Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.073482

REVIEW

Intrusion Detection Systems in Industrial Control Systems: Landscape, Challenges and Opportunities

Tong Wu, Dawei Zhou, Qingyu Ou* and Fang Luo

Department of Information Security, Naval University of Engineering, Wuhan, 430000, China

*Corresponding Author: Qingyu Ou. Email: ouqingyv@163.com

Received: 18 September 2025; Accepted: 13 November 2025; Published: 12 January 2026

ABSTRACT: The increasing interconnection of modern industrial control systems (ICSs) with the Internet has enhanced operational efficiency, but also made these systems more vulnerable to cyberattacks. This heightened exposure has driven a growing need for robust ICS security measures. Among the key defences, intrusion detection technology is critical in identifying threats to ICS networks. This paper provides an overview of the distinctive characteristics of ICS network security, highlighting standard attack methods. It then examines various intrusion detection methods, including those based on misuse detection, anomaly detection, machine learning, and specialised requirements. This paper concludes by exploring future directions for developing intrusion detection systems to advance research and ensure the continued security and reliability of ICS operations.

KEYWORDS: Industrial control system; industrial control system network security; intrusion detection; cyberspace security; ICS network; network security

1 Introduction

Industrial control systems (ICSs) manage critical processes across sectors such as power generation, water supply, oil and gas, manufacturing, and transportation. Initially, these systems were not designed with security considerations in mind [1]. However, as the Internet has grown in use, remote management capabilities have expanded, enabling ICSs to be linked to information technology (IT) systems. In the context of Industry 4.0, the convergence of operational technology (OT) and IT has introduced security vulnerabilities from IT environments, such as insecure protocols and remote access points, into OT systems. This shift has led to a rise in cyberattacks that were once limited to IT networks and now target ICS environments. The consequences of these attacks have been significant, affecting the environment, security, and public safety, while also impacting ICS asset owners, governments, and society as a whole [2].

The scale of ICS network devices is rapidly expanding, with a growing number of protocols and increasingly complex processors, such as CPUs, which has led to a larger attack surface. Several major cybersecurity attack incidents targeting ICS are shown in Fig. 1. One of the earliest significant ICS network attacks was the Stuxnet malware incident at Iran's nuclear facilities [3], where specific programmable logic controllers (PLCs) were compromised, resulting in the damage of approximately 1000 centrifuges used in Iran's nuclear program. In 2015, a cyberattack using BlackEnergy3 malware targeted Ukraine's power grid, resulting in widespread blackouts that affected nearly 250,000 individuals [4]. In May 2021, a cyberattack on the Colonial Pipeline, which supplies 45% of the fuel along the U.S. East Coast, forced a temporary shutdown, resulting in fuel shortages, price increases, and panic buying nationwide [5]. In April 2022, Russia attempted a destructive cyberattack on Ukraine's power grid using Pipedream malware [6].

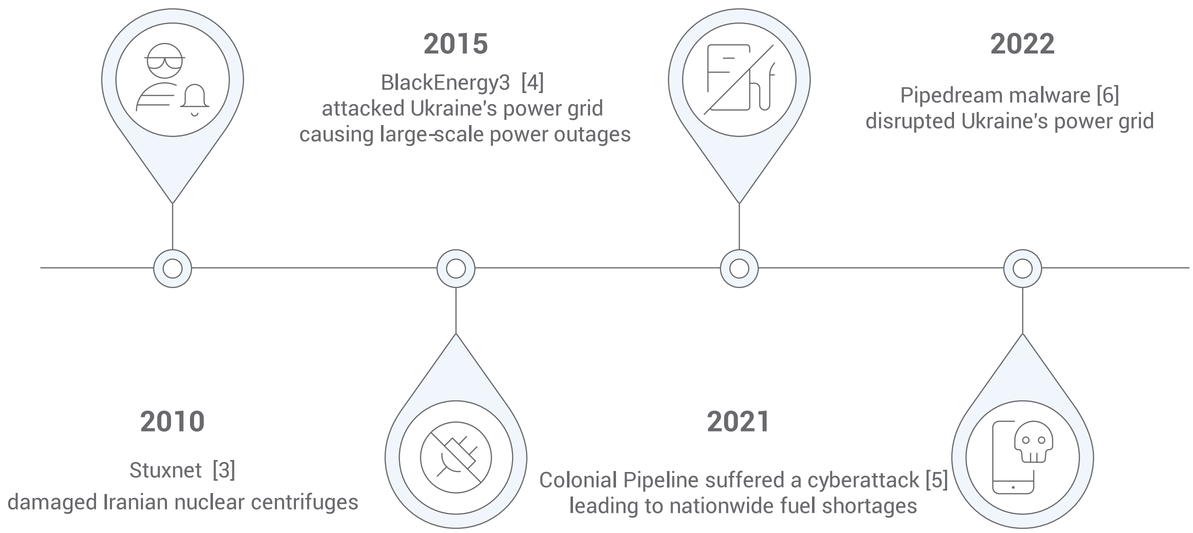

Figure 1: Major ICS cybersecurity incidents [3–6]

ICSs play a pivotal role in critical security environments, handling essential functions, such as authentication, encryption, and data transmission, and have become integral to everyday operations and production. The interactions between various hardware components, as well as between hardware and software, make ICSs more complex than traditional IT systems, exposing them to even greater cybersecurity risks. Consequently, there is an urgent need to strengthen intrusion detection mechanisms within ICS networks, with a focus on improving detection accuracy and real-time performance. This study focuses on cybersecurity for ICS, with a core focus on industrial cyberattacks exploiting network vulnerabilities, and proposes intrusion detection systems suitable for industrial scenarios. It should be specifically noted that this study does not involve cross-domain research on cyber-physical systems (CPS), nor does it include analysis of cyberattacks on non-industrial infrastructure.

The primary contributions of this paper are as follows:

- An in-depth analysis of the distinctive characteristics and attack vectors in ICS network security.
- A classification and evaluation of the intrusion detection techniques utilised in ICSs, providing an overview of current advancements and limitations in research at both national and international levels.
- An exploration of emerging trends in key technologies and the evolving industrial landscape within this field.

2 Systematic Literature Review Methodology

To systematically summarize the research status, core challenges, and development trends of ICS intrusion detection technology, this study adopts the Systematic Literature Review (SLR) methodology. By defining research questions, formulating standardized search strategies, conducting rigorous literature screening, extracting key data, and performing comprehensive analysis, this methodology effectively avoids the subjectivity and one-sidedness of traditional literature reviews, ensuring the reproducibility, reliability, and objectivity of the review results. This section details the specific implementation process of the SLR, laying a methodological foundation for subsequent technical analysis and trend assessment.

2.1 Research Questions (RQs)

Centering on the core theme of "current status, challenges, and opportunities of ICS intrusion detection technology," this study designs the following 4 progressive research questions to guide the literature retrieval and analysis process in a targeted manner, ensuring coverage of key dimensions of technical research:

RQ1: What are the unique characteristics of ICS cybersecurity? Specifically, what typical vulnerabilities and attack vectors are derived from the characteristics of industrial scenarios?

RQ2: What core categories can current ICS intrusion detection systems be divided into? What are the core principles, applicable industrial application scenarios, and technical advantages/disadvantages of each category?

RQ3: What are the main challenges faced by existing ICS intrusion detection systems in their implementation in real industrial scenarios? What are the technical roots of these challenges and their potential impacts on industrial operations?

RQ4: What are the research hotspots and future evolutionary directions of ICS intrusion detection technology in recent years? To address current technical bottlenecks, what innovative paths (e.g., lightweight models, physically network-integrated detection) can promote the practical application of the technology?

2.2 Search Strategy

To ensure the comprehensiveness, timeliness, and domain relevance of the literature, the retrieval process adheres to the following specifications, covering core research achievements in the field of ICS intrusion detection:

2.2.1 Selection of Retrieval Databases

Focusing on authoritative academic databases in the fields of industrial control and cybersecurity, while balancing technical depth and research breadth, the selected databases include:

IEEE Xplore: Focuses on collecting journal papers and conference literature in the fields of industrial information technology, control engineering, and ICS security, covering research on detection technologies related to PLCs and SCADA systems.

ACM Digital Library: Emphasizes computer security and network protocol analysis, including cutting-edge research on the exploitation and defense of protocol vulnerabilities in ICS intrusion detection.

SpringerLink: Centers on review literature in industrial automation and system security, providing insights into the development context and trends of ICS security technology.

ScienceDirect: Focuses on the empirical analysis of ICS vulnerabilities, reviews of attack cases, and performance verification of detection technologies.

2.2.2 Search Terms and Combination Logic

Based on the core dimensions of the RQs, Chinese and English search term combinations are designed to capture the target literature accurately. Core search terms include "Industrial Control System (ICS)", "Intrusion Detection Technology (IDS)", "Network Security", "Industrial Protocol Security", "Machine Learning", and "Anomaly Detection". The search logic uses Boolean operators for combination: ("Industrial Control System" OR "ICS" OR "SCADA" OR "Programmable Logic Controller" OR "PLC") AND ("Intrusion Detection" OR "IDS" OR "Anomaly Detection") AND ("Network Security" OR "Cyber Security" OR "Machine Learning" OR "Industrial Protocol").

Based on the aforementioned keyword combinations, the specific results of the search conducted in the 4 target databases are as follows:

IEEE Xplore: 180 matched papers, with core coverage in the fields of industrial control and network security;

ACM Digital Library: 120 matched papers, focusing on computer security and protocol analysis;

SpringerLink: 95 matched papers, mainly concentrating on reviews of industrial automation and research on system security;

ScienceDirect: 110 matched papers, focusing on empirical studies of Industrial Control System (ICS) vulnerabilities and verification of detection technologies;

The total number of initial search results was 505 papers. Before language or type filtering, duplicate papers accounted for 16.8% (85 papers), which provides a basis for the subsequent deduplication stage.

2.2.3 Retrieval Time Range

Considering the rapid iteration of ICS security technology—especially the large-scale application of technologies such as machine learning and edge computing in the ICS field since 2017—this study sets the retrieval time range from January 2017 to August 2025 (as of the completion date of literature retrieval) to cover the latest research achievements. Meanwhile, retrospective supplementation is conducted for classic foundational literature in the field (e.g., analysis of Stuxnet attacks, early research on ICS protocol security) to ensure the integrity of the technical development context.

2.3 Inclusion and Exclusion Criteria

To ensure the relevance and academic quality of the included literature, this study formulates strict inclusion and exclusion criteria and determines the final analysis samples through two rounds of screening:

2.3.1 Inclusion Criteria

1. Relevance of Research Object: The core research content of the literature is ICS intrusion detection technology, or basic research involving ICS security characteristics, vulnerability analysis, and attack methods.

2. Requirement for Content Depth: The literature must clearly elaborate on the principles of detection technologies, experimental design, and performance indicators, or provide technical details of ICS attack cases and insights for defense.

3. Standardization of Publication Form: The literature is peer-reviewed journal papers, international conference papers, or chapters in academic monographs. Conference abstracts, technical reports, and non-reviewed industry white papers are excluded.

2.3.2 Exclusion Criteria

1. Topic Deviation: Literature focusing on intrusion detection for traditional IT systems or security technologies in non-ICS fields (e.g., smart homes, general Internet of Things).

2. Content Duplication: For duplicate literature published by the same research team based on the same dataset and experimental scheme, only the latest or most comprehensive version is retained.

3. Substandard Quality: Literature without a clear experimental design, a lack of data support, or illogical conclusions.

4. Language Restriction: Only Chinese and English literature is retained, and literature in other languages is excluded to ensure the research team's accurate understanding of the content.

2.3.3 Screening Process and Results

This study strictly adheres to the PRISMA 2020 Guidelines. The quantity flow at each stage and its association with the manuscript's references are shown in Table 1 below:

Table 1: PRISMA full-stage screening process

Screening stage	Operation description	Quantity change
1. Identification	Keyword search in 4 databases	505 papers
2. Duplicate Removal	EndNote automatic deduplication + manual verification (excluding cross-database duplicate records)	505→420 papers
3. Title/Abstract Screening.	Exclude topic deviation, non-peer-reviewed, and non-Chinese/English literature	420→328 papers
4. Eligibility	Verify clarity of technical principles, completeness of experimental design, and scenario relevance	328→125 papers
5. Inclusion	Cross-verify the literature quality and the matching degree with the manuscript's research topic	115 papers

- Title/Abstract Screening Stage (92 articles excluded):

Topic deviation (68 articles): Research objects involve traditional IT networks (e.g., general Internet DoS detection) or non-ICS fields (e.g., smart grid non-control layer security), irrelevant to "ICS-IDS";

Non-peer-reviewed (16 articles): Including industrial vendor technical reports (e.g., "PLC Security Configuration Guide") and conference abstracts (without complete experimental data);

Language restriction (8 articles): Non-Chinese/English literature (4 in German, 4 in Japanese), making accurate content interpretation impossible.

- Full-Text Screening Stage (203 articles excluded):

Insufficient content depth (102 articles): Fail to clarify ICS-IDS technical details (e.g., only mention "machine learning can be used for detection" but without explaining models or verification datasets);

Content duplication (45 articles): Duplicate publications by the same research team based on identical experimental protocols;

Scope mismatch (56 articles): Focus on cross-domain cyber-physical system research or non-industrial infrastructure, beyond the scope of this study.

2.4 Data Extraction

For the final 115 literature pieces, a structured data extraction form is designed to systematically collect the following key information, providing a quantitative basis for technical classification, performance comparison, and challenge analysis:

Basic Literature Information: Authors, publication year, name of journal/conference, research institution.

Core Technical Information: Category of intrusion detection technology, core principles, and dependent datasets.

Experimental and Performance Indicators: Detection accuracy, false positive rate, recall rate, detection latency, and deployed hardware platform.

Key Conclusions and Limitations: Technical innovations proposed in the literature, verified adaptability to industrial scenarios, and clearly identified technical bottlenecks.

Two researchers independently complete the data extraction process. For literature with discrepancies in extraction results, cross-validation and team discussions are conducted to reach consensus and ensure data accuracy.

2.5 Synthesis and Analysis

Based on the extracted structured data, this study adopts a three-level analysis framework of "Classification and Comparison—Bottleneck Identification—Trend Assessment" to systematically deconstruct ICS intrusion detection technology:

1. Technical Classification and Comparison: The classic framework for the technical classification of IDS has provided an essential reference for the technical review in this SLR. Liao et al. [7] first proposed a multidimensional IDS classification system in their review, systematically integrating existing achievements across detection methods, technical types, and evaluation metrics. They highlighted the core issue that a single technology cannot cover multiple scenarios and emphasised that hybrid detection is key to improving generalisation. The classification of ICS-IDS into rule-based, anomaly-based, machine learning-based, and specific requirement-based categories in this study is precisely an extension of this framework in industrial scenarios. In particular, it inherits the core logic of classification based on detection strategies and scenario adaptability, thereby ensuring coherence with the technical context [7]. According to detection principles and application scenarios, the technical solutions in the 115 literature pieces are divided into four categories: "Rule-Based Detection", "Anomaly-Based Detection", "Machine Learning-Based Detection", and "Detection for Specific Needs". By comparing indicators such as accuracy, real-time performance, and deployment cost across technologies, the applicable boundaries of each are clarified.

2. Core Bottleneck Identification: Statistical analysis is conducted on the technical challenges mentioned in the literature, and core issues such as "conflict between real-time performance and edge computing power", "dataset imbalance and sample scarcity", and "contradiction between high false positive rate and low industrial fault tolerance" are summarised. The root causes of these issues are analysed by linking them to specific technical scenarios (e.g., millisecond-level response requirements in power systems, insufficient sample data for zero-day attacks).

