lamaPLC: Simatic and Modbus

Introduction

Certainly, I am aware that numerous descriptions of Modbus can be found online and in technical literature. As the oldest and most widely used industrial communication method, it serves as the backbone of industrial connectivity. While newer, more sophisticated communication protocols have emerged, Modbus remains prevalent. In fact, you might even encounter it on the first intergalactic spacecraft.

Although this communication method is widespread and often underestimated, it can lead to unexpected issues during commissioning, usually more negatively than positively. With over 25 years of experience in automation programming, primarily with Simatic systems, I'm sharing my observations. While the following is somewhat subjective, I hope many readers will have an „aha” or facepalm moment, helping them resolve certain problems.

Modbus Fundamentals

Origin and basics of Modbus

Modbus originated in 1979 and was created by Modicon (now part of Schneider Electric). During this period, industrial automation moved from relay-based systems to digital logic. As the pioneer of the first Programmable Logic Controller (PLC) a decade earlier, Modicon developed Modbus to facilitate communication among these controllers and with external devices via serial lines. The protocol features a straightforward query-response model, in which a *“master”* (client) initiates communication with one or more *“slaves”* (servers) to transfer data.

The protocol's emergence as a worldwide industry standard was fueled by several key factors:

- **Open and Royalty-Free:** Since its inception, Modicon has made the protocol available as an open standard, enabling any manufacturer to implement it without licensing costs.
- **Technical Simplicity:** Its minimal processing requirements and simple message format facilitated its adoption by hundreds of vendors for applications ranging from sensors to motor controllers.
- **Adaptability:** Initially designed for serial interfaces such as RS-232 and RS-485, the protocol has evolved to meet industry needs. In 1999, Modbus TCP was introduced, allowing the original protocol to operate over modern Ethernet and TCP/IP networks.

In 2004, Schneider Electric officially transferred the rights to the Modbus Organization, an independent nonprofit that continues to manage and promote it as a public domain standard. Today, it is often called the “grandfather of industrial networking” due to its continued widespread use in both legacy factories and modern IoT systems.

Core application areas of Modbus

Industrial Automation & Manufacturing

- **Control Systems:** Connecting Programmable Logic Controllers (PLCs) with sensors, actuators, inverters, and motors to automate assembly lines.
- **Data Acquisition:** Using SCADA (Supervisory Control and Data Acquisition) systems to monitor real-time production data, such as oven temperatures, vibration levels, and pressure.
- **Legacy Integration:** Retrofitting older machines to communicate with modern control systems through Modbus-to-IoT gateways.

Smart Buildings & Facility Management

- **HVAC Control:** Managing heating, ventilation, and air conditioning systems based on occupancy and environmental conditions.
- **BMS Integration:** Centralizing data from lighting, security, and elevator systems for improved energy efficiency.
- **Smart Metering:** Connecting Modbus-enabled smart meters to monitor electricity, water, and gas usage across residential or commercial complexes.

Energy Management & Renewables

- **Solar & Wind:** Monitoring Photovoltaic (PV) inverters, trackers, and batteries to optimize energy generation and storage.
- **Electric Vehicles (EV):** Integrating charging infrastructure with building energy systems to manage load and prevent grid strain.
- **Smart Grids:** Enabling real-time communication between grid management systems and remote sensors at substations.

Water & Wastewater Management

- **Process Monitoring:** Automating chemical dosing units, monitoring pump station status (pressure, flow rate), and checking water quality (pH, conductivity).
- **Infrastructure Safety:** Detecting sudden pressure changes to identify pipeline leaks or bursts immediately.

Modbus Client and Server

In the Modbus protocol, the terms Client and Server specify the roles of devices during communication. These terms are the current, official replacements for the older “Master/Slave” terminology.

Modbus Client (formerly Master)

The Client is the active device that initiates all communication transactions. It's sending questions.

- **Action:** It sends a “Request” to a specific device to read or write data to it.
- **Behavior:** It should wait for a response or a timeout before issuing the next command.
- **Typical Devices:** SCADA systems, HMI panels, or a primary PLC.

Modbus Server (formerly Slave)

A server is a passive device that responds to client requests.

