

## Comunicaciones industriales en ambientes extremos

# Las redes críticas que no pueden fallar

**Polvo, humedad, vibraciones, interferencia electromagnética, corrosión, sismos y largas distancias obligan a repensar la conectividad industrial en Chile. En minería, energía, puertos y otras operaciones críticas, la robustez de la red dejó de ser un atributo técnico deseable para convertirse en una condición básica de continuidad operacional.**



Mailyn Calderón, UNAB.



Luis Garcés, AIE.

**E**n la industria, la digitalización suele asociarse a sensores, automatización, analítica o control remoto. Sin embargo, todos esos avances dependen de una capa menos visible, pero decisiva: las comunicaciones. Cuan-

do esa red debe operar en el desierto, en alta cordillera, en puertos expuestos a salinidad o en subestaciones con fuerte interferencia electromagnética, la exigencia deja de ser simplemente transmitir datos y pasa a ser resistir, recuperarse y seguir operando bajo condiciones severas.

A lo largo de todo su territorio, Chile ofrece varios de esos escenarios. La minería, por su escala y nivel de auto-

matización, es probablemente el caso más exigente. También lo son el sector energético, los puertos, la industria forestal y la acuícola, donde el aislamiento geográfico, la humedad, la corrosión o la criticidad del servicio elevan el estándar técnico. Mailyn Calderón, Directora del Magíster en Gestión TI y Telecomunicaciones e investigadora ITiSB de la UNAB, lo resume así: "Un ambiente extremo para las comunicaciones industriales es aquel donde las condiciones superan lo que soporta un equipamiento estándar y obligan a usar tecnología diseñada para alta robustez y continuidad operacional".

La definición parece amplia, pero en terreno es concreta. Una red industrial en alta cordillera puede enfrentar temperaturas de -40 °C; un gabinete expuesto al sol en el desierto puede llegar a 70 o 75 °C; una instalación portuaria debe convivir con alta humedad y salinidad, mientras una subestación de alta tensión exige inmunidad frente a perturbaciones electromagnéticas. Calderón advierte que en este tipo de aplicaciones "la resiliencia no se mide solo por velocidad, sino por la capacidad de mantener la operación continua y segura incluso ante fallas mayores".

### Cuando el entorno pasa a ser parte de los requerimientos

La diferencia entre una red para ambiente controlado y una diseñada para condiciones extremas está en la lógica de ingeniería. En una sala técnica o planta cerrada, el foco puede estar en eficiencia y costo. En una operación minera o







energética, en cambio, el diseño parte de la base de que el entorno atacará permanentemente a la infraestructura. Por eso, explica Calderón, “mientras en un ambiente controlado se optimiza el rendimiento, en uno extremo se diseña para resistir, mantener la continuidad operacional y tolerar fallas sin detener el proceso productivo”.

Esa exigencia se traduce primero en lo físico. Luis Garcés, Director de AIE y CEO de Intrónica, sostiene que en minería uno de los casos más complejos es la interferencia generada por los motores, donde “la alta vibración y el ruido interfiere en el cableado industrial que soporta las comunicaciones”. A partir de esa realidad, añade, el sistema debe responder a normas como TIA-1005, orientada a plantas industriales y ambientes severos, con requerimientos de cableado blindado y puesta a tierra para minimizar el impacto de las interferencias.

A ello se suma la protección frente al ingreso de polvo y agua. Garcés remarca que “el cableado industrial para sectores extremos no debe permitir el ingreso de material particulado y humedad”, por lo que en estos entornos se recurre a conectores, cajas y empalmes con grados IP67, IP68 o incluso IP69K. La IEC 60529 precisamente define el sistema de clasificación IP para grados de protección de

---

**En la industria chilena, la discusión sobre comunicaciones dejó de ser una conversación secundaria de TI. En ambientes extremos, la red es parte estructural de la seguridad, la productividad y la continuidad operacional.**

---

envolventes eléctricas frente al ingreso de agua y partículas.

También importa la química del entorno. En zonas costeras o con exposición a agentes corrosivos, Garcés advierte que debe reforzarse especialmente la protección de los puntos de contacto para evitar pérdidas de comunicación en faena.

