7
Noviembre
Diciembre
2017

AADECA

La Revista de los Profesionales de Automatización y Control

Seguridad industrial y ciberseguridad

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

SEMANA DEL CONTROL AUTOMÁTICO

AADECA '18

Buenos Aires, 13, 14 y 15 de noviembre de 2018

- 26º Congreso Argentino de Control Automático
  - Presentación de trabajos de los grupos de investigación
  - Sesión especial de trabajos de la industria
  - Prestigiosas conferencias plenarias
- Concurso "Desarrollos Estudiantiles" Colegios técnicos y universidades
- Foro de Automatización y Control
- Cursos de actualización
- Mesas de intercambio entre PYMES y de servicios y mucho más ...

ORGANIZA

AADECA

Asociación Argentina de Control Automático

INFORMES

+54 (11) 4374-3780

congreso2018@aadeca.org

aadeca.org

Sede AADECA
Av. Callao 220 piso 7
Ciudad Autónoma de Buenos Aires
(C1022AAP) Argentina

Control inteligente aquí. **Empleados empoderados aquí.**

Convierta la automatización industrial en el generador de ganancias en su empresa

La Internet Industrial de las Cosas está transformando a la industria. La tecnologia y el expertise de Schneider Electric pueden ayudarlo a desbloquear todo el potencial de sus operaciones y a cambiar el gerenciamiento de su empresa brindándole el control absoluto en tiempo real.

Con control inteligente y el empoderamiento de sus empleados, Usted puede optimizar continuamente el desempeño de sus activos industriales, con mediciones que mejoran el rendimiento operativo, la seguridad y la sustentabilidad.

Bienvenido al futuro de la automatización.

schneider-electric.com/smartoperations

Life Is On Schneider Electric

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

La seguridad en la era de la industria 4.0

La seguridad es y ha sido una de las áreas prioritarias en diseño, operación y mantenimiento de plantas de producción.

En la industria de procesos, un adecuado diseño considerando todas las especialidades (mecánica, eléctrica, civil, del proceso y de la instrumentación y control, etc.) se complementa generalmente con un sistema instrumentado de seguridad (SIS). Estas especialidades de diseño deben, además, sustentarse en metodologías y personal competente (con conocimientos y experiencia), para que a través de una tarea rigurosa, y probada, se evalúen todas las posibilidades de fallas, tanto del equipamiento como humanas, y se dé importancia a todas las situaciones que pudieren afectar la seguridad, creando los mecanismos tendientes a evitar los peligros y a controlar los riesgos. Esto es: se debe contar con un adecuado sistema de gestión de la seguridad funcional.

Partes imprescindibles para garantizar que la seguridad cumpla con los objetivos buscados son: un correcto diseño y mantenimiento de las alarmas, los enclavamientos de seguridad, las válvulas de seguridad, la instalación, y un sistema orientado a la seguridad bajo metodologías adecuadas y con participación de profesionales idóneos debidamente calificados. Es imperioso el permanente cuidado, concientización y presencia de los especialistas en seguridad, para no degradar lo diseñado con operatorias erróneas, o por el incumplimiento de procedimientos que han sido diseñados precisamente para evitar desastres. Incumplimientos que, sin embargo, vemos en forma frecuente, como el forzado de salidas, la anulación de enclavamientos, etc.

Esto no es nuevo. Hacia fines del siglo pasado, varios accidentes aceleraron el proceso de desarrollar metodologías, diseños, normativas, y la necesidad de generar personal competente y equipamiento adecuado para evitar los desastres que se produjeron, como el de Flixborough, en 1974; o el escape de radiación de la central nuclear de Three Mile Island, en 1979; o la planta química de Bophal, en India, en 1984, etc. Sin embargo, esto no evitó los más recientes desastres, como el derrame del Golfo de México en 2010, y otros, lo que nos muestra que, pese a los avances logrados, no hay que descuidarse, ya que fallas sistemáticas durante el diseño, la ingeniería, la operación o el mantenimiento (generalmente derivadas del apuro por producir) conducen a situaciones catastróficas.

En este nuevo siglo, el de la industria 4.0, en la cual la cibernética juega un rol fundamental, se nos presentan nuevos desafíos para mantener la seguridad. Por eso, la última revisión de la norma IEC 61511 (seguridad funcional para la industria de procesos) incluye la necesidad de proteger los SIS contra los ciberataques. En palabras de la norma: "El diseño del SIS debe ser tal que provea la necesaria resiliencia contra los riesgos de seguridad (*security*) identificados".

Podríamos decir entonces que, en la era de la industria 4.0, necesitamos también seguridad 4.0. En este número, expertos describen las normas, las cualidades humanas y técnicas requeridas y las buenas prácticas que deben llevarse a cabo.

Destacamos el hecho de que en AADECA se brindan cursos relativos a seguridad, que existen bibliografía y cuadernillos profesionales, así como especialistas vinculados a la institución que pueden ser aprovechados por aquellos que tengan problemas puntuales o que deseen profundizar en el tema.

Un cordial saludo a todos los colegas por el Día del Profesional de la Instrumentación, Automatización y Control (25 de Noviembre).

Nota: el autor de este editorial agradece a Lic. Ricardo Vittoni por su contribución a este editorial

Edición 7
Noviembre/Diciembre 2017

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

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

Impresión
Grafica Offset
Santa Elena 328 - CABA

R.N.P.I.: N°5341453
ISSN: *a definir*

En esta edición encontrará los siguientes contenidos

Reporte especial

Seguridad industrial y ciberseguridad

Además...

Estas empresas acompañan a AADECA Revista

Asamblea Anual Ordinaria de asociados y cena de camaradería

AADECA, *www.aadeca.org*

El pasado 28 de noviembre de 2017, en la Ciudad Autónoma de Buenos Aires, se celebró la Asamblea Anual Ordinaria de asociados de AADECA, con gran participaron de sus socios.