- **Action:** It waits for an incoming message, processes the request (for example, looks up a sensor value), and sends back a *“Response”*.
- **Behavior:** It never initiates a conversation; it only responds when spoken to.
- **Typical Devices:** Sensors such as temperature and humidity sensors, motor drives like VFDs, power meters, or I/O blocks.

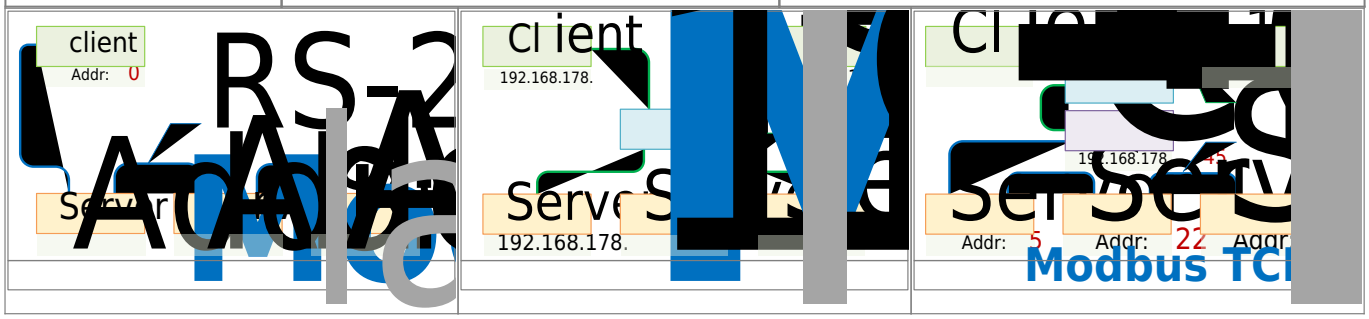
Modbus RTU and TCP, and Hybrid

The core difference is the transport layer: Modbus RTU is designed for a physical wire (Serial), while Modbus TCP is designed for a network (Ethernet). Before Ethernet's advent, only the RTU (*Remote Terminal Unit*) protocol was available, primarily using RS-232 or RS-485. The rise of Ethernet greatly expanded options, enabling communication over the faster, more versatile TCP/IP protocol. Today, these two methods serve as the Modbus transport layer.

Although quite different, they can sometimes be integrated, such as in multimaster (hybrid) RTU scenarios. In this scenario, a signal converter needs to be integrated into the TCP network. The converter has its own IP address to receive Modbus/TCP telegrams. It's crucial that the client is aware of the Modbus/RTU network behind the converter, which uses traditional RTU addressing. Often, clients cannot manage both RTU addressing and TCP simultaneously, so verifying their ability to do so is essential. The Siemens TIA Portal is suitable for this task, and I will offer an example of its use later.

Feature	**Modbus RTU**	**Modbus TCP**
Media	Serial (RS-485/232)	Ethernet / Wi-Fi
Error Check	CRC (at the end)	TCP/IP Checksum (built-in)
Topology	Daisy-chain	Star (Switch-based)
Speed	Typically 9600 or 115200 baud	10/100/1000 Mbps
Master/Client	Only one Master	Multi-Master

Feature	Modbus RTU	Modbus TCP
Port	Serial COM Port	TCP Port 502
Segment distance	1200 meters	100 meters between switches
Addressing	Master ID: 0, slave ID: 1 to 247	IP Address (like: *192.168.178.123*)
Wiring	3-core cable with shielding or 4-core cable	Ethernet cables (RJ45) and network switches



