Asian Journal of Technology and Applied Sciences
ISSN: 2301-xxxx (online) | IF: 10.01 | Vol: 1, issue 1
Available: http://asiansciencejournal.org

ENHANCING ROBOTIC SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE AND IT TECHNOLOGIES: PERSPECTIVES ON INTELLIGENT CONTROL, AUTONOMOUS OPERATION, AND SAFETY

LAPASOV NURISLOM FARXOD O‘G‘LI
Senior Lieutenant, Senior Instructor (AI and IT Technologies Section), Department of Advanced Military Technologies, Faculty of the Central Military District, University of Military Security and Defense of the Republic of Uzbekistan

Abstract: This article analyzes the integration of artificial intelligence (AI) and information technology (IT) into robotic systems. Utilizing systemic, comparative, and functional analysis, as well as methods of generalization, the study examines the safety and control aspects of deploying robots. A five-stage conceptual model—spanning from task definition to monitoring—is proposed. While this model has not yet undergone practical testing, it serves as a foundation for future research.

Keywords: robotics, artificial intelligence, IT technologies, autonomous robots, sensors, intelligent control, human-robot collaboration, functional safety.

Introduction

Robotics is a multidisciplinary field based on the integration of mechanical devices, electronics, control theory, sensors, and software. Modern robots are utilized in manufacturing, logistics, agriculture, medicine, the service sector, education, and scientific research. Advancements in sensors and computational power enable robots to gather data from their environment, control their movements, and execute predefined tasks.

Artificial intelligence equips robotic systems with the ability to analyze visual and sensor data, recognize objects, adapt to environmental changes, and support planning processes. Meanwhile, IT technologies connect robots to networks, databases, cloud or edge computing infrastructure, control dashboards, and other production systems. Consequently, a robot ceases to be merely an isolated mechanical device and instead becomes an integral component of a digital system capable of exchanging data and being controlled.

However, the increasing complexity of intelligent robotic systems also gives rise to new requirements. Issues such as sensor errors, communication failures, software glitches, inaccurate model inferences, or unexpected interactions with humans can pose risks. Therefore, in addition to system efficiency, factors such as safety, reliability, testing, and human oversight must be taken into account from the initial stages of design.

The International Federation of Robotics monitors developments in various fields of robotics by publishing statistics and market analyses concerning industrial and service robots. Meanwhile, the NIST AI Risk Management Framework emphasizes the necessity of managing risks associated with artificial intelligence systems throughout their design, development, deployment, and evaluation. These approaches provide a foundation for integrating safety management with technical capabilities in robotics projects.

Research Goal and Objectives

The goal of the research is to propose a conceptual model for integrating AI and IT technologies into robotic systems, encompassing perception, control, data exchange, human oversight, and safety.

Objectives: (1) to identify the core technological components of intelligent robotics; (2) to analyze the possibilities and limitations for practical application; (3) to systematize

requirements for safety and risk management; (4) to develop implementation stages and evaluation criteria.

Object and Subject of Research

The object of the research is the processes involved in the design, control, and operation of robotic systems. The subject of the research is the technical, organizational, and safety-related conditions for integrating AI and IT technologies into robotics.

Scientific-Theoretical Foundations and International Approaches

A robotic system typically consists of a mechanical platform, actuators, sensors, a control module, software, and a user interface. In intelligent robots, these components may be augmented with AI methods, such as machine learning, computer vision, planning, or environmental modeling. However, not all robots require AI: for rigid and repetitive tasks, traditional control algorithms may be simpler, more understandable, and easier to verify.

The International Federation of Robotics (IFR) *World Robotics* reports provide international statistics and practical trends regarding industrial and service robots. While this data helps in understanding the development of robotics within a broader context, it does not replace the need for organization-level metrics to evaluate the effectiveness of a specific project.

The NIST AI Risk Management Framework focuses on reliability, safety, robustness, transparency, and risk management throughout the entire lifecycle. In the field of robotics, these principles can be adapted to assess factors such as potential model errors, the quality of sensor data, environmental changes, and human-robot interaction.

The ISO 10218 series of standards for industrial robot safety outlines requirements for the safe design, integration, and operation of industrial robots and robotic applications. The specific part of the standard and the current version should be verified based on the type of project and the applicable jurisdiction. This article does not replace the full text of the standard, nor does it constitute a certification of compliance.

