University of Kent

Kent Academic Repository

Moura, Ralf Luis de, Franqueira, Virginia N. L. and Pessin, Gustavo (2023) *Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems*. In: 2023 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE'23). Conference Publishing Services (CPS) . IEEE (In press)

Downloaded from

https://kar.kent.ac.uk/101558/ The University of Kent's Academic Repository KAR

The version of record is available from

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

UNSPECIFIED

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Cybersecurity in Industrial Networks: Artificial Intelligence Techniques Applied to Intrusion Detection Systems

1st Ralf Luis de Moura
Operational Technology Architecture
Vale S.A.
Vitória, Brazil
ralf.moura@vale.com

2nd Virginia N. L. Franqueira
School of Computing
University of Kent
Canterbury, UK
v.franqueira@kent.ac.uk

3rd Gustavo Pessin
Department of Automation Engineering
Instituto de Tecnologia Vale
Ouro Preto, Brazil
gustavo.pessin@itv.org

***Abstract*—Industrial control systems (ICS) operate on serial-based networks which lack proper security safeguards by design. They are also becoming more integrated to corporate networks, creating new vulnerabilities which expose ICS networks to increasing levels of risk with potentially significant impact. Despite those risks, only a few mechanisms have been suggested and are available in practice as cybersecurity safeguards for the ICS network layer, maybe because they might not be commercially viable. Intrusion detection systems (IDS) are typically deployed in the corporate networks to protect against attacks since they are based on TCP/IP. However, IDS are not used in serial-based ICS networks yet. This study examines and compares modern Artificial Intelligence (AI) techniques applied in IDS that are potentially useful for serial-based ICS networks. The results showed that current AI-based IDS methods are viable in such networks. A mix of AI techniques would be the best way forward to detect known attacks via rules and novel attacks, not previously mapped, via supervised and unsupervised techniques. Despite these strategies' limited use in serial-based networks, their adoption could significantly strengthen cybersecurity of ICS networks.**

***Index Terms*—Artificial Intelligence, Industrial Networks, Serial Protocols, Cybersecurity, and Intrusion Detection Systems.**

I. Introduction

INDUSTRIAL control systems (ICS) are a combination of control components that enable remote and real-time governance of production cycles [1]. Supervisory and data acquisition systems (SCADA), Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), sensors, and actuators are examples of these control components that, together, facilitate reaching industrial objectives [2].

All components that encompass an ICS typically exchange information through industrial networks that operate with communication protocols, commonly referred to in a generic way as Industrial Network Protocols (INP) [1], [3]. INPs are real-time communication protocols developed to interconnect components that compose an ICS [4].

INPs were designed to communicate serially over serial connections (e.g., RS-232, RS-485). Over the years, most of these protocols evolved to operate over Ethernet-based (e.g., Ethernet-APL [5]) networks based on routable protocols like TCP/IP (Transmission Control Protocol / Internet Protocol) [4]. Therefore, serial protocols are gradually being replaced by these protocols; however, they are still present in many industries, supporting a set of devices in specific networks [6]. Currently, serial-based protocols are mainly applied to integrate sensors and actuators, usually in lower industrial network layers [4], [6].

Cybersecurity of Ethernet-based ICS has increasingly gained attention recently, which may explain the plenty of studies that board industrial Ethernet-based networks, sometimes called SCADA networks, e.g., [7]–[11]. However, the security of serial-based ICS has been overlooked despite successful attacks [4], [12], [13].

Industrial networks comprise protocols, physical parts, and communication hardware. Industrial networks are commonly segregated from business networks in security zones separated by firewalls and DMZs (Demilitarized Zones) that improve defenses against attackers and reduce cybersecurity vulnerabilities [14]. It is expected the use IDS in these zones as additional security mechanisms. IDS is considered a vital line of defense in industrial networks [8], [13], [15], but they are not usually applied in serial-based networks.

Serial-based networks have poor cybersecurity mechanisms [2] because they were created with the assumption of isolation [16] when the main desirable characteristics of such networks were determinism and performance [6]. They are usually the lowest-level networks in an ICS ecosystem below multiple network layers [4]. As the serial protocols that support these networks implement almost no cybersecurity defenses [4], [17], in a successful penetration, an attacker can easily take control and manipulate sensors and actuators directly, endangering assets and human lives [18]. Thus, IDS may be applied as an additional or, in some cases, the only line of defense [19] in this critical layer.

This study aims to review intrusion detection AI techniques and compare techniques that may be applied to serial-based industrial protocols, proposing to extend defenses to the lowest industrial network layer and expanding the industrial cyberse-

curity frontiers. These are the research questions:

- What are the leading AI techniques applied in IDS for Industrial Networks?
- What AI techniques can be applied in IDS for Industrial Serial-based networks?

The contributions of this paper are threefold:

1) It reviews AI techniques for intrusion detection potentially applicable to serial-based industrial networks.
2) It compares the uncovered techniques in terms of techniques and benefits.
3) It discusses extending cybersecurity defenses to the lowest industrial networks.

The work is organized as follows: Section 2 presents the background of AI techniques, such as industrial networks, threats, vulnerabilities, and mitigation. Section 3 shows the main AI techniques applied in IDS for industrial networks, and finally, section 4 discusses the application of IDS in serial-based networks.

