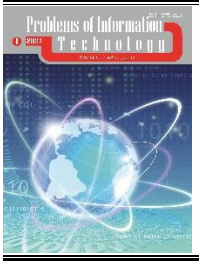

Available online at www.jpit.az

15 (1)
2024

Cybersecurity risks management of industrial control systems: A review

Ramiz H. Shikhaliyev

Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

ramiz@science.az

https://orcid.org/0000-0002-8594-6721

ARTICLE INFO

Keywords:

Industrial control systems
Cybersecurity risks
Cybersecurity risk management
Risk management standards
Risk management methods

ABSTRACT

Industrial control systems (ICS) form the basis of critical infrastructures, managing complex processes in various sectors of industry, energy, etc. With the increasing frequency and complexity of cyber threats, effective management of ICS cybersecurity risks is critical. This paper is devoted to the analysis of approaches used in the field of cybersecurity risk management of automated process control systems. The study examines the cybersecurity risks of ICS and the role of international standards in managing cybersecurity risks. The results of the analysis carried out in this paper can serve as information for the development of new reliable cybersecurity risk management systems for ICS.

1. Introduction

Industrial control systems (ICS) play a key role in ensuring efficiency and productivity in various industries. ICSs are used in process control in industries such as electric power, nuclear power, oil and gas, automotive and aerospace, etc. (Stouffer et al., 2011). In general, ICSs are part of critical infrastructures that are of great importance for any country, and a violation of their security can lead to catastrophic consequences in various areas of the country's security, including national security, economic security, public safety, etc. The increasing integration of ICS with information technology and a wider connected environment exposes them to several risks that can have serious consequences. At the same time, the ever-changing landscape of cyber threats threatens the integrity, availability, and confidentiality of ICS. The vulnerability of ICS to cyberattacks poses significant risks to the continuity of operation of critical systems, data integrity, and public safety of the country.

Today, new communication technologies and devices, such as smart devices, open wireless sensors, open software, etc., are being widely introduced into ICS. These technologies and devices have many vulnerabilities that are difficult to detect and/or fix, making them a target for cyberattacks. To mitigate the impact of these attacks, risk management techniques are used that assess the risks and consequences of cyberattacks and provide recommendations for minimizing the risks. The complexity and integration of today's ICS and network environments require robust cybersecurity risk management practices to protect against potential threats. Although the number of attacks on ICS is small compared to attacks on the Internet, the consequences can be catastrophic. Therefore, it is very important to ensure the

Received 20 September 2023, Received in revised form 21 November 2023, Accepted 06 December 2023
http://doi.org/10.25045/jpit.v15.i1.05

protection of ICSs from cyber threats (Leszczyna, 2021).

ICS cybersecurity risk management is the process of identifying, analyzing, assessing, and managing potential security threats that may arise in the ICS. Risk assessment is one of the most important parts of the risk management process since it is the basis for decisions on risk treatment (ISO 31000:2009). This includes risk identification, risk analysis, and risk assessment. Essentially, the sources of risks and possible consequences are first identified, then the likelihood and impact of the risks are analyzed, and finally, the risks are assessed. In general, risk assessment allows enterprises to find ICS vulnerabilities and subsequently take appropriate measures to optimize management, equipment, and control (Teixeira et al., 2015).

Many ICS cybersecurity risk management techniques can be applied to protect ICS from various types of cyberattacks and threats. One of the main approaches to managing cybersecurity risks of automated process control systems is the application of information security standards. These standards provide a set of requirements and recommendations for information security management and can be used to assess vulnerabilities and security risks in ICS. Another method of managing ICS cybersecurity risks is the use of access control mechanisms such as authentication, authorization, and auditing. These methods allow you to control access to the system and prevent unauthorized access. Methods for managing cybersecurity risks of ICS also include the use of perimeter protection measures, such as firewalls and IDS/IPS. The use of cryptographic methods for protecting data and communications, such as encryption, hashing, and electronic signature can also be classified as methods for managing the cybersecurity risks of ICS. These methods help protect sensitive data and prevent unauthorized access to information.

This paper analyzes the various cybersecurity risk management techniques used in ICS. The analysis will provide insight into these methods and may be useful in developing cybersecurity strategies for specific ICSs.

