A Review of Intrusion Detection Systems for Industrial Control Systems

Mohamad Kaouk, Jean-Marie Flaus, Marie-Laure Potet, Roland Groz. *Univ. Grenoble Alpes, France*
firstname.lastname@univ-grenoble-alpes.fr

Abstract— **Industrial Control Systems are found often in industrial sectors and critical infrastructures to monitor and control industrial processes. Recently, the security of industrial control systems has gained much attention as these systems now exhibit an increased interaction with the Internet. In fact, classical SCADA systems are already lacking with security problems, and with the increased interconnectivity to the Internet, they are now exposed to new types of threats and cyber-attacks. Intrusion detection technology is one of the most important security solutions used today in industrial control systems to detect potential attacks and malicious activities. This paper summarizes previous work for Intrusion Detection Systems approaches in Industrial Control Systems and highlights challenges and opportunities in implementing such solutions. We believe that such insights are valuable for further research in the industrial security context.**

I. Introduction

Industrial Control Systems (ICS) encompass several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). ICS have been used widely in the industrial sector to control and monitor industrial processes. In the past, ICSs were operated as standalone and designed to meet performances, availability, safety, and flexibility requirements of industrial processes. In most cases, they were physically isolated from outside networks and based on proprietary hardware, software, and communication protocols. The security of ICS has been viewed as a low priority goal and handled by using proprietary and closed-source components and standards with limited connectivity.

Nowadays, modern ICS are extensively interconnected with external networks and with the Internet, and encapsulate legacy control protocols in conventional networking protocols such as Ethernet and TCP/IP protocols, and even with the new IoT protocols [1]. The integration of Information technologies (IT) in ICS has led to the evolution of these systems to more intelligent and open systems. Today, ICSs are transitioning from legacy electromechanical-based systems to modern information and communication technology (ICT)-based systems. This transition allows a greater efficiency, lower costs, and a better performance. However, it also raises concerns about the security of these systems as ICS facilities became more vulnerable to internal and external cyber-attacks [2].

In recent years, the security of ICS has gained an increasing attention. The reason behind this is that there a significant increase in the number of security incidents in ICS recently, which clearly illustrate critical infrastructure vulnerabilities [3]. Secondly, ICS control critical infrastructures often (e.g. power grids, water and gas distribution systems, transport systems or nuclear plants), and cyber-attacks on ICS might produce a variety of financial damage and harmful events to humans and their environment. Finally, the continuous evolution of industrial systems to more open and more interconnected systems with the emerging Industrial Internet of Things (IIoT) trend is creating new specific threats and security risks in ICS [4]. Thus, security protection of the relevant control system becomes an important concern.

Intrusion detection technology has emerged since 1980 in Anderson's work [5], which focused on detecting abnormal behavior using the system's audit data. Intrusion Detection Systems (IDS) are designed to detect potential attacks and malicious activities in the network or the system by monitoring its resources and the traffic generated in search of behaviors that violate the security policies. Because of the increasing dependence on information systems in ICS, IDS have become a necessary addition to the security infrastructure of an ICS [6]. However, traditional intrusion detection systems in the IT domain are not entirely adapted to industrial processes [7]. Therefore, the subject of IDS for ICS has drawn great attention in the research field, and many IDS techniques for ICS have been proposed over the past years.

The purpose of this article is to review existing intrusion detection techniques for ICS and to discuss some of the challenges and opportunities for implementing IDS in industrial systems, in order to promote future research in this field. The rest of this article is organized as follows. Section II introduces the architecture of ICS and IDS and enumerates some of the threats and the security requirements of ICS. Section III presents the different approaches for IDS in ICS. The paper concludes in section V.

II. Background

A. Industrial Control Systems (ICS)

An Industrial Control System (ICS) consists of combinations of networked control components that act together in order to achieve real-time monitoring and control of industrial processes. The main difference between ICS and traditional information systems is the close relationship with the physical world. As shown in Fig. 1, the architecture of a modern industrial control system follows the Purdue model defined as the reference model for enterprise architecture [8].

