UDC 004.738:006.91

Metrological risks of industrial IoT systems: classification, assessment, and risk mitigation strategies

O. Honsor, M. Mykyychuk

Lviv Polytechnic National University, S. Bandera Str., 12, 79013, Lviv, Ukraine
oksana.y.honsor@lpnu.ua; mykola.m.mykyichuk@lpnu.ua

Abstract

The rapid development of the Industrial Internet of Things (IIoT) has significantly increased the reliance on distributed intelligent sensor systems. These technologies allow for real-time monitoring, predictive maintenance, and adaptive control. At the same time, they pose unique metrological risks that may affect data quality, interoperability, and system reliability. This paper provides the classification of risks associated with the IIoT in terms of metrological support and how to assess them. The paper considers the interdependence between the risk categories, accounting for cascading effects that may lead to the increased number of failures in the IIoT ecosystems. To assess the levels of metrological risks, a quantitative model is presented, which includes the main parameters of metrological support for IIoT systems.

Strategies for preventing the risks and mitigating their effects, such as use of digital calibration certificates, preventive maintenance of the system, and protection of audit reports with blockchain technologies, have been developed. Future areas of study that are necessary to ensure the reliable operation of the IIoT with support for intelligent systems have been identified.

Keywords: metrological support; industrial internet of things (IIoT); metrological risks; risk assessment; uncertainty.

Received: 29.10.2025 Edited: 19.11.2025 Approved for publication: 24.11.2025

Introduction

In the modern world, the efficiency and safety of automated production processes are heavily reliant on the reliability, accuracy, and traceability of measurement data. Therefore, the assessment of metrological risks of IIoT systems is a relevant area of modern metrology. The systems are based on networks of distributed smart sensors. These systems generate large amounts of real-time data that are used for decision-making without human involvement. Under these conditions, even minor metrological errors, caused by sensor drift, loss of calibration traceability, or data distortion, can bring about negative technological and economic effects. Therefore, transition from controlling the metrological characteristics of measuring equipment using widely accepted methods to risk-oriented metrology is necessary to ensure the quality, safety, and reliability of digital production systems.

This study aims to analyse the metrological risks arising from using IIoT and smart sensor systems, the interdependence between the categories of the risks and assess their impact on IIoT systems. Based on this analysis, risk mitigation strategies will be proposed. This will provide a comprehensive framework for understanding, assessing, and managing the risks arising from metrological support of IIoT systems, thereby maintaining their reliability, efficiency, and compliance with regulatory requirements.

Analysis of recent studies and problem statement

The process of collecting data in IIoT systems involves various applications and programmes. However, the quality of this data is often poor. In critical areas of the Internet of Things (IoT), acceptable limits of errors and uncertainty shall be clearly specified. National and international metrology institutions have developed methods to ensure the reliability of traditional measurement data. Active work is currently underway to digitise these practices, to make them more accessible and to facilitate their application. The following papers

[1–3] outline the experience of using distributed ledger technology (DLT) for digital metrology in the IoT. This paper studies the application of digital calibration certificates (DCCs) in the context of the IoT data description, certification, authentication, and quality assurance. The paper [4] presents a method based on a multi-user cloud platform designed for exchanging digital data related to calibration. The primary benefit of this approach is its cost-effectiveness in terms of deployment and utilisation, in addition to ensuring data traceability and integrity. A study [5–7] considers an assessment method for the IoT solutions in terms of metrological support of measurement processes. The approach is based on the principles of metrology and verified practices of the software application in the field of physical quantity measurements.

Industrial digital metrology is closely associated with quality assurance systems, and collectively, they contribute to enhancing the reliability, compatibility, and availability of measurement information for other operations. The study presented in [8] focuses on integrating measuring instruments into the IoT architecture. This integration is achieved through the implementation of open international standards [9–11] that are focused on quality assurance and control procedures in manufacturing.

The availability of numerous and diverse data sources, as well as wireless communication standards, increases the risk of failures in the IoT scenarios. The papers [12, 13] propose a one-size-fits-all methodology for assessing data security risks. It is noteworthy that the system objectively considers both static and dynamic functions and components of a IoT system, tracking the entire data lifecycle.

