BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXVIII No. 1/2016	65 – 70	Seria Tehnică

Determining Safety Integrity Level using Risk Matrix Method

Alina-Simona Băieşu

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

Abstract

Risk Matrix is one of the most popular qualitative methods used to determine the Safety Integrity Level (SIL) that characterizes a Safety Instrumented System (SIS). Risk Matrix is a matrix that has two dimensions which are obtained after a risk analysis, namely the frequency and the severity of an unwanted event/accident,. The frequency of the unwanted event that can occur is quantified in terms like low, medium or high and can be measured qualitatively or quantitatively. The consequences or severity of the unwanted event can be also quantified in terms like minor, serious or catastrophic and can be measured by various risk factors such as personnel, capital etc. in accordance with the level of severity. The categories can be selected either qualitatively or quantitatively by attaching economic figures, deaths etc. If each cell of the Risk Matrix, which is obtained by joining the two dimensions, has a Safety Integrity Level (SIL) associated to it, the process of determining the necessary Safety Integrity Level (SIL) is easy.

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

Introduction

Basically, according to [12] Safety Integrity Level (SIL) is a statistical representation of the integrity of a Safety Function (SF) of a Safety Instrumented System (SIS) when this function receives a demand and must be activated. SIL level concept can be applied only to whole SIS that meets one or more Safety Functions, not to each individual item within it, such as sensor [3].

SIL level determines a number of quantitative and qualitative constraints that needs to be imposed to the SIS that is characterized. Depending on the SIL level, IEC 61508 defines different requirements on the design of a SIS, thus several stages of its life cycle. In general, the higher the SIL level is, the requirements are more stringent. According to [11], especially SIL 3 and 4 involve significant costs and requires highly skilled personnel.

Overall, about 95% of SIS requires no more than SIL 1, SIL 2 about 5% and SIL 3 about 1%. SIL 4 is not justified in most of industrial applications; an alternative is the use of multiple layers of protection [5].

Safety Integrity Level (SIL) is a measure of SIS performance and is not a direct measure of the process risk. As the degree of the risk of one process is larger, the SIS must be more efficient, and the number that accompanies SIL increases as the value.

There are four categories of methods and tools for determining the Safety Integrity Level (SIL) of a Safety Instrumented System (SIS): quantitative and semi-quantitative methods (e.g. Layer

Of Protection Analysis - LOPA), qualitative (e.g. risk matrix, layer of protection risk matrix, risk graph) and semi-qualitative methods (e.g. calibrated risk graph) [10].

Quantitative methods use a series of formulas for computing certain features of the system and by employing them in certain ranges the required SIL is determined.

Semi-quantitative methods use computing formulas but the numerical values used are approximated by orders of magnitude for each parameter.

In case of using qualitative methods, the parameters used as basis of decisions are subjective and estimated by one or more experts.

Semi-qualitative methods use the same principles as those qualitative only that for the used parameters certain numerical values are estimated.

In this paper the qualitative Risk Matrix method is described.

Risk Analysis and Safety Integrity Level (SIL) related to a Safety Instrumented System (SIS)

Risk is defined as the probability of human exposure and of the assets created by him to the action of a particular hazard. The risk is quantified by the number of casualties, the number of injured, property and economic activities damage etc. [1].

Risk is a function of frequency of an event and the severity of the consequences of that event/hazard. Risk can influence personnel, production, environment etc. [4].

RISK = FREQUENCY x HAZARD CONSEQUENCES

The risk can be measured both quantitatively and qualitatively [5].

The qualitative approach uses descriptive terms such high, low or moderate. If these terms are calibrated meaning that are defined relative to a scale of values generally accepted, this qualitative version can be also used.

The quantitative approach is more easily defined in terms of frequency and severity of the consequences, if there are studies and statistics.

Preventing accidents by analyzing technological hazards and risks involves additional activities from the design stage of a process. If the hazard cannot be eliminated, the risk must be minimized by reducing the frequency and/or consequences.

