CEUR-WS.org/Vol-3970/SHORT3.pdf

AI-Enhanced Software Architecture Assessment for Cyber-Resilient Industrial Automation Systems*

Roman Feniak[1,†], Yaroslav Vyklyuk[2,†]

[1] *Lviv Polytechnic National University, Lviv, Ukraine*
[2] *Lviv Polytechnic National University, Lviv, Ukraine*

Abstract

The rise in Artificial Intelligence, IIoT, and automation adoption in industrial systems adds greater efficiency and benefits for organizations but also brings enormous cybersecurity risks. Legacy security cannot defend against the new breed of cyber attacks — ransomware, adversarial AI, and supply chain attacks. This paper introduces an AI-enhanced software architecture assessment and design approach where advanced threat recognition, automated vulnerability, risk assessment, and security-by-design are combined to mitigate cyber resilience risk better. This solution will improve industrial security, reduce attack surface exposure, and improve automation resilience..

Keywords

AI-enhanced software architecture, industrial cybersecurity, cyber resilience

1. Introduction

In recent years, industrial systems and smart manufacturing have been rapidly transformed due to Industry 4.0, automation, artificial intelligence, and the Internet of Things technologies. Today, industries have a rapid yet sophisticated digitization process alongside facilities that have enabled real-time monitoring, predictive analytics, and autonomous decision-making to improve operational efficiency, trim costs, and enhance product quality [1].

Here are the key technological developments of smart manufacturing:

- Industrial Internet of Things (IIoT): Enabling sensors, machines, and devices to connect and form an interconnected digital space for real-time analytics and data collection
- Cyber-Physical Systems (CPS): Connecting software and industrial hardware to create intelligent automation and self-adaptive production systems
- Edge and Cloud Computing: Processing industrial data either at the edge (near the production line) or in the cloud for optimized performance and decision-making
- Artificial Intelligence (AI) and Machine Learning (ML): AI-based analytics enable predicting failures, optimizing operations, and automating industrial control processes

These innovations enable industries to progress towards autonomous manufacturing (interconnected self-optimizing machines in conjunction with self-optimizing processes), wherein AI-empowered analytics incessantly enhance productivity. However, the growing interconnectivity of industrial systems brings substantial cybersecurity and safety challenges.

[1*] 2nd International Conference on Smart Automation & Robotics for Future Industry, April 03 -05, 2025, Lviv, Ukraine 1* Corresponding author. † These authors contributed equally.
[†] These authors contributed equally.

roman.y.feniak@lpnu.ua (R. Feniak); yaroslav.i.vykliuk@lpnu.ua (Y. Vykliuk)
0009-0002-4084-0613 (R. Feniak); 0000-0003-4766-4659 (Y. Vykliuk)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

2. Cybersecurity and Safety Challenges in Industrial Systems

As industrial systems become more digitized and connected, cybersecurity and safety challenges become more complex. New vulnerabilities are introduced by the continued growth of industrial automation, IIoT, smart manufacturing, and cloud-based industrial control systems, which existing traditional security measures are unable to address. Cybersecurity is increasingly a key focus and priority topic for modern industrial ecosystems, as one cyber attack can result in enormous economic losses, production and operation failures, loss of safety, or even threat to the environment.

2.1. Increasing Complexity and Expanding Attack Surface

The use of the Industrial Internet of Things, cyber-physical systems, AI-enabled robotics, and cloud-based manufacturing execution systems has created a complex digital landscape. These technologies improve productivity but also greatly expand the attack surface of industrial networks. Unlike industrial control systems, traditional IT infrastructure is not designed for operational reliability. As a result, if an attacker infiltrates a single component, they can quickly spread across the network, affecting multiple production lines or an entire supply chain.

One of the most critical issues is that systems are connected without unified security policies. Most industrial facilities have different security frameworks for various plants, vendors, and software platforms. Such fragmentation results in inconsistency in security implementations and thus leaves room for attackers to exploit vulnerabilities. Additionally, IIoT devices tend to ship with very little embedded security, simple soft-based firmware, weak authentication, low encryption levels, etc. Compromised devices become entry points for attackers, providing access to critical control systems and disrupting industrial operations.

