BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXVIII No. 2/2016	41 – 46	Seria Tehnică

Establishing Safety Integrity Level of a Safety Instrumented System using Risk Graph Method

Alina-Simona Băieşu

Petroleum and Gas University of Ploiesti, B-dul Bucuresti, Nr. 39, Ploiesti
e-mail: agutu@upg-ploiesti.ro

Abstract

Safety Instrumented Systems (SIS) have become increasingly important because of the dangerous substances handled in the industrial units requiring special reliable protection systems. Any SIS is characterized by an integrity level named Safety Integrity Level (SIL). Risk Graph is a qualitative method that can be used to determine the integrity level SIL that needs to be imposed to a SIS. This method takes into account the possible consequences of a dangerous event, the occupancy frequency of the dangerous affected area, the likelihood that an unwanted event to appear but also the probability that the personnel to avoid the danger. The consequences of the unwanted event can be from minor injuries to many deaths, the occupancy frequency can be from rarely to continuous, the probability to avoid the consequences can be from possible to almost impossible and the likelihood can be from very unlikely to a relatively high probability that the unwanted event to appear. Choosing a value for each Risk Graph parameter a Safety Integrity Level (SIL) results. This SIL must be accomplished by the Safety Instrumented System (SIS).

Key words: *Risk Graph, Safety Integrity Level (SIL), Safety Instrumented Systems (SIS).*

Introduction

Because of the hazardous substances that are handled in the industrial processes and the need to mitigate or eliminate their dangerous potential, appeared and developed systems that have as goal the safety and protection of these industrial processes, of the operating personnel or of the environment. These systems are referred as Safety Instrumented Systems (SIS).

A SIS contains three types of elements [9]:

- sensors – that are used to give a measure of some process parameter values. These parameters (such pressures, temperatures, etc.) are considered potentially dangerous for the process. The value of these parameters are used to determine whether a device or process is in a safe or unsafe state. The sensors can be simple switches, pneumatic or electric, or sensors with intelligent diagnostics.
- logic solvers – that are designed to give the decision that should be made based on the sensors information. In most cases the logic solver is a Programmable Logic Controller (PLC).
- final elements – are usually two states open / close (on / off) valves, operated pneumatically that carry out the command from the logic solver.

In Figure 1 is presented a Safety Instrumented System (SIS).

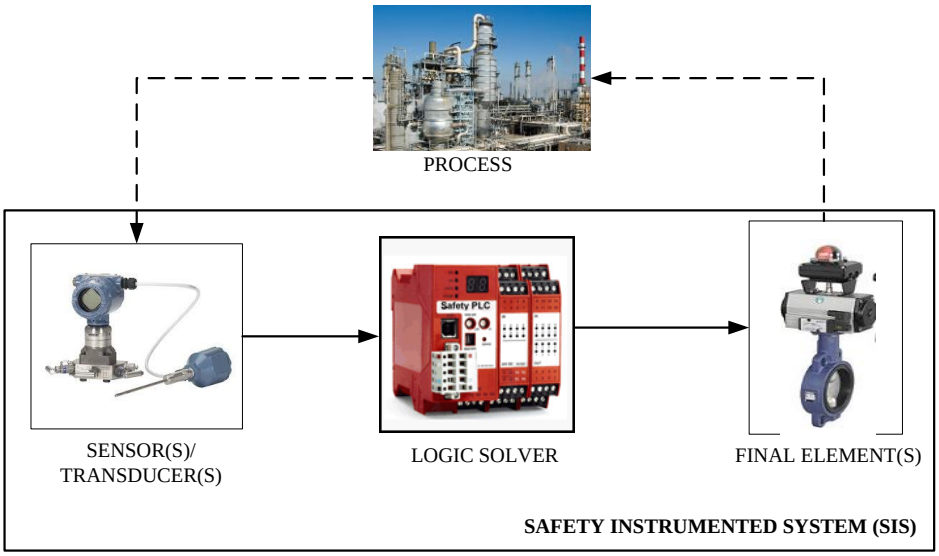

Fig. 1. The structure of an industrial Safety Instrumented System (SIS) [10]

A function that is implemented by a Safety Instrumented System (SIS) is named Safety Instrumented Function (SIF). A SIF is designed to bring and to maintain the process in a safe state when a hazardous dangerous event appears, as often happens in automated industrial processes [6, 8]. This Safety Instrumented Function (SIF) gives with automat action a predefined level of risk reduction [7].

