

Modbus/TCP - Client

PLC500, PLC500ED, PLC500MC
PLC410

Application Note



Application Note

PLC410, PLC500, PLC500ED, PLC500MC

Document: 10010165984

Revision: 01

Publication Date: 12/2024

SUMMARY OF REVISIONS

The information below describes the reviews made in this manual.

Version	Revision	Description
1.4.0	R01	Update of information and inclusion of PLC models PLC410, PLC500ED, and PLC500MC.
1.0.0	R00	First edition.

CONTENTS

1	INTRODUCTION	1-1
1.1	TERMS AND DEFINITIONS USED	1-1
1.2	NUMERIC REPRESENTATION	1-1
1.3	MODBUS/TCP DOCUMENTS	1-2
1.4	IMPORTANT NOTICE ABOUT CYBERSECURITY AND COMMUNICATIONS	1-2
1.5	TRADEMARKS	1-2
2	ETHERNET INTERFACE	2-1
2.1	INDICATION LEDS	2-1
2.2	MODBUS/TCP NETWORK INSTALLATION	2-2
2.3	MODBUS/TCP NETWORK TOPOLOGIES	2-3
2.4	EXAMPLE MODBUS/TCP NETWORK ARCHITECTURE	2-4
3	PROJECT IN CODESYS	3-1
3.1	CREATING THE PROJECT	3-1
3.2	ADDING CLIENT DEVICE	3-2
3.3	ADDING SERVER DEVICE	3-3
4	CONFIGURATION OF MODBUS/TCP	4-1
4.1	ETHERNET INTERFACE CONFIGURATION	4-1
4.2	NETWORK CONFIGURATION	4-1
4.3	MODBUS CHANNEL CONFIGURATION	4-3
4.4	CONFIGURATION OF MODBUS RTU GATEWAY READING	4-6
5	MONITORING	5-1
5.1	MONITORING VARIABLES	5-1
5.2	COMMUNICATION ERRORS	5-2

1 INTRODUCTION

This Application Note aims to assist in the use of the **Modbus/TCP** protocol on WEG PLCs, models PLC410, PLC500, PLC500ED, and PLC500MC. Throughout this document, the PLC500 is used as an example. However, the information presented is applicable to the other PLC models mentioned earlier.

This document provides information about the Modbus/TCP protocol, a description of the Ethernet interface, installation recommendations, possible network topologies with the protocol, and a guide to establish Modbus/TCP communication between the PLC500 (client) and the PLC300 (server) in **CODESYS**.



NOTE!

In the official technical documentation of the Modbus/TCP protocol, the terms “master” and “slave” have been replaced with “client” and “server”. This application note uses the new terminology.

For more information about the hardware, interfaces, and communication protocols, refer to the User Manual of the respective product, available on the [WEG](#) website. For a more in-depth and detailed description of the operation of the Modbus/TCP network, access the online help at [CODESYS Online Help](#).



ATTENTION!

This application note is intended for professionals trained in industrial networks. The installation and configuration of the devices should be performed according to the manufacturer's manual.



NOTE!

This application note is intended for the CODESYS programming tool. It is recommended to use **CODESYS V3.5 SP19** or later. It is also recommended to use the latest available version of the Modbus/TCP network configuration libraries.

1.1 TERMS AND DEFINITIONS USED

CODESYS: PLC500 programming software. A programming platform that allows the development, configuration, and monitoring of solutions for industrial automation and system integration.

DHCP: from English “*Dynamic Host Configuration Protocol*”, a network management protocol that automatically assigns IP addresses and other configuration information to devices connected to a network.

Gateway: A device that connects different communication protocols, enabling data exchange between distinct devices and systems, ensuring interoperability and efficiency in process management.

Mbps: Megabits per second.

min: minute.

ms: millisecond = 0.001 seconds.

s: second.

USB: from English “*Universal Serial Bus*”, a type of serial communication interface designed to operate according to the “*Plug and Play*” concept.

1.2 NUMERIC REPRESENTATION

Decimal numbers are represented by digits without a prefix. Hexadecimal numbers are represented with the prefix ‘0x’.

1.3 MODBUS/TCP DOCUMENTS

It is recommended to consult the documents related to the Modbus/TCP network presented in [Table 1.1 on page 1-2](#).

Table 1.1: Reference Documents.

Document	Version	Source
MODBUS Application Protocol Specification, December 28th 2006	V1.1b	MODBUS.ORG
MODBUS Messaging On TCP/IP Implementation Guide, October 24th 2006	V1.0b	MODBUS.ORG

1.4 IMPORTANT NOTICE ABOUT CYBERSECURITY AND COMMUNICATIONS

The WEG PLCs, models PLC410, PLC500, PLC500ED, and PLC500MC, have the capability to connect and exchange information through networks and communication protocols. Although they have been designed and tested to ensure proper functioning with other automation systems using the protocols mentioned in this manual, it is essential for the customer to understand the responsibilities associated with information and cybersecurity when using this equipment.

Therefore, it is the customer's sole responsibility to adopt defense-in-depth strategies and implement policies and measures to ensure the security of the system as a whole, including communications sent and received by the equipment. These measures include, but are not limited to, the installation of firewalls, antivirus and anti-malware programs, data encryption, authentication control, and physical access control for users.

WEG and its affiliates are not responsible for damages or losses resulting from cybersecurity breaches, including but not limited to unauthorized access, intrusion, data or information leakage and/or theft, denial of service, or any other form of security violation. The use of this product in conditions for which it was not specifically designed is not recommended and may result in damage to the product, the network, and the automation system.

In this regard, it is essential that the customer understands that external interventions through third-party programs, such as sniffers or programs with similar actions, have the potential to cause interruptions or restrictions in the functionality of the equipment.

1.5 TRADEMARKS

All other registered trademarks are the property of their respective owners.

2 ETHERNET INTERFACE

The Modbus/TCP communication is performed through Ethernet connections, as shown in [Figure 2.1 on page 2-1](#) for the PLC500 and PLC410. Initially, each Ethernet port has the IP address indicated in [Table 2.1 on page 2-1](#), which can be changed at any time through the CODESYS software.

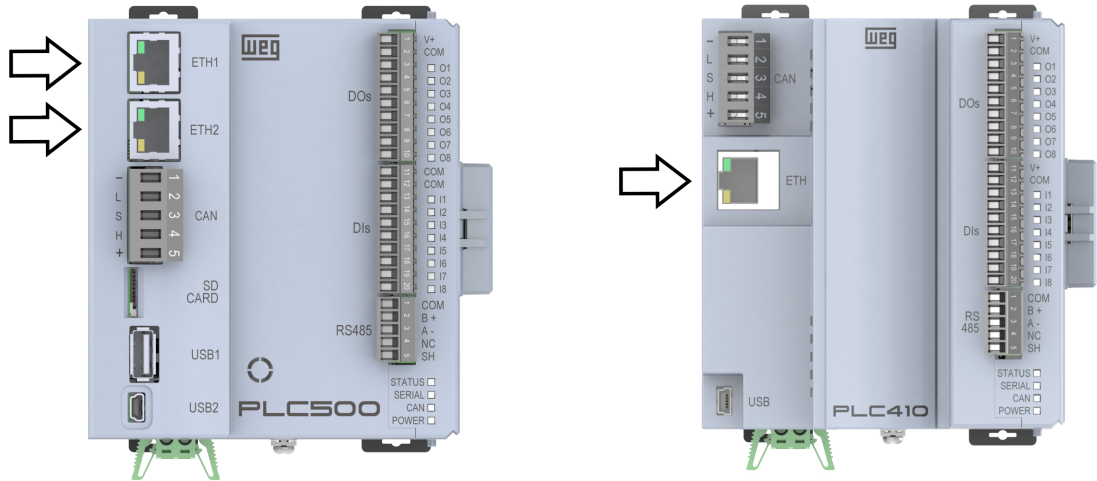


Figure 2.1: Indication of Ethernet connections on PLC500 and PLC410.

