RESEARCH PAPERS FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

2015

Volume 23, Special Number

EVALUATION OF SAFETY PARAMETERS ACCORDING TO IEC STANDARDS

Peter CUNINKA, Maximilián STRÉMY

Ing. Peter Cuninka, doc. Ing. Maximilián Strémy, PhD. Slovak University of Technology in Bratislava, Faculty of Materials Science and Technology in Trnava, Advanced Technologies Research Institute, Bottova 25, 917 24 Trnava, Slovakia, e-mail: peter.cuninka@stuba.sk maximilian.stremy@stuba.sk

Abstract

The article deals with different procedures for determining the safety integrity level and its applications. The purpose of this research was to evaluate the system and associate it with certain safety integrity level. In this article, we will use IEC 61508, IEC 61511 and IEC 62061 for comparison. The first standard is specified as the superior standard for all safety-critical systems. The second one acts as an extension of the superior standard in the field of functional safety. The last one is aimed at machinery safety.

Key words

safety system, evaluation of safety, risk analysis, IEC 61508

INTRODUCTION

The development of science and technology has brought the historically lowest physical burden on the manufacturing process. However, even using the most modern machinery and equipment, there still could be damage to health, property or the environment. Therefore, each process is constantly subjected to safety analysis. Security issues are discussed in the most comprehensive international standards. They are universally applicable in all countries that have adopted them (1).

Our aim is to mitigate risk to its minimal values to prevent hazardous events. The necessary risk reduction has to be achieved to meet tolerable risk for specific situation. The tolerable risk will depend on many factors (for example severity of injury, the frequency at which a person or people are exposed to danger and duration of exposure). Important factors will be the perception and views of those exposed to the hazardous event (2).

These standards provide us with an insight into the monitored processes, production equipment, etc. from the aspect of safety. International standards mentioned in this paper are IEC 61508 - Functional safety and IEC 62061 - Safety of Machinery.

METHODS

Risk analysis methods are described in each standard for specified systems. There are many methods specified in IEC 61508, such as the ALARP method, the risk graph method or Layer of protection analysis (LOPA).

The Layer of Protection Analysis (LOPA) is a semi-quantitative methodology that can be used to identify safeguards that meet the independent protection layer (IPL) criteria established by CCPS in 1993. Since IPLs (Fig 1) are extrinsic safety systems, they can be active or passive systems, as long as the following criteria are met:

- specificity the IPL is capable of detecting, preventing or mitigating the consequences of specified potentially hazardous event(s), such as a runaway reaction, loss of containment, or an explosion,
- independence an IPL is independent of all the other protection layers associated with the identified potentially hazardous event,
- dependability the protection provided by the IPL reduces the identified risk by a known and specified amount,
- auditability the IPL is designed to permit regular periodic validation of the protective function.

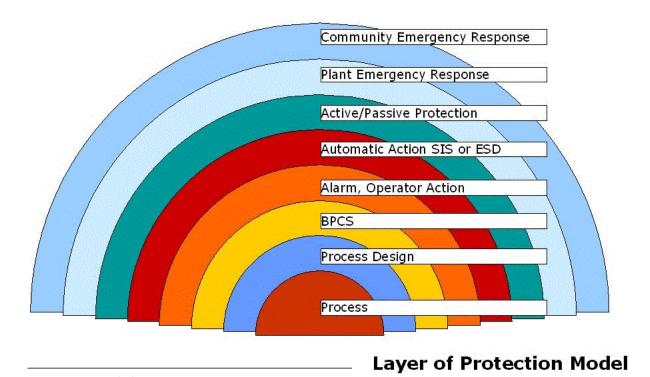


Fig. 1 Layer of Protection Model (3)

LOPA can be used at any point in the lifecycle of a project or process, but it is most cost effective when implemented during front-end loading when the process flow diagrams are complete and the P&IDs are under development. For existing processes, LOPA should be used during or after the HAZOP review or revalidation. LOPA is typically applied after a qualitative hazards analysis has been completed, which provides the LOPA team with a listing of hazard scenarios with the associated consequence description and potential safeguards for consideration (4).

The Risk Graph Method is the most qualitative method used to determine the safety integrity level of which described in part 5 of IEC 61508 Standard. Although the risk graph is a relatively easy method for application and allowing a fast assessment of SIL, it has also some disadvantages in the interpretation of linguistic terms used to define the parameters C, F, P and W, which may differ between evaluators due to the subjectivity related to the definition of these parameters. The risk graph is based on the following equation: $R=F \times C$, where R is the risk during the absence of the related safety system, F is the frequency of the dangerous event during the absence of the safety systems and C is the consequences of the dangerous event. The frequency of dangerous event supposed to be the result of three following factors:

- Probability that the exposed area is occupied;
- The probability of avoiding the hazardous situation;
- Number of times per year that the hazardous situation would occur.

