

# **CYBERSECURITY CHALLENGES IN INDUSTRY 5.0: HUMAN-CENTRIC SECURITY, CONVERGED VULNERABILITIES, AND RESILIENCE-BY-DESIGN IN SMART MANUFACTURING**

*Plamen Stanchev (1), Denitsa Ivanova-Mutafchieva (1), Nikolay Hinov\* (2)*

<sup>(1)</sup> Department of Intelligent Technology in Industry, Technical University of Sofia;

<sup>(2)</sup> Department of Computer Systems, Technical University of Sofia  
Bulgaria

\* Corresponding Author, e-mail: hinov@tu-sofia.bg

**Abstract:** Industry 5.0 redefines industrial transformation by complementing automation and connectivity with human-centricity, sustainability, and resilience. The increasing integration of artificial intelligence, industrial Internet of Things, collaborative robotics, cyber-physical systems, and cloud-edge infrastructures enhances manufacturing adaptability, but simultaneously enlarges the cyber-attack surface of industrial environments. Unlike conventional industrial settings, cyber incidents in Industry 5.0 may compromise not only data and control functions, but also operator safety, process integrity, and production continuity. This paper analyzes the cybersecurity challenges of Industry 5.0 through three complementary dimensions: human-centric security requirements, vulnerabilities arising from IT/OT/IoT/AI convergence, and resilience-by-design protection strategies. The study provides a structured perspective for developing secure, trustworthy, and resilient smart manufacturing ecosystems.

**Key words:** Industry 5.0; cybersecurity; human-centric manufacturing; IT/OT convergence; industrial Internet of Things; cyber resilience.

## **1. INTRODUCTION**

Industry 5.0 has emerged as a new stage in industrial development that extends the technology-driven orientation of Industry 4.0 by explicitly incorporating human-centricity, sustainability, and resilience as core design principles. In the European Commission's framework, Industry 5.0 is not limited to productivity enhancement through automation, but is positioned as a broader industrial vision in which technological progress must support worker well-being, societal value, and environmentally responsible production. This conceptual shift is especially important for manufacturing environments where intelligent systems increasingly operate in close interaction with human operators and critical physical processes [1, 2].

The transition toward Industry 5.0 is enabled by the growing deployment of artificial intelligence (AI), industrial Internet of Things (IIoT), collaborative robots, cyber-physical systems (CPS), digital twins, and cloud-edge computing infrastructures. These technologies improve adaptability, productivity, decision support, and operational visibility across modern production systems. At the same time, their integration significantly expands the cyber-attack surface of industrial environments by increasing connectivity, interdependence, and data exchange between heterogeneous components. As a result, cybersecurity in Industry 5.0 must address not only confidentiality and data protection, but also process integrity, system availability, operational continuity, and worker safety [3, 4].

Unlike conventional industrial settings, Industry 5.0 relies on tightly coupled interactions among IT, OT, IoT, and AI-driven decision layers. This convergence introduces new classes of vulnerabilities associated with insecure interfaces, weak identity control, lateral movement across interconnected assets, manipulation of sensor and process data, and compromise of intelligent control functions. Recent ENISA threat landscape reporting continues to identify ransomware, supply-chain compromise, and increasingly complex cross-system threat scenarios as major cybersecurity concerns, reinforcing the need for stronger protection models in digitally intensive industrial ecosystems [5, 6].

A further distinguishing characteristic of Industry 5.0 is the central role of human-machine collaboration. In such environments, cybersecurity must protect more than networked infrastructure; it must also preserve trust in intelligent systems, ensure safe cooperation between operators and autonomous devices, and reduce the risk of cyber incidents that may propagate into physical hazards or unsafe decisions. Therefore, the cybersecurity problem in Industry 5.0 is inherently multidimensional, combining technical, organizational, and human factors. This makes traditional perimeter-based and device-isolated security approaches increasingly insufficient for next-generation smart manufacturing [7].

To address these challenges, modern industrial protection strategies increasingly require security-by-design and cyber-resilience-by-design principles. In this context, zero trust has gained importance as a relevant architectural model because it shifts protection away from implicit trust based on network location and toward continuous verification of identities, assets, and access decisions. NIST defines zero trust architecture as an enterprise cybersecurity approach designed to prevent data breaches and limit internal lateral movement, making it particularly suitable for highly interconnected industrial environments with distributed assets and dynamic trust boundaries [8, 9].