Modbus/RTU

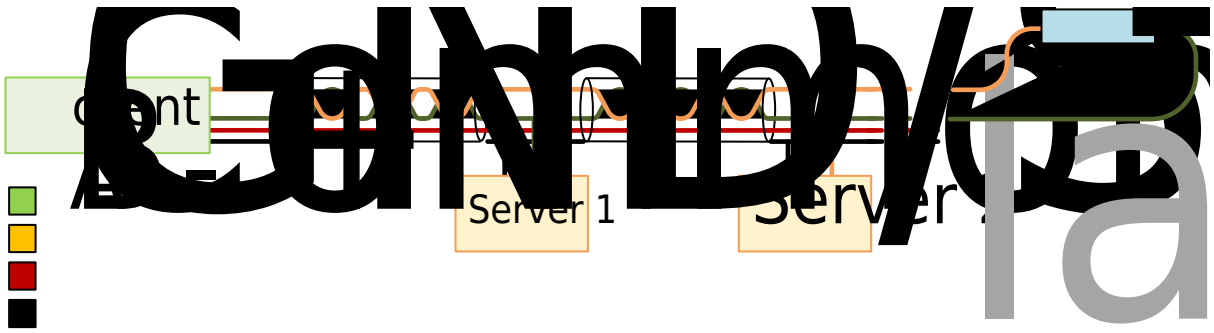
Comparison of RS-232 and RS-485

The Modbus/RTU transmission options depend on the physical layer: RS-232 or RS-485. RS-232 is quite uncommon because it only supports point-to-point connections, meaning one Client and one Server. In contrast, RS-485 is a more flexible option; its technical specifications are outlined in the table below.

	RS-232	**RS-485**
Operating mode	asynchronous transmission	synchronous transmission
Number of drives and receivers per line	1 drive 1 receiver (point-to-point)	32 stations per segment
Data transfer method	half-duplex, full-duplex	half duplex
Data transmission	p2p	multipoint
Max. cable length	15 m	1200 m
Max. data transfer **12 m** **1200 m**	 20 kbps (1 kbps)	 35 Mbps 100 kbps
Receiver input resistance	3..7 kΩ	≧ 12 kΩ
Drive Load-Impedance	3..7 kΩ	54 Ω
Receiver “dead band”	±3 V	±200 mV
Receiver voltage level	±15 V	-7..+12 V
Drive output voltage max.	±25 V	–9..+14 V
Drive output voltage min. (with load)	±5 V	±1.5 V
Drive output short circuit current limit	500 mA to Vdc or Ground	150 mA to Ground 250 mA to Vdc
Receiver Hysteresis	1.15 V	50 mV

Modbus/RTU wiring

For Modbus/RTU communication, use RS-485 with either a 3-wire with shield or a 4-wire cable. To improve noise immunity, using shielded cables and twisted pairs is recommended. The units should be connected in a daisy-chain layout, though star topology can also work in some cases with a few units.



In a Modbus RTU over RS-485 network, it is vital to terminate the bus to prevent signal reflections that could cause communication errors and CRC failures.

Guidelines on Proper Terminator Placement

- **Both Ends Only:** Install a termination resistor at the first and last device of the trunk cable.
- **Do Not Terminate Middle Devices:** Adding resistors at intermediate nodes can overload drivers and cause signal loss.
- **Daisy Chain Topology:** RS-485 should be wired in a continuous line. Avoid star or tree configurations with long branches or stubs, as these cannot be correctly terminated.

Resistor Specifications

- **Value:** Usually **120 Ω** to match the characteristic impedance of standard twisted-pair cable.
- **Power Rating:** Select a resistor with a power rating of at least 0.25W to 0.5W.
- **Connection:** Attach the resistor directly between the A (D0/-) and B (D1/+) data lines.

Modbus/RTU RS-485 Signaling

In a Modbus/RTU network (which uses the RS-485 physical layer), **A** and **B** represent the two wires of a differential pair used to transmit data.

- **Differential Signaling:** The receiver measures the voltage difference between two lines instead of against a common ground. This helps the signal resist electrical noise because

interference usually impacts both wires equally.
- **Half-Duplex:** Modbus/RTU uses these two wires for transmission and reception, but only one device can communicate at a time.

The Naming Confusion (A vs. B)

Since there is no universal naming standard, wiring errors are common. Terminal labels vary by manufacturer as follows:

Labeling Convention	Non-Inverting Signal	Inverting Signal
Common/Modbus	B or B+	A or A-
TIA/EIA-485 Standard	A (Negative)	B (Positive)
Alternate Labels	D+, Data+, Tx+	D-, Data-, Tx-

- **Standard Rule:** In the official TIA-485 standard, **A is negative (A-)** and **B is positive (B+)**.
- **Industry Practice:** Many Modbus device manufacturers (such as those following Modbus Organization guidelines) use A for negative (-) and B for positive (+).

