REMOTE MONITORING AND CONTROL SYSTEM WITH INCREASED OPERATIONAL TECHNOLOGY CYBERSECURITY RESILIENCE

Aurel-Ionuț CHIRILĂ[1], Cristina-Gabriela SĂRĂCIN[2], Ioan-Dragoș DEACONU[3], Dragoș-Ștefan NICOLESCU[4], Alexandru RADULIAN[5]

It presents the structure of a remote monitoring and control system for an external high-voltage circuit breaker, with vacuum switching, envisioned for the railway system. The described system is part of a Supervisory Control and Data Acquisition (SCADA) system. Given the final application of the switching gear, the information that is transmitted through the entire communication network of the system should be completely secured, so that the people travelling by railway framework enjoy safe journeys.

The monitoring and control tasks are performed based on a programmable logic controller (PLC) making the system an operational technology (OT) type. Thus, such a system must have cybersecurity features, which are also described.

Keywords: cybersecurity, programmable logic controller (PLC), operational technology (OT), industrial control system (ICS), industrial control and automation system (ICAS), Supervisory Control and Data Acquisition (SCADA)

1. Introduction

Industrial Control and Automation Systems (ICAS) or Industrial Control Systems (ICS), presently, have remote control and monitoring capabilities due to the increasing performance of network systems. Such features allow for the devices which are widely distributed on large areas or on large distance sites to be controlled from a central unit, thus in case of malfunctions this failure state is quickly and easily signaled and acknowledged by the human operator located on that central unit zone. The immediate effect of this swift detection is the lowest

[1] Assoc. Prof., PhD. Eng., Dept. of Electrical Machines, Materials and Drives, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: aurel.chirila@gmail.com

[2] Assoc. Prof., PhD. Eng., Dept. of Measurements, Electrical Devices and Static Converters, National University of Science and Technology POLITEHNICA Bucharest, Romania, Romania, e-mail: cristina.saracin@upb.ro

[3] Prof. Habil, Dept.of Electrical Machines, Materials and Drives, National University of Science and Technology POLITEHNICA Bucharest, Romania, e-mail: dragos.deaconu@gmail.com

[4] PhD Student, SC ICPE SA, Romania, e-mail: dragos.nicolescu@icpe.ro

[5] PhD Eng., Head of the Electric Apparatus Department, SC ICPE SA, Romania, e-mail: alex.radulian@icpe.ro

losses possible. The losses refer not just to money costs but also to physical and time resources. Operating decisions can be put in place very quickly based on the detected events and the existing resources at the time being. Almost all ICASs are based on Programmable Logic Controllers (PLCs), which are the main control part of the automation process, where the software component resides. As such, ICSs are Operational Technology (OT) systems.

These types of systems are currently major targets of cyber-attacks. The first cyberattack on OT systems is Stuxnet worm [1] (2010) designed to introduce a rootkit onto the PLC software with the aim to destroy gas centrifuges for separating nuclear material in Iranian nuclear facilities.

At the time of writing this article, in [2][3] (2024) the ransomware attacks target mainly OT frameworks [4].

The remote monitoring and control system is designed to be used for a high voltage circuit breaker which is found within the feeder stations of Romanian national railway system. Practically, this circuit breaker feeds with electric energy the railway system's overhead lines from a high -voltage electrical grid. In turn, these overhead lines power the trains with electric energy for the entire journey, by means of physical electric contact, namely the pantograph that is mounted on the trains' roofs (Fig. 1). It must be underlined that the overhead lines are split in sections, thus more separated feeding points and more high voltage circuit breakers are used for each section along the railway system.

