Case Study

Securing 800+ Substations Before the NERC CIP-003-9 Deadline

How Zero-Trust Secure Access Delivered Full CIP-003-9 Section 6 Compliance Across All Low-Impact BES Cyber System Sites — With a Two-Person Team.

xona

Executive Summary

A leading investor-owned electric utility operating more than 800 substations and generation sites faced the **April 1, 2026 NERC CIP-003-9 compliance deadline** — requiring documented vendor electronic remote access controls at all low-impact BES Cyber System sites.

With no standardized vendor access governance, an understaffed compliance team, and dozens of OEM vendors using VPNs, TeamViewer, or on-site visits, the utility deployed **Xona Critical System Gateways** managed through the Xona Central Manager (XCM). The result is zero direct network access — users interact with OT systems in real time, but their endpoints are never connected to the OT network.

This architecture delivered full CIP-003-9 Section 6 compliance across all control areas, vendor access reduced from 4+ hours to 8 minutes, zero compliance findings, and a complete rollout by a two-person team using pre-configured DIN-rail appliances requiring no network changes.

RESULTS AT A GLANCE	
800+	Sites Secured
100%	CIP-003-9 Section 6 Compliance
20 min	Avg Deployment per Site
4 hrs → 8 min	Vendor Access Time
0	Compliance Findings
2-Person	Deployment Team
800+	Sites Secured

The Challenge

Like many large utilities, this organization operates a geographically dispersed fleet of substations and generation sites. The vast majority — over 800 — are classified as **low-impact BES Cyber Systems**. Historically, these sites received less cybersecurity attention than medium- and high-impact counterparts. Vendor access was informal: some vendors used corporate VPNs, others relied on TeamViewer, and many simply traveled to the site.

When NERC approved CIP-003-9 with Section 6 requirements for vendor electronic remote access at low-impact sites, the utility confronted several challenges:

- **Regulatory urgency:** The April 1, 2026 deadline required controls for preauthorization, monitoring, logging, recording, alerting, and disabling of all vendor sessions — none of which existed at any low-impact site. A missed deadline means potential NERC violations, civil penalties up to $1 million per violation per day, and mandatory disclosure — consequences no compliance team can absorb.
- **Scale:** 800+ sites requiring uniform controls, many in rural locations with limited connectivity and no on-site IT staff.
- **No vendor access governance:** No intermediate system, no session recording, no centralized logging. Vendor credentials were often shared and access was not time-limited.
- **Understaffed compliance team:** Fewer than five dedicated staff for evidence collection, policy development, and audit preparation across all CIP standards.
- **40+ OEM vendors:** Each requiring access to diverse OT assets — protective relays, RTUs, PLCs, substation automation systems, and SCADA servers.

Why Legacy Approaches Fall Short

The utility evaluated extending its enterprise VPN, deploying jump servers, and repurposing its IT PAM tool. Each failed to meet CIP-003-9 Section 6:

- **VPNs** grant broad network access rather than user-to-asset access, provide no session recording or moderated approval workflows, and do not satisfy the intermediate system requirement.
- **Jump servers** are themselves attack surfaces — the Colonial Pipeline breach entered through a compromised VPN credential, exposing how broad network access amplified the blast radius of a single stolen password. They lack native session recording and JIT controls, and are impractical to deploy at 800+ sites.
- **IT-centric PAM tools** require endpoint agents, complex network integrations, multi-week deployment cycles per site, and lack OT protocol support and industrial hardware form factors for substations.

The Solution: Xona Critical System Gateway

The utility selected the Xona CSG as the purpose-built solution for CIP-003-9 compliance across all low-impact sites.

Protocol Isolation

OT protocols (RDP, SSH, VNC) terminate inside the trusted network at the gateway. Only encrypted pixel streams reach the vendor's browser over HTTPS 443. No direct endpoint-to-OT connectivity ever exists — breaking the cyber kill chain and satisfying the intermediate system requirement.

20-Minute Deployment

Pre-configured DIN-rail appliances (IEC 61850 / IEEE 1613 compliant) install without network reconfiguration, firewall changes, or OT asset modifications. Only HTTPS 443 outbound is required.

Centralized Fleet Management

The XCM provides a single pane of glass for policy control, identity federation, log aggregation, and reporting across all 800+ sites. Sites operate autonomously during WAN outages.

JIT Vendor Access

Moderated approval workflows ensure no standing access. Sessions are scoped to specific assets with TBAC that auto-terminates on expiry.

Full Session Recording

Every RDP, SSH, and VNC session is recorded with timestamps and keystroke metadata. Administrators can shadow live sessions and terminate any session instantly via Kill Button.