978-1-7281-0521-5/19/$31.00 ©2019 European Union

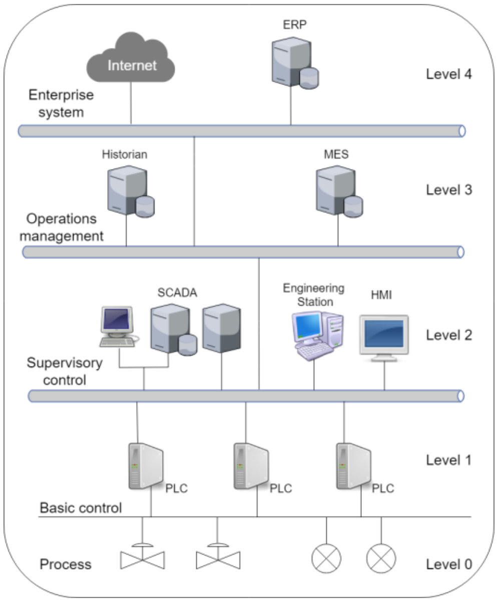

Figure 1. Architecture of an Industrial Control System

ICS can be divided into five layers:

- Level 0: The physical process - concerns the physical reality that an ICS observes and controls.

- Level 1: The basic control - contains field devices, such PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units) that link the physical world to the digital world and are responsible for controlling local operations, receiving signals from the process and sending notifications to upper layers.

- Level 2: The Supervisory control - concerns the servers and operator stations that are used to remotely observe and control field devices.

- Level 3: The process management - responsible for managing production and its related operations (scheduling, storage, maintenance …). It includes manufacturing execution/operations management systems (MES/MOMS) and other components such as data historians.

- Level 4: The enterprise system - manages the business-related activities of the manufacturing operation.

Devices and control components in ICS relay information between different levels through communication protocols. There are many communication protocols that have been used in ICSs such as Modbus, Profibus, dnp3, OPC, BACnet, EtherCAT and many others. Most of these protocols have been designed for specific purposes such as process automation, without security consideration. Therefore, they have been targets for many cyber-attacks. In the next section, we discuss some of the threats and the security considerations in ICS.

B. *Threats and Security considerations in ICS*

Cyber threats to ICS can come from different sources. There is a lot of work addressing cyber-attacks and vulnerabilities in ICS. For example, some researchers focused on cyber-attacks on communication protocols [9]. Other researchers have studied also attacks on software and hardware of different components in the ICS [10].

Cyber-attacks on ICS can be classified in two types of attacks. Firstly, there is the attacks that strike the IT control infrastructure in the ICS. Secondly, other attacks instead rely on knowledge about the controlled process and target the physical process. This type of attacks is known as semantic attacks, and cannot be detected by traditional security approaches as it neither violates protocol specifications nor causes abnormal network traffic. Thus, security systems designed to protect IT systems are not effective in protecting ICS.

The security requirements of ICS differ significantly from those of traditional information systems. According to NIST [11], there are some special considerations when considering the security of ICS such as:

- Timeliness requirements: ICS are generally time-critical and operate in real-time. In contrast. IT systems can accept some level of delay.

- Availability Requirements: ICS processes may be continuous and hence need to be highly available.

- Risk Management Requirements: In a typical IT system, data confidentiality and integrity are typically the primary concerns. However, for an ICS, human safety and fault tolerance are the primary concerns.

- Physical Effects: ICS have often interactions with physical processes and consequences in the ICS domain that can manifest in physical events.

- Communications: ICS use variety of industrial protocols for control and communications that are typically different from IT systems.

C. *Intrusion Detection Systems*

Intrusion Detection Systems monitor networks or systems to detected potential intrusions. They collect and analyze different sources of data (network traffic, security logs, audit data and system/application's information…) to detect abnormal behavior and malicious activities in the system. In general, IDS have three main phases:

- Data collection: responsible for collecting different types of data from the monitored system, e.g., system calls, logs, network flows…
- Selection features: responsible for selecting relevant attributes required for decision-making and represents them as a feature vector.
- Decision engine: processes the given data, as represented as a feature vector, to identify intrusive activities.

Detection techniques can be categorized as misuse-based or anomaly-based detection. In misuse-based or signature-based detection, the IDS monitors all packets and events in the system and compares them against a database of signatures of well-known attacks. While this technique is very effective in detecting known threats, it fails to detect unknown threats and zero-days attacks. On the other hand, anomaly-based IDS are based on identifying a model of system's normal behavior that is used to automatically classify significant deviations from this model as being anomalies. Anomaly detection systems can detect new attacks but they suffer from high false alarm rate.

