OT Network Monitoring

Visibility and Detection in Industrial Networks

OT Security Learning Series

Document 500 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Network monitoring in OT environments provides visibility into industrial communications, enabling detection of anomalies, threats, and operational issues. Unlike IT monitoring, OT monitoring must account for specialized protocols, safety constraints, and the critical nature of industrial processes.

Information

You cannot protect what you cannot see. OT network monitoring is foundational to any industrial security program—it enables asset discovery, threat detection, and incident response.

1.1 Key Differences from IT Monitoring

- **Passive only:** Active scanning can disrupt OT devices
- **Protocol awareness:** Must understand Modbus, DNP3, OPC, etc.
- **Process context:** Security events need operational context
- **Availability focus:** Monitoring must not impact operations

2 Monitoring Approaches

2.1 Passive Network Monitoring

Key Point

Passive monitoring is the preferred approach for OT:

- Listens to network traffic without injecting packets
- No risk of disrupting sensitive control systems
- Uses SPAN ports, TAPs, or packet brokers
- Can decode industrial protocols for deep inspection

2.2 Active vs Passive Comparison

Aspect	Passive	Active
Impact on OT	None	Can crash devices
Discovery	Traffic-based	Query-based
Coverage	Only active communications	All addressable devices
Protocol support	Deep inspection	Limited
Recommended	Yes	Only with caution

Critical

Active scanning (Nmap, vulnerability scanners) can crash PLCs and other OT devices. Never perform active scanning in OT without explicit approval, testing, and during maintenance windows.

3 Data Collection Methods

3.1 Network TAPs

- **Hardware devices** that copy traffic without interruption
- **Fail-safe:** Network continues if TAP loses power
- **Full duplex:** Captures both directions of traffic
- **Recommended** for critical OT network segments

3.2 SPAN/Mirror Ports

- **Switch feature** that copies traffic to monitoring port
- **Lower cost** than dedicated TAPs
- **Limitations:** May drop packets under load
- **Suitable** for less critical segments

3.3 Strategic Placement

Monitor at key network boundaries:

- **IT/OT boundary:** DMZ firewalls, data diodes
- **Zone boundaries:** Between Purdue levels
- **Critical assets:** Historians, engineering workstations
- **Remote access:** VPN and jump server traffic

4 Detection Capabilities

4.1 Asset Discovery

Passive monitoring reveals:

- IP and MAC addresses of communicating devices
- Device types and vendors (from protocol fingerprinting)
- Communication patterns and relationships

- New or unauthorized devices on the network

4.2 Threat Detection

Detectable Threats

- **Reconnaissance:** Port scans, protocol enumeration
- **Unauthorized access:** New connections, failed authentication
- **Malicious commands:** Dangerous write operations to PLCs
- **Lateral movement:** Unusual communication patterns
- **Data exfiltration:** Large transfers, unusual destinations
- **Malware C2:** Known bad IPs, DNS anomalies

4.3 Operational Anomalies

- **Protocol violations:** Malformed packets, invalid commands
- **Timing anomalies:** Unusual polling intervals
- **Configuration changes:** PLC logic modifications
- **Network issues:** Retransmissions, packet loss

5 Implementation Considerations

5.1 Protocol Support

Ensure monitoring solution supports your protocols:

Category	Protocols
Process Control	Modbus, DNP3, IEC 60870-5-104, IEC 61850
Industrial Ethernet	EtherNet/IP, PROFINET, Modbus TCP
Building Automation	BACnet, LonWorks
Enterprise Integration	OPC UA, OPC DA

5.2 Integration Points

- **SIEM integration:** Forward alerts to security operations
- **Asset management:** Sync discovered assets to inventory
- **Ticketing systems:** Create incidents for investigation
- **Historian data:** Correlate network events with process data

5.3 Challenges

Warning

Common OT monitoring challenges:

- Encrypted traffic (OPC UA, TLS) limits visibility
- High-volume networks require significant storage
- Proprietary protocols may lack decoder support
- Alert tuning needed to reduce false positives

6 Further Reading

Standards

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-3-3** – System Security Requirements
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA** – ICS Network Monitoring
  https://www.cisa.gov/resources-tools/resources
- **MITRE ATT&CK for ICS**
  https://attack.mitre.org/techniques/ics/