



Acuity Hub

Industrial Operations Management Platform

Cloud HMI. SCADA. IIOT Software

Security Statement



Intelligent Operations

2025

Zero-Trust Architecture



In today's digital utility landscape, security cannot rely on outdated assumptions of trust. Traditional SCADA systems—many built decades ago—leave critical infrastructure exposed to modern cyber threats. Acuity Hub is built on a true zero-trust foundation, enforcing strict identity verification, role-based access, and continuous authentication across every connection. This cloud-native approach safeguards data integrity and system availability while minimizing the attack surface, ensuring resilient operations in an era of escalating cyber risk.

Acuity Hub: Secure by Design

Acuity Hub leverages the latest in cybersecurity best practices to provide a fundamentally more secure alternative to legacy SCADA platforms:

- **Edge-Initiated Communications:** Leveraging XiO's unique communication strategy, all data flows are initiated from the edge device to the cloud—never the other way around. This eliminates the need for inbound connections or open firewall ports, drastically reducing the attack surface and providing a fundamentally more secure architecture.
- **Encrypted Transmission:** Communication between edge devices and the cloud is secured using private key infrastructure (PKI). Each device is assigned a unique private key, ensuring encrypted, authenticated data exchange.
- **Configurable Access Control:** Devices can be configured to reject all local access, including to their internal web servers, providing additional layers of protection against physical or network-based tampering.
- **Secure User Interface Access:** All UI interactions are routed exclusively through the cloud, leveraging HTTPS encryption, strong passwords, and multi-factor authentication (MFA)—the same standards used in banking.
- **Always Assume Breach:** Acuity Hub assumes that any system—internal or external—may be compromised and enforces strict security controls accordingly:
 - Limit Blast Radius with data sanitation thresholds in control functions
 - Role-Based Access Control (RBAC) for precise permissioning
 - Deep Network segmentation to shield critical assets
 - End-to-end encryption
 - Audit logging & real-time monitoring

Secure Access Without VPN Risks

Unlike traditional VPNs that create vulnerabilities in flat networks, Acuity Hub uses authenticated, cloud-routed connections to provide role-based access without exposing internal systems. This eliminates the need for tools like TeamViewer, RDP, or port forwarding while delivering fine-grained control and audit visibility for every user and device.

Multi-Layered Authentication

Security begins with controlling access, and XiO employs a three-tiered authentication model designed for today's threat landscape. This layered framework ensures that only the right people, in the right places, with the right credentials can interact with critical systems. By combining multiple factors, XiO reduces the risk of compromised accounts, enforces Zero Trust principles, and gives utilities confidence that access to their operational technology remains tightly controlled.

This three-pillar model includes:



1. **What You Know:** Strong password and credential policies enforced at login.
2. **Where You Are:** All access is routed through XiO's authorized VPN server. Users must originate from trusted networks.
3. **Who You Are:** MFA with biometric validation (fingerprint or facial recognition) ensures access is tied to individual identity, not just credentials.

This approach minimizes lateral movement opportunities and prevents common attack vectors that target single-point authentication methods.

Continuous Security & Resiliency

Acuity Hub is built to defend against both known and emerging cyber threats through proactive, always-on security measures:

- **Real-Time Updates & Patch Management** – Cloud-native architecture allows seamless deployment of critical updates and vulnerability patches, addressing risks that often linger in unpatched, on-premise SCADA systems.
- **Disaster Recovery & Redundancy** – Geo-redundant server infrastructure and secure cloud backups enable rapid failover and data recovery, ensuring operational continuity during outages or incidents.
- **Centralized Monitoring & Anomaly Detection** – Built-in monitoring provides immediate visibility into abnormal behaviors, enabling rapid incident response and minimizing downtime.

