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)

INTELLIGENT CYBER-PHYSICAL MODULES FOR MONITORING DIGITAL PROTECTION OF PRODUCTION FACILITIES FOR USE IN EMERGENCY SITUATIONS

Olena Chala, Yevhenii Borodai
Kharkiv National University of Radio Electronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: olena.chala@nure.ua, yevhenii.borodai@nure.ua

***Annotation*:** This paper highlights the intermediate results of research related to the development, design, and implementation of intelligent cyber-physical monitoring modules for digital protection of production facilities for use in emergencies. This allows for data processing directly on devices (at the "edge" of the network) to minimize delays in critical situations. The use of Digital Twins will ensure continuous synchronization of a physical object with its digital model for simulating emergency response scenarios without risk to real production.

The research results provide insights into the initial aspects of designing and developing intelligent cyber-physical modules for monitoring digital protection in production for use in emergencies, which could be useful for researchers and developers in the fields of production automation, civil security, and emergency response robotics.

Key words: modules, intellectualization, digital twins, production, security, protection, emergency, enterprise, cyber-physical systems.

ІНТЕЛЕКТУАЛЬНІ КІБЕРФИЗИЧНІ МОДУЛІ МОНІТОРИНГУ ЦИФРОВОГО ЗАХИСТУ ВИРОБНИЦТВ ДЛЯ ЗАСТОСУВАННЯ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Олена Чала, Євгеній Бородай
Харківський національний університет радіоелектроніки,
Україна, 61166, Харків, пр. Науки 14
E-mail: olena.chala@nure.ua, yevhenii.borodai@nure.ua

Анотація: У цій роботі висвітлено проміжні результати досліджень, що стосуються розроблення, проєктування, та впровадження інтелектуальні кіберфизичні модулі моніторингу цифрового захисту виробництв для застосування у надзвичайних ситуаціях. Це дає можливість для обробки даних безпосередньо на пристроях (на «краю» мережі) для мінімізації затримок у критичних ситуаціях. Використання цифрових двійників забезпечить постійну синхронізацію фізичного об’єкта з його цифровою моделлю для симуляції сценаріїв ліквідації надзвичайних ситуацій без ризику для реального виробництва.

Результати дослідження дають уявлення про початкові аспекти проєктування та розробки інтелектуальних кіберфизичних модулів для моніторингу цифрового захисту виробництв для застосування у надзвичайних ситуаціях , що може бути корисним для дослідників і розробників у галузі автоматизації виробництва та цивільної безпеки та робототехнічні системи аварійно-рятувальних робіт

Ключові слова: модулі, інтелектуалізація, цифрові двійники, виробництво, безпека, захист, надзвичайна ситуація, підприємство, кіберфізичні системи.

In modern conditions of production digitalization, there is a need to create systems capable of ensuring reliable cybersecurity for production processes. This becomes particularly relevant in critical infrastructure sectors and manufacturing processes, both intermittent and continuous, where any intervention or delay at any stage can lead to technological accidents or a complete halt in the process.

To minimize or even eliminate non-standard emergency or dangerous situations, modules based on cyber-physical approaches and intelligentization can be used [1]. Such modules or modular systems

combine sensor technologies, data analytics, and artificial intelligence. They allow for the timely detection of cyberattacks, technical failures, and anomalous deviations in equipment operation.

Such systems are an integral part of production and civil safety in emergencies. Their task is not only to record violations but also to predict dangerous scenarios for the development of events.

As part of a deep analysis of the research we conducted, we have proposed and developed (with subsequent refinement) an approach that involves integrating cyber-physical modules into the operation of remotely controlled production lines.

The use of intelligent algorithms should ensure high adaptability of systems to new types of threats. Implementing such modules will enable an increase in the enterprise's level of digital resilience in unpredictable and emergency situations [2].

The developed solutions can be applied in the energy sector, mechanical engineering, chemical production, logistics processes, including warehouse operations and emergency services systems.

Speaking globally and broadly, cyber-physical systems are a complex of hardware and software that enables interaction between physical processes and digital solutions.

Using MEMS sensors to monitor vibration, temperature, pressure, and humidity. For example, Machine Learning-based models (Random Forest) achieve 95% accuracy in predicting equipment failures. Implementing intelligent intrusion detection systems (IDS) and adaptive AI algorithms to protect against unauthorized access and attacks on digital twins of manufacturing facilities.

The use of PWA applications and push notifications to inform personnel about being in a danger zone, integrated with mobile robotics [3-7].

The modules are capable of independently initiating protective measures (such as an emergency stop or network segment isolation) upon detecting a threat, without waiting for an operator command.

