Proceedings of the Estonian Academy of Sciences
2025, **74**, 2, 143–148

https://doi.org/10.3176/proc.2025.2.11

www.eap.ee/proceedings
Estonian Academy Publishers

CYBERSECURITY IN AUTOMATION

RESEARCH ARTICLE

Received 3 February 2025
Accepted 4 March 2025
Available online 21 April 2025

Keywords:
cybersecurity, MQTT, Modbus, OPC UA, PROFIBUS, IEC 62443

Corresponding author:
Sergei Ponomar
sergei.ponomar@taltech.ee

Citation:
Ponomar, S. and Sarkans, M. 2025. Overview of the development of cybersecurity in data transmission protocols used in industry. *Proceedings of the Estonian Academy of Sciences*, **74**(2), 143–148. https://doi.org/10.3176/proc.2025.2.11

Overview of the development of cybersecurity in data transmission protocols used in industry

Sergei Ponomar[a] and Martinš Sarkans[b]

[a] School of Engineering, Tallinn University of Technology, Virumaa College, Järveküla tee 75, 30322 Kohtla-Järve, Estonia

[b] School of Engineering, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

ABSTRACT

The fourth industrial revolution (Industry 4.0) has enabled the digitalization of almost all technological processes. While industrial robots and systems communicate with each other mainly through data transfer protocols, humans at the same time primarily play the role of process observers. Initially, the development of data transfer protocols focused primarily on speed and data quality, with minimal attention paid to cybersecurity. As more and more industrial devices share data with each other, it has become essential to ensure cybersecurity during communication. This article briefly discusses the security of data exchange protocols from this perspective. In recent decades, cyberattacks against industrial facilities have been increasing, prompting the incorporation of various security methods into communication protocols. This article provides a review of studies conducted in recent years on how cybersecurity has evolved in industrial data transmission protocols and its impact on technological processes. Additionally, the article explores how cybersecurity will influence the transition to the fifth industrial revolution (Industry 5.0). The outcome of this research will highlight how the addition of protective mechanisms to the data transmission protocols affects their functionality and quality. It will also examine the challenges that arise during the integration of security features into the data transmission protocols.

1. Introduction

With the development of information and communication technologies (ICT), it has become possible to improve automation levels in industrial enterprises. Currently, many manufacturing plants are implementing ICT to achieve full automation. Also, to reach the level of Industry 4.0, a wide range of smart devices are deployed to gather data and oversee the entire manufacturing processes. Initially, enterprise architecture models were used to assess the alignment between business processes and IT infrastructure. However, these are now increasingly utilized for cybersecurity analysis within the organizations [1]. During the implementation of smart devices, it is necessary to establish a data transmission infrastructure. Wired and wireless transmission technologies for data exchange can be used. One of the key challenges during data transmission is to ensure the transmission speed, integrity, and reliability of the information. When analyzing the security of industrial control systems (ICS), one of the key criteria is ensuring a secure transmission of data between devices [2].

Various industrial data transfer protocols, such as MQTT, Modbus, OPC UA, S7CommPlus, and PROFIBUS/PROFINET, have been developed to ensure reliable data transmission. While these protocols were designed for fast and accurate data exchange between devices, they initially lacked built-in cybersecurity measures. There are many additional protocols available; however, this article focuses only on a few of them and further examines the development of cybersecurity in industrial protocols. The article is divided into several sections: the first section describes the areas in which data transmission protocols are used, the second provides an overview of standards for defining and describing the protocols, and the third includes a comparison of some protocols, focusing on how cybersecurity is implemented in each of them.

2. Modern industrial systems

This chapter discusses modern production systems and their architecture through layers of communication. The automation pyramid allows to describe these systems through five levels [3]:

1. Field level: various measuring instruments and actuators are located at this level.
2. Control level: process control occurs and data is transmitted between various devices, such as robots and programmable logic controllers (PLC).
3. Supervisory level: supervisory control and data acquisition (SCADA) systems and human-machine interfaces (HMI) are located at this level.
4. Planning level: the entire process from components to finished products is planned, using manufacturing execution systems (MES).
5. Management level: a similar task is performed as at the planning level but within the framework of entire corporations using enterprise resource planning (ERP) systems.

