Intrusion Detection for OT

IDS/IPS deployment strategies for industrial environments

OT Security Learning Series

Document 520 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 IDS vs IPS in OT **3**
2.1 Deployment Modes 4

3 Detection Methods **4**
3.1 Signature-Based Detection 4
3.2 Anomaly-Based Detection 4
3.3 Protocol-Aware Detection 5

4 OT-Specific Considerations **5**
4.1 Industrial Protocol Support 5
4.2 Baseline Considerations 5

5 Deployment Architecture **6**
5.1 Sensor Placement 6
5.2 Key Monitoring Points 6

6 Implementation Best Practices **6**
6.1 Deployment Checklist 6
6.2 Alert Management 7
6.3 IPS Deployment (If Required) 7

7 Integration Points **7**

8 Summary **8**

9 Further Reading **8**

1 Introduction

Information

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network traffic for malicious activity. In OT environments, these systems must understand industrial protocols and prioritize availability over aggressive blocking.

Key differences in OT intrusion detection:

- **Protocol awareness:** Must parse Modbus, DNP3, OPC, EtherNet/IP, etc.
- **Availability focus:** False positives can disrupt operations
- **Passive preferred:** Active blocking requires careful consideration
- **Deterministic traffic:** OT traffic patterns are predictable
- **Long baselines:** Systems run unchanged for extended periods

2 IDS vs IPS in OT

Aspect	IDS (Detection)	IPS (Prevention)
Action	Alert only	Block malicious traffic
Deployment	Passive (SPAN/TAP)	Inline
Availability risk	Low	Higher (can block legitimate)
Response time	Human review required	Immediate automated response
OT suitability	Preferred for OT	Use with caution

Table 1: IDS vs IPS Comparison

Warning

IPS Caution in OT: Inline IPS can block legitimate traffic due to false positives, potentially disrupting critical processes. Most OT environments use IDS (detection) rather than IPS (prevention) to avoid availability impacts.

2.1 Deployment Modes

Figure 1: IDS (Passive) vs IPS (Inline) Deployment

3 Detection Methods

3.1 Signature-Based Detection

Signature-Based Detection

Compares network traffic against a database of known attack patterns (signatures). Effective for known threats but cannot detect novel attacks.

- **Pros:** Low false positives, well-understood, fast
- **Cons:** Requires signature updates, misses zero-days
- **OT consideration:** Need OT-specific signatures (Modbus exploits, etc.)

3.2 Anomaly-Based Detection

Anomaly-Based Detection

Establishes a baseline of "normal" behavior and alerts on deviations. Can detect novel attacks but may generate more false positives.

- **Pros:** Detects unknown attacks, learns environment
- **Cons:** Higher false positive rate, requires tuning
- **OT advantage:** OT traffic is predictable—anomalies stand out

3.3 Protocol-Aware Detection

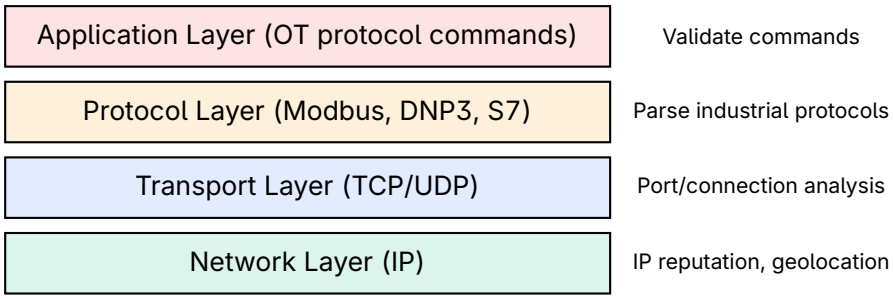

Figure 2: Deep Packet Inspection for OT Protocols

Key Point

OT Protocol Inspection Examples:

- Detect unauthorized Modbus write commands to PLCs
- Alert on DNP3 commands from unexpected sources
- Identify firmware upload attempts via S7comm
- Flag changes to safety system parameters

4 OT-Specific Considerations

4.1 Industrial Protocol Support

Essential protocol support for OT IDS:

Protocol	Detection Capabilities
Modbus TCP/RTU	Function codes, register addresses, read vs write
DNP3	Object types, data link layer, secure authentication
EtherNet/IP	CIP commands, tag access, configuration changes
OPC UA/DA	Node access, browse requests, write operations
S7comm	Block transfers, program downloads, start/stop
IEC 61850/GOOSE	Substation communications, control commands
BACnet	Building automation, property writes

Table 2: OT Protocol Detection Capabilities

4.2 Baseline Considerations

- **Learning period:** Allow sufficient time to capture normal operations
- **Operational modes:** Include startup, shutdown, maintenance periods
- **Seasonal variations:** Some processes vary by time of year
- **Update on changes:** Re-baseline after legitimate modifications

Warning

Baseline Risks: If the network is already compromised during baseline creation, malicious traffic may be learned as "normal." Conduct security assessment before establishing baselines.