Table 2.1: Default IP addresses for Ethernet ports.

Ethernet (PLC410)	Ethernet (PLC500)	Default IP address
ETH	ETH1	192.168.1.10
-	ETH2	192.168.2.10

The pinout of the connector follows the Ethernet 1000BASE-TX standard. The Ethernet interface of the PLC410 supports speeds of up to 100 Mbps, while the Ethernet interfaces of the PLC500 support up to 1000 Mbps.

The PLC500, PLC500ED, and PLC500MC have two Ethernet interfaces, which can be configured in **Independent** mode, where the interfaces operate with different IPs, or in **Switch** mode, where the interfaces share the same IP address.

The interface is compatible with various communication protocols, including Modbus/TCP, and can be used simultaneously for multiple Ethernet-based protocols. For instructions on how to configure these additional networks, refer to the product Application Notes available on the [WEG](#) website.

2.1 INDICATION LEDS

The Ethernet ports have LEDs to indicate speed and link/activity status, as shown in [Figure 2.2 on page 2-1](#). These LEDs follow the behavior described in [Table 2.2 on page 2-2](#) and [Table 2.3 on page 2-2](#).

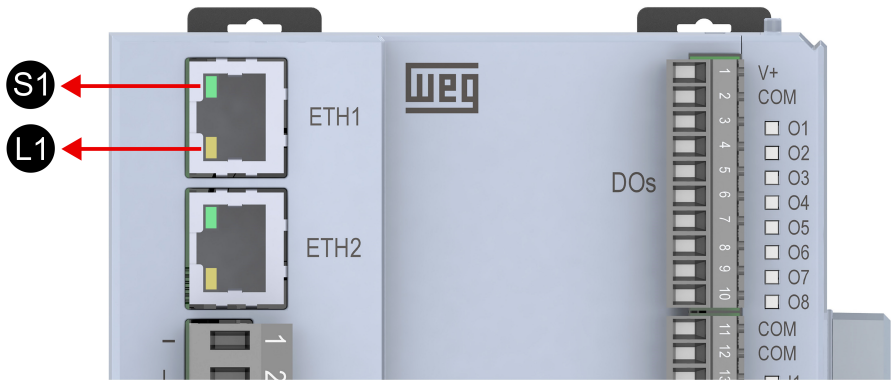


Figure 2.2: Speed and link/activity LEDs of the PLC500 Ethernet interface.

Table 2.2: LED S1 - Speed.

State	Description
Off	Device off or 10 Mbps link
Green, solid	100 Mbps link

Table 2.3: LED L1 - Link/Activity.

State	Description
Off	Device off or no link
Amber, solid	Link present with no network activity
Amber, blinking	Link present with network activity

2.2 MODBUS/TCP NETWORK INSTALLATION

The Modbus/TCP network, like many industrial communication networks, requires certain precautions to be taken due to its frequent use in harsh environments with high exposure to electromagnetic interference, in order to ensure a low error rate during operation.



ATTENTION!

It is recommended to use passive components (cables, connectors, switches, hubs) certified for industrial applications.

The recommended characteristics for the cable used in the installation are:

- Ethernet standard cable, 1000Base-TX, CAT 5e or higher.
- Shielded cable.
- Maximum length of 100 m for connection between devices.

An appropriate grounding system connection is essential to reduce electromagnetic interference problems in industrial environments. It is important to avoid connecting the cable to multiple grounding points, especially where there are grounds with different voltage potentials. Additionally, it is recommended that signal and communication cables be installed in dedicated routes, away from power cables.



DANGER!

Defective grounding installations can lead to death and malfunction of the Modbus/TCP network.

2.3 MODBUS/TCP NETWORK TOPOLOGIES

The network topologies in a Modbus/TCP system can vary according to the project requirements and the installation architecture. Notable topologies include the star topology, where a central switch connects all devices, as illustrated in [Figure 2.3 on page 2-3](#); the daisy-chain topology, which allows devices to be connected in sequence, as shown in [Figure 2.4 on page 2-3](#); and the combination of both topologies, as exemplified in [Figure 2.5 on page 2-3](#).

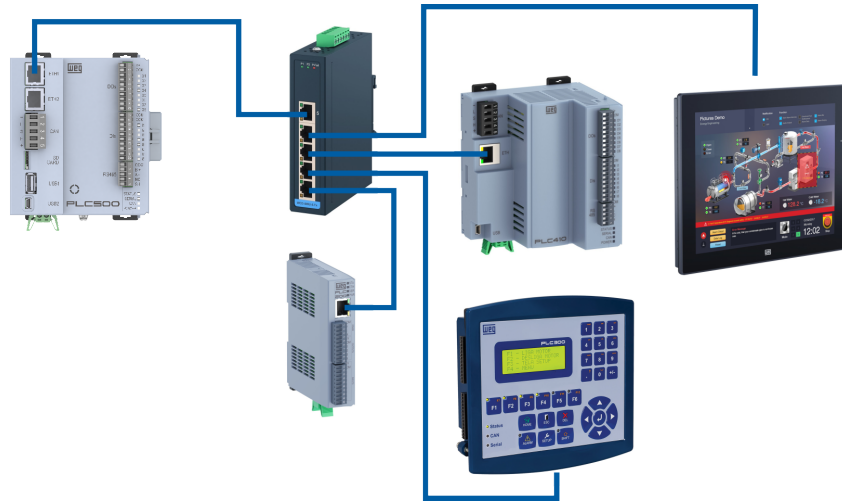


Figure 2.3: Modbus/TCP star topology.



Figure 2.4: Modbus/TCP daisy-chain topology.

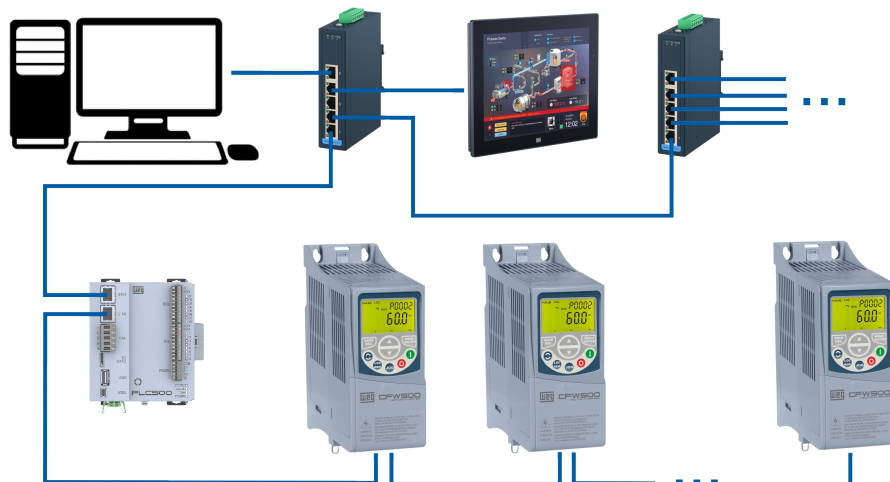


Figure 2.5: Modbus/TCP star and daisy-chain topology.

2.4 EXAMPLE MODBUS/TCP NETWORK ARCHITECTURE

This application note presents an example where a PLC500 acts as the client and a PLC300 as the server. [Figure 2.6 on page 2-4](#) illustrates the components and architecture of the Modbus/TCP network. In this scenario, a computer programs the PLC500 via the Ethernet interface, and the communication between the two devices is established through the same network medium.

