SHIELDWORKZ

ICS Security Myths Busted – What You Really Need to Know

SHIELDWORKZ

SHIELDWORKZ

1. INTRODUCTION

Industrial Control Systems (ICS) and Operational Technology (OT) teams have defended physical processes for decades. Today's attackers are technically capable, adaptive, and patient - and many successful intrusions start outside the OT network and then move in through overlooked pathways. The consequence: downtime, environmental harm, regulatory penalties, reputational risk and high recovery costs.

This e-book strips away comforting assumptions and replaces them with operationally useful guidance. We'll take the common myths that can lull teams into false security, explain why each is dangerous, and present practical actions you can take immediately. No product hype - only actions that reduce risk while preserving availability and safety.

2. HOW MYTHS FORM IN OT/ICS ENVIRONMENTS

Myths about ICS security grow from consistent, predictable causes -

- **Era of isolation thinking -** For decades, many industrial systems were isolated. That "air-gap" thinking persists even though modern operations use remote maintenance, cloud integrations, and vendor portals.
- **Tool transplant -** Organizations often try to apply IT tools and expectations to OT without adjusting for the realtime, safety-critical nature of industrial environments.
- **Legacy inertia -** Field devices and controllers have decade-long lifecycles. When replacing assets is expensive, teams accept legacy constraints instead of adapting controls around them.
- **Wishful simplification -** Leaders often want a simple answer - a single product or policy that "solves" security - creating unrealistic expectations.
- **Skills shortage -** Experienced OT security professionals are relatively scarce. Where skills are missing, teams rely on assumptions rather than measurement.

The remedy is straightforward - replace assumptions with measurements, and replace one-off projects with a repeatable program that blends operations, engineering and security.

3. TOP 12 ICS SECURITY MYTHS - BUSTED, EXPLAINED, AND WHAT TO DO INSTEAD

Below are the most common and most dangerous myths we encounter. Each entry includes the reality, a technical explanation, expected operational impact, and recommended actions.

Myth 1 - "If it's air-gapped / not on the internet, it's safe."

Reality - Off-network systems are still vulnerable. Attack paths include removable media, vendor maintenance sessions, supply-chain firmware updates, compromised laptops, and physical access.

Why the myth is wrong - Attackers don't need an internet connection to reach systems. They exploit any path - human, physical or logical - to gain a foothold and then move laterally.

Operational impact - A false sense of security delays essential hygiene (inventory, backups, endpoint controls) and can allow incidents to grow unseen.

Actions -

- Treat "air-gapped" segments as high-risk, not invulnerable.
- Enforce strict removable-media policies and scanning.
- Monitor physical access and portable device connections.
- Harden vendor access with just-in-time sessions, session recording and strong authentication.

Myth 2 - "Monitoring only at supervisory levels is sufficient."

Reality - Attackers often manipulate level-0 and level-1 communications (sensors and actuators). Monitoring only at higher supervisory layers misses low-level commands that cause physical effects.

Why the myth is wrong - Dangerous actions setpoint - changes, actuator writes, direct device commands - often happen at low levels and may be invisible at aggregated view points.

Operational impact - Operators can be shown "normal" dashboards while field devices are being manipulated. Detection is delayed until physical symptoms appear.

Actions -

- Add passive monitoring for fieldbus and serial traffic where safe.
- Baseline normal command patterns and alert on unexpected writes or timing anomalies.
- Collect packet-level evidence to enable effective forensics.

Myth 3 - "Safety Instrumented Systems (SIS) will save us."

Reality - SIS are designed to reduce process risk, but they are not a substitute for cybersecurity. SIS themselves can be compromised, misconfigured or defeated by attacks that manipulate sensors or control logic.

Why the myth is wrong - SIS sometimes share maintenance channels or dependencies that can be exploited. Attackers who understand process logic can create conditions that circumvent SIS protections.

Operational impact - Overreliance on SIS can mask gaps in controls and increase the chance of a safety incident if attackers plan for bypass scenarios.

Actions -

- Treat SIS as high-value assets requiring strict isolation, documented access controls and separate recovery plans.
- Test SIS behavior under cyber-incident scenarios via tabletop exercises and engineering drills.

Myth 4 - "Only large enterprises attract advanced attackers."

Reality - Advanced adversaries frequently use smaller vendors, integrators or suppliers as stepping stones to reach larger targets. Small organizations are often easier to compromise and can provide access to critical infrastructure.

Why the myth is wrong - Compromise of a vendor's account, build system or remote management bridge can enable an attacker to introduce malicious firmware or credentials into otherwise well-secured operators.

Operational impact - Neglecting supplier and vendor risk can create severe exposure.

Actions -

- Implement supply-chain assessments and vendor security requirements.
- Require secure build and delivery practices (cryptographic signing where feasible).
- Log and audit vendor actions in your environment.