II. Background

A. Overview of Industrial Networks

Industrial networks have fundamentally different requirements compared to (conventional) business networks. The main difference is that industrial networks are connected to physical equipment to control and monitor real-world actions and conditions. These characteristics emphasize network features such as determinism, temporal consistency, and real-time data transfer [20]. Industrial networks' primary function is control of physical equipment, while business networks are data processing and transfer. The hierarchy of ICS networks is deeper and works with many protocols and physical standards. The failure severity and reliability are high. Round trip times are between 250 μs to 10 ms, while business networks work with periods greater than 50 ms. Industrial networks also operate in hostile conditions, often with high dust, heat, and vibration [21].

Many types of equipment, devices, and instruments coexist in an industrial network and are segregated hierarchically to establish more adequate connections for each automation subsystem [22]. Implementing different layers (e.g., sensor bus, device bus, and Fieldbus layers) in ICS infrastructure is expected. However, this infrastructure and the number of layers are not standardized and vary among industries [17].

The Sensor bus layer works with signals based on the bit-level messages, connecting simple equipment like sensors and actuators. The Device bus layer interconnects more complex field devices transmitting byte-level messages. Device bus networks are called backbone networks because they commonly concentrate traffic from other layers. The Fieldbus layer allows the use of various information derived from more complex instruments, transmitting block-level messages. They commonly replace the classic 4-20 mA analog communications in the manufacturing process [23].

The traditional approach connects the layers through gateways that allow real-time data exchange in automation layers, DMZs, and firewalls between business security zones. Gateways may transfer and translate network variables and messages among layers until they reach business networks [24], [25].

Serial industrial protocols run over non-routable networks created to interconnect control components and may compose many industrial networks. These networks are often in the sensor bus and Fieldbus levels. Regarding technology, this network does not differ substantially from routable networks; the main differences are in the communication patterns [3], [4].

Serial communications usually implement only three layers of the OSI (Open System Interconnections) model: the physical layer, the data link layer, and the application layer. They usually use serial standards interfaces like RS-232 and RS-485 or specific physical layer specifications such as IEC 1158-2 [26]. The arbitration method for media access and the communication mode can be centralized using traditional master-slave, token-pass, or distributed bus arbitration in which all devices select the next bus master. The master has control of the bus and defines which equipment may use it. DeviceNet, Profibus DP, Profibus PA, M-BUS, DLSM/COSEM, and Interbus are examples of serial-based networks [6].

Recently, new industrial networks emerged based on TCP/IP protocols. The protocols and the network components were adapted to support the industrial environment's rigor and temporal requirements (e. g. determinism, repeatability, and response time) [3], [6]. Due to the wide acceptance of these protocols, the interconnection facility with the business networks, structure, and services inherited from these same networks, gradually TCP/IP industrial networks, are replacing the classic serial networks.

From a purely technical standpoint, Ethernet-based networks are not necessarily better than serial-based networks for automation applications. They have the advantages of being more integrated with business networks and, in some applications, can deliver more performance and low cost [3]. Ethernet/IP, MODBUS/TCP, and ProfiNet are examples of Ethernet-based networks. As these protocols are based on Ethernet and TCP/IP, they may reuse virtually all services and cybersecurity mechanisms already created for business networks like firewalls, Identity and Access Management (IAM), Intrusion Detection systems (IDS), Intrusion Prevent Systems (IPS).

B. Security Issues in Industrial Networks

Industrial networks support almost all processes and manufacturing operations. A successful attack in an industrial network may impact those processes. The consequences could range from little disruptions of the operation and alteration of processes parameters to deliberate acts of sabotage that could result in environmental damages, injury, loss of life [18], and destructive acts, such as explosions [4].

In general, security professionals consider serial protocols secure because they are non-routable. Many still think the

same countermeasures applied to protect general-purpose computer networks are enough to protect ICS [25]. However, Stuxnet, Duqu, Shamoon, Flame, and Gass [12], [17], [27] malware, using the business network as an entry point (e.g., Stuxnet/Flame - USB ports, Duqu - Keylogger), showed that this is not always true.

There are many limitations in serial-based industrial networks. Equipment used in serial networks commonly does not implement cryptography mainly because of devices' resources (storage, processing, etc.) and bandwidth limitations. Internal user controls usually limit authentication and authorization. Firewalls only work over routable networks [25]. Replacing devices or upgrading software and firmware is sometimes unrealistic for ICS. Furthermore, some vendors do not even support upgrades of cybersecurity features [28].

Security requirements for industrial serial-based networks are similar to industrial routable networks, including perimeter and security controls with access, authentication, and ports and services control. Host security controls with anti-malware, asset configuration control, and monitoring ports and services [29]. However, some cannot be implemented due to physical (hardware capabilities) limitations and restrictions [28].

Serial-based industrial protocols have cybersecurity limitations, often implementing no cybersecurity mechanism [30]. They are designed for use in a secure environment with little or no security features [31]. The limitations come from these networks being created when ICSs were isolated. Back then, there was no concern about security issues as an attacker would have to be physically connected to the network to perform an attack. At that time, the main concerns were network performance and availability [3].

The lack of authentication among network entities, such as masters and slaves, allows attackers to send forged messages using malware that infects the network. This fragility may enable denial-of-service attacks by impersonating the master and sending meaningless messages to slave devices, causing exhaustion of processing resources [32].

The lack of integrity checks enables an attacker with access to the network to modify legitimate messages, fabricate messages or reuse legitimate messages (Man-in-the-Middle) sent to or from slave devices [32]. The attacker may control an automation component (e.g., master or slaves) [33] and cause financial losses or hazard humans' lives, modifying parameters or turning equipment on/off. For example, industrial network penetration can severely affect critical infrastructures such as nuclear power plants and autonomous vehicles, causing severe societal problems.

