14
Octubre
Diciembre
2019

# AADECA

La Revista de
los Profesionales de
Automatización y Control

## Reporte especial:
## *Ciberseguridad y seguridad industrial*

- ¿Quién es el dueño de la ciberseguridad industrial? **Enrique Larrieu Let**
- Ciberseguridad industrial: el diseño integral es la base. ***Phoenix Contact***
- Estrategias para atender la ciberseguridad. ***Siemens***
- Visión práctica sobre la implementación de niveles de seguridad según la norma IEC 62443 en aplicaciones de control industrial. **Daniel DesRuisseaux, *Schneider Electric***

| Instrumentación | Control | Automatización | Robótica | IT Industrial | Elementos finales de Control |

# Expo2019 CVMNQN

## 1ª Exposición y congreso para el Cluster Vaca Muerta Neuquén

30 y 31/octubre y 01/noviembre 2019

**Espacio DUAM**, Acceso Aeropuerto, Ciudad de Neuquén

- Exposición de productos y servicios
- Jornadas de actualización técnica
- Foros de discusión para profesionales

*www.expocvm.com.ar*

Realización y organización:

EDITORES

Tecnoplús

SIEMENS

*Ingenio para la vida*


# Su conexión con la Empresa Digital

## Totally Integrated Automation Portal

Las innovaciones en materia de automatización hoy tienen una dirección muy clara: Industrie 4.0

Modelado digital, integración de la ingeniería al ciclo de vida de la planta, producto asociado al sistema de producción, integración horizontal y vertical completa, son algunos de los factores que Siemens asegura con la plataforma TIA Portal y todo su portfolio de equipos y sistemas en la vanguardia de la tecnología industrial.

siemens.com/tia-portal

Por
Ing. Sergio V. Szklanny,
Coordinador editorial AADECA Revista
Director SVS Consultores
Responsable grupo ACTI,
Universidad de Palermo

# Los nuevos temores industriales

La industria (como muchas otras actividades) fue siempre fuente de peligros: Incendios, explosiones y/o emisiones y contaminaciones peligrosas en industrias como las del gas y petróleo, petroquímicas, nucleares, mineras.

Los fenómenos naturales también son una fuente de peligro: terremotos, tsunamis, huracanes, hicieron (y hacen) lo suyo

Otras fuentes de peligro fueron los atentados y guerras: ataques con armas a zonas de producción, contaminaciones de aguas y sabotajes, etc.

Estos hechos fueron frecuentes en el siglo XX y, si bien siguen ocurriendo, los especialistas han tomado conciencia de la existencia de estos riesgos e hicieron desarrollos que permiten, en buena medida, mantener acotados los problemas y riesgos.

La instrumentación y el control de las plantas han evolucionado para enfrentar los temas mencionados: los sistemas instrumentados de seguridad (SIS) han resultado un claro avance en los temas de seguridad industrial. Las metodologías a usar durante la fase de diseño y a lo largo de todo el ciclo de vida de las plantas permite disminuir notablemente los riesgos. La toma de conciencia empresarial (en todos los niveles) hace que un accidente o una muerte en el trabajo impliquen fuertes repercusiones, tanto a niveles dramáticos en las personas colegas de trabajo del/los afectado/s, como a nivel de toda la estructura que cuida que estas situaciones sean lo menos frecuentes posibles.

Los fenómenos naturales y los ataques físicos son tenidos en cuenta en el diseño y funcionamiento de las plantas basándose en normas y buenas prácticas asociadas.

Lo novedoso del nuevo milenio, (y algo antes también) son los ataques asociados a la ciberseguridad, incluyendo en este término no solo los ataques remotos vía intrusión en redes digitales, sino también a través de ataques internos, (por ejemplo; razones de revancha o sabotaje). Hay decenas de ejemplos de ataques industriales (centrífugas enriquecedoras de uranio en Irán, plantas de agua países en África y Estados Unidos, ataques a infraestructura productiva en general)… Las estadísticas muestran un crecimiento exponencial mundial del que nuestra zona no está exenta.

La concientización en este tema no parece crecer al mismo ritmo. Y la especialización en ciberseguridad aplicada a las industrias de producción requiere de cuidados y conocimientos específicos que difieren de otros ámbitos de afectación.

Desde AADECA, hemos desarrollado jornadas y eventos asociados a este tema, y en este número de la *Revista de AADECA* prestigiosos especialistas desarrollan en el Reporte Especial sus puntos de vista. Por supuesto que hay más artículos por demás interesantes que esperamos que les sean útiles y puedan disfrutarlos.

Hasta el próximo número de la *Revista*.

**Edición 14**
**Octubre-Diciembre 2019**

Revista propiedad:
AADECA
Asociación Argentina de Control Automático

**Av. Callao 220 piso 7**
**(C1022AAP) CABA, Argentina**
**Telefax: +54 (11) 4374-3780**
***www.aadeca.org***

**Coordinador Editorial:**
**Ing. Sergio V. Szklanny, AADECA**

**Editor-productor:**
Jorge Luis Menéndez, Director
EDITORES
Av. La Plata 1080
(1250) CABA, Argentina
(+54-11) 4921-3001
info@editores.com.ar
**www.editores.com.ar**

EDITORES SRL es miembro de la Asociación de la Prensa Técnica y Especializada Argentina, APTA.

**Impresión**
Grafica Olfset
Santa Elena 328 - CABA

**R.N.P.I.:** N°5341453
**ISSN:** *a definir*

Revista impresa y editada totalmente en la Argentina.
Se autoriza la reproducción total o parcial de los artículos a condición que se mencione el origen. El contenido de los artículos técnicos es responsabilidad de los autores. Todo el equipo que edita esta revista actúa sin relación de dependencia con AADECA.
Traducciones a cargo de Alejandra Bocchio; corrección, de Sergio Szklanny, especialmente para *AADECA Revista*.



## En esta edición encontrará los siguientes contenidos

### Reporte especial — *Ciberseguridad y seguridad industrial*



## Además...

# Capacitación en AADECA

Nuestra Asociación Argentina de Control Automático se prepara para transitar el último trimestre del año con expectativa, y llevando adelante los cursos de capacitación dictados por profesionales especialistas del sector, y en miras a responder a las necesidades de la industria local.

El 28 de octubre, llega "Redes y comunicaciones industriales", a cargo de la ingeniera electricista Fabiana, Ferreira, directora del Departamento de Electrotecnia de la facultad de Ingeniería de la UBA.

El 4 de noviembre, el especialista Víctor Jabif, capacitado en Alemania y Brasil, será docente de "Introducción a la automatización con motores eléctricos".

El 9 de diciembre, "Energía solar fotovoltaica", a cargo de Pablo Di Pasquo, ingeniero con ocupación en altos cargos directivos en empresas vinculadas al tema, con estudios e investigaciones importantes llevadas a cabo tanto en nuestro país como en entidades educativas de prestigio del exterior.

Por otro lado, el 11 de noviembre, el ingeniero Gustavo Klein visitará la sede para ofrecer una conferencia introductoria gratuita sobre la ingeniería básica en instrumentación, control de procesos y automatización; un adelanto del curso sobre la misma temática que se llevará acabo el año próximo. ❖

## Nuestro actual Consejo Directivo (2018 – 2020)

**Presidente**: Marcelo Petrelli
**Vicepresidente 1º**: Ariel Lempel
**Vicepresidente 2º**: Víctor Matrella
**Secretario general**: José Luis del Río
**Prosecretario**: Cristina Boiola
**Tesorero**: Eduardo Néstor Álvarez
**Protesorero**: Carlos Godfrid
**Vocal titular 1º**: Carlos Behrends
**Vocal titular 2º**: Emiliano Menéndez
**Vocal titular 3º**: Raul Di Giovambattista
**Vocal supl. 1º**: Marcelo Lorenc
**Vocal suplente 2º:** Diego Maceri

## Socios adherentes

**Micro Automación | Cruxar | CV Control Editores | Emerson | Festo | Grexor Honeywell | Pepperl+Fuchs Arg. Schneider Electric Argentina Siemens | Supertec | Viditec**

## ¿Desea recibir AADECA Revista?

**Socios AADECA:** Gratis
**No socios:** Suscripción por 4 ediciones corridas, $450

**Más información, suscripcion@editores.com.ar**

# Velocidad y seguridad para el ensayo de soldaduras en cañerías

**CV Control**
*www.cvcontrol.com.ar*

Los sistemas convencionales de ensayo acarrean costos y riesgos elevados, como son las demoras y los tiempos muertos, la disposición de agua de desecho y las condiciones de trabajo potencialmente riesgosas. *EST Group*, una compañía de *Curtiss-Wright*, desarrolló el tapón de aislamiento *Grip Tight* para resolver estos desafíos reduciendo los tiempos de ensayo y mejorando, además, significativamente las condiciones de seguridad durante el trabajo en caliente.

*El sistema de mordazas está diseñado para un sello confiable y adhiere al principio "a mayor presión mejor agarre".*

## Aislación segura y confiable

El tapón de aislación *Grip Tight* es una solución en una pieza que aísla y controla con seguridad los vapores potencialmente explosivos o peligrosos aguas arriba de un trabajo de soldadura, y permite realizar el test hidrostático de la nueva conexión soldada.

El tapón de aislación cuenta con la tecnología de mordazas *GripTight*, un sistema probado a lo largo de más de veinte años de uso exitoso en los tapones de la empresa fabricante. El sistema de mordazas está diseñado para un sello confiable y adhiere al

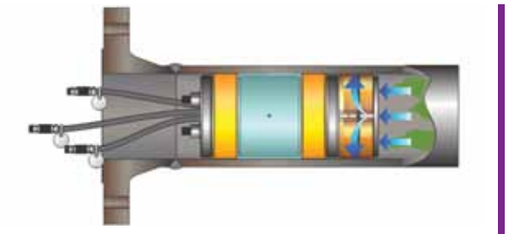


Imagen 1

principio "a mayor presión mejor agarre". Si una válvula defectuosa, o cualquier otro evento, causaran un rápido aumento de la presión aguas arriba del tapón, las mordazas se valen de esa presión para incrementar el agarre sobre la pared interna de la cañería. Las mordazas sostienen al tapón de aislación *Grip Tight* al tiempo que soportan una presión de línea de hasta 100 barg (1.500 psig), previniendo de este modo una falla que pudiera dañar la línea o lesionar al personal que realiza el trabajo.

## Sistema de dos sellos

El tapón de aislación *Grip Tight* está construido con la función de doble bloqueo y purga (DBB) que revoluciona la manera en que las conexiones son aisladas y testeadas. El tapón DBB tiene un puerto dual que permite que gas inerte o agua sean introducidos entre los sellos a través de un puerto de llenado. Al mismo tiempo, el aire es evacuado a través del puerto de venteo, resultando en una barrera segura entre el trabajo en caliente y cualquier gas residual aguas arriba.

Esta cavidad es presurizada y continuamente monitoreada. Cualquier descenso en la presión de la cavidad que puede indicar una pérdida, se detecta inmediatamente. Esto permite al operador detener la operación de soldado e inmediatamente atender la caída de presión para evitar una situación peligrosa.

El puerto dual también permite hacer circular agua u otro fluido entre los sellos, permitiendo

Imagen 2

mejorar la capacidad de enfriamiento tanto antes como después del procedimiento. Esta capacidad de enfriamiento puede mejorar la seguridad en áreas con restricciones de espacio donde el tapón debe ser colocado más cerca del área del trabajo.

## Ensayo de presión

Una vez que se ha realizado la soldadura y el área ha enfriado por debajo de los 82 grados centígrados, los sellos se aflojan y el tapón puede moverse para reposicionar la cavidad sobre la soldadura. El tapón se reinstala y presuriza para testear la integridad de la soldadura, hasta una presión de 155 barg (2250 psig).

De esta manera, los ensayos de presión se pueden llevar a cabo en tan solo diez minutos (10 min) desde la inserción del tapón hasta su retiro.

El tapón de aislación también permite realizar ensayos de presión con una cantidad de agua significativamente menor que los métodos tradicionales. Por ejemplo, utilizando un sistema tradicional de brida ciega para ensayar una soldadura en una cañería de doce pulgadas (12") de trescientos metros (300 m) de longitud, requeriría de aproximadamente 22.000 litros de agua para llenar la línea. Utilizar el tapón de aislación *Grip Tight* para misma situación solo requerirá menos de cuatro litros. Esto no solamente reduce drásticamente el volumen de agua potencialmente contaminada que hay que disponer, sino


Imagen 3.

que minimiza el tiempo total para realizar el ensayo y devuelve la línea a operación más rápidamente.

*Las mordazas sostienen al tapón de aislación Grip Tight al tiempo que soportan una presión de línea de hasta 100 barg (1.500 psig), previniendo de este modo una falla que pudiera dañar la línea o lesionar al personal que realiza el trabajo.*

## Confiabilidad y disponibilidad

Cada tapón de aislación se produce en una fábrica certificada ISO 9001:2015 y se diseña de acuerdo al Código ASME de Calderas y Recipientes de Presión. Los tapones satisfacen las normas ANSI N45.2 , NQA-1 y 10 y 10 CFR 50 anexo B.

Grip Tight está disponible para diámetros nominales desde ¾ a 48 pulgadas, e incluso se puede fabricar para tamaños mayores a pedido. Se construye con cuerpo de aluminio ligero y componentes de acero que lo hacen fácil de transportar, evitando la necesidad de grúas u otros métodos pesados de trasporte e izaje. Cada tapón de aislación se construye en forma estándar con sellos de uretano, pero están disponibles materiales alternativos. ❖

**Fuente: EST Group**

***EST Group* se especializa, desde 1968, en desarrollar y fabricar herramientas y sistemas que simplifican el mantenimiento de intercambiadores de casco y tubos y aeroenfriadores. También ofrece tapones de ensayo que mejoran la inspección in situ de cañerías, ductos y recipientes de presión. *EST Grup* esta representada en Argentina por *CV Control SA***

# Edge computing como ventaja competitiva

Por Rainer Brehm
Siemens
*www.siemens.com*

Rainer Brehm es ingeniero. Actualmente, se desempeña como gerente mundial de Factory Automation Products and Systems, para Siemens AG.

## Delineando el futuro de la automatización

Internet industrial de las cosas (IIoT) y la convergencia entre tecnologías de la información y tecnología operacional (IT/OT) fueron la base de la revolución en la manufactura industrial. No obstante, en la realidad, ciertas limitaciones prácticas pueden impedir el progreso. *Edge computing* (procesamiento en los dispositivos) emergerá como el facilitador de la manufactura inteligente que nos llevará al futuro de la automatización.

Ahora, ya se conoce el impresionante potencial de IIoT y, en todo el sector de la manufactura, la conectividad está creciendo en alcance y sofisticación. Aun así, adoptar formas inteligentes de operar ayuda a hacer mejoras adicionales y a eliminar deficiencias. Por ejemplo, los servicios en la nube ofrecen beneficios increíbles, sin dudas. Analizar los datos en una nube brinda nueva información sobre el proceso de producción o las máquinas para obtener más eficiencia y disponibilidad. Sin embargo, transferir los datos de y hasta la nube lleva mucho tiempo y, en algunos casos, no se justifica.

En la producción industrial, cada segundo cuenta. Aquí se necesita tener la capacidad de analizar y utilizar los datos para mejorar los resultados de la producción, rápido y de forma segura. *Edge computing* es una solución muy prometedora para cubrir la brecha entre la planta y la nube, es decir, les permite a los fabricantes aprovechar los beneficios de la nube, manteniendo el máximo grado de respuesta y flexibilidad que el mercado les exige.

## El próximo paso de la automatización

*Edge computing* ofrece una escalabilidad óptima a la arquitectura de IT de las aplicaciones que operan con datos, y combina los beneficios de la nube con las necesidades del fabricante para procesar los datos cerca de su fuente, a pie de la máquina. Las aplicaciones se pueden escalar eficientemente en todos los niveles. A pesar de que es una tecnología relativamente madura, aún faltan muchos años para que se masifique el uso de analítica también en ese nivel en la manufactura. Los pioneros en su adopción ya están activos y aplican *edge* en algunas partes de sus procesos.

A algunos les preocuparía tener que desechar sus sistemas de automatización existentes y reinvertir en nuevas tecnologías, pero eso no necesariamente ocurre. *Edge* es una tecnología complementaria, cubre la brecha que existe actualmente entre las máquinas y la nube y, por lo tanto, mejora ambos sistemas.

Hoy, los controladores como los *Simatic*, de *Siemens*, son la base para un amplio rango de conceptos de automatización. La tecnología *edge* expande los dispositivos de automatización para incluir análisis de datos y otras funciones, maximizando así los beneficios de Internet de las cosas (IoT) y aportando más flexibilidad y eficiencia a la fábrica. Para simplificar la implementación, la solución industrial *edge*, de la misma empresa, tiene un diseño compatible con la mayoría de las plataformas existentes, incluyendo las de otros fabricantes.

## Seguridad y protección

Algunos fabricantes tienen reservas sobre la conexión de sus equipos a la nube, por ejemplo, porque les preocupa la seguridad de los datos. Edge computing ofrece una etapa inicial ideal con una solución local, en el sitio, con la opción de escalar su funcionalidad paso a paso, tanto como se desee o necesite. Esto suma flexibilidad y es particularmente útil cuando hay mala conectividad.

Como las soluciones in situ se integran con el entorno local de las plantas de producción, requieren ser muy robustas en términos de ciberseguridad. También se puede lograr que, incluso el *back-end* de la infraestructura *edge*, que normalmente está en la nube, se instale de forma local. De este modo, la conexión con la nube solo sería necesaria para realizar actualizaciones u otras tareas específicas.

Como proveedor de tecnologías *edge* y en la nube, *Siemens* se compromete con la ciberseguridad y forma parte de la iniciativa *Charter of Trust*. Por lo tanto, los usuarios ya cuentan con una base sólida para abordar estas aplicaciones que aportarán valor al combinar la nube con *edge*.

## Análisis de datos en *edge*

Para la producción, el análisis de datos es clave para ayudar a los ingenieros de planta a monitorear el rendimiento de las máquinas. Los técnicos pueden enterarse de los posibles problemas antes de que ocurran y, en consecuencia, optimizar los cronogramas de mantenimiento para evitar tiempos de parada innecesarios.

Con *edge*, tener funciones como el procesamiento y almacenamiento de datos, la comunicación, e incluso, poder tomar decisiones cerca de los sensores (como fuentes de datos) mejora los beneficios del análisis porque tiene tiempos de reacción más breves (análisis en tiempo real), alto nivel de seguridad y mayor escalabilidad en términos de fuentes de procesamiento y tráfico de datos.

Además, las unidades de control (como los PLC) conectadas a dispositivos *edge* se benefician con una menor carga de trabajo de elaboración de datos.

Figura 1

Las infraestructuras *edge* son fácilmente escalables, los clientes pueden comenzar con una inversión pequeña y ver los resultados antes de expandirse. El objetivo principal de *Siemens* es que la analítica en *edge* sea lo más sencillo posible de usar para que sea compatible con la experiencia y el saber-hacer de los clientes.

