International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 3 June 2026, hal., 411-424 e-ISSN: 3047-6151

CYBERSECURITY FRAMEWORK FOR AUTONOMOUS ENGINEERING SYSTEMS IN INDUSTRY 5.0

Syawal Aprian*[1]
Politeknik Amamapare Timika, Indonesia
Email: syawalapriano2@gmail.com

Adhe Ronny Julians
Politeknik Amamapare Timika, Indonesia
Email: adhe.ronnyj@gmail.com

Nursahar Buang
Politeknik Amamapare Timika, Indonesia
Email: adesalinfo@gmail.com

Abstract

The rapid adoption of autonomous engineering systems in the Industry 5.0 era has transformed industrial operations through the integration of artificial intelligence, the Internet of Things, cyber-physical systems, and advanced automation technologies. While these innovations enhance productivity, flexibility, and human–machine collaboration, they also introduce complex cybersecurity challenges that threaten system reliability, data integrity, operational continuity, and organizational resilience. This study aims to examine the development of cybersecurity frameworks for autonomous engineering systems within the context of Industry 5.0 through a literature review approach. The research method employs a systematic examination of scholarly articles, conference proceedings, industry reports, and relevant policy documents related to cybersecurity, autonomous systems, and Industry 5.0. The findings indicate that effective cybersecurity frameworks require a multidimensional approach encompassing risk assessment, zero-trust architecture, artificial intelligence-driven threat detection, secure communication protocols, continuous monitoring, and human-centered security governance. Furthermore, the integration of cybersecurity-by-design principles throughout the system lifecycle is essential for minimizing vulnerabilities and improving resilience against evolving cyber threats. The study concludes that a comprehensive cybersecurity framework is a critical prerequisite for ensuring the secure, reliable, and sustainable deployment of autonomous engineering systems in Industry 5.0 environments. The results contribute to the development of strategic guidelines for organizations, engineers, and policymakers seeking to

[1] Correspondence author

strengthen cybersecurity readiness in increasingly autonomous industrial ecosystems.
Keywords: Industry 5.0, Cybersecurity Framework, Autonomous Engineering Systems, Cyber-Physical Systems, Artificial Intelligence Security, Industrial Resilience

INTRODUCTION

The development of the industrial revolution has brought significant transformations in how organizations manage production processes, decision-making, and the integration of digital technology. Following the Industry 4.0 era, which emphasized automation, the Internet of Things (IoT), big data, and artificial intelligence, the concept of Industry 5.0 has emerged as a new paradigm focused on harmonious collaboration between humans and intelligent machines. Industry 5.0 not only pursues efficiency and productivity but also prioritizes sustainability, system resilience, and human well-being (Adewusi, 2025). In this context, autonomous engineering systems are a crucial component, enabling various engineering and manufacturing processes to run autonomously through sensing, learning, reasoning, and adaptive decision-making capabilities. These systems are capable of analyzing data in real time, optimizing operations automatically, and adapting to environmental changes without intensive human intervention.

The increasing use of autonomous engineering systems in the Industry 5.0 environment offers various strategic benefits for organizations. The integration of artificial intelligence, machine learning, intelligent robotics, and cyber-physical systems allows for increased operational efficiency, reduced human error, and accelerated production processes. In the manufacturing sector, autonomous systems are capable of dynamically managing production chains based on actual conditions in the field. In the energy sector, these systems can automatically optimize resource distribution and consumption. Meanwhile, in the transportation and logistics sector, autonomous technology supports faster and more accurate decision-making in distribution network management (Kour & Karim, 2026). However, the increasing level of system autonomy and connectivity also increases the complexity of cybersecurity risks faced by organizations.

Cybersecurity is becoming an increasingly crucial issue in the implementation of autonomous engineering systems because these systems rely on massive data exchange through interconnected digital networks. Extensive connectivity opens up opportunities for various cyber threats such as malware, ransomware, data breaches, denial-of-service attacks, spoofing, and

manipulation of artificial intelligence algorithms. Attacks on autonomous systems not only have the potential to cause financial losses but can also disrupt critical operations, damage critical infrastructure, and endanger human safety. In an Industry 5.0 environment that increasingly integrates humans and machines, cybersecurity failures can directly impact user trust, business continuity, and the stability of the industrial ecosystem as a whole (Hassan et al., 2024a).

