Transactions of the VŠB - Technical university of Ostrava Vol. VII, No. 2, 2012
Safety Engineering Series p. 44 - 48, DOI 10.2478/v10281-012-0011-z

FUNCTIONAL SAFETY IN INDUSTRIAL EXPLOSION PROTECTION

Kazimierz LEBECKI[1]

Review article

Abstract: The article presents the methodology for quantitative risk assessment, which was mainly directed towards the assessment of explosion risks at workplaces. The methodology is based on the principles of functional safety to be able to determine quantitatively the level of risk for typical manufacturing processes.

Key words: Aramis methodology, Functional safety, Industrial explosions.

Introduction

All industrial installations working in potentially explosive atmospheres, in industries such as energetic, chemistry, food processing and storage and others are generally supplied with protective, detecting, alarming devices preventing explosion occurrence or effectively mitigating it, if explosion appears. Explosion event for a given installation occurs rarely, sometimes never in the life cycle and that is a reason to assure the highest level of reliability of protective devices. The main principles of such reliability is given by the functional safety concept generally defined according to (IEC-EN 61508, 2008) as the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. The details of the functional safety concept are given in the European Standard EN 61-508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). According to the spirit of this standard functional safety could be understood as the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the fight consequence of the hazardous event. This idea is realized in the standard EN 15 233, 2007, "Methodology for functional safety assessment of protective systems for potentially explosive atmospheres" (EN-15233, 2009). This standard formulate definition of functional safety as" a part of the overall safety relating to the intended use in terms of the function and integrity of the protective system including any safety related devices that are part of the protective system performance". This definition deviates from the definition in EN 61508-4 to reflect differences in explosion safety terminology.

Such definition covers all aspects where safety depends on the correct functioning of the protective system and other technology safety-related systems. These standards formulate the general requirements of functional safety and their universal nature makes them more widely adopted to improve modern risk management systems.

Materials and methods

Explosion risk assessment in practice

Fig. 1 presents the general principles of risk assessment for designing of protective system. The scheme relates not only for explosion protection but generally to every protection system.

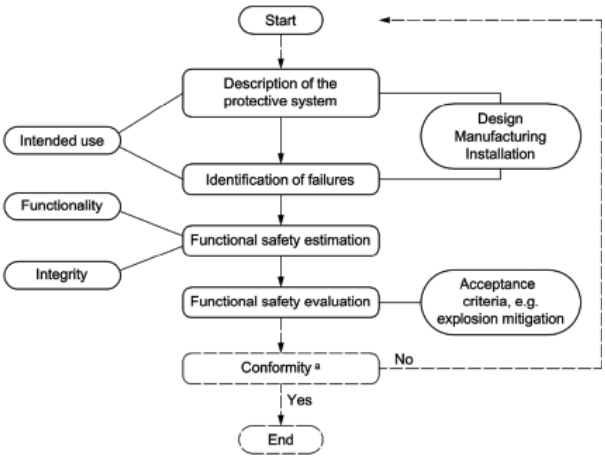

Fig. 1 Functional safety assessment of protective systems in explosion hazardous areas (EN 15233, 2009)

The method of adapting the approach of these standards to assess the effects of catastrophic events has been proposed in the methodology of the ARAMIS project (**A**ccidental **R**isk **A**ssessment **M**ethodology for **I**ndustries) (Salvi and Debray, 2006), realized the Fifth Framework Program. The project concerned the principles of quantitative

[1] Central Mining Institute and School of Occupational Safety Management, Katowice, Poland, kazimierz.lebecki@gmail.com

risk assessment for disaster prevention mainly in the chemical industry, and it was associated with the need to implement the safety requirements of the Seveso II Directive. Using the experience of ARAMIS proposed a method of risk assessment for explosion was proposed. In this paper the case of dust explosion will be considered generally and example of coal dust explosion in underground mine will be presented. For dust explosion hazard the following dust properties are taken into account: dust substances flammability, dispersabillity of dust, dust settling in workplaces, the presence of combustible gases in the atmosphere. According to the general safety philosophy adopted in the European Union, the risk acceptance criteria are defined according to the principle ALARP - "As Low As is Reasonably practicable" - as low as is reasonably justified. ALARP principle was first introduced in the UK and there has been best described.

In ALARP there are three basic risk levels:

- **Unacceptable (intolerable) risk** - the risk level above which the work cannot be done. In such a case, the installation must be, rebuilt, completed with devices and systems of risk reduction.
- **Acceptable risk** - the risk perceived as insignificant. Acceptable risk is similar to the risks of everyday life. It is assumed, however, that if it is possible to reduce the risk in this respect, it shall be reduced in accordance with ALARP principle.
- **Tolerable risk** - is the range in which the risk is acceptable if it meets the ALARP principle.

The proposal to adapt the ALARP rules for explosion risk assessment in hazardous areas at work is summarized in Tab. 1 and 2.

Tab. 1 Risk level classification depending on the frequency of events and their consequences leading to development of hazardous scenario

Occurrence Probability (qualitatively)	Frequency (number of event/ year)	Consequences			
		Disastrous	Critical	Marginal	Negligible
Frequently	$>10^{-3}$	I	I	I	II
Likely	$<10^{-3}$ - 10^{-5}	I	I	II	III
In some cases	$<10^{-5}$ - 10^{-6}	I	II	III	III
Rarely	$<10^{-6}$ - 10^{-7}	II	III	III	IV
Unlikely	$<10^{-7}$ - 10^{-8}	III	III	IV	IV
Almost impossible	$<10^{-8}$	IV	IV	IV	IV

Separate consequences categories are defined as follows:

- Disastrous - collective accident with fatalities, permanent exclusion of work place.
- Critical - serious and collective accidents without fatalities, professional diseases, temporary exclusion of work place.
- Marginal - lightweight accident, catarrh of upper respiratory tracts, losses do not causing work place excluding.
- Negligible - quasi accidental events not causing of work place excluding.

Risk levels I to IV presented in the Tab. 1 result directly from ALARP principle and their interpretation is shown in Tab. 2.

Tab. 2 Risk level interpretation

Risk level	Interpretation
Level I	Range of intolerable risk
Level II	Risk acceptable only in case of big technical difficulties of risk reduction, or in case of costs unproportional relating to achieved safety improvement
Level III	Tolerable risk if costs of its reduction are adequate to the achieved safety level a.
Level IV	Range of acceptable risk

In practice it is necessary to achieve the level III - tolerable risk with objective to achieve the level IV - acceptable risk, being the main objective of risk reduction. In case of explosion hazards it is necessary to approach to the following frequencies of hazard activation (confidence level):

- Dust explosions - 10^{-7} - 10^{-8} hazardous events/ year.
- Igniting and gas explosion - 10^{-6} - 10^{-8}.

Dust explosions, particularly in underground coal mines are difficult to be handled and bring disastrous consequences. Gases are easier to be detected and removed by ventilation. To predict the hazardous scenario it is useful to use the analytical methods, the Best Fault Tree Analysis (FTA) and Event Tree Analysis (ETA). Aramis methodology proposes the algorithm leading to the construction of Bow-Tie Tree - joining Fault Tree and Event Tree. Analysis should be done in 7 following steps:

- Step 1 - gather information needed.
- Step 2 - identify the potentially dangerous situation in the factory.
- Step 3 - determine the primary hazards bound with these situation.
- Step 4 - define the primary event for every such situation.
- Step 5 - built the fault tree from primary events and lead it to the critical event.
- Step 6 - built the event tree for every critical event.
- Step 7 - establish the principles of protection and prevention for every stage of hazard development.

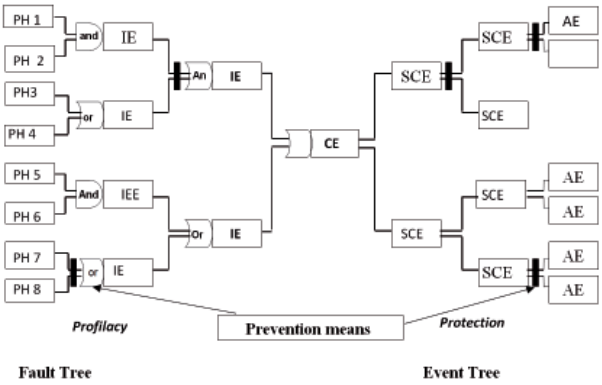

Fig. 2 Bow-Tie scenario of hazardous event development

If the bow-tie tree the following symbols is used:

- PH - primary hazard, for example occurrence of flammable gases or dusts.
- IE - initiating event, for example insufficient ventilation, machine failure, gas leaks, unreliable gas monitoring.
- CE - critical event - for example - intensive gas leak, failure of welding apparatus, deposited flammable dust.
- SCE - secondary critical events, for example - occurrence of explosible gas concentration , occurrence of ignition sources.
- AE - accidental event - for example gas and/or dust explosion, accident, fatality.

To prevent the dangerous scenario development it is necessary to assure the respective functional safety level by applying of Layer of Protection or Safety Layers understood as properly chosen methods of prevention and protection leading to limitation of primary event and initiating event. It is also necessary to take into account the mutual interaction of different kinds of hazard.

Selection of Protection Layers and estimation of their functionality

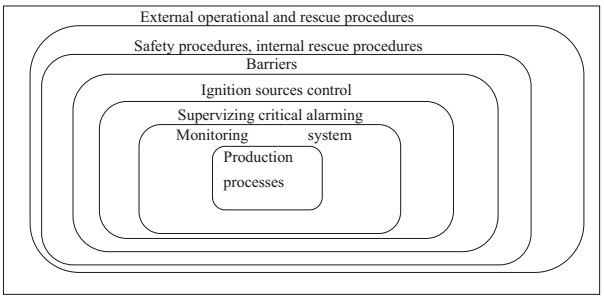

Fig. 3 Layer of protection - example for coal mine explosion

General objectives of protection layer against explosion are: avoiding, preventing, monitoring, mitigating. There are the following types of protection layers (or protective barriers):

- Physical, softening the explosion effects; there are passive physical barriers such as walls, stoppings , bulkheads , barriers and those requiring activation as fire curtains.
- Functional - electric, electronic, controlling the processes in the given range of parameters.
- Functional - electronically programmable - which halt undesirable process conduct by the operation defined by the logical or temporal coupling. Activation of these measures does not require human intervention and its safety features are independent of the control system.
- Symbolic - which require the proper interpretation to achieve the objectives of their destination. There are various types of conventional signs, symbols and signals indicating the state.
- Human related - which depend on the knowledge and experience of the operator. Typical intangible protective measures are national regulations or internal requirements, instructions, rules for safe handling (safety culture).

To achieve the desired risk level, every event in the bow-tie tree must be examined branch after branch for responses to the question „whether the proposed protective layer permits to avoid, prevent, control or limit this event?“. If the answer is yes, then you should include specific protective layer to a specific branch of the bow-tie. Layer will be placed „upstream“ toward the event, if you prevent or to avoid the occurrence of a particular event. If its task is to control or limit a specific event, it must be placed according to the sequence diagram, running events.

The barrier confidence level LC (Level of Confidence) is defined as the probability of failure or an incorrect response to required safety functions. The confidence level should be estimated for the whole protective layer (not for a single barrier). The specific protective layer may consist of many, if necessary, the various subsystems (sensors, management system, procedures and mechanisms of conduct for specific processes). For each subsystem must be assessed level of confidence, efficiency and response time. Quantification of these three components allows the calculation of the overall confidence level of safety barriers. The methodology of the quantitative expression of the confidence level to each LC protective barriers was based on the methodology described in Standard EN 61 508 focused on determining the safety integrity level SIL (Safety Integrity Level) for electrical/electronic/programmable electronic safety-related devices (IEC-EN 61508, 2008).

The values of confidence levels are given in the Tab. 3.

Tab. 3 Recommended values of confidence levels according to EN 61508 for separate safety barriers resulting from applied prevention and protection measures

Confidence level	Coefficient of risk reduction	Probability of failure or incorrect action
4	10 000	$>10^{-5}$ do $<10^{-4}$
3	1 000	$>10^{-4}$ do $<10^{-3}$
2	100	$>10^{-3}$ do $<10^{-2}$
1	10	$>10^{-2}$ do $<10^{-1}$

Examples of confidence level for three types of safety barriers- physical, functional and human in coal mines are given in tables 4, 5, 6.

Tab. 4 Confidence level for selected physical passive barriers (based on accidents analysis)

Material Safety Level	Probability of failure or incorrect action	Confidence Level
Automatic extinguishing systems	$>10^{-2}$ do $<10^{-1}$	1
Neutralization or removing of dust	$>10^{-2}$ do $<10^{-1}$	1
Dust collector on the machine	$>10^{-2}$ do $<10^{-1}$	1
Central dust collecting system	$>10^{-3}$ do $<10^{-2}$	2

These barriers are acts continuously with limited human action, generally do not need sophisticated information about existing hazards.

Tab. 5 Confidence level for selected functional safety barriers (based on industrial data analysis)

Functional Safety Layer	Probability of failure or incorrect action	Confidence level (LC)
Automatic methane monitoring system i	$>10^{-3}$ do $<10^{-2}$	2
Automatic CO monitoring system	$>10^{-3}$ do $<10^{-2}$	2

Those are active barriers, built of the three main subsystems: Detection (D), signal processing or treatment (T) and action either automatic or human.

Example of human related protective layers are internal regulations and safety procedures like rules of gas concentration control, maintenance of ventilation system and so on. General view of human related confidence level is given in Tab. 6.

Tab. 6 Examples of human action confidence level

Human related safety level	Probability of failure or incorrect action	Confidence level (LC)
Prevention	$>10^{-3}$ do $<10^{-2}$	2
Normal action	$>10^{-3}$ do $<10^{-2}$	2
Intervention	$>10^{-2}$ do $<10^{-1}$	1

Identification of safety barriers, to be included in a bow-tie tree should be done with the participation of employees (operators, safety inspectors, employees of the establishment, etc.), analyzing the processes and equipment used.

The checklist helps to identify the functions of the various protective layers and safety barriers in the tree, bow-tie. It can also be used to identify the type of activities to be implemented in a new or modified process in order to improve the existing level of security. Each identified protective layer (or barrier) must meet all the requirements set before it. Defined only as protective, layers can be used when constructing scenarios of failure events. The confidence level estimated using the methodology discussed above is a "proposed" level of confidence. This means that all the proposed protective layers (or its individual barrier) are at least as effective as a barrier actually installed. You should also consider the possibility of reducing the effectiveness of the protective layer over time, due for example to changes in organization and management system. Becomes important to take into account the impact of the safety management system on the functioning of the protective layers.

Results

The article presents the methodology for quantitative risk assessment, which was mainly directed towards the assessment of explosion risks at workplaces. The methodology is based on the principles of functional safety to be able to determine quantitatively the level of risk for typical manufacturing processes The methodology consists of the following steps:

- determine based on the of ALARP principle, risk acceptability criteria, quantitative measures for the production processes,
- define hazardous scenarios of events leading to accidents and incidents, and covering the technical and human threats,
- determine protective barriers to prevent the development of specific event scenarios (barriers relating to methods of prevention and protection),
- determine quantitatively the degree of confidence to the individual protective barriers based on the methodology of determining SIL for electrical/electronic/programmable electronic safety-related,
- development of management principles to ensure the maintenance under the control of the risks by ensuring the effective functioning of the protective barriers.

Conclusion

For the presented methodology gained credibility and has become a common tool for risk assessment, it should be implemented gradually with the following conditions:

a) all processes should be carefully studied based on the best knowledge in this field in order to anticipate potential hazardous events and their probability,

b) should be used: the current state of knowledge to be able accurately estimate the effects of hazards on the work environment, all available information, particularly those that are useful in deciding on activities to secure the development of the factory,

c) use the most recent available data on material properties, process parameters, indicators of reliability of equipment and human factors,

d) work in a transparent manner to allow to explore both the external supervisors and workers concerned with the scale of the risks analyzed and the resulting consequences,

e) the results should be used in the analysis of similar systems, installations, or processes,

f) the methodology should be transformed and continuously improved, with the development of methods for estimating risk, improve safety management systems, emergency systems and emergency response to the potentially affected areas,

g) when assessing the risk of explosion and applying the principles of functional safety for protection against dust explosion it is necessary to break away from the "mentality of the gas," and not to seek an analogy with explosive gases. This applies especially to the concept of explosion limits.

References

EN-15233 (2009). Methodology for functional safety assessment of protective systems for potentially explosive atmospheres.

IEC-EN 61508 (2008). Functional Safety of Electrical /Electronic/ Programmable Electronic Safety Related Systems.

SALVI, Olivier, DEBRAY, Bruno (2006). A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive. *Journal of Hazardous Materials*. 2006, Vol. 130, No. 3, pp. 187-199. ISSN 0304-3894.