ANNALS OF FACULTY ENGINEERING HUNEDOARA
– International Journal of Engineering
Tome XI (Year 2013) – FASCICULE 2 (ISSN 1584 – 2665)

[1.] Roland Iosif MORARU

FROM REALISTIC SAFETY OBJECTIVES TO ACCIDENT SCENARIO SELECTION IN INDUSTRIAL SYSTEMS OPERATION

[1.] DEPARTMENT OF MINING ENGINEERING & INDUSTRIAL SAFETY, UNIVERSITY OF PETROȘANI, PETROȘANI, ROMANIA

ABSTRACT: Risk can only be effectively managed if it is fully understood; therefore a multi-disciplinary approach is often needed to assemble the required knowledge in areas such as probability and statistics, engineering, systems analysis, health sciences, social sciences, and physical, chemical, or biological sciences. A risk assessment must be included in all phases of a system's life cycle to be effective. The paper gives a summery of author's considerations regarding these issues, based on concepts such as verisimilitude of safety objectives, selection of accident scenarios and absolute level of negligible probability. There are emphasized the advantages and drawbacks of probabilistic language and tools in safety studies.
KEYWORDS: risk analysis, verisimilitude, accident scenario, safety objective

INTRODUCTION

In industrial systems operation can appear certain events judged sometimes as quasi - impossible, having extremely low probabilities of occurrence [7]. Risk is defined as the measure of a hazard that combines a measure of the occurrence of an undesirable event and a measure of its consequences [8]. A situation is a hazard if it can be harmful to man, the society, or the environment [2]. The occurrence of an undesirable event is usually measured by its occurrence probability over a given period or by its frequency (number of events occurring per unit of time), or even by its rate of appearance [6]. During the development of safety studies, this kind of events can be taken into consideration in different stages, such as:

a. *When defining the study's objectives, where the probabilities of subjective nature are explicitly related to specific unwanted events.*
b. *In the process of selection of the scenarios considered as potentially generating the unwanted event. Most of the time, based on qualitative analysis, the manager considers the most plausible scenarios from those identified or built by risk assessors.*
c. *In the process of "a posteriori" evaluation of each scenario's probability, when certain event combinations can lead to negligible values.*

Figure 1. The subjective character of risk perception

Consequently, a major problem in all the stages of a safety study can appear, namely: starting from what probability level or non-verisimilitude can be neglected the events or the combination of identified events, events which will be ignored in the stage of decision making [3, 9]. This should be done considering meanwhile the perceived risk, which is a subjective measure of real industrial and occupational cases (see Figure 1, above). Structured on the above - mentioned issues, there will be presented some considerations regarding this field of concern.

BASIC CONCEPTS EMPLOYED IN SYSTEMS SAFETY

The system's operation safety represents, through his four specific components (safety, availability, reliability and maintenance), a basic feature of the different life cycle stages of a system. The concept of safety for a system's operation can be illustrated by the diagram presented in the Figure 2. The common point of the safety of the system operation is the use of probabilistic tool, as assessment technique of risks specific for the analyzed system.

It must be noted that, employed in this field, the language suffers a partial lack from his initial rigorousness existing at probabilities theory level. The safety state of a system can be defined as the *absence of the circumstances which can disturb the system's operation. The probabilistic and statistical methods allow assessing the occurrence probability of failures and unsafe conditions induced in the system by their propagation as scenarios [5].*

Theoretically the absolute (or total) safety of system corresponds with the impossibility of any accident's occurrence, regardless of the considered timing, the system's and his environments status, with regard to all the possible technical failures, human errors and external aggressions. Consequently, the system's design would require a "perfect and complete" knowledge of the system's elements and status, in all the life cycle stages and for all the external environmental conditions.