## Combinando *edge* y la nube

Tanto *edge*, como la nube, serán cada vez más indispensables en más sectores de la manufactura porque reducen el costo de implementación, incluso para compañías pequeñas y medianas.

Un aspecto clave será hallar la combinación óptima de *edge* y la nube, ya que ambas tecnologías se complementan. A partir de los análisis realizados en nivel computacional de *edge*, por ejemplo, se optimiza el algoritmo de inteligencia artificial en la nube y las mejoras luego se descargan nuevamente en la infraestructura *edge*.

Los dispositivos *edge* de *Siemens* que los usuarios instalen se pueden administrar con la infraestructura central *Edge Management System*. Este sistema permite, no solo controlar el estado de todos los dispositivos conectados, sino también instalar y actualizar las aplicaciones y el software, y transferir las funciones de la nube al sistema de manufactura local como se desee.

La nube tendrá un rol fundamental en el futuro. Los beneficios de *edge* —en especial, su gran compatibilidad, el alto nivel de seguridad y su impacto en la escalabilidad— implican que los servicios de la nube pueden ser accesibles y administrables para más compañías. Seguramente demuestre ser el catalizador de la transformación digital de la industria de la manufactura en su totalidad. ❖

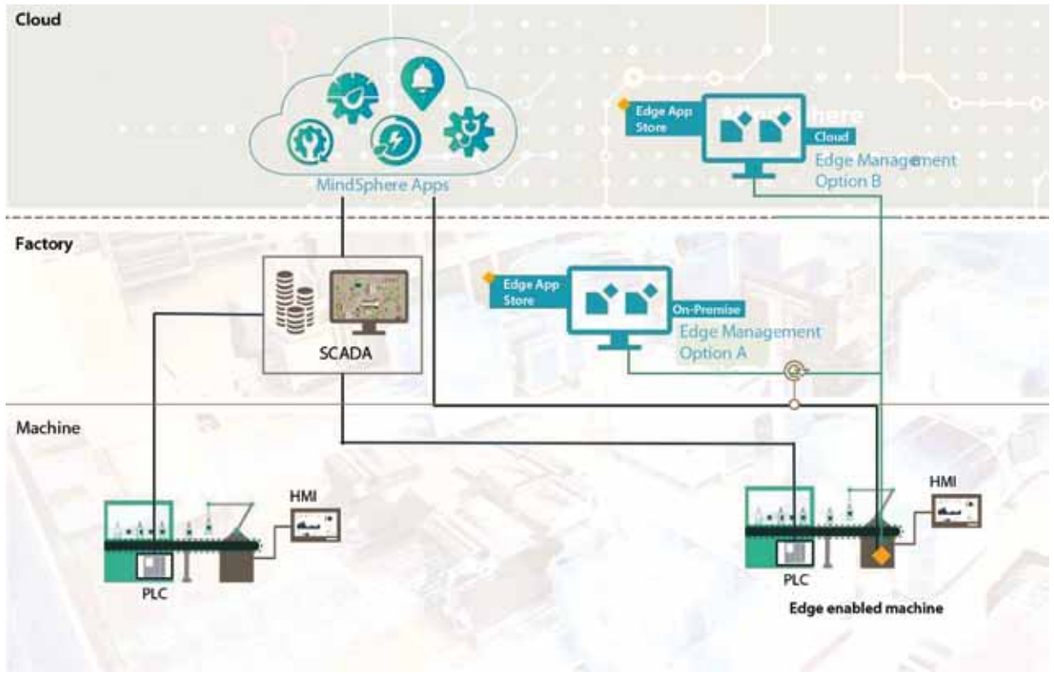



Figura 2

# ¿Quién es el dueño de la ciberseguridad industrial?

Conflicto y acciones de la ciberseguridad en la industria

**Enrique Larrieu Let**
*elarrieulet@gmail.com*

Enrique Larrieu-Let es ingeniero, CISM, profesional de seguridad y tecnologías de sistemas de información. Miembro de la Asociación de Auditoría y Control de Sistemas de Información. ADACSI, IAIA, Universidad del Salvador.

En materia de ciberseguridad industrial, no creo que nadie se sienta con derecho a tener toda la verdad y todas las respuestas a las posibles amenazas y ataques, y también creo que todos lo saben. Pero entonces, ¿quién debe ocuparse del tema y hacerse responsable?

*Las diferentes prioridades de IT y OT son la causa de los conflictos entre ambos grupos.*

## La situación

Observamos un cambio significativo en estas infraestructuras que evolucionaron de sistemas monopólicos y monolíticos aislados a configuraciones de mercado abierto integradas al resto del mundo. Este cambio de paradigma permite proporcionar al usuario final servicios más efectivos, eficientes, centrados en el usuario y fáciles de usar, con una reducción significativa de los costos. Sin embargo, esto las expone a una gran cantidad de amenazas peligrosas potenciales.

Esto se debe a que el escenario socio-técnico actual comienza a caracterizarse por un gran aumento en las interacciones y especialmente de las dependencias (recíprocas) entre las diferentes infraestructuras.

Este fenómeno contribuye severamente a aumentar la complejidad de todo el escenario que, si bien es más robusto a los eventos de bajo impacto y de alta frecuencia, aparece cada vez más propenso a fallas sistémicas y catastróficas como lo demuestra la estadística de incidentes en el mundo.

## Prioridades de seguridad

Las diferentes prioridades de IT y OT (tecnologías de la información y tecnologías operacionales) son la causa de los conflictos entre ambos grupos, y eso se explica porque tienen objetivos diferentes, como lo muestra la figura 1, ya que IT tiene a las TIC (tecnologías de la información y la comunicación) y OT tiene a los ICS (soluciones de información y comunicación).

La principal prioridad de TI es proteger los datos. Sin embargo, la prioridad de OT es proteger la disponibilidad e integridad del proceso con énfasis en la seguridad de las personas y la planta, la confidencialidad queda en el último lugar.

Cada grupo tiene una lente sesgada cuando considera los riesgos y consecuencias en ciberseguridad.

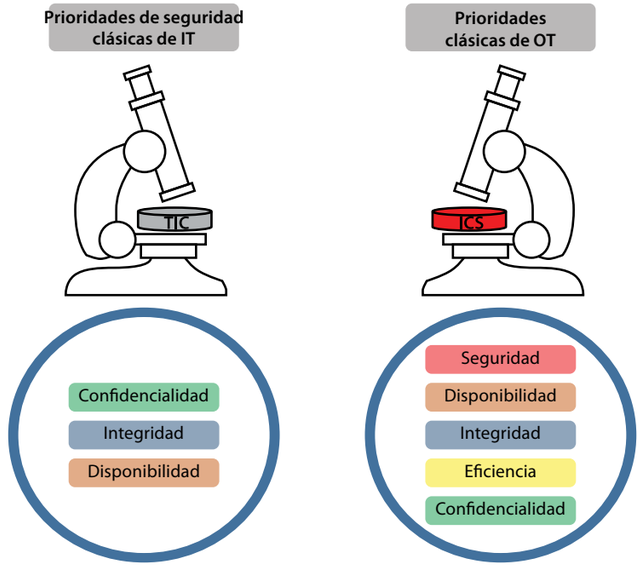



**Figura 1. Propiedades clásicas de IT y OT**

## El conflicto

Ambos mundos, el de IT y el de OT, vivían felices y contentos cuando cada uno se ocupaba de lo suyo sin interacciones ni físicas ni virtuales.

Pero el entorno, de la mano de la tecnología, creó demandas sociales y comerciales que los obliga a vincularse y, como en toda convivencia, surgen los conflictos. En este caso, totalmente justificados dado que, si bien la protección de la información es importante, las pérdidas de producción que se traducen inmediatamente en pérdidas comerciales también lo son.

Pero el conflicto es aún peor porque, no solo es por diferencia de intereses, sino que además existe una doble desconfianza entre ambos, tanto en lo operativo, como en los riegos.

En cuanto a lo operativo, por lo general, los equipos de OT dudan en aceptar los cambios de IT en el entorno operativo por resistencia a detener la producción de manera planificada o temor de que se produzca una interrupción prolongada causada por un problema con la implementación. Y en cuanto a los riesgos, las amenazas cibernéticas provenientes por conectarse a IT también pueden interrumpir la producción, causar daños, afectar la visibilidad y el control o poner en peligro la seguridad de la infraestructura, las personas y el medioambiente, además, por supuesto, de afectar la rentabilidad del negocio. Y por otra parte las vulnerabilidades de los ICS hacen temer a IT que los ciberdelincuentes penetren por allí para robar secretos comerciales.

Todo esto es cierto y posible y ya lo sabemos. Veamos ahora algunas acciones para comenzar a mediar entre ambos y minimizar los impactos del conflicto.

## Acciones

Desafortunadamente, los consultores que realizan evaluaciones de riesgos en entornos de operaciones de ICS dicen que muchas organizaciones deben experimentar un ciberincidente de alto impacto antes de estar dispuestas a tomar medidas significativas.

Entonces, ¿cuáles son las acciones posibles que una organización industrial podría tomar para facilitar la convivencia de IT y OT y minimizar el impacto de los conflictos y la desconfianza y al mismo tiempo aumentar la seguridad de los ICS?

*Si bien la protección de la información es importante, las pérdidas de producción que se traducen inmediatamente en pérdidas comerciales también lo son.*

### Establecer una alineación estratégica en los niveles más altos

La mayoría de las industrias aún poseen dos áreas fuertemente disociadas de operaciones y de tecnología de la información. Tienen diferentes personas, objetivos, directivas y proyectos.

Para mejorar esto, se recomienda desarrollar (si no la tiene aún) una estrategia de ciberseguridad para toda la organización, y que se encuentre alineada con la estrategia global del negocio para que sirva y agregue valor a las necesidades de este.

Cumplido este requisito indispensable, se debe comenzar reorganizando los departamentos de IT y OT, para que estén estratégicamente alineados y unificados con la estrategia global de ciberseguridad. Se sugiere que, como mínimo, el director de información (CIO), el director de seguridad de la información (CISO) y el director de operaciones (COO) tenga objetivos y metas parcialmente comunes y alineadas, lo que los obligaría a trabajar de manera cooperativa.

El CIO y el CISO también deben aceptar la responsabilidad total de la ciberseguridad del ICS y de cualquier incidente de seguridad, incidentes de integridad o fallas o daños al equipamiento e instalaciones causados directa o indirectamente por incidentes cibernéticos.

### Coordinar un equipo de trabajo conjunto

El NIST (Instituto Nacional de Normalización y Tecnología, dependiente del Departamento de Comercio de Estados Unidos), en su documento SP800-82r2, recomienda crear un equipo de trabajo conjunto, como un equipo de ciberseguridad multifuncional y multidisciplinario, para compartir su variado conocimiento y experiencia, con la finalidad de evaluar y mitigar el riesgo para los ICS.

En el documento, además, se sugiere designar específicamente algunos cargos que deberían ser parte de este equipo de trabajo de ciberseguridad: un miembro del personal de TI, un ingeniero de control, un operador del sistema de control, un experto en seguridad de redes y sistemas y un miembro del departamento de seguridad física.

*Se debe comenzar reorganizando los departamentos de IT y OT, para que estén estratégicamente alineados y unificados con la estrategia global de ciberseguridad.*

### Proyectos piloto

Una de las primeras cosas que puede hacer el grupo de trabajo conjunto de ciberseguridad es identificar proyectos piloto simples para trabajar vinculados. Una sugerencia podría ser crear de mutuo acuerdo una lista de los activos de ICS más críticos que deben estar absolutamente protegidos, clasificarlos en orden de prioridad y evaluar sus riesgos e impactos, para luego comenzar a implementar acciones de monitoreo y control en ciberseguridad.

Estos proyectos piloto brindarán valor al negocio, ayudando a la organización a capacitarse y desarrollar progresivamente una suite específica de habilidades compartidas de IT/OT. Esto también ayudará a determinar cómo minimizar los impactos del conflicto al estar motivados a decidir de manera consensuada los pasos hacia la mejora de la ciberseguridad de los ICS.

### Gobierno de las tecnologías

Una cosa es la gestión y otra, el gobierno de las tecnologías en general y de la ciberseguridad en particular.

Mientras que la gestión debe recaer en cada área de trabajo de IT y OT, el gobierno debe recaer en el equipo conjunto de ciberseguridad, que debería tener autoridad para ejecutar proyectos, armonizar sistemas y procesos y promover el desarrollo de las habilidades interdisciplinarias necesarias para proteger los ICS y satisfacer las necesidades del negocio a la vez.

## Conclusión

La mitigación exitosa de los conflictos inherentes a la convergencia de IT y OT, y la posterior mejora de la seguridad de ICS, no ocurre de la noche a la mañana. Este es un desafío complejo para cualquier organización. Los gerentes deben aprender a compartir objetivos, evaluar conjuntamente los riesgos y hacer frente a los impactos en el negocio juntos. Para esto, se requiere de mucho trabajo previo de concientización y de capacitación para cambiar conductas que conduzcan a productos, procesos, políticas y personas de seguridad de ICS apropiados. ■

# Instrumentación precisa para áreas peligrosas

Calibrador Ex, calibrador y registrador de presión y temperatura, e higrómetro: tres equipos de medición para áreas industriales peligrosas

Ing. Capino
*www.ingcapino.com.ar*

En este artículo, la descripción de tres productos comercializados en el país por *Ing. Capino*, para tareas de medición en áreas peligrosas, con presencia de gases explosivos, corrosión, polvos, agua, etc. Los tres, de diversas marcas representadas por la firma, están construidos satisfaciendo los requisitos más exigentes de calidad y funcionamiento de orden internacional. Asimismo, destacan por la precisión en sus valores.

## Calibrador Ex: *MC6-Ex*, de *Oy Beamex ab*

El *MC6-Ex* es un calibrador avanzado de campo multifunción e intrínsecamente seguro con certificación ATEX e IEC y clasificación Ex ia IIC T4 Ga. Está diseñado para usar en entornos potencialmente explosivos tales como plataformas petrolíferas y de gas offshore y on-shore, refinerías de petróleo o plantas químicas y petroquímicas. Asimismo, puesto que su carcasa posee grado de protección IP 65, contra polvo y agua, el equipo es idóneo para entornos húmedos y polvorientos sometidos a cambios de temperatura.

Es un equipo con cinco modos de operación distintos, lo que hace que sea muy rápido y fácil de usar, y que el usuario tenga que llevar menos equipos a campo. Los modos de funcionamiento son: medidor, calibrador, calibrador-documentador, registro de datos y comunicador Fieldbus. Lleva a cabo funciones de medición, generación y simulación de voltaje, corriente, frecuencia, termopar, resistencia, termorresistencia, pulsos; contador de pulsos; detección del estado de contactos; fuente de alimentación interna.

Contiene un comunicador de bus de campo (fieldbus) completo para instrumentos que sean compatibles con Hart, Foundation Fieldbus y Profibus PA; incluso se pueden instalar simultáneamente los tres protocolos. En su memoria, el equipo guarda las distintas bibliotecas de los instrumentos con bus de campo.

Además, se comunica con un software de gestión de calibración, lo que permite realizar y documentar las calibraciones de una forma totalmente automatizada y libre de todo uso de papel.

Por último, se destaca la pantalla táctil a color con alta resolución y retroiluminación ajustable y el teclado de membrana.

## Calibrador y registrador de presión y temperatura: *nVision*, de *Ametek Calibration*

Con certificaciones ATEX, IEC, IECx, CE, CSA y DNV, entre otras, para áreas peligrosas (resistente a ataques químicos agresivos y corrosión), este calibrador y registrador de presión es lo suficientemente preciso como para reemplazar una balanza de peso muerto, lo suficientemente robusto como para sumergirse bajo un metro de agua, y fácil de usar y portátil, para llevarlo a realizar calibraciones a cualquier lado.

El equipo cuenta con indicadores led que indican el estado de data logger y sobrepresión, así como un puerto miniUSB de fácil acceso.

En su amplia pantalla retroiluminada, permite visualizar las mediciones gráficamente, con o sin una computadora, en tiempo real, y es capaz de almacenar más de un millón de mediciones.

Calibrador Ex: *MC6-Ex*

Además, es fácil de usar y rápidamente se puede cambiar de un módulo a otro para llevar a cabo las tareas de medición. El módulo para medir presión (relativa, absoluta o diferencial), opera en rangos de hasta 15.000 psi, 1.000 bar y 100 Mpa, con una precisión de 0,025 por ciento de la lectura.

Para la medición de temperatura (PT100), el rango va de cero a cuatrocientos ohmios (0-400 Ω), con resolución de 0,01 en todas las escalas. Opera con diversas unidades (°C, K, °F, R, Ω), en conexión con dos, tres y cuatro hilos.

El módulo para medición de voltaje responde en un rango de cero a veintiocho voltios en continua (0-28 Vcc) con una resolución de 0,001 voltios. Para medición de corriente, el rango es de cero a 55 miliamperes, con resolución de 0,001 miliamperes.

Dadas sus prestaciones, se puede aplicar para placas orificio, prueba de filtros, transmisores diferenciales, medidores de gas rotativos, válvulas de seguridad, reemplazo de la balanza de peso muerto, calibración y mantenimiento o reemplazo de registradores de carta, solo por mencionar algunos de sus usos.


Calibrador y registrador de presión y temperatura: *nVision*

### Medidor de punto de rocío avanzado: *MDM300*, de *Michell Instruments*

El *MDM300* es un higrómetro para determinación de punto de rocío, óptimo para mediciones o chequeos rápidos de punto de rocío o contenido de humedad en diferentes aplicaciones, incluyendo aire comprimido, gas natural, gas de aislación de contactos de alta tensión. Este equipo posee certificaciones ATEX, IECEx, FM, CAS, GOST e INMETRO y permite realizar una mayor cantidad de mediciones por hora gracias a su rápido tiempo de respuesta y la larga duración de la batería. Asimismo, cuenta con entrada para sensor externo de cuatro a veinte miliamperes (4-20 mA) para calibración y validación.

En base a su principio de medición de sensor cerámico de la propia empresa fabricantes, opera con gran variedad de unidades de medición de temperatura, punto de rocío, presión, gas natural, etcétera, con un nivel de precisión destacable: un grado de punto de rocío (1 °Cdp) dentro de un rango amplio comprendido entre -60 y veinte grados (-60-20 °Cdp). Todos los instrumentos se entregan con un certificado de calibración en trece puntos, trazable al NPL (Reino Unido) y NIST (Estados Unidos).


Medidor de punto de rocío avanzado: *MDM300*

Este instrumento es liviano (pesa menos de 1,5 kilos), se presenta en kits para diferentes aplicaciones con una caja de transporte sólida pero ergonómica, y su interfaz permite un uso práctico y confortable en los ambientes industriales más agresivos.