The rest of the paper is structured as follows: In Section 2 presents the cybersecurity risks of ICSs. Section 3 describes the cybersecurity risk management standards for ICSs and Section 4 presents the methods of cybersecurity risk management of ICSs. Section 5 presents the conclusions of work.

2. ICSs cybersecurity risks

ICS can be considered as a subset of cyber-physical systems in which threats can arise in both the cyber and physical spheres and endanger assets in both of them (Yampolskiy et al., 2013). The number and variety of cyber-attacks are growing, aimed not only at obtaining data from cyber-physical systems but also managing the production process itself (Alguliyev et al., 2021). For example, by exploiting a vulnerability in a programmable logic controller (PLC) to manipulate control parameters, a remote attacker could launch a cyber-physical attack. Typically, physical properties complicate the assessment of security risks because the process being controlled is closely related to the system under consideration. In addition to the physical consequences, other aspects are critical to assessing the safety risks of ICS. Because, attacks can be carried out at various levels of automation, such as the level of physical processes, the level of sensors, actuators, and controllers, the SCADA level, the operational level, and the enterprise level (IEC 62264-3:2016). To effectively deal with external and internal changes, it is necessary to achieve a predictable level of inspection and measurement quality (Alguliyev et al., 2018).

Cybersecurity risks for ICS can be caused by various threats and attacks that can lead to serious consequences, including disruption of production processes, leakage of confidential information, damage to equipment, etc. The most common cybersecurity risks of ICS include attacks on vulnerabilities in ICS; phishing attacks and fraud; distribution of malware; unauthorized access to networks and systems; leaks of confidential information, etc.

Vulnerabilities in ICS may appear as a result of vulnerabilities in software, protocols (Xu et al., 2017; Volkova et al., 2019), and system settings. In particular, the diversity of industrial control network protocols increases the vulnerability of ICS. Attackers to gain unauthorized access to the ICS can use these vulnerabilities. Subsequently, this may lead to changes in settings or unauthorized control of the equipment, which can lead to an emergency or disruption of the production process.

For phishing attacks and fraud, attackers can use social engineering techniques (Merz et al., 2019) such as phishing to trick employees into gaining access to ICS or confidential information.

When malware is distributed, attackers can use malware such as Trojan horses and spyware to gain access to ICS or steal sensitive information. Typically, malware uses hard-coded credentials built into the software. At the same time, malware can also be complemented by industrial espionage capabilities (Keliris et al., 2017).

Unauthorized access to networks and systems can occur as a result of weak authentication or insufficient access control in the ICS. The vulnerability is because passwords are encrypted using a weak encryption algorithm (Makrakis et al., 2021). Security mechanisms designed to prevent unauthorized access to ICS devices can be easily circumvented. This poses a major risk to the ICS network, even if alternative security measures are available. Potential countermeasures to mitigate the current situation could include more secure cryptography techniques such as digital signatures.

Leaked confidential information can become the target of threats and cyber attacks for ICS. An information breach could result in sensitive information being made available to third-party vendors, contractors, or partners who may not have the same level of security or privacy policies as the ICS. Data breaches can also lead to conflicts of interest, liability issues, or regulatory violations. The loss of confidential information can result in significant reputational damage and financial loss and can even cause long-term damage to the organization (Cheng & Liu, 2017). To prevent information leakage in the ICS, the information itself must be protected from unauthorized access. To do this, it is necessary to use a solution capable of applying one or another form of protection to the information, which is transmitted along with it, and ensures the protection of data regardless of its state or location.

To reduce the above-listed cybersecurity risks of ICS, it is necessary to apply appropriate risk management methods and follow information security recommendations. This includes the use of information security standards, access control mechanisms, perimeter protection measures, cryptographic methods for protecting data and communications, etc. For example, to ensure the security of information technology, NIST has developed appropriate guidance (NIST SP 800-53). NIST also established the ICS Security Project to investigate and apply the NIST SP800-53 recommendations for ICS (Katze et al., 2006). In addition, additional security controls include firewalls, intrusion detection systems, virtual private networks, antiviruses, etc. (Hentea, 2008; Aissa et al., 2010; Nicholson et al., 2012; Shikhaliyev, 2023).