Motivated by these developments, this paper examines the cybersecurity challenges of Industry 5.0 through three complementary perspectives: human-centric security requirements, vulnerabilities caused by IT/OT/IoT/AI convergence, and resilience-by-design protection strategies. The paper aims to provide a structured analytical view of the threat landscape and to outline a conceptual foundation for secure, trustworthy, and resilient smart manufacturing ecosystems [10, 11].

## **2. HUMAN-CENTRIC CYBERSECURITY IN INDUSTRY 5.0**

Human-centricity is one of the core pillars of Industry 5.0 and distinguishes it from earlier industrial paradigms focused mainly on automation, efficiency, and connectivity. In this context, cybersecurity should not be understood only as the protection of data, devices, and industrial networks, but also as a means of safeguarding human trust, safe interaction, and reliable decision support in digitally intensive manufacturing environments [12, 13].

This perspective broadens the traditional security objectives of industrial systems. While confidentiality, integrity, and availability remain essential, Industry 5.0 also requires attention to operator safety, transparency of machine behavior, cognitive reliability, and the resilience of human-machine collaboration. This is particularly important in environments where workers interact with collaborative robots, adaptive control systems, wearable devices, AI-assisted tools, and cyber-physical production systems. In such settings, cyber incidents may affect not only digital assets, but also machine behavior, operator decisions, and confidence in automated support systems [14].

A major challenge is the growing dependence on AI-enabled decision support and semi-autonomous industrial functions. In Industry 5.0, operators are increasingly expected to supervise and cooperate with intelligent systems rather than simply follow predefined procedures [15]. Therefore, trustworthy AI becomes a cybersecurity-relevant requirement. Characteristics such as reliability, safety, security, transparency, explainability, and interpretability are especially important when AI supports diagnostics, scheduling, maintenance, quality control, or human-robot interaction [16].

From a human-centric cybersecurity perspective, explainability and transparency are critical because operators must be able to understand and verify intelligent system behavior. If AI-assisted recommendations cannot be interpreted or validated, even technically correct outputs may become operationally unsafe. For this reason, cybersecurity in Industry 5.0 should support not only system protection, but also usable situational awareness, interpretable automation, and predictable operation under adverse conditions [17, 18].

Figure 1 summarizes the main human-centric cybersecurity challenge areas in Industry 5.0. It places the human operator at the center and highlights key domains such as human-robot collaboration safety, trust in AI recommendations, explainability and transparency, training and awareness, privacy and identity protection, access control, interface manipulation, and decision reliability under cyber attack. The figure also shows that these challenges are shaped by human, technical, and organizational factors.

Another important issue is the propagation of cyber threats through human-machine interfaces and collaborative workflows. Manipulated data, unauthorized access, altered digital instructions, and compromised AI-assisted monitoring may distort human perception and decision-making. In addition, effective protection depends on workforce preparedness. Secure industrial transformation cannot rely only on technical measures if operators are not trained to recognize anomalies, validate machine outputs, and respond appropriately to cyber-physical disruptions.

