Tchórzewska-Cieślak Barbara

Pietrucha-Urbanik Katarzyna

Szpak Dawid
Rzeszow University of Technology, Rzeszow, Poland

The use of the FMEA method in the analysis and assessment of technical systems safety

Keywords

FMEA, risk, safety, failure analysis.

Abstract

The analysis and assessment of the protection of technical system was performed using the FMEA method (Failure Mode and Effect Analysis). The FMEA method allows the product or process to be analysed, to identify weak points, and then introduce corrections and new solutions to eliminate sources of undesirable events. The developed methodology was presented on the example.

1. Introduction

The failure modes and effects analysis (FMEA) method is a technique for determining the ways in which equipment can fail and the consequences of the failure in terms of reliability and safety. The FMEA method belongs to one of the most frequently used tools for quality planning and management analysis and risk assessment because of its versatility. The method of failure modes and effects analysis has been developed for the Apollo space program in the 1960s, as to verify the designs of spacecrafts in order to ensure maximum safety of astronauts. Since that time it is widely used in whole industry, as chemical, electronic, construction, etc. Risk analysis is a key phase of the process of water supply safety management. It consists of threats identification and qualification of their consequences and frequency. Sources of information about the operation of water supply facilities are in the determined form, through standards, regulations, orders and sometimes in the probabilistic form, as field tests, modelling and simulation [1, 6, 7, 12, 13, 20, 21]. The FMEA method can be applied in different areas, it depends on the analysed system and the planned objectives. The failure modes and effects analysis constitutes an inductive method of risk analysis, which for the assumed failure of the component seeks the successive events and determines the possible final effects. The FMEA can be applied at the level of systems, subsystems and components [4, 8, 15]. Before taking decision on the scope and application of the FMEA in a particular system or element it is necessary to consider the overall life-time of the system as well as other activities. The procedure of the FMEA includes many stages, as defining the system and its decomposition into subsystems, objects and elements. Components of the system have the possible failures assigned to them, then the frequency of occurrence and the possibility of detection and prevention are determined and the potential effects and consequences are analysed [IEC 60812]. Also the FMEA analysis include evaluation and assessment of risk associated with various types of threats. The qualitative result of the FMEA is a list of potential threats to technical system users safety. The significance of threat is determined by different parameters with associated point weights [11, 14, 18]. The quantitative result of the FMEA is risk estimation through the point weights, so the final result of the FMEA is the determination of the risk priority number RPN. In the paper the method of analysis and safety assessment of technical system was presented using the failure mode and effects analysis method (FMEA), which assumes independence of events. The developed model was presented on the example of analysis of risk of failure of the technical system.

