On the use of a new possibilist importance measure to reduce Safety Integrity Level uncertainty

Mohamed Sallak, Christophe Simon, Jean-François Aubry

On the use of a new possibilist importance measure to reduce Safety Integrity Level 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: Safety Instrumented Systems (SIS) play a key role in process industry to achieve safety. One of the most important criteria for SIS design is the requirement that the user assigns and verify Safety Integrity Level (SIL) of SIS. This paper proposes a new possibilist importance measure to reduce the SIL uncertainty when the SIS components failure probabilities are uncertain.

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

1. Introduction

Safety Instrumented Systems (SIS) play a key role in process industry to achieve safety. The ANSI/ISA S84.01-1996 [1] and IEC 61508 [2] safety standards are intended to address the application of SIS for the process industries. One of the most important criteria for SIS design is the requirement that the user assigns and verify Safety Integrity Level (SIL) of SIS. However, the uncertainty associated with the SIS components reliability

parameters must be considered in the evaluation of the SIL. 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], [5], [6]). 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. 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 and al. [7] discussed the impact of data uncertainty in determining the SIL level. 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 SIL level in these cases.

The goal of this paper is to propose a new possibilist importance measure to reduce the SIL uncertainty, when the components failure probabilities are difficult to be precisely estimated. The evaluation of the SIL is done by a fuzzy/ possibilist fault tree analysis [8].

2. Procedure to achieve the safety target level of the process

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

2.2. 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:

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 $\leq 10^{-1}$	$10^{-6} \leq N \leq 10^{-5}$

Table1. Definition of SIL from IEC 61508

- 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 below the safety target level.

3. Determining SIL [8]

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 according to the extension principle and the use of α-cut method [8].

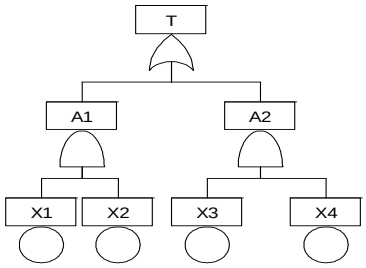

Fig.1. Fault tree example

For example, in fault tree shown in Fig. 1, 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: $\pi_{P_{A_1}} = \pi_{P_{X_1}} . \pi_{P_{X_2}}$; $\pi_{P_{A_2}} = \pi_{P_{X_3}} . \pi_{P_{X_4}}$.

For more details about the fuzzy/possibilist fault tree analysis, see our publication [8].

4. Possibilist importance measure

The methods for evaluating the relative influence of components reliability on the reliability of the entire system provide useful information about the importance of these elements. Many measures are available in probabilistic approach ([9], [10], [11]). These measures are based on the evaluation of the contribution of components failure probabilities to the system failure probability. However, the probabilistic measures are not suitable in uncertainty fault tree analysis because they are defined for crisp values of probabilities. Therefore, fuzzy importance measures were introduced by Furuta and Shiraishi [12]. They have proposed a fuzzy importance measure equivalent to structural importance. Liang and Wang [13] proposed a fuzzy importance index based on a ranking method of triangular fuzzy numbers. Suresh et al. [14] introduced a fuzzy importance measures based on the Euclidian distance between two fuzzy sets.

Here, we introduce a new possibilist importance measure ξ_i, based on α-cut method and arithmetic fuzzy operations, and defined by:

$$\xi_i = defuz(\tilde{\xi}_i)$$

where *defuz* is the centre of area method of defuzziffication used to obtain a crisp value from the possibility distribution $\tilde{\xi}_i$ defined by:

$$\tilde{\xi}_i = \pi_P - \pi_{P_{Pi=cte}}$$

where π_P is the possibility distribution of the system failure probability, and $\pi_{P_{Pi=cte}}$ is the possibility distribution of the system failure probability when the failure probability of component *i* is a crisp value (there is no uncertainty about its value, i.e $P_{X_i} = m_i$ where m_i is the modal value of the possibiity distribution $\pi_{P_{Xi}}$).

5. Application

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 [4] (see Fig. 2). A fuzzy/possibilist fault tree analysis is used to evaluate the SIL of the SIS by determining its PFD [8]. Our goal is to help reducing the SIL uncertainty of the SIS. The fault tree of SIS PFD (SIS probability to fail on demand) is shown in Fig. 3. 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.

4.1. Fuzzy/possibilist approach [8]

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).