3. ICSs cybersecurity risk management standards

For decades, there have been many risk management standards in the information technology (IT) field. For example, the ISO/IEC 27000 series of information security management standards addresses the security issues of IT systems (ISO/IEC 27000 family). In particular, the ISO/IEC 27001:2013 standard defines the requirements for information security management systems, including risk management (ISO/IEC 27001:2022). This standard provides methods for assessing risks and determining appropriate security controls. In addition, several standards have been developed, which include: ISO/IEC 27005:2018 (ISO/IEC 27005:2018); ISO Guide 73:2009 (ISO Guide 73:2009); ISO 31000:2009 (ISO 31000:2009); NIST Special Publication (SP) 800-30 (NIST Special Publication (SP) 800-30); NIST Special Publication (SP) 800-39 (NIST Special Publication (SP) 800-39). They describe how to measure or assess information security risk. However, these standards were not developed and are not intended for direct application in ICS.

Various standards govern the management of cybersecurity risks in automated ICS. These standards offer guidance and methods for managing the cybersecurity risks of ICS. The International Society of Automation (ISA) has produced many standards and technical reports under the ISA 99 standards committee, collectively known as ISA/IEC 62443. These are based on best practices in information security as well as industrial automation.

ISA/IEC 62443 is a series of standards that have been developed to ensure the safety of industrial automation systems, including ICS. It defines the requirements for the architecture, protection, and management of security systems and provides a flexible framework for addressing and mitigating current and future security vulnerabilities in ICS (Iaiani et al., 2021). The ISA/IEC 62443 series of standards establishes that quantifying safety levels and requirements is a long-term goal. This makes methods for quantifying cyber risks ultimately indispensable in the context of ICS (ISA/IEC 62443-1-1:2007, ISA/IEC 62443-3-3:2013). The new ISA/IEC 62443 Part 3-2 was released in February 2020 and aims to define a set of engineering controls that will guide an organization through the process of

assessing the risk of a specific process control system and identifying and applying security countermeasures (IEC 62443-3-2:2020).

NIST SP 800-82 Rev. 2 "Guide to Industrial Control Systems (ICS) Security" was developed by the US National Institute of Standards and Technology (NIST) (Stouffer et al., 2015). This document provides recommendations for ensuring the safety of ICS, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLCs), while addressing their safety concerns, unique requirements for performance, reliability, and safety. The document provides an overview of ICS and typical system topologies, identifies common threats and vulnerabilities of these systems, and presents recommended security measures to reduce the risks associated with them.

In the field of functional safety, there is the ISA/IEC 61511 standard "Functional Safety – Safety Instrumented Systems for the Process Industry Sector" (ISA/IEC 61511.1:2016). This standard defines the safety requirements for functional safety in industrial process control processes, including ICS.

The standards discussed above assume a qualitative approach to assessing cybersecurity risks. However, there is a growing trend towards the use of quantitative methods. The reason for this is that qualitative approaches to security risk assessment have been subject to considerable criticism (Freund & Jones, 2014; Hubbard & Seiersen, 2023) due to their inherent uncertainty. Gaining a quantitative understanding of risks can aid the decision-making process and is therefore useful for improving information security.

Existing review papers (Cherdantseva et al., 2016; Cook et al., 2016) indicate that quantifying the safety risks of ICS is an active area of research in the scientific community.

4. ICSs cybersecurity risk management methods

Attacks on ICS are expanding due to the convergence of information technology (IT) and operational technology (OT) systems. Therefore, IT vulnerabilities affect OT security (David, 2017) and two types of risk analysis must be taken into account when considering the cybersecurity of ICS (Flaus, 2019). The first type of analysis is an IT system risk analysis, which will be carried out using analysis methods developed for IT systems. The second type of analysis is the analysis of safety risks associated with occupational safety, which will use, for example, a preliminary hazard analysis (PHA) or a hazard and operability study (HAZOP). These two types of analysis are not independent, since the consequences of an attack on ICS IT can trigger a dangerous scenario in the OT.

Methods for managing cybersecurity risks of ICS include such stages as identifying risks; risk assessment; development of a risk management plan; implementation of risk management measures; and monitoring and auditing of vulnerabilities and threats. In addition, ICS cybersecurity risk management practices may include training employees on security rules and risk management, as well as creating a security culture within the organization.

To identify risks, it is necessary to analyze the vulnerabilities of the ICS and identify potential threats that could lead to a violation of the cybersecurity of the ICS. In addition, it is necessary to consider the consequences of loss of OT control.

