TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

THE IMPACT OF AI ON OT CYBERSECURITY

Péter HUNORFI, Alexandru BABOȘ

Abstract: *OT systems are interconnected with IT networks and cloud services, which increases their exposure to cyber threats. AI is rapidly being integrated into intrusion detection systems, threat intelligence and risk management workflows. This study is based on academic literature, industrial case studies and OT-specific threat reports to analyse how AI is changing OT cybersecurity. The paper examines AI enabled offensive capabilities, such as AI enhanced malware, AI optimized denial-of-service, data exposure, HMI manipulation, power analysis and RF technology, timing-based and side channel attacks. These attack classes are mapped to corresponding defence strategies. The reviewed literature reports improved detection accuracy and response efficiency in OT environments, but simultaneously introduces new attack surfaces, data-quality dependencies and model-transparency issues. The study concludes that AI should be deployed as an additional, carefully governed analytical layer on top of robust OT security architectures, segmented network design, and human oversight.*

Keywords: *Operational Technology, OT; Cybersecurity; Artificial Intelligence, AI; Anomaly Detection; AI-based attacks.*

1. INTRODUCTION

OT refers to hardware and software systems that control industrial systems and critical infrastructure, including for example energy grids, manufacturing plants and transportation networks. The increasing convergence of OT with IT has exposed these traditionally isolated systems to new cyber threats. Unlike IT environments, where cybersecurity focuses on confidentiality, integrity and availability of data, OT cybersecurity places stronger emphasis on the safety, availability and reliability of physical processes. Recent industry threat reports show that OT environments have become explicit and strategic targets rather than collateral damage in wider IT campaigns. The 2025 Dragos OT/ICS Cybersecurity Year in Review document reports the increase in activity by state-linked and financially motivated threat groups against industrial control systems including campaigns by actors such as VOLTZITE and ELECTRUM. These groups systematically abuse exposed remote access services, VPN vulnerabilities and misconfigured perimeter devices to pivot from IT into OT networks [1]. Many successful intrusions still leverage relatively simple weaknesses such as internet-facing ICS assets, default credentials and poorly governed vendor access. This can result in severe operational disruption once adversaries gain visibility into field devices and control logic. The Dragos report reinforces the need for advanced, context-aware detection and response capabilities and supports the integration of AI-based monitoring and analytics as examined in this study. AI can support real-time detection, alert correlation, and selected response activities, but its benefits are mostly evidenced in datasets, testbeds, and case-study settings.

This research aims to identify how AI is reshaping OT cybersecurity practices to understand its limitations, benefits and future potential based on these questions:

1. How can intrusion and anomaly detection models used in OT networks be designed, trained and validated so that they would be effective during adversarial activity (evasion,

poisoning, model stealing) and still provide explainable, trustworthy alerts for safety critical decisions over long term field deployments?

2. What methodologies and frameworks are needed to systematically collect, anonymise, share and maintain realistic OT data that capture both normal process behaviour and evolving AI-enabled attack patterns, while respecting operational, safety and reliability constraints?

By addressing these questions, this paper positions AI in OT cybersecurity through an integrated analytical framework that links defensive AI capabilities, AI-enabled offensive techniques and OT-specific operational constraints. In addition to a structured synthesis of recent literature, it provides an explicit mapping between representative AI-enabled OT attack types and defence strategy families and derives practical design principles for deploying AI as decision support in OT security operations. The paper also highlights research gaps that require stronger empirical validation, particularly realistic OT datasets, concept drift under process changes and the operational impact of false positives in safety-critical environments. Where the available evidence is primarily conceptual, this paper explicitly acknowledges this limitation and formulates testable directions for future empirical validation.

2. METHODOLOGY

This paper applies a PRISMA-inspired selection logic adapted to a qualitative synthesis. Records were identified from three academic indexing databases. Manual citation checking was then used to capture additional highly relevant items. This paper assembled a combined bibliographic corpus and cross-checked it against the manuscript's final reference list to ensure coverage of seminal and domain-defining sources. Deduplication was performed using DOI or URL identifiers as primary keys and title–year matching as a fallback. This paper then screened records at title and abstract level using predefined eligibility criteria. A record was included if it addressed OT, ICS, SCADA, or critical infrastructure environments and contained an explicit AI or machine learning component relevant to cybersecurity. Sufficient technical detail was required to support consistent extraction. Sources were excluded if they focused on IT-only contexts without OT relevance, applied AI outside cybersecurity, or did not describe methods in adequate detail. This paper assessed the full texts of eligible records and performed structured content analysis. For each source, the extracted fields included the type of OT environment and assets, the data sources used for security monitoring, the model family or analytic approach, the evaluation design and metrics, and any OT-specific constraints or limitations reported by the authors. The extracted evidence was synthesised into the thematic discussion of AI-enabled OT security operations and into the attack–defence mapping table to make the review more transparent and auditable. A key limitation is the scarcity of openly available, representative OT datasets and the limited number of published field evaluations, which restricts direct comparability across studies.

