Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра комп'ютерно-інтегрованих технологій, автоматизації, робототехніки та безпекової інженерії

I Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт»

I All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations”

ICSTRO

2026

I All-Ukrainian Conference

February 12 - 13, 2026

Kharkiv

УДК: 005:004.896:62-65:338.3

Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт 2026: матеріали І-ої Всеукраїнська конференція, Харків, 12-13 лютого 2026 р.: тези доповідей / [редкол. І.Ш. Невлюдов (відповідальний редактор)].-Харків: [електронний друк], 2026. – 192 с.

У збірник включені тези доповідей, які присвячені сучасним тенденціям розвитку технологій та засобів моделювання, прогнозування та управління ризиками у сфері цивільної безпеки; техногенна та виробнича безпека: технічні засоби, оцінка ризиків, експертиза; інтелектуальні та робототехнічні системи аварійно-рятувальних робіт; кіберфізичні системи, інформаційна безпека та цифровий захист виробництв; інформаційно-комунікаційні технології в системах управління та моніторингу надзвичайних ситуацій; сталий розвиток, екологічна безпека та соціальна відповідальність у сфері цивільної безпеки; інтелектуальні системи прийняття рішень у сфері цивільного захисту.

Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations 2026: Proceedings of I st All-Ukrainian Conference, Kharkiv, February 12 - 13, 2026: Thesises of Reports / [Ed. I.Sh. Nevlyudov (chief editor).] .- Kharkiv .: [electronic version], 2026. - 192 p.

The collection includes the thesises of reports on devoted to current trends in the development of technologies and tools for modeling, forecasting, and risk management in the field of civil safety; industrial and technological safety, including technical means, risk assessment, and expert evaluation; intelligent and robotic systems for emergency and rescue operations; cyber-physical systems, information security, and digital protection of industrial facilities; information and communication technologies in emergency management and monitoring systems; sustainable development, environmental safety, and social responsibility in the field of civil safety; and intelligent decision-support systems in civil protection.

Харківський національний університет радіоелектроніки
Кременчуцький національний університет імені Михайла Остроградського
Національний університет «Запорізька політехніка»
Національний університет «Львівська політехніка»
Державне підприємство «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості»
Головне управління ДСНС України у Харківській області

Всеукраїнська конференція «Інтелектуальні технології цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт» (ICSTRO-2026)

All-Ukrainian Conference “Intelligent Civil Safety Technologies and Robotic Systems for Emergency and Rescue Operations” (ICSTRO-2026)

ЗМІСТ

SECURITY ANALYSIS OF PROTOCOLS FOR INTEGRATION WITH ACCESS CONTROL SYSTEM

R. Marunich, S. Sotnik
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: rostyslav.marunich@nure.ua

***Annotation*:** The paper examines key aspects of the security of protocols used for integration with access control systems. It analyzes current challenges and vulnerabilities related to data transmission in ACS, particularly comparing the Wiegand and OSDP protocols. The main information security threats are identified, and approaches to minimize them are proposed. Special attention is given to encryption, authentication, and two-way communication as critical elements of protection. The research results have practical value for the development and implementation of reliable and secure ACS.

***Key words*:** access control systems, protocol security, Wiegand, OSDP, cybersecurity.

АНАЛІЗ БЕЗПЕКИ ПРОТОКОЛІВ ДЛЯ ІНТЕГРАЦІЇ З СИСТЕМОЮ КОНТРОЛЮ ДОСТУПУ

Р. В. Маруніч, С. В. Сотник
Харківський національний університет радіоелектроніки
Україна, 61166, Харків, пр. Науки, 14
E-mail: rostyslav.marunich@nure.ua

Анотація: У роботі розглядаються ключові аспекти безпеки протоколів, що використовуються для інтеграції з системами контролю доступу. Проаналізовано сучасні виклики та вразливості, пов’язані з передачею даних у СКУД, зокрема порівняно протоколи Wiegand та OSDP. Визначено основні загрози інформаційній безпеці та запропоновано підходи до їх мінімізації. Особливу увагу приділено шифруванню, автентифікації та двосторонній комунікації як критичним елементам захисту. Результати дослідження мають практичну цінність для розробки та впровадження надійних та безпечних СКУД.

Ключові слова: системи контролю доступу, безпека протоколів, Wiegand, OSDP, кібербезпека.

