ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-3

A PROTOTYPE DEVELOPMENT FOR AN AUTOMATED CONTROL SYSTEM FOR PRODUCTION CHECKPOINTS

Svitlana Maksymova [1], Vladyslav Yevsieiev [1], Amer Abu-Jassar [2]

[1]Department of Computer-Integrated Technologies, Automation and Robotics, Kharkiv National University of Radio Electronics, Ukraine

[2]Department of Computer Science, College of Information Technology, Amman Arab University, Amman, Jordan

ABSTRACT

This paper presents a prototype development for an automated control system for production checkpoints within the Industry 4.0 framework. The system integrates biometric recognition, RFID technology, and automated access control mechanisms to enhance security and efficiency. The study highlights the advantages of an event-driven model for real-time access control and system scalability. The proposed solution ensures seamless integration with enterprise control systems, reducing operational risks and improving workforce monitoring.

Keywords: Automated System, Access Control, Industry 4.0, Biometric Recognition, RFID, Cybersecurity, Efficiency, Real-Time Monitoring, Prototype.

Introduction

In today's digital transformation of industrial enterprises, the implementation of automated access control systems is becoming not only a necessity, but also a key element of security and effective production processes control. Within the framework of the Industry 4.0 concept, which involves the integration of intelligent technologies, big data, the Internet of Things (IoT) and cyber-physical systems, an important task is to develop a prototype of an automated control system for production checkpoints [1]-[18]. Traditional access control mechanisms based on physical passes or manual verification are inefficient and prone to human error, which can lead to security threats, violations of the internal regime and unauthorized access to critical areas of the enterprise. Automation of this process allows you to significantly increase the level of control, ensure operational monitoring of personnel and transport, as well as integrate the system with other enterprise management modules. Various methods and approaches to the analysis and development of such systems can be used here [19]-[41].

The use of biometric technologies, RFID cards, facial recognition systems and license plates allows for a high level of accuracy in identifying individuals and vehicles, which in turn increases security and minimizes the risks of unauthorized entry. In addition, the use of big data analytics and artificial intelligence allows you to predict abnormal behavior, identify possible threats and respond promptly to any violations. The implementation of such a system allows you to optimize the time of passing checkpoints, which is important for increasing the productivity of the enterprise and reducing the costs of personnel control.

Within the framework of Industry 4.0, automated access control systems can be integrated with other digital solutions, such as ERP systems, production control platforms and intelligent video surveillance systems, which create a single enterprise control ecosystem. This allows you to not only ensure effective control of checkpoints, but also conduct analytics on employee flows, assess shift workload, monitor the level of security on the territory of the enterprise and automate reporting. The implementation of such solutions also contributes to compliance with international safety standards and regulatory requirements, which is critically important for industrial enterprises in the global economy [42]-[45].

Thus, the development of a model of an automated checkpoint control system within Industry 4.0 is a relevant and necessary area of research that allows increasing the level of safety, optimizing

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

production processes and integrating modern digital technologies into the production control system. It will contribute to the effective allocation of resources, minimizing risks and improving the overall organization of work, which are key factors for the successful development of industrial enterprises in modern conditions.

Related work

Various methods of restricting physical access in production are of considerable interest to researchers. Such methods are described in many studies. Let us consider several such works.

The inherent complexity of operational technology systems, along with their advanced-in-age nature, prevents defenders from fully applying contemporary security controls in a timely manner [46]. Authors in [46] note that existing vulnerabilities in the design and implementation of several of the operational technology-specific network protocols may easily grant adversaries the ability to decisively impact physical processes. We provide a categorization of such threats and the corresponding vulnerabilities based on various criteria.

García-Rodríguez, J., and co-authors in [47] propose to tie attribute-based credentials to biometric features of the credential holder and to require biometric verification on every use. In such settings, attribute-based credentials that are tied to biometrics, which we call Biometric-Bound Attribute-Based Credentials (bb-ABC), allow to implement scalable and privacy-friendly systems to control physical access to (critical) infrastructure and facilities.

Gupta, S., & et al. in [48] describe their Step & Turn prototype that addresses the fundamental limitations of the conventional physical access control schemes, i.e., users having a specific knowledge or possessing a particular device or token, to satisfy both usability and security requirements.

The paper [49] propose a new three-factor user authentication and key agreement scheme (UAKA-5GSICPS) for 5G-enabled SDN based ICPS environment. UAKA-5GSICPS allows an authorized user to access the real-time data directly from some designated Internet of Things (IoT)-based smart devices provided that a successful mutual authentication among them is executed via their controller node in the SDN network.