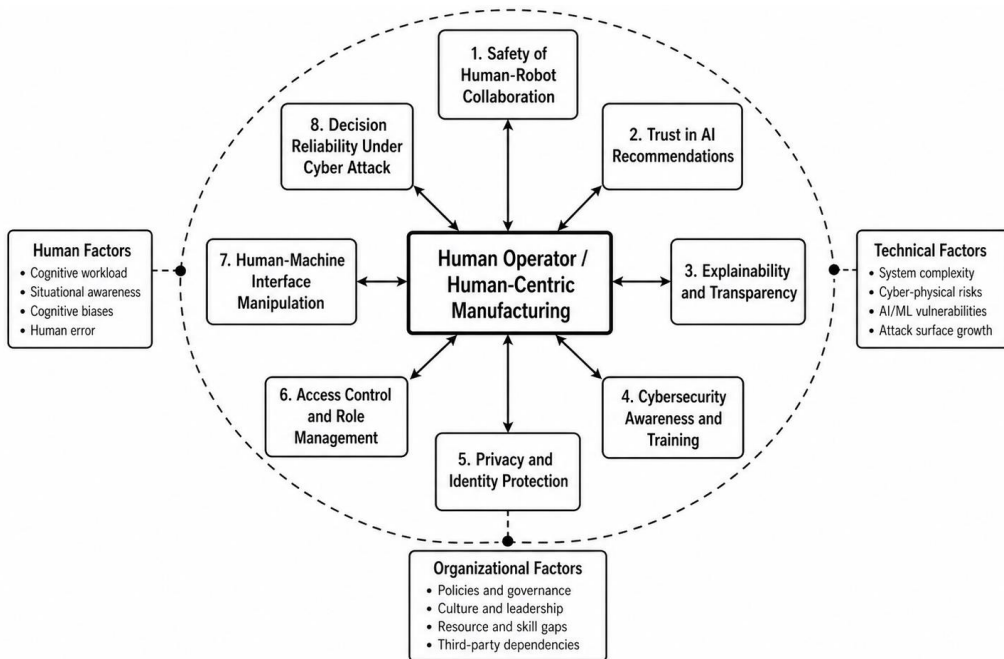


Figure 1. Main human-centric cybersecurity challenge areas in Industry 5.0

Therefore, human-centric cybersecurity in Industry 5.0 should be understood as a security paradigm that extends beyond infrastructure protection toward safe, trustworthy, and resilient cooperation between humans and intelligent industrial systems. This broader perspective is essential because the success of Industry 5.0 depends not only on connectivity and automation, but also on keeping digital transformation understandable, controllable, and safe for human operators.

### 3. CYBERSECURITY CHALLENGES IN IT/OT/IoT/AI CONVERGED INDUSTRIAL ENVIRONMENTS

One of the main cybersecurity challenges in Industry 5.0 arises from the convergence of information technology, operational technology, industrial IoT, and AI-enabled decision systems. Although this convergence improves connectivity, visibility, and adaptive control, it also creates a highly interconnected attack surface in which vulnerabilities can rapidly propagate across digital and physical layers. Unlike traditional industrial architectures, where operational systems were relatively isolated, Industry 5.0 environments rely on continuous interaction among enterprise platforms, production assets, intelligent devices, cloud-edge services, and human-machine interfaces. This increases exposure to cyber threats and complicates the protection of manufacturing infrastructures.

A major difficulty in these environments is the blurring of boundaries between IT and OT. Historically, these domains were developed with different priorities: IT emphasizes confidentiality and interoperability, while OT focuses on availability, safety, and deterministic operation. Once tightly integrated, weaknesses in enterprise systems,

such as compromised credentials, phishing-enabled access, vulnerable remote services, or unpatched software, may become entry points toward operational assets that directly influence physical processes. Consequently, what begins as an information security incident may escalate into a cyber-physical disruption affecting safety and production continuity.

Figure 2 illustrates the propagation of threats across converged IT, OT, IoT/edge, and AI/data layers in Industry 5.0. It shows how external threats, including phishing, ransomware, insider activity, supply-chain compromise, and adversarial AI, may spread from enterprise-facing components toward operational and intelligent manufacturing layers. The figure also highlights that cyber incidents in Industry 5.0 rarely remain isolated, but may cascade across interconnected domains and lead to process disruption, data manipulation, safety risks, loss of trust, and production downtime.