The analysis of recent studies proves that digital metrology and metrological support for the IoT are being rapidly developed. Nevertheless, the risks that may affect the effectiveness of metrological support and systems of production quality assurance remain overlooked. The majority of studies in this field focus on risks associated with data security. Consequently, a comprehensive study of potential risks associated with the IoT metrological support and the development of strategies for their prevention, mitigation, and management has become a matter of paramount importance.

Classification and assessment of risks in terms of metrological support for IIoT systems and strategy for their mitigation

Risks in terms of metrological support of industrial IoT systems are ushered in by the complex nature of measurements in industrial automation. The following list comprises significant risks which have been categorised for subsequent identification and analysis.

I. Technical and measurement risks

1. Measurement errors caused by sensor drift over time due to ageing; unstable ambient conditions (temperature, humidity, vibrations); and electromagnetic interference.

2. Improper calibration or incorrect verification of sensors.

3. Non-compliance of metrological characteristics of measuring instruments with the established requirements.

4. Outdated or incompatible standards (calibration modules are not synchronised with modern IoT protocols).

5. Data loss or distortion during transmission (especially when utilising wireless technologies such as LoRa, Zigbee, NB-IoT, etc.).

II. Information and technology risks

1. Cyber threats that affect the reliability of measurement data, namely: spoofing or modification of sensor data; man-in-the-middle attacks between the sensor and the gateway; unauthorised access to calibration databases.

2. Insufficient control over measurement results during their collection, transmission, and storage.

3. Lack of common protocols for reliable measurements (e.g. entrusted time stamp, digital calibration certificates).

4. Inconsistency between data formats received from different sensors, which complicates comparisons and metrological compatibility.

5. Violation of the integrity of calibration result databases or their incorrect synchronisation in a cloud environment.

III. Organisational and regulatory risks

1. Absence or outdated regulations on metrological support for IIoT systems.

2. Differences between the requirements of conventional metrology and digital measurement practices.

3. Insufficient qualifications of personnel operating and calibrating sensor systems.

4. Lack of a system of metrological supervision of "digital measurements"; lack of confidence in the virtual environment.

5. Uncertainty of responsibility between sensor manufacturer, IIoT system integrator, and data consumer.

IV. Operational risks

1. Failure of sensors or gateways, resulting in loss of measurement information.

2. Problems with time synchronisation, which is critical in terms of metrological information ageing.

3. Disruption of the calibration chain due to software updates or network topology changes.

4. Insufficient monitoring of the sensor status.

5. High cost of metrological services, which stimulates savings "on accuracy".

V. Confidence and data quality risks

1. Uncertainty of the data source when it is impossible to track the origin of a particular measurement.

2. Lack of digital metrological traceability in the metrological chain in accordance with DSTU ILAC-G 24/OIML D 10 [14].

3. Insufficient data validation during processing in AI/ML systems, which leads to incorrect decisions.

4. Data distortion during aggregation or filtering.

5. Loss of user confidence in the system data if its metrological reliability is not confirmed.

Risks shall be assessed according to the FMEA methodology – Failure Modes and Effects Analysis [15]. It allows one to identify: all potential types of risks; the level of risk impact on the system; factors that cause the risks; ways to avoid the risks and/or reduce their impact on the system.

A quantitative assessment of the risk level can be formulated using the FMEA tables, thereby producing a comprehensive indicator. This allows for the generalisation of various aspects of metrological risks in IIoT systems, facilitate management decision-making, and enable tracking of the dynamics of changes in risks and factors affecting them.

Table 1 shows the potential effects of the described risks and ways to prevent, mitigate, or overcome them with the implementation of the FMEA methodology (Failure Modes and Effects Analysis).

Typical indicators for assessing the risk level are: severity (S), probability of occurrence (O), probability of detection (D) and risk priority number (RPN = S × O × D). Limits of indicators:

S: 1 (minimal) – 10 (catastrophic).

