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.

Master and Slave (Client)

Monomaster and Multimaster

Modbus RTU and TCP, addressing

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