MM-ISAC REFERENCE ARCHITECTURE

Mining Operational Technology

Public Overview and Design Principles

PUBLIC WHITE PAPER | V1.02 | AUGUST 2026

A sector-informed orientation for new mine projects and a target-state architecture for established mining and metals operators.

> **Governing principle.** Enterprise services should coordinate and aggregate. They should not become runtime dependencies for safe production. Every site should remain locally authoritative, capable of 30 days of independent operation, and structurally ready to be permanently severed from its parent enterprise.

Prepared by the Mining and Metals Information Sharing and Analysis Center

Vendor-neutral | Purdue-aligned | Designed for diverse mine and plant environments

Executive summary

Mining operational technology is not a single control network. It is a system of systems: fixed plant control, mobile and autonomous equipment, private wireless, process and security video, physical access control, vendor support, cloud analytics, enterprise applications and—increasingly—Integrated Remote Operations Centers (IROCs). These capabilities create value, but they also create dependencies and pathways through which disruption can reach production.

The MM-ISAC architecture establishes a common trust model from the enterprise to Purdue Level 3.5 while allowing each mine and plant to retain the technology and topology required below that boundary. The site OT DMZ is the protected services plane and local authority. It contains the identity, monitoring, data, controlled-access, change and recovery capabilities required to run independently.

The model assumes enterprise and cloud services will sometimes be unavailable. Thirty-day autonomy therefore includes more than the control system. A technically healthy plant is not operationally resilient if personnel cannot issue work orders, receive fuel, procure reagents, identify critical spares or reconcile transactions. The architecture couples local OT authority with continuity data, procedures, delegated authority and tested recovery for ERP, EAM/CMMS, logistics and supply-chain dependencies.

The mining operating context

- Sites are geographically distributed, frequently bandwidth-constrained and expected to operate safely despite loss of enterprise connectivity.
- Plant and mine environments have different control patterns; autonomous systems control belongs in Level 2, while fleet management, maintenance monitoring and legacy dispatch belong in Level 3.
- Private LTE/5G carries traffic for multiple logical zones, but the radio system is transport—not a Purdue zone and not a policy boundary.
- Vendors require practical access, but vendor networks must never become directly routed extensions of OT.
- Mines are acquired and divested regularly; separation must be an engineered lifecycle capability, not an emergency network redesign.

> **THE STANDARD TO DESIGN FOR** A site must fail local: retain local control authority, local visibility and local recovery; reject unsafe or stale external commands; and continue minimum viable operations for at least 30 days.

Contents

Reference Architecture at a glance

The diagram shows the common enterprise-to-site pattern. It is intentionally prescriptive above and through level 3.5, while leaving level 3 and below adaptable to site requirements

