MINERÍA · OT Y CONTROL DE PROCESO · VIDEOANALÍTICA

Videoanalítica en Minería: La Capa de Percepción que el Sistema de Control Necesita

Por qué la videoanalítica es la dimensión de percepción para el mantenimiento predictivo y la línea de defensa en seguridad de personas, y por qué su escalabilidad depende de la arquitectura de conectividad y de la ciberseguridad, no del modelo de visión.

AUDIENCIA
Planta, control/OT, confiabilidad y ciber

FOCO
Escalabilidad, ciber y conectividad privada

REGIÓN
LATAM

Contenido

01 El Sistema de Control No Puede Ver el Contexto 3

02 Lo que los Instrumentos No Miden 3

03 Una Cámara, Dos Funciones Críticas 4

04 Por Qué la Videoanalítica Muere en Piloto 5

05 Ciberseguridad: el Riesgo que Paraliza el Despliegue 6

06 Conectividad: el Factor Habilitador que se Subestima 7

07 Qué Verificar Antes del Próximo Piloto 8

08 Síntesis de Principios 9

09 Fuentes 10

01

EL SISTEMA DE CONTROL NO PUEDE VER EL CONTEXTO

Un gerente de planta con el que trabajamos opera un sistema de control avanzado de procesos (APC) de alta madurez. No buscaba otro tablero de monitoreo. Me lo planteó en una frase: quería darle ojos a su sistema de control. Su lazo, por bien calibrado que esté, optimiza lo que puede medir —temperaturas, presiones, flujos— y es ciego a todo lo demás: una correa que empieza a descentrarse, un rodamiento dos grados más caliente que sus pares, un derrame formándose bajo un chute, una persona ingresando a una zona que debería estar vacía. Le falta el contexto situacional que, en la práctica, es lo que detiene la producción.

Esa es la brecha real. La industria avanza aceleradamente hacia la autonomía y la optimización con inteligencia artificial, pero la capa que determina si la operación es segura y si los activos sobreviven sigue rezagada. La percepción para mantenimiento y seguridad avanza más lento que la IA operacional, y esa asimetría es el riesgo.

PRINCIPIO CLAVE — Un sistema de control avanzado es, por diseño, ciego al contexto físico que lo rodea. La videoanalítica es el mecanismo para darle percepción situacional, sin pedirle al lazo de control nada que no sepa hacer.

02

LO QUE LOS INSTRUMENTOS NO MIDEN

El control avanzado de procesos es un instrumento numérico: razona sobre flujos de sensores y actúa dentro de un modelo del proceso. Lo que no hace es ver. Un estudio reciente de visión por computador integrada al proceso en un tren de laminación de acero lo establece sin rodeos: los sistemas basados en sensores operan sobre datos de series de tiempo y no pueden evaluar visualmente lo que ocurre a la vista —un defecto de superficie, un

material fuera de norma, el lugar exacto donde una falla empieza a formarse—.[1] Para un VP de operaciones la consecuencia es simple: el problema casi siempre se ve antes de que aparezca en una tendencia, y hoy nadie en la sala lo está mirando.

La videoanalítica cubre ese espacio. Transforma cámaras que la planta ya posee en una capa de sensado que ve lo que los instrumentos no ven, y devuelve esa percepción a las personas y sistemas que actúan. No es vigilancia más sofisticada: es que el lazo de control gane la conciencia situacional que, por diseño, le falta estructuralmente, y vea la falla mientras todavía es barata de corregir.

03

UNA CÁMARA, DOS FUNCIONES CRÍTICAS

Una cámara con analítica cumple dos funciones simultáneas de alto valor, y ambas pesan en el resultado del negocio.

Mantenimiento Predictivo. El calor y el desgaste aparecen en cámara antes que en la tendencia. Hay trabajo revisado por pares sobre termografía de polines en correas transportadoras que detecta rodillos sobrecalentados con alta confiabilidad —la firma clásica de calor antes de falla— y los especialistas reportan que las anomalías térmicas afloran días o semanas antes de la falla mecánica.[2] Los modos de falla que una ronda humana de dos horas no detecta —una correa desalineada, una granulometría fuera de rango deteriorando el revestimiento de un chancador, una empaquetadura con fuga— son precisamente los que la visión continua captura. Un caso documentado por un proveedor de analítica (Razor Labs), sobre una flota de correas de mineral de hierro en puerto —usando sensores de vibración, no cámaras— puso la cifra sobre la mesa: del orden de 800 horas de detención no programada al año, valorizadas en decenas de millones de dólares, frente a fallas detectadas con más de tres meses de antelación.

