



Baština Akademije nauka i umjetnosti Bosne i Hercegovine

SMART MANUFACTURING ON THE HORIZON: A Conceptual Shift from Industry 4.0 to Industry 5.0: Industrija

Karabegović, Isak

2026

Academy of Sciences and Arts of Bosnia and Herzegovina

<https://bastina.anubih.ba/handle/123456789/875>

Preuzeto s Baštine Akademije nauka i umjetnosti Bosne i Hercegovine

<https://bastina.anubih.ba/>

Cyber Security of Smart Manufacturing According to the Industry 5.0 Model: Challenges, Solutions and Future Development Directions

Sonja Dimitrijević¹, Vidosav D. Majstorovic^{*2}

Abstract: *As manufacturing increasingly embraces the digital transformation of Industry 4.0/5.0, the integration of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), robotics and edge/cloud computing has led to the creation of highly interconnected and automated systems. Industry 5.0 emphasizes human-centered innovation, resilience and sustainability. In this advanced industrial paradigm, humans and intelligent machines work closely together, making cybersecurity not just a technical requirement, but a strategic necessity. While these advancements improve operational efficiency, flexibility and productivity, they also introduce significant cybersecurity challenges and risks.*

To mitigate these risks, it is critical to adopt robust cyber security strategies. This includes implementing practices like network segmentation, strong authentication mechanisms, encryption and regular patch management. New technologies like AI-driven threat detection, blockchain for data integrity, and Zero Trust security models offer promising solutions. Additionally, adherence to industry standards such as ISO 27001 and IEC 62443 is critical to ensuring safe manufacturing operations.

Real-world case studies highlight both the consequences of cyber security breaches and the success of proactive security measures. The future of cyber security in smart manufacturing lies in continuously adapting to new threats, integrating security throughout the entire product life cycle, and fostering collaboration between industries and sectors.

In conclusion, cyber security is integral to the long-term success and resilience of smart manufacturing systems. As technology evolves, so must cybersecurity practices, ensuring that industries can take advantage of smart manufacturing without compromising security and reliability.

Keywords: Industry 5.0, Smart manufacturing, Cyber security, Case study

1. Introduction

In this one at the moment we are witnesses evolution Industry 4.0 (new concept automation, IoT, CPS), etc Industry 5.0 (focus) human, resistance and sustainability) [1]. It grows digitalization, with others sides brings to of that yes we have expanded surface cyber attacks, so yes are smart factories vulnerable on:

¹"Mihailo Pupin" Institute, Belgrade, Serbia

^{*2}The University of Belgrade, Faculty of Mechanical Engineering, Belgrade, Serbia

E-mail: vidosav.majstorovic@gmail.com

ransomware, manipulation data (e.g. metrological and data about quality are exposed risks), and we also have and cyber attacks in chain supply, figure 1.

With others side, in this one areas we have research gap, which is experiment in lack integrated model cyber security directed on a man and coordinated with principles Industry 5.0.

Goals this one work are: identifying key challenges cyber security, proposing solutions based on Industry 5.0, with an example for practice, i defining future direction research.

2. Literature Analysis

Cyber security in smart manufacturing in context Industry 5.0, is here analyzed through literature in last two year, table 1 [2-10].

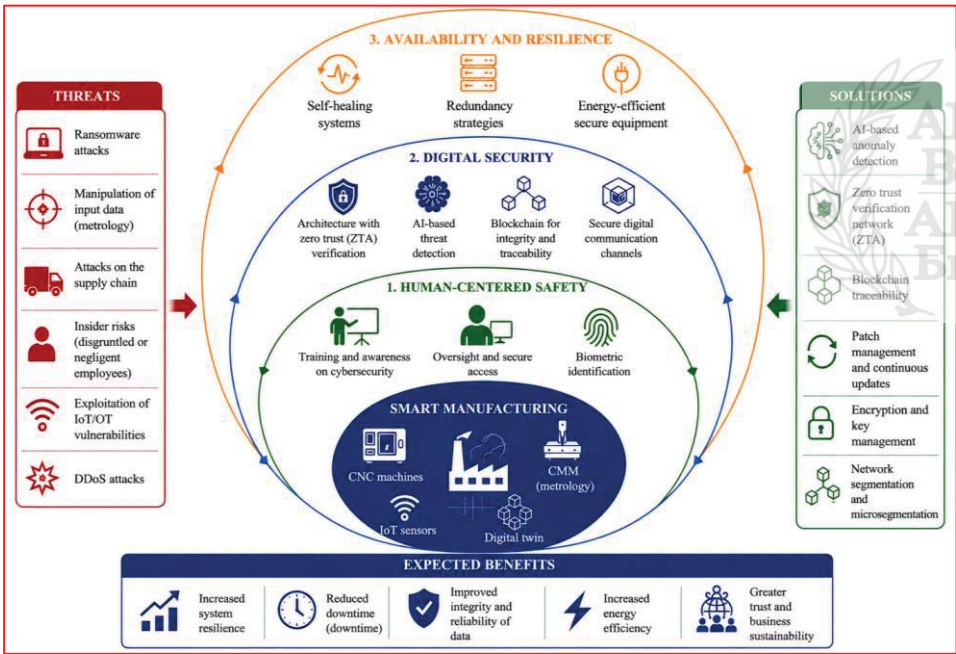


Figure 1. Cyber security system architecture for smart manufacturing systems based on Industry 5.0 principles

Table 1. Overview of selected references for cyber security analysis

Ref.	Approach / Focus	Key technologies	Level of analysis	Key contributions	Limitations	Research gap
[2]. Kour et al. (2024)	Cyber security trends in Industry 5.0	AI, Blockchain, IIoT	Conceptual / Review	It identifies new paradigms of cyber security in Industry 5.0	Lack of implementation framework	No integration with real manufacturing systems or metrology
[3]. Santos et al. (2024)	Security challenges of Industry 5.0	CPS, human-centered security	Conceptually	It connects cyber security with people-centric manufacturing	There is no architecture-level solution	A tiered model of cyber security is missing
[4]. Chaudhuri et al. (2025)	The transformation of cyber security	Organizational + digital systems	Empirical	Identifies the drivers of cybersecurity adoption	Weak connection with the systems in the manufacturing plant	No relation to CNC/CMM/IIoT environments
[5]. Rahman & Shafae (2025)	CPS Vulnerability Classification	IIoT, CPS, Industrial systems	Technical taxonomy	Multilevel classification of vulnerability	No experimental validation	Not adapted to metrological systems
[6]. Antipenko et al. (2026)	Function-driven cyber security	Automated manufacturing systems	At the system level	It connects security with industrial functions	Limited real-time integration	Lack of integration of DT and AI
[7]. Khan et al. (2024)	XAI-based intrusion detection	AI, explainable AI	Algorithmic	Increases confidence in AI-based cyber security	Vulnerable to enemy attacks	No integration with industrial processes
[8]. Rojas et al. (2024)	AI-powered IIoT security	AI, Edge/Cloud, IIoT	At the system level	It integrates AI with IIoT architectures	A human-centered perspective is missing	No compliance with Industry 5.0
[9]. Leirimo et al. (2024)	DT in Industry 5.0	DT, simulation	Conceptually	DT as a human-centered decision-making tool	Limited focus on cyber security	DT security not resolved
[10]. Whaiduzzaman et al. (2026)	DT-based security	DT, IIoT, VI	Applied concept	DT used for anomaly detection	Limited industrial validation	There is no focus on the protection of metrological data

A summary analysis of the references from table 1 shows us the following facts: (a) *fragmentation of approaches*, shows that the analyzed works focus on isolated domains: AI security, CPS vulnerabilities, DT and organizational transformation. This means that an integrated cyber security architecture is lacking; (b) *lack of metrology cyber security* for measurement data integrity (CMM, sensors), calibration traceability and cyber security quality assurance). This is a critical gap for smart manufacturing systems; (c) *poor compliance with Industry 5.0*, because the paradigm of Industry 4.0 is applied, which does not take into account safety, explainability and sustainability; (d) *security gap for DT*, because cyber security

is extremely important for them, because they work online. This is particularly important due to: secure synchronization, data manipulation protection and trust validation mechanisms.

The contribution of this work is to integrate an Industry 5.0 cybersecurity framework for smart manufacturing, which combines human-centric security, AI/XAI-based detection, secure AI, and sustainability-aware resilience mechanisms.

3. Basics Models Cyber Security for Smart Manufacturing

CIA triad. This one concept represents basic model security in models cyber security, which defines three basic principles [11]: *confidentiality (C)*, what means protection data from unauthorized access, *integrity (I)*, meaning protection data from unauthorized modifications, and *availability (A)*, provision reliable access systems and data.

In smart manufacturing and Industry 5.0, CIA triad evolves in cyber - physical - human paradigm security, where are data, machines and people are strong each other connected.

The classic structure of the CIA triad is a triangular model, where each component is interdependent, and the removal of one element threatens the entire system, but there are trade-offs (eg, stronger confidentiality may reduce availability). In Industry 5.0, the CIA triad expands into a multi-layered architecture: the human layer (trust, awareness, behavioral safety); digital layer (data, networks, AI systems); a physical layer (machines (CNC, CMM), sensors, robots), and a sustainability layer (energy-aware security, resilience), thus transforming the CIA into a cyber-physical-human security framework.