In addition, IDS can be also categorized based on the information source it uses and its position within the network architecture. This can gives Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDS are generally software components that monitor a single system. They use different source of data such as logs and systems calls to identify intrusion behavior in the monitored system. On the other hand, NIDS are generally physically separate devices located on the network of the system being monitored. NIDS collect and analyze network traffic to detect potential intrusions.

Because ICS are quite different from IT systems in some ways, traditional intrusion detection systems in the IT domain are not entirely adapted to ICS. This is due to the presence of a production process. Thus, the close relationship between the cyber and the physical must be considered as a whole for the security issue of industrial systems.

III. IDS FOR ICS

Since the occurrence of Stuxnet in 2011, the research on methods and technologies of ICS information security problem has attracted widely concern in the research field. Intrusion detection technology has been widely regarded as an important technology to detect intrusions and malicious activities in the ICS. At present, there are several types of IDS available on the market that have been used in the industrial sector such Snort and Bro IDS. Snort is a rule based open source network intrusion detection developed by Cisco. Snort analyzes network traffic in search for rule violations, and alerts the administrator of suspicious activities. Bro is a network-based IDS developed by the University of Berkeley that uses a protocol parser to parse network packets In this section, we review some of the different techniques used in IDS for ICS.

A. Signature-based IDS

In his work [12], Perterson proposed Quickdraw: a Snort based IDS that uses a set of rules developed for the industrial control protocols Modbus/TCP and DNP3. Quickdraw rules can detect several attacks on the ICS such as configuration attacks, coil and register read/write attacks, Modbus attacks and others. Morris et al. [13] have also used a Snort-based IDS to detect illegal data in the Modbus protocol in a serial-based ICS. They provided details on 50 intrusion detection rules to detect malicious activity in ICS [14].

B. Anomaly-Based IDS

The basic idea with anomaly-based approach is to construct models that characterize the expected behavior of the system. An approach to do this is to collect traffic data from the ICS and then applying statistical analysis or machine learning algorithms to the collected data, in order to identify normal behavior patterns of the system. While another approach focuses on specifying the allowed behavior of the system instead of capturing the normal behavior. This technique is known as specification-based and designed to combine the strengths of signature-based and anomaly-based detection. In general, Anomaly-Based techniques can be classified in three categories:

Statistical-based: in this approach, events or network traffic are processed using statistical algorithms (e.g. Parametric and nonparametric-based methods, Time series analysis, Markov chains …) to verify whether a piece of data conforms or not to a given statistical model, in order to confirm the existence of intrusions. During the anomaly detection process, when an event occurs, it is given an anomaly score estimated by comparison of the currently observed profile and the previously trained statistical profile. The anomaly score indicates the degree of irregularity for the specific event, and if the anomaly score is higher than a certain threshold, the IDS will generate an alert.

Machine learning-based: are based on establishing a mathematical model that enables the events analyzed to be categorized. Based on the learning methods, machine learning techniques can be supervised or unsupervised. In supervised learning, the training data is labeled. This means that for every input data in the training set, the data is characterized as normal or abnormal behavior. In contrast, in the unsupervised learning, the data is not labeled and the machine will learn by analyzing the data characteristics to construct the classifier. Machine learning algorithms include: Artificial neural networks, Bayesian networks, Support Vector Machines (SVM), Fuzzy logic, Deep learning, Clustering and classification, Decision trees...

Specification-Based: in this approach also known as knowledge-based, the model is constructed based on specifications defined by experts to characterize legitimate system's behaviors, which reduces the number of false positives. State diagrams, finite automata, formal methods, etc. are used often in specification-based IDS.

In addition, we can divide anomaly-based IDS based on the data they use. Similar to IT systems, some IDS work in the cyber part of the system, and focus on detecting changes in protocols format or in the traffic transmitted in the industrial network. However, ICS are cyber-physical systems that interact with a physical process. Taking into account this aspect is paramount to the detection of attacks relying on advanced knowledge of the process. Therefore, researchers have developed IDS solutions that make full use of the semantic information by monitoring process data, control commands, and even ICS physical model. This type is known as process-aware IDS. Table 1 represents a several IDS for ICS that can be found in the literature.

