ebook

Identity-Based Access Risks in Critical Infrastructure

As IT and OT environments converge, access risk stops being an IT administration problem and becomes an operational one. In critical infrastructure, a weak credential, a shared vendor login, or an unmanaged remote connection can do more than expose data. It can disrupt production, trigger environmental incidents, and put safety at risk.

This ebook examines why identity has become one of the most consequential control points in OT, where conventional IAM approaches break down, and what critical infrastructure operators can do to regain control.

It outlines five of the most pressing IAM challenges facing operators of critical infrastructure and offers a practical roadmap for reducing identity-based risk without disrupting operations.

Why OT Still Lacks Unified Access Control

Critical infrastructure does not typically suffer from a shortage of access controls. It lacks unified ways to enforce them.

OT environments were built for isolation, not identity. Security depended on physical separation. That model breaks down once systems are connected to enterprise networks, cloud platforms, and third-party vendors.

The IT/OT Convergence Problem

Modern OT environments now routinely exchange data with enterprise resource planning (ERP) systems, historian databases, cloud-based analytics platforms, and third-party vendor portals. Each integration introduces new identity touchpoints and potential vulnerabilities.

The challenge is deepened by the realities of OT environments. A typical utility or manufacturing facility may operate PLCs, RTUs, HMIs, DCS platforms, and SCADA systems from a dozen different vendors, each with distinct authentication mechanisms, credential stores, and access models, none of which integrate natively with enterprise identity providers.

48%

of OT orgs still lack OT-specific security monitoring

$5.56M

average industrial sector breach point

The Visibility Gap

Without a unified access control view, security teams cannot answer basic questions: Who has access to what system? When was that access last reviewed? Is this account still needed?

That is where OT access risk becomes hard to govern. Teams cannot consistently see who has access, whether it is appropriate, or whether it should have been removed weeks ago.

- Shared accounts and device credentials obscure individual accountability
- Privileged sessions in OT environments are seldom recorded or monitored in real time
- OT assets often lack native logging or export access events to siloed local databases
- Vendor and contractor accounts are frequently provisioned outside standard HR workflows
- Access reviews are manual, infrequent, and rarely cover OT-specific systems

Result: When teams cannot see who accessed which asset, under what identity, and for what purpose, misuse is usually discovered too late.

Five Major IAM Challenges in Critical Infrastructure

The access problems in OT are not edge cases. They are structural. Most critical infrastructure operators are trying to govern identities across environments that were never designed for centralized control, never standardized around modern authentication, and often cannot tolerate disruption.

1. **Protocol Incompatibility & Legacy Authentication**
   OT systems frequently rely on proprietary protocols (Modbus, DNP3, Profibus) or decades-old authentication schemes with no support for modern identity standards such as SAML, OAuth 2.0, or LDAP. Retrofitting these systems with identity controls without disrupting operations is a significant technical challenge that most IAM platforms are ill-equipped to handle.
2. **Widespread Use of Shared & Generic Credentials**
   Shared accounts (e.g., 'admin', 'operator', 'plant-user') remain standard practice across many OT environments. These accounts are passed between shifts, contractors, and integrators, making it impossible to attribute actions to specific individuals, a foundational requirement for both security investigations and regulatory compliance.
3. **Unmanaged Third-Party & Vendor Access**
   Critical infrastructure operators rely heavily on OEM vendors and system integrators for remote maintenance and support. These third parties often connect via unmonitored pathways such as direct dial-up connections, unmanaged VPNs, or even cellular modems with credentials that are never rotated, reviewed, or revoked after the engagement ends.
4. **Operational Uptime Constraints Limit Access Reviews**
   Many OT processes run continuously with zero tolerance for downtime. A nuclear plant, water treatment facility, or transmission substation cannot pause operations for a patch or a credential rotation. This creates a powerful disincentive to apply identity controls that might introduce any risk of disruption, even where the security benefit is clear.
5. **Regulatory Fragmentation Across Frameworks**
   Organizations must simultaneously satisfy requirements from NERC CIP (energy sector), AWIA (water), TSA security directives (pipelines), IEC 62443 (industrial automation), and NIST SP 800-82 (general ICS guidance). Each framework has different access control requirements, creating compliance complexity that strains security teams.

