Original Scientific Paper/Original naučni rad UDC/UDK: 005.334:004.8
Paper Submitted/Rad primljen:31.12.2025.
Paper Accepted/Rad prihvaćen:10.01.2026.
DOI: 10.5937/SJEM2601026M

Konceptualizacija sadržaja procene rizika primene veštačke inteligencije (AI) u sistemima bezbednosti

Milica Mladenović[1], Katarina Janković[2], Nenad Komazec[3], Zoran Vučinić[4]

[1] Regional Association for Security and Crisis Management, Belgrade, Republic of Serbia mladenovicmilica21@yahoo.com,
[2] Technical test center, Ministry of Defense, Belgrade, Republic of Serbia Jankovickatarina95@gmail.com,
[3] Military academy, Ministry of Defense, Belgrade, Republic of Serbia nenadkomazec@yahoo.com,
[4] Karlovac University of Applied Sciences, Karlovac, Republic of Croatia zoranvucinic5@gmail.com

Apstrakt: Primena veštačke inteligencije u svakodnevnom životu ljudi je postala neizbežna, posebno u poslovnom okruženju. Međutim, većina organizacija potvrđuje činjenicu da je upotreba AI Sistema neophodna, ali su neophodne i smernice za prilagođavanje ubrzanoj ekspanziji veštačke inteligencije. Sistemi bezbednosti predstavljaju posebno osetljivu kategoriju kada je u pitanju primena veštačke inteligencije s obzirom na ogromne nepoznanice o rizicima koje ovi sistemi sa sobom nose. Sadržajni okvir za procenu rizika u ovoj oblasti se nameće kao neophodan, posebno, jer postojeće metode za procenu rizika uglavnom ne prepoznaju AI rizike, čime se onemogućava njihovo sveobuhvatno sagledavanje. U ovom radu je dat sveobuhvatan konceptualni sadržaj procene rizika primene AI u sistemima bezbednosti koji obuhvata rizike tokom celokupnog životnog ciklusa AI sistema čime se omogućava identifikacija, analiza, ocena i tretman prepoznatih rizika i praćenje i kontrola njihovog uticaja na sistem.

Ključne reči: procena rizika, AI, sistem bezbednosti

Risk Assessment Content Conceptualization for the Application of Artificial Intelligence in Security Systems

Abstract: The application of artificial intelligence in people's daily life has become inevitable, especially in the business environment. However, most organizations acknowledge the fact that the use of AI Systems is necessary, but guidelines are also necessary to adapt to the accelerated expansion of artificial intelligence. Security systems represent a particularly sensitive category when it comes to the application of artificial intelligence, given the huge unknowns about the risks that these systems carry with them. A substantive framework for risk assessment in this area is imposed as necessary because the existing risk assessment methods generally do not recognize AI risks, which prevents their comprehensive overview. This paper provides a comprehensive conceptual content of the risk assessment of the application of AI in security systems, which includes risks during the entire life cycle of the AI system, which enables the identification, analysis, assessment and treatment of recognized risks and the monitoring and control of their impact on the system.

Keywords: risk assessment, AI, security system

1. Introduction

Artificial intelligence is gaining more importance in security systems considering their complexity and the growing need for these systems to respond to growing risks in their practice as soon as possible. The application of artificial intelligence in security systems facilitates the performance of many tasks and enables faster and more efficient decision-making. Application of AI in alarm systems e.g. reduced the huge number of false alarms and increased the level of their accuracy, while for security managers it significantly accelerated the process of finding the best security solutions and quickly selecting the tools needed to implement security measures. Machine and deep learning in security practice can be extremely useful, because their mechanisms are based on self-learning, which means that they are able to quickly recognize threats or incidents and transfer what they have learned to other elements, such as robots, which leads to significant savings in the long term.

The fact is that the application of AI is a growing trend in security systems and its expansion in the future is inevitable, as are the risks it brings with it, which impose consideration of the role of assessing those risks, the consequences of which may not be known now. The risks of applying AI technologies in security systems can be political, social, economic, social, technological, legal, ethical, environmental risks and many others, which means that their consequences can be extensive and require such protection measures. To see all that, it is necessary to have a precise methodology for assessing all those risks, or at least those that can be seen now so that the security system can be reliable, efficient and effective.

