Case Study

A Global Mining Company Connects Remote Operations Without Compromising Safety

How a base metals mining operator secured OEM access across 12 remote sites on 4 continents — cutting vendor response times from days to minutes while eliminating $2.1M in annual travel costs.

xona

Executive Summary

A global base metals mining company operating 12 mine sites across four continents faced a growing operational and security challenge: how to provide timely, secure remote access for OEM vendors servicing complex ore processing equipment in some of the world's most remote locations. With sites spanning the Africa, South America, Canada, and Australia, the company was spending over $3 million annually on vendor travel — and still experiencing response times measured in days, not hours.

The company relied on eight different vendor-specific remote access tools, each representing an unmanaged pathway into its SCADA and DCS systems. Physical site visits were not only expensive ($5,000 to $15,000 per trip) but also hazardous, requiring personnel to enter underground workings, open-pit operations, and processing plants with extreme environmental conditions.

By deploying the Xona Platform across all 12 sites — including DIN-rail hardware for harsh environments and paired with cellular backup for the four most remote locations — the company consolidated eight remote access tools into a single, secure platform. Vendor response times dropped from days to minutes, annual travel costs fell by $2.1 million, and the organization achieved alignment with IEC 62443 security requirements — all without disrupting production operations.

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. For a mining company with remote sites spanning four continents, this architecture eliminated the fundamental risk of direct vendor-to-asset connectivity while enabling faster, more reliable support than physical site visits ever could.

RESULTS AT A GLANCE	
$2.1M	Annual vendor travel cost savings
Days → Minutes	OEM response time improvement
8 → 1	Remote access tools consolidated into a single, auditable platform
Zero	Connectivity-related access failures with cellular backup deployed
73%	Reduction in safety incidents from unnecessary physical access to hazardous areas
12 Sites	Secured across 4 continents

Industry Context

The Digital Transformation of Mining

The global mining industry is undergoing a significant digital transformation. Driven by the pursuit of operational efficiency, improved safety outcomes, and rising commodity demand, mining companies are investing heavily in connected operations — from autonomous haul trucks and drill rigs to real-time process optimization in ore processing plants.

This transformation has created a paradox: the same connectivity that enables operational improvement also introduces cybersecurity risk. Ore processing plants — with their crushers, conveyors, grinding mills, and flotation cells — run on complex SCADA and DCS systems that were never designed for remote connectivity. Yet the specialized OEM vendors who service this equipment increasingly need remote access to deliver timely support.

The OEM Dependency Challenge

Mining operations are uniquely dependent on OEM support. The equipment used in mineral processing — from heavy mobile equipment to precision analytical instruments — is highly specialized. A single flotation cell controller failure can halt an entire processing circuit, costing tens of thousands of dollars per hour in lost production.

For a company operating across four continents, this creates an acute logistical challenge. When a critical ABB drive controller requires diagnostics at a site in the Zambian Copperbelt, the nearest qualified technician may be in Zurich or Perth. When a process optimization issue arises at a South American operation at 4,200 meters elevation, weather and accessibility constraints can delay physical visits by a week or more.

IEC 62443 and Mining Cybersecurity

The mining sector is increasingly adopting IEC 62443 as its industrial cybersecurity framework. While not yet mandated by regulation in most jurisdictions, major mining companies are proactively implementing IEC 62443 to protect against the growing threat of ransomware and state-sponsored attacks targeting critical infrastructure. Research from industry analysts indicates that mining organizations experience an average of 6 to 16 different remote access tools across their operations — each representing an uncontrolled access pathway that IEC 62443 was designed to eliminate.

The Challenge

The company's operational reality presented several interconnected challenges that demanded a comprehensive solution:

Remote and Hostile Environments

The company's 12 mine sites span some of the most challenging environments on earth. Four of the most remote sites — two in sub-Saharan Africa, one in Northern Canada, and one in the Australian outback — had limited or satellite-only internet connectivity. Bandwidth at these locations was inconsistent and often insufficient for conventional remote access tools, which relied on full-session RDP or VNC connections that performed poorly over high-latency satellite links.

Unmanaged Vendor Access Sprawl

Over time, the company had accumulated eight different vendor-specific remote access tools. Each major OEM — covering drives, instrumentation, process control, mobile equipment, and analytical systems — had installed its own preferred remote access software. Some used TeamViewer, others used vendor-proprietary VPN clients, and several had deployed standing VPN tunnels that remained active even when no maintenance was being performed.

This created a fragmented, unauditable access landscape. The OT security team had no centralized visibility into who was accessing which systems, when, or for how long. There was no session recording, no individual accountability, and no ability to instantly terminate a vendor session in the event of a cybersecurity incident.

Excessive Vendor Travel Costs and Response Times

When remote access was unavailable or unreliable, the company had no choice but to fly vendor technicians to site. The cost was staggering:

- Average cost per vendor site visit: $5,000–$15,000 (including flights, logistics, accommodation, and per diem for remote locations)
- Average vendor response time for on-site visits: 3–7 days
- Total annual vendor travel expenditure: over $3 million across all 12 sites
- Estimated production losses during wait time: $40,000–$120,000 per day depending on the processing circuit affected

The cost of waiting was not abstract. At one Zambian site, a variable-frequency drive failure on a primary SAG mill shut down the grinding circuit entirely. The nearest qualified ABB technician was in Zurich. Between flight booking, visa logistics, and travel to the remote site, the technician did not arrive for five days — costing an estimated **$480,000 in lost copper production**. The equipment issue itself was a configuration error the technician resolved in under two hours. With secure remote access, it could have been diagnosed and corrected in minutes.

Safety Risks from Physical Access

Every physical site visit to a mine — particularly underground operations — introduced safety risk. Vendor technicians required safety inductions, PPE, underground training certifications, and escorts. Despite rigorous safety protocols, the company recognized that reducing unnecessary physical access to hazardous areas was both a moral imperative and an operational best practice.

The Solution

After evaluating several remote access platforms — including extending its existing IT VPN infrastructure and purpose-built OT solutions — the company selected the Xona Platform as its enterprise-standard platform for OEM and third-party remote access to all processing plant OT systems.

Why Xona

Several factors drove the selection:

- **Protocol isolation:** Xona's pixel-streaming architecture means OT protocols (RDP, SSH, VNC) are terminated inside the plant network. Vendors interact with systems through encrypted pixel streams delivered to a standard web browser — no direct endpoint-to-asset connectivity, no lateral movement risk, and no OT protocol exposure on untrusted networks.
- **Low-bandwidth optimization:** Xona's PNG-based pixel rendering is specifically designed for constrained links, including satellite connections. The technology had been proven in production in maritime satellite environments — a strong indicator of performance in remote mining contexts.
- **DIN-rail industrial hardware:** For underground substations, processing plant control rooms, and dusty environments, Xona's DIN-rail form factor — compliant with IEC 61850 and IEEE 1613 — could be deployed without requiring dedicated server rooms.
- **Cellular backup:** For the four most remote sites with unreliable primary WAN links, pairing Xona with a cellular modem provided emergency access continuity, ensuring that critical maintenance sessions could proceed even during primary link outages.
- **Single-platform consolidation:** One Xona deployment replaced all eight existing vendor remote access tools, providing a single, auditable platform with centralized policy management.

> *"We were flying technicians to the Zambian Copperbelt for issues that Xona now resolves in fifteen minutes. The response time improvement alone paid for the platform in the first month."*
>
> **— VP Technical Services, Global Mining Company**

Solution Highlights — Xona Features Deployed
• **Xona Critical System Gateway (CSG)**
• **DIN-Rail Industrial Hardware**
• **Para-Pack Cellular Backup**
• **Low-Bandwidth Pixel Streaming**
• **Xona Central Manager (XCM)**
• **Credential Injection & Vault**

- **Moderated Vendor Access (Wait Room)**
- **Role-Based Access Control (RBAC)**
- **Time-Based Access Control (TBAC)**
- **Kill Button & Lockbox**
- **SIEM Integration (Splunk)**
- **Session Recording & Audit Trail**

Implementation

Phase 1: Pilot at a Single Processing Plant

The company began with a pilot deployment at its largest copper-gold processing plant — a facility with 80+ OT assets including DCS controllers, variable-speed drives, instrumentation networks, and SCADA workstations. The Xona CSG was installed in the plant's control room and operational within 25 minutes. No network reconfiguration was required; the gateway was deployed as an overlay on the existing network architecture.

During the four-week pilot, three OEM vendors were onboarded to the platform. Vendor technicians accessed the system through a standard web browser — no client software, no VPN, no plugins. The OT security team could observe live sessions in real time, review recorded sessions, and terminate access instantly when needed.

Phase 2: Enterprise Rollout Across 12 Sites

Following the successful pilot, the company deployed Xona CSGs across all 12 sites over a 10-week period. Deployment was managed centrally through the Xona Central Manager (XCM), which provided fleet-wide policy control, identity federation, and centralized log aggregation.

Key implementation details included:

- DIN-rail hardware was deployed at eight sites with space-constrained or harsh-environment control rooms, including underground substations and dusty processing environments.
- 1U rack-mounted appliances were installed at the four largest processing plants with established server infrastructure.
- Cellular backup modems were deployed at four remote sites (Zambian Copperbelt — 2 sites, Canadian Arctic — 1 site, Australian outback — 1 site) to ensure connectivity during primary WAN outages.
- All eight legacy vendor remote access tools were decommissioned as each site came online, with a two-week overlap period for transition.
- OEM vendors were transitioned to the Xona platform using just-in-time (JIT) access with moderated approval workflows — each session required authorization from the on-site OT team before going live.

Results

Within six months of completing the enterprise rollout, the company measured the following outcomes:Operational Efficiency

- Vendor response time reduced from 3–7 days (for physical site visits) to under 15 minutes for remote session initiation — in many cases, OEM support was available within minutes of a request.
- OEM "follow the sun" support became a reality: vendors in different time zones could support any site at any hour, significantly reducing the impact of equipment issues on production uptime.
- Mean time to repair (MTTR) for OEM-supported equipment fell by 68%, directly improving processing plant availability.Safety Improvement
- Physical vendor visits to underground and open-pit operations reduced by 73%, directly lowering the company's exposure hours for third-party personnel in hazardous environments.
- The safety team reported the reduction in non-essential site visits as a contributing factor in the company's improved Total Recordable Incident Rate (TRIR) for the year.

Cost Savings

- Annual vendor travel costs reduced from $3.2 million to $1.1 million — a savings of $2.1 million per year. The remaining travel was limited to commissioning, major overhauls, and capital projects requiring physical presence.
- Estimated production uptime gains of $4.2 million annually, attributable to faster issue resolution and reduced equipment downtime.
- Eight separate vendor remote access tool licenses, support contracts, and management overhead eliminated — consolidated into a single Xona platform.

Security and Compliance

- Eight unmanaged remote access tools consolidated to one centrally managed platform with full session recording, individual user accountability, and role-based access controls.
- Protocol isolation eliminated the risk of lateral movement from vendor endpoints to OT networks — no vendor endpoint ever touches the OT network directly.
- The company achieved alignment with IEC 62443 requirements for identification and authentication, use control, data confidentiality, and audit — a critical milestone as the mining industry moves toward formal IEC 62443 adoption.

Connectivity Resilience

- Zero connectivity-related access failures at sites equipped with cellular backup. During two satellite outages at the Northern Canadian site (each lasting 4+ hours), OEM vendors maintained access through the cellular backup path.
- Xona's low-bandwidth pixel streaming delivered consistent performance even over satellite links with 600+ ms latency and sub-2 Mbps throughput — a critical capability for the company's most remote operations.

Looking Ahead

With secure, reliable remote access now established across all processing operations, the company is exploring several strategic extensions of its Xona deployment:

Autonomous Operations Integration

As the company invests in autonomous mining equipment — including autonomous haul trucks and drill rigs — secure remote access to the control systems governing these assets will become essential. Xona's protocol-isolated architecture provides a foundation for extending secure remote monitoring and intervention capabilities to autonomous fleet management systems without introducing new network pathways.

Predictive Maintenance Remote Support

The company is piloting predictive maintenance analytics across its processing plants. When algorithms detect an impending equipment issue, OEM specialists will need rapid remote access to diagnose and intervene before failure occurs. The Xona platform's ability to deliver sub-minute vendor onboarding makes it a natural enabler of this proactive maintenance model — transforming remote access from a reactive cost center into an uptime-enhancing capability.

Expansion to Mobile Equipment OT

While the initial deployment focused on fixed processing plant infrastructure, the company is evaluating extension of the Xona platform to cover remote access for heavy mobile equipment control systems — including fleet management, engine diagnostics, and tire pressure monitoring systems — further consolidating its OT access governance under a single platform.

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***