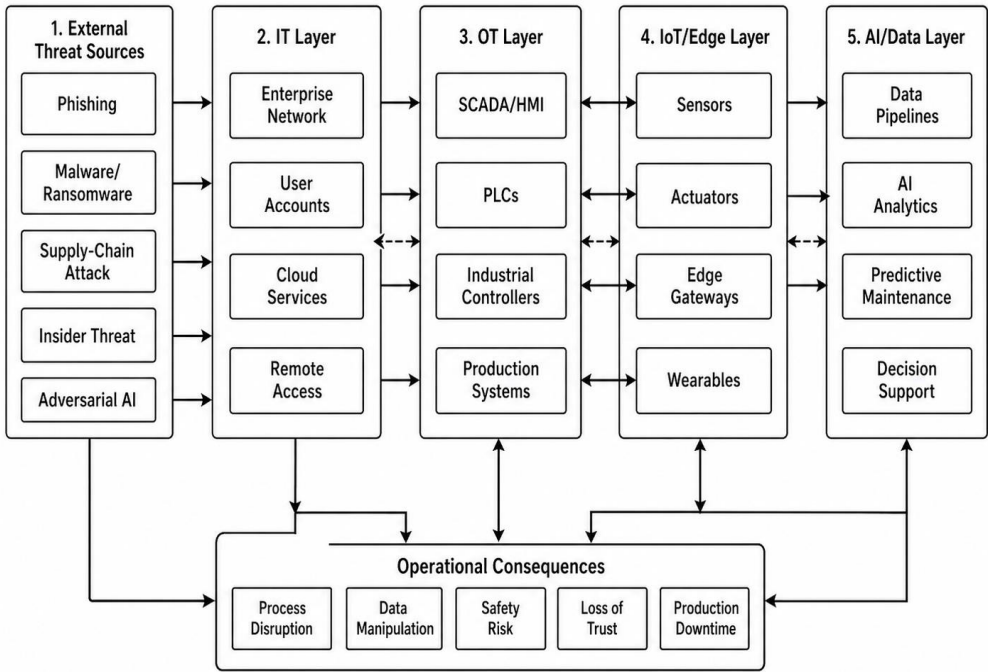


Figure 2. Cybersecurity threat propagation across converged IT/OT/IoT/AI layers in Industry 5.0 environments.

The proliferation of IIoT devices adds further vulnerabilities. Sensors, actuators, gateways, and embedded monitoring devices often operate with constrained resources, heterogeneous firmware, and uneven security controls. Weak authentication, insecure configurations, limited encryption, and poor update mechanisms can make such devices attractive entry points for unauthorized access, data manipulation, and service disruption. Because Industry 5.0 depends on distributed intelligence and fine-grained situational awareness, compromised IIoT components can undermine both operational visibility and automated decision support.

Another challenge is the growing use of AI within industrial decision loops. AI-based modules are increasingly employed for anomaly detection, predictive maintenance, scheduling, quality control, and operator support. However, they also introduce risks related to data poisoning, adversarial manipulation, compromised inference pipelines, and model integrity. In industrial contexts, AI should therefore be regarded not merely as an analytical tool, but as an operationally significant component whose compromise may distort machine behavior, maintenance priorities, alarm handling, or operator decisions.

Cloud-edge integration further expands the security problem by introducing additional trust boundaries, exposed interfaces, and third-party dependencies. In modern Industry 5.0 systems, data are often collected and processed at the edge, then synchronized with cloud platforms for analytics, orchestration, and digital twin services. While this improves scalability and responsiveness, it also increases dependence on external software, vendors, APIs, and connected service ecosystems. As a result, supply-chain compromise and inherited vulnerabilities become especially relevant.

A further concern is lateral movement across interconnected assets once an attacker gains an initial foothold. Weak segmentation, shared credentials, insecure remote access, and implicit trust relationships may allow attackers to move from enterprise or edge systems toward high-value operational assets. In Industry 5.0, this is especially dangerous because interdependence between digital and physical functions allows local compromise to produce system-wide consequences.

Finally, the protection of converged industrial environments is complicated by organizational and lifecycle factors. Industry 5.0 systems often combine legacy equipment with newer digital services, resulting in uneven security maturity. Long asset lifetimes, patching constraints, skills shortages, and the need for uninterrupted operation frequently delay the deployment of modern security controls. For this reason, cybersecurity in Industry 5.0 should not be treated as an isolated technical issue, but as a structural challenge requiring coordinated governance across architecture, identity, network segmentation, data integrity, AI assurance, supplier risk management, and human oversight.

#### **4. SECURITY-BY-DESIGN AND CYBER-RESILIENCE FRAMEWORK FOR INDUSTRY 5.0**

The cybersecurity requirements of Industry 5.0 cannot be addressed through conventional perimeter-based protection alone. Because Industry 5.0 combines human-centricity, cyber-physical integration, and adaptive digital intelligence, security should be embedded into system architecture from the design stage. In this context, security-by-design and cyber-resilience-by-design provide a suitable basis for trustworthy industrial ecosystems in which protection, continuity, and recovery are treated as inherent system properties.

The proposed framework is structured into six interrelated domains: identity and access security, network and communication protection, device and edge security, data and AI integrity assurance, continuous monitoring and anomaly detection, and resilience, response, and recovery management. Together, these domains aim to reduce

the likelihood of compromise, limit attack propagation, preserve safe operation, and support timely recovery. Since Industry 5.0 closely links digital and physical assets, the framework must also protect human-machine collaboration as a core security objective.

Identity and access security is essential for addressing weak authentication, excessive privileges, shared credentials, and implicit trust. Network and communication protection should ensure segmentation, secure protocols, and controlled interaction among IT, OT, cloud, and edge environments. Device and edge security should include secure configuration, firmware integrity, authenticated updates, and hardened interfaces for sensors, controllers, and embedded devices. Data and AI integrity assurance is equally important because AI increasingly supports diagnostics, maintenance, scheduling, and operator assistance, making trustworthy data and validated model behavior critical.