Lockbox Emergency Controls

Logically disables all access to a gateway or physically disables Ethernet ports — providing instant, verifiable access revocation for incident response.

Solution Highlights
✓ Protocol Isolation (pixel streaming, HTTPS 443)
✓ Lockbox Emergency Access Disable
✓ Xona Central Manager (XCM) Fleet Management
✓ DIN-Rail Hardware (IEC 61850 / IEEE 1613)
✓ JIT Vendor Access with Moderated Approval
✓ SAML 2.0 / MFA Integration
✓ Full Session Recording (RDP, SSH, VNC)
✓ SIEM Export (Splunk, QRadar, Sentinel)
✓ Time-Based Access Control (TBAC)
✓ Credential Injection

> *"Managing 800 substations, we couldn't afford an 18-month deployment. We needed CIP-003-9 controls on every site before April — and we got there with a two-person team. That's not something I thought was possible before Xona."*
>
> **— VP of OT Security, Investor-Owned Electric Utility**

Implementation

The utility adopted a phased rollout: 10 pilot sites in weeks 1–2, approximately 100 sites per week through weeks 3–10, and full fleet coverage by week 16. The same two-person team completed the entire deployment.

- **Average time per site:** 20 minutes from hardware mount to first vendor session
- **Network changes:** Zero — overlay design with single outbound HTTPS 443
- **Vendor onboarding:** 40+ OEMs onboarded with individual SAML-federated identities and MFA; no shared credentials
- **Configuration:** Local technicians mounted DIN-rail hardware; remote XCM configuration handled centrally

Results

Full CIP-003-9 Section 6 Compliance

The utility achieved documented compliance with all 14 control requirements. The following table maps each requirement to the Xona capability:

Sec.	Requirement	Xona CSG Capability
6.1.1	Preauthorization	SAML 2.0 SSO + MFA; user-to-asset RBAC; time/date controls; JIT provisioning
6.1.2	Vendor logon alerts	Moderated Access with admin notification on all vendor activity
6.1.3	Session monitoring	Live session shadowing by Administrator and Monitor roles
6.1.4	Logging/alerts	Splunk, RSyslog, Generic HTTP log export; cryptographic log signing
6.1.5	Time-of-need access	TBAC restricts sessions to maintenance windows or specific date/time ranges
6.1.6	Session recording	Full video recording of all RDP, SSH, VNC sessions with timestamps
6.1.7	System logs	Connection history, system events, user actions; SIEM export; 90-day+ retention
6.2.1	Disable accounts	Lockbox + per-user account revocation; immediate access termination
6.2.2	Disable ports/services	Lockbox + Kill Button; software and hardware port disable
6.2.3	Disable protocols	Edit Connection disables individual protocols (RDP, SSH, VNC)
6.2.4	Remove physical connectivity	Lockbox physically disables trusted/untrusted Ethernet ports
6.3.1	Anti-malware	Protocol isolation prevents injection; moderated file transfer with AV scanning
6.3.3	Log review	Video + data logs; local review or automated SIEM forwarding
6.3.4	Alerting	SIEM for automated alerting; Moxa relay for physical alerting at site

Operational & Security Improvements

- **Vendor access:** Reduced from 4+ hours to 8 minutes through JIT moderated access with browser-based connectivity.
- **Audit evidence:** All session recordings, access logs, and policy configurations centrally stored and exportable — eliminating hundreds of hours of manual evidence collection.
- **Compliance findings:** Zero findings in first internal audit post-deployment (previously 3 findings).
- **Attack surface:** Protocol isolation eliminated all direct endpoint-to-OT connectivity. Ransomware, malware, and lateral movement are architecturally impossible.
- **Credential hygiene:** Credential injection eliminates shared passwords. Vendors never see or handle OT asset credentials.
- **Incident response:** Lockbox and Kill Button provide instant access revocation — reducing response time from hours to seconds.

Looking Ahead

With CIP-003-9 Section 6 compliance achieved, the utility is now positioned for the next phase of operational expansion and evolving NERC requirements:

- **Medium/high-impact expansion.** Extending Xona to medium and high-impact BES sites, replacing legacy jump servers and VPNs at control centers and critical generation facilities.
- **Forescout integration.** Automated asset discovery and dynamic risk-based access policy enforcement through the Forescout 4D OT Security platform.
- **CIP-005-7 readiness.** Xona's Kill Button and Lockbox natively support upcoming requirements for identifying and disabling active vendor sessions at medium/high-impact sites.
- **SIEM expansion.** Correlating Xona session telemetry with Splunk network security data for automated alerting and SOAR-driven incident response.

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**.*