Industrial Network Fundamentals

Understanding OT network technologies, topologies, and fieldbus systems

OT Security Learning Series

Document 070 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Industrial networks connect field devices, controllers, and supervisory systems in OT environments. Unlike IT networks optimized for data throughput, industrial networks prioritize **determinism**, **reliability**, and **real-time performance** for process control.

Understanding industrial networking is essential for OT security because:

- Network architecture affects segmentation strategies
- Legacy protocols lack security features
- Physical layer differences impact monitoring capabilities
- Redundancy mechanisms must be preserved during security implementations

2 Network Topologies

Industrial networks use various topologies based on reliability, cost, and application requirements.

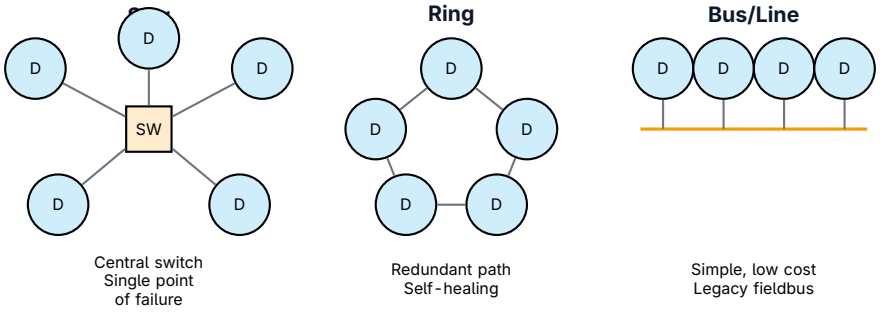

Figure 1: Common Industrial Network Topologies

Topology	Redundancy	Cost	Common Use
Star	None (single switch)	Medium	Ethernet networks
Ring	High (dual path)	Higher	Critical systems
Bus/Line	None	Low	Legacy fieldbus
Mesh	Very high	Highest	Wireless, critical

Table 1: Topology Comparison

3 Serial Communications

Many legacy industrial systems use serial communications for device connectivity.

3.1 RS-232

- Point-to-point communication only
- Short distance (typically $<$ 15 meters)
- Common for HMI-to-PLC connections, programming ports
- Speeds up to 115.2 kbps

3.2 RS-485

- Multi-drop bus supporting up to 32 devices
- Longer distances (up to 1200 meters)
- Half-duplex or full-duplex operation
- Basis for Modbus RTU and many fieldbus protocols
- Speeds up to 10 Mbps (distance dependent)

Warning

Security Note: Serial protocols typically have **no authentication or encryption**. Physical access to the bus allows reading and injecting traffic. Serial-to-Ethernet converters can expose these insecure protocols to IP networks.

4 Fieldbus Technologies

Fieldbus networks connect sensors, actuators, and controllers at the field level.

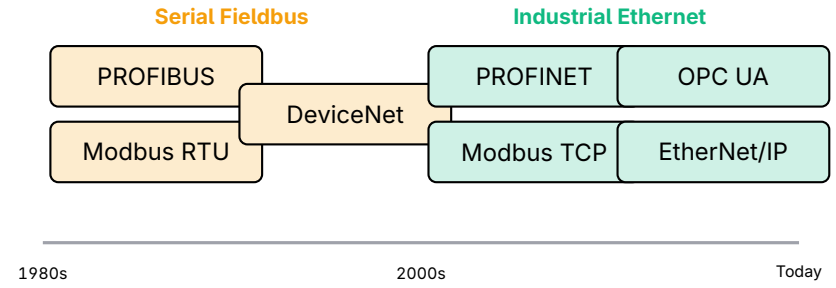

Figure 2: Evolution from Serial Fieldbus to Industrial Ethernet

4.1 Legacy Fieldbus

5 Industrial Ethernet

Industrial Ethernet adapts standard Ethernet for factory and process automation with enhanced reliability and real-time capabilities.