### Acerca de *Ing. Capino*

*Ing. Capino SRL* es una compañía nacional fundada en el año 1978 por el ingeniero Osvaldo H. Capino, orientada totalmente al mercado de instrumentación y control automático. Actualmente, cuenta con una planta productiva de 1.200 metros cuadrados, ubicada en la localidad de Villa Ballester (provincia de Buenos Aires) que ocupa a veinte personas en forma directa para desarrollar las actividades de comercialización, fabricación, calibración y administración.

La firma representa en el país empresas internacionales como *Baumer*, *Beamex*, *Ametek Calibration*, *Michell Instruments* y *Bopp & Reuther*; además, integra un mix de productos con una línea de producción y armado, lo cual permite ofrecerles a los clientes productos personalizados, acordes a sus instalaciones y requerimientos

En sus más de cuarenta años, se ha especializado en industrias como gas y petróleo, siderúrgicas, alimentos y bebidas, farmacéutica, generación de energía, nuclear, automotriz, petroquímicas y mineras. La provisión de instrumentos (entre los que se cuentan manómetros, termocuplas, termorresistencias, transmisores de presión, presostatos, termómetros bimetálicos, calibradores de presión y temperatura, calibradores multifunción y software de gerenciamiento de calibraciones) se complementa con servicios como calibraciones en laboratorio propio de metrología (con patrones de última generación), calibraciones in situ, capacitación y workshops. ❖

# La visión de rayos X

Una fractura complicada en la pierna, un implante dental o una incomodidad en la columna: en medicina, la tomografía computada se usa con frecuencia para crear imágenes del cuerpo humano. Esto facilita el diagnóstico y el tratamiento. La tomografía computada también se usa en la industria. Puede mostrar de manera no destructiva el interior de componentes, lo que beneficia tanto el aseguramiento de la calidad como la reconstrucción de los componentes.

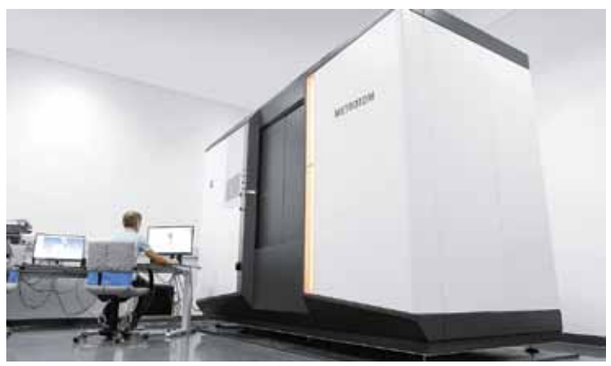
**Festo**
*www.festo.com*

Un equipo bien conocido por los doctores en cirugías y hospitales: el tomógrafo. Sin embargo, este equipo se puede usar no solo para analizar huesos y órganos, también juega un rol importante en la industria, al proveer imágenes detalladas de la estructura interna de los componentes sin tener que desmantelarlos.

## Medición, análisis y reconstrucción

Un área principal de aplicación del tomógrafo es para la medición y para el aseguramiento de la calidad. Por ejemplo, los tomógrafos se pueden usar para determinar la calidad de fundición del aluminio, para chequear la porosidad y para calcular las dimensiones de los componentes. En caso de componentes inyectados en plástico, se puede determinar si hay no deformaciones. También se pueden examinar grupos enteros de componentes.

Otra área es la ingeniería inversa, mediante la cual se reconstruyen componentes para los cuales no hay un modelo CAD disponible. La tomografía genera los llamados datos STL de los componentes.



El formato STL representa la superficie de cuerpos 3D con triángulos. Los archivos STL se pueden usar para crear modelos CAD de los componentes, que no existen aún

El formato STL describe la superficie de las partes analizadas en forma de triángulos. Estos se pueden usar con reglas geométricas en el diseño de ingeniería para generar nuevos modelos CAD.

## Visión completa con un solo escaneado

El tomógrafo toma una gran cantidad de imágenes 2D de con rayos X. El volumen tridimensional se calcula, luego, a partir de los datos y en una computadora. Al mismo tiempo, se pueden remover los artefactos de con distorsión (falsificaciones). Un volumen generado con esta técnica es más claro en comparación con la imagen de rayos x de sobreimposición de capa sobre capa.

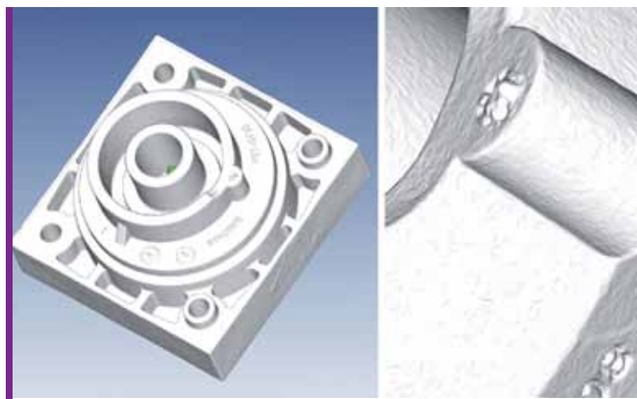
La fuente de rayos x y el detector están fijos en el tomógrafo, y solamente el objeto que está siendo examinado rota 360 grados. Uno de los puntos clave es el sostén: no debe interferir con el láser del rayo x; al mismo tiempo, sin embargo, debe asegurar que el componente se mantenga firme. Incluso si el componente solo se mueve pocos micrómetros, la medición se falsearía.

Otro desafío es que los componentes a menudo comprenden varios materiales. Una mezcla de muchos materiales, como un objeto de latón con un sello de goma, requiere una herramienta de software adicional para recalcular el volumen y minimizar los artefactos en una sola imágenes.

## Un tomógrafo en *Festo*

En la empresa *Festo*, entre otras cosas, se usa un tomógrafo en el proceso de desarrollo de nuevos productos. Antes de que los componentes nuevos o los cambios pasen a la producción en serie, se lleva a cabo un análisis de tomografía computada para examinar si los componentes satisfacen las propiedades especificadas y los requisitos de calidad.

Otro campo de aplicación es para el análisis de componentes defectuosos. Si, por ejemplo, se produce un derrame, el tomógrafo se usa para buscar la pérdida, quizá la carcasa está porosa o el sello de goma se corrió de su posición. El dispositivo también se usa para reclamos del cliente. La mayor ventaja acá es que los componentes se pueden analizar de forma no destructiva sin tener que gastar tiempo irrecuperable en desarmarlos. ❖



Los componentes analizados tienen diferentes tamaños, desde unos pocos milímetros hasta varios metros. El sostén se debe ajustar con precisión, a fin de que nada se salga de lugar

# Ciberseguridad industrial: el diseño integral es la base

**Phoenix Contact**
*www.phoenixcontact.com*

Vivimos en una época en la que el desarrollo de las tecnologías de comunicación permite que millones de equipos intercambien información en todo el mundo. Por eso, es necesaria una estrategia para garantizar la seguridad de red y la disponibilidad de la planta. En este contexto, *Phoenix Contact* desarrolla soluciones para proteger los sistemas, los conocimientos técnicos y todos los datos confidenciales que dan forma a los procesos comerciales y de producción de las empresas.

*El tema de la ciberseguridad incumbe a todos, tanto fabricantes como empresas explotadoras, la industria o la infraestructura crítica.*

## Relevancia de la ciberseguridad en todas las industrias

La lista de incidentes de seguridad en la industria es cada vez más larga: *Stuxnet*, un programa dañino especial para sistemas SCADA, los virus *Industroyer* (2016) y *Triton* (2017), un ataque selectivo a los controles de seguridad y el software de extorsión *WannaCry* (2017), que ha atacado a más de 230.000 sistemas en todo el mundo.

El tema de la ciberseguridad incumbe a todos, tanto fabricantes como empresas explotadoras, la industria o la infraestructura crítica. La creciente interconexión y conexión de sistemas de control y automatización industriales (ICS) a Internet también hace que estos cada vez estén más expuestos a ataques cibernéticos y cambios no deseados. Por este motivo, la ICS Security cada vez adquiere más relevancia.

Para los fabricantes de maquinaria, la seguridad aumenta la fiabilidad y disponibilidad de sus máquinas. Para el mantenimiento remoto de cara al cliente se precisa, además, una conexión remota segura.

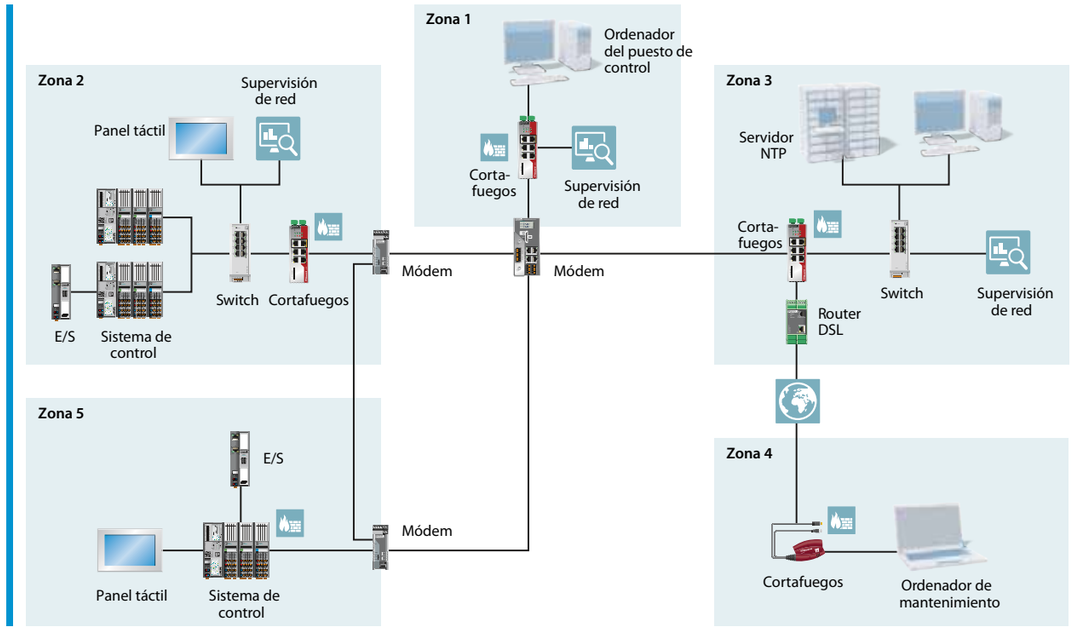
Para el explotador de la instalación, la seguridad, no solo garantiza la disponibilidad y el desarrollo fiable de sus instalaciones y procesos, sino que protege, además, sus conocimientos técnicos sobre producción.

En la industria automovilística, la disponibilidad de sus instalaciones es su activo más preciado. Los mecanismos de seguridad garantizan la disponibilidad de las líneas de producción y pueden incluso aumentarla.

En el sector energético, las empresas juegan un papel importante en el suministro básico a las personas. Por este motivo, los legisladores de muchos países obligaron a los explotadores a proteger la infraestructuras de importancia crítica de sus instalaciones para evitar un acceso no autorizado.

En el caso de tratamiento de aguas y aguas residuales, su tarea más importante es garantizar el suministro continuo de agua potable y la limpieza de las aguas residuales. La seguridad garantizará el acceso remoto a las estaciones remotas de bombeo y elevación y protegerá los sistemas de automatización frente al creciente número de ciberataques por Internet.

Respecto de petróleo y gas, la seguridad debe considerarse un requisito en el ámbito de la protección (safety), en particular en entornos explosivos o ligeramente inflamables. No en vano, una instalación hackeada, no solo puede suponer un riesgo financiero, sino también un riesgo para la seguridad de sus empleados.

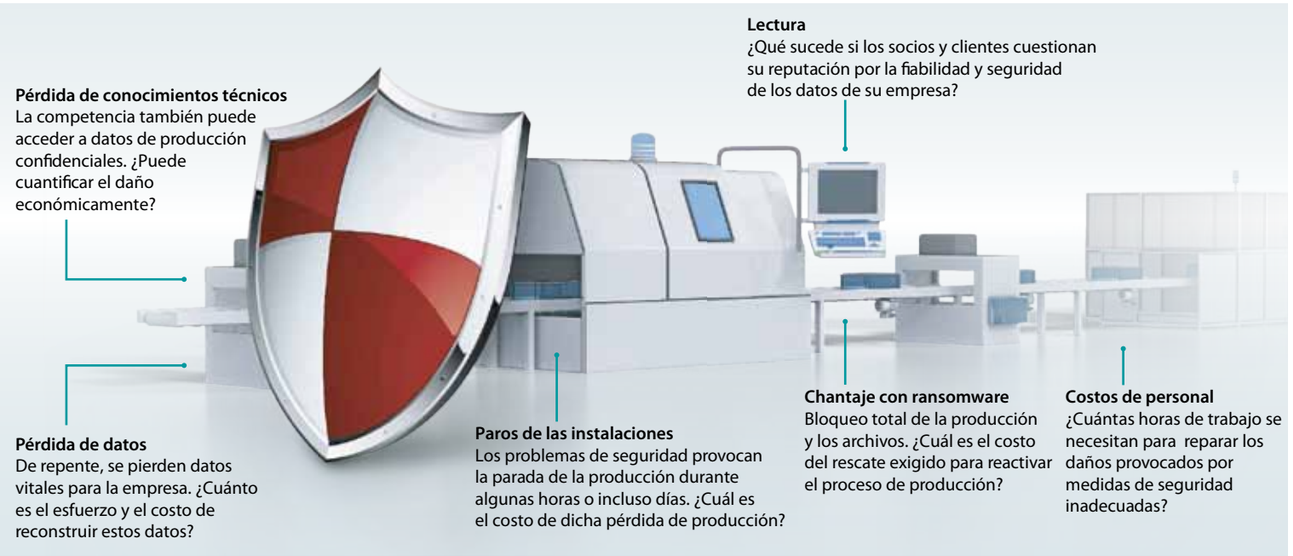


## Posibles consecuencias de un incidente de seguridad

Las empresas solo tienen éxito si sus plantas de producción funcionan de forma segura y sin fallos. Los fallos, los sabotajes o las pérdidas de datos pueden causar un alto daño económico. Y es que las paradas no solo implican pérdidas financieras, sino que también ponen en peligro los plazos de entrega y, como consecuencia, la imagen y la reputación de la empresa. En un análisis de sitios y procesos, se pueden evaluar los riesgos relativos de un sistema industrial y su interacción con el sistema de información de la instalación.

Los cuestionamientos que vale la pena hacerse son los siguientes:

- Pérdida de conocimientos técnicos. La competencia también puede acceder a datos de producción confidenciales. ¿Se puede cuantificar el daño económicamente?
- Pérdida de datos. De repente, se pierden datos vitales para la empresa. ¿Cuánto es el esfuerzo y el costo de reconstruir estos datos?
- Paros de las instalaciones. Los problemas de seguridad provocan la parada de la producción durante algunas horas o incluso días. ¿Cuál es el costo de dicha pérdida de producción?
- Lectura. ¿Qué sucede si los socios y clientes cuestionan la reputación por la fiabilidad y seguridad de los datos de la empresa?
- Chantaje con *ransomware*. Bloqueo total de la producción y los archivos. ¿Cuál es el costo del rescate exigido para reactivar el proceso de producción?
- Costos de personal. ¿Cuántas horas de trabajo se necesitan para reparar los daños provocados por medidas de seguridad inadecuadas?




## Riesgos de seguridad habituales y soluciones

Los fallos y virus provenientes de Office se pueden contagiar directamente al entorno de producción. La solución a esto es la división de grandes redes en pequeños segmentos, se puede controlar el intercambio de datos entre las diferentes zonas, por ejemplo, entre la producción y Office, o entre diferentes partes de la instalación. Los segmentos individuales se pueden separar con ayuda de VLAN o cortafuegos. Para la comunicación entre los segmentos de red individuales deben emplearse routers o switches de capa 3. Estos equipos captan los errores de red, de manera que no se puedan expandir al resto de la red.

*Las paradas no solo implican pérdidas financieras, sino que también ponen en peligro los plazos de entrega y, como consecuencia, la imagen y la reputación de la empresa.*

Otro riesgo es la infección por software dañino. Con frecuencia, el software dañino está concebido de forma que intenta expandirse a los sistemas vecinos para dañarlos. Un ejemplo es el software dañino *WannaCry*, que infecta los sistemas Windows no actualizados.

La solución al software dañino es la limitación de la comunicación. El uso de cortafuegos puede limitar o impedir la propagación del software dañino. Si se bloquean todas las posibilidades de comunicación que no son técnicamente necesarias, se pueden evitar muchos ataques. Además, el monitoreo integral apto para la industria ayuda a detectar y contener en una fase temprana cambios y manipulaciones en sistemas basados en Windows, como sistemas de control, unidades de operación o PC.

El ataque de hackers, por su lado, implica un riesgo en tanto que los delincuentes pueden usar una conexión abierta a Internet para copiar datos o realizar cambios en el sistema. La solución es la transmisión de datos codificada. Se debe impedir el acceso a los sistemas de automatización a través de Internet. Esto se puede lograr mediante un cortafuegos, que limita todo el tráfico entrante y saliente a las conexiones necesarias y permitidas. Todas las conexiones de amplio alcance deben estar cifradas, por ejemplo, a través de VPN con Ipsec.

Para el acceso no autorizado a las instalaciones, la solución consiste en un acceso remoto seguro a una o más máquinas, y quizá con diferentes soluciones tecnológicas. Por un lado, la comunicación externa está codificada, por ejemplo, a través de IPsec u OpenVPN. Por el otro, se puede iniciar el mantenimiento remoto en la máquina a través de un conmutador de llave. De esta forma, se garantiza que solo se realicen los cambios en la máquina en la que está previsto. Al mismo tiempo, el conmutador de llave se puede utilizar para bloquear las reglas de comunicación en la red durante el tiempo del mantenimiento remoto.

Un gran amigo de los ciberataques es la administración insuficiente de usuarios. on frecuencia, se utilizan contraseñas colectivas para el acceso. Cuando los empleados dejan la empresa, estas contraseñas no se modifican ni se desactivan. El resultado es que demasiados empleados conocen la contraseña colectiva y pueden provocar usos inadecuados. La solución es una administración de usuarios centralizada, en donde se concede acceso individual a cada empleado.

Otro riesgo lo presentan los equipos y terminales móviles no autorizados que se comunican a través de la interfaz WLAN. Para este caso, se puede asignar una contraseña WLAN segura, con contraseñas individuales. Si se conocen las contraseñas WLAN y no se cambian durante un largo periodo de tiempo, se puede producir un acceso incontrolado a la red de maquinaria. Además, se puede proteger

la comunicación WLAN con una zona desmilitarizada y aislarla del resto de la red.

Por último, vale destacar el riesgo por configuración incorrecta o insegura de los equipos. Las configuraciones estándar se han diseñado para garantizar que los componentes funcionen correctamente y que sean fáciles de poner en funcionamiento y, en este contexto, los mecanismos de seguridad juegan con frecuencia un papel secundario. Como respuesta a esto, se pueden implementar gestión de dispositivos y parches.