The researchers in [50] design a system model that can guarantee secure communication and transparently manage user identification data in metaverse environments using blockchain technology. They also propose a mutual authentication scheme using biometric information and Elliptic Curve Cryptography (ECC) to provide secure communication between users and platform servers and secure avatar interactions between avatars and avatars.

The accidents ones caused by malicious attacks represent a very challenging issue especially in Industry 5.0 concept [51]. This includes maliciously hijacking and controlling robots and causing serious economic and financial losses. This paper reviews the main security vulnerabilities, threats, risks, and their impacts, and the main security attacks within the robotics domain. In this context, different approaches and recommendations are presented in order to enhance and improve the security level of robotic systems such as multi-factor device/user authentication schemes, in addition to multi-factor cryptographic algorithms.

So, we see that the problem of ensuring security is very diverse and multifaceted. Consequently, the ways to solve this problem differ significantly. Further in this article we will consider the possibility of physically restricting access in production when passing through checkpoints.

An automated control system structure and a prototype development for production checkpoints

A flowchart design is a critically important stage in the development of an automated access control system in production, as it provides a comprehensive view of the functioning of the system and the interaction of its components. The flowchart allows identifying the main elements of the system, such as identification sensors, access controllers, data collection, information processing and

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

signal transmission systems. This makes it possible to clearly imagine all the processes occurring in the system and their logical sequence. The design also helps to identify potential risks, such as possible system failures or vulnerabilities that can be used for unauthorized access. In addition, the flowchart helps developers optimize the interaction between components, which contributes to increasing the reliability and efficiency of the system, as well as its flexibility for possible modifications in the future. Such a diagram is also a key tool for further technical documentation and coordination between the various departments involved in the development and implementation of the system.

When designing the structural diagram of an automated system for the production checkpoints control, it is necessary to take into account several key criteria that ensure efficiency, reliability and safety. One of the important criteria is the possibility of contactless identification of employees, which reduces physical contact and increases the speed of passage. This necessitates the use of computer vision systems and wireless networks based on RFID or NFC technologies. Computer vision allows you to automatically recognize people or other identification features without the need for additional carriers, which is convenient in large-scale production. The use of RFID or NFC provides fast data reading, without the need for physical contact with devices, which significantly increases the efficiency of the system. These technologies also provide a high level of security, as they allow you to avoid counterfeiting of identifiers and unauthorized access. Table 1 presents an analysis of the selected technologies and their description that will be used for the developed automated system for controlling the passage of checkpoints in production.

Table 1: Analysis of the selected technologies for the automated access control system in production development

Technology	Description
Contactless identification	Ensures speed and safety when passing through checkpoints
RFID or NFC	Provide reliable and fast reading of identification data without physical contact
Computer vision	Allows automatic face recognition, increasing the accuracy and convenience of the system
Data processing speed	Important for large flows of people to avoid delays in the identification process
Security and data protection	Guarantee that data will not be tampered with or access to the system will not be compromised

Based on the selected criteria that must be met by the automated access control system in the production being developed and the selected technologies given in Table 1, the following structural diagram of the automated access control system in production is proposed (Figure 1).

The structure diagram in Figure 1 shows a control system based on the use of automated access control system with the integration of various modules for face recognition and identification using RFID. The following is a description of the purpose of each of the blocks:

– camera, responsible for reading an image or video from a person's face for its further analysis. It is used in the face recognition module to identify the user based on biometric data;

– RFID, a module for reading RFID cards or other identifiers. This block contains a reader that interacts with an RFID chip that can be embedded in a card or other object to confirm the identification of a person or object;

– lock, an electronic lock or access blocking mechanism that receives signals from the control system to open or lock the door after successful identification of the user through face recognition modules or RFID;

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-3

– MM (microprocessor module), the control unit of the system that processes data received from the RFID module. It is responsible for reading data from the user card, decoding information and transmitting it to the laptop. The MM also receives data from the laptop and controls the opening or non-opening of the electric lock;

– laptop (single-board computer) – a device that performs the function of information processing and system management. Contains two main software modules: a face recognition module and an RFID data module;

– a face recognition module, a software part of the system that analyzes data from the camera and determines whether the user's face image matches the previously recorded biometric data. If the identification is successful, the data is transmitted to the control module to grant access;

– an RFID data module, this software module stores RFID code data that has access rights to the production premises.