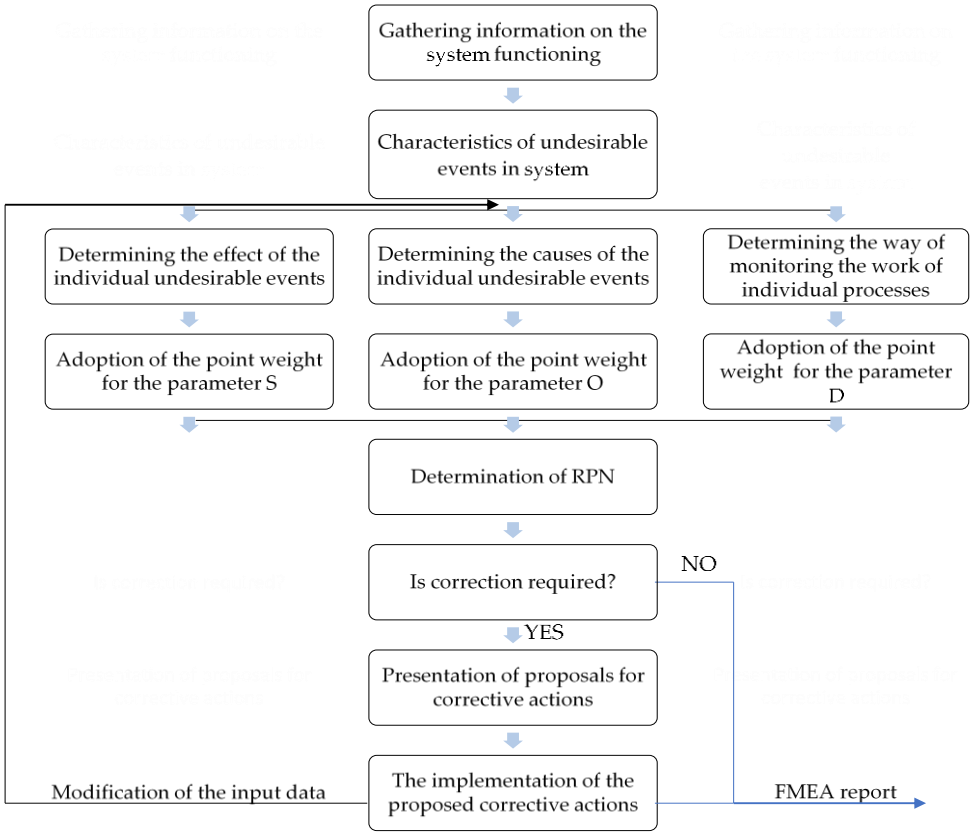

Figure 1. Conventional analysis process of FMEA, on the basis of [10, 19]

2. The use of the FMEA method to analyze the risk of failure in technical system

The main objectives of the FMEA analysis, in accordance with the principle of "continuous improvement", include eliminating defects in the product or production process by recognizing the reasons for their appearance, taking appropriate preventive actions, avoiding the emergence of recognized and hypothetical defects in new products or processes through the use of knowledge and experience with previous analyzes [3, 5].

The method of performing FMEA analysis in the technical system is shown in Figure 1 [10, 19].

Technical assessment of the safety system can be performed using the FMEA method, on the basis of Risk Priority Number - RPN, according to the formula [3, 10, 16, 19]:

$$RPN = S \cdot O \cdot D \qquad (1)$$

where:

S – point weight associated with the importance of undesirable event, severity,

O – point weight associated with the frequency of undesirable event, occurrence,

D – point weight associated with the ability to detect undesirable event, detection.

The individual parameters are described by an integer from 1 to 10, which is assumed on the basis of expert knowledge and experience of technical system exploiter. The result of the analysis is the RPN, taking values ranging from 1 to 1000. The higher RPN value, the lower level of safety. The input criteria for the individual parameters are assumed on the basis of the information contained in Tables 1-3, according to work [19]. The general assumptions of the method are as follows:

- undesirable events are random, they are inseparable from the functioning of the technical system,
- early identification of potential undesirable events and the introduction of corrective or remedies actions allow to significantly reduce the frequency of these events,
- each undesirable event has a specific cause and effect. The method allows to establish cause and effect relationships in the occurrence of individual undesirable events.

The final effect of the analysis is the value of RPN, which can be the basis for adopting the proper management plan, as well as for identifying the weak points of the system. Complete elimination of the causes of undesirable events is impossible, therefore

measures should be taken to reduce their frequency, reduce the adverse effects of undesirable events and increase the possibilities of their detection.

The safety assessment is based on comparison of the obtained value with the adopted scale. In the paper five levels of safety were proposed [14, 19]:

- neglected level of safety (NLS) – RPN ≤ 20, in which as a result of the technical system operation there is not any threat to users lives or health,
- tolerable level of safety (TLS) – 20 < RPN ≤ 40, in which as a result of the technical system operation there is not any threat to users lives or health, however, may be felt slight inconvenience associated with its operation,
- controlled level of safety (CLS) – 40 < RPN ≤ 60, in which as a result of the technical system operation, there may be a threat to users' health, but there are sufficient safety barriers,
- intolerable level of safety (ILS) – 60 < RPN ≤ 100, in which as a result of the technical system operation, there may be a threat to users' health,
- unacceptable level of safety (ULS) – RPN > 100, beyond which as a result of the technical system operation users are at risk of loss of health or lives.

Table 1. The assessment criteria and point weights for the importance of undesirable event – parameter S, on the basis of [9, 10, 19, 23]

Importance of undesirable event	Linguistic description	Point weight of *S* parameter
very low	There is no discernible effects, failure does not affect functioning of the technical system	1
low	Disruptions in the operation of individual subsystems are not felt by the technical system users	2
		3
moderate	Disruptions in the operation of individual subsystems cause a high degree of dissatisfaction by the technical system users	4
		5
		6
high	The system does not work, there may be a threat to the technical system users' health	7
		8
very high	Undesirable event is a threat to the technical system users' health and lives	9
		10

Table 2. The assessment criteria and point weights for the frequency of undesirable event – *O* parameter, on the basis of [9, 10, 19, 23]

