Anomaly Detection of Security Threats to Cyber-Physical Systems: A Study

Nicholas Jeffrey[1[0000-0001-6384-5746]], Qing Tan[2[0000-0002-6447-2133]], José R. Villar[3[0000-0001-6024-9527]]

[1,3] University of Oviedo, Oviedo, Spain
[2] Athabasca University, Athabasca, Canada
[3] University of Oviedo, Oviedo, Spain
[1]njeffrey1@athabasca.edu, [2]qingt@athabascau.ca, [3]villarjose@uniovi.es

Abstract. As the presence of Cyber-Physical Systems (CPS) becomes ubiquitous throughout all facets of modern society, malicious attacks by hostile actors have increased exponentially in recent years. Attacks on critical national infrastructure (CNI) such as oil pipelines or electrical power grids have become commonplace, as increased connectivity to the public internet increases the attack surface of CPS. This paper presents a study of the current academic literature describing the state of the art for anomaly detection of security threats to Cyber-Physical Systems, with a focus on life safety issues for industrial control networks (ICS). As a new contribution, this paper also identifies outstanding challenges in the field, and maps selected challenges to potential solutions and/or opportunities for further research.

Keywords: Cyber-Physical Systems Security, IoT Security, SCADA Security, AI/ML in CPS, Human-in-the-Loop Cyber-Physical Systems (HitL-CPS), Anomaly Detection in CPS.

1 Introduction

Cyber-Physical Systems (CPS) are integrated systems that combine software and physical components [1]. CPS have experienced exponential growth over the past decade, from fields as disparate as telemedicine, smart manufacturing, autonomous vehicles, Internet of Things, industrial control systems, smart power grids, remote laboratory environments, and many more. Academia tends to use the term Cyber-Physical System, while industry tends to use IoT for consumer-grade devices, and IIoT (Industrial Internet of Things) [2] for industrial control systems (manufacturing, process control, etc.).

The rapid growth [3] of CPS has outpaced advancements in cybersecurity, with new threat models and security challenges that lack a unified framework for secure design, malware resistance, and risk mitigations. Much of the attention from academia and industry is focused on consumer-grade IoT devices (smart home automation, etc.). Industrial-grade IoT seems to have less attention from academia and industry, which is

unfortunate, as the consequences of IIoT failure are much higher (power grid failure, oil pipeline shutdowns, train switching, etc.) [4].

Threat detection and prevention is a mature industry in enterprise networks, with large and entrenched vendors (Checkpoint, Cisco, F-Secure, Kapersky, Microsoft, Sophos, Trend Micro, etc.) providing host-based and network-based Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS). Cyber-Physical Systems do not yet have similar IDS/IPS capabilities [5].

Traditional ICS (Industrial Control Systems), also known as SCADA (Supervisory Control and Data Acquisition) have not adjusted to the ubiquitous connectivity of Industry 4.0 [7], and still largely consider security to be an afterthought [7]. Much of this is due to the (no longer accurate) assumption that the ICS / SCADA environment is on an isolated, air-gapped, and trusted network [8,9]. Historically, the primary design goal of SCADA / ICS systems was extreme reliability and predictability. Basic cybersecurity practices such as complex passwords or onerous authentication requirements were seen as barriers to system accessibility and were therefore avoided by the designers and operators of these systems [8]. Anti-malware programs such as signature-based antivirus tools were similarly avoided, to eliminate the possibility of a false positive inadvertently quarantining critical system files. These historical systems typically ran on fully isolated and trusted networks, without connectivity to corporate networks, and definitely without any connectivity to the public Internet.

Additionally, the lack of standardization [10,11] of historical SCADA / ICS systems resulted in widespread usage of proprietary communication protocols, leading to “security by obscurity” [12], due to lack of a robust method of peer review. System vendors typically lacked any method of providing updates or bug fixes, so newly discovered vulnerable systems would typically remain in place for the entire lifespan of the system, relying on network isolation for protection from threats. As modern CPS grew out of legacy SCADA / ICS systems, those historical design considerations became untenable, as connectivity to wireless networks became ubiquitous, as well as a rapid abandonment of isolated air-gapped network environments.

Legacy protocols used in SCADA / ICS (Modbus, DNP, Fieldbus, HART, etc.) [13] are increasingly giving way to TCP/IP used in CPS, largely driven by commercial motivations for connectivity to corporate computer networks and the Internet. The modern reality of CPS is a hyper-connected world where threat actors are omnipresent, and a hostile network environment must be assumed. As modern CPS become increasingly interconnected with other networks, the attack surface has increased exponentially, leading to increasingly frequent breaches of critical national infrastructure (CNI) such as oil pipelines [14], power grids [4], etc.

Due to historical design goals of SCADA/ICS, observability of system state [4] has typically been limited to the current real-time status of a particular sensor or actuator, with relatively simple threshold-based alerts for the system operator. The historical assumption of a SCADA/ICS running on an isolated and fully trusted network meant that intrusion detection and intrusion prevention (IDS/IPS) were not design priorities, leading to a lack of observability in the increasingly hostile network layer of the CPS, making it difficult to detect threats and malicious activity in an increasingly connected world. Anomaly detection of security threats to CPS has become more urgent and

critical to industry and life safety, as CNI becomes increasingly interconnected to public networks. Therefore, further study is needed to advance the state of academic research on the issue, and to develop and apply preventative solutions for industry to ensure safe and secure implementations of CPS.

This study aims to gather a full understanding of the research issue, and to identify existing gaps in the current state of the art that are opportunities for further research efforts. The remainder of this paper is organized as follows; Section 2 provides a statistical analysis of the areas of coverage in existing literature, which will allow identification of gaps in the current research. Section 3 provides a literature analysis for key identified topics. Section 4 illustrates the currently outstanding challenges in the field, with potential solutions for advancing the state of art. Finally, section 5 discusses the conclusions reached in this paper, as well as identifies opportunities for future research.

2 Statistical Analysis

The keywords described previously were used to search literature from the various described sources. A total of 310 papers and online articles were selected and reviewed for this study. As a study done by literature review, this section will provide statistical analysis to describe the existing research presented in the reviewed literature by publisher, publication type, publication year, and country of origin.

The top 5 publishers (IEEE 47%, ScienceDirect 15%, Springer 12%, ACM 9%, MDPI 4%, all others 13%) comprise the bulk of available research in this field and are all well-established academic publishers with robust levels of peer review and quality assurance. It is particularly interesting to note that the *IEEE Access* journal is becoming increasingly popular, due to its open access policies across multiple disciplines, of which CPS is only one of many. The rapid review process (typically 4-6 weeks) retains the traditional high quality of other IEEE publications, but combines the rigour of academic journals with the rapid review process of academic conferences.

Most of the research in this area is published in academic journals (59%), with academic conferences a close second (39%). The field of CPS security is also heavily influenced by industry, but those efforts are typically for short-term tactical responses to current market threats and opportunities. For competitive advantage and trade secret reasons, industry efforts are rarely shared with the broader community, with “security by obscurity” still a common tactic in industry. There is a noticeable lack of industry and academic collaboration in this field, which is an opportunity for improvement.

To maintain relevance in a rapidly changing field, the reviewed literature in this paper is within the last decade, with most articles from the past 3 years. The term “Cyber-Physical Systems” was coined in 2006 by the US-based National Science Foundation (NSF) [4], so little research exists before that date. Earlier research related to CPS existed in fields of cybernetics, industrial process control, and control logic and engineering.

The USA is the largest single source of research in the area, with the top 5 countries generating more research than all other countries combined. Of the top 5 countries, there are 3 countries (USA, UK, India) with English as an official language, making

the overwhelming majority of the available research available in English, often to the exclusion of other languages. The remaining 2 countries in the top 5 (China and Germany) typically publish research in English as well, due to greater availability of reference literature and collaboration opportunities. China and Russia appear to be the only two countries with significant publications in local languages, perhaps due to the large sizes of their domestic industry and academic communities.

3 Literature Analysis

Two of the commonly recurring themes in the available literature are CPS Security Design, and Anomaly Detection / Threat Detection in CPS, each of which will be discussed further below.

