Remote Control and Monitoring Protocols for PLC and HMI Systems: A Case Study of MODBUS, WMI and VNC

2025 9th International Symposium on Innovative Approaches in Smart Technologies (ISAS) | 979-8-3315-1482-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISAS66241.2025.11101982

1st Ercan AYKUT
Electric
Istanbul Gelisim University
Istanbul, Türkiye
eaykut@gelisim.edu.tr

2nd Kübra ERDOĞAN
Mechatronics
Istanbul Gelisim University
Istanbul, Türkiye
kerdogan@gelisim.edu.tr

3rd Sena Nur BENLİ
Computer Programming
Istanbul Gelisim University
Istanbul, Türkiye
snbenli@gelisim.edu.tr

4th M. Cihat MUMCU
Electric
Istanbul Gelisim University
Istanbul, Türkiye
mcmumcu@gelisim.edu.tr

5th İzzet YAVUZ
Electric
Istanbul Gelisim University
Istanbul, Türkiye
izyavuz@gelisim.edu.tr

***Abstract*—This electronic document is Programmable Logic Controllers (PLC) are used in Automation systems in a variety of applications. PLC is the control unit of the systems or machines. It collects information from sensors and controls the output ports. PLCs can also be used to communicate between the devices or sensors. In this study, remote control protocols of PLC have been investigated and a remote control and monitoring implementation has been realized by using Windows Management Instrumentation (WMI), RS-485, RS-232, and VNC protocols. A machine has been designed to separate the sprue from the injected plastic. The machine is equipped with GMT brand 396R model PLC, a 7" touch screen Human Machine Interface (HMI) and Variable Frequency Driver (VFD). PLC is remotely controlled through WMI connection from Ethernet port, HMI is monitored and controlled by VNC protocol, VFD is controlled by the PLC through RS-485 and HMI is connected to PLC through RS-232 MODBUS protocol. The advanced communication gave extra flexibility and increased the efficiency while reducing the maintenance cost.**

Keywords—Remote control, PLC, Monitoring, VNC, SCADA

I. INTRODUCTION (*HEADING 1*)

Automation systems increase the efficiency and reduce the cost of the systems [1]. Programmable Logic Controllers (PLC) are the main controllers of automation systems [2]. PLCs are used to control digital input outputs as well as analog input and output. The cooperation of PLCs and Human Machine Interface (HMI) increases the flexibility of the system [3]. PLCs can communicate with other devices and sensors by means of some rules called protocol [4]. One of the communication protocols between PLCs and other devices is MODBUS RS-232 or RS-485 protocol [5]. Another remote control protocol of PLC can be depicted as Ethernet protocol. PLCs can be accessed from a remote location by means of Ethernet connection protocol which is called Windows Management Instrumentation (WMI) [6]. Supervisory Control and Data Acquisition (SCADA) system is another type of remote control and monitoring system used with PLCs [7]. Moreover, PLCs can communicate with IOT devices by a protocol called MQTT [8]. Besides, there is another remote control protocol called Virtual Network Computing (VNC) [9].

Some of the studies in the literature about PLC, HMI and the protocols can be listed as follows. Karaalp and Aykut [10] designed a PLC and stepper motor based conveyor system which makes a stamping process by means of a valve, actuator and sensors. Salunke et al., [11] implemented a real time remote communication between MATLAB and PLC by using VNC protocol. Abrishambaf et al., [12] investigated a SCADA system for an office building. Da'na et al., [13] developed a remote control and monitoring system by means of GSM and TCP/IP network. In the study they used Siemens S7 PLC and CP343 and CP340 Ethernet and GSM modules respectively. They achieved web based access to the PLC and SMS based control over GSM. Mozaryn et al., [14] designed a system for failure isolation and remote monitoring by using Industrial Internet of Things (IIOT). In the study they implemented failure detection using Unknown Input Observer (UIO) algorithm, also they developed continuous monitoring and failure maintenance scenarios by means of IOT network and they integrated embedded programming with PLC. Karemore and Jagtap [15] designed an IOT based industrial monitoring and remote control system with PLC. In the study they used sensors for monitoring the system and Wifi modules for data communication as an alternative to SCADA systems.

