DOI: 10.34185/1991-7848.2026.01.23
UDC 004.056:681.518:621.31:622.7

Shvets D.V., Kotov I.A., Karabut N.O.

CYBERSECURITY OF AUTOMATED INFORMATION SYSTEMS OF ELECTRIC POWER COMPLEXES IN THE MINING AND PROCESSING INDUSTRY

Abstract. *The implementation of digital manufacturing concepts and intelligent sensor networks in the mining and processing industry exponentially increases the risk of targeted cyberattacks on enterprises' electric power complexes, where interference with algorithms can cause technogenic disasters. To enhance the cyber resilience of automated information systems, a comprehensive architectural model based on the Defense-in-Depth concept has been developed. A multi-level infrastructure is proposed, featuring microsegmentation of industrial networks, Deep Packet Inspection for basic industrial protocols, hardening operating system configurations on engineering workstations, and the use of microkernel platforms for network gateways. It is demonstrated that combining international security standards with predictive hardware monitoring of programmable logic controller supply currents reliably prevents software-based control-logic spoofing, effectively mitigates intrusion vectors, and guarantees the continuity of energy-efficient control in raw-material processing operations.*

Keywords: *cybersecurity, mining and processing plant, automated information system, Defense-in-Depth, programmable logic controllers, electric power complex, IEC 62443.*

Problem Statement. The operation of mining and processing plants (MPPs) as fundamental links of critical infrastructure determines the stability of the raw material base for the metallurgical industry and the economic security of the state as a whole. The strategic importance of these enterprises dictates stringent reliability requirements for their electric power complexes, which supply power to the most energy-intensive production stages: grinding, classification, and magnetic separation of iron ore raw materials. Any interference with power supply control algorithms can cause not only massive economic losses due to equipment downtime

ISSN-print 1991-7848
ISSN-online 2707-9457

but also industrial accidents and technogenic disasters, such as the clogging of autogenous grinding mills or the disruption of tailings management facilities.

The current stage of the industry's development is characterized by a transition from isolated local systems to extensive automated information systems (AIS). The convergence of information technology (IT) and operational technology (OT) enables the optimization of specific power consumption per ton of concentrate; however, it also widens the range of potential cyber threats. The use of open data transmission protocols (Modbus TCP, IEC 60870-5-104, OPC UA) and the implementation of intelligent protection and monitoring devices make the digital infrastructure of power complexes vulnerable to targeted attacks aimed at manipulating telemetry data or directly intercepting the control of industrial controllers.

Despite the existence of general information security standards, the issue of protecting specific electric power nodes of MPPs, where technological and energy parameters are tightly interconnected, remains insufficiently researched. This highlights the need to develop comprehensive approaches to ensuring the cyber resilience of AIS that account for both the architectural features of industrial networks and the dynamics of transient processes in high-power electric drives of grinding equipment.

Analysis of Recent Research and Publications. When analyzing the primary threats and vulnerabilities, it is pertinent to begin with those targeting Supervisory Control and Data Acquisition (SCADA) systems. Historically, SCADA systems, which form the control foundation for automated electric power complexes, were designed as isolated segments (air-gapped networks), with priority given to the continuity of the technological process rather than protection against external intrusions. The convergence of IT and OT infrastructures, along with the transition to standardized protocol stacks, creates new critical attack vectors [1]. Based on the classification proposed in the cited work, it is advisable to examine threats to SCADA in the energy sector through the lens of the information security triad (CIA triad), taking into account industrial specifics:

1. Compromise of availability: implemented via DDoS attacks on data acquisition servers, intentional overloading of network equipment, or physical

damage to communication channels. In the energy sector, this results in the operator's loss of view of the technological process.

2. Compromise of integrity: telemetry data spoofing (false data injection), modification of protective relay settings, or unauthorized changes to the configuration of switching devices. The lack of cryptographic protection in fundamental industrial protocols leaves the system vulnerable to Man-in-the-Middle (MitM) attacks.

3. Compromise of confidentiality: interception of operational status information and power consumption scheduling data, which is most often a reconnaissance stage in preparation for more complex, targeted attacks.

Specific threats to the mining and processing industry are discussed in [2]. This research applies fuzzy logic methods and identifies three priority targets for cyberattacks at such enterprises: databases, internal communication networks, and the equipment itself. Typical attack scenarios have been identified for each level of process automation.