3.1 CPS Security Design

CPS is a broad field, and there is an interesting schism between the traditional SCADA systems used for industrial process control (now commonly referred to as IIoT), and the more consumer-focused IoT industry.

Due to product lifecycles measured in years or decades [15], and the historical design assumptions of operating in a fully trusted and air-gapped isolated environment, the traditional Industrial Control Systems (ICS) are much slower to adopt new technologies than their more agile counterparts in consumer-focused IoT devices that have product lifecycles measured in months to a few years.

Unlike their IIoT-based counterparts, the consumer-focused IoT industry was born in an age when ubiquitous connectivity to an increasingly hostile Internet was assumed, which helped drive adoption of standardized communication protocols around TCP/IP, with integrated authentication and encryption [16] functionality designed for the lightweight messaging protocols of devices assumed to have constrained processing power, battery life, and unreliable network connectivity.

Security design efforts for ICS/IIoT tend to focus on a hardened perimeter firewall separating the CPS from other networks, with little in the way of protection once inside the trusted network, reminiscent of the “hard shell, soft center” security posture of enterprise networks in decades past [17]. Due to historical design assumptions of a fully trusted network environment, there is still considerable resistance to actively blocking Intrusion Prevention Systems (IPS) being deployed with CPS, due to the high cost of false positives. Passive Intrusion Detection Systems (IDS) are seeing increasing acceptance in CPS, but due to the extreme heterogeneity, false positives are still a significant issue, making it difficult for the CPS operators to determine what is truly hostile network activity.

The more modern consumer-focused IoT industry has been quicker to adopt a zero-trust model of information security, accepting the reality that they operate in a potentially hostile network environment, and embedding strong authentication and encryption protocols by default [16]. Unfortunately, the rapid advancement of IoT means that product lifecycles are very short, making devices become obsolete quickly, leaving many “orphaned” devices without ongoing vendor support or upgrades to counter new

security threats. While some vendors have included functionality for receiving trusted over-the-air updates to counter newly discovered threats, there are many IoT devices that entirely lack any sort of update functionality, leaving them permanently vulnerable to emerging threats.

Human-in-the-Loop Cyber-Physical Systems (HitL-CPS) are a unique subset of CPS that partially or completely rely on human operator input to control the CPS. This introduces unique security challenges, due to unpredictability from human error, inattentiveness, slower reaction time of humans, susceptibility to social engineering, inconsistent decision-making, etc. The most significant outstanding challenges in this area are gathering a full understanding of the problem domain, improvements in modeling unpredictable human behaviour, autonomic mitigations against intentional and unintentional human-introduced risks, and development of a formal methodology of integrating human feedback in the control loop. Each of these challenges are still in rapid states of development, so the maturity of this area of research is still in its early stages [18].

3.2 Anomaly Detection / Threat Detection in CPS

Threat detection methodologies can be broadly categorized [19] as signature-based, threshold-based, or behaviour-based. Traditional antivirus programs are an examples of a signature-based threat detection methodology, using a centralized and regularly updated database of signatures of malicious files or traffic to trip an alarm on an IDS and/or IPS. Signature-based detection works well on IT networks thanks to standardized communication protocols and low levels of heterogeneity but suffers from high levels of false negatives on OT networks due to their proprietary communication protocols and heterogeneous physical components.

Threshold-based methodologies rely on known ranges of acceptable operation, which are relatively easy to define on IT networks. Examples of threshold-based threat detections for IT networks include network link utilization, communication latency, processor utilization levels, etc. However, OT networks have proven more difficult to accurately define known ranges of acceptable operation, due to real-world environmental fluctuations [20]. For example, a wireless mesh network of air quality sensors in a smart city environment may have communication latency impacted by fog or rain, making the thresholds of acceptable operation differ based on unpredictable weather conditions.

Behaviour-based methodologies are the most difficult to accurately define on IT networks and are even more challenging for OT networks [21]. Defining an accurate baseline of normal behaviour on an IT network requires a deep understanding of what normal system activity looks like, and it is rare that IT networks are completely unchanged over their entire lifecycle, making any definition of normal behaviour a moving target at best. These challenges are exacerbated on OT networks, which tend to be even more dynamic due to environmental factors such as weather-related variations in temperature, humidity, ambient light, etc. Additionally, the negative impact of a false positive or false negative detection on an OT network has more significant consequences, including physical equipment damage and life safety concerns.

