txOne networks

The Industrial Control System (ICS) Security Playbook

Practical Strategies for Safeguarding Industrial Operations in a Connected World

Discover. Assess. Protect.

Executive Summary

Securing Industrial Control Systems (ICS) has become a core business imperative. As information technology (IT) and operational technology (OT) become connected, industrial organizations face new challenges in protecting resources that power manufacturing processes, critical infrastructure, and more. This playbook offers an operations-focused approach to ICS security that recognizes both the unique requirements of industrial environments and the evolving threats they face.

Introduction

Industrial control systems were originally designed for reliability and efficiency in isolated environments, not cybersecurity in interconnected settings. This fact, combined with the integration of legacy systems, Industry 4.0 initiatives, and supply chain vulnerabilities, has created a complex risk landscape that traditional IT security approaches cannot adequately address.

Asset-Centric Security

This **ICS Security Playbook** provides a prevention-first framework for protecting cyber-physical systems throughout their entire lifecycle with these complexities in mind. It is built around TXOne's **Asset-Centric Security**—unlike conventional security approaches that focus primarily on perimeter protection, TXOne's approach is to focus specifically on each stage of an asset's lifecycle and protect it along the way.

Understanding ICS and ICS Security

Security in industrial environments is now a critical business concern that spans departments, affects strategic planning, and directly impacts operational continuity.

An Industrial Control System (ICS) includes the devices, networks, systems, and controls used to operate and automate industrial processes. Unique components include:

- Sensors and Field Devices
- Programmable Logic Controllers (PLCs)
- Remote Terminal Units (RTUs)
- Human-Machine Interfaces (HMIs)
- Supervisory Control and Data Acquisition (SCADA) Systems

Unlike typical IT systems that primarily process data, industrial control systems interact directly with the physical world, controlling equipment and processes that may be critical to safety, production, or essential services.

What is ICS Security, and Why Do You Need It?

ICS security includes the practices, technologies, and methodologies that protect industrial control systems from threats to their availability, integrity, or confidentiality. Beyond traditional IT security, it prioritizes operational continuity, system integrity, and safety—a different risk profile that prioritizes operational requirements in industrial environments.

Here is a closer look at some of IT and OT security's differences:

Aspect	IT Security	ICS/OT Security
Primary Concern	Data confidentiality	System availability and safety
Update Processes	Regular patching	Limited maintenance windows
System Lifecycle	3-5 years	15-20+ years
Downtime Tolerance	Minutes to hours	Seconds or zero tolerance
Protocol Standardization	Standardized (TCP/IP)	Mix of proprietary and standard
Change Control	Relatively flexible	Highly restrictive
Physical Impact	Limited	Potentially severe

The consequences of inadequate ICS security can be complex and severe. They often extend beyond data loss or service disruption, and may include:

- physical damage to equipment
- environmental hazards
- safety risks to personnel
- prolonged operational downtime

Production downtime from cyberattacks can cost manufacturers hundreds of thousands of dollars per hour, while safety-critical systems breaches can potentially endanger human lives. These potential impacts make ICS security not just an IT concern but a fundamental operational priority.

Causes of ICS Vulnerability

Several key factors have created a more challenging threat landscape, driving today's growing need for sophisticated ICS security. These include both inherent risks and external threat developments, such as:

- **IT/OT Convergence**: Integration between traditional business IT systems and operational technology has expanded the attack surface and introduced new vulnerabilities. Networks that were once isolated have now been connected for data collection, analysis, and remote management, creating potential pathways for attackers.
- **Legacy Systems**: Many industrial environments use control systems that were designed decades ago when cybersecurity was not a primary concern. These systems can be difficult to patch, upgrade, or replace without significant operational disruption.
- **Evolving Threat Landscape**: Targeted attacks against industrial infrastructure have grown in sophistication and frequency. State-sponsored actors, hacktivists, and financially motivated cybercriminals view industrial targets as high-value objectives.
- **Remote Access Proliferation**: The growth of remote work, vendor maintenance, and cloud connectivity has extended the potential attack surface, creating new vectors that attackers can exploit.

Recent incidents have demonstrated that attacks can cause severe damages to physical equipment, extended operations, and business results.

