Machine Learning for Cybersecurity in Industrial Control Systems (ICS)

Bhanuprakash Madupati

United Airlines, IL
Jan 2020

Abstract

ICS (Industrial Control Systems) are the backbone of power, water, and manufacturing, amongst other critical infrastructure sectors. Like everything else, traditional ICS is evolving with the modern Information and Communication Technologies (ICT) getting integrated into its stack, exposing itself to potential cyber-attacks. Because of the real-time operational requirements and legacy technology, traditional security methods are frequently ineffective in protecting ICS. Machine Learning (ML) techniques are the major solution to improve Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). This article is a survey paper in which we discussed the use of ML for cybersecurity, such as anomaly detection, integrations with crypto, and adversarial attacks within ICS. Through a discussion of the challenges and future directions around the deployment of ML models inside the ICS environment, this work aims to demonstrate how advanced technologies can help safeguard critical infrastructure against adaptive threats. More focus is given to enhancing the robustness and scalability of the ML models across device/ICS networks.

Keywords: Machine Learning; Cybersecurity; Industrial Control Systems (ICS); Intrusion Detection Systems (IDS); Anomaly Detection; Adversarial Attacks.

1. Introduction

Industrial control systems (ICS) are widely used to control essential processes across industries ranging from power generation to water treatment and manufacturing. In the past, ICSs were closed systems serving particular purposes in well-defined domains. However, with increasingly ubiquitous Islamic communication technology in these systems, they have recently become intercommunicating, which raises questions about new security challenges. The fusion between these modern tools and legacy systems is why Intrusion Control Systems are recognized as one the most common types of cyber threats, such as unauthorized access, malware-infected workflow, and system malfunctioning [6].

ICSS, unlike traditional IT systems, has different design requirements that make sense to be functional over available (redundancy vs. failover in cascade state), real-time over on-time operation, and safety are more important concerns as it is a physical process being automated by such a system. Conventional security methods are inadequate as these do not adequately consider the proprietary protocols, long equipment lifecycles, and extensive geographical spread of ICS environments [6]. With the dynamic nature of cyber threats, an increasing demand for more sophisticated security solutions geared directly towards ICS is necessary.

Machine learning: Among the most exciting advances in ICS security is adopting machine learning (ML) methods. ML capabilities provide new ways to detect and manage potential cyber threats in real-time using Intrusion Detection and Prevention Systems (IDS/IPS). Tracking and correlating an ML model can help you monitor Network Traffic, detect anomalies in System operations, or classify threats based on learnings from

historical data patterns [1].

Specifically, the merger of ML and Programmable Logic Controllers (PLCs), which are an integral part of most ICS environments, has been helpful. Due to their crucial position in commanding physical devices, malware often focuses on PLCs. This will enable ICS systems to do things, such as detect anomalous behaviors, encrypt sensitive communications, and improve the overall security posture of ML [2]. He matriculated into ML for ICS but noted that doing so is not without its difficulties — notably, the vulnerability of ML models to adversarial attacks, wherein slight alterations in input data result in incorrect predictions or classifications [4].

This paper surveys anomaly detection, encryption, encumbrance detection, and adversarial attacks in ICS cybersecurity to enhance aspects. By reviewing state-of-the-art ICS ML applications, this work points out progress and future inspirations toward securing CI from cyber threats.

2. Industrial Control System (ICS) Cybersecurity Challenges

Their operational requirements, technological limitations, and modern network integration present ICS with various cybersecurity challenges. Compounding this complexity is that ICSs do not operate like traditional IT systems — they must never stop running (availability) and respond to real-time events, requiring real-time security solutions [6]. Major cybersecurity challenges for ICS:

2.1. Unique Characteristics of ICS Security

ICS is very different from traditional IT systems mainly due to the real-time aspect and strong requirements for high availability. Several characteristics of ICS make it more complex to secure [6]:

Real Feed Operation: ICSs work around the clock and must respond quickly to control physical processes.

Legacy, Proprietary Protocols: Most ICS systems rely on legacy, proprietary protocols built without security.

Long Lifecycles: ICS components, like PLCs, usually last 10–20 years, making modern security solutions nearly impossible to implement without large-scale system upgrades.

Safety: In many cases, ICSs are responsible for controlling processes that pose risks, where loss of control might cause physical damage or even fatalities.

2.2. Vulnerabilities in ICS

These ICSs face more cyberattacks because they are connected to common networks such as the Internet. Primary vulnerabilities:

No Built-In Security: ICS systems were built for reliability and availability, not security, so these endpoints are open to current cyber threats.

Weak Access Controls: In ICS devices, weak or missing authentication methods undermine confidentiality and lead to unauthorized access to critical systems.

