PILLAR 04 · IT/OT CONVERGENCE IN MINING

IT/OT Convergence in Mining Operations

From functional silos to an interoperable operating platform — enabling the autonomous mine, real-time decision-making, and the connected worker

01

01 · Executive Summary

01 · Executive Summary

2:47 AM — SEVEN CALLS

At 2:47 AM on a Tuesday in February, the shift supervisor at the operations control room detected a deviation. The ore blend arriving at the concentrator had dropped from 2.1% planned copper grade to 1.87%. Not a crisis — but a decision with a 20-minute window before the effect propagated through the circuit and correcting it became significantly more expensive. By the time the deviation appeared on the dashboard, most of that window was already gone.

The decision in principle was simple: adjust the blend from the secondary stockpile, or accept the grade and compensate with reagent dosing. Each option had a different cost profile and a different consequence for what they would be able to load onto the ship berthing 14 hours later, 320 kilometers away at the port.

To make that decision correctly, she needed three things:

First: whether the deviation originated in the mine — a change in ore hardness at the active face — or in the plant — a crusher behaving differently since the shift change two hours earlier. That information lived in the dispatch system, operated by the mine team, running on a network physically isolated from the concentrator SCADA for security reasons. There was no shared dashboard. There was no API. There was a phone number.

Second: the current loading schedule and grade commitments at the port terminal. That data lived in a logistics contractor's terminal management system, accessible through a portal the control room computers did not have configured. The logistics coordinator went to sleep at midnight.

Third: the energy tariff forecast for the next three hours. Running the SAG mill at higher intensity to compensate would cost differently at 3 AM than at 6 AM. That data was in a corporate finance system, accessible only through a VPN that had not been provisioned for the control room workstations.

She made seven phone calls in 14 minutes. She reached four people. She made the decision at 3:01 AM with two of the three inputs confirmed and one assumed.

The 20-minute window had closed eleven minutes earlier.

That scenario — a mine, a plant, a port, and an energy system that cannot share a coherent operational picture in real time — is not a technology failure. Every one of those systems was functioning correctly. The dispatch system was tracking every truck. The port terminal system had a precise loading schedule. The energy management system had real-time tariff data. The problem was structural: a mine-to-port value chain that had never been built to operate as one.

This is the problem IT/OT convergence actually solves — not the technology problem, but the integration, governance, and architecture problem that sits beneath it.

The convergence between Information Technology (IT) and Operational Technology (OT) has become a critical enabler for modern mining. It is not simply about integrating platforms or networks — it is about creating an enterprise capability that connects decisions, processes, assets, and people across the value chain, from the mine to the port.

In most mining companies, IT and OT were born and grew under different leaders, with different metrics, budgets, and priorities. OT has historically been closer to operational continuity and process control; IT, in contrast, concentrated on corporate networks, infrastructure, and back-office applications. That separation, valid in the past, today limits decision velocity, interoperability, and digital scalability.

The problem is not only organizational. Mining tends to operate through functional silos: mine, plant, maintenance, energy, logistics, and port adopt different technologies with misaligned data models and integration layers built case by case. In that context, talking about autonomy, remote operations, advanced analytics, or artificial intelligence without a common foundation of connectivity, data, and architecture is promising more than the platform can deliver.

> *"IT/OT convergence in mining is not solved by merging org charts; it is solved with an interoperable architecture, a common operating model, high-fidelity telecommunications, and a cultural transformation that connects the worker to the data and to the decision."* — NTT DATA · Mining & Resources, 2026

IT/OT convergence must be approached as a business and architectural transformation: high-fidelity telecommunications, resilient infrastructure, security by design, data interoperability, operable analytical applications, and a mindset shift that converts the worker into an active participant in the connected ecosystem.

WHY NOW

The pressure for greater productivity, safety, sustainability, and traceability is pushing mining companies to operate with increasingly shorter time horizons. What was analyzed at end of shift must now be observed in real time; what was decided from local experience must now be optimized with telemetry, models, and remote collaboration.