There is considerable interest in the use of machine learning (ML) algorithms [22] for automated threat detection in CPS, but few of the proposed frameworks from academia have seen significant adoption in industry. Due to the extreme diversity in CPS, it has proven difficult to generate a useful training model for AI/ML algorithms, which has resulted in unacceptably high levels of false positives and false negatives for automated anomaly detection. This appears to be a significant discontinuity between the efforts of academia and industry, and is an opportunity to improve collaboration.

4 Outstanding Challenges

A modern CPS can be considered as a combination of corporate computer networks and industrial control networks, sometimes referred to as IT (Information Technology) and OT (Operational Technology), each of which have differing priorities.

Traditional IT networks have used the so-called CIA (Confidentiality, Integrity, Availability) triad to define the organizational security posture, with each facet listed in order of importance. OT networks reverse that order [23], with availability being the most important factor, followed by integrity, with confidentiality the least important facet of overall system security. This difference is largely due to CPS growing out of earlier SCADA / ICS networks used for industrial control processes, where availability was of the utmost importance, with integrity and confidentiality rarely considered due to usage of trusted and air-gapped isolated network environments.

As OT networks merged with IT networks to form modern CPS, those differing priorities have resulted in ongoing challenges that have yet to be fully resolved. IT networks heavily prioritize authentication (who you are) and authorization (what you are allowed to do), which roughly map to the confidentiality and integrity facets of the CIA triad of information security. However, OT networks have traditionally focused so heavily on the availability facet of the CIA triad, that authentication and authorization were assumed to be true [24] by virtue of physical access to the trusted and isolated OT network.

This historical assumption of a fully trusted and isolated environment is no longer true after the interconnection of IT and OT networks, resulting in vulnerability to common network-based attacks such as DDoS, MitM, replay attacks, impersonation, spoofing, false data injection, etc. Compounding the problem, OT networks typically lack integration with antimalware programs, as well as detailed logging capabilities, making it difficult to observe potentially hostile activity on OT networks [25].

There are ongoing efforts [26] to extend the IDS/IPS capabilities of IT networks into OT networks, but the lack of standardized protocols and interfaces to the physical components of CPS makes threat detection very challenging. Those IDS/IPS systems that have been extended into CPS environments struggle with high levels of false positives and false negatives, due to the complexity of CPS.

The single largest challenge facing the secure design and operation of Cyber-Physical Systems is their lack of standardized communication protocols and proprietary nature [27]. Due to the lack of even rough industry consensus for the system development life cycle of CPS, each system designer essentially builds each new CPS from scratch,

without much consideration for multivendor interoperability, secure and robust patching mechanisms, or exposing system telemetry details in a consistent manner for health and security monitoring. This is slowly changing with industry consortiums forming standards bodies such as O-PAS (Open Process Automation Standard) [28], but broad industry consensus has proved elusive.

The highly proprietary nature of CPS products is due to their historical evolution from ICS (Industrial Control Systems), which were designed to operate on closed networks without interoperability or communication requirements with external networks. As OT (Operational Technology) and IT (Information Technology) networks merged to become CPS, the open standards and communication protocols used by IT networks have been rapidly adopted by OT networks [29], but there is still significant opportunity for improvement, particularly for the OT networks that have unexpectedly found themselves connected to public and untrusted networks, including the Internet.

5 Conclusions

As a relatively young (since 2006) field of study, the state of the art for CPS is still rapidly evolving. For historical reasons, CPS lacked a coherent or standardized architecture, so are notable by their extreme diversity, which has hampered the development of threat mitigations in increasingly hostile networked environments. As malicious attacks on critical infrastructure continue to increase, the need for secure and resilient CPS becomes more urgent every day.

Opportunities for further development include increased collaboration between academia and industry, towards the development of best practices for secure design and operation of CPS, with security and observability included much earlier in the system development life cycle.

