BIOMEDICAL MEASUREMENTS AND DEVICES

CYBER-PHYSICAL SYSTEMS AS A TOOL FOR DIGITAL MODERNISATION OF LABORATORY DIAGNOSTICS IN ACCORDANCE WITH ISO 15189

Mykola Mykyychuk , Dr.Sc., Prof.
Lviv Polytechnic National University, Ukraine;
Olesia Chaban, PhD, As.-Prof.
Danilo Halytsky Lviv National Medical University, Ukraine
Oleh Chaban,PhD student
Lviv Polytechnic National University, Ukraine
e-mail: mykolamm@ukr.net

https://doi.org/10.23939/istcmtm2025.03.

Abstract. The application of information technologies particularly decision support systems in laboratory diagnostics and healthcare in general is becoming increasingly significant. This article presents an analysis of the implementation of a risk-based approach within management system processes and the operational activities of medical laboratories. Approaches to the identification of innovative risks in medical laboratories are substantiated in accordance with the requirements of international standards governing laboratory practice. Of particular relevance is the issue of introducing cyber-physical systems into laboratory information systems which determine the degree of controllability of all laboratory processes and automate all aspects of laboratory activities allowing for optimisation and increased efficiency. A particularly pressing issue is the integration of cyber-physical systems into laboratory information systems as they determine the level of controllability of all laboratory processes and ensure the automation of all aspects of laboratory operations thereby facilitating optimization and enhancing overall efficiency.

Key words: Risk, risk assessment, medical laboratory, risk management, international standards, cyber-physical systems.

1. Introduction

The fundamental objective of medical laboratories is to address the needs of diverse categories of laboratory users by delivering guaranteed accurate and reliable laboratory test results, along with high-quality services that align with user expectations [1]. International standards regulating the quality of medical laboratory practices such as ISO 15189:2022, ISO 22367:2020 and ISO 35001:2019 define comprehensive requirements for risk management, assurance of quality and safety of laboratory investigations, reduction of errors across all phases of the laboratory process (pre-analytical, analytical, and post-analytical) as well as the establishment of mechanisms for continual improvement of the quality management system [3,4].

The implementation of ISO 15189:2022 within laboratory operations necessitates substantial organizational and financial resources. This includes conducting systematic risk assessments, designing and implementing mitigation strategies, and monitoring the effectiveness of corrective and preventive actions. Collectively, these measures provide a structured framework for managing risks and opportunities, thereby fostering continuous improvement and ensuring the sustained delivery of high-quality laboratory services.

Furthermore, the integration of intelligent data analytics and real-time processing of test results within cyber-physical systems enhances the laboratory's ability to effectively identify, assess, and monitor risks. Such capabilities support informed decision-making aimed at preventing threats to both the quality and continuity of laboratory processes, ultimately contributing to the robustness and resilience of modern medical laboratory practice.

2. Drawbacks

The implementation of ISO 15189:2022 is essential for medical laboratories regardless of their ownership structure (private, municipal, or state), including institutions funded by the National Health Service of Ukraine (NHSU). This applies to laboratories performing tests and providing results in such fields as biochemistry, virology, hematology, hemostasiology, general clinical analyses, immunochemistry, microbiology, and parasitology. The implementation of a management system for medical laboratories will improve the quality of research, minimise errors, standardise processes and increase the trust of patients and customers. Clinical laboratories will be able to achieve guaranteed accuracy of results, unify testing methodologies, ensure process traceability and gain international recognition. Private laboratories, in particular, will obtain competitive advantages, opportunities for entering the international market, transparency of business processes, and the ability to attract new clients. However, the complexity and scope of the new requirements, especially regarding risk management, require in-depth analysis and the development of a risk-based approach at all stages of laboratory activities. This involves not only the identification of potential threats but also continuous monitoring, evaluation of the effectiveness of implemented measures, and ongoing process improvement.

Thus, medical laboratories must focus on developing and implementing a risk-based approach in their operations in accordance with ISO 15189:2022 requirements. Risk awareness and assessment enable laboratories to prioritize risks, anticipate potential

consequences, and plan appropriate measures for their mitigation or elimination.

In ISO 15189:2022, significantly greater emphasis is placed on risk management, with an increased number of requirements for risk analysis compared to the previous edition. The main updates in the latest version of the standard are centered on the digitalization of laboratory processes, expanded requirements for laboratory information systems and automation, strengthened validation requirements for digital systems, and a strong focus on data management and cybersecurity. Digital transformation implies increased dependence on digital systems, more stringent software validation requirements, and a heightened focus on data governance and information security. Nevertheless, technologies should not increase the workload of healthcare professionals but conversely provide them with processed information ready for clinical application [5].