Threats to ICS components may be highly diverse [1]. Common security threats of ICS may be summarized using some categories, following the IETF standard-7416 [1], [16]:

- Availability threats: Distributed Denial of Service (DDoS), a replay of messages (relay attacks), selective forwarding, grey hole, virus, worm, and botnets.
- Integrity Threats: Sabotage, terrorism, scavenging, intercepting or altering data, service spoofing, tunneling, bypassing controls, logic bombs, and data modifications.
- Confidentiality Threats: Sniffers, information leakage, traffic analysis, and spying.
- Authentication / Authorization treats unlawful use, piggybacking, repudiation, unauthorized access, physical intrusion, back door, Trojan, and masquerade.

Table I consolidates potential industrial network incidents, potential impacts, and typical ICS' malware programs.

TABLE I
POTENTIAL INDUSTRIAL NETWORK INCIDENTS

Type of Threat	Examples of Potentials Impacts	Malware Examples
Changes in the control system	Suppression of alarms. Alteration in processes behavior with unpredictable results.	Stuxnet, Black Energy, Crashoverrride
Changes in programmable logic	Damage equipment or facilities. Shutdown processes.	Stuxnet, Black Energy, Crashoverrride
Misinformation reported to operators	Causing unappropriated operators' actions.	Shamoon, NotPetya
Tampering controls or safety systems	Suppression of protections and other safeguards with unpredictable consequences.	Triton
Malware infection or DoS Attacks	Force assets will be taken offline for forensics analysis. Damaged system files or compromised the system by controlling it. Consume system or network resources.	Night Dragon, Duqu/Flame/Gauss, Dragonfly, Dragonfly 2.0
Information theft	Sensitive information, for example, industrial secrets.	Night Dragon, Duqu/Flame/Gauss, Dragonfly, Dragonfly 2.0
Information alteration	Sensitive parameters or configurations. Decalibrate sensors.	Shamoon, NotPetya

Based on [4], [12], [13], [18], [34].

Signature-based and knowledge-based techniques use rules and comparisons to identify deviations from the network's normal behavior. This form of detection is highly efficient for known situations. Still, it has difficulties detecting anomalies that do not necessarily change the behavior of the network visibly. An attacker can use permitted operations to evade detection. Techniques based on statistics and anomalies consider the usual behavior of the network to detect differences. In highly periodic networks, they can generate a model based on normal data and, through minor deviations, identify abnormal situations that may represent attacks. Techniques based on machine learning can also detect deviations based on previously generated models. Still, the main techniques applied in IDS need named data, which makes it challenging to create these models. They can be used as long as historical attack data is

TABLE II
GENERAL AI TECHNIQUES FOR INTRUSION DETECTION SYSTEMS

Technique	Description
Signature-based	Trying to find specific patterns in the frames transmitted in the network; is good for highly periodic networks; however, it does not detect new types of attacks. It detects attacks by comparing the gathered information with attack signatures.
knowledge-based	Use knowledge about specific attacks to identify threats. (rules, logic-based, etc.) It is based on observing data against a set of predefined rules.
Statistical-based (Semi-supervised)	Use inference tests to verify whether part of the data conforms to a given statistical model. A model of network traffic is created that characterizes the stochastic behavior of the network.
Anomaly-based (Semi-supervised)	Compare the system's current state and generate data with normal behavior to identify deviations present when the intrusion occurs. Detects anomalies by analyzing deviations from normal (modeled) behavior. Normal traffic is used to train a model to identify normal behavior. Traffic profiles are created using system indicators, such as CPU usage and login failure correlated to the time and day of the week. An alarm is triggered when new traffic data fails to fit a predetermined indicator.
Machine-learning based (Supervised)	Create mathematical models that learn and improve themselves over time to detect intrusions. Artificial intelligence (e.g., neural networks) and statistical models are also applied (e.g., classification, clustering). It compares an established model to validate the collected data patterns, and they rely on training with previously observed data and usually apply classification techniques.
Machine-learning based (Unsupervised)	Does not require training data. Commonly use statistical techniques like clustering.

Based on [1], [8], [13], [18], [27], [34]–[36]

available.

Several defense techniques may be applied in industrial networks. IDS are recognized as a strong line of defense mainly in situations with no other efficient cybersecurity mechanisms [19]. One evidence of this is the volume of studies related to these subjects.

Most studies on IDS in industrial networks are concentrated on techniques and algorithms for detecting anomalies or intrusions in SCADA networks based on routable protocols and the traditional techniques already applied in business networks. Some studies propose solutions for networks based on serial protocols but are limited to specific protocols, like Modbus and CAN [30]. Although these works deal with serial networks, they are not generic to the point of being implemented in other well-known protocols and used in industry, such as Profibus DP / PA, Interbus, and DeviceNet.

A notorious gap needs to be addressed in networks based on serial protocols with the primary objective of strengthening the cybersecurity defenses in ICS where these networks are still applied.

C. Intrusion Detection Systems

Over the years, various countermeasures have been developed for ICS; however, most were applied in devices and applications interconnected by Ethernet-based networks. Some examples are embedded security in devices that authenticate and authorize devices connected to the network, access control defining privileges of users, and applications defined by the policies to gain access to services and resources. The networks that compound the industrial and business networks commonly use cryptography to keep messages protected by encryption, firewalls to inspect the packets for traffic control, and updates and patches for program flaws [13].

An ideally secure ICS would not have any vulnerabilities; however, an ICS with this level of security would only be possible if it can be completely isolated even from human users, which is impossible with integrated networks scenario [11]. This situation is even worse in industrial networks based on serial protocols because of their limitations. So, if there is always a vulnerability that can be exploited, a system that performs analytical tests against anomalous patterns could be a second line of defense [19]. IDS often implement this type of protection in ICS [11], which is indicated to be present in any industrial networks [8], [13], [15].