Security challenges in autonomous engineering systems differ from those in conventional information systems (Anbalagan et al., 2023). Autonomous systems rely on algorithm-based decision-making processes that continuously learn from the data they receive. This creates new vulnerabilities, including adversarial attacks against artificial intelligence models, data poisoning, and exploiting weaknesses in communication between smart devices. Furthermore, the integration of various technologies such as cloud computing, edge computing, digital twins, and industrial IoT expands the attack surface that must be secured. This complexity demonstrates that traditional reactive security approaches are no longer adequate to protect autonomous systems operating in the dynamic and interconnected Industry 5.0 environment.

Various cybersecurity standards and frameworks have been developed to improve the protection of digital systems, but most still focus on general information technology systems and fail to fully consider the unique characteristics of autonomous engineering systems. The security approaches applied often emphasize technical aspects such as authentication, encryption, and access control, while aspects of adaptability, resilience, and automated response capabilities to threats have received insufficient attention. Yet, in an Industry 5.0 environment, security systems must be able to detect, analyze, and respond to threats in real time without disrupting human-machine collaboration (Fernández-Miguel et al., 2025). Therefore, the development of a more comprehensive cybersecurity framework tailored to the needs of modern autonomous systems is necessary.

A cybersecurity framework designed for autonomous engineering systems must integrate various security dimensions, from governance, risk management, data protection, network security, artificial intelligence security, to incident response and system resilience. The framework must support predictive capabilities in identifying potential threats before an attack occurs, while also providing rapid recovery mechanisms when security incidents occur. Furthermore, an effective framework must accommodate the human-centricity principle, the fundamental foundation of Industry 5.0, so that security is

oriented not only toward technological protection but also toward user safety, privacy, and trust (Santos et al., 2024).

The study of a cybersecurity framework for autonomous engineering systems is becoming increasingly relevant given the rapid adoption of autonomous technology across various industrial sectors. Organizations need clear guidelines to systematically and sustainably manage cybersecurity risks. Without a structured framework, the implementation of autonomous technology has the potential to face various obstacles, ranging from increased security vulnerabilities to decreased stakeholder trust in the systems used. Furthermore, the increasingly sophisticated development of cyberthreats demands a proactive and adaptive security approach to keep pace with the ever-changing dynamics of the digital environment.

Based on this description, research on a Cybersecurity Framework for Autonomous Engineering Systems in Industry 5.0 is crucial. This research aims to examine the concepts, challenges, and key elements required to develop an effective cybersecurity framework for autonomous engineering systems. Through a literature review approach, this research is expected to provide theoretical contributions in enriching the understanding of autonomous system security and provide conceptual recommendations for organizations and stakeholders in building a safe, resilient, and sustainable Industry 5.0 environment.

RESEARCH METHOD

This research uses a literature review method to identify, analyze, and synthesize various concepts, theories, models, and research findings related to the development of a cybersecurity framework for autonomous engineering systems in the context of Industry 5.0. This approach was chosen because it allows researchers to gain a comprehensive understanding of the cybersecurity challenges arising from the integration of artificial intelligence, the Internet of Things (IoT), cyber-physical systems, cloud computing, and autonomous technologies in modern industrial environments. Research data was obtained from various relevant scientific sources, including reputable international journal articles, conference proceedings, academic books, international organization reports, and policy documents published over the past ten years.

The selected literature was analyzed thematically to identify patterns, research gaps, and security approaches that have been implemented in automation-based industrial environments. The synthesis results were used to formulate a conceptual cybersecurity framework capable of supporting

confidentiality, integrity, availability, system resilience, and human trust in autonomous technology in the Industry 5.0 era. Through this approach, research is expected to provide theoretical and practical contributions in the development of adaptive, sustainable, and collaboration-oriented cybersecurity strategies between humans and intelligent machines.