2.1 Evolution of OT cybersecurity

OT systems were historically designed for resilience and safety and isolated from external networks. With the rise of the IIoT, Industry 4.0 and cloud-integrated architectures, these systems are now tightly interconnected with corporate IT, internet-facing and cloud services. This significantly increased their exposure to cyber threats [2]. Traditional OT security measures, such as static network segmentation and perimeter defences are no longer sufficient on their own to address sophisticated threats like APTs, supply chain attacks and zero-day vulnerabilities. Early incidents, such as Stuxnet demonstrated that cyber operations can deliberately manipulate industrial processes, but the threat landscape has evolved considerably in the 2020s. Recent literature on AI-based intrusion detection systems and ICS security testbeds suggests that attacks against electric

power grids, gas pipelines, and water treatment facilities can cause large-scale service disruptions and economic losses. This turns cyber incidents into physical safety and resilience problems [3]. Industry reporting shows that OT/ICS environments are now systematically targeted by state sponsored groups, ransomware operators and hacktivists [1]. This shift from isolated bespoke attacks to a persistent and diversified threat landscape has motivated a surge of research into AI-driven anomaly detection, process-aware intrusion detection and virtual testbeds for OT.

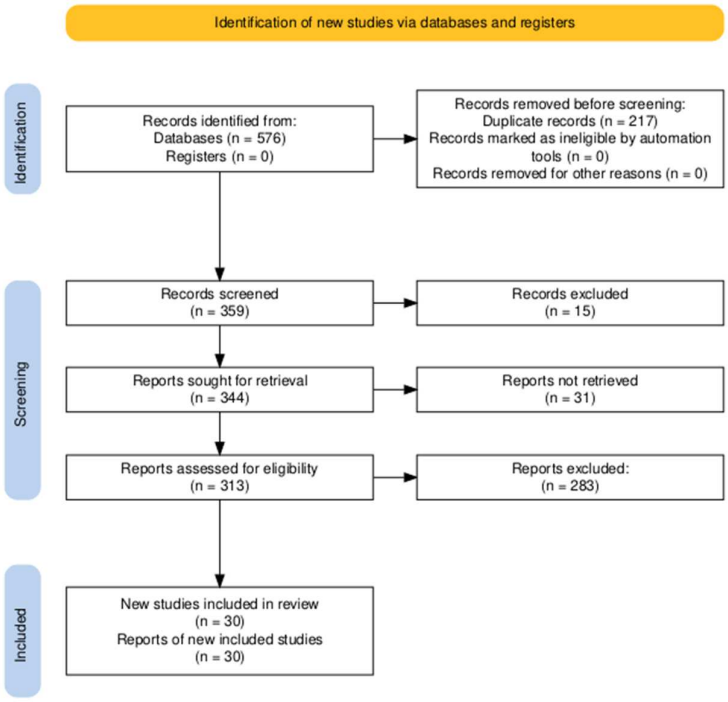


Fig. 1. PRISMA flowchart of article selection and screening process.

2.2 Theoretical framework

AI's role in cybersecurity has evolved from rule-based automation toward data-driven detection and response especially in environments characterized by high volume and heterogeneous data. ML algorithms can learn statistical patterns of normal and malicious activity, making them suitable for intrusion detection and malware classification in large-scale networks [4]. Supervised learning models can be trained on labelled traffic or event data to recognize known attack families, while unsupervised or anomaly-based models can learn "normal" behaviour and flag deviations that may indicate previously unknown or low-frequency threats [5]. Recent works on AI-driven SIEM shows that such models can also correlate events across multiple data sources and automatically prioritize or aggregate alerts [6]. This can reduce analyst workload and speed up incident triage. DL further extends these capabilities by extracting hierarchical representations from complex input data. DL architectures such as CNNs and RNNs can model spatial and temporal dependencies in network flows, system calls and sensor time series. This improves the detection of stealthy or multi-stage attack patterns compared with shallow classifiers. NLP techniques support threat intelligence workflows by processing unstructured text from incident reports, vulnerability advisories, log messages and open-source feeds. Research on adversarial machine learning has demonstrated that these models can themselves become targets. Maliciously crafted inputs could cause misclassification or evade detection. This highlights the need to treat AI components as security critical elements rather than neutral tools [7].