Security Standards

**NIST**

Federal Information
Processing Standard
(FIPS) 199 Standard

**AWWA**

Water Sector Cybersecurity
Risk Management Guidance

**FedRamp**

Federal Risk and Authorization
Management Program Standard
for Cloud Service Providers

Resiliency & Redundancy

XiO's platform is engineered to keep critical operations running under all conditions. Services are distributed across multiple geographic regions, with each node monitoring the others to detect failures and trigger automatic recovery—ensuring that even “alarm silence” is flagged as a fault rather than overlooked. Our teams regularly rehearse disaster recovery, reducing redeployment times from thirty minutes to under five, and real-world events have shown less than two minutes of user impact. Over the past fourteen years across hundreds of systems, total downtime has amounted to less than ninety minutes. Beyond the cloud, operators are trained to maintain safe manual control during disruptions, and every backup is verified through restoration testing, reflecting our philosophy that if you haven't restored it, you don't truly have it.

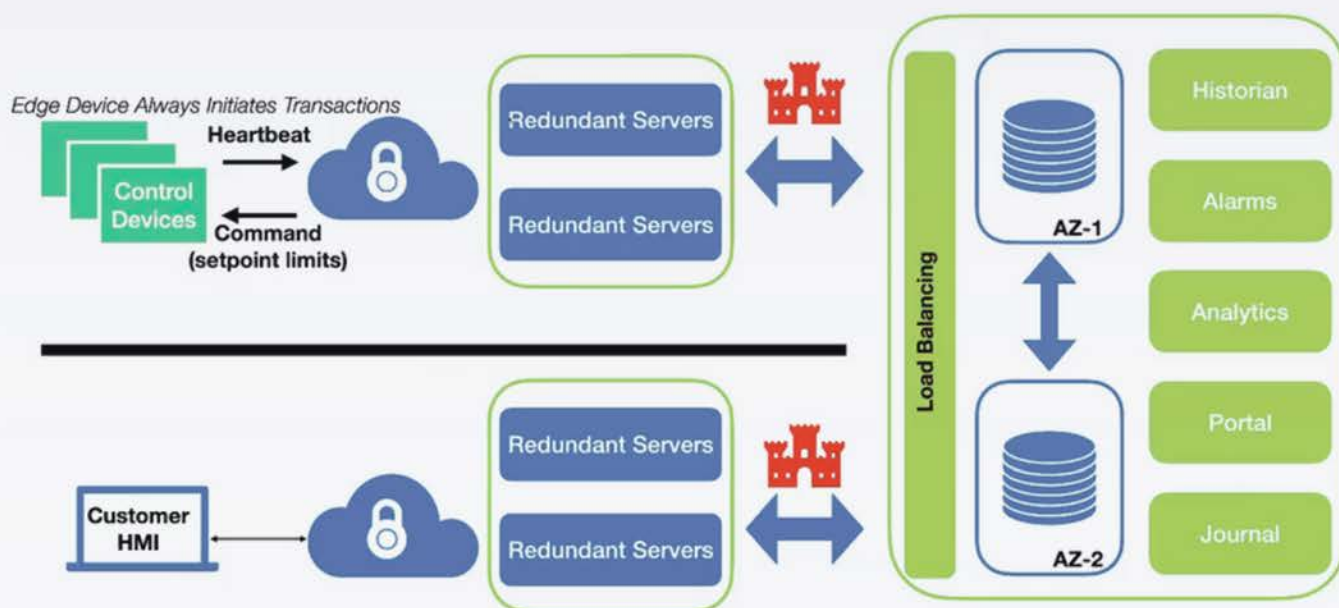


Figure 1. XiO's cloud architecture uses redundant servers, multi-region load balancing, and verified backups to ensure resilient, secure operations with continuous monitoring and manual fallback protection.

What makes XiO's Platform different?

XiO was founded with a vision to bridge operational technology and information technology in a way that modernizes industrial operations without sacrificing safety or control. From the beginning, the platform has been built around autonomous local control with cloud augmentation—ensuring plants can operate independently while leveraging the cloud for visibility, analytics, and optimization.