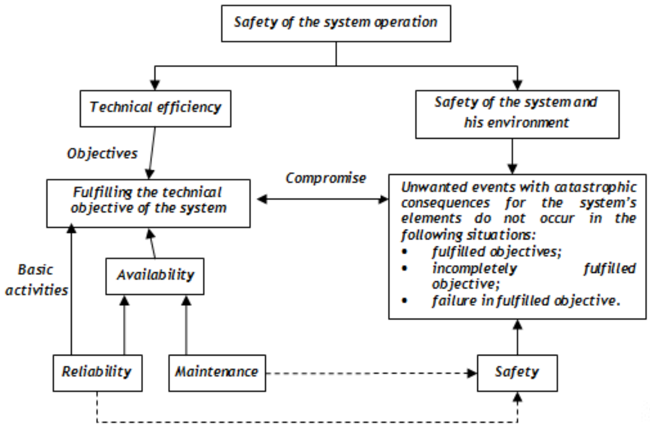

Figure 2. Basic elements of the safety of the system operation

Such an assumption is not reasonable from reasons related to the scientific and technical level and, mainly, from reasons emerging from the inherent limits of human imagination. These general considerations are leading us to one of the basic principles employed in the study of systems safety: "The absolute safety is a myth".

It follows that the primary notion used is that of "safety objective" related to an acceptable risk level, based on rational technical and financial resources, such as illustrated by the ALARP concept (Figure 3).

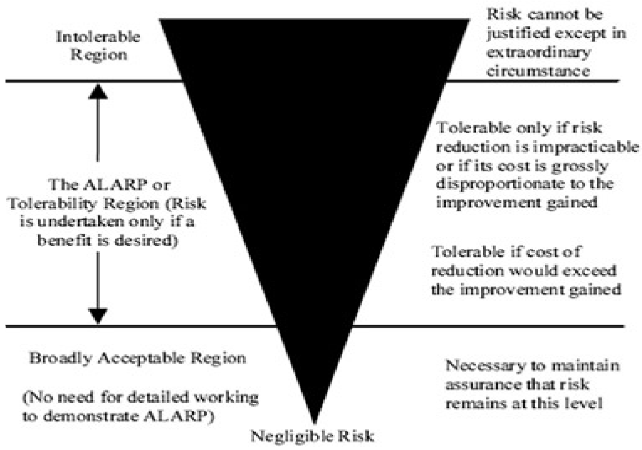

Figure 3. Levels of Risk and As Low As Is Reasonably Practicable (ALARP)

For the operation of a system, there can be defined:

- *a field of knowledge, in which the accurate description of all the operational status and of malfunctions is possible, together with the predictable consequences on the external environment;*
- *a field of ignorance, in which the operation status is unknown.*

If in the field of knowledge it is possible to assess, with a certain level of accuracy, the occurrence probability for an undesired event and the magnitude of his consequences the estimation of an event's occurrence probability and consequences, if the event is incompletely defined qualitatively, is impossible. The probability of the damage occurrence during the exposure to a risk factor describes the accidental, stochastic and uncertain character. The exposure frequency expresses the time lapse in which the worker is exposed to the risk factor action.

A value must be allotted to the probability of occurrence. This designation is not the result of an inspirational moment. Normally, the risk assessment process should start upwards, by defining for each working task, of the hazards and for each hazards of the risks related. Only after this hazard and risk identification phase (e.g. based on a check-list) the quantification can be initiated.

Quantitative Risk Analysis involves the calculation of probability, and sometimes consequences, using numerical data where the numbers are not ranks (1st, 2nd, 3rd) but rather "real numbers" (i.e. 1, 2, 3, 4 where 2 is twice 1 and half of 4). As such, accurate quantification of risk offers the opportunity to be more objective and analytical than the qualitative or semi-qualitative approaches. Most commonly, quantification of risk involves generating a number that represents the probability of a selected outcome, such as a fatality.

Table 1. Probabilities of risk occurrence of a fatality per year from various causes [4]

Crt.	Cause/activity	Probability of a fatality per year
1.	Lightning	0.0000001 or 1 in 10 million
2.	Fire / explosion at home	0.000001 or 1 in 1 million
3.	Death in a 'safe' industry	0.00001 or 1 in 100,000
4.	Death in a road traffic accident	0.0001 or 1 in 10,000
5.	Death in mining	0.001 or 1 in 1,000
6.	Flying in commercial aircraft	1 -0.00001 or 1 in 100,000
7.	Smoking	0 .05 or 1 in 200