In his article, Matthew Gordon-Box [3] examined the levels of industrial automation systems according to the ANSI/ISA-95 standard, which is used for developing interfaces between enterprises and control systems. He also presented the automation pyramid that shows the structure of industrial production in the context of Industry 4.0.

One of the most important contents of the Industry 4.0 concept is data. Data needs to not only be collected and stored but also analyzed to improve the functionality of the automation system. To properly understand and manage the production processes, data must be transmitted without delays and errors. Industrial data transmission protocols are used to transfer data between devices, such as PLCs, robots, sensors, and actuators. In this article, the data transmission protocols at the control and supervisory levels are analyzed. As shown in Fig. 1, data is transmitted between devices by using the data exchange protocol (DEP) in multiple directions, for example, between a PLC and a robot or between a PLC and an HMI, and so on.

To visualize and monitor parameters in a web browser, it is necessary to create HTML pages, with HTTP/HTTPS as the primary protocol for data exchange between the browser and the server. The server, in turn, processes the information received from the client and converts it for transmission to a controller or a robot using specialized industrial protocols, such as Modbus and PROFINET.

For example, in his thesis, Tunkkari [4] discusses the implementation of the Modbus protocol security using an OPC UA server. The publication also provides a detailed overview of the structures of the Modbus and OPC UA protocols, which can significantly simplify the development of web applications for configuring communication with industrial systems. Profanter et al. [5] compare the performance of Industry 4.0 protocols: OPC UA, ROS, DDS, and MQTT. They evaluate the protocols' latency, throughput, and reliability in industrial networks. The study highlights the strengths and weaknesses of each protocol in the context of industrial applications.

3. Overview of standards for industrial data communication protocols

As there are many different standards on the structure and security of industrial data communication protocols, the most relevant ones in this context are outlined here. The IEC 61784 standard outlines the main criteria for data transmission protocols between devices. The main criteria of this standard include fast and accurate data transmission between devices, compatibility between various devices, real-time support and scalability, naming a few.

As the control systems are getting more advanced and the complexity of process control structures increases, cyber-

