DOI: https://doi.org/10.17762/turcomat.v10i2.13630

Research Article

Anomaly Detection in Industrial Control Systems using Machine Learning Techniques

Kiran Kumain
Dept of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

Abstract
Machine learning techniques are being widely used to identify and respond to unusual events in industrial controls systems (ICS), where they play a vital role in preventing potential catastrophes. This paper reviews the various techniques that are used in anomaly detection in these systems. The paper discusses the definition of an anomaly detection process and provides a comprehensive review of the various techniques involved in this area. It also explores the applications of machine learning and statistical techniques in this domain. Some of the techniques that are commonly used in this area include clustering, decision trees and random forests, and control charts. The paper also covers the applications and challenges of anomaly detection in different industrial control systems such as water treatment plants, power grid systems, and chemical plants. Case studies are presented to demonstrate the effectiveness of learning-based techniques in identifying anomalies in these facilities. The paper also presents an evaluation of the performance of various machine learning techniques in performing anomaly detection. The evaluation metrics that are used in these experiments include false positive rate, accuracy, recall, area under receiver characteristic curve, and F1 score. The paper concludes by providing a summary of the findings of the review and the future directions of the investigation in anomaly detection for industrial control systems. The paper offers valuable insights into the latest state-of-art techniques in this area, and it can help practitioners and researchers make informed decisions when it comes to choosing the appropriate ones for their specific projects.
Keywords: ICS, Cyber-attack, ML, Supervised learning, Un-supervised learning.

Introduction

An industrial control system is a collection of hardware, software, and networking technologies that are used to control and monitor various industrial processes as shown in figure-1. These technologies are commonly used in sectors such as water treatment, chemical processing, and power generation. Failure or compromise of an ICS could have a severe effect on the operations of a facility, its environment, or its equipment. The complexity of industrial control systems has increased significantly over the years. They now integrate various sensors, actuators, and controllers, and they have introduced new attack surfaces that can potentially be exploited by unauthorized actors.[1]–[3]

An industrial control system's security is often improved by detecting anomalies, which can indicate a potential security breach or a process irregularity. This process involves monitoring various parameters, such as network traffic and sensor readings, to identify deviations from the expected behavior. If the system finds a deviation, it can then take corrective actions to address the issue. Machine learning techniques are becoming widely used in the detection of anomalies in industrial control systems (ICSs). They can analyze vast amounts of data and adapt to changing conditions to identify previously unrecognized anomalies. This paper aims to provide an overview of the various techniques used in this process.[4]

An anomaly detection process is used in industrial control systems to identify events or patterns that deviate from the system's statistical norms and behavior. It involves comparing historical data with current conditions. Sometimes, an anomaly can be caused by human error, environmental changes, or equipment failure. Unidentified anomalies can be categorized into two types: rule-based techniques and machine learning-driven methods. The former uses predefined rules to identify anomalies, while the latter uses algorithms to learn correlations and patterns from the collected data. Based on the type of labeled data and the availability of unsupervised, semi-supervised, or supervised methods, machine learning techniques can be classified as both.