As the proprietary communication protocols of legacy CPS environments give way to modern standards-based TCP/IP protocols, there are opportunities for cross-pollination between the OT networks of yesterday and the IT networks of today. The use of AI/ML for threat detection is already commonplace in IT networks, but OT networks have seen very limited adoption of this technology, due to the higher cost of false positives. Further research work in this area is recommended.

It is particularly notable that the goals of academia and industry do not appear to be entirely aligned, with industry extremely hesitant to make adopt academic proposals for changes to safety-critical systems. This is a potential opportunity for improved collaboration, as well as research into the development of more realistic simulated CPS environments for low-impact testing. Collaboration efforts are further hampered by the extreme diversity of CPS, making consensus-building around standardized best-practice design and architectural strategies for CPS a significant opportunity for improvement.

Acknowledgement

This research has been funded by the SUDOE Interreg Program -grant INUNDATIO-, by the Spanish Ministry of Economics and Industry, grant PID2020-112726RB-I00, by the Spanish Research Agency (AEI, Spain) under grant agreement RED2018-102312-T (IA-Biomed), and by the Ministry of Science and Innovation under CERVERA Excellence Network project CER-20211003 (IBERUS) and Missions Science and Innovation project MIG-20211008 (INMERBOT). Also, by Principado de Asturias, grant SV-PA-21-AYUD/2021/50994.

References

1. S. Zanero (2017). "Cyber-Physical Systems", Computer, vol. 50, no. 4, pp. 14-16, April 2017, https://doi.org/10.1109/MC.2017.105
2. P. Radanliev, D. De Roure, M. Van Kleek, O. Santos, U. Ani (2021). "Artificial intelligence in cyber physical systems", AI & Society, volume 36, pp 783-796 (2021), https://doi.org/10.1007/s00146-020-01049-0
3. H.M. Rouzbahani, H. Karimipour, A. Rahimnejad, A. Dehghantanha, G. Srivastava (2020). "Anomaly Detection in Cyber-Physical Systems Using Machine Learning", Handbook of Big Data Privacy, pp 219-235, https://doi.org/10.1007/978-3-030-38557-6_10
4. M. Wolf and D. Serpanos (2018). "Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems", Proceedings of the IEEE, vol. 106, no. 1, pp. 9-20, Jan. 2018, https://doi.org/10.1109/JPROC.2017.2781198
5. R. Langner (2011). "To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve", The Langner Group, https://www.langner.com/to-kill-a-centrifuge/
6. G. Tsochev, M. Sharabov (2021). "Artificial intelligence methods used in industry 4.0 in par-ticular industrial control systems", AIP Conference Proceedings 2333, 070017, 2021, https://doi.org/10.1063/5.0041610
7. B. Craggs and A. Rashid (2017). "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design", 2017 IEEE/ACM 3rd International Workshop on Software Engi-neering for Smart Cyber-Physical Systems (SEsCPS), 2017, pp. 22-25, https://doi.org/10.1109/SEsCPS.2017.5
8. W. M. S. Stout (2018). "Toward a Multi-Agent System Architecture for Insight & Cybersecuri-ty in Cyber-Physical Networks", 2018 International Carnahan Conference on Security Technology (ICCST), 2018, pp. 1-5, https://doi.org/10.1109/CCST.2018.8585632
9. R. Das, V. Menon and T.H. Morris (2018). "On the Edge Realtime Intrusion Prevention System for DoS Attack", Proceedings of 5th International Symposium for ICS & SCADA Cyber Secu-rity Research 2018 (ICS-CSR 2018), https://doi.org/10.14236/ewic/ICS2018.10
10. M. Maloney, E. Reilly, M. Siegel and G. Falco (2019). "Cyber Physical IoT Device Management Using a Lightweight Agent", 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2019, pp. 1009-1014, https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00176
11. S. Rehman, V. Gruhn (2018). "An Effective Security Requirements Engineering Framework for Cyber-Physical Systems", Technologies 2018, 6, 65, https://doi.org/10.3390/technologies6030065