Of particular concern are the destructive impacts on the power-supply subsystems of energy-intensive units. A sudden power disconnection to the main electric drives of grinding mills or the shutdown of tailings pumping stations under load causes more than just a cycle interruption. Such incidents lead to the clogging of the equipment's working space, require lengthy scheduled unloading operations, and are accompanied by colossal inrush currents during the subsequent restart, which exponentially increases the risk of damage to the stator winding insulation and the failure of power transformers.

The security of industrial controllers represents a distinct challenge. The level of programmable logic controllers (PLCs), which directly control power circuits, has its own spectrum of vulnerabilities. The study [3] examines in detail the complex nature of threats associated with Control Logic Injection attacks, which can lead to the physical sabotage of production processes, specifically, equipment destruction due to intentional overloading. The authors emphasize that the most common infection vector for a closed OT perimeter is the compromise of engineering workstations (EWS) used by technical personnel via external media or vulnerable points of interaction with corporate networks.

ISSN-print 1991-7848
ISSN-online 2707-9457

Another critical risk factor for the architecture of modern PLCs is the possibility of unauthorized downloading of modified application software. Having gained access to an engineering station, an attacker can alter control algorithms (e.g., those written in IEC 61131-3 languages) so that the protective interlocks of electrical equipment are programmatically bypassed during emergency conditions. This allows the critical state to be concealed from operators, which will inevitably lead to equipment failure.

Regarding the regulatory framework, it should be noted that the international standard IEC 62443 is foundational for ensuring the cybersecurity of Industrial Automation and Control Systems (IACS). It defines Security Levels (SL) and requirements for various system components [4]. For MPP electric power complexes, implementing this standard entails: network segmentation and the creation of security zones; role-based access control (RBAC); secure remote access; and patch management.

Reference [5] describes the process of managing critical infrastructure cybersecurity using the integrated sectoral management system for national cybersecurity in Ukraine, based on the Law of Ukraine "On the Basic Principles of Ensuring the Cyber Security of Ukraine", which defines critical infrastructure facilities (to which MPPs belong) and the requirements for their protection. The study also indicates a growing level of cybercrime in Ukraine, underscoring the urgency of enhancing protection [6].

Presentation of the main research material. Enhancing the cyber resilience of MPP electric power complexes requires transitioning to an integrated architectural model. This model must account for the continuity of the technological processing cycle, the high cost of equipment failure, and the integration of edge computing and Industrial Internet of Things (IIoT) devices into the enterprise's multi-level power perimeter.

The proposed model is based on the Defense-in-Depth concept, adapted to the ISA-95 industrial hierarchy. Its architecture is illustrated in Figure 1 and structured across interdependent levels:

1. The corporate level and demilitarized zone (DMZ) (Levels 4 and 3.5) ensure the isolation of the industrial segment from external networks. Multi-factor authentication (MFA) is implemented here to minimize the risks of insider threats

(given the significant number of line personnel in the processing workshops), alongside the enforcement of end-to-end security policies and event auditing.

2. The network control and SCADA level (Level 3) is implemented through deep microsegmentation of the OT network using industrial Next-Generation Firewalls (NGFW) and Intrusion Detection/Prevention Systems (IDS/IPS). The latter are capable of performing Deep Packet Inspection (DPI) of specific fieldbuses (Profibus, Modbus/TCP, IEC 61850). This level also requires the configuration hardening [7] of general-purpose operating systems on EWS and integrity control of the control code, specifically algorithms implemented in IEC 61131-3 standard languages.

3. The controller level (Level 2) requires strict spatial isolation of PLCs and switching equipment, accompanied by video surveillance and physical access control systems.

4. The field level and IIoT segment (Levels 1 and 0) involves the use of a specialized embedded OS with a microkernel architecture for peripheral nodes, which prevents straightforward privilege escalation during cyberattacks.