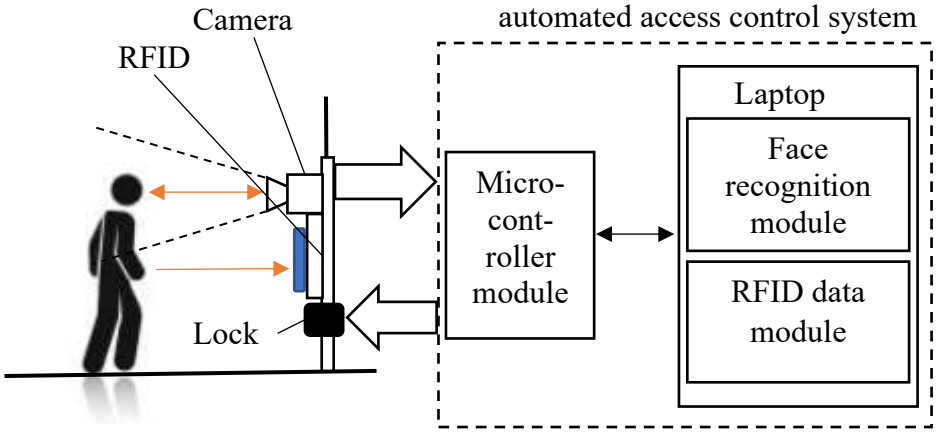

Figure 1: Structural diagram of the automated access control system prototype in production

The principle of operation of the developed scheme of the ASKPP layout in production is built as follows:

– the object of identification approaches the checkpoint in production;

– the system scans the face and reads data from the RFID card;

– the data received from the camera is directly transmitted to a laptop or single-board computer, and the data from the RFID card is decoded in MM and in the form of a 16-bit code via the USB port is also transmitted to a laptop or single-board computer;

– on a laptop or single-board computer, the facial recognition module analyzes the received facial image and checks it with existing samples, and at the same time checks the 16-bit code from the RFID card. Provided that these two parameters have a positive response to requests, the system via MM gives a command to open the lock. If one or all parameters do not match, the system does not give a command to open the lock.

The developed system combines two identification methods – biometric (facial recognition) and RFID, providing a multi-factor approach that increases access security.

Developing a wiring diagram for the automated access control system prototype in production is an important step to ensure the correct operation of all modules. The diagram will help to clearly determine how to connect components such as a camera, RFID module, relay, lock and Arduino Nano controller, which will prevent possible installation errors. Without the correct diagram, malfunctions may occur, which will affect the functionality of the entire system.

In addition, the wiring diagram will allow you to identify and eliminate potential power problems, ensure safe control of electronic components, avoid overload or short circuit. It will also

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

facilitate future maintenance and modernization of the system, which is important for its effective operation in production. The developed wiring diagram in the Fritzing environment is presented in Figure 2.

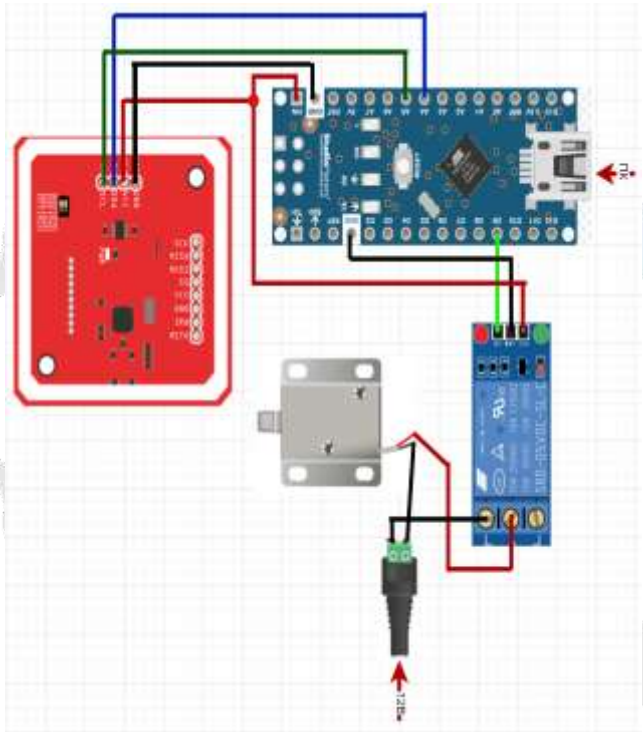

Figure 2: Connection diagram of the automated access control system hardware modules in production