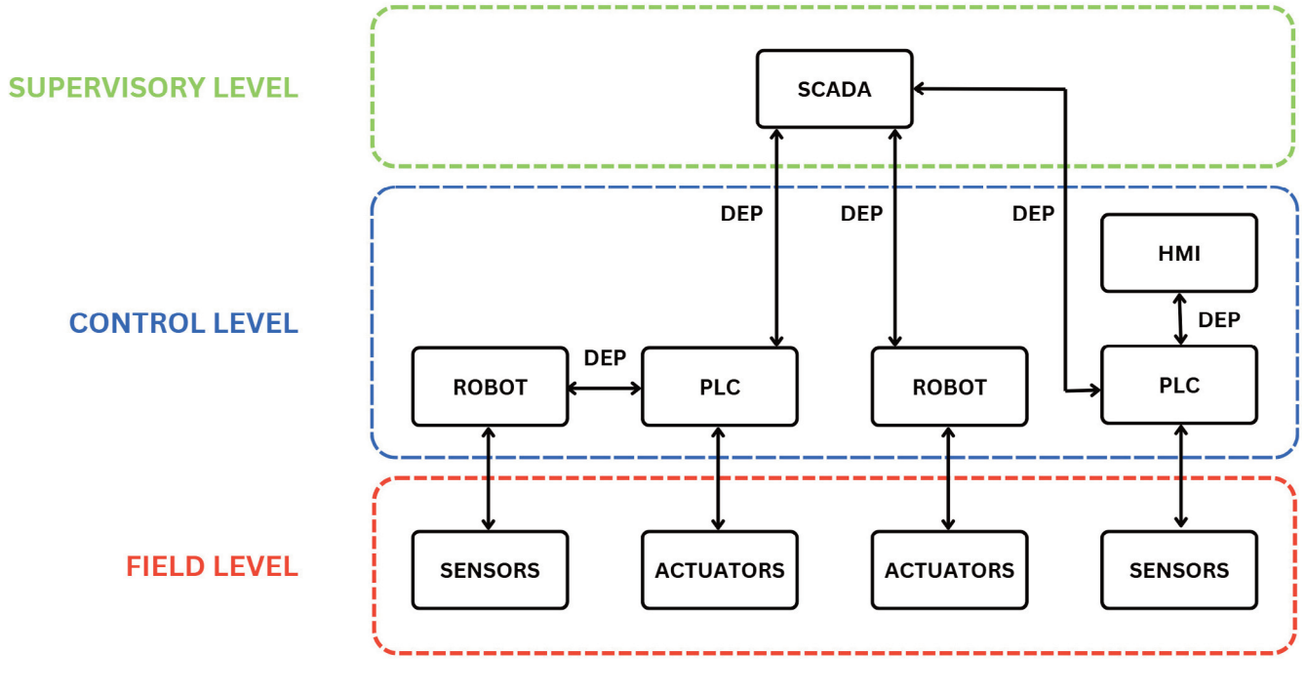

Fig. 1. Example of three levels of data transfer in the automation pyramid.

security becomes a critical challenge. Before the implementation of ICT in industrial enterprises, there were relatively few cyberattacks. This was mainly because industrial enterprises operated mostly in local networks, and access to their facilities was physically restricted. In their article, Hemsley et al. [6] describe the history of cyberattacks on enterprises. The history shows that the number of cyberattacks continues to increase every year. For example, before 2009, three cyberattacks on industrial enterprises were documented: the Maroochy Water Services Breach, the Night Dragon malware, and the Stuxnet malware. Each of these posed a serious threat to industrial systems and could have led to large-scale human and environmental disasters.

To prevent cybersecurity issues and establish criteria for creating a secure industrial environment, the IEC 62443 standard was published. The standard IEC 62443 defines security requirements for automated systems, including physical protection of the automation devices, control systems, data transmission networks, and other components [7]. This standard offers guidelines for selecting suitable data transmission protocols and includes recommendations for encryption, access control, network scanning, and protection against cyberattacks.

In industrial automation and IoT (Internet of Things), various protocols are used to transfer data between devices. Each of them has its own features, advantages, and disadvantages. In this article, we consider the main protocols and their applications: MQTT, Modbus, OPC UA, S7CommPlus, and PROFIBUS/PROFINET.

MQTT is a lightweight messaging protocol designed for devices with limited resources and networks with low bandwidth. It operates on the publish-subscribe model and uses a broker to transmit messages between clients. It also supports cybersecurity at the level of TLS/SSL encryption and authentication. One of its drawbacks is the amount of data transmitted. One of the key parameters of this protocol is the quality of service (QoS), which is divided into three levels: QoS 0 – message is delivered once without acknowledgment, QoS 1 – message is delivered at least once with mandatory acknowledgment, QoS 2 – message is delivered exactly once using a two-step handshake, no duplicates [8].

The Modbus protocol was developed in 1979 to facilitate communication between industrial devices. It uses a client-server model and supports several physical layers (RS-232, RS-485, TCP/IP). There are three different data transmission formats in this protocol: Modbus RTU, Modbus ASCII, and Modbus TCP/IP. Since the protocol was primarily designed for data exchange between automation devices, it is now supported by many companies and has low resource requirements. A drawback is that cybersecurity was not implemented during the initial development of the protocol [9].

The OPC UA protocol is designed to ensure secure and reliable data transmission while supporting a semantic data model. The protocol includes built-in support for encryption and authentication. Additionally, this protocol is compatible with various operating systems [10].