Seguridad de Personas. En una operación donde se ha retirado la presencia humana del terreno, la cámara con inteligencia artificial se convierte en la primera línea de defensa, no en un respaldo. La interacción con equipo móvil es la principal causa de fatalidades en minería: los miembros del ICMM la identifican como el factor de riesgo número uno, y la mesa redonda EMESRT atribuye entre el 30 % y el 40 % de las muertes del rubro a fallas en los controles de interacción con vehículos. En Chile, el Reglamento de Seguridad Minera (DS 132 del Ministerio de Minería), que el SERNAGEOMIN fiscaliza, existe precisamente para proteger la vida y la integridad física de quienes trabajan en la faena; con quince fatalidades reportadas por el servicio en 2025 — el registro más alto desde 2018 —, la presión por reforzar el control de la interacción equipo-persona no es teórica.[3] Una cámara que monitorea la zona

[1] El estudio reporta que las anomalías visuales —defectos de superficie, problemas de material, la localización espacial de una falla en desarrollo— suelen preceder cualquier cambio medible en un parámetro del proceso.

[2] La termografía revisada por pares de polines reporta una precisión superior a 0,97 en la detección de rodillos sobrecalentados; el dato técnico no cambia la decisión ejecutiva, que es instrumentar la vigilancia continua.

[3] SERNAGEOMIN —Servicio Nacional de Geología y Minería— es el organismo que aplica y fiscaliza el Reglamento de Seguridad Minera en Chile, hoy en proceso de actualización. El DS 132 no se cita aquí por un artículo específico de

de exclusión cada segundo, en lugar de cada ronda de dos horas, es lo que se interpone entre una ruta de acarreo autónoma y una persona que no debería estar ahí.

PRINCIPIO CLAVE — Donde la presencia humana se retiró del terreno, la cámara con IA es la primera línea de defensa, no la última: vigila la zona de exclusión cada segundo, no cada ronda, sobre los mismos activos ópticos que ya hacen mantenimiento predictivo.

04

POR QUÉ LA VIDEOANALÍTICA MUERE EN PILOTO

Prácticamente toda operación minera ha ejecutado un piloto de videoanalítica. Muy pocas lo han escalado. La causa no es el modelo de visión: los modelos de detección son hoy la parte más madura de la solución. Los obstáculos reales son siempre los mismos tres:

- **Escalabilidad:** una demostración en una cámara, en un rincón de la planta, no prueba nada sobre cien cámaras transmitiendo inferencia a lo largo del sitio.
- **Interoperabilidad:** una detección que no cierra el lazo con el sistema de control o de mantenimiento no genera valor, genera ruido.
- **Ciberseguridad:** escalar sin una arquitectura adecuada expone la red OT[4] a vectores de ataque que los equipos de operación no están dispuestos a aceptar, y con razón.

Un piloto de una cámara no prueba ninguno de esos tres factores. Por eso no escala.

PRINCIPIO CLAVE — El modelo de visión no es el cuello de botella. La escalabilidad, la interoperabilidad y la ciberseguridad son los tres factores que deciden si un piloto se vuelve programa. Ahí, y no en el modelo, es donde muere la prueba de concepto.

detección de proximidad; se invoca como el marco chileno de seguridad minera dentro del cual se gestiona el riesgo de interacción equipo-persona.

[4] OT — Operational Technology, los sistemas de control e instrumentación que operan procesos físicos.

05

CIBERSEGURIDAD: EL RIESGO QUE PARALIZA EL DESPLIEGUE

Este es el factor que los equipos de operación y ciberseguridad señalan con mayor consistencia como el impedimento real para escalar. La ruta aparentemente más rápida para "escalar" una flota de cámaras es enviar los streams a una nube a través de internet público. Es también la forma más directa de entregar a un atacante las llaves del equipamiento que se pretende proteger.

La evidencia no es teórica. La botnet Mirai secuestró más de 600.000 dispositivos expuestos a internet, en su mayoría cámaras IP y routers alcanzables con una lista corta de contraseñas por defecto, y los convirtió en arma para derribar a un proveedor mayor de DNS, dejando offline una fracción significativa de internet. Claroty identificó en su análisis de exposición 2025 que la conducta más riesgosa en entornos industriales es conectar un dispositivo OT directamente a internet, y una proporción importante de las organizaciones sigue haciéndolo.