The connection diagram (Fig. 2) of the created automated access control system prototypet uses several hardware modules. The circuit is based on the Arduino Nano board, which controls all components. The PN532 NFC RFID module is connected to the board via 4 wires: GND to Arduino ground, VCC to 5V for power, SDA to analog port A4, and SCL to A5 for data exchange via the I2C bus. A 1-channel 12V relay is also used, which is controlled by Arduino via digital output D6, which allows switching the power supply for the lock. The relay is supplied with 12V power, which is also used for an electromechanical solenoid lock. Arduino powers the relay via GND and controls it to lock or open the door.

The 12V power is supplied through a separate power supply unit, which is connected to the relay and the lock. This allows the lock to receive enough energy for proper operation.

The Logitech C920 HD Pro camera is connected to a laptop or microcontroller via a USB port. In this work, a laptop with a built-in webcam will be used to implement the prototype. As a result, Arduino Nano will be directly connected via USB port to the laptop.

According to the developed connection diagram (Figure 2), a automated access control system ptototype in production, the general view of which is presented in Figure 3.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-3

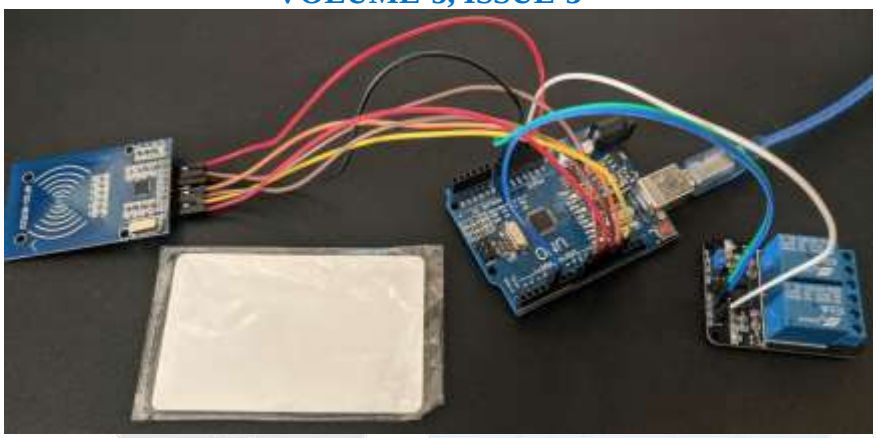

Figure 3: Assembled hardware component of the automated access control system prototype in production

Development of a general algorithm for the operation of the checkpoint control system

The development of a general algorithm for the operation of the automated access control system software in production is necessary to ensure the coordinated and effective operation of all system components. The algorithm determines the sequence of actions required for the correct identification, authentication and passage of employees or visitors. It takes into account the integration of various hardware modules (cameras, RFID, relays), as well as data processing by neural networks for face recognition. A clear algorithm allows you to optimize the operation of the system, reduce delays and increase the accuracy of identification, which is critically important for the safety and productivity of production. The general algorithm also simplifies the process of debugging, testing and future improvement of the system, ensuring its scalability and adaptability. Based on this, the following general algorithm for the operation of the automated access control system prototype in production is proposed, which is presented in Figure 4. The algorithm, which is presented in Figure 4, describes the process of the automated access control system prototype functioning in production. The process begins with loading the system settings. After that, the system waits for the RFID card to be raised. If the card is not read, the system continues to wait. Once the card is read, the data is read from it. If no data is received, the system returns to waiting for the card.

In case of successful data reading, they are transferred via the COM interface to the PC for further processing, after which the system waits for a response from the PC. In parallel, a search for matches with the database is launched on the PC. If the data is found, the camera is initialized to capture the face image. The system receives key points of the face and compares them with the template stored in the database.

If the data matches, a command is sent to open the lock. In case of a mismatch of the face or if the data on the card does not match the database, the card is blocked and the security service is called to ensure security. Thus, the algorithm provides two levels of authentication: by RFID card and by facial recognition, which increases the security of access to the checkpoint.