3. Future Trend Assessment: Combining the innovative directions proposed in the literature (e.g., lightweight models, digital twin verification, federated learning) and industrial scenario requirements, potential research hotspots such as "physical-network integrated detection", "application of interpretable AI", and "construction of systematic defense systems" are identified, providing a basis for the subsequent evolutionary path of the technology.

2.6 Comparison with Related Work

This section takes 6 core surveys in the field of ICS intrusion detection as comparison objects. It systematically distinguishes this study from existing surveys along 4 key dimensions, as shown in Table 2. It clarifies that this study does not repeat existing achievements but makes incremental contributions through full-spectrum technology integration, an empirical closed loop, and scenario-based implementation.

Table 2: Comparative analysis of core surveys in ICS IDS and this paper

Comparison dimension	This study	[2]	[8]	[9]	[10]	[11]
Core technologies	Covers the entire technical spectrum of ICS intrusion detection	Takes classical ML as the core, with limited involvement in DL	Only covers ML techniques	Only covers cutting-edge deep learning technologies	Focuses on ICS cloud security, basic threats and encryption technologies	Only covers transfer learning technologies
Empirical support & Dataset	Integrates simulation data, real cases, and industrial-grade datasets	Mentions ML model performance indicators	Mentions ML model performance, but datasets only cover IT scenarios	Mentions Trans-former/LLM empiricism, but datasets focus on IT/IIoT	Slightly mentions cloud environment encryption tests	Only mentions transfer learning applications in SWaT/WADI datasets
Industrial scenario adaptation	Adapts to 5 types of segmented scenarios	Not segmented	Generalizes critical infrastructure	Adapts to IT/IIoT scenarios	Cloud-based ICS	Not segmented
Core innovations	1. A three-level classification system for 4 types of technologies; 2. Multi-dimens ional empirical integration; 3. Three types of actionable implem entation frameworks	1. Summarizes opportunities and challenges of ML in ICS security networks; 2. Analyzes optimization directions of ML models under resource constraints	1. Combs the application status of ML in critical infrastructure IDS; 2. Compares the performance of different ML algorithms in IT datasets	1. Systematically surveys Trans-former/LLM applications in IDS; 2. Analyzes technical details of models like ViT/GPT	1. Early combing of ICS cloud security risks; 2. Proposes cloud-based ICS encryption protection schemes	1. First systematic combing of transfer learning applications in ICS IDS; 2. Proposes paths for transfer learning to solve sample scarcity under resource constraints

In summary, the core differences between this study and the 6 core surveys lie in: at the technical dimension, upgrading from single technology/partial technologies to full-spectrum integration; at the empirical dimension, upgrading from scattered empiricism to a systematic closed-loop of simulation data and real cases; at the scenario dimension, upgrading from generalized scenarios to precise adaptation for ICS segmented industries. Through systematic integration and extension, this paper provides a more comprehensive, industry-practice-aligned reference for the ICS intrusion detection field, facilitating the technology's transition from theory to practice.

3 Particularities of Cyberspace Security in ICS

3.1 Uniqueness of Cybersecurity in ICS

In recent years, malicious cyberattacks against ICSs have surged significantly. Incidents such as Stuxnet and BlackEnergy attacks illustrate how a single spear-phishing email or compromised USB drive can provide attackers with access to remote networks [12]. Traditional security measures are no longer sufficient to protect ICS from these threats, underscoring the need for an in-depth analysis of ICS security vulnerabilities arising from their distinct network characteristics. This analysis is crucial for developing effective detection and defense strategies and for enhancing system design.

Initially, OT networks were designed to remain isolated from IT networks, with devices and applications in OT environments prioritizing reliability and availability over cybersecurity. For instance, in an ICS infrastructure, equipment that allows multi-user access often operates numerous processes with elevated privileges in an "always on" mode [2]. The primary goal of the ICS infrastructure is to ensure continuous, stable operations for as long as possible. Consequently, ICS systems emphasize availability and integrity over confidentiality. This prioritization begins with maximizing system availability to prevent disruptions, followed by ensuring data integrity to guarantee the system accurately represents ongoing operations. Finally, confidentiality is addressed through the encryption of real-time data within ICS environments.

Unlike traditional IT networks, OT networks in ICS environments handle both standard network traffic using TCP/IP protocols and data generated by physical processes and low-level components [13]. This integration between different layers creates opportunities for novel cyberattacks that exploit previously unseen vulnerabilities. Table 3 compares OT networks in ICS with traditional IT networks.

Table 3: Comparison of OT networks and IT networks

Property	OT networks	IT networks
Target	Data management and processing	Control and monitoring
Focus	Reliability and availability	Confidentiality and privacy
Delay sensitivity	High	Low
Fault tolerance	High	Low

The security requirements of ICS can be summarized as follows [14]:

- High real-time demands: In ICS, each physical device has a strictly limited operational time, and even minor deviations can lead to serious accidents.
- Limited computational resources: The sensors and actuators within ICS possess restricted processing and storage resources, which hinder the implementation of security programs.
- Fixed business logic: Any compromise of this logic can lead to catastrophic failures.
- Continuous operation requirement: It is essential to maintain the uninterrupted functioning of physical devices, as performing hard updates or restarts on industrial equipment is often challenging.
- Weakness in ICS protocols: The inadequate security features of ICS protocols increase the risk of attacks, particularly when these systems are connected to the Internet.

With the emergence of Industry 4.0, the convergence of IT and OT is accelerating. As the fundamental component of OT networks, ICS networks are increasingly exposed within IT environments, heightening security risks. Therefore, employing novel technologies for the detection and protection of ICS is crucial for ensuring their stable and reliable operation.

3.2 Method of ICS Network Attack

Network attacks targeting ICSs [15] typically follow a sequence that includes monitoring, system mapping, initial infection and data exfiltration, information preparation, final attack testing, event detection and response, and ultimately executing the attack. Specific manifestations of these network attacks against ICS [15] include loss of visibility, manipulation of views, denial of control, control manipulation, and loss of power. The various types of attacks can generally be categorized based on their methods, such as reconnaissance attacks [16], man-in-the-middle (MitM) attacks [17], injection attacks [18], replay attacks [19], and DoS attacks [20], as illustrated in Table 4.

Table 4: ICS attack types (classified according to attack methods)

Attack category	Methods of attack
Reconnaissance attacks [16]	• Understand the topology of the ICS • Identify vulnerable devices and the associated physical processes
Man-in-the-middle attacks [17]	• Read or modify communications • Inject or drop data packets
Injection attacks [18]	• Inject data or commands through compromised nodes • Drive the system into an unsafe state
Replay attacks [19]	• Replay previously valid messages
DoS attacks [20]	• Overload system resources, render devices unavailable • Disrupt communication between machines in the system

In the practical design and development of industrial systems, key concerns typically include real-time response performance, operational efficiency, and business continuity, while network security considerations often take a backseat. Once an ICS is tested and deployed, it must maintain a stable operational state for extended periods, which can limit future maintenance and upgrade flexibility. This inflexibility may inadvertently create opportunities for malicious attackers to introduce viruses and Trojans. Furthermore, due to the high availability requirements of ICS, redundant architecture designs are frequently implemented to ensure stable operations. However, this redundancy can also compromise the effective execution and comprehensive enforcement of various security policies.

At the same time, network security considerations are often marginalized. Once ICS is tested and deployed, it must maintain a stable operating state for an extended period, which often limits the flexibility of subsequent maintenance and upgrade activities for users, inadvertently creating opportunities for malicious attackers to introduce viruses and Trojans. Furthermore, given the stringent requirements for high availability in ICS, redundant architecture designs are commonly adopted to ensure stable operation. However, this also somewhat weakens the effective implementation and comprehensive coverage of various security policies. With the rapid development of Internet technologies, the integration of industrial control equipment and networks has significantly increased. Although several security measures have been deployed, the defense system remains vulnerable to complex security challenges posed by vulnerabilities, malware, and wireless technologies. Once attackers successfully exploit these security vulnerabilities, the consequences will likely be highly destructive. Given this, implementing uninterrupted real-time monitoring of information flow within industrial control networks to identify and respond to abnormal attack behaviors rapidly is a critical and indispensable link in ensuring system security and maintaining the security and stability of the industrial environment.

With its ability to instantly monitor and deeply analyse network communication activities, network intrusion detection technology effectively identifies and alerts to potential malicious attack attempts, laying a solid foundation for the subsequent deployment of defence strategies and rapid system recovery processes. This technology stands out for its high real-time responsiveness and proactive defence characteristics, which are increasingly becoming a focal point of research in ICS network security. It demonstrates significant practical significance in safeguarding industrial environment security and fully showcases its broad and far-reaching application prospects and value.

4 Landscape of ICS-IDS Technologies

As a core component of the security protection system for ICS, the IDS primarily identifies malicious attack behaviours or abnormal operational patterns within the ICS by collecting and analysing multidimensional data. It can effectively detect malware intrusions and various types of network attacks (e.g., Denial of Service (DoS) attacks, Man-in-the-Middle (MitM) attacks) [17].

From the perspective of technical principles, the working mechanism of ICS-IDS centers on "data-driven analysis": First, massive amounts of raw data are collected from the entire ICS link, covering both the network communication layer (e.g., features such as the time sequence of data packets in network traffic and the number of transmitted bytes) and the physical control layer (e.g., parameters such as real-time sensor measurements and actuator operating status) [21]. Subsequently, through methods such as feature extraction, pattern matching, or model inference, a baseline for the normal operating state of ICS is established and compared with real-time monitoring data. Finally, the determination of abnormal or attack behaviours is achieved. The technical classification and feature engineering of IDS can be traced back to classical data mining frameworks. The MADAM ID framework proposed by [22] extracts key features from audit data using association rule mining and frequent itemset mining. It combines them with the RIPPER classifier to classify attacks. This work was the first to systematically verify the IDS development workflow that integrates data mining, feature construction, and model training. The successful application of this framework to the 1998 DARPA dataset not only provided an early theoretical basis for the technical classification of rule-based, anomaly-based, and machine learning-based methods in this SLR but also offered a reference paradigm for the feature engineering of ICS-IDS [22].

Combining the current research achievements of ICS intrusion detection technology with the actual needs of industrial scenarios, this study classifies existing ICS intrusion detection technology systems into four core categories based on two dimensions: "differences in detection strategies" and "technical adaptation characteristics." These categories include rule-based, anomaly-based, machine learning-based, and specialised detection technologies. The core principles, typical methods, and application scenarios for each technology type will be elaborated in detail in subsequent sections. The technical classification framework is illustrated in Fig. 2.

With the "detection technology category" under the "data extraction dimension" in Section 2 of the SLR as the core, and combined with the typical characteristics of the literature, we classify the ICS-IDS using a three-level classification system consisting of general categories, technical principles, and specific methods. The details are presented in Fig. 2, which shows a three-level classification system for ICS-IDS, organised hierarchically into major categories, technical principles, and specific methods. By combining differences in detection strategies and adaptability to industrial scenarios, this classification system provides a framework for subsequent principal component analysis and performance comparisons of various technologies.

4.1 Rule-Based Detection

The Misuse-based Intrusion Detection System (MIDS) is a classic technical solution in ICS intrusion detection. Its core detection logic relies on pre-defined rules to match known attack features and vulnerability characteristics, thereby accurately identifying explicitly defined malicious behaviours within the system. A key advantage of this technology lies in its ability to build a standardised attack signature database using mature detection tools (e.g., Snort [23], Suricata [24]). For attack types included in the signature database, it can achieve a high detection rate without requiring complex model training processes.

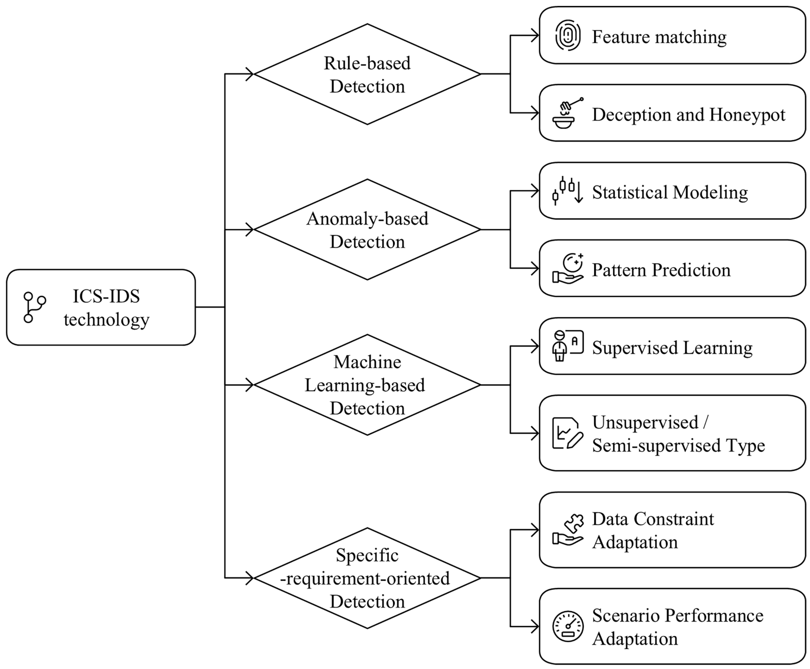

Figure 2: Classification of ICS-IDS

Unlike traditional Information Technology (IT) systems, ICS exhibits distinct industrial-scenario characteristics: its control loops operate according to fixed polling cycles (e.g., periodic collection of sensor data by PLCs and periodic issuance of actuator commands), resulting in highly stable communication and operational patterns. This characteristic is highly compatible with MIDS's detection logic: MIDS can optimise rule design based on ICS's fixed operating rules (e.g., by formulating matching rules for the periodic data frame structure of the Modbus protocol), thereby further improving detection accuracy. Meanwhile, MIDS only responds to "known threats" that match pre-defined rules, eliminating the need for complex anomaly modelling and analysis. As a result, it has low resource requirements, making it suitable for edge devices with limited computing power in ICS (e.g., embedded PLCs and Remote Terminal Units (RTUs)). Additionally, it can effectively control the false-positive rate, preventing unnecessary shutdowns of industrial processes triggered by false alarms.

However, MIDS also has significant technical limitations: its detection capability depends entirely on the coverage of the attack signature database, and it cannot identify zero-day attacks or new attack types not included in the database. This flaw is particularly prominent against the backdrop of continuous evolution in ICS attack methods. Within the rule-based detection technology system, the current mainstream implementation methods can be divided into the following two categories, as shown in Fig. 3. This figure illustrates the two core architectures and workflows of rule-based detection. For feature matching, a real-time comparison is conducted between the attack feature database and Snort/Suricata rule-matching engines, which output alerts for known attacks or labels for expected behaviours, and iteratively update the rule database. For deception and honeypot-based detection: Honeypot devices simulating PLCs (Programmable Logic Controllers)/RTUs (Remote Terminal Units) are deployed at the honeypot interaction layer to attract malicious attack behaviours and collect threat data. After extracting attack features, they are added to the attack feature database, enabling continuous detection of multi-stage attacks.