The aim of this paper is to conceptualize the content of the risk assessment of the application of AI in security systems, based on the existing normative basis and international and national standards, by defining the key elements of the assessment. The existence of this content enables the management of risks arising from the application of AI in security systems, provides a practical framework based on existing normative and standardized rules applicable in security practice and creates space for further research in finding the most effective solutions.

2. Concept of risk and risk assessment in using ai technology

In theory, the concept of risk has always been very complex, multidimensional and ambiguous. In modern security systems, risk means uncertainties in relation to the outcomes that may arise and may originate from different sources. Risk means "potential danger that is predictable, inherent in a situation or activity". It is the possibility of the occurrence of some future event, of uncertain or indefinite duration, which may cause loss or some other consequences (Ineris, n.d.). Risk represents the effect of uncertainty on goals (International Organization for Standardization, 2018). Risk is a concept that affects decision-making at all organizational levels, and therefore it is necessary to comprehensively understand all its elements: risk exposure, system vulnerability, probability of occurrence, damage it can cause, criticality of the system and the consequences it can leave. The entire process requires effective management of all identified risks to ensure the highest possible level of system resilience. To successfully manage risks, a key step is risk assessment, which enables the implementation of a systematic process of identifying, analyzing and evaluating risks (Institute for Standardization of Serbia, 2025), and then implementing reasonable control measures to eliminate or reduce them.

In modern security systems, the integration of artificial intelligence (AI) is becoming a standard practice and defines the processes in these systems, which implies numerous new risks that are not yet well defined or adequately identified and therefore require a methodological framework for risk assessment that will enable this. The content of the risk assessment in the use of artificial intelligence should be practical, adaptable to the development of AI and applicable to most security systems. The application of artificial intelligence in modern security systems brings specific risks such as performance failures, unintentional behavior, impact on human rights, bias, misuse of data, independent decision-making, violations of regulations and ethical problems. The management of those risks should lead to minimizing the potential negative consequences of using AI technology, while at the same time providing opportunities to increase all its positive impacts. Effective management of AI risks should lead to the creation of more reliable security systems (Mladenović et al., 2025).

The use of artificial intelligence in security systems has opened numerous legal issues, given the lack of a universal definition of AI and the possibility of autonomous system behavior, which led to the first comprehensive law regulating the use of AI - the EU AI Act (EU Artificial Intelligence Act), which was adopted in July 2024. The aim of the Act is to ensure the use of AI systems in a safe and ethical manner. This law classifies all risks in AI systems into 4 categories (European Union, 2024):

- Prohibited risks – systems that are completely prohibited:
- High-risk AI - allowed, but under strict conditions:
- Limited risk – basic transparency is required:
- Minimal risk - no special restrictions.

The EU AI Act mandated manufacturers to establish, implement, document and maintain a risk assessment system for high-risk AI systems as a process that must last throughout the system's entire lifecycle — from development, testing, commissioning, and beyond — with regular and systematic upgrades. The assessment should be regularly reviewed and updated as new information or changes in system use become available. Article 9.2 a–d defines the stages of the Risk Assessment (European Union, 2024):

- Identification and analysis: Disclosure of all known and foreseeable risks, considering intended use and potential misuse.

- Assessment and evaluation: Quantifying the probability and level of risk, by analyzing the occurrence of risk in different scenarios.
- Assessment based on post-market monitoring: Risk analysis after system commissioning, using data from post-market monitoring.
- Application of risk management measures: Defining measures to reduce/eliminate risk, in accordance with user requirements and system functionalities, which means that risk should be eliminated or reduced as much as possible through technical design and development. If a residual (remaining) risk occurs, it must be acceptable for each hazard, and information about it must be communicated to all users.

The EU AI Act represents the first step towards the responsible use of AI. It does not prohibit the use of AI but sets rules to prevent abuses.

