EBOOK

Why 2026 Becomes the Breaking Point for VPN-Based OT Remote Access

INTRODUCTION

Remote access in operational technology (OT) environments has evolved from an occasional troubleshooting tool to a daily operational necessity. As industrial organizations operate with fewer on-site specialists, greater reliance on external service providers, and increasingly distributed assets, the limitations of legacy VPN-based access are no longer theoretical. They are becoming operational constraints.

By 2026, these pressures converge. What once functioned as a tolerable workaround becomes a systemic risk, separating organizations that deliberately modernized OT access from those forced to react under regulatory, operational, or incident-driven pressure.

THE SHIFTING LANDSCAPE

What's Driving Change in OT Remote Access

Industrial organizations face converging pressures that are fundamentally reshaping remote access requirements and compressing timelines for change.

01 **Workforce Distribution**

Fewer on-site specialists and greater reliance on external service providers

02 **IT/OT Convergence**

Centralized identity, security, and audit expectations extending into environments built for isolation

03 **Expanded Attack Surface**

More geographically distributed assets requiring frequent, authorized remote interaction

04 **Legacy Infrastructure**

Environments never designed for frequent remote access now dependent on it for uptime and support

FIVE PREDICTIONS FOR OT REMOTE ACCESS IN 2026

1

Cyberattacks Will Target Access Paths Over Network Perimeters

Current Challenge

Nation-state actors and ransomware groups are shifting from brute-force network intrusions to exploiting legitimate access paths. Remote access channels, particularly those used by third parties and OEMs, represent prime targets. A single exposed engineering workstation or HMI session can disrupt operations without requiring full network compromise.

Prediction

Traditional VPN approaches that grant broad network access will be recognized as incompatible with modern ICS threat models. Organizations will prioritize access models that minimize lateral movement, enforce session-level controls, and provide continuous visibility into user activity.

2

IT/OT Convergence Will Force Unified Access Governance

Current Challenge

Siloed IT and OT teams create fragmented security and governance. ICS environments require access mechanisms that respect operational constraints: legacy protocols, unpatchable systems, deterministic uptime requirements, and segmented architectures like the Purdue Model.

Prediction

Identity, policy, and monitoring will centralize while enforcement remains tailored to OT constraints. Secure Remote Access (SRA) gateways will bridge IT identity systems and OT assets, isolating and auditing interactions to maintain operational safety while enabling unified governance

FIVE PREDICTIONS FOR OT REMOTE ACCESS IN 2026

3

SRA Will Replace Network Access As The Default For Third Parties

Current Challenge

Third-party access has shifted from an exception to an operational dependency. OEMs, system integrators, and service providers increasingly require frequent, remote interaction to support uptime, safety, and change management. VPN-based models, built for occasional access, struggle to govern this scale without expanding trust boundaries, accumulating unmanaged credentials, and obscuring accountability.

Prediction

By 2026, SRA will become the default model for third-party access with:

- Time-bound, task-specific permissions
- Restrictions to specific assets or protocols
- Complete recording and auditability
- Automatic revocation when no longer needed

This shift reflects Zero Trust principles adapted for OT, emphasizing session mediation and protocol isolation as a way to support continuous third-party access without continuous network exposure.

4

Compliance Will Shift From Checkbox To Architecture

Current Challenge

Compliance in OT is often treated as a checklist rather than embedded in system design. Regulatory frameworks like IEC 62443, NERC CIP, and NIS2 continue expanding in scope and enforcement.

Prediction

Compliance will become a byproduct of system architecture. Organizations will favor technologies that produce audit-ready evidence by design: session recordings, immutable logs, enforced least privilege, and demonstrable separation of duties. SRA platforms will function as compliance accelerators rather than relying on after-the-fact reporting.

FIVE PREDICTIONS FOR OT REMOTE ACCESS IN 2026

5

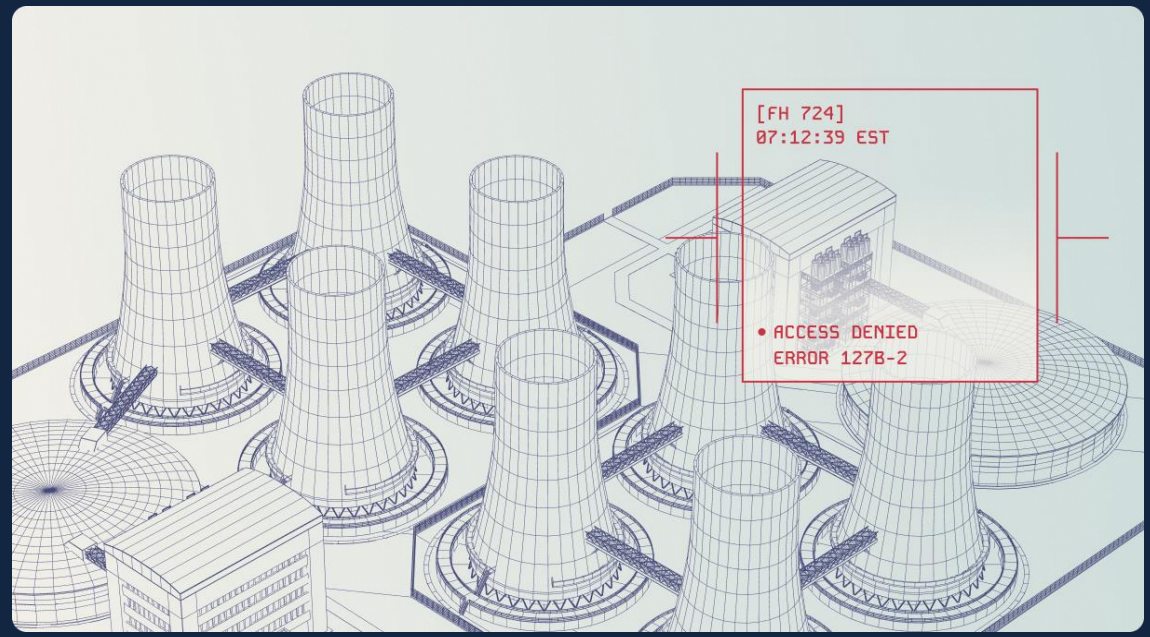
SRA Platforms Will Become Security Integration Hubs

Current Challenge

Traditional ICS security monitoring focuses on networks and endpoints, overlooking access activity, which is one of the strongest indicators of compromise. Without visibility into who connects, when, and how, organizations struggle to detect and respond to threats effectively.

Prediction

SRA platforms will evolve into security integration hubs, enabling real-time observation, analysis, and response to anomalous access behavior. This embeds threat detection and incident response directly into access workflows without disrupting operations.



WHY VPNS FAIL IN OT ENVIRONMENTS

1. VPNs Overextend Trust Boundaries

VPNs provide secure network connectivity but are poorly suited to environments where access must be frequent, shared across organizations, and tightly governed. Once authenticated, users typically gain broad access to network segments rather than being limited to specific assets, protocols, or tasks.

The OT Impact:

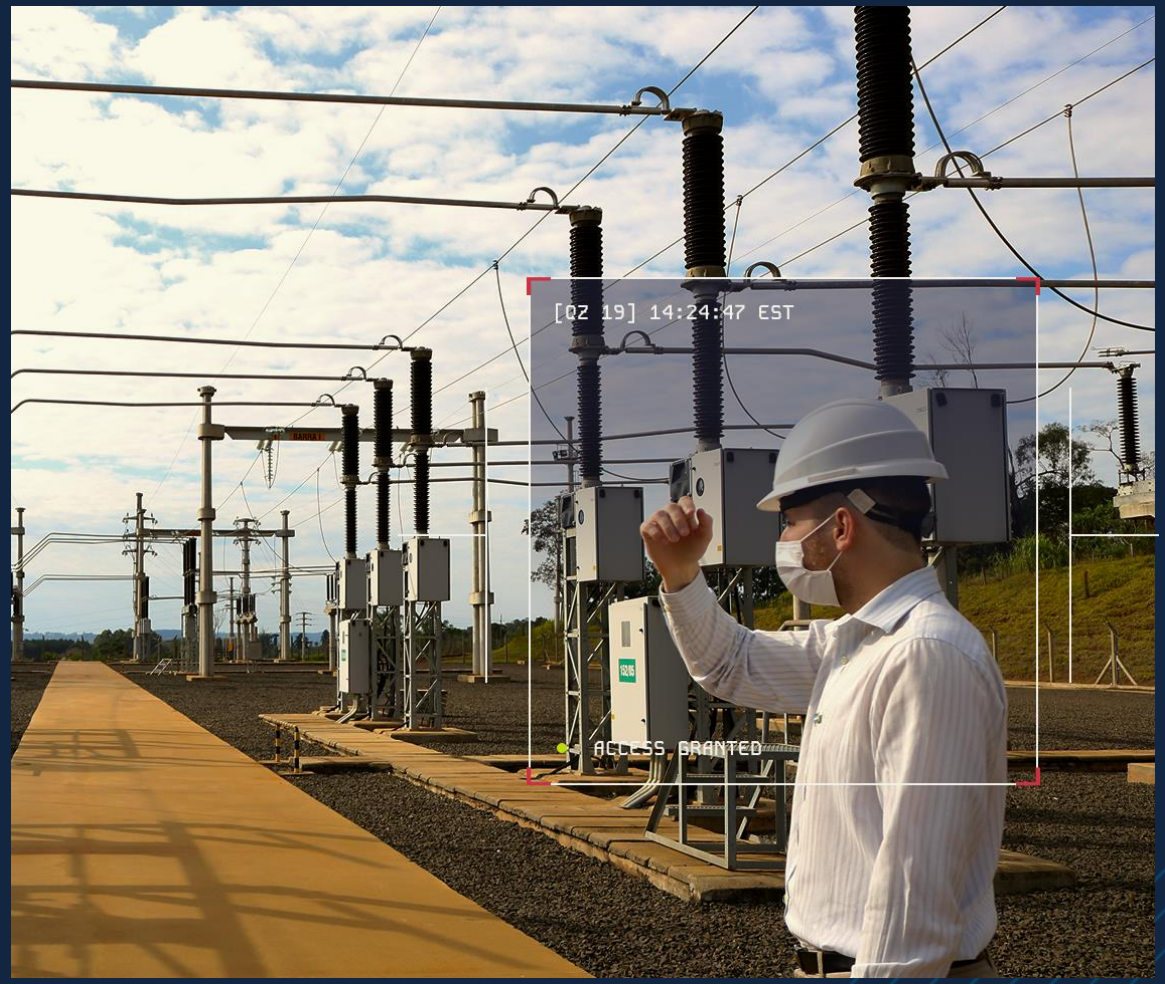
- Access expands over time to keep operations moving
- Exceptions and workarounds become permanent
- Least-privilege erodes as access patterns scale
- A single VPN connection can expose multiple critical systems during routine third-party work

WHY VPNS FAIL IN OT ENVIRONMENTS

2. VPNs Lack OT-Specific Access Controls

VPN-based models don't support access controls required to govern modern OT operations at scale, especially when third parties are involved:

- Time-bound access that automatically expires
- Approval workflows aligned to maintenance or change windows
- Session monitoring and recording to establish accountability across organizations
- Protocol-aware least privilege (e.g., allowing RDP but blocking engineering tools)



WHY VPNS FAIL IN OT ENVIRONMENTS

3. VPNs Create Operational Overhead

Maintaining and scaling VPN-based access across OT environments demands constant effort from both IT and OT teams:

- Manual configuration of firewalls, user accounts, and routing rules
- Difficulty standardizing access across multiple plants, regions, or vendors
- Troubleshooting pulls OT teams away from core operations
- Increased dependency on IT teams unfamiliar with OT constraints
- No built-in audit visibility or approval workflows, making it difficult to track access activity, enforce least privilege, or prove compliance

THE COMPLIANCE CHALLENGE

VPN-Based OT Access Is Becoming a Regulatory Liability

Regulators and auditors increasingly expect organizations to demonstrate effective control over remote access, not simply document that access occurred. This includes:

- Least privilege access
- Strong identity verification
- Granular audit trails
- Segmentation and isolation
- Continuous monitoring

VPNs struggle to meet these expectations because they were built to establish network connectivity, not to enforce, monitor, and prove appropriate use of access.

The Audit Gap

VPN logs show when a connection was established and terminated, but not what occurred during that session. Once connected, organizations are often unable to clearly demonstrate:

- What systems were accessed
- What actions were taken
- Whether those actions aligned with role, approval, or change scope
- Whether access was limited to a defined time window
- Whether activity was observable or supervised

For auditors, "they had a VPN connection" isn't sufficient evidence of control. This creates an audit gap where security teams may understand intent but cannot prove enforcement, leaving organizations exposed during audits, investigations, or post-incident reviews.

ZTNA grants access only to what users explicitly need, without placing users onto the OT network itself.

A 2026-Ready OT Remote Access Model

A modern approach built on Zero Trust Network Access (ZTNA) addresses these requirements without requiring wholesale network redesign or disruption to OT operations. This model focuses on mediating access instead of extending networks and does so through five co re capabilities:

1

Fine-Grained, Least-Privilege Access

ZTNA grants access only to what users explicitly need, without placing users onto the OT network itself.

What it enables:

- Vendors restricted to specific HMIs or workstations
- Technicians limited to defined PLCs or asset groups
- Access scoped by role, site, time window, and approval

Why it matters:

If credentials are compromised, attackers cannot pivot across the OT network because access is mediated and scoped. VPNs do the opposite: once connected, users inherit broad network reach that was never intended for continuous external use.

2

Strong Identity and Continuous Authentication

ZTNA builds on modern identity controls and ongoing validation while integrating with existing enterprise identity systems rather than introducing standalone access silos.

What it enables:

- Phishing-resistant MFA
- SSO integration with corporate identity systems
- Continuous verification during sessions
- Credential vaulting to remove the need for shared/local device credentials

Why it matters:

Passwords alone cannot grant access, reducing the risk of shared or long-lived credentials and giving OT teams clear control over when and how third parties connect.

A 2026-Ready OT Remote Access Model

3

Reduced Exposure Through Outbound Connectivity

VPNs require internet-facing gateways that can be discovered, scanned, and attacked. OT-aligned ZTNA architectures invert this model by establishing outbound connectivity from inside OT environments, avoiding the need to expose inbound access points.

What it enables:

- No inbound OT ports exposed to the internet
- Fewer perimeter devices to patch and defend
- Brokered sessions instead of open tunnels

Why it matters:

OT systems remain hidden from the public internet, and access becomes event-driven and policy-controlled rather than continuously available. This aligns remote access with operational intent instead of network availability.

4

Monitoring, Logging, and Session Accountability

VPN tunnels provide encryption but offer limited visibility into session actions. ZTNA emphasizes oversight and auditability.

What it enables:

- Detailed session logs tied to user identity
- Activity tracking for third-party work
- Optional live monitoring
- Session recordings for compliance and forensics

Why it matters:

Security teams can answer who accessed what, when, why, and what they did. This builds accountability without slowing operations and strengthens incident response.

- No inbound OT ports exposed to the internet
- Fewer perimeter devices to patch and defend
- Brokered sessions instead of persistent tunnels

A 2026-Ready OT Remote Access Model

5

Scalability, Reliability, and Operational Focus

Legacy VPN infrastructure becomes a bottleneck as remote work, vendor access, and distributed operations increase. ZTNA architectures are distributed and designed to scale.

What it enables:

- Fewer single points of failure
- Improved user experience across geographies
- Better performance under higher remote load
- Reduced bandwidth and gateway choke points

Why it matters:

Organizations gain stronger uptime and fewer remote access disruptions, which is critical when access is needed for production support.

CONCLUSION

THE VPN ERA IS ENDING

In 2026, VPN-based OT access will increasingly be viewed as a security and compliance liability, not because it suddenly stops working, but because it can no longer withstand scrutiny at operational scale.

The drivers are clear:

- Remote access is expanding faster than legacy controls can govern
- Attackers increasingly exploit legitimate access paths rather than perimeter defenses
- Compliance demands evidence of enforcement, not just connection records
- OT teams need remote access that preserves safety and uptime under constant use

VPNs were never designed for this operating model.

The future model is already emerging: Zero Trust OT remote access, where access is brokered, restricted, monitored, and auditable by design.

For OT and ICS organizations, the question is no longer whether VPNs will be replaced. It's whether the transition is planned and controlled, or forced by an incident, audit finding, or operational disruption that leaves little room for choice.

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 or schedule a demo.

ABOUT
XONA SYSTEMS

Xona Systems provides Zero Trust secure remote access built specifically for operational technology and critical infrastructure environments. The Xona Platform replaces VPN-based access with identity-driven, least-privilege control, full session visibility, and audit-ready accountability, without exposing OT networks or disrupting operations. www.xonasystems.com