Network Access Control for OT

NAC implementation in industrial environments

OT Security Learning Series

Document 820 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 NAC Fundamentals **3**
2.1 NAC Functions 3
2.2 NAC Methods 3

3 OT NAC Challenges **4**
3.1 OT Device Limitations 4

4 OT NAC Architecture **4**
4.1 Recommended Approach 4
4.2 Deployment Zones 5

5 Implementation Strategy **5**
5.1 Phased Rollout 5

6 Device Profiling **6**
6.1 Profiling Techniques 6
6.2 OT Device Signatures 6

7 Policy Examples **6**

8 Integration Points **6**

9 Summary **7**

10 Further Reading **7**

1 Introduction

Information

Network Access Control (NAC) ensures that only authorized and compliant devices can connect to the OT network. It provides visibility into connected assets and enforces security policies before granting network access.

NAC addresses critical OT challenges:

- Unauthorized devices connecting to the network
- Contractors bringing unmanaged laptops
- Rogue devices introduced during maintenance
- Shadow IT and unauthorized equipment
- Lack of visibility into connected assets

Warning

Traditional IT NAC solutions may not work in OT environments. Many industrial devices cannot run agents, support 802.1X, or tolerate authentication delays.

2 NAC Fundamentals

2.1 NAC Functions

Core NAC Capabilities

- **Authentication** – Verify identity of users and devices
- **Authorization** – Determine access level based on policy
- **Assessment** – Check device compliance (patches, AV, etc.)
- **Remediation** – Quarantine or fix non-compliant devices
- **Visibility** – Inventory all connected devices

2.2 NAC Methods

Method	Description	OT Suitability
802.1X	Port-based authentication via RADIUS	Limited
MAC Authentication Bypass	Authenticate by MAC address	Common
Agent-based	Software agent on endpoint	Very limited
Agentless	Passive profiling, no endpoint software	Recommended
Inline	NAC device inline with traffic	Moderate
Out-of-band	NAC monitors via SPAN/mirror	Recommended

Table 1: NAC Methods and OT Applicability

3 OT NAC Challenges

Critical

Why traditional NAC fails in OT:

- PLCs and RTUs cannot run authentication agents
- Legacy devices don't support 802.1X
- Authentication delays may disrupt real-time control
- Blocking a device could stop production
- Many OT devices use static IPs and configurations
- Rebooting devices for NAC enrollment may be impossible

3.1 OT Device Limitations

Device Type	802.1X	Agent	MAC Auth
Modern Windows HMI	Yes	Yes	Yes
Legacy Windows XP	Limited	Limited	Yes
Engineering Workstation	Yes	Yes	Yes
PLC / RTU	No	No	Yes
Network Switch (managed)	Yes	No	N/A
Field Sensor / Actuator	No	No	Maybe
IP Camera	Limited	No	Yes

Table 2: OT Device NAC Capability Matrix

4 OT NAC Architecture

4.1 Recommended Approach

Key Point

OT NAC best practices:

- Use **agentless, passive** profiling for OT devices
- Deploy **out-of-band** monitoring (not inline blocking)
- Implement **802.1X** only for capable devices (HMIs, workstations)
- Use **MAC Authentication Bypass (MAB)** for PLCs, RTUs
- Start in **monitor mode** before enforcement
- Integrate with **OT asset inventory** solutions

4.2 Deployment Zones

Zone	NAC Mode	Rationale
Enterprise IT	Full 802.1X	Standard IT devices support it
Industrial DMZ	802.1X + MAB	Mix of IT and OT devices
Manufacturing	MAB + Monitoring	HMIs may support 802.1X
Control	Monitor only	Cannot risk blocking PLCs
Safety	No NAC	Isolation is better than NAC

Table 3: NAC Deployment by Zone

5 Implementation Strategy

5.1 Phased Rollout

1. **Phase 1: Visibility**
   - Deploy passive monitoring
   - Build complete asset inventory
   - Profile all device types
   - No enforcement, only alerting
2. **Phase 2: Classification**
   - Categorize devices by type and criticality
   - Define policy groups
   - Identify 802.1X-capable devices
   - Document MAC addresses for MAB
3. **Phase 3: Selective Enforcement**
   - Enable 802.1X on IT-like OT devices
   - Implement MAB for industrial devices
   - Start with low-risk zones
   - Monitor for issues
4. **Phase 4: Full Deployment**
   - Extend to all zones (except safety)
   - Automate quarantine for unknown devices
   - Integrate with incident response

6 Device Profiling

6.1 Profiling Techniques

- **DHCP fingerprinting** – Identify device by DHCP options
- **MAC OUI lookup** – Manufacturer identification
- **Traffic analysis** – Protocols and behavior patterns
- **Active scanning** – Probe devices (use carefully in OT)
- **Integration** – Import from asset management tools

6.2 OT Device Signatures

NAC systems should recognize:

- Industrial protocols (Modbus, EtherNet/IP, PROFINET)
- PLC vendors (Siemens, Rockwell, Schneider, ABB)
- HMI systems and historians
- Industrial switches and routers

7 Policy Examples

Condition	Action
Known PLC (MAC in inventory)	Allow, assign to Control VLAN
Known HMI with valid certificate	Allow, assign to Manufacturing VLAN
Unknown device on control network	Alert SOC, monitor traffic
Contractor laptop	Quarantine VLAN, require approval
Device fails posture check	Limited access, remediation portal
Known device, wrong port	Alert, investigate

Table 4: Example NAC Policies for OT

8 Integration Points

- **SIEM** – Send NAC events for correlation
- **Asset Management** – Sync device inventory
- **CMDB** – Validate against authorized asset list
- **Firewall** – Dynamic policy updates
- **Vulnerability Scanner** – Trigger scans on new devices

- **Ticketing** – Auto-create tickets for violations

9 Summary

Key Takeaways

- **Agentless for OT** – Most industrial devices can't run agents
- **MAB for PLCs** – MAC Authentication Bypass for non-802.1X devices
- **Monitor first** – Start passive before enforcement
- **Zone-based** – Different NAC modes for different zones
- **Don't block control** – Alert rather than block critical devices
- **Visibility is key** – NAC provides asset inventory benefit

10 Further Reading

Standards

- **IEEE 802.1X** – Port-Based Network Access Control
  https://standards.ieee.org/standard/802_1X-2020.html
- **IEC 62443-3-3** – System security requirements
  https://webstore.iec.ch/publication/7033

Resources

- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Part of the OT Security Learning Series