Anomaly Detection in OT

Behavioral analysis for industrial security monitoring

OT Security Learning Series

Document 540 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Anomaly detection identifies deviations from established normal behavior. OT environments are ideal for anomaly detection because industrial processes are predictable, repetitive, and change slowly—making unusual activity easier to spot.

Why anomaly detection is powerful for OT:

- **Predictable traffic:** PLCs communicate in consistent patterns
- **Stable configurations:** Systems rarely change once deployed
- **Defined processes:** Operations follow predictable cycles
- **Novel attack detection:** Can find threats without signatures
- **Insider threat detection:** Identifies unusual authorized user activity

2 Types of Anomaly Detection

2.1 Detection Categories

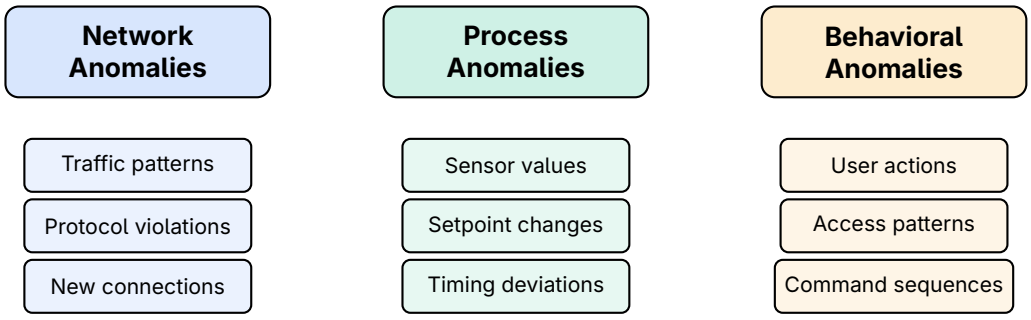

Figure 1: Categories of Anomaly Detection in OT

2.2 Network Anomalies

Network-Based Anomaly Detection

Monitors network traffic patterns to identify unusual communications, new devices, unexpected protocols, or abnormal data volumes.

Detectable network anomalies:

- New device on OT network (unauthorized asset)
- Communication between devices that never communicated before
- Unusual traffic volume or timing patterns

- Protocol violations or malformed packets
- Connections to external/internet addresses
- Port scans or reconnaissance activity

2.3 Process Anomalies

Process-Based Anomaly Detection

Analyzes physical process data (sensor values, control signals) to detect deviations that may indicate attacks or equipment problems.

Detectable process anomalies:

- Sensor values outside normal operating ranges
- Unexpected setpoint modifications
- Control commands inconsistent with process state
- Timing anomalies in control loops
- Correlation breaks between related variables

2.4 Behavioral Anomalies

Behavioral Anomaly Detection

Tracks user and system behavior to identify actions that deviate from established patterns, potentially indicating compromise or insider threats.

Detectable behavioral anomalies:

- User accessing systems outside normal hours
- Unusual command sequences from operators
- Access to assets outside normal job function
- Excessive data downloads or queries
- Login from unusual locations

3 OT-Specific Advantages

3.1 Why OT is Ideal for Anomaly Detection

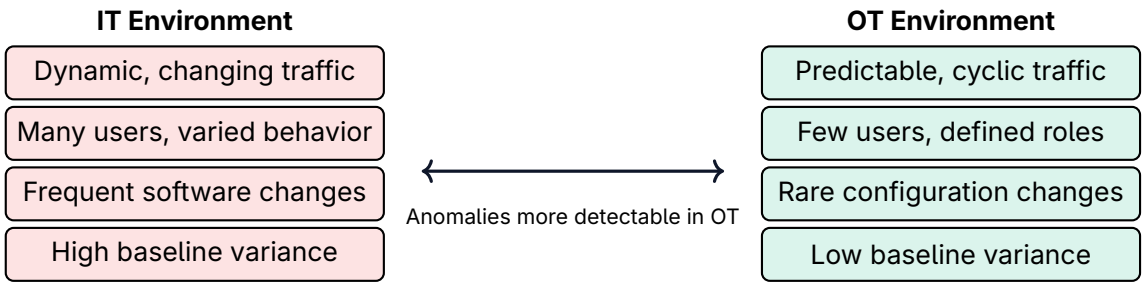

Figure 2: IT vs OT Anomaly Detection Suitability

Key Point

OT Anomaly Detection Advantages:

- PLCs poll sensors at fixed intervals—timing anomalies are obvious
- Communication pairs are static—new connections stand out
- Process values follow physical laws—violations indicate problems
- Operators follow procedures—deviations may indicate compromise

4 Detection Techniques

4.1 Statistical Methods

Method	Application
Threshold-based	Alert when values exceed defined limits
Standard deviation	Flag values outside N standard deviations
Moving average	Detect sudden changes from recent baseline
Seasonal patterns	Account for time-of-day, day-of-week variations
Correlation analysis	Identify breaks in related variable relationships

Table 1: Statistical Anomaly Detection Methods

4.2 Machine Learning Approaches

Approach	Description
Clustering	Group similar behaviors, flag outliers
Autoencoders	Learn to reconstruct normal data, flag reconstruction errors
One-class SVM	Model normal class boundary, detect outside points
LSTM networks	Learn temporal sequences, detect sequence breaks
Isolation forests	Efficiently identify outliers in high-dimensional data