Insecure Communications: Encryption of ICS communication is weak or non-existent, opening the door to eavesdropping and man-in-the-middle attacks.

2.3. Legacy Systems And Its Most Current Form

Concerning cyberattacks, ICS are becoming easier targets as they increasingly apply new Information and Communication Technologies (ICT) technologies. Most of these new attack surfaces are distinct from the isolated systems and introduce remote exploits by just being networked systems [6]. As a result, evolved threats require advanced security measures to be integrated, e.g., Intrusion Detection Systems (IDS) and Machine Learning (ML) based defenses [1].

Table 1: Comparison Between ICS and IT System Security Requirements

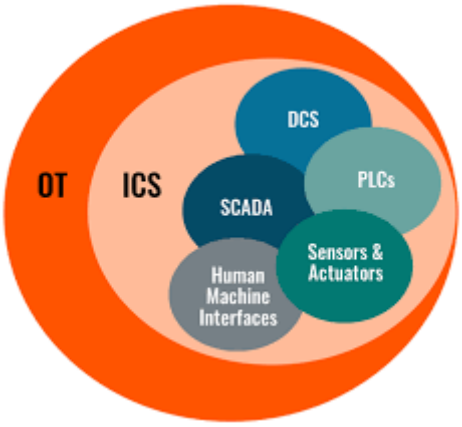
Aspect	ICS	IT Systems
Primary Objective	Availability and Safety	Data Confidentiality and Integrity

Lifespan of Components	10–20 years (long lifecycle)	3–5 years (shorter lifecycle)
Response Time	Real-time response required	Flexible response times
Network Isolation	Historically isolated, now increasingly connected	Traditionally connected to the internet
Protocols	Proprietary, legacy, often unencrypted	Standard, typically encrypted protocols
Security Prioritization	Low (focus on reliability and availability)	High (focus on data protection)

2.4. The Current Cyber Threat Landscape for ICS

As we have learned from the data above, creating a comprehensive picture of our current threat landscape for ICS is a good idea. This can all change whenever these ICS vulnerabilities are exploited en masse to crippling effect by either cyber-criminalists or nation-state actors [6]. Attack Vectors-Deployment Template Changes
Remote Access Trojans (RATs): We routinely observe using RATs to remotely infiltrate and control ICS devices, frequently leveraging weak access controls.
DoS (Denial of Service) Attacks: Attackers may easily saturate ICS networks, causing systems to go down and stopping physical processes.
State-Sponsored Threat Agents (APTs): State-sponsored actors deploy highly evolved tactics to hack ICS for extended periods without getting discovered.

Figure 1: Key Components of ICS Infrastructure Vulnerable to Cyberattacks



2.5. Security Requirements in ICS

With growing threats, ICS must meet several critical security requirements [6]:
Authentication: Authorization from a user authenticated to use the system.
Encryption: keeps communications confidential so they cannot be eavesdropped or tampered with.
Integrity Monitoring: Identifying rogue changes to your ICS configurations or control processes.

3. Intrusion Detection and Prevention using Machine Learning in ICS

Legacy security solutions in ICS environments can no longer keep up with the ever-evolving cybersecurity threats. Traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are being augmented with Machine Learning (ML) to recognize and deflect cyber adversaries. AI/ML models can sift through thousands of data points, spot deviations from normal behavior, and learn the complex patterns in trends from past incidents to foresee future threats rapidly. This section discusses ICS using ML for cybersecurity.

3.1. Machine Learning in Cybersecurity

ML models are widely used in real-time to identify threats, especially where human monitoring at scale can get very expensive. ML algorithms scrape through network traffic patterns to spot unusual activities, producing alerts when they notice them [1]. In contrast with traditional IDS, which uses predefined signatures of known threats, ML-based IDS learns to detect unknown new threats from deviations in system behavior considered normal [4].

3.2. ML Algorithms in ICS Security

Many ML algorithms to improve ICS security Algorithms that are used frequently include:

Support Vector Machine (SVM): SVM is a classification technique used for categorization in cybersecurity. It can classify network traffic as normal or malicious by predicting the patterns in the data on which it is training [2].

Random Forests are also an ensemble learning method to detect all possible intrusions and reduce false positives in supervised matching.

Neural Networks: Deep learning models such as neural networks are very effective in identifying complex attack patterns that could handle vast data; hence, they can be well suited for ICS environments.