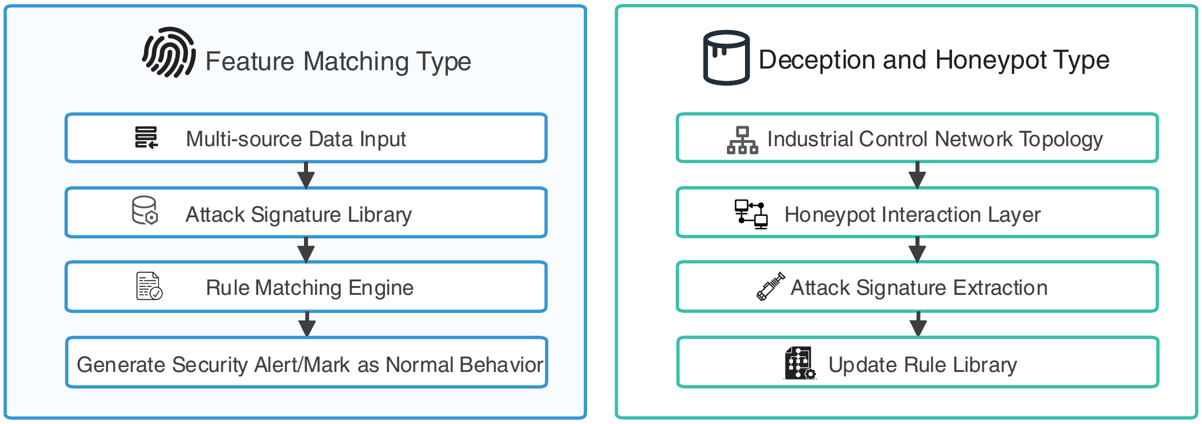

Figure 3: Architecture and workflow of rule-based detection

- **Feature Matching Type:** This method abstracts potential attack behaviors or known intrusion patterns into rule sets. Intrusion is flagged when system behavior or network traffic matches predefined rules—for instance, as described by Myers et al. [25] proposed an ICS anomaly detection technique based on process mining, constructing expected behavior models by collecting and preprocessing ICS device logs, and performing consistency checks for analysis. Bhardwaj et al. [26] introduced a behavior-based attack identification method tailored to IoT-oriented ICSs, utilizing process and task execution flow mining to detect deviations in the task and log events, verified through consistency checks.

This technique monitors the transitions between different system states to detect intrusions. An example is XSense [27], developed by CyberX, which detects attacks by classifying ICS state transitions as usual or malicious based on signals and indicators. Researchers are exploring additional parameters, such as industrial remote control systems [28] and response times, to detect abnormalities. For example, by analyzing these parameters directly or indirectly, researchers can detect alterations in current attack traffic patterns [29], identify fraudulent control devices [30], reveal subtle manipulations of the controller device code [31] roller device code o [31], and even deduce PLC CPU loads [32]. Additionally, some studies have explored innovative parameters in intrusion detection, such as control device radio frequency emissions and power consumption [33]. Sheng et al. [34] proposed a cyber-physical model for SCADA systems. This model detects cyber intrusions by extracting and correlating the communication patterns and states of ICS devices, and then evaluating the risk level of these intrusions to industrial processes. Experimental results demonstrate that the model achieves high accuracy in detecting various attack types, and its risk assessment method effectively distinguishes between different attack scenarios. Yang et al. [35] developed the iFinger method, which generates a deterministic finite automaton (DFA) as the device fingerprint from the register-state sequence of industrial equipment. Attack detection is realized through multiple approaches: analyzing visible registers in network traffic and sending crafted packets to obtain information from invisible registers. Validated on 10 types of industrial equipment, the method achieves a device identification F1-score of 97.1%, a recall rate of 98.0% for detecting attacks such as register replacement and code modification, and a detection latency of less than 2 s. This method addresses the challenge in industrial environments where equipment communication protocols are fixed. Still, attacks are highly concealed, thereby enhancing the ability to identify device identity forgery and logical tampering. Acharya et al. [36] proposed the ISERA architecture, which integrates network micro-segmentation, access control, industrial IDS, and the FTAS algorithm to achieve real-time threat detection and response. In tests involving DoS attacks and malware intrusions, the architecture exhibits response times of 1.5 s at the IT layer and 2 s at the OT layer, while maintaining system availability over 95% and successfully isolating affected areas. This solution addresses the vulnerabilities in traditional ICS architectures, including single points of failure and excessive reliance on the integration between IT and OT layers.

• **Deception and Honeypot Type:** This approach involves deploying honeypots—decoy systems designed to attract and analyze malicious activities. These systems collect information on threats and attacks, enabling the detection of compromised devices. For instance, Dutta et al. [37] developed an enhanced honeypot using SNAP7 and IMUNES to generate signatures and identify multi-stage attacks. Mesbah et al. [38] focused on low-interaction honeypots for analyzing unsolicited traffic and identifying tampering in SCADA networks. Yang et al. [39] designed a highly interactive honeypot for threat management, enabling sustained attack detection and proactive defense. Kempinski et al. [40] proposed a goal-oriented honeypot design to address the lack of structured reasoning for ICS honeypots. Pashaei et al. [41] designed a dual-agent honeypot system based on SARSA reinforcement learning. This system enhances detection capabilities through adversarial training and deploys Conpot and HoneyPLC to simulate Siemens S7 series Programmable Logic Controllers (PLCs). In detecting MitM and Distributed Denial of Service (DDoS) attacks, the system achieves an accuracy and F-measure of 0.98, with a false positive rate reduced by 99.9% compared to traditional IDSs. This solution addresses the issues of low interactivity and high vulnerability to attacker identification in traditional honeypots. Liang et al. [42] constructed a high-interactivity ICS simulation system that supports protocols such as Modbus and S7comm and actively diverts attack traffic through a P4-programmable switch. In Nmap fingerprint scanning and attack tests, the system demonstrates 100% consistency in responses with real industrial devices and can simulate the behavior of PLCs such as Schneider M580 and Siemens S7-1500.

Although the rule-driven type offers irreplaceable advantages in known-attack detection and real-time performance, its reliance on attack signatures makes it unable to cope with the evolution of industrial attacks. It must be combined with a dynamic update mechanism; otherwise, it will quickly become ineffective in complex attack scenarios.

4.2 Anomaly-Based Detection

The anomaly-based Intrusion Detection System (AIDS) is a core detection solution for unknown attacks and emerging threats in ICS. Its technical core lies in first constructing a baseline model of the ICS's normal operating state, then identifying abnormal behaviors beyond the normal range by comparing real-time monitoring data with the baseline. Unlike rule-based detection technology that relies on known attack signatures, AIDS does not require a pre-established attack signature database. It can detect unrecorded attack patterns (such as zero-day attacks and unknown command-tampering attacks) solely through the logic of "normal behaviour definition—abnormal deviation identification," thereby inherently advantageous for addressing the iterative evolution of ICS attack methods [14].

In traditional IT systems, AIDS often suffers from insufficient generalisation ability of baseline models due to the randomness and complexity of IT network behaviours, leading to a high false positive rate. However, this issue is significantly mitigated in ICS scenarios. The industrial nature of ICS determines that its operating process exhibits strong regularity: on the one hand, the periodic operations of control loops (e.g., fixed-frequency sampling of sensors by PLCs, periodic action commands for actuators) result in predictable temporal characteristics of network traffic and device state changes; on the other hand, ICS networks are usually physically or logically isolated from the external Internet, with relatively fixed network topologies and data interaction relationships, which reduces the impact of irrelevant interference factors on the normal behavior baseline [43]. This characteristic of "predictable behaviour and relatively isolated environment" dramatically improves the accuracy and stability of the AIDS baseline model, effectively reducing the risk of false positives and making its application in ICS scenarios significantly more reliable than in the traditional IT field. The implementation of anomaly-based detection technology in ICS focuses on accurately constructing a normal behaviour baseline suitable for industrial scenarios. The current mainstream technical paths can be divided into the following two categories, as shown in Fig. 4. This figure presents the dual-path modelling and detection logic of anomaly-based detection. In statistical anomaly detection, Industrial time-series data undergo data cleaning and feature extraction to construct a baseline of normal behaviour. The deviation calculation module compares real-time data with the baseline and dynamically adjusts thresholds to trigger anomaly alerts. In pattern-prediction-based anomaly detection, A frequent pattern database is built by mining ICS event sequences. The sequence comparison engine matches real-time sequences against patterns in the database to identify abnormal sequences and outputs detailed reports, including anomaly levels and involved devices.

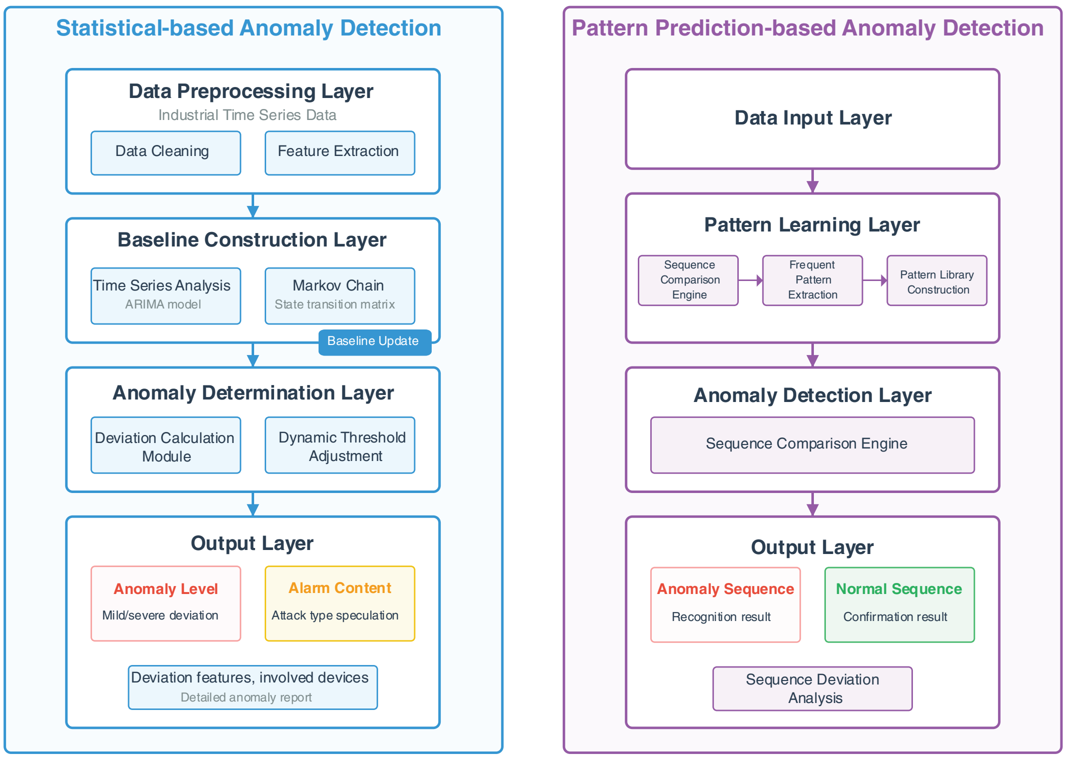

Figure 4: Dual-path modelling and detection logic for anomaly-based detection

- **Statistical-based Anomaly Detection:** This technique uses statistical algorithms to establish a behavioral profile for normal ICS operations, detecting deviations as potential anomalies. Time series analysis and Markov chains are commonly applied to analyze network traffic and system events [44]. For example, Marsden et al. [45] developed an IDS that uses probabilistic risk identification to detect replay attacks by analyzing Modbus TCP/IP traffic. Similarly, Ike et al. [46] introduced SCAPHY, which detects ICS attacks by analyzing physical process dependencies and identifying control activities that deviate from legitimate system behaviors. Jadidi et al. [47] proposed an automated method for detecting flooding attacks. This method collects PLC logs and network traffic to generate NetFlow data, and combines unsupervised histogram clustering with ARIMA/GARCH predictors to detect anomalies. Validated on the factory automation, Modbus, and SWAT datasets, the method achieves accuracies of 0.96, 0.83, and 0.92, respectively, and can effectively detect flooding attacks. Ryšavý et al. [48] developed a network traffic processing library that extracts packet-level and flow-level features, enabling an automated workflow from data preprocessing and feature engineering to model training. In terms of performance, its processing speed is an order of magnitude faster than that of the traditional tshark tool, supporting real-time traffic analysis and multiple detection methods. Aoudi et al. [49] proposed PaSaD (Pattern-based Sensor Anomaly Detection), a technology that detects stealthy attacks by monitoring structural changes in sensor time series. Specifically, singular spectrum analysis is used to extract the signal subspace of the system under regular operation, and the deviation score between real-time data and the normal subspace is calculated; an alarm is triggered when this score exceeds a predefined threshold.

- **Pattern Prediction-based Anomaly Detection:** This method analyses event sequence patterns within ICS networks to detect anomalies. Classic studies on sequence pattern analysis have provided a semantic-layer perspective for anomaly detection in ICS. Caselli et al. [50] noted that there exists a category of sequence attacks in ICS that trigger physical failures by tampering with the timing of legitimate events. In contrast, the individual events themselves show no anomalies. To address this, they proposed a modelling method based on a discrete-time Markov chain, extracting event sequences from industrial protocols to construct a state transition model, and detecting anomalies by calculating the weighted distance between real-time sequences and the standard model. In a test using Modbus traffic from a water treatment plant, this method successfully identified rapid valve opening-closing attacks with a false-positive rate of only 0.8%. The idea of integrating physical process semantic modelling in this work provides key technical references for subsequent anomaly detection of industrial time-series data [50]. Mitchell et al. [51] built a model based on ICS protocols and system behaviour specifications to monitor and detect intrusions. Lee et al. [52] applied machine learning techniques to identify patterns in network traffic and used fingerprinting to identify unregistered users. Ayodeji et al. [53] proposed an intrusion detection approach that identifies intrusions by analysing changes in process variables, which involves correlating physical processes. This method addresses the high false-positive rates in existing intrusion detection systems for complex industrial systems and improves detection accuracy by integrating multidimensional information. Gönen et al. [54] investigated false data injection (FDI) attacks targeting PLC registers. By analysing vulnerabilities in the Modbus protocol, they proposed a LiFi-based authentication model combined with continuous monitoring. This research fills the gap in the correlation analysis between physical processes and network behaviours in FDI attack detection.

Beyond the aforementioned anomaly-based detection approaches, hybrid detection is a classic technical direction in IDS, and early studies have provided valuable references for integrating ICS-IDS modules. The hybrid architecture proposed by [55] achieves complementary advantages by combining Self-Organising Maps and J48 decision trees: SOM identifies unknown attacks based on the quantisation error of normal behaviour baselines, while J48 matches known threats using attack signature rules, with the final judgment unified by a decision support system. This architecture achieved a detection rate of 99.9% and a false positive rate of only 1.25% on the KDD Cup 99 dataset, verifying that the hybrid mode effectively improves both detection accuracy and generalisation capability. It has thus established a paradigm for subsequent hybrid IDS solutions in ICS scenarios [55].

4.3 Machine Learning-Based Detection

With the increasing sophistication and stealth of attacks targeting Industrial Control Systems (ICS), traditional detection technologies relying on rules or single-anomaly modelling can no longer meet the defence requirements of high accuracy and wide coverage. Against this backdrop, Machine Learning (ML) technology has emerged as a core development direction in the field of ICS intrusion detection, leveraging its ability to extract features from complex data and conduct dynamic learning—its core logic is to enable algorithmic models to autonomously learn the pattern characteristics of normal and abnormal behaviors from massive ICS data (e.g., network traffic, device status, physical process parameters), thereby achieving intelligent classification and identification ICS.

