Hybrid control system: Integration of sensors and controllers using MQTT and Modbus-RT

Oleksandr Sokolov [1,2], Miroslav Malaga [1], Pavel Raška [1], Serhii Sokolov [1], Petro Leontiev [1],

[1] Technical University of Kosice,
1, Bayerova Street, 080 01 Presov, Slovak Republic
[2] Sumy State University
116, Kharkivska Street, Sumy 40007, Ukraine
o.sokolov@teset.sumdu.edu.ua, s.sokolov@ksu.sumdu.edu.ua,
p.leontiev@ksu.sumdu.edu.ua
[3] University of West Bohemia
Univerzitní 2732/8, 301 00 Pilsen, Czech Republi
malaga@fst.zcu.cz
praska@fst.zcu.cz

Abstract: With the rapid development of Industrial Internet of Things (IIoT) technologies and increasing requirements for process automation, the integration of modern IIoT devices with traditional industrial systems is becoming increasingly important. This article explores the issue of combining devices based on the MQTT (Message Queuing Telemetry Transport) protocol, widely used in IIoT systems, with obsolete but still popular industrial systems operating on the Modbus-RTU protocol. The main attention is paid to the possibility of controlling such systems via SCADA (Supervisory Control And Data Acquisition)-systems, which act as the main interface for monitoring and control. The article considers different approaches to integration, describes possible problems and limitations that engineers may encounter when implementing such hybrid solutions, and suggests ways to overcome them. The advantages of using the MQTT protocol in combination with Modbus-RTU are analysed, such as improved scalability, flexibility and increased efficiency of data Exchange.

1 Introduction

Nowadays, imagining any automatic control system without using Industrial Internet of Things (IIoT) technology is not easy. This technology complements and opens up new control possibilities while increasing efficiency. On the other hand, new technologies require new communication protocols. The most promising communication protocol used in the IoT is MQTT, which, along with its ease of implementation and management, allows optimised data transmission even in unstable networks and resource-constrained environments. However, traditional industrial protocols such as Modbus-RTU, for example, are still used for data transmission between industrial devices.

https://doi.org/10.24132/PI.2024.12594.078-087

IoT technology used in SCADA-based hybrid control systems makes it possible to maximise the benefits of these protocols.

Taking advantage of both protocols in hybrid SCADA-based control systems is important. However, data transmission over SCADA requires considering many factors, including security, reliability and compatibility of the two protocols. Major challenges include incompatibility of communication models (Modbus uses request-response and MQTT uses publish-subscribe), security issues when transmitting data over open networks, and the need to provide real-time for manufacturing processes.

Numerous studies have focused on developing methods to integrate MQTT and Modbus-RTU in hybrid control systems. For example, Găitan and Zagan [1] proposed an IoT gateway implementation to extend Modbus capabilities to enable more efficient operation in industrial IIoT environments. Their work confirms that it is possible to improve the efficiency of monitoring systems by optimising data collection in hybrid systems. Also, a study by Cena et al. [2] proposed an extension to the Modbus protocol that improves the timing characteristics of communication for distributed embedded systems. This makes Modbus more adaptable to integrate with MQTT in IIoT-oriented SCADA systems.

Rughiniș and Rosner [3] demonstrated the successful use of MQTT in energy systems, emphasising this protocol's benefits for dealing with large amounts of real-time data. Their study showed that a hybrid architecture utilising Modbus and MQTT can improve the performance and flexibility of control systems.

However, there are several security concerns. Jaloudi [4] emphasises the vulnerability of Modbus when used in open IIoT networks, pointing out the need to implement additional security measures. As shown in the study by Abdullah et al. [5], one effective solution is implementing tokenised authentication methods such as TTAS to protect data in SCADA systems using MQTT and Modbus.

Integration also requires consideration of access control issues. Rehman et al. [6] proposed a role-based access control model for SCADA systems with Modbus, which adds an extra layer of security in managing access rights to devices and data. This is particularly important in scalable control systems using both MQTT and Modbus.

A detailed analysis of different industrial communication protocols for CNC machine tool monitoring, described in a study by Jauch et al. [7], concluded that using both Modbus and MQTT protocols could improve the accuracy of process monitoring and control of distributed systems.