Al gestionar varios equipos, una gestión de dispositivos y parches inteligente y eficiente puede automatizar procesos que requieren mucho tiempo y reducir, además, los riesgos de una configuración incorrecta. Ayuda a configurar, desplegar y gestionar los equipos y reduce los riesgos de seguridad y cumplimiento acortando los ciclos de parches y actualizaciones. La gestión de dispositivos y parches permite la creación y gestión centralizadas de todos los ajustes de los equipos relevantes para la seguridad, además de facilitar las actualizaciones de firmware

*Las medidas organizativas y técnicas sostenibles, ajustadas al ciclo de vida de una instalación, minimizan el riesgo de posibles ataques.*

## Una respuesta posible

*Phoenix Contact* ofrece seguridad normalizada en productos, soluciones industriales y servicios para lograr un funcionamiento seguro en el futuro de máquinas, instalaciones e infraestructuras. La seguridad está anclada en todo el ciclo de vida de los productos y soluciones.

Las medidas organizativas y técnicas sostenibles, ajustadas al ciclo de vida de una instalación, minimizan el riesgo de posibles ataques. Para lograr la máxima estabilidad y transparencia, la empresa ayuda a seleccionar el hardware adecuado, a desarrollar conceptos de protección personalizados y a impartir cursos de formación práctica.

Su idea de "Security by Design" (seguridad bajo diseño), conforme a la norma internacional IEC 62443-2-4, significa:

- Determinación de los requisitos de protección
- Realización de un análisis de riesgos y amenazas
- Desarrollo de un concepto de red segura, con zonas y conductos, teniendo en cuenta la norma IEC 62443
- Selección de productos de automatización seguros
- Documentación y puesta en marcha de la instalación
- Servicios complementarios para la instalación (por ejemplo, gestión de parches) a lo largo del ciclo de vida ❖

# Estrategias para atender la ciberseguridad

**Siemens**
*www.siemens.com.ar*

Internet se presenta como un gran acelerador de procesos de negocio y ha revolucionado las operaciones en todo el mundo.

Los cambios resultantes en la industria de producción también se pueden describir como "revolución": algunos se animan a hablar de "cuarta revolución industrial". La Industria 4.0 afecta todos los aspectos de la cadena de valor industrial, incluyendo comunicación industrial y seguridad.

Más todavía, ahora la seguridad se regula con leyes que atienden infraestructuras críticas particulares. Como ejemplos, se puede mencionar el IT Security Act, en Alemania; la certificación ANSSI, en Francia, y NERC CIP, en Estados Unidos. Después de todo, la comunicación abierta y el crecimiento de la red en los sistemas de producción involucran no solo grandes oportunidades, también grandes riesgos. Para proveer una planta industrial de seguridad integral contra posibles ataques, se deben tomar medidas apropiadas. La empresa *Siemens* tiene herramientas para realizar la tarea.

*Después de todo, la comunicación abierta y el crecimiento de la red en los sistemas de producción involucran no solo grandes oportunidades, también grandes riesgos.*

## Defensa en profundidad

Con la defensa en profundidad, la empresa *Siemens* busca ofrecer un concepto multifacético que otorgue protección al sistema. El concepto está basado en la seguridad de planta, la seguridad de red y la integridad del sistema, de acuerdo a las recomendaciones de ISA 99/IEC 62443, la normativa de seguridad más importante en la automatización industrial.

### Seguridad de planta

La seguridad de planta se vale de una cantidad de métodos diferentes para prevenir que personas no autorizadas ganen acceso físico a componentes críticos. Esto comienza con un acceso convencional y se extiende a la construcción de áreas sensibles a las que se accede solamente por medio de tarjetas de ingreso.

Los servicios de seguridad de planta incluyen servicios de consultoría, paquetes de

| Nro. | Amenaza | Explicación |
|---|---|---|
| 1 | Infección de malware a través de Internet o de la intranet | Los componentes IT estándar, tales como los sistemas operativos, servidores de aplicación y bases de datos en general contienen desperfectos y puntos débiles que los atacantes pueden aprovechar. |
| 2 | Introducción de malware a través de hardware externo o medio removible | Los medios removibles como los pendrives son objeto de introducción de infección de malware. El uso de notebooks con data externa y software de mantenimiento que podría haber sido usada en otras compañías implica un gran peligro. |
| 3 | Ingeniería social | La ingeniería social es un método para ganar acceso no autorizado a información o sistemas IT casi sin llevar a cabo procedimientos técnicos, puesto que se puede aprovechar de actitudes humanas como la colaboración, la confianza, el miedo o el respecto a la autoridad. Un ejemplo de esto son los sitios de Internet que infectan el sistema de la víctima con malware. |
| 4 | Error humano y sabotaje | El personal que trabaja en ICS ocupa un lugar especial cuando se trata de seguridad. Esto se aplica tanto a personal propio como externo involucrado en tareas de mantenimiento o construcción. La seguridad nunca puede estar garantizada solamente por medidas técnicas; también se requieren regulaciones organizacionales. |
| 5 | Intrusión a través de acceso por mantenimiento remoto | El acceso desde el exterior al ICS por mantenimiento es una práctica muy extendida. Y cuando se puede ingresar a un sistema por mantenimiento, otros quedan más accesibles. A menudo, la falta de autentificación o autorización, o jerarquías de red planas, son las causas de los incidentes de ciberseguridad. |
| 6 | Componentes de control conectados a Internet | Los componentes inseguros de ICS tales como PLC a menudo se conectan directamente a Internet, en contra de las recomendaciones del fabricante, sin las medidas de seguridad correspondientes. |
| 7 | Malfuncionamientos técnicos y de fuerza mayor | Siempre son posibles las fallas a causa de influencias ambientales extremas o defectos técnicos. Aquí, el riesgo potencial de daño solo se puede minimizar. |
| 8 | Comprometer teléfonos inteligentes en el entorno de producción | La posibilidad de ver y modificar parámentros de producción y operación en un teléfono inteligente o una táblet es una característica que se promociona y utiliza cada vez más en los componentes ICS. Esto significa un caso especial de acceso remoto por mantenimiento, por lo que el uso de teléfonos inteligentes implica un punto de ataque adicional. |
| 9 | Introducción de componentes extra net o en la nube | La tendencia generalizada de externalizar los componentes IT está llegando a los ICS. Por ejemplo, los proveedores de soluciones de mantenimiento remoto colocan los sistemas del cliente en la nube, pero esto lleva a que los dueños del sistema solo tengan control limitado sobre la seguridad de los componentes. |
| 10 | Ataques (D)DoS | Los ataques de denegación de servicio (distribuido) (DDoS) se pueden usar para interrumpir conexiones de red y recursos requeridos y causar el colapso en los sistemas, por ejemplo, para quebrantar la funcionalidad de un ICS. |

**Fuente. Industrial Control System Security: Top 10 Threats and Countermeasures v1.1**
**Publication date: March 26, 2014**
**Nota. Esta lista de amenazas fue elaborada junto con BSI (Oficina Federal Alemana para Seguridad de la Información)**

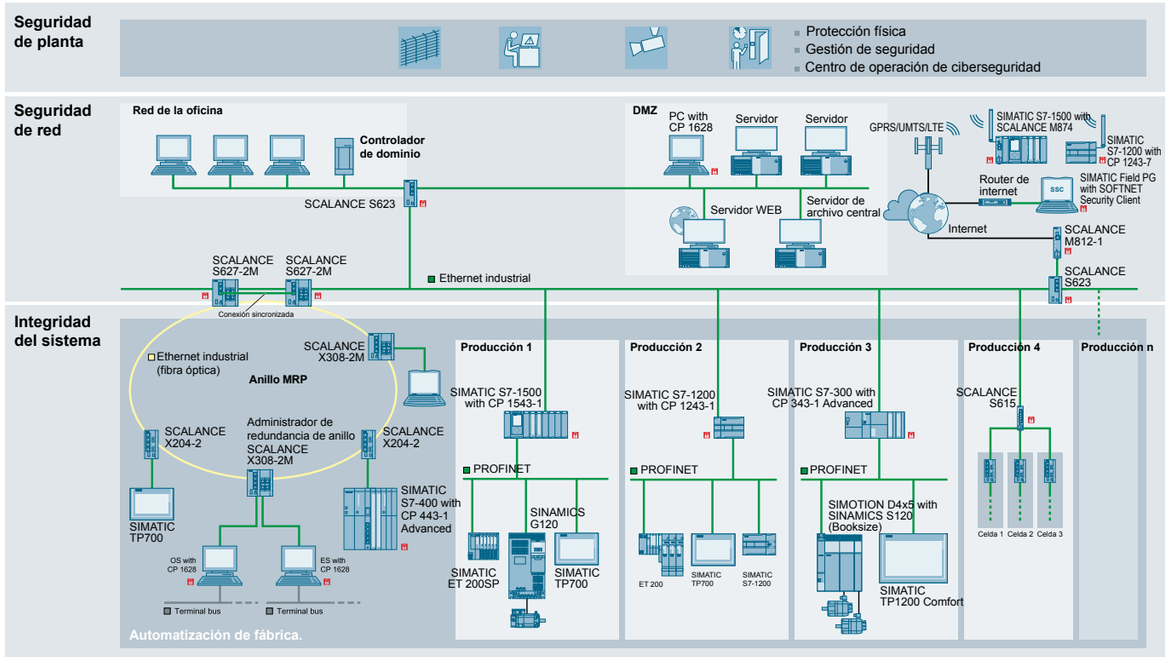
implementación y servicios de seguridad administrada, para lograr una protección holística de la planta y a largo plazo.

*Atender la seguridad implica analizar y atender el estado de la planta respecto de la tecnología, la arquitectura de red y el personal.*

Las instalaciones productivas están constantemente a merced de las amenazas. Dispositivos infectados, personal no autorizado, acceso no autorizado a través de red y la Internet, requieren tomar medidas.

Atender la seguridad implica analizar y atender el estado de la planta respecto de la tecnología, la arquitectura de red y el personal. Los paquetes de implementación van desde brindar apoyo para la planificación de red y la instalación de sistemas de detección de ataques hasta la integración de medidas de fortalecimiento del sistema.

Con actualizaciones continuas y un monitoreo comprehensivo, los servicios de seguridad pueden asegurar que se ajustarán rápidamente a las amenazas, que son cambiantes; y que serán transparentes a la hora de mostrar el estado de seguridad de la planta, gracias al monitoreo en todo el mundo y alertas en tiempo real.




Defensa en profundidad de *Siemens*

**La clave: seguridad de red**

La seguridad de red significa proteger las redes de automatización de accesos no autorizados. Esto incluye monitorear todas las interfaces entre las redes de oficina y planta, o el acceso a Internet por mantenimiento remoto.

*La segmentación de la red de planta en celdas de automatización protegidas individualmente minimiza los riesgos e incrementa la seguridad.*

Se puede atender a través de firewalls y, si aplica, estableciendo una zona desmilitarizada (DMZ) segura y protegida. La DMZ se usa para hacer que pueda haber data disponible a otras redes pero sin otorgar acceso directo a la red de automatización en sí misma.

La segmentación asegurada de la red de planta en celdas de automatización protegidas individualmente minimiza los riesgos e incrementa la seguridad.

La división por celdas y la asignación de dispositivos se basan en los requisitos de protección y comunicación.

La transmisión de datos se puede encriptar con un VPN, y así queda protegida contra el espionaje y la manipulación. Las estaciones de comunicación se están autentificadas de forma segura. Las redes de automatización, los sistemas de automatización y la comunicación industrial se pueden asegurar con componentes *Scalance* de "seguridad integrada", tales como los módulos de seguridad *Scalance S*, *Scalance M*, routers inalámbricos móviles y PC de seguridad para *Simatic*.

*La integridad del sistema también implica autentificación de usuarios, autorizaciones de acceso o para realizar cambios, y fortalecimiento del sistema; en otras palabras, la robustez de los componentes en contra de los ataques.*

**Integridad del sistema**

El tercer pilar de la defensa en profundidad es el resguardo de la integridad del sistema. Aquí, el énfasis está puesto en la protección de los sistemas de automatización y componentes de control tales como *Simatic S7-1200* y *S7-1500*, así como sistemas SCADA y HMI contra acceso no autorizado; también, es satisfacer requisitos especiales como protección del saber-hacer.

Además, la integridad del sistema también implica autentificación de usuarios, autorizaciones de acceso o de realizar cambios, y fortalecimiento del sistema; en otras palabras, la robustez de los componentes en contra de los ataques. ❖

# Crónica de una transformación tecnológica en la industria de producción

El artículo aquí presentado fue elaborado por Alejandra Bocchio para *AADECA Revista* en base a la presentación que Mario López hiciera en el Panel de Petróleo en la Era Digital que se llevó a cabo en la última edición de AADECA '18 "Evolucionando en la era digital".

**Mario López**
AxionEnergy
*mario.r.lopez@axionenergy.com*

Acerca del disertante
El ingeniero Mario López es gerente de proyectos de *AxionEnergy*, a cargo de la refinería de Campana, en donde ha desarrollado su carrera. Cuenta con una experiencia de más de treinta años en control y automatización industrial de alta envergadura.

## Historia tecnológica de la refinería de Campana

En 1905, capitales austro-húngaros establecieron una Compañía Nacional de Aceites. En 1906 comenzó el procesamiento de crudos para la fabricación de kerosén y aceites lubricantes. Así comienza la historia de la refinería de Campana, que con el transcurrir de los años ha sabido incorporar en sus procesos las nuevas tecnologías. Hoy se rige por la era digital.

Ha pasado por todas las épocas. Desde salas de control donde era necesario llevar manómetros a la consola; hasta la creciente actualización: desde la década de 1980, de analógica neumática a analógica electrónica, y analógica con procesamiento digital y continua.

*En 2018, la refinería se embarcó en un nuevo proyecto de transformación tecnológica, que buscaba incrementar la capacidad de producción de combustibles, mejorar la calidad de los combustibles reduciendo el contenido de azufre y reducir las emisiones de gaseosas.*

Los sectores de la refinería son: muelles, unidad de producción, planta de despacho y unidad de tanques. Hace treinta años, todas estas unidades eran analógicas y, en gran parte, neumáticas. Con el tiempo, comenzó a incorporar electrónica y tecnología digital en la planta de generación, lo primero fue un sistema de control distribuido. Luego, llegaron más equipos con el objetivo de obtener mayor cantidad de datos que permitieran controlar las unidades, había paneles, una pared cubierta de controladores analógicos, neumáticos o electrónicos, y en la playa de tanques todo se hacía de forma manual, había que subir al tanque y medir.

Las transformaciones de procesos iban acompañadas de transformaciones del personal pues, por ejemplo, no se necesitan las mismas habilidades para operar una válvula que para operar un panel.

Hace treinta años, también, llegó la primera tecnología de telemedición de tanques, que trajo consigo un cambio en el concepto de "operador" mismo: dejaba de ser la persona que subía hasta el tanque para convertirse en una que tiene frente así una terminal y puede "ver" el tanque.

Toda esta vorágine atravesaba el sector de tanques principalmente. Los demás permanecían en soluciones analógicas, con salas distribuidas, con información en carta y sin historizadores.

Hace quince años, la refinería optó por migrar de tecnología analógica a tecnología de control distribuido, lo cual implicó una gran transformación a nivel general: la información se podía concentrar, historizar, recabar y, sobre todo, analizar. Fue ahí, en 2005, cuando empezó la era de los datos, que abrió la puerta a la optimización y creatividad de los procesos.

Se abrieron las puertas a los sistemas de optimización en tiempo real, sistemas de alarma, sistemas de control de automatismo de lazos

## La transformación sigue

En 2018, la refinería se embarcó en un nuevo proyecto de transformación tecnológica, que buscaba incrementar la capacidad de producción de combustibles, mejorar la calidad de los combustibles reduciendo el contenido de azufre y reducir las emisiones gaseosas.

Para eso, era necesario construir una nueva planta y todo lo que esto implica: un nuevo cocker, una planta de tratamiento, un nuevo diésel/nafta, más energía, más vapor, más aire, otra antorcha, otra torre de agua, otra sala de control. También

una red nueva que vincule todos los sectores entre sí y con el resto de la refinería, y todo debía hacerse sin interrumpir las tareas, en funcionamiento.

250 personas se pusieron "manos a la obra", entre químicos, mecánicos, electricistas, instrumentistas.

Infraestructuraprevia:

- Sistema de control digital (DCS)
- Sistema de gestión de potencia (PMS)
- Sistemas integrados de seguridad (SIS) independientes, no vinculados entre sí
- Sistemas de fuego y gases no integrados
- Red totalmente integrada
- Analizadores, integrados al DCS

Proyecto de expansión:

- Expansión de DCS, PMS, analizadores
- Integración SIS
- Nueva red de fuego y gases integrada al DCS, es decir, no solamente una única red, sino también integrada al DCS
- Refuerzo de la red con ciberseguridad
- Control de motores integrado al DCS (ProfiBus)

El proyecto de expansión se basó en la infraestructura vigente. Se añadieron 7.200 señales con catorce controladores, 15.607 instrumentos (incluyendo manómetros), once analizadores, veintiocho sistemas tipo PLC, una red de 45.000 metros de fibra óptica con cincuenta switches nuevos, once firewells y veintiún gabinetes.

También se necesitaron en total seis edificios nuevos: una nueva sala de control de ochocientos metros cuadrados (800 $m^2$), tres shelters de control de campo y dos shelters de operadores para que la gente pueda estar a resguardo en una operación segura.

"El papel resiste cualquier cosa" se dice. Una cosa es el proyecto, otra muy distinta es llevarlo a la realidad. Enfrentar desafíos a la hora de hacer especificaciones, contratos, diseños. Y poco a poco, se fue haciendo realidad, junto a equipos de ingeniería y el soporte de varias empresas.

*El diseño nuevo permitió crecer en forma ordenada sobre la infraestructura vigente de la refinería [...]. De hecho, todo se hizo con las plantas en marcha, sin tiempos de parada.*

## Palabras finales

El diseño nuevo permitió crecer en forma ordenada sobre la infraestructura vigente de la refinería, porque no se colocaron nuevas redes, sino que se amplió la existente. De hecho, todo se hizo con las plantas en marcha, sin tiempos de parada.

Aumentó la confiabilidad de la infraestructura de automatización y control. También se unificaron tecnologías y se priorizó que estas fueran fáciles de entender.

Asimismo, se dejaron bases tecnológicas para futuros crecimientos productivos, porque la refinería continúa con proyectos de envergadura en su agenda.

El desafío de la transformación digital fue acompañar el cambio con acciones concretas sobre el personal y sobre la forma de llevar a cabo los procesos. En primer lugar, la capacitación de las personas en las nuevas tecnologías y la reorganización del equipo de soporte.