In this study, remote control of PLC and HMI based systems is designed by means of 4 different protocols which are WMI, RS-232, RS-485 and VNC. In the literature, the studies are mainly based on a unique protocol. This advanced control gives extra flexibility, cost effectiveness and more efficiency which makes the study original and different from the other studies in the literature. follow.

II. MATERIAL AND METHODS

A. SCADA

SCADA (Supervisory Control and Data Acquisition) is a system that is particularly useful in industrial applications, as it targets both control and supervisory levels. The implementation of these systems is not hardware-based, but rather completely software-based applications interfaced through Programmable Logic Controllers (PLCs) or other commercial hardware modules. SCADA systems are employed in industrial production processes and are also crucial in certain experimental facilities, including the chemical industry, nuclear fusion, energy production and distribution (both traditional and nuclear), and steel production [16]. SCADA systems collect data from local or remote devices and store and process this data in a central computer. In this manner, they fulfill the role of overseeing

979-8-3315-1482-2/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.

and regulating industrial processes. The basic components of SCADA systems are classified as follows:

1) Supervisory Control: Control of industrial processes is carried out with Human-Machine Interface (HMI) software. HMI allows users to interact with the system and provides central control by communicating with field devices such as Main Terminal Unit (MTU) and Remote Terminal Units (RTUs) via the SCADA network.

2) Data Collection: Data is collected via PLCs and RTUs. PLCs are solid-state devices that support decision-making mechanisms by continuously monitoring and controlling industrial physical processes.

3) Data Storage: SCADA systems generally use structured query language (SQL) databases to store time-stamped data. Historian software, which can work integrated with SCADA systems, collects real-time data from SCADA devices and records this data in a central database.

4) Data Exchange: Various communication protocols are used to provide data communication between different components in SCADA systems [17].

Upon examination of the historical development of SCADA systems, it is evident that they have a lengthy and extensive history. First, first-generation SCADA systems were built on monolithic structures and had a structure based entirely on proprietary network technologies. The flexibility and scalability of the systems increased significantly with the use of distributed architectures in the second-generation SCADA systems. With the third-generation SCADA systems, a fully networked structure was achieved by utilizing internet technologies. Future fourth generation SCADA systems are expected to grow based on concepts related to the Industrial Internet of Things (IoT) and the Future Internet of Things (FIN). The system will use advanced methodologies such as cloud and fog computing, big data analytics and mobile computing [18].

B. MODBUS

The MODBUS Ethernet protocol facilitates straightforward and dependable communication among devices on the same network and is extensively utilized in contemporary industrial environments. The substantial demand for this protocol necessitates an algorithm or technique capable of transforming any slave sensor device into a MODBUS-compatible device. In this way, it will be possible for different sensors to communicate via the MODBUS protocol. The MODBUS devices to be developed must possess sufficient compatibility to operate on any processor platform and must be adaptable to evolving requirements while maintaining the protocol format. MODBUS was first developed in 1979 by Modicon, a pioneer in the programmable logic controller (PLC) market. It was designed to enable internal point-to-point communication between the first Modicon PLCs and the panels that program them. Following some acquisitions over time, the Modicon brand has now been incorporated into AEG Schneider Automation and continues to operate under the brands "Modicon," "Square D," and "Telemecanique" [19]. Since 1979, the MODBUS protocol's performance metrics, such as accuracy, reliability, and robustness, have been accepted as basic criteria in industrial applications, and the protocol is used as a generally accepted standard. MODBUS communication occurs in two basic forms:

• Query/Response: It describes bidirectional communication between a master and a slave device.

• Broadcast: This means that the master device sends a command to all slaves simultaneously without waiting for a response.

A MODBUS transaction is made up of a single query/response or broadcast frame. A MODBUS frame message contains the intended recipient's address, the command to be executed, and the information needed to carry out the command. The master terminal's command is known as query, and the slave's response is known as response [20]. Fig 1 depicts the simplified structure of messages that can be used as a format, query, or response.t. Please do not revise any of the current designations.



Fig. 1. Simplified MODBUS message format

The MODBUS protocol defines a variety of operation codes, each of which corresponds to a specific command. Example operation codes for conveyor control in automation systems are given below:

• Write Single Coil (0x05): Used to start or stop the conveyor motor. 0xFF00 (ON) or 0x0000 (OFF) is written to the output coil to which the motor is connected. The address and value written are confirmed with the response message.