Currently, mature ML methods applied in ICS intrusion detection span multiple technical areas: In the field of supervised learning, classification algorithms such as Support Vector Machines (SVM) [51] and Random Forests can train models on labelled "normal-attack" samples to achieve accurate discrimination of known attacks. In the field of deep learning, models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) [56] can capture deep correlation features in ICS time-series data (e.g., periodic sensor sampling values, PLC command sequences), enabling effective identification of stealthy attacks. Additionally, unsupervised/semi-supervised learning methods such as clustering and autoencoders can distinguish abnormal behaviours by exploiting the inherent data distribution patterns in scenarios where attack sample labels are scarce. Some advanced detection systems also integrate rule-based feature matching mechanisms [57,58], forming a hybrid detection framework of "dynamic ML identification + static signature database matching". This framework not only ensures efficient identification of known attacks but also achieves generalised detection of unknown threats. To address the challenges of IIoT dataset imbalance and multi-scenario adaptation, Popoola et al. [59] proposed a multi-stage deep learning architecture. This architecture optimises the detection of minority-class attacks through a three-stage process: coarse-grained filtering, fine-grained classification, and anomaly calibration. Its core innovation lies in integrating industrial temporal features into the feature engineering process, thereby adapting to the high-frequency data scenarios of energy IIoT devices. However, it fails to address the issue of adapting computing power for edge deployment.

Recent research achievements have fully verified the advantages of ML technology in ICS intrusion detection: For instance, Chang et al. [60] proposed a detection scheme combining reinforcement learning with convolutional autoencoders, where reinforcement learning dynamically optimises the feature extraction process of the autoencoder, significantly improving the accuracy of identifying ICS network anomalies; The statistical-ML hybrid method designed by Hao et al. [61] supports interactive traceability analysis of abnormal events while processing ICS stream data in real-time, balancing detection efficiency and interpretability; Experimental verification by Dini et al. [62] shows that, compared with traditional detection technologies, ML models (especially those for anomaly detection) perform better across key indicators, such as ICS attack classification accuracy and stealthy attack identification rate, making them more adaptable to the complex and ever-changing security protection needs of ICS. Given the high data noise and imbalanced distribution in IIoT, Dini et al. [62] systematically compared the performance of 6 machine learning (ML) models, including Random Forest (RF) and XGBoost, under different preprocessing strategies. Experimental validation demonstrated that on the X-IIoTID dataset, the XGBoost model with the combined SMOTE+Tomek Links balancing strategy achieved optimal performance, with an accuracy of 96.8%. In particular, the recognition rate for Mirai botnet attacks was improved by 12%.

Based on the model training methods and data dependency characteristics, current ML-based ICS intrusion detection systems can be further subdivided into two categories: supervised and unsupervised/semi-supervised. Their specific technical paths, adaptability to industrial scenarios, and performance, as shown in Fig. 5, will be analysed in detail in subsequent content.

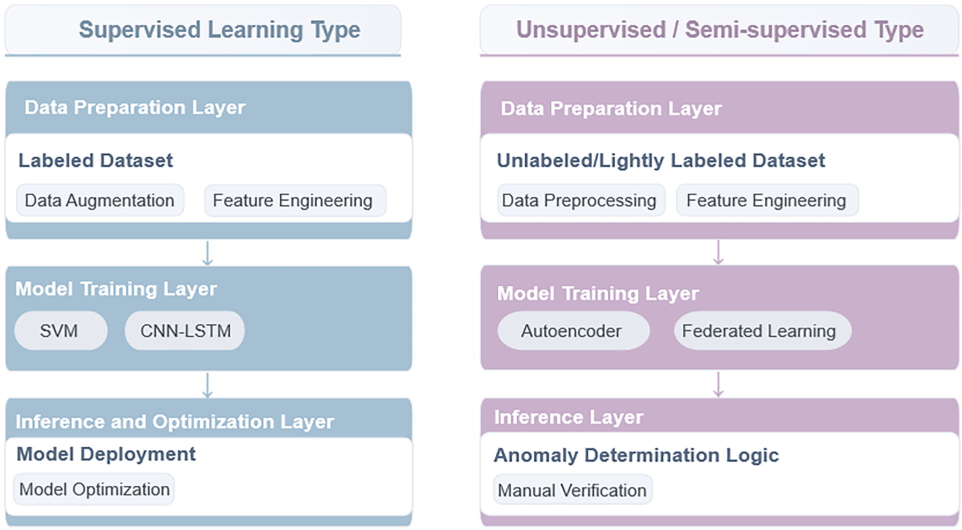

Figure 5: Workflow of typical models for machine learning-based detection

- **Supervised Learning Type:** It is noteworthy that early applications of machine learning in IDS have already focused on efficiency optimisation. A classic example is the CT-SVM framework proposed by [63]. This method screens support vectors using hierarchical clustering with a Dynamically Growing Self-Organising Tree and locates inter-class boundary points to reduce redundant training data. On the large-scale 1998 DARPA dataset, CT-SVM shortened the training time by 361 times compared with pure SVM while maintaining a detection accuracy of 69.8%, and outperformed methods such as Rocchio Bundling. This work provides core insights for the lightweight deployment of algorithms (e.g., SVMs and Random Forests) in subsequent ICS-IDS systems [63]. Anton et al. [64] suggested using SVMs and Random Forests for detecting DoS attacks. Vargas et al. [65] proposed a host-based intrusion detection system (HIDS) architecture suitable for embedded industrial devices. A prototype was implemented and evaluated on a PLC equipped with a real-time operating system (RTOS). The results demonstrate that the architecture can effectively detect intrusions while having minimal impact on system performance. Fang et al. [66] developed a feature selection method for ICS using a genetic algorithm and a novel fitness function. Experimental results show that this method effectively reduces feature dimensionality and improves classification accuracy. Ling et al. [67] proposed a bidirectional simple recurrent unit (Bi-SRU) method, which integrates skip connections and a bidirectional structure to alleviate the vanishing gradient problem and enhance temporal feature extraction. On the gas pipeline and water tank datasets, the method achieves accuracies of 96.23% and 92.94%, respectively, with shorter training time than the long short-term memory (LSTM) and gated recurrent unit (GRU) models. It is thus suitable for processing high-dimensional temporal traffic data. Mubarak et al. [68] adopted supervised machine learning algorithms to analyse communication traffic between ICS components. They extracted flow-based network features and implemented anomaly detection through port analysis and behaviour modelling. Nagarajan et al. [69] proposed a hybrid deep learning model. The hybrid honey badger-world cup algorithm (HHB-WCA) is employed for optimal feature selection, and the filtered features are then input into an autoencoder-bidirectional extended long short-term memory network (A-Bi-LSTM) for intrusion detection. On datasets such as the APA-DDoS and NSL-KDD, the model achieves 98.35% accuracy and 98.28% F1-score, with lower computational complexity than traditional methods. Imran et al. [70] evaluated the performance of multiple machine learning models in detecting advanced persistent threats (APTs) in ICS, using the Synthetic Minority Oversampling Technique (SMOTE) to address data imbalance. Among these models, the random forest performs best, achieving 99% accuracy, 97% F1-score, and a training time of only 0.12 s, outperforming deep learning models. Yang et al. [71] proposed a standardised ICS network data processing workflow that includes feature dimensionality reduction and data generation. They also extracted latent features using a bidirectional recurrent neural network (Bi-RNN) combined with an attention mechanism. The data generated by the generative adversarial network (GAN) achieves an F1-score of 92.88% on the SWaT dataset, outperforming other generation methods, and can identify key influential features. Al-Abassi et al. [72] proposed an ensemble deep learning model. Multiple stacked autoencoders are used to generate balanced representations from imbalanced data, and then a deep neural network (DNN) combined with a decision tree is employed to detect attacks. The model achieves 99.67% accuracy on the SWaT dataset and 96% on the Gas Pipeline dataset, with an F1-score significantly higher than that of traditional methods. Anthi et al. [73] proposed a three-level detection architecture, which sequentially realizes malicious packet identification, general attack type classification, and specific attack type subdivision. On the Gas Pipeline dataset, the random forest achieves a detection accuracy of 87.4%, the J48 algorithm attains an F1-score of 74.5% for general attack identification, and the F1-score for specific attack classification reaches 44.5%. Hwang et al. [74] designed a multi-model fusion Bi-LSTM anomaly detection framework that incorporates SHAP (Shapley Additive exPlanations) technology to visualise the contributions of abnormal sensors. On the HAI dataset, the framework achieves an eTaPR F1-score of 0.959, outperforming the champion model from HAICon 2020. It successfully detects 49 of 50 attack types, missing only 1. Wang et al. [75] proposed a layer-wise relevance propagation (LRP) method to explain the basis of DNN detection. They also improved data normalisation to enhance the distinguishability between normal and attack data. On the gas pipeline dataset, the method accurately identifies key attack attributes, such as command injection and response injection. Cluster analysis shows that the hidden-layer output is highly correlated with attack types, achieving an accuracy of over 95%. Zhang et al. [76] proposed a multi-layer defence intrusion detection system that integrates network traffic, host system data, and physical process data. Supervised learning models, such as k-nearest neighbours (KNN) and decision trees, are utilised for network and system data. In contrast, the autoassociative kernel regression (AAKR) model is employed to process the data. Experiments show that the KNN model achieves an actual positive rate of 98.84%. The Bagging and random forest models have a false positive rate of 0. The AAKR model can trigger alarms in the early stage of physical process anomalies.

- **Unsupervised/Semi-supervised Type:** Early explorations of hybrid architectures in machine learning-based IDS have provided essential references for industrial scenarios. The DT-SVM hybrid model proposed by [77] extracts data node information using decision trees to assist the SVM in feature learning, while designing an ensemble method to weight-fuse the outputs of multiple classifiers. On the KDD Cup 99 dataset, this method achieved a 100% detection rate for Probe attacks, improved the accuracy for R2L attacks to 97.16%, and reduced computational overhead by 32% compared to pure SVM. Such a classifier-complementary optimisation approach laid the foundation for the design of subsequent hybrid models in ICS-IDS, such as CNN-LSTM combined with Random Forest, and is particularly instructive for addressing the detection bottlenecks of minority industrial attacks [77]. Bernieri et al. [78] developed an unsupervised machine learning-based framework that separates IT and OT traffic to capture side-channel data, detecting otherwise overlooked attacks. Zainudin et al. [79] proposed a low-complexity technique for Software-Defined Networking ICS using Federated Learning, enhancing detection efficiency through feature selection. Ortega-Fernandez et al. [80] introduced a deep autoencoder-based system for detecting DDoS attacks in an unsupervised learning environment, achieving superior performance. Nedeljkovic et al. [81] proposed a semi-supervised method based on CNNs, which automatically selects appropriate CNN architectures and detection thresholds for detecting communication link attacks. On the SWaT dataset, the method achieves an F1-score of 0.902, an accuracy of 97.846%, and a false positive rate of 0.135%. In a custom electro-pneumatic positioning system, it can detect multiple types of attacks in real time, such as linear attacks and harmonic injection. Zeng et al. [82] proposed a federated intrusion detection backdoor defence framework based on multi-objective clustering combinations. The non-dominated sorting genetic algorithm II (NSGA-II) is employed to optimise the combination of 12 clustering strategies and their corresponding confidence levels, aiming to maximise both the true positive rate (TPR) and the true negative rate (TNR). On the SWaT, WADI, and PSA datasets, compared with single clustering strategies and traditional methods, the backdoor sample misclassification rate of this framework is reduced to below 0.03, and the maximum TNR reaches 96.76%, enabling effective defence against SIG and BadNet backdoor attacks. Kim et al. [83] compared the performance of five time-series anomaly detection models on the SWaT and HAI datasets. This study addresses two key issues in ICS anomaly detection: the lack of unified standards for model selection and the high costs caused by large-scale training data. It clarifies the applicable scenarios of different models and provides a basis for model selection in practical deployment. Kravchik et al. [84] proposed a 1D convolutional neural network model. By predicting sensor and actuator time-series data, the model detects attacks by calculating deviations between predicted and actual values. This method addresses the challenges of complex training and high computational costs associated with traditional recurrent neural networks, enabling efficient detection of stealthy attacks and meeting the real-time requirements of ICS. Khan et al. [85] proposed an IDS model based on LSTM autoencoders. The model processes network traffic through statistical feature extraction and detects attacks by combining standardised probability transformations and reconstruction-error analysis. On the Gas Pipeline dataset, it achieves 97.95% accuracy, and on the UNSW-NB15 dataset, 97.62% accuracy. The training time is only 7–8 min, and the detection latency is as low as 0.021 ms. Chahal et al. [86] proposed the FedAvg-integrated classifier architecture, which enables collaborative model training among distributed IIoT nodes via Federated Learning while preserving the privacy of local device data. On the TON-IoT dataset, this model achieved a detection accuracy of 98.2%, reduced latency by 50 ms compared to the centralised CNN, and maintained an accuracy of 92% even when 50% of node data was missing, thus adapting to the heterogeneous network environments of multi-factory IIoT. Srinivasan and Senthilkumar [87] proposed a CNN-blockchain-RL hybrid framework, which uses CNN for IIoT traffic anomaly identification, leverages blockchain to ensure the integrity of detection results, and employs reinforcement learning (RL) to achieve autonomous threat mitigation. On the BoT-IoT dataset, this framework achieved 96.8% recognition accuracy for DDoS attacks, reduced threat response time by 90.8%, and thus adapts to the real-time detection and active defence requirements of IIoT in smart manufacturing. Bansal et al. [88] systematically summarised the lightweight IIoT-IDS technology routes and proposed a compressed CNN and edge preprocessing scheme. By pruning 30% of redundant convolutional kernels, the scheme maintained an accuracy of 94.3% on the Edge-IIoTset dataset while reducing the model size by 65%, making it suitable for resource-constrained devices such as PLCs.

Although machine learning-based methods can detect unknown attacks, their “black-box” nature makes it challenging to build trust in industrial decision-making. For example, when the model identifies abnormalities in PLC registers, operation and maintenance personnel cannot determine whether they are caused by real attacks or by sensor noise. It is necessary to improve credibility by integrating interpretable AI with industrial knowledge; otherwise, it will be challenging to implement in practice.

4.4 Specific-Requirement-Oriented Detection

Although ICS intrusion detection systems based on rules, anomalies, and machine learning have been applied in some scenarios, the complexity and diversity of industrial environments have led to numerous implementation bottlenecks for existing general-purpose detection solutions. These bottlenecks include limited coverage of emerging and stealthy attacks, excessive latency in real-time data stream processing (which fails to meet the millisecond-level response requirements of industrial control), low efficiency in feature extraction caused by high-dimensional industrial data (e.g., concurrent data collected by multiple sensors), and dataset imbalance arising from scarce attack samples and excessive normal data [89]. The superposition of these issues directly results in reduced detection accuracy and increased false favorable rates of general-purpose detection solutions in real industrial scenarios, making it difficult for them to adapt to the differentiated operating requirements of ICS across various industries (e.g., power SCADA systems, water treatment PLC systems, and oil and gas pipeline control networks).

To address the bottlenecks above, the research community has begun to focus on developing "scenario-specific" and "customised" detection technologies. Dedicated intrusion detection solutions are designed to cater to the specific operational needs and environmental constraints of ICS. The industrial adaptability of detection systems is enhanced by specifically resolving single or composite technical challenges. Such specific requirement-based detection technologies are not entirely new systems, independent of the three preceding technology categories; instead, they are optimisations and innovations based on existing technical frameworks, combined with the characteristics of industrial scenarios. For example, sample generation and model training strategies are optimised to address dataset imbalance, lightweight detection algorithms are designed to meet real-time requirements, and industrial physical mechanisms are integrated to verify results, thereby reducing high false favourable rates.