An example of such a SIF is the protection in case of a high temperature in a heater (fig. 3) that can lead to an explosion. This event can be avoided using a temperature sensor and a PLC that actuates a shutdown valve closing the heater inlet (steam flow) when the temperature exceeds the preset temperature value.

Each Safety Instrumented Function (SIF) must have a specified Safety Integrity Level (SIL) that is a statistical representation of the integrity of the SIF [5].

SIL is a measure of the safety system performance and represents a number of quantitative and qualitative constraints imposed to the SIS. Depending on the process risk level, IEC 61508 defines four SIL levels denoted SIL 1, 2, 3 and 4. In general, a higher risk level requires a higher SIL level and the number that accompanies SIL increases as value [2].

In other words, the higher SIL is, the higher is the probability that the required SIF to be carried out successfully.

There are several tools for establishing the Safety Integrity Level (SIL) that needs to be imposed to a Safety Instrumented System (SIS): quantitative and semi-quantitative methods (e.g. Layer Of Protection Analysis - LOPA), qualitative methods (e.g. risk matrix, risk graph) and semi-qualitative methods (e.g. calibrated risk graph) [4].

In this paper Risk Graph method is described. This method is a qualitative way to obtain the necessary SIL that needs to be imposed to a SIS.

Risk Graph Method

Using Risk Graphs method the Safety Integrity Level (SIL) of a Safety Instrumented System (SIS) can be determined based on some methods described in German publication DIN 19250 [1].

Risk Graph is a qualitative method that takes into account the frequency and consequence of a dangerous event, but also the probability that the personnel to avoid the danger [4].

Table 1 shows the classification of risk parameters suggested by the IEC 61511 standard [3].

Table 1. Risk parameters classification according to IEC 61511 [3].

RISK PARAMETER	NOTATION	CLASSIFICATION
CONSEQUENCES (C)	C1	minor injuries
	C2	serious injuries of one or more people
	C3	the death of one person
	C4	catastrophic effect - many deaths
OCCUPANCY FREQUENCY OF THE AFFECTED AREA (F)	F1	rarely to most often (<0.1)
	F2	often to continuous (>0.1)
THE PROBABILITY TO AVOID THE CONSEQUENCES (P)	P1	possible under certain conditions (>90%)
	P2	almost impossible (<10%)
THE LIKELIHOOD OF UNINTENDED CONSEQUENCES (A)	L1	very unlikely (<0.01/an)
	L2	unlikely that an undesirable event to appear (>0.01/an)
	L3	a relatively high probability that unwanted events to appear (>0.1/an)

For the Consequences parameter (C) in relation to personnel risk are suggested four categories of consequences ranging from minor injuries to several deaths. C1 is the least severe category. Generally, the consequences will be measured by the degree of people's injury but also by environment or financial measures [3].

The occupancy frequency (F) indicates the fraction of time that the dangerous zone is occupied by personnel. F2 indicates a higher risk than F1, because the area is occupied more frequently. Usually, according to IEC 61511, F1 can be selected if the dangerous zone is occupied less than 10% of time.

The possibility that the personnel to avoid the danger is represented by parameter P. This parameter reflects what method should be identified by the staff in order to escape the danger. In addition, the rate of the dangerous event is considered. There are two categories denoted by P1 and P2, P2 indicating the highest risk. In order to select P1 a list of statements must be validated. Such lists of statements are suggested in IEC 61511.

The final parameter is the Likelihood (L) which is the frequency of the occurrence of an unintended event on a year, without a SIF (Safety Instrumented Function).

Figure 2 represents a typical risk graph for the personnel risk. Similar graphs can be obtained for equipment risks, loss of production or environment impact.

The path from left to right is determined by the selected values of the risk parameters. The selected consequence, occupancy frequency and avoiding probability lead to a specific output

row, O. Each row output parameter value corresponds to three parameter values of the Likelihood L. Choosing L is the last step in determining the SIL level. Choosing the highest probability that an unwanted event to appear, the value of parameter L is established to L3.