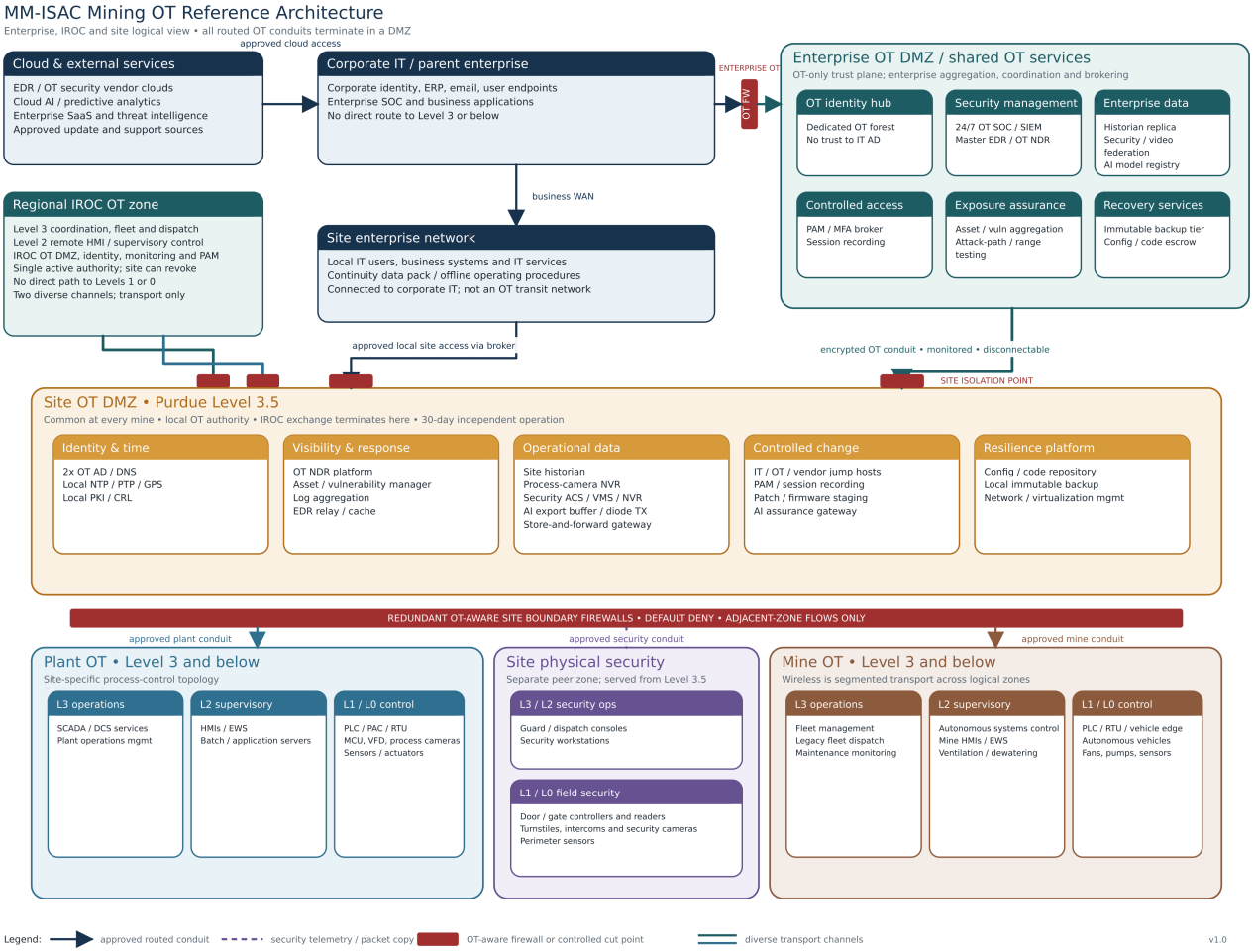

Figure 1. Enterprise, IROC, and site-local view. Every routed OT conduit terminates in a controlled DMZ

Zones, Boundaries and Local Authority

The enterprise and site OT DMZs have different jobs

The enterprise OT DMZ is a coordination and aggregation plane. It may host enterprise OT identity, central security management, replicated historians, exposure assurance and recovery services. It must not be a hidden runtime dependency for safe site operation, and corporate IT must not have a direct route to Level 3 or below.

The site OT DMZ at Level 3.5 is the operational boundary and protected services plane. It should be segmented internally—not implemented as one flat server VLAN—and sized to operate locally for at least 35 days so the 30-day requirement retains contingency. Typical local capabilities include OT identity and time, EDR relay/cache, passive OT monitoring, log aggregation, historian, access control, video management, remote access, patch and firmware staging, configuration escrow and immutable backup.

Below Level 3.5

Plant and mine zones remain site-specific. Level 3 contains operational management functions. Level 2 contains supervisory control, HMIs and engineering workstations. Levels 1 and 0 contain deterministic controllers, equipment gateways, safety logic, sensors, actuators and physical equipment. Process cameras remain with their plant or mine observation function; perimeter and building security cameras belong to a separate physical-security zone.

The boundary rules

- Use redundant, OT-aware firewalls at every Level 3.5 boundary. Apply default-deny policy and allow only documented adjacent-zone flows.
- Use OT-aware inter-zone firewalls where consequence and engineering risk justify them; validate inspection, failover and latency before production use.
- No direct enterprise, cloud, vendor, IROC or AI route may reach Levels 1 or 0.
- Provide a tested site isolation point, with local administration, local logging and a controlled reconnection procedure.
- Treat the site as the authority for control. Remote systems may request or coordinate; the site must be able to reject, revoke and continue locally.

ARCHITECTURE TEST

If removing the enterprise connection prevents safe production, local monitoring, identity, recovery or essential physical security, the service is in the wrong place or the continuity design is incomplete.

Security Capabilities That Make the Model Work

Segmentation alone does not produce a defensible operating environment. The architecture depends on a set of local, OT-designed capabilities that remain useful during isolation and are operated by people who understand both cyber risk and industrial consequence.