Currently, ICS intrusion detection systems based on specific requirements have formed several distinct research branches, each focused on addressing specific pain points in industrial scenarios. In subsequent sections, from dimensions such as "data constraint adaptation" and "scenario performance adaptation," the optimisation ideas, implementation methods, and application effects of various technologies in typical industrial scenarios will be elaborated in detail, providing customised technical references for the security protection of ICS in different industries, as shown in Fig. 6. This figure shows the scenario-specific solution architecture for specific demand-oriented detection, with optimisation paths designed for four types of core industrial pain points. To address adaptation to imbalanced datasets, SMOTE is used to synthesise attack samples, and feature selection is applied to address the low proportion of attack samples. To optimise the false-positive rate, Joint verification of network anomaly detection and physical models is implemented to eliminate misjudgments caused by industrial noise/transient faults. To address the real-time response requirement, Model compression, edge deployment, and feature simplification are adopted to meet the millisecond-level latency requirements of scenarios such as power SCADA. To address the adaptation to noisy environments, Noise suppression, data augmentation, and robust model training are combined to resist data noise caused by electromagnetic interference in industrial sites.

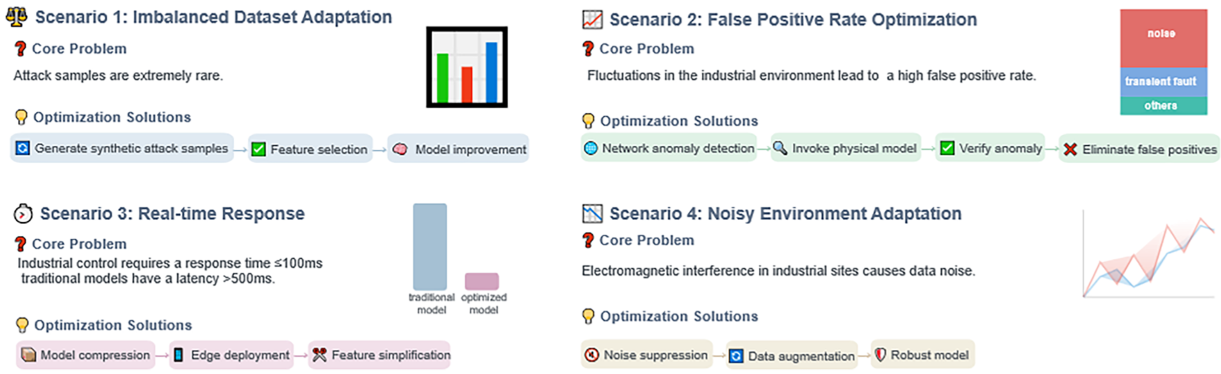

Figure 6: Scenario-based solution architecture for specific-requirement-oriented detection

- **IDS for Imbalanced Datasets:** Traditional ICS intrusion detection systems often neglect the imbalance in resource allocation across hierarchical devices, focusing primarily on known attack patterns. This leaves critical nodes vulnerable to unknown threats. To resolve this, Soliman et al. [89] introduced an intelligent detection system that uses singular value decomposition to reduce data features while employing the synthetic minority over-sampling technique to mitigate overfitting and underfitting issues, improving classification accuracy. Al-abassi et al. [72] proposed a detection method using ensemble deep learning to create balanced dataset representations, enhancing the system's ability to detect attacks. Ali et al. [90] presented an instance-based intrusion detection technique for SCADA systems to improve detection performance. Wang et al. [91] developed a hybrid approach combining convolutional neural networks and bidirectional long short-term memory networks, using the synthetic minority over-sampling technique in the preprocessing stage to address data imbalance and thereby reduce the impact of noise in the majority classes. Finally, Xiang et al. [92] proposed a multi-level hierarchical framework that deploys packet signature models and an enhanced fast search and find of density peaks model at different layers, facilitating the detection of both known and unknown attacks with improved speed and accuracy.
- **Integrated Perception-Based IDS:** Traditional anomaly detection systems mainly perform local analyses, often missing correlations between devices and attack processes. This limitation hinders their ability to detect network-wide attacks or anticipate future ones. To overcome this, Jadidi et al. [93] proposed a comprehensive anomaly detection solution using recurrent neural networks that not only detects attacks but also predicts future attack patterns. Additionally, multi-layer and multi-domain detection methods have gained attention. Bernieri et al. [78] adopted a distributed detection approach, integrating information from various ICS points to identify more complex vulnerabilities. Kim et al. [83] developed a hierarchical IDS that consolidates data from distributed sources to detect distributed-impact attacks. Caselli et al. [50] introduced a sequence-aware IDS that monitors ICS network security by analyzing event sequences, enhancing the detection of evolving threats.
- **Real-Time Response-Based IDS:** Current ICS intrusion detection methods often struggle with latency and are unable to extract relevant features from real-time data, underscoring the need for more efficient and responsive detection approaches. Ahakonye et al. [57] employed a fusion feature selection method in real-time SCADA networks to classify and detect attacks, developing a highly effective intrusion detection model with improved detection rates. Similarly, Abid et al. [51,94] integrated cloud computing and big data technologies for data fusion, creating an ICS real-time intrusion detection system that reduces false alarms while enhancing accuracy and efficiency. The introduction of digital twin technology also presents new opportunities for safeguarding real-time ICS environments [95].

Unlike traditional systems that rely on historical data for security, digital twins can operate in multiple modes [96]. Akbarian et al. [97] showed that a digital twin system reduces negative impacts on real-time operations while using fewer computing resources. Dietz and Pernul [98] further demonstrated that digital twins can simulate historical data and optimize performance.

- **Explainable IDS:** Traditional rule-based methods depend heavily on manual configurations, and the subtlety of attacks complicates the effectiveness of these rules. Machine and deep learning approaches often lack transparency due to their complex designs, and the semantic gap between the models and operational interpretations restricts their practical use. To address these issues, Xu et al. [99] proposed an intrusion detection method grounded in anomaly logic representation learning. This approach employs a lightweight neural network and uses knowledge distillation to achieve robust classification, enabling the direct generation of clear, concise intrusion detection rules from the model's learned knowledge. The model's hierarchical structure and residual connections enhance the explainability of the regulations.
- **IDS for Noisy Environments:** Most existing intrusion detection techniques are developed in noise-free, ideal settings, overlooking the inherent noise and complexity present in actual industrial environments. To tackle this challenge, Izuazu et al. [100] introduced a security framework that effectively differentiates between attacks, normal operations, and noise through the analysis of ICS network traffic. This approach can successfully identify malicious activities amidst routine industrial network operations, showcasing enhanced robustness and detection accuracy. Gu et al. [101] proposed a data-augmented intrusion detection system. This system expands attack data using the CenterBorderline_SMOTE algorithm and combines a reconstructed convolutional neural network (CNN) to extract features and perform classification. On the SWaT and S7 datasets, the system achieves a detection accuracy of over 97% and a relative error reduction rate (RERR) that is significantly higher than that of traditional methods. Perales et al. [102] proposed a unified framework based on edge computing, software-defined networking (SDN), and network function virtualization (NFV). This framework deploys applications such as cyber threat detection, indoor positioning, activity recognition, and shared workspace security. On the Electra dataset, neural network-based models within the framework can process 217 feature vectors per second, achieve attack-detection accuracy over 97%, and provide real-time responses. Fan et al. [103] proposed a defense-in-depth system that includes firewalls, intrusion detection, and access control, and discussed both anomaly detection and signature-based detection technologies. Nankya et al. [104] integrated IDS, anomaly detection, and signature-based detection, and combined them with the Dragos platform to achieve real-time monitoring and response. Experiments show that this integrated system achieves a detection rate of 92%, a false-positive rate of 5%, a response time of 2 s, and a CPU utilization of 30%, covering 85% of threat types. Hui et al. [105] constructed a testbed consisting of 4 physical sub-processes and a multi-layer network architecture. This testbed supports protocols such as S7comm and Profinet, can simulate the interaction between PLC control logic and physical processes, and provides a testing environment for IDS algorithms.

4.5 Multi-Dimensional Comparison of Core ICS-IDS Methods

The core architectures of the above four types of detection technologies are compared in Table 5.

Table 5: Comparison of ICS attack detection technologies

Technology	Data input	Core processing module	Output result
Rule-Based detection	Network traffic device logs	Attack signature database Snort/Suricata rule matching engine	Alerts for known attacks

(Continued)

Table 5 (continued)

Technology	Data input	Core processing module	Output result
Anomaly-based detection	Sensor data PLC status	Normal behavior baseline model deviation calculation engine	Alerts for abnormal behaviors
Machine learning-based detection	Multi-source heterogeneous data	Feature extraction model training, classifier	Attack type confidence
Specific-requirement-oriented detection	Imbalanced dataset real-time streaming data	SMOTE sampling lightweight quantization model cyber-physical fusion verification	Attack alerts adapted to scenarios

The rule-driven type excels in scenarios involving known attacks and high real-time requirements, but cannot address unknown attacks. The machine learning-based type can detect unknown attacks but sacrifices real-time performance and increases resource consumption, making it only suitable for scenarios with low real-time requirements. When an industrial scenario involves both known and unknown attacks, a hybrid framework combining rule-driven approaches and lightweight ML models can be adopted to balance detection coverage and real-time performance. The high false-positive rate of anomaly-driven approaches leads to dire consequences in industrial settings, so this technology is only suitable for high-fault-tolerance scenarios. However, the rule-driven type's inability to detect unknown attacks poses security risks to critical infrastructure, and it is necessary to pair it with technology tailored to specific requirements to address this deficiency.

Next, we systematically compare differences across three dimensions—performance quantification, scenario scalability, and practical trade-offs—among four method types: rule-based, anomaly-based, machine learning-based, and specific-requirement-oriented detection, to provide a clear basis for technology selection in industrial scenarios, as shown in Table 6.

Table 6: Multi-dimensional comparative analysis of ICS attack detection technologies

Dimension	Indicator	Rule-based detection	Anomaly-based detection	Machine learning-based detection	Specific-requirement-oriented detection
Performance indicators	Detection accuracy	92%–98% = (known attacks only) [23,35]	85%–93% (including unknown attacks) [49,52]	90%–99% (known + unknown attacks) [70,72]	93%–97% (after scenario adaptation) [51,82,96]
	False positive rate	0.1%–1.2% [35]	2.5%–5.0% (affected by industrial noise) [49]	1.0%–3.5% (afte model optimization) [67,70]	0.8%–2.0% (after scenario verification) [82,92]
	Detection latency	0.1–10 ms (lightweight matching) [23,36]	50–200 ms (baseline modeling time) [45,49]	20–150 ms (model inference time) [67,85]	5–80 ms (optimized on demand) [51,82,94]
Scalability and compatibility	Industrial device adaptation	High [35]	Medium [49,54]	Low–Medium [65,85]	Medium–High [82,97]

(Continued)

Table 6 (continued)

Dimension	Indicator	Rule-based detection	Anomaly-based detection	Machine learning-based detection	Specific-requirement-oriented detection
	Industrial protocol compatibility	Medium [35]	Medium [41,53]	High [69,83]	High [93,102]
	Data Volume Dependence	Low [23]	Medium [45,48]	High [62,72]	Medium [89,91]
Core trade-off relationships	Detection Capability vs. Resource Occupation	Strong in known attack detection, extremely low resource occupation, but completely unable to handle unknown attacks	Can detect unknown attacks, but higher resource occupation than rule-based and greatly affected by industrial noise	Widest detection range, but high resource occupation, limited edge deployment	Balances detection capability and resources, but development cost is higher than the first three
	Deployment Cost vs. Maintenance Difficulty	Low deployment cost, high maintenance cost [24,40]	Medium deployment cost, medium maintenance cost [47,52]	High deployment cost, low maintenance cost [66,74]	High deployment cost, medium maintenance cost [90,98]
	Scenario Adaptation vs. Universality	Poor universality, but optimal adaptation to known attack scenarios	Medium universality, optimal adaptation to unknown attack scenarios, but prone to misjudgment due to normal fluctuations	High universality, optimal adaptation to multiple scenarios, but requires scenario-specific parameter tuning	Optimal scenario adaptation, but worst universality

Next, with reference to Table 6, the underlying causes of differences in performance indicators among the technologies above are discussed from a quantitative perspective.

- **Accuracy Difference:** The rule-driven type (92%–98%) achieves higher accuracy for known attacks than the anomaly-driven type (85%–93%). This is because the former relies on predefined attack signatures, enabling unambiguous matching; in contrast, the anomaly-driven type relies on normal behavior baselines, and sensor noise in industrial environments can cause deviations from these baselines, thereby reducing accuracy. The machine learning-based type (90%–99%) offers a wide range of accuracy: supervised learning models can optimize attack detection using labeled samples, while unsupervised models can capture unknown attack patterns. However, sample quality significantly impacts accuracy—when the proportion of attack samples is <5%, the accuracy of ML models drops to approximately 95%, requiring techniques such as SMOTE to balance the dataset.
- **Latency Difference:** The latency of the rule-driven type (0.1–10 ms) is much lower than that of the machine learning-based type (20–150 ms). The core reason is that rule matching only requires packet feature comparison. In contrast, ML models require additional steps such as feature extraction and model inference, resulting in a significant increase in inference time on edge devices. The specific

requirement-oriented type reduces latency to 5–80 ms through model lightweighting, which can adapt to some real-time scenarios. Still, its development cost is 2–3 times higher than that of the rule-driven type.

- **False Positive Rate Difference:** The rule-driven type has the lowest false-positive rate (0.1%–1.2%), as its rules are based on explicit attack signatures, thereby avoiding misjudgments of normal behavior. The anomaly-driven type has the highest false positive rate (2.5%–5.0%), since normal fluctuations in industrial environments are easily misclassified as attacks. The machine learning-based type controls the false positive rate within 1.0%–3.5% through feature engineering and model optimization. However, this rate is still higher than that of the rule-driven type, necessitating a trade-off between detection range and false positive rate.

4.6 Empirical Verification of ICS-IDS Technologies

This section, based on the selected literature, integrates the experimental results of various detection technologies. Through quantitative tables and case studies, it provides empirical support for technical performance claims and verifies the practicality of these technologies in industrial settings. The details are presented in Table 7.

Table 7: Comparison of ICS-IDS technologies empirical verification

Technology	Representative method	Validation dataset/Experimental scenario	Core performance indicators
Rule-Based detection	iFinger (Device Fingerprint Matching) [35]	Measured data of 10 types of industrial devices (PLC/RTU)	F1-score for device identification: 97.1%; Recall rate for register tampering attack: 98.0%; Detection delay: <2 ms
	ISERA architecture [36]	Simulated DoS attack + malicious software intrusion scenario	IT layer response time: 1.5 s; OT layer response time: 2 s; System availability: maintained above 95%; Attack isolation success rate: 100%
Anomaly-based detection	PaSaD (Sensor Temporal Analysis) [49]	SWaT water treatment ICS dataset	Accuracy of stealth attack detection: 92%; False positive rate: 2.3%; Recognition rate of sensor data injection attack: 90%+
	Traffic temporal analysis [48]	Factory automation dataset + Modbus dataset	Data processing speed: surpasses traditional tools by one order of magnitude; Real-time detection accuracy: 0.96 (factory automation), 0.83 (Modbus)

(Continued)

Table 7 (continued)

Technology	Representative method	Validation dataset/Experimental scenario	Core performance indicators
Machine learning-based detection	Bi-SRU (Bidirectional Simple Recurrent Unit) [67]	Gas pipeline dataset + water tank control dataset	Accuracy in gas pipeline scenario: 96.23%; Accuracy in water tank scenario: 92.94%; Training time: 30% shorter than LSTM
	A-Bi-LSTM (Autoencoder + Bidirectional LSTM) [69]	APA-DDoS + NSL-KDD dataset	Highest accuracy: 98.35%; F1-score: 98.28%; Computational complexity: reduced by 40% compared to traditional DL models
Specific-requirement-oriented detection	Federated clustering fusion framework [82]	SWaT+WADI water treatment/water supply ICS dataset	When the proportion of attack samples is 3%, accuracy still reaches 95.2%; Backdoor sample misclassification rate: <0.03; True negative rate (TNR): up to 96.76%
	Dual-proxy honeypot system [41]	Simulated S7 series PLC communication scenario	MitM/DDoS attack detection accuracy: 0.98; False positive rate: reduced by 99.9% compared to traditional IDS; PLC simulation interaction consistency: 100%

The core of applicability in real-time industrial environments lies in the degree of alignment between technical performance and scenario requirements. For scenarios with extremely high real-time requirements (≤100 ms) and clear attack types (e.g., power systems, automotive manufacturing), the rule-driven type is the optimal choice, as its low latency and low false-positive rate directly meet these needs. For scenarios with moderate real-time requirements (≤200 ms) that need to address unknown attacks (e.g., water treatment, general manufacturing), the lightweight machine learning-based type is more suitable—it balances real-time performance and detection range through model compression. For scenarios with low real-time requirements (>200 ms) and data imbalance (e.g., cloud monitoring in smart factories), the requirement-oriented type can improve detection capabilities through sample generation and cross-domain learning, without concern for real-time constraints.

