, A_L^{(\alpha)}.B_R^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)})]$$

2.2. Fuzzy probabilities

In conventional fault tree analysis, the failure probabilities of system components are treated as crisp values. However, it is often difficult to evaluate the components failure probabilities from past occurrence. Instead of the probability of failure, we propose the fuzzy probability of failure. By resorting to this concept, we can allocate a degree of uncertainty to each value of the failure probability.

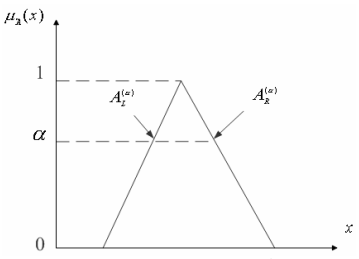

Fig.1. Bounds points of $\mu_{\tilde{A}}(x)$

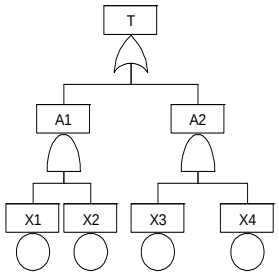

Fig.2. Fault tree example

Definition 4 A *fuzzy probability, i.e. a fuzzy set defined in probability space, represents a fuzzy number between 0 and 1 assigned to the probability of an event.*

One can choose depending upon the suitability different types of membership function for fuzzy probability; the more confident portion is given the value 1 and other portions are given values between [0,1].

2.3. Possibility theory

Possibility theory is an information theory which is related to both fuzzy sets and probability theory. Technically, a possibility distribution is a fuzzy set. In particular, all fuzzy numbers and fuzzy probabilities are possibility distributions [12].

Definition 5 A *possibility distribution π(.) on Ω is a mapping from the reference set Ω into the unit-interval,*

$$\pi : \Omega \to [0,1].$$

The possibility distribution is described in terms of a possibility measure by: $\pi(x) = \Pi(\{x\})$,

where the possibility of some event A is defined by: $\Pi(A) = \sup_{x \in A} \pi(\{x\})$. The possibility measure is a coefficient ranging between 0 and 1 which evaluates how possible the event is. The value 1 means that the event is completely possible; the value 0 means that the event is impossible.

2.4. Fuzzy/possibilist fault tree analysis

In this paper, the fault tree analysis is based on possibility theory. So, we can allocate a degree of uncertainty to each value of the failure probability. The possibility of system failure probability is determined from the possibility of components failure probabilities. For example, in fault tree shown in Fig. 2, if we assume that the events *Xi* are independent, and have low failure probabilities (rare-event approximation), the possibility distribution of top event occurrence probability can be expressed by: $\pi_{P_T} = \pi_{P_{A_1}} + \pi_{P_{A_2}}$

where: $\pi_{P_{A_1}} = \pi_{P_{X_1}} . \pi_{P_{X_2}}$; $\pi_{P_{A_2}} = \pi_{P_{X_3}} . \pi_{P_{X_4}}$.

3. Application example

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 safety target level for the vessel is: no release to the atmosphere with a frequency of occurrence greater than 10^{-4} in one year. A SIS is used to perform the safety target level for the vessel. The example process and the SIS are defined in ISA-TR84.00.02-2002 [3] (see Fig. 3).

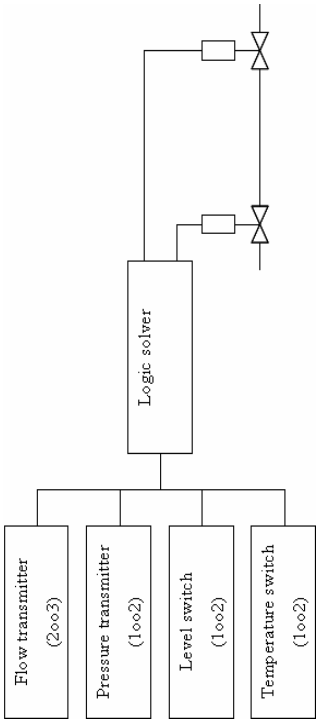

Fig.3. Schematic SIS configuration

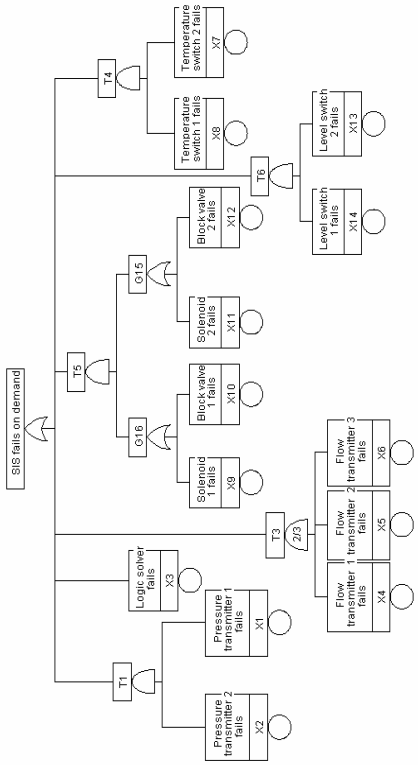

Fig. 4. Fault tree for SIS example

A fuzzy/possibilist fault tree analysis is used to evaluate the SIL of the SIS by determining its PFD. The fault tree of SIS PFD (SIS probability to fail on demand) is shown in Fig. 4. Furthermore, we assume that:

- The basic events of the fault tree are independent;
- The SIS components can not be repaired;
- The failure probabilities represent the average failure probabilities on demand over a period test interval.

