Case Study

Rail Operator Secures Signal and Control Systems Under TSA Directive

How a major Class I freight railroad consolidated 40+ vendor access tools into a single platform — achieving TSA compliance across 15,000+ miles of track without disrupting operations.

XONA

Executive Summary

A major Class I freight railroad operating more than 15,000 miles of track faced a convergence of challenges: TSA cybersecurity directives mandating remote access controls, 40+ signaling and control system vendors each using their own remote access methods, and the operational reality that rail systems cannot be taken offline for security upgrades.

By deploying the Xona platform, the railroad consolidated all vendor access through a single secure gateway, achieved full TSA compliance, and established a unified audit trail covering every session at every location — with zero operational disruptions during rollout. The result is zero direct network connectivity — users interact with OT systems in real time, but their endpoints are never connected to the OT network.

RESULTS AT A GLANCE	
40+ → 1	Vendor access tools consolidated to a single Xona platform
240+	Locations secured (dispatch centers, signaling hubs, field sites)
TSA Compliant	Full alignment with TSA cybersecurity directives for rail
100%	Session recording for all vendor and internal user access
Zero	Operational disruptions during phased rollout

Industry Context: Rail Cybersecurity at a Crossroads

Following the Colonial Pipeline attack, TSA issued cybersecurity directives for freight and passenger rail operators requiring cybersecurity implementation plans covering remote access controls, network segmentation, vendor access governance, and incident response. TSA's 2024 rail cybersecurity NPRM — separate from the pipeline cybersecurity NPRM — signaled intent to make these requirements permanent for surface transportation, including continuous monitoring and supply chain security controls.

Rail cybersecurity is not abstract compliance. Signaling systems prevent collisions. Positive Train Control (PTC) enforces speed restrictions. Dispatch centers coordinate traffic across thousands of miles. A compromise of any of these systems has direct public safety consequences — making rail OT security fundamentally different from enterprise IT. A compromise of positive train control systems could result in catastrophic incidents with direct liability in the hundreds of millions.

Modern rail infrastructure relies on 40+ specialized vendors: signaling manufacturers, PTC providers, communications suppliers, dispatch system developers, and rolling stock OEMs. Each requires routine remote access with their own proprietary tools, credentials, and processes — creating a fragmented access landscape with limited operator visibility.

The Challenge: 40+ Vendors, Zero Unified Governance

The railroad's OT footprint spanned 15,000+ miles of track, hundreds of field locations, 5 regional dispatch centers, and 35+ major signaling hubs. The security problems were significant:

- **No unified access governance.** Each vendor managed their own credentials and connection methods. When vendor personnel changed, the railroad had no timely way to revoke access across all tools.
- **Fragmented audit trail.** With 40+ access tools, the railroad could not produce a unified record of who accessed which system, when, and what they did — a direct TSA compliance gap.
- **No session recording.** Most vendor sessions were unrecorded. In the event of a misconfiguration or suspected compromise, no forensic evidence existed.
- **No instant disconnect.** Contacting 40+ vendors to suspend individual access methods would take hours — unacceptable for safety-critical systems.
- **Operational continuity constraints.** Signaling, PTC, and dispatch systems cannot be taken offline for security tool installation during active train movements.

The Solution: One Platform for All Vendor Access

Protocol Isolation

Xona's CSG terminates OT sessions inside the trusted rail network, streaming only encrypted pixels to vendor browsers. No VPN tunnel, no direct network path, no opportunity for malware traversal. For safety-critical signaling systems, this provides the digital equivalent of a physical air gap while maintaining full interactive access.

Centralized Management via XCM

A single pane of glass for provisioning and deprovisioning all vendor access across the network, with RBAC/TBAC controls, real-time session monitoring, Kill Button for instant termination, and unified audit reporting. Every vendor access event across all 240+ locations is visible from one console.

DIN-Rail Hardware for Field Locations

Xona's industrial DIN-rail CSG — meeting IEC 61850 and IEEE 1613 standards — was purpose-designed for space-constrained wayside signal cabinets and equipment enclosures that standard rack equipment cannot fit. Pre-configured units were installed by field technicians during routine maintenance windows with no network changes required.

Moderated Access ("Wait Room")

Every vendor session requires railroad administrator authorization before going live. Vendors request access through the portal; the OT team verifies the maintenance ticket and approves for a specific asset and time window. No vendor can access any system without explicit, per-session authorization.