• Write Multiple Coil (0x0F): Used to control multiple coils in a conveyor system (for example, forward/reverse direction or alarm) simultaneously. The desired number of coil states are written beginning at the start address. The response message includes the start address and the number of changed coils.

• Write Holding Register (0x06): Used to adjust the conveyor motor speed or another analog parameter. A 16-bit value is written to the relevant register address, and the written value indicates the motor speed or the set parameter.

• Read Input Records (0x04): Used to read analog data records from sensors on the conveyor. The start addresses and the number of records to be read are specified in the request message and the sensor data is sent in 16-bit format with the response message [21].

C. ETHERNET

In today's technology, the internet and internet-connected device technologies are indispensable. In 1972, Robert Metcalfe of Xerox Palo Alto and his team created a local area network (LAN) technology that connected stations, servers, and peripherals within the same structure using a common data path architecture. Metcalfe and his team developed a collision detection algorithm to improve the efficiency of the existing ALOHA network and filed a patent application in 1977, resulting in Ethernet's media access control protocol, Carrier Sense Multiple Access and Collision Detection (CSMA/CD) [22].

Ethernet has become an essential component of today's internet infrastructure, and it is widely used in offices, homes, data centers, transportation, automotive, aviation, and industrial sectors. Originally designed as a decentralized, flexible, and low-cost LAN system with 3 Mbps bandwidth and connections for up to 256 devices, Ethernet technology's capacity has increased significantly in tandem with research

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.

in this field, making Ethernet the most widely used wired LAN technology today with its various variations. When the historical process is examined, Ethernet configurations at 10 Mbps speed, where all hosts share the same coaxial cable, gained significant popularity in the 1980s. Switched, full-duplex, collision-free Ethernet systems with speeds of up to 1 Gbps are now accepted as standard low-cost network solutions for workstations and laptops.

Alternatively, Ethernet connections at 10 Gbps are becoming more common for servers and high-performance hosts. The literature contains studies on expanding Ethernet segments in terms of coverage and capacity using various methods and algorithms. When the studies are examined, network administrators design end-to-end Ethernet infrastructures to reduce upper layer operations such as IP routing and addressing, with the goal of reducing the network's internal communication loads. In larger Ethernet segments, the goal is to improve efficiency by processing data traffic in lower layers rather than IP. When compared to IP routers, Ethernet switches allow for faster network configuration and use less energy. While IP routers require complex operations like extracting headers from data frames and matching addresses, Ethernet switches reduce processing time and system complexity by routing only through the MAC address table. Researchers direct the development of Ethernet technologies using various methods to achieve the application's desired optimizations [23]. The basic Ethernet frame structure is depicted in Fig 2.

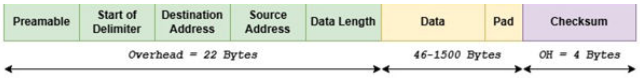


Fig. 2. Ethernet (CSMA/CD) frame format.

The total overhead of the frame is 26 bytes, and the data field ranges from 46 to 1500 bytes. According to the standards, the minimum length of the frame from the destination address to the checksum is 64 bytes, which increases to 72 bytes with the prefix and separator. When the data field is shorter than 46 bytes, padding is added to keep the frame size to a minimum. The minimum frame slot time for Ethernet networks with 1 Gbps speed, 100 meters length, and four repeaters is 0.512 microseconds, which is the time required to transmit a 64-byte frame at 1 Gbps [24].

D. HMI

Processes in the system are monitored and managed via a Human-Machine Interface (HMI). HMI devices are graphical user interfaces that make it simple and direct for operators to communicate with machines. Operators can issue commands, change system parameters, monitor real-time data, and respond to alarms using the HMI [25]. HMI devices and PLCs are mostly connected to each other by means of some industrial communication protocols such as MODBUS, Profinet or Ethernet/IP. An HMI not only improves process transparency and traceability but also transfers data of the process rapidly [26]. Beside displaying data, HMI may include advanced features such as alarm management, recipe control, data logging and access control. Moreover, operator errors can be minimized by means of HMI [27].