RESULT AND DISCUSSION

Artificial Intelligence Integration in Autonomous Engineering Systems

The integration of Artificial Intelligence (AI) in Autonomous Engineering Systems has become a key driver of modern industrial transformation. Advances in digital technology, the Internet of Things (IoT), cloud computing, and data analytics enable engineering systems to operate autonomously with increasingly high levels of intelligence. Autonomous Engineering Systems refer to engineering systems capable of observing their environment, analyzing data in real time, making decisions automatically, and executing necessary actions without continuous human intervention (Kour et al., 2024). In this context, AI serves as the core of the system's cognitive capabilities, enabling learning, adaptation, and decision-making processes previously only possible by humans. The presence of AI not only improves operational efficiency but also expands the system's capabilities to cope with dynamic and complex environments.

The application of AI in Autonomous Engineering Systems is characterized by the use of various techniques such as machine learning, deep learning, computer vision, natural language processing, and reinforcement learning. Machine learning enables systems to recognize patterns in historical data and generate more accurate predictions to support decision-making. In smart manufacturing environments, for example, machine learning algorithms are used to predict equipment failures through the analysis of continuously collected sensor data (Torkjazi & Raz, 2024). This capability allows the system to take proactive maintenance actions before damage occurs, impacting productivity. Meanwhile, deep learning provides more complex capabilities for processing unstructured data such as images, videos, and sounds, enabling the system to recognize objects, detect anomalies, and understand environmental conditions more accurately.

AI integration also strengthens the ability of autonomous systems to make adaptive decisions. Conventional systems generally operate based on pre-programmed rules, thus having limitations in dealing with unexpected conditions. In contrast, AI-based systems are able to learn from experience and adjust their operational strategies based on environmental changes. This

adaptive capability is crucial in Industry 5.0, which demands high flexibility and collaboration between humans and machines (Torkjazi & Raz, 2026). In the manufacturing sector, AI-powered autonomous robots can adjust work paths, optimize resource utilization, and independently identify production bottlenecks. Thus, AI integration enables increased efficiency while enhancing system resilience to operational disruptions.

In addition to enhancing decision-making capabilities, AI also plays a crucial role in optimizing engineering processes. Autonomous Engineering Systems require the ability to simultaneously process large amounts of data from multiple sources. AI provides analytical mechanisms that enable the identification of hidden patterns and complex relationships within the data. Through predictive and prescriptive approaches, the system can determine the best course of action to achieve specific goals, taking into account various operational variables. In the energy sector, for example, AI is used to automatically manage energy distribution based on consumption patterns and network conditions. This approach not only improves energy efficiency but also supports sustainability by reducing resource waste (Nesterov, 2023).

AI's ability to support human-machine collaboration is also a crucial aspect of Autonomous Engineering Systems. Although the systems are designed to operate autonomously, human involvement is still required for strategic oversight and high-level decision-making. AI enables more intuitive interactions between humans and systems through intelligent interfaces that understand user needs. Within the concept of human-centric engineering, a key characteristic of Industry 5.0, AI acts as a supporting technology that enhances human productivity, rather than completely replacing it. With the ability to analyze quickly and accurately, humans can focus more on activities that require creativity, innovation, and ethical considerations (Mulge, 2024).

Despite offering numerous benefits, the integration of AI into Autonomous Engineering Systems also faces a number of challenges. One of the main challenges is data quality and security. The performance of AI algorithms is highly dependent on the availability of accurate, complete, and representative data. Poor quality data can lead to inappropriate decisions and potentially pose operational risks. Furthermore, increased system connectivity also opens up the possibility of cyberattacks that can disrupt automated decision-making processes. Therefore, the implementation of AI must be supported by robust cybersecurity mechanisms to protect the integrity of the data, algorithms, and digital infrastructure used.

Another challenge relates to the transparency and accountability of AI-generated decisions. Some AI models, particularly deep learning models, often operate as "black boxes," making it difficult to understand how they arrived at a decision. This can pose problems in engineering environments that require high levels of reliability and safety. Therefore, the development of Explainable Artificial Intelligence (XAI) is becoming increasingly important to ensure that system decisions are understandable, verifiable, and accountable. This transparency also plays a role in increasing user trust in autonomous systems used in various industrial sectors.

