HUNGARIAN JOURNAL
OF INDUSTRIAL CHEMISTRY
VESZPRÉM
Vol. 38(2). pp. 193-196 (2010)

RISK METHODS AND CHANCE OF PRACTICES

G. N. TÓTH[1], L. BEREK[2]

[1]University of Obuda, 1081 Budapest Népszínház utca 8, HUNGARY
E-mail: toth.georgina@bgk.uni-obuda.hu
[2]Zrínyi Miklós University of National Defence
E-mail: berek.lajos@zmne.hu

Risk analysis is made in several fields of science, moreover in business, manufacturing, protection of enviroment, disaster recovery, hygiene, labour safety, or in the increasingly important information security. Laws and standards control the risk assessement in many cases, however they don't contain any guide for the execution. The aim of this article is to highlight some well-defined risk analysis methods in my article and shortly present the possible adaptations thereof. In case of different processes the most difficult task is to adjust the processes to the problems in a way, which enables to minimize deviations and faults resulting from men's subjective judgement. Both qualitative and quantitative processes are contained the methods, and advantages, disadvantages, application possibilities thereof in details are presented.

Keywords: Risk methods, risk management software

Introduction

Many forces are obliging safety design; legal requirements, quality, costs, market and international influences, competition, the desire to have knowledge and the costs of retraining engineers.

The aim of the risk assessment is to reduce risks to a tolerable level. Many times the zero risk level is not realizable.

Risk assesment

Although many industries use different risk assessment methods, the traditional risk assessment process includes the same basic steps:

- identify risks,
- assess risk,
- minimize risk,
- accept remainder risks
- documenting the results and continuous monitoring

In many cases individuals or organizations start with a going risk assessment method, but it's not always suitable. So they need better methods. The research could take one of two paths. One of them, that looks for other methods and adopts all. The other one that modifies an extant technique to create a method better suited for the given application. [1, 2, 3]

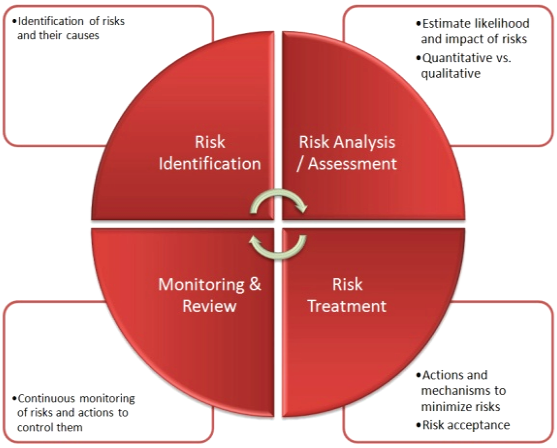

Figure 1: Process of the risk assesment [4]

A cleary distinction is usually made among three main types of methods, as two primary ones and hybrid methods of risk which are the mixture of the two above ones:

- Qualitative methods
- Quantitative methods
- Hybrid methods

In this arrticle these types and some risk assessment methods are presented [2, 3].

Qualitative risk analysis methods

In these methods risk is analyzed with the help of adjectives without using mathematical tools.

Qualitative methods are simple and easy to use but in some cases result in inconsistent outcomes.

Such techniques don't use tools like mathematics and statistics to model the situation. The results of method are mostly depended on the team. The problem of the qualitative methods are the subjective results thereof. [1, 2, 3]

Quantitative risk analysis methods

These methods use statistical and mathematical tools to estimate risks. In course of quantitative risk analysis methods intensive mathematical measures are used to model different types of risks, due to the enviromental elements, the model applied, furthermore the subject of the model istelf are complex. Today's complex risk situations cannot be modelled only by using quantitative methods. [1, 2, 3]

Hybrid method

A selected combination of the previous two methods. These methods are generally applied to implement the components utilizing pieces of information and minimizing the metrics to be calculated and collected. Fewer numerical calculations and cheapness compared to a fully deep analysis are the advantages. [1, 2]

Risk analysis methods, techniques

Hazard and Operability studies(HAZOP)

The HAZOP was developed in the 1970s by Imperial Chemical Industries Ltd. This technique is generally known as an application of a formal systematic critical examination of the process and engineering intentions of new or existing facilities. With the HAZOP tool the hazard potential arising from deviation in design specifications and the consequential effects on the facilities as a whole is assessed.