ISSN-print 1991-7848
ISSN-online 2707-9457

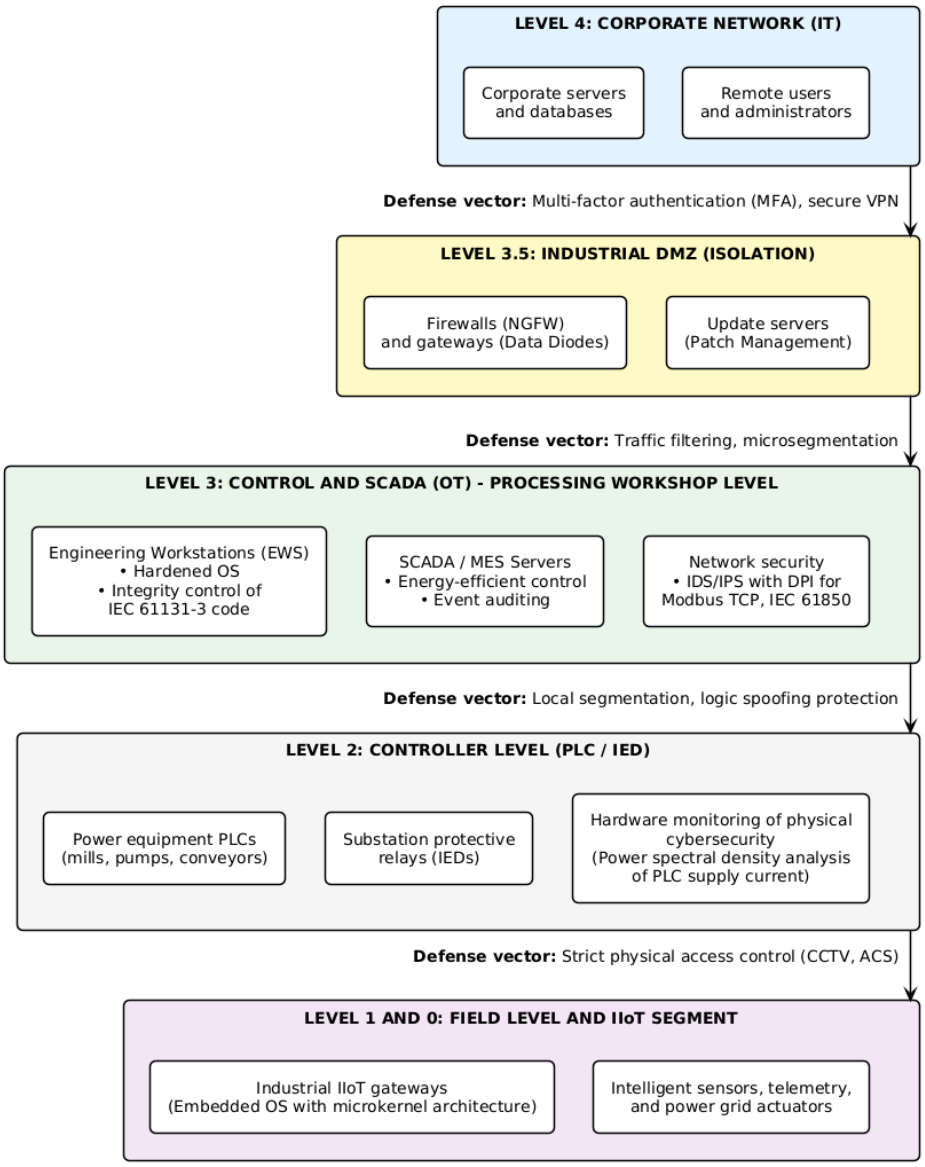

Figure 1 – Architecture of the defense-in-depth cybersecurity for the automated information system of the enterprise's electric power complex

To ensure fault tolerance at the lower (field and controller) levels of systems, it is advisable to implement physical cybersecurity monitoring. As noted in [8], analyzing PLC power signals enables the detection of operational anomalies before they affect the technological process. By evaluating the power spectral density of the consumed current, the system can identify the execution of unauthorized or malicious hardware-level software. Considering the catastrophic consequences of disrupting the energy-efficient control of energy-intensive units at technogenic facilities, this method serves as an essential predictive tool for MPPs.

Furthermore, the formulation of security policies for electric power complexes must rely on specialized risk assessment methodologies. An adapted method integrating the Kaplan-Garrick approach and fuzzy logic [2] enables the quantitative assessment of the probability of target node compromise based on the enterprise's degree of automation. The algorithm is structured in five stages:

1. Determination of the actual automation level of the technological chain (taking into account the deployment density of IIoT sensor networks).

2. Identification of priority attack targets (electrical substations, relay protection and automation systems, commercial and technical electricity metering complexes).