A cyber-physical system should facilitate effective risk management since the effectiveness of such a system in medical laboratories largely depends on the application of well-developed and substantiated approaches to risk assessment. The system must incorporate clearly defined performance indicators that enable objective, real-time evaluation of its effectiveness.

The detection of errors and nonconformities at early stages makes it possible to respond promptly and prevent adverse consequences such as compromised quality of test results, financial losses, or reputational risks. It is important not only to reduce risks but also to optimize their profile by leveraging opportunities to improve processes and enhance laboratory efficiency.

3. Goal

The aim of this study is to substantiate the relevance and determine the directions for implementing cyber-physical systems as a tool for the digital modernization of quality management in medical laboratories in accordance with the requirements of ISO 15189:2022. The focus is placed on improving the processes of risk identification, assessment, monitoring, and mitigation at all stages of the laboratory workflow, with the ultimate goal of ensuring the reliability of test results, maintaining the continuity of laboratory operations, and enhancing overall efficiency.

4. Identification of risks in a medical laboratory based on an analysis of the functioning of the laboratory information system

In accordance with the requirements of ISO 15189:2022 "Medical laboratories — Requirements for quality and competence"a medical laboratory must establish, document, implemented and maintained processes for identifying hazards associated with laboratory testing and services in particular identifying and assessing the associated risks and opportunities for improvement, managing these risks and monitoring the effectiveness of management.

Hazard identification processes include [1]:

a) preventing or reducing unwanted effects and potential disruptions to laboratory operations;

b) achieving improvement by exploiting opportunities;

c) ensuring that the management system achieves its intended results;

d) reducing risks to patient care;

e) contributing to the achievement of the laboratory's goals and objectives.

Risk management should ensure the detection, identification, analysis, assessment and decision to accept or reject risk. The objectives of risk management are [1]:

– ensuring confidence that the quality management system of a medical laboratory can achieve the planned results;

– maintaining the effectiveness of the medical laboratory;

– preventing or reducing undesirable effects;

– ensuring continuous improvement.

In a medical laboratory the management and assessment of non-conforming output data is carried out at all stages of the laboratory's work, covering pre-analytical, analytical and post-analytical processes.

The risk management process in a medical laboratory includes:

– risk management plan

– risk analysis;

– risk assessment;

– risk control;

– risk management review;

– risk monitoring.

The input data for the process are:

– input control data;

– results of internal audits;

– quality management system documentation and processes performed in departments;

– complaints about the quality of the service provided;

– complaints about the functioning of the quality management system;

– results of monitoring and measurement of processes and services;

– quality indicators in accordance with acceptance criteria;

– staff suggestions.

The output data for the process includes:

– corrective actions;

– information for analysis by executives;

– documents (non-compliance reports, complaints);

– analysis of department quality indicators;

– process improvement goals.

Identified risks are subject to analysis. The process of risk analysis is carried out in order to identify critical risks [2]. Risk analysis involves qualitative and quantitative analysis. The impact of potential risks should be assessed individually or in relation to the medical laboratory as a whole. Qualitative analysis of identified risks is carried out by surveying the structural units of the medical laboratory. Quantitative risk analysis is assessed based on the maximum possible damage from the occurrence of each specific risk.

Risk identification begins with a qualitative analysis of identified risks based on which the possible causes (conditions) of risk occurrence, expected consequences of risk, expert assessment of priority, impact and timing of risk are determined, risk management measures are proposed, and in the case of unacceptable risk, a reassessment of the residual risk after mitigation measures have been taken. Risk management is a complex process as each stakeholder may assess the risk of harm differently. The following risk management scheme for medical laboratories is proposed (Fig. 1).

The overall process of analysing and assessing risks in a medical laboratory is carried out using a system of quantitative and qualitative indicators which in turn must be selected based on the results of their analysis in relation to their impact on the controlled process and its results. Identifying risk indicators only makes sense if there is an assessment scale for each of them according to which a corresponding assessment can be made. The essence of constructing an assessment scale for any risks lies in finding patterns of transition from the measurement (observation) of risks to their assessment.

A comparative analysis of risk assessment methods leads to the conclusion that statistical and probabilistic methods do not ensure operational efficiency as they require significant amounts of objective information. Expert methods may contain a significant subjective component. Therefore given the need for efficiency and integration of risk assessments into the medical laboratory quality management system it is advisable to use index methods for risk assessment. A risk index is an indicator of possible losses in points which allows for a comprehensive assessment of the degree of impact and level of threat of the corresponding risk.