The Role of Cyber-Physical Systems (CPS) in Smart Industrial Environments

Cyber-Physical Systems (CPS) are the primary foundation for developing smart industrial environments, a key characteristic of the transformation towards Industry 4.0 and Industry 5.0. CPS integrate physical components with computing systems, communication networks, and real-time data analysis capabilities, enabling continuous interaction between the physical and digital worlds (Zhang et al., 2023). In modern industrial environments, CPS serve as a link between machines, sensors, actuators, software, and humans, creating more adaptive, responsive, and efficient production systems. Through this integration, manufacturing processes no longer rely solely on manual supervision but instead are able to automatically monitor, make decisions, and adjust operations based on actual conditions in the field.

The role of CPS in smart industry is evident in its ability to support continuous data collection through various sensors installed on machines and production equipment. The collected data is then sent via industrial communication networks to computing systems for analysis and interpretation. The results of this analysis are used to generate decisions that can be directly applied to the physical system through actuators or other control devices. This mechanism creates a feedback loop that enables production processes to run more dynamically and precisely (Mutua, 2024). With this capability, companies can quickly identify changes in operational conditions and take corrective action before disruptions develop into larger problems.

In addition to supporting automation, CPS also plays a crucial role in improving industrial operational efficiency. The integrated system allows simultaneous monitoring of various production parameters such as temperature, pressure, machine speed, energy consumption, and product quality. The information obtained can be used to optimize resource usage, thereby reducing waste of raw materials, energy, and production time. In the

context of modern manufacturing, efficiency is not only related to increased output but also includes the ability to minimize operational costs while maintaining high product quality. CPS enables companies to achieve these goals through data-driven decision-making that is more accurate than conventional approaches (Chen et al., 2020).

CPS also plays a significant role in the implementation of predictive maintenance. Through real-time monitoring of machine conditions, the system can detect early signs of failure based on vibration patterns, temperature, noise, or other technical parameters. This data is analyzed using artificial intelligence and machine learning algorithms to predict potential component failures before they occur. This approach helps companies reduce unplanned downtime and reduce maintenance costs, which are often one of the largest expenses in the manufacturing industry. Thus, CPS not only improves equipment reliability but also extends the operational life of industrial assets (Khan et al., 2021).

In a smart industrial environment, CPS supports the production flexibility increasingly needed to address changing market demand. Modern consumers tend to demand more personalized and diverse products, requiring companies to be able to adapt their production processes quickly. CPS enables automatic reconfiguration of production systems based on order data, product specifications, and ongoing operational conditions. This capability supports the concept of mass customization, namely large-scale production with a high degree of personalization. Through the integration of physical and digital systems, companies can increase adaptability without having to make major changes to their existing production infrastructure.

Another advantage of CPS is its ability to support real-time decision-making. In conventional industrial environments, operational decisions are often based on periodic reports that often have information delays. In contrast, CPS provides constantly updated data so managers and automated systems can respond quickly to changing conditions. The resulting decisions are more accurate because they are based on actual conditions on the ground. This is crucial in a competitive business environment, where responsiveness to change can be a determining factor in a company's success in maintaining productivity and service quality (Kayan et al., 2022).

The role of CPS is further expanding with its integration with other technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), cloud computing, and digital twins. This integration creates an interconnected industrial ecosystem capable of continuous optimization. IoT serves as a means

of inter-device connectivity, AI provides more advanced analytical and predictive capabilities, cloud computing provides large data storage and processing capacity, and digital twins enable the simulation of physical system conditions in a virtual environment. The combination of these technologies strengthens CPS's ability to create smarter, more efficient, and more innovation-oriented production processes.

Despite its numerous benefits, CPS implementation also faces a number of challenges, particularly related to cybersecurity, system interoperability, and the need for competent human resources. Because CPS connects various devices through digital networks, the risk of cyberattacks increases. System disruptions can directly impact physical operations and cause significant losses. Furthermore, integrating devices from different vendors often faces communication standard compatibility issues. Therefore, a comprehensive security strategy and the implementation of interoperability standards are required to ensure smooth data exchange between systems. Developing workforce competencies is also crucial for human resources to be able to manage and utilize CPS technology optimally.

