Ten Hidden Threats Lurking in Your Industrial Network *(and How to Fix Them)*

Fix these overlooked issues before they cost your downtime, dollars – or worse.

This guide outlines ten of the most common — and often overlooked — issues encountered in the field. If you manage or support industrial networks, use this list as a proactive checkpoint to strengthen your environment before minor issues escalate into major incidents.

These aren't hypothetical risks. They're the real-world problems we keep finding — across industries, across sites, again and again. The good news? Most of these issues aren't hard to fix. You just need to know where to look.

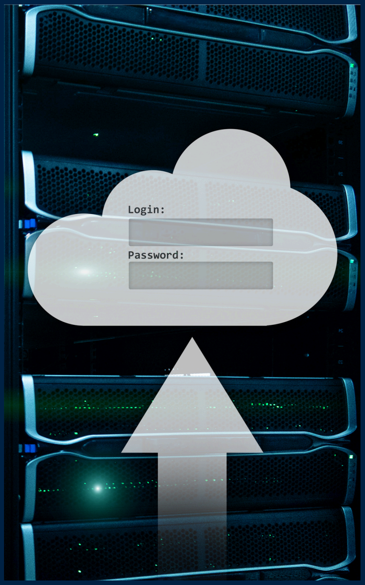
Ten Common Missteps That Open the Door to Downtime, Vulnerabilities, and Headaches

01. Tribal Knowledge Network Mapping

THE ISSUE:	No up-to-date network diagrams; critical knowledge is confined to a single individual.
WHY IT MATTERS:	When that person is unavailable, on vacation, or leaves the company — troubleshooting stalls, or production grinds to a halt. Recovery takes longer, and visibility gaps persist.
QUICK FIX:	Develop and maintain a living network map, including VLANs, IP schema, device roles, and interconnects.

02. Flat Networks Without Segmentation

THE ISSUE:	No separation between control systems, corporate IT, and guest or Wi-Fi networks.
WHY IT MATTERS:	Flat networks allow easy lateral movement for malware or unauthorized users and generate noisy, hard-to-monitor traffic.
QUICK FIX:	Implement VLANs and access control lists (ACLs) to enforce segmentation using a “least privilege” methodology.

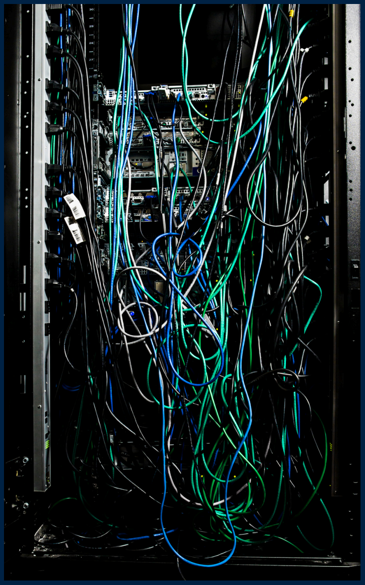


03. Default Credentials on Critical Equipment

THE ISSUE:	Devices still use factory default passwords.
WHY IT MATTERS:	Default credentials are widely known and targeted by automated scanning tools and attackers.
QUICK FIX:	Conduct a credential audit and update all passwords using NIST-aligned complexity and rotation standards.

04. Unsupported or End-of-Life Firmware

THE ISSUE:	Outdated firmware with known vulnerabilities remains in use.
WHY IT MATTERS:	Unpatched systems are exposed to well-documented exploits.
QUICK FIX:	Track firmware versions, subscribe to vendor bulletins, and maintain a regular update cycle.

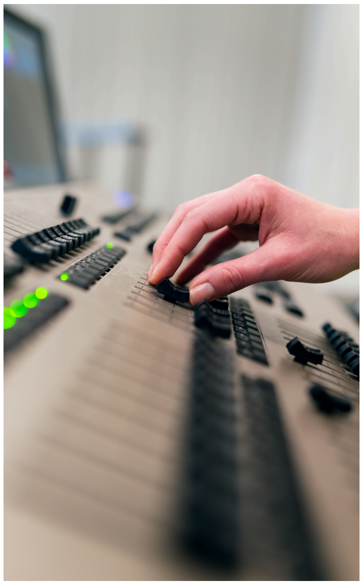


05. Insecure Remote Access Tools

THE ISSUE:	Public-facing RDP, VNC, or VPN solutions lack strong authentication.
WHY IT MATTERS:	These are frequent targets for brute force and credential-stuffing attacks.
QUICK FIX:	Require multi-factor authentication (MFA), use secure VPNs, and enforce logging and endpoint validation

06. Lack of Centralized Logging

THE ISSUE:	No visibility into device or network activity.
WHY IT MATTERS:	In the event of a failure or breach, there's insufficient data for incident response or forensic analysis.
QUICK FIX:	Deploy centralized logging or a SIEM solution and configure all critical assets to report in.



07. "Shadow" Devices and Rogue Installs

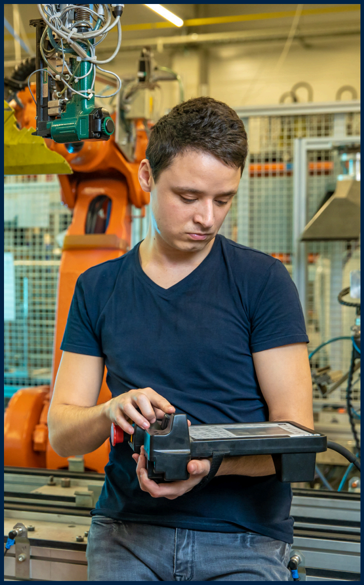
THE ISSUE:	Unauthorized or unknown devices appear on the network.
WHY IT MATTERS:	They may create backdoors, introduce vulnerabilities, or cause performance issues.
QUICK FIX:	Perform regular physical and logical inventories. Use MAC filtering or 802.1x to control access.

08. No Backups for Configurations and Systems

THE ISSUE:	Critical infrastructure lacks system and configuration backups.
WHY IT MATTERS:	Recovery is delayed or impossible following a failure, increasing operational risk.
QUICK FIX:	Automate routine backups and store them securely, ideally offline or in a dedicated management VLAN.

09. No Documentation of Change History

THE ISSUE:	Changes occur without tracking who made them or why.
WHY IT MATTERS:	Troubleshooting becomes guesswork, and root causes remain unclear.
QUICK FIX:	Implement a basic change management log — even a shared document can make a difference.



10. Physical Access Weakness

THE ISSUE:	Racks are left unlocked, ports exposed, and access is unmonitored.
WHY IT MATTERS:	Physical security is foundational. Unauthorized access can bypass all cyber protections.
QUICK FIX:	Secure all equipment, restrict room access, and monitor entry with badge logs or door sensors. Security cameras are also great, but only if they are actively monitored.

↘ WHY WORK WITH US:

- **We cut through the noise.** No buzzwords, no fluff—just real operational improvements.
- **We meet you where you are.** Whether you're at Stage 1 or Stage 5, we make the next step easy.
- **We stick around.**From system setup to staff training and ongoing coaching, we make sure you get results.

↘ HOW TO GET STARTED:

- **Schedule a Consultation.** Let’s map out the exact next steps for your business.
- **Get a Free Digital Maturity Assessment.** Find out where your operations stand right now.
- **Talk to Our Experts.** Have questions? Let’s discuss how we can help.

YOUR GOALS, OUR GUIDANCE.
SHARED SUCCESS.

inflexion point

www.inflexionpoint.ai

info@inflexionpoint.ai