Probability of undesirable event	Frequency occurrence	Point weight of *O* parameter
very low	> 1 for 20 000 d	1
low	(1 for 4000 d – 1 for 20 000 d>	2
	(1 for 1000 d – 1 for 4000 d>	3
moderate	(1 for 400 d – 1 for 1000 d>	4
	(1 for 80 d – 1 for 400 d>	5
	(1 for 40 d – 1 for 80 d>	6
high	(1 for 20 d – 1 for 40 d>	7
	(1 for 8 d – 1 for 20 d>	8
very high	(1for 2 d – 1 for 8 d>	9
	< 1 for 2 d	10

Table 3. The assessment criteria and point weights for the possibility of not detecting the undesirable event – parameter D, on the basis of [9, 10, 19, 23]

Not detecting the undesirable event	Linguistic description	Point weight of *D* parameter
very low	Complete monitoring, on-line equipment, potential undesirable event almost certainly will be detected	1
low	Potential undesirable event is detected by automated checks, which lead to error detection and protection from its development	2
		3
moderate	Undesirable event will not be detected until the loss of productivity	4
		5
		6
high	Undesirable event will not be detected until inspection	7
		8
very high	There is no monitoring system, there is no chance to detect potential undesirable event	9
		10

3. Analysis of the risk of interference in the functioning of the seaport using FMEA

Cause-and-effect analysis and assessment of undesirable events in seaports can be performed on the basis of conventional FMEA method. Based on the information contained in *Tables 1-3*, the appropriate values of parameters *S*, *O* and *D* should be assumed and the RPN value should be determined, according to Table 4. All potential undesirable events that may occur in a seaport should be analyzed. Table 4 should be complemented by the expert team taking into account the information presented in this article. Table 4 shows an example of analysis for one of the undesirable event.

FMEA method can be an important tool to improve products and processes for managing sea ports, primarily due to the fact that it is quite simple and clear tool. Nevertheless, FMEA can, however, be used to analyze very complex processes.

After determining the risk value, the next step should be to rank the undesirable events in terms of the threat posed to technical system users' and present proposals for corrective or remedies actions (after the given event has reached the NAPB level) and to test their effectiveness.

Corrective or remedies actions include, among others:

- developing a response plan in the event of a crisis situation,
- indication of persons responsible for corrective actions,
- informing the persons responsible for the operation of the technical system about the effects of potential negligence,
- proper organization of the work of renovation teams,
- regular employee training,
- regular inspections of technical condition of individual subsystems/elements,
- developing a method of providing users with information about the threat,
- successive renovation or replacement of the oldest elements of the technical system,
- proper monitoring of the technical system operation.

The main effect of the analysis should be to reduce the probability of occurrence of undesirable events and increase the possibility of their detection.

5. Conclusions

The FMEA method can be used to analyze the functioning of any technical system, including the sea port. It allows making decisions in the case of lack of complete information, based on the knowledge and experience of the technical system users and external experts. The proposed method can help to maintain or improve the safety of technical system. In case of lack of data or unreliable data the fuzzy approach can be applied, which can include different opinions and knowledge of experts. The determination of undesirable events that threaten the safety of the operation of technical system is based on the choice that distinguishes the consequences of failures. The performed analysis through identification types and symptoms of threats and the causes of failures can help in determining the effects of failures and create a ranking of criticality, as well as ways to prevent failures and establish projects for remedies actions. Adaptation of the FMEA method is based on the expert's method, from which it is also due to the possibility of its application. The FMEA method constitutes one of the firstly systemic approaches to the analysis of undesirable events in technical system. It can be performed starting from the level of a single element of the system or from the level of the whole system towards its constituent elements.

Table 4. Risk analysis – FMEA method, on the basis of [2, 3, 10, 19]

Phase of the process	Requirement/ Function/Characteristic	Potential type of failure	Potential effect of failure	Severity - *S*	Potential cause of failure	Prevention	Occurrence - *O*	Control	Detection - *D*	RPN	Rank
Ensuring the transport safety of the	Ship's entrance to the port	Ship collision with the construction of port	Ship damage	8	Human error	Developing a response plan in the event of a crisis, instruction/training of operators	4	Regular inspections of the technical condition of technical devices, monitoring of the operation of technical	3	96 NTPB	1
					Ship failure		3		3	72 NTPB	2
					Damage to technical devices		3		3	72 NTPB	2

Acknowledgements

The paper presents the results developed in the scope of the HAZARD project titled "Mitigating the Effects of Emergencies in Baltic Sea Region Ports" that has received funding from the Interreg Baltic Sea Region Programme 2014-2020 under grant agreement No #R023. https://blogit.utu.fi/hazard/

References

[1] Gilchrist, W. (1993). *Modeling failure mode and effect analysis*, International Journal of Quality & Reliability Management, 10(5), 16–23.