Following is an example of probabilistic information concerning the risk of a fatality per year (table 1). British Nuclear Industry research suggests the following probability of death from various causes in the UK [4]. The figures are based on past history. The history of fatalities in the Australian *mining industry from 1991 to 2001 suggests the following risk of death in Australian mining - .0005 or 1 in 5,000. In western industrialized countries, disease results in a death rate of approximately 10^{-2} per year (1 in every 100 are at risk of death from disease), a high-level risk involuntarily accepted by society. On the other end of the spectrum, natural events such as lightning, flood, and insect bites produce a death rate around 10^{-6} per year, the lowest level of involuntarily accepted risk.*

Most Quantitative Risk Analysis for industrial applications attempts to establish probabilities of unwanted events and subsequently the probability of the consequences from the unwanted event. For example, the risk of a total large petroleum storage tank structural failure might be .003 per year. If there are multiple events that must happen before a major loss can occur then assigning numerical probabilities allows for risk calculations that are normally not possible with qualitative or semi-qualitative data.

Structurally, the field of knowledge comprises two areas: the area of uncertainty and the area of certainty. The uncertainty area corresponds to a qualitative knowledge of system's status and a transient knowledge of each status in a given situation. The uncertainty can be associated to the existing inaccuracy concerning one of the system's status using a probability density, which allows to characterize the deviations from a mean value [1]. This approach represents one of the bases of the fuzzy logic. The certainty area corresponds to a deterministic knowledge of all the system's status and their consequences.

THE CREDIBILITY OF SAFETY OBJECTIVES

A safety objective can be defined through the following two basic parameters:

- *denomination of an undesired event (e.g. outrunning of a maximal allowable limit for a noxious gas concentration);*
- *frequency or likelihood related to the undesired event, expressed in an adapted measuring unit.*

The credibility of a system's safety state is directly linked to the aimed safety level, which can be defined by:

- *the "ambition" of the safety objective;*
- *the confidence in achieving the proposed goal, starting from a well identified and documented ensemble of skills and tasks, clearly described in a safety plan.*

Available data for probabilistic techniques based assessments will be gathered after studies and actions carried out during the stages of design, development and operation of any systems. As a direct consequence, the real problem of safety objectives credibility arises. Most of the studies concerning the safe operation of technical and/or working systems are employing, as a tool, the modeling of accidents occurrence scenarios, whose credibility is characterized by:

- *the representativeness of models employed, specifically determined by the degree of comprehensibility, at his turn defined through the number of variables and parameters considered and the laws describing the significant relationships existing between the internal and external variables of the system;*
- *the credibility of data employed.*

Therefore, a so - called "natural" uncertainty concerning the procedures, results and their interpretation will appears. This should not be mixed up with the uncertainty related to the impossibility of undesired event's occurrence, event deployed in the safety objective. If, in the first case, can be studied and envisaged adequate prevention measures, in the second one the statement "such an event or such a scenario can not occur", will allow and - even - facilitate the perpetuation of a real unsafe state, with potentially catastrophic consequences.

ACCIDENT SCENARIO SELECTION IN INDUSTRIAL SAFETY STUDIES

The identification of scenarios able to lead to any undesired event highly depends on the expertise and imagination of the experts having as task the Preliminary Hazard Analysis for the studied system [10]. The list of the scenarios delivered in this stage will be not ranked, the only classification being done by framing the scenarios in one of the following categories:

- *S_1: Scenarios already observed and judged as realistic;*
- *S_2: Scenarios already observed, but judged as non - realistic, considering the existing prevention and control measures;*
- *S_3:Scenarios not met before in practice, but considered as realistic;*
- *S_4: Scenarios which were not encountered before and are considered highly improbable.*

The quality of judging the scenarios as realistic or not, depends on the amount of knowledge and skills of the assessment work team members and of the decision maker. The role of the decision maker is usually prevalent, due to his responsibility within the organization.