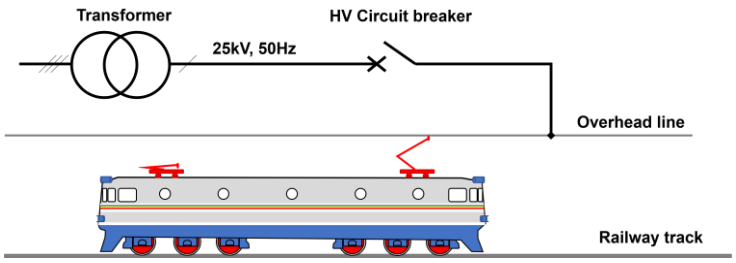

Fig. 1. The high-voltage part of the remote monitoring and control system

In consequence, this circuit breaker and its associated remote monitoring and control system are of major importance. All the framework that manages the exchanged data must be protected against cybersecurity threats. Otherwise, an attacker can tamper with data.

Let us consider for example the scenario where the attacker manipulates the monitoring information of the high-voltage circuit breaker by signaling a false over-voltage event. The remote-control system triggers the alarm procedure and performs the action to open the circuit breaker. The immediate effect is that even though there is no over-voltage, the existing train which is powered from the

given overhead line section will be disconnected and possibly it will stop or travel at lower velocity.

2. Remote monitoring and control system

A general overview of the designed system is shown in Fig. 2. It comprises the remote and control system and the driving part i.e., the high voltage circuit breaker.

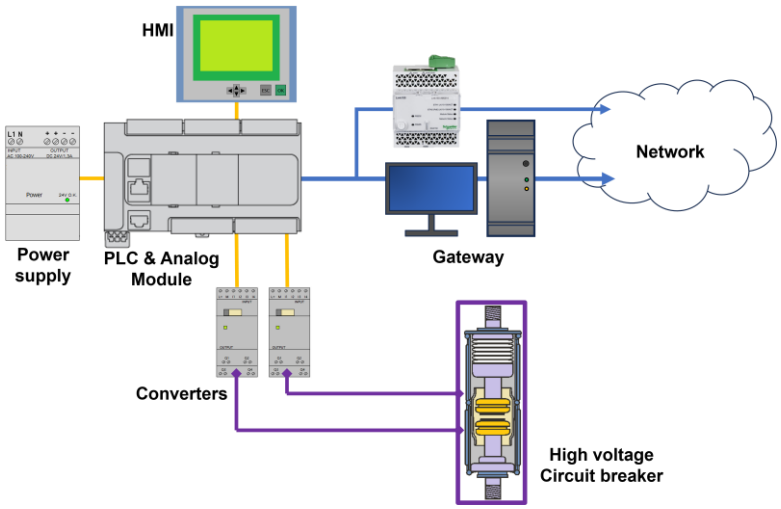

Fig. 2. The system overview

For local interaction with the operator, it is used a Human Machine Interface (HMI) device, which has been programmed as shown in the following.

The main screen of the developed application is shown in Fig. 3. The operator has many options to choose from. The options top to bottom, left to right are the following: Monitoring system, Communication system, Analog sensors, Alarm system, Configuration and Emergency stop.

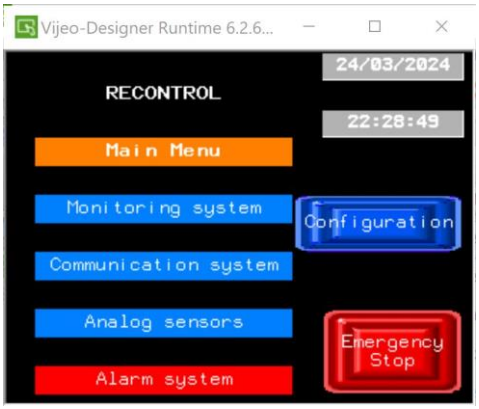

Fig. 3. The remote monitoring and control system

In Fig. 4 it is shown the Monitoring system display. On the left side it is shown a sample for the circuit breaker coil's maximum allowable voltage (400V DC) and maximum allowable current (100A DC). On the right side it is shown a sample for the main circuit of the circuit breaker, i.e., rated voltage (25000V AC, 50Hz) and rated current (1250A AC, 50Hz). The test is performed with maximum values.