Table 2: Common Machine Learning Algorithms Used in ICS Security

Algorithm	Strengths	Challenges
Support Vector Machines (SVMs)	Effective for classification tasks; good at detecting known patterns	Limited in handling large-scale, real-time data
Random Forests	Reduces false positives; improves accuracy by using multiple decision trees	High computational cost for large datasets
Neural Networks	Can handle large amounts of data and complex patterns	Requires large datasets and extensive training

3. Intrusion Detection and Prevention using Machine Learning in ICS

Legacy security solutions in ICS environments can no longer keep up with the ever-evolving cybersecurity threats. Traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are being augmented with Machine Learning (ML) to recognize and deflect cyber adversaries. AI/ML models can sift through thousands of data points, spot deviations from normal behavior, and learn the complex patterns in trends from past incidents to foresee future threats rapidly. This section discusses ICS using ML for cybersecurity.

3.1. What is Machine Learning in Cybersecurity

ML models are used widely in real-time to identify threats, especially where human monitoring at scale can get very expensive. ML algorithms scrape through network traffic patterns to spot unusual activities, producing alerts when they notice them [1]. In contrast with traditional IDS, using predefined signatures of known threats, ML-based IDS learns to detect unknown new threats from deviation in system behavior consideration as normal [4].

3.2. ML Algorithms in ICS Security

Many ML algorithms to improve ICS security Algorithms that are used frequently include:

Support Vector Machine (SVM): SVM is a classification technique used for categorization in cybersecurity. It can classify network traffic as normal or malicious by predicting the patterns in the data on which it is training [2].

Random Forests are also an ensemble learning method used to detect all possible intrusions and reduce false positives in supervised matching.

Neural Networks: Deep learning models such as neural networks are very effective in identifying complex

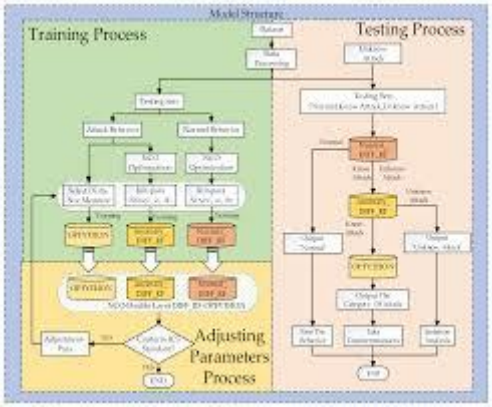
attack patterns that could be handling vast data; hence, they can be well suited for ICS environments.

3.3. Appliances of ML with PLCs

PLC (Programmable Logic Controllers): PLC is one of the fundamental ICS components used in different industrial processes. This lets one embed the machine learning algorithms directly inside PLCs and do real-time anomaly detection, strengthening security capabilities. Recent research suggests that combining ML with PLCs can increase the detection capabilities of unauthorized alterations in control logic, allowing targeted outcomes to be identified and disrupted before damage is caused [2].

Additionally, ML-boosted PLCs execute more sophisticated Intrusion Prevention Systems (IPS) by detecting unusual activities and blocking them instantly. For example, when PLCs spot abnormal traffic or unauthorized access attempts, they automatically block the right of access (denied) or lock up the systems due to ML models [2].

Figure 2: Intrusion Detection method for Industrial Control System Based on Machine Learning



3.4. Encryption and ML in ICS

Apart from anomaly detection, machine learning can also be coupled with encryption methods to fortify the security of ICS. Suppose ML models track any communication channels in ICS (e.g., man-in-the-middle attacks on encryption keys [2]). In that case, this helps ensure the confidentiality and integrity of ICS communications by enabling encryption in ML-empowered security solutions used to protect critical operations.

3.5. Weighing up the pros and cons of ML for ICS security

Although there are many benefits of using ML for ICS security, at the same time, there are several challenges that cannot be ignored:

Advantages:

Real-Time Detection: ML processes real-time data, allowing fast anomaly/threat detection.

Using ML, it can be scaled across large ICS networks, which is suitable for a distributed environment.

Can learn from historical data: ML can keep on learning new attack patterns regularly by analyzing the historical information of attacks, which eventually allows it to improve its detection rate over time [1]

Challenges:

Data Need: Many ML models need data, and many labeled training data may need to be more readily available in ICS environments.

Computational Cost: Training advanced ML models, especially those like neural networks, which are compute-heavy, can be problematic for some components of ICS.

False positives: ML can help decrease the number of false positives; however, misclassifications could occur, especially when new or more sophisticated attack vectors are involved [3].

4. Machine Learning: Anomaly Detection in ICS

Almost Anytime Anomaly Detection via Residual Additional Learning for Security of Industrial Control Abstract & Keywords by Machine Learning (ML), among the most essential applications in improving cybersecurity for Industrial Control Systems (ICS) is anomaly detection. This ability to detect new types of threats sets anomaly detection apart from signature-based intrusion detection systems (IDS), which focus on what they are looking for rather than the ART of overall normal system behavior. This characteristic makes it well-suited to anomaly detection in ICS systems because carried out proactively, as outlined here, could help to make the responses more prompt and efficient on a general scale, considering that both ICS often operate under tight conditions and anomalies may be a sign of cyberattacks or failures [1].