How do OT Leaders Solve IAM Challenges

Addressing OT identity risk requires a purpose-built, phased approach, one that respects operational constraints while systematically closing access control gaps.

Principle 1 - Establish a Unified Identity Foundation

If identity remains fragmented across IT and OT, every other control is working uphill. Operators need one authoritative way to establish who a user is, what they should be allowed to reach, and when that access should expire. This does not mean forcing OT systems to support enterprise identity protocols immediately; it means creating a translation layer (often called an OT-aware Identity Broker) that can federate identity signals from diverse OT assets into a central platform.

1. Deploy an OT-compatible privileged access management (PAM) solution that understands ICS protocols
2. Integrate OT asset directories with enterprise identity providers via secure federation
3. Establish a centralized visibility into access across all OT zones and levels
4. Synchronize identity lifecycle events (onboarding, role changes, terminations) to OT systems

Principle 2 - Eliminate Shared Credentials Through Just-in-Time Access

Just-in-Time (JIT) provisioning eliminates standing privileges by granting access only when needed, for the minimum duration required, with full session recording. This approach is particularly valuable in OT environments because it removes persistent shared accounts while preserving operational flexibility.

Traditional Approach	JIT / Zero-Standing-Privilege
Shared 'operator' account used by all shifts	Individual identity, time-bound session token
Credentials known to dozens of personnel	Credential checked out, auto-rotated after use
No session recording or audit trail	Full session video
Access persists indefinitely after need ends	Access automatically terminates

Principle 3 - Govern Vendor & Third-Party Access Rigorously

Third-party access is consistently the highest-risk vector in OT environments. A dedicated Vendor Privileged Access Management (VPAM) program should enforce: identity verification before any remote session; scoped access limited to specific assets and time windows; real-time session monitoring with automatic termination on policy violation; and mandatory access reviews tied to contract status.

Principle 4 - Automate Access Lifecycle Management

Manual provisioning and de-provisioning processes are the root cause of the slow accumulation of unneeded permissions over time. Automating these lifecycle events, triggered by HR system changes, project completions, or access certifications, is essential for maintaining least-privilege access across large, complex OT environments.

Legacy Access Solution Limitations

Most traditional PAM and IAM platforms were built for enterprise IT. That matters more than vendors admit. OT environments have different protocols, different uptime requirements, different network boundaries, and far less tolerance for control-plane failure.

No Native OT Protocol Support

Enterprise PAM solutions typically support RDP, SSH, and HTTPS for session management. They lack connectors for Modbus, DNP3, PROFINET, or proprietary HMI interfaces, leaving the most sensitive OT touchpoints entirely unprotected by privileged access controls.

High-Availability Architecture Mismatch

Legacy PAM solutions often introduce single points of failure incompatible with the uptime requirements of OT environments. An outage of the PAM vault can lock operators out of critical systems during emergencies.

IT-Centric Identity Models

Traditional IAM systems model identity around human users and enterprise applications. They struggle to represent machine identities, device accounts, process accounts, and the hierarchical zone-based access models required by Purdue/ISA-95 OT architectures.

Inadequate Session Monitoring for OT Protocols

Video-based session recording of proprietary OT HMIs captures what happened but cannot parse or alert on the specific commands executed. Without protocol-aware monitoring, detecting a malicious setpoint change in recorded footage requires manual, expert-level review.

Rigid Change Management Incompatibility

Enterprise IAM tools assume frequent credential rotation and access reviews aligned with IT change windows. OT environments have extended maintenance cycles — sometimes years — making the rigid rotation schedules enforced by legacy PAM tools either operationally disruptive or frequently bypassed.

Limited Air-Gap & DMZ Deployment Support

Many enterprise IAM solutions require cloud connectivity or complex network paths inconsistent with OT security architectures that mandate strict DMZ controls and prohibition of direct internet connectivity for OT-zone systems.