The UNESCO Recommendations on the Ethics of Artificial Intelligence (2021) represent the first global framework that addresses ethical principles and values in the development and use of artificial intelligence. The recommendations were adopted with the aim of promoting ethical principles in AI systems: human rights, sustainability, privacy, diversity and transparency. The UNESCO recommendations on the ethics of artificial intelligence contain guidelines for assessing the ethical risks of AI systems - Ethical Impact Assessment (EIA) - which includes the following stages (UNESCO, 2021):

- Scoping and preliminary analysis
- Risk assessment
- Verification and testing in real conditions
- Monitoring during the life cycle
- Mitigation and control measures.

As part of the UNESCO recommendations, an EIA comprehensive instrument was developed aimed at assessing and managing risks before and after the implementation of AI systems. RAM (Readiness Assessment Methodology), which measures how countries are ready to implement the recommendation of the methodology and encourages public transparency, human oversight and a multidisciplinary approach, is supported (UNESCO, 2021).

Within the framework of national legislation, various normative acts were adopted with the aim of regulating the use of AI technologies within the security system. The Law on the Protection of Personal Data of the Republic of Serbia ("Official Gazette of RS", No. 87/2018) is harmonized with the General Data Protection Regulation (GDPR) of the EU and sets rules on how to collect, store, process and protect personal data of citizens and contains certain provisions related to the application of AI technologies in security systems, especially those that use automatic decision-making, profiling, biometrics or the processing of large amounts of data. According to the Personal Data Protection Act and the GDPR, a Data Protection Risk Assessment (DPIA) is mandatory before starting data processing if the AI system uses new technologies, biometric systems in public spaces, including profiling or processes large amounts of data.

The Republic of Serbia also adopted the Conclusion on the Adoption of Ethical Guidelines for the Development, Application and Use of Reliable and Responsible Artificial Intelligence ("Official Gazette of RS", No. 23/2023). The new Strategy for the Development of Artificial Intelligence in the Republic of Serbia 2025-2030, adopted by the Government on January 10, 2025, represents a continuation and specifies the institutional, legal, educational and infrastructural framework for the reliable and responsible application of AI. All this shows that great efforts are being made in the comprehensive legal regulation of the use of AI in security systems, which confirms that defining the content of the risk assessment is an inevitable step in this process.

3. Methodological basis of risk assessment: international and national standards

In security practice, different risk assessment models are applied depending on the specifics required by each security area. The application of artificial intelligence in security systems makes the changes in these systems even more dynamic, so the regulations on artificial intelligence must also reflect this phenomenon. Globally, all countries are considering how best to regulate the application of AI technologies without hindering the innovation where it is necessary. Therefore, a responsible and precise normative framework becomes even more important, because the way in which these technologies are approached will play a decisive role in shaping regulations and standards. The existence of a standardized concept of the content of risk assessment of the application of AI in security systems would significantly contribute to the regulation of this area.

Methodologies for risk assessment in security systems are most often found in different groups of ISO standards, and taking into account the sensitivity of the area itself, some assessment methods require updating and pre-definition in order to arrive at a comprehensively applicable methodology. Standards such as ISO 31000:2018 - Principles of risk management, EN 17640:22, SRPS AL.2.003:2025 regulate certain elements of risk assessment, while 23894:2023 - Artificial Intelligence - Guidance on risk management is currently the only comprehensive standard that provides basic guidelines on risk management in AI systems.

ISO 31000:2018 - Principles of risk management include guidelines for managing the risks faced by organizations. The standard provides a common approach for managing any type of risk, is used throughout the entire life cycle of an organization but is not specific to AI risks. (Institute for Standardization of Serbia, 2018) According to this standard, the risk assessment process includes:

- Risk identification,
- Risk analysis,
- Risk assessment.

Figure 1. Risk management process

Source: (Institute for Standardization of Serbia, 2018)

The standard itself allows organizations to see and assess the risks they face but does not provide specific instructions (methodology) for risk assessment in AI systems.