Intrusion detection detects and tracks anomalous activity in computing and network resources [8]. IDS are based on the fact that an intruder's behavior will be noticeably different from that of a legitimated user [37]. As part of IDS techniques, anomaly detection techniques assume something abnormal is suspicious and track behavior, learning from continuous monitoring and data collecting [8]. Anomalies are patterns in data that do not conform to a notion of normal behavior [38].

IDS has requirements that should be delivered to ensure the correct and reliable operation. (1) Data trustworthy - the data collected must be trustworthy and protected against tampering. (2) Interoperability: IDS must interoperate with other components (IT components, for example). (3) Flexibility and scalability: IDS must be adaptable and extend as needed. (4) Robustness: IDS is also susceptible to attacks and must be protected. (5) Completeness: IDS must detect everything (exploits, misuses, and intrusions). (6) Up-to-date: IDS must be updated to detect new threats. (7) reconfigurability: IDS must allow adjustments as needed. (8) Real-time: IDS must detect and respond to anomalies in a timely manner [39]. IDS aims to find patterns of expected devices' behavior.

Like IDS, IPS monitors the network for suspicious activity. The difference is that it can implement measures such as restricting suspicious activity by blocking the access of the element responsible for it [40]. IPS may also be applied to ICS; however, as ICS has high solid availability requirements, the prevention measures can impact the operation, mainly if there is a high number o false-positive. That is why its application is often avoided in the ICS context.

Intrusion detection may be classified according to their internal algorithm. Table II consolidates AI techniques for intrusion detection systems. Signature-based and knowledge-based techniques try to find specific known patterns to identify threats. Sometimes signature-based techniques are considered a sub-group of knowledge-based techniques. Both techniques have difficulty identifying new (no pre-mapped) attacks [11], [15], [22].

Statistical semi-supervised, Anomaly semi-supervised, and Machine-learning supervised techniques need a previous training database to create models to learn about normal and abnormal behavior in the machine-learning case. Based on these models, the algorithms may detect deviations from normal network behavior and generate alerts [11], [15], [22], [41]. Machine-learning unsupervised techniques can be grouped into a broad family that can detect not pre-mapped attacks.

Industrial Serial Networks are cyclic and have regular communication characteristics. This type of communication facilitates the detection of variations in operations, commands, and traffic data, which indicates the updating of a technique based on rules or knowledge. However, using only these techniques limits detecting new attacks not yet pre-mapped. That's why it is recommended for a mix of technics to cover a broad spectrum of detection.

TABLE III
EXAMPLES OF SUSPICIOUS ANOMALIES

Anomaly	Detection	Indication
A significant number of HMI (Human-Machine Interface) workstations	Increase number of IP addresses detected by network flows analysis or logs	A new, unauthorized device into the network, a new system installed, a rogue HMI running using a spoofed IP address
Two devices with the same physical address	More than one physical address per device, detect by network flows or logs	Spoofing address or a device has failed
Traffic increases	Increase in total network traffic, detected by network flow analysis	Unauthorized service running, a network device failure, a batch or process completed
Traffic decrease	Decrease in total network traffic, detected by network flow analysis	Services stopped, a scan running, a new batch or process started
Changes in programming logic indicated by an industrial network monitor code review	Any variation in the individual function code and/or frequency detected by protocol monitors and logs	Process altered, the new process implemented, old process removed, process sabotaged
Unauthorized user logs	Any variation from analysis authentication logs	Personal changes, illegal user authenticated, account compromised
Sensors and actuators anomaly behavior / Command injection, Data Injection	Operational process variations, abnormal function or network operations, detected by processing and use of memory rates, logs and, network flow analysis	Increase of maintenance needs, the unscheduled process stopped
Block information flow	Detected by network flow analysis	Service stopped running, decrease in process performance

Based on [4], [18].

Each technique has advantages and disadvantages, and selecting the best approach depends on several factors such as traffic characteristics, temporal behavior, type of protocol, etc [41]. The choice is no guarantee of success. No single technique can address all potential threats, and sometimes it is necessary to combine various techniques to provide an adequate level of defense [1]. All these techniques are successfully applied in TCP/IP networks such as business networks or Ethernet-based industrial networks. However, they are not still broadly applied in serial-based networks.

III. MAIN AI TECHNIQUES APPLIED IN IDS FOR INDUSTRIAL NETWORKS

Intrusion detection is related to various applications that range from anomalous network patterns to fraud detection and outliers in statistic studies [38]. In the network context, they pick up where other cybersecurity mechanisms end by providing techniques not based on policies and rules but on behaviors [4]. Besides all cybersecurity mechanisms, the IDS takes action when something out of the ordinary happens; in industrial networks, it is expected that variations in the behavior should be minimal due to the solid defense-in-depth posture commonly maintained and the repeatability and determinism characteristics of INPs [17]. Thus, the operational behavior of industrial networks, mainly serial-based ones, should be very predictable.

To implement a successful IDS based on anomalous behavior is necessary has clearly defined what "abnormal", "normal" or "good behavior are". The definition may start from rules and policies and established baselines of behavior. These policies may assess various behaviors, and exceptions to these rules may show suspicious activities. The level of assessment could encompass network traffic patterns, user access, and operation control [38]. Anomalies might be induced for a variety of reasons. Table III shows examples of suspicious activities.