The developed algorithm provides a high level of security of access to the checkpoint by combining two authentication methods: RFID card reading and facial recognition. This minimizes the risks of unauthorized access, since each stage controls the authenticity of the user. The algorithm also ensures fast identification, as it searches for matches in the database and reads the image in parallel. The integration of the camera and processing of facial key points increases the reliability of recognition and reduces the likelihood of errors. In case of detection of a mismatch or suspicious actions, the system automatically blocks the card and calls the guard, which adds an additional layer of protection.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-5, ISSUE-3

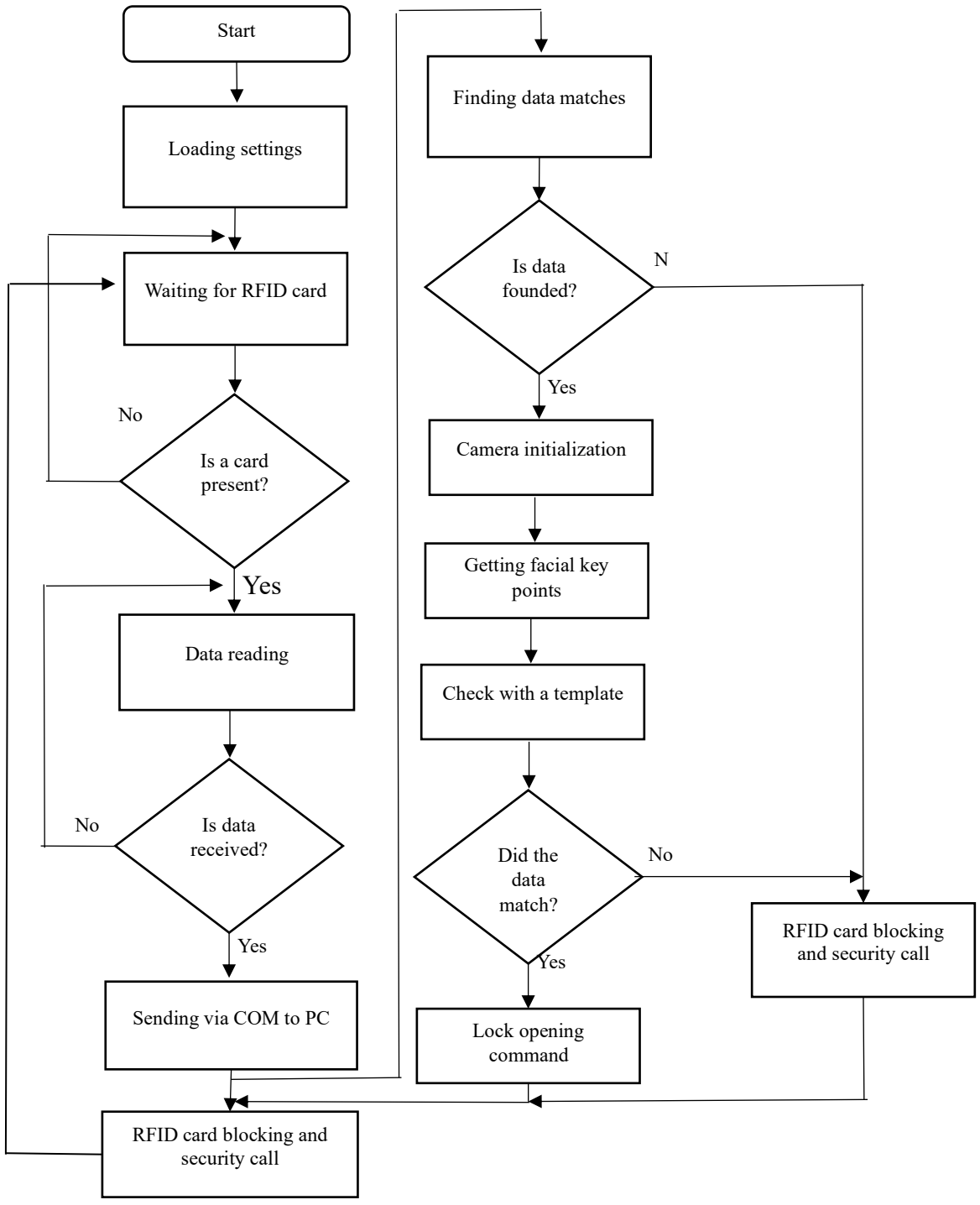

Figure 4: General algorithm of automated access control system operation in production