At the risk assessment stage, the likelihood of a threat and its consequences is assessed, and the critical components of the ICS are identified from a safety point of view. The most common way to analyze risks in ICS is to use the concept of probability. However, this probability changes from time to time as technology develops and attack strategies change (Cook et al., 2016). Based on the results of the risk assessment, a risk management plan is developed, which includes measures to reduce the likelihood of a threat occurring and reduce its consequences.

Risk management measures may include technical and organizational measures such as strengthening perimeter security, access controls, and security monitoring and auditing. ICS cybersecurity systems must be constantly monitored to ensure their effectiveness, as well as the adaptation of security measures to new threats. Monitoring ICS networks will help maintain visibility of network activity and identify potential security gaps. Regular monitoring and audit of ICS will also help analyze the source of the attack.

When identifying vulnerabilities and threats, the first step is to determine which ICS components may be susceptible to attack and what vulnerabilities exist. This can be done through ICS analysis, penetration testing, and other methods.

Overall, successfully managing ICS cybersecurity risks requires a comprehensive approach that includes technical and organizational security measures, training, and monitoring.

Traditional risk assessment models are widely used frameworks for assessing and managing risks in various fields. These models provide structured methodologies for identifying, analyzing, and mitigating risks to achieve organizational goals.

Failure mode and effect analysis (FMEA) (https://www.ifm.eng.cam.ac.uk/research/dmg/tools-and-techniques/fmea-failure-modes-and-effects-analysis/) is a systematic method for evaluating processes to determine where and how they are likely to fail and to evaluate the relative impact of different failures. Commonly used in manufacturing, healthcare, and engineering to prioritize failure modes and guide preventative actions.

Fault tree analysis (FTA) (https://fiixsoftware.com/glossary/fault-tree-analysis/) is a deductive fault analysis technique that models the causes of system failures using tree diagrams. Often used in the nuclear, aerospace, and chemical industries to analyze complex systems and identify root causes of failures.

A Hazard and operability study (HAZOP) (Haugen & Rausand, 2020) is a structured and systematic study of a complex planned or existing process or operation to identify and evaluate problems. Widely used in process industries including chemical, petrochemical, and pharmaceutical industries.

Bowtie risk assessment (Hocking & Sproston, 2019) visualizes the relationship between a high-level hazardous event, its causes (threats), and consequences (impacts). Used in aviation, healthcare, and high-risk industries to effectively communicate and manage risk information.

Quantitative risk assessment (QRA) involves numerical risk analysis using techniques such as probabilistic risk assessment (PRA) and fault tree analysis to quantify the likelihood and consequences of risks (Eckhart et al., 2019). Common in industries that place a high emphasis on numerical risk values, such as finance, insurance, and some aspects of engineering.

There is a wide range of cybersecurity risk management techniques currently in use in the ICS field, but most are adaptations of techniques that were used to assess enterprise risk and are therefore tailored to the specific threat landscape and characteristics of a business enterprise. Moreover, most approaches do not take into account the dependencies between components and between parts of different ICS.

Traditional approaches to cybersecurity risk management ICS are initially focused on IT infrastructure, making such approaches inapplicable in a complex ICS environment (Georgios et al., 2012). However, methods have been proposed that follow a holistic point of view in the process of managing ICS cybersecurity risks. In particular, in (Digioia et al., 2012), the authors use a mixed holistic-reductionist approach to assess the impact of cyberattacks. The proposed conceptual methodology models heterogeneous systems and evaluates the consequences of an attack by identifying different agents and their dependencies.

With the increase in computing power, it is becoming increasingly easier to implement solutions based on artificial intelligence for ICS. Recent years have seen a surge in research into the use of AI. Many researchers use machine learning models such as decision trees, SVM, k-NN, random forest, AdaBoost, and other deep learning models to detect any anomalies in the system (Al-Abassi et al., 2020; Alguliyev et al., 2022; Sukhostat, 2022; Sukhostat, 2021).

5. Conclusion

The analysis carried out in this paper provides information on approaches to managing the cybersecurity risks of ICSs. The analysis shows a variety of methods for managing the cybersecurity risks and importance of eliminating vulnerabilities of ICSs.