Aquí conviene desarmar la objeción que escuchamos en cada faena: "yo ya tengo CCTV; no voy a tocar mi red OT". El punto es exactamente el contrario. La videoanalítica que proponemos opera *sobre* las cámaras y los feeds que la planta ya tiene; no reemplaza la red ni la infraestructura de video existente, le agrega la capa de inferencia y la integra de forma segmentada. Lo que no se negocia no es la cámara: es el camino del dato. Una cámara mal segmentada —nueva o legada— es un punto de pivote hacia la misma red que gobierna el sistema de control, y ese es el escenario que los responsables de ciberseguridad no están dispuestos a aceptar. Es también el argumento que detiene proyectos que técnicamente funcionan.

> **PRINCIPIO CLAVE —** La videoanalítica opera sobre el CCTV que ya existe; no reemplaza la red OT, le añade inferencia segmentada. Lo que no se negocia es el camino del dato: una cámara expuesta es un vector de acceso lateral hacia el control, no un problema de privacidad.

06

CONECTIVIDAD: EL FACTOR HABILITADOR QUE SE SUBESTIMA

El segundo obstáculo estructural es la interoperabilidad, y es donde se gana o se pierde el valor. Una detección que enciende un tablero aislado, sin conectarse a ningún sistema que actúe, es ruido. El valor aparece cuando la detección cierra el lazo —hacia el sistema de control, el APC o el sistema de gestión de mantenimiento (CMMS)— de modo que un rodamiento caliente se convierte en una orden de trabajo y una persona en zona de exclusión se convierte en un enclavamiento, de forma automática. Detección sin integración es un proyecto de laboratorio.

La arquitectura de inferencia determina si esa integración es posible. La analítica crítica de seguridad —colisiones, intrusión, proximidad— debe correr en el edge: la respuesta se mide en decenas de milisegundos y el dato debe quedarse local. La analítica de mantenimiento, que observa tendencias de horas y días, puede agregarse a un servidor central en planta. Ambas exigen una red de alto ancho de banda, baja latencia y, lo no negociable, privada.

Por eso los operadores eligen redes celulares privadas sobre enlaces públicos y Wi-Fi. Newmont migró a 5G privado tras comprobar que no podía conectar de forma confiable más de dos máquinas a más de cien metros sobre Wi-Fi, y desplegó sus propios núcleos y SIMs para que solo su propio equipamiento accediera a la red. En LATAM el patrón ya está en terreno: la LTE privada de Nokia en la operación Minera Centinela de Antofagasta Minerals, en Chile, fue construida para transportar exactamente este tipo de tráfico controlado y de baja latencia. Son justamente los operadores con los que esta conversación tiene sentido —Codelco, BHP, Antofagasta Minerals— los que ya están resolviendo la capa de conectividad privada sobre la cual la videoanalítica puede por fin escalar.

Donde llega un backbone fotónico como IOWN[5] de NTT, el video y la inferencia agregados pueden comportarse como si fueran locales a través de largas distancias: sus metas al 2030 de 100x eficiencia energética, 125x capacidad y una reducción de 200× en latencia apuntan a un transporte que escala sin tocar nunca la internet pública.

PRINCIPIO CLAVE — No todo escala, y conviene decirlo: la analítica crítica de seguridad pertenece al edge y la de mantenimiento puede ir a un servidor central en planta, pero ninguna escala sobre internet público. El requisito habilitador es una red privada dimensionada para la flota completa, no para la demo.

[5] IOWN — Innovative Optical and Wireless Network, la iniciativa de NTT cuyo núcleo es la All-Photonics Network (APN), una arquitectura fotónica de extremo a extremo.

07

QUÉ VERIFICAR ANTES DEL PRÓXIMO PILOTO

No son las preguntas técnicas las que frenan estos programas; lo que hemos visto frenarlos es organizacional. Antes de comprometer recursos en una nueva prueba de concepto, vale la pena tener respuesta honesta a estas cuatro:

1. **¿Quién es dueño del presupuesto, y quién va a pelear por él?** La videoanalítica cae entre OT, confiabilidad y ciberseguridad, y cada área asume que es de otra. Hemos visto pilotos morir no por la tecnología sino porque ningún dueño claro defendió la línea presupuestaria cuando llegó el recorte. Defínelo antes de empezar.
2. **¿Qué área tiene poder de veto, y por qué lo usaría?** Ciberseguridad puede vetar la arquitectura; operaciones puede vetar cualquier cosa que toque la red OT. Si no sentaste a ciber en la mesa el día uno, vas a chocar el muro el día noventa. Haz que pongan su objeción sobre la mesa antes, no después.
3. **¿Qué pasa con el CCTV legado?** Casi siempre existe una base instalada de cámaras y una red que nadie quiere rehacer. El programa que escala es el que opera *sobre* ese parque existente y lo segmenta, no el que pide reemplazarlo. Si la propuesta empieza por "cambiemos las cámaras", ya perdió a operaciones.
4. **¿La detección cierra un lazo, y la red está dimensionada para la flota?** Si una alerta no se vuelve orden de trabajo o enclavamiento, compraste un tablero, no una defensa; y cien cámaras son un problema de ancho de banda y latencia cualitativamente distinto al de una sola cámara. Dimensiona para la operación que construyes, no para el piloto que muestras.

PRINCIPIO CLAVE — Lo que mata estos programas rara vez es el modelo de visión: es no haber definido quién paga, no haber neutralizado el veto de ciber temprano, y haber ignorado el CCTV que ya está instalado.

08

SÍNTESIS DE PRINCIPIOS

Los fundamentos de este artículo, cada uno sostenible de forma independiente.

1 Le pides al lazo de control que vea algo para lo que nunca tuvo sensores. La videoanalítica le da esa percepción usando las cámaras que ya tienes, no reemplazándolas.

2 El mismo activo óptico cumple dos funciones que rara vez comparten presupuesto: anticipa la falla mecánica y vigila la seguridad de personas. Quien las separa paga dos veces.

3 El marco de seguridad —ICMM, EMESRT y, en Chile, el DS 132 fiscalizado por SERNAGEOMIN— pone la interacción equipo-persona como el riesgo a controlar. Vigilancia continua, no rondas espaciadas.

4 El modelo de visión es la parte madura. El piloto muere en escalabilidad, interoperabilidad y ciberseguridad —y antes de todo eso, en quién es dueño del presupuesto.

5 Conectar una cámara a internet público convierte tu video en un vector de acceso lateral hacia la red de control. El camino del dato, privado y segmentado, no se negocia.

6 El interlocutor real es el operador que ya está construyendo su red privada —Codelco, BHP, Antofagasta Minerals—; sobre esa capa, y solo sobre ella, la videoanalítica escala.

09

FUENTES

Las fuentes públicas que respaldan las afirmaciones de este artículo.

- Process-Integrated Computer Vision for Real-Time Failure Prediction in a Steel Rolling Mill — arXiv, 2025. *Los sistemas basados en sensores operan sobre datos de series de tiempo y no pueden evaluar visualmente defectos de superficie o desalineamientos.*
- Automated identification of overheated belt-conveyor idlers in thermal images using CNN — Sensors (MDPI), 2022. *La visión térmica detecta polines sobrecalentados con alta confiabilidad.*
- Vehicle Interaction — 9 Layers of Defence — EMESRT. *Entre el 30 % y el 40 % de las fatalidades mineras se atribuyen a fallas en los controles de interacción con vehículos.*
- Reglamento de Seguridad Minera, Decreto Supremo Nº 132 de 2004, Ministerio de Minería — Chile, fiscalizado por SERNAGEOMIN. *Marco que protege la vida y la integridad física de quienes trabajan en la faena minera.*
- Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis — Cloudflare, 2017. *Más de 600.000 dispositivos, en su mayoría cámaras IP, usados para derribar a un proveedor mayor de DNS.*
- State of CPS Security: OT Exposures 2025 — Claroty (Team82), 2025. *Conectar un dispositivo OT directamente a internet es la conducta más riesgosa en entornos industriales.*
- Newmont on how private 5G changes mining — RCR Wireless News, 2025. *Por qué una red privada, y no Wi-Fi ni internet público, para equipo crítico en latencia.*
- Nokia & Antofagasta Minerals private network, Minera Centinela, Chile — Computer Weekly, 2022. *Red privada en LATAM transportando tráfico de flota autónoma con baja latencia.*
- Compañía líder de mineral de hierro reduce la detención no programada de su flota de correas en puerto — caso de estudio de Razor Labs. *~800 horas/año de detención no programada, >US$70M/año, fallas detectadas 3+ meses antes — vía sensado de vibración, no cámaras.*

Para más información sobre este tema, contacte a: ***Isabel Torres****, Intelligent Industry & OT, NTT DATA* · Isabel.TorresManquelafquen@emeal.nttdata.com.