PILLAR 01 · THE FLOOR

# PISO Framework: Platform for Intelligence on Operational Systems

The four layers that determine whether your operation's floor can sustain — and lead — the intelligence the business demands

# 01

## 01 · Executive Summary

## 01 · Executive Summary

For thirty years, OT was the floor of the plant and the mine. Silent. Reliable. Ignored.

Today the business wants that floor to be intelligent — and OT has the opportunity to lead it. But it also faces three problems that no AI vendor will solve on their own: fragmented responsibilities across contracts, response speed the business no longer accepts, and an identity crisis in the face of IT arriving with transformation proposals.

The PISO Framework — Platform for Intelligence on Operational Systems — is NTT DATA's response to that situation. It is not an OT technology catalog. It is a four-layer codependent architecture that describes **the conditions that must be coherently active for operational intelligence to deliver sustainable value in a mining operation.**

The central thesis of this document is direct: **no layer delivers value in isolation.** An OT technology arsenal without a written mandate is infrastructure without governance. A learning loop without the data integrity of Layer 1 learns lies. A decision architecture without the sovereign connectivity of Layer 3 cannot act in real time. The activation sequence matters — and it is the same for all operations, even though the specific content of each layer varies.

### WHO THIS DOCUMENT IS FOR

- **OT managers and leaders:** who see AI proposals arriving from IT without anyone asking whether the floor is ready — and who need a language to articulate what is missing before the project starts.
- **OT systems architects:** who design or evaluate industrial infrastructure and need a framework to integrate cybersecurity, connectivity, on-premise inference, and agent-readiness into a coherent architecture.
- **CTOs and VPs of operations:** who approve technology budgets and need to understand why 72% of AI projects in mining fail to meet their objectives — and which infrastructure conditions determine whether the next project falls in that 72% or not.

# 02

## 02 · The Tension No One Has Named Yet

## 02 · The Tension No One Has Named Yet

Business Talk Article 07 described the case of the dashboard that lasted two weeks. A technically correct system that died because the organization's objective function defeated the best system. Behind that failure — and hundreds of similar cases — lies a structural tension in the OT world that has become impossible to ignore:

| FRAGMENTATION | VELOCITY | IDENTITY |
| --- | --- | --- |
| Three contracts, zero responsible parties. The problem lives between vendors and no one has the mandate to resolve it. When something fails at the intersection between the industrial network contract, the SCADA, and the dispatch system, the problem circulates between providers without anyone owning it. | Response takes hours of escalations. The business expects it to take ten minutes. The gap is not technology — it is decision architecture: who can act, on which system, at what level of autonomy, without depending on an approval chain that invalidates real-time operation. | IT arrives with an AI proposal. OT has process knowledge but no proposal ready. Without a framework that articulates what conditions OT needs resolved before AI can capture value, OT loses the conversation — and with it, the mandate. |

These three tensions are not technical problems. They are organizational architecture and governance problems. The PISO Framework addresses them systematically — not because technology resolves them alone, but because it has the structure to name them precisely before the project begins.

> *The floor has sustained the mine for 30 years. It is time for it to also think.* — PISO Framework · NTT DATA, 2026

### 2.1 · WHY NO LAYER DELIVERS VALUE ALONE

The most common error in OT implementations is treating technology as the solution itself — buying the arsenal without resolving the terrain, installing on-premise inference without having an intersection mandate, activating the learning loop without data integrity. The result is infrastructure that does not sustain itself when the project ends.

The NTT DATA and MIT Technology Review study (2025) identified that legacy system integration (10.14%) and technological reliability (11.59%) are frequently cited barriers — but both are symptoms of poorly activated layers, not independent technical problems. A legacy historian does not integrate well because no one defined the IT-OT architecture before trying to connect it. An unreliable system is unreliable because the Layer 1 asset baseline was never documented.

# 03

## 03 · The Four Layers of the PISO Framework

# 03 · The Four Layers of the PISO Framework

Each layer has a central question that defines whether it is active. Each layer has specific conditions that must be met. And each layer has a downward dependency: Layer 2 produces no value if Layer 1 is not active, and so on.