Machine learning-based control models have been proposed to improve the flexibility of systems. For example, Ahmad and Tariq [8] proposed a hybrid access control model for SCADA networks using MQTT and Modbus using machine learning. This solution increased security and control accuracy, which is critical for IIoT environments.

Research such as the study by Kohler and Meier [9] look at the integration of legacy industrial equipment into new control systems. Their study confirms that legacy devices using Modbus can be successfully integrated into SCADA using MQTT protocols, allowing the modernisation of existing infrastructure with minimal cost.

Finally, security issues in cloud-based SCADA systems have been addressed in a study by González and Suri [10], which highlights the vulnerabilities of cloud-based SCADA systems and proposes methods to protect data using protocols such as Modbus and MQTT.

In summary, existing research confirms that integrating MQTT and Modbus-RTU into hybrid SCADA systems significantly improves control systems' flexibility, security and performance but requires addressing several interoperability and data security issues. Therefore, the aim of this article is to explore method for integrating MQTT and Modbus-RTU in hybrid SCADA systems to enhance the monitoring and control of industrial processes in an IIoT environment. This paper is divided into 4 sections. Section 1 describes the challenges of integrating systems based on MQTT and Modbus-RTU protocols. Section 2 describes the methodology proposed for data collection and exchange. Section 3 contains the results on the development of a hybrid SCADA system. Section 4 summarizes the paper.

2 Methodology

The Figure 1 shows a hybrid control system that integrates the operation of various sensors and controllers to transmit data via MQTT and Modbus-RTU protocols to a SCADA system located on a laptop. The main element of the system is the TXT 4.0 controller, which receives data from various sensors (environmental sensors, light sensor and motion sensor) and transmits it to the ESP8266 controller using the MQTT protocol. The ESP8266 controller then transmits the data via Modbus-RTU to a laptop, where the data can be visualised in the SCADA system.

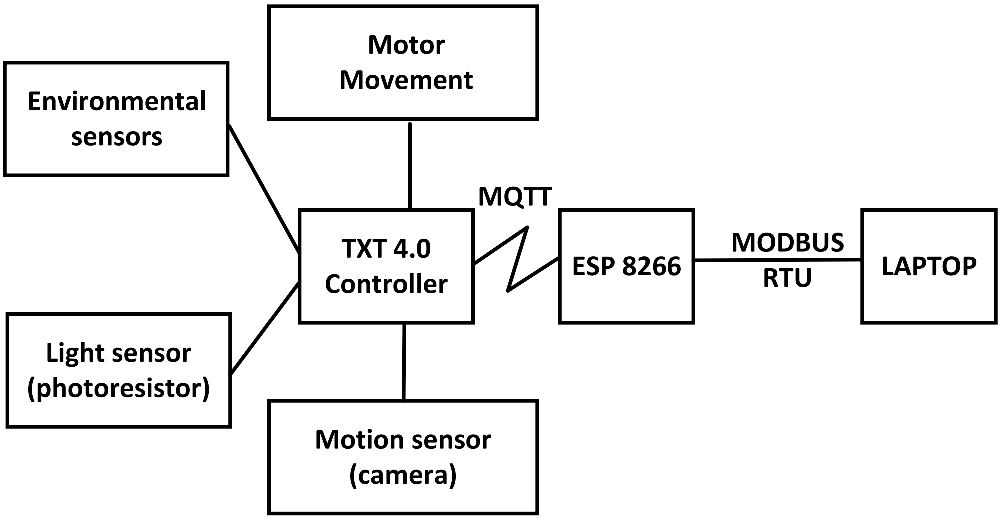

Figure 1. Schema of a hybrid control system with SCADA

This system simulates a measuring system for an automated warehouse conveyor, which is used to transport, sort and manage goods in large warehouses and production lines. The main purpose of this system is to monitor moving objects on the conveyor and their parameters, as well as to automatically control movement and lighting to improve operational efficiency. The design of such a system is shown in Figure 2.

The mosquitto broker was chosen as the MQTT broker because it is an open sorce. Data from sensors about temperature, humidity, pressure, motor movement and general movement were sent to the 'temperature', 'humidity', 'pressure', 'movement', 'motor 1', 'motor 2', 'light' topics. An example of its operation is shown in Figure 3.