O: 1 (very rare) – 10 (very frequent).

D: 1 (easy to detect) – 10 (almost impossible to detect).

RPN = S×O×D (the higher the RPN value, the higher the priority for actions).

Threshold-value interpretation of the RPN (applied):

RPN $\geqslant$ 200 → Critical (urgent measures);

100 $\leqslant$ RPN < 200 → High priority;

50 $\leqslant$ RPN < 100 → Medium priority;

RPN < 50 → Low priority.

In this case, risks with RPN > 300 are critical (they require immediate action). They belong to technical, informational, and regulatory categories, i.e. the areas with the highest impact on accuracy and confidence. Organisational and operational risks are moderate, but can exacerbate critical risks if not adequately controlled.

The analysis shows that risks in different categories are closely interrelated. Companies using the IoT shall maintain a comprehensive and consistent policy at the

Table 1

Risks in the field of metrological support in the IoT systems

№	Risk category	Potential failure	Possible effects	S	O	D	RPN	Mitigation strategies
1	Technical	Drift of sensor parameters	Incorrect measurement data, control errors	8	7	6	**336**	Regular calibrations, self-diagnosis of sensors
2	Technical	Absence of temperature compensation	High error in unstable environments	7	6	5	**210**	Using sensors with built-in compensation
3	Informational	Substitution or modification of data	Loss of measurement reliability	9	5	7	**315**	Cryptographic protection, digital signature on measurement protocols
4	Informational	Data format incompatibility	No processing of indicators	6	6	4	**144**	Implementation of unified protocols (OPC UA, MQTT)
5	Regulatory	Lack of digital traceability standards	No certification of the measuring system	9	8	8	**576**	Develop industry standards and confidence policies
6	Organisational	Low staff qualifications	Calibration errors, data loss	8	6	5	**240**	Personnel training, development of standard operating procedures
7	Operational	Failure of a sensor node	Data loss, interruption of process control	8	5	6	**240**	Redundancy, automatic backup
8	Operational	Lack of time synchronisation	Loss of measurement traceability	7	5	7	**245**	NTP/PTP synchronisation, monitoring of measurement standards of time
9	Confidence/quality	Lack of a digital traceability chain	Decreased confidence in the system	9	6	6	**324**	Use of blockchain or DCCs
10	Confidence/quality	Incorrect operation of an AI model due to false data	Wrong decisions in the management	10	5	7	**350**	Data validation, quality control of datasets

management level to prevent, mitigate, or eliminate so many potential risks [16].

The S, O, and D indicators can be adapted to a specific industry based on previous measurement data (the assessment criteria shall be documented). Adding a propagation factor (P) will allow for the consideration of cascading effects.

Let us consider the interrelations between different categories of risks, the structure of which is shown in Fig. 1.

Risks form a closed system of effects, where the source is technical and information factors, and the point of reverse influence is the risks of confidence and data quality, which change the regulatory and technical policy of the system. Table 2 shows a structured map of risk interrelations in terms of metrological support for IIoT systems.

This model is helpful in the following ways:

• Root cause analysis: identifying the initial risk factors that influence others.

• Prioritisation: Concentrating on mitigating risks with high impact and interdependence (e.g. calibration or cyber security).

• System design: Ensuring redundancy and verification in vulnerable areas, such as sensor calibration and communications.

• Organisational policy development: Developing an integrated metrological support policy that accounts for cross-risks.

This structure describes the Digital Metrological Trust Loop, a concept that is currently being actively developed as part of Smart Manufacturing and Trustworthy AI.