Access control and management systems (ACMS) are a critical component of modern facility security today – from corporate offices and industrial enterprises to government institutions and critical infrastructure [1-4]. The widespread implementation of automation technologies, aimed at increasing efficiency and reducing human intervention, simultaneously expands the attack surface for potential cyberattacks and makes the issue of reliability of basic communication protocols even more urgent [5-11]. In the context of rapidly growing cyber threats and the increasing convergence of physical security systems with information technology, the issue of communication protocol security in ACMS becomes particularly acute. The historically dominant Wiegand protocol no longer meets modern cybersecurity requirements due to the complete lack of encryption, authentication, and mechanisms to protect against basic attacks such as interception, replay, and signal spoofing. This vulnerability creates serious risks for organizations, as compromise of an ACMS can lead not only to unauthorized physical access but also to the leakage of confidential information, sabotage of critical systems, and disruption of business continuity. The relevance of the research is further intensified by the need to integrate ACMS with broader building automation and industrial management ecosystems, which use protocols such as BACnet, Modbus, and KNX/EIB. These protocols, while effective for their primary tasks, often lack built-in security mechanisms, creating additional attack

vectors and turning integrated systems into potential entry points for malicious actors. The emergence of the modern Open Supervised Device Protocol (OSDP) with built-in AES-128 encryption, two-way communication, and authentication mechanisms demonstrates the evolution of industry standards in response to new security challenges. However, the process of migrating from obsolete solutions to modern standards requires a comprehensive analysis of the security characteristics of different protocols, an understanding of their vulnerabilities, and the development of practical recommendations for building secure integrated systems. Such research has direct practical value for security professionals, system integrators, and organizations seeking to ensure an adequate level of protection for their facilities in the conditions of the modern threat landscape.

The Wiegand protocol is historically one of the earliest and most widespread standards for communication between readers and controllers in access control systems. Its emergence dates back to the 1970s, and since then, it has gained widespread recognition due to its simplicity of implementation and relative reliability in an era when cybersecurity concerns were not as prominent. The operating principle of Wiegand is based on data transmission in the form of electrical pulses over two wires (Data 0 and Data 1), representing the binary code of the card identifier. This simplicity ensured its market dominance for many decades. However, with the development of technology and the growth of cyber threats, the main disadvantages of the Wiegand protocol have become critical. The chief among them is the complete absence of data encryption and authentication. This means all information, including the unique identifiers of access cards, is transmitted in an open, unprotected form. This approach makes the protocol extremely vulnerable to various attacks, such as Sniffing, where an attacker can easily connect to the Wiegand wires and intercept the transmitted data using simple equipment. A Replay Attack is also possible: after intercepting a card identifier, an attacker can replay this signal, imitating legitimate access, since the system cannot distinguish a genuine card from its copy due to the lack of authentication mechanisms. Furthermore, there is a risk of Spoofing, which involves creating duplicate cards or emulating a signal to gain unauthorized access. Moreover, Wiegand is a one-way protocol, meaning data is transmitted only from the reader to the controller. This limits opportunities for feedback, monitoring the reader's status, and detecting tampering attempts. The controller cannot verify the authenticity of the reader or obtain information about its malfunction or sabotage attempt. These fundamental flaws make Wiegand unsuitable for modern security requirements, especially at facilities with high protection standards. Unlike the outdated Wiegand, the OSDP was developed with modern cybersecurity and functionality requirements in mind. It is an open standard created by the Security Industry Association (SIA) and is actively being adopted as a new industry standard for communication between access control system components. A comparison of the Wiegand and OSDP protocol architectures is shown in Fig. 1.

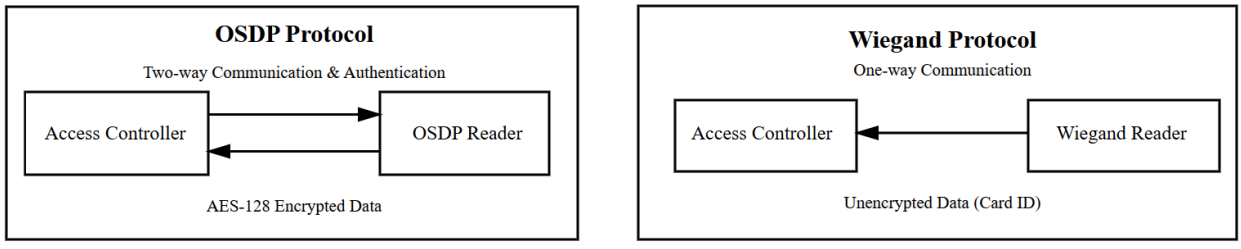

Figure 1 – Comparison of Wiegand and OSDP protocol architectures

The key advantages and security mechanisms of OSDP include bidirectional communication, which, unlike unidirectional Wiegand, enables data exchange between the reader and controller. This allows for transmitting identification data and receiving feedback on the reader's status, sabotage attempts, or errors. This opens up possibilities for more complex authentication scenarios and interactive experiences. OSDP also employs robust AES-128 encryption to protect all data