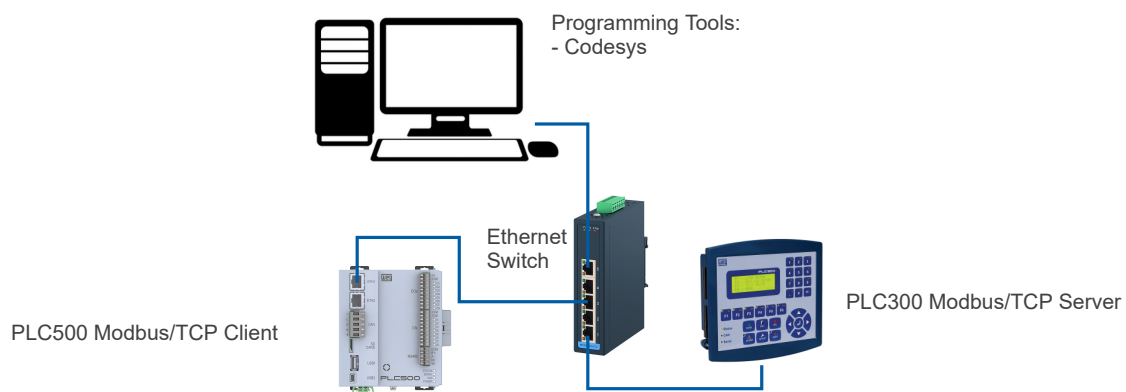


Figure 2.6: Example Modbus/TCP network components.

3 PROJECT IN CODESYS

This chapter presents the steps on how to create a project and add the client and server devices of the Modbus/TCP network in CODESYS.

3.1 CREATING THE PROJECT

For Modbus/TCP network configurations and settings, you should first create the project and include the PLC500 programmable controller. In CODESYS software, create a new project using the **Standard project** template, choose the directory and the application name. Then, select the PLC500 device and the desired programming language, as shown in [Figure 3.1 on page 3-1](#).

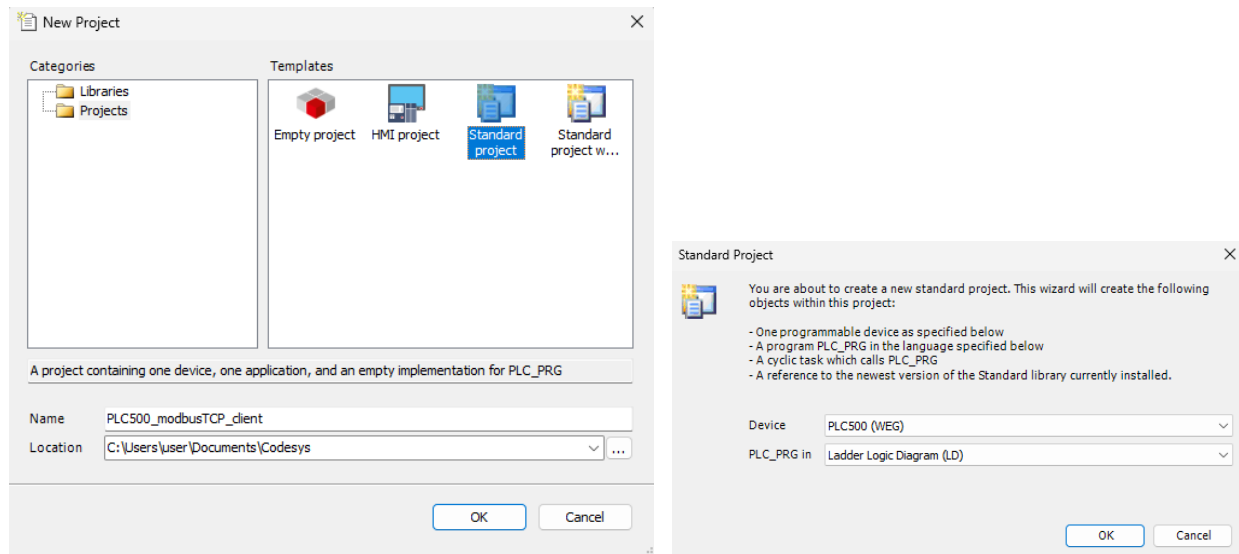


Figure 3.1: Creating the project in CODESYS.



NOTE!

If the PLC410, PLC500, PLC500ED, or PLC500MC device is not yet available in the CODESYS options, you must download and install the configuration file. Check the **Product Manual** available on the [WEG](#) website for the necessary steps and configurations.

With the PLC500 device selected, this will result in the project tree, as shown in [Figure 3.2 on page 3-1](#).

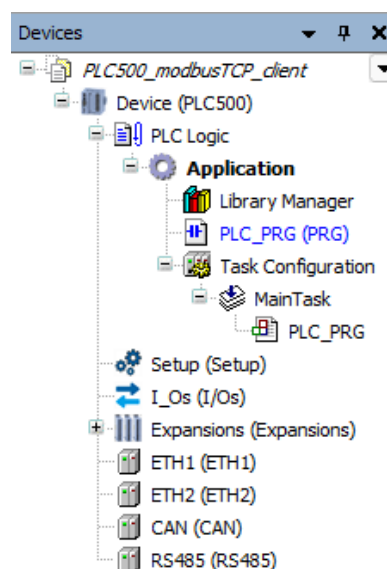


Figure 3.2: Initial project tree of the PLC500.

3.2 ADDING CLIENT DEVICE

In the next step, the **Modbus_TCP_Client** device must be added. Right-click on the network icon **ETH1** and select **Add Device**. A new window will open. Expand the **Modbus** and **Modbus TCP Master** icons using the **+** symbol until the **Modbus TCP Client** device appears, as shown in [Figure 3.3 on page 3-2](#). With the device selected, click on **Add Device**.

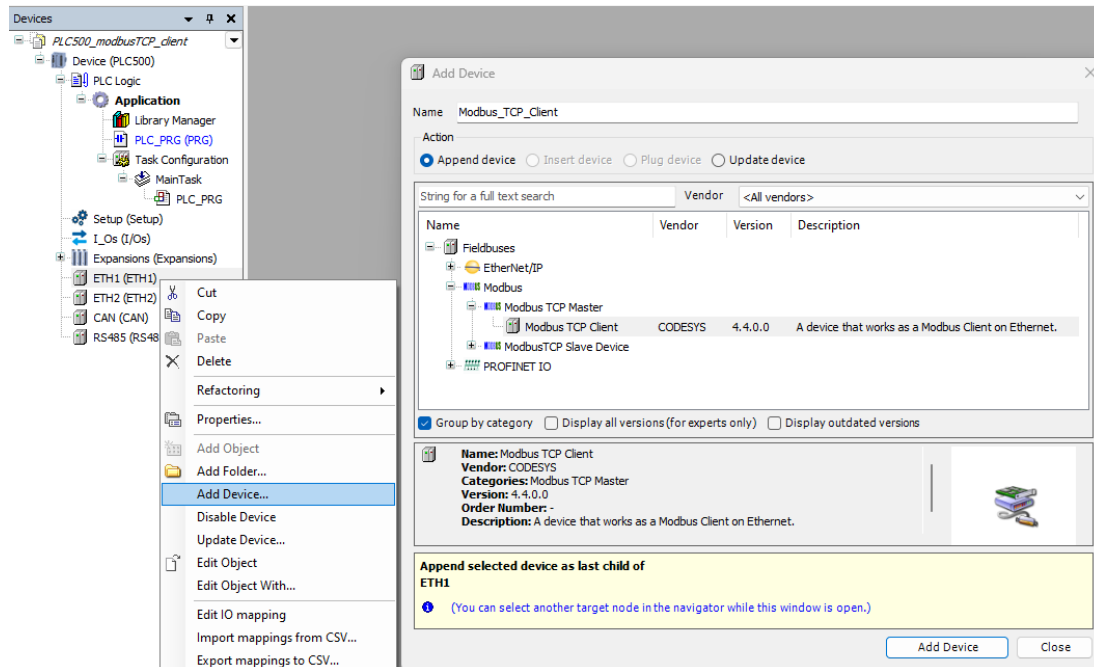


Figure 3.3: Adding Modbus TCP Client device.

The device will be added to the project tree just below the **ETH1** interface, as shown in [Figure 3.4 on page 3-2](#).