S7CommPlus is a communication protocol used in Siemens S7-1200 and S7-1500 series PLCs. It is an improved version of the S7Comm protocol, which was used in earlier models such as S7-300 and S7-400. Operating over TCP/IP, S7CommPlus enables integration with industrial Ethernet networks and SCADA systems [11].

The PROFIBUS (Process Field Bus) protocol was developed by Siemens AG for its SIMATIC controllers. It uses a serial bus (RS-485) or optical cable and supports data transfer speeds of up to 12 Mbps. With the advancement of the internet and technologies, the PROFINET protocol was created, which is based on the Ethernet (IEEE 802.3) standard. This allows for the use of standard network technologies, and the data transfer speed reaches 1 Gbps [12].

4. Analysis of the industrial data communication protocols

In this section, a selection of data transfer protocols has been analyzed to highlight their cybersecurity capabilities. For this purpose, the following key security criteria were defined:

1. Data encryption
2. Authentication
3. Access control
4. Data integrity
5. Protection against attacks

An additional criterion was identified as compliance with the IEC standards. Some protocols, such as MQTT and S7CommPlus, do not have a separate IEC standard. For example, the MQTT protocol does not have its own specific standard, only the implementation documentation exists. In the case of the S7CommPlus protocol, the documentation is provided by Siemens.

The early versions of protocols generally did not include security features, as these were primarily designed for closed systems. The only protocol where security was considered from the outset was the OPC UA protocol.

Since most of the industrial data transmission protocols operate in the TCP/IP model, encryption, authentication, and data integrity in many protocols are implemented using the transport layer security (TLS) protocol.

Before the introduction of the TLS layer in the Modbus protocol, authentication and authorization functions were not fully implemented. The addition of TLS not only enabled the use of these functions but also provided additional data protection through SHA-256 encryption [13]. In 2015, the SHA-3 encryption standard was adopted, including the functions such as SHA-3-224, SHA-3-256, SHA-3-384, SHA-3-512, SHAKE128, and SHAKE256. Vandervelden et al. [14] analyzed the performance of various encryption methods on resource-constrained devices and compared their efficiency with SHA-2 algorithms. The results showed that SHA-3 consumes more computational resources compared to SHA-2. There is also the MBAPS (Modbus application protocol security) specification, which precisely outlines the security measures that must be implemented at each level. It also specifies which methods can be used when implementing the protocol and which ones are not allowed.

In the MQTT v5.0 protocol specification, data access is also secured through the TLS layer. However, data trans-

Table 1. Comparison of characteristics of different data transmission protocols

	Modbus/TCP Secure	OPC UA	MQTT	PROFINET	S7CommPlus
Data encryption	TLS	TLS	TLS	TLS	Depends on version
Authentication	TLS	TLS	TLS	TLS	TLS
Access control	TLS	TLS	TLS	VLAN	Depends on version
Data integrity	TLS	TLS	TLS	TLS	TLS
Protection against attacks	TLS	TLS	TLS	TLS	TLS
Standards	IEC 60870-5	IEC 62541	Only specification	IEC 61784	Siemens standard
Benefits	Industrial protocol, wide industry support	Industrial protocol, wide industry support, high security	IoT protocol, works with devices with limited resources	Industrial protocol, wide industry support	Industrial protocol
Shortages	Cannot send a lot of data, limited security features	High resource requirements for use	Difficult to use in real-time industrial control, limited built-in security	Requires specialized hardware	Works with Siemens devices, documentation is not public

mission without cryptographic protection and encryption is allowed, although it should be avoided. Alternative protection methods, such as virtual private networks (VPN), should be used [15].

In some cases, such as in the S7CommPlus protocol, this implementation depends on the version of the protocol itself [16]. When transmitting data between Siemens devices, it is recommended to choose the latest firmware version, as it includes all modern cybersecurity methods. However, there is no option to select the version of the data transmission protocol, and you can use older versions of firmware when programming PLCs.

