

GOOD PRACTICES IN THE FIELD OF THE RISK ANALYSIS WITH THE USAGE OF THE FMEA METHOD

Ilona Mańka, PhD

imanka@wsb.edu.pl

University of Dąbrowa Górnicza, Poland

Abstract

In the article there were presented good practices in the field of the risk analysis in the project by the FMEA method, which were collected on the basis of author's longstanding experiences, achieved during investigations. There were indicated typical problems, which can be met during such analysis and ways of counteractions, as well as there were described and characterised basic elements of that method.

Key words: FMEA, project management, risk analysis.

Introduction

Every aspect of the people's activity requires of continuous decisions. Taking of decisions is an inevitable task of the company management or a project in particular. A person, who is obliged to take a decision, most often must act without complete information and data or that information is encumbered with uncertainty. The uncertainty is connected also with the future events, which are possible to foresee in some field. The possibility to provide, or more precise identification of dangers, is exactly a key element, which enables to prevent unfavourable events or to minimize losses in case of their appearance (Sitarz, Chruzik 2010; Borysiewicz et al. 2000). Skill of a dangers identification, search of the weakest elements of realized undertakings and a possibility of earlier prevention can be the most important element, which enables not only on correct implementation of the singular project, but also on survival and development of the whole enterprise. In common opinion "A very good employer or a manager is a person, who takes decisions and faces their consequences and more than 50% of his decisions are good". It should be pointed out, that decisions taken on the basis of the risk analysis are undertaken inherently on the basis of knowledge

and experiences of an interdisciplinary group of people, which have great professional experience in the analysed field in principle. It allows not only to avoid a lot of surprises during the implementation of the project (which single person could not provided due to limited knowledge, education and professional experience), but also provide to a staff, that has a real possibility to influence on taking decisions in the company, integrate the personnel and support in the field of responsibility effect of singular people for quality of a manufacture or realized service (Romanowska-Słomka, Słomka 2008).

As shows many years experience of the author in the field of the risk analysis in the transport branch, the management in the first phase has approached the risk analysis with aversion and deal with it, as the following document to fill in. However, after description of a few examples during training and then after making that analysis individually, the risk analysis by the FMEA method was used not only to meet requirements of the safety systems, but also as a tool in every other moment, in which there was indispensable to identify a source of the problem and to define a method of its solution.

According to author's experience the risk analysis by the FMEA method is the most often used one in the railway branch, e.g. by approx. 98% of companies in Poland (Mańka, Wachnik 2010; Sitarz 2009; Sitarz, Chruzik 2010). It should be also underlined, that the rest of the companies make use mainly of modified COSO II method, which is counted and compatible to the FMEA method with the concept.

1. The FMEA Method

In spite of a lot of risk management methods, the most common used is the FMEA method (Failure Mode and Effect Analysis) – „Analysis of causes and effects of faults”. That method is also often used for the risk analysis in the project, and then we can find pFMEA designation. However, taking into account the method of the analysis and the estimation of adequate indicators, it does not diverge from the FMEA method.

The method by itself was developed in the United States and issued 9th of November 1949 as MIL-P 1629. It was applied, among other thing, in armaments industry, including by NASA in space programmes (Apollo) and in Florida from 70's, the FMEA standard is included in SAE J-1739, IEC 60812 i QS-9000 at present (Mańka, Wachnik 2010).

The risk analysis by the FMEA method was described in PN-EN 60812 standard “Analysis techniques for system reliability – Procedure for failure mode and effect analysis” (FMEA) relate mainly to motor branch, which indicate to for example, multiserial, unfortunately presented examples

cannot be directly refer to other branches, including e.g. the risk management in the project.

In this method at first the owner of the project management procedure constitutes a interdisciplinary working group, which should consist of representatives of the whole company, for example (Sitarz 2009):

- moderator (is a person, who supervises the FMEA analysis and look for proper atmosphere and analysis),
- labourer (operator),
- technology,
- production engineering,
- process engineering,
- design engineer,
- logistician,
- supplier,
- other workers, who can contribute in an essential way to the conducted analysis, including also a customer.