- The mine of the future relies on autonomous or semi-autonomous equipment, remote operation centers, and continuous optimization models.
- Decision-making requires reliable, synchronized data across operational and corporate domains.
- Industrial cybersecurity is no longer an add-on layer: it must be part of operational design and business continuity.
- Competitive advantage will migrate from isolated technology acquisition toward the ability to integrate, govern, and scale it.

02

02 · The Structural Problem: An Industry Operated in Silos

02 · The Structural Problem: An Industry Operated in Silos

Operating in silos is not an accidental flaw; it is a historical consequence of how operations, processes, and technologies evolved. Each area optimized its decisions with a local focus, generating tools effective for solving specific problems but poorly suited to sharing operational context with other functions. The cost of that fragmentation becomes visible when companies try to scale advanced control, predictive maintenance, ore traceability, or mine-to-port integration.

STRUCTURAL FACTOR	COMMON MANIFESTATION	BUSINESS AND OPERATIONAL IMPACT
Separate governance	IT and OT report to different leaders and prioritize different agendas	Cross-functional decisions on architecture, cybersecurity, data, and investment roadmap become difficult
Technology by domain	Each area selects solutions with local criteria	Point-to-point integrations multiply and dependence on tacit knowledge increases
Non-harmonized data	Labels, events, and catalogs without a common model	Analytics loses traceability, quality, and ability to scale across sites
Networks not treated as critical assets	Insufficient or heterogeneous connectivity in operational zones	Remote operation, video, telemetry, and mobility become exposed to outages or latency
Incomplete cultural shift	Users see digital tools as additional demands rather than work support	Adoption is low and benefits are limited to pilots or central initiatives

> **DIAGNOSTIC QUESTION** *Can your organization make a critical operational decision in less than 10 minutes with verified data from three distinct domains (mine, plant, and maintenance) without phone calls or manual spreadsheets?*

03

03 · The Limit of the Org-Chart-Only Approach

03 · The Limit of the Org-Chart-Only Approach

Many companies attempting IT/OT convergence start with the organizational structure: creating a shared management, a center of excellence, or a new digital VP role. That move can facilitate conversations and accelerate certain decisions, but by itself it does not eliminate silos. If the architecture remains fragmented, connectivity remains insufficient, domains maintain incompatible data, and the operating model does not change, convergence becomes nominal, not real.

True convergence demands a common language between business, technology, and operations. This means defining architecture principles, interoperability standards, investment priorities, resilience criteria, and governance that combines speed with control. In other words, the company must move from uniting areas to building a common operating platform.

> **Convergence is NOT...** Merging org charts, centralizing all teams, imposing a single tool, or transposing corporate IT logic onto industrial environments without adaptation.
>
> **Convergence IS...** Creating a transversal capability to operate connected assets, protect critical processes, integrate data from edge to corporate, and enable timely decisions from the control room to the remote operations center.

04

04 · The Mine of the Future: Autonomous, Remote, and Data-Driven

04 · The Mine of the Future: Autonomous, Remote, and Data-Driven

The mine of the future is no longer explained solely by mechanization or local automation. It is explained by the ability to coordinate complete processes with continuous, visible, and reliable information. Autonomy is not simply a truck without a driver; it is a different way of operating where planning, dispatch, process control, maintenance, energy, and logistics exchange context to optimize decisions and react rapidly.

That reality demands redesigning the technological foundation. Mobile assets require robust mobility and handover; remote processes require low latency and continuity; distributed supervision needs correlated video, telemetry, and events; artificial intelligence needs consistent, governed data; and cybersecurity must protect both information and operational availability.

> *"There is no autonomous mine with an analog culture. Autonomy requires data discipline, consistent tool usage, confidence in assisted recommendations, and line leadership capable of combining operational experience with digital evidence."* — NTT DATA · Mining & Resources, 2026

The reference architecture for IT/OT convergence in mining is organized in layers: sensors, PLC, and SCADA at the field level feed edge computing nodes at the operation site, which connect upward to an OT/IT integration platform and corporate cloud. Data governance and cybersecurity operate as cross-cutting capabilities across all layers — not as add-ons at the top.

