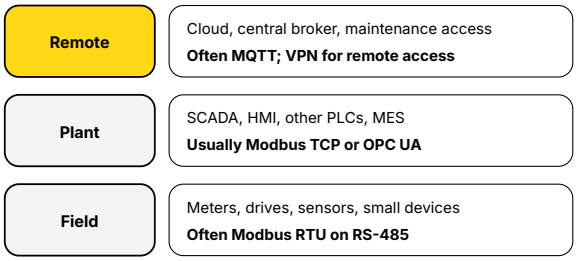
# Choosing a PLC, part 2: which communications you really need

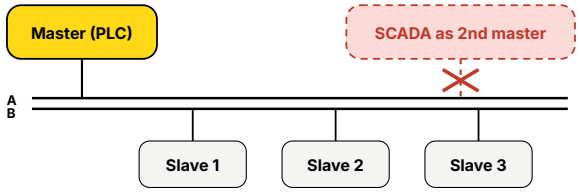
A long protocol list tells you what the PLC supports, not what your installation needs. Before you compare models, answer six questions for every link. Valid for any PLC; part 1 covers the I/O count.

## Three layers, one master per line




Common choices, not rules: the manual of each device decides.

**Talk to what:** list the devices of each layer and the protocol each one speaks. The PLC needs a port and a protocol for every link that matters.




One master on the line at a time. Slave addresses 1 to 247.

PLC polls the devices and a SCADA polls the PLC? Two lines.

Source: Modbus over Serial Line V1.02, section 2.1.

**Who asks:** on a Modbus RTU line only one master asks at a time. A second master on the same pair causes collisions.

### Write the list before the datasheet

Fill in device, protocol, role, distance, ports at once, data and remote access for each link. Then compare the datasheets against that list.

### A gateway is one more device

A protocol gateway can cover a missing port or protocol. Count it as one more device to configure, power and maintain.

## Six questions, before you choose

| Question | What to define | Good answer |
|---|---|---|
| **1. Talk to what?** | Devices by layer: field (meters, drives, sensors), plant (SCADA, HMI, PLCs), remote (cloud, maintenance). Protocol from each manual. | A list of devices with their protocol. |
| **2. Who asks?** | One master per Modbus RTU line: the PLC that polls the devices, or a SCADA that polls the PLC. | One master per line, unique slave addresses. |
| **3. Distance and site** | Copper Ethernet: 100 m per segment. RS-485: up to 1000 m at 9600 baud with AWG26 or wider. No cable: test the radio on site. | Every link within its limit, or a radio test done. |
| **4. Ports at once** | Links that run at the same time: serial lines, Ethernet, Wi-Fi, modem. Master on one bus and slave on another: two serial ports, or a gateway. | Ports counted for simultaneous use. |
| **5. Data** | How many values and how often. Few values, rarely: LoRaWAN or NB-IoT can fit. Fast or heavy: usually Ethernet. | Volume and period written for each link. |
| **6. Security** | Plain Modbus has no built-in security: keep it in a segmented plant network. Remote: VPN, OPC UA security or MQTT over TLS. | Nothing unprotected exposed outside the plant. |

## Common mistakes when choosing communications

| Mistake | What can happen | Question to ask |
|---|---|---|
| **Choosing by the length of the protocol list** | The PLC supports protocols the plant does not use and lacks a port it needs. | Question 1. |
| **Two masters on one Modbus RTU line** | Collisions and timeouts that look like wiring faults. | Question 2. |
| **PLC as master and slave on one serial port** | One line cannot take both roles; you need a second port or a gateway. | Questions 2 and 4. |
| **Copper Ethernet run longer than 100 m** | Errors or no link. Add a switch or use fibre. | Question 3. |
| **Radio chosen from the datasheet range** | Range on site can be much lower: walls, metal, antenna position. | Question 3; test on site. |
| **LoRaWAN or NB-IoT for fast or heavy data** | Messages delayed or limited by airtime and duty cycle. | Question 5. |
| **Modbus TCP reachable from the internet** | Whoever reaches the port can read and write registers. | Question 6. |

### Figures with a source

- Modbus serial line: one master at a time, slave addresses 1 to 247, up to 32 devices without a repeater.
- RS-485: up to 1000 m at 9600 baud with AWG26 or wider cable.
- Twisted pair Ethernet: 100 m per segment.

### Ports worth knowing

Modbus TCP: 502. Modbus/TCP Security (TLS): 802.

MQTT: 1883 without TLS, 8883 with TLS.

Open in the plant firewall only what each link needs.

### Worksheet for each link

- Device and protocol.
- Role of the PLC: master or slave.
- Distance and environment.
- Other links active at the same time.
- Data, period and response time.
- Remote access and how it is protected.

### Typical, not a rule

The protocols per layer are common choices. Some field devices speak Modbus TCP and some plants use other buses.

The manual of each device decides what the PLC must speak.

References: Modbus Organization, Modbus over Serial Line Specification and Implementation Guide V1.02 (sections 2.1, 3.4); Modbus Organization, Modbus/TCP Security Protocol Specification; IEEE 802.3 (twisted pair segment length); OASIS MQTT Version 5.0; OPC Foundation, OPC 10000-1 OPC UA Overview and Concepts; LoRa Alliance, About LoRaWAN; 3GPP, The Cellular Internet of Things. Device manuals and local regulations take precedence over this general guide.