Reducing risk is the purpose of Safety Instrumented Systems (SIS) [2]. When such a system is designed the degree of the risk that must be reduced should be known. It should be reduced from an unacceptable value a tolerable one. This principle has a fundamental impact in how to design a SIS.

A Safety Instrumented System (SIS) is the opposite of a control system. It only works at certain times, access to it must be restricted, must be reliable and to respond instantly when it needs to act. One example is the Pressure Safety Valve (PSV) which should stay closed as long as the pressure in a vessel is below a certain value and to open when the pressure reaches a certain limit. If the pressure never reaches this limit, the valve should not be opened. Also, it may happen that because the valve is closed for a period of time, when there is a problem and should be open, it cannot be opened. As such, these systems can hide defects that cannot be observed directly.

Because the elements of a SIS stay long time in standby, it is possible that when is necessary to entry into service, not to go. As such, these systems must be constantly tested and must incorporate techniques that offer the possibility of self-testing.

Safety Instrumented Systems (SIS) are designed to involve as little human intervention as possible. The operator interacts with the control system, if it fails, the next step is the direct intervention of the operator by passing the process on manual. If this intervention also fails, the last line of defense, SIS should operate automatically and independently. Human interventions are only allowed to start or maintain certain parts of the system.

In table 1 is presented the dependence between the Safety Integrity Levels (SIL) of a Safety Instrumented System (SIS) and the Risk Reduction Factor (RRF) or the Probability of Failure on Demand (PFD) in case of a low rate of demand system and with the Probability of Dangerous Failure per Hour (PFH) or the Mean Time to Failure (MTTF) in case of a high rate of demand system.

Table 1. Safety Integrity Levels for low rate or high rate of demand systems [6].

	SYSTEMS WITH A LOW RATE OF DEMAND		**SYSTEMS WITH A HIGH RATE OF DEMAND**	
SIL	**PFD**	**RRF=1/PFD**	**PFH**	**MTTF**
4	10^{-4}-10^{-5}	10^{4}-10^{5}	10^{-9}-10^{-8}	10^{4}-10^{5}
3	10^{-3}-10^{-4}	10^{3}-10^{4}	10^{-8}-10^{-7}	10^{3}-10^{4}
2	10^{-2}-10^{-3}	10^{2}-10^{3}	10^{-7}-10^{-6}	10^{2}-10^{3}
1	10^{-1}-10^{-2}	10^{1}-10^{2}	10^{-6}-10^{-5}	10^{1}-10^{2}

Risk Matrix

Due to its simplicity Risk Matrix is one of the most popular qualitative methods for determining Safety Integrity Level (SIL) of a Safety Instrumented System (SIS). Risk Matrix takes into account the frequency and consequence/severity of an unwanted event, based on a classification of the risk parameters.

The frequency that an unwanted event will occur can be quantified in terms like LOW, MEDIUM, HIGH or any other suggestive terms. Levels can be measured qualitatively or quantitatively (Table 2) for a single part or more, for a process or the whole facility.

Table 2. An example of the risk frequency values [8].

Level	**Frequency**	**Qualitative evaluation**
3	**HIGH**	One event may occur more than once in the predicted lifetime of the plant
2	**MEDIUM**	One event may occur once in the predicted lifetime of the plant
1	**SMALL**	One event may occur with a low probability in the predicted lifetime of the plant

The consequences or severity of an unwanted event can be measured by various risk factors such as personnel, environmental, production equipment, capital etc.

Table 3 shows an example of the severity of the associated risk to personnel, environment and production.

According to Table 3, the consequences may be MINOR, SERIOUS or CATASTROPHIC in accordance with the level of severity. The categories can be selected either qualitatively or quantitatively by attaching economic figures, deaths etc.

Table 3. Sample values of severity/risk consequences [8].

