ebook

# Why VPNs Fail To Meet New OT Regulatory Requirements Such As NERC CIP

The NERC CIP-003-9 marks a meaningful shift in how regulators think about accountability. For years, logging a successful connection was considered sufficient, but the new compliance standards require something fundamentally different: a verifiable record of every action taken during a session. VPNs, regardless of vendor, were simply not built to provide governed access to critical infrastructure assets. They create a tunnel, and what happens inside remains invisible. Meeting the new standards means rethinking the OT architecture entirely, and that is where Xona Systems comes in, delivering isolated remote sessions with full activity logging so there are no tunnels, blind spots, or compliance gaps.

# The Compliance Clock Started

NERC CIP-003-9 took effect April 1, 2026, and for the first time, low-impact BES Cyber Systems face mandatory vendor remote access controls.

This changes the math for every utility with remote vendor connections. Before April 1, low-impact facilities had no specific requirement to manage how vendors connect, which means many have been operating without the controls the standard now demands.

Requirement R1, Part 1.2, Section 6 requires documented security controls for vendor electronic remote access. Your auditor will check three specific things.

Can you identify each vendor's remote access session individually? Not "a vendor connected today." Which vendor, which user, which asset, for how long? VPN credentials are often shared across multiple users at the same vendor organization, and a shared credential tells you nothing about who actually did what during that session.

Can you disable vendor remote access on demand? VPNs can be disabled, so this one is doable with what you have but cannot provide active defense to disable an active session in real-time based on emerging vulnerabilities.

Can you detect known or suspected malicious communications during a vendor remote access session? This is where VPN architecture fails completely. Your VPN encrypts traffic between the user and the network, giving it zero visibility into the payload. It cannot distinguish a legitimate Modbus polling request from a Modbus write command that changes a safety setpoint, and it cannot detect malicious communications because it cannot see the communications at all.

**Passing two of three requirements does not make you compliant.** Your auditor will assess all three starting April 1, 2026.

CIP-003-9 is not the only regulation tightening remote access controls. TSA Security Directive SD-02F, active through May 2026, requires pipeline operators to monitor remote access sessions at all times — and connection logs do not meet that bar. TSA expects you to know both that a session occurred and what happened within it.

| Regulation | What It Requires | The Gap It Exposes |
|---|---|---|
| **CIP-003-9** | Remote access controls for low-impact BES assets | Session visibility, not just connection logs |
| **TSA SD-02F** | Continuous monitoring of all remote sessions | Logs don't satisfy "monitor at all times" |
| **IEC 62443** | Zone and Conduit model for all OT connections | VPN tunnels bypass zone boundaries entirely |
| **NIST SP 800-82 R3** | Adapted controls for OT environments | "Adapted" means workable — not weaker |

The deadlines are not converging by coincidence. CIP-003-9 takes effect April 1, 2026. TSA SD-02F is active and renewing. IEC 62443 Zone and Conduit requirements are already appearing in procurement contracts across energy, manufacturing, and water.

Regulators and buyers are asking the same question: **"*Can you prove what happened during that session?*"**

# Your VPN Credentials Are the Way In

In 73% of the incident response cases Dragos has investigated, the entry point was the same: compromised credentials for VPNs, jump hosts, or valid accounts. The year before, when Dragos assessed industrial sites directly, 65% had insecure remote access configurations. The SANS 2025 ICS/OT survey found that 31% of respondents cannot even name all their remote access points, and half of all ICS/OT incidents in the past year began with an outside connection.

| 73% | 65% | 50% |
|---|---|---|
| of IR engagements involved compromised credentials | of assessed sites had insecure remote access configurations | of ICS/OT incidents started with a remote connection |

The threat tempo is not gradual. Dragos tracked 119 ransomware groups targeting industrial companies in 2025, up 49% in a single year, hitting 3,300 organizations in total. Remote access is not one of the ways they get in. It is the way.