**Normas, ensayos y clasificación del ambiente**

En este ámbito, la robustez no puede quedar a criterio del integrador o del fabricante; debe demostrarse. Calderón señala como referencias centrales la serie IEC 60068 para ensayos ambientales, IEC 60529 para grados de protección IP, IEC 61000 para compatibilidad electromagnética e IEC 61850 en subestaciones eléctricas. La IEC define a la norma 60529

como la del “IP Code” para clasificación de protección por envolventes, mientras que la serie IEC 61850 aborda las redes y sistemas de comunicación para automatización de servicios eléctricos.

En paralelo, Garcés destaca el marco TIA-1005A e ISO 11801-3, que incorporan la clasificación MICE para ambientes industriales según severidad mecánica, ingreso de partículas, condiciones climáticas/químicas y compatibilidad electromagnética. En esa escala, MICE 1 corresponde a un ambiente tipo oficina, MICE 2 a uno de exigencia intermedia y MICE 3 a un entorno industrial pesado. “Con esto se consigue cableado que puede funcionar, aunque se aplaste, se caliente, se sumerja o sea expuesto a productos químicos cáusticos”, señala.

Otro aspecto decisivo es la validación. Garcés subraya que el cableado de cobre





## 8 | COMUNICACIONES INDUSTRIALES

y los enlaces deben comprobarse con instrumentos capaces de medir el comportamiento en rangos de frecuencia definidos y compararlo con los estándares aplicables, incluyendo protocolos como PROFINET, EtherNet/IP, EtherCAT y Modbus-TCP.

### Redundancia: diseñar para que la falla no detenga la operación

Si el ambiente es agresivo, la falla no es una hipótesis remota, sino una probabilidad de diseño. Por eso, la redundancia y la tolerancia a fallos han pasado al centro de la arquitectura de red. Calderón explica que hoy “la redundancia se incorpora desde el diseño de la red”, evitando puntos únicos de falla mediante anillos o mallas, enlaces de respaldo por fibra o radio, sistemas eléctricos duplicados y UPS. Además, añade, se separan las redes más críticas para que un problema localizado no derribe toda la operación. Esto es particularmente importante en minería y energía, donde la continuidad 24/7 es intransable. En esos sectores, la resiliencia también debe considerar la condición sísmica del país, con fijaciones estructurales adecuadas, rutas físicas

diversificadas y continuidad energética posterior a un evento telúrico.

La propia ingeniería de red ha ido adoptando marcos específicos para ese objetivo. Calderón menciona, junto con IEEE 802.3, protocolos de redundancia como ITU-T G.8032 para protección en anillos Ethernet. Las guías de la UIT para G.8032 están precisamente orientadas a recuperación rápida frente a fallas en topologías en anillo.

### Lo que viene: IIoT, 5G privado, TSN y PoE industrial

El futuro de estas redes no apunta solo a mayor robustez, sino también a mayor inteligencia y densidad de conexión. Calderón prevé que “el futuro de las comunicaciones industriales en ambientes extremos estará marcado por redes más resilientes, inteligentes y distribuidas”. Entre los impulsores de esa evolución identifica la expansión del IIoT, las redes privadas 5G, el avance hacia 6G, y tecnologías como TSN y OPC UA, que permiten intercambio de datos sincronizado, seguro e interoperable entre sistemas industriales.

Desde la mirada de AIE, otra tendencia

relevante será la expansión del PoE industrial. Garcés destaca que esta tecnología permitirá energizar dispositivos IIoT por el mismo cableado de datos, reduciendo costos y evitando tendidos eléctricos convencionales en ciertas aplicaciones de monitoreo o seguridad. En la industria chilena, la discusión sobre comunicaciones dejó de ser una conversación secundaria de TI. En ambientes extremos, la red es parte estructural de la seguridad, la productividad y la continuidad operacional. Una falla en esa capa puede interrumpir procesos, dejar sin monitoreo activos críticos o impedir decisiones en tiempo real. Por eso, más que conectar equipos, hoy se trata de diseñar una infraestructura capaz de sobrevivir al entorno.

En esa tarea, Chile enfrenta una exigencia singular: automatizar y digitalizar en algunos de los ambientes más hostiles del continente. Y justamente allí, donde el polvo, la vibración, la distancia o la corrosión desafían a diario la operación, las comunicaciones industriales muestran su verdadero valor: ser la red invisible que sostiene la industria cuando el entorno juega en contra. ■