Continuous monitoring and anomaly detection provide the visibility needed to identify cyber threats across converged industrial environments. At the same time, resilience, response, and recovery management ensure that critical functions can degrade safely, recover in a controlled manner, and maintain continuity under attack or disruption. For this reason, cybersecurity in Industry 5.0 should be viewed not as an isolated technical function, but as a multilayer and continuous process aligned with human-centric, resilient, and sustainable industrial transformation.

Figure 3 illustrates the proposed human-centric cyber-resilience framework for Industry 5.0. The model places the human operator at the center of intelligent manufacturing and connects this core with enabling technological domains and outer cybersecurity protection layers, highlighting the need for multilayer protection of human-machine collaboration, digital assets, AI-enabled functions, and operational continuity.

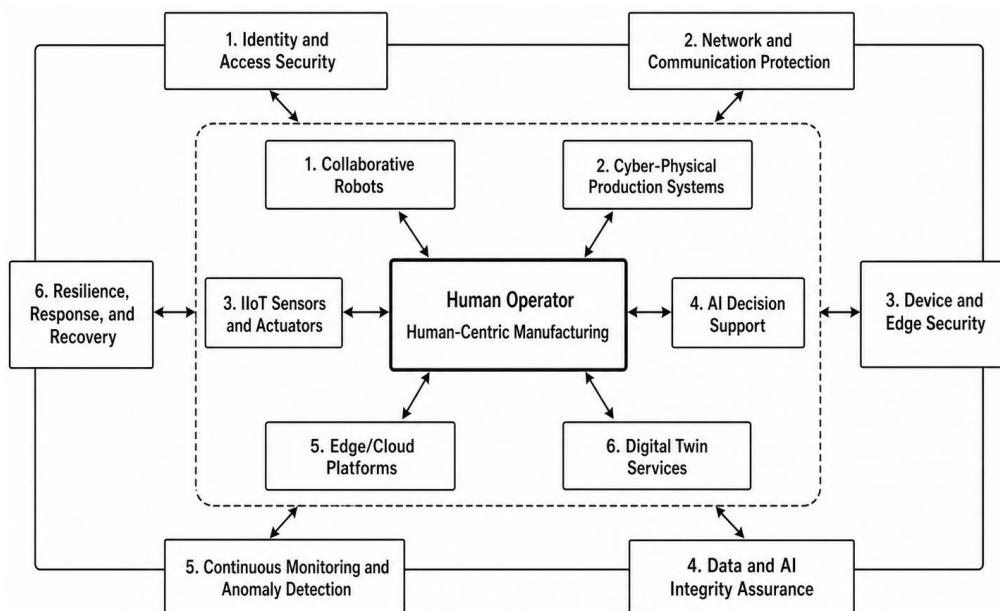


Figure 3. Proposed human-centric cyber-resilience framework for Industry 5.0 manufacturing environments

Table I summarizes the main cybersecurity challenge areas in Industry 5.0 together with their likely operational consequences and recommended protection directions. It shows that the cybersecurity problem extends beyond conventional industrial network defense and includes human-machine collaboration, AI assurance, device trust, and resilience across distributed digital infrastructures.

Table I. Main cybersecurity challenges and corresponding protection directions in Industry 5.0

| <b>Challenge domain</b>            | <b>Main cybersecurity issue</b>                                             | <b>Potential impact</b>                                                 | <b>Recommended protection direction</b>                             |
|------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Human-machine collaboration</b> | Unsafe or manipulated interaction between operators and intelligent systems | Safety risks, incorrect human decisions, loss of trust                  | Human-centric security design, explainable AI, safe fallback modes  |
| <b>IT/OT convergence</b>           | Weak segmentation and cross-domain attack propagation                       | Production disruption, process compromise, lateral movement             | Zero trust, strict segmentation, access control, policy enforcement |
| <b>IIoT ecosystems</b>             | Insecure sensors, gateways, and embedded devices                            | Data manipulation, unauthorized access, reduced visibility              | Secure device lifecycle, authenticated updates, hardened interfaces |
| <b>AI-enabled decision systems</b> | Data poisoning, adversarial manipulation, unreliable inference              | Incorrect diagnostics, unsafe recommendations, degraded control quality | Trustworthy AI assurance, data validation, model monitoring         |
| <b>Cloud-edge integration</b>      | Expanded trust boundaries and third-party dependencies                      | Service compromise, exposure of industrial data, supply-chain risk      | Hybrid security governance, secure APIs, vendor risk management     |
| <b>Operational resilience</b>      | Inadequate incident response and recovery readiness                         | Downtime, unsafe degradation, delayed restoration                       | Cyber-resilience planning, backup strategies, recovery procedures   |

Figure 4 presents a conceptual security-by-design and cyber-resilience lifecycle for Industry 5.0 systems. The lifecycle includes risk assessment, secure architecture design, identity and access control, device and edge hardening, data and AI integrity assurance, continuous monitoring, incident response, and recovery with continuous improvement. The figure also links cybersecurity to the three core principles of Industry 5.0—human-centricity, sustainability, and resilience.

