OT and industrial systems: what if you can't patch or reboot?

This month, close port forwards and modems that reach your controllers from the internet, put vendor access behind your own gateway with MFA, and change every default or shared password. Then route remote access through one broker in the OT DMZ, keep verified offline copies of controller logic and rehearse running the plant by hand.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for

IT/OT security, engineering and plant operations leads at EU manufacturers, utilities, water and building operators, including KRITIS and NIS2 entities in Germany

Latest version

sheets.einblick.dev/ot-security/

If you only do five things

1. **Close every path in from the internet.** Check routers for port forwards and cabinets for modems[1]. Iranian-affiliated actors have disrupted exposed PLCs since at least March 2026[2].
2. **Change every default and shared password.** Attackers used default accounts at over 30 Polish wind and solar sites in December 2025; password reuse across sites is common[3].
3. **Put all remote access through one broker.** One gateway in the OT DMZ, with phishing-resistant MFA and enabled per job, replaces per-vendor VPNs[5] and stray modems.
4. **Keep offline copies of controller logic.** Back up PLC programs, configurations and firmware offline and test them on a spare controller[2,7].
5. **Rehearse running the plant by hand.** Test manual operation and islanding[6], and an isolation plan with options from one vendor link to the whole site[5].

Build an inventory you can act on

1. **Walk the plant, not just the network.** Combine a physical inspection with network data and documents[7]. Modems and gateways often show an antenna or a Gateway label[1].
2. **Listen before you scan.** Passive discovery adds no traffic. Active scans can make devices unstable, so schedule them for planned outages where possible[8].
3. **Collect the fields that matter.** CISA and eight partner agencies rank 14 attributes high priority, such as criticality, protocols, ports, accounts and logging[7]. Add firmware, last backup and remote access path.
4. **Rank by consequence, keep it current.** Classify assets by what their failure would do to operations and safety, group them into zones, and update the list whenever a device is added or removed, even in emergencies[7].

Protect what you can't patch

- **Split the deadlines.** Remote access gateways rarely affect real-time control, so patch them promptly[9], within the patching sheet's deadlines. Patch PLCs in planned downtime unless a flaw is known exploited[2], and test first[10].
- **Wrap obsolete devices.** Put a current protocol gateway or hardened jump host in front, and log every interaction[5].
- **Use the protection you have.** Validate the logic, then lock mode switches in RUN[2]; allow programming only from named engineering workstations[10]. No Polish RTU with signed firmware support had it on[3].
- **Switch off what you don't use.** Disable unused web servers, FTP, Telnet and VNC[2,10]. A relay's default FTP account let attackers delete its system files[3].

Monitoring that understands OT

- **Watch passively.** Feed SPAN ports or taps at the OT boundary[8] and in the control network into ICS-aware intrusion detection[10]. On a small site, Malcolm shows which devices connect out[1].
- **Alert on changes to the process.** Flag program downloads, mode changes, controller writes, and programming from non-engineering machines or outside change windows[2,10].
- **Tie alerts to work orders.** Tell the SOC about maintenance windows, and make any break-glass login its top alarm[5].
- **Get logs off the devices.** The Polish attackers factory-reset firewalls, erasing their logs[3]. Forward gateway, firewall, modem and HMI logs.

When something looks wrong on the plant

1. **Make the process safe, then suspect an attack.** Operations decides on manual operation or shutdown. A Polish CHP plant took an attack for a contractor's error[4].
2. **Isolate in stages.** Revoke one vendor's access, or isolate the site and keep only the flows your plan exempts[5]. Do it before restoring: a Polish CHP plant restored with the attacker still inside[4].
3. **Check the logic before you restart.** Compare programs and backups with known-good logic, and reimage what the attacker reached[2].

Engineering access and safety systems

- **Dedicate engineering workstations.** Use application allowlisting[10], and keep them in OT with no email or web access.
- **Control media and laptops.** Use registered company media, scan it on a station with a different operating system, block unused USB ports and quarantine contractor laptops[11].
- **Keep safety systems separate.** Combined control and safety networks could give an attacker both; keep safety keys in RUN unless programming[8]. F-series safety CPUs are among the Siemens targets[10].

Suppliers and products

- **Buy secure by default.** Require the 12 Secure by Demand elements, such as no default passwords; they align with IEC 62443-4-2 Security Level 3[12].
- **Contract the remote access.** Integrators use your broker, add no modems, list who has access and hand over an inventory and backups[15]. If you cut remote access, they come on site.[5]
- **Mind 2027.** The CRA's main obligations apply from 11 December 2027[13]. Under the Machinery Regulation, machines placed on the market from 20 January 2027 must be protected against corruption.[14]

What regulators expect in Germany

- **Treat plant systems as in scope.** For NIS2 entities, § 30 BSIG covers the IT systems, components and processes used to provide their services[16]. Energy grid and plant operators under §§ 5c to 5e EnWG follow the EnWG instead.[16] Reporting is in the EU security laws sheet.
- **Critical facilities need attack detection.** § 31 BSIG requires it[16], BSI's pre-NIS2 guidance includes OT,[17] and operators prove their measures to the BSI every 3 years.[16]
- **BSI calls exposed OT a breach of duty.** It says operators who expose OT to the internet without adequate protection breach their duties[1].