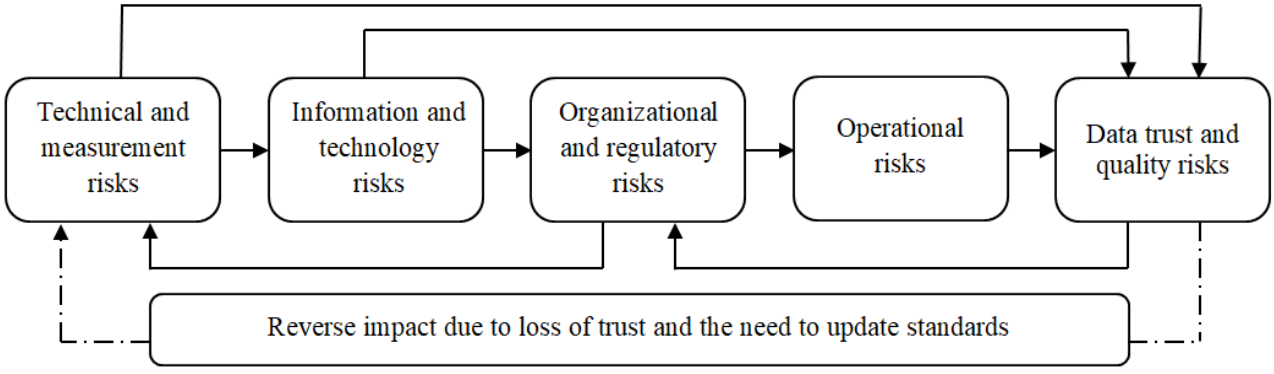

Fig. 1. Flowchart of iterrelations between risk categories

Table 2

Map of interrelations between risk categories

№	Risk source category	Category affected	The nature of the interrelation	Type of influence	Effects of interaction
1	Technical	Information	Sensor errors cause data distortion	Direct	Inaccurate information in digital systems
2	Technical	Confidence and quality risks	Measurement instability reduces confidence in data	Direct	Doubts about the measurement result validity
3	Information	Regulatory	The lack of secure protocols complicates certification	Direct	Inability to confirm metrological traceability
4	Information	Confidence and quality risks	Data loss or tampering undermines the system reliability	Direct	Decreased confidence in measurements
5	Regulatory	Organisational	Unclear or outdated standards cause chaos in staff work	Direct	Lack of unified calibration procedures
6	Regulatory	Technical	Standard requirements influence the selection and configuration of sensors	Reverse	The need to update technical solutions
7	Organisational	Operational	Low staff qualifications lead to system failures	Direct	Calibration errors, measurement failures
8	Operational	Confidence and quality risks	Sensor failure or time asynchrony distorts results	Direct	Loss of reliability of the monitoring system
9	Confidence and quality risks	Regulatory	Loss of confidence stimulates updating of metrological standards	Reverse	Developing new digital traceability standards
10	Confidence and quality risks	Technical	The need to improve the accuracy and digital certification of sensors	Reverse	Improving hardware and metrological characteristics

To determine the level of influence of different types of metrological risks on IIoT systems or their components, it is advisable to use a mathematical model that incorporates a complex indicator of a metrological risk. For a separate category of risks, the mathematical model of the complex indicator will be as follows:

$$R_{base} = f\{L, I, D, U, T, C, S\}, \quad (1)$$

where L is the likelihood of a metrological failure/problem (0 – impossible, 1 – guaranteed);

I is the impact/effect of failure on the safety, quality, or performance of the system (0 – none, 1 – catastrophic).

D is the detection of failures (0 – not detected, 1 – fully detected).

U is the normalised measurement uncertainty (0 – insignificant, 1 – unacceptable).

T is the traceability assessment (0 – no traceability, 1 – full traceability).

C is the vulnerability to cyber threats/data integrity breaches (0 – protected, 1 – very vulnerable).

S is the system/integration vulnerability (compatibility, scalability, unclear roles) (0 – reliable, 1 – vulnerable).

The value of complex indicator R_{base} is calculated using the weighting coefficients determined according to the method described in [17]. Moreover, $\sum w_k = 1$, with possible values $w_k \geqslant 0$.

Formula (2) for calculating a comprehensive indicator of the level of a metrological risk is as follows:

$$R_{base} = w_L \cdot L + w_I \cdot I + w_D \cdot (1-D) + \\ + w_U \cdot U + w_T \cdot (1-T) + w_C \cdot C + w_S \cdot S. \quad (2)$$

The formula uses $(1-D)$ and $(1-T)$ because low detectability and low tracking increase the risk. All indicators are in the range [0.1], so $R_{base} \in [0.1]$.