E. MQTT

Message Queuing Telemetry Transport (MQTT) protocol was developed to realize the data communication between the devices in limited bandwidth networks [28]. By means of MQTT protocol, PLCs can make safe and low latency data communication in industrial automation systems and the flexible structure and low energy consumption of MQTT make it popular in IOT based applications [29].

F. VNC

Virtual Network Computing (VNC) protocol permits the users to monitor and control a real time system from a remote location by accessing a graphical interface. It is mainly preferred to be used in industrial automation projects to control the HMI from remote locations [30].

III. DISCUSSION

In this study a combined remote control and monitoring system has been designed for a PLC and HMI based automation process. Plastic parts are produced by the plastic injection machines by means of moulds. The injected plastic product can be designed as multiple pieces in one mould and they are connected to a sprue as seen in Fig 3. After the injection the plastic products are separated from the sprue which requires labor.



Fig. 3. The injected plastic product connected to the sprue

In this context, a machine has been developed to separate the plastic parts from the sprue. The photo of the designed machine has been presented in Fig 4.



Fig. 4. The machine which separates the sprue

A. Components Used in the System

The main components used in the system consist of PLC, HMI, AC motor driver and valves.

1) PLC: As the controller unit, a GMT brand 396R model PLC has been used in the system. The PLC has a modular structure and just the main unit is suitable for this application.

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.

This model has 9 digital inputs and 6 digital outputs whereas it also has analog inputs and outputs. Moreover, the GMT 396R model PLC has RS-232 and RS-485 MODBUS connection ports. Also it has relay outputs and while the program can be downloaded through Ethernet connection, the ladder program can be designed by using GMTsoft software which is free to download. This model PLC supports Windows Management Instrumentation (WMI) which allows remote connection to PLC. The photo of the GMT 396R PLC is shown in Fig 5.



Fig. 5. GMT 396R PLC

2) HMI: As the operatör panel, a 7" GMT brand TSG-070E model touch screen HMI has been used in the study. The HMI is connected with PLC through RS-232 MODBUS and programmed by PDesigner software which is freely available. This model HMI has an Ethernet port which enables Virtual Network Computing (VNC). The picture of the HMI is presented in Fig 6.



Fig. 6. GMT TSG-070E model HMI

3) Variable Frequency Driver (VFD): In the system, a three phase induction motor has been used and the speed and control of the motor has been achieved by a Variable Frequency Driver (VFD). PLC and the VFD are connected through RS-485 MODBUS connection. Start- stop and the frequency control is made by the PLC by means of the HMI. ISISO brand VFD is used in the system and its picture is presented in Fig 7.



Fig. 7. ISISO brand VFD

4) Valves: In the system, 2 piece 24VDC valves have been used to operate the pneumatic actuators. Even if the valves can be directly connected to the output pins of the PLC, additional external relays have been used to protect the pins of the PLC.

B. Operation of The System

The control of the system is managed from the HMI. There are two operation modes one of which is manual mode and the other is automatic mode. In manual mode the valves and motor have manual buttons on the screen and can be controlled manually. This mode is mainly designed for maintenance and problem detection. In automatic mode, at first the start button on the screen is pressed and the motor turns the tank at initial speed and the plastic parts produced by the injection machine are put into the tank. The low speed rotation of the tank allows more product to be added. Then, a buzzer gives a signal and the upper cover of the tank is closed by means of a valve and actuator. There are 2 sensors sensing the position of the actuator. The photo of the upper cover, actuator and the sensors are shown in Fig 8.

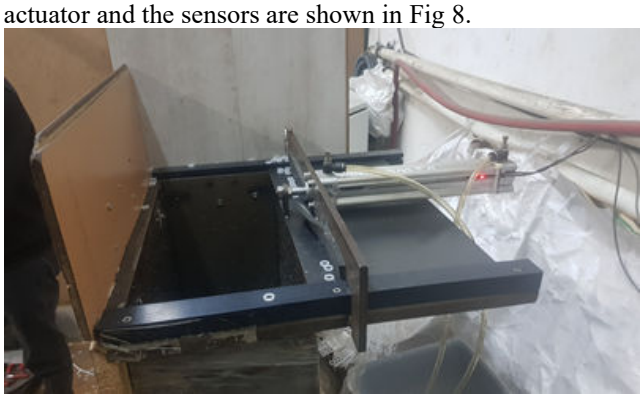


Fig. 8. A view showing the upper cover, actuator and sensors

After the cover is closed the motor turns at a higher speed adjusted through the HMI. The time of this operation is also entered from the screen. There are bars inside the tank which separate the plastic product from the sprue. The picture of the bars inside the tank is presented in Fig 9.

