Case Study

Protecting the Nation's Water: A Municipal Utility's Zero-Trust Transformation

How a regional municipal water authority secured 50 distributed sites — achieving EPA AWIA compliance and complete vendor accountability without a single network change.

Executive Summary

Organization	Regional Municipal Water Authority
Sites	50 (40 wastewater + 10 water treatment/distribution)
SCADA Team	7 operators — GE iFIX, Rockwell PLCs, VMware vSphere
Previous Access	On-site only at most plants; inconsistent VPN at select sites
Deployment	3-year phased rollout: 30 → 45 → 50 sites

A regional municipal water authority responsible for 50 distributed sites faced a stark reality: most plants had no remote access at all, and the few that did relied on inconsistent VPN configurations with shared credentials and manual firewall port-opening for vendors. With 12 confirmed attacks on water infrastructure in a single 12-month period and EPA AWIA recertification deadlines approaching, the authority needed a solution its seven-person SCADA team could deploy without disrupting existing infrastructure.

By deploying Xona's Critical System Gateway (CSG) in a phased three-year rollout, the authority achieved zero-trust secure access across all 50 sites without a single network change. Vendor access transitioned from shared credentials and manual firewall rules to named accounts with MFA, moderated approval workflows, and full session recording — all for approximately $112,000 to $150,000 per year in a phased rollout aligned to municipal budget cycles.

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	
50 sites secured	Across water treatment and wastewater collection
Zero network changes	To existing SCADA infrastructure
100% vendor accountability	Shared credentials eliminated
~$150K/year	Affordable for municipal budgets
30 minutes	Deployment per site by existing SCADA team
Full EPA AWIA alignment	With audit-ready session logs

Industry Context: Water Under Siege

The water and wastewater sector has become one of the most actively attacked segments of critical infrastructure. Between November 2023 and November 2024, researchers documented 12 confirmed successful attacks on water infrastructure worldwide — from the Muleshoe, Texas tank overflow caused by exploited default passwords, to American Water's forced shutdown after attackers used living-off-the-land techniques for lateral movement, to CISA's emergency alert on Chinese state-sponsored actors targeting ICS systems across U.S. water utilities.

Research by Semperis found that 81% of cyberattacks on utilities originate from compromised identity systems. The most common attack path is not a sophisticated zero-day exploit — it is stolen or default credentials used through legitimate remote access pathways. Nation-state actors including Volt Typhoon and the BAUXITE threat group have been confirmed targeting water and wastewater systems across the United States, Europe, and the Middle East.

The EPA's America's Water Infrastructure Act (AWIA) requires community water systems to complete cybersecurity-inclusive Risk and Resilience Assessments with recertification deadlines between March 2025 and June 2026. EPA inspectors are specifically seeking evidence of MFA on all remote access, named and time-boxed vendor accounts with session logging, and IT/OT segmentation. The forthcoming CIRCIA regulation will require 72-hour incident reporting — utilities without proper access controls and audit trails will struggle to comply.

The Challenge: Fragmented Access Across 50 Sites

The authority's 50 sites ran GE iFIX for HMI and supervisory control, Rockwell PLCs for process automation, and VMware vSphere for virtualization. The access situation was fragmented:

- **No remote access at most sites.** The team drove to facilities for every issue — a major constraint for seven people covering a large geographic region.
- **Shared credentials for vendors.** Process control integrators used shared usernames and passwords with no individual accountability.
- **Manual firewall port-opening.** Each vendor request required manually opening ports, a process that often left ports open longer than intended.
- **No MFA, no session recording.** Neither staff nor vendor access was protected by multi-factor authentication, and there was no record of vendor activity.

> *"We needed something we could deploy ourselves without bringing in an army of consultants. And it had to work with what we already had — we couldn't rip and replace our network."*
>
> *— SCADA Manager*

The Solution: One Platform for All Site Access

The authority selected Xona based on three decisive factors: zero network changes required, browser-based simplicity, and phased licensing that aligned with municipal budget cycles. Xona's CSG deploys at each site as an overlay — no reconfiguration of firewalls, switches, or SCADA systems. Users connect via any standard browser over HTTPS (port 443 only). The CSG terminates OT protocols (RDP, SSH, VNC) inside the plant network and streams only encrypted pixel images to the browser. The user's device never connects directly to any SCADA asset.