EN 17640:2022 - Methodology for evaluation of cyber security in a fixed time for ICT products includes the assessment of security measures of ICT products, which is carried out through various scenarios aimed at vulnerabilities, development, testing and resilience of the system (Institute for Standardization of Serbia, 2022), but its applicability is limited in relation to AI systems, because it deals with classic ICT products, does not follow the entire life cycle of AI models and does not contain a methodology applicable in the field of AI.

ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations and the national counterpart SRPS ISO/IEC 38507:2023 Information technologies - IT management - Implications of the use of artificial intelligence on the management of organizations emphasize management, which is carried out by people using AI, and not on the AI systems themselves (Raković, 2024). In addition, the standards ISO/IEC 24028:2020 Security aspects and reliability of AI, ISO/IEC TR 24027:2021, Assessment of bias in AI, ISO/IEC 22989:2022 - Terminology and concepts of AI

contain different types of guidelines for risk assessment in AI systems, but do not propose a methodology for these assessments.

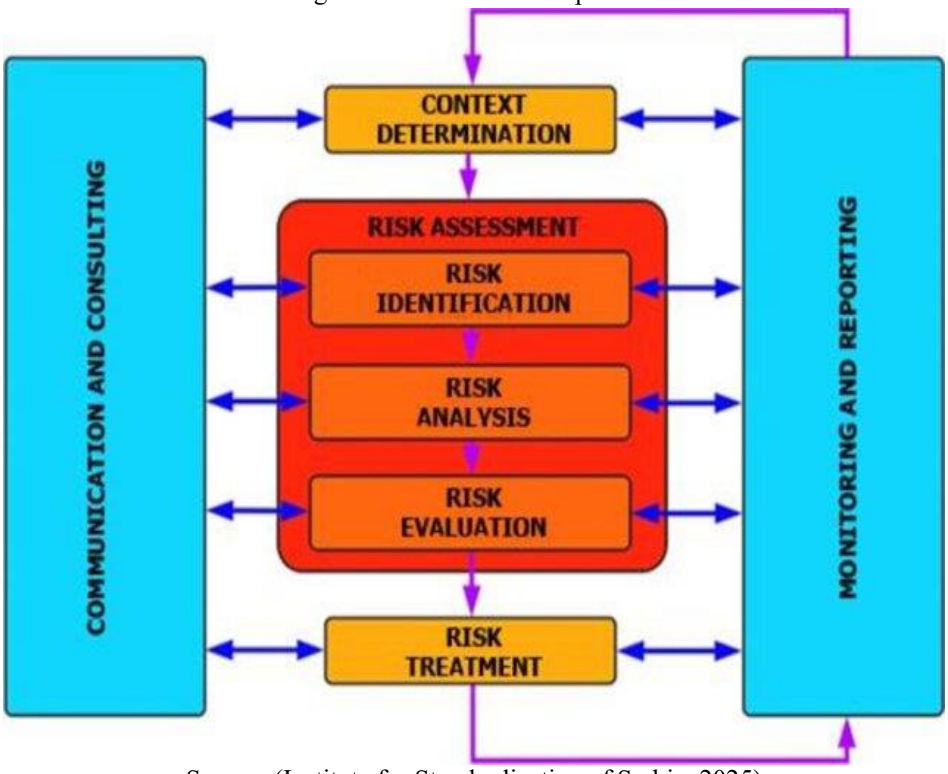
ISO/IEC 42001:2023 - "Artificial intelligence — Management system" is a standard for the management of AI systems that includes provisions on risk management as part of a mandatory policy and process, defines requirements for the assessment and treatment of risks associated with the use of AI and emphasizes the need for compliance with ethical principles, security and data protection in AI systems, but its scope in the area of risk assessment of the application of AI in security systems is significantly limited due to the high level of generality and the lack of security-specific methodological solutions.

The national standard for risk assessment in the protection of persons, property and business SRPS AL.2.003:2025 - Security and resilience - Risk assessment - Requirements and instructions for assessing compliance in the Republic of Serbia contains a methodology for assessing different types of risks in the field of security (Institute for Standardization of Serbia, 2025). According to this standard, the risk assessment process includes:

- Risk identification
- Risk analysis
- Risk assessment

SRPS A.L2.003 does not contain provisions related to the application of AI technologies or risk management in the field of AI but only addresses risks in the field of ICT infrastructure, without defining the requirements regarding artificial intelligence and its application.