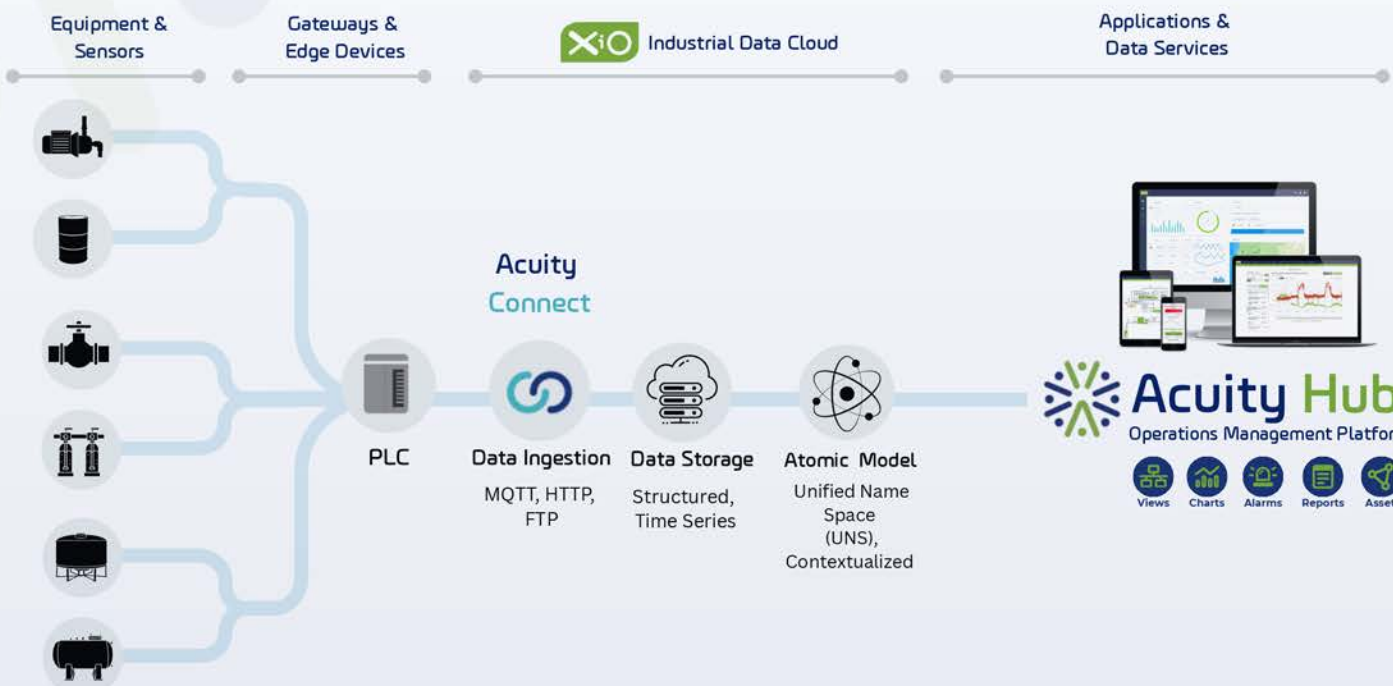
This vision is inseparable from our security philosophy, which embraces Zero Trust Architecture, role-based access, and edge-initiated communications to minimize vulnerabilities. By combining future-focused innovation with uncompromising security, XiO delivers a platform that empowers utilities to modernize with confidence, knowing that resiliency, reliability, and protection are embedded in every layer.

Scalable Solution

Acuity Hub is engineered for seamless scalability — whether you're starting with a single lift station or managing a global portfolio of industrial sites. The platform's architecture is cloud-native and multi-tenant by design, allowing organizations to onboard new locations rapidly without the complexity of managing on-premise infrastructure. It integrates effortlessly with virtually any existing control hardware — from Modbus-based PLCs to advanced systems like Allen-Bradley, Siemens, and Schneider — making it ideal for retrofit scenarios as well as greenfield builds.



With centralized user access, standardized templates, and secure edge-to-cloud communication, Acuity Hub empowers utilities, operators, and service providers to scale operations efficiently, maintain consistency, and unify data across hundreds or even thousands of sites — all within a single pane of glass.