In Table 3, examples of qualitative risk levels are converted into numerical values in the range [0–1] for the parameters of formula (2).

For L (likelihood) and I (impact), the following pattern is observed: the higher the level is, the closer the indicator is to 1.

For D (Detection) and T (Tracking), the higher the level is, the closer the indicator is to 1. However, the formula uses $1-D$ and $1-T$ because low detection and tracking indicators increase the risk.

For U, C, S: the higher the risk level is, the closer its value is to 1.

As mentioned above, different categories of risks influence one another. Therefore, it is advisable to rewrite mathematical model (1), accounting for the cascading effect (3):

$$R = \min\{1, R_{base} \cdot P\}, \quad (3)$$

where R is a complex indicator of the level of a metrological risk, which accounts for cascading effects and shall be mitigated;

P is the propagation/interdependence coefficient ($\geqslant 1$), which shows how much a failure is amplified in the system (1 – no amplification, >1 – cascading effect). The coefficient is calculated based on the number of dependent subsystems or the graph metric. It is estimated using network topology or interdependence analysis (e.g., $P = 1.0$ – no cascading interdependence, $P = 1.2$ – moderate effect, $P \geqslant 1.5$ – significant interdependence and cascading effect).

Below is the four-level interpretation of the R level:

$0.75 \leqslant R \leqslant 1.0$: **Critical –** immediate action is required.

$0.50 \leqslant R < 0.75$: **High –** prioritisation and monitoring.

$0.25 \leqslant R < 0.50$: **Medium –** planned corrective actions.

$0 \leqslant R < 0.25$: **Low –** acceptable risk, regular monitoring is recommended.

A visual representation of potential outcomes is provided in Fig. 2.

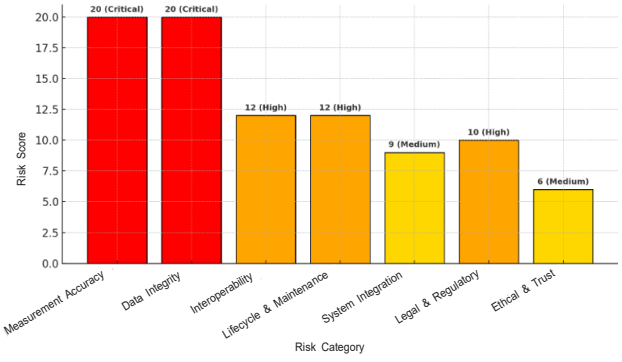

Fig. 2. Estimates and levels of metrological risks by categories

Risk assessment in terms of metrological support for IIoT systems is crucial to ensure data quality, reliability, and traceability. Since the IIoT relies heavily on

Table 3

Numerical values of risk levels

Level	(*L*) / (*I*)	(*D*)	(*U*)	(*T*)	(*C*)	(*S*)
Very low	0.0 – 0.1	0.9 – 1.0	0.0 – 0.1	0.9 – 1.0	0.0 – 0.1	0.0 – 0.1
Low	0.2 – 0.3	0.7 – 0.8	0.2 – 0.3	0.7 – 0.8	0.2 – 0.3	0.2 – 0.3
Medium	0.4 – 0.6	0.4 – 0.6	0.4 – 0.6	0.4 – 0.6	0.4 – 0.6	0.4 – 0.6
High	0.7 – 0.8	0.2 – 0.3	0.7 – 0.8	0.2 – 0.3	0.7 – 0.8	0.7 – 0.8
Very high	0.9 – 1.0	0.0 – 0.1	0.9 – 1.0	0.0 – 0.1	0.9 – 1.0	0.9 – 1.0

sensor networks for monitoring and control, metrology plays a pivotal role in maintaining system performance and safety. Therefore, methods for quantitative prediction of metrological risks are a promising area for further studies.

Conclusion

The metrological support of the IIoT is critical to ensure reliable and efficient performance of industrial systems. As demonstrated in this study, metrological risks have a direct impact on data reliability, system resilience, and industrial safety. The classification of such risks, together with structured methods for their assessment, provides a systematic basis for identifying and prioritising deficiencies.