Asimismo, mantener y aumentar aspectos de ciberseguridad, pues la posibilidad de ciberataques es creciente, y ante proyectos del tipo como el implementado en la refinería, debe estar considerada desde la etapa de diseño. Esto significa una mayor colaboración con profesionales IT, y aprender a balancear las prioridades de disponibilidad y seguridad. ❖

# Visión práctica sobre la implementación de niveles de seguridad según la norma IEC 62443 en aplicaciones de control industrial

**Por Daniel DesRuisseaux**
Director del Programa de Ciberseguridad Industrial

Schneider Electric
*www.schneider-electric.com.ar*

Daniel DesRuisseaux tiene más de veinticinco años de diversa experiencia en roles relacionados con estructuración, ventas y márketing en empresas de alta tecnología. En la actualidad, es el director de Ciberseguridad de la División Industrial de *Schneider Electric*. Desde este cargo, trabaja para garantizar una implementación adecuada y consistente de características de seguridad en toda la cartera de diversos productos industriales de la empresa.

Las exigencias de las aplicaciones para la Internet industrial de las cosas (IIoT) modernas aumentan la complejidad de la infraestructura de los sistemas y ejercen una presión adicional sobre la seguridad de los sistemas informáticos (TI) y operativos (TO). A medida que se incrementan la frecuencia y la sofisticación de los ciberataques, las operaciones deben aprovechar los estándares industriales para lograr una protección consistente.

En este informe se expondrá cómo puede aplicarse la norma IEC 62443 a los sistemas de control industrial para mejorar la comprensión de las diversas prioridades y los múltiples pasos requeridos para ayudar a mitigar las amenazas cibernéticas.

## Introducción

Durante los últimos diez años se ha observado un aumento exponencial de los ciberataques a los sistemas de control industrial (ICS). La industria ha respondido a las amenazas contra la ciberseguridad creando normas para ayudar a los usuarios finales y los fabricantes de equipos a brindar seguridad para los sistemas de control industrial. En la actualidad existen varias normas clave disponibles en el mercado. La norma IEC 62443 fue desarrollada por los comités de ISA99 e IEC para mejorar la seguridad, la disponibilidad, la integridad y la confidencialidad de los componentes o los sistemas usados para automatización y control industriales. La serie de estándares IEC 62443 puede usarse en todos los segmentos de control industrial, y fue aprobada en muchos países. En su evolución, se ha ido convirtiendo en una norma clave para la industria, y *Schneider Electric* está creando su estrategia de ciberseguridad en torno a ella.

Este documento fue ideado para presentar estos conceptos a usuarios con un limitado conocimiento sobre ciberseguridad para sistemas de control industrial y brindar pautas para la implementación usando ejemplos prácticos. Debe tenerse en cuenta que este es un documento genérico concebido como la introducción a estos conceptos. Las pautas que aquí se presentan no deben usarse para brindar seguridad para los sistemas de control industrial sin estudiar en detalle las redes específicas.

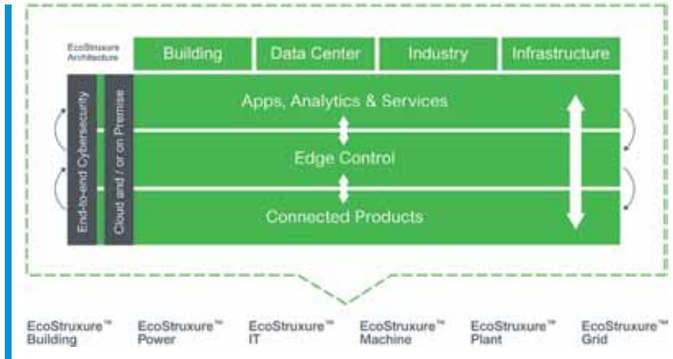



Figura 1

| Nivel de seguridad (SL) | Objetivo | Habilidades | Motivación | Medios | Recursos |
|---|---|---|---|---|---|
| SL1 | Violaciones casuales o accidentales | Sin habilidades para atacar | Ninguna, por error | No intencionales | Un individuo |
| SL2 | Delincuentes informáticos, háckers | Genéricas | Baja | Simples | Bajos (individuo aislado) |
| SL3 | Háckers activistas, terroristas | Específicas de ICS | Moderada | Sofisticados (ataque) | Moderados (grupo de háckers) |
| SL4 | Estado nacional | Específicas de ICS | Alta | Sofisticados (campaña) | Extensos (equipos multidisciplinarios) |

Tabla 1

## *EcoStruxure*

*EcoStruxure* es la arquitectura y plataforma de sistemas abierta, interoperativa y compatible con la Internet de las cosas (IoT) de *Schneider Electric*. Potencia los avances en las áreas de Internet de las cosas, movilidad, detección, entornos de nube, análisis y ciberseguridad para brindar innovación en todos los niveles. La arquitectura incluye productos conectados y control en el extremo de la red, así como aplicaciones, herramientas de análisis y servicios. *EcoStruxure* se ha implementado en más de 450.000 establecimientos, con la asistencia de 9.000 integradores de sistemas, y conecta a más de mil millones de dispositivos.

Uno de los requisitos clave de las arquitecturas *EcoStruxure* es una ciberseguridad intrínseca e integral. En este informe técnico, se estudiará cómo *Schneider Electric* usa técnicas basadas en estándares para brindar seguridad a sus soluciones *EcoStruxure*.

## Conceptos de ciberseguridad

En esta sección, se presentarán conceptos que son necesarios para comprender las recomendaciones expuestas más adelante.

**Niveles de seguridad garantizados**

La norma IEC 62443 incluye el concepto de niveles de seguridad garantizados. Su especificación define una serie de requisitos diseñados para alcanzar cada uno de los cuatro niveles de seguridad en los sistemas. En la tabla 1 se presenta un resumen de los aspectos de cada nivel, junto con la caracterización del tipo de atacante al que ese nivel fue diseñado para enfrentar.

Por ejemplo, los usuarios finales interesados en una solución diseñada para enfrentar ataques de háckers o delincuentes informáticos comunes deben implementar un sistema con las características especificadas para el nivel 2 de seguridad garantizado. Nótese que las caracterizaciones que se muestran en la tabla 1 son clasificaciones genéricas para ofrecer una mayor orientación a los clientes; implementar el nivel SL2 no garantiza que el sistema pueda detener el ataque de todo hácker o delincuente informático.

**Defensa en profundidad**

La defensa en profundidad es el uso coordinado de medidas de seguridad para proteger la integridad de los activos informáticos de una red. Una implementación adecuada de una estrategia de defensa en profundidad se compone de seis pasos. A continuación se presenta un breve resumen de cada paso.

- Creación de un plan de seguridad. El paso más importante en el proceso general de defensa en profundidad es el de la creación de un plan de seguridad. En este, el personal realiza una auditoría detallada de todos los equipos conectados a la red de control industrial, un diagrama de conexiones de los equipos, una revisión de la configuración de seguridad de los equipos y una evaluación de las vulnerabilidades potenciales del sistema. El plan de seguridad incluye el impacto para los productos, las arquitecturas, las personas y los procesos corporativos. Debe realizarse un plan de seguridad completo antes de efectuar cualquier otro paso para mejorar la seguridad del sistema. De lo contrario, el personal puede suponer que el sistema está seguro y no ser consciente de vectores de ataque potenciales.
- Redes separadas. Una vez que se generó un mapa detallado de la red en el plan de seguridad, las redes pueden separarse según alguna función principal. Por ejemplo, puede dividirse la red en zonas para la empresa, la planta, los procesos y los dispositivos de campo. Todas las rutas entre las zonas deben identificarse.
- Protección del perímetro. En este paso, se protegen adecuadamente las rutas entre zonas. Parte importante de este paso es la seguridad del acceso remoto.
- Segmentación de la red. En este paso, las zonas que se crearon en el segundo paso pueden dividirse en zonas más pequeñas en base a la ubicación o la función. Los perímetros de estas zonas segmentadas deben estar protegidos. Es importante notar que el nivel de seguridad asignado a cada zona puede diferir. Por ejemplo, el nivel de seguridad para los equipos de monitoreo puede establecerse en SL1, mientras que el asignado a un sistema instrumentado de seguridad (SIS) puede ser SL3. El nivel de cada zona segmentada no tiene por qué ser igual al de las zonas vecinas.
- Protección de dispositivos. En este paso se agregan características a los dispositivos de ICS para mejorar su capacidad de resistir un ciberataque. Esto reduce la probabilidad de que estos elementos se vean comprometidos si un hácker obtuviera acceso a una red.
- Monitoreo y actualización. Un monitoreo activo de la actividad de la red detecta amenazas potenciales, y las revisiones de software/firmware para los productos se ponen a disposición para responder a vulnerabilidades o agregar funcionalidades de seguridad.

Muchos clientes industriales no tienen experiencia en ciberseguridad. *Schneider Electric* cuenta con servicios de ciberseguridad para ayudar a estos clientes. Sus expertos en seguridad pueden ayudar a los clientes a diseñar e implementar estrategias de defensa en profundidad. También ofrece un servicio que le permite al fabricante realizar un monitoreo activo de las redes de clientes.

**Controles de compensación**

Otro concepto importante son los controles de compensación. Si un producto no tiene una funcionalidad de seguridad necesaria, el sistema puede igualmente cumplir con los requisitos si tal funcionalidad la presta un componente diferente del sistema. Por ejemplo, supongamos que un sistema usa un PLC antiguo. Este PLC carece de las características de seguridad necesarias, pero si se agrega un firewall delante de él se obtiene la funcionalidad necesaria para protegerlo. El agregado del firewall permitirá que el sistema cumpla con los requisitos para su certificación.

**Visión general**

Se usará una red de referencia para ayudar a ilustrar los cambios necesarios para mejorar la seguridad para cada uno de los niveles de seguridad

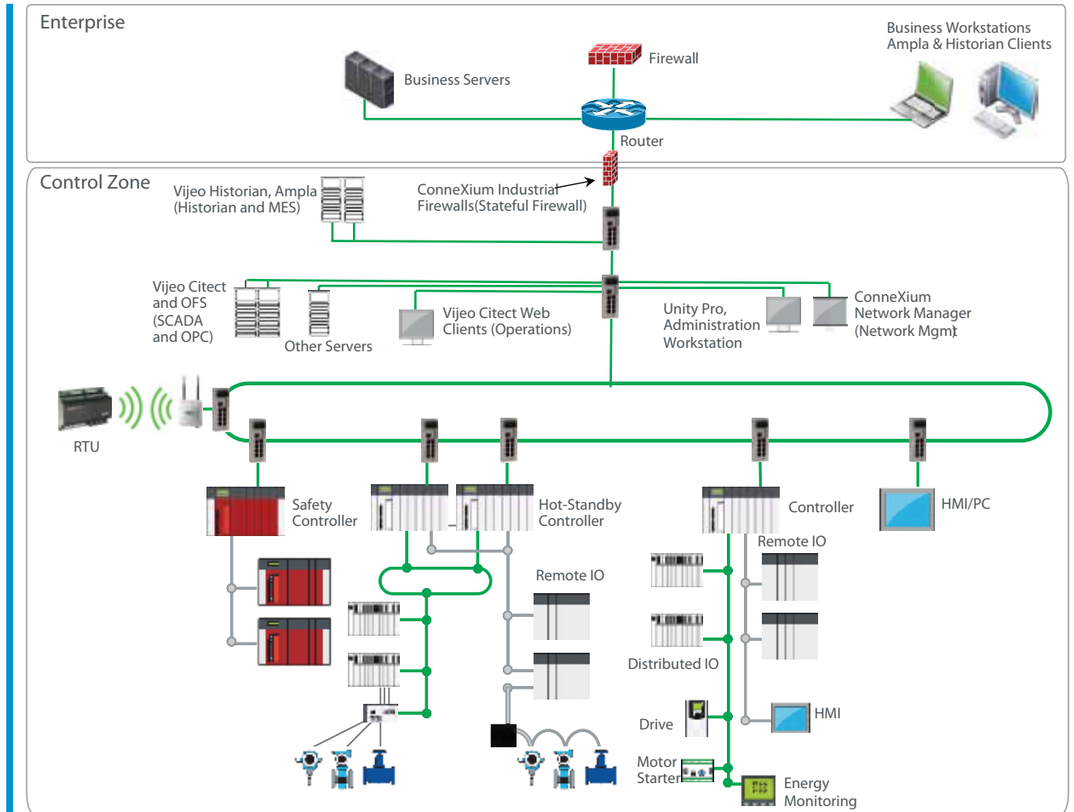



Figura 2

(SL) deseados. La red de referencia se presenta a continuación.

Los componentes de ICS se interconectarán mediante la red, incluidos los controladores, los sistemas de seguridad instrumentada (SIS), los variadores de velocidad y las interfaces HMI. La red de referencia es un sistema de control industrial genérico que puede usarse en diversos segmentos industriales.

En este informe, se examinarán los requisitos de ciberseguridad para redes basadas en Ethernet. Los elementos conectados usando interfaces de conexión serial no son parte del alcance de este documento.

A lo largo de este informe, la red de referencia que se acaba de presentar se modificará para ilustrar cambios que permitan satisfacer los requisitos de cada uno de los niveles de seguridad según IEC 62443. El foco de este informe serán los tres primeros niveles de seguridad, ya que en ellos se incluye la gran mayoría de las aplicaciones industriales, en particular, los requisitos de sistema según se especifican en el estándar de sistema IEC 62443-3-3. Se presentará cada uno de los niveles de seguridad (SL) conjuntamente con una descripción de los cambios necesarios. Para simplificar la presentación, en este informe se presupone que cuando se eleva el nivel de seguridad, se lo eleva para toda la red (no se configurarán segmentos de red específicos con niveles de seguridad diferentes).

Los cambios sugeridos serán los mínimos necesarios para permitir que el sistema alcance el nivel de seguridad deseado. Por ejemplo, puede usarse un firewall sencillo para segmentar las redes en el nivel SL1. Un firewall más avanzado con inspección profunda de paquetes o una puerta de enlace unidireccional pueden brindar una mayor seguridad que un simple firewall, pero en este nivel no se especifican capacidades de seguridad adicionales; estas pueden establecerse en niveles avanzados. Los clientes siempre pueden usar técnicas especificadas en niveles avanzados en sus sistemas.

En este informe también se hablará de productos y arquitecturas. No se tratarán otros aspectos que pueden definirse en un plan de seguridad (capacitación del personal, políticas corporativas de seguridad, etc.).

| N° de ítem | Requisito | Técnica para cumplir con el requisito |
|---|---|---|
| 1 | El sistema de control puede autentificar y autorizar a usuarios humanos. Pueden crearse y gestionarse cuentas de usuario. La robustez de las contraseñas es configurable. Se hace un seguimiento de los intentos fallidos de inicio de sesión. | Las cuentas de usuario final se crean en dispositivos o un servidor de autentificación centralizado. |
| 2 | El sistema de control puede autentificar y autorizar a usuarios con conexión inalámbrica. | Los dispositivos móviles y la infraestructura de red autentifican a los usuarios. |
| 3 | El sistema de control debe brindar la capacidad de monitorear y controlar el acceso desde redes no confiables. | Los firewalls monitorean el tráfico desde redes no confiables. |
| 4 | El sistema de control debe poder restringir código incrustado en correo electrónico o medios de almacenamiento. | Los firewalls de inspección profunda de paquetes monitorean el tráfico, analizando el contenido de cada trama desde redes no confiables. |
| 5 | Los sistemas de control deben brindar la capacidad de generar registros de auditoría. | Los equipos pueden generar registros de auditoría. |
| 6 | El sistema de control debe proteger la integridad de la información transmitida. | Los equipos admiten protocolos cifrados y métodos robustos de checksum/hashing. |
| 7 | El sistema de control debe detectar, prevenir e informar los efectos de código malicioso. | Puede habilitarse una lista blanca de aplicaciones en los dispositivos terminales. |
| 8 | El sistema de control debe proteger la confidencialidad de la información almacenada o en tránsito. | Los equipos admiten nombres de usuario y contraseñas para autorización. |
| 9 | El sistema de control debe segmentar las redes y proteger las fronteras entre zonas. | Los firewalls segmentan redes y protegen las fronteras entre zonas. |
| 10 | El sistema de control debe poder evitar que se reciban mensajes de usuarios o sistemas externos. | Un firewall puede filtrar mensajes de redes externas. |
| 11 | El sistema de control debe admitir la partición de datos, aplicaciones y servicios en base a su criticidad para implementar un modelo con zonas. | Las redes debe segmentarse usando modelos en base a zonas y rutas. |
| 12 | El sistema de control debe operar en modo degradado durante los eventos de negación de servicio. | Los elementos de red (switches, rúters, etc.) admiten limitación de velocidad de transferencia. |
| 13 | El sistema de control debe prohibir el uso de funciones, puertos, protocolos y servicios innecesarios. | Los dispositivos de ICS tienen la capacidad de deshabilitar capacidades innecesarias. |
| 14 | El sistema de control debe contar con un respaldo de información a nivel del usuario y del sistema. | Hay archivos de respaldo disponibles dentro de cada dispositivo individual. |

Tabla 2. Requisitos clave estipulados para SL1

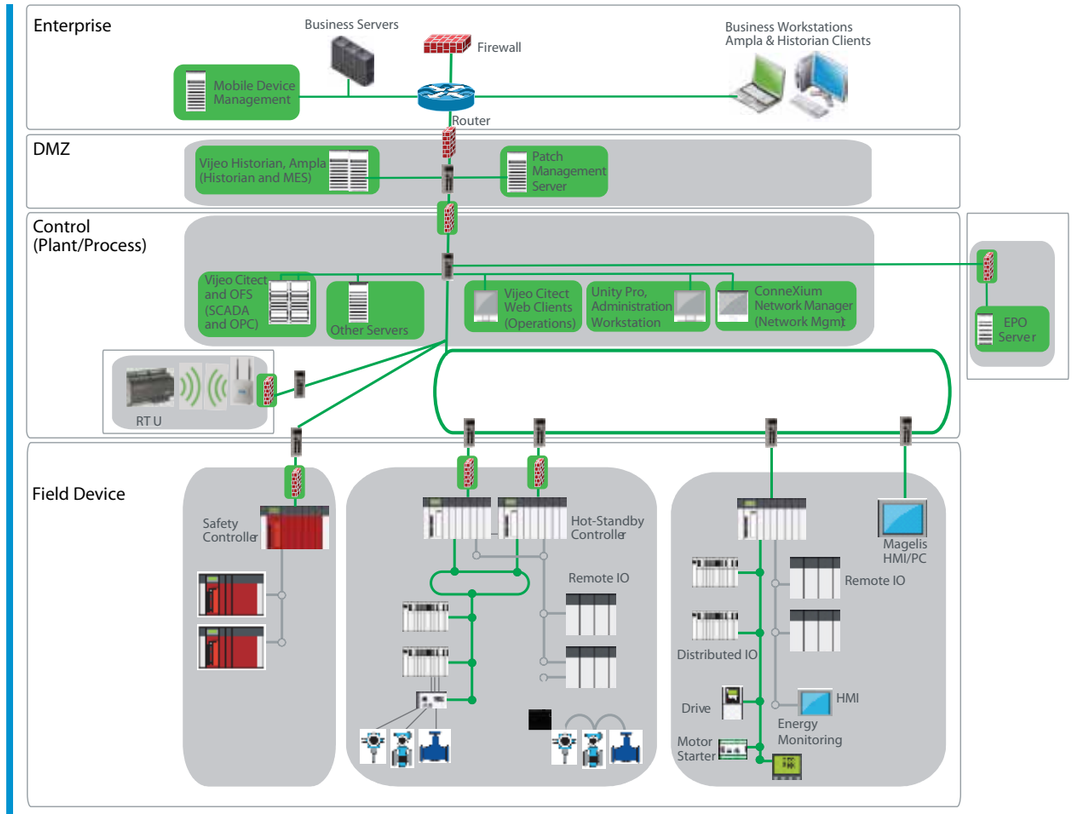



Figura 3

## Nivel de seguridad SL1

El nivel 1 de seguridad (SL1) está diseñado para proteger al sistema de violaciones por casuales o accidentales. Las especificaciones en IEC 62443-3-3 definen una larga lista de requisitos que cumplir para lograr este nivel de seguridad. La tabla 2 resume los requisitos clave estipulados para SL1. Nótese que el estándar IEC 62443-3-3 establece 37 requisitos individuales. La tabla 2 apunta a brindar una reseña de catorce de los requisitos más importantes. Para obtener más detalles, deben consultarse las normas IEC.

