Journal of Automation, Electronics and Electrical Engineering

THE USE OF THE INDUSTRIAL MODBUS NETWORK IN CONTROL AND MEASUREMENT SYSTEMS OF LABORATORY STATIONS

Roman KWIECIEŃ [1*]

[1]Casimir Pulaski Radom University, Faculty of Transport and Electrical Engineering and Computer Science, Malczewskiego 29, 26-600 Radom, Poland, r.kwiecien@uthrad.pl

DOI: https://doi.org/10.24136/jaeee.2025.016

Abstract – This article presents the potential of using the Modbus TCP industrial computer network in measurement tests of electrical machines and devices used in laboratory stations. The Modbus interface is the primary communication channel for most measuring equipment for reading electrical parameters, such as current, voltage, and power, as well as mechanical parameters, such as rotational speed and torque at the shaft of the tested machine. The measurement system is designed to acquire data in steady states of the electric drive assembly, where the measured parameters indicate approximately the same value. The article presents the tasks and role of the measurement system in a modern approach to collecting and processing measurement data using intelligent communication devices.

Keywords – industrial computer networks, Modbus TCP, laboratory measurements, measurement system design.

INTRODUCTION

Today, computer networks are widely used for communication connections between computer units. They constitute an excellent transmission medium for transferring large amounts of data. The most widespread network is Ethernet, which is the most popular standard in LANs (Local Area Networks) [8]. Ethernet technology was developed by Robert Metcalfe at Xerox PARC and published in 1976. It includes a specification in the IEEE1 802 standard, in which the data link layer specifies cable access using the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) algorithm.

Simultaneously, with the development of local networks, industrial computer networks also developed. One of the first such networks was Modbus, based on the RS-485 interface [1, 11]. Modbus was developed by Modicon and soon became a standard adopted by most well-known manufacturers of industrial controllers for asynchronous, character-based information exchange between automation devices and control and measurement equipment.

Technological advancements have led to the development of industrial computer networks in terms of data transfer speed, information security, and network organization. This has led to the development of various network designs, such as Profibus, CAN, EtherCat, Ethernet Powerlink, and others [1]. Network organization defines information transfer management and priority algorithms for transmitting data packets onto a common communication channel. Some of these network types utilize a bus topology, while others are based on the Ethernet physical layer due to integration with higher-level measurement systems. While EtherCat and Ethernet Powerlink networks were developed as separate projects, Profinet and Modbus TCP networks were developed by transferring the Profibus and Modbus physical layer to an Ethernet interface [12]. This allows data packet transmission in a Modbus network to be converted to data packets using the TCP/IP protocols.

Most manufacturers of control and measurement devices incorporate a Modbus communication interface into their products. The cost of such an interface is low, so the price of the devices allows for the creation of a measurement system in laboratory stations for testing various operating states of electrical machines and devices [5, 6]. This includes measurements of DC and AC current and voltage, power, energy, rotational speed, and torque on the machine shaft. This method allows for the creation of a computer-based measurement system operating in a local area network (LAN) that will read data packets from the Modbus network via Modbus/TCP converters. This measurement system will include a proprietary "Modbus HTTP" server, managed by any web browser using the HTTP protocol. This server has a configuration interface for manually or automatically saving measurement data locally on the hard drive or remotely to an email inbox.

1 MEASURING SYSTEM INFRASTRUCTURE MODEL

In the infrastructure model of a measurement system using industrial computer networks, three layers can be distinguished (**Fig. 1.1**) [1, 2, 3]:

- Process layer – this layer consists of control and measurement devices, including a Programmable Logic Controller (PLC), sensors, actuators, and other devices operating in a local Fieldbus – Modbus computer network. The primary task of this layer is to control devices to perform laboratory research tasks and to collect information. Information obtained from these devices is stored in a local database, which constitutes archived data.
- The Operations – Layer is responsible for executing operational plans based on the measurement server's configuration data. This layer also includes various visualization and supervision systems, including Supervisory Control and Data Acquisition/Human Machine Interface (SCADA/HMI) and Manufacturing Execution Systems (MES).
- Business layer – the primary role is played by supervisory units, whose purpose is to manage the measurement system. This layer is where measurement decisions are made and visualization is performed based on data collected in the server's local database. For dissemination of measurements, an option is available to send data to an email address.