Hazard and Operability studies can be used to hazard analysis. Problems and threats are explored systematically. The methods are widely applied in chemical industries.

The advantage of the method is that the modification of the components can be easily followed and any deviations to the limits and pertaining effects can be checked.

On the other hand, experts are only in the position to utilize them in an appropriate way, furthermore, the methods are time and cost consuming. [5, 6]

CRAMM (CCTA Risk Analysis and Management Method)

CRAMM is applied in IT security. It is a qualitative risk analysis and management tool. It is developed by UK government's Central Computer and Telecommunications Agency in 1985. It's a method for information systems security reviews.

Figure 2: CRAMM process [8]

The method provides the risks of the threats in details, however, it needs waste of time and resources, hence the daily usage thereof is expensive.

CRAMM modell comprises three basic components needed for an occurance of a security occasion (attack):

- Threat
- Asset
- Vulnerability

As a result of the above elements the measure of the risk can be determined as a product of threat, vulnerability and asset values:

Risk = Threat * Asset * Vulnerability

CRAMM modell consists of three levels. On the first level security considerations are determined. The second level means the assessment of the risks. The third one comprises the elaborating of the defensive measures. [1, 7]

Tree based techniques

The tree based technique is considered a multidisciplinary tool, successfully applied in several fields of studies.

It is generally utilized in some territories of quality assurance and it is a widely used application in IT to visualize database structures (binary tree). It is also capable to easily access to data in course of programming.

The tree based technique is a graphical tool, which enables to user to present different types of relationships (hierarchical, horizontal).

The quantification of the results is halting, nevertheless the method can be easily used to demonstrate the logical relations.

In such a case, the relations among the components can be described with "logical operators".

It is basically applied as a part of cause-consequence technique in quality assurance, and in FMEA procedures as well.

A tree diagramms have couple of types: fault-tree analysis(FTA), event-tree analysis(ETA), cause-consequence analysis(CCA), management oversight risk tree(MORT) and safety management organisation review technique (SMORT).

The fauls tree is also capable for quantitative assessment, however, it is difficult that the users need to have great experience in the given field. [1, 5, 9]

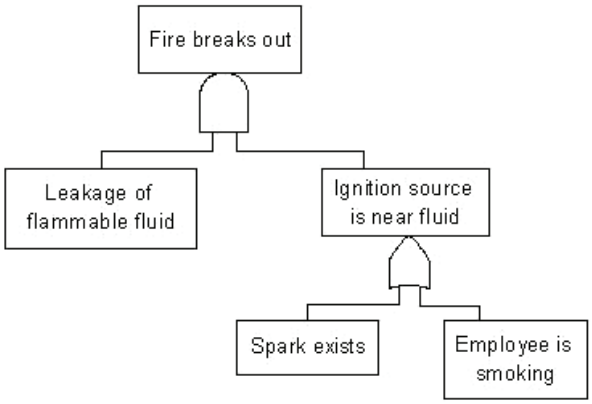

Figure 3: Example of the fault-tree analysis(FTA) [5]

FMEA-Failure Mode Effects and Analysis

A FMEA process was successfully introduced in Ford automobil company. It is practically to apply this process both in product develompent and technology planning.

The omissions, the possibility and consequencies of the construction and the steps of the manufactoring process in case of either products or technology can be explored by using this method.

The process itself is construed as an inductive method, in course of which omissions, causes of fauls and consequencies of the occurance likelihood systematically explored are scored in 1 to 10 scale from severity (S), occurrence (O) and detection (D) perspective.

In course of setting up the scale the specific nature of the given field, additionally, the human subjectivity may present difficulty.

Risk Priority Number (RPN) can be determined from the product generated based on the points, which RPN is capable for ranking each sources of threats.

$$RPN = S*O*D$$

where: RPN- Risk Priority Number
S- severity
O- occurrence
D- detection.

In the assessment process by using Pareto-diagramm, risk components which need action can be determined.

Following the decrease of risk value it is practical to re-determine the value of RPN, then being aware of remainder risk continue the evaulated activity.

From time to time a review needs to be made for a continuous development.