During the analysis, there are determined coefficients: Zn (meaning of the risk), Pr (probability of appearance) i Dt (possibility of detection), which have values from 1 to 10, and next measuring their product, a risk priority number RPN (Risk Priority Number) is characterized and referred to acceptable value set in the enterprise or imposed by the customer – RPN_{dop} (e.g.: 100). According to PN-EN 60812 standard these coefficients are adequately Sr, Oc i Dt. However, considering the facility of memorizing in Polish language, there were proposed above named symbols. In practice, the most often used is $RPN_{dop} = 120 \div 150$. Getting a value exceeding RPN_{dop} for any process, causes the necessity to characterize preventive and corrective actions together with indispensable means and to appoint a responsible person and time of implementation of these actions (PN-EN 60812; Mańka, Wachnik 2010; Sitarz 2009).

$$\begin{array}{ccccccc}
 & & RPN = Zn \cdot Pr \cdot Dt & & & & \\
 & 1-1000 & 1-10 & 1-10 & 1-10 & & (1)
 \end{array}$$

Next stage of the risk analysis in the project is to define by the participants of the working group results of conceivable faults and threats and then to specify their meaning. Meaning of fault or threat are characterised numerally (Zn) in the field from 1 to 10. When faults and threats are defined, potential causes of their formation should be fixed. On that stage, there are necessary the knowledge and experience of the participants of the FMEA interdisciplinary group and systematic causal link approach to the problem. It is recommended to use tools of the Ishikawa diagram type. The 5-WHY

method is the other helpful tool to establish reasons of faults and effects of unauthorized events, which are specified in the FMEA as the risk (Mańka, Wachnik 2010; Sitarz 2009).

The best way to carry out the method of „five questions why” is to write the following answers in order to all the participants of the FMEA working group could see them. That very easy and fast method of the following asking questions „but why it does happen” allows to find a real reason of faults arising. The number of question is not required obviously. It should be noticed here, that the result „operator error” or „error of a person directly connected with the process” can in fact come from defects or faults of the organization system, method of work or course of processes.

The probability of appearance of different faults or effects of unauthorized events in the project can be distant. In order to make possible to give direction of activities to these faults, which result is significant and at the same time there is a great probability of its appearance, during the FMEA analysis it is advisable to characterise Pr value, which it describes.

Next stage of the FMEA analysis is to define used means of fault prevention at present and description of detection measures of these faults. In order to evaluate the possibility of detection (Dt) it should be used the classification of the possibility of the detection, also in the scale 1-10. The greater possibility of earlier detection of the fault, the lowest assigned value of that coefficient, in opposite to two other components.

In the event, when the risk analysis by the FMEA method is conducted by the interdisciplinary group, there is a problem with a subjectivism of the threat’s evaluation by different members of the group. Therefore, it is effective to prepare tables with a reference of individual values to verbal and quality description. These tables are recommended to use in the first analyses in order to prevent divergences in the greatest degree as possible. However, in the subsequent analyses, more important are an expert knowledge, the best branch practices and legal requirements, which will be related to the particular threats individually.

2. Good practices in the field of the risk analysis using FMEA method

Instruction:

1. **Ensure, that** on all key stages of the project, and as an indispensable minimum on its initial stage, **the risk analysis was provided** – e.g. by including such requirement in the quality system of the company (ISO, series 9000 or branch systems). Within a framework of the quality system, it is also necessary to take into account results of the risk analysis, as a subject of the evaluation

during internal audits. These results should be initial data for activities included in the strategy of the company;