**Threat Group Activities:**

**SYLVANITE + VOLTZITE**
SYLVANITE exploited vulnerabilities in Ivanti VPN appliances within 48 hours of public disclosure, then handed that access to VOLTZITE, a group that specializes in OT environments and long-term persistence. Patches existed. But 48 hours between disclosure and exploitation is faster than most OT patch cycles, and that window is all an attacker needs — not to break in, but to walk in.

**Poland Energy Sector**
Coordinated attacks hit Poland's energy sector after attackers entered through internet-facing FortiGate VPN appliances using default credentials and known vulnerabilities, then moved laterally across more than 30 wind, solar, and heat generation sites. Wiper malware destroyed RTU firmware and corrupted HMI data, wiping out remote monitoring and control entirely. Power continued flowing, but operators were blind. CISA published an advisory in February 2026 urging U.S. infrastructure operators to study what happened.

The pattern is consistent across every case: attackers do not defeat VPN authentication, they use it. Stolen credentials, reused passwords, unrevoked vendor accounts are not sophisticated techniques so much as the logical consequence of how VPNs were designed.

Once a session authenticates, it is trusted, and everything that happens inside it is invisible. That is not a vulnerability waiting to be patched. It is the architecture working exactly as intended.

# Three Architectural Failures VPN Hardening Cannot Fix

When remote access becomes a liability, the instinct is to harden the VPN. Stronger authentication. Tighter firewall rules. More logging. None of it addresses what is actually broken, because these failures are structural, not configuration problems.

- **The first is access scope.** A VPN authenticates you and hands you the network. A technician validating firmware on a single Siemens S7 PLC has no need to reach the historian, the DCS, or the safety instrumented system. VPN-based access grants it anyway. The technician gets an IP on the OT subnet and can reach every device on that segment. Modbus PLCs do not authenticate connections. DNP3 outstations do not verify whether the user issuing commands is authorized. These protocols were built for physically secured facilities where network presence meant physical access. A VPN extends that assumption to anyone with valid credentials, anywhere on the internet. ISA/IEC 62443-3-3 requires authorization enforcement at the asset level. A VPN has no mechanism for that. It inherits whatever segmentation problems already exist in your environment.
- **The second failure follows from the first.** Broad access through an encrypted tunnel means the VPN has no visibility into what that access is actually doing. In 2024, FrostyGoop malware targeted Modbus TCP directly to manipulate heating controllers at a Ukrainian energy facility. No exploit. No zero-day. Just legitimate Modbus commands sent to devices that executed whatever they received. A protocol-aware gateway would have flagged the unauthorized write commands. The VPN forwarded them without inspection. To a VPN, a Modbus write that changes a setpoint on a safety system and a routine read request look identical. Both are encrypted packets.
- **The third failure is what the first two make inevitable.** The third failure is what the first two make inevitable. Your VPN logs confirm a connection existed. They cannot tell you what happened inside it, and that distinction is exactly what NERC CIP-003-9 and TSA SD-02F are asking you to prove. Both regulations demand session-level evidence, not timestamps and source IPs. Only 13% of organizations implement session recording for remote OT access, and only 23% use session brokering, which places a gateway between the remote user and the target asset so every action passes through a point where it can be inspected, recorded, and controlled. Without that architecture, your security team spends roughly six months before every NERC CIP audit manually reconstructing activity from fragmented logs scattered across SIEMs, firewall records, and endpoint telemetry. With session-level recording at the access point, that same preparation takes three weeks. The difference is not operational efficiency. It is whether your architecture can produce the evidence the regulation requires.

# Three Mistakes Organizations Make When Replacing Their VPN

**Assuming Better Authentication Means Better Architecture** A lot of products marketed as OT remote access replacements authenticate differently but still give the remote user a network path to OT assets. The login is stronger, but the attack surface is identical. An attacker who compromises valid credentials can still reach the same devices, use the same protocols, and operate with the same lack of visibility as before. Stronger authentication is a narrower door into the same room.