Access control is typically implemented by using the role-based access control (RBAC) and X.509 certificates. These mechanisms are integrated into the TLS layer, although their implementation may vary depending on the version. For example, in the MQTT and S7CommPlus protocols, there is an option to transmit the username and password in plaintext, which is not a secure method for data transmission [17].

Table 1 above shows the differences between industrial data transmission protocols, considering the five key criteria defined previously. Additionally, the connection with the standards is shown. As can be seen in Table 1, a conclusion can be drawn that most of the industrial data transmission protocols use similar solutions implemented at the TLS level, which are compliant with the IEC 62443-3-3 security standard. Future research for our needs aims to identify which protocols provide the most effective level of protection. Although standards and specifications define the functions that protocols should implement, it is important to seek optimal implementations that balance speed, security, and load efficiency.

4.1. Cybersecurity problems

As cybersecurity methods are added into data transmission protocols, the size of the packets to be transmitted increases. Without the protection layer, a packet can contain only the destination address and the data itself. If the data in the packet needs to be verified, a message authentication code (MAC) is added to the packet. Authentication requires including information for verifying authenticity, which can be encrypted, thus increasing the packet size and adding processing demands. Access control lists (ACL) also contribute additional data to the packet. Encrypting the data itself increases the packet size due to additional metadata, such as the initialization vector or padding. Each element that provides data protection affects the packet size and complicates its processing. The challenges that need to be considered are reduced packet processing speed, increased time for encryption and decryption, higher network bandwidth usage, increased latency, and others.

One of the main challenges that needs to be analyzed and solved when implementing cybersecurity measures is energy efficiency. In automation environments with IoT devices, processing secured packets can become overly complex and resource-intensive for low-performance devices.

As there is a need for the development of a web-based SCADA system for our research purposes, the key criterion is the accuracy of the displayed data and its alignment with the actual situation. It is crucial to ensure that no data is lost or distorted during transmission between devices and software. Additionally, the speed of data transmission between systems and devices must be considered, as it directly affects operational efficiency. In Table 2, these challenges are grouped together based on the cybersecurity method used.

Since data must be protected by using various cybersecurity methods, it is necessary to analyze how well each system component can handle security measures and how security is implemented in the devices. In real-time systems, where data is transmitted continuously, we need to ensure that all data is moving without any errors or delays. Also, when interacting with a robot, it is important to ensure the safety of both the human operator and the equipment, so that data from the controllers, sensors, and control systems can respond effectively to any potential interference. Additionally, it is necessary to assess how well the implementation of web-based SCADA is suited for real-time operation and to evaluate the impact of adding cybersecurity methods on the speed of data transmission and processing.

Table 2. Cybersecurity methods and data transmission challenges

Cybersecurity method	Impact on packet size	Challenges in data transmission	Considerations for web-based SCADA
No protection layer	Smallest packet (only destination address and data)	No authentication or encryption, vulnerable to attacks	Data can be easily intercepted or modified
MAC	Increases packet size due to authentication data	Additional processing for MAC generation and verification	Ensures data integrity but may slow down processing on devices with limited resources
Authentication (encrypted verification data)	Adds extra data for authentication and encryption	Increased processing demand may introduce delays	Ensures data integrity but may slow down processing on devices with limited resources
ACL	Adds additional metadata for access control	More complex packet processing may reduce speed	Helps restrict access to SCADA systems, improving security
Data encryption	Increases packet size (includes metadata such as initialization vectors, padding)	Requires additional computational resources, increases latency	Protects against data breaches but affects real-time performance
Real-time constraints	All security measures add processing overhead	May reduce transmission speed and increase latency	Critical for SCADA systems to ensure real-time data without errors or delays
Energy efficiency concerns	More security layers mean higher energy consumption	IoT devices with low power may struggle with security processing	Must balance security with power efficiency for continuous operation
SCADA system accuracy	Data must be protected without loss or distortion	Security layers can introduce errors or slow updates	Ensures displayed data aligns with actual system status
Human and equipment safety	Data from sensors and controllers must be reliable	Security delays can impact response times	Essential for robotic interaction and industrial safety
Web-based SCADA feasibility	Cybersecurity adds complexity to implementation	Security features must not compromise real-time operation	Needs careful evaluation of security vs. system performance trade-offs