In general, it is a challenge to define normal behavior in industrial networks. For example, attackers often adapt their behavior to appear normal; a current normal behavior might change in the future; due to the industrial characteristics, a noise in the data may be very similar to the anomalous action. Thus, the boundary between normal and anomalous behavior is often not precise [38].

Due to these challenges, most existing intrusion detection techniques try to solve a specific problem induced by many factors like the nature of data, availability of labeled data, type of anomalies, etc. Researchers have adopted and applied specific problem concepts and techniques from diverse disciplines such as statistics, data science, information theory, etc [7]–[11]. Table IV presents a briefly summarized list of intrusion detection techniques.

Table IV presents the application of intrusion and anomaly detection techniques using various algorithms that cover all the abovementioned techniques, but most were applied in routable networks. In serial networks, anomaly detection and knowledge-based techniques were employed. This is unsurprising, as these methods show good detection levels in highly cyclic networks. Despite being applied in routable networks,

TABLE IV
AI TECHNIQUES APPLIED IN IDS FOR INDUSTRIAL NETWORKS

Method	Description	AI Technique	Protocol	References
Snort intrusion detection	It converts MODBUS traffic on a serial link to Ethernet TCP/IP traffic. It transmits it on a closed private network to enable Snort-based intrusion and intrusion prevention features.	Signature	Serial	[42], [43]
Pattern matching method	Regular expression matching modules using an extended shift-And algorithm.	Signature	Routable	[44]
SVM and PSO-OCSVM (Particle Swarm Optimization One-class Support Vector Machine)	OCSVM assumes the coordinate origin as an abnormal sample and then tries to use a hyper-plane to separate the data in the feature space from the origin with maximum margin. Based on the particle swarm algorithm.	Statistical	Routable	[45]
Fuzzy and SVM (Support Vector Machine)	Cooperative network intrusion detection based on Fuzzy SVMs.It implements three types of detecting agents: TCP, UDP, and ICMP.	Statistical	Routable	[19]
Multi-Feature Data Clustering	Data's weighted distances and security coefficients are classified based on the priority threshold of data attribute feature for each node in the network. Based on the classification, the cluster can be marked as normal or abnormal.	Statistical	Routable	[36]
Autoassociative Kernel Regression (AAKR) model and Statistical Probability Ratio Test (SPRT)	AAKR is nonparametric and uses historical exemplars to predict new observations. The SPRT tests whether a new observation is more likely to be in a normal or abnormal mode.	Statistical	Routable	[8]
Payload-based anomaly detection	It is implemented by four stages: Network sensor to capture packages, Features extraction in which byte sequences are mapped in a feature space, similarity computation to compute the pairwise distance between their vectorial representation, and anomaly detection that compares the learned model based on the distance score.	Statistical	Routable	[46]
Multi-Agent Systems (MAS)	Multi-agents approach: Host agent (for hosts data collection), Collector agent (for network data collection), Network analysis agent, and Hybrid Intrusion detection agent (aggregate and analyze information received from network and host agents).	Knowledge	Routable	[39]
Critical State analysis and state proximity.	Multidimensional metric providing a parametric measure of the distance between a given state and the set of critical conditions. The detection is based on the analysis of the system evolution.	Knowledge	Routable	[10]
ILRT (Inter-layer Response Time) and INTM-based (Industrial Network Traffic Monitoring)	INTM for real-time traffic monitoring and ILRT: IRLT depends on the time interval between two consecutive packets with the same source and destination. Thus, the fingerprint signature is defined by a generated histogram, including a specific number of ILRTs.	Knowledge	Routable	[28]
DFA (Deterministic Finite Automation)	It is a finite set of states, a limited set of input symbols, and a transition function. An action is associated with every state transition, and any deviation from the predicted pattern triggers may cause an IDS alert.	Knowledge	Routable	[7]
Rough-Fuzzy Hybrid	It consists of two steps: (1) attribute selection (filtering out redundant and spurious information) based on rough set theory for five classes of intrusions. (2) clustering by using fuzzy c-means.	Anomaly	Routable	[47]
Support Vector Machine (SVM), Random Forest, k-nearest neighbor, and k-means	Those algorithms are used to find outliers using features. Outlier detection can be seen as a binary classifier: An instance is normal or abnormal.	M. Learning	Routable	[48]
Deep Learning	Hierarchically uses successive layers of information-processing stages to classify patterns and learn how to represent them.	M. Learning	Routable	[2], [35]
Hybrid model for anomaly-based intrusion	Hybrid approach using anomaly detection hybrid classifier and feature selection model.	M. Learning	Serial	[16]
Fuzzy C-means (FCM) and Fuzzy Inference System (FIS)	It contains three key steps: unsupervised learning (clustering), anomaly detection, and a rule-based inference engine.	M. Learning	Routable	[18]
Deep Learning	Uses successive layers of information-processing stages hierarchically to classify patterns and learn how to represent them.	M. Learning	Routable	[2], [35]
AI-enabled multimodal fusion-based intrusion detection system (AIMMF-IDS)	Uses recurrent neural network (RNN), bi-directional long short-term memory (Bi-LSTM), and deep belief network (DBN).	M. Learning	Routable	[49]

the other techniques can also be used in serial networks. Technically there is no limitation for your application. Techniques such as statistics or based on neural networks are flexible and adapt to the specific needs of serial networks. Each technique has advantages and limitations, and to amplify the intrusion detection capacity, it would be coherent to combine these techniques to increase their benefits and reduce their limitations. Combining them supposedly can increase detection rates while reducing false positive and false negative rates.