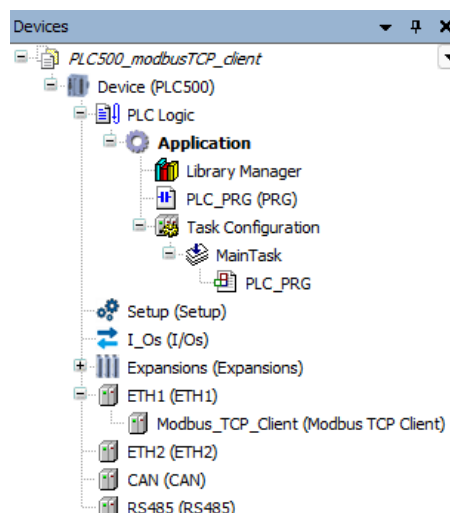


Figure 3.4: Modbus_TCP_Client device added to the project tree.

3.3 ADDING SERVER DEVICE

By right-clicking on the **Modbus_TCP_Client** icon, the Modbus/TCP server device **Modbus_TCP_Server** is added to the Modbus/TCP network following the same steps as before. [Figure 3.5 on page 3-3](#) shows the steps for this configuration.

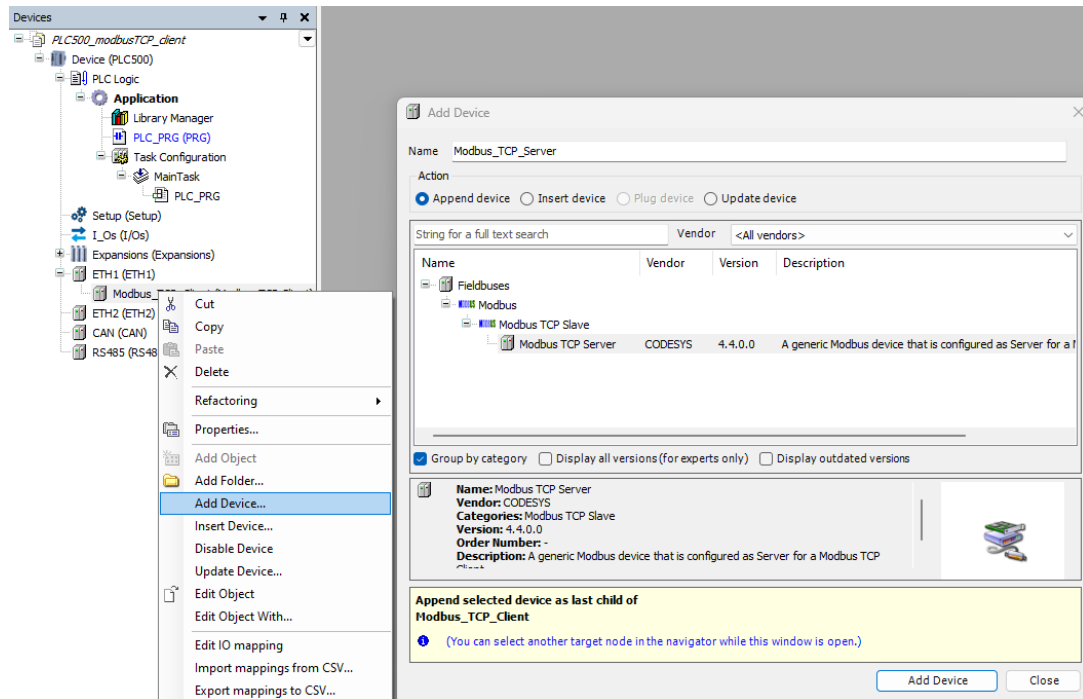


Figure 3.5: Adding Modbus TCP Server device.

At this point, the **ETH1** interface should have the items shown in [Figure 3.6 on page 3-3](#). Additional server devices can be added by following the same procedures.

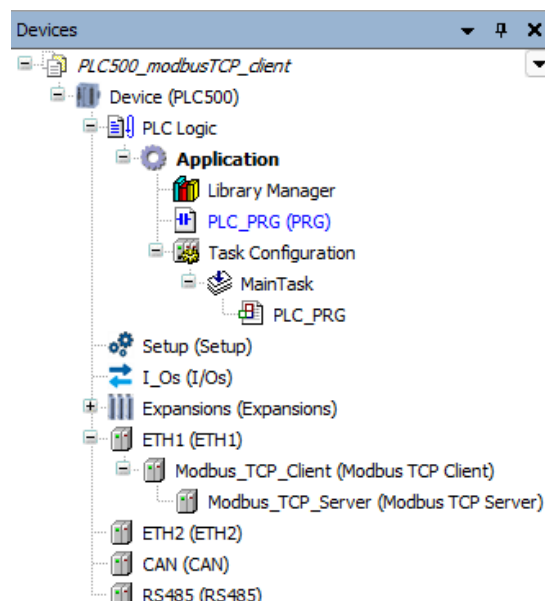


Figure 3.6: ETH1 interface with Modbus/TCP client and server.

4 CONFIGURATION OF MODBUS/TCP

This chapter outlines the steps to configure a Modbus/TCP network, with the PLC500 acting as the client and the PLC300 as the server in CODESYS.

4.1 ETHERNET INTERFACE CONFIGURATION

The configuration of the Ethernet interfaces of the PLC500 can be done through the **Setup** tab in CODESYS, as shown in [Figure 4.1 on page 4-1](#).

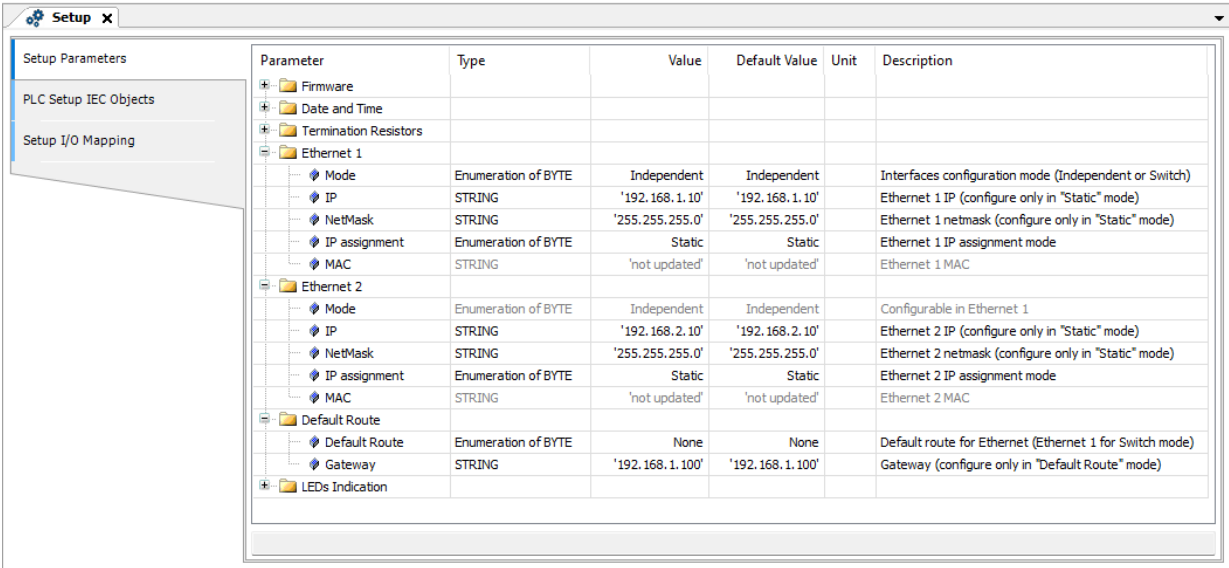


Figure 4.1: Network interface configuration for the PLC500.

To obtain the IP address of an interface automatically on the network, modify the **IP assignment** field to **DHCP**. When this option is selected, the interface will request an IP address from a DHCP server available on the network, which will assign a valid IP along with other configurations, such as subnet mask and default gateway.



ATTENTION!

When Ethernet ports are configured in **Independent** mode, they must operate in **separate networks**. Do not use the address range **192.168.234.xxx**, as it is reserved for access to the PLC500 via the USB2 interface. **Incorrectly configuring these ports may result in loss of access to the PLC**, making it inaccessible via Ethernet until the configurations are corrected.