5 Deployment Architecture

5.1 Sensor Placement

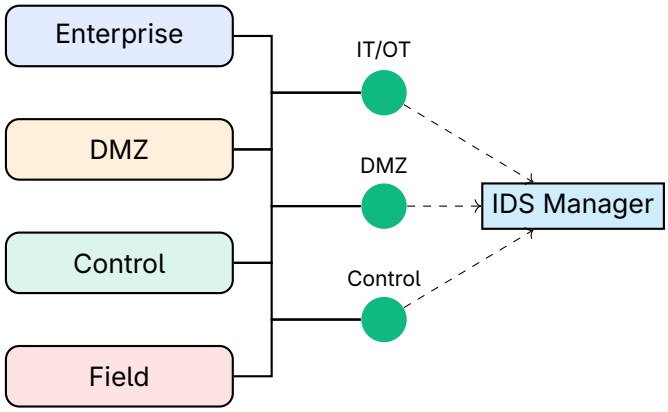

Figure 3: IDS Sensor Placement by Zone

5.2 Key Monitoring Points

Location	Monitoring Focus
IT/OT boundary	North-south traffic, unauthorized access attempts
DMZ connections	Data transfers, remote access sessions
Control network	East-west OT traffic, protocol anomalies
Engineering workstations	Configuration changes, downloads to PLCs
Remote access points	VPN sessions, jump server activity

Table 3: Key IDS Monitoring Points

6 Implementation Best Practices

6.1 Deployment Checklist

1. **Assess before deploying:** Understand network architecture first
2. **Start in detection mode:** Alert only, no blocking initially
3. **Allow adequate baseline:** Capture normal operational patterns
4. **Tune aggressively:** Reduce false positives before expanding

5. **Integrate with SIEM:** Correlate with other security data
6. **Define response procedures:** Know what to do with alerts
7. **Test regularly:** Verify detection capabilities

6.2 Alert Management

Tip

Reducing Alert Fatigue:

- Prioritize alerts by asset criticality
- Suppress known false positives
- Correlate related events into single incidents
- Route OT alerts to personnel who understand the context
- Establish clear escalation procedures

6.3 IPS Deployment (If Required)

If inline prevention is required:

- **Fail-open mode:** If IPS fails, traffic continues
- **Whitelist approach:** Block only confirmed threats
- **Test extensively:** Validate in lab before production
- **Bypass capability:** Ability to disable quickly if issues
- **High availability:** Redundant deployment for critical paths

7 Integration Points

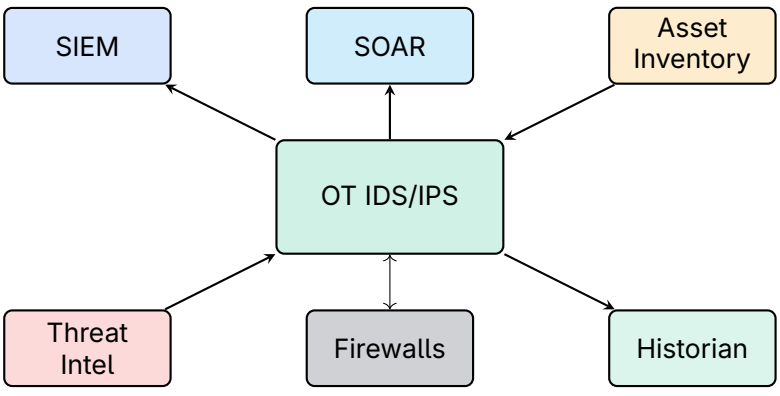

Figure 4: IDS Integration Architecture

8 Summary

Key Takeaways

- **Detection over prevention:** IDS preferred over IPS in OT
- **Protocol awareness:** Must understand Modbus, DNP3, etc.
- **Anomaly detection:** OT traffic predictability is an advantage
- **Strategic placement:** Monitor zone boundaries and critical segments
- **Baseline carefully:** Ensure network is clean before learning
- **Tune thoroughly:** Reduce false positives before expanding
- **Integrate:** Connect to SIEM, asset inventory, threat intel

9 Further Reading

Standards

- **IEC 62443-3-3** – System security requirements and security levels
  https://webstore.iec.ch/publication/7033
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Industrial Control Systems Detection and Response
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS** – ICS Security Resources
  https://www.sans.org/cybersecurity-focus-areas/industrial-control-systems-security

Part of the OT Security Learning Series