Device Management in OT

Centralized Management, Directory Services, and Software Deployment

OT Security Learning Series

Document 890 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Device management in Operational Technology (OT) environments presents unique challenges that differ significantly from traditional IT infrastructure. While enterprise environments benefit from mature centralized management solutions, OT networks must balance operational requirements, safety considerations, and security constraints when implementing device management strategies.

Information

This document explores device management concepts for OT environments, including directory service integration, software deployment strategies, and configuration management. It addresses the challenges of managing diverse industrial assets while maintaining system availability and security.

1.1 Scope of Device Management

OT device management encompasses several key areas:

- **Asset Inventory:** Maintaining accurate records of all devices
- **Configuration Management:** Tracking and controlling device settings
- **Software Deployment:** Distributing updates and applications
- **Identity Management:** Centralized authentication and authorization
- **Monitoring:** Health and compliance status tracking

2 OT Device Management Challenges

2.1 Heterogeneous Device Landscape

OT environments contain diverse device types with varying management capabilities:

Device Type	Management Capability	Typical Approach
Windows-based HMI/SCADA	Full domain integration	Directory services, centralized updates
Linux-based servers	SSH, configuration management	Ansible, Puppet, or manual
PLCs/RTUs	Proprietary protocols	Vendor-specific tools only
Network equipment	SNMP, SSH, web interface	Network management systems
Embedded devices	Limited or none	Firmware updates via USB
Safety systems (SIS)	Restricted access	Isolated, manual management

Table 1: Device types and management approaches in OT

2.2 Availability Requirements

Warning

OT systems often operate 24/7 with minimal maintenance windows. Device management activities must be carefully planned to avoid disrupting critical processes. Forced reboots or automatic updates can cause production outages or safety incidents.

2.3 Network Segmentation Constraints

Management traffic must respect zone boundaries defined by network segmentation. Direct connections from IT management systems to deep OT networks violate security principles and create attack paths.

3 Directory Services in OT

3.1 Architecture Considerations

Directory services provide centralized authentication and authorization. In OT environments, the architecture must address:

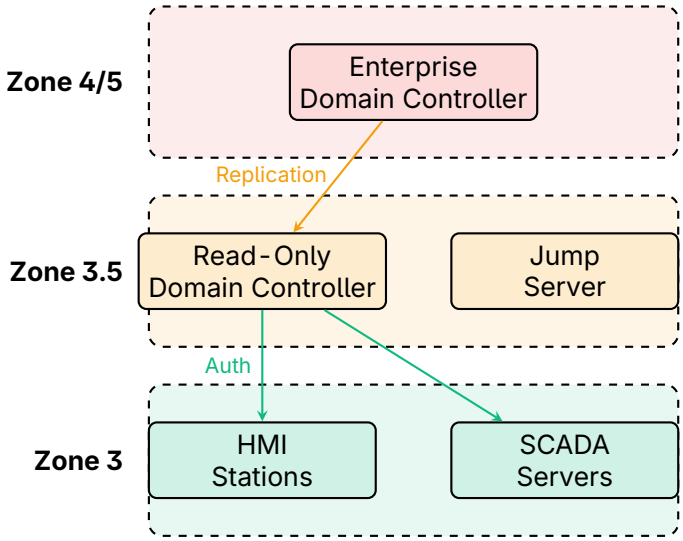

Figure 1: Directory services architecture with DMZ placement

3.2 Deployment Options

3.2.1 Dedicated OT Domain

A separate domain for OT systems provides isolation from enterprise threats:

- **Advantages:** Complete isolation, independent policies, no trust dependencies
- **Disadvantages:** Duplicate administration, separate credentials for users

3.2.2 Extended Enterprise Domain

OT systems join the enterprise domain with dedicated organizational units (OUs):

- **Advantages:** Single sign-on, unified management, existing infrastructure
- **Disadvantages:** Attack path from IT to OT, shared vulnerability exposure

3.2.3 One-Way Trust Relationship

OT domain trusts enterprise domain for authentication, but not vice versa:

- **Advantages:** Users authenticate with enterprise credentials, OT remains isolated
- **Disadvantages:** Complex setup, trust relationship management

Key Point

Recommendation: Use dedicated OT domains or one-way trusts. Place Read-Only Domain Controllers (RODCs) in the DMZ to service OT authentication without exposing writable directory services.

3.3 Group Policy Considerations

Group policies for OT systems require different settings than enterprise IT:

Policy Area	IT Approach	OT Consideration
Automatic updates	Enabled, auto-install	Disabled or controlled
Screen lock timeout	5-15 minutes	Extended or disabled for operators
Password expiration	60-90 days	Longer periods or certificates
USB device control	Often blocked	May need access for maintenance
Software restriction	AppLocker/SRP	Application whitelisting

Table 2: Group policy differences between IT and OT

4 Software Deployment Strategies

4.1 Centralized Update Management

Centralized update management systems distribute patches and software across the network:

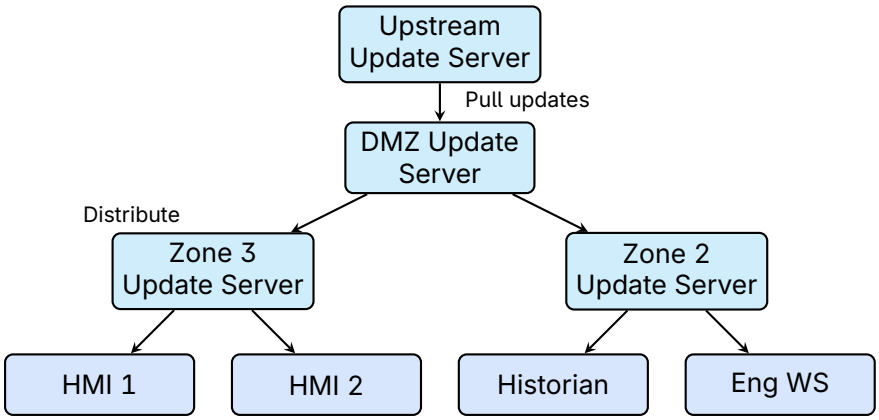

Figure 2: Hierarchical update distribution architecture

4.2 Update Server Placement

- **Enterprise Zone:** Primary server syncs with external sources
- **DMZ:** Downstream server receives approved updates
- **Manufacturing Zone:** Local servers distribute to OT clients

Warning

Never configure OT systems to pull updates directly from internet sources. All updates should flow through controlled internal servers after testing and approval.

4.3 Configuration Management Tools

Configuration management automates system state enforcement:

Approach	Model	OT Suitability
Agentless (SSH/WinRM)	Pull or Push	Good – no software installation on end-points
Agent-based	Pull	Requires agent installation and connectivity
Image-based	Push	Suitable for standardized HMI deployments
Manual scripts	Push	Limited scalability, prone to errors

Table 3: Configuration management approaches

4.4 Software Distribution Best Practices

1. **Testing Environment:** Validate all updates in a test environment that mirrors production
2. **Staged Rollout:** Deploy to pilot systems before full deployment
3. **Rollback Plan:** Maintain ability to restore previous state
4. **Change Windows:** Schedule deployments during planned maintenance

5. **Vendor Approval:** Confirm updates are approved by OT system vendors

5 Asset Management Integration

5.1 OT Asset Inventory Requirements

Effective device management requires comprehensive asset tracking:

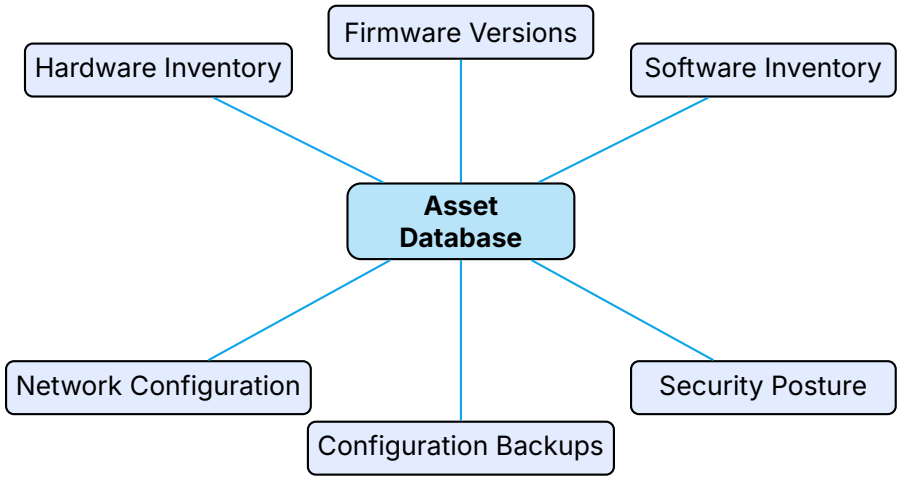

Figure 3: Asset management data elements

5.2 Discovery Methods

- **Passive Monitoring:** Network traffic analysis to identify devices
- **Active Scanning:** Controlled queries using safe OT protocols
- **Agent-based:** Software agents report device information
- **Integration:** Data from existing management systems

Critical

Active scanning can disrupt sensitive OT devices. Always use OT-aware discovery tools and schedule scans during appropriate maintenance windows. Never scan safety systems or process control networks without explicit approval.

6 Management Network Design

6.1 Dedicated Management Plane

Separating management traffic from operational traffic enhances security:

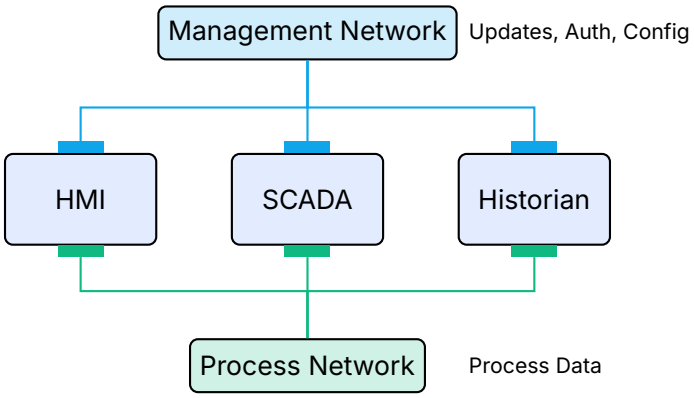

Figure 4: Dual-homed devices with separate management and process networks

6.2 Access Control for Management

- **Jump Servers:** All management access through hardened bastion hosts
- **Multi-Factor Authentication:** Required for all administrative access
- **Session Recording:** Log and record administrative sessions
- **Time-based Access:** Limit management access to defined windows

7 Compliance and Monitoring

7.1 Configuration Compliance

Device management systems should verify systems meet security baselines:

- Operating system hardening standards
- Required security software presence
- Prohibited software detection
- Account and permission compliance
- Patch level verification

7.2 Alerting and Reporting

Tip

Integrate device management status into OT security monitoring. Alert on unauthorized changes, missing patches on critical systems, and configuration drift from approved baselines.

8 Summary

Key Takeaways

- **Segmented Architecture:** Place management infrastructure according to zone boundaries; use DMZ servers and one-way trusts to limit attack paths
- **OT-Specific Policies:** Device management policies must accommodate operational requirements including extended maintenance windows and availability needs
- **Hierarchical Distribution:** Use tiered update servers to control software flow from enterprise to OT zones
- **Testing Before Deployment:** All updates and configuration changes require validation in test environments before production rollout
- **Comprehensive Inventory:** Maintain accurate asset records including firmware, configuration, and security posture for all managed devices

9 Further Reading

Standards and Guidelines

- **IEC 62443-2-1** – Security Program Requirements for IACS Asset Owners
  https://webstore.iec.ch/publication/7030
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **CISA** – Securing Industrial Control Systems
  https://www.cisa.gov/topics/industrial-control-systems

Resources

- **SANS ICS** – Industrial Control Systems Security Resources
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials
- **CIS Controls** – Center for Internet Security Controls
  https://www.cisecurity.org/controls

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Stouffer, Keith et al. – *Guide to Industrial Control Systems Security* (NIST)

Part of the OT Security Learning Series