TABLE I. A TAXONOMY OF IDS FOR ICS

Ref	IDS Type	Technique type	Data	Process / control semantics	Method
[15]	NIDS	Machine learning (ant colony clustering)	Network packets	No	Perform online nearest neighbor clustering on the training dataset, in order to get clusters and then transform them into fuzzy rules that determine if the data is normal
[16]	NIDS	Statistical	System indicators	No	Use an auto-associative kernel regression model coupled with a statistical probability ratio test to identify normal and anomalous behavior patterns in SCADA systems based on several indicators, including link utilization, CPU usage and login failure.
[17]	NIDS	Specification-based	Modbus attributes	No	Define the specifications for the expected communication patterns and the legal values in the Modbus data fields and use them to extract the snort rules
[18]	NIDS	Statistical	Network packets	No	Find malicious traffic in network traffic flows using statistical methods to calculate the probability that a pattern is normal or malicious
[19]	NIDS	Specification-based	Modbus attributes	Yes	Detect illegal packets sent by PLCs or RTUs by making a semantic analysis of control commands and modeling the states of the system to detect invalid control commands usually drive the system into a critical state
[20]	NIDS	Machine learning (neural network)	Network packets	No	Modeling the normal behavior of the system using combination of two neural network learning algorithms (Error Back-Propagation and Levenberg-Marquardt) with a specific window based feature extraction technique proposed to extract 16 kinds of network features
[21]	NIDS	Statistical	Network packets	No	The anomaly detector learns a global model of normal behavior then byte sequences of packets are compared to the previously learned model and based on the distance (deviation) an anomaly score is calculated
[22]	NIDS	Specification-based	Network packets and system specifications	No	Extract legal and illegal network traffic patterns from the predefined protocol specifications and the formal description of a system and then transforms them into models of legitimate and illegitimate traffic
[23]	NIDS	Machine learning (neural network)	Process data	Yes	A neural network based IDS monitors the physical properties of the controlled system to detect false response injection attacks
[24]	NIDS	Machine learnig (fuzzy logic)	Network packets	No	Fuzzy rules that represent the normal behavior patterns of ICS are be extracted from the network packet using an adapted online nearest neighbor clustering algorithm
[25]	HIDS	Specification-based	Process variables	Yes	Design a formal modeling language to describe the states of the system, then a parametric measure of the distance between a given state and the set of critical states can be used to track the evolution of the system to a critical state
[26]	HIDS	Specification-based	Process data and control commands	Yes	Describe the behavior of the system using linear model that can be used to predict the output of the physical system based on the control input sequence and thus any attack to the sensor or controller data can be detected by comparing the expected output with the received signal

[27]	NIDS	Specification-based	Packet attributes	No	Develop a packet parser for DNP3 protocol and using process specifications the security policies of the system are extracted and used by a Bro-based IDS to verify the legal values of the different fields in the DNP3 packets
[28]	NIDS	Specification-based	Control commands	Yes	Propose a semantic analysis framework that combines system knowledge of both cyber (control commands) and physical infrastructure (sensor measurements) in power grid to estimate what the system state will be if a control command is allowed
[29]	HIDS	Machine learning (autoregressive model)	Process variables	Yes	Detect process control attacks by watching variables in the network traffic in an ICS and compare captured values to predicted values that have been computed from a learning period using autoregressive model
[30]	NIDS	Machine Learning (One-Class SVM)	Network traffic	No	Use One-Class Support Vector Machine (OCSVM) method, which does not require labeled training data and used to construct the traffic models to distinguish the normal behaviors from the abnormal behaviors
[31]	HIDS	Machine learning (clustering)	Process variables	Yes	Propose an unsupervised learning approach, which consists of identifying consistent/inconsistent states from unlabeled data by giving an inconsistency score to each observation using the density factor for the k-nearest neighbors of the observation than extracts proximity-based detection rules for each behavior, whether inconsistent or consistent
[32]	NIDS/ HIDS	Statistical methods	Network packets and Process variables	Yes	A multimodel-based IDS uses different models that represents different aspects of the system (communication, physical states, control flow) to detect anomalies then an intelligent classifier based on hidden Markov model (HMM) is used to distinguish the attack from the fault
[33]	NIDS	Statistical	Network packets and Process variables	Yes	Model network traffic traces into used a Discrete-Time Markov Chain (DTMC) model and extracts their semantic meaning to describe the normal message sequences then a detection mechanism based on the computation of a weighted-distance among Markov chain states is used to detect semantic attacks
[34]	NIDS	Machine learning (classification)	Network packets	No	Monitor and analyze data of the network traffic to calculate a running average of the telemetry data, then using a classification algorithm the IDS can detect the anomalies in the traffic
[35]	NIDS	Specification-based	Network packets	No	Perform deep inspection for Modbus TCP traffic in real time. It consists of two parts: rule extraction and deep inspection. The rule extraction module is responsible for extracting normal and abnormal rule set. The deep inspection module performs anomaly detection based on the extracted relationships