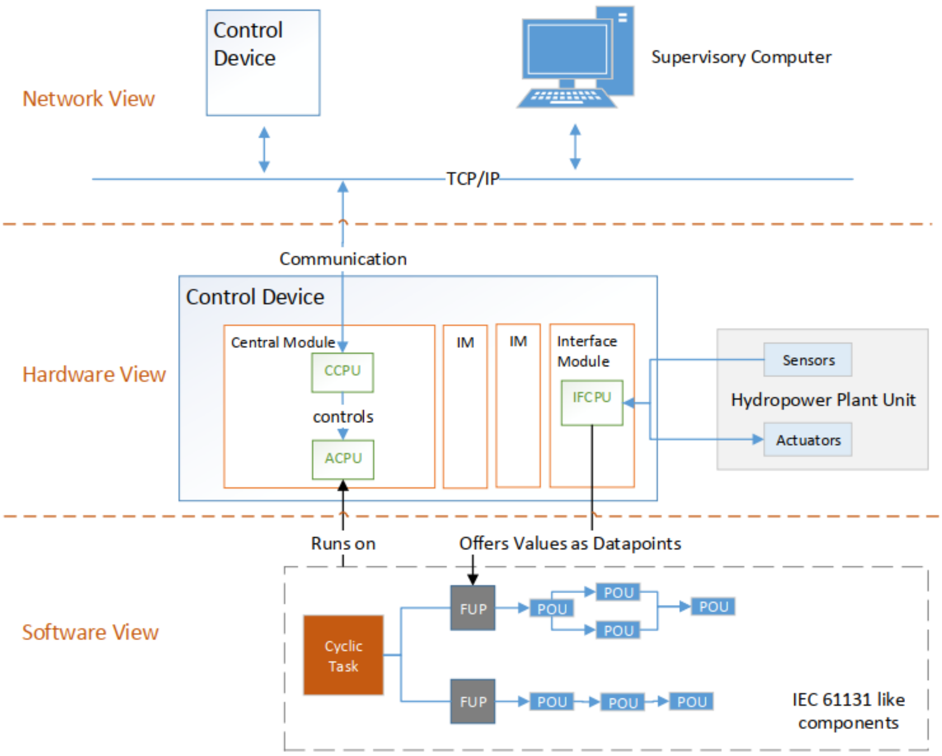

Figure 1 Overview of ICS[5]

An anomaly detection process is very important in industrial control system security as it can help prevent incidents such as security breaches and equipment malfunctions. The consequences of an attack or a failure in the system can range from minor to catastrophic. For example, A cyberattack on an electric power grid system could cause major disruptions to different services, including transportation and communication. A system that can detect anomalous activity or suspicious network traffic can respond to such attacks.

An anomaly detection process can also help improve the efficiency of a process by identifying potential issues that could lead to inefficiencies and costly repairs. In real-time, it can inform the system about possible corrective actions and maintenance.

Due to the increasing number of data sources and the complexity of an industrial control system, machine learning techniques are being widely used to detect anomalies. The most common type of machine learning used for anomaly detection is the unsupervised learning method.

- This method requires that the data collected by the system is labeled, which means that it should be classified as either anomalous or normal. Through supervised learning, the algorithm can map the output labels and input features to identify the anomalies. Machine learning techniques commonly used for anomaly detection in industrial control systems include neural networks, decision trees, and support vector machines.
- Unlike supervised learning, unsupervised techniques do not require labels. Instead, they use a learning algorithm to analyze the data and identify anomalies that do not fit the predefined structure. Unsupervised techniques for detecting anomalies in industrial control systems include clustering, autoencoders, and PCA.
- This technique is commonly used in semi-supervised learning, which combines the advantages of unsupervised and supervised learning. It allows the system to learn with a small amount of data while also leveraging the vast amount of unlabeled information. Some of the commonly used semi-supervised techniques for detecting anomalies in industrial control systems include GANs, self-organization mappings, and special type vehicles (SVMs).

This review paper aims to provide a comprehensive overview of the various machine learning techniques that are used to detect anomalies in industrial control systems. It also explores their limitations and advantages.

RQ-1. What are the most commonly used machine learning techniques for anomaly detection in ICSs, and how do they compare in terms of performance and complexity?

DOI: https://doi.org/10.17762/turcomat.v10i2.13630

RQ-2. What are the advantages and limitations of machine learning-based anomaly detection compared to rule-based approaches?
RQ-3. What are the key factors that affect the performance of machine learning-based anomaly detection in ICSs, such as data quality, feature selection, algorithm selection, and hyperparameter tuning?
RQ-4.What are the open research challenges and future directions for machine learning-based anomaly detection in ICSs, such as the detection of stealthy and sophisticated attacks, the integration of physical and cyber models, and the development of explainable and interpretable algorithms?
The paper aims to provide guidance and insights to practitioners and researchers who are interested in learning machine learning methods for detecting anomalies in industrial control systems. It can also help them identify areas of research that they can pursue in the future.