Conclusion

The developed prototype of an automated control system for production checkpoints demonstrates high efficiency in ensuring security and access control within the framework of the Industry 4.0 concept. The use of biometric identification and RFID technologies allows to significantly increase the accuracy and speed of verification of individuals, reducing the risks of unauthorized access. Integration of the system with other enterprise information platforms, such as ERP and MES, provides a comprehensive approach to personnel management and logistics. An event-based model of request processing allows reducing the load on the system and increasing its

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

adaptability to changes in production processes. Analysis of the obtained results confirms that the implementation of such a system contributes not only to security, but also to the optimization of internal processes at the enterprise, reducing the time of passing control and increasing overall productivity. Automation of data collection, processing and analysis in real time allows to promptly responding to potential threats and anomalous behavior, which is especially important in modern production conditions. The implementation of such systems also helps enterprises to comply with international security standards and the requirements of regulatory authorities. The proposed approach proves its effectiveness in creating a reliable, scalable and easily adaptable system that can be integrated into production processes of any level of complexity. Further research can be aimed at expanding the capabilities of user behavior analysis, implementing additional authentication levels, and integrating with advanced artificial intelligence systems for risk prediction.

References:

1. Yevsieiev, V., & et al. (2024). Human Operator Identification in a Collaborative Robot Workspace within the Industry 5.0 Concept. Multidisciplinary Journal of Science and Technology, 4(9), 95-105.
2. Gurin, D., & et al. (2024). Using the Kalman Filter to Represent Probabilistic Models for Determining the Location of a Person in Collaborative Robot Working Area. Multidisciplinary Journal of Science and Technology, 4(8), 66-75.
3. Chala, O., & et al. (2024). Switching Module Basic Concept. Multidisciplinary Journal of Science and Technology, 4(7), 87-94.
4. Abu-Jassar, A., & et al. (2024). Building a Route for a Mobile Robot Based on the BRRT and A*(H-BRRT) Algorithms for the Effective Development of Technological Innovations. International Journal of Engineering Trends and Technology, 72(11), 294-306.
5. Yevsieiev, V., & et al. (2025). Development of a program for processing 3d models of objects in a collaborative robot workspace using an HD camera. ACUMEN: International journal of multidisciplinary research, 2(1), 194-210.
6. Gurin, D., & et al. (2024). Effect of Frame Processing Frequency on Object Identification Using MobileNetV2 Neural Network for a Mobile Robot. Multidisciplinary Journal of Science and Technology, 4(8), 36-44.
7. Basiuk, V., & et al. (2024). Command System for Movement Control Development. Multidisciplinary Journal of Science and Technology, 4(6), 248-255.
8. Chala, O., & et al. (2024). Analysis of Systems for Coordination of Enterprise Subsystems Control. Journal of universal science research, 2(10), 127-137.
9. Gurin, D., & et al. (2024). Using Convolutional Neural Networks to Analyze and Detect Key Points of Objects in Image. Multidisciplinary Journal of Science and Technology, 4(9), 5-15.
10. Vizir, Y., & et al. (2024). Lighting Control Module Software Development. Journal of Universal Science Research, 2(2), 29–42.
11. Yevsieiev, V., & et al. (2024). HR data visualization of the distance to the object in the collaborative robot workspace based on hc-sr04 sensor. ACUMEN: International journal of multidisciplinary research, 1(4), 388-401.
12. Attar, H., Abu-Jassar, A. T., Amer, A., Lyashenko, V., Yevsieiev, V., & Khosravi, M. R. (2022). Control system development and implementation of a CNC laser engraver for environmental use with remote imaging. Computational intelligence and neuroscience, 2022(1), 9140156.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