4.2 NETWORK CONFIGURATION

Every device on an Ethernet network requires an IP address and a subnet mask. The network should be configured with valid addresses for each client and server device, ensuring that the addresses are unique and within the allowed IPv4 address range. Otherwise, connectivity issues may arise.

By double-clicking the **ETH1** interface, a window will open, as shown in [Figure 4.2 on page 4-2](#). The **Browse** box is used to select the Ethernet port. Below this box, you can change the IP, network mask, and gateway for the device. In this example, the **eth1** interface is selected with the default static IP address **192.168.1.10**.



NOTE!

To use the **Browse** box, the PLC500 must be properly connected and identified on the computer. Otherwise, a network communication error will occur.

CONFIGURATION OF MODBUS/TCP

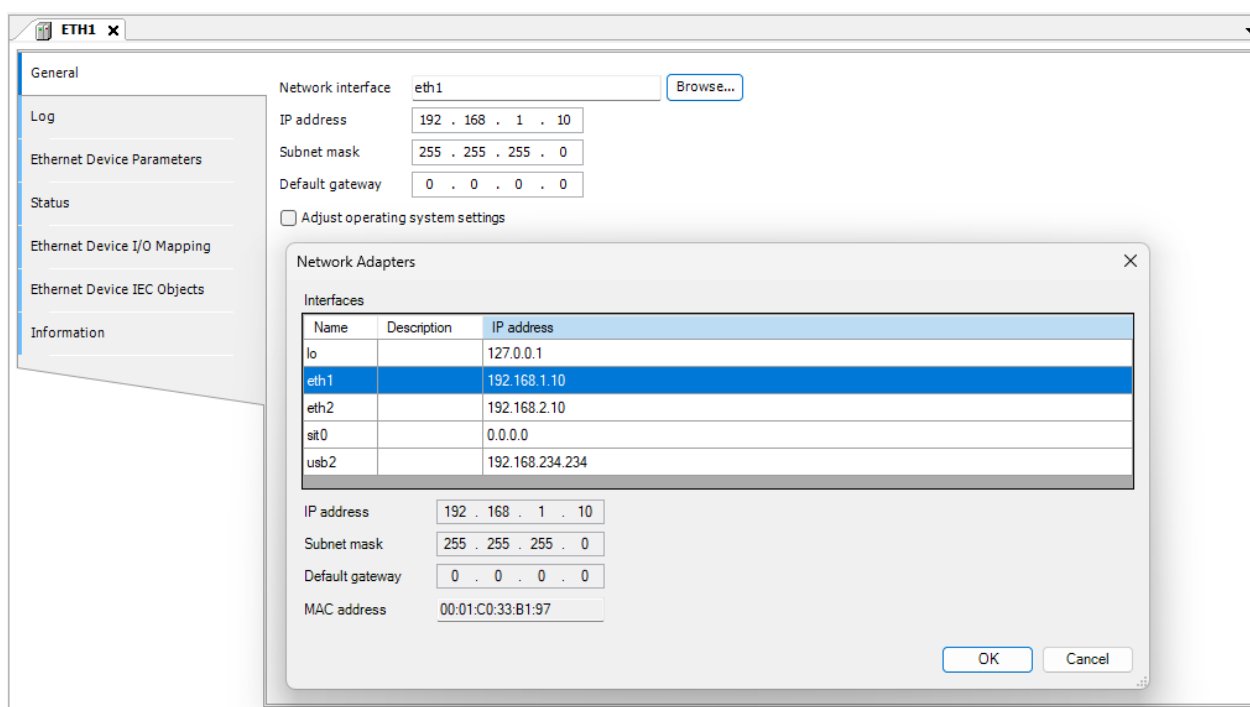


Figure 4.2: Network configuration for the client device.

To enable automatic network reconnection, double-click **Modbus_TCP_Client** and enable the **Auto-reconnect** option in the **General** tab, as shown in Figure 4.3 on page 4-2.

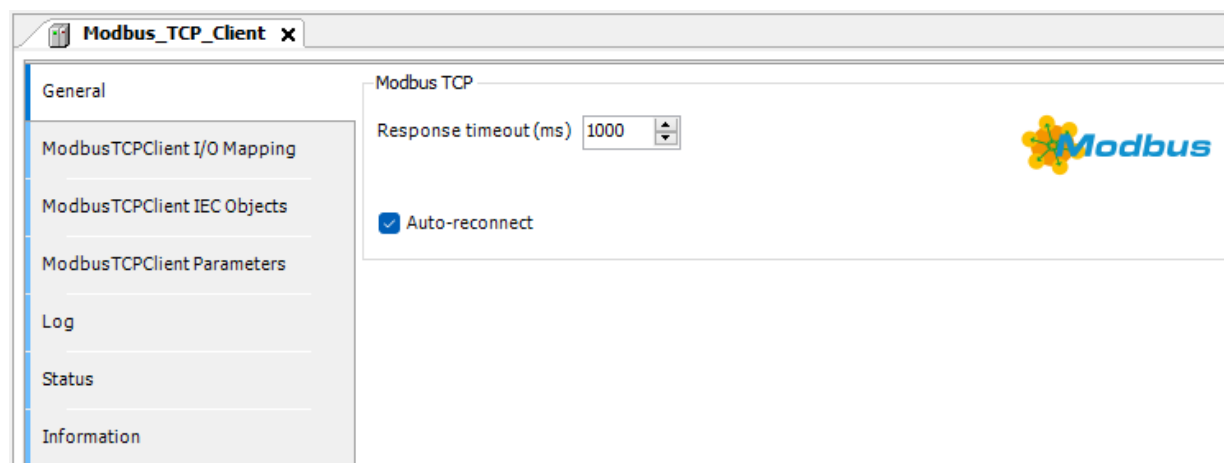


Figure 4.3: Enabling automatic reconnection for the Modbus/TCP network.

To configure the network for the server device, double-click **Modbus_TCP_Server**, and a window will open as shown in Figure 4.4 on page 4-3. Each server must have its own address and be within the available IPv4 address range. Other settings, such as transmission rate, will be managed automatically by the network. In this example, the **Server IP address** is changed to **192.168.1.11**, which is within the **192.168.1.XXX** range of the **ETH1** interface on the PLC500. **Response timeout(ms)** and **Port** are kept at their default values.



Figure 4.4: Network configuration for the server device.



NOTE!

The PLC300 has the Ethernet port configured with the default IP **192.168.0.10**. To change this address, refer to the product documentation available on the [WEG](#) website.

4.3 MODBUS CHANNEL CONFIGURATION

Variables and memory addresses configured for a server must be declared within the memory ranges reserved for transmission variables. The declaration of transmitted addresses is done in the **Modbus Server Channel** tab, as shown in [Figure 4.5 on page 4-3](#).

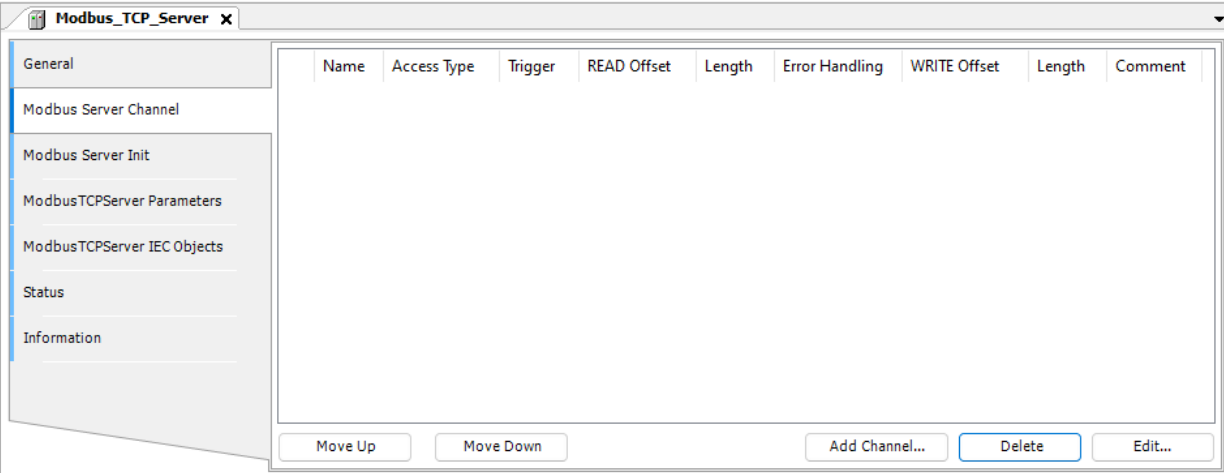


Figure 4.5: Tab to add Modbus/TCP network channels.