La implementación de los requisitos de SL1 tiene un impacto en la arquitectura de la red. SL1 requiere la implementación de pasos para defensa en profundidad, en particular, la segmentación de redes y la protección de las fronteras entre las zonas. Los cambios en la arquitectura de referencia están se destacan en la figura 3.

En el ejemplo de la figura 3, la zona de control en la red de referencia se dividió en siete zonas más pequeñas marcadas en gris. Los elementos nuevos están marcados en verde.

Las zonas son:

- Zona desmilitarizada (DMZ). Una subred que contiene y muestra los servicios de la zona de control dirigidos al exterior hacia la red empresarial. Los servidores en la zona empresarial nunca deben conectarse directamente a los elementos dentro de la zona de control. Sin embargo, los sistemas de negocios necesitan acceso a los datos de la zona de control, y los elementos en la zona de control necesitan acceso a archivos que se originan en redes no confiables (por ejemplo, actualizaciones de firmware). La DMZ contiene sistemas que necesitan acceso a los equipos de control y a los empresariales.
- Zona de planta/procesos. Zona que aloja productos y aplicaciones que posibilitan la gestión de la planta y los procesos.
- Zona de dispositivos del sistema instrumentado de seguridad. Zona centralizada que aloja diversos dispositivos de seguridad.
- Zona de conexión inalámbrica. Infraestructura inalámbrica que queda separada en una zona independiente.
- Zonas de controladores. En el ejemplo, el área de dispositivos de campo está dividida en tres zonas. Dos son zonas de control estándar, y una es una zona de controladores del sistema instrumentado de seguridad. La segmentación de zonas es resultado del plan de seguridad y dependerá de las aplicaciones; este es simplemente un ejemplo.

Se agregaron firewalls de clase industrial (destacados en verde) para segmentar la red. Además, se agregaron un servidor para apagado de emergencia (EPO) y otro para gestión de dispositivos móviles, junto con software para lista blanca de aplicaciones para los servidores que alojan el software ICS.

## Nivel de seguridad SL2

La especificación para el nivel 2 de garantía de seguridad incluye los requisitos estipulados para SL1 y agrega los requisitos de la tabla 3. Nótese que el estándar IEC 62443-3-3 establece veintitrés requisitos individuales. Aquí se presenta una lista resumida de los once requisitos más importantes. Para obtener más detalles, deben consultarse las normas IEC.

Es importante notar que algunos de los requisitos son mejoras de los estipulados para SL1, y otros son nuevos. Por ejemplo, en SL1, el sistema debe autentificar y autorizar a los usuarios humanos. En SL2, el sistema debe además autentificar y autorizar los dispositivos y los procesos de software. En SL1, el sistema debe detectar, informar y evitar la ejecución de software malicioso. En SL2, el sistema debe detectar, informar y evitar la ejecución de software malicioso en todos los puntos de entrada y salida de la zona. En algunos casos, se agregan nuevos requisitos, como la capacidad de admitir certificados de autentificación.

Algunas de estas especificaciones requieren el agregado de productos a la red. Se agregaron a la red un dispositivo para gestión de cuentas unificadas, un servidor de certificados (Certificate Authority), un servidor para respaldo, un servidor de eventos y un sistema de detección de intrusos en la red; estos están destacados en verde en la figura 4. Además, la red de control se segmentó en dos redes independientes.

Nótese que los posibles dispositivos de ICS que podrían reemplazarse para admitir nuevas características necesarias en SL2 (por ejemplo, una actualización a un nuevo controlador PLC que admita protocolos seguros) no están plasmados en el diagrama.

## Nivel de seguridad SL3

La especificación para el nivel 3 de garantía de seguridad incluye los requisitos estipulados para SL2 y agrega los requisitos de la tabla 4. Nótese que el estándar IEC 62443-3-3 establece treinta requisitos individuales. Aquí se presenta una lista resumida de los doce requisitos más importantes. Para obtener más detalles, deben consultarse las normas IEC.

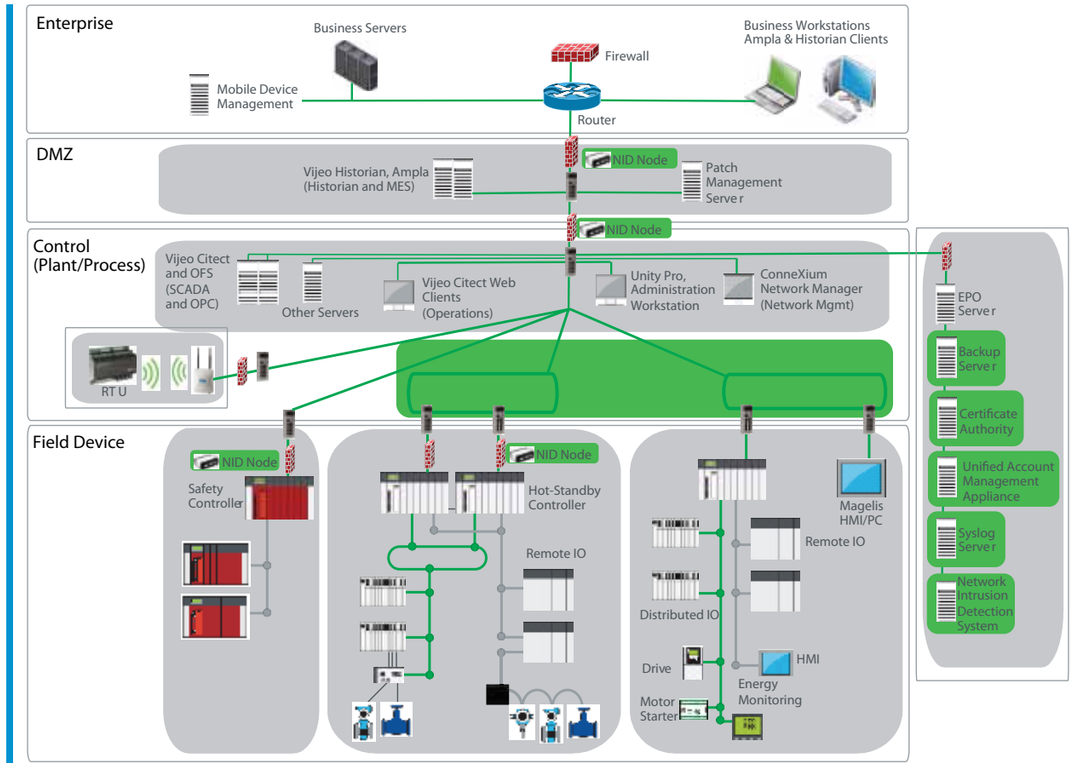



Figura 4

Varios de los requisitos de SL3 se implementan en los componentes de ICS. Entre los ejemplos, se incluyen los protocolos seguros obligatorios y el uso de elementos seguros para proteger claves. En el nivel 2 de garantía de seguridad, las características requeridas pueden implementarse mediante software nuevo. En el nivel 3 de garantía de seguridad, los equipos probablemente deberán reemplazarse o rediseñarse.

Algunas de estas especificaciones requieren el agregado de productos a la red. Por ejemplo, el servidor de eventos que se agregó para SL2 tendrá que actualizarse a un servidor SIEM para adaptarse a los requisitos de SL3. Además, deben agregarse un servidor de hora sincronizado por GPS y un dispositivo contra amenazas inalámbricas.

## Certificación del producto y del sistema

La norma IEC 62443 define requisitos para niveles de seguridad para los productos y el sistema. Estos requisitos proveen valor para los usuarios finales y los fabricantes de equipos.

» Usuarios finales. Por lo general, los usuarios finales evalúan los productos de los fabricantes en base a criterios entre los que se incluyen el contenido de características, el precio y los términos de la entrega. La especificación de características puede ser un proceso complejo. La norma IEC 62443 simplifica el proceso de definición de requisitos de seguridad al permitir que los usuarios finales especifiquen un nivel de seguridad como objetivo, en lugar de detallar una lista complicada de características individuales. Los usuarios finales sabrán las características exactas disponibles en los equipos en base a su cumplimiento con los estándares establecidos en IEC 62443.

» Fabricantes de equipos. Los fabricantes de equipos pueden diferenciar sus soluciones de las de la competencia mediante los estándares IEC 62443. Generalmente era difícil demostrar claramente que una solución es más segura que otra, ya que cada una puede tener un conjunto distinto de características de ciberseguridad. Los fabricantes que diseñan y certifican sus soluciones para los niveles de seguridad definidos en la norma IEC 62443 pueden diferenciar claramente sus capacidades de ciberseguridad promocionando su producto como certificado para los estándares de SL2 vs. productos que solo están certificados para SL1.

Los fabricantes pueden obtener certificaciones para dispositivos terminales (como se establece en IEC 62443-4-2) o sistemas (como se establece en IEC 62443-3-3). En ambos casos, el cumplimiento de estos estándares debe validarlo una fuente independiente. Los usuarios finales deben incluir

| N° de ítem | Requisito | Técnica para cumplir con el requisito |
|---|---|---|
| 1 | El sistema de control debe autentificar y autorizar los procesos de software y los dispositivos. | El software y los dispositivos se autentifican usando certificados. |
| 2 | El sistema de control debe autentificar usuarios humanos y de software que establecen comunicaciones inalámbricas. | Los dispositivos móviles y la infraestructura de red autentifican a los usuarios mediante un servidor de autentificación centralizado. |
| 3 | El sistema de control debe admitir autentificación por infraestructura de clave pública (ICP) y basada en certificados, si se utilizan. | Se agrega en la red de control un servidor de certificados (Certificate Authority). |
| 4 | El sistema de control debe poder denegar las solicitudes de acceso desde redes no confiables, salvo que sean aprobadas por un rol asignado. | Se habilita esta funcionalidad en dispositivos terminales. |
| 5 | El sistema de control debe permitir que usuarios autorizados definan y modifiquen la asignación de permisos para cada rol. | Se habilitan roles y permisos en un dispositivo para gestión de cuentas unificadas o equipos. |
| 6 | El sistema de control debe usar una protección contra código malicioso en todos los puntos de entrada y salida. | Se admite un sistema de detección de intrusos en la red que protege contra código malicioso. Se implementa un servidor centralizado con redes de protección para nodos remotos. |
| 7 | El sistema de control debe proteger la integridad de las sesiones. | Los equipos admiten protocolos cifrados. |
| 8 | El sistema de control debe proteger la información de auditoría. | Se utiliza un servidor de eventos como repositorio centralizado para registros de equipos. Los dispositivos terminales envían los registros al servidor de eventos. |
| 9 | El sistema de control debe proteger la confidencialidad de los accesos remotos que transitan por una red no confiable. | La VPN iniciada desde el firewall brinda seguridad para las conexiones por acceso remoto. |
| 10 | El sistema de control debe brindar la capacidad de segmentar en forma física las redes de sistemas de control de las redes de otros sistemas. | La comunicación desde los sistemas críticos transita por redes diferentes de las de los sistemas no críticos. |
| 11 | El sistema de control debe brindar una lista de componentes instalados con sus propiedades asociadas. | Los datos se registran en el repositorio. Esta capacidad puede proveerla el sistema de detección de intrusos. |

Tabla 3.

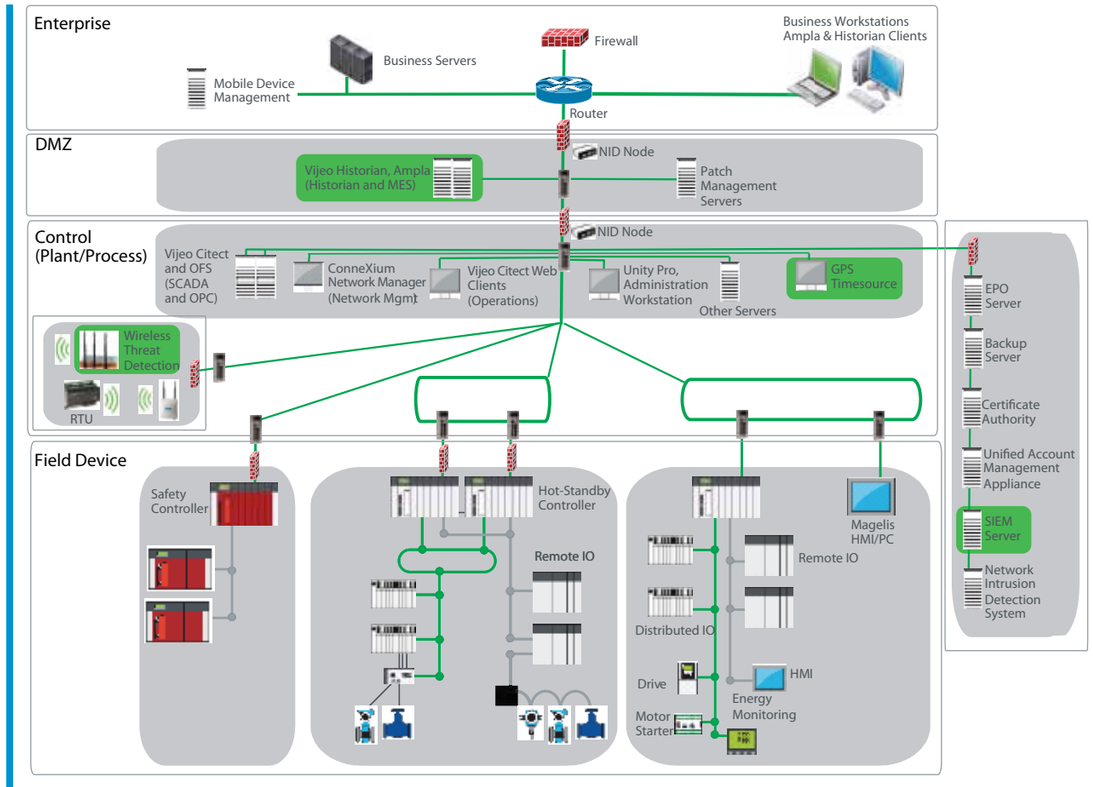



Figura 5

certificaciones de ciberseguridad en sus requisitos para adquisición de equipos

## Conclusión

La norma IEC 62443 brinda pautas esenciales para los usuarios finales que buscan contar con soluciones industriales seguras. Este marco de niveles de seguridad garantizados ayuda a agrupar requisitos de ciberseguridad para asistir en la implementación. Aumentar la seguridad del sistema puede dar como resultado la necesidad de actualizar equipos de ICS antiguos y de adquirir nuevos dispositivos de ciberseguridad. La inversión necesaria y la complejidad de la implementación se incrementarán al elevarse el nivel de seguridad deseado.

Un plan de seguridad detallado es esencial antes de iniciar cualquier trabajo en pos de brindar seguridad a una solución industrial. Los productos y las arquitecturas seguros son solo parte del proceso necesario. La capacitación del personal y políticas corporativas sensatas de seguridad son cruciales para brindar seguridad a los sistemas de control industrial. ❖

| N° de ítem | Requisito | Técnica para cumplir con el requisito |
|---|---|---|
| 1 | El sistema de control debe admitir autentificación de múltiples factores para interfaces no confiables. | Esta característica se habilita mediante la gestión de cuentas centralizada y los dispositivos terminales. |
| 2 | El sistema de control debe identificar y autentificar los procesos de software en forma unívoca. | Se admite esta característica mediante un servidor de certificados (Certificate Authority). También pueden usarse protocolos seguros. |
| 3 | El sistema de control debe admitir gestión de cuentas unificadas. | La gestión de cuentas unificadas se habilita con la gestión centralizada de cuentas. |
| 4 | El sistema de control debe proteger las claves privadas con mecanismos de hardware. | Se cuenta con un elemento seguro en los equipos de ICS. |
| 5 | El sistema de control debe identificar e informar la presencia de dispositivos inalámbricos no autorizados. | Se identifican los dispositivos inalámbricos no autorizados mediante el agregado de un dispositivo de detección de amenazas inalámbricas. |
| 6 | El sistema de control debe verificar la integridad del código para dispositivos móviles antes de permitir su ejecución. | La integridad del código para dispositivos móviles se verifica desde el servidor EPO y el servidor de certificados (Certificate Authority). |
| 7 | El sistema de control debe brindar un registro de auditoría con gestión central que abarque todo el sistema. | Los dispositivos terminales envían los archivos de memoria al servidor de monitoreo de eventos e información de seguridad (SIEM). |
| 8 | El sistema de control debe sincronizar el reloj interno del sistema a una frecuencia configurable. | Se agrega a la red un servidor de hora sincronizado por GPS. |
| 9 | El sistema de control puede admitir mecanismos criptográficos para reconocer cambios en la información durante las comunicaciones. | Esta capacidad se habilita mediante el uso de protocolos seguros. |
| 10 | El sistema de control debe gestionar en forma centralizada mecanismos de protección contra código malicioso. | Se protege contra código malicioso mediante el servidor EPO y el servidor SIEM. Todos los problemas detectados se reenvían al servidor SIEM. |
| 11 | El sistema de control debe admitir el respaldo automático a una frecuencia configurable. | La función de respaldo automático la admite el servidor para respaldo. |
| 12 | El sistema de control debe informar la configuración de seguridad actual en los dispositivos terminales. | El servidor EPO, juntamente con los sistemas de administración de redes informa las configuraciones de seguridad. |

Tabla 4

# Las cuatro aplicaciones más importantes de Internet industrial de las cosas

Plataforma IIoT EVO

**Ing. Gustavo Risi**
Cirlatina Argentina
*www.cirlatina.com.ar*

La irrupción del Internet de las cosas (IoT, por sus siglas en inglés) ha provocado grandes cambios en la industria por las oportunidades que brinda para reducir costos e incrementar la competitividad de las compañías.