The functions of the CIA components are: *confidentiality* (ensuring that information is accessible only to authorized entities), and this is ensured through the basic functions: access control (RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control)), encryption (data at rest and in transit), authentication and identity management, and data classification and privacy protection. The following technologies are applied here: AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman cryptosystem) encryption, multi-factor authentication (MFA (Multi-factor authentication)), and zero trust architecture (ZTA (Zero Trust Architecture)). The context of smart manufacturing is about protecting CAD/CAM models, securing digital twin data, and preventing industrial espionage; *integrity* (ensures that data remains accurate, consistent and unchanged), and the main functions are: hashing (SHA-256 (Secure Hash Algorithm 256-bit), etc.), digital signatures, blockchain-based immutability and version control and traceability of checks. This aspect is supported by the following technologies: cryptographic hash functions, blockchain system and AI-based anomaly detection. In smart manufacturing, this refers to: protecting

metrology data (CMM results), ensuring the accuracy of calibration of these systems and preventing data manipulation in quality control, for example; *availability* (ensuring that systems and data are available when needed), and its core functions are: redundancy (failover systems), backup and disaster recovery, load balancing, and fault tolerance. Supporting technologies are: cloud/edge computing, distributed systems. The context of smart manufacturing refers to the continuous operation of MES/ERP systems, then real-time monitoring via IoT, as well as avoiding downtime in manufacturing lines, figure 2.

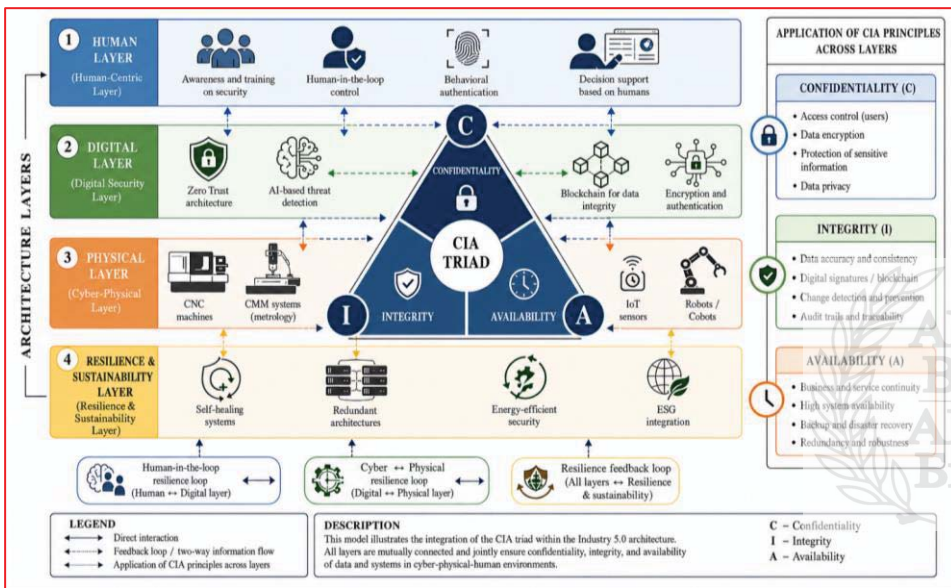


Figure 2. The structure of the CIA triad model in the Industry 5.0 architecture

Zero Trust Architecture (ZTA). Here, an in-depth, structured analysis shows that this model is more aligned with the model of smart manufacturing, Industry 5.0 and smart metrology. It is a modern paradigm of cyber security based on the principle - "never trust, always verify". Unlike the CIA model, ZTA (Zero Trust Architecture) assumes: no implicit trust (inside or outside the network), continuous verification of users, devices and systems, and dynamic, context-aware access control. In Industry 5.0, ZTA becomes necessary due to hyper-connectivity (IoT, CPS), human-machine interaction, and distributed cloud-edge environments. The key components of the ZTA model are [12]: (a) *policy engine (PE)*, which represents a central decision-making unit, which evaluates access requests using identity, device status, and context (location, time, behavior), (b) *policy administrator (PA)*, where decisions are converted into actions, configures access sessions, and communicates with enforcement mechanisms, and (c) *policy*

enforcement point (PEP), where access control decisions are executed, such as: allow / deny / restrict access, and these reside on gateways, applications, and endpoints.

Applications in smart manufacturing (Industry 5.0), refers to: smart cyber physical systems (CPS/CPPS), for secure communication between machines, isolation of vulnerable nodes and detection of threats in real time; smart metrology (CMM, DT and IoT sensors) to authenticate measurement system devices, check the integrity of measurement data and control limited access to calibration records. Here, it is prevented that the data is changed without authorization or false measurement results are generated; DT security, where we have security synchronization (physical ↔ digital), access control for simulation models and protection against model manipulation; AI-driven manufacturing where this model is applied to protect artificial intelligence models and datasets, detect cyber attacks and protect inference nodes in ML models; supply chain security, reflected through secure third-party access, supplier authentication, and data integrity among partners.

Defense in depth (DID). Defense in depth is a cyber security strategy based on multiple coordinated layers of protection. The key idea is simple: if one control fails, other controls continue to protect the system. This model is particularly important in smart manufacturing and Industry 5.0, where manufacturing systems combine people, machines, IoT devices, cloud/edge platforms, digital twins, AI systems and supply chain connections.

According to this model, cyber security represents defense in depth (DID (Defense-in-depth)), so it can be understood as a layered security architecture, with elements as in table 2.

Table 2. Layers of the security architecture of the DID model

Layer	Purpose	Typical controls
Management layer	Policies, roles, risk management	ISO 27001, procedures, audits
Human layer	It reduces the risks associated with people	Training, awareness, discipline of approach
Physical layer	Protects equipment and facilities	Locks, surveillance, access cards
Network layer	Controls communication	Firewalls, segmentation, IDS/IPS
Identity layer	Controls who can access systems	MFA, RBAC, least privileges
Endpoint/Device Layer	Protects machines and devices	EDR, patching, strengthening
Application layer	It provides software and platforms	Secure encryption, authentication, logging
Data layer	Protects the information itself	Encryption, backup, digital signatures
Tracking layer	Attack and anomaly detection	SIEM, SOC, AI-based detection
Recovery layer	Restores normal operation.	Backup, redundancy, disaster recovery

The basic functions of this model are [13]: *prevention*, which refers to the function of reducing the probability of attacks (firewalls, access control, MFA (Multi-Factor Authentication), network segmentation, secure configuration and employee training for cyber security). In smart manufacturing, prevention protects

systems such as CNC machines, CMM systems, robots, MES/ERP, IoT sensors and DT; *detection* is a defense in depth system, which assumes that prevention is never perfect. For these reasons, systems must quickly detect attacks, which includes: intrusion detection systems, log monitoring, AI anomaly detection, behavioral analytics, and industrial network monitoring. For example, abnormal communication between the CMM system and the MES may indicate manipulation of quality data; *response*, where after detection, the system must react, with a response that includes: isolating infected devices, blocking suspicious users, disabling further operation of compromised accounts, activating procedures for responding to incidents and switching to safe operation mode. In manufacturing, the response must be carefully thought out because a system shutdown can affect the safety and availability of manufacturing; *recovery*, returns the system to normal operation after an incident. Recovery mechanisms include: backup and restore, disaster recovery plans, redundant servers, failover systems, and clean system images. For Industry 5.0, recovery is related to resilience, meaning that a system can resume or quickly return to acceptable performance after an interruption; *continuous improvement*, where defense in depth is not static, as it requires: regular risk assessment, analysis of lessons learned after incidents, updating security policies, updating system patches (patches), improving employee awareness and updating and testing backup and recovery procedures.

4. Cyber Security Challenges for Smart Manufacturing

4.1 Technological Challenges

IoT vulnerabilities (low power devices, weak encryption). IoT devices are the "Achilles' heel" of smart manufacturing, not because they are poorly designed, but because they are resource-constrained and often neglected in the security architecture. Industrial IoT (IIoT) devices: have limited processing power, use minimal memory, operate in a real-time environment, and often have long lifetimes (10–20 years). As a result we have a compromise between performance, energy and safety. What are the sources of cyber security risks in IoT devices? These are [2,14]: *(a) low - power devices as source risks* - limitations hardware (weak CPU (eg micro - controllers - LPC), small RAM / Flash memory and limited battery). As consequences we have : impossibility implementations strong cryptographic algorithms, there are none space for advanced security mechanisms and rarely update firmware ; energy restrictions (encryption spend energy, continuous monitoring increases consumption, authentication is additional overhead, devices often use weaker algorithms or them completely omit); minimal operational systems (bare - metal or RTOS systems, without advanced insulation process and without sandboxing, so one vulnerability causes

compromise the whole devices, *(b) weak encryption* is key problems, because of - outdated algorithms (use is DES, RC 4, as and weaker TLS versions) what causes easy breaking through modern tools ; hardcoded keys (keys built - in in firmware and no rotations keys) because one compromised device, means compromise all; unencrypted communication is do plain - text protocols : MQTT without TLS, HTTP instead of HTTPS. Attacks is they perform as man - in - the - middle (MITM), interception data and modification command ; weak authentication (default) password, none MFA and simple tokens) what brings to easy downloads controls over device.

