Modbus and HART

Quick reference for instrumentation and control engineers

ib

instrumentationblog.in

Function codes

Code	Action
01	Read coils
02	Read discrete inputs
03	Read holding registers
04	Read input registers
05	Write single coil
06	Write single register
15	Write multiple coils
16	Write multiple registers

Register numbering

Type	Doc. number	Access
Coils	0xxxx	Read/write bit
Discrete inputs	1xxxx	Read bit
Input registers	3xxxx	Read 16 bit
Holding registers	4xxxx	Read/write 16 bit

Protocol addresses are 0 based: 40001 is holding register address 0.

RTU frame

Frame	**Address | Function | Data | CRC (low byte first)**
Slave address	**1 to 247 (0 = broadcast)**
Character	**11 bits (start, 8 data, parity or 2nd stop, stop)**
Frame gap	**≥ 3.5 character times**
CRC	**CRC 16, polynomial 0xA001 (reflected)**

Modbus TCP

Port	**502**
Header (MBAP)	**7 bytes: transaction, protocol, length, unit ID**
Error check	**By TCP (no CRC)**

Floats and longs

- 32 bit values use two registers.
- IEEE 754 float; word order varies by device (big or little endian, swapped).
- If values look huge or tiny, try swapping words.

RS485 rules

- Daisy chain, no stars; short stubs.
- 120 Ω termination at both ends only.
- Bias resistors at one point.
- 32 unit loads per segment; up to about 1200 m at low baud.
- Twisted pair plus common reference; screen earthed at one point.

HART essentials

Signal	**FSK 1200 Hz = 1, 2200 Hz = 0, 1200 bit/s**
Loop resistance	**≥ 250 Ω (typically 230 to 1100 Ω)**
Connect	**Across the transmitter or the loop resistor**

Common HART commands

No	Command
0	Read unique identifier
1	Read primary variable
2	Read loop current and % range
3	Read dynamic variables and current
6	Write polling address
12	Read message
13	Read tag, descriptor, date
15	Read device information
17	Write message
18	Write tag, descriptor, date

Troubleshooting

- No response: address, baud, parity, A/B swapped, termination.
- CRC errors: noise, grounding, wrong baud or stubs.
- Wrong values: register offset of one, word order, scaling.