4.1. The Relevance of Anomaly Detection in an ICS

Why is Anomaly Detection so Important in ICS?

Real-Time Monitoring: Many ICSs need to be monitored in real-time formal time for ongoing, regular operation and safety. Anomalies in control commands or network traffic can also indicate abnormal behaviors, which may postnatally be due to malfunctions or attacks [3].

Unknown Threat Detection: With ICS more connected to the outside world, traditional security methods find it difficult to be updated with new or evolving threats. Anomaly detection using ML models can give another perspective on finding Zero-day vulnerabilities or recognizing new attack patterns.

Physical Process Integrity: In ICS, errors mess up data and can result in physical outcomes like machine breakdowns or safety occurrences. Hence, detecting abnormal behavior is important so that industrial service remains functional [6].

4.2. Anomaly Detection with Machine Learning

Different ML models are used to detect anomalies in ICS environments. These models are trained with existing data and differentiate between usual behavior, default settings, and unusual statistics.

Supervised Learning: With Supervised ML models, experts provide labeled datasets to the system, which help in the training phase to learn about normal and abnormal behavior. These models, like Support Vector Machines (SVMs), work well in a rich data environment [2].

Unsupervised Learning—Unsupervised learning models are very useful in ICS environments where there is little labeled attack data. Examples of unsupervised learning include clustering algorithms and autoencoders. These models detect anomaly behavior based on flow data among hosts. An anomaly behavior is a deviation from normal operation [3].

Reinforcement Learning—These algorithms can learn how to handle proper changes in ICS environments by learning from their performance feedback and thus evolve with time to optimize their anomaly detection functions. This is advantageous in ICS setups with a high level of dynamism [1].

Table 3: Comparison of ML Techniques for Anomaly Detection in ICS

ML Technique	Strengths	Challenges
Supervised Learning	High accuracy in detecting known anomalies	Requires labeled datasets, limited for zero-day attacks
Unsupervised Learning	Effective in detecting unknown or novel threats	Higher false-positive rate, no labeled data required
Reinforcement Learning	Adaptive to changes in real-time environments	Complex training process and high computational cost

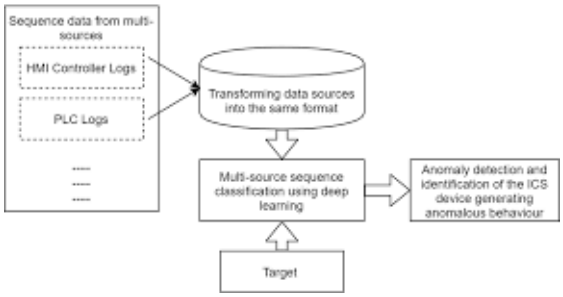
4.3. Applying Anomaly Detection on Key Performance Indicators (KPI)

Key Performance Indicator (KPI): ICS is a critical measure to track the health and well-functioning of different industrial processes. ML models can monitor performance by taking in KPIs, such as temperature,

pressure, or flow rates accustomed to normalcy changes, and send alerts when anomalies arise that may signal operational disruptions or security breaches. ML models can detect abnormal system behaviors by learning the usual operational boundaries of these KPIs [3],

For instance, they could use a Long-Short-Term Memory (LSTM) model on time-series KPI data to aim at future values and flag when the current value is seemingly wrong for an impending failure or attack. This approach allows such characteristics to be tracked early enough that operators detect something odd and possibly take corrective actions before severe damage occurs [3].

Figure 3: Anomaly Detection for Key Performance Indicators in ICS



4.4. Issues with ML-Based Anomaly Detection in ICS

Although machine learning is a significantly valuable foundation for anomaly detection in ICS, many challenges should be resolved as follows:

False Positive Detect: One key problem with anomaly detection is the generation of many false positives from potential negative signals. Although ML models are capable of recognizing anomalies, they do not necessarily imply malicious activities or system breakdowns. These generate avoidable alerts, which operators need to handle, which increases their work [3].

Less data availability: ML Models need data to be well-trained. However, a key challenge in ICS environments is obtaining enough labeled data due to the freshness and obscurity of many threats. Unsupervised models partially alleviate this issue but tend to yield more false positives [2].

Accurate model Interpretability: In ICS, which are critical systems, it is important to understand why an anomaly detection model flags particular behavior as an anomaly for reasons of trust and validation. Nontransparent complex models like neural networks can be highly accurate but difficult to explain because the basis of detection is difficult to understand [3].