2.3 OT cybersecurity integration with AI

Recent OT focused studies show that AI can enhance cybersecurity through real-time monitoring, predictive analytics and partially automated response workflows. In testbed evaluations, ML-based intrusion detection systems for industrial networks often report better performance than traditional signature-based approaches in detecting previously unseen attacks, particularly when models learn normal process behaviour and flag deviations in network flows or sensor data [8]. Newer architectures like transformer-enhanced LSTM models further improve the detection of malicious traffic in ICS by capturing long range temporal dependencies in protocol sequences. They can achieve high accuracy on realistic ICS datasets [9]. Complementary work on gas pipeline and power system testbeds provides labelled datasets and evaluation environments that reflect real OT processes, providing better training and benchmarking of anomaly detection models. AI-driven security information and event management platforms can aggregate alerts from these detectors and correlate them with logs and asset inventories. They can then prioritise incidents for human analysts in OT security operations centres. AI can support predictive maintenance and risk management in OT by identifying patterns that precede equipment failures or unsafe operating conditions. This can reduce downtime and limit the operational impact of cyber incidents [10]. However, the same learning mechanisms that make these models powerful can introduce new surfaces for attack. Research about recent attacks against ML shows that maliciously crafted inputs or poisoned training data can cause misclassification or systematic blind spots in DL-based detectors, raising concerns about the resilience of AI-enabled OT defences under targeted manipulation. This means that integrating AI into OT security requires not only accurate models and realistic testbeds, but also explicit design measures against adversarial interference and continuous human supervision.

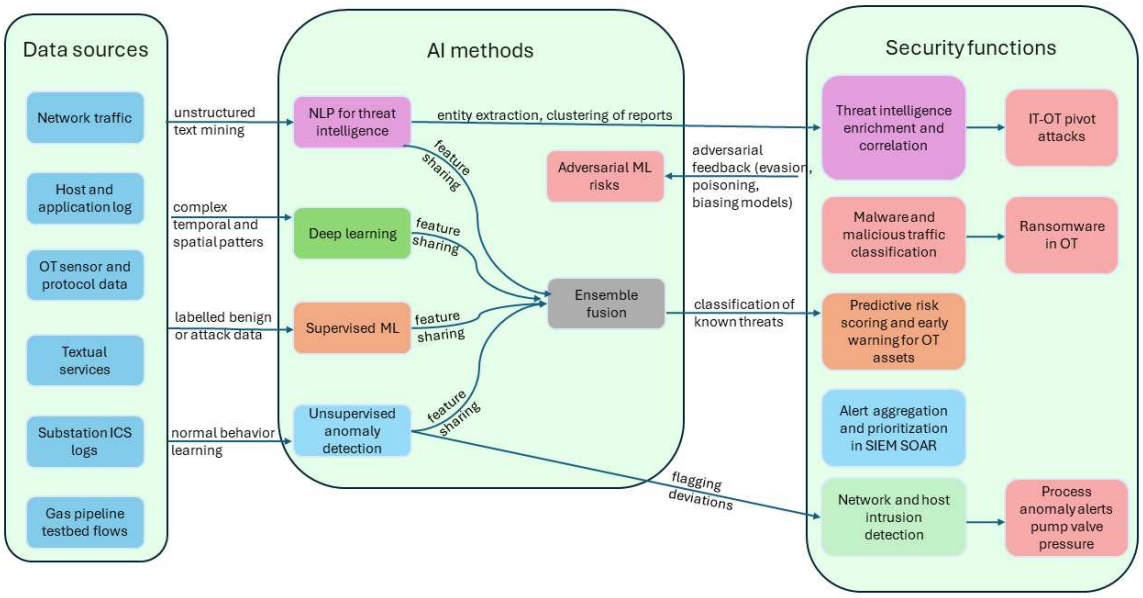


Fig. 2. AI methods and data flows for cybersecurity in OT environments.

Figure 2 summarises the typical AI-enabled data flow in OT cybersecurity. Telemetry is collected from multiple layers, including industrial network traffic (e.g., protocol sequences and flow metadata), process variables and sensor time series (e.g., PLC/RTU tags), and security-relevant logs from engineering workstations, HMIs and gateways. These heterogeneous sources are pre-processed (normalisation, time alignment, feature engineering) and then analysed by ML/DL models for process-aware anomaly detection

and intrusion detection. The resulting alerts are enriched with asset context and correlated within SIEM workflows to support triage and prioritisation in OT security operations. Importantly, the figure also highlights that AI outputs should be treated as decision support: thresholds, response actions and safety-critical decisions require governance controls and human validation to minimise operational risk from false positives or model drift.

3. FINDINGS AND ANALYSIS

3.1 Enhanced threat detection capability

AI-based approaches can significantly improve threat detection in OT environments compared with traditional, signature-driven systems. Instead of using only predefined attack patterns, ML and DL models learn statistical data of normal OT traffic and process behaviour, allowing them to flag previously unseen or emerging threats. Experimental studies on industrial and ICS testbeds report that ML-based intrusion detection systems consistently outperform conventional methods in detecting network intrusions and stealthy attacks. For example, Khan et al. propose the HML IDS anomaly-based intrusion detection system and show that on a real gas pipeline SCADA dataset. Their ML-based approach outclassed several benchmark IDS models with an overall detection accuracy of about 97%, clearly improving intrusion detection performance in an OT setting [11]. In these works, unusual behaviour detection models are trained on benign traffic and sensor time series from substations, gas pipelines or other ICS processes and then used to identify deviations that may indicate command injection, manipulation of control logic or other cyberattacks against OT. Most reported performance gains are demonstrated on labelled datasets or OT testbeds; published field evaluations and false-positive cost analyses remain limited.

3.2 Risk management and predictive capabilities

Predictive analytics can identify shifting vulnerabilities and signs of process degradation prior to their exploitation or progression into system failures, allowing organizations to implement preventive measures and targeted hardening. Recent work on predictive maintenance and predictive monitoring in manufacturing and process industries shows that anomaly detection models trained on multivariate sensor data can detect abnormal patterns. This can potentially reduce downtime and operational risk. In the oil and gas domain, case studies and reviews report that DL-based models such as CNN and LSTM are increasingly used to support leak detection, corrosion prediction and remaining service life estimation in pipeline systems, facilitating faster intervention than conventional methods. More recent frameworks that integrate service life forecasting with anomaly detection demonstrate that AI can support accurate early fault warnings while keeping computing resources manageable, further strengthening predictive maintenance as a security relevant control for critical industrial assets [12]. This is particularly important in critical infrastructure, where cascading equipment failures and process interruptions can increase both safety and cybersecurity consequences. Evidence for predictive benefits is largely derived from domain case studies and prototype evaluations, with limited reproducible comparison across plants and sectors.

3.3 Automation and response efficiency

AI also enables more automated incident detection and response in OT environments, lowering the delay between threat identification and mitigation. In the smart grid domain, the SPEAR SIEM system shows how a field-specific SIEM platform can collect and correlate large volumes of security events across an ecosystem [13]. It aggregates telemetry from hydropower plants, substations, power plants, and smart homes to detect attacks and support coordinated security operations. Building on this idea, recent frameworks for critical infrastructures propose autonomous or semi-autonomous AI services that support incident triage, selection of defensive actions and coordination of response and recovery activities across the incident lifecycle [14]. Studies on AI

enhanced SCADA security and ICS anomaly detection architectures similarly report that integrating ML-based detectors with SIEM/SOAR style dashboards can automate much of the event analysis, prioritise alerts and trigger predefined playbooks, thereby shortening response times and easing the workload on security teams [15]. Reported SIEM and SOAR benefits are mainly shown in domain-specific prototypes and integration case studies rather than in longitudinal, multi-site OT deployments.

3.4 Challenges identified in studies

Notwithstanding the advantages, AI integration in OT cybersecurity presents challenges. Papernot et al. highlighted the risk of adversarial machine learning, where attackers manipulate input data to mislead AI models [16]. Additionally, the success of AI depends on the quantity and quality of the provided training data. Hodo et al. noted that obtaining high-quality and labelled data from OT environments is challenging due to proprietary systems and legacy equipment [17].

4. AI-ENABLED ATTACKS ON OT

AI driven cyber-attacks on OT systems include AI enhanced malware, DoS (Denial of Service) attacks, sensitive data exposure, HMI-based attacks, power analysis attacks, side-channel attacks, timing-based attacks and RF technology attacks. These attacks use AI for automation, evasion and optimization, making them more effective against ICS. Protection strategies include AI supported threat detection, zero-trust security, network segmentation, encryption, anomaly monitoring, redundant security measures and behavioural analysis. Introducing adaptive AI defense, regular updates and cybersecurity training is crucial to mitigating these evolving threats.

AI-based attacks on OT consist of the following defence strategies:

- (D1) AI-based detection & monitoring,
- (D2) Access & identity controls,
- (D3) Network & communication security,
- (D4) System & hardware hardening,
- (D5) Resilience & redundancy,
- (D6) Awareness & governance.

Table 1 links each attack types to defence strategy families D1–D6 to make the mapping explicit and actionable.

Table 1

AI-enabled OT attack classes mapped to defence strategy families (D1–D6).