13. Al-Sharo, Y. M., Abu-Jassar, A. T., Sotnik, S., & Lyashenko, V. (2021). Neural networks as a tool for pattern recognition of fasteners. International Journal of Engineering Trends and Technology, 69(10), 151-160.
14. Abu-Jassar, A. T., Al-Sharo, Y. M., Lyashenko, V., & Sotnik, S. (2021). Some Features of Classifiers Implementation for Object Recognition in Specialized Computer systems. TEM Journal: Technology, Education, Management, Informatics, 10(4), 1645-1654.
15. Abu-Jassar, A. T., Attar, H., Yevsieiev, V., Amer, A., Demska, N., Luhach, A. K., & Lyashenko, V. (2022). Electronic user authentication key for access to HMI/SCADA via unsecured internet networks. Computational intelligence and neuroscience, 2022(1), 5866922.
16. Nevliudov, I., Yevsieiev, V., Baker, J. H., Ahmad, M. A., & Lyashenko, V. (2020). Development of a cyber design modeling declarative Language for cyber physical production systems. J. Math. Comput. Sci., 11(1), 520-542.
17. Lyashenko, V., Abu-Jassar, A. T., Yevsieiev, V., & Maksymova, S. (2023). Automated Monitoring and Visualization System in Production. International Research Journal of Multidisciplinary Technovation, 5(6), 9-18.
18. Nevliudov, I., & et al.. (2020). Method of Algorithms for Cyber-Physical Production Systems Functioning Synthesis. International Journal of Emerging Trends in Engineering Research, 8(10), 7465-7473.
19. Mustafa, S. K., Yevsieiev, V., Nevliudov, I., & Lyashenko, V. (2022). HMI Development Automation with GUI Elements for Object-Oriented Programming Languages Implementation. SSRG International Journal of Engineering Trends and Technology, 70(1), 139-145.
20. Nevliudov, I., Yevsieiev, V., Lyashenko, V., & Ahmad, M. A. (2021). GUI Elements and Windows Form Formalization Parameters and Events Method to Automate the Process of Additive Cyber-Design CPPS Development. Advances in Dynamical Systems and Applications, 16(2), 441-455.
21. Kobylin, O., & Lyashenko, V. (2014). Comparison of standard image edge detection techniques and of method based on wavelet transform. International Journal, 2(8), 572-580.
22. Abu-Jassar, A. T., Attar, H., Lyashenko, V., Amer, A., Sotnik, S., & Solyman, A. (2023). Access control to robotic systems based on biometric: the generalized model and its practical implementation. International Journal of Intelligent Engineering and Systems, 16(5), 313-328.
23. Babker, A. M., Abd Elgadir, A. A., Tvoroshenko, I., & Lyashenko, V. (2019). Information technologies of the processing of the spaces of the states of a complex biophysical object in the intellectual medical system health. International Journal of Advanced Trends in Computer Science and Engineering, 8(6), 3221-3227.
24. Al-Sherrawi, M. H., Lyashenko, V., Edaan, E. M., & Sotnik, S. (2018). Corrosion as a source of destruction in construction. International Journal of Civil Engineering and Technology, 9(5), 306-314.
25. Al-Sharo, Y. M., Abu-Jassar, A. T., Sotnik, S., & Lyashenko, V. (2023). Generalized procedure for determining the collision-free trajectory for a robotic arm. Tikrit Journal of Engineering Sciences, 30(2), 142-151.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

26. Tvoroshenko, I., Lyashenko, V., Ayaz, A. M., Mustafa, S. K., & Alharbi, A. R. (2020). Modification of models intensive development ontologies by fuzzy logic. International Journal of Emerging Trends in Engineering Research, 8(3), 939-944.
27. Khan, A., Joshi, S., Ahmad, M. A., & Lyashenko, V. (2015). Some effect of Chemical treatment by Ferric Nitrate salts on the structure and morphology of Coir Fibre Composites. Advances in Materials Physics and Chemistry, 5(1), 39-45.
28. Sotnik, S. Overview: PHP and MySQL Features for Creating Modern Web Projects/ S Sotnik, V. Manakov, V. Lyashenko //International Journal of Academic Information Systems Research (IJAISR). – 2023. – Vol. 7, Issue 1. – P. 11-17.
29. Matarneh, R., Tvoroshenko, I., & Lyashenko, V. (2019). Improving Fuzzy Network Models For the Analysis of Dynamic Interacting Processes in the State Space. International Journal of Recent Technology and Engineering, 8(4), 1687-1693.
30. Lyashenko, V. V., Matarneh, R., Baranova, V., & Deineko, Z. V. (2016). Hurst Exponent as a Part of Wavelet Decomposition Coefficients to Measure Long-term Memory Time Series Based on Multiresolution Analysis. American Journal of Systems and Software, 4(2), 51-56.
31. Lyashenko, V. V., Deineko, Z. V., & Ahmad, M. A. Properties of wavelet coefficients of self-similar time series. In other words, 9, 16.
32. Kuzemin, A., Lyashenko, V., Bulavina, E., & Torojev, A. (2005). Analysis of movement of financial flows of economical agents as the basis for designing the system of economical security (general conception). In Third international conference «Information research, applications, and education (pp. 27-30).
33. Deineko, Zh., & et al.. (2021). Features of Database Types. International Journal of Engineering and Information Systems (IJEAIS), 5(10), 73-80.
34. Lyashenko, V., Laariedh, F., Ayaz, A. M., & Sotnik, S. (2021). Recognition of Voice Commands Based on Neural Network. TEM Journal: Technology, Education, Management, Informatics, 10(2), 583-591.
35. Ahmad, M. A., Baker, J. H., Tvoroshenko, I., & Lyashenko, V. (2019). Computational complexity of the accessory function setting mechanism in fuzzy intellectual systems. International Journal of Advanced Trends in Computer Science and Engineering, 8(5), 2370-2377.
36. Tahseen A. J. A., & et al.. (2023). Binarization Methods in Multimedia Systems when Recognizing License Plates of Cars. International Journal of Academic Engineering Research (IJAER), 7(2), 1-9.
37. Abu-Jassar, A. T., Attar, H., Amer, A., Lyashenko, V., Yevsieiev, V., & Solyman, A. (2025). Development and Investigation of Vision System for a Small-Sized Mobile Humanoid Robot in a Smart Environment. International Journal of Crowd Science, 9(1), 29-43.
38. Abu-Jassar AT, Attar H, Amer A, et al. Remote Monitoring System of Patient Status in Social IoT Environments Using Amazon Web Services (AWS) Technologies and Smart Health Care. International Journal of Crowd Science, 2024.
39. Attar, H., Abu-Jassar, A. T., Lyashenko, V., Al-qerem, A., Sotnik, S., Alharbi, N., & Solyman, A. A. (2023). Proposed synchronous electric motor simulation with built-in permanent magnets for robotic systems. SN Applied Sciences, 5(6), 160.
40. Abu-Jassar A. Building a Route for a Mobile Robot Based on the BRRT and A*(H-BRRT) Algorithms for the Effective Development of Technological Innovations / Amer Abu-Jassar,