Another challenge comes from legacy systems. Many industries run ICS software that is decades old and that was never built to withstand today's cyber threats. These systems typically use legacy communication protocols without encryption, making them easily targetable by man-in-the-middle (MITM) eavesdropping and command injection attacks. Its ongoing use means industrial environments are increasingly vulnerable to cyberattacks that can exploit weaknesses at every level of the operational technology stack.

2.2. Rise in Sophisticated Cyber Threats Against Industrial Systems

An increasing number of targeted cyberattacks aimed at disrupting operations, stealing intellectual property, or causing financial impact have become a fact of life in the industrial sector. One of the most dangerous threats is a type of computer sabotage known as a ransomware attack, which effectively locks up critical control systems, often commanding ransom payments to restore access. High-profile incidents like the Colonial Pipeline attack and Norsk Hydro cyberattack have shown that ransomware can paralyze whole manufacturing processes, resulting in millions of dollars in loss.

APTs (advanced persistent threats) and nation-state-level cyberattacks add another layer of complexity to industrial cybersecurity [2]. Such highly coordinated attacks are typically conducted by state-sponsored groups that are attempting to dislocate critical infrastructure. Examples include Stuxnet, which targeted Iranian nuclear facilities; Industroyer, which attacked Ukraine's power grid; and Triton, which attacked industrial safety systems. Zero-day vulnerabilities in industrial software are leveraged by APT groups to silently embed themselves in target networks for months before weakening an organization with a devastating attack.

Data manipulation and supply chain attacks are also becoming more established, where attackers change sensor readings or interfere with IIoT systems to promptly create defective or unsafe products that are hard to detect. By breaching industrial software vendors, they can insert backdoors and malware into legitimate software updates, like in the case of the SolarWinds supply chain attack. Most of these techniques help attackers circumvent classic security protections, evading detection and mitigation of threats by industrial organizations before they have a chance of causing damage.

As one of the more emergent threats, cyberattacks powered by artificial intelligence involve adversaries who use machine learning to bypass detection and modify attack strategies in real-time. For example, AI models used for predictive maintenance and process optimization can be attacked: the attacker can submit requests to the predictive maintenance or process optimization model for the model to make incorrect predictions. This will break the industrial workflow. This idea, which is referred to as adversarial AI, enables hackers to deliberately twist input data to deceive AI-based security systems, thereby leaving industrial automation systems vulnerable to stealthy cyberattacks.

2.3. Safety Risks in Automated Industrial Environments

Cybersecurity breaches within industrial environments do more than leak data—dangerous, real-world safety implications abound [3]. Systems in industrial automation can malfunction dangerously, putting workers, machines, and the environment at risk. One of the most alarming threats is the malicious takeover of industrial robots and autonomous systems. Examples of robots that perform such functions include industrial robots and Autonomous Guided Vehicles (AGVs), which require real-time sensor data to navigate and carry out their tasks safely and efficiently. If attackers were to manipulate these inputs, robots could be induced to take actions that are not safe — leading to collisions, equipment damage, and injuries to human operators.

Factories and power plants, including process control systems (PCS), are also prime targets of cyber threats. Changing chemical processing parameters without authority could lead to explosions, toxic leaks, or structural failures. Likewise, cybercriminals who tamper with automated machinery settings can produce defective product batches, which can cause financial loss and reputational harm.

Industrial espionage and theft of trade secrets is a huge issue as well. Hackers can penetrate AI-supported predictive maintenance solutions to gain production information and proprietary algorithms. Intellectual property theft — classified information, proprietary data, and technologies — is especially damaging in semiconductors, aerospace, pharmaceuticals, and automotive manufacturing sectors, where competitive advantage is raced on the cutting edge of technological innovation and process optimization.