What changed in 2026

- **Destructive attacks reached EU energy.** On 29 December 2025, attackers damaged controllers at over 30 Polish wind and solar sites and hit two CHP plants, one through a private APN[3,4]. Audit your APNs.[4]
- **PLC attacks now target safety logic.** AA26-097A's July 2026 update describes a malicious project file that overrode logic keeping a process within safe limits[2].
- **Attackers use AI to write PLC exploits.** The NSA-led AA26-231A (August 2026) describes AI-generated scripts that read and write Siemens S7 memory. Block TCP port 102 at the perimeter[10].
- **BSI set a baseline for small plants** in October 2026: no direct internet access, secured remote access, current software, routine checks[1].

What you can skip

- **Active scans of a running plant.** Test the tool offline and schedule scans for planned outages where possible[8].
- **Emergency patching every ICS advisory.** Fix exposed and known exploited flaws first; the rest can wait for planned downtime[2].
- **Agents the vendor hasn't approved.** Measures must not cost you warranty or support[11].
- **Anomaly detection instead of blocking.** The NCSC says it must not replace disabling unused commands, services and ports[5].

Mistakes that cost the most

- **Calling a VLAN isolation.** Many Polish sites had separate VLANs, but the attacker held admin rights on the firewall that joined them[3].
- **Letting one domain reach everything.** At the large Polish CHP plant, attackers with privileged domain accounts pushed a wiper through Group Policy; EDR stopped it[3]. The segmentation sheet covers a separate OT identity.
- **Assuming the integrator handled it.** Owners whose providers have remote access may not know their PLCs are exposed[10].

What this looks like at your size

Small team, no security staff

- Check the router for port forwards[1] and get Shadowserver's free reports for your IP addresses.[18]
- Get every remote access path, account, modem and PLC program from your integrator[15].
- Drop cloud links operation doesn't need[1]; practice manual operation yearly.

Growing, with IT or security staff

- Build the inventory with CISA's fields and a passive sensor at the IT/OT boundary.
- Replace vendor VPNs and modems with one broker, enabled per job.
- Back up logic after every change and test a restore on a spare each quarter.

Enterprise or regulated

- Run attack detection that covers OT[17] and use your sector's B3S where one exists.[1]
- Exercise an attack on all sites at once and test fleet-wide isolation[5].
- Put Secure by Demand and IEC 62443-4-2 in tenders, and CRA conformity for later deliveries.

Version history

5 Nov 2026, version 1.1 Reviewed for company readers: Shadowserver's free reports replace Shodan InternetDB, which is free only for non-commercial use.

Sources

1. Risks Posed by Internet-Connected OT Systems (BSI-CS 154E). BSI, 14 Oct 2026. bsi.bund.de
2. Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers (AA26-097A). FBI, CISA, NSA and partners, updated 22 Jul 2026. ic3.gov
3. Energy Sector Incident Report: 29 December 2025. CERT Polska, 30 Jan 2026. cert.pl
4. Follow-up analysis of the 29 December 2025 energy sector incident. CERT Polska, 8 Aug 2026. cert.pl
5. Secure connectivity principles for operational technology (OT). NCSC (UK) and partners, 14 Jan 2026. ncsc.gov.uk
6. Primary Mitigations to Reduce Cyber Threats to Operational Technology. CISA, FBI, EPA and DOE, 6 May 2025. ic3.gov
7. Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators. CISA and partners, 13 Aug 2025. epa.gov
8. SP 800-82r3, Guide to Operational Technology Security. NIST, Sep 2023. nvlpubs.nist.gov
9. Fernwartung im industriellen Umfeld (BSI-CS 108). BSI, version 2.0, 11 Jul 2018. allianz-fuer-cybersicherheit.de
10. Defending Against an Active Threat to Siemens S7 Series PLCs (AA26-231A). NSA, CISA, FBI, DOE and EPA, 19 Aug 2026. ic3.gov
11. ICS Security: Top 10 threats and countermeasures 2022 (BSI-CS 005E). BSI, version 1.50, 3 May 2022. allianz-fuer-cybersicherheit.de
12. Secure by Demand: Priority Considerations for OT Owners and Operators. CISA and partners, 13 Jan 2025. ic3.gov
13. Cyber Resilience Act. European Commission, 7 Sep 2026. digital-strategy.ec.europa.eu
14. Regulation (EU) 2023/1230 (Machinery Regulation), Article 54 as corrected, Annex III. EUR-Lex, 2023. eur-lex.europa.eu
15. Considerations for Critical Infrastructure Operators Working With Third-Party ICS Integrators. FBI and CISA, 23 Sep 2026. ic3.gov
16. BSI-Gesetz (BSIG), §§ 28, 30, 31 and 39. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
17. Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung. BSI, version 1.1, 18 Nov 2024. bsi.bund.de
18. Subscribe to Reports. Shadowserver Foundation, checked 5 Nov 2026. shadowserver.org