Literature Review

The control systems used in industrial facilities such as water treatment plants and power grids are vital to their operations. These systems are equipped with software and hardware to monitor and control their processes. However, due to the increasing number of interconnected systems, they are vulnerable to cyber-attacks. Researchers have proposed using machine learning techniques to analyze and identify cyber-attacks on industrial control systems. This method can perform a comprehensive analysis of the data collected from these systems. This review aims to provide a comprehensive analysis of the literature on the use of machine learning techniques in detecting industrial control system anomalies. It will cover various approaches such as contextual anomaly detection, sequence-aware intrusion detection, and physics-based attack detection. The review will additionally provide an overview of the limitations and strengths of each approach.

A. A. Cárdenas et al.[6] discusses the various security risks that are associated with process control systems. It provides an overview of the techniques that can be used to respond to these attacks. The authors of this study recommend that stakeholders, such as end users, security personnel, and system administrators, collaborate to develop effective response plans and policies.

N. Goldenberg et al.[7] presents a method for analyzing the behavior of the TCP/M2O protocol, which is often used in industrial systems. By combining statistical analysis and data mining techniques, the authors were able to create a model that can accurately predict the potential intrusions.

M. Cheminod et al.[8] study thoroughly cover the various security threats that industrial networks face. They identify several common ones, such as malware attacks and network intrusions. They also discuss effective strategies to minimize these risks.

S. Pan et al.[9] presents a hybrid approach to detecting intrusions in power systems, which combines data mining and rule-based techniques. The authors claim that this method can effectively identify different types of attacks.

S. McLaughlin et al.[10] looks into the cybersecurity landscape for industrial control systems, providing an overview of the challenges faced by the security personnel and system administrators, as well as the various vulnerabilities they identify. The authors also talk about the effective strategies to address these risks.

In order to develop a more accurate and effective system for detecting industrial network anomalies, Kravchik et al.[11] proposed a CNN-based system. They tested the proposed system against a dataset of traffic generated by a water treatment facility.

A framework for detecting cyber-physical security threats in smart grids is proposed by A.M.Kosek. et al.[12] It uses an AI neural network model to analyze and identify anomalies in the system. The model was trained using real-world data from a smart grid environment. The results of the study revealed that the proposed system can effectively identify different types of attacks. The paper summarizes the framework's effectiveness and discusses its potential to improve the security of smart grids.

The study conducted by Giraldo et al.[13] looked into the literature on physics-based techniques for detecting attacks in cyber-physical systems. It discussed the limitations and challenges of these methods.

Yip et al.[14] presented a framework that can analyze and identify energy theft and other anomalies in smart grids. It was built using supervised and unsupervised learning techniques. The researchers were able to achieve high accuracy and a low false positive rate with their system.

Caselli et al.[15] presented a framework that can analyze and identify industrial network anomalies. It was built using a Hidden Markov Model. The researchers were able to achieve high accuracy and a low false positive rate with their system.

The literature review indicates that various machine learning techniques, such as deep learning, have been successfully used to identify industrial control system anomalies. But, their performance is heavily dependent on

DOI: https://doi.org/10.17762/turcomat.v10i2.13630

the quality of the collected data and the specific attributes of the system being monitored. Further research is needed to develop systems that can effectively detect industrial control system anomalies.

Anomaly Detection Techniques

Unidentified deviations from the normal behavior of industrial control systems can be detected using techniques such as anomaly detection. There are two types of these techniques: machine learning-based and statistical. In this section, we'll talk about the various techniques used in this field.

A. Statistical Anomaly Detection Techniques:

The goal of statistical anomaly detection is to detect deviations from the normal data distribution. This method is relatively simple and efficient, but it can't detect complex anomalies.