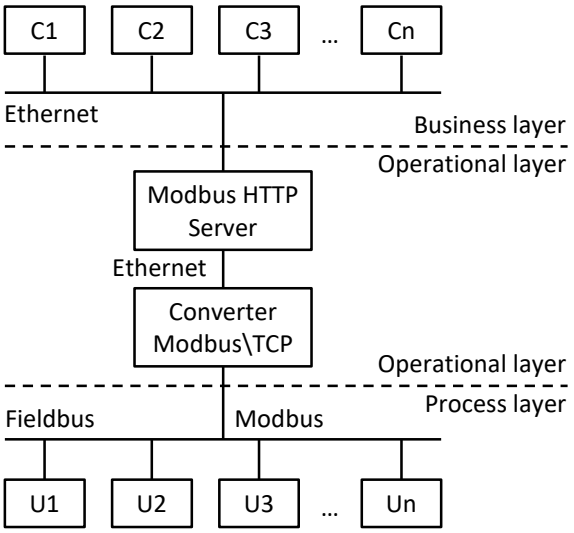


Fig. 1.1 Infrastructure model of the measurement system using the Modbus industrial computer network; U1÷Un – control and measurement devices; C1÷Cn – measurement system clients

The proposed measurement system model utilizes the industrial Modbus TCP network in the process layer. This network doesn't offer the highest data transfer rates, but its interfaces are used in various measuring equipment and actuators. Therefore, it will serve as the primary communication channel for steady-state laboratory measurements.

2 MODBUS TCP

The Modbus network was developed by Modicon and soon became a standard adopted by most well-known manufacturers of industrial controllers for asynchronous, character-based information exchange between automation devices and control and measurement equipment. It is based on a bus topology. (**Fig. 2.1**). Slave nodes (CN) are controlled by master nodes (PN). The physical layer of the Modbus OSI model uses a hardware RS-485 interface. In the linear layer, the algorithm in the link access sublayer is polling. In this algorithm, the master node sends a message containing data or a data request to the slave node. After transmitting a frame containing information to the recipient in connection-oriented communication, the master node waits a certain time for a response in the form of an acknowledgment of message receipt or a data datagram. If this time is exceeded, the same message is retransmitted. If a slave node fails to respond three times, this may be due to a failure (e.g., a power outage) or a bus failure. Depending on the network organization, the master node may exclude the slave node from the query flow or send messages sporadically, as the node may function properly after some time (the failure will be repaired). When the network and nodes are functioning correctly, immediately after receiving the query, the slave node sends back a response containing data or information about its absence [1, 7, 11].

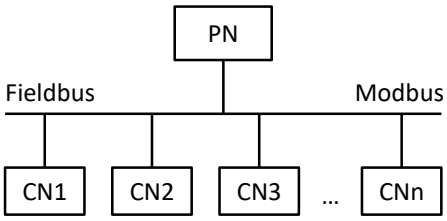


Fig. 2.1 Diagram of a Modbus industrial computer network with a bus topology

Messages sent in the Modbus network are in the form of a communication protocol in two modes: ASCII and RTU. (**Fig. 2.2**). In ASCII mode, the SM and EM fields constitute the beginning and end of the datagram frame and are respectively: the ":" character and the "CR LF" characters, while the remaining fields are two bytes terminated with the LRC checksum. For RTU mode, the SM and EM fields are transmission pauses of four times the duration of one bit, while the remaining datagram fields are one byte, and the checksum is the CRC16 algorithm.

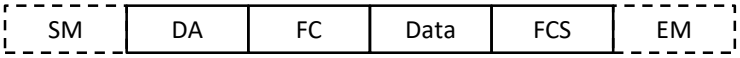


Fig. 2.2 Modbus communication protocol format; SM – Start Marker; DA – Address; FC – Function; FCS – Checksum; EM – End Marker

One of the varieties of the Modbus communication protocol is Modicon, created in 1980. It consists of fields such as the destination node address DA and source node address SA, and the function FC (**Tab. 2.1**), register address REG, length LE of the data field, Data1 and Data2 data and the FCS field of the CRC16 checksum (**Fig. 2.3**).