Know what exists and what it affects

Maintain an authoritative inventory of all OT assets: identity, owner, site, zone, addresses, device type, vendor/model, firmware or operating system, open ports and services, protocols, support status, vulnerabilities, backup status, remote-access paths and expected communications. Most importantly, relate each asset to the process, equipment, safety function and production consequence it supports. Passive discovery should be the default; any active method requires engineering approval.

Detect and respond locally

Windows and Linux systems at Level 3 and below should run OT-compatible endpoint detection or application control where supported, reporting to a local controller or relay in the site OT DMZ. Network devices should provide SPAN/TAP telemetry to a passive OT network detection and response platform. Local logging, time synchronization and retention must continue when cloud or enterprise services are unreachable.

Manage exposure without disrupting control

OT vulnerability management should combine inventory, passive protocol intelligence, vendor advisories, configuration context, exploitability and process consequence. Prioritize treatment by operational risk—not CVSS alone—and use compensating controls when patching is unsafe or unsupported. Conduct formal attack-surface assessments at least twice a year; continuous exposure monitoring is preferred.

Operate around the clock

Centralize governance and monitoring, but ensure the security function has genuine OT knowledge. Alerts affecting mining operations require 24/7 triage by OT-aware personnel, whether delivered internally or through an MSSP. Site operations, engineering and safety must retain clear escalation, containment and restoration roles.

FORWARD-LOOKING ASSURANCE

Frontier-model attack simulation may help identify what capable attackers can infer or chain together, but it belongs in a cyber range, digital twin or offline replica—not against live control systems.

Wireless, Vendors, AI and Remote Operations

Mine wireless is a shared transport underlay

Private LTE/5G often carries autonomous-haulage commands, fleet services, RoIP and safety communications across surface and underground operations. Separate those services with dedicated APN/DNN and VRF contexts, apply QoS appropriate to safety and control, and break traffic out locally through controlled security gateways. Routing and Purdue policy belong at those gateways—not inside the radio network. Wireless-management traffic requires its own protected context.

Vendor access is brokered, named and temporary

Provide isolated vendor access networks in both mine and plant environments. On-site and remote vendors should authenticate through the same Level 3.5 remote-access enclave using MFA, PAM, approval, jump hosts, named-target access, time limits and session recording. Vendor devices do not connect directly to OT, and approval to reach one target never creates general zone access.

AI has two deliberately different paths

For outbound predictive analytics, export approved historian or condition data through a hardware-enforced one-way gateway. For future Zone 2 input, use an AI assurance gateway at Level 3.5 and a site-local execution broker at Level 3. The exchange should carry signed, versioned, schema-constrained recommendations or bounded intent—not free-form commands or executable code. Validate provenance, units, ranges, confidence, freshness, replay, rate and approval policy. There is never an AI conduit to Levels 1 or 0.

IROCs are operating zones, not trusted extensions of a site

An IROC that supervises one or more operations is a distinct OT zone with its own DMZ, identity, monitoring and privileged-access controls. Each site connection uses two genuinely diverse transport channels, but those channels are communications underlays—not Purdue conduits. The application path still terminates at controlled OT boundaries. Only one authority is active for a function at a time; command freshness, site acceptance, revocation and observable link health are mandatory.

FAIL-LOCAL REQUIREMENT

Loss or degradation of the IROC must transfer authority to trained local personnel through a tested procedure. The site must be able to operate for 30 days without the remote centre and to permanently separate from it if ownership changes.

Thirty-day Operational Resilience

Cyber resilience in mining is not proven by keeping PLCs online. Production also depends on identity, maintenance records, fuel and reagent availability, receiving, inventory, work permits, technical documentation, communications, physical security and human authority. An outage that leaves the control system healthy but prevents the mine from obtaining diesel, grinding media, explosives, lime, cyanide or a critical bearing is still an operational outage.

Design the minimum viable operating mode

For every site-critical process, document the application, tenant, identity, network, API, data, provider, support and physical-supply dependencies. Define maximum tolerable outage, recovery objectives, minimum local dataset and accountable owner. The result should be a site continuity data pack that can be refreshed, protected and used without the primary enterprise environment.

What must remain available locally

- Current asset, configuration and network records; operating procedures; emergency contacts; vendor and support information; and locally usable identity and time services.
- Critical maintenance history, open and preventive work, bills of material, spare-parts location, minimum stock levels and the technical records needed to repair equipment safely.
- Reagent, fuel and consumable inventories; approved suppliers; specifications; lead times; receiving records; and authority to place emergency orders.
- Offline numbering, approval, receiving, inventory, labour and work-order processes, plus a controlled method to reconcile transactions after recovery.
- Local security monitoring, backups, configuration escrow, access-control authority, video retention and incident records.