In the context of digital transformation in manufacturing, such systems are becoming the foundation for safe management of technological processes. However, the increasing number of connected devices increases the risks of cyber-attacks. Therefore, cybersecurity monitoring should be carried out in real-time using adaptive modules. That is exactly the module that is planned to be developed. The intelligent monitoring module will include its own set of sensors (adapted to a specific task or cycle of tasks), analytical blocks, and machine learning systems. Thanks to the use of a decentralized architecture, it will be able to operate autonomously if it loses contact with the control center. One of the key elements of the proposed module's architecture is the telemetry anomaly detection subsystem.

The module classifies deviations and determines the danger level using a neural network. In case of an emergency, the system automatically puts the equipment into safe mode. This working principle enhances not only cybersecurity but also technological safety.

An important aspect is the application of predictive analytics methods or, as an alternative, an information system for analyzing the performance indicators of sensors on technological lines. They allow you to predict failures based on historical data [4,7].

An example of implementation could be a pump station monitoring system using an IoT module and artificial intelligence.

Upon detecting unusual engine behavior, the system sends a message to the operational dispatcher. Modules can also integrate with digital twins of enterprises. This allows for the simulation and evaluation of various emergency scenarios. During the trial tests, our proposed system promptly detected a pressure sensor failure and prevented critical overheating.

Additionally, the module provided data transmission channel protection thru blockchain technology. This made it impossible to distort information or interfere from the outside.

An adaptive user interface was also developed for the monitoring system. It allows emergency services to quickly obtain up-to-date information about the state of production or its individual modules.

In emergencies, data from the module can be automatically transmitted to civil defense centers. Integration with unmanned robotic complexes that conduct remote inspections of territories is also provided. Such decisions create a unified digital response system. Increasing the autonomy of the modules opens up prospects for their use in hard-to-reach regions.

The distinctive feature of the proposed technology is the self-updating of artificial threat models. This allows for a reduction in false positives and an increase in the reliability of the assessments.

Thus, intelligent cyber-physical modules form the basis of a new digital security paradigm for manufacturing.

CONCLUSIONS The conducted studies confirmed the effectiveness of using intelligent cyber-physical monitoring modules. They ensure an increase in the level of digital and technological protection of production facilities.

Integrating modules into an enterprise management system helps with the early detection of threats. The developed algorithms ensure adaptability to new types of cyber-attacks.

In emergencies, the system operates automatically, minimizing the influence of the human factor.

The proposed approaches and solutions, after refinement, can be scaled for different types of enterprises and crisis conditions. The implementation of such modules will contribute to the development of digital resilience in Ukraine's critical infrastructure. Further research is planned to focus on improving communication protocols.

Another promising direction is integration with robotic systems for emergency response operations.

Therefore, the research, development, and implementation of intelligent cyber-physical monitoring modules represent an important step toward building a secure digital manufacturing future.

References:

1. DEVELOPMENT OF A MATHEMATICAL MODEL FOR SIMULATING A DECENTRALIZED CONTROL SYSTEM FOR COLLABORATIVE ROBOT NETWORKS. (2025). Multidisciplinary Journal of Science and Technology, 5(5), 1187-1202. https://mjstjournal.com/index.php/mjst/article/view/3640.

2. Vzhesnievskyi, M., & Chala, O. (2024). Автоматизація внутрішньо-складських виробничих логістичних процесів для впровадження концепції Industry 4.0: енергоощадливість, продуктивність, мобільність, модульність, автономність. Системи управління, навігації та зв'язку. Збірник наукових праць, 2(76), 34-38.

3. Давидов , Н., & Чала , О. (2025). ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИЗОВАНИХ СИСТЕМ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ. UNIVERSUM, (16), 62–66. Вилучено з https://archive.liga.science/index.php/universum/article/view/1567

4. Lighting Control Module Development / Y. Vizir, O. Chala, S. Maksymova, Ahmad Alkhalaileh // Journal of Universal Science Research. – 2023. – № 1(12). – P. 645–657.

5. Automation of Mathematical Modeling of Physical and Technological Processes in the Electronic Devices Manufacture / I. Nevliudov, O. Chala, I. Botsman, et al. // Functional Basis of Nanoelectronics : proceedings of the XII International Scientific Conference, Odessa, September 20-24, 2021. – Odessa, 2021. – P. 74-77.

6. Филипенко, О.І., Чала, О.О., Відешин, М.І. (2017). Технологічні дефекти виробництва кремнієвих підкладок для функціональних відбиваючих поверхонь МОЕМС-перемикачів. Системи управління, навігації та зв'язку, Полтава: ПНТУ, 2 (42), 61-63.

7. A METHOD DEVELOPMENT FOR MODELING THE TECHNOLOGICAL PROCESS OF PRINTED CIRCUIT BOARD PRODUCTION BASED ON THE Q-SCHEME. (2025). Multidisciplinary Journal of Science and Technology, 5(4), 9-21. https://mjstjournal.com/index.php/mjst/article/view/3036