Attack types/Defence strategy	D1	D2	D3	D4	D5	D6
4.1 AI enhanced malware	✓	✓	✓	✓		
4.2 AI optimized DoS	✓		✓		✓	
4.3 AI driven sensitive data exposure	✓	✓				
4.4 AI enabled HMI attack	✓	✓		✓		
4.5 AI augmented power analysis	✓			✓	✓	✓
4.6 AI driven side channel attack	✓			✓		
4.7 AI timing-based attack	✓		✓			
4.8 AI enhanced RF attack	✓		✓			

The mapping is qualitative and derived from the reviewed literature; openly available evidence is predominantly conceptual or testbed-based, with limited publicly documented field demonstrations attributable to specific attack classes.

4.1 AI enhanced malware

Attack types could be self-adapting malware, which shifts based on OT network behaviour to avoid detection, AI guided ransomware, which detects and ranks critical assets for encryption and AI powered worms, which learn system topology and spread autonomously within OT networks. The possible protection strategies could be AI-based EDR to detect self-adapting malware, network segmentation to separate critical systems, zero-trust security and application whitelisting to prevent unauthorized execution

and regular patching and firmware updates to close vulnerabilities [18].

4.2 AI optimized DoS attack

Attack types could be intelligent DoS attacks, when AI finds the most efficient way to exhaust system resources, adaptive botnets, which adjust attack tactics dynamically to avoid detection and protocol aware DoS, which exploits OT specific protocols (e.g. Modbus, DNP3) to disrupt operations [19]. The possible protection strategies could be AI-based anomaly detection to detect traffic spikes and patterns, rate limiting and traffic filtering to block suspicious traffic, redundant network paths to mitigate attack impact, and firewalls and IPS for deep packet analysis [20].

4.3 AI driven sensitive data exposure

Attack types could be AI powered reconnaissance, which analyses network traffic and organisational metadata to extract or infer sensitive data, behavioural analytics bypass, where AI mimics legitimate user behaviour to evade anomaly-based monitoring and model extraction attacks, where adversaries reverse engineer OT related AI models to predict or manipulate their behaviour. The possible protection strategies could be data encryption and masking to protect sensitive information, MFA to prevent unauthorized access, zero-trust security model to continuously verify system access, honeypots, decoy data to detect reconnaissance attempts and study attacker techniques [21].

4.4 AI enabled HMI-based attack

Attack types could be deepfake social engineering like AI created voice and video used to impersonate operators, automated HMI exploitation, where AI scans for misconfigurations in HMI interfaces and AI controlled interface manipulation, which alters HMI displays to deceive operators [22]. The possible protection strategies could be secure authentication for HMI access with biometrics and RBAC, AI-based behaviour monitoring to detect abnormal operator interactions, patch vulnerabilities by constant software updates and deepfake detection training to educate employees on social engineering risks. Also building on behaviour-based intrusion detection and AI supported risk management approaches proposed for critical infrastructures [23].

4.5 AI augmented power analysis attack

Attack types could be ML-based power profiling, where AI analyses power consumption patterns to deduce system states, AI optimised fault injection, where AI determines when and where to disrupt power most effectively and predictive power anomaly exploitation, where AI manipulates fluctuations to cause malfunction in critical equipment [24]. The possible protection strategies could be for example AI supported abnormal power behaviour detection to monitor atypical fluctuations, shielding and EMI reduction to prevent electromagnetic leakage, redundant power supplies to avoid system failures and isolated PMS to decrease the attack surface, building on AI supported IDS and risk mitigation concepts proposed for SCADA and ICS.

4.6 AI driven side channel attack

Attack types could be neural network-based signal analysis, where AI extracts sensitive information from electromagnetic or other physical emissions, AI assisted acoustic side-channel attacks, where AI detects operational states via sound recognition and memory access profiling, where AI infers hidden data through timing behaviour or access footprints [25]. The protection strategies could be shielding and hardware hardening to minimise the risk of data leaks, AI supported monitoring for side-channel leaks to detect abnormal emissions, randomized execution timing to disrupt AI-based timing analysis and hardened cryptographic algorithms and detection models to safeguard against manipulation and key recovery [26].

4.7 AI optimized timing-based attack

Attack types could be automated jitter analysis, when AI detects timing inconsistencies to exploit them, AI supported clock skew attacks, where AI manipulates system clocks to

desynchronise operations and timing-based AI evasion, where AI adapts attack execution timing to remain undetected [27]. The protection strategies could be time-synchronisation security with authenticated time servers, AI-based timing outlier detection to spot deviations, secure RTOS to reduce the likelihood of timing manipulation and cryptographic timestamps for integrity verification, building on recent DL and hybrid IDS frameworks for ICS and critical infrastructure systems [28].