05

05 · Target IT/OT Convergence Architecture

05 · Target IT/OT Convergence Architecture

The target architecture must be conceived in layers, not as a product list. Its purpose is to ensure information is captured once, travels with context, can be consumed by multiple domains, and enables action. To achieve this, critical connectivity, edge computing, OT/IT integration, governed data, industrialized analytics, and transversal security must be combined.

Architecture principles:

- **Interoperability by design:** integrate through APIs, events, and shared information models, avoiding dependency on point-to-point connections.
- **Processing where it adds value:** control and low latency near the process; aggregation, governance, and scaling on common platforms.
- **Operational resilience:** controlled degradation, redundancies, continuity, and tested recovery for critical services.
- **Integrated industrial security:** identities, segmentation, monitoring, and secure remote access, without compromising process availability.
- **Data governance:** catalog, lineage, common semantics, and clear data product owners.
- **Multi-site scalability:** each implementation must be replicable without rewriting the architecture from scratch.

PRINCIPLE	WHAT IT REQUIRES IN PRACTICE	OPERATIONAL BENEFIT
Critical connectivity	Comprehensive coverage, mobility, traffic prioritization, and redundancies where criticality requires	Stable remote operation and lower exposure to outages that impact safety or production
Edge and hybrid cloud	Distribute loads based on latency, data sovereignty, and continuity	Better local response without losing analytical capacity and corporate scaling
Shared data	Common model of assets, locations, events, and states	Consistent traceability and analytics across domains and sites
Security by zones	Segment networks and access by process criticality	Smaller attack surface and better incident containment
Domain services	Define platform and digital product owners by process	Clear ownership, fewer ad hoc integrations, greater reuse

06

06 · Dimensions That Must Be Addressed

06 · Dimensions That Must Be Addressed

A mature convergence program cannot be limited to the technology layer. It must combine decisions on strategy, architecture, talent, governance, and adoption. The following view summarizes the dimensions that deliver most value when worked in a coordinated manner.

Structural dimensions of IT/OT convergence:

DIMENSION	QUESTIONS IT MUST RESOLVE	EXPECTED CAPABILITIES
Strategy and value	What business problems justify convergence and in what sequence	Prioritized portfolio by safety, continuity, productivity, and sustainability
Governance and architecture	Who decides standards, exceptions, investments, and technical debt	Architecture principles, decision committee, and common roadmap
Telecommunications	What level of availability, coverage, and mobility each process requires	Network treated as a critical asset with observability and SLAs by criticality
Resilient infrastructure	What must run at edge, what on common platform, and how to recover from failures	Hybrid capacity, redundancies, continuity, and obsolescence management
Data and interoperability	How to share context between mine, plant, maintenance, and corporate	Common data model, catalog, APIs, and data products
OT cybersecurity	How to protect processes, remote access, and third parties without affecting operations	Segmentation, identities, monitoring, response, and change discipline

Scaling and adoption dimensions:

DIMENSION	RECOMMENDED APPROACH	TARGETED OUTCOME
Analytics and AI	Industrialize models and not just pilot them; define owners, MLOps, and monitoring	Operable, auditable, and cross-site replicable use cases
Connected worker	Bring data, procedures, and collaboration to the work front with industrial mobility	Lower operational friction, improved safety, and faster response
Mindset shift	Move from the heroic expert who resolves by exception to the team that learns with data	Greater adoption, operational discipline, and continuous improvement capacity
Talent and capabilities	Mix profiles in operations, automation, data, cybersecurity, and product	Domain teams with a common language and shared responsibility
Ecosystem and sourcing	Manage providers under common integration and security standards	Less dependence on closed solutions and better lifecycle control

07

07 · The Connected Worker and the Mindset Shift

07 · The Connected Worker and the Mindset Shift

In many mining transformation programs, technology is defined in detail and adoption is left for the end. That approach usually fails. IT/OT convergence transforms how operators, maintainers, supervisors, and specialists interact with information and decision-making. For that reason, the human dimension is not a complement: it is a success condition.