One review cyber threats for IoT and countermeasures for them for context smart of manufacturing / Industries 5.0, table 3.

Table 3. IoT threats and countermeasures for the Industry 5.0 model

Threat category	Threat description	Cause / vulnerability	Influence (CIA)	Countermeasures (state-of-the-art)
Unauthorized access	Unauthorized access to IoT devices	Default password, weak authentication	C, I, A	MFA, Zero Trust, RBAC/ABAC, Device Identity
Interception of Communication (MITM)	An attacker intercepts and modifies the data	Unencrypted communication (MQTT/HTTP)	C, I	TLS 1.3, VPN, end-to-end encryption
Data manipulation	Modification of sensor or metrology data	Lack of validation and integrity	And	Hash functions, digital signatures, blockchain
Botnet attacks (eg Mirai botnet)	IoT devices are used for DDoS	Weak authentication, open ports	A	Network segmentation, IDS/IPS, patch management
Firmware attacks	Injection of malicious firmware	Unprotected update mechanism	I, A	Secure boot, signed firmware, OTA security
Repeat attack	Resending valid messages	Lack of time tokens	And	One time, timestamp validation, session token
DoS/DDoS attacks	Disabling the system	Lack of network protection	A	Speed limiting, firewall, cloud protection
AI/ML attacks	Manipulation of models or data	Unprotected AI streams	And	XAI, robust ML, input validation
Lateral movement	Spreading attacks through the network	Lack of segmentation	C, I, A	Microsegmentation, ZTA
Industrial espionage	Data and know-how theft	Weak encryption and access control	C	End-to-end encryption, DLP systems
Physical attacks	Direct access to devices	Lack of physical protection	C, I	Tamper protection, secure hardware
Insider Threats	Malicious or employee errors	Lack of control and training	C, I, A	Training, audit logs, least privileges
Supply chain attacks	Compromised vendor or software	Lack of verification	C, I	SBOM, supplier verification
Energy attacks	Device battery drain	Inefficient protocols	A	Energy-aware security, edge network filtering
Outdated systems	Outdated devices without security	Long IoT lifecycle	C, I, A	Protection gate, virtual patching

IoT security is moving from "device-level security" to system-level intelligent protection (AI and ZTA and Edge security).

Cloud/Edge cyber security risk. Cloud and Edge are not "bonus layers", they are the backbone of smart manufacturing. This is precisely why they are critical points of attack. In modern systems, the cloud has centralized analytics, AI, data storage (history), and the edge is characterized by local processing and real-time control. The combination of these two models enables low latency, scalability and intelligent manufacturing, but also introduces a distributed attack surface.

The key vulnerabilities are [3,15]: (a) *security risks in the cloud* are multiple: incorrect configuration (misconfiguration), where we have open storage (eg public buckets), and poorly defined IAM policies; weak identity control (IAM), where too broad privileges, lack of MFA, and compromised API keys occur, so that an attacker gains access to the entire system; unprotected API interfaces, where we have an API without authentication and weak input validation; multi-tenancy risks, where shared infrastructure and potential data leakage between users occur; loss of control over data, where we have data outside the local infrastructure and legal/regulatory issues, (a) *security risks in the edge model* are reflected in the following approaches: physical exposure of devices (edge devices often in the field and easily physically compromised); limited resources (like IoT), where we have weak encryption and minimal protection; irregular updates refers to difficult patch management as well as long life cycle; insecure communication between edge ↔ cloud without encryption, as well as MITM attacks; local compromise, where the attacker gains control over the edge node, and data manipulation is done before sending it to the cloud, (c) *combined cloud-edge risks* refer to the following approaches: trust gap gap in trust, where we have that the edge device is compromised, so the cloud trusts false data. This risk is particularly dangerous for digital twin and AI models; data integrity attacks, where we have an attack on data integrity, as a manipulation on the edge, and for these reasons cloud analytics works on the wrong data (garbage in → garbage out); lateral movement (Lateral Movement), where the attack starts from edge devices and spreads to cloud services and MES / ERP systems, (d) supply chain risk, where we usually have edge devices from different manufacturers as well as third-party cloud services.

The impact on smart manufacturing is realized here through several elements: CNC manufacturing (wrong processing parameters and tool wear), metrology (measurement manipulation and loss of traceability), DT (incorrect simulations and wrong optimizations) and AI systems (wrong predictions and model drift).

Vulnerabilities of AI/ML systems in smart manufacturing. AI/ML systems are a key component in: predictive maintenance (PrM), quality control, DT and process optimization. However, unlike classical systems, they are dependent on data and subject to manipulation, the main categories of attacks are attacks during training (data poisoning), and attacks during inference (adversarial attacks).

Data poisoning is an attack in which an attacker injects malicious or manipulative data into the training set, with the aim of making the model learn wrong patterns. Here the following types of attacks [5,16]: label poisoning (misabeled data, for example a defective product marked as "correct"); feature poisoning (manipulation of input values (eg sensor data), and these are subtle changes that are not easily noticeable); backdoor attacks (inserting a "hidden trigger " into the data, where we have the model behave normally, until the trigger is activated). The attack mechanism is performed in several steps: inserting compromised data into the dataset, training the model on such data, the model internalizes wrong patterns, and wrong decisions are made in real work.

Adversarial attacks involve the manipulation of input data during the operation of the model, with the aim of making the model make a wrong decision. A key feature is that small, often imperceptible changes in the input lead to a large error in the model's output. Here we have the following types of attacks: evasion attacks (alteration of input to avoid detection); gradient-based attacks (using model structure to create attacks); physical attacks (manipulation of real sensor data). Industrial examples refer to: predictive maintenance (failure not detected, the consequence is a breakdown), visual control (defect not recognized), robotics (misinterpretation of the environment).

Advanced protection strategies are implemented through the following approaches: explainable AI (XAI) (understanding model decisions), ZTA for AI (verification of each input and data source), secure DT (comparative validation of real and digital systems), and continuous monitoring of AI systems (detection of anomalies in model operation), and blockchain for data (immutability of training dataset).

Research challenges in this area are: AI security in metrology, DT protection, integration of AI and measurement uncertainty, and tinyML security on edge devices.

In conclusion, we can say that AI/ML vulnerabilities represent a new generation of threats, because attacks no longer target only the system, but the intelligence of the system. AI in Industry 5.0 must be: safe, explainable and under human supervision.

A detailed analysis of AI threats against the Industry 5.0 model is shown in Table 4.

Table 4. AI threats vs industrial impact in Industry 5.0

AI threat	Description of the attack	Industrial system domain /	Industrial influence	Influence (CIA)	Recommended countermeasures
Data poisoning	Training data manipulation	Predictive maintenance, DT	Wrong predictions, system degradation	I, A	Data validation, anomaly detection, reliable dataset
Side attacks	Input manipulation during model operation	Visual inspection, robotics	Undetected defects, wrong actions	And	Training for flanking attacks, robust models, sanitizing entrances
Model extraction	Model theft via API	Cloud platforms	Loss of intellectual property	C	Speed limiting, API protection, encryption
Inversion model	Reconstruction of training data	Healthcare, metrology	Leakage of sensitive data	C	Differential privacy, access control
Backdoor attacks	Hidden trigger in the model	Autonomous systems, QC AI	Unexpected system behavior	And	Model inspection, training verification
Data “lakes”	Data leakage through the AI pipeline	Cloud/Edge systems	Industrial espionage	C	Encryption, DLP, secure lines
Model drift	Changing data distribution	Predictive systems	Reduced model accuracy	I, A	Continuous retraining, monitoring
Lines of compromise	Attack on ML pipeline	CI/CD systems	Complete compromise of the model	C, I, A	ZTA, secure MLOps
AI hallucination	Generating incorrect results	Generative AI in industry	Wrong decisions	And	Output validation, man in the loop
Insider AI abuse	Abuse by employees	All systems	Model/data manipulation	C, I	Audit logs, least privileges
Edge AI attacks	Edge model compromise	IoT / CNC systems	Wrong local decisions	I, A	Secure edge, TPM, monitoring
Resource depletion	AI system overload	Cloud AI	Service unavailability	A	Scalability, load balancing

The summary link of the analysis in the previous table with the CIA triad is: confidentiality (C), protection of models and data, integrity (I), accuracy of AI decisions and availability (A), continuity of AI services.

Security of digital twins (DT). A digital twin is a digital replica of a physical system (eg CNC, CMM, manufacturing line), which is updated in real time. Key features are continuous data exchange, AI integration and simulation of physical ↔ digital links. It is this connectivity that creates new security vulnerabilities.

The main categories of vulnerabilities are [10,17]: data integrity gap, where the problem is that DT depends on real data (IoT, CMM, sensors). Risk is the manipulation of data, which causes errors in the simulation. For example, wrong metrology data, DT gives incorrect optimization; insecure communication (communication gap), where the problem is weak communication protection: IoT ↔ Edge, Edge ↔ Cloud and Cloud ↔ Digital Twin. The risk is MITM attacks and data interception and modification; AI/ML vulnerabilities in DT come from the risk of data poisoning, adversarial attacks, as well as the occurrence of model

drift, so DT makes wrong decisions; access control (Access Control Gap), problems arise due to inadequate authentication and authorization, it arises due to the risk of unauthorized access to the model and manipulation of simulations; synchronization gap, as a risk arises as a difference between the real and digital system, because DT no longer represents the real state, as well as wrong decisions in manufacturing; cloud/edge dependency, and problems arise because DT is often hosted in the cloud, so the risk arises because we have cloud compromise and loss of control over data; IoT vulnerabilities are caused by weak IoT devices (low-power, weak encryption), so the risk is an entry point for an attack on DT; the human factor is a risk due to insufficient training and insider threats, and the risk is misconfiguration and misuse of the system.