### LAYER 01 · OPERATIONAL TERRAIN

**Is the foundation documented, intact, and with a clear mandate for what is coming?**

Layer 1 is the most ignored and the most critical. It is not glamorous — it is inventory, documentation, data integrity. But without it, everything built afterwards rests on assumptions the actual operation contradicts.

| COMPONENT | WHAT IT IS | WHY IT IS CRITICAL |
|---|---|---|
| **OT Asset Inventory and Baseline** | What exists, where it is, how it is configured today — not on installation day. | The existing map is typically the installation blueprint from 12 years ago. Without a current reference, observability and modernization are impossible. |
| **Industrial Data Integrity** | The data the AI system will consume is the real data — not the corrected version. | Historians record the corrected version of reality: silenced alarms, manually adjusted setpoints, data cleaned before export. A model learns that version, not the real one. |
| **OT Knowledge Preservation** | The understanding of why each parameter is at its specific value — before whoever knows it retires. | The engineer who knows why that specific setpoint is at that value is 58 years old. When they leave, no one will want to touch that configuration — and the system will not be able to optimize it. |
| **OT Mandate Definition** | What OT decides and what IT decides — written, agreed, and defensible. | What is not written is lost by omission. The boundary is defined better when OT has a clear proposal, not when it is negotiated project by project. |

**LAYER 01 DIAGNOSTIC QUESTIONS** - Does an updated OT asset inventory exist — not the installation-day version, but today's? - Do the historian data reflect what actually happens in the operation, or the version someone cleaned before reporting? - Is there a written document defining what IT can and cannot do within the OT environment?

## LAYER 02 · OT DECISION ARCHITECTURE

### Who decides what — and who answers when the problem lives between systems?

Layer 2 is the one most frequently missing from OT implementations — because it is not technology, it is governance. And governance does not come in the vendor's catalog.

#### The Intersection Mandate

The most frequent pain point in OT does not live within a contract — it lives between two. There is a contract for the industrial network, another for the SCADA, another for the dispatch system. When something fails at the intersection, no one has the mandate to resolve it.

This problem exists long before there is AI: it exists every time a system fails at the boundary between two contracts and resolution takes hours because each vendor points to the other. It becomes more critical — and its consequences more visible — as autonomous systems are added on top of an infrastructure whose responsibility boundaries were never explicitly written.

#### OT Identity in the AI World

**THE IDENTITY PROBLEM**

IT arrives with an AI proposal. OT has the process knowledge — it knows exactly why the model cannot touch the control system, why network segmentation is non-negotiable.

But OT does not have the proposal ready. And without a proposal, the mandate goes to IT by default.

**The PISO Framework is the proposal.** OT moves from being a technical actor that approves or rejects IT requirements to being the architect of process intelligence — with its own criteria, its own language, and an explicit mandate.

#### Human-System Design

What the model decides, what the operator decides, what decision should not exist. In OT this question carries an additional constraint that IT frequently ignores: **the level of autonomy a model acting on an actuator in a critical process can have is bounded by functional safety — not by design convenience.**

A model that adjusts a process setpoint in real time without human confirmation may be fully compliant with IEC 62443 and simultaneously lack the IEC 61511 safeguards that prevent an incorrect recommendation from activating an actuator in unsafe conditions. That tension is not resolved with more AI — it is resolved by explicitly designing the boundary before deployment.

#### Designed IT-OT Relationship

IT-OT convergence delivers more value when it has an explicit architecture: what enters the OT environment, under what conditions, with what governance. Without that architecture, convergence is invasion — and OT resists it for reasons that are perfectly rational from a functional safety standpoint.