AI-powered anomaly detection systems have integrated act as vital for protecting ICS (Industrial Control Systems) from being compromised by cyber threats. These systems use machine learning algorithms to learn a baseline of normal network behavior, allowing them to spot deviations that could indicate a potential security incident [7]. AI-powered anomaly detection systems can perform a deep-dive analysis on the network activity in real-time and can be easily updated to accommodate new developments, therefore getting a step ahead of even sometimes stealthy threats and ensuring that even the slightest anomalies are reported [7]. This preemptive action is critical for the effortless execution of operations and shielding vital infrastructure against cyberattacks.

However, deploying AI-based anomaly detection in industrial settings is not without its challenges, including the requirements of vast datasets to train accurate models and the inherent complexity of deciphering alerts generated by AI. The challenges to the implementation of these technologies can necessitate the use of several techniques from the cybersecurity domain, such as training data and model decision analysis (TE) and ML algorithms to address complex challenges and collaborate with established security measures AIA to boost detection capabilities, allowing to develop an ongoing feedback loop for the AI systems. A comprehensive approach like this bolsters the overall cyber resilience of industrial practices.

2.4. The Need for AI-Driven Cybersecurity in Industrial Software Architecture

Many industrial organizations rely on outdated perimeter security measures that cannot withstand modern attacks despite the increasing sophistication of cyber threats. Firewalls and VPNs are great, but they won't protect against insider attacks or lateral movement after an attacker has compromised the network. As cyber threats continue to evolve at a breakneck pace, AI-powered cybersecurity capabilities should be built at the center of any modern industrial software architecture. Accordingly, security frameworks for industrial systems need to build upon and seamlessly blend elements of real-time threat monitoring, automated response actions, and adaptive risk management. AI-driven cybersecurity can:

- Continuously monitor industrial networks and detect threats to minimize the risk of operation interruption
- Automate the response to threats, allowing security systems to contain and minimize attacks autonomously without human intervention
- Automatically adjust security policies in real time according to AI systems' intelligent risk calculations

A Zero Trust Architecture (ZTA) is now employed in industrial systems as an essential strategy for well-ahead cybersecurity. ZTA uses the concept of never trust, constantly verifying and authenticating, and authorizing every user, device, and application trying to gain access to resources. The combination of AI and Zero Trust provides an additional level of security that will help organizations manage the complexity of today's threat landscape [9]. Data processing in a scalable manner is one of the key features of AI, and by identifying patterns, it helps in the automation of plenty of processes in the security domain, which contributes towards making detection and response much quicker and smarter.

As a response to these cybersecurity challenges, software architectures powered by LLMs, Reinforcement Learning, and Retrieval-Augmented Generation have also been developed that can be used to proactively protect industrial systems. The following section describes how an AI-driven cybersecurity solution can be embedded into the industrial software design to create a cyber-resilient automation environment able to sustain modern cyber threats.

3. AI-Enhanced Software Architecture for Cyber Resilience

As industrial systems grow increasingly complex and intertwined, a continuous and systematic assessment of software architectures is required to sustain cybersecurity resilience. Conventional security methodologies depend on static, rule-based techniques that cannot match the ever-changing cyber threats. In addition, security audits and architectural enhancements are usually reactive measures undertaken once vulnerabilities have been exploited.

A better alternative would be to use Generative AI for an iterative cybersecurity review of the software architecture. AI-powered tools analyze current industrial software architectures and detect known weaknesses, offering recommendations for fortifying security. This is not a one-off exercise but a regular periodic refresh process designed to keep industrial environments evolving, enabling them to adapt and remain resilient/pervasive against evolving threats. Moreover, extending the same concept to shaping novel cyberspace resilient software architecture for industrial systems from the ground up will enhance its security consideration.

3.1. AI-Assisted Cybersecurity Assessment and Risk Identification

Industrial networks and automation systems produce considerable amounts of operational data, so manually reviewing this data is often slow and error-prone. Data-driven, AI-assisted assessment [5] can methodically analyze software architectures, identify high-risk areas, and suggest mitigation strategies rooted in historical cyberattack data, industry best practices, and security frameworks, including NIST, IEC 62443, and ISO/IEC 27001.