- Control Charts: A widely-used technique for detecting industrial control system anomalies is control charts. These are designed to monitor the system's behavior over time and identify deviations that are significant. In addition to plotting the data's values, control charts also add control limits to define the expected range. Control charts are categorized into three types: Shewhart, cumulative sum, and exponential weighted average. Shewhart charts are commonly used to detect persistent and large anomalies, but they can't be used for detecting short-lived or small anomalies. On the other hand, the exponential weighted average and cumulative sum charts are more sensitive to changes in the data.
- Gaussian Mixture Models (GMM): A type of probabilistic approach to detecting anomalies is known as a Gaussian mixture model. It assumes that the normal distribution follows a Gaussian distribution. This allows GMMs to detect complex anomalies and low probability data points. GMMs are designed to fit a combination of K Gaussian distributions into a data set, where K is its number of components. Their various parameters, such as the mixing coefficients, mean, and covariance, can be estimated through the EM algorithm. Once the training is completed, the GMMs can classify the new data points into either anomalous or normal. GMMs have been used in various applications, such as medical diagnosis and intrusion detection. Unfortunately, their performance may be affected by dimensionality, which increases the number of parameters and makes them hard to train.
- Principal Component Analysis (PCA): A principal component analysis is a method that aims to reduce the overall dimensions of a data set by preserving as much of its original data as possible. It can also be used to detect anomalous patterns. PCA is a process that involves finding a set of principal components that represent the major sources of variance in the data. These components are calculated by taking into account the maximum and lowest variance. After the principal components have been calculated, new data points are projected onto them. Any significant deviations from the predicted pattern are then considered anomalies. PCA can be useful in detecting irregularities in high-dimensional data, and it can be used with other techniques such as GMMs and control charts. Although control charts and Gaussian mixture models are relatively simple and effective methods for detecting anomalies in complex industrial control systems, they can't reliably identify unknown or complex anomalies. However, these techniques can be combined with machine learning approaches to improve the performance of anomaly detectors.

B. Machine Learning-Based Anomaly Detection Techniques:

Machine learning-based techniques are becoming more popular in the detection of complex and unusual anomalies. These methods involve training a model and then testing its accuracy to identify deviations from the normal behavior. Machine learning-based techniques are commonly used in the detection of complex and unusual anomalies. There are three types of these techniques: supervised, semi-supervised, and unsupervised. The former requires the use of labeled data, while the latter uses density estimation and clustering techniques to identify anomalous objects.

- One-Class Support Vector Machines (SVMs): A one-class machine learning technique is known as a supervised learning method that learns a boundary between the normal data and the anomalous data. It can then identify data points outside this boundary.
- Autoencoders: A machine learning technique known as an autoencoder learns a compressed version of the data and then produces a reconstructed representation of the data. It can be used to identify unusual data points and complex anomalies. A semi-supervised model learning technique known as a deep learning technique known as a generator and a discrminator is called a Ganz (GAN). This method trains a neural network to identify synthetic data points that are similar to the normal ones. It can also detect complex and unusual anomalies.
- Generative Adversarial Networks (GANs): A machine learning technique known as a GAN is composed of two neural networks: a discriminator and a generator. The former learns to differentiate between the synthetic and the

DOI: https://doi.org/10.17762/turcomat.v10i2.13630

normal data, while the latter generates the same data. These two networks can be trained to identify complex and unusual anomalies.

We have covered the various techniques for detecting industrial control system (ICS) anomalies using machine learning and statistical methods. Although control charts, principal component analysis, and Gaussian mixture models can be used to identify simple anomalies, they're not ideal for detecting complex ones. On the other hand, machine learning-based methods such as GANs, autoencoders and one-class support vector machines (SVMs) can reliably identify unknown and complex ones.

The selection of an appropriate technique for detecting industrial control system (ICS) anomalies depends on the requirements of the organization and the data it has available. A combination of machine learning and statistical techniques can provide the best possible solution. In the next sections, we'll discuss the various strengths and limitations of machine learning-based anomaly detection.

Industrial Control Systems

An industrial control system is a type of computer-based device that's used to monitor and control various processes in an industrial facility. These systems are commonly utilized in sectors such as transportation, manufacturing, and energy. Failure of an ICS can have dire environmental, safety, and economic consequences.[16], [17]

A. Types of Industrial Control Systems:

- Supervisory Control and Data Acquisition (SCADA) Systems: A typical control system for large-scale industrial processes, such as water distribution systems, oil and gas pipelines, and electrical power grids, is composed of a master control station. It communicates with various remote devices, such as PLCs and terminal units. Data from various devices, such as flow meters, pressure gauges, and temperature sensors, are collected and sent to a central control station, which then processes and analyzes it. The central control station then sends commands to the PLCs and RTUs to adjust the parameters of the process.