Robust detection mechanisms that can identify both known and unknown threats must be put in place to ensure timely response and containment. Cybersecurity strategies must be tailored to meet stringent operational requirements without compromising the security posture. In addition, it is necessary to comply with international standards when managing cybersecurity risks of ICS. Organizations must align their risk management systems to established standards to ensure a comprehensive and structured approach to cybersecurity.

Traditional risk assessment models have difficulty adapting to the real-time and operational constraints of ICS, so it is necessary to harness the potential of new technologies, including artificial intelligence and machine learning.

The results of the analysis lay the foundation for future research and practical implementation aimed at strengthening the cybersecurity of ICS. Future research should examine how new intelligent technologies can be integrated into existing structures to enhance protective mechanisms.

Acknowledgments

This work was supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

References

Aissa, A. B., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2010). Quantifying security threats and their potential impacts: a case study. Innovations in Systems and Software Engineering, 6, 269-281. https://doi.org/10.1007/s11334-010-0123-2

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. IEEE Access, 8, 83965-83973. https://doi.org/10.1109/ACCESS.2020.2992249

Alguliyev, R., Sukhostat, L., & Mammadov, A (2022). Anomaly detection in cyber-physical systems based on BiGRU-VAE. 2022 IEEE 16th International Conference on Application of Information and Communication Technologies (AICT), Washington, USA, October 2022 (pp. 1-5). https://doi.org/10.1109/AICT55583.2022.10013581

Alguliyev, R. M., Imamverdiyev, Y. N., & Sukhostat, L. V. (2021). Hybrid DeepGCL model for cyber-attacks detection on cyber-physical systems. Neural Computing and Applications, 33(16), 10211-10226. https://doi.org/10.1007/s00521-021-05785-2

Alguliyev, R. M., Imamverdiyev, Y. N., & Sukhostat, L. V. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100, 212-223. https://doi.org/10.1016/j.compind.2018.04.017

Cheng, L., & Liu, F. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211. https://doi.org/10.1002/widm.1211

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

Cook, A., Smith, R., Maglaras, L., & Janicke, H. (2016). Measuring the risk of cyber-attack in industrial control systems. 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR'16), Belfast, UK, August 2016 (pp. 1-11). https://doi.org/10.14236/ewic/ICS2016.12

David, L. (2017). Cybersecurity: Industrial Control Systems and the U.S. Electric Grid. https://mse238blog.stanford.edu/2017/07/dllove/cybersecurity-industrial-control-systems-and-the-u-s-electric-grid/.

Digioia, G., Foglietta, C., Panzieri, S., & Falleni, A. (2012). Mixed holistic reductionistic approach for impact assessment of cyber attacks. 2012 European Intelligence and Security Informatics Conference (EISIC), Odense, Denmark, August 2012 (pp. 123-130). https://doi.org/10.1109/EISIC.2012.30

Eckhart, M., Brenner, B., Ekelhart, A., & Weipp, E. (2019). Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges. Journal of Internet Services and Information Security (JISIS), 9(3), 52-73. https://doi.org/10.22667/JISIS.2019.08.31.052

Enterprise-control system integration – part 3: Activity models of manufacturing operations management. IEC 62264-3:2016.

Fault tree analysis (FTA). https://fiixsoftware.com/glossary/fault-tree-analysis/

Flaus, J.-M. (2019). Cybersecurity of industrial systems. London: ISTE Ltd.; Hoboken, NJ: John Wiley & Sons, Inc. https://doi.org/10.1002/9781119644538

FMEA (Failure Modes and Effects Analysis). https://www.ifm.eng.cam.ac.uk/research/dmg/tools-and-techniques/fmea-failure-modes-and-effects-analysis/

Freund, J. & Jones, J. (2014). Measuring and managing information risk: A FAIR approach. Newton, MA: Butterworth-Heinemann.

Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements. ISA/IEC 61511.1:2016.

Georgios, G., Roberto, F., & Muriel, S. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, EUR - Scientific and Technical Research Reports.

Guide for Applying the Risk Management Framework. NIST Special Publication (SP) 800-39.

Guide for Conducting Risk Assessments. NIST Special Publication (SP) 800-30.