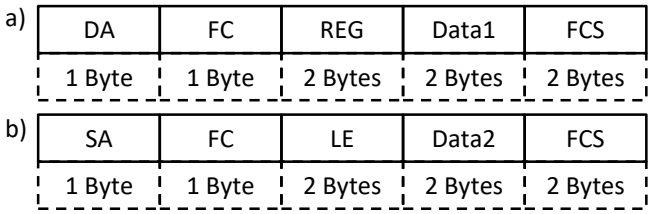


Fig. 2.3 Modicon communication protocol format for query (a) and answer (b); DA – Destination Address; SA – Source Address; FC – Function; REG – Register; LE – Length; FCS – Checksum

Tab. 2.1 Function value of Modicon protocol

Function value	Description	Function value	Description
1	Read binary	5	Write binary
2	Read binary	6	Write binary 16-bits
3	Read binary 16- bits	15	Write binary
4	Read binary 16- bits	16	Write binary 16-bits
7	Read flags	21	Write file 16-bits
20	Read file 16- bits		

Modbus TCP is built from a datagram on the TCP/IP protocol layer (**Fig. 2.4**) [12]. Modbus data is encapsulated from the Ethernet layer through the IP and TCP layers. This data takes the form of a communication protocol whose fields represent (**Fig. 2.5**):

- Transaction ID – next transaction number,
- Protocol ID – communication protocol identifier, for Modbus it is equal to 0,
- Length – data field length,
- Unit ID – communication device address,
- Function Code – task execution function.

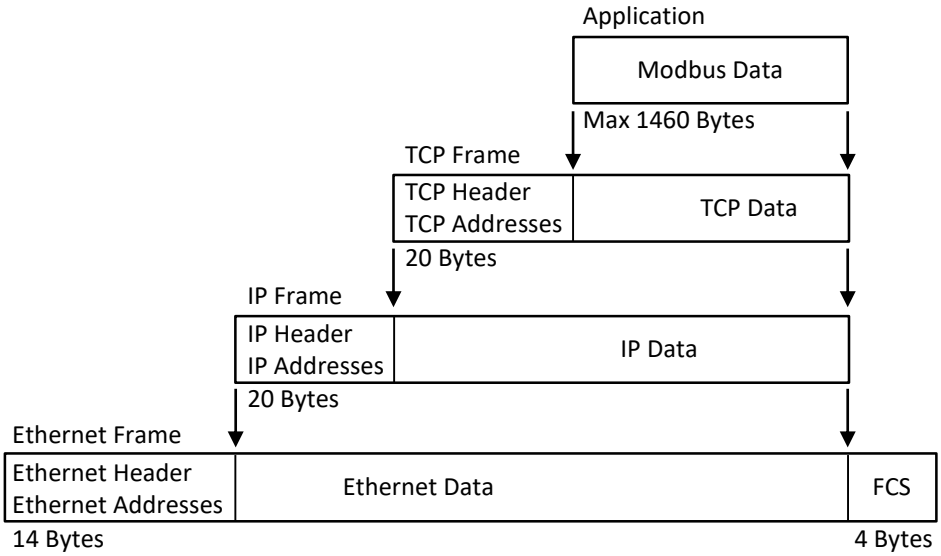


Fig. 2.4 Construction of a TCP/IP-Ethernet data packet for Modbus; FCS – Ethernet Checksum