Protocol	Physical Layer	Typical Use
Modbus RTU	RS-485	Universal, simple I/O
PROFIBUS DP	RS-485	Siemens environments
DeviceNet	CAN bus	Rockwell/Allen-Bradley
Foundation Fieldbus	H1 (31.25 kbps)	Process instrumentation
HART	4-20mA analog + digital	Smart instruments

Table 2: Common Serial Fieldbus Protocols

5.1 Key Differences from IT Ethernet

- **Deterministic timing** – Guaranteed message delivery within defined time
- **Ruggedized hardware** – Extended temperature, vibration, EMI resistance
- **Ring redundancy** – Sub-50ms failover (MRP, HSR, PRP)
- **Application layer protocols** – Industrial-specific (not just TCP/IP)

5.2 Common Industrial Ethernet Protocols

Protocol	Vendor/Org	Real-Time Method
EtherNet/IP	ODVA (Rockwell)	Standard TCP/IP + CIP
PROFINET	Siemens/PI	IRT (Isochronous Real-Time)
Modbus TCP	Modbus.org	Standard TCP/IP
EtherCAT	Beckhoff/ETG	Processing on the fly
OPC UA	OPC Foundation	Pub/Sub, TSN

Table 3: Industrial Ethernet Protocols

6 Network Redundancy

Industrial networks implement redundancy to ensure availability of critical control functions.

Common Redundancy Protocols

- **MRP** (Media Redundancy Protocol) – Ring topology, $<$200ms recovery
- **RSTP** (Rapid Spanning Tree) – Standard Ethernet, $<$2s recovery
- **HSR** (High-availability Seamless Redundancy) – Zero recovery time
- **PRP** (Parallel Redundancy Protocol) – Dual parallel networks

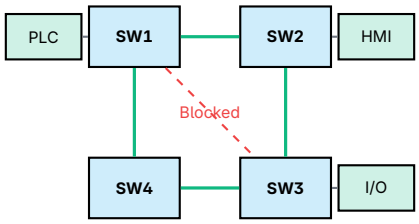

Figure 3: Media Redundancy Protocol (MRP) Ring Topology

7 Security Considerations

Critical

Industrial networks often lack basic security controls. Many protocols were designed decades ago without security considerations and cannot be easily updated due to availability requirements.

7.1 Common Vulnerabilities

- **No authentication** – Most fieldbus protocols accept any command
- **No encryption** – Traffic readable by anyone on the network
- **Flat networks** – No segmentation between zones
- **Legacy devices** – Cannot be patched or upgraded
- **Broadcast traffic** – Easy reconnaissance via passive sniffing

7.2 Security Best Practices

Key Point

Network Security Measures:

- Segment networks by function and criticality (zones and conduits)
- Deploy industrial firewalls at zone boundaries
- Use managed switches with port security, VLANs
- Implement network monitoring and anomaly detection
- Disable unused ports and services
- Consider encrypted tunnels for sensitive traffic

8 Summary

Key Takeaways

- **Topology matters** – Star, ring, and bus have different reliability profiles
- **Serial still exists** – RS-485 and fieldbus remain common in brownfield sites
- **Industrial Ethernet differs** – Determinism and redundancy, not just TCP/IP
- **Redundancy is critical** – MRP, HSR, PRP ensure availability
- **Legacy = insecure** – Most industrial protocols lack authentication/encryption
- **Segment and monitor** – Compensating controls for protocol weaknesses

9 Further Reading

Standards and Guidelines

- **IEC 62439** – Industrial communication networks – High availability
  https://webstore.iec.ch/publication/6990
- **IEC 62443-3-2** – Security risk assessment for system design
  https://webstore.iec.ch/publication/30727

Resources

- **ODVA** – EtherNet/IP specifications
  https://www.odva.org/
- **PROFIBUS/PROFINET International**
  https://www.profibus.com/

Books

- Zurawski, R. – *Industrial Communication Technology Handbook* (CRC Press)
- Galloway, B. & Hancke, G. – *Introduction to Industrial Control Networks* (IEEE)

Part of the OT Security Learning Series