- Distributed Control Systems (DCS): A distributed control system is used to monitor and control the various processes in a facility, such as the production of chemicals and pharmaceuticals. It comprises a central control room and a network of devices, which include sensors, actuators, and valves. The data collected by the devices is then sent to the central control room for analysis and adjustment.

- Programmable Logic Controllers (PLCs): A PLC is a type of device that's utilized to control and monitor various discrete processes, such as robotic systems and assembly lines. It has three components: a processor, an input/output module, and a memory. The memory is used to store a program that's designed to control the process.

B. Challenges of Anomaly Detection in Industrial Control Systems:

- Complexity of the data: The vast amount of data generated by an industrial control system makes it hard to identify potential anomalies. This is because the information is often multi-dimensional and noisy.
- Lack of labeled data: It can be hard to train and develop effective anomaly detection models in industrial control systems due to the lack of labeled data. This is because it's typically hard to simulate the behavior of real-world processes.

- High consequences of false alarms: In industrial control systems, false alarms can have significant consequences. They can disrupt operations, increase costs, and lead to lost production and downtime.

- Cybersecurity threats: When it comes to cybersecurity threats, it's important to design an anomaly detection system that can effectively identify and prevent unauthorized access and activities in an industrial control system.

C. Applications of Anomaly Detection in Industrial Control Systems:

- Fault detection and diagnosis: An anomaly detection system can help identify and prevent industrial processes from experiencing significant malfunctions. This process can also help minimize downtime and improve the efficiency of the facility.

- Process optimization: An analysis of anomalies in an industrial process can help identify inefficiencies and improve the efficiency of the process. This process optimization technique can also help decrease waste and improve product quality.

- Cybersecurity: An anomaly detection system can help prevent unauthorized access and activities within an industrial control system. It can analyze network traffic and detect anomalous behavior to identify threats and safeguard critical infrastructure.

- Quality control: An anomaly detection system can help identify potential issues in industrial products before they reach the market. This process can then be used to improve the quality of the products and reduce the costs associated with controlling the production.

- Predictive maintenance: An anomaly detection system can help predict the likelihood of an equipment failure, which would enable quick repairs and a reduction in downtime. It can also help prevent costly repairs and improve the efficiency of a facility.

- Energy management: An anomaly detection system can help identify potential energy-saving opportunities in an industrial facility. It can then help reduce the overall energy consumption of the facility.

An anomaly detection system is a critical component of an industrial facility's operations to ensure the safety and reliability of its processes. It can also help prevent equipment from experiencing failure. In addition, anomaly detection can help improve the efficiency and productivity of an industrial facility by identifying potential issues that could affect the operations of the plant. However, it's important to note that the development and implementation of such systems can be very challenging due to the complexity of the data.

Anomaly Detection in Industrial Control Systems using Machine Learning Techniques

In industrial control systems, anomaly detection is becoming more important in order to identify potential safety hazards or equipment failure. Traditional techniques for detecting complex or subtle anomalies in data are not able to identify them effectively. Through the use of machine learning techniques, such as those used in deep learning, we can improve the accuracy and timeliness of our detection of industrial control systems (ICSs) anomalies. These techniques can learn about the system's behavior and identify deviations from its normal state. They can also help us predict potential problems by adapting to changes over time. In order to improve the effectiveness of anomaly detection in industrial control systems, various case studies have been carried out to analyze the use of machine learning techniques.