Vendor Access Transformation

Named accounts with MFA

Every vendor technician gets an individual account with mandatory multi-factor authentication.

Moderated access (wait room)

A SCADA team member must approve each vendor session before it goes live.

Credential injection

Vendor technicians never see plant passwords — the CSG injects stored credentials automatically.

Time-based controls

Access windows expire automatically. No more forgotten open firewall ports.

Session recording

Every session is video-recorded with timestamps for complete audit trail.

Instant revocation

The Kill Button ends any session immediately; Lockbox disables all site access in an emergency.

Solution Highlights: Xona Key Features
✓ **Protocol Isolation — encrypted pixel streaming; no direct endpoint-to-SCADA connectivity**
✓ **Zero Footprint Access — browser-based; no VPN client, agent, or plugin**
✓ **Xona Central Manager (XCM) — single-pane policy management across 50 sites**
✓ **Credential Injection — vendors never see or handle plant passwords**
✓ **Moderated Access / Wait Room — dual-approval for all vendor sessions**
✓ **Full Session Recording — video + keystroke logging for every session**
✓ **Kill Button & Lockbox — instant termination and site-wide access disable**
✓ **MFA Enforcement — TOTP and hardware token support at the gateway**

Phased Implementation

The three-year phased rollout distributed costs across municipal budget cycles and allowed the team to build confidence incrementally.

Phase	Sites	Users	Year	Annual Cost
Foundation	30	50	Year 1	~$112,000
Expansion	45	125	Year 2	~$150,000
Full Coverage	50	150	Year 3	~$150,000

Each site deployment averaged 30 minutes. The SCADA team performed all deployments themselves — no external consultants. CSGs were preconfigured, shipped to each facility, connected, and activated. The XCM at the data center provided centralized policy management, identity federation, and log aggregation. Vendor accounts were configured centrally and scoped to specific sites and time windows.

Results

Operational Improvements

Remote troubleshooting

The team diagnosed and resolved issues at any site within minutes instead of driving for hours — transformative for a seven-person team covering 50 sites.

Complete vendor audit trail

Every vendor session documented with video recording, timestamps, and user attribution.

Eliminated manual firewall processes

Vendor access governed through automated policy rather than phone calls and manual port changes.

Security Improvements

Zero shared credentials

Every user has a unique, named account with MFA enforced at the Xona gateway.

No SCADA exposure

Protocol isolation means no RDP, SSH, or VNC traffic leaves the plant network. Attack surface reduced to a single HTTPS endpoint.

Instant incident response

Kill Button terminates sessions immediately; Lockbox restores air-gapped posture in seconds.

Regulatory Alignment

EPA AWIA

Xona's controls directly address the access governance, MFA, and audit trail requirements that EPA AWIA risk assessments require utilities to demonstrate.

CIRCIA readiness

Session logs, access records, and forensic video recordings support incident reporting within the mandated 72-hour window.

Looking Ahead

With full deployment achieved, the authority is exploring SIEM integration for real-time monitoring, OT visibility platform integration for dynamic risk-aware access policies, Para-Pack cellular backup for critical treatment facilities, and extending secure access to additional field instrumentation as the SCADA infrastructure grows.

For municipal water utilities navigating EPA AWIA recertification and the forthcoming CIRCIA requirements, this deployment demonstrates that comprehensive access governance does not require operational sacrifice or large consultant engagements. Security, reliability, and compliance coexist — when the access architecture is purpose-built for operational technology.

> *"We went from having almost no remote access and no visibility into vendor sessions, to having complete control over every connection to every site — and we did it with the team we already had. No consultants, no network redesign, no disruption to operations. For a municipal utility, that's exactly what we needed."*
>
> *— SCADA Manager, Regional Municipal Water Authority*

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***