Figure 2. Risk assessment process



Source: (Institute for Standardization of Serbia, 2025)

ISO/IEC 27001 Information security, cyber security and privacy protection — Information security management systems — Requirements are an international standard that regulates information security (ISMS) and defines requirements for the establishment, implementation, maintenance and continuous improvement of a security management framework aimed at protecting the confidentiality, integrity and availability of information. This standard focuses on the modernization of risk control in the context of new technological challenges, including the integration of digital services, cloud environments and automated systems such as AI tools. ISO 27001 requires systematic risk management through:

- identification of risks and vulnerabilities,

- probability and impact assessment,
- risk treatment through control and measures.

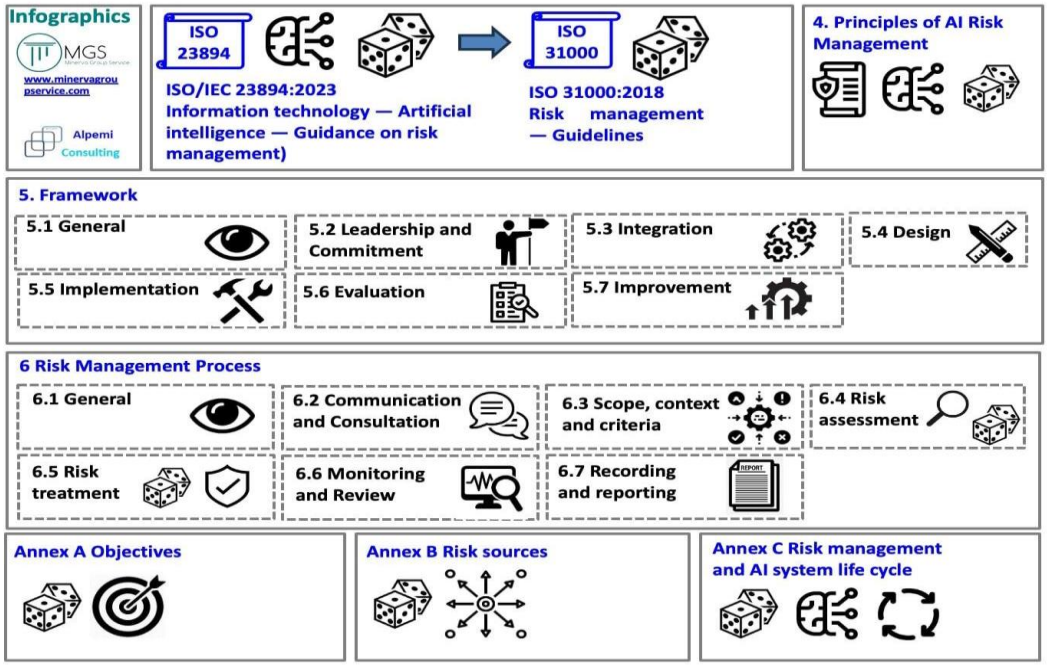
According to this standard, each organization must define risk assessment criteria and methodology that reflect their objectives and context. Risks must be continuously monitored and updated. The ISO 27001 standard does not contain explicit provisions that directly name AI risks, but the risk assessment process within an ISMS is flexible enough to include AI-specific risks (ISO, 2025).

In the last few years, due to the expansion of AI systems, international standards specific to risk assessments in this area have been adopted. ISO/IEC 23894:2023 - Artificial Intelligence - Guidance on risk management is a comprehensive standard that provides basic guidance on risk management in AI systems. The standard enables the assessment of specific AI risks during the life cycle of the AI model in compliance with prescribed ethical principles. Risk assessment according to this standard includes:

- Context of organization and system
- Risk identification
- Risk analysis
- Risk assessment
- Risk treatment
- Supervision and audit
- Communication and consultation (International Organization for Standardization, 2023)

This standard is the first international standard solely dedicated to risk assessment in AI systems and provides guidance on how organizations that develop, produce, implement or use products, systems and services that use artificial intelligence (AI) can manage risks specifically related to these systems. The guidelines also aim to help organizations integrate risk management into their AI-related activities and functions and describe processes for effective implementation and integration of AI risk management (Raković, 2024).