4.5. Anomalies Detection in Future Direction

Future developments for anomaly detection in ICS include increasing the accuracy of the detection models and minimizing false positives. This study is an important first step towards building more effective transfer models in ICS, where data are often scarce and labeling difficult. Future research Future studies should also seek to develop models that require smaller datasets. Further, making ML models more interpretable will help the operators to get better understanding and trust on AD systems Describe what; avoid Looping [3].

5. Attacks on ICS Machine Learning Models

However, machine learning (ML) has further enhanced cybersecurity issues in industrial control systems (ICS). Adversarial attacks have become a significant issue of late, where perpetrators alter the input data to fool machine-learning models so they make incorrect predictions or classifications. These attacks are extremely dangerous to ICS environments as misclassification may engage unsafe control actions that cause physical damage or result in system shutdowns [4].

5.1. Adversarial Attacks Explained

Adversarial attacks take advantage of the vulnerabilities inherent in ML models by making slight changes to

input data that lead the model to bad decisions. The changes are often invisible to humans but may have a dramatic impact on the model's output. Adversarial attacks in an ICS setting can tamper with sensor readings, control signals, or network traffic data such that the ML-based Intrusion Detection Systems (IDS) either fail to detect malicious activity or raise false alarms on legitimate behaviors [4].

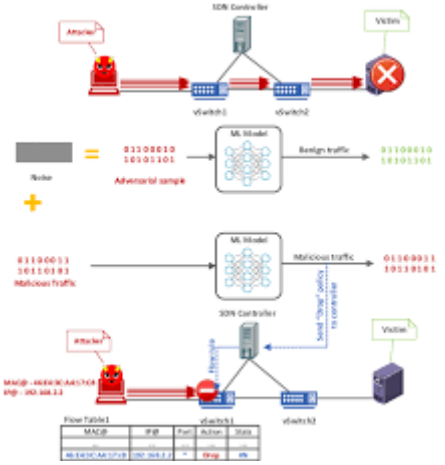
Relevant adversarial attacks relevant to ICS can be grouped into three categories: Accuracy-oblivious Attack (AOA), Black-Box Attack (BBA), and Targeted Attack(TA).

Evasion Attacks: In these attacks, adversaries create inputs that bypass the ML models. For example, small modifications to network traffic structures could make referring intrusion prevention unaccountable for deterring the attack [4].

Poisoning Attacks: In these, the attacker inserts anomalous data into the training dataset [4], distorting the ML model and causing it to make incorrect classifications for new input.

Attack on the Inference by Model Inversion attack: The adversary learns sensitive information about ICS infrastructure from the model's predictions, which might be used for later attacks [4].

Figure 4: Example of Adversarial Attacks on ML Models in ICS



5.2. How they apply to ICS Adversarial attacks

Adversarial attacks on ML models are disastrous in ICS, as system-wide-level effects are severe because of the criticality of these systems. The ICS can be used for nefarious purposes, as well as data from the sensors and to interrupt physical processes. One example may be an adversary tampering with the sensor readings within a Programmable Logic Controller (PLC), which sends out wrong commands to the machinery, leading to damage or even safety incidents [4]. Trend analyzers based on statistical process control techniques are typically used to monitor process-related data under production conditions, where deviations from predefined values pinpoint possible defects in the production equipment early on [3].

System Downtime: Unfortunately, the same scenario pointed out above is also a defense play example. If an adversarial input is misclassified, it can lead to unnecessary system shutdowns that would result in costly downtime in critical industries such as energy or manufacturing.

Trust Erosion: When operators mistrust ML-based detection systems due to frequent false positives resulting in hijacking detection failures, they may return to manual monitoring again, redirecting the benefits of automation.

Table 4: Types of Adversarial Attacks and Their Effects on ICS

Attack Type	Description	Impact on ICS
Evasion Attacks	Crafting inputs to evade detection	Attack goes undetected, resulting in system compromise

Poisoning Attacks	Injecting malicious data into the training set	Model becomes inaccurate, leading to future misclassifications
Model Inversion Attacks	Inferring sensitive information from the model's output	Attackers gain valuable insights for further exploitation

5.3. Attacks Adversarial defense

Adversarial attack defense strategies — To reduce the vulnerability of an ML model against adversarial attacks, several defense mechanisms can be used:

Adversarial Training: This is a training process with adversarial examples to make the ML models more robust. Training With Gate-based Defenses Models can learn to detect and prevent attacks by being exposed to potential adversarial examples in training [4].