Figure 1 summarizes the advantages and disadvantages of each AI technique. Signature and knowledge-based techniques have low false-positive rates due to their pattern-match algorithm and are indicated to the highly periodic networks with repeatable behavior. However, they need an attack vector dictionary updated, and they have difficulty detecting unknown attacks [11], [38].

Machine-learning, statistical and anomaly-based techniques may be in some way considered in the same family of algorithms because they don't need a complete specification of the attack vector, they can detect unknown attacks, and the supervised and semi-supervised algorithms need previous training labeled data. In semi-supervised algorithms, only the expected behavior should be labeled; in the supervised ones, both normal and abnormal data should be labeled. These categories' disadvantage is that often hard to obtain representative training labeled data when normal and abnormal data should be labeled. Most of them need the effort to generate a model and frequent actualization. Anomaly-based techniques have a low-false negative rate because the abnormal event will disrupt the system's normal behavior. Unsupervised machine learning doesn't need training in labeled data. However, it has a high false-positive rate because it assumes that normal behavior is more frequent than anomalies in the test data [11], [38], [50].

IV. IDS in Industrial Serial-based Networks

Industrial serial-based networks have static network configurations for optimized, repeatable, and deterministic operations cycles [17]. Intrusion detection techniques applied in business networks have different behavior with large change numbers of applications, protocols, and the user with unpredictable and non-periodic traffic trends, usually in short-lived bursts [51].

For industrial serial-based networks, an intrusion detection technique could be built on the deterministic model and applied to analyze execution procedures of protocols, the pattern of communications, and states of operations to detect causes that result in deviations [34]. For these networks, a model can be established based on a set of behavior indicators [4]:

- Network traffic: Total of devices address, traffic volume, flow duration.
- User activity: Total number of active users, total logon and logoffs, configurations change activities (if applicable).
- Process/control behavior: Total unique function codes, the number of unique function codes, total set-point, or other configuration changes.
- Event/incident activity: Total number of events, events by severity.

From the perspective of a serial-based network, there are no restrictions on using all AI techniques. Serial-based protocols are highly periodic, and their traffic characteristics are cyclic (periodic) [17], [42], [43] and less complex than routable (Ethernet-based/TCP) networks [3], [6]. The regular traffic tends to converge in a pattern in the long term.

Knowledge-based and signature-based techniques perform well over highly periodic network behavior present serial-based networks [17]. However, they are limited to unknown attacks [27]. To mitigate this limitation, machine learning, statistical, or anomaly-based techniques can be combined to increase the unknown attack detection rate.

Several techniques can be combined to reduce the low-positive rate, reduce the false-negative rate, and increase the general detection rate (for known and unknown attacks). Supervised learning techniques are commonly used for anomaly detection [18] and have good acceptance among scholars [2], [16], [35], [48], [52]. A voting system, for example, can combine various techniques and improve the overall performance of false positives and negatives.

As serial-based networks have periodic cycles [3], [6], building a training database may not be a problem. Cyclic data capture and simulations could create a consistent and representative database for training, mitigating one of the supervised technique's disadvantages.

V. Conclusion

Industrial networks based on serial protocols usually do not implement security mechanisms natively. This was not a problem when systems were isolated. With the increased interest in the intelligent use of data, interconnections are inevitable. Interconnections lead to new vulnerabilities and threats that need to be adequately mitigated.

TCP/IP industrial networks already have several defense mechanisms, but this is not the reality in serial networks. Although these networks are usually at the lower layers of industrial protocol stacks, they can still be attacked. As they are legacy networks with bandwidth and equipment limitations, the most suitable solution would be an external entity.

IDSs are considered ideal for this situation with the necessary adaptations. Although they are networks with unique characteristics with temporality stipulations and a limited number of operations, there is no apparent restriction for applying these algorithms.

Each technique has advantages and disadvantages, but none can successfully detect all attacks. Thus, the combination of techniques seems to be more coherent.

Future work can evaluate the possibility of applying multiple supervised, unsupervised, or knowledge-based techniques. Using these techniques in serial networks would add defense in a part of the ICS that lacks cybersecurity mechanisms.