Research Methodology

The research is conceptual and based on documentary analysis. The sources selected include official reports on robotics from the International Federation of Robotics (IFR), materials from the NIST Artificial Intelligence Risk Management Framework (AI RMF), and official documentation regarding the ISO 10218 series of standards for industrial robot safety. Selection criteria included the official nature of the sources, their direct relevance to the subject matter, verifiability, and their coverage of principles related to robotics, AI governance, or safe operation.

1. Systems analysis method. A robotic system was examined as a unified entity comprising a mechanical platform, actuators, sensors, software, AI modules, IT infrastructure, operators, and safety mechanisms. The interdependencies between sensor data, perception, planning, control, communication, and human oversight were analyzed. This approach helped establish that system effectiveness does not depend on a single algorithm, but rather on the coordinated functioning of all components and the implementation of safety measures.

2. Comparative analysis method. A comparison was made between the IFR reports—which cover the development and application trends of robotics—the NIST AI RMF (with its focus on managing AI-related risks), and the ISO 10218 standards, which address the safety of industrial robots. The criteria used for this comparison included the purpose of each source, its scope of application, and the guidance it provides for practical design. The analysis concludes that while these sources serve different functions, they complement one another regarding the context of development, the management of AI risks, and aspects of physical safety.

Asian Journal of Technology and Applied Sciences
ISSN: 2301-xxxx (online) | IF: 10.01 | Vol: 1, issue 1
Available: http://asiansciencejournal.org

3. Functional analysis method. Functions such as acquiring data from sensors, perceiving the environment, identifying objects, planning motion, controlling actuators, exchanging information via networks, and collaborating safely with humans were analyzed individually. For each function, the necessary conditions and constraints—including sensor errors, communication latency, model uncertainty, physical safety, and maintenance requirements—were examined. Consequently, it was determined that the expected benefits of implementing AI cannot be evaluated in isolation from the specific task, operational environment, and safety requirements.

4. Generalization method. The principles and challenges identified through the previous three methods were synthesized to establish a logical sequence for the implementation of robotic systems. Based on this, a five-stage conceptual model was proposed, comprising: task and risk identification; preparation of sensor and IT infrastructure; integration of AI and control systems; testing and safety validation; and monitoring and continuous improvement. Furthermore, a unified set of evaluation criteria was developed, covering task performance quality, perception and navigation, operational efficiency, safety, reliability, cybersecurity, and the human factor.

In this study, no robot prototype was developed, no experiments were conducted, and no new sensors or control algorithms were tested. Consequently, no empirical claims—such as specific degrees of improvement in speed, accuracy, or safety—are made. The model is a conceptual proposal developed by the author based on an analysis of international sources; further laboratory and pilot testing will be required to determine its effectiveness.

The Role of AI and IT in Robotics

Sensors and Environmental Perception

Cameras, LiDAR, radar, ultrasonic sensors, encoders, and inertial measurement units (IMUs) enable a robot to gather information about its environment and its own state. AI techniques can be employed to detect and classify objects within images or to identify patterns in data streams from sensors. In cases where sensor data is contradictory or noisy, the system must account for uncertainty and incorporate protocols for transitioning to a safe state.

Intelligent Planning and Control

A robot’s movements are planned in accordance with specific tasks, the environment, mechanical constraints, and safety requirements. AI can assist in path selection, object manipulation, or adapting to changing tasks. However, it cannot be assumed that the output of a learned model will automatically comply with physical safety constraints. Motion commands must pass through a supervisory control layer, and a mechanism for emergency stops must be in place.

IT Infrastructure and Inter-Robot Communication

Networking, edge computing, cloud computing, and centralized control software facilitate the integration of robots with production management systems, warehouse platforms, or remote monitoring infrastructure. However, for real-time control, factors such as network latency, communication interruptions, and cybersecurity risks must be taken into account. Key safety-related control functions should not be entirely dependent on the availability of external communication.