Level	Severity/ Consequences	Qualitative measure		
		Personnel	**Environment**	**Production/ Equipment**
III	**CATASTROPHIC**	More deaths	Leaks of hazardous substances outside the facility perimeter	Higher losses than 1.500.000 $
II	**SERIOUS**	A single death or an accident requiring recovery time	Leaks of non-hazardous substances outside the perimeter of the facility and leaks of hazardous substances in facility perimeter	Loses between 100.000 $ şi 1.500.000 $
I	**MINOR**	Accidents requiring medical treatment or first aid	Leaks of hazardous substances in a restricted perimeter area or without leakage	Lower losses than 100.000 $

By joining the values of the two properties (Tables 2 and 3), the frequency and the severity of risk, is obtained the Risk Matrix, represented in (fig. 1).

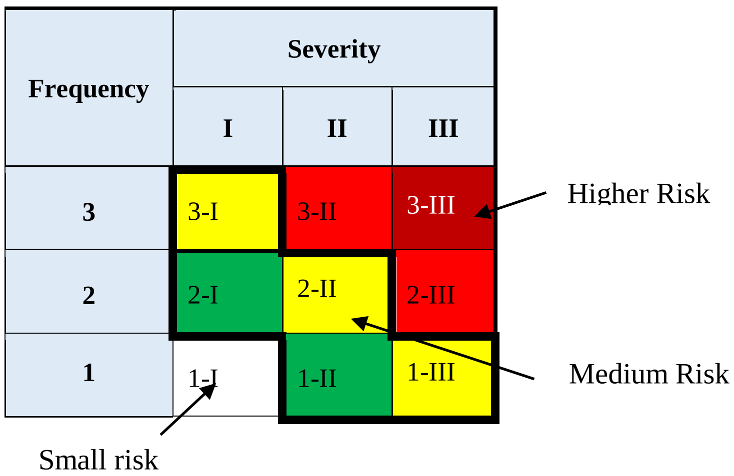

Fig. 1. Global risk (Risk Matrix) [9].

If the identified risk is high, it is recommended to introduce changes. If the identified risk is medium, it is necessary to add additional safety layers. If the identified risk is small, does not require changes or additional layers of protection.

If each cell of the Risk Matrix has a SIL level associated to it, the process of determining the necessary SIL level is easy [8].

Fig. 2 shows a typical chart of a modified Risk Matrix used to determine the SIL level.

Minor severity/consequence - small frequency results to unnecessary SIL. This means that the risk is deemed tolerable.

Minor severity/consequence - medium frequency results in lower SIL, while catastrophic consequence - high frequency leads to higher SIL levels. If the conclusion is that a higher SIL 3 or SIL 4 level is needed, additional studies should be conducted because a single SIF may not provide a sufficient risk reduction [10].

Frequency	Severity		
	I	**II**	**III**
3	SIL 2	SIL 3	SIL 4
2	SIL 1	SIL 2	SIL 3
1	No SIL	SIL 1	SIL 2

Fig. 2. Modified Risk Matrix used to determine the SIL level of a SIS [9].

Sometimes due to assessment that can be made, the result may be unrealistic. In such cases, the use of other tools and methods in conjunction with this method in order to improve the quality of determination must be considered [7].

Risk Matrix has two dimensions, namely the frequency and severity of an event. Sometimes in some practical applications in addition to the two dimensions, a third dimension can be added. This dimension takes into account the additional layers of protection, resulting the layers of protection Risk Matrix.

Conclusions

This paper presents a qualitative method for determining the necessary Safety Integrity Level (SIL) that characterizes a Safety Instrumented System (SIS). This method is based on the results of the risk analysis that is made from the design stage of an industrial system and is named Risk Matrix.

In any industrial system, in order to prevent accidents the technological hazards and the risks involved are analyzed. If the hazard cannot be eliminated, the risk must be minimized by reducing the frequency and/or consequences of the accident.

Safety Integrity Level (SIL) is a measure of the risk reduction factor that a Safety Instrumented System must provide to an industrial process.