- **What IT can bring to the OT environment:** validated inference models, IT-enriched context data, visualization dashboards
- **What cannot enter without OT validation:** direct access to PLCs or actuators, setpoint changes in control systems, models trained on IT data without process validation

---

LAYER 03 · OT ARSENAL

### Does the technology environment have the capabilities to sustain the intelligence the process requires?

Layer 3 is where technology appears — but it appears in its correct place, as an enabler of the previous layers, not as an autonomous solution. An OT arsenal without active Layers 01 and 02 is infrastructure without a mandate: it can be installed, it cannot be sustained.

| COMPONENT | WHAT IT ENABLES | STANDARD / TECHNOLOGY |
|---|---|---|
| **Sovereign Connectivity and High Availability** | Designed and documented OT network. Operation that can live in a datacenter with photonic connectivity — near-zero latency. No people on the hill, system resilient by design. | IOWN Photonic Networks (125x capacity, 200x lower E2E latency) · Private 5G/6G owned by mine · Edge computing on-premise |
| **OT Modernization: Agent-Readiness** | SCADA, DCS, historians designed for humans — converted into resources agents can invoke directly. From screens for humans to APIs for agents. Modernize without stopping production. | OPC-UA · Modbus · PROFINET · Apache Kafka + Avro for real-time streaming · RESTful APIs over historians |
| **Inference on the Floor** | AI models running on-premise, within the OT network, feeding control systems in real time. No dependency on the cloud or external connectivity. The decision travels less than the signal that triggers it. | Industrial edge computing · Models optimized for local inference · Latency < 10ms for real-time control |
| **OT-Native Shielding** | Cybersecurity designed from the ground up for operational environments — not adapted IT security. Segmentation by zones that does not paralyze operations when applied. | IEC 62443 (OT cybersecurity) · Purdue Model / ISA-95 · Zero Trust adapted to OT · Integrated IT/OT SOC |
| **Functional Safety** | The mechanism that detects when a model drifts from the process and contains it before generating physical risk. Protects against the system itself — distinct from cybersecurity. | IEC 61508 / IEC 61511 · Safety Instrumented Systems (SIS) · Safety Integrity Level (SIL) testing |
| **Observability Without Exposure** | Real-time monitoring with reference to the Layer 1 baseline. Seeing must have rules: monitoring from inside, remote access controlled by policies. | Grafana + Prometheus for OT · Infrastructure self-diagnostics · Remote access with MFA authentication and session segmentation |

**IEC 62443 AND IEC 61511: THE DISTINCTION IT FREQUENTLY IGNORES**

**IEC 62443 (OT Cybersecurity):** protects the system from external threats — malicious actors, malware, unauthorized access. Defines segmentation zones, access policies, threat monitoring.

**IEC 61511 (Functional Safety):** protects the process from failures of the system itself — including AI model failures. Defines the integrity level (SIL 1–4) at which a safety instrumented system must operate when the AI model fails or produces a recommendation outside the safe operating range.

*An AI model can be perfectly protected under IEC 62443 and simultaneously lack the IEC 61511 safeguards that prevent an incorrect recommendation from activating an actuator in unsafe conditions. Both standards are necessary. They are not interchangeable.*

---

LAYER 04 · GOVERNANCE IN MOTION

## Can the OT system sustain itself, learn, and scale as the autonomy frontier advances?

Layer 4 is what differentiates an AI project from a living system. Layer 2 designs the decision rules before deployment. Layer 4 governs how those rules evolve as the autonomy frontier advances — in production, under pressure, with incomplete information.

### Governance of Autonomy in Evolution

As the model gains more authority, who decides when and how that perimeter expands? Not the initial design — but the governance of how that design changes over time with accumulated trust.

The AI trust ladder — from copilot to orchestrator — is not governed from Day 1. It is governed from the first divergence between what the model recommended and what the operator did, and the first decision about whether that divergence warrants updating the model or holding it.

### The OT Learning Loop

What distinguishes a static AI system from one that grows wiser with each shift. Without this loop, the system learns in the laboratory and fossilizes in production. With it, each shift makes the next one smarter.

**THE LOOP IN 6 STEPS** 1. Operator adjusts setpoint the model would not have adjusted 2. System detects and records the deviation 3. System asks: 'Why did you make that decision?' 4. Operator explains the expert criterion 5. Human validation before updating the model 6. The next shift inherits that criterion

*This loop requires all three layers active: Layer 02 (cultural permission to deviate), Layer 03 (infrastructure that captures the deviation), Layer 04 (governance to update the model in production).*

#### OT Lifecycle Management

How to modernize without stopping production. An OT lifecycle logic that the business can approve and fund — and that does not leave the team running 15-year-old systems because no one authorized the change.