The Industry 5.0 perspective for this area is reflected in the following facts: human-centric approach (man validates critical decisions), digital aspect (integration of AI + DT + IoT) and sustainability (accurate simulations, we have less scrap).

4.2 Operational Challenges

In the field of cyber security, smart manufacturing, operational challenges can occur as: integration of old systems, limitations of real-time systems and interoperability of complex systems [6,18].

Legacy systems in this context refer to old CNC machines, outdated SCADA/PLC systems and supporting software without modern interfaces. The problem here is how to integrate old systems into modern digital architectures (IoT, Cloud, DT, AI)? The key challenges are technological incompatibility, such as the lack of standard protocols (eg OPC UA) and outdated interfaces. Their lack of security is without encryption and authentication with a high risk of attack. As far as the data is concerned, access to them is limited, because the data is not digitized and does not have the possibility of real-time analysis. There are high modernization costs, equipment replacement is expensive and the risk of manufacturing interruption is high.

Real-time system limitations appear as a real problem, because smart manufacturing requires reactions in milliseconds, system synchronization and continuous operation without downtime. The problem is how to ensure high security and complex data processing without impairing real-time performance? The key challenges are latency, where there is a delay in cloud processing, and AI models require additional processing time. All of the above is critical for CNC control and robotics. System determinism refers to the fact that industrial systems require predictable behavior and AI systems are probabilistic. The security overhead is characterized by the fact that encryption and authentication increase latency, and ZTA models require continuous verification. Resource limitations (Edge/IoT) are small CPU and memory, as well as the inability to perform

complex analysis. The industrial impact is reflected in the fact that there is a delay in decision-making, process instability and the risk of breakdowns. The solutions are edge computing (local processing), real-time operating systems (RTOS), hardware acceleration (GPU/FPGA), and AI model optimization (TinyML).

Complex system interoperability is the ability of systems to exchange data, understand data and function together, and in Industry 5.0 systems include: CNC, CMM (metrology), IoT, MES/ERP, DT and AI systems. The key challenges are different standards and protocols, such as OPC UA, MQTT, Modbus and REST API. The disadvantage here is that there is no universal standard. A semantic mismatch is a different meaning of data, e.g. "temperature" can have different contexts (cause of appearance). The heterogeneity of the system is reflected in the increased complex interoperability of the system through IT + OT integration, as well as cloud + edge + on-premise. Scalability here refers to a large number of devices, as well as the fact that we have a complex system orchestration. The industrial impact, from a negative aspect, is ineffective communication, data loss and the impossibility of process optimization. Solutions to these problems are standardization (OPC UA, RAMI 4.0), application of ontology and semantic models, digital thread and DT integration and API-first architecture, figure 3.

4.3 Human-Centered Challenges

An in-depth analysis of the human-centric challenges in smart manufacturing cyber security shows that it depends on insider threats, lack of cyber security awareness and human-machine interaction risk. Insider threats represent security risks originating from employed engineers, operators and external collaborators (suppliers, maintenance). They can be intentional (malicious) as well as unintentional (mistakes, carelessness). Types of insider threats are [9,19]: malicious insider (theft of industrial data, system sabotage and manipulation of AI/DT models), careless insider (weak passwords, clicking on phishing links and wrong system configuration), compromised insider (account taken over by attackers and attacks through stolen credentials).

The industrial impact of this concept is reflected in the manipulation of metrological data (CMM), wrong decisions in MES/QMS, sabotage of CNC processes and industrial espionage. The connection with the CIA triad is reflected in the following relationships: confidentiality (data theft), integrity (data manipulation), and availability (system sabotage). Protection measures are least privilege access, user monitoring (UEBA), audit logs, ZTA and system segmentation.

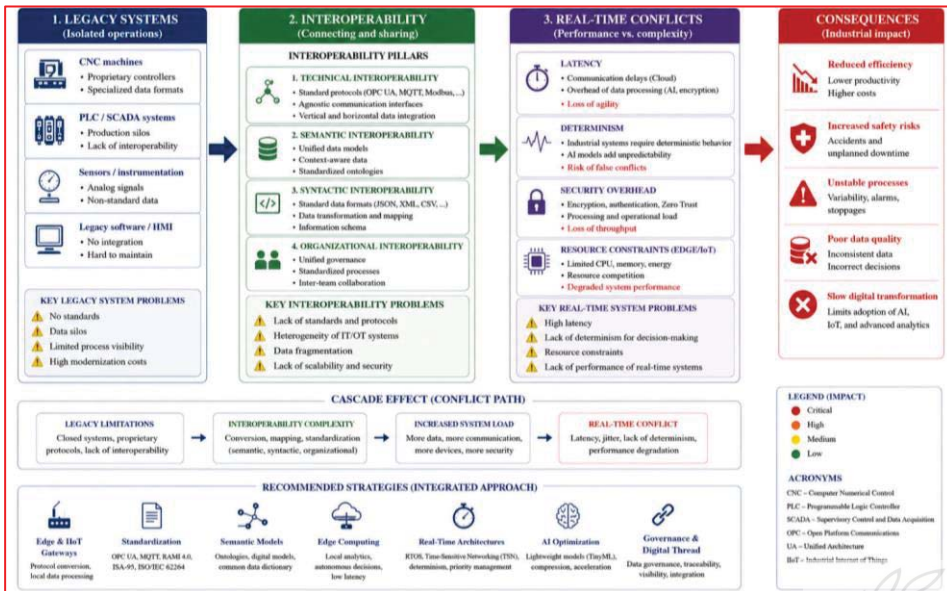


Figure 3. Cyber security operational challenges in smart manufacturing

In Industry 5.0, man and machine work together, such as cobots, AI systems, DT and autonomous systems, and the problem is that man-machine interaction introduces new safety and operational risks. Key challenges are excessive trust in AI (operators blindly trust AI decisions, lack of verification), lack of transparency (AI models are a "black box", and sometimes it is difficult to understand decisions), misinterpretation of data (operator misunderstands AI output, or wrong actions in manufacturing), safety of cobots (physical interaction with people, risk of injury), cognitive load (too much information for the operator, as well as stress and errors). Industrial impact manifests itself through wrong manufacturing decisions, reduced product quality, safety incidents and employee health risks. Safeguards include explainable AI (XAI), human-in-the-loop systems, interface ergonomics, operator training, and safety protocols for robots.

4.4. Supply Chain Vulnerabilities

This important aspect of digital business relates to third-party risks, as well as risks related to software/hardware dependencies.

Risks arising from third parties depend on equipment suppliers (CNC, CMM, IoT), software vendors (MES, ERP, AI platforms), cloud service providers and maintenance companies [5,20]. Therefore, the problem of system security also depends on the security of external partners. Key vulnerabilities occur in the

following cases: insufficient supplier security (suppliers do not have adequate controls or weak protection of development processes); remote access of the provider (VPN access for maintenance or insufficient control of activities); unverified updates (the software update may contain malicious code), for example, a compromised firmware update; lack of transparency (because there is no insight into how the software is developed, or which components are used). Typical attacks are supply chain malware (compromised update), insider attacks at suppliers and cloud provider compromise. Industrial influence in this area is reflected in the compromise of CNC and CMM systems, manipulation of metrological data, interruption of manufacturing and industrial espionage.

Software and hardware dependencies are based on the fact that industrial systems depend on a complex ecosystem, which includes operating systems, libraries and frameworks, firmware, industrial controllers, and IoT devices. The problem with this concept is that one vulnerability in a dependency can compromise the entire system. Key vulnerabilities are: outdated components (unupdated software or unsupported versions), open-source dependencies (use of libraries without verification, unknown vulnerabilities), firmware vulnerabilities (hardcoded keys, unprotected boot process), hardware backdoors (malicious or compromised chips, supply chain compromise at the hardware level), lack of patch management (delay in applying security patches). The industrial impact of these aspects relate to the compromise of AI and DT systems, wrong manufacturing decisions, loss of data integrity and system downtime. Here we also have the effect of the so-called cascade effect, which is realized in the chain: a vulnerable library, a compromised AI model, a wrong decision and the physical system reacts. Protection measures are SBOM and dependency analysis, regular patch management, secure development lifecycle (SDLC), firmware verification and trusted hardware (TPM, secure element).

4.5 Risks Related to Metrology and Quality Data

Cyber security risks in this area arise from the manipulation of measurement data, as well as threats to the integrity of calibration data. Manipulation of measurement data implies unauthorized modification or falsification of measurement results from CMM systems, sensors (IoT), laboratory tests and online control systems. The aim of the attack is to present a defective product as a correct one, as well as to conceal errors in the process. The attack vector is complex and can include [5,21]: compromise of IoT sensors (false input data and signal manipulation), MITM attacks (communication), which are reflected in the interception and modification of data between CMM ↔ MES, as well as Edge ↔ Cloud, attacks on databases (modification of historical measurement data and deletion of records), and insider manipulation (manual modification of results, as well as "correction " of data to meet standards). The industrial impact is reflected in the

possibility of unwanted events: faulty quality control, passing of defective products, rejection of correct products and loss of traceability. In smart metrology, data integrity represents confidence in product quality. Protection measures are: digital signatures of measurement data, hash validation, blockchain for traceability, redundant measurements and AI anomaly detection.