4.8 AI enhanced RF technology attack

Attack types could be AI powered RF signal analysis, which uses DL to capture and decode wireless OT communications, AI-based jamming attacks, which identify optimal frequencies to jam and automated RF protocol exploits, where AI reverse engineering wireless communication protocols. The possible protection strategies could be FHSS to switch frequencies dynamically, AI powered RF disturbance detection to spot unusual RF activity. To reduce the risk of eavesdropping it can be beneficial to use encrypted wireless signalling, directional antennas and shielding to limit exposure to external signals. This aligns with DiD and AI-supported monitoring in IIoT and ICS environments, where layered controls are used to reduce both exposure and detection latency. [29].

5. RESULTS

The results indicate that AI can enhance OT cybersecurity through improved threat detection, predictive insight and automated response. However, the challenges identified in the literatures point out the importance of taking a balanced approach. Using AI without human oversight can lead to blind spots, particularly in complex OT environments where false positives can seriously affect critical operations. The support of OT cybersecurity by AI also brings up regulatory and ethical questions and concerns. Ensuring the transparency of AI decisions is crucial in sectors like healthcare and energy, where cybersecurity decisions can have life or death consequences.

Regarding to the first research question, intrusion and anomaly detection for OT networks is most effective when AI is implemented as part of a hybrid “defence in depth” architecture rather than as standalone “black boxes”. Robust training pipelines need to explicitly address adversarial activity by using data augmentation, adversarial examples, combine models and regular red-team exercises against the AI pipeline so that evasion, poisoning and model stealing attempts are part of the evaluation, not an afterthought. Trustworthy use in safety critical environments further requires that models are clear enough for operators to understand and question their outputs. This can be achieved by favouring architectures with interpretable features, visualising anomalies in the context of process tags, assets and control logic rather than only as abstract scores. Long-term field deployment also needs lifecycle management, monitoring for concept drift, periodic re-training on updated OT data, access control, logging and clear procedures for human override. AI-based IDS for OT can remain effective under cyberattack and still provide trustworthy alerts if they are engineered as governed, explainable decision support components embedded into existing SOC workflows and not just blindly replacing human judgment.

Answering the second question, the study shows that realistic OT data for AI-based security cannot be obtained by simple IT style log collection. It requires a structured data-governance and testbed framework tailored to industrial processes. A practical approach is a two-layer methodology. First, high fidelity OT/ICS testbeds and digital twins to be used to generate labelled datasets capturing normal operation and a wide range of attack scenarios, including AI enabled attacks without endangering production. Second, carefully engineered data collection points in live OT environments (gateways, data diodes) aggregate network flows, process variables and security events under strict safety and performance constraints. To make these datasets shareable, it is necessary to anonymize assets and users, aggregate or bin sensitive process values,

remove business-critical context, and apply additional statistical protections. Data sharing then has to be embedded in formal governance approach that define roles, access rights, retention periods and acceptable use. This shall be preferably harmonised with existing OT security and IIoT standards. Maintaining realism over time requires continuous updates, integrating traces from new incidents, red-team exercises for new AI driven attack techniques and versioning datasets so that model accuracy can be compared across generations.

To realise benefits while managing risks, AI should be integrated as a governed decision-support layer within defence-in-depth OT architectures rather than as a standalone replacement for established controls. Empirical studies on AI-supported intrusion detection and SIEM in industrial networks report improved detection and triage but also emphasise expert validation and rule-based safeguards in safety-critical environments. Model performance depends on representative, well-labelled data, yet OT data collection is constrained by proprietary protocols, legacy systems, and limited logging. Finally, adversarial resistance and lifecycle management are also important. AI components shall be treated as security-critical assets, monitored for drift, and regularly validated through red-team exercises and updated datasets. These needs motivate further research that combines AI evaluation, OT engineering, and security governance, including longitudinal field studies that quantify operational impact and false-positive costs [30]. Supporting such research including field deployments, longitudinal case studies and "human in the loop" evaluations will be important for maturing AI enabled OT security. Building on these principles, operational recommendations emerge from the reviewed literature, as summarised in Figure 3.



Fig. 3. AI-based operational framework.

First, AI-based threat intelligence and anomaly detection should be used for real-time monitoring of OT networks and processes, enabling early spotting of anomalies in normal behaviour and improved incident triage. Second, a zero-trust security model and secure OT–IT segmentation are essential to limit lateral movement between IT and OT, enforce proper authentication and reduce exposure of ICS devices to the internet in line with IIoT security guidance. Third, continuous cybersecurity training for engineers and operators should explicitly cover AI enabled threats, like deepfake based social engineering to ensure that human defenders remain an effective last line of defence. Fourth, adaptive AI defences that

continuously adjust detection thresholds and correlation logic based on observed changes in the threat landscape can increase resilience even further. Finally, strict patch and vulnerability management across OT assets especially for gateway devices, HMIs and engineering workstations remains a fundamental requirement, as unpatched systems continue to be a major enabler for both traditional and AI supported attacks in industrial environments. Taken together, these strategic and operational measures outline a roadmap in which AI strengthens OT cybersecurity but always in combination with robust architectures, disciplined basic controls and informed human decision making.