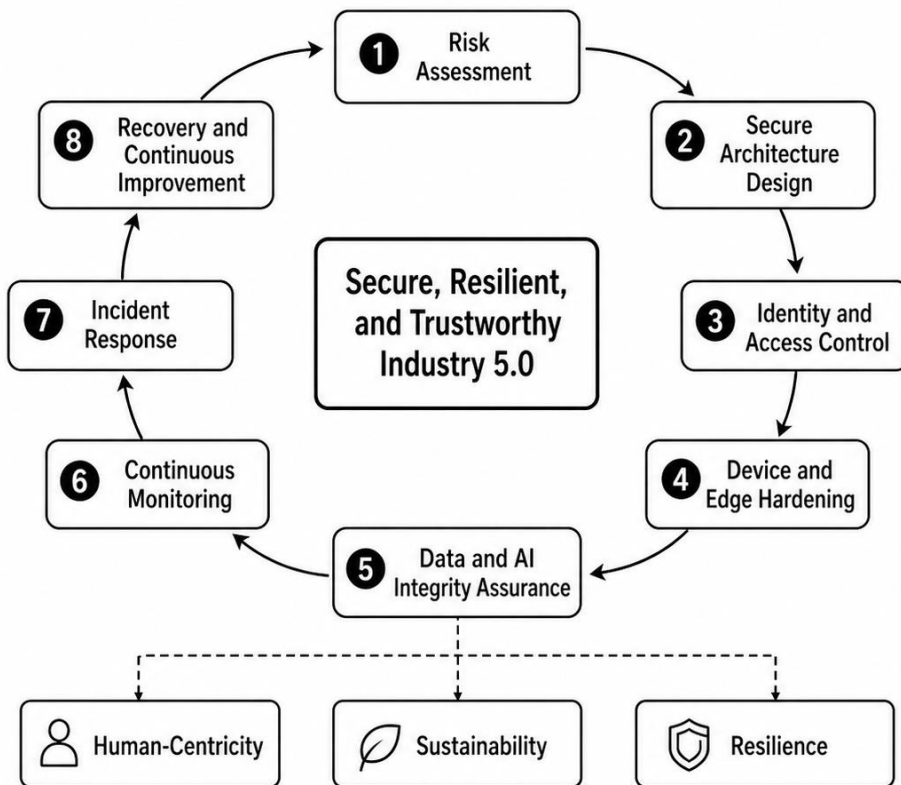


Figure 4. Security-by-design and cyber-resilience lifecycle for Industry 5.0 systems

## 5. DISCUSSION

The analysis shows that cybersecurity in Industry 5.0 should not be treated as a conventional extension of industrial information security. The transition from automation-centered production to human-centric, intelligent, and resilient manufacturing expands both the scope of protected assets and the logic of protection. In this context, cybersecurity must address not only technical infrastructure, but also operator safety, trustworthy human-machine collaboration, production continuity, and confidence in AI-assisted decisions.

This shift also shows the limitations of traditional industrial protection models. Static perimeters, weakly governed trust zones, and device-level hardening are insufficient in highly interconnected IT/OT/IoT/AI environments, where weaknesses in one domain may quickly propagate across others. As a result, cyber incidents in Industry 5.0 may simultaneously produce digital, operational, and physical consequences.

Another important observation is the increasing dependence on trustworthy AI. Because AI is now embedded in monitoring, diagnostics, predictive maintenance, optimization, and operator support, failures in AI security or reliability may directly affect industrial judgment and decision-making. Therefore, cybersecurity in Industry 5.0 should include not only infrastructure protection, but also assurance of intelligent decision layers.

The discussion further suggests that human-centricity should be understood as a cybersecurity design requirement. In Industry 5.0, effective protection depends not only on blocking attacks, but also on preserving understandable system behavior, meaningful human oversight, and safe intervention under degraded conditions. For this reason, usability, transparency, and interpretability become important elements of security architecture.