5. Cyber Security Solutions in Industry 5.0

5.1 Human-Centered Security Layer

In Industry 5.0, security is no longer exclusively a technological problem, but an interaction between man, systems and intelligent technologies. The human-centered security layer includes [9,21]: education and awareness, active human participation in security and advanced identification methods (behavioral).

Cyber security *training and awareness includes continuous education of employees about cyber threats, security practices and rules of conduct in the digital environment*. Key challenges are: low level of awareness (operators focused on manufacturing, security as a secondary priority), rapid evolution of threats (ransomware, phishing, AI attacks, as well as outdated training programs), different levels of knowledge (engineers vs operators, IT vs OT staff). The industrial impact of cyber security is reflected in the reduction of insider risk, faster response to incidents and reduction in the success of phishing attacks. The advanced approach, related to the application in the Industry 5.0 model, is: adaptive training (AI-driven learning), attack simulations (phishing, SOC scenarios), gamification (cyber drills) and personalized training programs. We can state that the greatest security risk is not technology, but an insufficiently educated user.

Human-in-the-loop monitoring is a model in which a human actively participates in monitoring and making security decisions together with AI systems. The role in Industry 5.0 is a combination of AI detection and human assessment. The goal is to increase accuracy and reduce false alarms. The key challenges are: over-reliance on AI (blind trust in automation), cognitive load (too many warnings and "vigilance fatigue", reaction delay (human decision can slow down the process). The industrial impact is related to more accurate detection of attacks, better decision-making and greater system resilience. Advanced approaches in this area are explainable AI (XAI), alarm prioritization, support for decision-making systems and interactive dashboards. The most secure system is not fully automated, but human synergy and AI.

Behavioral biometrics uses patterns of behavior to identify users: typing style (keystroke dynamics), mouse movements, operating patterns on the system, and how to interact with machines. The advantages of this approach are continuous authentication, difficult forgery and this is a non-invasive method, figure 4. The

key challenges are: privacy (monitoring of user behavior), variability of behavior, due to changes (stress, fatigue and experience), and false positive/negative results (false detection). The industrial impact is reflected in the detection of insider threats, prevention of unauthorized access and protection of critical systems (CNC, CMM, MES). Advanced approaches are AI models for behavior, integration with ZTA, multi-factor authentication and edge behavior analysis. The most important message is that user identity is no longer just "who you are", but how you behave.

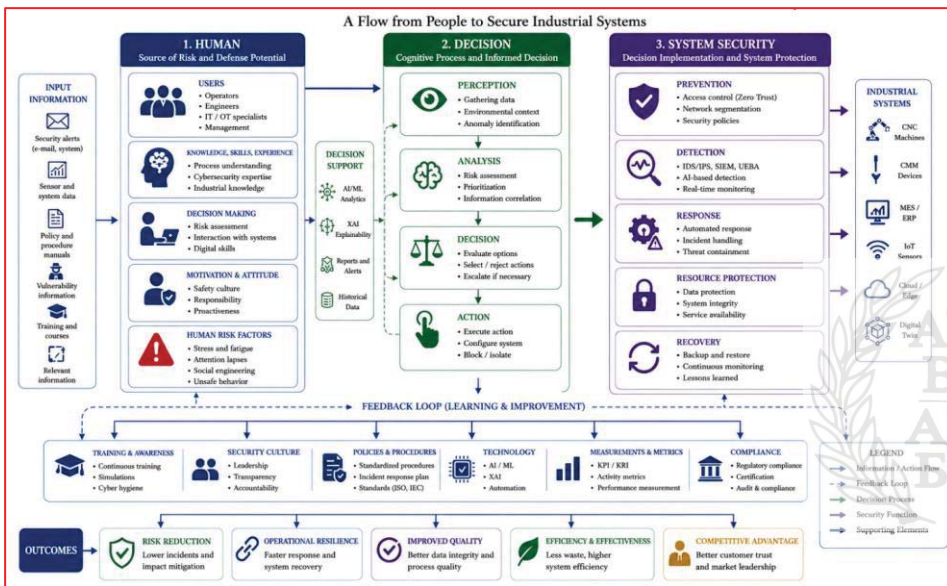


Figure 4. General cyber security model for Industry 5.0

5.2 Digital Security Layer

The digital security layer within Industry 5.0 is based on security solutions, with a focus on: Zero Trust Architecture (ZTA), AI-driven threat detection, application of blockchain for data integrity and security DT [9,22].

Secure DT is a secure version of the digital twin that protects data, validates models, and ensures the integrity of simulations. The key risks of the DT system are data manipulation, non-synchronization between real and digital, AI vulnerabilities and cloud dependence, and security mechanisms are data validation, communication encryption, ZTA and AI monitoring. Industrial application refers to CNC optimization, predictive maintenance and metrology (virtual metrology). The benefits relate to reliable simulations, process optimization and risk reduction. The integrated model of digital security

represents the interaction of technologies: ZTA → access control, AI → threat detection, blockchain → data integrity and DT → intelligent management. Together, these elements form a holistic security system of Industry 5.0. The connection to the CIA triad is reflected in the following facts: ZTA (confidentiality + integrity), AI detection (integrity + availability), blockchain (integrity), and DT (integrity + availability). The Industry 5.0 perspective refers to their basic elements: human at the center (transparent and explainable systems (XAI)), digital model (integration of AI, IoT, DT), and sustainability (energy-efficient security and long-term system resilience). Research challenges in this area relate to the integration of ZTA in industrial systems, AI security and XAI, scalable blockchain systems and DT security in metrology.

Here is a structured table of technology vs features vs benefits vs challenges within the Industry 5.0 digital security layer, Table 5.

Table 5. Technologies vs functions vs advantages vs challenges for Industry 5.0

Technology	Key functions	Advantages	Challenges / limitations
WHAT?	- Continuous authentication and authorization - Network microsegmentation - Identity-based access policies	- Reduced attack surface - Prevention of lateral movement - High level of access control	- Complex implementation - Integration with legacy systems - Latency overhead
AI-guided threat detection	- Anomaly detection - Predictive threat analysis - Behavioral monitoring - Real-time data analysis	- Fast and adaptive detection - Scalability - Security automation	- Data poisoning and adversarial attacks - “Black box” problem - The need for quality data
Blockchain for data integrity	- Immutable ledger - Digital signatures - Data traceability - Smart contracts	- High data integrity - Transparency - Elimination of the need to trust a central entity	- Scalability - Latency - Energy consumption - Complexity of implementation
Safe DT	- Synchronization real ↔ digital - Data validation - Simulation and optimization - Integration of AI models	- Reliable simulations - Process optimization - Predictive maintenance - Reduction of risks and costs	- Depends on the quality of the data - Complex integration - IoT/Cloud security risks - AI vulnerabilities
Explainable AI (XAI)	- Explanation of AI system decisions - Model transparency - Decision-making support	- Increased trust in AI - Better system control - Easier error detection	- Reduced efficiency compared to “black-box” models - Complexity of interpretation
Edge security	- Local data processing and filtering - IoT device protection - Latency reduction	- Real-time security - Reducing dependence on the cloud - Better system resilience	- Limited device resources - Complex management - Physical exposure of the device
Cloud security (CSPM, ZTA Cloud)	- Configuration management - Data encryption - IAM control - Monitoring and auditing	- Scalability - Centralized control - High availability	- Misconfiguration risks - Problem with multiple users - Dependence on the provider

A key research insight can be defined that no technology alone is sufficient, but the greatest value comes from their integration. The conclusion is, ZTA → access control, AI → intelligent detection, blockchain → data trust and DT → optimization and simulation, together form the basis of a secure and intelligent Industry 5.0 system.

5.3 Resilience and Sustainability Layer

In Industry 5.0, cyber security is not only system protection, but the system's ability to survive, adapt and maintain functionality despite attacks and disruptions, and this layer integrates resilience, sustainability, and business continuity, and their basic components are: self-healing systems, redundancy strategies and energy-aware cyber security [8,23].

Self-healing systems are systems that can detect anomalies, automatically react and recover without human intervention, and are inspired by biological systems (digital immune system). The key functions of this model are automatic attack detection (AI/ML), isolation of compromised components, system reconfiguration, and automatic recovery (self-healing). Industrial application refers to CNC systems → automatic stop and correction, IoT networks → isolation of a compromised node, and DT → deviation identification, and the advantages are the minimization of downtime, fast response to incidents and reduction of the need for human intervention. As far as implementation is concerned, there are the following challenges, namely implementation complexity, false positive alarms and dependence on the quality of the AI model. We can conclude that future systems will not only detect attacks, but actively recover.