transmitted between devices, making interception and decryption of confidential information impossible. The protocol includes device authentication mechanisms, ensuring only authorized devices can connect, as well as data integrity control to protect against data tampering. OSDP is an extensible and flexible protocol, allowing for the integration of new technologies such as biometric readers and mobile identifiers. Thanks to these built-in security features, OSDP represents a significant step forward compared to Wiegand and is becoming the de facto standard for building secure and reliable access control systems, especially under heightened requirements for information and physical access protection.

In addition to specialized protocols for access control systems such as Wiegand and OSDP, the integration of access control systems with broader building automation and industrial control systems often involves the use of other protocols. These include BACnet, Modbus, and KNX/EIB, which, while effective for their primary tasks, have significant security gaps that can be exploited to compromise access control systems. BACnet (Building Automation and Control Networks) is widely used for building automation, including heating, ventilation, air conditioning (HVAC), lighting, and other engineering systems. However, BACnet often operates without built-in encryption and proper authentication. This creates serious risks: an attacker who gains access to the engineering systems network can easily intercept unencrypted data or, more dangerously, transmit unauthorized commands. For example, through BACnet, a command can be sent to the access control system to «open all doors», leading to a complete breach of the facility's security. To address these vulnerabilities, it is recommended to use BACnet/SC (Secure Connect), which provides built-in encryption and authentication, or to implement additional measures, such as virtual private networks (VPNs), to protect traffic. Modbus (Industrial Protocol) is one of the oldest and most common industrial protocols used for communication between electronic devices in industrial automation systems. Its main drawback is the complete lack of built-in security mechanisms. The Modbus protocol allows any device on the network to read and write data to controllers without any authentication or encryption. This means that an attacker who gains access to the industrial network can easily manipulate data or send commands to controllers that manage access control systems, which can lead to unauthorized access or disruption of critical systems. Protecting Modbus systems requires the use of external means, such as firewalls, network segmentation, and VPNs. KNX/EIB (Konnex/European Installation Bus) is used for the automation of residential and commercial buildings, controlling lighting, heating, blinds, and other functions. Older KNX/EIB implementations have weak cryptography, making them vulnerable to attacks. Although newer KNX Secure versions offer improved encryption and authentication mechanisms, a large number of already installed systems remain unprotected. Compromising KNX/EIB can allow an attacker to manipulate engineering systems, which could potentially affect the operation of integrated access control systems (ACS).

To minimize risks and ensure a high level of security for integrated ACS, the following recommendations must be followed. First, priority should always be given to OSDP for communication between readers and controllers. In cases where a full transition to OSDP is not possible, additional security measures for Wiegand systems must be implemented, such as physical protection of cabling runs and monitoring for anomalous activity. Second, it is critically important to ensure encryption and authentication at all levels of integration. For protocols that lack built-in security mechanisms (BACnet, Modbus), VPNs, TLS/SSL tunnels, or specialized secure protocol versions (BACnet/SC) should be used. Third, network segmentation is necessary to isolate ACS networks and engineering systems from corporate and external networks using firewalls and VLANs, which limits the spread of potential attacks. Fourth, regular software and firmware updates for all ACS components and integrated systems should be conducted to eliminate known vulnerabilities. Fifth, it is necessary to implement monitoring and auditing systems to detect suspicious activity, unauthorized access attempts, and anomalies in system operation. Finally, physical protection of controllers, readers, and cabling runs from unauthorized access and sabotage must be ensured.

Architecture of an integrated access control system with network infrastructure protection is shown in Fig. 2. The conducted analysis has shown that the security of protocols is a critically important aspect for the reliable operation of an ACS. Despite its widespread use, the Wiegand protocol has significant security flaws due to the lack of encryption and one-way communication, making it vulnerable to data interception and forgery. In contrast, OSDP offers a significantly higher level of protection thanks to AES-128 encryption, bidirectional communication, and authentication, making it the preferred choice for modern ACS. Building automation and industrial system protocols, such as BACnet, Modbus, and KNX/EIB, also have significant vulnerabilities that can be exploited to compromise an ACS.