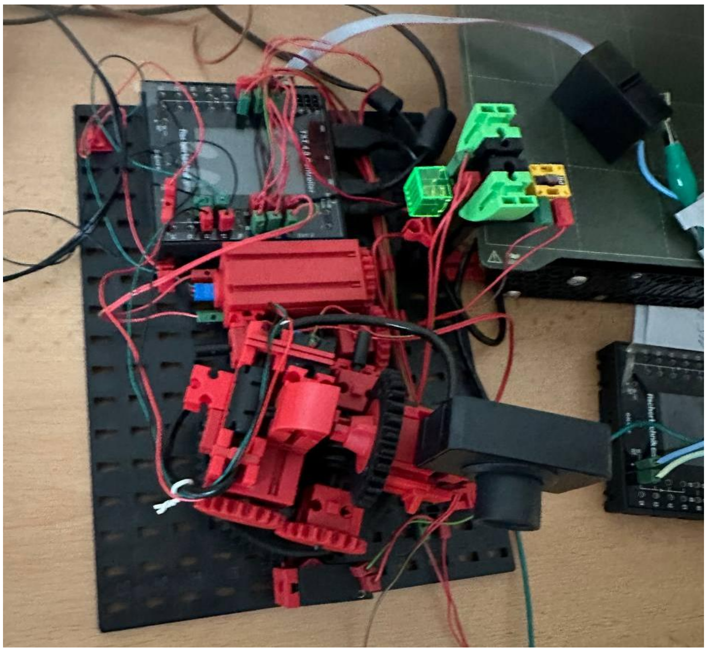

Figure 2. Design of proposed system

```
C:\Program Files\mosquitto>mosquitto_sub -t temperature
22.49
22.51
22.54
22.59
22.67
22.77
22.91
23.03
23.23
23.42
23.6
23.79
23.98
24.17
24.35
24.52
24.7
24.86
25.00
25.17
```

Figure 3. Collecting data from topics using the mosquitto broker

Considering that it is necessary to convert the MQTT protocol to MODBUS-RTU, we have chosen the approach using additional hardware such as the ESP8266 board, which is shown in Figure 4.

Figure 4. Design of ESP8266 board

The next step of the proposed solution is the configuration of the OPC server, which allows the data received from the ESP8266 board to be converted into MODBUS-RTU protocol data. To transmit data from sensors, it was proposed to use Holding Register, which allows the transmission of continuous signals having Float type. To create feedback and the ability to control the motor were used registers called coils, which are of Boolean type. The configuration of the OPC server is shown in Figure 5.

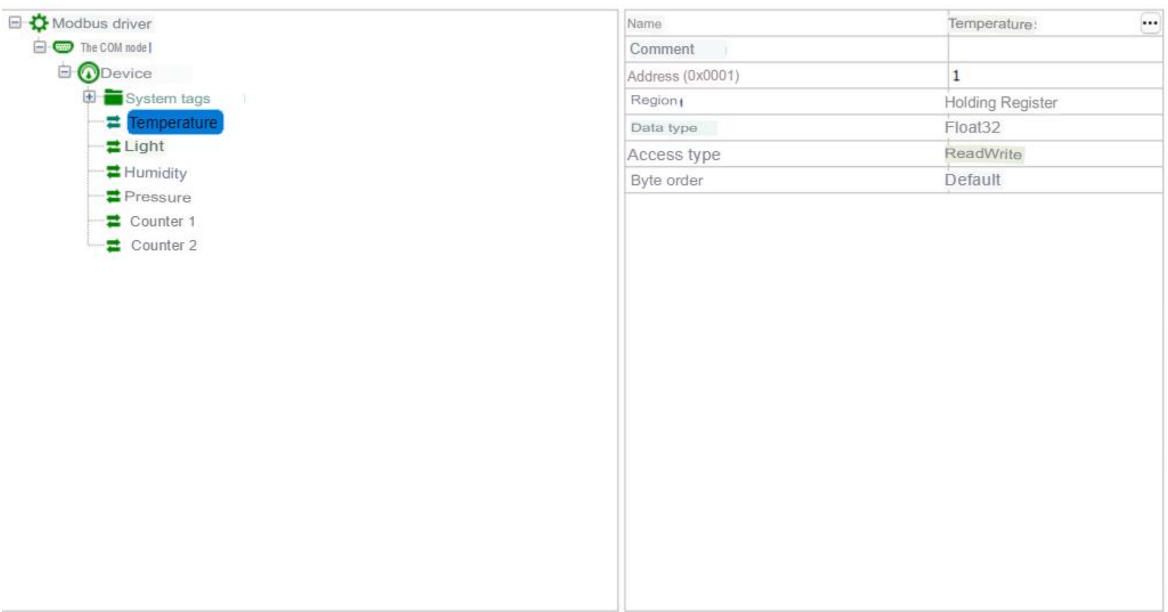

Figure 5. OPC server configuration

The final step of the proposed methodology is the development of a mnemonic scheme followed by the configuration of the elements. In this study, the mnemonic scheme shown in Figure 6 is used.