[2] Gucma, L. (2005). *Modelowanie czynników ryzyka zderzenia jednostek pływających z konstrukcjami portowymi i pełnomorskimi,* Wyd. 44, Studia - Akademia Morska w Szczecinie.

[3] Hamrol, A. & Mantura, W. (1999). *Zarządzanie jakością – teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa-Poznań.

[4] Hubbard, D.W. (2009). *The failure of risk management*, Wiley. New York.

[5] IEC 60812:2006. *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA).*

[6] Kołowrocki, K. & Soszyńska-Budny, J. (2011). *Reliability and Safety of Complex Technical Systems and Processes: Modeling – Identification – Prediction – Optimization.* Springer, London.

[7] Kołowrocki, K., Kuligowska, E. & Soszyńska-Budny, J. (2017). *Critical infrastructure operation process including operating environment threats.* Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars, 8(2), 7–14.

[8] Liu, H. C., Liu, L., Bian, Q. H., Lin, L., Dong, N. & Xu, P. C. (2011). *Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory*, Expert Systems with Applications, 38, 4403–4415.

[9] Liu, H.C., Liu, L. & Liu, N. (2013). *Risk evaluation approaches in failure mode and effects analysis: A literature review*, Expert Systems with Applications, 40, 828–838.

[10] Pillay, A. & Wang, J. (2003). *Modified failure mode and effects analysis using approximate*

reasoning, Reliability Engineering & System Safety, 79, 69–85.
[11] Rak J. (2009). *Bezpieczeństwo systemów zaopatrzenia w wodę*. PAN, Instytut Badań Systemowych. Warszawa.
[12] Rak, J., Pietrucha-Urbanik, K. (2015). *New directions for the protection and evolution of water supply systems - smart water supply*. Czasopismo Inżynierii Lądowej, Środowiska i Architektury - Journal of Civil Engineering, Environment And Architecture. JCEEA, z. 62 (3/I/2015), pp. 365-373. DOI: 10.7862/rb.2015.121
[13] Rak, J. & Tchórzewska-Cieślak, B. (2010). *The possible use of the FMEA method to ensure health safety of municipal water*, Journal of KONBiN 2010, No. 2, 3 (14, 15), 143–154.
[14] Rak, J. & Tchórzewska-Cieślak B. (2005). *Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę*. Oficyna Wydawnicza Politechniki Rzeszowskiej.
[15] Rak, J., Tchórzewska-Cieślak, B. & Studziński, J. (2013). *Bezpieczeństwo systemów zbiorowego zaopatrzenia w wodę*, Instytut Badań Systemowych PAN, Warszawa.
[16] Sharma, R.K., Kumar, D. & Kumar P. (2005). *Systematic failure mode effect analysis (FMEA) using fuzzy linguistic modelling*, International Journal of Quality & Reliability Management, 22(9), 986–1004.
[17] Stamatis, D. H. (1995). *Failure mode and effect analysis: FMEA from theory to execution,* ASQC Press, New York.
[18] Stewart, M. & Melchers, R. (1997). *Probabilistic risk assessment of engineering systems*, Copyright by Chapman and Hall, London.
[19] Szpak, D. (2017). *Method of water consumers safety analysis and assessment*. E3S Web of Conferences, 17, 00092, 1–8.
[20] Tchórzewska-Cieślak, B. & Szpak, D. (2015). *Propozycja metody analizy i oceny bezpieczeństwa dostawy wody,* Ochrona Środowiska, 37(3), 43–47.
[21] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2017). *Development of cause-effect dependence model of undesirable events using Bayes network*. 2017, Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 8(1), 149–156.
[22] Tchórzewska-Cieślak, B., Pietrucha-Urbanik, K. & Szpak, D. (2017). *Review of methods for identifying threats including the critical infrastructure systems within the Baltic Sea*. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 8(1),139–148.
[23] Wang, Y.M., Chin, K.S., Poon, G.K.K. & Yang, J.B. (2009). *Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean,* Expert Systems with Applications, 36, 1195–1207.