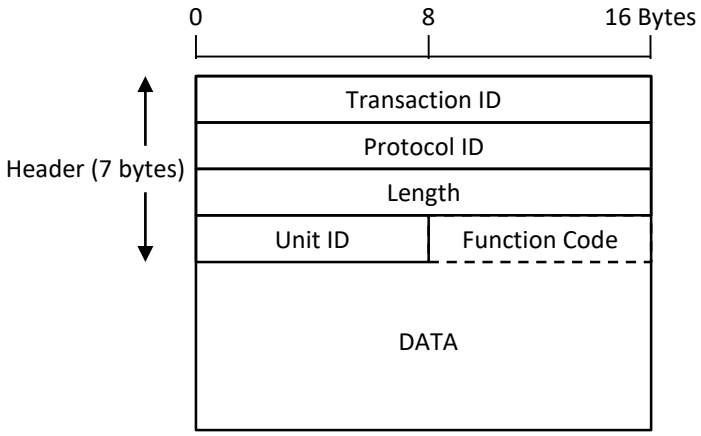


Fig. 2.5 Modbus TCP/IP Application Data Unit

The Modbus TCP communication protocol is similar to a Modbus datagram with an RS-485 interface. It also has a header that specifies the data field length and the device address, which is also the beginning of the Modbus datagram (**Fig. 2.3**). This protocol does not have a checksum; it is calculated in the Modbus\TCP converter. This fact causes inconvenience in communication with devices that do not have the correct checksum. An example of a transaction frame with a device is shown in **Tab. 2.2**.

Tab. 2.2 Query and answer in Modicon protocol in HEX values; DA = 64(hex) = 100(dec); FC = 03(hex); REG = 17C4(hex) = 6084(dec); Data1 = 02(hex); Data2 = 00004268(hex); LE = 04(hex)

Query	18 02 00 00 00 06 64 03 17 C4 00 02
Answer	18 02 00 00 00 07 64 03 04 00 00 42 68

In a Modbus TCP network, converters such as the "Ethernet TO RS232/422/485 Serial Converter MODEL USR-N510" or the "Waveshare RS485 TO POE ETH" are used to convert RS-485/TCP signals. Using the converter's IP address, it is possible to configure it using a dedicated computer application or via an HTTP interface on a website. The main settings include serial communication parameters for control and measurement devices (Baud Rate, Data Bit, Parity, Stop Bit, Serial Mode, and Flow Control) and TCP/IP network socket parameters (IP Address, Work Mode: TCP Server/Modbus TCP, and Local Port Number: 502).

3 COMPUTER MEASUREMENT SYSTEM

The computer-based measurement system is a proprietary design, primarily consisting of a "Modbus HTTP" server. Two communication connections are established during its operation [4, 9, 10]:

- TCP\IP – in this layer, control and measurement devices are periodically polled to obtain the current signal value or to perform a specific task in the laboratory. The polling process

is performed according to an algorithm (**Fig. 3.1**), in which the server periodically formulates an appropriate datagram and sends it to the device on the TCP network. After an appropriate response time, the data from the devices is updated in the server's tag list.

- HTTP – connection used to execute orders from web browsers. Using queries directed to the server, current measurement values can be retrieved. (**Fig. 3.2**).

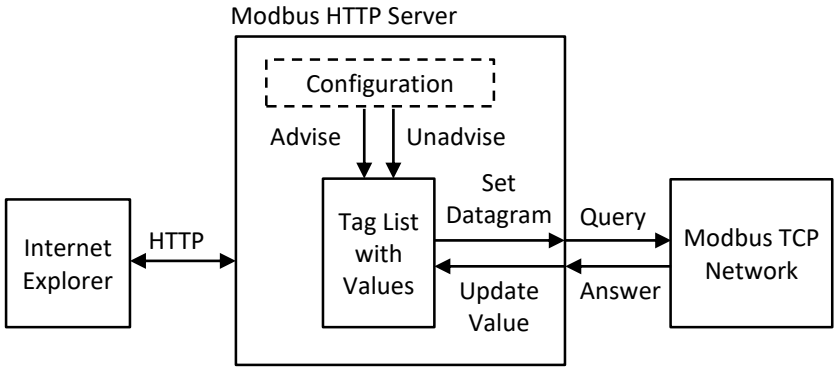
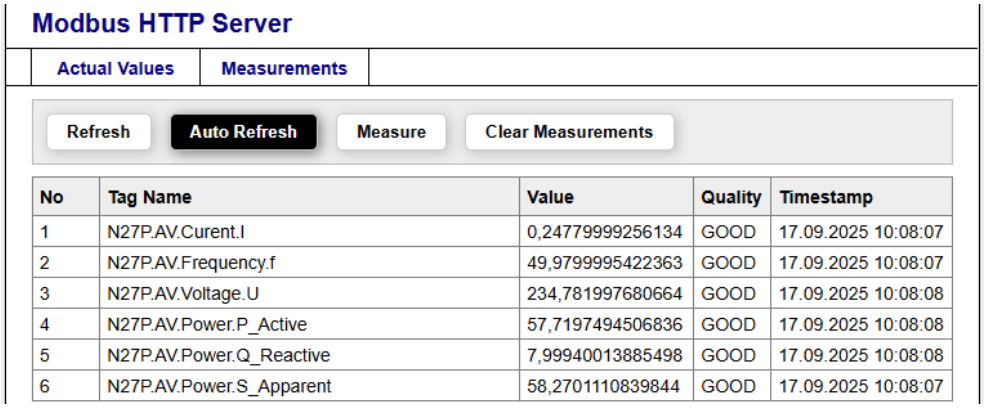