TXOne Networks' Asset-Centric Security Approach addresses these challenges with defense-in-depth protection tailored specifically for industrial environments. It emphasizes continuous verification and authentication, least-privilege access controls, and operational technology-specific protection mechanisms that secure assets throughout their entire lifecycle.

Elements of a Robust ICS Security Framework

A robust ICS security program reduces risk and delivers measurable operational benefits, including system reliability, reduced downtime, enhanced regulatory compliance, and greater operational visibility.

Effective ICS security not only reduces risks—it translates to greater business value through higher productivity, lower maintenance costs, and improved quality control. Measurable operational and competitive benefits include:

- fewer unplanned outages
- improved regulatory compliance
- protection from advanced threats targeting industrial environments

You can achieve your own robust ICS security by understanding your operational context, prioritizing protection of critical assets, and implementing defense-in-depth strategies tailored to your environment.

6 Core Principles of Successful ICS Security

TXOne has identified six principles of ICS security that can enhance industrial organizations' security posture while maintaining the operational continuity that industrial processes demand. Once you have considered these principles, we will explore technologies, role-based impacts, and a step-by-step implementation roadmap for your own ideal ICS security framework.

1. Asset-Centric Security For CPS

Unlike a factory floor surrounded by walls, cyber-physical systems cannot rely on a single perimeter for protection, because they are made up of assets such as HMIs, PLCs, and engineering workstations. Any asset can be connected to the internet, and once exposed it bypasses the wall. The most reliable defense is to shield each asset individually, so that security is built from the inside out. Ideally, that shield should stay in place throughout an asset's entire lifecycle, meaning:

- During **onboarding**, when new assets are introduced to the shopfloor.
- In **staging**, when configurations and updates are applied to the assets.
- Through **production**, when assets begin their duties, carrying the weight of daily operations.
- During**maintenance,** the longest stage for most assets, when vulnerabilities and changesare meticulously managed to keep them safe.

By protecting every stage, you can reduce the risk of any single device becoming a weak link. The combined resilience of each individually secured asset will ultimately form a stronger security posture than any outer wall.

2. Real-Time Asset Inventory (Passive)

Naturally, operators can't protect what they don't know they have. In many plants, devices get added quietly, and once connected, they become unmonitored risks. Hidden devices, shadow OT, and legacy endpoints easily fly under the radar. Without visibility, risk management and security can only go so far. The issue is that traditional IT discovery tools send probes and scans that can unintentionally disrupt sensitive controllers or legacy systems. Alternatively, passive real-time inventory doesn't probe; it listens silently to network traffic and identifies devices based on how they communicate, providing a map of your assets without risking downtime. This gives you visibility and the ability to protect assets while leaving operations uninterrupted.

3. Network Segmentation & Virtual Patching

Flat OT networks are convenient for operations but dangerous for security. They leave every device exposed — like meeting an opponent on an open field, with no cover and no barriers to slow their advance. If one endpoint is compromised, an attacker can often move laterally without resistance. Segmentation breaks that chain by containing communication to only what is necessary. An HMI can talk to its PLC, but it doesn't need to reach every device on the network. Limiting interactions this way makes it easier to contain the blast radius if a cyberattack does befall your network.

Patching is far more impractical in OT environments than in IT environments. Downtime is intolerable in OT networks, so taking them down to patch them isn't feasible. Also, many assets run on legacy OSes that no longer receive vendor support, meaning there aren't even patches that can be applied to them. Virtual patching shields legacy or unpatchable devices at the network layer by intercepting and blocking exploit attempts and other malicious traffic.

Together, these controls preserve operational uptime while reducing exposure.

4. Secure Remote Maintenance & MFA

In modern OT environments, the ability for vendors and technicians to remotely access equipment for repair or maintenance has been a boon for many. However, these remote access connections are also highly risky entry points for attackers. If these connections are made without strong safeguards, they can provide a direct path to critical assets for bad actors. A simple but strong safeguard is access control through multi-factor authentication (MFA), which verifies identities and reduces the risk of unauthorized access.