Intrusion Detection System (IDS) Strategy in Industry 5.0 Environments

The development of Industry 5.0 presents a new paradigm that integrates collaboration between humans and intelligent machines in increasingly connected production environments. Unlike Industry 4.0, which focused on automation and digitalization, Industry 5.0 places humans at the center of innovation, supported by technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), cyber-physical systems (CPS), cloud computing, and edge computing. The integration of these various technologies creates a highly complex and dynamic industrial ecosystem, but also expands the surface of cyberattacks. High connectivity between devices, sensors, collaborative robots, and digital platforms increases the risk of unauthorized access, data manipulation, ransomware, and operational disruptions that can threaten human safety and the continuity of production processes. In this context, an Intrusion Detection System (IDS) is a key component of a cybersecurity strategy, enabling it to detect suspicious activity and potential attacks in real time (Javeed et al., 2024).

IDS implementation strategies in Industry 5.0 environments must consider the characteristics of modern industrial networks, which combine operational technology and information technology (Govindarajan et al., 2026). In traditional industrial systems, OT networks are typically siloed and have

limited connectivity. However, the transformation to Industry 5.0 has led to tighter integration between production systems and digital networks, allowing threats that previously targeted only IT systems to directly impact manufacturing processes. Therefore, IDSs must be designed to monitor data traffic across both environments in an integrated manner. This approach enables the identification of anomalies originating from industrial device communications, user access, and data exchange between digital platforms.

One widely implemented strategy is the simultaneous use of signature-based IDSs and anomaly detection. Signature-based IDSs work by comparing network activity against a database of known attack patterns. This method is effective in detecting documented threats and has a high degree of accuracy against common attacks (Babbar et al., 2025). However, Industry 5.0 environments face evolving threats, including zero-day attacks with previously unidentified patterns. To overcome these limitations, anomaly-based IDSs are used to identify behavior that deviates from normal system conditions. By studying industrial device communication patterns and daily operational activities, the system can detect indications of new attacks even when specific attack signatures are not yet available.

The use of artificial intelligence and machine learning is a crucial strategy for increasing the effectiveness of IDSs in Industry 5.0. Machine learning algorithms are capable of automatically analyzing massive volumes of data from sensors, IoT devices, and production systems. Through training using historical data, machine learning models can identify normal patterns and distinguish them from suspicious activity. This approach is particularly relevant in modern industrial environments that generate vast amounts of data at high speeds. In addition to improving threat detection capabilities, AI technology also helps reduce the false positive rate, a major challenge in conventional IDS implementations (Salam et al., 2023). This allows security teams to focus more on incidents that truly require a rapid response.

Another important strategy is the implementation of distributed IDSs deployed across multiple layers of industrial infrastructure. In the Industry 5.0 ecosystem, production devices are no longer centralized in a single location, but rather spread across a network that includes edge devices, cloud platforms, and intelligent manufacturing systems. A distributed IDS enables monitoring of activity at every critical network node, allowing for early detection of threats before they spread throughout the system. Each IDS sensor can collect local information and transmit the analysis to a security management center for

further correlation and evaluation. This approach improves security visibility while accelerating the incident identification process in complex environments.

In addition to technological aspects, an IDS strategy in Industry 5.0 must also be supported by the implementation of a risk-based security concept. Organizations need to identify critical assets that could significantly impact operations if disrupted. Based on the results of this risk analysis, IDS configuration can be adjusted to prioritize the required level of protection. Production systems that control critical processes, such as collaborative robots or automated control systems, require stricter oversight than assets with a lower risk level. A risk-based approach enables more effective allocation of security resources and enhances an organization's ability to respond to evolving threats (Hassan et al., 2024b).