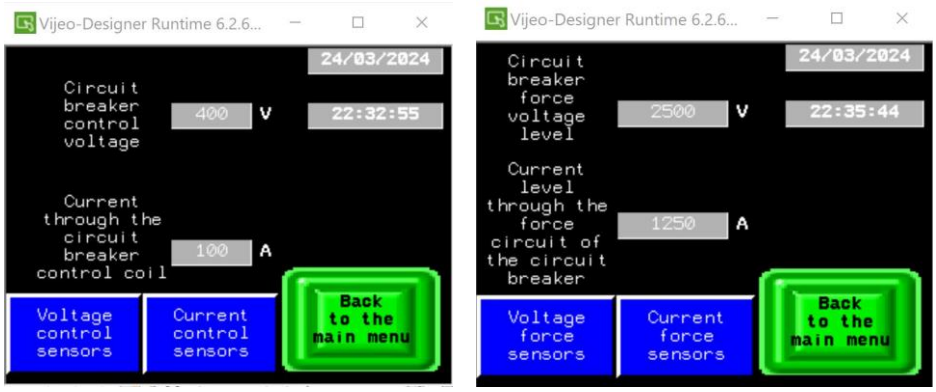

Fig. 4. The remote monitoring and control system

The advantages of HMI are many. Thus, an HMI allows operators to quickly identify all the alarms or warnings by seeing some drawings, messages, or color changes. In this way, the operators can swiftly provide a reaction. Sometimes, the alerts refer to future events that have not yet developed, so that by providing a before alert followed by the proper action, failure is avoided. The HMI is advantageous not just for alarms or warning, but also for reliable messages, such as the current state of the system. Another great plus of HMI devices is that it allows the use of graphical objects which are quite suggestive and even display animations. An HMI device allows for cost reduction from the manufacturer's point of view, by replacing many control devices such as push buttons, indicator lights, selectors, switches, individual displays and more. The lack of these devices leads to a more reduction of cost by eliminating the requirements for connecting cables, wires, panels, terminals, consoles etc.

The PLC receives information regarding the status of the high voltage circuit breaker. The information is encoded as electrical signals (voltages and currents) of both alternative and direct current types. The adaptation from their real high-value range to lower range is performed by the analog converters. Then, the low value converted signals are transmitted to the PLC using the analog input module. It is worth mentioning that this PLC is part of a Supervisory Control and Data Acquisition (SCADA) system which receives data from such PLCs, and it provides control signals for the devices monitored and controlled by each PLC. The central node is not part of the current description. The remote monitoring and

control system is advantageous because the operator does not have to physically be present within the controlled system area. which can be a dangerous area, but he/she can still perform the monitoring and controlling function of the system from a safe location. The main parts of the physically implemented local part of the remote monitoring and control system is depicted in Fig. 5.

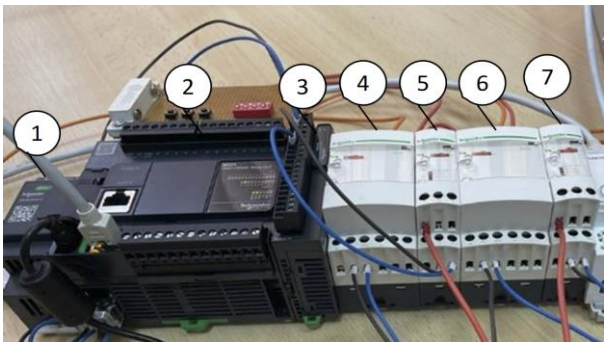

Fig. 5. The local part of the remote monitoring and control system

In Table 1 are given the main specifications for each part of the local part of the remote monitoring and control system.

Table 1

Components main features

Part no.	Model	Description	Main features
1	ABLM1A24012	Power supply	▪ rated input voltage: 100...240 VAC (1 ph.) ▪ rated power: 30 W ▪ output voltage: 24 VDC ▪ output current: 1.25 A
2	TM221CE24R	Programmable Logic Controller	▪ rated supply voltage: 100…240VAC ▪ discrete input number: 14 ▪ analogue input number: 2 (0...10) VDC ▪ discrete output type: relay normally open ▪ discrete output number: 10 relays ▪ discrete output DC voltage: 5...125 VDC ▪ discrete output AC voltage: 5...250 VAC ▪ discrete output current: 2 A
3	TM3AI8	Analog input module	▪ provides 8 inputs with 11bit + sign and 12bit resolution ▪ analogue input type: current 4...20 mA / 0...20 mA; voltage 0...10 V / - 10...10 V
4,6	RMCA61BD	Isolated analog converter	▪ rated supply voltage: 24 V DC +/- 20 % ▪ analogue input type: ▪ current 0...1.5 A AC/DC 50/60 Hz ▪ current 0...15 A AC/DC 50/60 Hz ▪ current 0...5 A AC/DC 50/60 Hz ▪ analogue output type:

			▪ current 0...20 mA ▪ current 4...20 mA ▪ voltage 0...10 V

5,7	RMCV60BD	Isolated analog converter	▪ rated supply voltage: 24 V DC +/- 20 % ▪ analogue input type: ▪ voltage 0...300V AC/DC 50/60 Hz ▪ voltage 0...50V AC/DC 50/60 Hz ▪ voltage 0...500V AC/DC 50/60 Hz ▪ analogue output type: ▪ current 0...20 mA ▪ current 4...20 mA ▪ voltage 0...10 V

The information read from the high voltage circuit breaker and the data conversion flows for each acquired quantity are explained in detail in Table 2.

Table 2

Monitoring and control system main analog inputs

Monitored quantity	Values	Converter input	Converter output (Analog input)	Converter device
Circuit breaker state	ON: VDC > 0 OFF: VDC = 0	0 / 10 V DC	0 / 10 V DC	PLC analog input
Circuit breaker main current	0 – 1250 A AC, 50 Hz	0 – 5 A AC	4 – 20 mA DC	RMCA61BD
Circuit breaker main terminals voltage	0 – 25 kV AC, 50 Hz	0 – 50 V AC	0 – 10 V DC	RMCV60BD
Circuit breaker coil current	0 – 100 A DC	0 – 1.5 A DC	0 – 20 mA DC	RMCA61BD
Circuit breaker coil voltage	0 – 400 V DC	0 – 50 V DC	0 – 10 V DC	RMCV60BD

All the values received at the analog input module terminals are sent to the PLC and then converted in accordance with the implemented program, which is downloaded into the PLC. These values are displayed locally on the display attached to the PLC i.e., the HMI device. In Fig. 6 it is presented only one sequence of the implemented program.

Fig. 6. The remote monitoring and control system

The purpose of this sequence is to read the value from the fourth analog input of the TM3AI8 module and store it into a memory word into the PLC. The

memory address of the fourth analog input is %IW1.3, while the storing memory address of the PLC is %MW3. The same approach is applied for all the analog inputs, and all the memory addresses are shown in Table 3.

Table 3

Monitoring and control system main analog inputs

Monitored quantity	Values	Analog input memory address	PLC memory address
Circuit breaker state	ON: VDC > 0 OFF: VDC = 0	%IW0.0	-
Circuit breaker main current	0 – 1250 A AC, 50 Hz	%IW1.3	%MW0
Circuit breaker main terminals voltage	0 – 25 kV AC, 50 Hz	%IW1.0	%MW2
Circuit breaker coil current	0 – 100 A DC	%IW1.4	%MW1
Circuit breaker coil voltage	0 – 400 V DC	%IW1.1	%MW3

The condition to copy the value from the analog inputs to other memory addresses is due to the requirement to also make these values accessible by the HMI device.

3. Data transmission framework

The process of transmitting data is described in the following. Firstly, a connection between the PLC and the client host is performed. The client host is the computer that behaves like a gateway for the local monitoring part of the system. In Fig. 7 it depicts the communication between the PLC and the Gateway, which is based on Modbus TCP protocol [5].