For each application, transmission addresses and relevant data can be defined. For example, the PLC500 writes a value to the digital outputs and reads the value from the PLC300's digital inputs every 100 ms. In [Figure 4.6 on page 4-4](#), the schematic representation of this network configuration is shown.

CONFIGURATION OF MODBUS/TCP

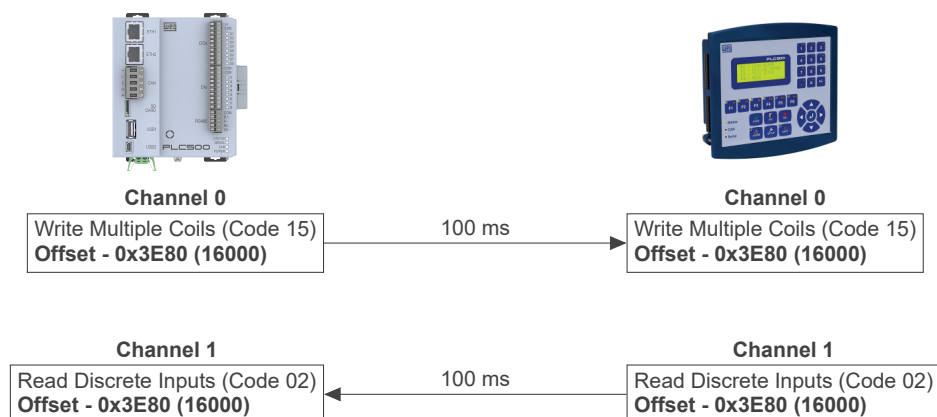


Figure 4.6: Schematic representation of Modbus channels configuration.

To add a new channel, click on **Add channel...**, and a window will appear as shown in [Figure 4.7 on page 4-4](#). To configure the writing of the 9 digital outputs from the PLC300, channel 0 is configured as shown in the figure.

The 'Modbus Channel' configuration window for Channel 0 shows the following settings:

- Channel Name: Channel 0
- Access type: Write Multiple Coils (Function Code 15)
- Trigger: Cyclic
- Cycle time (ms): 100
- Comment: Digital Outputs PLC300
- READ Register: Offset 0x0000, Length 0, Error handling: Keep last value
- WRITE Register: Offset 0x3E80, Length 9

Figure 4.7: Channel 0 configuration example for Modbus/TCP network.

For reading the 10 digital inputs of the PLC300, channel 1 is configured as shown in [Figure 4.8 on page 4-4](#).

The 'Modbus Channel' configuration window for Channel 1 shows the following settings:

- Channel Name: Channel 1
- Access type: Read Discrete Inputs (Function Code 2)
- Trigger: Cyclic
- Cycle time (ms): 100
- Comment: Digital Inputs PL300
- READ Register: Offset 0x3E80, Length 10, Error handling: Keep last value
- WRITE Register: Offset 0x0000, Length 0

Figure 4.8: Channel 1 configuration example for Modbus/TCP network.



NOTE!

The **Offset** field accepts addresses in either decimal or hexadecimal format with the '0x' prefix.

After these procedures, the channels will be added in the **Modbus Server Channel** tab, as shown in [Figure 4.9 on page 4-5](#).

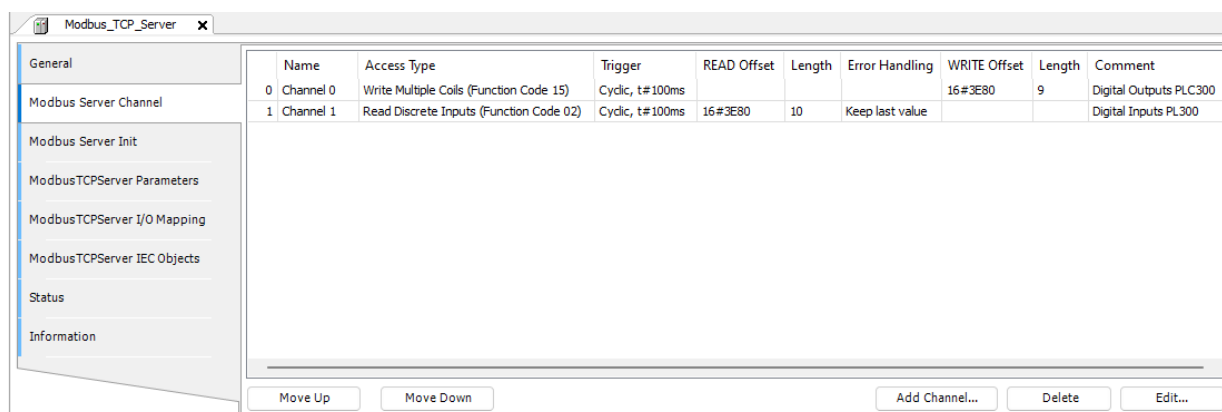


Figure 4.9: Channels added in the Modbus/TCP network example.

The available function codes to access different types of data for the Modbus protocol in CODESYS are:

- **Read Coils (code 1):** reads a block of bits of type coil.
- **Read Discrete Inputs (code 2):** reads a block of bits of type discrete inputs.
- **Read Holding Registers (code 3):** reads a block of holding registers.
- **Read Input Registers (code 4):** reads a block of input registers.
- **Write Single Coil (code 5):** writes a single bit of type coil.
- **Write Single Register (code 6):** writes a single holding register.
- **Write Multiple Coils (code 15):** writes a block of bits of type coil.
- **Read Input Registers (code 16):** writes a block of holding registers.
- **Mask Write Registers (code 22):** writes to a holding register using a mask.
- **Read/Write Multiple Registers (code 23):** reads and writes a block of holding registers.
- **Read Device Identification (code 43):** identifies the device model.



NOTE!

The availability of Modbus addresses and the way to access data types may vary from device to device. Therefore, during configuration, use the **Product Manual** to obtain information on the available addresses.

4.4 CONFIGURATION OF MODBUS RTU GATEWAY READING

The PLC500, acting as a Modbus/TCP client, can establish communication with a Modbus/RTU device through a server that has a gateway. To do this, it is necessary to add a **Modbus TCP Server** device to the **Modbus TCP Client**, as shown in [Figure 4.10 on page 4-6](#).

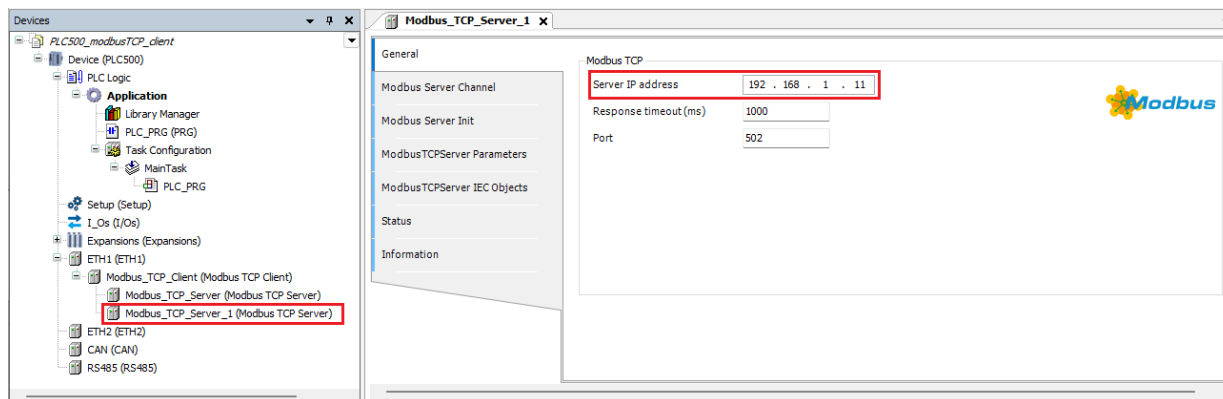


Figure 4.10: Modbus/TCP server device added for Modbus RTU Gateway.