Figure 3. Risk management process



Source: (ISO/IEC 23894:2023)

The application of these guidelines is adaptable to any organization and its context.

On the basis of the presented standards, it can be concluded that there are a small number of developed methodologies for assessing AI risks in security systems, but that the risks that AI carries with it are multiplying daily, so that the existing regulations and standards can serve as the basis on which the methodology for assessing

risks arising as a consequence of the development of artificial intelligence, especially in security systems, will be further developed.

4. Risk assessment content of ai application in security systems

Risk assessment of the application of AI in security systems requires an expanded methodological framework compared to classic security systems, due to the specific characteristics of AI technologies, such as autonomy, adaptability and limited explainability of decisions (International Organization for Standardization [ISO], 2023). Based on the already existing normative framework and valid standards that deal with this topic, a comprehensive content of the risk assessment of the application of AI in security systems can be reached, which is applicable to any type of organization and during the entire life cycle of AI technology. The conceptualization of the content of the risk assessment is obtained by integrating the guidelines from the relevant normative frameworks and international standards, which ensures consistency and verifiability of the results. ISO/IEC 27001 prescribes mandatory elements of the risk assessment and treatment process within an information security management system (ISO, 2022), while ISO/IEC 23894 provides guidelines for adapting this process to the specifics of an AI system (ISO, 2023). In addition, the principles from the ISO 31000 standard provide a conceptual framework for the integration of risk into the wider management system of the organization (ISO, 2018), while the provisions of the EU Act and GDPR allow, among other things, the categorization of risks according to acceptability and oblige them to constantly review, control and assess. An integrated risk assessment model based on the application of multiple standards and normative acts enables a holistic approach to risk management in security systems with AI components. By combining the principles of ISO 31000, the requirements of ISO/IEC 27001 and the guidelines of ISO/IEC 23894 and other standards, organizations can identify the interdependencies between technical, organizational, ethical and other risks, thereby improving the overall resilience of security systems (ISO, 2018; ISO, 2022; ISO, 2023). This approach is in line with the recommendations of the NIST AI Risk Management Framework, which emphasizes the need for continuous and iterative AI risk management (NIST, 2023). Based on existing guidelines, a comprehensive and systematic content of risk assessment in the application of AI technologies in security systems can be reached, which can be applied in any type of organization, is independent of the size of the organization and applicable throughout the entire life cycle of AI.

Risk assessment begins with scoping/preliminary analysis and establishing a context that includes an analysis of the observed organization, leadership and commitment to risk management, the internal and external context of the organization, assignment of organizational roles, powers and responsibilities, provision and distribution of resources, establishment of communication, consultation and mechanisms for monitoring, reporting, implementation, evaluation, adaptation and continuous improvement (1).

After the initial phase of establishing the context, there is a phase of risk assessment. The risk assessment process consists of the identification, analysis and evaluation of risks. (2) Risk identification (2.1) represents the starting point of risk assessment and includes the systematic recognition of risk sources that may negatively affect the functioning of AI security systems. In addition to traditional threats to information security, such as unauthorized access and data compromise, specific AI risks are also identified, including manipulation of input data (adversarial attacks), model bias, performance degradation over time, and dependence on the quality of learning data (ISO, 2022; ISO, 2023). This approach is in accordance with the requirements of the ISO/IEC 27001 standard, which emphasizes the need to identify and document relevant risks within the information security management system (ISO, 2022). In the risk identification phase, it is necessary to identify all possible risks to make a comprehensive assessment. The list of identified risks classified according to the EU AI Act (Article 5 of the EU AI Act) can roughly be:

1. Unacceptable risks (prohibited systems)

    - AI for manipulating human behavior (e.g. subconscious)
    - Credit rating system by governments
    - Real-time biometric identification in public spaces (except in exceptional cases)

2. High-Risk AI Systems

    - AI in critical infrastructure (traffic, energy...)
    - AI in education (e.g. automatic grading)
    - AI for recruitment (e.g. automatic selection of candidates)
    - Biometric identification (under strictly controlled conditions)

3. Limited Risks (Limited Risk AI Systems)
    - Chatbot must clearly inform the user that it is not human
    - AI that generates images, video or text must indicate that the content was generated
4. Minimal risks (Minimal / Low Risk AI Systems)
    - AI in video games, spam filters...