Prove it

Exercise loss of enterprise applications, cloud identity, APIs, WAN and remote support at commissioning, after material change and at least annually. Run representative maintenance, procurement, receiving and inventory workflows with local people, data and authority. Recover into a non-production environment, reconcile offline records, restore interfaces in stages and verify that stale or duplicate transactions are rejected.

CAPACITY TARGET

Engineer local services, licences, certificates, storage, logs, video, backup, fuel and operational data for at least 35 days. The additional five days protect the 30-day objective from forecast error and recovery delay.

Permanent Severability

Mining portfolios change. Mines and processing facilities are bought, sold, placed into care and maintenance, restarted and transferred into joint ventures. An architecture that can isolate only for an incident is incomplete if it cannot be separated permanently and handed to a successor operator without destabilizing control or exposing the seller.

What the architecture should make possible

- Cut every enterprise, IROC, cloud and shared-service conduit at known, documented points while the site continues safe local operation.
- Transfer site-local identity, certificates, DNS, time, monitoring, backups, historian, access control, video, licences, repositories and administrative authority without reliance on the seller's corporate domain.
- Export a complete, usable record of assets, configurations, code, data, alarms, maintenance context, vulnerabilities, remote-access relationships and process dependencies.
- Replace parent-owned security, cloud and support services through defined transition interfaces rather than discovering hidden dependencies during the transaction.
- Revoke the former owner and its vendors, rotate secrets and certificates, establish clean monitoring baselines, and verify that no residual path or data flow remains.

Design choices that reduce transaction risk

Use site-specific namespaces, address plans and identity boundaries; maintain a register of shared services and ownership; keep licences and contracts traceable to their operating dependency; escrow configurations and automation code; and ensure each critical dataset has an exportable, documented format. Where enterprise platforms remain necessary, expose the minimum approved dataset through controlled interfaces rather than embedding site control in a corporate application.

Acceptance should be evidence-based

A divestiture readiness test should demonstrate local operation, clean isolation, successor access, data export, credential rotation, licence continuity, monitoring continuity and controlled reconnection to a new parent. Evidence should include dependency maps, inventories, configuration baselines, flow records, test results, ownership records and unresolved exceptions.

BUSINESS VALUE

Permanent severability reduces cyber exposure and transaction friction at the same time. It shortens separation planning, makes hidden dependencies visible, supports cleaner representations and warranties, and gives the buyer a site that can be operated and secured from day one.

From Reference Pattern to Operating Capability

The architecture is a target pattern, not a universal bill of materials. Sites differ in consequence, age, vendor support, topology and operating model. Adoption should therefore begin with dependencies and boundaries, then build the local capabilities that make isolation, recovery and transfer real.

A practical implementation sequence

1. Establish governance, accountable owners, OT engineering participation and the site's minimum viable operating mode.
2. Create the process-linked asset inventory and validate current data flows, remote paths, shared services and external dependencies.
3. Define zones and conduits; establish the enterprise OT DMZ, site OT DMZ, redundant OT-aware boundary firewalls and controlled isolation points.
4. Deploy local identity, time, passive OT visibility, endpoint protection, logging, remote access, historian, backup and configuration escrow.
5. Segment plant, mine, physical security, wireless and vendor access; validate safety, latency, failover and operational support.
6. Engineer IROC, cloud analytics and AI exchanges as bounded application workflows that fail local and never create direct reach to Levels 1 or 0.
7. Build and exercise the 30-day continuity data pack, offline business procedures, staged recovery and permanent-severability plan.
8. Operate the architecture: 24/7 OT-aware monitoring, passive vulnerability management, continuous exposure assurance, annual isolation testing and controlled change.

The destination

A mature operator should be able to point to every site and answer five questions with evidence: What does this asset support? Who can reach it? What happens when the enterprise disappears? How is authority returned locally? Can this operation be safely handed to another owner? A new mine should answer those questions before commissioning—not after the first incident, outage or transaction.

MM-ISAC POSITION

The strongest mining OT architecture is not the one with the most centralized technology. It is the one that creates common governance and visibility while preserving local authority, safe failure, operational continuity and a clean path to separation.

References

National Institute of Standards and Technology.

NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security. Primary guidance for OT architecture, segmentation, logging, remote access and availability.

International Society of Automation.

ISA/IEC 62443 Series of Standards. Zones, conduits, risk assessment, system security requirements and lifecycle responsibilities.