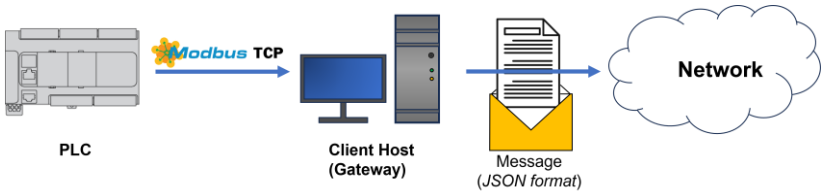

Fig. 7. Data transmission framework of remote and monitoring system

Regarding the encapsulation of the Modbus TCP protocol, within the OSI model it is positioned on the seventh, sixth and fifth layers. On the fourth layer is the Transmission Control Protocol (TCP). On the third layer is Internet Protocol. On the second and first layer there is IEEE 802.3 protocol. Thus, Modbus features a five-layer Internet model. The required data is retained within the registers of the PLC. It must be underlined that the Gateway is the client side regarding

Modbus TCP protocol, while the PLC is the server side. Once the values are read from the PLC it must be processed and formatted in accordance with a known data structure, such as JavaScript Object Notation (JSON) [6]. There are advantages to choosing this data format: it is openly accessible and usable by anyone. The next step is to send this data to the central node of the remote control and monitoring system.

4. OT Cyber resilience features

The simplest method to send messages is to send them by plain text. In this case the values of different quantities are sent directly as they are, as shown in Fig. 8.

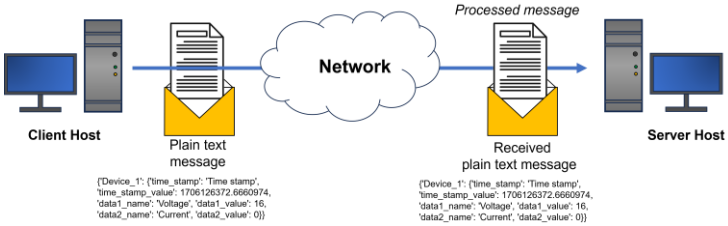

Fig. 8. Plain text message

Using this approach all the data can be completely sniffed or snooped by an attacker as shown in Fig. 9. Moreover, the attacker can tamper with data.

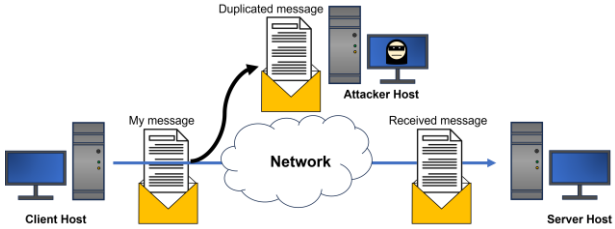

Fig. 9. Sniffing/snooping attack

By tampering with data, the attacker can trigger false alarms. In cybersecurity there are some information properties that should be present: confidentiality, integrity, availability and authenticity [7]. The integrity and authenticity are achieved for the designed system by using Hash-based message authentication code (HMAC) [9]. In an HMAC transaction, both the client and server must agree on the same secret key (#hmac_key) and hashing algorithm (H) [8]. Hashing is a mathematical function (algorithm) which transforms any string of characters into a fixed number of bits. Of course, there is a possibility to obtain the same number of bits for two different strings of characters, which is called hash collision [10], but if wisely used this issue can be overcome. Now, let us

suppose the client wants to send the payload (#payload), it will generate the following signature (|| means concatenation):

$$\#Sent\_msg\_signature = H[\#hmac\_key \,//\, H(\#hmac\_key \,//\, \#payload)] \quad (1)$$

The server side receives the #payload and the #Sent_msg_signature and computes the same signature, using (1), because it knows the same secret key #hmac_key and hashing algorithm (H). If there is a signature match (client and server) it means the message is authenticated and it is processed. Otherwise, the server discards the received message, and it is not processed. A second layer of protection is to encrypt the payload, i.e., JSON format message with data values. Thus, confidentiality of the information is obtained. The HMAC procedure is then applied for this encrypted payload. To still increase the security, the encryption key of the payload can be a different one than #hmac_key. All processes are shown in Fig. 10.