Fig. 3.1 Architecture of Modbus HTTP Server



No	Tag Name	Value	Quality	Timestamp
1	N27P.AV.Curent.I	0,24779999256134	GOOD	17.09.2025 10:08:07
2	N27P.AV.Frequency.f	49,9799995422363	GOOD	17.09.2025 10:08:07
3	N27P.AV.Voltage.U	234,781997680664	GOOD	17.09.2025 10:08:08
4	N27P.AV.Power.P_Active	57,7197494506836	GOOD	17.09.2025 10:08:08
5	N27P.AV.Power.Q_Reactive	7,99940013885498	GOOD	17.09.2025 10:08:08
6	N27P.AV.Power.S_Apparent	58,2701110839844	GOOD	17.09.2025 10:08:07

Fig. 3.2 View of data read in a web browser from the „Modbus http" server at: http://localhost:55123/

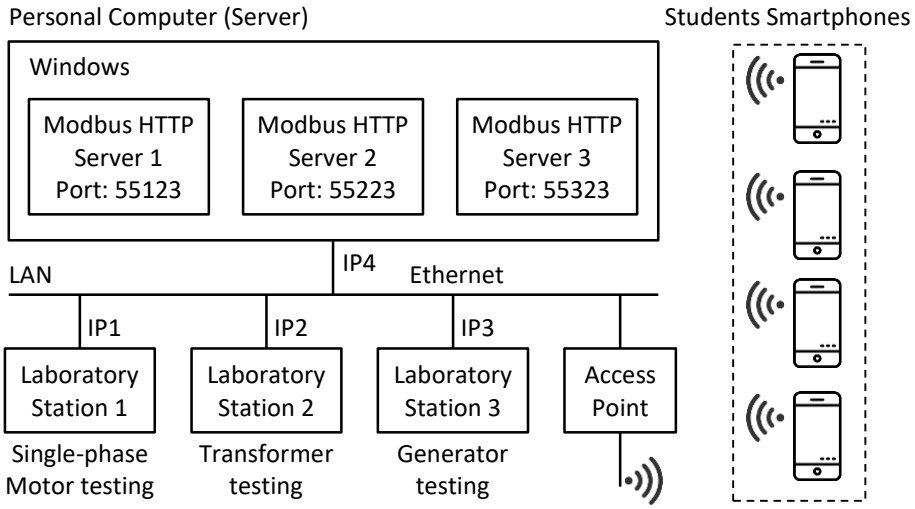


Fig. 3.3 Organizational diagram of laboratory stations connected in LAN

With a "Modbus HTTP" server, it is possible to build a network of laboratory stations operating in LAN connected to a network switch with Wi-Fi (**Fig. 3.3**). A server running on different TCP ports is replicated on a designated computer unit. Each server connects to a designated laboratory station, e.g., Single-phase Motor, Transformer, and Generator, via its IP address. Each laboratory station can be accessed via smartphones with a web browser by entering the IP4 address of the "Modbus HTTP" server and the port of the appropriate station, e.g., http://10.100.20.150:55123. The web browser, as a client of the measurement system, has options for:

- Cyclic refreshing of current measurements from the laboratory station,
- Saving current measurements to the server database,
- Clearing archived measurements,
- Viewing archived measurements,
- Sending measurement data to a defined e-mail address.