Solution Highlights — Xona Features Deployed
• **Protocol Isolation (PNG pixel streaming)**
• **CSG — 1U rack and DIN-rail form factors**
• **Xona Central Manager (XCM) for fleet governance**
• **MFA via SAML 2.0**
• **RBAC per vendor per asset + TBAC for maintenance windows**
• **Moderated Access / Wait Room for vendor sessions**
• **Just-In-Time (JIT) access provisioning**
• **Full Session Video Recording**
• **Live Shadowing & Kill Button**
• **Lockbox Emergency Revocation**
• **SIEM Integration for centralized logs**
• **Credential Injection (no shared passwords)**
• **Zero Footprint — browser-based, no vendor agents**

Implementation: Phased Rollout, Zero Disruption

Phase 1 - Dispatch Centers (Weeks 1–4)

1U rack CSGs deployed at 5 regional dispatch centers. XCM configured for centralized management. SIEM integration validated. Operational baseline established for all subsequent phases.

Phase 2 - Signaling Hubs (Weeks 5–12)

35 major signaling hubs secured. All signaling vendors migrated to Xona with asset-specific RBAC and maintenance-window TBAC. Session recording activated across all hub locations.

Phase 3 - Field Locations (Weeks 13–24)

200+ field sites equipped with pre-configured DIN-rail CSGs, installed by field technicians during routine maintenance. No network changes, no IT deployment teams required.

Phase 4 - Consolidation (Weeks 25–30)

All 40+ vendors migrated to Xona. Legacy VPN concentrators, TeamViewer, proprietary tools, and modem connections decommissioned. Unified audit trail validated end-to-end.

> *"The ability to govern all vendor access from a single platform — and produce a unified audit trail for every session across 240 locations — fundamentally changed our compliance posture. We went from fragmented visibility to complete control."*
>
> **— Director of OT Cybersecurity, Class I Freight Railroad**

Results

Dimension	Before Xona	After Xona
Remote access tools	**40+ vendor-specific tools**	**1 unified platform (Xona)**
Vendor onboarding	**Days to weeks per vendor**	**Minutes — browser-based, no agents**
Session visibility	**Fragmented; many sessions unrecorded**	**100% recording and monitoring**

Access governance	**Vendor-managed; no central control**	**Operator-controlled RBAC/TBAC per asset**
Credential management	**Shared credentials common**	**Credential injection; no shared accounts**
Incident response	**No instant disconnect**	**Kill Button + Lockbox for immediate revocation**
TSA compliance	**Non-compliant**	**Fully compliant**
Audit trail	**Scattered across 40+ tools**	**Unified, centralized via XCM**

Every signaling vendor, PTC provider, communications manufacturer, and dispatch developer now accesses their systems exclusively through Xona. Deployed in 30 weeks across 4 phases, the platform now governs 240+ locations, consolidates 40 vendor access tools to 1, and has onboarded all 40+ vendors with unique identities — eliminating shared credentials entirely. TSA compliance achieved across all requirements. Every session at every location is video-recorded and searchable. The entire phased deployment was completed without a single disruption to live rail operations.

Regulatory Alignment: TSA, IEC 62443, NIST

Requirement	Framework	How Xona Addresses It
Remote access controls	TSA Directives	**Protocol isolation; all sessions brokered through CSG with MFA + RBAC**
Network segmentation	TSA Directives	**CSG in DMZ; OT protocols inside trust boundary; only HTTPS/443 crosses zones**
Vendor access governance	TSA Directives	**Centralized portal via XCM; moderated access; JIT provisioning**
Session recording & audit	TSA / IEC 62443	**Full video recording; keystroke logging; SIEM integration; log signing**
Incident response disconnect	TSA Directives	**Kill Button for instant termination; Lockbox to disable all access**
Authentication (SR 1.1–1.13)	IEC 62443	**MFA via SAML 2.0; hardware tokens; FIPS-validated crypto**

Use control (SR 2.1–2.12)	IEC 62443	**RBAC; TBAC; concurrent session control; supervisor override**
Boundary protection (SC-7)	NIST 800-53	**Protocol isolation; single HTTPS port; no OT protocol exposure**
Audit & accountability	NIST 800-53	**Comprehensive logging; session video; SIEM export; log integrity**

Looking Ahead

The railroad is extending Xona to PTC back-office systems and wayside equipment maintenance, station automation and facility OT, and pursuing formal IEC 62443 certification. Automated compliance dashboards drawing on Xona session data will maintain continuous audit readiness as TSA finalizes permanent rulemaking.

For rail operators navigating increasingly prescriptive regulations, the Xona deployment demonstrates that comprehensive vendor access governance does not require operational sacrifice. Safety, reliability, and compliance coexist — when the access architecture is purpose-built for operational technology.

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***