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.



Fig. 9. The bars inside the tank

When the time of the operation finishes, the motor slows down and the lower cover is opened. The plastic products are poured into a box and the process finishes. The picture of the plastic products separated from the sprue can be seen in Fig 10.



Fig. 10. The plastic parts separated from the sprue

C. Remote Control Protocols of the System

The designed system has some remote access protocols both used by PLC and HMI.

1) Ethernet-WMI Function: The PLC used in the system has a built-in Ethernet port and the program is written from that port. Ethernet TCP/IP connection also allows access and program the PLC from a remote location. To do this, the WMI function is used in the ladder program. If a PLC is connected to an Ethernet network, another client from a remote location can write the MAC address of the PLC and make the connection. Then the PLC can be controlled and the program inside the PLC can be modified or re-written. This remote connection saves time and labor cost since the location of the PLC and the service agent may be in a long distance or they may be in different cities or countries.

2) MODBUS Protocol: In the study PLC and HMI are connected by RS-232 MODBUS protocol. For the connection a 3 wire cable is used which consists of TX, RX and GND. PLC is connected to the COM0 port of the HMI. Besides, VFD is connected to PLC through RS-485 MODBUS protocol which requires only two wires. The same communication setup must be done both in PLC and other devices in order to communicate correctly.

3) VNC Protocol: VNC connection is made between the HMI and a remote computer, tablet or mobile phone. This communication needs Ethernet connection. HMI is connected to the internet through its Ethernet port. The remote machine has VNC Viewer software which is freely available. In VNC Viewer the IP Address, Mask and Gateway is entered and the connection between the HMI and computer is made. With this connection, both reading and writing is possible which means the data on the HMI can be seen or the buttons on the HMI can be turned ON and OFF from a remote location. A view from the HMI panel can be seen in Fig 11.

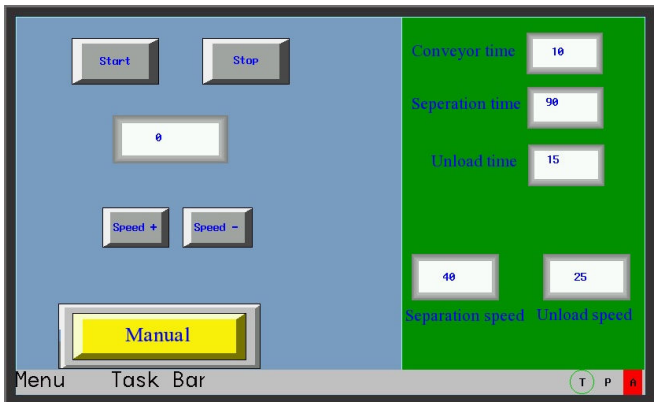


Fig. 11. A View from HMI Panel

IV. CONCLUSION

In the study, the remote connection protocols of PLC have been examined and a combined remote control and monitoring application have been done.

- The connection between PLC and HMI is made through RS-232 MODBUS
- PLC and VFD are connected through RS-485 MODBUS
- PLC is remotely controlled by WMI connection through Ethernet TCP/IP
- HMI is remotely control through VNC protocol by means of VNC Viewer software

By means of Ethernet TCP/IP connection, remote connection of PLC is available which permits reading or writing programs to a PLC from a remote location. This may save time and cost in case the machine is far away from the service agent. Besides, VNC protocol enables watching the pages of the HMI by a computer, tablet or mobile phone. The client can see the registers or states of the bits and also can control the buttons on the HMI. The advantage of VNC against SCADA is the cost of software. While VNC software is free, SCADA has a higher cost.

For future study IOT devices can be integrated by MQTT protocol and camera control can be added.