12. Q. S. Qassim, N. Jamil, M. N. Mahdi and A. A. Abdul Rahim (2020). "Towards SCADA Threat Intelligence based on Intrusion Detection Systems - A Short Review", 2020 8th Internation-al Conference on Information Technology and Multimedia (ICIMU), 2020, pp. 144-149, https://doi.org/10.1109/ICIMU49871.2020.9243337
13. L. Benbenishti (2017). "SCADA MODBUS Protocol Vulnerabilities", Cyberbit, https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/
14. C. Osborne (2021). "Colonial Pipeline attack: Everything you need to know", Zdnet, https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
15. J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez (2019). "Current cyber-defense trends in industri-al control systems", Computers & Security,Volume 87,2019,101561,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.06.015
16. O. Toshihiko (2017). "Lightweight Cryptography Applicable to Various IoT Devices", NEC Technical Journal, Volume 12, Issue 1, https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html
17. F. Adamsky, M. Aubigny, F. Battisti, et al (2018). "Integrated protection of industrial control systems from cyber-attacks: the ATENA approach", International Journal of Critical Infrastructure Protection, Volume 21, 2018, Pages 72-82, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2018.04.004
18. D. Nunes; J. Sá Silva, F. Boavida (2018). "A Practical Introduction to Human-in-the-Loop Cyber-Physical Systems", Wiley Publishing, 2018, https://doi.org/10.1002/9781119377795
19. M. Wu, Z. Song, Y.B. Moon (2019). "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods", Journal of Intelligent Manufacturing 30, 1111-1123 (2019), https://doi.org/10.1007/s10845-017-1315-5
20. P. Kabiri and M. Chavoshi (2019). "Destructive Attacks Detection and Response System for Physical Devices in Cyber-Physical Systems", 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2019, pp. 1-6, https://doi.org/10.1109/CyberSecPODS.2019.8884999
21. S. Etalle (2019). "Network Monitoring of Industrial Control Systems: The Lessons of SecurityMatters", CPS-SPC'19: Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy, November 2019, https://doi.org/10.1145/3338499.3357354
22. F. A. Alhaidari and E. M. AL-Dahasi (2019). "New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning", 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-6, https://doi.org/10.1109/ICCISci.2019.8716432
23. Y. Ashibani, Q.H. Mahmoud (2017). "Cyber physical systems security: Analysis, challenges and solutions", Computers & Security, Volume 68, 2017, pp 81-97, https://doi.org/10.1016/j.cose.2017.04.005
24. W. M. S. Stout (2018). "Toward a Multi-Agent System Architecture for Insight & Cybersecu-rity in Cyber-Physical Networks", 2018 International Carnahan Conference on Security Technolo-gy (ICCST), 2018, pp. 1-5, https://doi.org/10.1109/CCST.2018.8585632
25. S. V. B. Rakas, M. D. Stojanović and J. D. Marković-Petrović (2020). "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems", IEEE Access, vol. 8, pp. 93083-93108, 2020, https://doi.org/10.1109/ACCESS.2020.2994961
26. Q. S. Qassim, N. Jamil, M. N. Mahdi and A. A. Abdul Rahim (2020). "Towards SCADA Threat Intelligence based on Intrusion Detection Systems - A Short Review", 2020 8th International Conference on Information Technology and Multimedia (ICIMU), 2020, pp. 144-149, https://doi.org/10.1109/ICIMU49871.2020.9243337

27. A. Sundararajan, A.Chavan, D. Saleem, A.I. Sarwat (2018). "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security", Energies 2018, 11, 2360, https://doi.org/10.3390/en11092360
28. R.D. Bartusiak, S. Bitar, D.L. DeBari, B.G. Houk, D. Stevens, B. Fitzpatrick, P. Sloan (2022). "Open Process Automation: A standards-based, open, secure, interoperable process control archi-tecture", Control Engineering Practice, Volume 121, 2022, 105034, ISSN 0967-0661, https://doi.org/10.1016/j.conengprac.2021.105034
29. R. Kabore, A. Kouassi, R. N'goran, O. Asseu, Y. Kermarrec, P. Lenca (2021). "Review of Anomaly Detection Systems in Industrial Control Systems Using Deep Feature Learning Approach", Engineering, 13, 30-44, https://doi.org/10.4236/eng.2021.131003