The connected worker is not simply a user with a tablet or digital radio. They are a person who has access to timely data, digital procedures, remote collaboration, event traceability, and tools that reduce friction in their workday. When done correctly, safety improves, shift coordination is more robust, and decisions depend less on isolated knowledge and more on shared context.

TRADITIONAL LOGIC	TARGET LOGIC IN IT/OT CONVERGENCE
Individual experience resolves the exception	Experience is amplified with data, intelligent alerts, and digital procedures
Each area optimizes its own result	The mine-to-port chain is managed as an integrated value flow
Technology is perceived as support or reporting	Technology is understood as part of the operating system
Change is avoided to not affect continuity	Change is governed with tests, windows, and rollback to protect continuity
Decisions are validated at shift or day close	Decisions are adjusted with real-time information and actionable dashboards

CHANGE MANAGEMENT PRACTICES WITH THE HIGHEST RETURN

- **Co-design** use cases with operators, maintainers, and supervisors from the start — not only in final training.
- **Launch visible quick wins:** digital handover, mobile checklists, integrated permits, remote assistance, and actionable alerts.
- **Train by role and operational context:** cyber hygiene, data reading, industrial mobility usage, and exception response.
- **Measure adoption with real indicators:** daily usage, rework avoided, response times, incidents, and process compliance.
- **Work with line leaders and informal referents;** if the supervisor does not change the habit, the work front does not either.

08

08 · Governance Model and Recommended Operating Model

08 · Governance Model and Recommended Operating Model

The most effective operating model does not replace Operations with Technology, or subordinate OT to corporate IT. Instead, it creates a shared responsibility scheme. Operations retains priority on process and operational risk; OT contributes control discipline, automation, and asset continuity; IT contributes scalability, platform, integration, and transversal services; and data, cybersecurity, and digital product capabilities connect those worlds with a common framework.

DECISION DOMAIN	LEADS	CO-LEADS	SCOPE EXAMPLE
Value case priorities	Operations	IT/OT	Safety, continuity, productivity, energy, and logistics
Architecture and standards	Enterprise Architecture	OT and IT	Integration, data, edge, interoperability, and exceptions
Critical networks and connectivity	IT/Telecom	OT and Operations	Coverage, mobility, QoS, redundancies, and SLAs
Industrial cybersecurity	Cybersecurity	OT and IT	Segmentation, remote access, monitoring, third parties, and response
Data products and analytics	Domain owners	Data and business	KPIs, models, catalog, and solution operation
Changes in production environment	OT/Operations	IT	Windows, tests, rollback, maintenance, and versioning

In practice, this model is best operationalized through mixed teams by business domain, not by isolated technology. For example, a maintenance domain can bring together Operations, Reliability, OT, IT, Data, and Cybersecurity around a common capability portfolio. This approach reduces the classic handoff of responsibilities between areas and accelerates decisions on value and architecture.

09

09 · Suggested Roadmap

09 · Suggested Roadmap

Real convergence is built in stages. The sequence matters: it is not efficient to pursue AI at scale without resolving critical connectivity, observability, data governance, and security. The roadmap must combine technology foundations, high-impact use cases, and a change narrative that demonstrates early value without mortgaging the future architecture.

PHASE	HORIZON	MAIN OBJECTIVES	TYPICAL DELIVERABLES
0	0–3 months	Diagnose maturity and breakpoints	Asset inventory, silo map, network criticality, OT risks, and value case backlog
1	3–9 months	Define foundations and governance	Target architecture, standards, decision rights, remote access policy, and critical telecom plan
2	9–18 months	Build the common platform	Priority edge, domain integration, data catalog, observability, and first digital products
3	18–30 months	Scale use cases	Operable analytics, industrialized AI, connected worker, and integrated operation centers
4	30+ months	Optimize and standardize multi-site	Replicable capabilities, federated governance, and data-driven continuous improvement

10

10 · Indicators and Expected Results

10 · Indicators and Expected Results

Although each operation must define its own business case, mature IT/OT convergence typically reflects in a common set of indicators. It is worth measuring not only technology availability, but also operational adoption, decision velocity, and data quality.

