UDC 004.056.5 (045)

N.V.Pashchenko (National Aviation University, Ukraine)
V.M.Mokiichyk, PhD (National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute")
O.V.Samoilichenko, PhD (International School of Technical Legislation and Quality Management, Ukraine)

Failure mode and effects analysis for laboratory computer systems risk evaluation

The application of the failure mode and effects analysis for laboratory computer systems risk evaluation is considered.

Nowadays the national standards for testing (calibration) laboratories DSTU ISO/IEC 17025:2017 [1] and medical laboratories DSTU ISO/IEC 15189:2015 [2] accreditation are being implemented in Ukraine very actively. As part of their implementation, the need for computer systems for the laboratory processes is growing significantly.

There is a large selection of laboratory computer (information) systems in Ukraine. However, to select the necessary system that fully satisfies the tasks of a test, calibration or medical laboratory is quite difficult, since not all laboratory computer systems meet the desired quality characteristics and reflect the particular features of the laboratory. It is difficult to evaluate such system from the point of view of the user (the laboratory) and the auditors for compliance with standards [1] and [2].

Standards [1] and [2] indicate that laboratories in their work must take into account risks and opportunities, plan and implement management measures to improve the efficiency of the management system, improve results and prevent negative effects and potential failures. Also, these standards include requirements for information management systems in the laboratory (laboratory computer systems) such as unauthorized access protection, interference and data loss, record accuracy, data and information integrity, system failure logging, immediate relevant and corrective actions.

According to the DSTU ISO 31000:2018 "Risk Management. Principles and Guidelines" the risk management process consists of the following main stages: identification, analysis and risk evaluation.

The laboratory should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Risk analysis involves developing an understanding of the risk and it provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk

analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

To evaluate the risks of laboratory computer systems, it is suggested to use the FMEA method (Failure Mode and Effects Analysis). An FMEA is a design and engineering tool which analyzes potential failure modes within a system to determine the impact of those failures.

This is a method of systematic analysis of the system to identify types of potential failures, their causes and consequences, as well as the impact of failures on the functioning of the system (both the system as a whole and its components). The FMEA analysis can identify the severity of the consequences of potential failures and provide risk mitigation tools [3].

Usually the analysis is performed by identifying the types of failures, the corresponding causes, immediate and final consequences. The analytical results can be presented in the form of a worksheet containing the most significant information about the whole system and the details. The worksheet takes into account the ways of potential system failures, components and types of the systems failures as well as the failure cause's.

The type of failures analysis also leads to the criticality analysis. It determines a qualitative measure of the consequences of failure modes applying. The purpose of the criticality analysis is to qualitatively determine the relative magnitude of each failure effect. These values are used to prioritize actions to eliminate failures or reduce their consequences.

One of the methods for quantifying criticality is the Risk Priority Number (RPN) calculation. Each identified risk is evaluated by the following indicators: the severity of a failure, the implementation probability and the identifying probability. Indicators, in turn, have a quantitative rating scale. RPN is the product of the quantitative values of the assessed risk indicators. Further, the RPN determines the risk criticality and acceptability, the level and the necessary actions to manage the risk. Table 1 shows an example of the laboratory computer systems failure severities.

Table 1.

The severity of failure consequences

Value	Degree	Description
5	Catastrophic	Complete data loss without recovery
4	Critical	Partial loss of data with the possibility of long-term recovery
3	Medium	Partial loss of data with the possibility of fast recovery
2	Small	Failures in the system with the possibility of rapid recovery
1	Insignificant	Minor system errors that are automatically corrected

Considering the severity of the consequences, it is also necessary to take into account such consequences as a complete laboratory stoppage (catastrophic and critical consequences), work suspension (medium consequences) or without laboratory stoppage (small and insignificant consequences).

The laboratory computer systems risk implementation probability may depend on various factors and its value can be determined by the frequency of occurrence, for example every day, week, month exc. If the value of the implementation probability is equal 5 it indicates that the implementation probability risk is high and a system failure can occur every day.

The laboratory computer systems risk identifying probability means the ability to detect failure with the help of the anticipated control operations. For example, if the value of the identifying probability is equal 1 it means that nearly 100% of errors are detected before they affects the laboratory computer system.

Table 2 shows an example of identified laboratory computer systems risk acceptability.

Table 2.

The risk assessment

RPN	Risk level	Description
1-5	Insignificant	Additional actions and entries are not needed
6-18	Small	No additional actions required. Monitoring is required
19-48	Acceptable	Actions with scarce means
49-80	High	Urgent actions to reduce risk
81-125	Unacceptable	Urgent actions irrespective of the necessary investments. Otherwise, the process should be stopped

Considering the risks of laboratory computer systems, they can be divided into three main groups - information confidentiality interruption, information integrity loss, technical failures. Examples of such risks include an unauthorized and disapproval information access, an exposure of confidential data, data loss and unauthorized data change, misleading data, computer equipment failure, etc.

It should be noted that Failure Mode and Effects Analysis for the laboratory computer systems risks evaluation was chosen because of its convenience and relative integration accessibility into the laboratory quality management system.

References

1. DSTU ISO/IEC 17025:2017 (2017), “Zaghaljni vymoghy do kompetentnosti vyprobuvaljnykh ta kalibruvaljnykh laboratorij” [General requirements for the competence of testing and calibration laboratories], Derzhspozhyvstandart Ukrajiny, Kyjiv.
2. DSTU ISO 15189:2015 (2015), “Medychni laboratoriji. Vymoghy do jakosti ta kompetentnosti” [Medical laboratories — Requirements for quality and competence], DP "UkrNDNC", Kyjiv, 46 p.
3. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). – IEC, 2018. – 165 c.