IV. Discussion

This paper reviews papers for IDS in ICS. Although the intrusion detection technology for ICS develops quickly, it is still need to improvements. A set of challenges faces the implementation of IDS in ICS. As we saw, the majority of the approaches found in the literature is anomaly-based, i.e. they try to detect any significant deviation from a reference behavior. However, an anomaly can be caused by a fault or an attack. A fault is handled in a different way than an attack. Therefore, there is a great need for methods that can distinguish between a fault and an attack to improve the way that IDS can respond to alarms. Another challenge is that most of developed IDS are network-based, and thus cannot work with encrypted data. For instance, hardware constraints hinder the use of encryption. However, with the improvements in hardware computation capabilities, new components in the ICS have started to provide encryption. Thus, IDS must rely on more information other than network traffic. Finally, we should consider the performance of IDS as ICS are becoming large and complex and consist of widely distributed systems. Therefore, there is necessary to develop new solutions based on distributed and collaborative IDS. We believe that such insights are valuable to promote the future research on the security of ICS.

V. Conclusion

In recent years, the intrusion detection technology for ICS has been developed quickly. This work reviews most of the approaches of IDS in the industrial sector and highlights challenges and opportunities for further improvements in future research.

References

[1] Jean-Marie Flaus. Cybersécurité des installations industrielles- SCADA et Industrial IoT, Techniques de l'ingénieur, 2018

[2] H Abdo, M. Kaouk, Jean-Marie Flaus, F. Masse. A safety/security risk analysis approach of industrial control systems: a cyber bowtie - combining new version of attack tree with bowtie analysis Computers & Security, 2017, 72, pp.175-195.

[3] Mohamad Kaouk, Francois-Xavier Morgand, Jean-Marie Flaus. A Testbed for cybersecurity assessment of industrial and IoT-based control systems. 21e Congrès de Maîtrise des Risques et Sûreté de Fonctionnement λμ21, Oct 2018, Reims, France

[4] Cybersécurité des systèmes industriels, Jean-Marie Flaus, 382p, ISTE Editions 2019.

[5] Anderson JP (1980) Computer security threat monitoring and surveillance. Tech Rep James P Anderson Co 56

[6] Jean-Marie Flaus, John Georgakis. Machine learning based intrusion detection approaches for industrial IoT control systems : a review International Conference on Industrial Internet of Things and Smart Manufacturing, Sep 2018, Londres, United Kingdom

[7] Review of machine learning based intrusion detection approaches for industrial control systems Jean-Marie Flaus and John Georgakis , conference C&ESAR 2018, Rennes

[8] Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in industry, 24(2-3), 141-158.

[9] Morris, T. H., & Gao, W. (2013, September). Industrial control system cyber attacks. In Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research (pp. 22-29).

[10] Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing (pp. 380-388). IEEE.

[11] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.

[12] Peterson, D. (2009, March). Quickdraw: generating security log events for legacy SCADA and control system devices. In Conference for Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology (pp. 227-229). IEEE.

[13] Morris, T., Vaughn, R., & Dandass, Y. (2012, January). A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems. In System Science (HICSS), 2012 45th Hawaii International Conference on (pp. 2338-2345). IEEE.

[14] Morris, T. H., Jones, B. A., Vaughn, R. B., & Dandass, Y. S. (2013, January). Deterministic intrusion detection rules for MODBUS protocols. In System Sciences (HICSS), 2013 46th Hawaii International Conference on (pp. 1773-1781). IEEE.