**Treating Agentless as Architecturally Disconnected** Agentless is a common selling point, and it sounds more secure than it is.

A product can require no agent on the user's device and still route a full network path to every Modbus device on your OT subnet. The absence of an agent says nothing about what the session can reach once it connects. What changed is the installation experience. The network exposure is identical.

### Applying IT-Centric ZTNA to OT Environments

IT-centric ZTNA moves authentication off-premises and may eliminate the VPN client, but underneath those changes the remote session still creates a network tunnel to the OT asset. The authentication is more sophisticated and the client footprint is smaller, but a remote user who authenticates successfully still lands on your OT network with the same reachability they would have had through a traditional VPN. OT environments require asset-level authorization, protocol awareness, and session isolation. IT-centric ZTNA was not designed for any of that.

## The Architecture That Fixes All Three Mistakes

The three mistakes share a common root: the architecture still puts a network between the remote user and your OT assets. The right architecture removes that network path entirely. Here is how each piece does that.

**✓ The Gateway Terminates OT Protocols Before They Reach The User**

Your technician never actually touches your OT assets. The gateway connects to them directly, translates the session into a visual stream, and that is all the user's device ever receives. If their machine is compromised, the attacker gets a video feed. A Modbus connection is never in play.

**✓ Every Session Is Locked To A User, An Asset, And A Time Window**

Every session is tied to a specific user, a specific asset, and a specific time window. When that window closes, access ends. There are no persistent credentials to rotate, no shared accounts to audit, and nothing left behind that an attacker can find later. Access that does not persist cannot be stolen.

**✓ Every Action Inside The Session Is Recorded**

Every command, every screen state, every mouse click is captured. Not a log entry that says a connection opened and closed. When an auditor asks what your vendor did during a two-hour session at 2am, you can show them exactly what happened, in sequence, with no gaps.

**✓ Nothing Gets Installed On Your OT Devices**

The gateway works with whatever is already on the OT side. Windows XP workstations, 20-year-old PLCs, proprietary HMI software. Nothing gets installed, nothing gets modified, and no firmware update is required. Many OT devices cannot accept software changes without full recertification, which means any solution that requires an endpoint agent cannot be deployed across a significant portion of your environment.

**✓ It Works Where Your OT Assets Actually Are**

The gateway operates over links as narrow as 512 Kbps. Satellite connections to offshore platforms. Microwave links to remote substations where bandwidth is measured in kilobits. No cloud dependency, no persistent internet connection required.

# What the Right Architecture Actually Delivers

OT and plant managers do not need another security product that creates work. They need remote access that works the way the plant works: controlled, auditable, and scalable.

Here is what it looks like:

### A Vendor Calls In For A Maintenance Window

Instead of opening a VPN account, creating a firewall exception, and hoping the vendor does not poke around outside the scope of the job, the plant manager provisions a time-bound session scoped to a single asset. The vendor connects through a browser. No agent to install. No network access beyond the device they are there to work on. When the window closes, the access closes. Nothing lingers.

### An Auditor Asks What Happened During A Vendor Session Three Months Ago

Instead of spending weeks pulling logs from the SIEM, the firewall, and endpoint telemetry and trying to reconstruct a timeline, the plant manager pulls the session recording. Every action, every command, every screen interaction is on record. The audit response takes hours, not months.

### A New Compliance Requirement Lands

Instead of scrambling to retrofit controls onto an architecture that was never designed to support them, the plant manager already has session brokering, identity-based access, and full session recording in place. The framework maps to what the architecture already does.

Every hour spent managing VPN exceptions, chasing audit evidence, and cleaning up after vendor sessions with no visibility is an hour not spent running the plant. The right architecture does not just reduce risk. It gives that time back. Xona is built for exactly this environment. Browser-based, no agents, no network reconfiguration, deployed in 20 minutes. Every session brokered, recorded, and scoped to the asset.