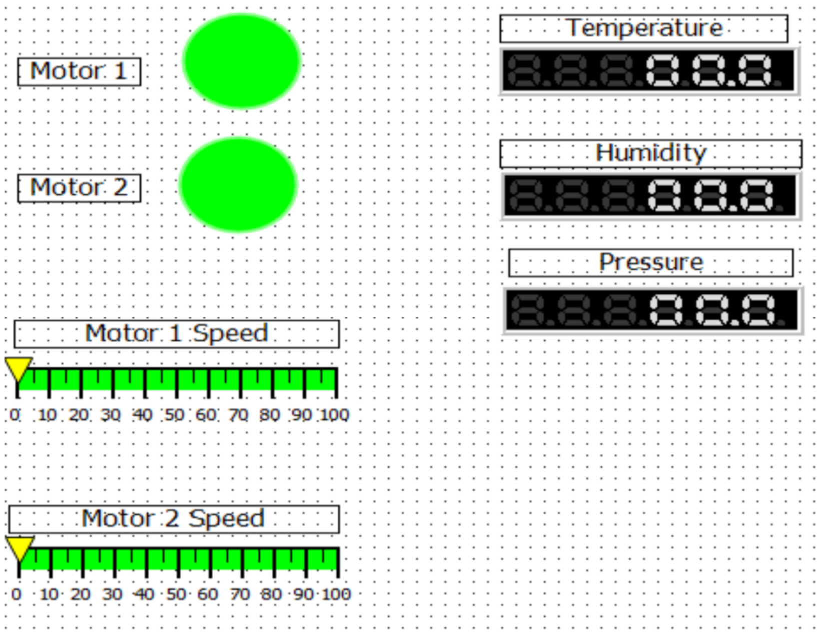

Figure 6. Mnemonic scheme for SCADA system

3 Discussion

The result of data transfer on the state of the current parameters is shown in Figures 7,8. The result of data transfer on the state of the current parameters is shown in Figures 7,8. Figure 7 shows SCADA system at the moment of its running (initialization), Figure 8 - at the moment of motor control.