Applications in Industry, Logistics, Medicine, and Education

In industry, robots are used for repetitive tasks such as assembly, welding, inspection, and material handling. In logistics, mobile robots can assist with transporting goods within warehouses and managing inventory. In medicine, robotic systems are employed for specific clinical or rehabilitative tasks; however, their implementation requires adherence to strict

Asian Journal of Technology and Applied Sciences
ISSN: 2301-xxxx (online) | IF: 10.01 | Vol: 1, issue 1
Available: http://asiansciencejournal.org

clinical, technical, and regulatory standards. In education, robotics serves as a practical platform for teaching programming, sensor technology, control theory, and collaborative problem-solving.

Human-Robot Collaboration

Collaborative robots (cobots) are designed to operate within the same workspace as humans. However, the term "collaborative" does not imply that a robot is safe under all circumstances. Factors such as risk analysis, speed and force limitations, maintenance of safe distances, emergency stop mechanisms, workspace design, and operator training all contribute to the overall safety of the system.

Key Challenges and Risks

Sensor and Model Errors

Sensor contamination, calibration inaccuracies, changes in lighting conditions, or obstructions within the field of view can degrade the quality of perception. Furthermore, AI models may be prone to errors when encountering situations that were rarely represented in their training data. Therefore, tests should cover not only typical scenarios but also edge cases and unexpected situations.

Physical Safety and the Human Factor

An incorrect movement by a robot can lead to human injury, equipment damage, or the halting of a production process. Safety should not rely solely on the AI model; physical safeguards, interlocks, emergency stops, designated safe working zones, and engineering measures for risk mitigation are essential.

Cybersecurity and Software

Network-connected robots may be exposed to risks such as unauthorized access, software vulnerabilities, misconfigurations, and supply chain threats. It is recommended to restrict access rights, manage software updates, implement network segmentation, maintain audit logs, and develop recovery plans.

Data and Model Reliability

The output of an AI model depends on data quality and how well the current situation aligns with the conditions under which the model was trained. Previous results may change following a model update. Therefore, it is necessary to manage model versions, conduct re-testing, and monitor performance during actual operation.

Costs, Maintenance, and Personnel Training

The total cost of a robotic system extends beyond its initial purchase price. Costs for integration, sensor calibration, software, safety inspections, spare parts, staff training, and ongoing service must also be taken into account.

Discussion

The application of AI in robotic systems can enhance perception and adaptability; however, selecting the most complex model for every task is not necessarily required. If a task can be reliably performed using strict, rule-based logic, traditional control methods may be preferable due to their simplicity and verifiability. The decision to implement AI should be based on technical benefits, risks, costs, and maintainability. The proposed model links a robot's intellectual capabilities with safety and operational management. Nevertheless, its effectiveness has not yet been tested across various platforms or operating environments. Future research could evaluate the model by applying it to industrial manipulators, mobile robots, or educational robots, while conducting a comparative assessment of task performance quality, safety, and the total cost of ownership.

Conclusion

Integrating artificial intelligence and IT technologies into robotics expands capabilities in areas such as sensor data analysis, environmental perception, task planning, control support, and the connection of robots to digital infrastructure. At the same time, the reliable operation of such systems depends on physical safety, software stability, cybersecurity, human oversight, and regular maintenance. The article proposes a five-stage conceptual model consisting of the following phases: identifying tasks and risks, preparing sensor and IT infrastructure, integrating AI and control systems, conducting testing and safety validation, and performing monitoring and continuous improvement. Its scientific and practical contribution lies in linking international management and safety principles to the practical execution of robotics projects, as well as in systematizing evaluation criteria.

When planning robotics projects, it is recommended to clearly define technological requirements, analyze risks at an early stage, conduct controlled testing, and maintain monitoring throughout the operational phase. Future empirical research is needed to determine the model's applicability, limitations, and effectiveness across various robotic platforms.

REFERENCES

1. International Federation of Robotics (IFR). World Robotics: Industrial Robots and Service Robots. Official reports and statistics. https://ifr.org/worldrobotics
2. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1
3. International Organization for Standardization (ISO). ISO 10218 series: Robotics — Safety requirements for industrial robots. Official standards catalog: https://www.iso.org/standards.html
4. National Institute of Standards and Technology (NIST). AI Risk Management Framework resources. https://www\.nist.gov/itl/ai-risk-management-framework/ai-risk-management-framework-resources