The **Server IP address** of this device must be the same as the one used by the server device that has the Modbus RTU gateway. In this case, the address **192.168.1.11** is configured, which is the same used for communication with the PLC300 via Modbus/TCP in the previous example. Next, it is necessary to modify the address for access to the RTU slave device via the gateway in the **ModbusTCPServer Parameters** tab, as indicated in [Figure 4.11 on page 4-6](#).

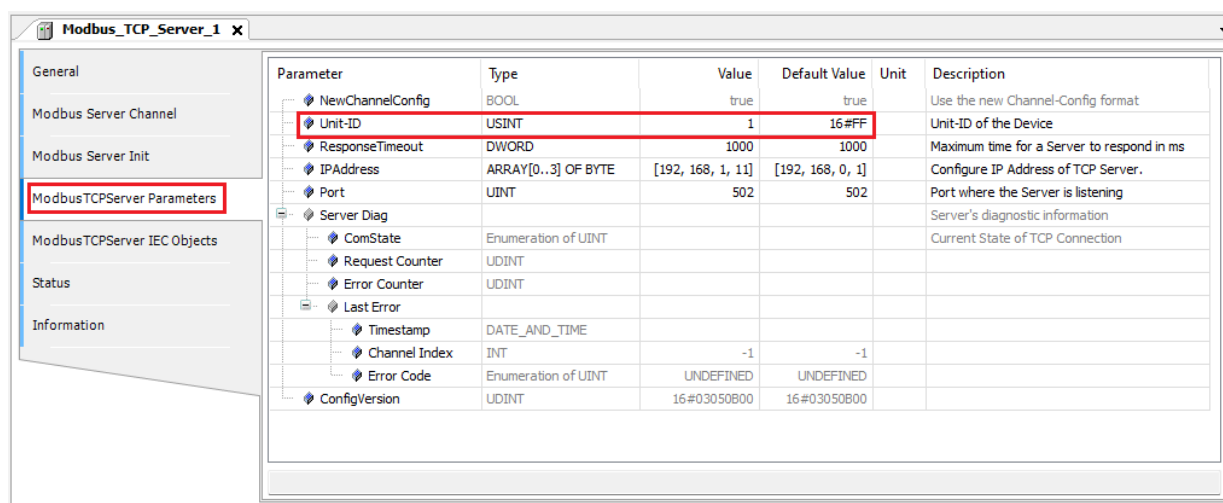


Figure 4.11: Configuration of the RTU slave device address accessed via the gateway.

After this configuration, it is possible to configure the Modbus channels for the addresses and variables of interest through the **Modbus Server Channel** tab, following the same previous steps. In [Figure 4.12 on page 4-6](#), an example is shown of a PLC500 accessing a remote unit RUW100 through the Modbus RTU gateway of a PLC300.



Figure 4.12: Example of Modbus RTU Gateway.

5 MONITORING

In this chapter, some methods for monitoring Modbus/TCP network variables and diagnosing communication errors in CODESYS are presented.

5.1 MONITORING VARIABLES

You can monitor the declared variables in the network through two methods. The first option is to add them to the CODESYS program and monitor the variable values online. The second method only requires enabling **Always Update Variables** in the footer of the **ModbusTCP Server I/O mapping** tab, as indicated by the red arrow in [Figure 5.1 on page 5-1](#).

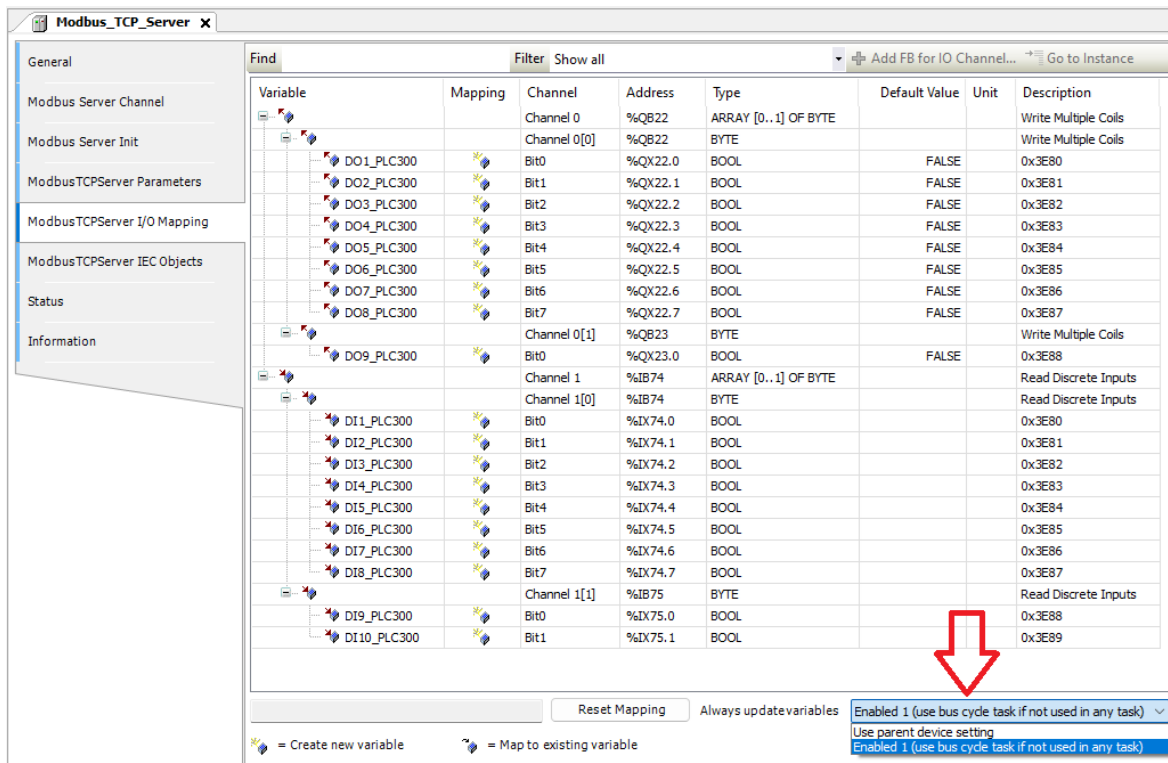


Figure 5.1: Option to always update the values of Modbus/TCP variables with the bus cycle task.

[Figure 5.2 on page 5-1](#) shows the CODESYS variable visualization screen for the Modbus/TCP server being used through online monitoring.