A project that depends on the vendor to sustain itself is not sovereignty — it is outsourcing with extra steps. Layer 4 defines how the internal OT team maintains the ability to operate, update, and scale the system without dependency on whoever built it.

#### Operational Scalability

What works in the SAG mill must be transferable to flotation — not as a copy but as a pattern with governance that travels with the system.

---

# 04

## 04 · Coherence with the Mining Autonomy Framework

## 04 · Coherence with the Mining Autonomy Framework

PISO is not a framework parallel to NTT DATA's Mining Autonomy Framework — it is its expression in OT-native language. Each PISO layer corresponds to a layer of the Autonomy Framework, with OT-specific depth added at each level.

| MINING AUTONOMY FRAMEWORK | PISO FRAMEWORK (OT) | WHAT PISO ADDS |
|---|---|---|
| **C01 · Structural Enabling Conditions** | **C01 · Operational Terrain** | Explicit OT mandate + physical asset inventory. OT adds the dimension of contaminated industrial data and the tacit knowledge of the process engineer. |
| **C02 · Behavior Engine** | **C02 · OT Decision Architecture** | Intersection mandate between vendors + explicit IT-OT architecture. OT adds the functional safety constraint that limits the level of autonomy possible on actuators. |
| **C03 · Technology Arsenal** | **C03 · OT Arsenal** | Technology in its correct place. OT adds mandatory on-premise inference, IEC 62443 + IEC 61511, and the distinction between sovereign and borrowed connectivity. |
| **C04 · Tactical Orchestration** | **C04 · Governance in Motion** | Sustainability and learning loop. OT adds lifecycle management without production downtime and scalability from pilot to multiple plants. |

PISO develops as a complete architecture what the Autonomy Framework names in Layer 3 (Technology Arsenal) — with the language and pain points of the OT leader. If the Autonomy Framework defines the *what*, PISO defines the *how* for the world of operational technology.

# 05

## 05 · NTT DATA's OT Differential

## 05 · NTT DATA's OT Differential

The correct question is not: what OT technology do you need? — it is: how are you going to sustain the intelligence of the process when the project ends, and who has the mandate to defend it?

Any vendor can deliver one or two PISO layers in isolation. NTT DATA's differential is the integration of all four layers with knowledge of the mining process — not of the product catalog.

| PROCESS KNOWLEDGE | FULL TECHNOLOGY CAPABILITY | GOVERNANCE ARCHITECTURE |
|---|---|---|
| · Industrial networks, photonics, OT Wi-Fi · Integration with SCADA, DCS, PLC, historians · OT protocols: OPC-UA, Modbus, PROFINET · We understand the model cannot touch the control system without going through SIS | · OT cybersecurity (IEC 62443) + functional safety (IEC 61511) · On-premise infrastructure for real-time inference · High availability and photonic connectivity (IOWN) · OT modernization without production downtime | · Intersection mandate between vendors · IT-OT boundary design · Sustainable OT lifecycle without dependency on original vendor · Production learning loop with governance |

## 5.1 · DOCUMENTED REFERENCE CASES

**REFERENCE CASE · AUTONOMOUS HAULAGE SYSTEM — MAJOR COPPER PRODUCER, NORTHERN CHILE** Chile · Copper mining

**Challenge:** Deploy an autonomous haulage system at a high-altitude copper operation with 4 autonomous trucks and 10 auxiliary vehicles across an active pit.

**Solution:** Private LTE network with full coverage and cybersecurity. Control room with 5 stations, real-time monitoring. Architecture validated to scale to 150+ trucks.

**Result: Proven scalability. Reinforced safety: operations controlled with zero incidents. Efficiency achieved: reliable data transmission, continuous operation.**

**REFERENCE CASE · INFRASTRUCTURE MODERNIZATION — MAJOR DIVERSIFIED MINING COMPANY, CHILE** Chile · Copper and mineral mining

**Challenge:** Multiple network and IT modernization projects across Chilean operations: network upgrades, obsolescence management, LTE, real-time monitoring systems, secure access. OT modernization: PLC, EWS, and concentrator upgrades.

**Solution:** Reinforced digital backbone for autonomy. LTE connectivity + real-time monitoring. Autonomous drilling and autonomous trucks enabled. IT/OT integration as the foundation for exception-based operations.