Voltage Levels

- **Logic 1 (Idle/Marking):** Occurs when the voltage at B is higher than A by at least 200mV.
- **Logic 0 (Active/Spacing):** Occurs when the voltage at A is higher than B by at least 200mV.
- **Idle State:** When no device is transmitting, the bus is *"idle."* Biasing resistors are often used to keep the B line slightly more positive than the A line, preventing noise from being misinterpreted as data.

If your devices have the correct baud rate and address but still can't communicate, try swapping the A and B wires on one side. This is a common cause of Modbus RTU setup failure and won't harm your hardware.

Modbus Registers and Coins

Modbus Register types

Modbus Register-adressing

Modbus Telegram structure

Modbus test programs, test methods

Modbus Problems and errors

Simatic and Modbus

Scheme of Simatic

Simatic and Modbus RTU and/or TCP

Modbus Installation examples, step by step

S7-1500 and Easton Energymeter

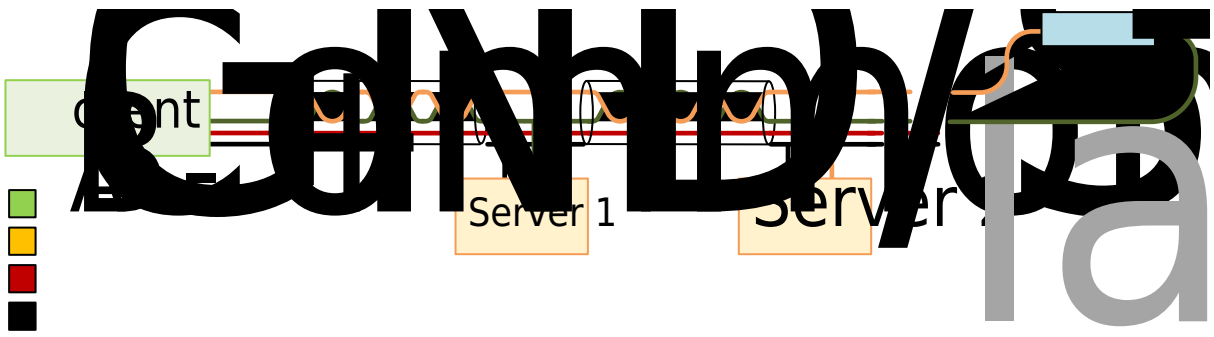
S7-1500 and Arduino Uno R4

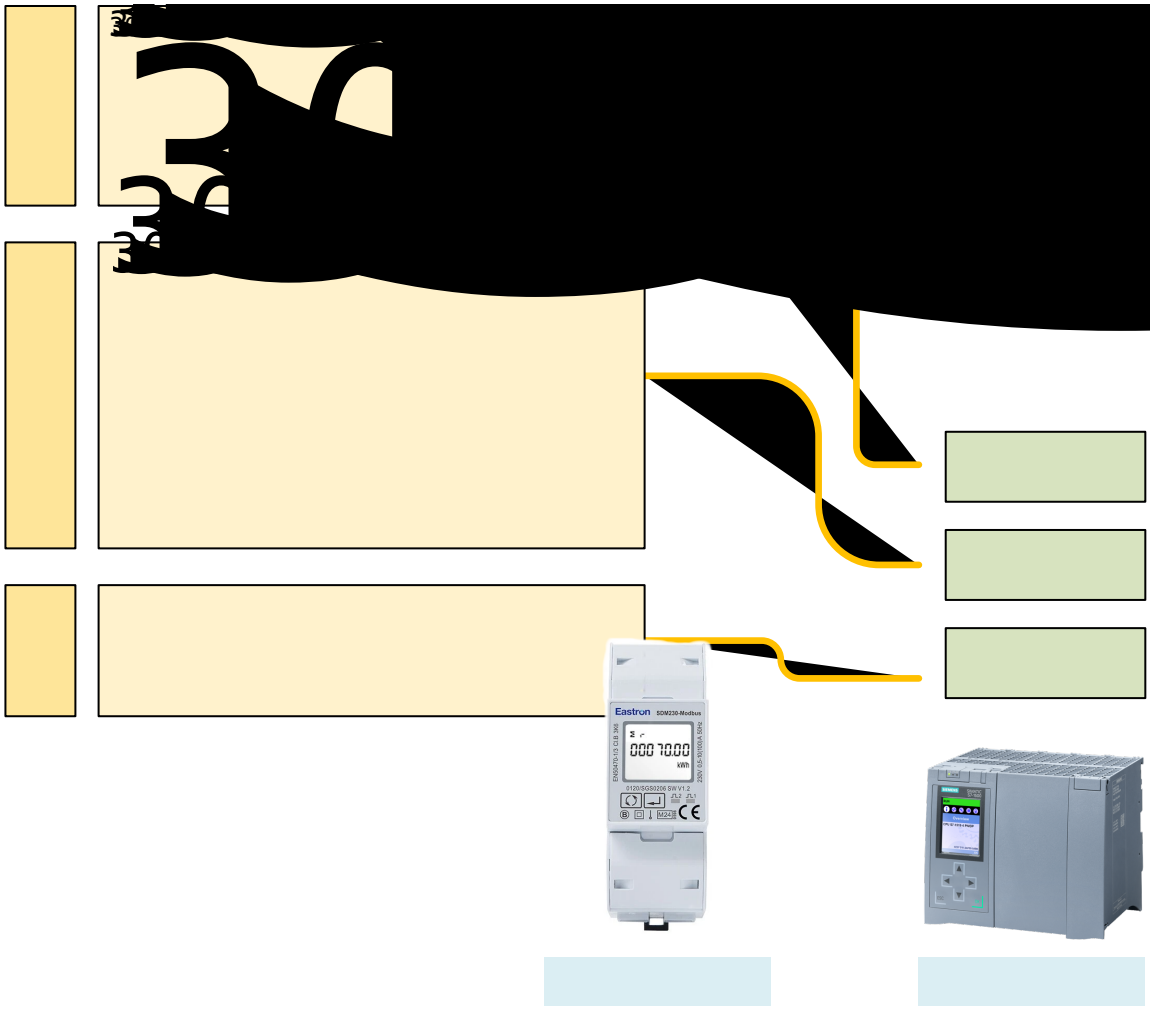
Arduino and Modbus

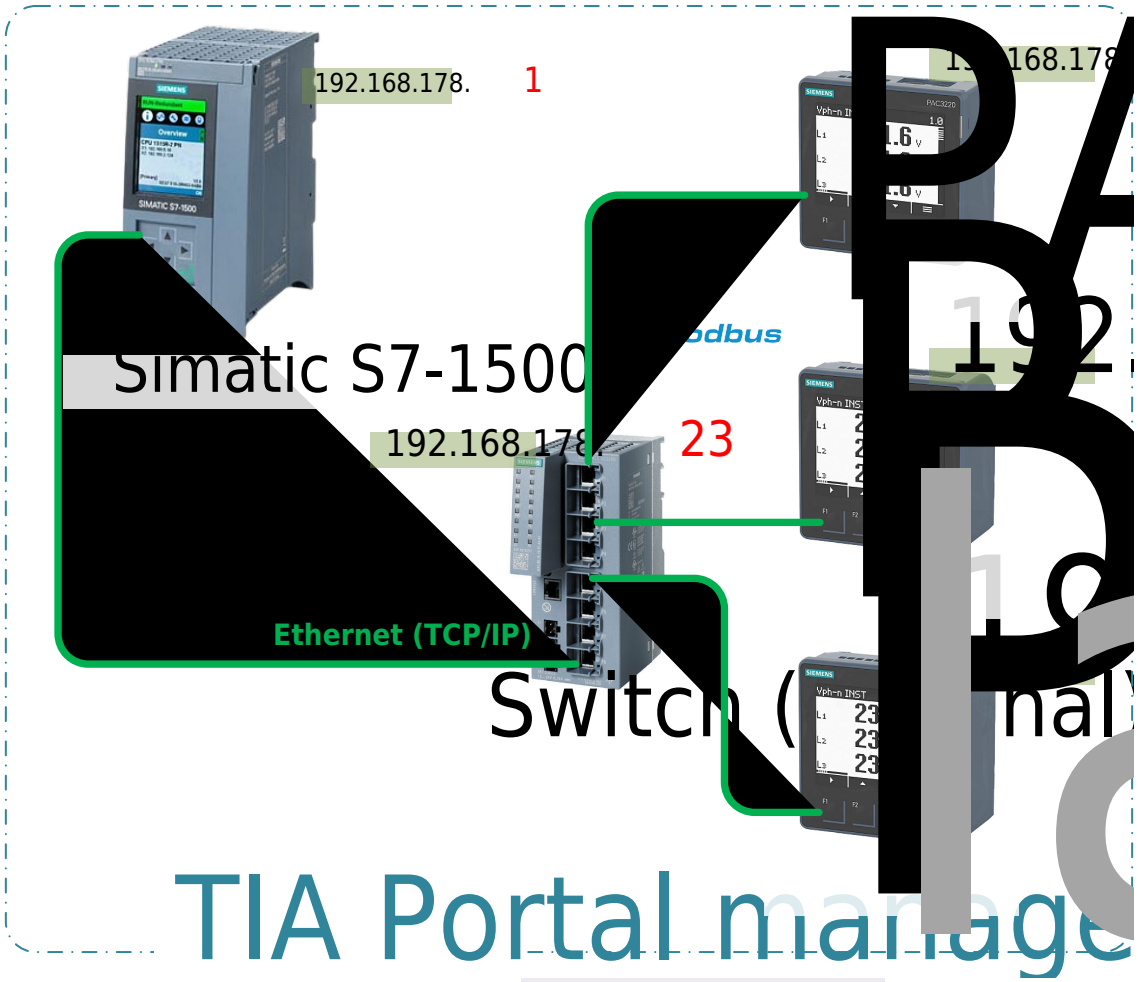
Arduino and Modbus RTU and/or TCP

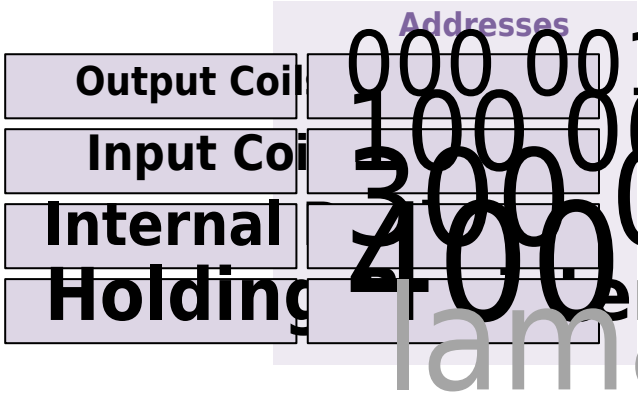
Modbus Installation examples, step by step