The dilemma of the decision maker, in the most of cases, consists in:

a. *Either to accept to consider a possible scenario considered "a priori" as having a low probability during the life cycle of the system. This kind of decision can generate supplementary technical, economical or operational compulsions.*
b. *Either to reject a scenario judged as improbable, accepting the possible consequences.*

It must be noted and stated that, depending on the considered component of risk (probability or gravity), the decision maker must pass from an extreme to another:

- *Considering only the low probability, the scenario will be rejected. This is a typical short - term decision.*
- *If the decision maker considers mainly the gravity of generated consequences, the scenario will be retained and will support further detailed analysis, indifferently of his occurrence likelihood. In this case, the decision is aimed to be as a long - term one.*

In the uncertainty area, an applicable decision rule regarding the taking into consideration of scenarios consists to allocate them "a priori" a certain likelihood level, starting from the objective associated with the analyzed undesired event. The level of likelihood can be assessed accepting, for example, the hypothesis that there can not exist more than 100 scenarios, identified or not, leading to the undesired event. There will be considered only the scenarios whose probability is with two magnitude orders lower that the probability of the unwanted event. So for an objective of 10^{-3}/h, there will be retained only the scenarios having an occurrence probability higher than 10^{-5}/h.

CONCLUSIONS ON THE USE OF PROBABILISTIC TECHNIQUES IN SAFETY STUDIES

Resorting to quantitative risk assessment techniques has as basic goal a detailed evaluation of the safety level in a working system, in order to achieve a significant improvement of the existing or designed systems safety level. The basic tool employed in quantitative assessment is the probabilistic computation, which offers various specific advantages, such as:

- *yields itself to mathematical processing of data;*
- *facilitates a better rational distribution of involved accountabilities, through the limitation of erroneous interpretations;*
- *emphasize the weight which should be allocated to each prevention and/or protection measure;*
- *facilitates the ranking of occupational accidents scenarios and the elimination of those who are unlikely to occur;*
- *leads, for any part of the system, to the optimization of design and to a better evaluation of the reached and proved safety level;*
- *according to the obtained results, it allows a more efficient estimation of the importance of "weak points" existing in the system, from the safety state point of view.*
- *The use of probabilistic language without discrimination can lead to two major drawbacks:*
- *an unwarranted increase of expenses for experimental work if the objective consists in a statistical demonstration of the reached safety level, an objective which is practically difficult to achieve;*
- *a limitation, or even a diminishment, of the "confirmed" safety level, in the case when there are considered only the absolute values of probabilities accepted based on experience acquired on comparable systems, previously analyzed.*

In the real world, however, managing risks frequently requires more than a series of calculations indicating something is sufficiently .safe.. It is not uncommon for people to demand additional safety precautions, or to decide a project is simply too risky, despite the results of quantitative analysis. Our perceptions shape all of our decisions about risky activities, from crossing a street to making a financial investment. Unfortunately for technical analysts, however, both our perceptions and our decisions related to risk are complex. They even appear irrational: someone may pass up one risk as unacceptably high, but then and accept another, technically higher, risk without hesitation. This is not necessarily irrational. It may simply be more complicated behavior than we are accounting for.

REFERENCES

[1] Bessis, J., La probabilité et l'évaluation des risques, Edition MASSON, Paris, 1984.

[2] Darabont, A., Pece, Şt., Dăscălescu A., Managementul securităţii şi sănătăţii în muncă (vol. I, II), Editura Agir, Bucureşti, 2002.

[3] Desroches, A., Concepts et méthodes probabilistes de base de la sécurité. Editions Lavoisier TEC&DOC, Paris, 1995.

[4] Joy, J., Griffiths, D., National minerals industry safety and health risk assessment guideline, version 3, March 2008, MCA and MISHC, Australia, www.planning.nsw.gov.au, Accessed at 20 August 2012

[5] Less, F.P., Loss Prevention in Process Industries (vol. I, II), Butterworths, London, U.K., 1980.

[6] Moraru, R., Băbuţ, G., Matei, I., Ghid pentru evaluarea riscurilor profesionale, Editura Focus, Petroşani, 2002.

[7] Moraru, R., Băbuţ, G., Analiză de risc, Editura Universitas, Petroşani, 2000.

[8] Moraru, R.I., Băbuţ, G.B., Participatory risk assessment and management: a practical guide, FOCUS Publishing House, Petroşani, Romania, 2010

[9] Paques, J.J., Gauthier, F., Pérez, A., Charpentier, F., Bilan raisonné des outils d'appréciation des risques associés aux machines industrielles, R-459, IRSST, Canada, 2006 (www.irsst.qc.ca).

[10] * * *, Guidance on risk assessment at work, European Commission, Luxembourg, Office for Official Publications of the European Communities, 1996.