Finally, we take the following four measures of the risk:

- Consequence of the hazardous event (C);
- Occupancy (F);
- Probability of avoiding the hazardous event (P);
- Demand rate (W).

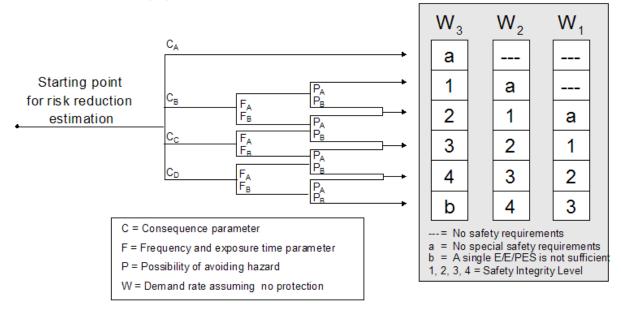


Fig. 2 Risk Graph Method (5)

The As Low As Reasonable Practicable (ALARP) principles may be used on its own or with other methods to determine the SIL requirements for a safety function. They can be used in a qualitative or quantitative ways. When used in a qualitative way, the SIL requirements for a specified safety function increase until the frequency of occurrence is reduced so that the conditions associated with risk classes are satisfied. When used in a quantitative way, frequencies and consequences are specified numerically and the SIL requirements increase until it becomes evident that the additional capital and operating cost associated with implementing a higher SIL would meet the condition associated with risk classes (2).

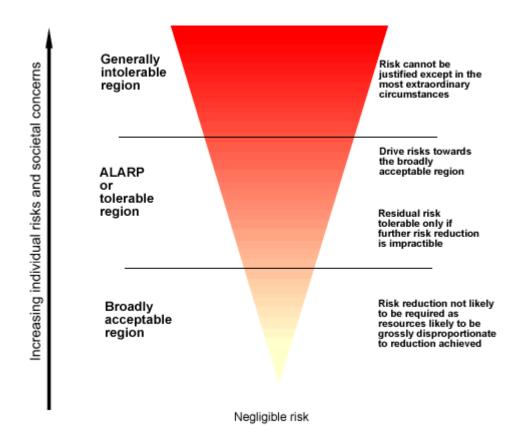


Fig. 3 Tolerable risk and ALARP (6)

According to Fig. 3, there are three stages of risk for ALARP method:

- a) the risk is so great that it shall be refused altogether, or
- b) the risk is, or has been made, so small as to be insignificant, or
- c) the risk falls between the two states specified in a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction (2).

For our system, we used Risk estimation and SIL assignment specified in IEC 62061. Functional requirements contain the details such as frequency of operations, requested reaction time, operating modes, operating environment and error reactions. Safety integrity requirements are expressed in Safety Integrity Level (SIL).

Risk estimation should be carried out for each hazard by determining the risk parameters that should be derived from the following:

- severity of harm (Se), and
- probability of occurrence of that harm, which is a function of:
 - o frequency and duration of the exposure of persons to the hazard (Fr),
 - o probability of occurrence of a hazardous event (Pr),
 - possibilities to avoid or limit the harm (Av) (7).

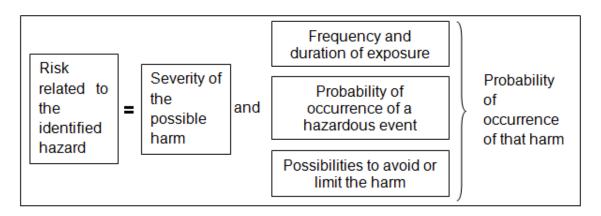


Fig. 4 Parameters used in risk estimation in IEC 62061 (7)

To achieve requested Safety Integrity Level we need to follow proposed procedure that is described in Fig. 4 above.

RESULTS

For example, let us consider each indicator for corresponding risk estimation on a production line model. There are different scenarios of potentially harmful incidents. We evaluated individual required parameters as seen in Fig. 5. Each parameter has specific conditions that need to be considered during risk analysis. We tried to make the most accurate version of risk analysis for this purpose.

To achieve the requested Safety Integrity Level, a simple equation is needed:

$$Cl = Fr + Pr + Av.$$

Using the table in the middle of Fig. 5, this would lead to specific Safety Integrity Levels that need to be assigned to the Safety Related Control Function (SRCF) (7).