Strong Model Architectures: It is imperative to create strong ML architectures to avoid or at least resist adversarial inputs. Defensive distillation is a technique that seeks to reduce the effect of small perturbations on the input data on model behavior (Papernot [4]).

Input Sanitization: Filter and sanitize inputs before passing them to the ML Model. This, in turn, provides the advantage that destructive manipulations can be removed and increases resistance to adversarial attacks [4].

5.4. Challenges to Protecting ICS from Adversaries

Though there are defense mechanisms, securing ML models deployed on ICS from adversarial attacks is still a tough task:

Real-Time Constraints: ICS are subject to real-time requirements, which makes it hard to use computationally intensive defense mechanisms that could introduce latencies [6].

Complexity of ICS Environments: ICS networks are often large and varied, including older systems alongside modern ones. Protecting such heterogeneous environments with strong defense mechanisms is quite difficult [6].

Adversarial examples are difficult to obtain for this task, and large labeled datasets must exist consequently to support adversarial training. Nevertheless, this kind of data is usually only available in some Industrial Control Systems (ICS) environments, making it difficult to develop reliable models [4].

Figure 5: Adversarial Defense Mechanisms for ML Models in ICS

5.5. Future Directions in Defending ML Models in ICS

Future research efforts should target lightweight defense mechanisms that can be seamlessly integrated with ICS environments. Increasing the scalability and efficiency of adversarial training techniques and designing inherently robust networks against those adversarial attacks are essential steps for the security of ICS [4].

6. ICS Security Design with a Human Bias

Technical defenses like Intrusion Detection Systems (IDS) and Machine Learning (ML) models are essential for protecting Industrial Control Systems (ICS), but considering the human factor in security design is just as crucial. The nutshell of secure ergonomics is a research discipline, the main goal of which is to make secure systems that are not just safe but also comfortable for human operators. Operators are the human element of monitoring and managing essential functions supporting critical infrastructure, which is even more critically important in ICS environments. Ignoring the human element creates the potential for security breaches, operator mistakes, and poor system performance [5].

6.1. The Importance of Usable Security in ICS

Usability plays a great role in ICS, ensuring users are not too bothered by their daily routines. When a security solution is overly complex or hard to use, operators can start bypassing it, increasing the vulnerability. For this reason, we need usable security systems—systems that achieve strong security yet are easy to manage [5].

One key lesson organizations must learn from ICS security incidents is human error, whether through configuration or failure to follow security best practices. A user-friendly interface and intuitive security controls can help reduce such mistakes [5].

Training operators who can work the security systems effectively and understand what they do is key to risk minimization [5]. Operators' preparedness to potential threats and ability to respond if sensed is also key.

6.2. A Different View on Security Ergonomics

By humanizing security, security ergonomics takes the principles of conventional physical design and applies them to another factor: how people physically interact with their security systems. This approach emphasizes:

Ease of Use: Systems need to be simple and straightforward so operators can respond rapidly when something is identified without worrying about how the system should be used [5].

Feedback Mechanisms: Security systems must provide status and alert feedback so operators can instantly recognize the operational picture and any problem areas [5].

Error Tolerant: Systems should tolerate user errors without adding material risk to the system's overall trustworthiness. This is especially critical in high-stress settings that necessitate quick decision-making [5].

Table 5: Key Principles of Security Ergonomics in ICS

Principle	Description	Benefit to ICS
Simplicity	Design systems that are easy to understand and use	Reduces operator error and training time
Feedback Mechanisms	Provide real-time feedback to users	Helps operators quickly identify and resolve issues
Error Tolerance	Allow for minor mistakes without compromising security	Improves resilience in high-stress environments

6.3. Configuring Security Systems for Human Operators

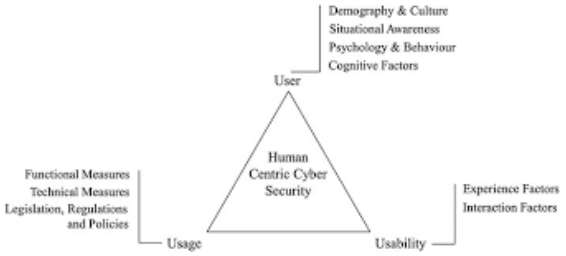
Human-centered design of ICS security means building tools and interfaces that operators can use effectively even under stress. Design should be done allowing this goal:

Increase Real-Time Visibility: Operators must know how the system is currently doing. Graphical depictions of facilities and dashboards for perspectives on the time-related performance of the system and security posture can be seen [5].

Automate the Mundane: Any routine security task, like health checking and log analysis, should be automated to take some of the work of input operators. That frees up operators for more qualitative high-level decision-making [5].