Cybersecurity and Infrastructure Security Agency.

Primary Mitigations to Reduce Cyber Threats to Operational Technology. Current baseline actions for OT exposure reduction and secure remote access.

National Cybersecurity Center of Excellence.

NIST SP 1800-10, Protecting Information and System Integrity in Industrial Control System Environments. Practice-guide examples for passive behavioral monitoring, allowlisting, integrity, identity and remote access.

Cybersecurity and Infrastructure Security Agency and international partners.

Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators. Asset inventory and taxonomy guidance supporting zone and conduit design.

ASD's Australian Cyber Security Centre, UK NCSC, Canadian Centre for Cyber Security, CISA and international partners.

Secure Connectivity Principles for Operational Technology. Current principles for OT connectivity, DMZ brokering, protocol/schema validation, data diodes, cross-domain solutions and isolation.

National Institute of Standards and Technology.

Artificial Intelligence Risk Management Framework (AI RMF 1.0). Lifecycle framework for governing, mapping, measuring and managing AI risk.

National Institute of Standards and Technology.

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Additional risk actions for generative and agentic AI, including governance, testing, provenance and incident handling.

National Institute of Standards and Technology.

AI RMF Profile on Trustworthy AI in Critical Infrastructure - Concept Note. Emerging critical-infrastructure profile under development; informative rather than a completed normative baseline in this draft.

ASD's Australian Cyber Security Centre and international partners.

Principles of Operational Technology Cyber Security. Safety-led OT principles emphasizing process knowledge, segmentation, supply-chain security and people with OT and cyber expertise.

ASD's Australian Cyber Security Centre, Canadian Centre for Cyber Security and international partners.
Creating and Maintaining a Definitive View of Your Operational Technology Architecture. Current joint guidance for an authoritative architecture record, passive monitoring, asset dependencies, exposure and safely controlled active discovery.

Canadian Centre for Cyber Security.
Joint Guidance: Foundations for OT Cyber Security - Asset Inventory Guidance for Owners and Operators. Canadian publication of the joint asset-inventory guidance and taxonomy for OT owners and operators.

Scope Systems, Important: Scope Systems Cyber Incident.
https://scopesystems.com.au/cyberincident/. Primary incident timeline for the May 2026 hosted ERP disruption, manual interim workarounds, restoration from backups and transaction reconciliation.

Canadian Centre for Cyber Security, Developing your IT recovery plan (ITSAP.40.004).
https://www.cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004. Guidance for recovery planning across incident response, business continuity and disaster recovery.

ASD's Australian Cyber Security Centre and CISA, Business Continuity in a Box.
https://www.cyber.gov.au/business-government/small-business-cyber-security/small-business-hub/business-continuity-in-a-box. Guidance for securely sustaining critical business functions when systems or data are unavailable or untrusted.

National Institute of Standards and Technology, SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.
https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final. Guidance for business impact analysis, recovery priorities, contingency strategies, testing and plan maintenance.

International Organization for Standardization, ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.
https://www.iso.org/standard/75106.html. Business-continuity management requirements for preparing for, responding to and recovering from disruption.

About the MM-ISAC

The Mining & Metals Information Sharing & Analysis Center (MM-ISAC) is an industry-owned, not-for-profit Information Sharing and Analysis Center serving the global mining and metals sector.

MM-ISAC brings together cybersecurity and operational technology professionals across the industry to share intelligence, strengthen resilience, and address sector-specific cyber risks. Through peer-to-peer collaboration, working groups, workshops, webinars, training, and actionable threat intelligence, MM-ISAC helps organizations of all sizes and maturity levels better prepare for and respond to cyber-related incidents.

Our Mission

To improve the resiliency of mining and metals organizations, preventing and minimizing the operational, safety, and environmental impacts of cyber-related incidents.

What we do

Threat Intelligence & Information Sharing
Timely, actionable intelligence shared across the mining and metals sector.

Incident Response & Collaboration
Supporting members before, during, and after cyber incidents.

Industry Working Groups
Practitioner-led collaboration addressing sector-specific challenges and developing practical resources.

Education & Training
Role-based education, workshops, webinars, exercises, and training focused on mining and metals.

Living Intelligence
Turning shared industry knowledge and experience into actionable, continuously evolving intelligence.

Connect with Us

Website:
MMISAC.ORG

E-Mail
INFO@MMISAC.ORG

LinkedIn
https://www.linkedin.com/company/mmisac/