Redundancy strategies imply the existence of alternative resources that take over the function in case of failure. Today there are several types of redundancies, namely: hardware (double servers and backup CNC controllers), software (automatic redundancy systems, backup applications), and network (alternative communication routes) and data redundancy (backup and data replication). Application in industry is reflected in the following approaches: MES systems with automatic redundancy systems, cloud + edge redundancy, and redundant IoT gateway. The benefits relate to maintaining business continuity, high availability and resistance to failures and attacks. On the other hand, challenges in implementation are related to high costs, complex management and system synchronization. So we can conclude, redundancy is not a luxury, but a basic requirement for system resilience.

Energy-conscious cyber security implies the application of security mechanisms with the optimization of energy consumption. Why is it important? Because Industry 5.0 emphasizes sustainability, on the other hand IoT/Edge devices have limited resources, and AI systems consume significant energy. The key challenges

are related to the application of the following approaches: energy-demanding algorithms (encryption and AI models), security vs. performance compromise (stronger protection → higher consumption), limitations of IoT devices (battery, CPU and memory). Industrial application is realized through the following concepts, namely: edge AI (TinyML), energy-efficient protocols and adaptive encryption. The advantages of these concepts are system sustainability, cost reduction and long-term stability, while the challenges are the compromise between safety and efficiency and the complexity of optimization. An important conclusion is that the future of security is not only "safe", but energetically sustainable.

5.4 Advanced Technologies

Here we have three key technologies: explainable AI (XAI) (increases trust and transparency of AI decisions), quantum-resistant cryptography (protects data from future quantum attacks), and digital immune systems (enable detection, adaptation and self-healing of the system) [7,24,25].

Explainable AI (XAI) stands for AI models and methods that make it possible to understand: why the AI made a certain decision, what data most influenced the result, and whether the decision is reliable, biased or risky. In Industry 5.0, XAI is important, as it connects AI automation with human supervision and trust. XAI functions in cyber security enable: explanation of anomaly detection, transparency of AI decisions in SOC/MES/OT systems, reduction of "black box" problems, better human-AI collaboration, and auditability of decisions for standards and regulation. For example, if the AI system detects unusual network traffic between the IoT gateway and the MES, XAI can indicate that an alarm has been triggered due to unusual access times, increased packet counts, and deviations from the normal device profile. The application in smart manufacturing can be illustrated with examples as in Table 6.

Table 6. Examples of XAI applications in smart manufacturing for cyber security

Area	Application of XAI
AI threat detection	An explanation of why the alarm was triggered
CMM/Metrology	Explanation of suspicious measurement patterns
DT	Understanding the difference between real and digital models
Predictive maintenance	Explanation of failure prediction
Man in the Loop Tracking	Support for the operator in making decisions

What are the advantages of this model? Here they are: increasing trust in AI systems, reducing the risk of wrong decisions, improving operator responsiveness, facilitating audit and compliance, and supporting ethical and responsible AI deployment. There are also possible challenges: explanations can be technically complex, some XAI explanations are not intuitive enough for operators,

transparency can reveal information to an attacker, and sometimes there is a trade-off between model accuracy and explainability. XAI serves not only to explain AI decision, but to enable trust, accountability and control in cyber-physical-human systems.

Quantum-resistant cryptography or post-quantum cryptography includes cryptographic methods that should remain secure in the era of quantum computing. The problem is that quantum computers could threaten classical algorithms such as RSA and ECC, which are widely used today for: digital signatures, certificates, VPN communication, secure industrial protocols and protection of cloud/edge communication. Why is this model important for Industry 5.0? Industrial systems have a long life cycle. CNC, CMM, PLC, SCADA and IoT systems often remain in service for 10–20 years. This means that data protected today may be compromised in the future. A particularly important risk is that “collect now, decrypt later”, the attacker today collects encrypted data and stores it until he has the quantum ability to decrypt. The functions of post-quantum protection are the protection of long-term industrial data, secure digital signatures, secure communication between OT, edge and cloud systems, protection of DT models, and protection of calibration and metrology data, and the application in smart manufacturing is analyzed in Table 7.

Table 7. Examples of XAI applications in quantum-resistant cryptography for cyber security

Area	Application of quantum resistant cryptography
Cloud/Edge communication	Post-quantum TLS / hybrid protocols
DT	Model and simulation data protection
Metrology	Long-term protection of calibration certificates
Supply chains	Secure digital signatures of components
IoT/OT systems	Gradual migration of cryptography

The advantages of this model are long-term confidentiality protection, resistance to future quantum attacks, greater trust in digital certificates, and protection of critical infrastructure. The challenges are larger keys and larger signature data, more demanding implementation on IoT/Edge devices, the need to migrate existing systems, compatibility with legacy equipment and performance in real-time systems. Post-quantum cryptography is not only a future need, but a strategic requirement for systems that must remain reliable for decades.

The digital immune system is a cyber security concept inspired by biological immunity. The system continuously monitors its own state, detects abnormalities, reacts to threats and learns from incidents. In Industry 5.0, this means that the manufacturing system is not only protected, but can also self-monitor, self-adapt, self-isolate and self-heal. Key functions are: anomaly detection (recognition of deviations in the network, devices and data), self-isolation (separation of the compromised component), self-recovery (returning the system to a stable state),

adaptive learning (learning from previous incidents), and continuous monitoring (continuous monitoring of the system).

Application in smart manufacturing of this model refers to: IoT networks, CNC machines, CMM systems, DT platforms, MES/ERP systems, cloud/edge infrastructure. For example, if an IoT sensor sends abnormal data, the digital immune system can automatically isolate the sensor, activate a redundant sensor, notify the operator, and update the detection rules. The advantages of this model are faster response to attacks, reduced downtime, greater manufacturing resilience, reduction of the need for manual intervention, and continuous improvement of security, while the challenges are complex integration with OT systems, the risk of wrong automatic response, the need for quality data, the dependence on AI models and the need for clear rules when a human must take control. The digital immune system represents a transition from passive protection to active, adaptive and self-healing security.

An integrated model of advanced technologies can be one, perhaps, the best solution, where a part of the solution is taken from each of them, namely: XAI (explains and validates AI decisions), post-quantum cryptography (protects data and communication in the long term), digital immune system (detects, reacts and recovers the system), creating an integrated flow of threat detection → XAI explanation → human/AI decision → isolation → recovery → learning → long-term data protection.

6. Proposed Conceptual Framework of Industry 5.0 Cyber Security Architecture

Cyber-security architecture for Industry 5.0 should be a multi-layered, adaptive and human-oriented system, in which security is not only seen as technical protection, but as an integration of people, digital technologies, physical manufacturing, risk management and sustainability. The basic logic of Industry 5.0 is based on three principles: man at the center, sustainability and resilience, i.e. on a human-oriented, sustainable and resilient industry. The layers of cyber-security architectures for Industry 5.0 are [2,3,5,26]: human layer, cyber security and intelligence layer, digital infrastructure layer, physical manufacturing layer and sustainability layer.

Human layer represents the most important element of the Industry 5.0 cybersecurity architecture, as operators, engineers, quality managers, metrology and IT/OT teams become active participants in system protection. In traditional Industry 4.0, humans were often viewed as a potential weakness, while in Industry 5.0, humans are treated as a critical carrier of security intelligence. In this layer, key functions are: employee training, cyber-awareness development, human-in-the-loop monitoring, ethical use of AI systems, and decision-making in crisis situations. When an AI safety mechanism detects an anomaly, humans as experts

must not be completely excluded from the process, especially if the decision involves stopping the manufacturing line, discarding measurement results or isolating the CMM/CNC system. The role of key components is: AI security engine analyzes user behavior, unauthorized access attempts, unusual commands and operator work patterns. The risk management system assesses human risks: insufficient training, operator errors, phishing attacks, insider threats and unclear responsibilities. The blockchain layer can record who approved the parameter change, who validated the measurement, and who accessed critical data. The DT security module enables the simulation of human decisions in crisis scenarios without endangering the real system, figure 5.

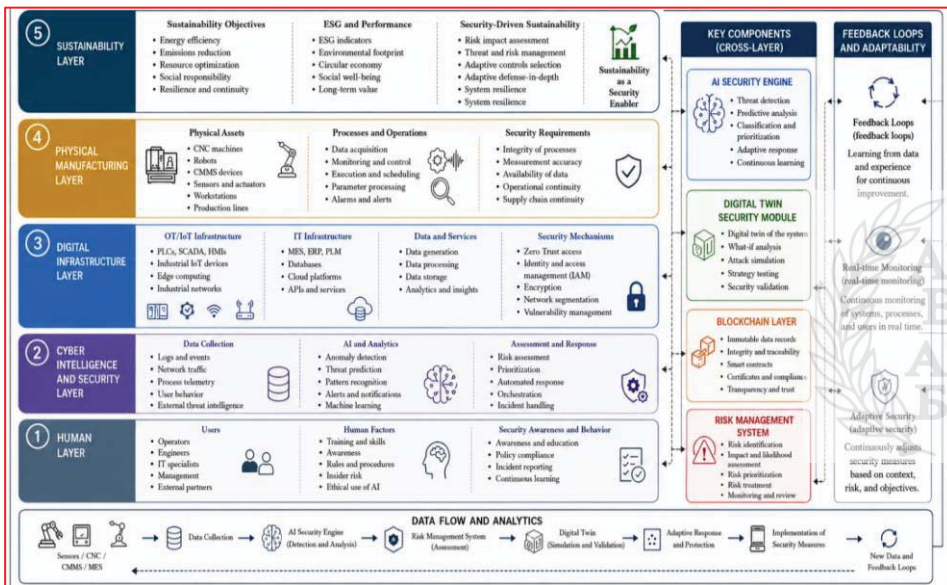


Figure 5. Proposed conceptual model of Industry 5.0 cyber security architecture with adaptive security layers, components and mechanisms

The cybersecurity intelligence layer is the central analytical layer of the architecture. Its role is to collect data from all parts of the system, analyze it using AI/ML algorithms and propose or automatically activate security measures. This layer connects real-time monitoring, predictive analytics, anomaly detection, risk assessment and adaptive response. This layer emphasizes the management of cyber risk through functions such as manage, identify, protect, detect, respond and recover, which is very suitable for mapping to this layer. The main functions of this layer are real-time threat detection, risk classification, attack prediction, correlation of events from IT and OT systems, automatic initiation of response and continuous learning from previous incidents. The role of key components is:

The AI security mechanism is the core of this layer. It detects anomalies in network traffic, manufacturing parameters, measurement results, logs and user behavior. The risk management system translates technical anomalies into business and manufacturing risks: downtime, loss of quality, compromise of measurement data or a security incident. The DT security module allows the response to be tested before it is applied to the physical system. The blockchain layer provides an immutable record of incidents, decisions and security events.

