MODBUS PROTOCOL-FUNDAMENTALS, SERIAL COMMUNICATION & ARCHITECTURE

-Shravan Shetty

Table of Contents

Acronyms and Abbreviations …………………………………………………..3

Introduction ………………………………………………………………….4

History ……………………………………………………………………….4

Master-Slave Architecture …………………………………………………...4

Data Model …………………………………………………………………..5

Serial Channel Parameters …………………………………………………..5

Implementation ……………………………………………………………...5

Reasons for the Widespread use of Modbus ………………………………...6

Industrial Applications ………………………………………………………6

Limitations …………………………………………………………………..6

Future Scope ………………………………………………………………...7

References …………………………………………………………………..8

Acronyms and Abbreviations

PLC: Programmable Logic Controller

VFD: Variable Frequency Drive

SCADA: Supervisory Control and Data Acquisition

RTU: Remote Terminal Unit

TCP: Transmission Control Protocol

TCP/IP: Transmission Control Protocol / Internet Protocol

RS-485(Recommended Standard 485)**:** Differential serial communication standard

RS-232(Recommended Standard 232)**:** Serial communication interface (point-to-point)

IP: Internet Protocol

A/B Communication Line: Differential Signal Pair

HVAC: Heating, Ventilation, and Air Conditioning

AHU: Air Handling Unit

MQTT: Message Queuing Telemetry Transport

OPCUA: Open Platform Communication Unified Architecture

REST: Representational State Transfer

IIoT: Industrial Internet of Things

1.Introduction

Modbus is one of the most commonly used communication protocols in industrial automation. It is known for being open, easy to work with, and reliable, which makes it suitable for connecting devices like PLCs, energy meters, VFDs, sensors, and SCADA systems.

The protocol works on a Master-Slave (or Client-Server) concept, where the master device is responsible for sending all communication requests, and the slave devices respond to those requests. Modbus is mainly used in two communication formats:

- **Modbus RTU** -Uses serial communication through RS-485 or RS-232
- **Modbus TCP** -Runs over Ethernet using TCP/IP

Both versions follow the same core principles, but they differ in how the data is transmitted (serial vs. Ethernet), allowing Modbus to fit into different types of industrial networks.

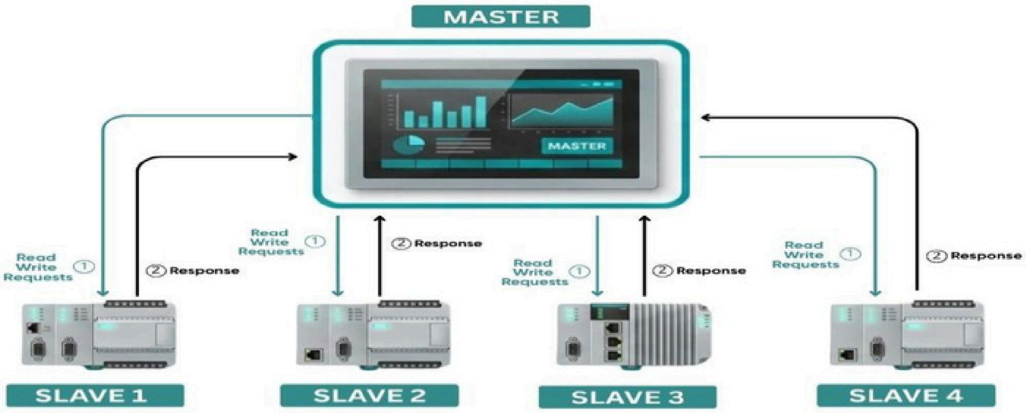
2.History of Modbus Protocol

Modbus was developed by Modicon (now Schneider Electric) in 1979 as a way for PLCs and industrial devices to communicate with each other. Over the years, it quickly became one of the most widely used communication protocols in automation.

The adoption of Modbus grew significantly during the 1980s and 1990s as more industries began using PLC-based control systems. In 1996, the protocol was released as an open and free standard, which further increased its usage because manufacturers could implement it without licensing costs.

To support its continued development and standardization, the Modbus Organization was established in 2004. Even today, Modbus remains one of the most commonly used industrial communication protocols due to its long history, simplicity, and compatibility with a wide range of devices.