REFERENCES

[1] E. R. Alphonsus and M. O. Abdullah, “A review on the applications of programmable logic controllers (PLCs),” Renewable and Sustainable Energy Reviews, vol. 60, pp. 1185–1205, Jul. 2016, doi: 10.1016/j.rser.2016.01.025.

[2] İ. Yavuz, M. C. Mumcu, S. N. Benli, and K. Erdoğan, “Ladder Diyagrami İle Arduino Programlama,” in Abstract Book, Bandırma: Ases, Oct. 2023, p. 167.

[3] E. Aykut, K. Erdoğan, İ. Yavuz, M. C. Mumcu, and S. N. Benli, “Üç Fazli Asenkron Motorun Plc Ve Hmi İle Modbus Üzerinden Kontrolü,” in Conference Book, Bandırma: Ases, Apr. 2024, p. 102.

[4] C. Hennig, K. Kneupner, and D. Kinna, “Connecting programmable logic controllers (PLC) to control and data acquisition a comparison of

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.

the JET and Wendelstein 7-X approach," Fusion Engineering and Design, vol. 87, no. 12, pp. 1972–1976, Dec. 2012, doi: 10.1016/j.fusengdes.2012.05.009.

[5] H. Nakanishi, M. Kojima, and S. Hidekuma, "Distributed processing and network of data acquisition and diagnostics control for large helical device (LHD)," Fusion Engineering and Design, vol. 43, no. 1999, pp. 293–300.

[6] C. Huffman, "System committed memory," in Windows Performance Analysis Field Guide, Elsevier, 2015, pp. 155–179. doi: 10.1016/B978-0-12-416701-8.00006-5.

[7] G. S. O.V., A. Karthikeyan, K. Karthikeyan, P. Sanjeevikumar, S. Karapparambil Thomas, and A. Babu, "Critical review Of SCADA And PLC in smart buildings and energy sector," Energy Reports, vol. 12, pp. 1518–1530, Dec. 2024, doi: 10.1016/j.egyr.2024.07.041.

[8] G. Patti, L. Leonardi, G. Testa, and L. Lo Bello, "PrioMQTT: A prioritized version of the MQTT protocol," Computer Communications, vol. 220, pp. 43–51, Apr. 2024, doi: 10.1016/j.comcom.2024.03.018.

[9] T. Haraikawa, T. Sakamoto, T. Hase, T. Mizuno, and A. Togashi, "µVNC over PLC: a framework for GUI-based remote operation of home appliances through power-line communication," IEEE Trans. Consumer Electron., vol. 48, no. 4, pp. 1067–1074, Nov. 2003, doi: 10.1109/TCE.2003.1196440.

[10] M. Karaalp and E. Aykut, "Plc Based Conveyor System With Stepper Motor For Stampling," in Abstract Book, Izmir: IKSAD, Dec. 2024, p. 101.

[11] R. Salunke, P. Vikhe, and T. Sarode, "Implementation of Real-Time Remote Communication between Matlab/Simulink and Plc via Visualization Interface Developed With B&R Automation Studio," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, no. 9, pp. 4253–4258, 2013.

[12] O. Abrishambaf, P. Faria, and Z. Vale, "SCADA Office Building Implementation in the Context of an Aggregator," in 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), Porto: IEEE, Jul. 2018, pp. 984–989. doi: 10.1109/INDIN.2018.8471957.

[13] S. Da'na, A. Sagahyroon, A. Elrayes, A. R. Al-Ali, and R. Al-Aydi, "Development of a monitoring and control platform for PLC-based applications," Computer Standards & Interfaces, vol. 30, no. 3, pp. 157–166, Mar. 2008, doi: 10.1016/j.csi.2007.08.008.

[14] J. Możaryn, K. Bogusz, and S. Juszczyński, "Development of PLC Based Fault Isolation and Remote IIoT Monitoring of Three Tank System," IFAC-PapersOnLine, vol. 55, no. 6, pp. 175–180, 2022, doi: 10.1016/j.ifacol.2022.07.125.

[15] P. Karemore and Prashant. P. Jagtap, "A Review of IoT Based Smart Industrial System for Controlling and Monitoring," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India: IEEE, Mar. 2020, pp. 67–69. doi: 10.1109/ICCMC48092.2020.ICCMC-00012.