Session controls should also be implemented to govern access; these controls can limit vendors to the assets they need (the principle of least privilege), bind access to specific maintenance windows, log all activity for accountability and automatically terminate idle or unauthorized sessions. Secure gateways provide another layer of protection: they isolate external connections from critical systems, inspect traffic and file transfers for malware, and enforce protocol rules defined by your security policy. Together, these safeguards make sure remote maintenance delivers efficiency without a stowaway of risk.

5. Change Control for Legacy Operating Systems

Many OT environments still depend on legacy operating systems like Windows XP or Windows 7. These platforms often run critical functions reliably but no longer receive vendor support or security patches. Upgrading can be risky or outright impossible, as newer systems may break compatibility with industrial applications or hardware.

In these situations, traditional patching isn't an option. Instead, organizations rely on strict change control and endpoint protection to defend against threats. Change control policies prevent unauthorized modifications to applications and system files, while endpoint safeguards block malware execution and restrict administrative privileges from being misused. This approach is about protecting the unpatchable — keeping legacy assets stable, trusted, and safe for ongoing operations even without official updates.

6. Continuous Monitoring & Anomaly Detection

Although segmentation goes a long way, it is not enough on its own. Access controls, patching, new threats, and insider-created risks can still arise. Therefore, continuous monitoring provides crucial visibility into what's happening on the network and at the endpoint in real time, ensuring that operators are alerted as soon as any activity deviates from the baseline. Anomaly detection tailored to ICS protocols, both at the endpoint and network level, enables this by identifying unusual patterns (e.g., a PLC receiving unexpected commands or abnormal user logins on an HMI) and flagging them. The speed of spotting these deviations gives organizations a better chance at containing threats before they cause disruption. This is how visibility becomes actionable defense.

Role-Based Impacts

Plant and Controls Engineers

On the shop floor, security is measured in uptime. In practice, that means the value of a security tool comes down to how little it disrupts operations. OT environments have virtually zero tolerance for interruptions since scanning tools, surprise reboots, or patch cycles could collide with production schedules. Instead, implementing passive asset inventory provides visibility into every connected device without disrupting fragile controllers. This can be delivered through TXOne's **Edge** series appliances which silently observe network traffic to identify assets and their communications without disruptions. **EdgeIPS** and **EdgeFire** perform the discovery, while **EdgeOne** enables operators to manage the results. Segmentation is a safety net that reduces the chance of a single point of failure. **EdgeIPS** also enforces OT-first micro-segmentation so that if one endpoint is compromised, the impact can't spread unchecked across the entire network. **StellarProtect** **Legacy Mode** applies change control to systems like Windows XP or 7 that can't be patched, shielding the machines that "just work", reducing the risk of tampering. These measures translate directly into safer updates, steadier processes, and overall greater stability for operations that cannot afford downtime.

Security Leaders and SOC Teams

Visibility is crucial to security teams, but is only truly meaningful if they can separate real issues from background noise. Continuous monitoring and anomaly detection, powered by **Stellar's** OBAD (Operations Behavior Anomaly Detection) at the endpoint and CPSDR (Cyber-Physical Systems Detection & Response) in the **Edge** series at the network layer, build a baseline for normal OT behavior so deviations stand out. With these, prioritization is simplified and actionable. Unpatchable legacy systems, which might otherwise offer attackers an exploitable surface, can be shielded with virtual patching that blocks known vulnerabilities. Segmentation confines potential breaches, limiting the scope of incident response and reducing the manpower required, since teams can focus their efforts where they are truly needed. Together, these tools generate intelligence that allows SOC teams to detect threats early and respond before they spread, reducing the time it takes to contain them.

Executive Stakeholders

For business leaders concerned with the bottom line, security must reinforce continuity, not clash with it. Remote maintenance secured through **EdgeFire's** VPN with MFA ensures vendors can service equipment without creating backdoors. Asset-centric protection, unified through **SenninOne**, keeps both new and legacy investments trustworthy across their long lifecycles. And **Element Safe Port** ensures removable media entering the environment is malware-free before it ever touches production assets. These measures protect not just operations but also reputation and revenue by reducing the risk of downtime — intolerable in OT environments — as well as regulatory penalties and safety incidents. In this way, cybersecurity becomes an operational safeguard that supports resilience and ROI, not just a compliance checkbox.