Here, the uncertainty of components failure probabilities is treated by taking fuzzy probabilities. 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 possibility distribution of the components failure probabilities. These parameters are given in Table 2. The possibility distribution of the SIS PFD can be expressed using the fault tree minimal cut sets *{T*1, *T*2, *T*3, *T*4, *T*5, *T*6*}* (cf. Fig. 4). Since basic events have low failure probabilities, we can use the rare-event approximation. Then the possibility of the top event occurrence probability is given by:

$$\pi_{PFD_{SIS}} = \pi_{P_{T_1}} + \pi_{P_{T_2}} + \pi_{P_{T_3}} + \pi_{P_{T_4}} + \pi_{P_{T_5}} + \pi_{P_{T_6}}$$

$\pi_{P_{T_i}}$ is the possibility distribution of a minimal cut set occurrence probability, and $\pi_{PFD_{SIS}}$ is the possibility distribution of the SIS PFD. The possibility distributions of the minimal cut sets occurrence probabilities are given by:

$$\pi_{P_{T_1}} = \pi_{P_{X_1}} . \pi_{P_{X\,2}} ; \pi_{P_{T_2}} = \pi_{P_{X_3}} ;$$

$$\pi_{P_{T_3}} = \pi_{P_{X_4}} . \pi_{P_{X_5}} + \pi_{P_{X_4}} . \pi_{P_{X_6}} + \pi_{P_{X_5}} . \pi_{P_{X_6}} ; \pi_{P_{T_6}} = \pi_{P_{X_{13}}} . \pi_{P_{X_{14}}}$$

$$\pi_{P_{T_4}} = \pi_{P_{X_7}} . \pi_{P_{X_8}} ; \pi_{P_{T_5}} = (\pi_{P_{X_9}} + \pi_{P_{X_{10}}})(\pi_{P_{X_{11}}} + \pi_{P_{X_{12}}})$$

$\pi_{P_{X_i}}$ is the possibility distribution of a component failure probability. Using α-cut method and arithmetic operations defined in the previous section, we determine the possibility distribution of

top event occurrence probability (SIS PFD) from the possibility distributions of components failure probabilities. Fig. 5 gives the possibility distribution of the top event occurrence probability. One can see that the total range of the top event occurrence probability (SIS PFD) is from 7.4×10^{-3} to 2.22×10^{-2}, which falls into SIL1(PFD $\in [10^{-2}, 10^{-1}]$) or SIL2(PFD $\in [10^{-3}, 10^{-2}]$).

SIS components	a_i	m_i	b_i
X1, X2: Pressure transmitters	0.01	0.032	0.0492
X3: Logic solver	0.005	0.006	0.0061
X4, X5, X6: Flow transmitters	0.0126	0.017	0.0211
X9, X11: Solenoids valves	0.01	0.028	0.0311
X7, X8: Temperature switches	0.0326	0.04	0.0403
X10, X12: Block valves	0.01	0.028	0.0311
X13, X14: Level switches	0.0199	0.039	0.049

Table 2. Parameters of possibility distributions

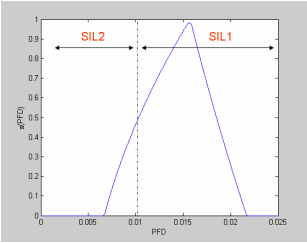

Fig. 5. Possibility distribution of SIS PFD

Conclusion

In this paper, we have proposed a fuzzy/possibilist approach for evaluating the SIL of the SIS, when there is an uncertainty about the components failures probabilities. To demonstrate the efficacy of our approach, we have applied it to a process example from the literature [3]. The results justify not only the effectiveness of the proposed methodology in evaluating the SIL of the SIS, but furthermore its computational efficiency as well. In a second paper [13], we propose a methodology to reduce the SIL uncertainty of the SIS.

References

[1] ANSI/ISA-S84.01-1996. *Application of Safety Instrumented Systems for the process control industry*. Instrumentation Society of America (ISA), 1996.

[2] IEC 61508. *Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems*. International Electrotechnical Commission (IEC), 1998.

[3] ISA-TR84.00.02-2002. *Safety Instrumented Functions (SIF), Safety Integrity Level (SIL), Evaluation Techniques*. Instrumentation Society of America (ISA), 2002.

[4] Beckman L. Expanding the applicability of ISA TR84.02 in the field. *ISA Transactions*, 39:357-361, 2000.

[5] Suresh P.V, Babar A.K, Venkat Raj V. Uncertainty in fault tree analysis: a fuzzy approach. *Fuzzy Sets and Systems*, 83:205-213, 1996.

[6] Page L.B, Perry J.E. Standard deviation as an alternative to fuzziness in fault tree models. *IEEE Transactions on Reliability*, 43:402-407, 1994.

[7] Wang Y, West H. H, Mannan M. S. The impact of data uncertainty in determining Safety Integrity Level. *Process Safety and Environmental Protection*, 82:393-397, 2004.

[8] Tanaka H, Fan L. T, Lai F. S, Toguchi K. Fault tree analysis by fuzzy probability. *IEEE Transactions on Reliability*, 32:453-457, 1983.

[9] Soman K.P, Misra K.B. Fuzzy fault tree analysis using resolution identity. *The Journal of Fuzzy Mathematics*, 1:193-212, 1993.

[10] Zadeh L. Fuzzy sets. *Information and Control*, 8:338-353, 1965.

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

[12] Dubois D, Prade H. Possibility theory, probability theory and multiple-valued logics: A clarification. *Annals of Mathematics and Artificial Intelligence*, 32:35-66, 2001.

[13] Sallak M, Simon C, Aubry J-F. On the use of a new possibilist importance measure to reduce Safety Integrity Level uncertainty. *The 4th International Conference on Safety and Reliability, KONBiN' 06*, Poland, 2006.