INDICATOR	WHAT IT MONITORS	MATURITY SIGNAL
Critical network availability	Telecom continuity in priority processes	Differentiated SLAs by criticality and end-to-end visibility
Latency and loss in key zones	Real capacity to support remote operation and mobility	Continuous measurement and actionable thresholds
Data integrity and quality	Consistency across domains, labels, and events	Active governance and reliable data products
Time from detection to decision	Speed at which information becomes action	Sustained reduction between alert, validation, and response
Tool adoption by role	Effective usage by operators, maintainers, and supervisors	Habit change, not just technical deployment
OT cyber incidents and third-party exposure	Operational risk associated with connectivity and access	Smaller attack surface and better containment

NTT DATA

11

11 · Common Risks and Anti-Patterns

11 · Common Risks and Anti-Patterns

- **Confusing convergence with excessive centralization** and distancing decision-making from operational context.
- **Investing in AI or advanced platforms** without having resolved data quality, observability, and critical connectivity.
- **Extending corporate IT practices to OT** without respecting criticality, change windows, and functional safety.
- **Leaving cultural change for the final stage** and assuming training equals adoption.
- **Accepting closed integrations** that prevent reuse, multi-site scaling, or data sovereignty.

> **DIAGNOSTIC QUESTION** *Is your organization investing in higher intelligence layers before resolving the foundation of connectivity, governed data, and OT cybersecurity?*

12

12 · Conclusions and Message for Senior Leadership

12 · Conclusions and Message for Senior Leadership

IT/OT convergence in mining is a competitiveness agenda, not an ancillary technical project. Organizations that maintain functional silos, disconnected data, and insufficient networks will continue to face structural limits in advancing toward autonomy, resilience, and real-time decision-making. Those that build an interoperable platform and a common operating model will be able to scale safety, productivity, and agility with greater consistency.

The recommendation for senior leadership is clear: sponsor convergence as an enterprise capability, prioritize a mine-to-port architecture, treat connectivity as a critical asset, demand a shared governance model, and place the connected worker at the center of change. Technology enables; architecture orders; culture sustains. Only when all three dimensions align can mining move from digitizing through initiatives to operating as an integrated system.

> *"True IT/OT convergence does not seek to homogenize everything. It seeks to enable every process, asset, and person to interoperate securely, resiliently, and with business purpose. That is the real bridge between today's mine and the autonomous mine."* — NTT DATA · Mining & Resources, 2026

13

13 · Related Reading and Next Steps

13 · Related Reading and Next Steps

RELATED CONTENT IN THIS SERIES

- **Pillar 01 · The Floor: PISO Framework** — The four OT layers that must be active before IT/OT convergence can deliver value at scale: operational terrain, decision architecture, OT arsenal, and governance in motion.
- **Pillar 02 · The Intelligence: Causal Reasoning and Hybrid AI** — The reasoning architecture that operates on the integrated data infrastructure this document describes: how causal graphs and hybrid agents consume the connected operational picture.
- **Pillar 03 · The Organization: Tacit Knowledge as Critical Infrastructure** — The human layer of convergence: how expert operational knowledge is captured, structured, and made available to the connected workforce.

All content available at biztalksnttdata.com

NEXT STEPS

1. **Execute IT/OT maturity diagnostic:** map silos, network criticality, data quality, and OT risks at the pilot operation.
2. **Define value case portfolio:** prioritize by safety, continuity, and productivity with Operations, IT, and OT participation.
3. **Establish target architecture and governance:** formalize principles, standards, and decision rights before beginning implementation.

> *Connected mining is not built with isolated technology: it is built with architecture, governance, and people aligned toward a system that operates as one.*

NTT DATA · Mining & Resources · 2026 · biztalksnttdata.com · Pillar 04 · IT/OT Convergence

For information about IT/OT convergence programs at your operation, contact: Nelson Wilson, Partner - Head of Natural Resources · nwilsong@nttdata.com