Meanwhile, it should be noted that the fault tolerance of industrial scenarios inversely affects technology selection. In low fault tolerance scenarios (e.g., nuclear power plants, oil pipelines), even if real-time requirements are met, technologies with a false positive rate exceeding 1% should be avoided; priority must be given to the rule-driven type (with a false positive rate <1%) or optimized machine learning-based type.

5 Analysis of Challenges

Based on an analysis of 115 studies (2000–2025) included in the SLR, the current IDS technology for ICS faces several core challenges in its implementation in real-world industrial scenarios, as illustrated in Fig. 7. These issues directly constrain the reliability and practicality of detection systems.

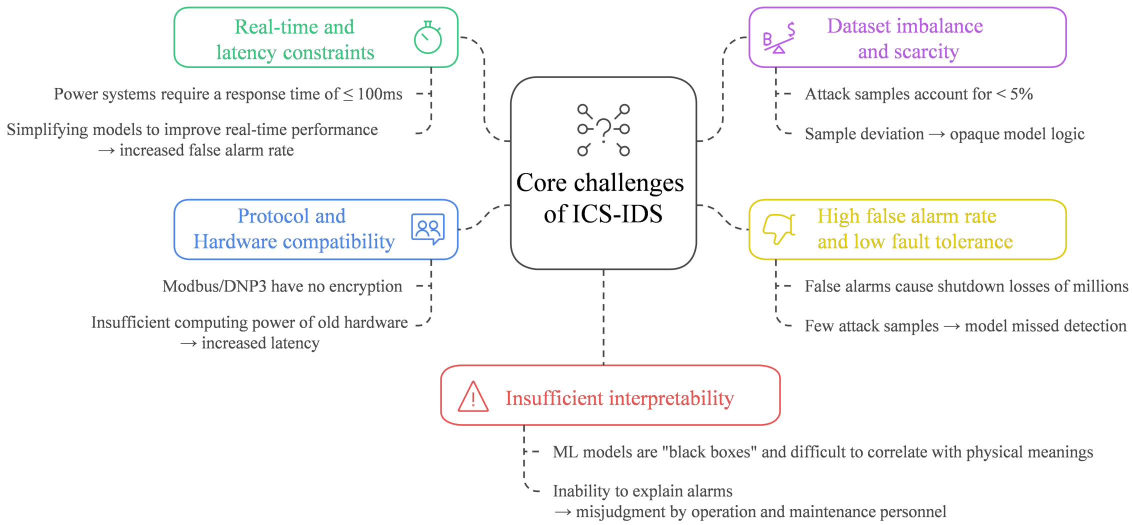

Figure 7: Core challenges of ICS-IDS

5.1 *Conflict between Real-Time Performance and Latency Constraints in Industrial Environments*

ICS imposes stringent requirements on real-time performance. For example, the response time for control commands in power systems must be ≤100 ms. However, existing detection technologies, such as machine learning, often suffer from detection latency exceeding the threshold due to their high computational complexity.

Deep neural networks require extensive parameter calculations. When deployed on edge devices such as Programmable Logic Controllers (PLCs) and sensors, they are limited by the low computing power of industrial hardware, making it challenging to meet millisecond-level response requirements [106]. During multi-source data fusion—e.g., integrating network traffic with physical sensor data—the high proportion of time consumed by data preprocessing further exacerbates latency [107].

5.2 *Dataset Imbalance and Sample Scarcity*

The number of ICS attack samples is far smaller than that of normal operational data, leading detection models to be biased toward standard patterns and resulting in a high false negative rate for unknown attacks.

Data in industrial scenarios is highly sensitive, and public datasets (e.g., CSE-CIC-IDS2018) mainly consist of simulated data, which exhibit a distribution discrepancy compared to real ICS environments [108]. For zero-day attacks, there are no historical samples, making it difficult for traditional supervised learning models to learn their features. Reliance on manual annotation further exacerbates sample scarcity [109].

5.3 *Contradiction between High False Positive Rates and Low Fault Tolerance of Industrial Systems*

In ICS environments, false positives can trigger unnecessary emergency shutdowns, causing substantial economic losses. Consequently, the tolerance for falsely favorable rates is much lower than that in IT systems, but existing technologies struggle to meet this requirement.

Normal fluctuations occur in industrial environments (e.g., sensor noise, transient equipment faults), which can be misclassified as attacks by anomaly detection models [110]. The specificity of industrial protocols—such as the periodic communication of Modbus—renders traditional threshold settings ineffective, and rule-based matching is vulnerable to interference from typically variable traffic [111].

5.4 Compatibility Limitations of Protocols and Hardware

ICS protocols are diverse, and some outdated protocols lack security extensions, making it difficult for detection technologies to adapt to heterogeneous environments. Meanwhile, the limited computing power of industrial hardware prevents the deployment of complex detection algorithms.

Traditional industrial protocols were not designed with security in mind and lack encryption or authentication fields, which hinders detection systems from distinguishing between normal and malicious traffic [112]. Early research on lightweight IDS in the IoT domain has provided valuable insights for the compatibility of edge devices in ICS. The SVELTE architecture proposed by [113], which integrates 6LoWPAN Border Route centralised modelling with lightweight node module design, directly inspired subsequent lightweight detection modules for PLC/RTU in ICS, effectively alleviating the contradiction between complex algorithms and hardware resource constraints [113].

With the integration of ICS into industrial clouds, the compatibility issues of traditional Intrusion Detection and Prevention Systems become even more prominent. A systematic review by [114] noted that the dynamic nature of cloud environments, virtualisation vulnerabilities, and multi-tenant isolation requirements demand that IDPSs possess greater scalability and adaptability. This conclusion is equally applicable to industrial cloud scenarios: the diversity of ICS protocols and the limited computing power of edge devices require drawing on classical approaches such as ontology-based unified knowledge sharing and autonomic computing self-configuration, which provide solutions for cross-protocol compatibility and lightweight deployment [114].

5.5 Conflict between Insufficient Interpretability and Trust in Industrial Decision-Making

In industrial scenarios, it is essential to clearly explain "why an event is identified as an attack." However, machine learning models are often "black boxes," and their outputs are challenging to interpret—this reduces the trust of operations and maintenance personnel.

The feature extraction process of complex models (e.g., deep autoencoders) is opaque, making it impossible to correlate model outputs with industrial physical meanings (e.g., the relationship between "abnormal temperature sensor data" and "attack vectors"). Existing interpretability methods, such as attention mechanisms, are susceptible to noise interference in industrial data, resulting in a decline in interpretation accuracy [115].

The challenges above are interrelated. For instance, simplifying models to improve real-time performance may lead to higher false positive rates; dataset imbalance can exacerbate model bias and further reduce interpretability. Collectively, these issues constitute core obstacles to the practical implementation of ICS-IDS technology and also provide clear directions for future development.

6 Future Hotspots of ICS-IDS

Based on the bibliometric analysis of relevant literature through a Systematic Literature Review (SLR), and considering the challenges encountered in the current technology implementation—such as insufficient real-time performance, defects in dataset quality, and high false favourable rates—the future research hotspots of ICS intrusion detection technology will focus on addressing the bottlenecks above. The specific evolutionary paths can be summarised into the following four directions, as shown in Table 7. The five future hotspots proposed in this paper are not general directions but rather targeted solutions that address the core research gaps identified in Section 5. Their corresponding relationships have been systematically clarified in Table 8.

Table 8: Comparison of hotspot directions

Hotspot direction	Addressed difficulties	Core technologies
Lightweight intelligent Detection technology	Conflicts between the edge device resources and real-time performance	Lightweight deep learning models edge-cloud collaborative architecture hardware-level customised algorithm optimisation
Data-driven robustness Enhancement technology	Data distribution differences and sample scarcity	Industrial scenario-specific data augmentation federated and cross-domain transfer learning in-depth application of unsupervised/semi-supervised learning
Physical-network Integrated accurate Detection technology	Misjudgment of normal fluctuations and lack of physical meaning in detection	Physical process-aware integrated detection digital twin virtual-real verification dynamic adaptive threshold adjustment
Cross-Protocol and interpretable universal architecture	Poor compatibility and credibility caused by protocol diversity	Cross-protocol abstraction layer fusion of interpretable AI and industrial knowledge, standardised interfaces, and open-source detection frameworks
Systematic defence system	Fragmentation of detection and defence and difficulty in real-time disposal	Detection-response linkage mechanism adaptive defence strategy optimisation

6.1 Lightweight Intelligent Detection Technology: Breaking Limitations of Real-Time Performance and Edge Deployment

To address the constraints of limited memory and computing power in industrial edge devices, a lightweight ICS-IDS supporting millisecond-level response times is developed through model compression, an edge-cloud collaborative architecture, and hardware-level optimization. This balances the demand for real-time detection with the resource constraints of industrial hardware. The core technical paths include:

Construction of Lightweight Deep Learning Models: Model compression techniques, such as knowledge distillation and pruning, are used to reduce the parameter count while maintaining detection accuracy. This lowers computational latency and adapts to the computing power requirements of edge devices.

Edge-Cloud Collaborative Detection Architecture: Edge nodes are responsible for real-time preliminary detection and for uploading only suspected abnormal data to the cloud. The cloud leverages sufficient computing power for in-depth analysis, forming a collaborative model of "real-time edge response + in-depth cloud verification" to balance real-time performance and detection accuracy.

Customized Optimization of Hardware-Level Algorithms: Targeting the architectural characteristics of industrial-specific chips, detection algorithms with fixed-point computing and low memory occupancy are designed. This reduces the algorithm's reliance on hardware resources and improves operational efficiency on edge devices.

6.2 Data-Driven Robustness Enhancement Technology: Resolving Dataset Imbalance and Sample Scarcity

To address distribution discrepancies between existing public datasets and real ICS environments, as well as the scarcity of historical samples for zero-day attacks, sample diversity is enhanced through data augmentation, cross-domain learning, and unsupervised learning. This reduces reliance on manually labeled data and improves the robustness of detection models. The specific technical directions are as follows:

Industrial Scenario-Specific Data Augmentation: Realistic attack samples are generated by integrating industrial physical mechanisms—for instance, simulating time-series data for attacks such as PLC command tampering and sensor data injection. This avoids sample detachment from actual scenarios caused by over-reliance on statistical methods.

Federated Learning and Cross-Domain Transfer Learning: Federated learning enables "decentralized training" across multiple institutions, addressing the problem of data silos in industry. Transfer learning adapts mature detection models from the IT domain to ICS scenarios, reducing the need for ICS-specific labeled data. For edge ICS scenarios (e.g., PLCs, RTUs, and other devices), it is necessary to optimize lightweight federated training protocols further—reducing computational overhead on edge devices through local training pruning and gradient parameter compression. Meanwhile, a collaborative architecture of edge gateway sub-aggregation and cloud-based global optimization is constructed to balance data privacy protection and millisecond-level detection requirements.

In-Depth Application of Unsupervised/Semi-Supervised Learning: Detection models are trained using readily available data from the regular operation of industrial systems. Anomaly detection is achieved by identifying behaviors that deviate from standard patterns, eliminating reliance on scarce attack samples. This is particularly suitable for detecting zero-day attacks.

6.3 Physical-Network Integrated Accurate Detection Technology: Reducing False Positives and Improving Credibility

To address problems such as misjudging normal fluctuations in industrial environments as attacks and the lack of physical significance in support for detection results, network traffic data is integrated with physical process data. Industrial mechanisms are used to verify detection results, reducing false positives caused by noise interference. The core technical approaches include:

Physical Process-Aware Integrated Detection: Network attack detection is correlated with physical system anomalies. For example, dual verification of "network traffic anomalies, physical parameter anomalies" is used to determine whether an attack is real, avoiding misjudgments caused by over-reliance on network data alone.

Digital Twin Virtual-Physical Mapping Verification: A virtual mirror of the industrial system is constructed using digital twin technology. The impact of attacks on the physical system is simulated in the virtual space to verify the authenticity of the detection model's results, thereby improving the credibility of the detection conclusions. Furthermore, for AI-generated adversarial attacks (e.g., micro-disturbance samples that tamper with protocol data frames), it is necessary to identify isolated adversarial samples that only exist at the network layer through cross-validation of network features and physical parameters (e.g., abnormal traffic must match physical anomalies such as valve opening and motor speed), thereby improving the robustness of the detection model.

Dynamic Adjustment of Adaptive Thresholds: Detection thresholds are dynamically optimized based on the range of normal fluctuations in industrial scenarios (e.g., traffic fluctuations caused by changes in production load). This prevents fixed thresholds from misclassifying normal operational fluctuations as attacks, thereby reducing false-positive rates.

6.4 Cross-Protocol and Interpretable Universal Architecture: Solving Compatibility and Trust Issues

To address the poor compatibility of detection systems due to the diversity of industrial protocols (e.g., Modbus, DNP3, S7COMM) and the reduced user trust caused by the "black-box" nature of deep learning models, a cross-protocol universal detection framework and interpretable models are developed to enhance system compatibility and user trust. The specific measures are as follows:

Design of Cross-Protocol Abstraction Layer: Common features of different industrial protocols (e.g., time-series interaction patterns, data frame structure rules) are extracted to construct a protocol-agnostic abstraction layer for detection models. This enables unified adaptation across multiple protocols without the need to redevelop detection algorithms for each protocol.

Integration of Interpretable AI and Industrial Knowledge: The decision logic of detection models is linked to industrial domain knowledge (e.g., ladder diagrams, process flow diagrams). Detection results are explained using terms understandable to industrial users (e.g., "unauthorized modification of PLC start-stop commands"), breaking the "black-box" barrier.

Construction of Standardized Interfaces and Open-Source Frameworks: Standardization of ICS-IDS interfaces is promoted to reduce integration costs between detection systems from different vendors and industrial control platforms. Open-source detection frameworks are designed to facilitate technology iteration and industry collaboration, thereby promoting widespread adoption.

6.5 Systematic Defense System: Closed-Loop Collaboration from Detection to Response

Breaking the current fragmented state of detection and defense links, a closed-loop defense system of "detection-response-repair" is constructed to achieve real-time attack disposal and dynamic defense optimization:

Detection-Response Linkage Mechanism: A linkage interface is established between ICS-IDS and industrial security devices (e.g., industrial firewalls and PLC security modules) to enable detection and response integration. When an attack is detected, defensive actions (e.g., blocking abnormal traffic, isolating compromised devices, and restarting control loops) are automatically triggered to minimize its impact. It can be combined with the "never trust, always verify" logic of zero trust—dynamic trust levels are assigned based on device fingerprints. Only the minimum necessary operational permissions are authorized. When the IDS detects anomalies, the permissions of suspicious devices are revoked in real time to prevent the spread of attacks; meanwhile, the impact is simulated via digital twins, thereby reducing interference from false alarms in industrial processes.

