DB-ELECTRONICS · LEAD MAGNET

IEC 62443 Network Segmentation Checklist

A practical, vendor-neutral 12-point checklist for industrial network operators. Each item is mapped to the IEC 62443-3-3 system requirements and includes a verification method you can run today.

For

OT / SCADA / ICS engineers
IT managers at industrial SMBs
Network admins running mixed-vendor fleets

Author

Ole Olorentzen
Network engineer, dB-Electronics

CONTENTS

What's in this checklist

Why this checklist

Most segmentation guidance is theoretical or vendor-biased. This is the 12 things you'd actually check on a real industrial network, mapped to specific clauses in IEC 62443-3-3, with a verification command or document you can produce for every item. Total time: 2-4 hours against a mid-size OT network.

SECTION 00

How to use this checklist

Pick the path that matches your starting point. Don't try to do all 12 items in one afternoon.

If you're starting a new network design

Work through the 12 items in order. Each builds on the previous. The first three (inventory, zones, conduits) are the foundation; everything else assumes those are in place.

If you're auditing an existing network

Run the 12 items as a gap analysis. Mark each ✓ (passes), ✗ (fails), or ? (can't verify right now). The ✗ and ? items are your work list. Triage by risk, not by volume: a 200-line config that drifts on a non-critical switch is less urgent than a 3-line gap that disables auth on a core router.

If you're prepping for an audit (NIS2, IEC 62443, NIS-2)

Run the full checklist, document every verification (the VERIFY lines in each item tell you what to capture), and keep the results. Auditors want evidence you ran the controls, not just that the controls exist.

Each item includes: what to check, how to verify, and the specific IEC 62443-3-3 system requirement (SR) it maps to. Treat the SR references as a checklist cross-walk, not a substitute for the standard itself.

SECTION 01 OF 06

Asset inventory

You cannot segment what you don't know exists. This is the foundation — every other section assumes you have an authoritative list of devices, their locations, and their roles.

01 **Authoritative device inventory exists and is current**

A single source of truth listing every network device: hostname, IP, vendor, model, role, location, owner. Updated within the last 30 days.

VERIFY: `PacketPilot Registry query, NetBox API, or spreadsheet dated within 30 days`

IEC 62443-3-3: *SR 5.1 (Network segmentation — requires knowing what's there)*

02 **OT devices are physically and logically mapped**

PLCs, HMIs, SCADA servers, and engineering workstations are tagged with site/zone. A walk-the-floor verification matches the inventory to reality.

VERIFY: `Site survey document or PacketPilot Registry site/zone hierarchy populated for >90% of OT assets`

IEC 62443-3-3: *SR 5.1*

SECTION 02 OF 06

Network zones (Purdue model)

Devices are grouped into zones based on function and trust level. The Purdue model is the reference architecture, but the principle (zone by function, not by physical location) applies regardless of which model you use.

03 **Zones are defined and documented**

Every device belongs to a documented zone. Zones map to the Purdue levels (L0-L5) or to a custom functional grouping. Each zone has a stated purpose and a list of authorized device types.

VERIFY: `Network diagram with zones overlaid, dated within 90 days`

IEC 62443-3-3: *SR 5.1, SR 5.2 (Zone boundary protection)*

04 **Zone boundaries are enforced at Layer 3**

Traffic between zones is filtered. Default-deny. No implicit "any any" rules. ACLs or firewall rules enforce the policy.

VERIFY: `Export ACL from each zone boundary device; grep for "any any" — should be empty or only justified exceptions`

IEC 62443-3-3: *SR 5.2*

SECTION 03 OF 06

Conduits between zones

Conduits are the controlled paths between zones. They're where the real risk lives — and where most OT networks have the weakest controls.

05 **Every cross-zone path is a documented conduit**

If traffic can flow between zones, there's a conduit. The conduit has a defined purpose, a list of authorized protocols/ports, and a list of source/destination endpoints.