Little or No Disruption: Security controls shall not prevent the normal function of an ICS. For instance, access controls must be tight without introducing drag on operators to perform their duties [5].

Figure 6: Human-Centric Security Design for ICS



6.4. Challenges in Human-Centric Security for ICS

While the advantages are clear, ICS human-centric security implementation also comes with a few challenges: Balancing usability with security: It is common to trade off ease of use and security in a system. The key lies in striking the right balance for any human-centered security design to succeed [5].

Training Costs—Keeping operators informed of new security systems and procedures requires training, which is often expensive. To ensure employees have the most recent information about emerging threats and security technologies, continuous training should be a quotidian investment [5].

Change aversion: When presented with new designs from a security perspective, operators who are used to ICS interfaces based on traditional design techniques may experience significant pushback. That said, if used judiciously and the benefits are demonstrated properly (avoided by careful change management), it is possible to establish these new systems [5].

6.5. Future Directions in Security Ergonomics

With a growing increase in ICS complexity, so will the demand for security ergonomics. Future work should address security mechanisms for ICS security, with cognition elements comprising the burden on the operators. As our ICS networks become more interconnected and lose the air gap today, these tools will become increasingly important as they help us make better decisions and potentially avoid human error [5].

7. Outlook to Machine Learning in ICS Security: Opportunities and Challenges

The rise of Machine Learning (ML) in securing Industrial Control Systems (ICS) is accompanied by promises and new challenges. Even though ML has shown to be useful for supplementing IDS, IPS, and anomaly detection systems, several challenges remain to establish a more flexible, robust, and scalable approach to applying ML in ICS environments.

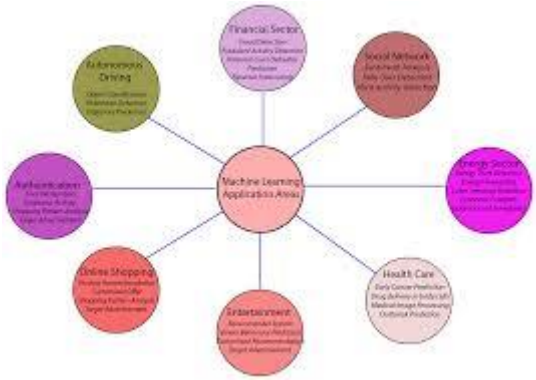
7.1. Increasing ML Scalability and Efficiency in ICS

These are generally large, distributed environments with many devices, including Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems. ML has to provide high scalability, as we expect it will be used in large-scale and decentralized networks with complex infrastructure [6].

Scalable ML Models: Newer ICS models should be able to ingest data from multiple sources and process it in real-time. Approaches such as federated learning, which allows ML models to be trained across distributed nodes without centralizing data, can help scale ML solutions over ICS without heavily loading any single part of the network [7].

Real-Time Limitations: This filtering framework requires rapid detection and response in ICS environments. IC Intelligent models with real-time processing capabilities enable ICS adherence to tight time constraints with algorithms and configurations of SR functionality [3].

Figure 7: Scalability Challenges in Implementing ML for ICS



7.2. Enhancing the Robustness of ML Models Against Adversarial Attacks

Adversarial attacks are still a big problem for ML in ICS. Cleverly crafted adversarial examples can fool ML models by altering raw input data to avoid detection or skew system responses. Security requirements of ML-based IT systems are critical to mitigate these attacks [4].

One approach is to increase the robustness of ML models against this type of attack, e.g., using adversarial training techniques [7], where we train the model using adversarial examples; this would require perpetual updating of models to identify and eliminate new adversarial inputs [4].

Ensuring Model Interpretability: While developing machine learning models in ICS, it is necessary to ensure that the models are transparent and interpretable to understand how decisions are made. This might help unmask backdoors in the model. For operators to trust the model's decisions, simple techniques such as explainable AI (XAI) can be used to give insight into how and why certain actions are being taken by the model [4].

7.3. The current situation with data in Industrial Control Systems (ICS)

A significant friction point regarding deploying ML for ICS is the absence of good, labeled data. ICS environments lack well-labeled historical attacks or anomalies — in contrast to the datasets where ML models are trained successfully in traditional IT systems [2] — resulting in limited effectiveness for ML to be applied.

Synthetic Data Generation: Synthetic data generation can be used to mitigate the shortage of labeled data. The structures orphaned here are synthetic datasets modeling ICS operations and assaults that can direct ML models [7].

Protection of Data Privacy: We also know that with the increasing integration of Information and Communication Technologies (ICT) into ICS environments, more data may be susceptible to being collected and analyzed. It is paramount to ensure data privacy while these models are being trained, especially in contexts like federated learning [7].