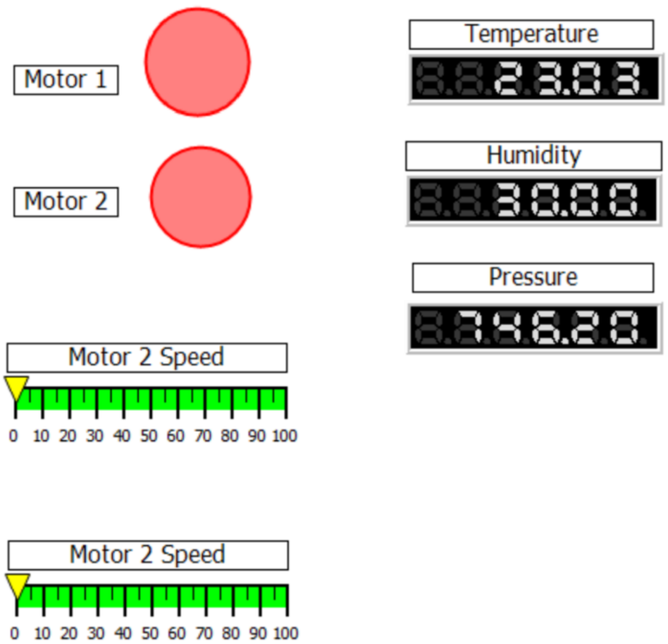

Figure 7. SCADA system at the moment of its initialization

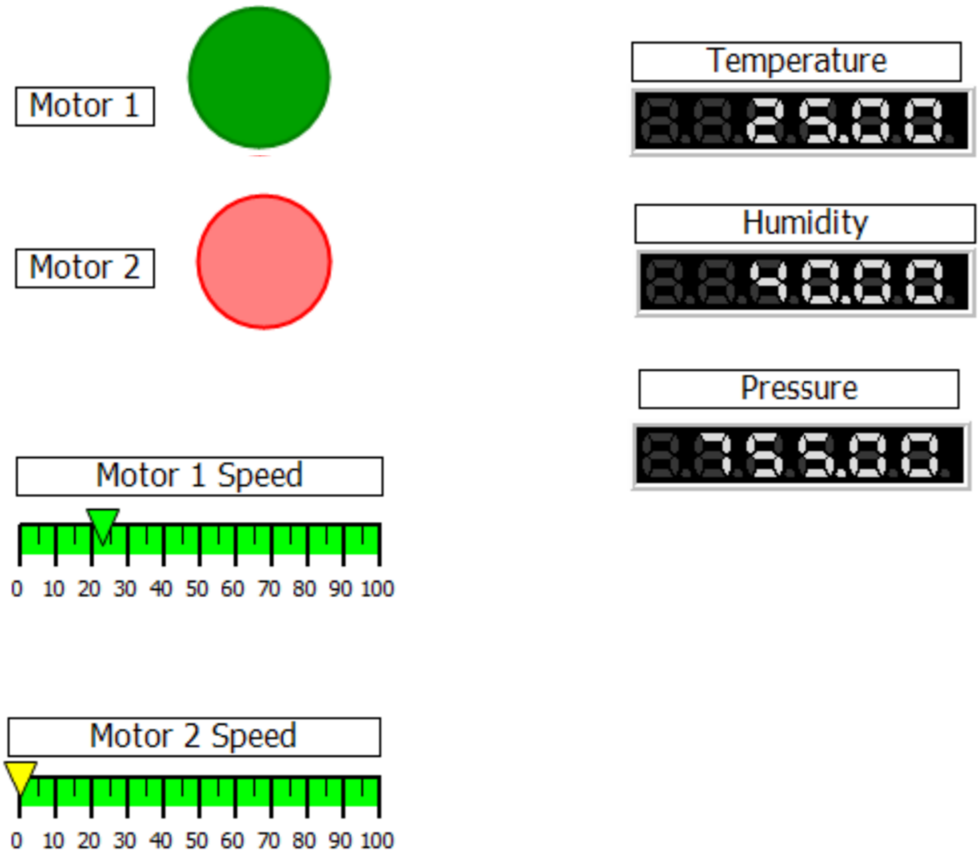

Figure 8. SCADA system at the moment of motor control

Figure 9 describes the motor speed values and the motor on (1) and off (0) states.