Para llegar al *machine learning*, se han aplicado las tecnologías del IoT directamente en los procesos productivos para encontrar la excelencia en el rendimiento de sus máquinas e instalaciones. El Internet industrial de las cosas (IIoT, por sus siglas en inglés) se basa en medir, centralizar, controlar y analizar.

A continuación, mostramos cuatro de las aplicaciones que más se están beneficiando del IIoT.

*El Internet industrial de las cosas se basa en medir, centralizar, controlar y analizar.*

## 1. *Smart grid* y ahorro energético

La instalación de medidores para monitorización de energía en puntos estratégicos de nuestros edificios, fábricas y almacenes se ha vuelto completamente necesaria para poder realizar un seguimiento y control adecuado de los consumos y calidad de nuestra red eléctrica. La detección de fallas y la eficiencia energética son la base de este proceso.

## 2. Automatización industrial

El rendimiento de los procesos de producción se puede mejorar en gran medida gracias a la automatización industrial. Herramientas de automatización como un PLC (controlador lógico programable, por sus siglas en inglés) conectadas a dispositivos con conexión a plataformas en la nube permiten recoger datos, analizarlos y realizar acciones para mejorar su comportamiento. Aumentar la eficiencia de procesos, reducir errores, prevenir acciones de mantenimiento y el control remoto son los principales objetivos de cualquier proyecto de automatización industrial.

*Aumentar la eficiencia de procesos, reducir errores, prevenir acciones de mantenimiento y el control remoto son los principales objetivos de cualquier proyecto de automatización industrial.*

## 3. Mantenimiento predictivo

Las máquinas actuales requieren estar equipadas con sensores que monitoreen constantemente el estado de los componentes más críticos e importantes, para detectar cualquier problema crítico antes de que la maquinaria se resienta de un error que provoque su parada. Dichos sensores son los encargados de alertar a la plataforma en la nube, para que el aviso llegue a la persona a cargo del mantenimiento.

Gracias a dichos datos, se crean calendarios de mantenimiento remoto sin la necesidad de realizar tareas rutinarias que provoquen paradas innecesarias de maquinaria y líneas de producción.

## 4. Agricultura

El conocido "Smart Farming". Lejos de plantas industriales de producción, el IIoT ha permitido dar un salto de calidad a la agricultura gracias a la instalación de sensores en campos y granjas para la recolección masiva de datos.

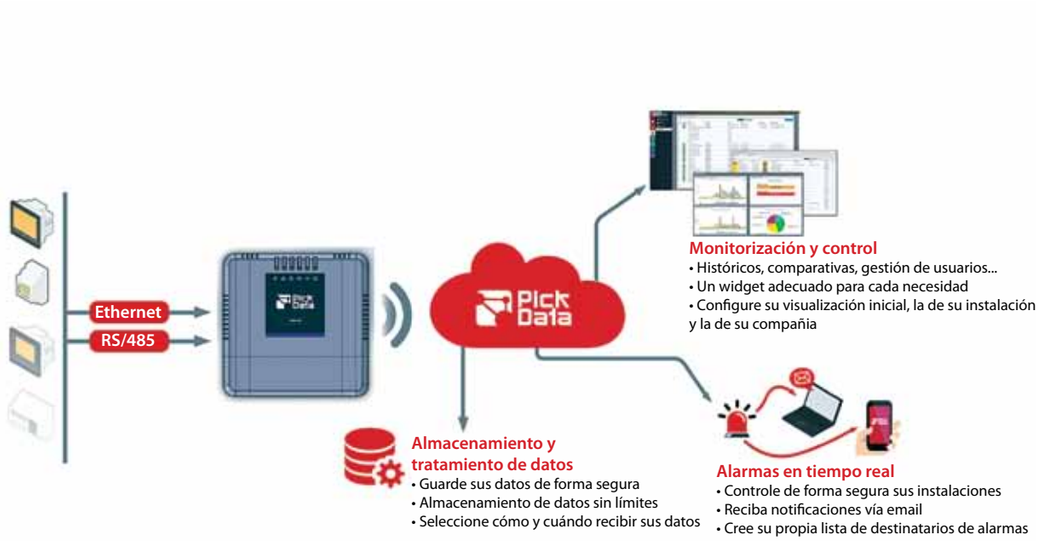



**Figura 1. Solución IIoT de *PickData***

En la agricultura, los procesos manuales rutinarios siempre han sido la parte menos productiva del negocio. Los sensores y las tecnologías inalámbricas actuales han permitido reducir los costos y aumentar la viabilidad de la automatización de la medición de la humedad y la riqueza del suelo. Además, combinado con la posibilidad de obtener las condiciones climatológicas en tiempo real, permiten optimizar la gestión remota de riegos de diferentes campos de forma simultánea.

*Los sensores y las tecnologías inalámbricas actuales han permitido reducir los costos y aumentar la viabilidad de la automatización de la medición de la humedad y la riqueza del suelo.*

## Una solución

Atendiendo a los requerimientos explicitados más arriba, *PickData* ofrece las herramientas necesarias para el concepto de IoT según el esquema de la figura 1.

Esta solución permite llevar los dispositivos al mundo del Internet de las cosas, y para ello se basa en tres grandes pilares: el gateway *Pick* VPN/3G, las comunicaciones integradas GPRS/3G y la plataforma IoT *Evo*.

Evo es la plataforma web encargada de recibir información en tiempo real de dispositivos repartidos por todo el planeta y almacenar, gestionar, monitorear o exportar esta información, recibir alarmas y tomar acciones, trabajar de forma simultánea con grandes volúmenes de dispositivos y datos, realizar análisis, visualizar los datos en múltiples widgets y generar informes específicos para cada aplicación.

Está permanentemente actualizada según las últimas tecnologías y se puede personalizar para cada cliente como si de un software propio se tratase.

En lo que al hardware concierne, *Pick* VPN/3G es un dispositivo diseñado específicamente para comunicar los sensores, máquinas, dispositivos o instalaciones con la plataforma a través de red móvil (GPRS/3G).

*Esta solución permite llevar los dispositivos al mundo del Internet de las cosas, y para ello se basa en tres grandes pilares: el gateway* Pick VPN/3G, *las comunicaciones integradas GPRS/3G y la plataforma IoT* Evo.

Asimismo, para aplicaciones especiales donde no encaje el gateway estándar, se pueden desarrollar gateways a medida con funcionalidades especiales.

Para enlazar software y hardware, la solución integra comunicaciones VPN globales de bajo costo a través de telefonía móvil (GPRS/3G), para enviar los datos desde todos los gateways hacia la plataforma, desde la mayor parte de países del planeta, reduciendo muy significativamente los costos de instalación y operación.

Este servicio se puede gestionar, monitorear, activar y desactivar con un solo clic, desde la propia plataforma web, en cualquier momento y para cualquier dispositivo. ❖





# Experiencia de una vida dedicada al control del gas

**Daniel Brudnick**
*dbrudnick@fibertel.com.ar*

Daniel Brudnick es ingeniero electromecánico con orientación electrónica e ingeniero especializado en gas. Con más de 35 años de experiencia en sistemas de medición, automatización y control en la industria del gas natural.

Cuando ingresé a Gas del Estado (GDE) como becario en 1981, cursando la carrera de posgrado de Ingeniería en Gas en el Instituto del Petróleo de la Universidad de Buenos Aires (IPUBA), no imaginaba todo lo que aprendería y la satisfacción que tendría al ver funcionando lo plasmado en planos, diagramas y circuitos.

Todo era nuevo para mí, pues la experiencia técnica y profesional recogida hasta ese entonces había sido en el desarrollo y la fabricación de equipos de audio y video.

Comencé en el Laboratorio Central de GDE reparando equipos para monitorear la calidad del gas. Allí, la especialidad electrónica parecía no "encajar" y hasta llegué a pensar que me había equivocado de empresa. Claro está, mis conocimientos sobre el gas se limitaban solamente a los artefactos domésticos y la factura bimestral que recibía en casa.

Las instalaciones que visité en aquella época, cuando GDE abarcaba todo el país, operaban manualmente y los controles, básicamente, eran neumáticos.

Para medir los volúmenes de gas, se utilizaban placas de orificio, unidades de presión diferencial y registradores de carta circular.

Los gráficos de presiones y temperatura se integraban con aparatos electromecánicos, obteniendo resultados que permitían facturar los consumos varios meses después de ser recogidos en el campo...

Los avances tecnológicos registrados en el campo de la electrónica, informática y comunicaciones fueron ganando aplicación en la industria del gas, y así me fui metiendo en lo que más me apasionaba: la instrumentación y el control de procesos.

Por inquietud propia y vocación docente, comencé a dictar cursos internos en GDE, capacitando a instrumentistas que luego llegaron a ser jefes de planta y gerentes. Más tarde, los cursos se extendieron a otras empresas, consejos profesionales e institutos.

A fines de 1991, con la privatización de GDE, continué trabajando en Transportadora de Gas del Sur (TGS), donde tuve la oportunidad de participar en proyectos y obras relacionadas con la automatización y el telecomando de plantas compresoras, supervisión y control remoto de estaciones de medición y regulación. Progresivamente, se fueron aplicando controladores lógicos programables (PLC), sistemas de control distribuido (DCS), unidades remotas (RTU), interfaces HMI, medidores ultrasónicos, transmisores inteligentes, analizadores, etc.

Con el nuevo equipamiento, TGS logró ampliar la capacidad del transporte de gas natural, mejorando la confiabilidad operativa, la calidad del servicio prestado y la exactitud de las mediciones fiscales, bajo las normativas del Ente Nacional Argentino Regulador del Gas (ENARGAS).

En el 2016, me jubilé con más de 35 años de labor en estas grandes empresas. Conocí lugares especiales y gente maravillosa, trabajé en lo que me gustaba, crecí profesionalmente y doy gracias por conservar muchas amistades. ❖

# Sistemas de almacenamiento vertical inteligente

**Daniel Guastadisegno**
DH Systems
*dguastadisegno@dhsystems.com.ar*

La mejor utilización de los recursos ha sido el motor de muchas de las invenciones.

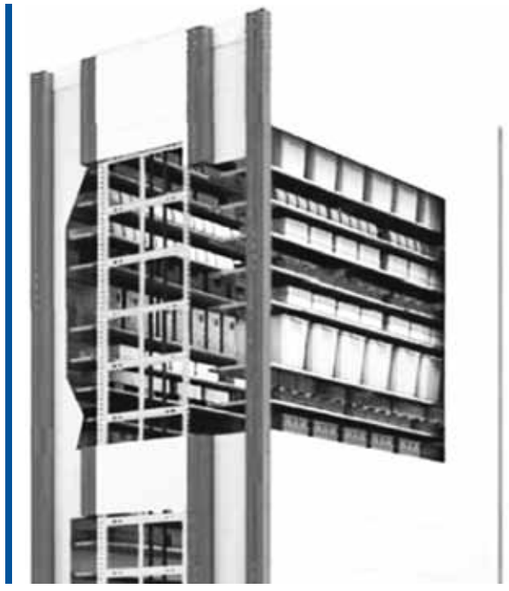
El alto costo por metro cuadrado, junto a las limitaciones de espacio, y la búsqueda de mejorar la tasa de utilización, ha puesto a los ingenieros a brindar más y mejores soluciones logísticas. Lograr soluciones en las que el material venga al hombre y no el hombre al material.

Una tecnología poco conocida, y de baja utilización en nuestro país, es el concepto de sistemas de almacenamiento vertical inteligente, el cual se puede presentar como almacenes tipo carrusel vertical (VLM, por sus siglas en inglés).

Un carrusel vertical está basado en el principio del *paternóster* (elevador circular, también conocido como "noria"). Se concibe específicamente para almacenamiento de pequeñas piezas, productos farmacéuticos, alimenticios, componentes electrónicos, repuestos y materiales diversos de pequeños volúmenes.

*El equipo, en base a la tasa de repetición de pedidos, tenderá a ubicar las piezas de mayor demanda en niveles más cercanos a la boca de expendio.*

El concepto básico del sistema es aprovechar intensamente los espacios verticales, con rapidez, agilidad y seguridad en el manejo y recuperación del material almacenado.



Paralelamente, es fácil integrar el conjunto de almacenes verticales a otros sistemas existentes en la planta, de manera de automatizar la gestión y control de materiales.

El VLM o lanzadera es un sistema ideal para el almacenamiento de piezas de diversos tamaños y cantidades, tal como turbinas de helicópteros, cajas de velocidad, engranajes, chips de computación, armamento, pañoles de repuestos, etc., logrando concentrar en una misma máquina diferentes tipos de mercadería, minimizando el espacio en planta y aprovechando los espacios verticales.

A su vez, es óptimo cuando se requiere la combinación entre velocidad de recogimiento (*picking*) y grandes volúmenes de almacenaje, logrando una ecuación equilibrada en el manejo y recuperación del material almacenado. Se pueden integrar con robots, cintas transportadoras, etc.

El operador, cuando requiere una pieza guardada en el equipo, disparará una orden al manipulador dentro de almacén, que buscará la bandeja en el nivel en el que la haya depositado previamente, y la llevará a nivel de despacho, en la zona de trabajo del operador, evitando pérdidas de tiempo por traslados en la búsqueda de piezas guardadas.

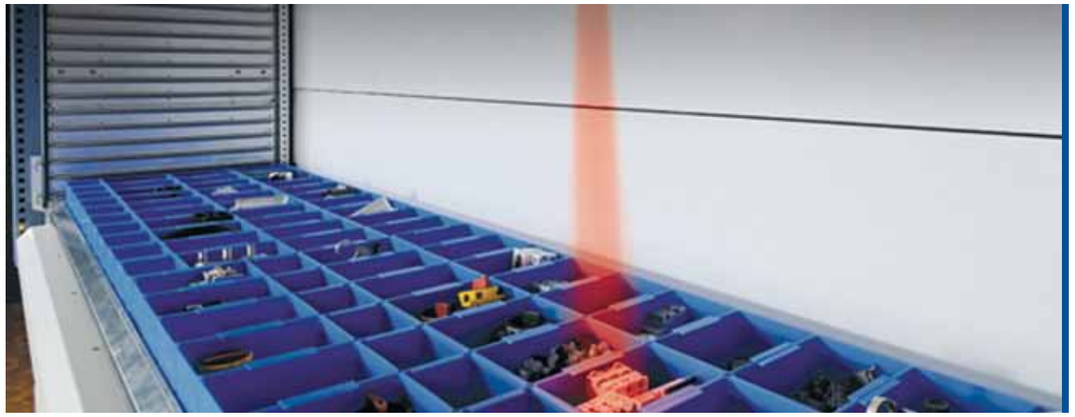
El equipo, en base a la tasa de repetición de pedidos, tenderá a ubicar las piezas de mayor demanda en niveles más cercanos a la boca de expendio, dejando las piezas de menor tasa de uso en los niveles superiores. Con este esquema, el equipo logra una mayor tasa de respuesta, un menor desgaste de partes móviles extendiendo su vida útil, y por sobre todo, un menor consumo energético.

*Se concibe específicamente para almacenamiento de pequeñas piezas, productos farmacéuticos, alimenticios, componentes electrónicos, repuestos y materiales diversos de pequeños volúmenes.*

Los sistemas de almacenamiento, y dependiendo de los productos que se almacenan, se pueden refrigerar a temperaturas acordes a los requerimientos técnicos del producto de cada cliente.

"Esta propuesta está alineada con la necesidad actual de eficientizar los recursos, que consiste en utilizar los recursos limitados de la Tierra de manera sostenible", declara el licenciado Gustavo Roisman, IT manager de *Ergometal*, única fábrica en Latinoamérica especializada en la producción de este tipo de almacenes, con tecnología desarrollada en el país.

Uno de los recursos, denominado como "Tierra" en la economía clásica, se puede asimilar a lo que en nuestros tiempos es la locación de un depósito. Cuanto más cerca de los ejes urbanos, más costoso será el metro cuadrado, por lo que toda empresa moderna que se preocupe por el medioambiente y la buena utilización de sus recursos debe pensar seriamente en la optimización de espacios, o en su maximización. ❖



# Software y servicios para la industria de gas y petróleo

Software para empresas de rango medio: *SAP Business One*

**Pragmatica**

*www.pragmaticaconsultores.com*

## Consultora especializada

Pragmática inició su actividad en el año 2001, a partir de identificar una oportunidad en el mercado de empresas de rango medio que requerían un asesoramiento profesional en materia de sistemas y procesos. Valiéndose de su propio perfil profesional, los socios fundadores (Ignacio Carnicero, contador público, y Cecilia Casanova, licenciada en Sistemas), diseñaron su oferta de servicios basada en los sistemas ERP (del inglés Enterprise Resourse Plannig , "planificación de recursos empresariales"), que buscan soportar el modelo operativo y administrativo de las empresas en una única plataforma de negocio integrada.

*En Neuquén, [SAP B1] cuenta con soporte local, tanto para llevar adelante el proceso de implementación como para brindar soporte y capacitación una vez que el sistema se encuentra operativo.*

La compañía cuenta con un plantel de consultores, profesionales con experiencia en procesos de la industria y certificaciones internacionales. Asimismo, todos sus procesos están certificados ISO 9001, desde el año 2009, por DNV-GL.

*SAP Business One*, en particular, es el sistema desarrollado para modernizar la gestión de información. Al software, Pragmática suma servicios asociados como aseguramiento de la calidad en la implementación, mesa de ayuda nivel 1, gerenciamiento de proyectos de implementación e implementación propiamente. En definitiva, la revisión de procesos proponiendo mejoras, el gerenciamiento de proyecto de cambio de sistemas y la gestión del cambio (*change management*) para apoyar los proyectos de cambio de sistemas y gestionar adecuadamente los impactos que estos tienen en las organizaciones.

Atendiendo principalmente las zonas de Neuquén y Río Negro, en el mercado nacional, ha desarrollado durante los últimos quince años diversos proyectos en compañías operadoras y de servicios, con experiencia concreta en compañías cuyo negocio se encuadra, tanto en el *upstream*, como en *midstream* y *downstream*.

*La compañía cuenta con un plantel de consultores, profesionales con experiencia en procesos de la industria y certificaciones internacionales.*

## El software de gestión

*SAP Business One* (*SAP B1*) es el software ERP para empresas de rango medio de *SAP*, la reconocida empresa alemana de sistemas de gestión para empresas.

Incluye módulos funcionales tales como "Ventas", "Stocks", "Compras", "Finanzas", "Activos Fijos", "Proyectos", "CRM", "Producción", etc., los cuales funcionan de manera integrada, generando información contable y alimentando indicadores de gestión en tiempo real.