2. **Set up an interdisciplinary group of people for the risk analysis.** These people should have special training in the field of the risk analysis by the FMEA method, and, first of all, should have indispensable knowledge and experience in the field of the realized project. In the risk analysis should participate people, who in competent way complete the whole area of the company's activity, which has influence on the quality of the product or service. It should be remembered, that the risk analysis without participation of the experts from key company branches is a mistake and the results can be counter-productive!
3. **Prepare information about the project,** indispensable initial data, present briefly the project or the problem (if there is no certainty, that all the people know the subject in the same degree). Verify if there was no risk analysis for the similar project. If there was one, download the threats, in order to analyze their validity in the current project;
4. **Hold a meeting** in such a way, that **according to the FMEA** method to guarantee the identification of the key threats, their correct evaluation and proper correct or preventive operations. Detailed guidelines to this point are listed below.
5. **Make sure, that for all the correct and preventive operations have assigned a responsible person, fixed date of implementation, as well as specified and secured means.** Without such settlements the risk analysis would not be effective.
6. **Ensure, that the repeated risk analysis will be carried out after the correct and preventive operations** in order to verify, if the goal was achieved, e.g. if the risk in the determinate field is permissible.

The most important factor, which influence on sense and effectiveness of the risk analysis is the staff consciousness (in particular of the highest level of management) of the goal and possibilities of the analysis and the knowledge on the method and principles of its implementation. Typical errors repeatedly identified by the author during the risk analysis and means of prevention are listed below:

- presence and activity of a superior oriented to demonstrate an absence of threats, reflecting lack of the knowledge and understanding of the possibility and the objective of the risk analysis;
- steering of values in order to not exceed the permissible value – RPN_{dop} . The only use of such analysis is to identify the threats

and a chance, that in spite of low RPN values, somebody will deal with the problem;

- no possibility to get a coherent estimation, mainly concerning the results of the threat e.g. „considerable differences in the threat evaluation”. Typical course of such analysis depends, that a part of the people proposes a very low value, on the level from 1 to 3, and the rest unequivocally and categorically demands very high ones, on the level between 8 and 10. That situation is very often and it should be underlined, that in the majority, both groups are right in the field of proposed values of the threat. The problem depends here on low-precise description of the analyzed threat and a lack of its full scenario. Often the results of the threats can be double-sized e.g. most often their effect appears relatively frequently and causes “small” results. It is also possible to form the worst reliable scenario, which – at the corresponding unfavorable coincidence – can bring on very serious consequences. An example (not from the branch) can be a lack of fasten seat belts during drive. In most cases, the effect of the drive without the seat belts will be a possible fine. However, it is also possible a situation, which will cause a frontal collision with other obstacle. Therefore, is there the drive without fasten seat belts safe or not? In such situations, the event should be divided on two separate (two independent lines in the FMEA table) and in one analyze the drive without the seat belts together with the scenario, which will be relatively often (but results will be small) and in the second one, take into account the drive without the seat belts, during which additionally the frontal collision occurs. It should be noticed, that in the second case a probability of simultaneous drive without the seat belts and collision is considerably lower, than the treat in the first variant, but the results will be on the highest level. A breakdown of the threat on the two separate will allow not only to mitigate a dispute during the meeting, but mainly will enable to make an efficient decision regarding probable correct and preventive operations. In the analyzed case, it can be deduced (despite the author do not put up to drive without fasten seat belts), that in the case, when the driver had to take a decision to drive without the seat belts, he knows the threat and can choose (decision) both in a situation of everyday drive to work, and in the emergency situations (transport of a person, who needs urgent medical help to the hospital). Therefore, it is important to present precisely the scenario of events to all participants of the meeting and possible break down