In accordance with the requirements of ISO 15189:2022 "Medical laboratories — Requirements for quality and competence" medical laboratories must analyse their work processes, assess the impact of potential failures on the quality of medical services, change processes to reduce or eliminate identified risks and document the decisions and actions taken. Overall, the LIS is an integral part of the workflow of a medical laboratory and can be a source of potential risks at all stages of employees' work.

Potential risks in the operation of laboratory information systems are presented in Table.

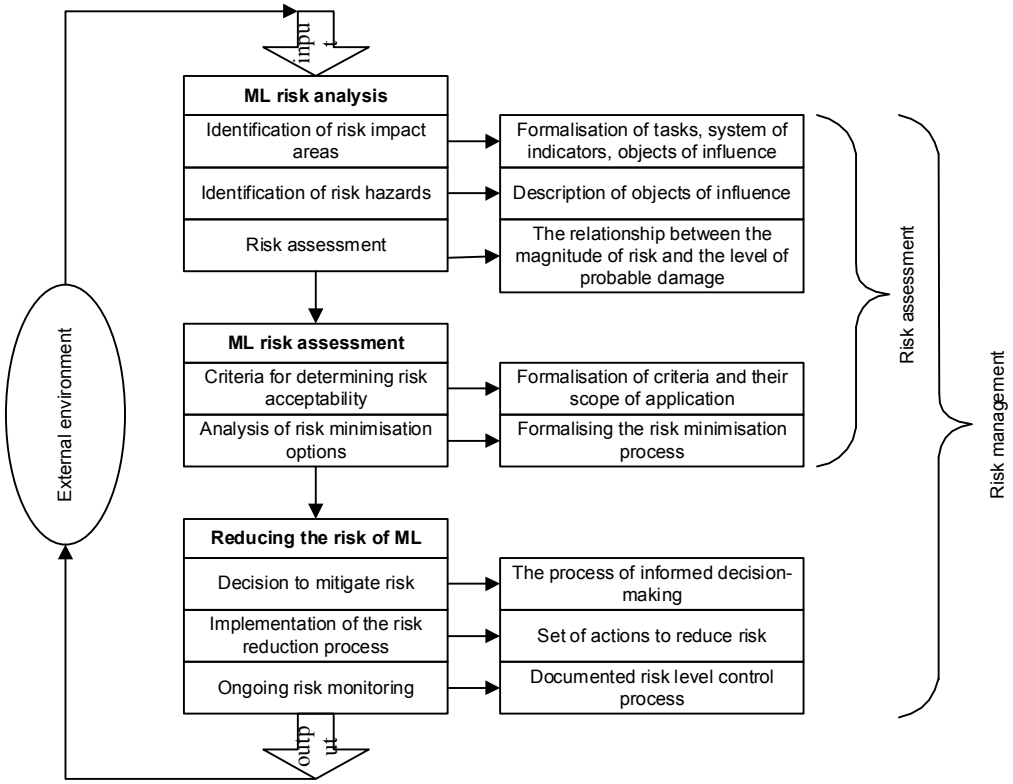

Fig. 1. Generalised ML risk management scheme

Table. Risks in the information systems of the medical laboratory

№	Problem area	Description of potential risk
1	Patient identification	Incorrect identification or tracking of a patient may result in the prescription or delivery of test results to another patient
2	Transmission and display of information	Incorrect transmission of test orders may complicate the interpretation of results by the doctor
3	Reliability of LIS	Failures in the operation of the laboratory information system (LIS) and difficulties with its recovery after failures
4	Software integrity	Defects in the software code (flaws in the software logic) that violate the reliability of the data or lead to system failures
5	Unauthorized access	Potential intrusion into the system via the Internet or leakage of confidential patient information
6	Cyber security	An insufficient level of information security increases the risk of data privacy threats, data destruction or manipulation.