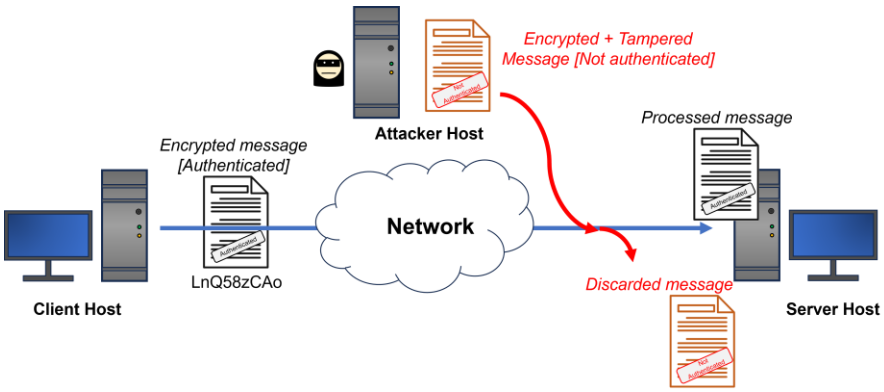

Fig. 10. HMAC approach

In Fig. 11 is shown the server side, which receives an authenticated packet. The #hmac_key is “my_secret_key”.

Fig. 11. Server side

6. Conclusions

The designed OT system both locally and remotely monitors the state of high-voltage circuit breakers that feed the overhead lines of railway transport system,

based on PLCs. The acquired data is remotely sent to a central node which can also perform the remote monitoring and control functions. The data stream must be secured for the safe operation of the railway system i.e., trains' journeys. More levels of security are described with the aim to obtain confidentiality, integrity, and authenticity so that to counterattack on-path attacks (data sniffing, tampering, spoofing). The implementation of the security levels has been performed and tested based on Python code. By this approach it is possible to develop security levels for a broad range of networking equipment regardless of the communication protocol or type (by wire or by wireless). As the attacks become more and more complex, so should the information security controls.

Acknowledgment

This work has been supported by the Executive Agency for Higher Education, Research, Development, and Innovation Funding (UEFISCDI) through the Financial Agreement PN III No.696PED_24/06/2022, project acronym RECONTROL, contract ID PN-III-P2-2.1-PED-2021-3731 granted by Romanian Ministry of Education.

R E F E R E N C E S

[1] *** Wikipedia – Stuxnet, https://en.wikipedia.org/wiki/Stuxnet
[2] SecurityWeek - https://www.securityweek.com/ot-maintenance-is-primary-source-of-ot-security-incidents-report/ - accessed on 2024, June 28.
[3] Ransomware tracker: The latest figures [June 2024] - https://therecord.media/ransomware-tracker-the-latest-figures - - accessed on 2024, June 28.
[4] *B:E.M. Camachi, D. Popescu*, Cyber security of SmartGrids infrastructure: protective measure against attacks, U.P.B. Sci. Bull., Series C, Vol. 82, Iss. 3, 2020.
[5] *** Modbus Organization – MODBUS Messaging on TCP/IP, 2006, https://www.modbus.org/
[6] *** Douglas Crockford – The JSON Saga - Youtube, 2011, https://www.youtube.com/watch?v=-C-JoyNuQJs
[7] *E. Neacșu, E. Simion*, A study on the encryption techniques and methods implemented within the critical infrastructures, U.P.B. Sci. Bull., Series C, Vol. 84, Iss. 2, 2022.
[8] *E. Neacșu, P. Șchiopu*, A security analysis of public key cryptographic systems used for electronic signature, U.P.B. Sci. Bull., Series C, Vol. 83, Iss. 1, 2021.
[9] *M. Bellare, R. Canetti and H. Krawczyk*, "Keying Hash Functions for Message Authentication". In: Koblitz, N. (eds) Advances in Cryptology — CRYPTO '96. Lecture Notes in Computer Science, vol 1109. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68697-5_1, 1996.
[10] *L. Metcalf, W. Casey*, Cybersecurity and Applied Mathematics, Syngress Publishing, 2016.