- of that scenario on two or more independent ones, in order to enable their evaluation and influence on safety of the project;
- taking into account only threats of technical character without organizational and economic ones or only own threats and omit common threats, which proceed as a result of cooperation with other subject, or external threats independent of the company's activity. In this case indispensable is the experience and the knowledge of the manager of the risk analysis – a moderator. The moderator should not suggest the values, which describe threat, but he can indicate different areas of the company's activity. Taking into account presented above types of threats, he should point also these groups of the threats, which were ignored by the interdisciplinary group of the risk analysis. In this case helpful is a control list with listed types of the threats or elements of the process or stages of the project;
 - evaluation of the threat results of value other than maximum, in the event when the result can cause a demise of the company, no possibility to realise the project or when the human life is menaced. It is essential to establish, which results are impermissible due to legal requirements, customer's requirement or professional ethics etc. and for these threats consequently should be values of significance /threat's results on the level of 10. It can be also stated, that generally, when the threat's result is estimated, it is better to inflate the value than write the medium value. It should be noticed here, that the threat's result can be evaluated and verified by any specialist from the branch, who can name possible irregularity in the analysis and accuse of an intentional underrate the value. The value of the probability of appearance and possibility of detection is subjective estimated including many years of practice in the enterprise or implementation of similar projects
 - a groundless change of the value regarding the threat's result in case of the repeated risk analysis after the correct and preventive operations. When the threat was evaluated originally on the specified level and after the correct or preventive operations, effective methods of prevention or the threat's detection were introduced, it is proper to make allowance for these operations during estimation of the probability of the threat or the possibility of its detection or prevention. However, it should be taken into consideration, that the correct and preventive operations usually do not change its results. Hence, the principle of rewriting of value regarding results from the original analysis to the analysis in the repetitive

estimation of the effectiveness of the correct and preventive operations (right part of the FMEA table);

- taking into account the threats, which are not connected with the subject and the goal of the risk analysis. Generally, all threats for the process or the project should be taken into consideration. These threats, which are not connected with the objective or the domain of analysis, should be omitted. However, there are exceptions to that principle, resulting from legal or normative requirements, which refer to e.g. product, service or ethics' rules. The example is life or health risk of a human, in spite of it could not has a direct influence on the implementation of the project or functioning of the company, it should be allowed as a superior aim of the analysis, not only due to legal requirements in this field.

For example, analysing possibility of implementation of a project connected with launching of a new production line, it is a good practice to carry out a risk's analysis, in which will be participated specialists of all fields of the project. A moderator should carry on discussion giving examples of threats, which are not only connected with technical aspects of the implementation, but also financial side, terms, legal aspects, human and technical resources in a broad sense. During the risk's analysis he should inspire the group to creativity and brainstorming, and should not impose his opinion. Finally, the risk's analysis creates a basis to channel appropriate financial means and resources, as well as counteraction of threats in the proper time and range. It gives the company the possibility to earlier prevention and to gain maximum profit with a minimal losses.

Conclusions

In conclusion, the FMEA method is used in management of the risk in the project or the risk of all aspects of the company's activity. That is a very effective tool of the threats' search and counteraction of them on the stage, where lower costs are generated by excluding events, consequences of which should be a serious danger, not only for the project, but also for the whole enterprise. Simultaneously that method enables to indicate areas, which in the first place should be included by the correct and preventive operations, in other words special hierarchization of these threats. Additionally, good practices increase effectiveness of the analysis and allow to prevent unfavourable situations e.g. during the meeting of the interdisciplinary group lead by the moderator.

References

1. Borysiewicz, M., Furtek, A., Potemski, S. (2000), Poradnik metod ocen ryzyka związanego z niebezpiecznymi instalacjami procesowymi. Instytut Energii Atomowej, Otwock – Świerk.
2. Mańka, A., Wachnik, R. (2010), Technical risk analysis of railway vehicle. Journal of Konbin, Vol. 14-15, pp. 351-358.
3. PN-EN 60812: 2009 Techniki analizy nieuszkodzalności systemów – procedura analizy rodzajów i skutków uszkodzeń (FMEA).
4. Romanowska-Słomka I., Słomka A., (2008), Ryzyko zawodowe. Procedury, metody, zagrożenia. Ośrodek Szkolenia PIP, Wrocław.
4. Sitarz M., Chruzik, K., Mańka, I. (2010), Zintegrowany system zarządzania bezpieczeństwem w transporcie kolejowym. System zarządzania bezpieczeństwem – podejście procesowe. Technika Transportu Szynowego (TTS), Łódź 7-8.
4. Sitarz M. (Ed.), (2009), Zintegrowany system i środki transportu w Polsce. Ocena ryzyka technicznego w transporcie kolejowym realizowana według wymagań normatywnych IRIS oraz RAMS. Katowice, pp. 142-151.