- Power Grid Systems: A power grid system is a complex network of interconnected equipment that delivers electrical power to consumers. It is subject to various threats such as natural disasters and cyber-attacks. The detection of anomalies in this type of system is very important to maintain its stability and prevent blackouts. Machine learning (ML) has been used to analyze and detect anomalies in power grid systems. Some of the techniques used include clustering algorithms, decision trees, and artificial neural networks.[3], [12], [14]

- Chemical Plants: A complex system that produces a wide range of materials and chemicals is known as a chemical plant. These facilities are prone to various safety hazards, such as fires and explosions. An anomaly detection system can help prevent accidents and maintain product quality. Artificial neural networks, decision trees, and support vector machines are some of the techniques used to detect anomalies in data in chemical plants.[18]

- Water Treatment Plants: A vital component of communities' water supply, water treatment plants are responsible for providing safe and clean water to their users. They are prone to malfunction due to various pollutants and contaminants that can affect the quality of water and public health. A detection system for anomalies in these systems can help prevent waste, improve water quality, and minimize health hazards. Machine learning (ML) has been used in the detection of anomalies in water treatment plants. Some of the techniques used include clustering algorithms, decision trees, and artificial neural networks.[2], [19]

The use of machine learning (ML) techniques has demonstrated the potential to improve the accuracy and timeliness of industrial control systems (ICSs) anomaly detection. However, there are still challenges that need to be overcome in order to implement these techniques in real-world environments. For instance, the need for large datasets and the need to adapt to the changes in the system are some of the factors that prevent the implementation of these techniques in real-world ICSs.

DOI: https://doi.org/10.17762/turcomat.v10i2.13630

Limitation and challenges

- Lack of labeled data: The sensitive and critical nature of ICS makes it challenging to collect and label data for training and testing machine learning models. This limits the ability to develop accurate models for anomaly detection.

- High dimensionality of data: The data generated by ICS can have high dimensionality, which makes it difficult to preprocess and analyze. This requires significant computational resources and expertise.

- Computation power and memory: Some machine learning techniques require a large amount of computation power and memory, which may not be available in some ICS environments. This limits the ability to deploy machine learning models in real-world ICS applications.

- Model interpretability: Some machine learning techniques, especially deep learning models, are known to be black boxes, making it difficult to interpret the decisions made by the model. This is a challenge for anomaly detection in ICS, where the accuracy and interpretability of the model are important.

- Adaptation to changes: ICS environments are dynamic, and the models need to be continuously updated and retrained to adapt to changes in the system. This requires significant computational resources and expertise.

- False alarms: Anomaly detection systems can generate false alarms, which can be costly and disruptive to ICS operations. Reducing false alarms requires careful design and development of the anomaly detection system, and the integration of domain knowledge and expertise.

- Security risks: Deploying machine learning models in ICS introduces new security risks, as adversaries can potentially exploit vulnerabilities in the models to disrupt or sabotage the system. This requires careful consideration of security risks and the development of secure and robust models.

Conclusion and Future scope

A significant task in industrial control systems (ICS) is the detection of anomalies, which can help ensure the safety and efficiency of the processes. Machine learning techniques can help in this process by identifying potential threats. This paper discusses the various techniques used in anomaly detection in the field, such as deep learning and statistical techniques. This paper presents case studies about the use of certain techniques in various applications, such as water treatment plants, power grid systems, and chemical plants. A performance comparison was also made to highlight the limitations and future directions of this research. Further studies are needed to analyze the limitations and advantages of machine learning techniques for detecting anomalies in industrial control systems. One potential avenue is developing unsupervised learning methods that can learn from the unlabeled data in the system. One of the main directions of this research is the integration of expertise and domain knowledge in the development and design of machine learning models that can be used for detecting anomalies in industrial control systems. This will help improve their interpretability and accuracy. Distributed and edge computing techniques can be used to address the issues related to memory and power consumption in industrial control systems, allowing the development of efficient models.

References

[1] H. Sandberg, S. Amin, and K. H. Johansson, “Cyberphysical security in networked control systems: An introduction to the issue,” *IEEE Control Syst.*, vol. 35, no. 1, pp. 20–23, 2015, doi: 10.1109/MCS.2014.2364708.

[2] D. Ramotsoela, A. Abu-Mahfouz, and G. Hancke, “A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study,” *Sensors (Switzerland)*, vol. 18, no. 8, pp. 1–24, 2018, doi: 10.3390/s18082491.