The proposed quantitative model for assessing metrological risks demonstrates how probability of detection, impact, uncertainty, traceability, and interdependency factors can be integrated into a single metric, enabling both practical decision-making and long-term monitoring. The analysis of interdependencies emphasises that the risks are rarely isolated. Instead, they often spring up across technical, organisational and regulatory levels, amplifying their potential effects.

Mitigation strategies, including prediction-based calibration, integration with the CMMS/MES platforms, use of digital calibration certificates, and blockchain-based audit tracking, provide practical ways to reduce the risks and increase the transparency. Compliance with international standards is crucial to ensure compatibility and legal security of measurements in global industrial ecosystems.

Thus, mitigation of metrological risks in IIoT systems is not only a technical challenge, but it is also a strategic requirement for a sustainable and ethical deployment of Industry 4.0 and Industry 5.0 solutions. For the future, it is advisable to continue studies of prediction-based AI-methods, the use of digital twins for risk modelling, and the implementation of harmonised global standards to build sustainable, adaptive, and reliable IIoT infrastructures.

Метрологічні ризики в промислових системах IoT: класифікація, оцінювання та стратегії мінімізації

О.Й. Гонсьор, М.М. Микийчук

Національний університет "Львівська політехніка", вул. С. Бандери, 12, 79013, Львів, Україна
oksana.y.honsor@lpnu.ua; mykola.m.mykyichuk@lpnu.ua

Анотація

У статті досліджено проблематику оцінювання метрологічних ризиків у системах промислового інтернету речей (IIoT), де мережі смарт-сенсорів формують дані про вимірювання, що надалі використовуються для автоматизованого прийняття рішень, керування технологічними процесами та прогнозування відмов обладнання. Показано, що перехід від централізованих вимірювальних систем до розподілених архітектур IIoT підвищує кількість джерел невизначеності та створює нові типи метрологічних ризиків, пов'язаних з деградацією сенсорів, втратою калібрувальної простежуваності, впливом умов середовища, нестабільністю каналів зв'язку та маніпуляцією даними на рівні мережевих протоколів. Навіть незначні похибки окремих сенсорів можуть призвести до каскадних відхилень у всьому цифровому ланцюгу, що негативно впливає на якість продукції, ефективність алгоритмів керування та безпеку виробничих процесів.

Запропоновано класифікацію метрологічних ризиків на п'ять груп: технічні, інформаційно-технологічні, нормативні, організаційні та ризики якості даних/довіри. Для їх оцінювання використано методи ризик-орієнтованого аналізу: побудовано матрицю ризиків, проведено FMEA та сформовано карту взаємозв'язків між категоріями ризиків. Уперше запропоновано наукову формулу кількісної оцінки рівня метрологічного ризику на основі вагових коефіцієнтів і нормованих параметрів: ймовірності виникнення, впливу на систему, ймовірності виявлення, невизначеності вимірювань, простежуваності, кібервразливості та системної інтегрованості. Додатково введено коефіцієнт поширення, що враховує каскадний ефект у мережевих структурах IIoT, коли єдина помилка вимірювання впливає на роботу кількох підсистем.

Обґрунтовано практичні стратегії мінімізації ризиків: автоматизоване калібрування, цифрові сертифікати калібрування, використання цифрових двійників для виявлення дрейфу сенсорів, інтеграція з платформами CMMS/MES, а також застосування стандартів ISO/IEC 17025 та IEEE 1451 для забезпечення простежуваності та сумісності. Запропонований підхід формує основу для впровадження ризик-орієнтованої метрології в цифровому виробництві й сприяє створенню надійних, масштабованих та стандартизованих IIoT-рішень.

Ключові слова: метрологічне забезпечення; промисловий інтернет речей (IIoT); метрологічні ризики; оцінювання ризиків; невизначеність.