Implications of Inadequate Access Control

The consequences of weak identity and access controls in critical infrastructure extend far beyond data breaches, they encompass physical safety, regulatory liability, and societal harm.

Operational Disruption & Physical Safety Risk	In critical infrastructure, unauthorized access is not just a security event. It can become an operational event within minutes. Unauthorized access to OT systems can trigger unplanned shutdowns, equipment damage, or process instability with real-world physical consequences.
Regulatory Non-Compliance & Financial Penalties	NERC CIP violations carry penalties of up to $1 million per violation per day. TSA security directive non-compliance can result in operational restrictions. AWIA 2018 requires risk and resilience assessments that explicitly address access control. Organizations without demonstrable identity controls face escalating enforcement risk.

Reputational & Public Trust Damage	A cyber incident affecting public utilities — water, power, transportation — generates intense public and media scrutiny. Even incidents that are contained without physical harm erode public confidence in critical infrastructure operators and intensify political pressure for regulatory intervention.
Cascading Supply Chain & Downstream Effects	Critical infrastructure sectors are deeply interdependent. A power grid disruption cascades to water pumping stations, telecommunications infrastructure, healthcare facilities, and fuel distribution networks. Inadequate access controls in one organization can become the entry point for attacks with sector-wide consequences.
Intellectual Property & Operational Data Theft	Sophisticated adversaries — including nation-state actors — use OT access not only for sabotage but for intelligence collection. Process recipes, operational parameters, maintenance schedules, and asset configurations represent high-value intelligence targets with significant commercial and national security implications.

Steps to Improve Secure Access for Critical Infrastructure

Improvement does not start with a rip-and-replace project. It starts with visibility, tighter control over privileged access, and disciplined reduction of standing trust.

Step 1	Conduct an OT Identity & Access Inventory
	› Enumerate all accounts (human, service, device, vendor) across OT zones
	› Identify shared, generic, and orphaned accounts — prioritize elimination
	› Map access paths to critical assets (PLCs, SCADA servers, HMIs, historians)
	› Document third-party access arrangements, including remote connection methods
	› Establish a baseline for least-privilege gap analysis

Step 2	Deploy OT-Aware Privileged Access Management
	› Select a PAM solution with native support for OT protocols and architectures
	› Implement credential vaulting for all privileged OT accounts
	› Enable just-in-time access provisioning for maintenance and vendor sessions

	› Configure session recording for all privileged OT access events
	› Ensure high-availability deployment compatible with OT uptime requirements

Step 3	Enforce Multi-Factor Authentication Across OT Access Points
	› Mandate MFA for all remote access to OT environments — no exceptions
	› Deploy MFA for privileged local access at operator workstations and HMIs
	› Select MFA methods compatible with OT environment constraints (hardware tokens, smartcards)
	› Integrate MFA with the central identity provider for unified policy enforcement
	› Establish emergency break-glass procedures with proper vaulting

Step 4	Implement Vendor & Third-Party Access Governance
	› Require identity verification and background checks for all OT vendors
	› Deploy a dedicated vendor access portal with time-limited, scoped session tokens
	› Implement real-time monitoring and auto-termination for vendor sessions
	› Tie vendor access to active contract status with automated de-provisioning
	› Conduct quarterly reviews of all third-party access agreements and credentials

Step 5	Establish Continuous Access Monitoring & Anomaly Detection
	› Integrate OT access logs with a security information and event management (SIEM) platform
	› Define behavioral baselines for each user/role/asset combination
	› Implement automated alerting for access outside approved windows or locations
	› Deploy User and Entity Behavior Analytics (UEBA) for privileged account monitoring
	› Establish OT-specific threat detection rules (after-hours access, lateral movement)

Step 6	Automate Access Lifecycle & Certification
	› Integrate OT access provisioning with HR systems for joiner/mover/leaver automation
	› Implement automated access certifications on a quarterly basis for all OT roles

	› Enforce time-bound access for project-specific and contractor roles
	› Establish a formal access request and approval workflow for OT privilege escalation
	› Generate automated compliance reports mapped to NERC CIP, IEC 62443, and NIST 800-82

How Xona Reduces Identity-Based Access Risks

The IAM challenges outlined in this ebook, protocol incompatibility, shared credentials, unmanaged vendor access, and compliance fragmentation, share a common thread: they are all symptoms of access architectures that were never designed for OT environments. Xona is purpose-built to address exactly this gap.