# How Xona Delivers the Right Architecture

| The Right Architecture Requires | How Xona Delivers It |
|---|---|
| **Remote users never touch the OT network directly** | **✓ Every session is brokered through a gateway. The user connects to Xona. Xona connects to the asset. The two connections are never bridged.** |
| **Access scoped to a specific asset, not a subnet** | **✓ Vendors are granted access to one defined asset for one defined purpose. No lateral movement. No reachability beyond the scope of the session.** |
| **Every session tied to a verified identity** | **✓ MFA, SAML, LDAP, and Active Directory enforced on every session. No shared credentials. No standing accounts.** |

| | |
|---|---|
| **Access that expires when the work is done** | **✓ Sessions are time-bound. When the window closes, access closes. No persistent tunnels. No residual network paths.** |
| **A complete record of what happened, not just that something happened** | **✓ Every session is recorded automatically. Every command, every screen, every action. Replay on demand. Compliance evidence generated at the access point.** |
| **Visibility into OT protocol activity** | **✓ The gateway terminates OT protocols at the boundary. It can distinguish a Modbus read from a Modbus write. A VPN cannot.** |
| **Compliance mapped to the framework, not retrofitted onto it** | **✓ NERC CIP, IEC 62443, TSA SD-02F, NIS 2, and NIST 800-53 mapped natively into the architecture.** |
| **Deployment that does not require network reconfiguration** | **✓ Browser-based, no agents, no firewall changes. Deployed in 20 minutes.** |

Xona is built for exactly this environment. No agents, no firewall changes, no network reconfiguration required. The gateway deploys in 20 minutes and sits at the boundary, brokering every session so that remote users connect to Xona and Xona connects to the asset, with those two connections never merged into a single tunnel. Access is scoped to a specific asset, bound to a verified identity, and closed the moment the session ends, leaving no persistent paths and no residual exposure.

What remains is a complete, tamper-evident record of everything that happened inside the session, generated natively at the access point and mapped directly to NERC CIP, IEC 62443, TSA SD-02F, NIS 2, and NIST 800-53.

# Take the Next Step

Connect with Secure Remote Access Experts for OT Environments. Learn how Zero Trust remote access can strengthen your OT security posture while improving operational efficiency.

Visit **www.xonasystems.com** to learn more or **schedule a demo** with our OT security specialists.About Xona Systems

# About Xona Systems

Xona Systems is the secure access platform purpose-built for OT and critical infrastructure. Recognized as an Overall, Product, Innovation, and Market Leader in KuppingerCole's 2025 Leadership Compass for Secure Remote Access for OT/ICS, Xona is deployed in 40+ countries across energy, utilities, manufacturing, oil & gas, maritime, water, defense, and mining.

Learn more at **xonasystems.com**

---

**Sources**


- Dragos, 9th Annual OT Cybersecurity Year in Review, 2026. https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review
- Dragos, 8th Annual OT Cybersecurity Year in Review, 2025. https://www.dragos.com/dragos-2025-ot-cybersecurity-report-a-year-in-review
- SANS Institute, State of ICS/OT Security 2025. https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- CISA, Poland Energy Sector Cyber Incident Advisory, February 2026. https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps
- CISA/NCSC-UK, Secure Connectivity Principles for OT, January 2026. https://www.cisa.gov/resources-tools/resources/secure-connectivity-principles-operational-technology-ot
- Gartner, Market Guide for CPS Secure Remote Access, February 2026. https://www.gartner.com/en/documents/6046877
  NERC, Standard CIP-003-9. https://www.nerc.com/standards/reliability-standards/cip/cip-003-9
- TSA, Security Directive Pipeline-2021-02F. https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
- NIST, SP 800-82 Revision 3, September 2023. https://csrc.nist.gov/pubs/sp/800/82/r3/final
- IEC, 62443-3-3 System Security Requirements and Security Levels, 2013. https://www.isa.org/products/ansi-isa-62443-3-3-2013-security-for-industrial-au