Risk Matrix is one of the most popular qualitative methods for determining the Safety Integrity Level (SIL) of a Safety Instrumented System (SIS) due to its simplicity.

Risk Matrix takes into account the frequency and consequence/severity of an unwanted event, based on a classification of the risk parameters.

The frequency that an unwanted event will occur can be quantified in terms like LOW, MEDIUM, HIGH and the consequences may be MINOR, SERIOUS or CATASTROPHIC in accordance with the level of severity. The categories can be selected either qualitatively or quantitatively by attaching economic figures, deaths etc.

By joining the values of the two properties the Risk Matrix is obtained.

The process of determining the necessary SIL level is easy if each cell of the Risk Matrix has a SIL level associated to it.

References

1. B ă l t e a n u , D . , R ă d u ţ ă , A . – *Hazarde naturale şi antropice*. Editura Corint, 2001.
2. B e r g s t r o m , J . – *Safety Instrumented Systems (SIS) and Safety Life Cycle*, Process Engineering Associates, 2009.
3. B r o w n , S . – Overview of IEC 61508 - Design of electrical/electronic/ programmable electronic safety-related systems, *Computing and Control Engineering Journal*, Vol. 11, 2000, pp. 6-12.
4. * * * – *Guidelines for Chemical Process Quantitative Risk Analysis*, CCPS (Center of Chemical Process Safety), American Institute of Chemical Engineers (AIChE), New York, 1989.
5. * * * – *Overview of Safety Instrumented Systems*, IDC TEHNOLOGIES, 2012.
6. * * * – IEC 61508 - *Functional safety of electrical/electronic/programmable electronic safety-related systems*, International Electrotechnical Commission, 1998.
7. * * * – IEC 61511 - *Functional safety - Safety instrumented systems for the process industry sector*, International Electrotechnical Commission, 2003.
8. L a s s e n , C. A. – *Layer of protection analysis (LOPA) for determination of safety integrity level (SIL)*, The Norwegian University of Science and Technology, Department of Production and Quality Engineering, 2008.
9. M a c d o n a l d , D . – *Practical Industrial Safety - Risk Assesment and Shutdown Systems*, 2004.
10. M a r s z a l , E., S c h a r p f , E. – *Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis*, The Instrumentation, Systems and Automation Society (ISA), Research Triangle Park, NC, 2002.
11. S m i t h , D.J., S i m p s o n , K.G.L. – *Functional safety. A straightforward guide to applying IEC 61508 and related standards*, Oxford: Elsevier Butterworth-Heinemann, 2004.
12. S u m m e r s , A.E. – Techniques for assigning a target safety integrity level, *ISA Transactions*, Vol. 37, 1998, pp. 95-104.

Determinarea nivelului de integritate a siguranţei utilizând metoda Matricei de Risc

Rezumat

Matricea de risc este una dintre cele mai populare metode calitative folosite pentru determinarea Nivelului de Integritate a Siguranţei (SIL) ce caracterizează un sistem automat de siguranţă şi protecţie. Matricea de risc este o matrice care are două dimensiuni care se obţin în urma unei analize de risc şi anume frecvenţa şi severitatea unui eveniment nedorit sau accident. Frecvenţa evenimentului nedorit care poate apărea este cuantificată în termeni cum ar fi scăzut, mediu sau ridicat şi poate fi măsurată calitativ sau cantitativ. Consecinţele sau severitatea evenimentului nedorit pot fi, de asemenea, cuantificate în termeni cum ar fi minore, grave sau catastrofale şi pot fi măsurate prin diverşi factori de risc cum ar fi personalul, capitalul etc., în conformitate cu nivelul de severitate impus. Categoriile pot fi selectate fie calitativ sau cantitativ prin ataşarea unor cifre economice, decese etc. Dacă fiecare celulă a matricei de risc, ce este obţinută prin unirea celor două dimensiuni, are un Nivel de Integritate a Siguranţei (SIL) asociat, procesul de determinare a nivelului SIL necesar este uşor.