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 9.948 / 2024

Hassan Al-Sukhni, Yasser Al-Sharo, S. Maksymova, V. Yevsieiev, V. Lyashenko // International Journal of Engineering Trends and Technology. – 2024. – V. 72(11). – P. 294-306.

41. Ababneh, J., Abu-Jassar, A., Abuowaida, S., Liubchenko, V., & Lyashenko, V. (2024, December). Evaluation of Three Different Operators for Object Highlighting in Medical RGB Images: Canny, Roberts, and LoG in Independent Color Spaces. In 2024 25th International Arab Conference on Information Technology (ACIT) (pp. 1-7). IEEE.
42. Kuzomin, O., Lyashenko, V., Tkachenko, M., Ahmad, M. A., & Kots, H. (2016). Preventing of technogenic risks in the functioning of an industrial enterprise. International Journal of Civil Engineering and Technology, 7(3), 262-270.
43. Serhiienko, O., Novikova, T., & Lyashenko, V. (2023). Comparative Analysis of the Dynamics of Futures for the Dow Jones, S&P 500 and Nasdaq. International Journal of Academic Accounting, Finance & Management Research (IJAAFMR), 7(9), 22-28.
44. Matarneh, R., Sotnik, S., Belova, N., & Lyashenko, V. (2018). Automated modeling of shaft leading elements in the rear axle gear. International Journal of Engineering and Technology (UAE), 7(3), 1468-1473.
45. Omarov, M., Tykha, T., & Lyashenko, V. (2019). Use of Wavelet Techniques in the Study of Internet Marketing Metrics. Eskişehir Technical University Journal of Science and Technology A-Applied Sciences and Engineering, 20, 157-163.
46. Makrakis, G. M., & et al. (2021). Vulnerabilities and attacks against industrial control systems and critical infrastructures. arXiv preprint arXiv:2109.03945.
47. García-Rodríguez, J., & et al. (2024). To pass or not to pass: Privacy-preserving physical access control. Computers & Security, 136, 103566.
48. Gupta, S., & et al. (2022). Step & turn—A novel bimodal behavioral biometric-based user verification scheme for physical access control. Computers & Security, 118, 102722.
49. Sutrala, A. K., & et al. (2021). Authenticated key agreement scheme with user anonymity and untraceability for 5G-enabled softwarized industrial cyber-physical systems. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2316-2330.
50. Ryu, J., & et al. (2022). Design of secure mutual authentication scheme for metaverse environments using blockchain. Ieee Access, 10, 98944-98958.
51. Yaacoub, J. P. A., & et al. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security, 21(1), 115-158.