**Result: Future-compatible digital backbone for autonomy and real-time operations. Foundation for Industry 4.0 and exception-based operations.**

**REFERENCE CASE · FLEET MANAGEMENT OPTIMIZATION — MINERAL SALT PRODUCER, ATACAMA REGION** Chile · Salt mining

**Challenge:** Improve the productivity of the mineral salt transport fleet from mine to port across a 400+ km logistics corridor.

**Solution:** FMS AVA analytics implementation to detect improvement opportunities in trucks, loaders, and operator performance.

**Result: Over USD 3M in fleet management improvement opportunities identified. Optimized haulage cycles and shift performance.**

**REFERENCE CASE · IT/OT MATURITY ASSESSMENT — MAJOR COPPER AND GOLD PRODUCER, ASIA-PACIFIC AND LATIN AMERICA** Multi-region · Copper and gold mining

**Challenge:** Evaluate IT/OT maturity to identify gaps and improvement opportunities across all plants, the mine, and power generation facilities spanning two continents.

**Solution:** Comprehensive assessment with inventory of systems, platforms, networks, and architecture. Recommendations in 3 areas: IT/OT integration, hybrid infrastructure optimization, and organizational capabilities for digital adoption.

**Result: Comprehensive report as the foundation of the IT/OT modernization plan. Clear investment prioritization with estimated ROI and implementation roadmap.**

**THE COST OF AN UNREADY FLOOR — ESTIMATED IMPACT FOR A USD 1B REVENUE OPERATION**

A mining operation with USD 1 billion in annual revenue typically allocates 3% of revenue to technology — USD 30M per year. Over a standard three-year digital transformation cycle, that represents a USD 90M portfolio of AI and autonomy projects.

Applying the NTT DATA and MIT Technology Review study finding — 72% of projects deliver only partial results — the average value capture across that portfolio is approximately 30–35% of projected value. For a portfolio targeting USD 90–120M in cumulative productivity gains, that partial capture yields USD 28–42M actually realized.

**The unrealized value: USD 50–80M over three years.**

The most common root cause is not model quality, vendor choice, or change management. It is the activation state of the four PISO layers at the moment each project began:

| LAYER INACTIVE | TYPICAL PROJECT IMPACT |
|---|---|
| Layer 01 (data integrity not established) | AI model learns corrected version of reality. Productivity gain: 30–40% of target |
| Layer 02 (no intersection mandate) | When something fails between systems, resolution takes hours. One IT maintenance event disrupts OT. Trust in system destroyed within 60 days |
| Layer 03 (telco-dependent connectivity) | Each network outage during autonomous operation requires full system restart. At USD 100K+/hour of lost production, 3–5 events per year = USD 1.5–5M in direct losses |
| Layer 04 (no learning governance) | System is correct on Day 1 and incorrect on Day 365. Mine changed; model did not |

**Investment to resolve the PISO floor before the next project cycle: USD 4–8M. Effective ROI on the floor investment: 8–15x, unlocking value from projects already budgeted.**

The floor is not a prerequisite to negotiate. It is the condition that determines which column of that table your next project lands in.

# 06

## 06 · Prerequisites: What Must Be Resolved Before Starting

# 06 · Prerequisites: What Must Be Resolved Before Starting

PISO is not a shopping list. It is a current-state diagnosis and a roadmap toward the target state. Before beginning any implementation, three conditions determine how fast and with what risk you can advance:

**CONDITION 01 · DATA INTEGRITY**

If the historian data is the corrected version of reality — silenced alarms, manually adjusted setpoints, events cleaned before export — the AI system that learns from that data will be more precise in replicating distortions than in describing what actually occurs.

Before implementing Layer 3, Layer 1 must have the data integrity baseline resolved. Without that, the arsenal learns lies faster than any operator.

**CONDITION 02 · WRITTEN MANDATE**

Layer 2 requires a mandate document that exists before the first model touches the first actuator. That document defines: what the system can decide autonomously, what requires human confirmation, what it can never do without physical validation.