3. Profiling of potential intrusion execution techniques.

4. Modeling of consequences (ranging from database failures to the destruction of power equipment).

5. Calculation of the final risk coefficient for engineering decision-making.

The practical implementation of a reliable AIS for an MPP electric power complex requires implementing a comprehensive set of organizational and technical measures. A mandatory condition is the establishment of a strict vulnerability management protocol, specifically the timely updating of firmware for PLCs and Intelligent Electronic Devices (IEDs), as well as regular patch management for network services and core operating systems across all levels of the Industrial Control Systems (ICS), including industrial IIoT gateways.

For the secure integration of the industrial segment with external corporate networks, specialized security gateways or unidirectional data transfer systems (data diodes) must be used, along with secure VPN channels, to establish legitimate remote access for engineering personnel. Furthermore, hardware and software solutions must be supported by organizational measures: the development of highly specialized incident response plans coordinated with the shutdown/startup protocols of the processing equipment, and regular training of personnel in the fundamentals of cyber hygiene, as the human factor remains one of the key vectors for the compromise of control systems.

Conclusions. Ensuring the cyber resilience of AIS in electric power complexes is a multifaceted scientific and technical problem that requires comprehensive architectural solutions. The specific nature of iron ore processing dictates stringent

ISSN-print 1991-7848
ISSN-online 2707-9457

requirements for the continuity of the technological cycle, as a failure of power supply systems results in significant economic losses. Under these conditions, the convergence of traditionally isolated OT with corporate IT infrastructures, along with the implementation of IIoT components, exponentially expands the vulnerability landscape of energy-intensive equipment.

It has been demonstrated that the systematic enhancement of security levels must be based on integrating the IEC 62443 standard methodology and the Defense-in-Depth concept. Priority directions for engineering implementation include: deep microsegmentation of the network environment, continuous hardware monitoring of physical cybersecurity at the PLC level, integrity controls for embedded operating systems, and regular risk assessments tailored to the facility's actual level of automation. Adequate protection of the power complex serves as the foundation without which the secure implementation of energy-efficient control algorithms for ore preparation and separation processes is impossible.

For Ukrainian MPPs, which are classified as critical infrastructure facilities, additional requirements are imposed regarding the resilience of control systems. Given the permanent threat of targeted attacks on the energy sector, ICS's ability to withstand external destructive impacts is a determining factor in the economic survival of these enterprises.

The successful implementation of technical solutions is possible only if they are supplemented by organizational measures, primarily the systematic enhancement of cyber hygiene among engineering and technical personnel to mitigate the risks posed by insider threats. Prospects for further research in this direction lie in developing adaptive anomaly detection methods capable of distinguishing legitimate transient electromechanical processes in high-power drives from the consequences of targeted cyber incidents.

ЛІТЕРАТУРА/ REFERENCES

1. Nicholson A., Webber S., Dyer S., Patel T., Janicke H. SCADA security in the light of Cyber-Warfare. Computers & Security. 2012. Vol. 31, no. 4. P. 418–436. DOI: 10.1016/j.cose.2012.02.009
2. Tubis A.A., Werbińska-Wojciechowska S., Góralczyk M., Wróblewski A., Ziętek B. Cyber-Attacks Risk Analysis Method for Different Levels of Automation of Mining Processes in Mines Based on Fuzzy Theory Use. Sensors. 2020. Vol. 20, no. 24. P. 7210. DOI: 10.3390/s20247210

3. Alsabbagh W., Langendörfer P. A Flashback on Control Logic Injection Attacks against Programmable Logic Controllers. Automation. 2022. Vol. 3, no. 4. P. 596–621. DOI: 10.3390/automation3040030
4. Piggin R. S. H. Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security. IET Conference on Control and Automation 2013: Uniting Problems and Solutions, Birmingham, UK. 2013. DOI: 10.1049/cp.2013.0001
5. Slipachuk L., Toliupa S., Nakonechnyi V. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2–6 July 2019. DOI: 10.1109/aiact.2019.8847877
6. Mazepa S., Dostalek L., Sharmar O., Banakh S. Cybercrime and Vulnerability of Ukrainian Critical Information Infrastructure. 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 16–18 September 2020. DOI: 10.1109/acit49673.2020.9208965
7. Ilyenko A., Ilyenko S., Kulish T. Prospective protection methods of the Windows operating system. Cybersecurity: Education, Science, Technique. 2020. Vol. 4, no. 8. P. 124–134. DOI: 10.28925/2663-4023.2020.8.124134
8. Bichmou A., Chiocca J., Hernandez L., Hoffmann R.W., Horsham B., Lam H., McKinsey V., Bibyk S. Physical Cyber-Security of SCADA Systems. NAECON 2019 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 15–19 July 2019. DOI: 10.1109/naecon46414.2019.9057860