Ineffective security assessments in industrial settings traditionally depend on periodic manual audits that frequently overlook new dangers. In this paper, we propose an AI-driven, iterative architecture security assessment framework that not only identifies security vulnerabilities but also provides architectural refactoring recommendations to ameliorate risks before they materialize. In contrast to traditional risk assessment techniques centered around compliance verification, the proposed method provides a more adaptive and scalable solution for industrial systems by combining machine learning-based threat detection with automated architectural recommendations.

In addition, this study improves the cybersecurity review by using the data generated from a meta-cell process and conducting risk analysis using the patterns before determining the actions to be taken to be an effective preventive strategy rather than just looking at a particular IT system. This AI-based continuous evaluation framework can be an embedded feature in software architecture that offers dynamic security self-adjustment capabilities to industrial organizations without affecting the operational environments, which is a significant advantage of the discussed AR against traditional static security architectures.

Some of the main benefits of AI-powered cybersecurity assessments are the following:

- Automated Risk Detection: AI models analyze system settings, software dependencies, and access rights to find vulnerabilities attackers could exploit
- Pattern Recognition for Threat Identification: AI can help identify common threats based on patterns and identify vulnerabilities throughout various industrial environments by analyzing data from previous cyber incidents
- Ongoing Architecture Review: AI can constantly monitor software architecture to ensure security practices stay relevant within the threat landscape

3.2. Using Generative AI to Design Cyber-Resilient Architectures

Generative AI can assess existing software and help create security-by-design principles for new industrial architectures. With AI-powered architecture modeling [6], organizations can seamlessly introduce cybersecurity best practices into new industrial control systems, IoT frameworks, and smart factory solutions.

This research finally introduces a Generative AI-driven approach that integrates security-first design principles directly into the software architecture, while existing cybersecurity frameworks focus on patch-based security upgrades. In contrast to reactive approaches that aim to patch holes after they occur, the proposed approach instills cybersecurity from the ground up by embedding mitigation policies in the architecture design (zero-trust access control, encrypted data at rest, etc.), as well as leveraging runtime AI for compliance verification and runtime enforcement.

This approach supports the context-specific automatic generation of security architecture, reducing the dependency on conventional manual security attributions through RAG and Reinforcement Learning. This solution's innovation is to test and validate potential cyberattacks through the digital twin AI simulation environment for the industrial system even before it is deployed, thus eliminating the attack surface before it is deployed.

Essential Advantages of AI combined with architecture design:

- Threat-Aware Architecture Planning: Using AI for crafting secure-by-default software architectures, employs holistic security ideas (Zero-Trust models, encryption best practices)
- Automated Security Policy Integration: AI can embed regulatory compliance early into the architecture by mapping the compliance requirements directly into the architecture
- Simulation and Validation: AI can simulate appropriate cyberattacks in a controlled environment on newly designed architectures. This allows organizations to preemptively test and harden security measures before deploying them into the wild

For example, a blueprint for a new IIoT-based industrial monitoring system that is generated by an AI request might guarantee that:

- All IIoT devices also employ encrypted communication protocols to protect against data interception
- Access controls are based on least-privilege principles to minimize exposure to insider threats
- It isolates potentially malicious traffic with network segmentation strategies

Industrial organizations will then be able to build secure systems based on the generated architecture rather than applying patches and fixes after the systems are deployed.

3.3. Scaling AI-Assisted Security Reviews Across Large Industrial Environments

Most industrial companies run multiple plants, each with heterogeneous software architectures, so manual security assessment efforts are impractical at scale. Organizations conduct security reviews through several distributed environments simultaneously.

This research is not simply about incrementally improving security using an AI technique; it offers a holistic methodology of design that recursively enhances industrial cyber security at the architectural level. Distinct from traditional approaches, which primarily provide retrospective risk mitigation, this study's AI-augmented architecture evaluation methodology underpins continuous, adaptive security improvements across the entire lifecycle of an industrial architecture.