These considerations support the relevance of zero trust and resilience-by-design approaches for Industry 5.0. However, zero trust alone is not sufficient unless it is combined with monitoring, anomaly detection, response readiness, and recovery planning. Therefore, the most suitable strategy for Industry 5.0 is an integrated security architecture that combines access control, segmentation, device assurance, AI assurance, monitoring, and cyber resilience.

Overall, the main challenge is not simply to make Industry 5.0 more connected, but to make it securely connected in a way that remains trustworthy, resilient, and sustainable. In this sense, cybersecurity should be viewed as a strategic enabler of Industry 5.0 rather than as a secondary technical function.

## **6. CONCLUSION**

Industry 5.0 extends industrial transformation beyond automation and connectivity by placing human-centricity, sustainability, and resilience at the core of next-generation manufacturing. This also broadens the cybersecurity problem, which must protect not only data, networks, and industrial assets, but also operator safety, trustworthy human-machine collaboration, process integrity, and production continuity.

This paper examined the cybersecurity challenges of Industry 5.0 through three main dimensions: human-centric security, vulnerabilities caused by IT/OT/IoT/AI convergence, and security-by-design resilience strategies. The analysis showed that interconnected industrial ecosystems create a broader and more dynamic attack surface, where cyber incidents may affect both digital and physical operations. In such environments, conventional perimeter-based protection is insufficient.

Effective cybersecurity in Industry 5.0 requires a multilayer approach combining identity-centric access control, segmentation, secure device and edge management, trustworthy AI assurance, continuous monitoring, and recovery-oriented resilience. Overall, cybersecurity should be viewed as a strategic prerequisite for secure, resilient, and trustworthy smart manufacturing. Future research may further develop this perspective through formal frameworks, sector-specific case studies, and quantitative validation in real industrial settings.

## **ACKNOWLEDGMENT**

The article is a result of the implementation of project BG16RFPR002-1.014-0004 CENTRE OF EXCELLENCE Universities for Science, Informatics and Technologies in e-Society (UNITE), funded under the grant aid procedure BG16RFPR002-1.014 “Sustainable Development of Centers of Excellence and Centers of Competence, Including Specific Infrastructures or Their Associations from the National Roadmap for Scientific Infrastructure”.

## REFERENCES

- [1] Xu, X., Lu, Y., Vogel-Heuser, B., Wang, L. Industry 4.0 and Industry 5.0—Inception, conception and perception. *Journal of Manufacturing Systems*, vol.61, 2021, pp. 530-535. DOI: 10.1016/j.jmsy.2021.10.006.
- [2] Huang, S., Wang, B., Li, X., Zheng, P., Mourtzis, D., Wang, L. Industry 5.0 and Society 5.0—Comparison, complementation and co-evolution. *Journal of Manufacturing Systems*, vol.64, 2022, pp. 424-428. DOI: 10.1016/j.jmsy.2022.07.010.
- [3] Valette, E., Bril El-Haouzi, H., Demesure, G. Industry 5.0 and its technologies: A systematic literature review upon the human place into IoT- and CPS-based industrial systems. *Computers & Industrial Engineering*, vol.182, 2023, Article 109426. DOI: 10.1016/j.cie.2023.109426.
- [4] Hassan, M. A., Zardari, S., Farooq, M. U., Alansari, M. M., Nagro, S. A. Systematic Analysis of Risks in Industry 5.0 Architecture. *Applied Sciences*, vol.14, no.4, 2024, Article 1466. DOI: 10.3390/app14041466.
- [5] Alabdulatif, A., Thilakarathne, N. N., Lawal, Z. K. A Review on Security and Privacy Issues Pertaining to Cyber-Physical Systems in the Industry 5.0 Era. *Computers, Materials & Continua*, vol.80, no.3, 2024, pp. 3917-3943. DOI: 10.32604/cmc.2024.054150.
- [6] Ahmed, I., Hossain, N. U. I., Fazio, S. A., Lezzi, M., Islam, M. S. A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges. *Sustainable Manufacturing and Service Economics*, vol.3, 2024, Article 100018. DOI: 10.1016/j.smse.2024.100018.
- [7] Chaudhuri, A., Behera, R. K., Bala, P. K. Factors impacting cybersecurity transformation: An Industry 5.0 perspective. *Computers & Security*, vol.150, 2025, Article 104267. DOI: 10.1016/j.cose.2024.104267.
- [8] Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., Hewage, C. Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. *Digital*, vol.3, no.3, 2023, pp. 200-231. DOI: 10.3390/digital3030014.
- [9] Wyrzykowska, B., Szczepaniuk, H., Szczepaniuk, E. K., Rytko, A., Kacprzak, M. Intelligent Energy Management Systems in Industry 5.0: Cybersecurity Applications in Examples. *Energies*, vol.17, no.23, 2024, Article 5871. DOI: 10.3390/en17235871.
- [10] Khan, N., Ahmad, K., Al Tamimi, A., Alani, M. M., Bermak, A., Khalil, I. Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review. *Information*, vol.16, no.12, 2025, Article 1036. DOI: 10.3390/info16121036.
- [11] Romansky, R. Preliminary organization of virtual network based on program monitoring. *International Journal on Information Technologies and Security*, vol.16, no.3, 2024, pp. 111-120. DOI: 10.59035/TQDU5702.
- [12] Zhukabayeva, T., et al. Cybersecurity Solutions for Industrial Internet of Things—Edge Computing Integration: Challenges, Threats, and Future Directions. *Sensors*, vol.25, no.1, 2025, Article 213. DOI: 10.3390/s25010213.
- [13] Baghirov, E. A comprehensive framework for real-time malware detection and monitoring in production. *International Journal on Information Technologies and Security*, vol.16, no.4, 2024, pp. 85-94. DOI: 10.59035/GLJY1234.