Myth 5 - "Attacks always come from the outside."

Reality - Insider threats - intentional or accidental - are a major cause of incidents. Misconfigurations, human error or misplaced privileges often facilitate attacks.

Why the myth is wrong - Legitimate credentials, maintenance activities and vendor sessions can be abused by malicious actors or hijacked by adversaries.

Operational impact - Ignoring insider risk leads to weak privilege models and inadequate monitoring.

Actions -

- Implement least-privilege access and strict privileged account management.
- Enforce segregation of duties and peer review for critical changes.
- Monitor and record privileged sessions.

Myth 6 - "Serial and legacy protocols will disappear soon."

Reality - Serial protocols and legacy field interfaces remain deeply embedded in industrial systems and will persist for years due to long equipment lifecycles.

Why the myth is wrong - Many field devices were designed to run for decades; replacing them for convenience is rarely feasible. Serial and fieldbus interfaces continue to be used for robust I/O in harsh environments.

Operational impact - Ignoring serial traffic creates blind spots that attackers can exploit to send direct commands or inject false sensor data.

Actions -

- Inventory serial devices and include them in firmware registers.
- Deploy passive serial/fieldbus monitoring where possible to observe real field communications.

Myth 7 - "Serial-to-Ethernet converters secure legacy devices."

Reality - Converters can increase exposure: many legacy devices accept commands without authentication, and converters often bridge those commands onto routable networks without adding security.

Why the myth is wrong - Converters become chokepoints that, if compromised or misconfigured, permit remote actors to send dangerous commands to field controllers.

Operational impact - A single compromised converter may grant broad control over field devices.

Actions -

- Harden and monitor converters as critical nodes.
- Use protocol proxies or command validators that enforce whitelists rather than simple converters that forward all commands.

Myth 8 - "A single vendor solution will stop all ICS attacks."

Reality - There is no single silver bullet. Effective ICS security is layered, combining visibility, segmentation, secure remote access, protocol-aware detection and practiced incident response.

Why the myth is wrong - Attacks exploit process knowledge, procedures and supply-chain weaknesses that no single product can fully address. OT constraints also limit what tools can safely do in production.

Operational impact - Overreliance on a single product leads to complacency and misplaced budget allocation.

Actions -

- Build a defense-in-depth architecture tailored to OT.
- Ensure tools interoperate with operations workflows and change processes.

Myth 9 - "Monitoring serial communications has low value."

Reality - Serial and fieldbus monitoring often yields high-value insights: unexpected writes, command timing anomalies and device behavior changes give early warning of malicious activity or device failure.

Why the myth is wrong - Many attacks manipulate low-level commands; without seeing them, detection is delayed until physical consequences occur.

Operational impact - Lack of fieldbus visibility delays detection and increases well time.

Actions -

- Add passive serial/fieldbus monitoring into your detection fabric.
- Correlate fieldbus anomalies with supervisory events in SOC workflows.

Myth 10 - "Legacy systems cannot be integrated securely."

Reality - Secure integration is feasible with compensating controls: passive telemetry, protocol proxies, command whitelisting and secure gateways allow operators to bridge legacy devices without unsafe exposure.

Why the myth is wrong - While legacy devices lack modern security features, architecture and process controls can protect them effectively.

Operational impact - Throwing away legacy systems is rarely practical; careful integration is the realistic path.

Actions -

- Use passive capture and micro-segmentation to close blind spots.
- Enforce robust change management and test integrations in isolated testbeds.

Myth 11 - "Patching everything immediately fixes the problem."

Reality - Patching in OT must be risk-aware; untested patches can cause downtime or unsafe behavior. Many teams delay patches until validated in test environments.

Why the myth is wrong - Firmware or control logic changes can affect timing and control flows, potentially endangering safety.

Operational impact - Improper patching risks availability and safety.

Actions -

- Implement a risk-based patching program: test in a lab, schedule during maintenance windows, and use compensating controls until patching is safe.

Myth 12 - "Detection is all about signatures and antivirus."

Reality - Signature-based detection is insufficient for ICS. Attackers often use legitimate commands or subtle process manipulation; detection must be behavior-based and protocol-aware, with correlation to process context.

Why the myth is wrong - Many manipulations do not match known malware signatures but manifest as abnormal command sequences or timing anomalies.

Operational impact - Relying only on signatures delays detection and increases dwell time.

Actions -

- Deploy protocol-aware monitoring and behavioral analytics.
- Correlate detection with process context and implement response playbooks that preserve safety.

4. FINAL THOUGHTS - SECURITY AS AN OPERATIONAL CAPABILITY

ICS security is not a one-off project or a checkbox. It is an operational capability requiring repeatable practices, close cooperation between operations and security, and constant improvement. Start by replacing assumptions with measurement: get an authoritative inventory, implement passive fieldbus visibility, harden vendor access, and run one validated restore. Those experiments produce measurable value quickly and build the case for longer-term investments.