This research introduces a new approach to industrial software design — one that proactively mitigates vulnerabilities before they can be exploited, rather than responding to exploit incidents after damage occurs — by coupling AI-based risk detection with Generative AI-based architecture optimization and large-scale security automation.

- Cross-Enterprise Security Benchmarking: In a federated approach, AI benchmarks systems within an enterprise portfolio, revealing security weak points and inconsistencies
- Automated Compliance Audits: AI continuously reviews whether each facility's software architecture complies with industry security standards, identifying systems that fall out of compliance for remediation
- Risk Prioritization for Resource Allocation: AI assigns risk scores to vulnerabilities based on their severity and business impact, enabling security teams to prioritize and address the most critical threats first

An industrial company, for example, that owns five manufacturing plants might find that, with AI-assisted security analysis, SCADA network vulnerabilities on Plant A remain unpatched while access controls in Plant B are misconfigured, creating a risk of insider threats. These insights allow for targeted remediation efforts, lowering risk exposure throughout the organization.

3.4. Key Benefits of AI-Assisted Architecture Review

AI-enabled cybersecurity assessments and architecture reviews serve as an iterative, preemptive methodology for industrial security. Organizations can use Generative AI to evaluate software architecture and systematically identify opportunities to refine security policies and design for cyber-resilient industrial systems. This seamless and continuous assessment process ensures the long-term hardening of cyber resilience in an industrial infrastructure rather than a point-in-time reactive step.

When Generative AI is applied to cybersecurity assessments and software architecture reviews, industrial organizations can achieve multiple benefits:

- Big data analysis makes it possible to predict security risks through proactive cyber risk management instead of reactive cyber risk management
- AI automates the process of evaluating architecture, drastically reducing the time and resources needed for security audits
- AI-enabled security architecture helps continuously evolve against new and emerging threat landscapes, ensuring that security architecture stays current
- AI promotes uniform implementation of cybersecurity best practices across all software architectures, ensuring industrial environment compliance with international security norms

Declaration on Generative AI

During the preparation of this work, the author(s) used scite.ai and Grammarly to: validate references and spelling checks. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] B. Zohuri, "Ai revolution: safeguarding tomorrow's frontiers - transforming cybersecurity across industries (a short approach)", Current Trends in Eng Sc, vol. 4, no. 2, p. 1-4, 2024. https://doi.org/10.54026/ctes/1057

[2] B. Familoni, "Cybersecurity challenges in the age of ai: theoretical approaches and practical solu tions", Computer Science &Amp; IT Research Journal, vol. 5, no. 3, p. 703-724, 2024. https://doi.org/10.51594/csitrj.v5i3.930

[3] S. Zeadally, E. Adi, Z. Baig, & I. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity", IEEE Access, vol. 8, p. 23817-23837, 2020. https://doi.org/10.1109/access.2020.2968045

[4] I. Sarker, M. Furhad, & R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions", SN Computer Science, vol. 2, no. 3, 2021. https://doi.org/10.1007/s42979-021-00557-0

[5] A. Shahana, R. Hasan, S. Farabi, J. Akter, M. Mahmud, F. Johoraet al., "Ai-driven cybersecurity: balancing advancements and safeguards", Journal of Computer Science and Technology Studies, vol. 6, no. 2, p. 76-85, 2024. https://doi.org/10.32996/jcsts.2024.6.2.9

[6] M. Yunis, A. Khalil, & W. Sammouri, "Towards a conceptual framework for ai-driven anomaly detection in smart city iot networks for enhanced cybersecurity", 2024. https://doi.org/10.20944/preprints202404.0924.v1

[7] Z. Amos, "Implementing AI Anomaly Detection in Industrial Cybersecurity", 2024. https://gca.isa.org/blog/implementing-ai-anomaly-detection-in-industrial-cybersecurity