6. CONCLUSION

AI is reshaping OT cybersecurity by improving anomaly and intrusion detection, supporting security operations workflows, and enabling more adaptive monitoring of industrial processes. At the same time, the reviewed evidence highlights OT-specific constraints and risks, including safety-critical operational judgement, data quality and representativeness challenges, model drift under process changes, and adversarial attacks against learning-based components. Therefore, AI should be deployed as a carefully governed decision-support layer on top of robust OT security architecture, segmented network design, and human oversight.

Key research gaps include adversarial robustness under realistic attacker models, access to representative OT datasets, and longitudinal field evaluations that quantify operational impact, false-positive costs, and maintainability. To narrow these gaps, future work should prioritise reproducible testbed studies, transparent evaluation protocols, and human-in-the-loop validation to support safe adoption of AI-enabled OT defences.

7. REFERENCES

[1]Dragos, 2025 *OT/ICS Cybersecurity Report*. 2025.

[2]M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, and I. Khalil, *An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems*, 2021, doi: 10.1109/TSUSC.2019.2906657.

[3]L. Deng, X. Zhang, Q. Zheng, D. Zhao, J. Zhou, and J. Xiang, *A New Dataset for Intrusion Detection in Industrial Control System - A Gas Pipeline Testbed Study*, 2023, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom59178.2023.00149.

[4]A. Abid, F. Jemili, and O. Korbaa, *Real-Time Data Fusion for Intrusion Detection in Industrial Control Systems Based on Cloud Computing and Big Data Techniques*, 2024, doi: 10.1007/s10586-023-04087-7.

[5]H. Karimipour and F. Derakhshan, *Artificial Intelligence for Threat Detection and Analysis in Industrial IoT - Applications and Challenges*, 2021, doi: 10.1007/978-3-030-76613-9_1.

[6]D. A. Yeager *et al.*, *Case Study- Architecting a Solution to Detect Industrial Control System Attacks*, 2020, doi: 10.1109/SSS47320.2020.9197724.

[7]E. Amer and T. Elboghdadly, *Evaluating Machine Learning Techniques for ICS Security - Insights from Dataset Limitations and Classifier Performance*, 2024, doi: 10.1109/MIUCC62295.2024.10783517.

[8]H. da Conceição Aberto, J. M. Dembele, I. DIop, and A. Bah, *Review of Intrusion Detection Systems for Supervisor Control and Data Acquisition - A Machine Learning Approach*, 2024, doi: 10.1007/978-3-031-72287-5_3.

[9]B. S. Ali *et al.*, *ICS-IDS-Application of Big Data Analysis in AI-based Intrusion Detection Systems to Identify Cyberattacks in*

ICS Networks, 2024, doi: 10.1007/s11227-023-05764-5.

[10] A. Howe and M. Papa, *Feature Engineering in Machine Learning-Based Intrusion Detection Systems for OT Networks*, 2023, doi: 10.1109/SMARTCOMP58114.2023.00086.

[11] I. Khan, D. Pi, Z. Khan, Y. Hussain, and A. Nawaz, *HML-IDS: A Hybrid-Multilevel Anomaly Prediction Approach for Intrusion Detection in SCADA Systems*, *IEEE Access*, vol. PP, pp. 1-1, July 2019, doi: 10.1109/ACCESS.2019.2925838.

[12] O. Polat, A. Ayid Ahmad, S. Oyucu, E. Algül, F. Doğan, and A. Aksöz, *Temporal-Spatial Feature Extraction in IoT-Based SCADA System Security-Hybrid CNN-LSTM and Attention-Based Architectures for Malware Classification and Attack Detection*, 2025, doi: 10.1109/ACCESS.2025.3577761.

[13] P. Radoglou-Grammatikis *et al.*, *SPEAR SIEM - A Security Information and Event Management system for the Smart Grid*, 2021, doi: 10.1016/j.comnet.2021.108008.

[14] J. Bertholat, M. Merad, J. Barbier, and J. Clerc, *Practical Use Of AI For Cyber Risk Management In Critical Infrastructures - A Review*, 2024.

[15] C. V. S. Suresh Babu, S. Manoharan, and P. A. Simon, *Cybersecurity for AI-Enhanced Supervisory Control and Data Acquisition (SCADA) Systems - Safeguarding Critical Infrastructure from Evolving Cyber Threats*, 2025, doi: 10.4018/979-8-3373-0583-7.ch010.

[16] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, *The Limitations of Deep Learning in Adversarial Settings*. 2016, p. 387. doi: 10.1109/EuroSP.2016.36.