- [14] Rudenko, R., Pires, I. M., Oliveira, P., Barroso, J., Reis, A. A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. *Electronics*, vol.11, no.11, 2022, Article 1742. DOI: 10.3390/electronics11111742.
- [15] Harkat, H., Camarinha-Matos, L. M., Goes, J., Ahmed, H. F. T. Cyber-physical systems security: A systematic review. *Computers & Industrial Engineering*, vol.188, 2024, Article 109891. DOI: 10.1016/j.cie.2024.109891.
- [16] Canonico, R., Sperli, G. Industrial cyber-physical systems protection: A methodological review. *Computers & Security*, vol.135, 2023, Article 103531. DOI: 10.1016/j.cose.2023.103531.
- [17] Sheth, A., Kusiak, A. Resiliency of Smart Manufacturing Enterprises via Information Integration. *Journal of Industrial Information Integration*, vol.28, 2022, Article 100370. DOI: 10.1016/j.jii.2022.100370.
- [18] Rahman, M. H., Wuest, T., Shafae, M. Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. *Journal of Manufacturing Systems*, vol.68, 2023, pp. 196-208. DOI: 10.1016/j.jmsy.2023.03.009.
- [19] Ivanova, Y. Integrating a DNS monitoring module into a cybersecurity architecture to enhance protection against spoofing and phishing attacks. *International Journal on Information Technologies and Security*, vol.17, no.2, 2025, pp. 111-122. DOI: 10.59035/LLQJ9022.
- [20] Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N., Salonitis, K. Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. *Cyber Security and Applications*, vol.3, 2025, Article 100067. DOI: 10.1016/j.csa.2024.100067.
- [21] Bajestani, M. S., Kim, C., Lee, K.-C., Kim, D. Self-X-based secure human-cyber-physical system (SSHCPs) for autonomous manufacturing in the era of Industry 5.0. *Advanced Engineering Informatics*, vol.69, 2025, Article 104054. DOI: 10.1016/j.aei.2025.104054.
- [22] Juma, M., Alattar, F., Touqan, B. Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB). *IoT*, vol.4, no.1, 2023, pp. 27-55. DOI: 10.3390/iot4010002.

### **Information about the authors:**

**Plamen Antonov Stanchev** – Associated Professor in Department of Intelligent Technology in Industry Technical University of Sofia, Sofia, Bulgaria. Current research interests: Electrical engineering, decentralized energy sources, relay protection.

**Denitsa Ivanova-Mutafchieva** – Assistant Professor in Department of Intelligent Technology in Industry Technical University of Sofia, Sofia, Bulgaria. Current research interests: intelligent technology, artificial intelligence; engineering; IoT; cybersecurity.

**Nikolay Lyuboslavov Hinov** – Professor in Department of Computer Systems, Technical University of Sofia, Bulgaria. Current research interests: modeling, simulation, and control; electric vehicles; smart energy and cyber-physical systems; artificial intelligence; engineering.

**Manuscript received on 03 May 2026**