Analog Signals

4-20mA Current Loop

- 2-wire loop, 24VDC supply
- Good for long runs, noise immunity
- Example: chemical storage tank far away from control room

0-10V Voltage Signal

- 3-wire (V+, GND, Signal)
- Low cost, easy to implement
- Short runs only, susceptible to EMI
- Example: Building automation, small-scale machinery

PHYSICAL LAYER

Serial Comms

RS-232

- Point-to-point, ~15m max cable, low speed
- Programming legacy devices, singe HMI to controller
- Example: Laptop plugged directly into VFD

RS-485

- Multi-drop bus, up to 1200m run
- Connects multiple instruments to one PLC
- Terminate both ends with resistors

Digital I/O

Digital Inputs

- 24V=ON/oV=OFF
- Limit/Prox Switches, Photoeye/Pushbuttons

Digital Outputs

- PLC controlled
- Solenoids/Contactors/Indicator lights

NPN vs PNP

- NPN (sinking): Sensor pulls input when ON.
 Common in Asia.
- PNP (sourcing): Sensor provides input when ON. Common in NA/Europe.

Wireless

BLE (Bluetooth Low Energy)

• Wearables for worker safety

ZigBee

- Building automation (lighting, HVAC thermostats)
- LoRaWAN
- Long range, low power sensors for environmental monitoring Wi-Fi
- HMIs and tablets, cameras and data loggers

NB-IoT/LTE-M

• Remote assets where no local network exists

5G

AGVs (Automated Guided Vehicles)

PLC

Use

Discrete control, sequencing, interlocks, safety

Cycle time

• 1-20ms/scan

Language

• Ladder, Function Block, Structured Text, Sequential Function Chart

Vendors

• Rockwell (Allen Bradley), Siemens, Schneider, Mitsubishi, Omron

CNC

Use

• Machine tools (mills, lathes, laser cutters)

Cycle time

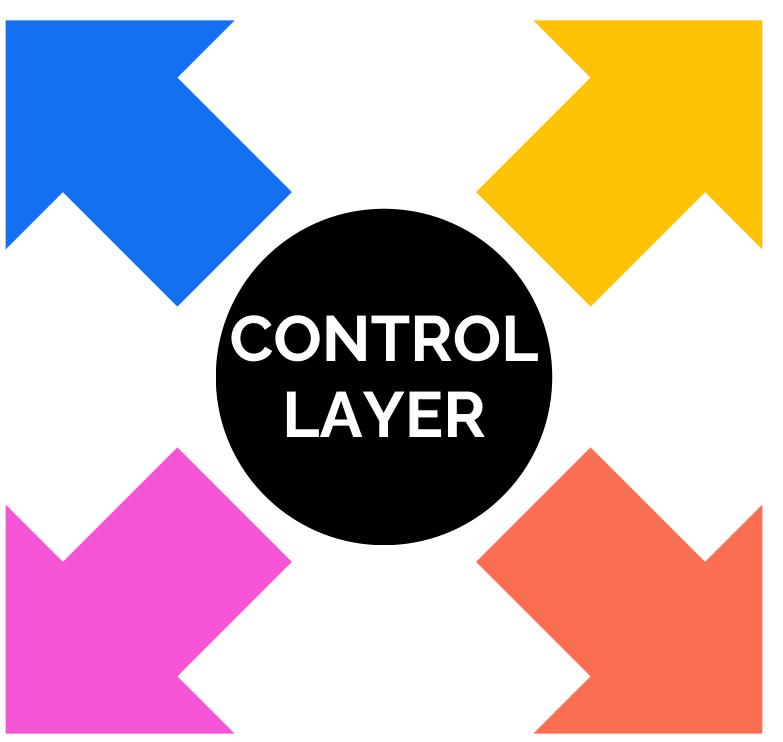
• <1ms loops

Language

• G-code, M-Code, Parametric, STEP-NC

Vendors

• FANUC, Siemens Sinumerik, Haas, Heidenhain



DCS

Use

Continuous process control

Cycle time

• 100-500ms loops

Language

 Function Block Diagrams, Sequential Function Charts, Structured Text

Vendors

Honeywell Experion, Emerson DeltaV,
 Yokogawa Centum, ABB System 800xA

Robots

Use

• Welding, painting, pick-and-place, palletizing, assembly

Cycle time

• 1-4ms servo updates

Language

• KAREL, RAPID, KRL, INFORM, URScript

Vendors

• FANUC, KUKA, ABB, Yaskawa, UR

Modbus

RTU (RS-485)

• Serial, master/slave polling, twisted pair, up to 32 devices/bus. 9600-115200 bps.

TCP (Ethernet variant)

Easier to integrate into IT networks, supports more nodes

Use

• Simple device integration, wide supported across meters, sensors, drives

Example

PLC polls power meter via Modbus RTU to log energy consumption

Profinet

NRT (Non Real Time)

• Runs on standard TCP/IP, diagnostics, configuration, file transfers

RT (Real Time)

• Bypasses TCP/IP for faster I/O exchange. Cycle time 1ms for standard I/O and control applications

IRT (Isochronous Real Time)

• Adds time slot + IEEE-1588 PTP synchronization. <1ms update times. Synchronized multi axis motion.