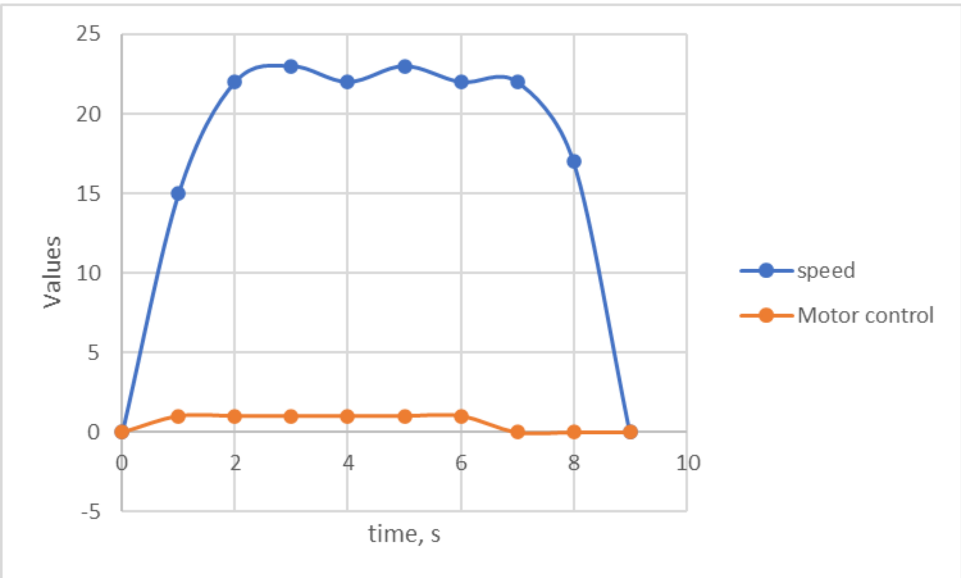

Figure 9. Time dependence of motor speed and motor state

As can be seen from the graph, there is a small delay of approximately 2 seconds. This is due to the fact that the sensor transmits data every second, as well as data using the MQTT protocol are sent every certain period of time, also the delay is affected by the time during which the conversion from MQTT protocol to MODBUS takes place. Thus, the current system has a short delay time, which allows it to be used for production in inert processes, while combining older and IIoT-enabled devices. However, there is also a challenge with the use in fast flowing processes as well as processes related to human safety, where the response time of the system needs to be several times faster.

4 Conclusion

To summarize, the study developed and tested a hybrid system that integrates MQTT and Modbus-RTU protocols to control an automated warehouse conveyor using SCADA. The system utilizes a TXT 4.0 controller to interface with sensors and actuators, and an ESP8266 controller to transmit data via MQTT and Modbus-RTU to the SCADA system. It was demonstrated that such integration allows efficient process control, lighting control and real-time monitoring of environmental parameters, providing system flexibility and reliability.

One of the key advantages of the system is the ability to integrate various devices and sensors, making it scalable and suitable for use in an industrial environment. The use of SCADA for data visualization and process control allows operators to easily monitor system status and make real-time decisions. Data protection techniques using tokenized authentication and access control have also been considered, which provides a high level of security for data transmission in IIoT networks.

However, challenges remain when integrating legacy systems with new technologies such as MQTT and Modbus-RTU. In particular, it is important to consider compatibility issues, response times and data security when transmitting over open networks. In the future, it is envisioned that the system capabilities will be expanded with the addition of new devices, enabling more sophisticated and intelligent solutions for industrial process automation.

Acknowledgment

This article was created with the subsidy of the project SGS-2024-032 "Intelligent production system" under the Internal Grant Agency of the University of West Bohemia.

References

[1] GĂITAN, V. G., ZAGAN, I. Experimental Implementation and Performance Evaluation of an IoT Access Gateway for the Modbus Extension. *Sensors*, 2021, 21(1), 246. DOI: https://doi.org/10.3390/s21010246.

[2] CENA, G., BERTOLOTTI, I. C., SCANZIO, S. Proposed Modbus Extension Protocol and Real-Time Communication Timing Requirements for Distributed Embedded Systems. *Technologies*, 2022, 12(10), 187. DOI: https://doi.org/10.3390/technologies12100187.

[3] RUGHINIȘ, R.-V., ROSNER, D. Smart Internet of Things Power Meter for Industrial and Domestic Applications. *Applied Sciences*, 2024, 14(17), 7621. DOI: https://doi.org/10.3390/app14177621.

[4] JALOUDI, S. Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study. *Future Internet*, 2019, 11(3), 66. DOI: https://doi.org/10.3390/fi11030066.

[5] ABDULLAH, M., ALI, T., KHAN, M. A. TTAS: Trusted Token Authentication Service of Securing SCADA Network in Energy Management System for Industrial Internet of Things. *Sensors*, 2021, 21(8), 2685. DOI: https://doi.org/10.3390/s21082685.

[6] REHMAN, A. U., BHATTI, A. R., ZAFFAR, N. A. A Role-Based Access Control Model in Modbus SCADA Systems. *Sensors*, 2019, 19(20), 4455. DOI: https://doi.org/10.3390/s19204455.

[7] JAUCH, C., MEIER, T., MÜLLER, S. Assessing Industrial Communication Protocols to Bridge the Gap between Machine Tools and Software Monitoring. Sensors, 2023, 23(12), 5694. DOI: https://doi.org/10.3390/s23125694.

[8] AHMAD, M., TARIQ, M. Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks Using Machine Learning. *Sensors*, 2023, 23(8), 3931. DOI: https://doi.org/10.3390/s23083931

[9] KOHLER, C., MEIER, F. Integration of Legacy Industrial Equipment in a Building-Management System Industry 5.0 Scenario. *Electronics*, 2023, 13(16), 3229. DOI: https://doi.org/10.3390/electronics13163229.

[10] GONZÁLEZ, F., SURI, N. A Survey of Security Challenges in Cloud-Based SCADA Systems. *Computers*, 2023, 13(4), 97. DOI: https://doi.org/10.3390/computers13040097.