The identified risks can also be categorized according to the stages of the life cycle of the AI system:

- Phase of concept and planning (purpose & scope)
- Phase of system design
- Phase of data collection and preparation
- Phase of model training
- Phase of testing and validation
- Phase of implementation and commissioning
- Phase of operational use
- Monitoring, maintenance and updating phase
- Phase of withdrawal and decommissioning

ISO/IEC 23894:2023 - Artificial Intelligence - Guidance on risk management forms a list of risks that can occur in AI systems. According to those guidelines, a comprehensive list of risks targeting AI systems can be made.

- Technical risks
- Data Risks
- Risks of bias and discrimination
- Risks of non-transparency and inexplicability
- Ethical risks
- Legal and regulatory risks
- Privacy and data protection risks
- Security risks
- Risks of model degradation (concept drift)
- Risks of Improper Use
- Risks of social and social influence
- Risks of Human Supervision and Interaction
- Risks of system trust and acceptability
- Risks related to interoperability and compatibility
- Risks related to the sustainability and resilience of the system.

After the identification of all risks and their detailed description, the size of the danger is determined based on an adequately chosen methodological model, which moves on to the risk analysis (2.2). In the analysis phase, the organization's exposure to those risks and its vulnerability are assessed to determine the probability of realization of the identified risks. By determining the damage and criticality, the size of the consequences for the organization is obtained, and by crossing them with the probability, the level of risk is reached. In the context of AI security systems, the consequences are not only reflected in operational or financial losses, but also in the potential violation of human security, violation of basic rights and loss of trust of stakeholders (Floridi et al., 2018). The assessment of AI risks in security systems, due to their scope and complexity, requires a combination of qualitative and quantitative assessment methods.

After the stage of obtaining the value of the risk level, there follows the stage of their evaluation, i.e. deciding on their admissibility or inadmissibility (2.3). Defining risk acceptability criteria is a key step in deciding on further risk treatment. According to risk management guidelines, acceptance criteria must be clearly defined, documented and aligned with the organization's strategy and applicable regulatory requirements (ISO, 2018). In the case of AI systems in the security domain, acceptance criteria are often more restrictive, especially when the system affects critical decision-making that may have direct consequences for the security of people, property and business (ISO, 2023).

Figure 3. AI Risk assessment

Source: Author

Assessed risk levels and defined acceptance criteria result in risks that we consider acceptable or unacceptable. All risks assessed as unacceptable by the organization require treatment to reduce their level to an acceptable level. Risk treatment includes various measures that organizations undertake in risk management, i.e. reducing the probability of their occurrence or mitigating their consequences (3). Measures can be physical protection measures, technical protection measures, normative-administrative and procedural measures, risk mitigation options, feasibility options (Institute for Standardization of Serbia, 2025). The ISO/IEC 27001 standard requires the application of appropriate technical and organizational measures, while ISO/IEC 23894 additionally emphasizes the need for specific AI measures, such as model validation, performance monitoring, decision explainability and human supervision of system operation (ISO, 2022; ISO, 2023a). These measures are the basis for building reliable and secure security systems in which AI technologies are applied.

In addition to treatment, every organization within the framework of risk assessment must foresee the ways of control and verification of applied measures, recording and reporting and constant review of risk assessment. Based on the entire assessment, within its content, there must be a final report (4) (Institute for Standardization of Serbia, 2025) in which the evaluation and presentation of the level and category of aggregate AI risk of the observed organization and analysis by risk groups with total data: level, category and acceptability can be seen. It is also necessary to draw a conclusion on the current state of protection and review new measures to improve the state to achieve maximum effectiveness and efficiency of protection.