[3] R. Moghaddass and J. Wang, “A hierarchical framework for smart grid anomaly detection using large-scale smart meter data,” *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5820–5830, 2018, doi: 10.1109/TSG.2017.2697440.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, “Security and Privacy in Cyber-Physical Systems: A Survey of Surveys,” *IEEE Des. Test*, vol. 34, no. 4, pp. 7–17, 2017, doi: 10.1109/MDAT.2017.2709310.

[5] J. Iber, T. Rauter, M. Krisper, and C. Kreiner, “The potential of self-adaptive software systems in industrial control

DOI: https://doi.org/10.17762/turcomat.v10i2.13630

systems," *Commun. Comput. Inf. Sci.*, vol. 748, no. September 2018, pp. 150–161, 2017, doi: 10.1007/978-3-319-64218-5_12.

[6] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," *Proc. 6th Int. Symp. Information, Comput. Commun. Secur. ASIACCS 2011*, pp. 355–366, 2011, doi: 10.1145/1966913.1966959.

[7] N. Goldenberg and A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 2, pp. 63–75, 2013, doi: 10.1016/j.ijcip.2013.05.001.

[8] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informatics*, vol. 9, no. 1, pp. 277–293, 2013, doi: 10.1109/TII.2012.2198666.

[9] S. Pan, T. Morris, and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3104–3113, 2015, doi: 10.1109/TSG.2015.2409775.

[10] S. McLaughlin *et al.*, "The Cybersecurity Landscape in Industrial Control Systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016, doi: 10.1109/JPROC.2015.2512235.

[11] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," *Proc. ACM Conf. Comput. Commun. Secur.*, no. 1, pp. 72–83, 2018, doi: 10.1145/3264888.3264896.

[12] A. M. Kosek, "Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model," *IEEE Proc. 2016 Jt. Work. Cyber-Physical Secur. Resil. Smart Grids, CPSR-SG 2016 - This Work. is Part CPS Week 2016*, 2016, doi: 10.1109/CPSRSG.2016.7684103.

[13] J. Giraldo *et al.*, "A survey of physics-based attack detection in cyber-physical systems," *ACM Comput. Surv.*, vol. 51, no. 4, 2018, doi: 10.1145/3203245.

[14] S. C. Yip, W. N. Tan, C. K. Tan, M. T. Gan, and K. S. Wong, "An anomaly detection framework for identifying energy theft and defective meters in smart grids," *Int. J. Electr. Power Energy Syst.*, vol. 101, no. July 2017, pp. 189–203, 2018, doi: 10.1016/j.ijepes.2018.03.025.

[15] M. Caselli, E. Zambon, and F. Kargl, "Sequence-aware intrusion detection in industrial control systems," *CPSS 2015 - Proc. 1st ACM Work. Cyber-Physical Syst. Secur. Part ASIACCS 2015*, pp. 13–24, 2015, doi: 10.1145/2732198.2732200.

[16] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, no. May, pp. 93–106, 2018, doi: 10.1016/j.jmsy.2018.04.007.

[17] D. Had iosmanović, R. Sommer, E. Zambon, and P. H. Hartel, "Through the eye of the PLC: Semantic security monitoring for industrial processes," *ACM Int. Conf. Proceeding Ser.*, vol. 2014-December, no. December, pp. 126–135, 2014, doi: 10.1145/2664243.2664277.

[18] Q. Lin, S. Verwer, S. Adepu, and A. Mathur, "TABOR: A graphical model-based approach for anomaly detection in industrial control systems," *ASIACCS 2018 - Proc. 2018 ACM Asia Conf. Comput. Commun. Secur.*, pp. 525–536, 2018, doi: 10.1145/3196494.3196546.

[19] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, "Anomaly detection for a water treatment system using unsupervised machine learning," *IEEE Int. Conf. Data Min. Work. ICDMW*, vol. 2017-November, pp. 1058–1065, 2017, doi: 10.1109/ICDMW.2017.149.