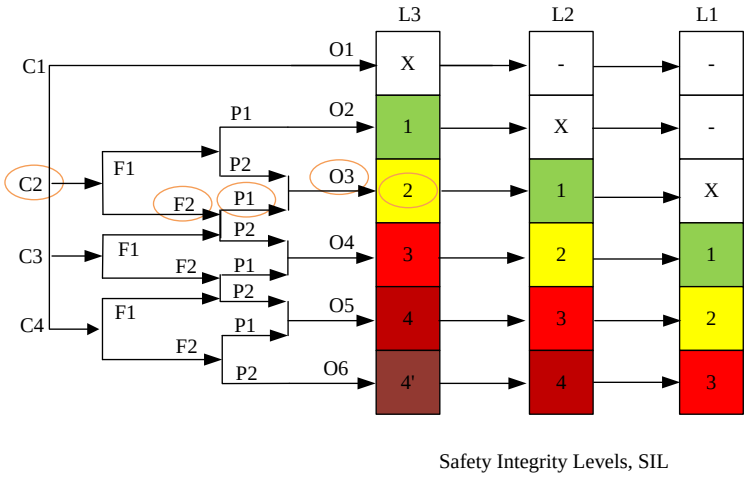

Fig. 2. Risk Graph method.
C - Consequences (C1 - minor injuries, C2 - serious injuries, C3 - a death, C4 - many deaths); F – occupancy Frequency (F1 - rarely to more often, F2 - often to continuous); P - Probability to avoid the consequences (P1 – possible under certain conditions, P2 - almost impossible); L - Likelihood (A1 - very unlikely, A2 - small A3 - relatively high); X – a SIS is not necessary, 1, 2, 3, 4 - the safety integrity level, SIL, 4 '- a SIS alone is not enough.

Case Study

An example of industrial process that needs a Safety Instrumented System (SIS) is in (fig. 3), which represents a heater (heat exchanger) equipped with a classical fuel temperature control system. The goal of the temperature control system that consists of the temperature transducer TT1, the controller TC1 and control valve CV1 is to maintain the temperature below a certain high value beyond which the raw material that is heated can become dangerous.

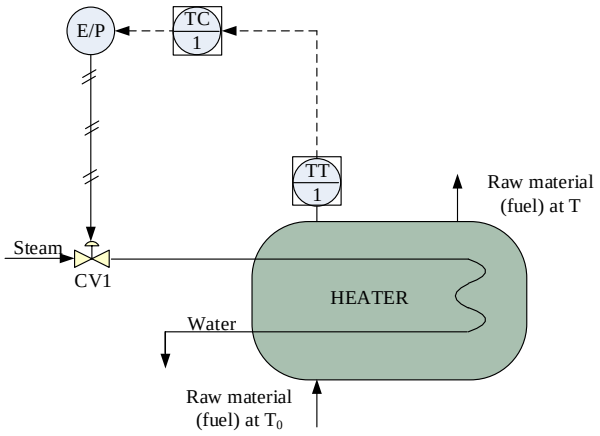

Fig. 3. Heat exchanger control system.
TC1 – Temperature Controller, TT1 – Temperature Transducer, E/P –Electro/Pneumatic converter, CV1 – Control Valve, T_0 – the inlet temperature of the raw material, T – the outlet temperature of the raw material, $T>T_0$.

To prevent the dangerous potential of the process, a Safety Instrumented System (SIS) must be used.

In order to establish the necessary integrity level – SIL of the SIS, Risk Graph method can be used.

From (fig. 2) if the probable consequence is assessed to be a serious injury of one or more persons, C2 option is selected. If the area is exposed to personal often to continuous, F2 is selected. Because it is possible that in certain circumstances the consequences may be avoided, the parameter P_1 should be chosen. The combination of these risk parameters leads to O3 output row. Considering a high probability that an undesirable event to occur, the probability of occurrence value is set to L3. According to (fig. 2) results a SIL 2 requirement for the necessary SIS.

In order to protect the system if the classical fuel temperature control system fails and the temperature reaches or exceeds the higher admissible value a SIS with SIL 2 requirement should be used. The SIS contains in its structure one or two temperature sensors, a logical solver (usually a PLC) and a safety shutdown valve as final element.

When a higher temperature is detected by the temperature sensor(s), the SIS can avoid that the system reaches the temperature that causes the ignition of the raw material in the heater, by stopping the steam supply. This is done by closing the safety shutdown valve and stopping the steam supply in the heater.