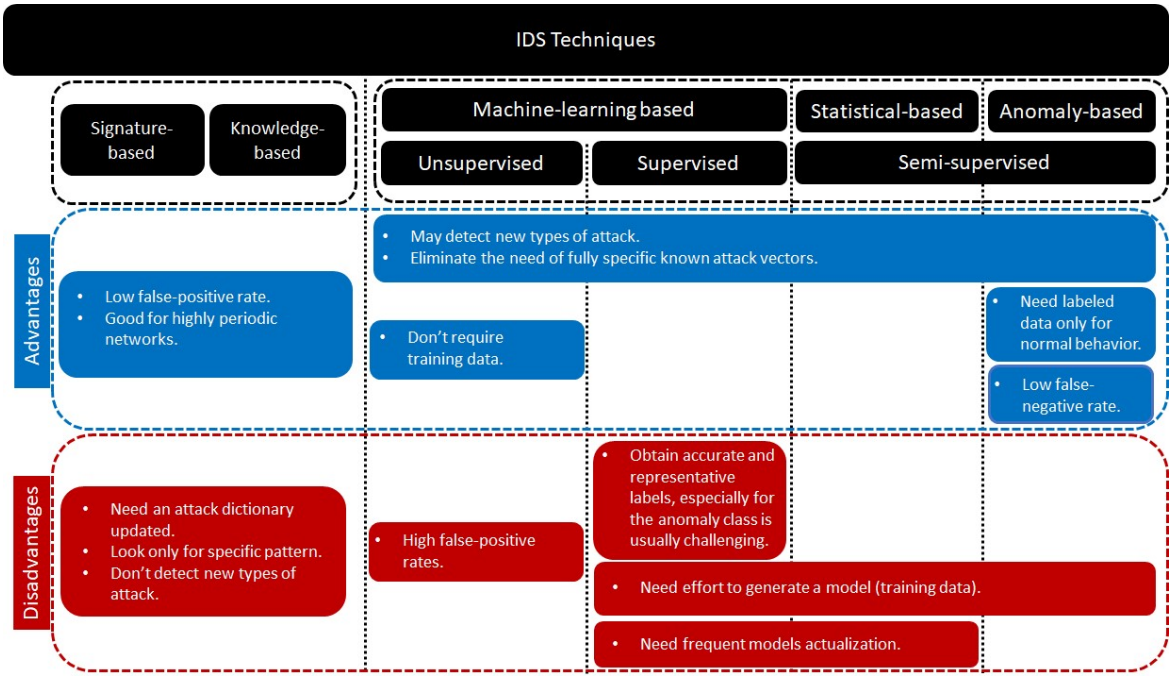

Fig. 1. AI techniques - Advantages and Disadvantages. Based on [11], [38], [50].

REFERENCES

[1] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Analysis of intrusion detection systems in industrial ecosystems," in *SECRYPT*, 2017, Conference Proceedings, pp. 116–128.

[2] A. Hijazi, A. El Safadi, and J.-M. Flaus, "A deep learning approach for intrusion detection system in industry network," in *BDCSIntell*, 2018, Conference Proceedings, pp. 55–62.

[3] P. S. Marshall and J. S. Rinaldi, *Industrial Ethernet: How to Plan, Install and Maintain TCP/IP Ethernet Networks, The Basic Reference Guide*, 3rd ed. ISA-The Instrumentation, Systems and Automations Society, 2016.

[4] E. D. Knapp, *Industrial Network Security - Securing Critical Infrastructure Networks for Smat Grid, SCADA, and other Industrial Control Systems*, 2nd ed. Syngress, 2014.

[5] P. Fuchs, "Apl advanced physical layer," TC002, Technical Report, 2020. [Online]. Available: https://www.pepperl-fuchs.com/brazil/pt/advanced_physical_layer.htm

[6] A. B. Lugli and M. M. D. Santos, *Redes industriais para automação industrial - As-I, Profibus e Profinet*, 2nd ed. Érica, 2018.

[7] N. Goldenberg and A. Wool, "Accurate modeling of modbus/tcp for intrusion detection in scada systems," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63–75, 2013.

[8] D. Yang, A. Usynin, and J. W. Hines, "Anomaly-based intrusion detection for scada systems," in *5th intl. topical meeting on nuclear plant instrumentation, control and human machine interface technologies (npic&hmit 05)*, 2006, Conference Proceedings, pp. 12–16.

[9] W. Tylman, *SCADA Intrusion Detection Based on Modelling of Allowed Communication Patterns*, ser. Advances in Intelligent Systems and Computing. Springer, 2013, book section Chapter 45, pp. 489–500.

[10] A. Carcano, I. N. Fovino, M. Masera, and A. Trombetta, "State-based network intrusion detection systems for scada protocols: a proof of concept," in *International Workshop on Critical Information Infrastructures Security*. Springer, 2009, Conference Proceedings, pp. 138–150.

[11] E. J. M. Colbert and S. Hutchinson, *Intrusion Detection in Industrial Control Systems*, ser. Advances in Information Security. Springer, 2016, book section Chapter 11, pp. 209–237.

[12] K. Hemsley and R. Fisher, "A history of cyber incidents and threats involving industrial control systems." in *Springer: International Conference on Critical Infrastructure Protection.*, 2018, Conference Proceedings, pp. 215–242.

[13] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, 2015.

[14] N. Jiang, H. Lin, Z. Yin, and C. Xi, "Research of paired industrial firewalls in defense-in-depth architecture of integrated manufacturing or production system," in *2017 IEEE International Conference on Information and Automation (ICIA)*. IEEE, 2017, Conference Proceedings, pp. 523–526.

[15] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," *International Journal of Distributed Sensor Networks*, vol. 14, no. 8, p. 1550147718794615, 2018.

[16] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in scada networks," in *2017 IEEE International Conference on Big Data (BIGDATA)*, 2017, Conference Proceedings, pp. 2160–2167.

[17] L. C. Branquinho, Marcelo A.and Moraes, J. Seidl, J. A. Junior, and B. Branquinho, Thigao, *Segurança de Automação Industrial e SCADA*. Campus, 2014.

[18] L. Tomlin, M. R. Farnam, and S. Pan, "A clustering approach to industrial network intrusion detection," in *Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16)*, 2016, Conference Proceedings.

[19] T. Shaohua, D. Hongle, W. Naiqi, Z. Wei, and J. S, "A cooperative network intrusion detection based on fuzzy svms," *Journal of Networks*, vol. 5, no. 4, 2010.

[20] J. D. Decotignie, "A perspective on ethernet-tcp/ip as a fieldbus. s," in *In 4th FeT'2001: IFAC international conference on fieldbus systems and their applications*. In 4th FeT'2001: IFAC international conference on fieldbus systems and their applications, 2001, Conference Proceedings, pp. 138–143.

[21] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications surveys & tutorials*, vol. 15, no. 2, pp. 860–880, 2012.

[22] S. Liyakkathali, F. Furtado, G. Sugumar, and A. Mathur, "Validating anomaly detection mechanisms in industrial control systems," in *Proceedings of TMCE 2020*. Organizing Committee of TMCE 2020, 2020, Conference Proceedings, pp. 89–102.