The digital infrastructure layer includes IoT/IIoT devices, edge and cloud platforms, MES, ERP, SCADA, DT, databases, API communication and industrial networks. This is the layer with the largest attack surface, because it connects the manufacturing system with analytics, suppliers, users and external services. In smart manufacturing, this layer must support ZTA, encryption, network segmentation, identity control, secure data exchange, and continuous access verification. The role of the key components is: AI security mechanism monitors network traffic, API requests, access to cloud platforms and anomalies in communication. The risk management system ranks risks according to the impact on manufacturing, quality, human safety and business continuity. The security module DT checks whether the digital model behaves in accordance with the physical system. If there is a difference between the actual CNC/CMM process and its DT, the system can flag a potential manipulation. The blockchain layer ensures data integrity, especially for measurements, calibration, certificates, parameter changes and quality records.

Physical layer includes CNC machines, robots, CMM devices, sensors, manufacturing lines, tools, measuring stations and control systems. In this layer, a cyber attack can have direct physical consequences: incorrect processing, tool damage, false measurement results, line downtime or endangering worker safety. The aspect of smart metrology is particularly important. If an attacker changes the measurement results or calibration data, the product may be mistakenly accepted as compliant. Therefore, cyber-security in Industry 5.0 must protect not only IT data, but also the physical-technical reliability of manufacturing and measurement. The role of the key components is: The AI safety mechanism detects unusual vibrations, changes in processing, deviations in measurements, unusual commands and parameter changes. The risk management system decides whether the risk is local, systemic or critical. The safety module DT compares the actual behavior of the machine with the expected model.

The sustainability layer extends cyber security beyond traditional data protection. In Industry 5.0, the security decision must take into account energy, resources, emissions, waste, manufacturing continuity and social responsibility. This means that cyber-security must be linked to ESG indicators, energy efficiency and system resilience. For example, an adaptive security system does not always need to shut down the entire manufacturing line. In some cases, it is better to isolate only the compromised segment, shift the load to a spare cell, or activate an energy-

efficient operating mode. This approach is in line with the Industry 5.0 idea that industry should contribute to sustainability, resilience and people's well-being.

8. Future Directions of Development

The evolution of Industry 5.0 in the field of cyber-security marks the transition from technologically oriented systems to human-centric, ethical and reliable security ecosystems. In this context, the focus is no longer only on the protection of infrastructure and data, but on the synergy between humans and AI, as well as on the development of ethical and transparent AI systems that inspire trust [2,27-30]. Key elements of this evolution are: human-AI collaboration in cyber-security and ethical and reliable AI systems.

The cooperation of man and artificial intelligence in cyber-security is the basis of Industry 5.0, where AI systems do not replace humans, but act as intelligent assistants that support decision-making. In cyber security, this means: AI detects threats and suggests actions, a human analyzes the context and makes the final decision, and the system continuously learns from the interaction. This approach is called the "man-in-the-loop" or more advanced "man-in-the-loop" model. Key features are: increased situational awareness - AI analyzes large amounts of data and provides an overview of the situation in real time, decision support - AI suggests multiple response scenarios (eg system isolation, parameter change, alert), adaptive collaboration - the system adapts to the operator's level of expertise, and learning from interaction - every human decision improves AI models. An application in smart manufacturing is an operator validates AI anomaly detection in CNC/CMM systems, a quality engineer decides if a deviation is critical, an IT/OT expert manages cyber incidents with AI support, and management uses AI reports for strategic decisions. The advantages of this concept are the reduction of decision errors, faster response to threats, better interpretation of complex data, and increased trust in AI systems. Challenges are too much dependence on AI, insufficient user training, conflict between AI recommendations and human intuition, and the need to clearly define responsibilities.

Ethical and reliable AI systems tell us that in Industry 5.0, AI systems must be not only efficient, but also transparent, fair, accountable, secure, and compliant with regulations and standards. This leads to the concept of "trusted AI", where users have confidence in the system's decisions. The key principles are: transparency (explainable - XAI), where AI must explain: why the threat was detected, based on which data, and what are the key decision factors. For example, the system explains that an anomaly was detected due to a combination of vibration, temperature and measurement deviation; fairness - AI systems must not be biased: towards users, towards processes, and towards types of data; accountability, where it must be clear who is responsible for AI System decisions, how decisions are

audited, and how errors are resolved; security, where AI systems must be protected from external attacks, data manipulation and model poisoning attacks; privacy, where it is particularly important in the context of human data, operator behavior and industrial secrets. Application in Industry 5.0 systems is XAI for explaining decisions in quality control, transparent models for predictive maintenance, audit trail (eg blockchain) for AI system decisions, and ethical framework for decision-making in crisis situations. The advantages are increased user confidence, easier implementation in the industry, regulatory compliance (EU AI Act, ISO standards), and reduced risk of wrong decisions. The challenges are the compromise between performance and transparency, the complexity of implementing the XAI model, the lack of standards in practice, and the need for a multidisciplinary approach. Within Industry 5.0, these two concepts are interconnected: AI detects the threat, the system explains the decision (XAI), the human makes the decision, the system records and learns from the decision, and reacts faster and more precisely the next time. This cycle forms a smart, adaptive and ethical security loop.

10. Conclusions

Cyber security is a key enabler of Industry 5.0, so this fact defines the paradigm for an integrated approach to human-digital sustainability, as human-digital technologies-sustainability. This integrated approach represents the essence of the evolution towards Industry 5.0 and the key framework for the development of modern smart manufacturing systems. This approach goes beyond traditional models focused solely on automation and efficiency, introducing a balance between technological progress, human role and sustainable development. The synergy of three key dimensions is realized through: *human dimension* - man becomes the central element of the system, not only as an operator, but as a decision maker, creator of innovations, supervisor of AI systems, and guarantor of ethics and responsibility. The role of man is being transformed from passive to active and strategic, with the support of intelligent systems. *Digital dimension*, where we have that digital technologies represent the driving force of the system, as they include AI and machine learning, DT, IoT and edge/cloud computing, as well as cyber-security platforms. These technologies enable real-time data analysis, predictive decision-making, and adaptive process management. The third dimension is *sustainability*, which introduces a new value dimension: optimization of resources and energy, reduction of waste and emissions, social responsibility, and ESG integration. Cyber-security in this context contributes to preserving the stability and long-term sustainability of the system. Integration through a closed loop is a key feature of this approach, as a closed, adaptive and intelligent loop, through the activities of data collection (IoT, CNC, CMM, systems), digital analysis (AI, DT), risk and performance assessment, human

validation of decisions, implementation of actions, and continuous learning and improvement. This cycle enables quick reaction to changes, continuous optimization of the system, and increase in reliability and quality. The key advantages of an integrated approach are: increased trust (transparent decisions, data traceability, and system security), greater resilience (adaptive reaction to disturbances, predictive risk management, and self-healing systems), sustainable development (reduction of energy consumption, process optimization, and waste reduction), quality improvement (integrated metrology, real-time control, and reliable measurement data). Better decision-making through AI support, human validation, and contextual understanding. Although it brings numerous advantages, this approach faces challenges, such as the complexity of system integration, the need for new skills and education, high initial costs, cyber-security risks, and lack of standardization. The strategic importance for Industry 5.0 is also reflected in the fact that the integrated approach is the foundation for the development of intelligent factories, digital transformation of the industry, improvement of global supply chains, implementation of ESG principles, and connection of technology and society. The integration of people, digital technologies and sustainability is not only a technological trend, but a new industrial philosophy.

Safe, resilient and human-oriented manufacturing systems define the future of Industry 5.0, because it represents the essence of the transformation of modern industry towards the Industry 5.0 model. She indicates that future manufacturing systems will not be defined only by the degree of automation or digitization, but above all by the quality of their safety, resilience and ability to integrate humans as the central element of the system.