Adaptive Defense Strategy Optimization: Detection rules and defense strategies are dynamically adjusted based on the evolutionary trends of attack behaviors (e.g., changes in DoS attack traffic characteristics, new command injection attacks). For example, redundant communication links are automatically switched in response to DoS attacks to enhance the defense system's adaptability.

6.6 Actionable Research Frameworks for ICS-IDS: Data, Experiment, and Deployment

The implementation of the aforementioned future hotspots relies on standardized data, reproducible experiments, and quantitative deployment metrics. Herein, three types of actionable research frameworks are proposed to cover the entire data collection, experimentation, and deployment process, providing specific action paths for research in this field.

(1) Standard Dataset Construction Framework

It aims to address the issue that the public datasets mentioned above are mostly simulated data with significant discrepancies in distribution from real ICS environments, and to provide standardized data resources for cross-industry reuse. The data sources of relevant studies [51] are integrated to ensure that the data covers three dimensions: network traffic, physical parameters, and attack samples. Based on the attack classification in Section 4, a three-level annotation system including attack categories, technical details, and physical impacts is formulated. A consortium is established by uniting universities and enterprises, and new attack types are added annually to ensure the dataset's timeliness. Currently, it is necessary to address standardization bottlenecks: first, there is a lack of unified cross-industry detection indicators, requiring industry alliances to formulate domain-specific standards; second, there are no specifications for dataset formats and interfaces between IDS and industrial control systems—reference should be made to the OPC UA protocol to unify data interaction formats, thereby reducing multi-vendor integration costs.

(2) Reproducibility Practice Scheme

It aims to address the challenges of reproducibility and comparability of technical effects, thereby enhancing research credibility. It is necessary to specify the hardware platform, software version, and network topology, and provide Docker environment configuration scripts. Data preprocessing steps, model hyperparameters, and calculation methods of evaluation metrics should be recorded.

(3) Deployment Indicator Evaluation System

It aims to solve the problem that technologies with excellent performance in the laboratory are unavailable in the industrial field, and to provide quantitative evaluation criteria from technological research and development to industrial deployment. The three-level indicator system is shown in Table 9.

Table 9: ICS-IDS deployment indicator evaluation systems

Indicator dimension	Specific indicator	Measurement method
Performance indicator	Detection accuracy	On-site injection attack real attack data verification
	False positive rate	Count misjudgments from normal fluctuations in 30 days
	Detection delay	Measurement based on PLC time difference
Resource indicator	CPU utilization	Collected by industrial monitoring software
Security indicator	DoS resistance	Simulated DoS attack test

As indicated by the bibliometric analysis of relevant literature via SLR and the challenges in technology implementation, future research will focus on resolving bottlenecks, such as insufficient real-time performance and dataset imbalance, to advance the evolutionary paths outlined above. This paper, through the logical closed loop of identifying challenges, proposing hotspots, and designing frameworks, not only clarifies the evolutionary direction of ICS-IDS technology but also provides feasible solutions to address existing research gaps, with the expectation of promoting the technology from theoretical research to industrial practice. Practical deployment requires overcoming two significant barriers: first, legacy devices have limited resources—lightweight detection modules can be deployed by connecting external low-power edge gateways to avoid production shutdowns for retrofitting; second, there are skill gaps among operation and maintenance personnel—automated model update platforms should be developed, and industrial control knowledge graphs should be integrated to simplify false alarm classification, thereby lowering the operation threshold.

7 Conclusion

This paper explores the unique aspects of ICS network security, highlighting its potential attack vectors. It assesses the current research landscape on ICS security detection technologies, both domestically and internationally, focusing on four main approaches: misuse-based intrusion detection, anomaly-based intrusion detection, machine learning-based intrusion detection, and intrusion detection tailored to specific requirements. Finally, the paper presents a forward-looking view of the development trends and research directions for ICS intrusion detection systems.

The ongoing innovation and development of key intrusion detection systems for ICS signal significant potential for future breakthroughs. By integrating new technologies and methodologies, ICS intrusion detection systems can provide more comprehensive and intelligent security measures, effectively addressing the constantly evolving cyber threats. This is crucial for ensuring the security of the national information infrastructure.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Tong Wu; methodology, Tong Wu; validation, Tong Wu, Dawei Zhou; formal analysis, Tong Wu; investigation, Qingyu Ou; resources, Qingyu Ou; data curation, Fang Luo; writing—original draft preparation, Tong Wu; writing—review and editing, Qingyu Ou, Dawei Zhou; visualization, Fang Luo; supervision, Fang Luo; project administration, Fang Luo. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable, as this is a narrative review based on existing literature.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

ICS	Industrial control systems
IT	Information technology
OT	Operational technology
PLC	Programmable logic controller
IDS	Intrusion Detection System
DoS	Denial of Service
MitM	Man-in-the-Middle
MIDS	Misuse-based Intrusion Detection System
AIDS	Anomaly-based Intrusion Detection System
HIDS	Host-based intrusion detection system

References

1. Hahn A. Operational technology and information technology in industrial control systems. In: Cyber-security of SCADA and other industrial control systems. Cham, Switzerland: Springer International Publishing; 2016. p. 51–68. doi:10.1007/978-3-319-32125-7_4.
2. Koay AMY, Ko RKL, Hettema H, Radke K. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. J Intell Inf Syst. 2023;60(2):377–405. doi:10.1007/s10844-022-00753-1.
3. Langner R. Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur Priv. 2011;9(3):49–51. doi:10.1109/MSP.2011.67.
4. Музика. BB. Analysis of cyber-attacks on Ukrainian power grid systems in the context of armed conflict in Donbas. Const State. 2020;2020(39):78–85. doi:10.18524/2411-2054.2020.39.212983.
5. Morisseau D. Pipeline. [cited 2025 Nov 1]. Available from: https://www.dramaonlinelibrary.com/audio?docid=do-9781682661635&tocid=do-9781682661635_63222075341122022.
6. Nakayama K, Koshijima I, Watanabe K. Analyzing important factors in cybersecurity incidents using table-top exercise. In: Proceedings of the (2024) International Conference; 2014 Jul 24–27; Nice, France. doi:10.54941/ahfe1004770.
7. Liao HJ, Richard Lin CH, Lin YC, Tung KY. Intrusion detection system: a comprehensive review. J Netw Comput Appl. 2013;36(1):16–24. doi:10.1016/j.jnca.2012.09.004.
8. Pinto A, Herrera LC, Donoso Y, Gutierrez JA. Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors. 2023;23(5):2415. doi:10.3390/s23052415.
9. Kheddar H. Transformers and large language models for efficient intrusion detection systems: a comprehensive survey. Inf Fusion. 2025;124(1):103347. doi:10.1016/j.inffus.2025.103347.
10. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: a survey. Comput Secur. 2020;89:101677. doi:10.1016/j.cose.2019.101677.
11. Kheddar H, Himeur Y, Awad AI. Deep transfer learning for intrusion detection in industrial control networks: a comprehensive review. J Netw Comput Appl. 2023;220:103760. doi:10.1016/j.jnca.2023.103760.
12. Bonandir NA, Jamil N, Ahmad Nawawi MN, Jidin R, Rusli ME, Yan LK, et al. A review of cyber security assessment (CSA) for industrial control systems (ICS) and their impact on the availability of the ICS operation. J Phys Conf Ser. 2021;1860(1):012015. doi:10.1088/1742-6596/1860/1/012015.
13. Shahzad A, Lee M, Lee YK, Kim S, Xiong N, Choi JY, et al. Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information. Symmetry. 2015;7(3):1176–210. doi:10.3390/sym7031176.
14. Hu Y, Yang A, Li H, Sun Y, Sun L. A survey of intrusion detection on industrial control systems. Int J Distrib Sens Netw. 2018;14(8):155014771879461. doi:10.1177/1550147718794615.
15. Haber MJ. Industrial control systems (ICS) and Internet of Things (IoT). In: Privileged attack vectors. Berkeley, CA, USA: Apress; 2020. p. 203–14. doi:10.1007/978-1-4842-5914-6_14.
16. Mazurczyk W, Caviglione L. Cyber reconnaissance techniques. Commun ACM. 2021;64(3):86–95. doi:10.1145/3418293.
17. Kaouk M, Flaus JM, Potet ML, Groz R. A review of intrusion detection systems for industrial control systems. In: 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT); 2019 Apr 23–26; Paris, France: IEEE; 2019. p. 1699–704. doi:10.1109/codit.2019.8820602.
18. False data injection attacks. In: Cloud control systems. Amsterdam, The Netherlands: Elsevier; 2020. p. 149–67. doi:10.1016/b978-0-12-818701-2.00014-7.
19. Hijazi S, Obaidat MS. Address resolution protocol spoofing attacks and security approaches: a survey. Secur Priv. 2019;2(1):e49. doi:10.1002/spy2.49.
20. Long M, Wu CH, Hung JY. Denial of service attacks on network-based control systems: impact and mitigation. IEEE Trans Ind Inform. 2005;1(2):85–96. doi:10.1109/TII.2005.844422.
21. Parian C, Guldimann T, Bhatia S. Fooling the master: exploiting weaknesses in the modbus protocol. Procedia Comput Sci. 2020;171:2453–8. doi:10.1016/j.procs.2020.04.265.
22. Lee W, Stolfo SJ. A framework for constructing features and models for intrusion detection systems. ACM Trans Inf Syst Secur. 2000;3(4):227–61. doi:10.1145/382912.382914.

23. Samrin R, Vasumathi D. Review on anomaly based network intrusion detection system. In: Proceedings of the 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT); 2017 Dec 15–16; Mysuru, India. p. 141–7. doi:10.1109/ICEECCOT.2017.8284655.
24. Veerasingam P, Abd Razak S, Abidin AFA, Mohamed MA, Mohd Satar SD. Intrusion detection and prevention system in sme's local network by using Suricata. Myjcam. 2023;6(1):21–30. doi:10.37231/myjcam.2023.6.1.88.
25. Myers D, Suriadi S, Radke K, Foo E. Anomaly detection for industrial control systems using process mining. Comput Secur. 2018;78(2):103–25. doi:10.1016/j.cose.2018.06.002.
26. Bhardwaj A, Al-Turjman F, Kumar M, Stephan T, Mostarda L. Capturing-the-invisible (CTI): behavior-based attacks recognition in IoT-oriented industrial control systems. IEEE Access. 2020;8:104956–66. doi:10.1109/access.2020.2998983.
27. Velasco C, Obrist M. xSense design cards for multisensory experiences. In: Multisensory experiences. Oxford, UK: Oxford University Press; 2020. p. 1–12. doi:10.1093/oso/9780198849629.003.0001.
28. Li H, Qin S. Optimization and implementation of industrial control system network intrusion detection by telemetry analysis. In: Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC); 2017 Dec 13–16; Chengdu, China. p. 1251–4. doi:10.1109/CompComm.2017.8322743.
29. Lin CY, Nadjm-Tehrani S, Asplund M. Timing-based anomaly detection in SCADA networks. In: Critical information infrastructures security. Cham, Switzerland: Springer International Publishing; 2018. p. 48–59. doi:10.1007/978-3-319-99843-5_5.
30. Ponomarev S, Atkison T. Industrial control system network intrusion detection by telemetry analysis. IEEE Trans Dependable Secure Comput. 2016;13(2):252–60. doi:10.1109/TDSC.2015.2443793.
31. Lontorfos G, Fairbanks KD, Watkins L, Robinson WH. Remotely inferring device manipulation of industrial control systems via network behavior. In: Proceedings of the 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops); 2015 Oct 26–29; Clearwater Beach, FL, USA. p. 603–10. doi:10.1109/LCNW.2015.7365904.
32. Nair R, Nayak C, Watkins L, Fairbanks KD, Memon K, Wang P, et al. The resource usage viewpoint of industrial control system security: an inference-based intrusion detection system. In: Cybersecurity for industry 4.0. Cham: Springer International Publishing; 2017. p. 195–223. doi:10.1007/978-3-319-50660-9_8.
33. Xiao YJ, Xu WY, Jia ZH, Ma ZR, Qi DL. NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers Inf Technol Electronic Eng. 2017;18(4):519–34. doi:10.1631/fitee.1601540.
34. Sheng C, Yao Y, Fu Q, Yang W. A cyber-physical model for SCADA system and its intrusion detection. Comput Netw. 2021;185(2):107677. doi:10.1016/j.comnet.2020.107677.
35. Yang K, Li Q, Lin X, Chen X, Sun L. iFinger: intrusion detection in industrial control systems via register-based fingerprinting. IEEE J Sel Areas Commun. 2020;38(5):955–67. doi:10.1109/jsac.2020.2980921.
36. Acharya P, Ramachandran H, David KA, Smith R, Al-Hadhrami T. Towards net zero resilience: a futuristic architectural strategy for cyber-attack defence in industrial control systems (ICS) and operational technology (OT). Comput Mater Continua. 2025;82(2):3619–41. doi:10.32604/cmc.2024.054802.
37. Dutta N, Jadav N, Dutiya N, Joshi D. Using honeypots for ICS threats evaluation. In: Recent developments on industrial control systems resilience. Cham, Switzerland: Springer International Publishing; 2020. p. 175–96. doi:10.1007/978-3-030-31328-9_9.
38. Mesbah M, Elsayed MS, Jurcut AD, Azer M. Analysis of ICS and SCADA systems attacks using honeypots. Future Internet. 2023;15(7):241. doi:10.3390/fi15070241.
39. Yang X, Yuan J, Yang H, Kong Y, Zhang H, Zhao J. A highly interactive honeypot-based approach to network threat management. Future Internet. 2023;15(4):127. doi:10.3390/fi15040127.
40. Kempinski S, Ichaarine S, Sciancalepore S, Zambon E. ICSvertase: a framework for purpose-based design and classification of ICS honeypots. In: Proceedings of the 18th International Conference on Availability, Reliability and Security; 2023 Aug 29–Sep 1; Benevento, Italy. p. 1–10. doi:10.1145/3600160.3605020.
41. Pashaei A, Akbari ME, Zolfy Lighvan M, Charmin A. Early Intrusion Detection System using honeypot for industrial control networks. Results Eng. 2022;16(2):100576. doi:10.1016/j.rineng.2022.100576.