[23] K.-H. Cho, B.-H. Kim, and K.-S. Park, "Case study on rate-based

traffic control of industrial networks employing lonworks," *International Journal of Systems Science*, vol. 33, no. 3, pp. 161–164, 2002.

[24] P. Fiedler, Z. Bradáč, and F. Zezulka, "New methods of interconnection of industrial fieldbuses," *IFAC Proceedings Volumes*, no. 1, pp. 145–147, 2000.

[25] M. Cheminod, L. Durante, and A. Valezano, "Review of security issues in industrial networks." *IEEE transactions on industrial informatics.*, vol. 9, no. 1, pp. 277–293, 2012.

[26] I. C. I. networks, "Iec standard 1158-2, fieldbus standard for use in industrial control systems – part2 physical layer specification and service definition," IEC - International Electrotechnical Commission, Geneva, CH, Standard IEC TR 61158-2:2010, 2010. [Online]. Available: https://webstore.iec.ch/publication/19160&preview=1

[27] W. Gao and T. Morris, "On cyber attacks and signature based intrusion detection for modbus based industrial control systems," *Journal of Digital Forensics, Security and Law*, 2014.

[28] C. Shen, C. Liu, H. Tan, Z. Wang, D. Xu, and X. Su, "Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 26–31, 2018.

[29] R. Moura, A. Gonzalez, V. N. Franqueira, and A. Neto, "A cybersecurity strategy for internationally-dispersed industrial networks." in *International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2020, Conference Proceedings, p. In press.

[30] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *2016 international conference on information networking (ICOIN)*. IEEE, 2016, Conference Proceedings, pp. 63–68.

[31] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 252–260, 2016.

[32] H. Kim, "Security and vulnerability of scada systems over ip-based wireless sensor networks." *International Journal of Distributed Sensor Networks*, vol. 8, no. 11, p. 268478, 2012.

[33] T. Kwon, J. Lee, and O. Yi, "Vulnerability analysis and security modeling of modbus," *Advanced Science Letters*, vol. 22, no. 9, pp. 2246–2251, 2016.

[34] L. Zhou and H. Guo, "Anomaly detection methods for iiot networks," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 2018, Conference Proceedings, pp. 214–219.

[35] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016, Conference Proceedings, pp. 21–26.

[36] W. Liang, K.-C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2063–2071, 2020.

[37] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE network*, vol. 8, no. 3, pp. 26–41, 1994.

[38] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey." *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[39] C. V. Martinez, M. Sollfrank, and B. Vogel-Heuser, "A multi-agent approach for hybrid intrusion detection in industrial networks: Design and implementation," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1. IEEE, 2019, Conference Proceedings, pp. 351–357.

[40] T. Alves, R. Das, and T. Morris, "Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers." *IEEE Embedded Systems Letters*, no. 10, pp. 99–102, 2018.

[41] A. Meshram and C. Hass, "Anomaly detection in industrial networks using machine learning: A roadmap," in *The International Conference ML4CPS 2016*. Springer, 2016, Conference Proceedings, pp. 75–72.

[42] T. Morris, R. Vaughn, and Y. Dandass, "A retrofit network intrusion detection system for modbus rtu and ascii industrial control systems," in *2012 45th Hawaii International Conference on System Sciences*, 2012, Conference Proceedings, pp. 2338–2345.

[43] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, "Deterministic intrusion detection rules for modbus protocols." in *In: 2013 46th Hawaii International Conference on System Sciences.*, 2013, Conference Proceedings, pp. 1773–1781.

[44] J. Kim and J. Park, "Fpga-based network intrusion detection for iec 61850-based industrial network," *ICT Express*, vol. 4, no. 1, pp. 1–5, 2018.

[45] W. Shang, L. Li, M. Wan, and P. Zeng, "Industrial communication intrusion detection algorithm based on improved one-class svm," in *2015 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE, 2015, Conference Proceedings, pp. 21–25.

[46] P. Düssel, C. Gehl, P. Laskov, J. U. Bußer, C. Störmann, and J. Kästner, "Cyber-critical infrastructure protection using real-time payload-based anomaly detection." in *In International Workshop on Critical Information Infrastructures Security*, 2009, Conference Proceedings, pp. 85–97.

[47] W. Chimphlee, A. H. Abdullah, M. N. M. Sap, S. Chimphlee, and S. Srinoy, "A rough-fuzzy hybrid algorithm for computer intrusion detection," *The International Arab Journal of Information Technology*, vol. 4, no. 3, pp. 247–254, 2007.

[48] H. Yang, L. Cheng, and M. C. Chuah, "Deep-learning-based network intrusion detection for scada systems." in *In: 2019 IEEE Conference on Communications and Network Security (CNS)*, 2019, Conference Proceedings, pp. 1–7.

[49] A. M. Alohali, F. N. Al-Wesabi, A. M. Hilal, D. Gupta, and A. Khanna, "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," *Cognitive Neurodynamics*, vol. 16, pp. 1045–1057, 2022.

[50] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[51] L. A., C. Papagiannaki K.and Crovella M.and Diot, K. E. D., and T. N., "Anomaly-based intrusion detection for scada systems," in *In Proceedings of the joint international conference on Measurement and modeling of computer systems*, 2004, Conference Proceedings, pp. 61–72.

[52] S. D. Anton, S. Kanoor, D. Fraunholz, and H. D. Schotten, "Evaluation of machine learning-based anomaly detection algorithms on an industrial modbus/tcp data set," in *In Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM, 2018, Conference Proceedings, pp. 1–9.