Conclusions

This paper goal is to describe a qualitative method that can be used in order to establish the necessary Safety Integrity Level (SIL) that must be imposed to a Safety Instrumented System (SIS). This method is based on the results of process risk analysis and is named Risk Graph.

Any industrial process is characterized by some technological hazards that involve some risks of accidents. If the hazard cannot be eliminated, the risk must be minimized. In order to do this a SIS must be used. Any SIS is characterized by an integrity level, named Safety Integrity Level (SIL) that is a measure of the risk reduction factor that must be provided to the industrial process by the SIS.

Risk Graph is a qualitative method that can be used for determining the Safety Integrity Level (SIL) of a Safety Instrumented System (SIS). This method takes into account the consequences of a dangerous event, the occupancy frequency of the affected area, the likelihood that the unwanted event to take place but also the probability that the personnel to avoid the danger.

By choosing a value for each parameter from the risk graph results a Safety Integrity Level (SIL) that the Safety Instrumented System must meet.

References

1. Baybutt, P. – An improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs), *Process Safety Progress*, **26**, 2007, pp. 66–76.
2. IEC 61508 – *Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission, 1998.
3. IEC 61511 – *Functional safety - Safety instrumented systems for the process industry sector*, International Electrotechnical Commission, 2003.
4. Marszal, E., Scharpf, E. – *Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis*, The Instrumentation, Systems and Automation Society (ISA), Research Triangle Park, NC, 2002.

5. Summers, A.E. – Techniques for assigning a target safety integrity level, *ISA Transactions*, Vol. 37, 1998, pp. 95-104.
6. Cangea, O. – Human Machine Interface for Production Line Monitoring and Control, *Buletinul Universitatii Petrol-Gaze din Ploiesti, Seria Tehnica*, Vol. LXVII, No.3, 2015, pp. 38-47.
7. Zurich Insurance Group Ltd. – *Risk Topics - Functional Safety – Safety Instrumented Systems in Process*, Industries Zurich – Switzerland, 2015.
8. Cangea, O., Moise, A., Bucur, G., Popescu, C. – Intelligent Transportation System. Case Study, *Proceedings of the 15th International Multidisciplinary Scientific Geoconference (SGEM)*, Albena, Bulgaria, June 18-24, 2015, pp.167-174.
9. http://www.documentation.emersonprocess.com/groups/public_valvesprodlit/documents/training_info/sis_training_course_1.pdf
10. https://www.honeywellprocess.com/library/support/Public/Documents/Safety%20Instrumented%20Systems%20(SIS),%20Safety%20Integrity%20Levels%20(SIL),%20IEC61508,%20and%20Honeywell%20Field%20Instruments.pdf

Stabilirea Nivelului de Integritate a Siguranței asociat unui Sistem de Siguranţă şi Protecţie utilizând metoda Grafului de Risc

Rezumat

Sistemele de siguranţă şi protecţie au devenit din ce în ce mai importante din cauza substanţelor periculoase vehiculate în procesele industriale fapt ce impune utilizarea unor sisteme speciale de protecţie. Orice sistem de siguranţă şi protecţie se caracterizează printr-un nivel de integritate notat SIL (Safety Integrity Level). Graful de Risc este o metodă calitativă care poate fi utilizată pentru a determina nivelul de integritate al siguranţei SIL ce trebuie impus unui SIS. Această metodă ia în considerare posibilele consecinţe ale unui eveniment periculos, frecventa de ocupare a zonei afectate, probabilitatea ca un eveniment nedorit să apară dar şi probabilitatea ca personalul să poată evita pericolul. Consecinţele evenimentului nedorit pot fi de la leziuni minore la mai multe decese, frecvența de ocupare poate fi de la rar la continuu, probabilitatea de a evita consecinţele poate fi de la posibil la aproape imposibil iar probabilitatea ca evenimentul nedorit să apară poate fi de la foarte puțin probabil la foarte probabil. Alegerea unei valori pentru fiecare parametru din Graful de Risc conduce la un anumit nivelul de integritate a siguranţei (SIL). Acest nivel SIL trebuie să fie realizat de către sistemul de siguranţă şi protecţie pe care îl caracterizează.