The 40-point OT security checklist.

A practical checklist for evaluating the security of PLCs, SCADA, HMIs, and the industrial networks that connect them. Work through each item and mark it done, partial, or missing. Every unchecked box is a finding; the sections are ordered so the highest-leverage controls come first.

01 Network segmentation (8)

- [ ] **OT and IT networks are separated** by a firewall or routed boundary, not just VLANs on a shared switch.
  A flat network means one phished laptop can reach a PLC.
- [ ] **Traffic between OT and IT is allow-listed**: only named systems, ports, and protocols cross the boundary.
- [ ] **An industrial DMZ exists** for anything both sides need (historians, file transfer, jump hosts).
- [ ] **Production cells or lines are zoned** so a compromise in one area can't spread laterally to all of them.
- [ ] **No OT device has a direct route to the internet.**
  Controllers should never originate or receive internet traffic.
- [ ] **Vendor and integrator connections terminate in the DMZ**, never directly on the control network.
- [ ] **Wireless on the plant floor is isolated** from control networks and uses its own SSIDs and credentials.
- [ ] **Segmentation is verified at least annually** by testing what can actually reach what, not by trusting the diagram.

02 Remote access (6)

- [ ] **All remote access to OT goes through a single audited path** (VPN plus jump host), no exceptions.
- [ ] **Multi-factor authentication is required** for every remote session that can reach control systems.
- [ ] **Vendor remote access is disabled by default** and enabled per session, with an expiration.

- [ ] **Cellular modems, TeamViewer-style tools, and vendor backdoors have been hunted down and removed.**
  The access you don't know about is the one that gets used.
- [ ] **Remote sessions into OT are logged and reviewable**: who, when, what they touched.
- [ ] **Terminated employees and former vendors lose access the same day**, verified against an access list.

03 Asset inventory and visibility (6)

- [ ] **A current inventory exists of every OT asset**: PLCs, HMIs, drives, sensors, gateways, with model and firmware.
- [ ] **Someone owns keeping that inventory current** when equipment is added or replaced.
- [ ] **Network monitoring can see OT traffic**, passively, without disrupting control communications.
- [ ] **You know which assets run end-of-life operating systems** and each one has a documented isolation plan.
- [ ] **Unknown devices appearing on the control network trigger an alert**, not a shrug.
- [ ] **Data flows are documented**: what talks to what, in which direction, over which protocol.

04 Patching and vulnerability management (6)

- [ ] **A patching policy exists for OT that respects production**: scheduled windows, tested first, rollback ready.
- [ ] **Windows machines on the plant floor (HMIs, engineering stations) are patched on a defined cadence.**
- [ ] **Firmware updates for controllers are evaluated on a schedule**, even when the answer is "not yet."
- [ ] **Compensating controls are documented for anything that can't be patched.**
  "We can't patch it" is acceptable; "we can't patch it and did nothing else" is not.
- [ ] **You subscribe to vulnerability advisories for the vendors you actually run** (Rockwell, Siemens, Schneider, etc.).
- [ ] **Engineering software (programming tools, project files) is controlled and current.**

05 Accounts and access control (5)

- [ ] **Default passwords have been changed on every OT device that supports a password.**
- [ ] **Shared operator accounts are limited and documented**; engineering and admin access is individual.
- [ ] **OT credentials differ from IT credentials.**
  A cracked office password should not open the plant.
- [ ] **Physical access to control cabinets and engineering stations is restricted.**
- [ ] **USB and removable media use on OT systems is governed**: scanned, allow-listed, or blocked.

06 Monitoring and detection (4)

- [ ] **Someone is alerted, day or night, when something anomalous happens on the OT network.**
- [ ] **Logs from OT-adjacent systems (firewalls, jump hosts, historians) are collected centrally.**
- [ ] **Baseline behavior is understood** well enough that new connections or protocols stand out.
- [ ] **Detection has been exercised**: you've tested that an alert actually reaches a human who acts.

07 Incident response and recovery (5)

- [ ] **An incident response plan exists that names OT scenarios**, not just office ones, and names who decides to isolate or shut down a line.
- [ ] **PLC programs and device configurations are backed up**, versioned, and stored off the control network.
- [ ] **You can rebuild an HMI or engineering station from media you control**, without a vendor visit.
- [ ] **Manual/degraded operating procedures are documented** for running or safely stopping production without the network.
- [ ] **An OT incident has been tabletop-exercised in the last 12 months** with operations in the room, not just IT.

Scoring

35–40 checked

Mature OT security posture. Keep exercising it; drift is the main enemy from here.

25–34 checked

Real foundations with real gaps. Prioritize unchecked items in sections 1, 2, and 7 first.

Below 25

Your plant network is likely one bad click from a production outage. Start with segmentation and remote access; they buy the most risk reduction per dollar.

Where to start if everything is unchecked: items 1, 5, and 9 (segment the boundary, cut OT internet access, force remote access through one door) eliminate the paths most ransomware actually takes into a plant.

Found gaps you're not sure how to close?

That's the normal outcome of this checklist, and it's fixable. Network Builders IT engineers work in manufacturing environments every day; we'll walk your unchecked boxes with you and help you sequence the fixes by risk, not by cost of the quote.

nbit.com/book-a-call
Book a 30-minute discovery call

(888) 816-6248
Talk to an engineer

info@nbit.com
Email us your questions