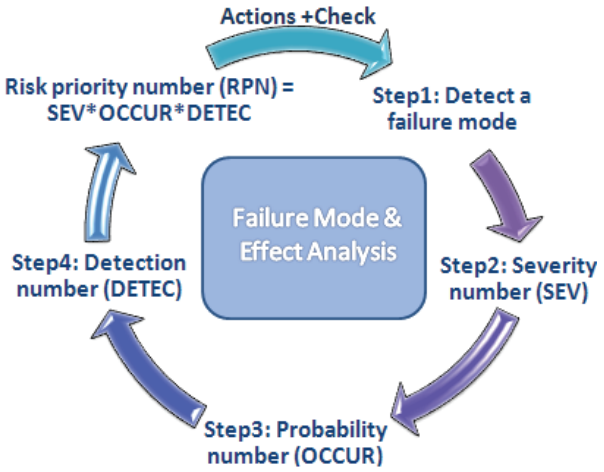

Figure 4: Steps of the FMEA process [10]

Providing a detailed overview on the vulnerability of a system by using simple mathematical operations is the advantage of the method, but at the same time the pre-knowledge of the process is needed and practical experiences regarding the system and the awareness of test results are essential.

We can receive Failure mode, effects and criticality analysis (FMECA) by extending FMEA, as a result of which the most critical failaure of the investigated system can be determined.

In most recent days the process can be made more effective with computer-supported team work [4, 5, 9].

Risk management softwares

A couple of softwers providing the aforementioned methods are accessible in the software market. All of them promise easy applicability, however in most cases it is difficult to implement a tailor made method as per the need of the company.

Most of the computer programs are capable for easing the administration, but are not suitable for solving problems resulting from the usage of the method.

I tried some risk softwares. I would like to emphasize SKILL Designer Pro /FMEA software relating to FMEA method.

It makes easy to handle the complicated administration of the FMEA documents and linkage thereof.

Virtual teamwork can be executed provided some conditions exist.

I examined one of the most general software, Risk optimizer 5.5, which enables to prepare risk assessment.

By relating to Microsoft Excel, the platform is not strange for the user.

We can calculate the risk costs and easy to choose the most economical results

Conclusion

Risk analysis is made in several fields of science, moreover in business, manufacturing, protection of enviroment, disaster recovery, hygiene, labour safety, or in the increasingly important information security. Laws and standards control the risk assessement in many cases, however they don't contain any guide for the execution. Some risk methods are executed in the article.

After the grouping of the methods, three techniques are presented in general, which techniques are used in different fields.

Methods can be implemented to a given bulk of problems.

Finally, I have dealt with a couple of risk assessment supporting programs and summarized my experience thereon.

REFERENCES

1. SANS Institute InfoSec Reading Room; A Qualitative Risk Analysis and Management Tool –CRAMM, SANS Institute 2002. (http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83) (2010.08.17.)
2. J. W. MERITT: CISSP: A Method for Quantitative Risk Analysis 22nd National Information Systems Security Conference 1999 October 18-21. (http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf) (2010.08.17.)
3. B. KARABACAK, I. SOGUKPINAR: ISRAM: information security risk analysis method, Computers & Security, 24 (2), March 2005, 147–159.
4. http://gpengineering.co.uk/Risk_Method_Management.html (2010.08.17.)
5. TAN HIAP KEONG: Risk Analysis Methodologies. (http://pachome1.pacific.net.sg/~thk/risk.html) (2010.08.18.)
6. G. CSEH: A hazai veszélyes üzemek által súlyos baleseti veszélyek azonosítására és kockázatok értékelésére alkalmazott módszerek összehasonlító vizsgálata Internetes publikáció. /In: www.mbf.hu/seveso2.html/ Magyar Műszaki Biztonsági Hivatal. 2004.09.11. 30p.
7. CRAMM modell. (http://hu.wikipedia.org/wiki/Cramm-modell) (2010.08.18)
8. Risk management as taught at Meerkat Manor – (CRAMM Lite – the "R" in "ROC" analysis) 23 January 2010. (http://thinkingproblemmanagement.blogspot.com/2007/10/risk-management-as-taught-by-meerkat.html) (2010.08.19.)
9. J. KALAPÁCS: Minőségirányítás, minőségtechnikák, X-Level Kft. 2001. Budapest p. 506 pp. 555-560. (ISBN 9630049708)
10. http://commons.wikimedia.org/wiki/File:FMEA.png (2010.08.19.)