5. Conclusions

One of the criteria for secure production is the security of data transmission between devices. In this article, five main data protocols and their security implementations were analyzed. The key conclusion is the continuous development of data transmission protocols, accompanied by the integration of advanced cybersecurity methods, such as authorization, authentication, and encryption. To enhance information security, a significant number of the examined protocols employ transport layer security mechanisms, particularly the TLS protocol. By choosing the appropriate industrial data transmission protocol and its implementation, before deploying it in production, it is necessary to monitor how often the protocol is updated and what methods are used to protect the data. In larger industrial enterprises, outdated device firmware versions are often used, which may already contain vulnerabilities.

In future research, it is necessary to investigate which protocol implementations are suitable for creating web-based SCADA systems. Additionally, it is important to analyze the limitations of each protocol and determine which one is best suited for Industry 5.0 purposes.

Data availability statement

All data are available in the article.

Acknowledgments

This article was supported by the project "Increasing the knowledge intensity of Ida-Viru entrepreneurship", co-funded by the European Union (IKRA-T5.0 – Development of process-adaptable robot platforms in the Industry 5.0 concept (incl. digital twin)), and by the project "Increasing the volume of continuing education in Ida-Viru and developing and launching new level education curricula in vocational and higher education" (No. 2021-2027.6.01.23-0095). The publication costs of this article were partially covered by the Estonian Academy of Sciences.

References

1. Jiang, Y., Jeusfeld, M. A., Mosaad, M. and Oo, N. Enterprise architecture modeling for cybersecurity analysis in critical infrastructures – a systematic literature review. *Int. J Crit. Infrastruct. Prot.*, 2024, **46**, 100700. https://doi.org/10.1016/J.IJCIP.2024.100700
2. Asghar, M. R., Hu, Q. and Zeadally, S. Cybersecurity in industrial control systems: issues, technologies, and challenges. *Comput. Networks*, 2019, **165**, 106946. https://doi.org/10.1016/j.comnet.2019.106946
3. Gordon-Box, M. The 5 layers of the automation pyramid and manufacturing operations management. https://www.syspro.com/blog/erp-for-manufacturing/the-5-layers-of-the-automation-pyramid-and-manufacturing-operations-management/ (accessed 2025-01-03).
4. Tunkkari, J. *Mapping Modbus to OPC Unified Architecture*. Master's thesis. Aalto University, Espoo, 2018.
5. Profanter, S., Tekat, A., Dorofeev, K., Rickert, M. and Knoll, A. OPC UA versus ROS, DDS, and MQTT: performance evaluation of Industry 4.0 protocols. In *2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, VIC, Australia, 13–15 February 2019*. IEEE, 2019, 955–962. https://doi.org/10.1109/ICIT.2019.8755050
6. Hemsley, K. and Fisher, R. A history of cyber incidents and threats involving industrial control systems. In *Critical Infrastructure Protection XII* (Staggs, J. and Shenoi, S., eds). *IFIP Advances in Information and Communication Technology*, **542**. Springer, Cham, 2018. https://doi.org/10.1007/978-3-030-04537-1_12
7. Leander, B., Čaušević, A. and Hansson, H. Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26–29 August 2019.* ACM, New York, USA, 2019. https://doi.org/10.1145/3339252.3341481