Without a written mandate, the first time the system does something unexpected — and it will — there will be no criterion to evaluate whether it was a system error or behavior outside the defined perimeter.

**CONDITION 03 · NETWORK SOVEREIGNTY**

On-floor inference requires the OT network to be sovereign — not borrowed from a telco, not shared with third-party systems, not dependent on external connectivity to function.

Ransomware events that have paralyzed drills and trucks in mining operations across the sector were not AI model security problems — they were network architecture problems that allowed an IT environment event to reach OT systems. Network sovereignty is not a luxury — it is the condition that determines whether the infrastructure can operate when the external network fails.

**THE QUESTION THAT ORGANIZES EVERYTHING**

**How are you going to sustain the intelligence of the process when the project ends?**

If the answer is 'the vendor handles it', Layer 4 is not active. If the answer is 'the internal OT team has the mandate, the knowledge, and the architecture to do it', the framework is on the right path.

# 07

## 07 · What PISO Does Not Resolve

# 07 · What PISO Does Not Resolve

| LIMIT | WHY AND WHAT IT REQUIRES |
| --- | --- |
| **Does not resolve organizational adoption** | A perfectly implemented OT infrastructure can be ignored if operators do not adopt it or if organizational incentives are not aligned with the system's optimal. The floor enables intelligence — it does not guarantee the organization uses it. Adoption requires the conditions of Pillar 03 (The Organization). |
| **Does not replace the reasoning system design** | PISO provides the substrate — data, connectivity, on-premise inference, governance. It does not define how the system reasons about that data. The hybrid flowchart+LLM architecture, the dynamic causal graph, and the AI trust ladder are components of Pillar 02 (The Intelligence) that operate on the floor PISO enables. |
| **Network sovereignty requires investment that is not always budgeted** | Migrating from telco-dependent connectivity to private 5G or IOWN photonic networks is a capital infrastructure decision that requires board approval, not just the OT team. PISO defines why it is necessary — it does not eliminate the budget negotiation. |
| **IEC 61511 requires specialized functional safety engineering** | Functional safety is not certified with a software audit — it requires process engineering to determine the Safety Integrity Levels (SIL) of each safety-instrumented function. That engineering is outside the scope of most AI projects that present themselves as 'OT modernization'. |
| **Sustainable OT lifecycle requires recurring budget** | Layer 4 is not a project — it is a program. OT modernization without production downtime, the learning loop, model updates are recurring activities that require continuous operational budget, not just capex investment. Organizations that treat PISO as an implementation project underestimate this requirement. |

# 08

## 08 · Related Reading and Next Steps

## 08 · Related Reading and Next Steps

### RELATED CONTENT IN THIS SERIES

- **Pillar 02 · The Intelligence:** Causal reasoning and hybrid intelligence — the reasoning system that operates on the infrastructure PISO enables
- **Pillar 02 · The Intelligence:** Data integrity in AI systems — the contaminated data problem that PISO's Layer 1 must resolve before the system learns
- **Pillar 03 · The Organization:** Tacit knowledge as critical infrastructure — PISO's Layer 1 includes OT knowledge preservation: the complete methodology is in that whitepaper
- **Pillar 03 · The Organization:** The Bainbridge paradox in mining — the organizational design that PISO's Layer 2 (OT decision architecture) must consider so autonomy does not destroy the competence it needs

*All articles available at biztalksnttdata.com*

### NEXT STEPS

**NEXT STEPS**

If this document describes a gap you recognize in your operation:

- **PISO Diagnostic:** assessment of the four layers in your operation — what is active, what is missing, and in what order to resolve it
- **IT/OT Assessment:** asset inventory, data integrity, and intersection mandate as a starting point (Layer 01)
- **Agent-readiness pilot:** selection of an existing system (historian, dispatch, or SCADA) to convert into an agent-ready resource with OPC-UA and Kafka

---

*No data, no autonomy. No floor, no intelligence. The floor has sustained the mine for 30 years. It is time for it to also think.*

---

**NTT DATA · Mining & Resources · 2026** · biztalksnttdata.com · Pillar 01 · The Floor

*For information about implementing the PISO Framework at your operation, contact: Jaime Rebolledo, Director - Mining · jrebollc@nttdata.com*