Topology

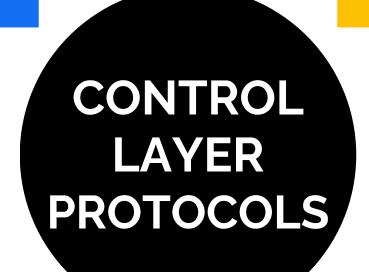
• Star, line, or ring.

Use

• High speed automation, drives, motion systems, large distributed I/O networks

Example

 High speed packaging machines uses Profinet IRT to synchronize multiple servo drives for coordinated, millisecond level motion



Profibus

DP (Discrete Peripherals)

 RS485 fieldbus for PLC <-> I/O communication. Cyclic master/slave exchanges. Widely used in discrete manufacturing. 12Mbps.

PA (Process Automation)

 Runs on MBP physical layer, designed for hazardous/explosive environments. Power + comms over same 2-wire bus.

Use

• Reliable communication with field devices, popular in Europe for both factory and process automation

Example

• Chemical plant uses Profibus PA to connect sensors in explosion-proof zone to control system

Ethernet/IP

CIP (Common Industrial Protocol)

 Object oriented architecture used across different transport layers: Devicenet, Controlnet, Ethernet/IP, Componet

Explicit Messaging (TCP)

 Request/response,for configuration, diagnostics, and less time critical data

Implicit Messaging (UDP)

• Real time, cyclic I/O data exchange between controllers and devices

Use

• Popular in North America, distributed I/O, drives, robots, PLC to PLC links

Example

 Rockwell PLC controls distributed I/O racks and VFDs over Ethernet/IP

OPC UA (Open Platform Communications Unified Architecture)

Type

Standardized, platform independent, client/server or pub/sub

Transport

TCP, HTTPS, MQTT, AMQP

Features

Strong security (TLS, certs, user roles), information modeling (values, metadata, hierarchy, units), Companion specs for industries

Use

Rich data integration between OT systems and IT/cloud

Example

MES queries OPC UA server for production counts, quality metrics, and alarms

MQTT (Message Queuing Telemetry Transport)

Туре

Lightweight pub/sub protocol

Transport

TCP/IP, always client \rightarrow broker

Features

Small footprint, great for IIoT and wireless, QoS levels for delivery guarantees, retained messages and LWT (last will/testament) for device health

Variants

MQTT Sparkplug B: adds standardized payload structure, state management, birth/death certificates

Use

Efficient distribution of plant floor events to many subscribers (cloud, SCADA, MES)

Example

Cloud apps subscribe to topics for analytics and dashboards

AMQP (Advanced Message Queuing Protocol)

Type

Enterprise messaging protocol

Transport

TCP/IP

Features

Queues, routing, filtering, priorities More complex than MQTT but powerful for enterprise scale systems

Use

Situations requiring guaranteed delivery, multi-app routing, financial grade messaging

Example

ERP, historian, mobile alert apps all consume from different queues



Type

Real time pub/sub

Transport

UDP, TCP, shared memory

Features

Fine grained QoS policies (latency, reliability, durability), decentralized

Use

DATA

ACCESS

LAYER

Aerospace, defense, robotics, mission critical distributed control systems

Example

Collaborative robots in assembly line share sensor data and motion states peer to peer using DDS

HTTP/REST

Type

Standard web protocol, request/response model

Transport

HTTPS

Features

Easy to integrate with IT systems and cloud APIs, best for configuration, batch reads, or sending reports. Not ideal for continous real time streams

Use

Configuration, periodic data uploads, integration with cloud services

Example

Gateway sends machine status snapshots every 15min to a REST API endpoint in AWS for production tracking

GATEWAYS

01



03





Protocol Translation

Southbound (OT): Modbus RTU/TCP, Profinet, Ethernet/IP, BACnet, Profibus
Northbound (IT): OPC UA, MQTT, HTTPS, AMQP, DDS

Data Aggregation

Collects signals from multiple devices (PLC1, PLC2, Robot) and packages them into one data model

Normalization, Filtering, Buffering

- Converts raw tags into standardized units.
- Local rules: only send changed values, filter noise, signal compression.
- Buffer during WAN outage, forward once reconnected

Security Boundary

- Terminate TLS/mTLS connections.
- Act as firewall/DMZ between IT and OT. Identity management

Edge Processing

- Run ML inference models, detect anomalies, trigger alarms.
- Pre-aggregate KPIs before sending

ENTERPRISE / CLOUD LAYER



Ingestion

OT data gets ingested into the cloud system

MQTT, REST, Kafka/Event Hubs bring data in

01



Storage

Where data lands and how it's organized

- Hot: real-time, shortterm (TSDB)
- Warm: operational, medium-term (RDS)
- Cold: historical, longterm (Data Lake)

02



Processing

Raw data is transformed, enriched, and analyzed

Stream (real-time), batch (ETL), ML/AI models

03

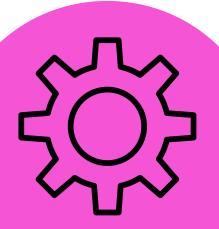


Serving

Data is consumed for business value

Dashboards, MES/ERP, APIs, alerts

04



Governance

Rules and infrastructure to ensure trust and compliance

Security, schemas, compliance, observability

05