Safety is becoming the foundation of every modern factory. In Industry 5.0, security is no longer just the protection of IT infrastructure, but includes: protection of manufacturing processes (CNC, robotics, CMM systems), integrity of measurement and metrology data, protection of DT and AI models, secure communication in the IoT and cloud environment, and protection against cyber attacks (ransomware, data manipulation, insider threats). Secure systems enable confidence in data and decisions, manufacturing stability, intellectual property protection, and business continuity. In this sense, cyber security becomes a strategic enabler, not just a technical function.

Resilient systems have the ability to recognize disruptions, react to them in real time, continue operations with minimal losses, and learn from previous incidents. Resilience is not only a technical characteristic, but also the organizational and strategic ability of the system to adapt to changes and crises, figure 6. One of the most important differences between Industry 4.0 and 5.0 is the return of man to the center of the system. In Industry 5.0, humans make key decisions, AI serves as a support, not a replacement, human-machine cooperation is developed, and the emphasis is on safety, well-being and employee education. Applying this

paradigm means that companies must invest in cyber security, develop AI and digital technologies, train employees, implement ESG principles, and establish integrated management systems.

Industry 5.0 is not just a technological revolution, but a transformation towards intelligent, safe, resilient and human-friendly systems that create long-term value for society and the economy.

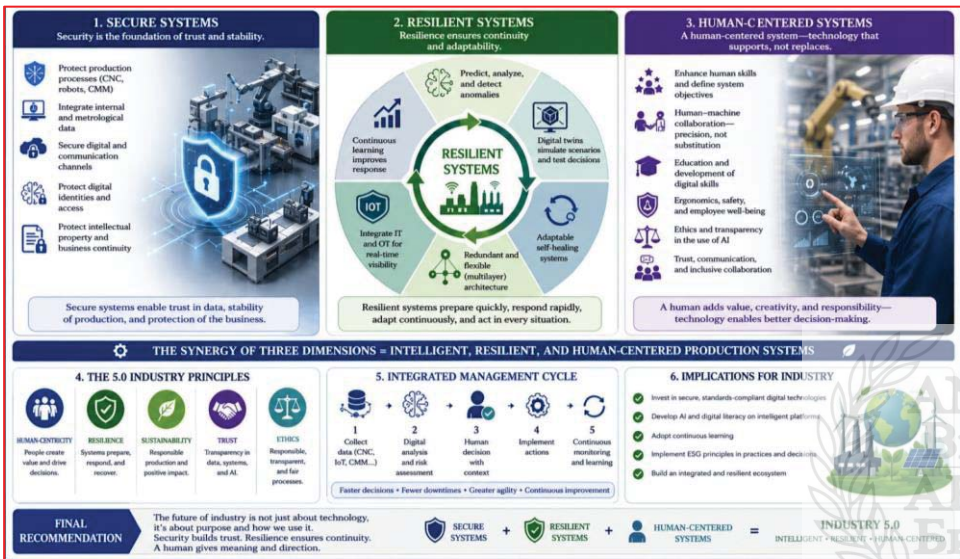


Figure 6. Safe, resilient and human-centered manufacturing systems define the future of Industry 5.0

References

- [1] European Commission: Directorate-General for Research and Innovation, Industry 5.0 – Towards a sustainable, human-centric and resilient European industry, Publications Office of the European Union, 2021, <https://data.europa.eu/doi/10.2777/308407> .
- [2] Kour R, et al. (2024) Cybersecurity for Industry 5.0: trends and gaps. *Front. Comput. Sci.* 6:1434436. 10.3389/fcomp.2024.1434436.
- [3] B. Santos, et al, Cybersecurity in Industry 5.0: Open challenges and future directions, *Proc. PST*, 2024. <https://doi.org/10.1109/PST62714.2024.10788065> .
- [4] A. Chaudhuri, et al, Factors impacting cybersecurity transformation: An Industry 5.0 perspective, *Computers & Security*, 2025. <https://doi.org/10.1016/j.cose.2024.104267> .

- [5] MH Rahman, T. Wuest, M. Shafae, Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies, *Journal of Manufacturing Systems*, Volume 68, 2023, Pages 196-208, ISSN 0278-6125, <https://doi.org/10.1016/j.jmsy.2023.03.009> .
- [6] Antipenko V., Matulevičius R. (2026). Function-driven cyber-physical security in smart manufacturing. *Software and Systems Modeling*. <https://doi.org/10.1007/s10270-026-01370-0> .
- [7] N. Khan et al., Explainable AI-based intrusion detection system for Industry 5.0, *arXiv*, 2024. 10.48550/arXiv.2408.03335.
- [8] Mario R., et al. (2024) Lack of verified Inclusive Technology for Workers with disabilities in industry 4.0: a systematic review, *International Journal of Sustainable Engineering*, 17:1, 190-210, 10.1080/19397038.2024.2328711.
- [9] Leirimo, T. (2024). Digital Twins for Industry 5.0: Unlocking the Human Potential. *Proceeding CIRP*. 130. 761–766. 10.1016/j.procir.2024.10.161.
- [10] Whaiduzzaman, M., et al. (2026). Enhancing IIoT Security Using Digital Twins in Industry 5.0 : A Systematic Literature Review. *Information*, 17 (2), 209. <https://doi.org/10.3390/info17020209> .
- [11] Rose Scott, ET AL. (2020). Zero Trust Architecture. 10.6028/NIST.SP.800-207-draft2.
- [12] K. Stouffer, *Cybersecurity for Manufacturing Systems*, NIST, 2020, <https://www.din.de/resource/blob/271310/5d3b71d57a0bd7a7349cf81b89df9787/07-smart-manufacturing-keith-stouffer-data.pdf> .
- [13] Barrett, M. (2018), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, NIST Cybersecurity Framework, <https://doi.org/10.6028/NIST.CSWP.04162018> .
- [14] Leng, J., et al. (2022). Secure Blockchain middleware for decentralized IIoT towards industry 5.0: a review of architecture, enablers, challenges, and directions. *Mach. Des.* 10:858. doi: 10.3390/machines10100858.
- [15] Sailio M, Latvala OM, Szanto A. Cyber threat actors for the factory of the future. *Appl Sci* 2020;10:4334. <https://doi.org/10.3390/app10124334> .
- [16] Rahat M., 2024, *Cyber Security in Smart Manufacturing (Threats, Landscapes & Challenges)*, *arXiv:2304.10180*. <https://doi.org/10.48550/arXiv.2304.10180> .
- [17] Souza J., et al. (2021). The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review. *European Journal of Business and Management Research*. 6. 188-194. 10.24018/ejbmr.2021.6.6.1173.
- [18] Humayed, AA, et al. (2018). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 4, 1802-1831. 10.1109/JIOT.2017.2703172 .

- [19] Williams B, Soulet M, Siraj A. A Taxonomy of Cyber Attacks in Smart Manufacturing Systems. 6th EAI Int. Conf. Manag. Manuf. Syst., Springer; 2023, p. 77–97. https://doi.org/10.1007/978-3-030-96314-9_6.
- [20] Kott, Alexander. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. 10.1007/978-3-319-77492-3_1.
- [21] Elhabashy AE, Wells LJ, Camelio JA. Cyber-physical attack vulnerabilities in manufacturing quality control tools. Qual Eng 2020;32:676–92. <https://doi.org/10.1080/08982112.2020.1737115>.
- [22] Bharti Anupriya, Hazela Bramah, (2024). Enhancing Cybersecurity in Smart Manufacturing: A Comprehensive Approach. Indian Journal of Computer Science and Technology. 192-201. 10.59256/indjst.20240302030.
- [23] Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, <https://doi.org/10.6028/NIST.CSWP.04162018>.
- [24] Bakkar, MN (2023). CyberSecurity essentials for industry 5.0, in Advanced Research and Real-World Applications of Industry 5.0, (IGI Global), pp. 49–65. 10.4018/978-1-7998-8805-5.ch003.
- [25] Alagic G, et al. (2025) Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Internal Report (IR) NIST IR 8545. <https://doi.org/10.6028/NIST.IR.8545>.
- [26] S. Sicari, et al. Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, Volume 76, 2019, Pages 146-164, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2014.11.008>.
- [27] Abraham, D., et al. Towards enhanced cybersecurity in industrial control systems: a systematic review of context-based modeling, digital twins, and machine learning approaches. Int. J. Inf. Secur. 24, 243 (2025). <https://doi.org/10.1007/s10207-025-01158-1>.
- [28] Deloitte, 2026, Cybersecurity for smart factories, <https://www.deloitte.com/us/en/industries/energy/articles/smart-factory-cybersecurity-manufacturing-industry.html>.
- [29] Ren, Anqi, et al. Cyber Security in Smart Manufacturing: Survey and Challenges Cyber Security in Smart Manufacturing: Survey and Challenges, IISE Annual Conference. Proceedings; Norcross (2019): 716-721.
- [30] Bahrami, AH, Rouzbahani, HM (2021). Cyber Security of Smart Manufacturing Execution Systems: A Bibliometric Analysis. In: Karimipour, H., Derakhshan, F. (eds) AI-Enabled Threat Detection and Security Analysis for Industrial IoT. Springer, Cham. https://doi.org/10.1007/978-3-030-76613-9_6.
- [31] Capgemini Research Institute (2026). Smart & Secure: Why smart factories need to prioritize cybersecurity. https://prod.ucwe.capgemini.com/wp-content/uploads/2022/06/Cybersecurity-in-Smart-Factories_Web-2.pdf.