Received 12.03.2026.
Accepted 13.04.2026.
Published 30.04.2026

УДК 004.056:681.518:621.31:622.7

Швець Д.В., Котов І.А., Карабут Н.О.

КІБЕРБЕЗПЕКА АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ЕЛЕКТРОЕНЕРГЕТИЧНИХ КОМПЛЕКСІВ ПІДПРИЄМСТВ ГІРНИЧО-ЗБАГАЧУВАЛЬНОЇ ГАЛУЗІ

Анотація. *Впровадження концепцій цифрового виробництва та інтелектуальних сенсорних мереж у гірничо-збагачувальну галузь експоненційно підвищує ризики цілеспрямованих кібератак на електроенергетичні комплекси об'єктів критичної інфраструктури.*

Постановка проблеми. Електроенергетичні комплекси гірничо-збагачувальних комбінатів забезпечують живлення найбільш енергоємних стадій виробництва. В умовах конвергенції операційних та корпоративних мереж критично розширюється спектр вразливостей. Несанкціоноване втручання в алгоритми керування здатне спричинити як економічні збитки, так і масштабні техногенні аварії.

Мета дослідження полягає у розробці комплексної архітектурної моделі та інженерних рішень для підвищення кіберстійкості автоматизованих інформаційних систем електроенергетичних комплексів гірничо-збагачувальних комбінатів.

ISSN-print 1991-7848
ISSN-online 2707-9457

Методи дослідження. Застосовано методологію стандарту IEC 62443 та концепцію ешелонованого захисту, адаптовану до промислової ієрархії ISA-95.

Результати. Запропоновано багаторівневу інфраструктуру кіберзахисту автоматизованих інформаційних систем. Для мережевого рівня обґрунтовано впровадження мікросегментації технологічних мереж із застосуванням глибокої інспекції трафіку для базових промислових протоколів. Продемонстровано необхідність конфігураційного загартування операційних систем інженерних станцій та використання захищених мікроядерних платформ для мережевих шлюзів.

Висновки. Для забезпечення відмовостійкості на рівні контролерів імплементовано концепцію предиктивного моніторингу фізичної кібербезпеки. Показано, що поєднання вимог міжнародних стандартів безпеки із апаратним моніторингом струмів живлення програмованих логічних контролерів надійно запобігає програмній підміні керуючої логіки. Це ефективно нівелює вектори вторгнення та гарантує безперервність енергоефективного керування процесами переробки сировини.

Ключові слова: *кібербезпека, гірничо-збагачувальний комбінат, автоматизована інформаційна система, ешелонований захист, програмовані логічні контролери, електроенергетичний комплекс, IEC 62443.*

Швець Дмитро Валерійович - кандидат технічних наук, доцент, доцент кафедри моделювання та програмного забезпечення, Криворізький національний університет. ORCID: https://orcid.org/0000-0001-5126-6405

Котов Ігор Анатолійович - доктор технічних наук, доцент, професор кафедри моделювання та програмного забезпечення, Криворізький національний університет. ORCID: https://orcid.org/0000-0003-2445-6259

Карабут Надія Олександрівна - старший викладач кафедри моделювання та програмного забезпечення, Криворізький національний університет. ORCID: https://orcid.org/0000-0002-2327-4595

Shvets Dmytro Valeriyovych - Ph.D., Associate Professor of the Modeling and Software Department, Kryvyi Rih National University. ORCID: https://orcid.org/0000-0001-5126-6405

Kotov Ihor Anatoliyovych - Doctor of Sciences, Professor of the Modeling and Software Department, Kryvyi Rih National University. ORCID: https://orcid.org/0000-0003-2445-6259

Karabut Nadiya Oleksandrivna - Senior Lecturer, Modeling and Software Department, Kryvyi Rih National University. ORCID: https://orcid.org/0000-0002-2327-4595.