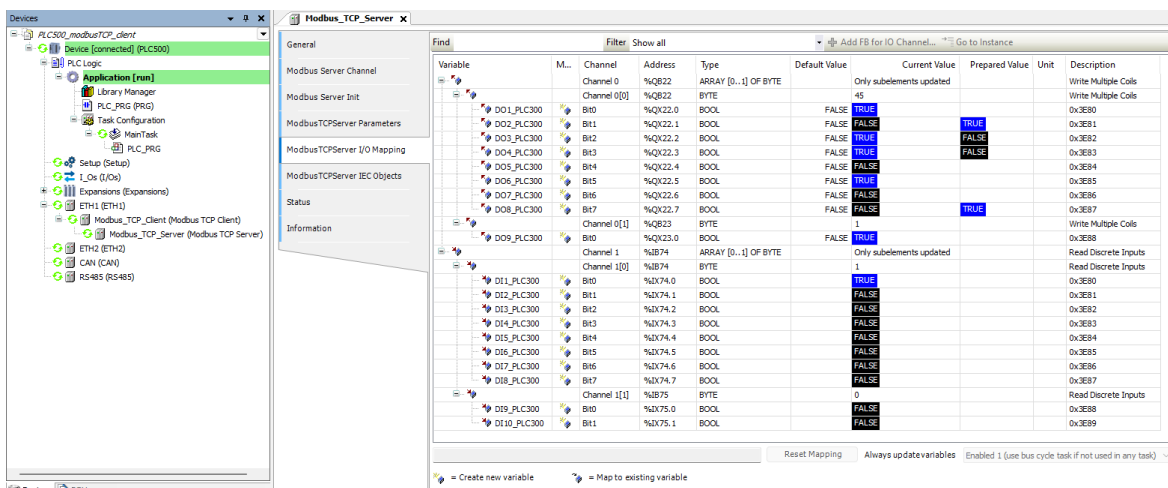


Figure 5.2: Monitoring Modbus/TCP variables online in CODESYS.

5.2 COMMUNICATION ERRORS

The monitoring of the network states can be done in **Devices**, indicating the status of each communication step and reporting the state (**Status**). When connection problems are found, as shown in [Figure 5.3 on page 5-2](#), check if the cables are properly connected, the status of the Ethernet port LED used in the PLC, and then review the settings made.

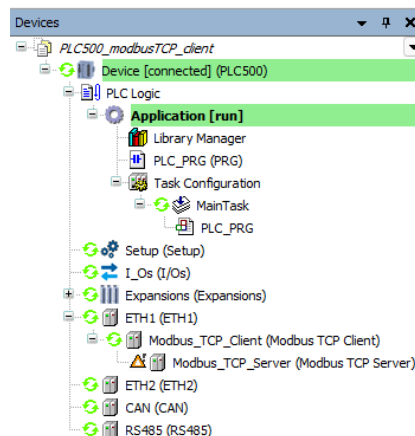


Figure 5.3: Error indication in communication.

In online mode, access the **Status** tab of the **Modbus_TCP_Server**, as shown in [Figure 5.4 on page 5-2](#). Here, CODESYS will inform you of the problem encountered when trying to establish communication. In this case, the cable was not properly connected to the server device.

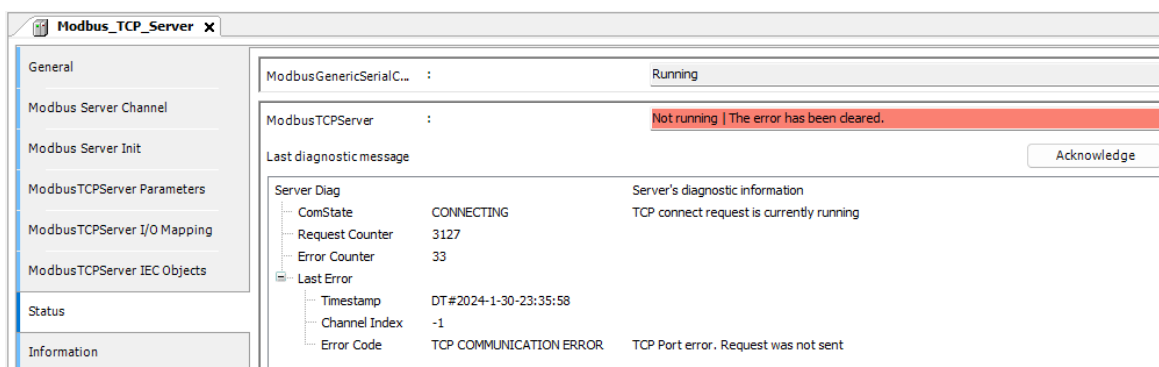


Figure 5.4: Error indication in communication.

After reconnecting the cable and waiting a few moments, the network communication is re-established, and the device icons turn green. An exclamation mark icon is displayed on the device, indicating that an error was declared, as shown in [Figure 5.5 on page 5-2](#).

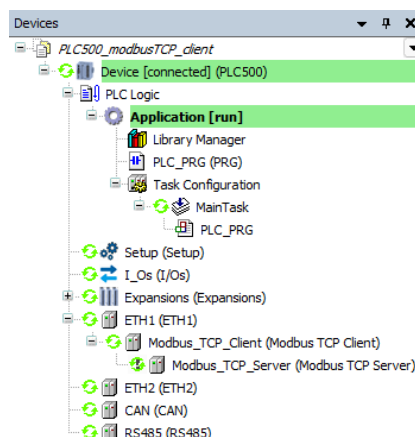


Figure 5.5: Error declared indication in the Modbus/TCP network.

To remove the warning, simply click **Acknowledge**, as indicated in [Figure 5.6 on page 5-3](#).

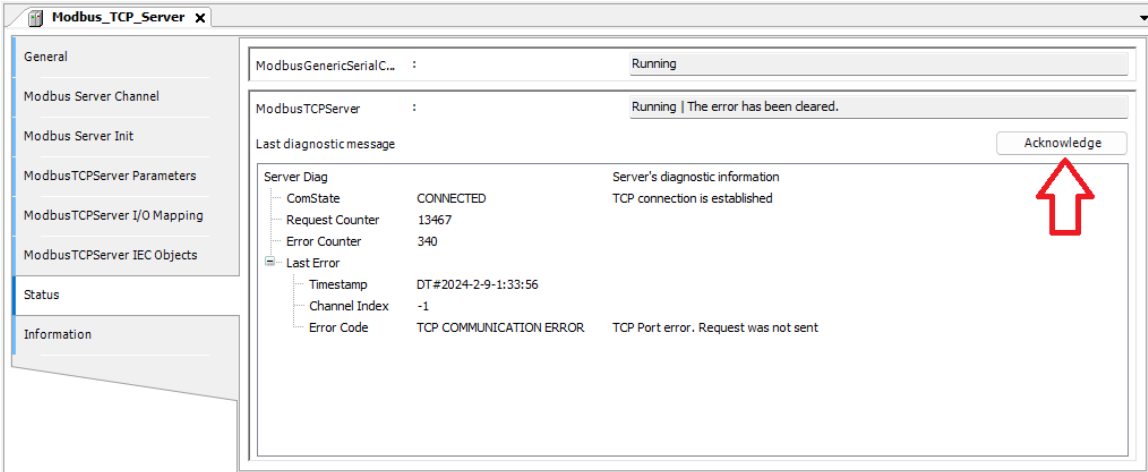


Figure 5.6: Acknowledging the declared error in the Modbus/TCP network.

After acknowledging the warning and verifying the proper operation of the network, the device icons will be displayed as shown in [Figure 5.7 on page 5-3](#).

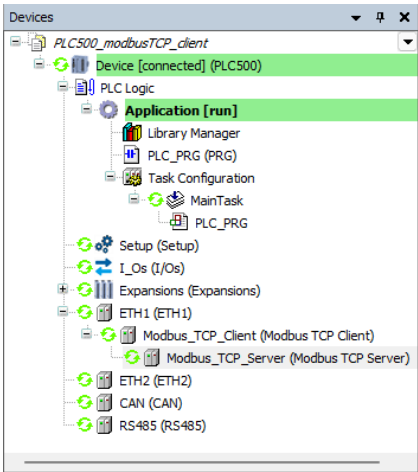


Figure 5.7: Modbus/TCP network running without errors and warnings between client and server.



NOTE!

It is recommended to consult the documentation available in the **Library Manager**, or access the online help at [CODESYS Online Help](#), for more information on configuring the Modbus/TCP network and the available methods and functions.



BRAZIL

WEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.

Av. Prefeito Waldemar Grubba, 3000

89256-900 - Jaraguá do Sul - SC

Phone: 55 (47) 3276-4000

Fax: 55 (47) 3276-4060

www.weg.net/br