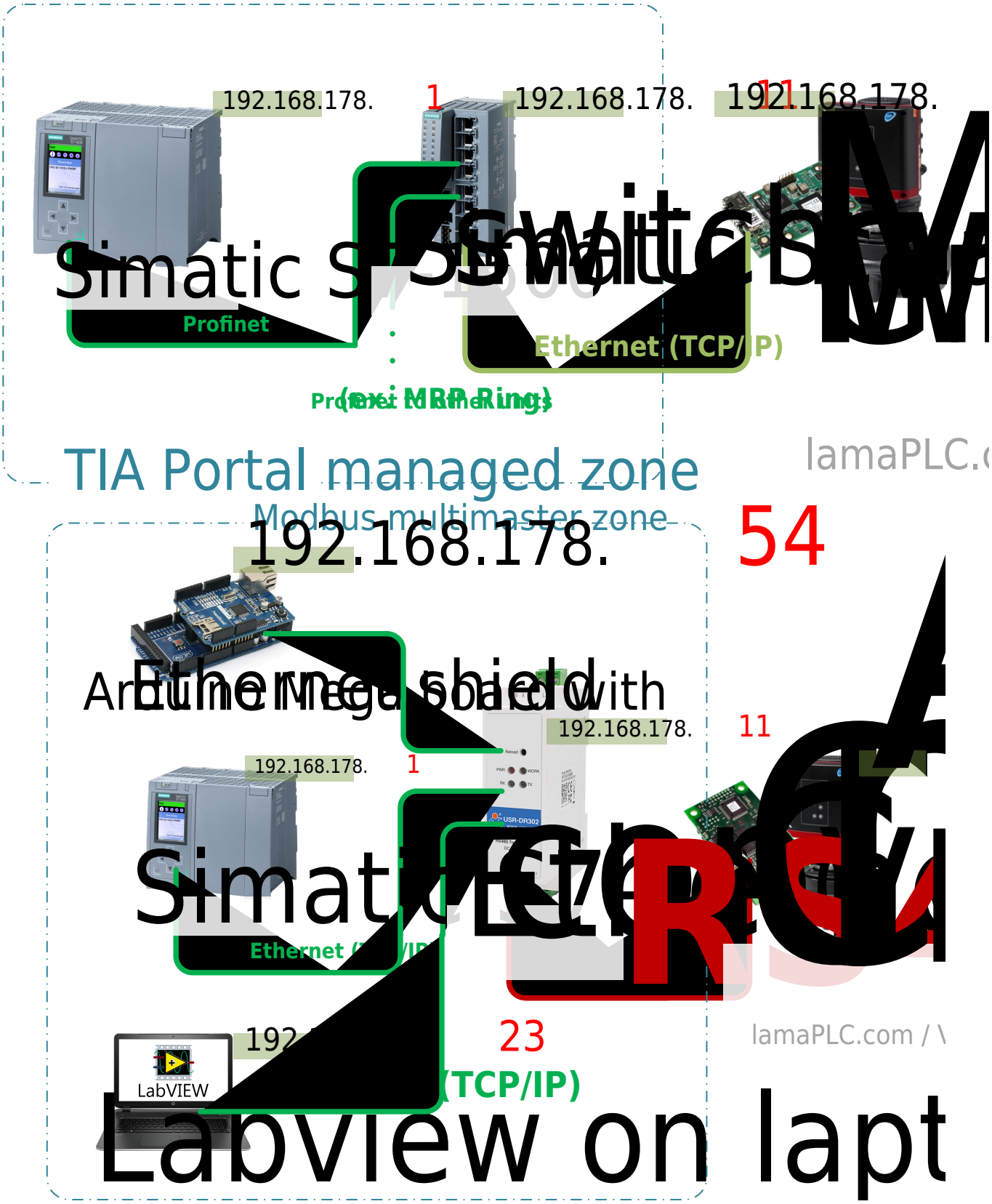
Appendix




Eastron
SDM230-Modbus
000 70.00
kWh


192.168.178. 1
Simatic S7-1500
odbus
192.168.178 23
Ethernet (TCP/IP)
Switch (
TIA Portal manage


Addresses
Output Coil
Input Coi
Internal
Holding
000 00
100 0
300 0
400
lam


192.168.178.
1
192.168.178.
11
Profinet
Ethernet (TCP/IP)
(ex: MRP Ring)
TIA Portal managed zone
lamaPLC.com
Modbus multimaster zone
192.168.178.
54
192.168.178.
11
192.168.178.
1
Ethernet (TCP/IP)
192.168.178.
23
LabVIEW
(TCP/IP)
lamaPLC.com / \


192.168.178. 1
192.168.178. 11
192.16
Profinet, Industria ernet
TCP Modbus
(ex: MRP Ring)
TIA Portal managed zone
lamaPLC.
192.168.178.
Ethernet (TCP/IP)
RS485
192.168.178.
Modbus
tester
Modbus clie
Ethernet (TCP/IP)


192.168.178. 1
Modbus
Simatic S7-150
192.168.178 44
192.168.1 8. 23
Ethernet (TCP/IP
Switch (optio
TIA Pc
192.168.178. 1
Simatic S7-15
192.168.178.
192.168.1
Scalance
TIA Portal managed zone
Energy
Inver
lama