7.4. Future Research Directions

Finally, more research and development are needed in several areas to keep ML-based security an effective practice for protecting ICS.

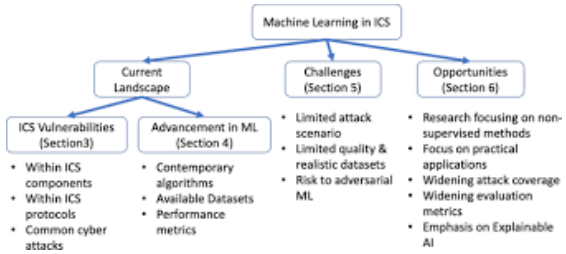
Hybrid Techniques: Traditional rule-based security systems can be combined with ML-based models to form stronger defense mechanisms. By hybridizing or mixing both methods, we can combine the benefits of Machine Learning (new detection capabilities) and rule-based systems (stability – valuable for known attack vectors) to deliver value to Industrial Control Systems [1].

This exercise can be regarded as Cross-Domain Learning, where some advancements made in ML from domains like finance or healthcare can help with the progress of ICS security. Transfer learning, an approach that allows modifying models trained in one domain to a different but similar one, may be an option based on some studies to enhance ICS security with less need for retraining [7].

Energy-Efficient ML: Many ICS environments are resource-constrained, so energy efficiency in ML models is desired. Further research must considerably minimize the computing and energy requirements of ML mo-

dels without affecting performance or accuracy [6].

Figure 8: ML for ICS Security



7.5. Overcoming Operational and Organizational Challenges

More than just technical hurdles, deploying ML within ICS also means overcoming operational and organizational impediments:

Training operators: One of the key requirements is to train site operators so they are confident and able to use ML-based security systems. This includes standardized training programs and simulated environments to help operators develop an effective interaction with such systems [5].

Cost of implementation — Implementing ML models in ICS can be costly, both computationally and integration wise. Organizations need to weigh the value of security investment against the potential savings of averting a costly cyberattack [5].

8. Conclusion

1. Growing ML in ICS Security: Machine learning (ML) algorithms allow for more accurate Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), enhancing cybersecurity for industrial control systems (ICS).

2. Benefits of ML for ICS: ML delivers real-time anomaly detection, helps in threat classification, and integrates encryption. This makes it possible for most existing systems to distinguish between known and unknown threats with greater ease, thereby addressing the ICS side of security.

3. Challenges to Overcome: These are the key challenge areas in how ML can be deployed in ICS: Frequency of happenings, Adversarial attacks, Data Scarcity, Complexity of the ICS environment

4. Adversarial Attacks Mitigation: ICS-based ML models are also susceptible to adversarial attacks. These include defense mechanisms like adversarial training and perhaps inherently safer model architectures.

5. Human-Centric Design Matters: ICS Security Should Be Considered From A Human Central Perspective Systems that consider security ergonomics can be created with high levels of security and operator usability, reducing the chances of human error.

6. Future Research and Development: rom a future research perspective, scalable ML models, energy-efficient solutions for devices operating in network-congested environments (that can manage the tradeoff between speed and accuracy), and enhanced model interpretability deserve special attention to mitigate the evolving threats on ICS environments.

7. Call for Collaboration: There will need to be teamwork between cybersecurity researchers, ICS operators, and ML experts to help overcome the current hurdles of leveraging ML techniques to improve the security of ICS.

Reference

1. Borkar, A. Donode, and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," IEEE Xplore, Nov. 01, 2017, doi: https://doi.org/10.1109/ICICI.2017.8365277.

2. T. Alves, R. Das, and T. Morris, "Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers," IEEE Embedded Systems Letters, vol. 10, no. 3, pp. 99–102, Sep. 2018, doi: https://doi.org/10.1109/les.2018.2823906.
3. J. Shi, G. He, and X. Liu, "Anomaly Detection for Key Performance Indicators Through Machine Learning," 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Aug. 2018, doi: https://doi.org/10.1109/icnidc.2018.8525714.
4. R. Izmailov, S. Sugrim, R. Chadha, P. McDaniel, and A. Swami, "Enablers of Adversarial Attacks in Machine Learning," Oct. 2018, doi: https://doi.org/10.1109/milcom.2018.8599715.
5. Craggs and A. Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), May 2017, doi: https://doi.org/10.1109/sescps.2017.5.
6. S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: https://doi.org/10.1109/jproc.2015.2512235.
7. H. M. Farooq and N. M. Otaibi, "Optimal Machine Learning Algorithms for Cyber Threat Detection," IEEE Xplore, Mar. 01, 2018, doi: https://doi.org/10.1109/UKSim.2018.00018.