8. Hillar, G. C. *MQTT Essentials - A Lightweight IoT Protocol*. Packt Publishing, Birmingham, 2017.
9. Buchanan, W. *Computer Busses*. Butterworth-Heinemann, 2000. https://doi.org/10.1201/9781420041682
10. Lehnhoff, S., Rohjans, S., Uslar, M. and Mahnke, W. OPC unified architecture: a service-oriented architecture for smart grids. In *2012 First International Workshop on Software Engineering Challenges for the Smart Grid (SE-SmartGrids), Zurich, Switzerland, 3 June 2012*. IEEE, 2012, 1–7. https://doi.org/10.1109/SE4SG.2012.6225723
11. Alsabbagh, W. and Langendörfer, P. You are what you attack: breaking the cryptographically protected S7 protocol. In *2023 IEEE 19th International Conference on Factory Communication Systems (WFCS), Pavia, Italy, 26–28 April 2023*. IEEE, 2023, 1–8. https://doi.org/10.1109/WFCS57264.2023.10144251
12. Kjellsson, J., Vallestad, A. E., Steigmann, R. and Dzung, D. Integration of a wireless I/O interface for PROFIBUS and PROFINET for factory automation. *IEEE Trans. Ind. Electron.*, 2009, **56**(10), 4279–4287. https://doi.org/10.1109/TIE.2009.2017098
13. Martins, T. and Oliveira, S. V. G. Enhanced Modbus/TCP security protocol: authentication and authorization functions supported. *Sensors*, 2022, **22**(20), 8024. https://doi.org/10.3390/s22208024
14. Vandervelden, T., De Smet, R., Steenhaut, K. and Braeken, A. SHA3 and Keccak variants computation speeds on constrained devices. *Future Gener. Comput. Syst.*, 2022, **128**, 28–35. https://doi.org/10.1016/j.future.2021.09.042
15. MQTT Version 5.0. https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (accessed 2025-01-03).
16. Hui, H., McLaughlin, K. and Sezer, S. Vulnerability analysis of S7 PLCs: manipulating the security mechanism. *Int. J. Crit. Infrastruct. Prot.*, 2021, **35**, 100470. https://doi.org/10.1016/j.ijcip.2021.100470
17. Di Paolo, E., Bassetti, E. and Spognardi, A. Security assessment of common open source MQTT brokers and clients. *CEUR Workshop Proc.*, 2021, **2940**, 1–13.

Ülevaade tööstuses kasutatavate andmeedastusprotokollide küberturvalisuse arengust

Sergei Ponomar ja Martinš Sarkans

Neljas tööstusrevolutsioon (Tööstus 4.0) on võimaldanud digitaliseerida pea kõik tehnoloogilised protsessid. Kui tööstusrobotid ja -süsteemid suhtlevad omavahel peamiselt andmeedastusprotokollide kaudu, siis inimesed tegutsevad eelkõige protsessi vaatlejatena. Esialgu keskenduti andmeedastusprotokollide arendamisel peamiselt kiirusele ja andmete kvaliteedile, pöörates küberturvalisusele minimaalselt tähelepanu. Kuna üha rohkem tööstusseadmeid vahetab omavahel andmeid, on muutunud oluliseks tagada sidepidamise ajal küberturvalisus. Artiklis käsitletakse lühidalt andmevahetusprotokollide turvalisust sellest vaatenurgast.

Viimastel aastakümnetel on tööstusrajatiste vastu suunatud küberrünnakud sagenenud, mis on ajendanud erinevate turvameetodite lisamist sideprotokollidesse. Artiklis antakse ülevaade viimaste aastate uuringutest, mis käsitlevad tööstuslike andmeedastusprotokollide küberturvalisuse arengut ja selle mõju tehnoloogilistele protsessidele. Lisaks uuritakse, kuidas küberturvalisus mõjutab üleminekut viiendale tööstusrevolutsioonile (Tööstus 5.0).

Uurimistulemused toovad esile, kuidas kaitsemehhanismide lisamine andmeedastusprotokollidele mõjutab nende funktsionaalsust ja kvaliteeti. Samuti uuritakse probleeme, mis tekivad turvaelementide integreerimisel andmeedastusprotokollidesse.