

DEVELOPMENT OF AN AUTOMATED ACCESS CONTROL AND MANAGEMENT SYSTEM FOR ENHANCED SECURITY IN INDUSTRIAL FACILITIES

Horban Andrii

Kharkiv National University of Radio Electronics

Ukraine, 61166, Kharkiv, Nauky av., 14

E-mail: andrii.horban@nure.ua

Annotation: This paper presents the development and design of an automated access control and management system (AACMS) for industrial facilities. The structural diagram integrates key modules such as facial recognition and RFID-based identification, ensuring multi-factor authentication for enhanced security. The system includes a camera for biometric facial recognition, an RFID reader for card-based identification, and an electronic lock mechanism. A microprocessor module (MM) acts as the control unit, processing data from the RFID module and communicating with a laptop or single-board computer. The system operates by scanning both the user's face and RFID card, verifying the data, and providing access if both criteria are met. The integration of these two identification methods – biometric (facial recognition) and RFID – ensures a robust and secure access control process, improving the overall safety of the industrial facility.

Key words: automated access control, RFID Identification, Multi-Factor Authentication, Industrial Security.

Automated access control systems are an integral part of modern industrial enterprises, as they ensure security and efficient personnel management. One of the critical stages in the development of such systems is the design of the structural diagram, which provides a comprehensive understanding of the system's functioning, the interaction of its components, and the logical sequence of operations. This allows not only for process optimization but also for increasing the reliability and security of the system, ensuring its adaptability to potential future changes [1-2].

The design of the structural diagram for an automated access control system (AACS) is a crucial stage that ensures a comprehensive understanding of the system. The diagram identifies key elements such as sensors, controllers, and information processing systems. It helps to detect potential risks, optimize component interaction, and improve system reliability. Important criteria in the design process include contactless employee identification using computer vision and wireless technologies (RFID, NFC), which enhance system efficiency and security [3-4].

Based on the selected criteria that the AACS being developed for the industrial facility must meet, as well as the selected technologies presented in Table 1, the following structural diagram of the AACS for the industrial facility is proposed, as shown in Figure 1.

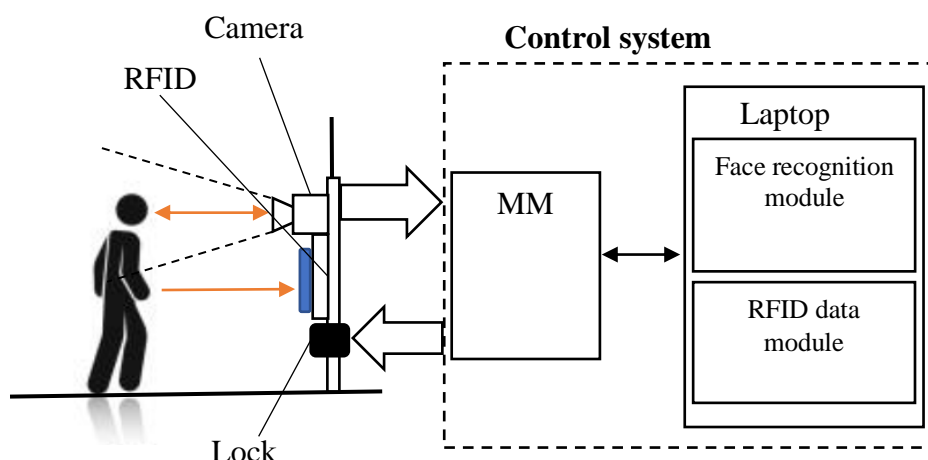


Figure 1 – Structural diagram of the layout of the automated system of access control and management in production

The structural diagram shown in Figure 1 illustrates a management system based on an automated access control and management system (AACMS), which integrates various modules for facial recognition and identification using RFID. Below is a description of the purpose of each component:

- Camera, responsible for capturing images or video of a person’s face for further analysis. It is used in the facial recognition module to identify the user based on biometric data.
- RFID, this module reads RFID cards or other identifiers. It contains a reader that interacts with an RFID chip embedded in a card or another 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 doors after successful user identification via the facial recognition or RFID modules.
- Microprocessor Module (MM, the system’s control unit, which processes data received from the RFID module. It reads user card data, decodes the information, and transfers it to a laptop. The MM also receives data from the laptop and controls whether the electronic lock should open or remain closed.
- Laptop, a device responsible for data processing and system management. It contains two primary software modules: the facial recognition module and the RFID data module.
- Facial Recognition Module, the system’s software component that analyzes data from the camera and determines whether the user’s facial image matches the pre-recorded biometric data. If the identification is successful, the data is transmitted to the control module to grant access.
- RFID Data Module, a software module that stores RFID code data, which grants access rights to the industrial premises.

CONCLUSIONS. Operation Principle of the AACMS Model for the Industrial Facility: the identified object approaches the access control point at the facility, the system scans the face and reads data from the RFID card, the data from the camera is directly transmitted to the laptop or single-board computer, while the RFID card data is decoded in the MM and sent via a USB port as a 16-digit code to the laptop or single-board computer, on the laptop or single-board computer, the facial recognition module analyzes the received facial image and checks it against the stored samples, while simultaneously verifying the 16-digit RFID card code. If both parameters match positively, the system sends a command via the MM to unlock the door. If one or both parameters do not match, the system does not unlock the door. The developed system combines two identification methods – biometric (facial recognition) and RFID – providing a multi-factor approach that enhances access security.

References:

1. Yevsieiev, V., Abu-Jassar, A., Maksymova, S., & Gurin, D. (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. Moiseev, M., Maksymova, S., Yevsieiev, V., & Alkhalailah, A. (2024). Program Algorithm for Monitoring System Development. *Journal of Universal Science Research*, 2(7), 33–43. Retrieved from <https://inlibrary.uz/index.php/universal-scientific-research/article/view/36023>.
3. Nevliudov, I. S., Yevsieiev, V. V., Maksymova, S. S., Omarov, A. O. M., & Klymenko, O. M. (2023). Conveyor Belt Object Identification: Mathematical, Algorithmic, and Software Support.
4. Nataliya, M., & Olexander, P. (2024). DEVELOPMENT OF A CYBERPHYSICAL SYSTEM FOR MONITORING FIRE SAFETY. *System technologies*, 1(150), 100-107.
5. Abu-Jassar, A. T., Attar, H., Amer, A., Lyashenko, V., Yevsieiev, V., & Solyman, A. (2024). 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*.
6. Yevsieiev, V., & Gurin, D. (2023). COMPARATIVE ANALYSIS OF THE BASIC METHODS USED IN INDUSTRY 4.0 AND INDUSTRY 5.0. *Collection of scientific papers «ΑΙΓΟΣ»*, (September 29, 2023; Bologna, Italy), 113-115.
7. Nevliudov, I., Yevsieiev, V., Maksymova, S., Demska, N., Starodubcev, N., & Klymenko, O. (2023, September). Monitoring System Development for Equipment Upgrade for IIoT. In *2023 IEEE 5th International Conference on Modern Electrical and Energy System (MEES)* (pp. 1-5). IEEE.