[16] V. F. Popescu and C. Scarlat, "Supervisory Control and Data Acquisition (SCADA) Systems for Industrial Automation and Control Systems in Industry 4.0," Land Forces Academy Review, vol. 27, no. 4, pp. 309–315, Dec. 2022, doi: 10.2478/raft-2022-0039.

[17] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state - of - the - art and open issues," Computers & Security, vol. 125, p. 103028, Feb. 2023, doi: 10.1016/j.cose.2022.103028.

[18] S. V. B. Rakas, M. D. Stojanovic, and J. D. Markovic-Petrovic, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," IEEE Access, vol. 8, pp. 93083–93108, 2020, doi: 10.1109/ACCESS.2020.2994961.

[19] P. Shukla et al., "Design and development of a MODBUS automation system for industrial applications," in 2017 6th International Conference on Computer Applications In Electrical Engineering-Recent Advances (CERA), Roorkee: IEEE, Oct. 2017, pp. 515–520. doi: 10.1109/CERA.2017.8343383.

[20] K. McLaughlin, I. Friedberg, B. Kang, P. Maynard, S. Sezer, and G. McWilliams, "Secure Communications in Smart Grid: Networking and Protocols," in Smart Grid Security, Elsevier, 2015, pp. 113–148. doi: 10.1016/B978-0-12-802122-4.00005-5.

[21] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and Implementation of a Secure Modbus Protocol," in Critical Infrastructure Protection III, vol. 311, C. Palmer and S. Shenoi, Eds., in IFIP Advances in Information and Communication Technology, vol. 311. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 83–96. doi: 10.1007/978-3-642-04798-5_6.

[22] T. Kiravuo, M. Sarela, and J. Manner, "A Survey of Ethernet LAN Security," IEEE Commun. Surv. Tutorials, vol. 15, no. 3, pp. 1477–1491, 2013, doi: 10.1109/SURV.2012.121112.00190.

[23] J. Sommer et al., "Ethernet – A Survey on its Fields of Application," IEEE Commun. Surv. Tutorials, vol. 12, no. 2, pp. 263–284, 2010, doi: 10.1109/SURV.2010.021110.00086.

[24] F. L. Lian, J. R. Moyne, and D. M. Tilbury, "Performance evaluation of control networks: Ethernet, ControlNet, and DeviceNet," IEEE Control Syst., vol. 21, no. 1, pp. 66–83, Feb. 2001, doi: 10.1109/37.898793.

[25] G. Beier, S. Niehoff, and B. Xue, "More Sustainability in Industry through Industrial Internet of Things?," Applied Sciences, vol. 8, no. 2, p. 219, Jan. 2018, doi: 10.3390/app8020219.

[26] D. Cahyagi, I. R. Kusuma, and A. Kurniawan, "Design HMI (Human Machine Interface) for Process Control System of Main Diesel Engine Fuel System," AMM, vol. 874, pp. 88–95, Jan. 2018, doi: 10.4028/www.scientific.net/AMM.874.88.

[27] P. Pauwels et al., "A semantic rule checking environment for building performance checking," Automation in Construction, vol. 20, no. 5, pp. 506–518, Aug. 2011, doi: 10.1016/j.autcon.2010.11.017.

[28] N. Saha, P. Paul, K. Ji, and R. Harik, "Performance evaluation framework of MQTT client libraries for IoT applications in manufacturing," Manufacturing Letters, vol. 41, pp. 1237–1245, Oct. 2024, doi: 10.1016/j.mfglet.2024.09.150.

[29] C. Gültunca and A. Zaim, "Examination And Comparison Of The Communication Protocols On The Application Layer In IOT," Istanbul Commerce University, Journal of Science, vol. 17, no. 33, pp. 41–50, Spring 2018.

[30] T. Tan-atichat and J. Pasquale, "VNC in High-Latency Environments and Techniques for Improvement," in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA: IEEE, Dec. 2010, pp. 1–5. doi: 10.1109/GLOCOM.2010.5683953.

Authorized licensed use limited to: Istanbul Gelism Univ. Downloaded on August 13,2025 at 08:20:52 UTC from IEEE Xplore. Restrictions apply.