OT PROTOCOL PRIMERS
MODBUS

BACKGROUND

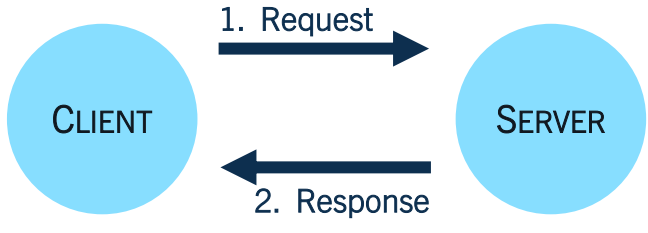
Modbus was developed by *Modicon Inc.* in 1979, the same company that invented the Programmable Logic Controller nearly a decade earlier. In 2004, rights to the Modbus protocol were transferred to the current owners, *The Modbus Organization*. [1]

Modbus is an open standard that's specification is available to download at https://www.modbus.org. [1]

Widely adopted by hundreds of vendors, the protocol is used in industrial environments to provide data transfer capabilities between control devices and endpoints. [1]

FUNDAMENTALS

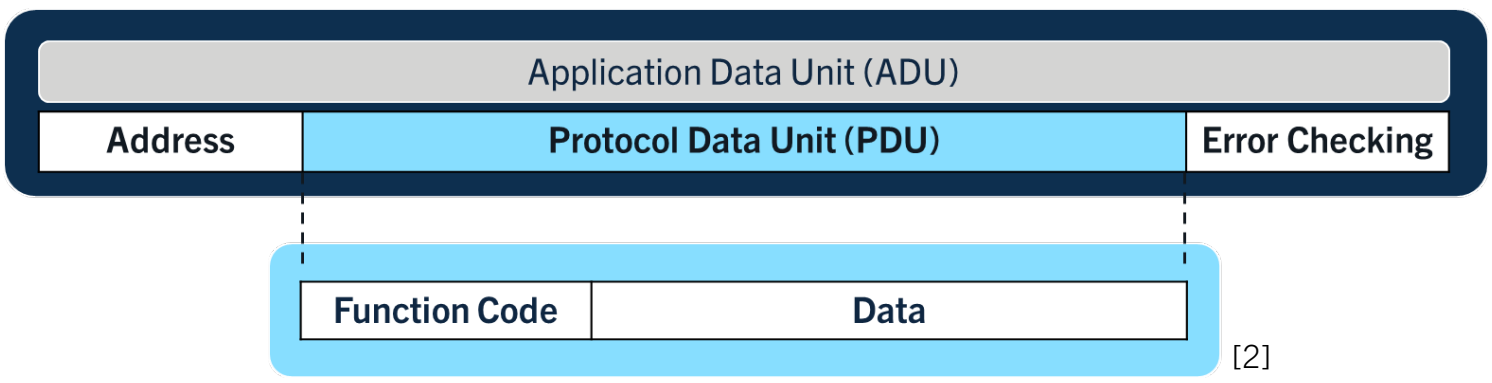
- Modbus follows a traditional client/server model. [1]
- Modbus supports both Serial and TCP/IP networks. [1]
- Modbus/TCP uses port 502. [1]
- Modbus has no native authentication mechanisms. [2]



**an invalid request will result in a server exception response* [1]

MESSAGE STRUCTURE

The Modbus protocol primary structure is captured by the Protocol Data Unit (PDU). The PDU is encapsulated within an Application Data Unit (ADU) which varies by transport mechanism. The function code can range from 0x00-0xFF and describes the action of the server. The data section may contain added specifics for request messages and holds the reply data for response messages. [2]



[2]

PROTOCOL FUNCTIONS

Function	Code	Hex
Read Coils	01	0x01
Read Discrete Inputs	02	0x02
Read Holding Registers	03	0x03
Read Input Register	04	0x04
Write Single Coil	05	0x05
Write Single Register	06	0x06
Write Multiple Coils	15	0x0F
Write Multiple Registers	16	0x10
Read File Record	20	0x14
Write File Record	21	0x15
Mask Write Register	22	0x16
Read/Write Multiple Registers	23	0x17
Read FIFO Queue	24	0x18
Read Exception Status	07	0x07
Diagnostic	08	0x08
Get Com Event Counter	11	0x1B
Get Com Event Log	12	0x1C
Report Slave ID	17	0x11
Read Device Identification	43	0x2B

**see specification for complete listing of functions and definitions* [2]

DATA TYPES

[2]

EXAMPLE MESSAGES

WRITE SINGLE REGISTER (Address: 1, Value: 100)

	Code	Adx Hi	Adx Lo	Val Hi	Val Lo
Request	0x06	0x00	0x01	0x00	0x64
Response	0x06	0x00	0x01	0x00	0x64

READ COILS (Address: 20, Quantity: 16)

	Code	Adx Hi	Adx Lo	Qty Hi	Qty Lo
Request	0x01	0x00	0x14	0x00	0x10

	Code	Bytes	Coils (20-27)	Coils (28-35)
Response	0x01	0x02	b'10101111	b'00001111

MITRE | Caldera™ for OT

https://www.github.com/mitre/caldera-ot

REFERENCES

[1] The Modbus Organization. (2023). *Modbus FAQ*, modbus.org/faq.php

[2] The Modbus Organization. (2012, Apr 26). *Modbus Application Protocol Specification V1.1b3*, https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf