OT EXPOSURE INTELLIGENCE · 2025 · INAUGURAL EDITION

The State of OT Security in Cement & Mining

An intelligence report built not from platform telemetry, but from a full year of hands-on OT network assessments and managed support across an active multi-plant cement operation. Every figure came off a plant floor.

THE HEADLINE CONDITION

82% of 267 OT network switches assessed were End-of-Life or Discontinued — outside vendor support, patches, and spare-part guarantees.

Discontinued · 122 (46%) End-of-Life · 97 (36%) Active Mature · 16 (6%) Active · 18 (7%) Unclassified · 14 (5%)

01 — Executive Summary

The exposure is structural, not exotic.

> Cement OT is not failing because of advanced threats. It is exposed because obsolescence, weak segmentation, and ungoverned access were allowed to persist.

The networks that run kilns, crushers, and packing lines are largely built on hardware their own manufacturers no longer support. With 82% of the switching fleet End-of-Life or Discontinued, the patch-management conversation is moot until the lifecycle problem is addressed.

The picture compounds. The installed base concentrates in a small number of automation and networking vendors, deepening lock-in. Obsolete fieldbus still carries production traffic. Unmanaged and consumer-grade switches sit in critical OT paths. And the physical separation between IT and OT — a baseline control — was still being established for the first time in 2025 at sites that had run for years without it.

Keeping these networks stable was not passive: **275 OT support activities** (76 incidents, 199 planned services) were required over the year — the operational tax of deferred modernization. Each of these conditions is solvable. This report maps where they sit and what to prioritize.

02 — Deep Dive

The lifecycle crisis

OT hardware is built to outlive IT hardware. The failure is not that equipment ages — it is that lifecycle status goes untracked, so obsolescence accumulates invisibly until a failed switch with no replacement takes systems offline.

SWITCH LIFECYCLE — 267 ASSESSED

Discontinued	122 · 46%
End-of-Life	97 · 36%
Active Mature	16 · 6%
Active	18 · 7%
Unclassified	14 · 5%

INSTALLED BASE — VENDOR SHARE

Rockwell	93
Cisco	65
Hirschmann	44
Allied Telesyn	13
Fortinet	12
All others	40

Concentration simplifies some support, but it means one vendor's lifecycle decisions ripple across the entire fleet — strengthening the case for an operator-governed standardization strategy rather than an OEM-driven one. Alongside the industrial equipment sat unmanaged and consumer-grade switches: blind spots by construction, installed quietly to solve an immediate connectivity need.

03 — Key Findings

Seven conditions, as observed

01 **OT switching is largely obsolete** — 82% EOL / Discontinued
The majority of the fleet sits outside vendor support.

02 **Current, supported equipment is the exception** — ~7% Active
A thin minority remains in active status.

03 **The installed base concentrates in a few vendors** — 3 vendors ≈ 75%
Three vendors hold the bulk of the fleet — lock-in by default.

04 **Obsolete fieldbus still carries production traffic** — in production
Legacy DeviceNet, mid-migration to EtherNet/IP.

05 **IT and OT were not yet physically separated** — just begun
A baseline control, established for the first time in 2025.

06 **Unmanaged & consumer-grade switches in OT paths** — present
No segmentation, no monitoring, no management plane.

07 **Obsolescence carries a continuous operational tax** — 275 activities / yr
76 incidents + 199 planned services to hold the line.

04 — Framework

The Potenza OT Maturity Model

A diagnostic of what an operator can see and control — not which products they own. Four stages, each enabling the next.

STAGE 01
Blind
No reliable inventory, topology, or lifecycle visibility. Basic questions about the OT network can't be answered.

STAGE 02
Aware
Inventory and topology exist on paper. Gaps and obsolescence are known, but not yet controlled.

STAGE 03
Controlled
Segmentation, governed access, and lifecycle management are in place and maintained for priority systems.

STAGE 04
Resilient
Controls are continuous and tested. The environment degrades gracefully under stress rather than failing silently.

Where cement plants sit: the assessed fleet entered the year largely between Blind and Aware. The year's work moved priority systems toward Controlled. Few cement OT environments operate at Resilient today.

05 — Analysis

The structural independence problem

A vendor-concentrated installed base raises a question the sector rarely asks aloud: if the OEM that supplies the equipment also governs its security, who provides the independent check?

> The OT service owner cannot be the OT vendor.

There is a product roadmap behind every recommendation an OEM makes. That is structural, not a criticism. An operator that lets a single vendor both supply and govern its OT environment has no party assessing that environment purely in the operator's interest.

Structural independence is the alternative: assessment, documentation, and governance by a party with no equipment to sell and no product quota. For an operator carrying 82% obsolete infrastructure, an independent modernization roadmap — one not anchored to a single vendor's catalog — is how it keeps leverage over its own future spend.

06 — Recommendation

The Cement & Mining OT Baseline

Five controls form the minimum defensible baseline. They are ordered — each enables the next.

1. **Inventory & lifecycle of record**
You can't secure or budget what you can't see. Lifecycle status turns 82%-obsolete from a surprise into a plan.
2. **Topology of record**
The authoritative map of assets, VLANs, flows, and remote paths — the artifact every later decision depends on.
3. **Purdue-aligned segmentation**
Separate IT from OT and zone the plant floor so one compromise can't traverse the whole network.
4. **Governed remote & privileged access**
Brokered, logged, least-privilege access — no single tool whose failure cuts off all support.
5. **Independent governance**
An operator-side owner that assesses and prioritizes in the operator's interest, not a vendor's roadmap.

Maps cleanly onto ISA/IEC 62443 and NIST SP 800-82r3 for operators who need framework alignment.

07 — Looking Ahead

What the next year turns on

CONVERGENCE	As plants connect OT to corporate networks and SD-WAN, the unestablished IT/OT boundary becomes the highest-leverage risk to close.
MODERNIZATION	With 82% of switching obsolete, the question shifts from whether to replace to how to phase replacement without halting production.
INDEPENDENCE	Operators carrying heavy OEM concentration will increasingly separate who governs OT security from who sells the automation.

Potenza Services, Inc. is a structurally independent OT cybersecurity and industrial networking firm for cement, mining, and heavy-industry operators. MSHA Part 46-certified engineers and Avetta-qualified contractor status let work begin on active sites without onboarding delays. Every figure in this report came from hands-on assessment and managed-support work.

Evaluate your OT environment →

Methodology. Twelve months of OT assessment and managed support across an active multi-plant North American cement operation. 267 OT switches inventoried and lifecycle-classified; 275 support activities logged. All data anonymized — no client, site, host, or individual is identifiable.

Service-Disabled Veteran-Owned · Founded 2012 · Purdue Model · ISA/IEC 62443 · NIST SP 800-82r3 · potenzaservices.com