4 CONCLUSIONS

This article presents a proprietary computer-based measurement system consisting of a "Modbus HTTP" server. Its main concept is the ability to transfer measurement data from laboratory stations to smartphones. This is achieved using the widely known HTTP and HTML communication standards, as well as AJAX (Asynchronous JavaScript and XML) technology. These technologies allow students to save their measurement data to their own email account and process them electronically for laboratory report preparation..

The proposed communication model is based on the Modbus TCP industrial computer network. This network provides a good link between the commonly used Ethernet LAN and the classic Modbus network with an RS-485 interface. Despite the many advantages of using existing LANs in offices, factories, workplaces, and laboratories, certain drawbacks arise, primarily related

to Modbus/TCP converters. They are programmed for one or more devices with the same data transmission parameters. If one device has parameters assigned without the ability to modify them, communication with it will not occur until the other devices have the same transmission parameters. It is obvious that a separate Modbus/TCP converter can be used for a specific control and measurement device, but this complicates the workflow of the "Modbus HTTP" server.

In the computer-based measurement system, access to the "Modbus HTTP" server is via a LAN. In this case, the server can be made available in a global MAN and WAN network via the HTTP protocol. With this architecture, the system can be used in e-learning processes. This would be a significant breakthrough in conducting laboratory research remotely, without the need to be present at the university. Students can register from home via a web browser and complete a laboratory exercise within a time window assigned by the measurement system.

BIBLIOGRAPHY

[1] Kwiecień R.: Komputerowe systemy automatyki przemysłowej, Computer systems for industrial automation, ISBN: 9788324651429/978-83-246-5142-9, Pub. Helion, Gliwice (2013)
[2] Kwiecień R.: Technologia OPC jednorodnym medium w procesie dostarczania informacji w logistycznym systemie komputerowym przedsiębiorstwa, OPC technology as homogeneous medium in the process of providing information in the logistics enterprise computing system, LogiTrans, Szczyrk, 7-10 IV (2014), ISBN 978-83-7351-424-9, Logistyka 3/2014, ISSN 1231-5478
[3] Iwanitz F., Lange J.: OLE for Process Control. Fundamentals, Implementation and Applications, Huthig Verlag heiderberg, RFN, (2001)
[4] Michalski A., Makowski Ł.: Praktyczne użycie XML w rozproszonych systemach pomiarowo-sterujących; Przegląd Elektrotechniczny 05/(2008) Str. 255-258
[5] Majkowski A., Rak R.: Systemy pomiarowe, Politechnika Warszawska, Ośrodek Kształcenia na Odległość OKNO, https://esezam.okno.pw.edu.pl/ pluginfile.php/1417/ mod_resource/ content/1/Systemy%20pomiarowe.pdf (2018)
[6] Biernat A., Przyborowski W.: System pomiarowy do wszechstronnych badań maszyn elektrycznych, Biuletyn WAT, Vol. LXIX, Nr 1, (2020)
[7] Mielczarek W., Szeregowe interfejsy cyfrowe, HELION, Gliwice (1993)
[8] Comer D., Sieci komputerowe TCP/IP (tom 1), WNT, Warszawa (2001)
[9] Chrupek R., Akwizycja Danych w systemach przemysłowych, „Napędy i Sterowanie", nr 4, kwiecień (2008)
[10] Kwiecień R., Sterowanie urządzeniami przemysłowymi, Prace naukowe ELEKTRYKA NR 1(19), Radom, s. 143–148, ISSN 1507-3025, (2005)
[11] Modbus: https://www.modbus.org; 17.09.2025
[12] Modbus TCP: https://www.waveshare.com/wiki/Modbus_Protocol_Specification; 17.09.2025