Xona Eliminates Direct OT Network Exposure Through Session Brokering

Traditional remote access tools extend network reach and then try to govern the risk. Xona works the other way around. It brokers the session at the boundary so the user never gains direct network-level access in the first place. Remote users connect to Xona and Xona connects to the asset. Those two connections are never bridged into a single tunnel. This means a compromised vendor credential cannot become a pivot point into the broader OT network, because the user never has direct network reachability in the first place.

Xona Prevents Lateral Movement by Scoping Access to a Single Asset

Lateral movement is one of the most dangerous consequences of over-provisioned access. Xona enforces access at the asset level, not the network level. A vendor granted access to a specific HMI can reach that HMI and nothing else. No subnet-wide exposure. No residual network paths once the session closes.

Xona Removes Shared Credentials by Tying Every Session to a Verified Identity

Shared accounts and standing credentials are eliminated by design. Xona enforces MFA, SAML, LDAP, and Active Directory authentication on every session. There are no generic operator accounts, no credentials passed between shifts, and no standing access that persists beyond the defined session window. When the work is done, the access closes automatically.

Xona Closes the Visibility Gap With Protocol-Aware Session Recording

Most access control tools can record that a session occurred. Xona can record what happened inside it, including at the protocol level. The gateway terminates OT protocols at the boundary, which means it can distinguish a Modbus read from a Modbus write, a legitimate configuration pull from a setpoint change. This is the difference between a compliance audit trail and actionable security intelligence.

Xona Reduces Compliance Burden by Mapping Natively to Regulatory Frameworks

Rather than generating logs that security teams must manually map to regulatory requirements, Xona's architecture natively aligns to NERC CIP, IEC 62443, TSA SD-02F, NIS 2, and NIST 800-53. Compliance evidence is generated at the access point, automatically, on every session, reducing the manual overhead that strains OT security teams across fragmented regulatory environments.

Xona Deploys Without Disrupting OT Operations

Consistent with the operational uptime requirements discussed throughout this ebook, Xona requires no agents, no firewall changes, and no network reconfiguration. The gateway is browser-based and deploys in approximately 20 minutes, making it one of the few enterprise-grade access control solutions that can be introduced into a live OT environment without scheduling a maintenance window.

The result is an access control posture where every session is brokered, scoped, authenticated, time-bound, recorded, and compliance-mapped from the moment it begins, closing the identity-based access gaps that make critical infrastructure a target, without compromising the operational continuity that keeps it running.

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

- Christopher, J. D. (2024). SANS 2024 state of ICS/OT cybersecurity. SANS Institute. **https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity**
- IBM. (2024). Cost of a data breach 2024: The industrial sector. IBM. **https://www.ibm.com/think/insights/cost-of-a-data-breach-industrial-sector**
- North American Electric Reliability Corporation. (n.d.). Sanction guidelines. NERC. **https://www.nerc.com/pa/comp/CE/Pages/Sanctions.aspx**
- SANS Institute. (2025). SANS 2025 state of ICS/OT cybersecurity. SANS Institute. **https://www.sans.org/white-papers/sans-2025-state-ics-ot-cybersecurity**
- Transportation Security Administration. (2025). Security directive pipeline-2021-02F: Cybersecurity mitigation actions, contingency planning, and testing. U.S. Department of Homeland Security. **https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf**
- U.S. Environmental Protection Agency. (2018). America's Water Infrastructure Act section 2013/SDWA section 1433: Risk and resilience assessments and emergency response plans. EPA. **https://www.epa.gov/waterresilience/awia-section-2013**
- Verizon. (2025). Data breach investigations report 2025. Verizon Business. **https://www.verizon.com/business/resources/reports/dbir/**