Integrating IDS with Security Information and Event Management (SIEM) is also becoming an increasingly relevant strategy in Industry 5.0 environments. SIEM collects and analyzes logs from various sources, including IDSs, firewalls, endpoint security, and other network devices. Through this integration, organizations gain a more comprehensive picture of the overall security condition of the system. Correlating data from multiple sources enables more accurate threat detection and helps identify complex attack patterns (Wisdom et al., 2025). Furthermore, integration with automated response mechanisms allows for rapid mitigation when threats are detected, minimizing the impact on production processes.

The success of IDS implementation is also influenced by human resources. Industry 5.0 emphasizes collaboration between humans and technology, so operators, technicians, and security personnel must have a sufficient understanding of cyber threats and intrusion detection mechanisms. Continuous training programs are needed to improve their ability to interpret detection results, conduct incident investigations, and respond to threats effectively. High security awareness at all levels of the organization will strengthen the effectiveness of IDS technology and reduce the risks of human error and unintentional actions.

CONCLUSION

The development of Industry 5.0 has driven the integration of increasingly complex autonomous engineering systems through the use of artificial intelligence, the Internet of Things, cloud computing, and cyber-physical technologies. A literature review shows that increasing system autonomy not only provides benefits in terms of operational efficiency, decision-making

accuracy, and production flexibility, but also expands the cyberattack surface, potentially threatening the continuity of industrial processes. Therefore, implementing a comprehensive cybersecurity framework is a strategic necessity to ensure the security, reliability, and resilience of autonomous systems in an Industry 5.0 environment. An effective cybersecurity framework must encompass critical asset identification, risk management, data protection, real-time threat detection, structured incident response, and recovery mechanisms capable of maintaining operational continuity.

This study also confirms that the successful implementation of a cybersecurity framework depends not only on technological aspects, but also on organizational governance, security policies, human resource competency, and collaboration between stakeholders. An adaptive and sustainable security approach is necessary to address the ever-evolving dynamics of cyberthreats as autonomous engineering systems become more intelligent and connected. By integrating security principles from design to system operation, organizations can increase trust in autonomous technologies while supporting a safe, resilient, and human-centric Industry 5.0 ecosystem. The findings of this study are expected to serve as a conceptual reference for the development of policies, standards, and further research related to cybersecurity in autonomous engineering systems in the future.

REFERENCES

Adewusi, M. A. (2025). A Design-Science, Conceptual Framework paper proposing a Zero-Trust Security Architecture and Implementation roadmap for AI-enabled Cybersecurity in University-Industry Digital Ecosystems within the Industry 5.0 era (SSRN Scholarly Paper No. 5837705). Social Science Research Network. https://doi.org/10.2139/ssrn.5837705

Anbalagan, S., Raja, G., Gurumoorthy, S., Suresh R, D., & Ayyakannu, K. (2023). Blockchain Assisted Hybrid Intrusion Detection System in Autonomous Vehicles for Industry 5.0. IEEE Transactions on Consumer Electronics, 69(4), 881–889. https://doi.org/10.1109/TCE.2023.3320282

Babbar, H., Rani, S., & Boulila, W. (2025). Fortifying the Connection: Cybersecurity Tactics for WSN-Driven Smart Manufacturing in the Era of Industry 5.0. IEEE Open Journal of the Communications Society, 6, 3417–3428. https://doi.org/10.1109/OJCOMS.2024.3428531

Chen, G., Wang, P., Feng, B., Li, Y., & Liu, D. (2020). The framework design of smart factory in discrete manufacturing industry based on cyber-physical system. International Journal of Computer Integrated

Manufacturing, 33(1), 79–101. https://doi.org/10.1080/0951192X.2019.1699254

Fernández-Miguel, A., Ortíz-Marcos, S., Jiménez-Calzado, M., Fernández del Hoyo, A. P., García-Muiña, F. E., & Settembre-Blundo, D. (2025). From Resilience to Cognitive Adaptivity: Redefining Human–AI Cybersecurity for Hard-to-Abate Industries in the Industry 5.0–6.0 Transition. Information, 16(10), 881. https://doi.org/10.3390/info16100881