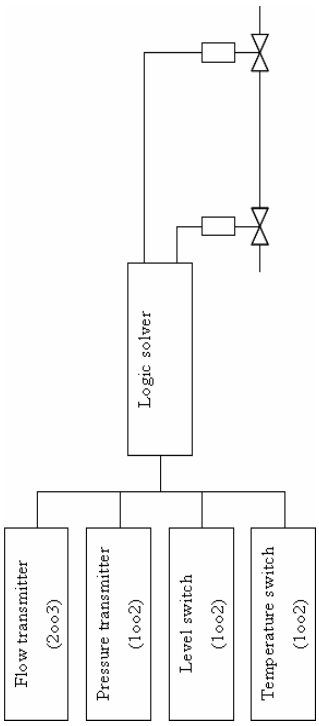

Fig.2. Schematic SIS configuration

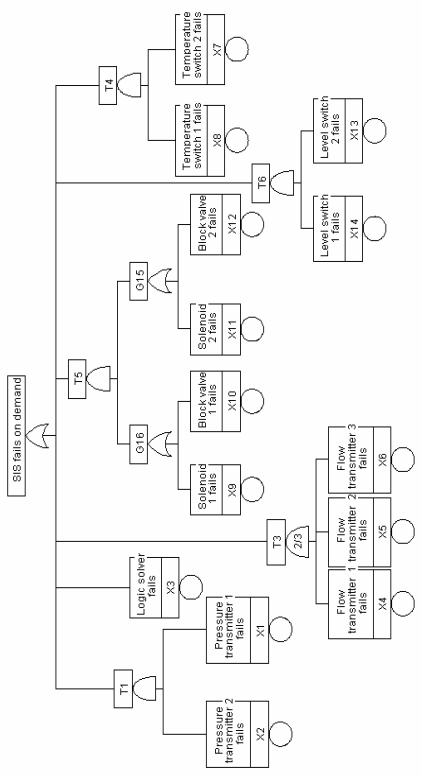

Fig.3. Fault tree for SIS example

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. Then, we determine the possibility distribution of top event occurrence probability (SIS PFD) from the possibility distributions of components failure probabilities [8].

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

Table2. Parameters of possibility distributions

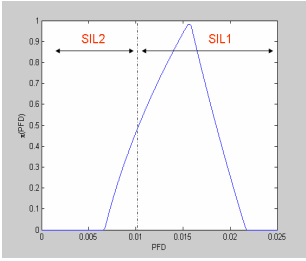

Fig.4. Possibility distribution of SIS PFD

Fig. 4 gives the possibility distribution of the top event occurrence probability. One can see that the total range of the top event occurrence probability is from 7.4×10^{-3} to 2.23×10^{-2}, which falls into SIL1(PFD $\in [10^{-2}, 10^{-1}]$) or SIL2(PFD $\in [10^{-3}, 10^{-2}]$). Therefore, there is an uncertainty about the SIL (1 or 2). To help reducing this uncertainty, we propose to use a new possibilist importance measure.

4.2. Possibilist importance measure

The results of possibilist importance measure calculation for SIS components are summarized in Table 3. We note that the most critical component to system failure is related to Temperature switches with an importance value of 0.045. This means that the Temperature switches is the most important component for the SIL uncertainty. To reduce this uncertainty, we propose to reduce the uncertainty of the Temperature switches failure probabilities (we assume that there is no uncertainty about Temperature switches failure probabilities, i.e $P_{X_{13}} = P_{X_{14}} = 0.04$).

SIS components	ζ_i	*Rank*
Pressure transmitters	0.038	5
Logic solver	0.039	2
Flow transmitters	0.006	7
Solenoids valves	0.039	2
Temperature switches	0.045	1
Block valves	0.039	2
Level switches	0.039	2

Table3. Possibilist importance measures

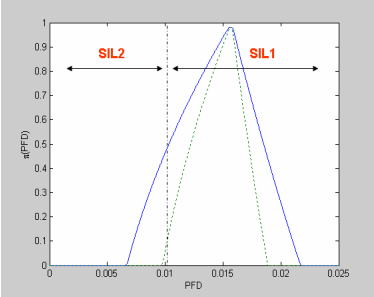

Fig.5. Possibility distribution of SIS PFD before and after reducing uncertainty

Fig. 5 shows the possibility distribution of the PFD of the SIS before (the continuous line) and after (the dashed line) reducing the uncertainty of the Temperature switches failure probabilities. We note that the SIL uncertainty is reduced efficiency after this operation.

5. Conclusion

In this paper, we offer guidance on reducing the SIL uncertainty based on a new possibilist importance measure. To demonstrate the efficacy of our measure, we have applied it to a process example from the literature [4].

The results suggest a number of ways for further investigation. One potentially important is to propose other fuzzy/possibilist measures to help reducing the SIL uncertainty, and compared them to the possibilist importance measure proposed in this paper.

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] IEC 61511. *Functional safety: Safety Instrumented Systems for the process industry sector*. International Electrotechnical Commission (IEC), 2000.

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

[5] Summers A. E. Viewpoint on ISA TR84.0.02 : simplified methods and fault tree analysis. *ISA Transactions*, 39:125-131, 2002.

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

[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] Sallak M, Simon C, Aubry J-F. Evaluating Safety Integrity Level in presence of uncertainty. *The 4th International Conference on Safety and Reliability, KONBiN' 06, Poland, 2006.*

[9] Birnbaum Z. W. On the importance of different components in a multicomponent system. In *Multivariate Analysis II*. P. R. Krishnaiah, Ed, N. Y:Academic, 1969.

[10] Lambert H. E. Measures of importance of events and cut sets in fault trees. *Reliability and Fault Tree Analysis*, pages 77-100, 1975.

[11] Barlow B. E, Proshan F. *Importance of system components and fault tree analysis*. Operations Research Center, Univ. of California, Berkeley, 1973.

[12] Furuta H, Shiraishi N. Fuzzy importance in fault tree analysis. *Fuzzy Sets and Systems*, 12:205-213, 1984.

[13] Liang G.S, Wang M.J.J. Fuzzy fault tree analysis using failure possibility. *Microelectronics and Reliability*, 33:583-597, 1993.

[14] 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.