[17] E. Hodo, X. Bellekens, A. Hamilton, P. Dubouilh, E. Iorkyase, and C. Tachtatzis, *Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System*. 2017. doi: 10.48550/arXiv.1704.02286.

[18] Blackfog, *The State of Ransomware 2024*. 2024. [Online]. Available: https://www.blackfog.com/the-state-of-ransomware-2024/

[19] F. B. Saghezchi, G. Mantas, M. A. Violas, A. M. Manuel De Oliveira Duarte, and J. Rodriguez, *Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs*, 2022, doi: 10.3390/electronics11040602.

[20] V. Ya. Ushakov, I. U. Rakhmonov, A. B. Askarov, and D. S. Nikitin, *Digitalization of Electrical Power Engineering - Scientific and Technical Fundamentals and Achieved Advantages*, 2025, doi: 10.1007/978-3-031-95705-5.

[21] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, *A Comprehensive Survey on Cyber Deception Techniques To Improve Honeypot Performance*, Computers & Security, vol. 140, p. 103792, May 2024, doi: 10.1016/j.cose.2024.103792.

[22] J. Squillace, J. Cappella, and A. Sepp, *User Vulnerabilities in AI-Driven Systems-Current Cybersecurity Threat Dynamics and Malicious Exploits in Supply Chain Management and Project Management*, 2024, doi: 10.1109/ICETSIS61505.2024.10459480.

[23] C. Gangadhar, R. G. Mapari, A. K. Muthevi, A. Suneetha, S. K. B V, and B. Mouleswararao, *Exploring the Role of*

Behavioral Analytics and Anomaly Detection in Securing Mobile Networks for Critical Infrastructure, 2025, doi: 10.1080/19393555.2025.2479027.

[24] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, *Deep Learning for Side-channel Analysis and Introduction to ASCAD Database*, Journal of Cryptographic Engineering, vol. 10, June 2020, doi: 10.1007/s13389-019-00220-8.

[25] S. D. D. Duque Anton, A. P. Lohfink, and H. D. Schotten, *Discussing the Feasibility of Acoustic Sensors for Side Channel-aided Industrial Intrusion Detection - An Essay*, 2019, doi: 10.1145/3360664.3360667.

[26] A. Flatscher, B. Stojanović, and O. Özdenizci, *Enhancing Adversarial Robustness of Anomaly Detection-Based IDS in OT Environments*, 2024, doi: 10.23919/CNSM62983.2024.10814511.

[27] A. Aruna *et al.*, *Hybrid Deep Learning Approaches for Cyberattack Detection and Prevention in Critical Infrastructure Systems*, 2025.

[28] M. Barbhaya, P. R. Dasari, S. K. Damarla, R. Srinivasan, and B. Huang, *A Deep Learning Framework for Cyberattack Detection and Classification in Industrial Control Systems*, 2025, doi: 10.1016/j.compchemeng.2025.109278.

[29] U. J. Otokwala and A. Petrovski, *Ensemble Common Features Technique for Lightweight Intrusion Detection in Industrial Control System*, 2023, doi: 10.1109/ICPS58381.2023.10128040.

[30] T. Gebremichael *et al.*, *Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges*, *IEEE Access*, vol. PP, pp. 1–1, Aug. 2020, doi: 10.1109/ACCESS.2020.3016937.

Impactul IA asupra securității cibernetice în domeniul OT

Rezumat: Sistemele OT sunt interconectate cu rețelele IT și serviciile cloud, ceea ce le crește expunerea la amenințările cibernetice. Inteligența artificială este integrată rapid în detectarea intruziunilor, informațiile privind amenințările și managementul riscurilor. Acest studiu se bazează pe literatura academică, studii de caz industriale și rapoarte privind amenințările specifice OT pentru a analiza modul în care AI transformă securitatea cibernetică OT. Lucrarea examinează capabilități ofensive bazate pe AI, precum malware îmbunătățit, atacuri denial-of-service optimizate, expunerea datelor, manipularea HMI, analiza puterii, tehnologia RF și atacurile bazate pe sincronizare și canale laterale, corelate cu strategii de apărare. Literatura analizată indică o detecție și un răspuns mai eficiente, dar și noi suprafețe de atac, dependențe de calitatea datelor și probleme de transparență a modelelor.

Peter HUNORFI, PhD Student, Óbuda University, Doctoral School of Safety and Security Sciences, hunorfi.peter@phd.uni-obuda.hu, Népszínház utca 8, Budapest, Hungary.

Alexandru BABOȘ, PhD, Associate Professor, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Romania, babos.alexandru@armyacademy.ro, +40 269 432 990, 3-5 Revoluției Street, Sibiu, Romania.