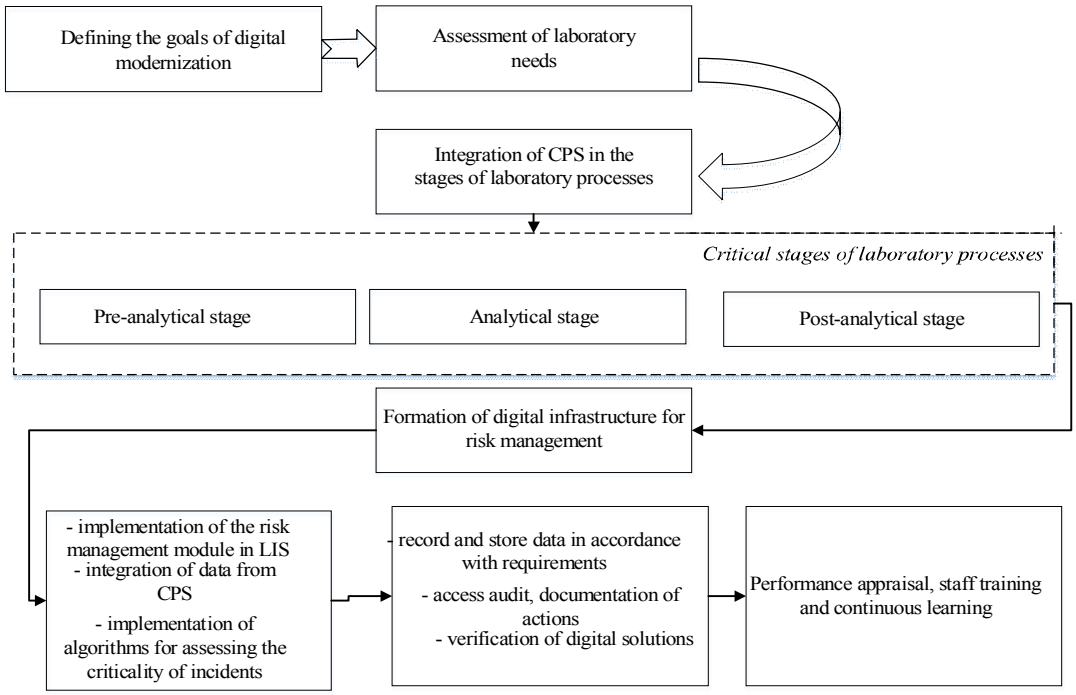

Fig. 2. Model for implementing cyber-physical systems into the quality management system of a medical laboratory

Modern cyber-physical systems (CPS) that integrate hardware and software to support laboratory processes manage medical data and verify data within the cyber-physical infrastructure can be exported to expert analytical systems for forecasting, anomaly detection and informed assessment of residual risk. This approach not only allows for the timely detection of critical deviations but also ensures that the risk management system complies with the requirements of ISO 15189. The sequence of implementation of the cyber-physical system in the quality management processes of a medical laboratory is shown in Fig. 2 and covers the pre-analytical, analytical and post-analytical stages of the laboratory's work.

The implementation of a cyber-physical system begins with strategic planning which includes defining the goals of digital modernisation in accordance with ISO 15189:2022, assessing the needs of the laboratory, analysing processes, existing digital solutions, weaknesses in the quality management system, and forming an interdisciplinary working group. The use of CPS will speed up laboratory work processes and optimise the use of the organisation's resources. The cyber-physical system should also perform analytics and multidimensional data analysis [6]. The generalised structure of CPS with integration into the LIS is shown in Fig. 3.

The integration of CPS into critical stages of laboratory work automates risk management processes. In particular at the pre-analytical stage where temperature control is extremely important for further work with biomaterial samples and ensuring the reliability and accuracy of laboratory results the use of sensors with the ability to automate monitoring of conditions will ensure sample traceability and prevent material spoilage or

contamination. IoT solutions for temperature control and storage of biomaterial in refrigerators or thermal containers which automatically transmit data to the system and ensure appropriate storage conditions allow detecting temperature violations in real time avoiding spoilage or changes in sample properties [7,8]. The implementation of ISO 15189:2022 requires medical laboratories to implement digital solutions such as QR codes and RFID tags which make the accounting and control of biomaterial samples more efficient. Sample identification (RFID, QR) will ensure the traceability of each sample, minimise the risk of errors during transport and storage and quickly identify deviations from specified conditions that directly affect the reliability of test results and the overall quality of the laboratory process[9].

At the analytical stage, CPS provides real-time monitoring of analytical equipment, automated quality control, collection and analysis of large data sets for rapid detection of deviations and inconsistencies, and finally, at the post-analytical stage, digital processing, validation and visualisation of research results, automated report generation and distribution of results are provided, which contributes to the accuracy, timeliness and traceability of results.