A comprehensive AI risk assessment in security systems makes these systems efficient, effective and reliable, which is of utmost importance for their successful functioning.

5. Conslusion

Security systems in which AI technologies are applied face specific risks, which require continuous updating of risk assessment and an adaptive approach to risk management. The lack of content of this risk assessment further complicates the establishment of an effective and efficient security system. The development of risk assessment content and methodology in AI security systems is aimed at strengthening standardization, developing qualitative and quantitative reliability metrics, and integrating ethical principles into formal risk management models. This allows future regulatory and standardization frameworks to further specify the requirements for assessing and managing AI risks in the security domain. The application of multiple standards in risk assessment enables a comprehensive and systematic approach to risk management in complex security systems where AI technologies are applied. However, this approach can lead to increased complexity of implementation, the need for additional resources and the potential overlap of requirements of different standards, which requires a high level of organizational maturity and a serious approach to risk management.

The presented comparative analysis of the existing normative and standardization framework shows that risk assessment in security systems with integrated artificial intelligence components requires a systematic, structured and standardized approach that goes beyond the scope of traditional risk management models. The identification of exposure and vulnerability, the analysis of probability and consequences, as well as the definition of risk acceptance criteria, are key elements for an objective assessment of the level and category of AI risk, both at the level of the organization as a whole and by individual functional units and locations.

The results of the work confirm that the application of an integrated model of risk assessment content based on a combination of several relevant standards enables a more comprehensive overview of technical, organizational, legal and ethical aspects of AI risks. The need for continuous monitoring of AI system performance, regular review of risk assessment and application of adequate control and mitigation measures, with clearly defined responsibilities and an active role of management, was particularly emphasized. This ensures not only a reduction in unacceptable risks, but also an increase in the overall resilience and reliability of the security system.

The work indicates that effective risk management in security systems with AI components is possible only through the integration of risk assessment into the wider system of corporate security and management, with constant improvement of the process in accordance with the development of technology and the regulatory framework. The proposed approach represents a viable basis for practical application in organizations, as well as a starting point for further research in the field of standardization and quantification of AI risks in security systems.

Literature

1. European Union. (2024). EU Artificial Intelligence Act (EU 2024/865). https://artificialintelligenceact.eu/ai-act-explorer/
2. Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707.
3. Ineris. (n.d.). How can risk be defined? Ineris. https://www.ineris.fr/en/risks/what-risk/how-can-risk-be-defined
4. Institute for Standardization of Serbia. (2018). ISO 31000:2018 Risk management - Guidelines. Belgrade: ISS.
5. Institute for Standardization of Serbia. (2022). SRPS EN 17640:2022 - Security - Risk assessment of security measures. Belgrade: ISS.
6. Institute for Standardization of Serbia. (2025). SRPS A.L2.003 – Safety and resilience – Risk assessment – Requirements and guidance for conformity assessment (III edition). ISS.
7. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 27001:2025 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
8. International Organization for Standardization. (2018). ISO 31000:2018 – Risk management — Guidelines. ISO.
9. International Organization for Standardization. (2023). ISO/IEC 23894:2023 – Information technology – Artificial intelligence – Guidance on risk management. ISO.
10. Mladenović, M., Janković, K., & Komazec, N. (2025). Risk assessment for AI applications in security systems: Challenges and opportunities. In 11th Scientific-Professional Conference Security and Crisis Management – Theory and Practice (SeCMan), Belgrade. https://doi.org/10.70995/YMSH5950

11. National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). NIST.
12. Raković, R. (2024). Artificial intelligence and ISO standards [Artificial intelligence and ISO standards]. Military Information Bulletin, 27(1), 19–29. https://doi.org/10.5937/VI24019R
13. Republic of Serbia. (2018). Law on Protection of Personal Data ("Official Gazette of RS", No. 87/2018).
14. UNESCO Recommendation on the Ethics of AI - https://www.unesco.org/en/artificial-intelligence/recommendation-ethics