Sus principales características son las siguientes:

- Incorporación de las mejores prácticas SAP
- Solidez tecnológica (HANA)
- Acceso web, dispositivo móvil, aplicación cliente servidor, escritorio remoto
- Modalidades de contratación: *on premise* (adquisición de licencias a perpetuidad, instalación en server propio), nube IAAS (del inglés, "infraestructura como un servicio", adquisición de licencias a perpetuidad, instalación en centros de datos de terceros), nube SAAS (del inglés, "software como un servicio": pago por uso, tanto de licencias como de infraestructura)
- Orientado a la gestión: KPI (indicadores) en tiempo real como pantalla de inicio de los distintos roles (grupos de usuarios)
- Trazabilidad y auditoría de todas las transacciones
- Contabilidad en tiempo real, bimonetaria
- Posibilidad de ampliar la funcionalidad nativa mediante incorporación de *Add Ons* (componentes desarrollados por terceras partes certificadas por SAP) o bien desarrollos a medida de cada cliente (funcionalidad específica o bien interfaces con sistemas preexistentes).

Asimismo, como elementos distintivos se destacan la escalabilidad de la solución, que garantiza acompañar en el tiempo el crecimiento de la empresa; el soporte postimplementación e implementación con consultores locales (Neuquén), y la localización del producto (adaptación a las normas

impositivas argentinas) realizada y soportada por *SAP* en forma directa.

La novedad del sistema reside en su tecnología. Su gestor de base de datos y fundamento es la plataforma HANA (del inglés, "aplicación analítica de alto rendimiento"). HANA es un componente que permite el procesamiento de grandes volúmenes de información en tiempos mínimos.

Adicionalmente, cuenta con diversas interfaces (web, aplicación de escritorio tradicional, dispositivo móvil) y la posibilidad de extender su funcionalidad mediante incorporación de desarrollos específicos para cubrir operatorias propias de cada empresa, o bien integrar aplicaciones pre existentes de terceros. También cuenta con una oferta de soluciones desarrolladas por terceras partes, que se integran por medio de soluciones verticales para distintas industrias (de "nicho").

Estas características posibilitan integrar la totalidad de los procesos corporativos en una única solución de software, una verdadera plataforma de negocios.

*[Pragmática cuenta] con experiencia concreta en compañías cuyo negocio se encuadra, tanto en el upstream, como en midstream y downstream.*

## Comercialización

Una licencia *SAP B1* habilita el acceso a la totalidad de las transacciones/funciones del sistema. Las restricciones se aplican desde la gestión de seguridad del sistema, es decir, cada usuario tendrá acceso a consultar o modificar información en función de lo que la empresa determine, más allá de lo que su "tipo de licencia" le permita. Esto significa que el producto no se comercializa por módulos independientes.

Cuenta con distintos tipos de licencias, profesionales y limitadas, con distinto costo, lo cual optimiza la inversión en licencias del producto, limitando en función de las necesidades de uso del sistema que hará cada usuario.

## En el mundo, en Argentina, en Neuquén

*SAP B1* se utiliza en más de 150 países, en veintisiete idiomas, desde hace veinte años. Actualmente lo utilizan más de un millón de usuarios en el mundo. En Argentina se comercializa desde hace tres años (momento en que *SAP* la puso disponible para el país), y cuenta con una base de más de trescientos clientes. En Neuquén, cuenta con soporte local, tanto para llevar adelante el proceso de implementación como para brindar soporte y capacitación una vez que el sistema se encuentra operativo. ❖





# Manómetro digital de precisión

Modelo CPG 1500, para industria de petróleo y gas, áreas de reparación y servicio, servicio de calibración y mantenimiento, calibraciones fáciles in situ y prueba de presión

**Wika**
*www.wika.com.ar*


El manómetro digital *CPG 1500*, de *Wika*, ofrece soluciones adecuadas para mediciones con una mayor precisión y una mayor capacidad requerida. Está diseñado para aplicaciones en petróleo y gas, generación de energía petroquímica, servicios de calibración y farmacéutica. Combina durabilidad de un medidor analógico en un gran dispositivo, con características valiosas a nivel de solución.

*El equipo proporciona una exactitud de 0,1 por ciento del valor final de escala.*

El equipo proporciona una exactitud de 0,1 por ciento del valor final de escala (opcionalmente 0,05 o 0,025 por ciento del valor final de escala) con compensación de temperatura en el rango de menos diez a cincuenta grados centígrados (-10 a 50 °C).

Es posible mostrar las mediciones en una de las veintiséis unidades de presión y cinco unidades de nivel, o también en unidades específicas del cliente, para evitar conversiones complicadas.

El dispositivo ofrece diversas configuraciones para servir a diferentes necesidades. Asimismo, cuenta con especificaciones aprobadas para todo tipo de industria, como ser protección contra polvo, agua a baja presión, exposición a ambientes de alta humedad, exposición a condiciones extremas de calor, frío y humedad. Las certificaciones internacionales que lo respaldan son Ex, IEC, IECEx, EAC Ex y CSA US.

*Es posible mostrar las mediciones en una de las veintiséis unidades de presión y cinco unidades de nivel, o también en unidades específicas del cliente.*

Para responder a las demandas de la tecnología digital actuales, posee un registrador de datos de gran capacidad, cuya batería tiene una duración de hasta 2.500 horas. Asimismo, no se necesitan cables para el registro de datos y todo se puede configurar en el mismo dispositivo, a través de una aplicación descargable. ❖

# Una serpiente en el cerebro

Prof. Roberto Ángel Urriza Macagno
*robertourriza@yahoo.com.ar*

## La complejidad del procedimiento en la actualidad

Los infartos cerebrales son la primera causa de muerte y discapacidad en Estados Unidos; se sabe que si no se tratan durante los primeros noventa minutos, decrecen de forma dramática las posibilidades de supervivencia del paciente. El problema es que el proceso de desatascar un conducto cerebral es muy complejo, por lo general, implica una intervención quirúrgica en la que los cirujanos deben manipular un delicado catéter encargado de llevar fármacos que disuelvan la obstrucción.

El procedimiento es harto complejo, pasible de provocar nuevos daños en el cerebro, y además obliga al paciente y a los propios médicos a someterse a una dosis usualmente elevada de radiación, procedente de un fluoroscopio que permite ver el cerebro del paciente por rayos X en tiempo real, necesario para guiar el catéter.

## El robot-serpiente

Investigadores del Instituto Tecnológico de Massachusetts (MIT, en Estados Unidos) crearon un robot con forma de serpiente o gusano para combatir los coágulos en el cerebro y aneurismas.

Este robot-serpiente tiene menos de un milímetro (1 mm) de espesor y puede viajar por las venas hasta llegar al cerebro y sin posibilidad alguna de atorarse en el camino o en su destino.

El sistema fue diseñado con materiales magnéticos y flexibles, por ello es capaz de navegar de forma ágil por las venas delgadas, con mucha facilidad.

Gracias al conocimiento de los hidrogeles basados en agua, y al uso de imanes para manipular pequeños robots, los ingenieros crearon esta serpiente o gusano, fabricada con una aleación plegable de níquel-titanio, con memoria de forma.

El núcleo de la serpiente se recubrió de un hidrogel, lo cual le permite deslizarse por el interior de un vaso sanguíneo sin provocar fricción que lo dañe.

Este robot se guía mediante un campo magnético variable que puede situarse a la suficiente distancia como para que quede fuera del cráneo del paciente, y sin radioactividad.

## Logros y futuras investigaciones

La primera prueba ha sido una pista de obstáculos formada por pequeños anillos. La segunda ha sido un modelo del cerebro formado por un complejo entramado de conductos que imitan los vasos sanguíneos. Ambas fueron superadas con éxito.

Este robot puede aún seguir desarrollándose para portar herramientas o fármacos que disuelvan el coágulo antes de que el daño cerebral sea irreversible, incluso es posible sustituir el cable interno de titanio por uno de fibra óptica, de manera que el robot pueda emitir pulsos láser desde la punta.

Por otro lado, en el estado actual de la investigación, se está trabajando para que sea el médico mismo quien controle el robot, solo para el caso en el que se produzca algún inconveniente, ya que la responsabilidad es muy alta. Por supuesto, las experimentaciones se realizan sobre animales, no sobre personas.

## Conclusiones

No cabe duda de que el empleo de estos robots va a permitir una enorme ayuda a pacientes con aneurismas o coágulos en el cerebro. No solo hará que las cirugías, en caso de infarto cerebral, sean mucho más rápidas, incluso evitará la exposición a la radioactividad. ❖

**Sergio Szklanny**
*svs@svsconsultores.com.ar*

# No todo es automatización y control

Sergio Szklanny es ingeniero químico egresado de la Universidad de Buenos Aires. Es director de *SVS Consultores*, profesor de la Universidad Tecnológica Nacional Regional Buenos Aires, responsable del Grupo de Automatización y Control con Tecnología Informática Industrial (ACTII) y coordinador editorial de la *Revista de AADECA*. Con más de cuarenta años de experiencia, trabajó en las áreas de procesos y de instrumentación y control en empresas como CNEA, *Techint*, *UTE Orimas/Roggio, Mc Kee del Plata* y *Foxboro Invensys*. Fue docente en la UBA. Fue Presidente de AADECA.

*En mis más de cuarenta años como profesional, atravesé por las distintas etapas que un profesional de nuestro país suele transitar: como hijo de inmigrantes trabajadores del calzado, lograr un crecimiento pasaba por estudiar y trabajar. La dificultad de encontrar un primer trabajo, ser docente ad honorem por años en la "Facu", sufrir los avatares de la Argentina (desde los "famosos" '70), con ciclos de cierre de empresas y, a veces, crecimiento. Tuve momentos difíciles y momentos muy buenos, hasta que la suerte de un crecimiento permanente me permitió llegar a puestos gerenciales con muy buenos trabajos pero con demasiada dedicación (casi adicto al trabajo). En ese momento, los avisos del cuerpo ("estrés", lo llaman) me hicieron replantear mi futuro y fui emprendedor a los 45 años, fundando la empresa en donde hasta el día de hoy me desempeño, trabajo y me divierto con el tema que siempre me gustó como profesión y sin dejar en ningún momento de dar capacitación (mi otra gran pasión), en la empresa o en ámbitos académicos.*

*Desde siempre he sido un deportista mediocre, no jugué bien al fútbol (en el secundario me mandaban siempre al arco). Pero tampoco era de lo peor (en fútbol, sí…). El vóley apareció como oportunidad… En la universidad jugué también algo de handball, pero nunca dejé de jugar al vóley, deporte más que interesante, si los hay: requiere reflejos, buen estado y, como todo, técnica. Además es altamente eficiente (doce personas en un espacio de nueve por dieciocho metros) y lo más interesante es el compañerismo y el divertimento. No puede ser un juego individual, los tres pases son la mejor táctica para ganar un punto, y conocer las fortalezas y debilidades de los compañeros es fundamental para divertirme (ganar, para mí a esta altura, es secundario).*

*¡Y de grande, viruela! A los 45 años el cambio laboral vino acompañado con salir del sedentarismo. ¡Comencé a entrenar en vóley! No soy alto, por lo que debo ser armador (el que busca la segunda pelota y la "arma" al pegador), y si bien mi habilidad es limitada, ir a todas, picar y llegar y levantar pelotas complicadas suelen estar entre mis virtudes (mis defectos no los cuento, solo uno: suelo hablar comentando cómo podemos tratar de mejorar en el equipo después de cada punto… ¿deformación profesional docente ingenieril? Algunos aprecian esos comentarios. ¿Y hoy? Algo casi increíble: juego junto a un grupo de más de dieciocho personas mayores de sesenta años (más de uno tiene más de ochenta), dos a tres veces por semana. Y lo más interesante es el horario: ¡De 8 a 9.30 de la mañana! Primero, media hora de gimnasia y entrenamiento (la profe, Clarissa, muy didáctica, piola y dedicada) y después, una hora de juego. Después, ducha, café y ¡a trabajar! Les aseguro que el hacer este tipo de actividad me mantiene el ánimo altamente positivo y me permite enfrentar las obligaciones de otra forma, con la mente despejada y el físico ejercitado… Y respecto del buen momento de las discusiones y debates en el café, ¡impagables y enriquecedoras! Después, no importa dar clases o trabajar más allá de las 21 horas, si hace falta.. ¡El cuerpo a los 66 aguanta! (al menos hasta que aguante).*

*No puedo dejar de comentar que el sábado por la mañana hay partido de tenis (dobles) con otro grupo igual de divertido. (Se me van a enojar los tenistas si no los menciono).*

*Recomiendo no descuidar el físico desde muy joven, es algo único que no podemos reemplazar. Hacer deportes (cualquiera, pero hacerlo activamente) es una buena receta para llegar bastante entero a los 66 años que tengo y poder alzar sin problemas a mis hermosos nietos.*

*Disfruten de la vida, que vale la pena ser vivida.* ❖

# AADECA

## Glosario de siglas de la presente edición

**AADECA**: Asociación Argentina de Control Automático

**ADACSI**: Asociación de Auditoría y Control de Sistemas de Información

***AG*** *(Aktiengesellschaft)*: sociedad anónima

***ANSI*** *(American National Standadrs Institute)*: Instituto Nacional Estadounidense de Normalización

***ANSSI*** *(Agence Nationale de la Sécurité des Systèmes d'Information)*: Agencia Nacional de Seguridad de Sistemas de Información (de Francia)

***ASME*** *(American Society of Mechanical Engineers)*: Sociedad Estadounidense de Ingenieros Mecánicos

**ATEX**: atmósferas explosivas

***CAD*** *(Computer Aided Design)*: diseño asistido por computadoras

**CE**: Comisión Europea

***CIO*** *(Chief Information Officer)*: director de Informática

***CISM*** *(Certified Information Security Management)*: gestión de seguridad de la información certificada

***CISO*** *(Chief Information Security Officer)*: director de seguridad de la información

***COO*** *(Chief Operating Officer)*: director de operaciones

***CSA*** *(Canadian Stanrdard Association)*: Asociación Canadiense de Normalización

***DBB*** *(Double Block and Bleed)*: doble bloqueo y purga

***DCS*** *(Distributed Control System)*: sistema de control distribuido

***DDoS*** *(Distributed DoS)*: DoS distribuido

***DMZ*** *(Demilitarized Zone)*: zona desmilitarizada

***DNV***: *Det Norske Veritas*

**DNV GL**: DNV y Germanischer Lloyd

***DoS*** *(Denial of Service)*: denegación de servicio

***EAC*** *(Eurasian Conformity)*: conformidad euro-asiática

***EACEx*** *(EAC Explosive)*: EAC explosivo

**ENARGAS**: Ente Nacional Argentino Regulador del Gas

***EPO*** *(Emergency Power Off)*: apagado de emergencia

***ERP*** *(Enterprise Resource Planning)*: planificación de recursos empresariales

**GDE**: Gas del Estado

***GOST*** *(Gosudarstvenny Standart)*: Estándar del Estado (de Rusia)

***GPRS*** *(General Packet Radio Service)*: Servicio general de paquetes vía radio

***HANA*** *(High Performance Analytic Appliance)*: aplicación analítica de alto rendimiento

***HMI*** *(Human-Machine Interface)*: interfaz humano-máquina

***IAAS*** *(Infraestructure as a Service)*: infraestructura como un servicio

**IAIA**: Instituto de Auditores Internos de Argentina

***ICS*** *(Industrial Control System)*: sistema de control industrial

***ICS*** *(Information and Communication Solutions)*: soluciones de información y comunicación

***IEC*** *(International Electrotechnical Comission)*: Comisión Electrotécnica Internacional

***IECEx*** *(IEC Explosive)*: IEC Explosivo

***IIoT*** *(Industrial IoT)*: IoT industrial

***INMETRO*** *(Instituto Nacional de Metrologia, Qualidade e Tecnologia)*: Instituto Nacional de Metrología y Calidad y Tecnología (de Brasil)

***IoT*** *(Internet of Things)*: Internet de las cosas

***IP*** *(Internet Protocol)*: protocolo de Internet

***IPsec*** *(IP security)*: seguridad IP

**IPUBA**: Instituto de Petróleo de la UBA

***ISA*** *(International Society of Automation)*: Sociedad Internacional de Automatización (ex-Sociedad Estadounidense de Automatización)

***ISO*** *(International Standard Organization)*: Organización Internacional de Normalización

***IT*** *(Information Technologies)*: tecnologías de la información

***KPI*** *(Key Performance Indicator)*: indicador de clave de desempeño

***NERC*** *(North American Electric Reliability Corporation)*: Corporación Norteamericana de Fiabilidad Eléctrica (de Estados Unidos, Canadá y México)

***NERC CIP*** *(NERC Critical Infrastructure Protection)*: NERC de protección de infraestructura crítica

***NIST*** *(National Institute of Standards and Technology)*: Instituto Nacional de Estándares y Tecnología (de Estados Unidos)

***NPL*** *(National Physical Laboratory)*: Laboratorio Nacional de Física (de Reino Unido)

**OpenVPN**: VPN abierto

***OT*** *(Operational Technology)*: tecnología operacional

***PC*** *(Personal Computer)*: computadora personal

***PLC*** *(Programmable Logic Controller)*: controlador lógico programable

***PMS*** *(Power Managemente System)*: sistema de gestión de potencia

***PROFIBUS DP*** *(Process Field Bus Decentralised Peripherals)*: bus de campo de proceso periférico decsentralizado

***RTU*** *(Remote Terminal Unit)*: unidad terminal remota

**SA**: sociedad anónima

***SAAS*** *(Software as a Service)*: software como un servicio

***SAP*** *(Systems, Applications and Products)*: sistemas, aplicaciones y ptoductos

***SCADA*** *(Supervisory Control and Data Acquisition)*: supervisión, control y adquisición de datos

***SIL*** *(Safety Integrrity Level)*: nivel de integridad de seguridad

***SIS*** *(Safety Instrumented Systems)*: sistemas instrumentados de seguridad

***SL*** *(Security Level)*: nivel de seguridad

**SRL**: sociedad de responsabilidad limitada

***STL*** *(Standard Triangle Language)*: lenguaje de triángulos estándar

**TGS**: Transportadora de Gas del Sur

**TI**: tecnología de la información

**TIC**: tecnologías de la información y comunicación

**TO**: tecnología operacional

**UBA**: Universidad de Buenos Aires

***VLAN*** *(Virtual Local Area Network)*: red virtual de área local

***VLM*** *(Vertical Lift Module)*: módulo de almacenamiento vertical

***VPN*** *(Virtual Private Network)*: red privada virtual

***WLAN*** *(Wireless Local Area Network)*: Red de área local inalámbrica


# AADECA

Asociación Argentina
de Control Automático

NEWSLETTER

INTERCAMBIO
PROFESIONAL

TALLERES
TEMÁTICOS

FORO

CURSOS Y
JORNADAS

CONGRESOS

**www.aadeca.org**

CV CONTROL

BAKER HUGHES
a GE company

Channel Partner

# Líderes en Calibración de Presión y Temperatura


DPI620 Genii, base, carrier, bomba y módulos

DPI612 Flex

TC Series

www.cvcontrol.com.ar | ventas@cvcontrol.com.ar