Edge-To-Cloud Security Advantage

XiO's Edge-to-Cloud model is not only safer, it's smarter:

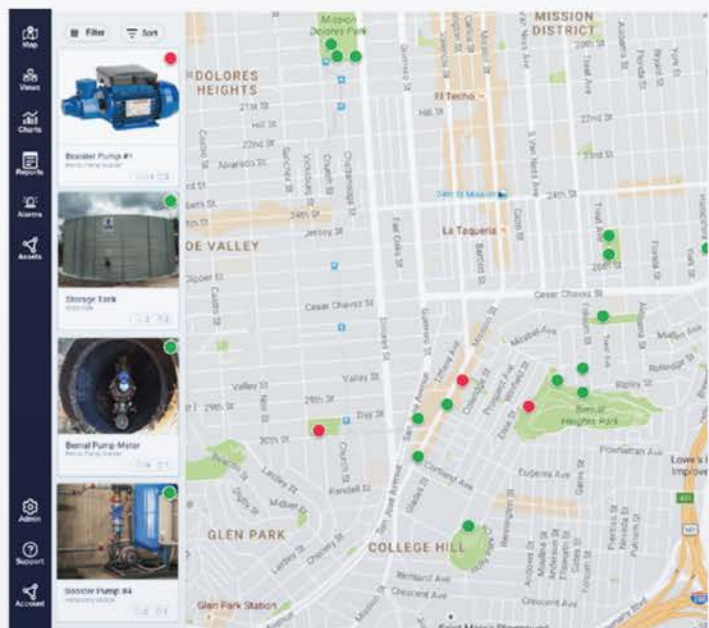
- Access PLC and legacy SCADA data securely—without exposing systems.
- Protect from phishing, keylogging, ransomware, and unauthorized local access.
- Keep your operations running efficiently while future-proofing your security infrastructure.

Intelligent Operations

By adopting Acuity Hub and the larger XiO platform, utilities and industrial operations unlock the path to Intelligent Operations. Rather than struggling with siloed systems or heavy on-premise infrastructure, teams gain a secure, cloud-native environment that unifies operational and organizational data. This unlocks real-time visibility across distributed assets, smarter alarming, advanced analytics, and centralized knowledge management that blends hard data with operator expertise. With Acuity Connect seamlessly linking edge devices and legacy systems to the cloud, XiO empowers staff to do more with less—driving efficiency, lowering costs, and building resilient, future-ready operations that are both secure and intelligent.

Holistic Management Platform

-  **Views** Intuitive dashboards and HMIs that give operators real-time visibility into system performance.
-  **Charts** Interactive trend analysis for identifying issues, optimizing operations, and validating performance.
-  **Alarms** SMS, Email, & Phone alarms with contextual alerts to help staff respond quickly and effectively.
-  **Reports** Automated, customizable reporting that delivers accurate, consistent insights on demand.
-  **Assets** Automated, customizable reporting that delivers accurate, consistent insights on demand.
-  **Control** Secure, cloud-augmented control functions that extend operator capabilities while maintaining local autonomy.



Together, these applications form a cloud-native toolkit for Intelligent Operations, empowering utilities to do more with less while staying secure, resilient, and future-ready.

KEY BENEFITS

For water, wastewater, and solid waste system managers



Real-time monitoring

Track KPIs, detect anomalies, and proactively respond.



Predictive analytics

Reduce downtime with analytical insights from operational data.



Remote access & control

Manage systems securely from anywhere.



Automated compliance reporting

Simplify regulatory requirements



Unify data silos

Centralize distributed data sources into a unified view.



Multi-tenant structure

Manage multiple systems in one platform.



Device Management

Manage and monitor device connectivity status and KPIs.



Robust cybersecurity

Implement zero-trust security measures.



Capture institutional knowledge

Capture and leverage institutional knowledge.



Modernize for a post-POTS world

Adopt future-forward signal transmission strategies that don't rely on phone lines.



Acuity Hub

Industrial Operations Management Platform

Zero-Trust. Total Confidence.

2025

Security Statement

Contact

 285 Bel Marin Keys Blvd Suite E, Novato, CA 94949

 (415) 462-1300

 info@acuityhub.io

 <https://xiowater.com>

 [@acuityhub.io](https://www.instagram.com/acuityhub.io)