Haugen, S. & Rausand, M. (2020). Risk Assessment: Theory, Methods, and Applications. Hoboken, NJ: John Wiley & Sons, Inc. https://doi.org/10.1002/9781119377351

Hentea, M. (2008). Improving security for SCADA control systems. Interdisciplinary Journal of Information, Knowledge, and Management, 3, 73-86. https://doi.org/10.28945/3185

Hocking, B. & Sproston, C. (2019). Bowtie risk assessment methodology in practice. https://shoalgroup.com/wp-content/uploads/2019/04/Hocking-and-Sproston-Bowtie-risk-assessment-methodology-in-practice-AMPEAK2019.pdf.

Hubbard, D. W. & Seiersen, R. (2023). How to measure anything in cybersecurity risk. Hoboken, NJ: John Wiley & Sons Inc.

Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2021). Analysis of cybersecurity-related incidents in the process industry. Reliability Engineering & System Safety, 209, 107485. https://doi.org/10.1016/j.ress.2021.107485

Information security management. ISO/IEC 27000 family.

Information security, cybersecurity and privacy protection - Information security management systems. Requirements. ISO/IEC 27001:2022.

Information technology – Security techniques – Information security risk management. ISO/IEC 27005:2018.

Katze, S., Stouffer, K., Abrams, M., Norton, D., & Weiss, J. (2006). Applying NIST SP 800-53 to Industrial Control Systems, NIST 2006.

Keliris, A., Konstantinou, C., & Maniatakos, M. (2017). GE multilin SR protective relays passcode vulnerability, Black Hat USA.

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. Computers & Security, 108, 102376. https://doi.org/10.1016/j.cose.2021.102376

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and attacks against industrial control systems and critical infrastructures. arXiv preprint arXiv: 2109.03945.

Merz, T. R., Fallon, C., & Scalco, A. (2019). A context-centred research approach to phishing and operational technology in industrial control systems. Journal of Information Warfare, 18(4), 24-36.

National Institute of Standards and Technology (NIST), SP 800-53, Guide to Industrial Control Systems (ICS) Security.

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare, Computers & Security, 31(4), 418-436.

https://doi.org/10.1016/j.cose.2012.02.009
Risk management – Principles and guidelines. ISO 31000:2009
Risk management – Vocabulary. ISO Guide 73:2009.
Security for Industrial Automation and Control Systems - Part 1-1: Terminology, Concepts, and Models. ISA/IEC 62443-1-1:2007.
Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. IEC 62443-3-2:2020.
Security for industrial automation and control systems, Part 3-3: System security requirements and security levels. ISA/IEC 62443-3-3:2013
Shikhaliyev, R. H. (2023). Using machine learning methods for industrial control systems intrusion detection. Problems of Information Technology, 14(2), 37-48. http://dx.doi.org/10.25045/jpit.v14.i2.05
Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST Special Publication. https://doi.org/10.6028/NIST.SP.800-82r3
Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2. http://dx.doi.org/10.6028/NIST.SP.800-82r2.
Sukhostat, L. (2021). An intelligent model based on deep transfer learning for detecting anomalies in cyber-physical systems, Radio Electronics, Computer Science, Control, 3, 124-132. https://doi.org/10.15588/1607-3274-2021-3-11
Sukhostat, L. (2022). Anomaly detection in industrial control system based on the hierarchical hidden Markov model. In O. Popov & L. Sukhostat (Eds.), Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems (pp. 48-55). IOS Press. http://dx.doi.org/10.3233/NICSP220033
Teixeira, A., Sou, K. C., Sandberg, H., & Johansson, K. H. (2015). Secure control systems: A quantitative risk management approach, IEEE Control Systems Magazine, 35(1), 24–45. http://dx.doi.org/10.1109/MCS.2014.2364709
Volkova, A., Niedermeier, M., Basmadjian, R., & Meer, H. (2019). Security challenges in control network protocols: A survey, IEEE Communications Surveys & Tutorials, 21(1), 619-639. https://doi.org/10.1109/COMST.2018.2872114
Xu, Y., Yang, Y., Li, T., Ju, J., & Wang, Q. (2017). Review on cyber vulnerabilities of communication protocols in industrial control systems, IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, November 2017 (pp. 1-6). https://doi.org/10.1109/EI2.2017.8245509
Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2013). Taxonomy for description of cross-domain attacks on CPS. 2nd ACM International Conference on High Confidence Networked Systems (HiCoNS'13), Philadelphia, Pennsylvania, USA, April 2013, pp. 135–142. https://doi.org/10.1145/2461446.2461465