After making calculations for each hazard in our study, we will assign required SIL to SRCF to mitigate the risk.

There is specific software to design the requested SRCF's. We used Safety Evaluation Tool by Siemens [8] because our control system is also made by Siemens so we do not need to specify safety functions for each component. This is integrated in the tool. This tool will also give us the final value of safety function for the whole system designed by our risk assessment study.

Risk assesment and safety measures														
Created	: Peter Cuninka													
Date : 15	5. 4. 2014													
				ue are een ai				sures requ sures reco	ired mmended					
Consequences Severity Se		Class Cl						Frequency and		Probability		Avoidance		
			3-4	5-7		8-10	11-13	14-15	duration Fr		Pr		Av	
Death, losing an eye or arm		4	SIL 2	SIL	2	SIL 2	SIL 3	SIL 3	≤1 h	5	Very high	5		Τ
Permanent, losing fingers		3		OM		SIL 1	SIL 2	SIL 3	>1 h ≤ 1 d	5	Likely	4		
Reversible, medical attention 2		2			OM		SIL 1	SIL 2	$>1 d \le 2 w$	4	Possible	3	Impossible	1
Reversible, first aid 1		1					OM	SIL 1	$>2 w \le 1 y$	3	Rarely	2	Possible	1
									>1 y	2	Negligible	1	Likely	1
Haz. Hazard			Se	Fr	Pr	Av	Cl	Safety measures S						
1.0	Worker intervention machine)	3	5	3	3	11-13	Installation of protective door, warning signs, worker guidance SIL2							
1.1	Worker intervention machine)	ng 2	5	4	2	11-13	Installation of protective door, warning signs, worker guidance SIL2							
1.2	Worker intervention machine)	^{ig} 4	5	3	1	8-10	Installation of protective door, warning signs, worker guidance SIL2							

Fig. 5 Risk evaluation according to IEC 62061

DISCUSSION

The results show that evaluation has to be based on the experience of more than one expert in the particular field, because even a small underestimation of conditions of hazard leads to miscalculation of the whole safety system which could lead to many injuries or even death of workers.

CONCLUSION

We outlined the risk evaluation methods according to IEC 61508 and IEC 62061. Risk evaluation described in IEC 62061 was used to demonstrate the evaluation of risks and potential hazards in machinery environment that could be dangerous to humans. The results gained by IEC 62061 were then projected to the Safety Evaluation Tool manufactured by Siemens to design all features of system in order to meet the requirements for the safety integrity level obtained as a result of risk evaluation. Using proper safety measures and proper SRCF, we can mitigate risk to a tolerable level and reach the required Safety Integrity Level. This is substantial for worker, environmental safety and financial growth.

Acknowledgement

This research was funded by the ERDF - Research and Development Operational Programme under the project "University Scientific Park Campus MTF STU - CAMBO" ITMS: 26220220179.

References:

1. CUNINKA, P. 2014. *Evaluation of safety-critical process according to selected standard and proposal of automation safety functions: Master thesis.* Trnava: Institute of Applied Informatics, Automation and Mathematics, Faculty of Materials Science and Technology in Trnava, Slovak University of Technology in Bratislava: 67 p.

- 2. IEC 61508 5: 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems Examples of methods for the determination of safety integrity levels.
- 3. S2S : A Gateway for Plant and Process [Online]. [Cit. 6. 2. 2015]. Available on: http://www.safety-s2s.eu/modules.php?name=s2s_wp4&idpart=2&op=v&idp=750
- 4. SUMMERS, A. E., 2002. Introduction to Layer of Protection Analysis. *Journal of Hazardous Materials*.
- FOORD, A. G., GULLAND, W. G., HOWARD, C. R., T. KELLACHER, T., SMITH, W. H. Applying the latest standard for Functional Safety - IEC 61511. [Online]. [Cit. 6. 2. 2015]. Available: http://wildeanalysis.co.uk/casestudies/functional-safety-iec-61511.
- 6. [Online]. [Cit. 18. 2. 2015]. Available on: http://www.petafry.com/images/ALARP%20diagram.gif
- 7. IEC 62061: 2005 Safety of machinery Functional safety of safety-related electrical, electronic and programmable electronic control systems.
- 8. SIEMENS. [Online]. [Cit. 15. 2. 2015]. Available on: http://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/pages/default.aspx.

Reviewers:

doc. Ing. German Michal'čonok, CSc. Ing. Andrej Trnka, PhD.