[15] Tsang, C. H., & Kwong, S. (2005, December). Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In Industrial Technology, 2005. ICIT 2005. IEEE International Conference on (pp. 51-56). IEEE.

[16] Yang, D., Usynin, A., & Hines, J. W. (2006, November). 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) (pp. 12-16).

[17] Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., & Valdes, A. (2007, January). Using model-based intrusion detection for SCADA networks. In Proceedings of the SCADA security scientific symposium (Vol. 46, pp. 1-12).

[18] Valdes, A., & Cheung, S. (2009, May). Communication pattern anomaly detection in process control systems. In Technologies for Homeland Security, 2009. HST'09. IEEE Conference on (pp. 22-29). IEEE.

[19] Carcano, A., Fovino, I. N., Masera, M., & Trombetta, A. (2009, September). State-based network intrusion detection systems for SCADA protocols: a proof of concept. In International Workshop on Critical Information Infrastructures Security (pp. 138-150). Springer, Berlin, Heidelberg.

[20] Linda, O., Vollmer, T., & Manic, M. (2009, June). Neural network based intrusion detection system for critical infrastructures. In Neural Networks, 2009. IJCNN 2009. International Joint Conference on (pp. 1827-1834). IEEE.

[21] Düssel, P., Gehl, C., Laskov, P., Bußer, J. U., Störmann, C., & Kästner, J. (2009, September). Cyber-critical infrastructure protection using real-time payload-based anomaly detection. In International Workshop on Critical Information Infrastructures Security (pp. 85-97). Springer, Berlin, Heidelberg.

[22] Hadeli, H., Schierholz, R., Braendle, M., & Tuduce, C. (2009, September). Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration. In Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on (pp. 1-8). IEEE.

[23] Gao, W., Morris, T. H., Reaves, B., & Richey, D. (2010, October). On SCADA control system command and response injection and intrusion detection. In eCrime (pp. 1-9).

[24] Linda, O., Manic, M., Vollmer, T., & Wright, J. (2011, April). Fuzzy logic based anomaly detection for embedded network security cyber sensor. In Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on (pp. 202-209). IEEE.

[25] Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Fovino, I. N., & Trombetta, A. (2011). A multidimensional critical state analysis for detecting intrusions in SCADA systems. IEEE Transactions on Industrial Informatics, 7(2), 179-186.

[26] Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM symposium on information, computer and communications security (pp. 355-366). ACM.

[27] Lin, H., Slagell, A., Di Martino, C., Kalbarczyk, Z., & Iyer, R. K. (2013, January). Adapting bro into scada: building a specification-based intrusion detection system for the dnp3 protocol. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (p. 5). ACM.

[28] Lin, H., Slagell, A., Kalbarczyk, Z., Sauer, P. W., & Iyer, R. K. (2013, November). Semantic security analysis of SCADA networks to detect malicious control commands in power grids. In Proceedings of the first ACM workshop on Smart energy grid security (pp. 29-34). ACM.

[29] Hadžiosmanović, D., Sommer, R., Zambon, E., & Hartel, P. H. (2014, December). Through the eye of the PLC: semantic security monitoring for industrial processes. In Proceedings of the 30th Annual Computer Security Applications Conference (pp. 126-135). ACM.

[30] Maglaras, L. A., & Jiang, J. (2014, August). Intrusion detection in scada systems using machine learning techniques. In Science and Information Conference (SAI), 2014 (pp. 626-631). IEEE.

[31] Almalawi, A., Yu, X., Tari, Z., Fahad, A., & Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Computers & Security, 46, 94-110.

[32] Zhou, C., Huang, S., Xiong, N., Yang, S. H., Li, H., Qin, Y., & Li, X. (2015). Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45(10), 1345-1360.

[33] Caselli, M., Zambon, E., & Kargl, F. (2015, April). Sequence-aware intrusion detection in industrial control systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (pp. 13-24). ACM.

[34] Ponomarev, S., & Atkison, T. (2016). Industrial control system network intrusion detection by telemetry analysis. IEEE Transactions on Dependable and Secure Computing, (1), 1-1.

[35] Yusheng, W., Kefeng, F., Yingxu, L., Zenghui, L., Ruikang, Z., Xiangzhen, Y., & Lin, L. (2017, March). Intrusion Detection of Industrial Control System Based on Modbus TCP Protocol. In Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on (pp. 156-162). IEEE.