3. Master-Slave Architecture



4.Modbus Data Model

Data Type	Address Range	Data Size	Access Type	Function Codes	Typical Use
Coils	00001-09999, 000001-065535(Modern)	1 bit	Read/Write	01 (Read), 05(Write Single), 15 (Write Multiple)	Digital outputs (e.g., relays, actuators)
Discrete Inputs	10001-19999, 100001–165535(Modern)	1 bit	Read-Only	02 (Read)	Digital inputs (e.g., switches, sensors)
Input Registers	30001-39999, 300001–365535(Modern)	16-bit unsigned	Read-Only	04 (Read Input Registers)	Analog or measured values (e.g., temperature, pressure)
Holding Registers	40001-49999, 400001–465535(Modern)	16-bit signed/unsigned	Read/Write	03 (Read), 06 (Write Single), 16 (Write Multiple)	Parameters, configuration, analog outputs

5. Modbus Serial Channel Parameters

The Modbus serial channel consists of several key communication parameters, including the baud rate, data bits, parity, stop bits, and flow control settings etc. These parameters must be identical across all devices on the RS-485 network to ensure reliable and consistent data exchange.

6. Modbus Protocol Implementation

Modbus RTU (Serial Communication)

Modbus RTU works over an RS-485 two-wire network where multiple devices share the same A/B communication line. It follows a request-response approach: the master sends a command, and the addressed slave returns the required data. Each device has a unique Slave ID, and communication uses Modbus function codes in a compact binary frame. Since all devices share the same bus, the master polls each slave sequentially, ensuring consistent and orderly data exchange.

Modbus TCP (Ethernet Communication)

Modbus TCP operates over standard Ethernet networks and uses TCP/IP for data exchange. Each device is assigned an IP address, and communication takes place through port 502. The client (master) sends a request over the network, and the server (slave) responds with the required data. This approach provides faster communication and easier integration with modern industrial systems.

7. Reasons for the Widespread Use of Modbus

Modbus remains popular in industrial automation because it is simple, open, and cost-effective. Its message structure is easy to understand, which makes implementation and troubleshooting straightforward. The protocol is free to use, reducing project costs, and works reliably over RS-485 networks that support long cable lengths and multiple devices in noisy environments. It is also widely supported by major automation vendors such as Siemens, Schneider Electric, ABB, Honeywell, Emerson, and Yokogawa, ensuring strong compatibility across different systems. Overall, Modbus is lightweight, dependable, and well-suited for real-time industrial communication.

8.Industrial Applications of Modbus

Modbus is applied across many industrial sectors because of its flexibility and strong device compatibility.

- **Industrial Automation:** Communication between PLCs, sensors, and machine control systems.
- **Energy Monitoring:** Used in energy meters, power analyzers, and power quality devices.
- **Building Automation:** Integrated into HVAC units, chillers, and AHU systems.
- **Water& Wastewater:** Supports level sensors, flow meters, and pump control equipment.
- **Manufacturing:** Commonly used with VFDs, motors, robotics, and production machinery.

9.Limitations

- **No Built-in Security:** Does not provide authentication, encryption, or data integrity mechanisms.
- **Low Bandwidth:** Serial communication speeds are limited and unsuitable for high-speed or large-volume data.
- **Basic Data Types:** Native support only for 1-bit and 16-bit values; complex types require custom handling.
- **Master-Slave Dependence:** Slaves cannot initiate communication; all data must be polled by the master.
- **No Device Discovery:** Manual configuration is required; the protocol does not expose device metadata.
- **Limited Scalability:** Not ideal for networks with many devices or high refresh-rate requirements.
- **Minimal Diagnostics:** Provides only simple exception codes, with no advanced diagnostic capabilities.
- **Legacy Address Restrictions:** Traditional Modicon ranges limit address space in older systems.

10.Conclusion and Future Scope

Modbus continues to remain relevant even after four decades due to its simplicity, reliability, and strong multi-vendor compatibility. As industries move toward Industry 4.0 and IIoT, Modbus RTU still supports stable serial communication, while Modbus TCP is increasingly used in Ethernet, cloud, and edge environments. Modern gateways extend Modbus connectivity to protocols like MQTT, OPC UA, and REST, ensuring integration with advanced systems.

Going forward, the focus will be on improving Modbus TCP security, enhancing

interoperability, and enabling hybrid architectures that combine Modbus with cloud and edge technologies. With its low cost, ease of use, and wide adoption, Modbus will continue to play an important role in industrial communication for both legacy and modern systems.

References

MODBUS Application Protocol 1 1 b

Modbus Addressing