Govindarajan, V., Ahmed, F., Faheem, Z. B., Bilal, M., Ayadi, M., & Ali, J. (2026). Aegis-5: A Hybrid Ensemble Framework for Intrusion Detection in Industry 5.0 Driven Smart Manufacturing Environment. ACM Transactions on Autonomous and Adaptive Systems. https://doi.org/10.1145/3787224

Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., & Nagro, S. A. (2024a). Systematic Analysis of Risks in Industry 5.0 Architecture. Applied Sciences, 14(4), 1466. https://doi.org/10.3390/app14041466

Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., & Nagro, S. A. (2024b). Systematic Analysis of Risks in Industry 5.0 Architecture. Applied Sciences, 14(4), 1466. https://doi.org/10.3390/app14041466

Javeed, D., Gao, T., Kumar, P., & Jolfaei, A. (2024). An Explainable and Resilient Intrusion Detection System for Industry 5.0. IEEE Transactions on Consumer Electronics, 70(1), 1342–1350. https://doi.org/10.1109/TCE.2023.3283704

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A Review. ACM Computing Surveys (CSUR), 54(11s), 229:1-229:35. https://doi.org/10.1145/3510410

Khan, F., Kumar, R. L., Kadry, S., Nam, Y., & Meqdad, M. N. (2021). Cyber physical systems: A smart city perspective. International Journal of Electrical and Computer Engineering (IJECE), 11(4), 3609. https://doi.org/10.11591/ijece.v11i4.pp3609-3616

Kour, R., & Karim, R. (2026). Cybersecurity framework for Operator 5.0. Organizational Cybersecurity Journal: Practice, Process & People, 1–13. https://doi.org/10.1108/OCJ-02-2025-0007

Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: Trends and gaps. Frontiers in Computer Science, 6. https://doi.org/10.3389/fcomp.2024.1434436

Mulge, P. (2024). Integration of Automation and Artificial Intelligence in Mechanical Engineering. Journal of Computer Science & Emerging Trends, 1(1), 59–62. https://journals.sharnbasvauniversity.org/index.php/cseat/article/view/9

Mutua, E. (2024). Cyber-Physical Systems and Their Role in Industry 4.0. Journal of Technology and Systems, 6(5), 57–69. https://doi.org/10.47941/jts.2149

Nesterov, V. (2023). Integration of artificial intelligence technologies in data engineering: Challenges and prospects in the modern information environment. Вісник Черкаського Державного Технологічного Університету. Технічні Науки, 28(4), 82–90. https://doi.org/10.62660/2306-4412.4.2023.82-90

Salam, A., Ullah, F., Amin, F., & Abrar, M. (2023). Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. Technologies, 11(4), 107. https://doi.org/10.3390/technologies11040107

Santos, B., Costa, R. L. C., & Santos, L. (2024). Cybersecurity in Industry 5.0: Open Challenges and Future Directions. 2024 21st Annual International Conference on Privacy, Security and Trust (PST), 1–6. https://doi.org/10.1109/PST62714.2024.10788065

Torkjazi, M., & Raz, A. K. (2024). A Review on Integrating Autonomy Into System of Systems: Challenges and Research Directions. IEEE Open Journal of Systems Engineering, 2, 157–178. https://doi.org/10.1109/OJSE.2024.3456037

Torkjazi, M., & Raz, A. K. (2026). A Systems Engineering Methodology for System of Autonomous Systems: Architecture and Integration. Systems Engineering, 29(2), 169–194. https://doi.org/10.1002/sys.70025

Wisdom, D. D., Vincent, O. R., Igulu, K. T., Aborisade, D. O., Christian, A. U., Hyacinth, E. A., Baba, G. A., Esther, O. O., & Olatunbosun, A. M. (2025). The Protection of Industry 4.0 and 5.0: Cybersecurity Strategies and Innovations. In Computational Intelligence for Analysis of Trends in Industry 4.0 and 5.0. Auerbach Publications.

Zhang, K., Shi, Y., Karnouskos, S., Sauter, T., Fang, H., & Colombo, A. W. (2023). Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives. IEEE Transactions on Industrial Informatics, 19(1), 716–729. https://doi.org/10.1109/TII.2022.3199481