PROFINET Protocol

Industrial Ethernet standard for Siemens and European automation

OT Security Learning Series

Document 204 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

PROFINET (Process Field Network) is the industrial Ethernet standard developed by Siemens and PROFIBUS International. It is the dominant industrial protocol in European manufacturing and widely used globally with Siemens automation systems.

Key characteristics:

- Real-time Ethernet communication
- Successor to PROFIBUS fieldbus
- Three performance classes (RT, IRT, NRT)
- Supports motion control and isochronous applications
- Managed by PROFIBUS & PROFINET International (PI)

2 Protocol Architecture

2.1 Communication Classes

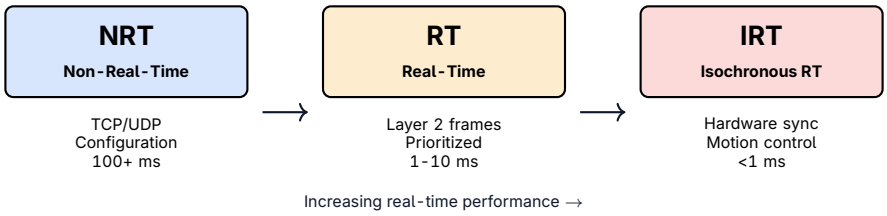

Figure 1: PROFINET Communication Classes

2.2 Protocol Stack

- **NRT Channel** – Standard TCP/IP for parameterization, diagnostics
- **RT Channel** – Layer 2 Ethernet frames (EtherType 0x8892)
- **IRT Channel** – Time-synchronized slots, requires special hardware

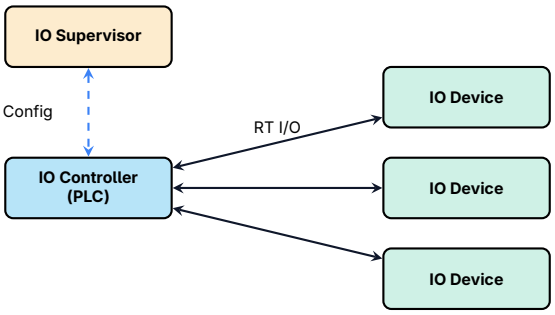

Figure 2: PROFINET Device Roles

2.3 Device Roles

PROFINET Device Types

- **IO Controller** – PLC that controls the process (master)
- **IO Device** – Field device providing I/O data (slave)
- **IO Supervisor** – Engineering/diagnostic station

3 Network Identification

3.1 Ports and Protocols

Port/Type	Protocol	Purpose
EtherType 0x8892	PROFINET RT	Real-time I/O data
UDP/34964	PROFINET DCP	Discovery, configuration
TCP/102	ISO-TSAP (S7)	Often used alongside
UDP/161	SNMP	Device management
TCP/80/443	HTTP/HTTPS	Web interface

Table 1: PROFINET Network Identifiers

3.2 Discovery and Configuration Protocol (DCP)

DCP is used for:

- Device discovery on the network
- Setting device names and IP addresses
- Identifying devices by MAC address
- Reading device information

Warning

DCP operates at Layer 2 and has no authentication. Any device on the same network segment can discover and reconfigure PROFINET devices.

4 PROFINET Communication

4.1 Application Relations (AR)

Communication is organized into Application Relations:

- **IO AR** – Cyclic I/O data exchange
- **Supervisor AR** – Diagnostic and configuration access
- **Device Access AR** – Device-level management

4.2 Cyclic Data Exchange

1. Controller establishes AR with device
2. Controller sends output data in RT frames
3. Device responds with input data
4. Cycle repeats at configured interval
5. Watchdog monitors communication health

5 Security Vulnerabilities

Critical

PROFINET was designed before cybersecurity was a primary concern. The protocol lacks authentication, encryption, and integrity protection in its base specification.

5.1 Protocol Weaknesses

- **No authentication** – Any device can act as controller
- **No encryption** – All data transmitted in cleartext
- **DCP vulnerabilities** – Unauthenticated device configuration
- **Layer 2 attacks** – RT traffic bypasses IP-based firewalls
- **Predictable timing** – IRT schedules can be analyzed

5.2 Known Attack Vectors

- **DCP attacks** – Change device names/IPs to disrupt communication
- **AR hijacking** – Take over controller role
- **I/O injection** – Send fake RT frames to devices

- **Denial of service** – Flood network with RT traffic
- **Network mapping** – Use DCP to enumerate all devices
- **Man-in-the-middle** – Intercept and modify RT traffic

6 PROFINET Security Extensions

6.1 PROFINET Security Class 1

PI has developed security extensions:

- Integrity protection for RT communication
- Authentication of devices
- Based on IEC 62443 requirements
- Requires compatible devices

6.2 Secure Communication

Newer implementations support:

- TLS for NRT/TCP communications
- SNMPv3 for secure management
- Secure DCP (authenticated configuration)
- Certificate-based device identity

Warning

Security extensions require newer hardware and software. Most existing installations lack these capabilities and must rely on network-level protection.

7 Security Mitigations

7.1 Network Architecture

Key Point

Since PROFINET RT uses Layer 2 frames, standard IP firewalls cannot filter this traffic. Use Layer 2 segmentation and PROFINET-aware security devices.

- **VLAN segmentation** – Isolate PROFINET traffic
- **Managed switches** – Control port access, disable unused ports
- **Industrial firewalls** – PROFINET-aware deep packet inspection

- **Cell protection** – Segment network into isolated cells

7.2 Device Hardening

- Disable unused services (HTTP, SNMP, Telnet)
- Use strong passwords for web interfaces
- Enable SNMPv3 instead of v1/v2c
- Keep firmware updated
- Disable DCP if static configuration is acceptable

7.3 Monitoring

- Monitor for unexpected DCP requests
- Alert on new devices appearing on network
- Baseline normal RT traffic patterns
- Detect AR establishment from unauthorized sources
- Watch for configuration changes

8 Common Implementations

- **Siemens** – S7-1200, S7-1500 PLCs, ET 200 I/O
- **Drives** – SINAMICS variable frequency drives
- **HMI** – SIMATIC HMI panels
- **Third-party** – Many vendors support PROFINET
- **Motion control** – Servo drives with IRT

9 Summary

Key Takeaways

- **Siemens ecosystem** – Dominant in European automation
- **Three classes** – NRT, RT, IRT for different timing needs
- **Layer 2 RT traffic** – Bypasses IP firewalls
- **DCP risks** – Unauthenticated discovery and configuration
- **No native security** – Base protocol lacks protection
- **Security extensions** – Available but limited adoption
- **VLAN segmentation** – Critical for protection

10 Further Reading

Standards

- **PROFIBUS & PROFINET International**
  https://www.profibus.com/
- **IEC 61158/61784** – PROFINET standards
  https://webstore.iec.ch/

Resources

- **Siemens Industrial Security**
  https://www.siemens.com/global/en/products/automation/topic-areas/industrial-security.html
- **CISA – ICS Advisories**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series