42. Liang M, Liu T, Song X, Peng W, Yang M, Hu N. EmuGuard: an active defense system for ICS emulation. In: Cyberspace simulation and evaluation. Singapore: Springer Nature; 2025. p. 73–89. doi:10.1007/978-981-96-4503-9_6.
43. Industrial Network Security. Industrial network security. Netw Secur. 2015;2015(3):4. doi:10.1016/s1353-4858(15)30014-3.
44. Jose S, Malathi D, Reddy B, Jayaseeli D. A survey on anomaly based host intrusion detection system. J Phys Conf Ser. 2018;1000:012049. doi:10.1088/1742-6596/1000/1/012049.
45. Marsden T, Moustafa N, Sitnikova E, Creech G. Probability risk identification based intrusion detection system for SCADA systems. In: Mobile networks and management. Cham, Switzerland: Springer International Publishing; 2018. p. 353–63. doi:10.1007/978-3-319-90775-8_28.
46. Ike M, Phan K, Sadoski K, Valme R, Lee W. Scaphy: detecting modern ICS attacks by correlating behaviors in SCADA and PHYsical. In: Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP); 2023 May 21–25; San Francisco, CA, USA. p. 20–37. doi:10.1109/SP46215.2023.10179411.
47. Jadidi Z, Foo E, Hussain M, Fidge C. Automated detection-in-depth in industrial control systems. Int J Adv Manuf Technol. 2022;118(7):2467–79. doi:10.1007/s00170-021-08001-6.
48. Ryšavý O, Matoušek P. A network traffic processing library for ICS anomaly detection. In: Proceedings of the 7th Conference on the Engineering of Computer Based Systems; 2021 May 26–27; Novi Sad, Serbia. p. 1–7. doi:10.1145/3459960.3459963.
49. Aoudi W, Iturbe M, Almgren M. Truth will out. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15–19; Toronto, ON, Canada. New York, NY, USA: ACM; 2015. p. 817–31. doi:10.1145/3243734.3243781.
50. Caselli M, Zambon E, Kargl F. Sequence-aware intrusion detection in industrial control systems. In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security; 2015 Apr 14–Mar 14; Singapore. p. 13–24. doi:10.1145/2732198.2732200.
51. Mitchell R, Chen IR. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv. 2014;46(4):1–29. doi:10.1145/2542049.
52. Lee KM, Cho MY, Kim JG, Lee KH. Anomaly detection method for unknown protocols in a power plant ICS network with decision tree. Appl Sci. 2023;13(7):4203. doi:10.3390/app13074203.
53. Ayodeji A, Liu YK, Chao N, Yang LQ. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. Nucl Eng Technol. 2020;52(12):2687–98. doi:10.1016/j.net.2020.05.012.
54. Gönen S, Sayan HH, Yılmaz EN, Üstünsoy F, Karacayılmaz G. False data injection attacks and the insider threat in smart systems. Comput Secur. 2020;97(1):101955. doi:10.1016/j.cose.2020.101955.
55. Depren O, Topallar M, Anarim E, Ciliz MK. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Syst Appl. 2005;29(4):713–22. doi:10.1016/j.eswa.2005.05.002.
56. Chiew KL, Hui B. An improved network intrusion detection method based on CNN-LSTM-SA. J Adv Res Appl Sci Eng Technol. 2024;44(1):225–38. doi:10.37934/araset.44.1.225238.
57. Ahakonye LAC, Nwakanma CI, Lee JM, Kim DS. SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. Internet Things. 2023;21:100676. doi:10.1016/j.iot.2022.100676.
58. Ahakonye LAC, Nwakanma CI, Lee JM, Kim DS. Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system. IEEE Internet Things J. 2023;10(12):10344–56. doi:10.1109/JIOT.2023.3237797.
59. Popoola SI, Tsado Y, Ogunjinmi AA, Sanchez-Velazquez E, Peng Y, Rawat DB. Multi-stage deep learning for intrusion detection in industrial Internet of Things. IEEE Access. 2025;13:60532–55. doi:10.1109/access.2025.3557959.
60. Chang CP, Hsu WC, Liao I. Anomaly detection for industrial control systems using K-means and convolutional autoencoder. In: Proceedings of the 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2019 Sep 19–21; Split, Croatia. p. 1–6.

61. Hao W, Yang T, Yang Q. Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems. IEEE Trans Autom Sci Eng. 2023;20(1):32–46. doi:10.1109/TASE.2021.3073396.
62. Dini P, Elhanashi A, Begni A, Saponara S, Zheng Q, Gasmi K. Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. Appl Sci. 2023;13(13):7507. doi:10.3390/app13137507.
63. Khan L, Awad M, Thuraisingham B. A new intrusion detection system using support vector machines and hierarchical clustering. VLDB J. 2007;16(4):507–21. doi:10.1007/s00778-006-0002-5.
64. Anton SDD, Sinha S, Dieter Schotten H. Anomaly-based intrusion detection in industrial data with SVM and random forests. In: Proceedings of the 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2019 Sep 19–21; Split, Croatia. p. 1–6.
65. Vargas Martinez C, Vogel-Heuser B. A Host Intrusion Detection System architecture for embedded industrial devices. J Frankl Inst. 2021;358(1):210–36. doi:10.1016/j.jfranklin.2019.03.037.
66. Fang Y, Yao Y, Lin X, Wang J, Zhai H. A feature selection based on genetic algorithm for intrusion detection of industrial control systems. Comput Secur. 2024;139(1):103675. doi:10.1016/j.cose.2023.103675.
67. Ling J, Zhu Z, Luo Y, Wang H. An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit. Comput Electr Eng. 2021;91:107049. doi:10.1016/j.compeleceng.2021.107049.
68. Mubarak S, Hadi Habaebi M, Rafiqul Islam M, Diyana Abdul Rahman F, Tahir M. Anomaly detection in ICS datasets with machine learning algorithms. Comput Syst Sci Eng. 2021;37(1):33–46. doi:10.32604/csse.2021.014384.
69. Nagarajan S, Kayalvizhi S, Subhashini R, Anitha V. Hybrid honey badger-world cup algorithm-based deep learning for malicious intrusion detection in industrial control systems. Comput Ind Eng. 2023;180:109166. doi:10.1016/j.cie.2023.109166.
70. Imran M, Siddiqui HUR, Raza A, Raza MA, Rustam F, Ashraf I. A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. Comput Secur. 2023;134:103445. doi:10.1016/j.cose.2023.103445.
71. Yang T, Hu Y, Li Y, Hu W, Pan Q. A standardized ICS network data processing flow with generative model in anomaly detection. IEEE Access. 2019;8:4255–64. doi:10.1109/access.2019.2963144.
72. Al-Abassi A, Karimipour H, Dehghantanha A, Parizi RM. An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access. 2020;8:83965–73. doi:10.1109/access.2020.2992249.
73. Anthi E, Williams L, Burnap P, Jones K. A three-tiered intrusion detection system for industrial control systems. J Cybersecur. 2021;7:tyab006. doi:10.1093/cybsec/tyab006.
74. Hwang C, Lee T. E-SFD: explainable sensor fault detection in the ICS anomaly detection system. IEEE Access. 2021;9:140470–86. doi:10.1109/access.2021.3119573.
75. Wang Z, Lai Y, Liu Z, Liu J. Explaining the attributes of a deep learning based intrusion detection system for industrial control networks. Sensors. 2020;20(14):3817. doi:10.3390/s20143817.
76. Zhang F, Kodituwakku HADE, Hines JW, Coble J. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. IEEE Trans Ind Inform. 2019;15(7):4362–9. doi:10.1109/TII.2019.2891261.
77. Peddabachigari S, Abraham A, Grosan C, Thomas J. Modeling intrusion detection system using hybrid intelligent systems. J Netw Comput Appl. 2007;30(1):114–32. doi:10.1016/j.jnca.2005.06.003.
78. Bernieri G, Conti M, Turrin F. King Fisher. In: Proceedings of the 1st Workshop on Machine Learning on Edge in Sensor Systems; 2019 Nov 10; New York, NY, USA. New York, NY, USA: ACM; 2019. p. 7–12. doi:10.1145/3362743.3362961.
79. Zainudin A, Akter R, Kim DS, Lee JM. Federated learning inspired low-complexity intrusion detection and classification technique for SDN-based industrial CPS. IEEE Trans Netw Serv Manag. 2023;20(3):2442–59. doi:10.1109/TNSM.2023.3299606.
80. Ortega-Fernandez I, Sestelo M, Burguillo JC, Piñón-Blanco C. Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. Wirel Netw. 2024;30(6):5059–75. doi:10.1007/s11276-022-03214-3.
81. Nedeljkovic D, Jakovljevic Z. CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. Comput Secur. 2022;114:102585. doi:10.1016/j.cose.2021.102585.

82. Zeng GQ, Shao JM, Lu KD, Geng GG, Weng J. MoCC-BD-FID: multi-objective clustering combination-based backdoor defense for federated intrusion detection of industrial control systems. IEEE Trans Inf Forensics Secur. 2025;20:6868–83. doi:10.1109/TIFS.2025.3586479.
83. Kim B, Ali Alawami M, Kim E, Oh S, Park J, Kim H. A comparative study of time series anomaly detection models for industrial control systems. Sensors. 2023;23(3):1310. doi:10.3390/s23031310.
84. Kravchik M, Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks. In: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy; 2018 Oct 19; Toronto, ON, Canada. p. 72–83. doi:10.1145/3264888.3264896.
85. Khan IA, Keshk M, Pi D, Khan N, Hussain Y, Soliman H. Enhancing IIoT networks protection: a robust security model for attack detection in Internet Industrial Control Systems. Ad Hoc Netw. 2022;134:102930. doi:10.1016/j.adhoc.2022.102930.
86. Chahal A, Gulia P, Gill NS, Rani D. Design of a federated ensemble model for intrusion detection in distributed IIoT networks for enhancing cybersecurity. J Ind Inf Integr. 2025;44:100800. doi:10.1016/j.jii.2025.100800.
87. Srinivasan M, Senthilkumar NC. Intrusion detection and prevention system (IDPS) model for IIoT environments using hybridized framework. IEEE Access. 2025;13:26608–21. doi:10.1109/access.2025.3538461.
88. Bansal K, Singhrova A. Review on intrusion detection system for IoT/IIoT-brief study. Multimed Tools Appl. 2024;83(8):23083–108. doi:10.1007/s11042-023-16395-6.
89. Soliman S, Oudah W, Aljuhani A. Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alex Eng J. 2023;81:371–83. doi:10.1016/j.aej.2023.09.023.
90. Ali BS, Ullah I, Al Shloul T, Khan IA, Khan I, Ghadi YY, et al. ICS-IDS: application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks. J Supercomput. 2024;80(6):7876–905. doi:10.1007/s11227-023-05764-5.
91. Wang J, Si C, Wang Z, Fu Q. A new industrial intrusion detection method based on CNN-BiLSTM. Comput Mater Continua. 2024;79(3):4297–318. doi:10.32604/cmc.2024.050223.
92. Xiang J, Zhang X, Zheng Q, Deng L, Zhao D, Zhou J. CIDF: combined intrusion detection framework in industrial control systems based on packet signature and enhanced FSFDP. In: Proceedings of the 15th Asia-Pacific Symposium on Internetware; 2014 Jul 24–26; Macau, China. p. 417–26. doi:10.1145/3671016.3674812.
93. Jadidi Z, Pal S, Hussain M, Thanh KN. Correlation-based anomaly detection in industrial control systems. Sensors. 2023;23(3):1561. doi:10.3390/s23031561.
94. Abid A, Jemili F, Korbaa O. Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. Clust Comput. 2024;27(2):2217–38. doi:10.1007/s10586-023-04087-7.
95. Rubio JE, Alcaraz C, Roman R, Lopez J. Analysis of intrusion detection systems in industrial ecosystems. In: Proceedings of the 14th International Joint Conference on e-Business and Telecommunications; 2017 Jul 24–26; Madrid, Spain. p. 116–28. doi:10.5220/0006426301160128.
96. Thalpage NS, Nisansala TAD. Exploring the opportunities of applying digital twins for intrusion detection in industrial control systems of production and manufacturing—a systematic review. In: Data protection in a post-pandemic society. Cham, Switzerland: Springer International Publishing; 2023. p. 113–43. doi:10.1007/978-3-031-34006-2_4.
97. Akbarian F, Fitzgerald E, Kihl M. Intrusion detection in digital twins for industrial control systems. In: Proceedings of the 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2020 Sep 17–19. Split, Croatia. p. 1–6.
98. Dietz M, Pernul G. Unleashing the digital twin's potential for ICS security. IEEE Secur Priv. 2020;18(4):20–7. doi:10.1109/MSEC.2019.2961650.
99. Xu X, Lai Y, Zhang X, Dong X. Abnormal logical representation learning for intrusion detection in industrial control systems. IEEE Trans Ind Inform. 2024;20(8):10624–35. doi:10.1109/TII.2024.3396348.
100. Izuazu UU, Ihekoronye VU, Kim DS, Lee JM. Securing critical infrastructure: a denoising data-driven approach for intrusion detection in ICS network. In: Proceedings of the 2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC); 2024 Feb 19–22; Osaka, Japan. p. 841–6. doi:10.1109/ICAIIC60209.2024.10463488.

101. Gu H, Lai Y, Wang Y, Liu J, Sun M, Mao B. DEIDS: a novel intrusion detection system for industrial control systems. Neural Comput Appl. 2022;34(12):9793–811. doi:10.1007/s00521-022-06965-4.
102. Perales Gómez ÁL, Fernández Maimó L, Huertas Celdrán A, García Clemente FJ, Gil Pérez M, Martínez Pérez G. SafeMan: a unified framework to manage cybersecurity and safety in manufacturing industry. Softw Pract Exp. 2021;51(3):607–27. doi:10.1002/spe.2879.
103. Fan X, Fan K, Wang Y, Zhou R. Overview of cyber-security of industrial control system. In: Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC); 2015 Aug 5–7; Shanghai, China. p. 1–7. doi:10.1109/SSIC.2015.7245324.
104. Nankya M, Chataut R, Akl R. Securing industrial control systems: components, cyber threats, and machine learning-driven defense strategies. Sensors. 2023;23(21):8840. doi:10.3390/s23218840.
105. Hui H, Maynard P, McLaughlin K. ICS interaction testbed: a platform for cyber-physical security research. In: Proceedings of the Electronic Workshops in Computing. BCS Learning & Development; 2019 Sep 10–12; Athens, Greece. p. 89–96. doi:10.14236/ewic/icscsr19.12.
106. He Q, Lin J, Fang H, Wang X, Huang M, Yi X, et al. Integrating IoT and 6G: applications of edge intelligence, challenges, and future directions. IEEE Trans Serv Comput. 2025;18(4):2471–88. doi:10.1109/TSC.2025.3586152.
107. Seydali M, Khunjush F, Dogani J. Streaming traffic classification: a hybrid deep learning and big data approach. Clust Comput. 2024;27(4):5165–93. doi:10.1007/s10586-023-04234-0.
108. Leevy JL, Khoshgoftaar TM. A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. J Big Data. 2020;7(1):104. doi:10.1186/s40537-020-00382-x.
109. Deldar F, Abadi M. Deep learning for zero-day malware detection and classification: a survey. ACM Comput Surv. 2024;56(2):1–37. doi:10.1145/3605775.
110. Kuchar K, Fujdiak R. Anomaly detection in industrial networks: current state, classification, and key challenges. IEEE Sens J. 2025;25(3):5031–43. doi:10.1109/jsen.2024.3512857.
111. Kheddar H, Dawoud DW, Awad AI, Himeur Y, Khan MK. Reinforcement-learning-based intrusion detection in communication networks: a review. IEEE Commun Surv Tutor. 2025;27(4):2420–69. doi:10.1109/comst.2024.3484491.
112. Wang Z, Thing VLL. Feature mining for encrypted malicious traffic detection with deep learning and other machine learning algorithms. Comput Secur. 2023;128:103143. doi:10.1016/j.cose.2023.103143.
113. Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. 2013;11(8):2661–74. doi:10.1016/j.adhoc.2013.04.014.
114. Patel A, Taghavi M, Bakhtiyari K, Celestino J Jr. An intrusion detection and prevention system in cloud computing: a systematic review. J Netw Comput Appl. 2013;36(1):25–41. doi:10.1016/j.jnca.2012.08.007.
115. Deng X, Xiao L, Liu X, Zhang X. One-dimensional residual GANomaly network-based deep feature extraction model for complex industrial system fault detection. IEEE Trans Instrum Meas. 2023;72:3520013. doi:10.1109/TIM.2023.3284940.