References

1. Mustapää T., Autiosalo J., Nikander P., Siegel J. E., Viitala R. Digital Metrology for the Internet of Things. *Proceedings of the Global Internet of Things Summit (GIoTS),* IEEE, 2020. doi: https://doi.org/10.1109/GIOTS49054.2020.9119603
2. Hackel S., Härtig F., Hornig J., Wiedenhöfer T. The Digital Calibration Certificate. *PTB-Mitteilungen*, 2017, vol. 127, no. 4, pp. 75–81. doi: https://doi.org/10.7795/310.20170499
3. Barcelo-Ordinas J.M., Doudou M., Garcia-Vidal J., Badache N. Self-calibration methods for uncontrolled environments in sensor networks: A reference survey. *Ad Hoc Networks*, 2019, vol. 88, pp. 142–159. doi: https://doi.org/10.1016/j.adhoc.2019.01.008
4. Mustapää T., Nummiluikki J., Viitala R. Digitalisation of Calibration Data Management in Pharmaceutical Industry Using a Multitenant Platform. *Applied Sciences*, 2022, vol. 12, no. 15, 7531. doi: https://doi.org/10.3390/app12157531
5. Moulla D.K., Mnkandla E., Abran A. Evaluation of IoT Measurement Solutions from a Metrology Perspective. *Computer Systems Science and Engineering*, 2023, vol. 47, no. 2, pp. 2455–2479. doi: https://doi.org/10.32604/csse.2023.039736
6. Moulla D.K., Mnkandla E., Abran A. Systematic literature review of IoT metrics. *Applied Computer Science*, 2023, vol. 19, no. 1. doi: https://doi.org/10.35784/acs-2023-05
7. Abdallah A., Abran A., Villavicencio M. Measurement solutions in the enterprise architecture literature: A metrology evaluation. *Journal of Theoretical and Applied Information Technology*, 2022, vol. 100, no. 9, pp. 2935–2957.
8. Sousa J., Mendonça J.P., Machado J. A generic interface and a framework designed for industrial metrology integration for the Internet of Things. *Computers in Industry*, 2022, vol. 138, 103632. doi: https://doi.org/10.1016/j.compind.2022.103632
9. IEC 62264-3:2016. Enterprise-control system integration – Part 3: Activity models of manufacturing operations management. Geneva, 2016. 151 p.
10. ISO 23952:2020. Automation systems and integration – Quality information framework (QIF) – An integrated model for manufacturing quality information. Geneva, 2020. 498 p.
11. IEEE 1451.0:2024 (Revision of 1451.0-2007). IEEE Standard for a Smart Transducer Interface for Sensors and Actuators – Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats. NJ, USA, 2024. 429 p.
12. Sicari S., Rizzardi A., Miorandi D., Coen-Porisini A. A risk assessment methodology for the Internet of Things. *Computer Communications*, 2018, vol. 129, pp. 67–79. doi: https://doi.org/10.1016/j.comcom.2018.07.024
13. Casola V., De Benedictis A., Rak M., Villano U. Toward the automation of threat modeling and risk assessment in IoT systems. *Internet of Things*, 2019, vol. 7, 100056. doi: https://doi.org/10.1016/j.iot.2019.100056
14. DSTU ILAC-G24/OIML D10:2013. Nastanovy shchodo vyznachennia mizhkalibruvalnykh intervaliv zasobiv vymiriuvalnoi tekhniky [Guidelines for the determination of calibration intervals of measuring instruments] (ILAC-G24/OIML D10:2007, IDT). Kyiv, 2013. 32 p. (in Ukrainian).
15. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). Geneva, 2018. 99 p.
16. DSTU ISO 31000:2018 (ISO 31000:2018, IDT). Menedzhment ryzykiv. Pryntsypy ta nastanovy [Risk management – Guidelines]. Kyiv, 2019. 28 p. (in Ukrainian).
17. Artemuk O.I. Metrologichni ryzyky zabezpechennia yakosti produktsii na etapi vygotovlennya: dys. d-ra filosofii [Metrological risks of product quality assurance at the production stage: PhD diss.]. Lviv, 2025. 160 p. (in Ukrainian).