Table 2: Machine Learning for Anomaly Detection

Warning

ML Model Considerations:

- Training data must represent true "normal" (not already compromised)
- Models need retraining after legitimate system changes
- Black-box models may be difficult to explain to operators
- False positive rates must be acceptable for OT operations

4.3 Rule-Based Detection

- **Whitelist approach:** Define allowed behaviors, alert on anything else
- **Communication matrix:** Specify valid source/destination/protocol combinations
- **Command validation:** Verify commands are appropriate for current process state
- **Sequence rules:** Define valid command sequences, flag violations

5 Baseline Development

5.1 Creating Effective Baselines

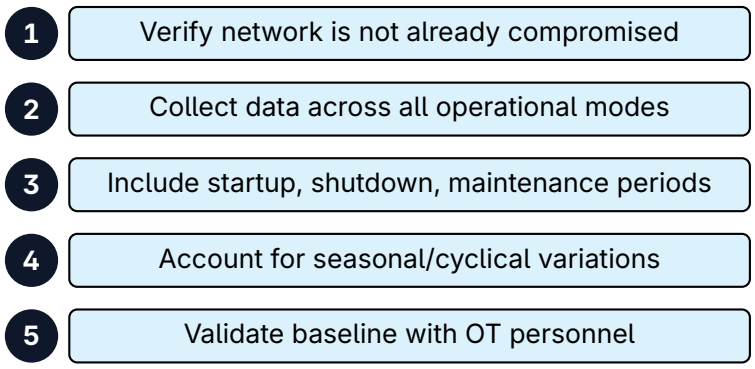

Figure 3: Baseline Development Process

5.2 Baseline Elements

Element	What to Capture
Communication pairs	Source IP, dest IP, ports, protocols
Traffic volume	Bytes/packets per time period
Timing patterns	Request/response intervals, polling rates
Protocol content	Function codes, register addresses
User behavior	Login times, systems accessed, commands used
Process values	Normal ranges, correlations, trends

Table 3: Baseline Elements for OT Anomaly Detection

Tip

Baseline Duration: Capture at least 2–4 weeks of normal operations, including any scheduled maintenance periods. For seasonal processes, longer baselines may be needed.

6 Implementation Architecture

6.1 Data Collection Points

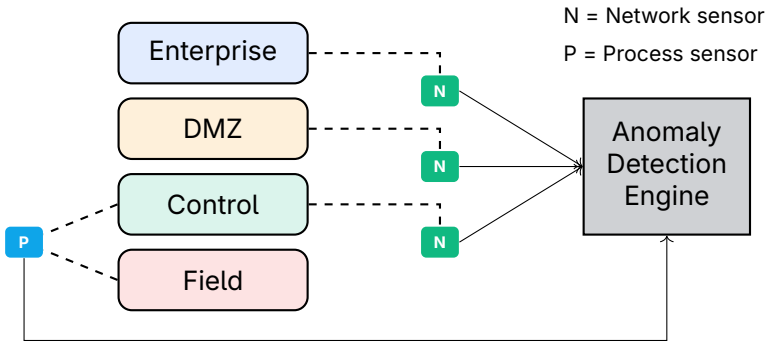

Figure 4: Anomaly Detection Sensor Placement

6.2 Integration with Other Systems

- **SIEM integration:** Send alerts for correlation with other events
- **Asset inventory:** Context about device type, criticality, owner
- **Change management:** Suppress alerts during planned changes
- **Historian:** Process data for process anomaly detection
- **IDS/IPS:** Complement signature-based detection

7 Operational Considerations

7.1 Handling False Positives

Warning

False Positive Management:
- High false positive rates cause alert fatigue
- Operators may disable or ignore detection systems
- Tune thresholds carefully based on operational feedback
- Create exception rules for known acceptable deviations
- Continuously refine models based on feedback

7.2 Responding to Anomalies

1. **Alert triage:** Determine if anomaly is security-relevant
2. **Context gathering:** Check for planned changes, maintenance
3. **OT consultation:** Verify with operators if behavior is expected
4. **Investigation:** If suspicious, investigate further
5. **Feedback loop:** Update model if false positive confirmed

7.3 Model Maintenance

- Retrain models after significant system changes
- Periodically validate detection effectiveness
- Update baselines when legitimate changes occur
- Document all model changes and tuning decisions
- Test detection with red team exercises

8 Summary

Key Takeaways

- **OT is ideal for anomaly detection:** Predictable, stable, cyclic
- **Three categories:** Network, process, and behavioral anomalies
- **Baseline is critical:** Must capture true normal before deployment
- **Multiple techniques:** Statistical, ML, and rule-based approaches
- **False positives matter:** High rates cause operational rejection
- **OT context required:** Operators must validate anomalies
- **Continuous refinement:** Models need ongoing maintenance

9 Further Reading

Standards

- **IEC 62443-3-3** – System security requirements
  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 Monitoring
  https://www.cisa.gov/topics/industrial-control-systems
- **MITRE ATT&CK for ICS** – Adversary Behaviors
  https://attack.mitre.org/matrices/ics/

Part of the OT Security Learning Series