Combatting myths is not just an exercise in education - it's about protecting people, the environment and reliable production. Focus on actions that reduce the most risk with the least operational disruption, and continually validate those actions with exercises and metrics.

5. NEXT STEPS - SHIELDWORKZ OFFER

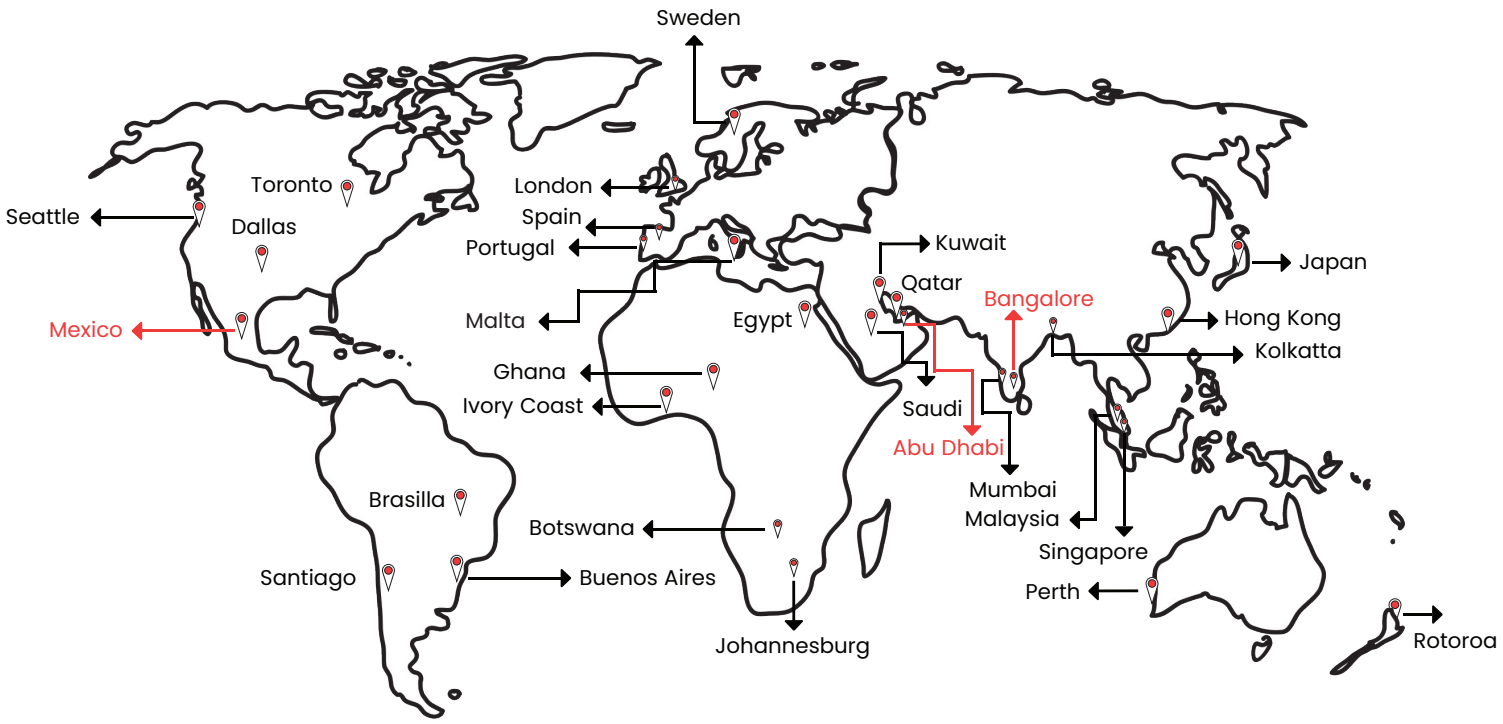
If you want to convert these recommendations into measurable outcomes, Shieldworkz can help you get started quickly and safely -

- **Free 14-day passive discovery pilot** to reveal blind spots and produce a Top-10 risk brief.
- **Serial & fieldbus monitoring pilot** for legacy assets using passive taps and non-intrusive analysis

- **Vendor access hardening package** with just-in-time access, session recording and a documented governance process
- **90-day remediation roadmap** aligned to your maintenance windows and safety procedures.

BOOK A SHIELDWORKZ DEMO OR REQUEST THE FREE PILOT AND WE'LL DELIVER AN EXECUTIVE BRIEF YOU CAN PRESENT TO OPERATIONS AND THE BOARD. START SMALL, MEASURE OUTCOMES, THEN SCALE.

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.