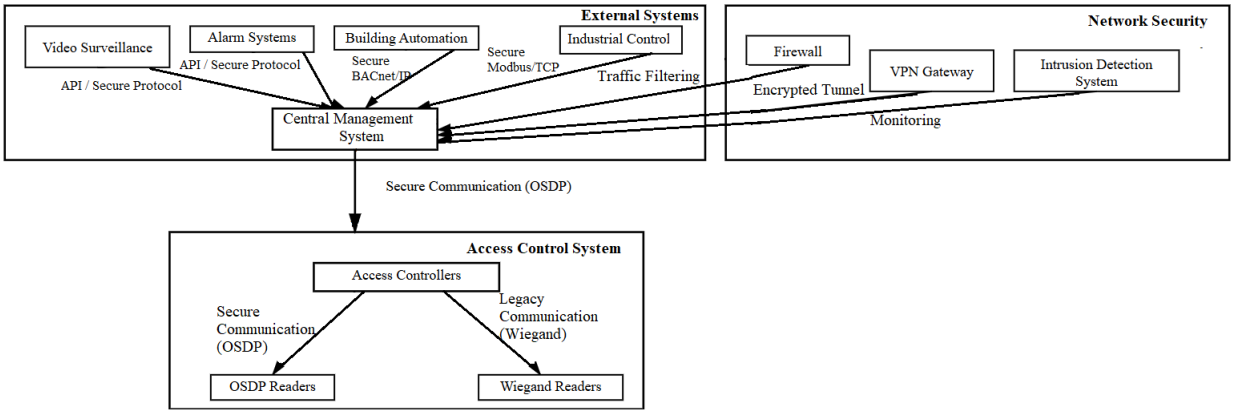

Figure 2 – Architecture of an integrated ACS with network infrastructure protection

To ensure comprehensive protection of integrated ACS, it is necessary to prioritize modern secure protocols like OSDP and implement additional security measures (encryption, authentication, network segmentation, regular updates, monitoring, and physical protection) for other integration protocols, which will minimize risks and enhance the overall system's resilience to cyber threats.

REFERENCES

1. Marunich, R. V. & et al.. Modern IoT technologies for creating automated access systems. Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports, 2025. – PP. 38-39

2. Tahseen, A.J.A. & et al.. Access control to robotic systems based on biometric: the generalized model and its practical implementation. International Journal of Intelligent Engineering & Systems, 2023. – PP. 313-328. Article ID ijies2023.1031.27, https://doi.org/10.22266/ijies2023.1031.27

3. Sotnik, S. Integration of IoT into security systems: opportunities and risks. International Journal of Academic Engineering Research (IJAER), 2024. – PP. 56-61

4. Sotnik S. V. Analysis of Personal Information Security Issues in Peacetime and Wartime. International Journal of Academic Engineering Research (IJAER), 2024. – PP. 108-113

5. Cherednichenko, T. & et al.. Features of automatic working time control systems. Manufacturing & Mechatronic Systems 2025: Proceedings of IX st International Conference, Kharkiv, October 25-26, 2025: Thesises of Reports, 2025. – PP. 54-57

6. Levenets, I. O. & et al. The role of artificial intelligence in optimizing information retrieval systems. Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025. – PP. 975-977

7. Khalimonov, Y. I. & et al.. Circular economy in automated systems. Sustainable smart cities and communities: business and innovation solutions 2025: Proceedings of I st I International Conference, Kharkiv, April 21, 2025: Thesises of Reports, 2025. – PP. 53-54

8. Danylenko, M. M. & et al.. Comparative analysis of modern SCADA packages for production automation. International Journal of Academic Engineering Research (IJAER), 2025. – PP. 26-34

9. Sotnik, S. V. Development of automated control system and registration of metal in continuous casting. Radio Electronics, Computer Science, Control, 2024. Article ID 1607-3274-2024-3-17, https://doi.org/10.15588/1607-3274-2024-3-17

10. Nevludov, I. Sh. & et al.. Application of artificial intelligence in additive manufacturing (3D printing). Information Technologies and Automation – 2025 / Proceedings of the XVIII International Scientific and Practical Conference. Odessa, October 30-31, 2025. – Odessa, ONUT Publishing House, 2025. – PP. 1006-1009

11. Danylenko, M. M. & et al.. Comparative analysis of modern SCADA packages for production automation. International Journal of Academic Engineering Research (IJAER), 2025. – PP. 26-34