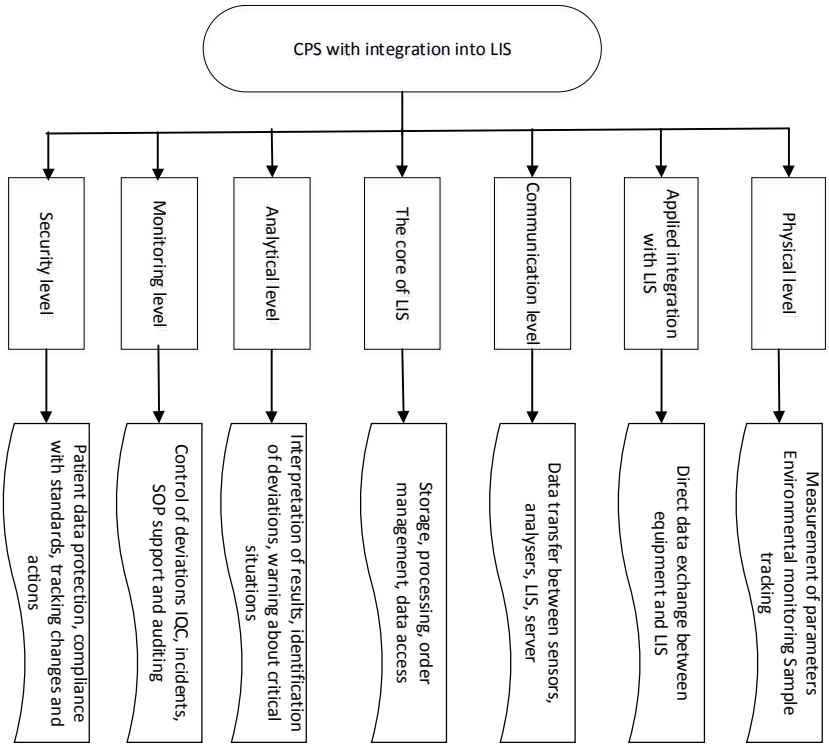

Fig. 3. Generalised structure of a cyber-physical system

The structure of the CPS should cover the interaction of physical devices and digital components, functional capabilities (speed and accuracy of operation, adaptability to conditions), data security and fault tolerance, compliance with quality standards and regulatory requirements, current challenges and development prospects. All this will enable the implementation of a risk-based approach in accordance with ISO 15189:2022 and ensure the continuous improvement of the laboratory system through the integration of intelligent data analysis tools and feedback mechanisms.

5. Conclusions

The article analyses the possibilities of implementing cyber-physical systems in a laboratory information system which showed that its effective use allows improving risk identification and monitoring, minimising human error and increasing the overall efficiency of laboratory processes. The integration of cyber-physical systems into laboratory information systems will ensure sample traceability, automated quality control, timely detection of critical deviations and improved feedback. Thanks to the capabilities of big data analytics cyber-physical systems allow for rapid response to potential threats, informed management decisions and laboratory operations in accordance with the principles of continuous improvement. In general the introduction of cyber-physical systems as a tool for digital modernisation is a promising direction for the development of quality management systems in medical laboratories. This not only ensures compliance with international standards in particular ISO 15189:2022 but also contributes to increasing the competitiveness of laboratories,

strengthening trust on the part of patients and customers and creating a basis for the innovative development of the laboratory diagnostics industry in the context of the digital transformation of healthcare.

Conflict of Interest

The authors state that there are no financial or other potential conflicts regarding this work.

References

[1] DSTU EN ISO 15189:2015 Medical laboratories — Requirements for quality and competence (EN ISO 15189:2012, IDT).

[2] Risk Management. Vocabulary, DSTU ISO Guide 73:2013 (ISO Guide 73:2009, IDT), 2013.

[3] DSTU EN ISO 22367:2022 Medical laboratories — Application of risk management to medical laboratories (EN ISO 22367:2020, IDT; ISO 22367:2020, IDT).

[4] ISO 35001:2019 Biorisk management for laboratories and other related organisations.

[5] Chaban O., Boiko O., Chaban O. "Application of health monitoring devices as a means of improving the quality of medical services", *VI All-Ukrainian Scientific and Technical Conference of Young Scientists in the Field of Information-Measurement Technologies and Metrology*, 2020.

[6] Mykyichuk M. M., Stadnyk B. I., Yatsyshyn S. P., Lutsyk Ya. T. (2017). Smart measuring instruments for cyber-physical systems. *Measuring Equipment and Metrology*, No. 77, pp. 3–17.

[7] Meissner H. Implications of cyber-physical production systems on integrated process planning and scheduling. *Procedia Manufacturing*, 2019, Vol. 28, pp. 167–173.

[8] Controlling Devices by IoT. *International Journal of Recent Technology and Engineering*. [Online]. Available: https://www.ijrte.org/portfolio-item/D8777118419

[9] A. O. Melnyk, V. A. Melnyk, V. S. Hlukhiv, A. M. Salo. *Cyber-physical systems: multilevel organization and design*. Magnolia 2006 Publishing, 2024.