VERIFY: `Conduit list document or network diagram with cross-zone arrows labeled by purpose`

IEC 62443-3-3: *SR 5.1, SR 5.3 (Person-to-person communication restrictions)*

06 **Conduits deny by default; only authorized flows pass**

Firewall rules on each conduit are deny-all plus explicit allow. No broad permits. Each allowed flow has a documented justification.

VERIFY: `Pull firewall ruleset; for each rule, verify there's a business justification on file`

IEC 62443-3-3: *SR 5.3*

SECTION 04 OF 06

IT/OT DMZ

The DMZ between IT and OT networks is the most attacked boundary. Vendor remote access, jump hosts, replication traffic — all should pass through it.

07 **A documented DMZ exists between IT and OT networks**

A separate network segment with firewalls on both sides. No direct IT-to-OT traffic; all flows transit the DMZ.

VERIFY: `Network diagram showing DMZ; verify no direct routes exist between IT and OT subnets (route table review)`

IEC 62443-3-3: *SR 5.2*

08 **Vendor remote access goes through the DMZ only**

No direct VPN tunnels from vendors into OT. All remote access terminates in the DMZ and is brokered through a jump host or privileged access management tool.

VERIFY: `Pull VPN config from perimeter devices; verify no vendor-issued tunnels exist directly into OT`

IEC 62443-3-3: *SR 5.2, SR 1.1 (Identity and authentication control)*

SECTION 05 OF 06

Identity and access

Segmentation assumes you know who's authorized. Without identity controls, an attacker on a low-trust zone can pivot to a high-trust zone by stealing a credential.

09 **AAA is enabled on every network device**

Authentication, Authorization, Accounting. Every switch, router, firewall uses central auth (TACACS+ or RADIUS). No local-only accounts except emergency break-glass (documented and monitored).

VERIFY: `For each device: show aaa; show tacacs; show running-config | include username. Local accounts should be empty or only the documented break-glass account.`

IEC 62443-3-3: *SR 1.1 (Human user identification), SR 1.5 (Authenticator management)*

10 **Privileged access is restricted and audited**

Privilege 15 / enable mode is granted only to specific named accounts. Each privilege-15 action is logged centrally.

VERIFY: `Pull AAA config; verify privilege levels per user/group. Pull audit logs for privilege-15 commands — should be centralized, not just local buffer.`

IEC 62443-3-3: *SR 2.1 (Authorization enforcement), SR 6.1 (Audit log accessibility)*

SECTION 06 OF 06

Logging and monitoring

Segmentation without monitoring is a wall without a guard. You need to see who's crossing your zone boundaries, when, and why.

11 Centralized syslog for every network device

Every switch, router, firewall, and zone-boundary device sends logs to a central SIEM. Local log buffer alone doesn't count — a successful attack often includes clearing local logs.

VERIFY: `For each device: show logging. Verify a remote syslog target is configured and reachable.`

IEC 62443-3-3: *SR 6.1, SR 6.2 (Continuous monitoring)*

12 Alerts on cross-zone traffic anomalies

Unusual cross-zone flows (a workstation in IT reaching a SCADA server, a vendor session at 3 AM, traffic to denied ports) trigger alerts. Detection, not just collection.

VERIFY: `SIEM rule list; verify rules exist for: cross-zone denies, after-hours OT access, new source IP into OT, large data transfers across the IT/OT DMZ`

IEC 62443-3-3: *SR 6.2*

What's next

You've got the checklist. Now make it operational. The companion blog post walks through each section in detail, with real device configs and worked examples.

Read the full guide →

Need an asset inventory that updates itself? PacketPilot Registry auto-populates from PacketPilot Config discoveries, so item 01 stays current without manual work.

Try PacketPilot Config free →

dB-Electronics
Self-hosted network operations software
Kristiansund, Norway · support@db-electronics.no
packetpilot.db-electronics.no