Se informó y aprobó por unanimidad el balance y otros estados contables cerrados al 1º de octubre de 2017.

Marcelo Petrelli, secretario general, presentó la memoria anual de actividades, finalizada al 31 de octubre del corriente año, la cual también fue aprobada por unanimidad.

Además, se hizo entrega de una plaqueta a los socios activos vitalicios que se incorporan este año a esta categoría por haber cumplido una membresía ininterrumpida en la Asociación de más de veinticinco años.

Cena de camaradería

A continuación se celebró la cena anual de camaradería en el restaurante Puerto Cristal de Puerto Madero; disfrutando de un ambiente ameno entre amigos y colegas pudimos compartir nuestras experiencias, proyectos y vivencias.

Nuestro actual Consejo Directivo (2016 – 2018)

Presidente: Diego Maceri
Vicepresidente 1º: Luis Pérez
Vicepresidente 2º: Carlos Behrends
Secretario general: Marcelo Petrelli
Prosecretario: Roberto Schottlender
Tesorero: Marcelo Canay
Protesorero: Ariel Lempel
Vocal titular 1º: Luis Buresti
Vocal titular 2º: Gustavo Klein
Vocal titular 3º: Norma Gallegos
Vocal supl. 1º: Eduardo Fondevila Sancet
Vocal suplente 2º: Norma Toneguzzo

Socios adherentes

Automación Micromecánica | **Cruxar** | **CV Control** | **Editores** | **Emerson** | **Festo** | **Grexor** | **Honeywell** | **Marlew** | **Pepperl+Fuchs Argentina** | **Phoenix Contact** | **Raien Argentina** | **Schneider Electric Argentina** | **Siemens** | **Soluciones en Control** | **Supertec** | **SVS Consultores** | **Viditec**

¿Desea recibir AADECA Revista?

Socios AADECA: Gratis
No socios: Suscripción por 6 ediciones corridas, $350

Más información, suscripcion@editores.com.ar

El estado actual de la ciberseguridad industrial en la Argentina

Enrique Larrieu-Let
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.

elarrieulet@gmail.com

El Centro de Ciberseguridad Industrial (CCI), dirigido por José Valiente y Miguel García Menendez, es una organización internacional, independiente, sin fines de lucro, con sede en España, cuya misión es impulsar y contribuir a la mejora de la ciberseguridad industrial. La entidad acaba de publicar (octubre de 2017), la primera edición del informe "Estudio sobre el estado de la ciberseguridad industrial en Argentina – Edición 2017".

Considero que este documento debe ser leído por todos los involucrados tanto en las decisiones estratégicas de negocio y de gobierno de las tecnologías como en las actividades tácticas del día a día vinculadas a las operaciones de tecnología de la información (TI) y los procesos de tecnologías operacionales (TO).

La idea de este artículo no es hacer catarsis, ni mucho menos que nos paralicemos, sino que sirva de reflexión y concienciación para que reaccionemos en resolver las falencias que detectemos en nuestras propias organizaciones al tratar de respondernos las preguntas que propone el estudio.

A continuación, una breve síntesis del contenido del estudio y sus principales conclusiones.

En su prólogo, el Ing. Gerardo Fabián González expresa "La ciberseguridad es una capacidad propia de las organizaciones para defender y anticipar amenazas y vulnerabilidades digitales, minimizando las consecuencias dentro del ecosistema en el que operan y asegurando la resiliencia tecnológica y operativa (TI y TO).

"Siendo esta una capacidad propia de las organizaciones, es fundamental recalcar la importancia de la concienciación de los altos directivos y que la ciberseguridad industrial forme parte destacada entre los puntos de sus agendas.

En este momento de transformación digital del sector industrial es imprescindible darnos cuenta de que la mayor amenaza no son los ciberataques derivados de la hiperconectividad, sino de no saber cómo manejar la gestión de riesgos que la ciberseguridad industrial nos trae aparejada en esta etapa de la Industria 4.0 y la Internet industrial de las cosas (IIoT)".

El estudio se ha realizado de manera *online*. Se envió por correo electrónico, con un formulario adjunto, a gestores de empresas argentinas. Durante el tiempo en el que el formulario estuvo abierto, desde el 4 de mayo de 2016 hasta el 22 de junio de 2017, 35 empresas industriales lo diligenciaron íntegramente.

Las empresas analizadas abarcan los principales sectores de la economía argentina, destacando, en primer lugar, las del sector TI, seguidas de las de petróleo y gas, y, en tercer lugar, las del sector eléctrico y fabricación.

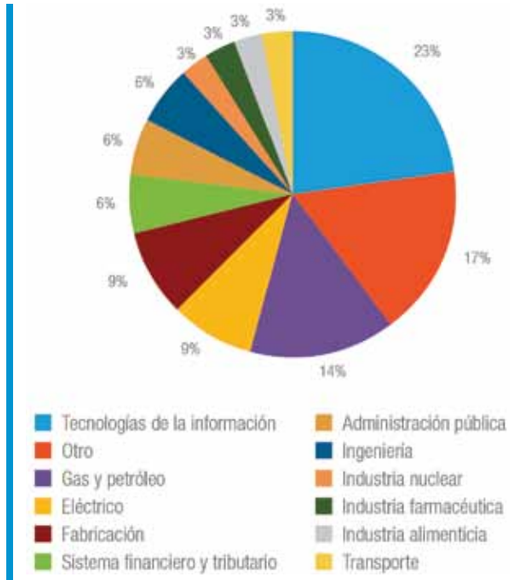


Figura 1. Sector de la organización a la que representa la empresa

En el documento, en este punto, se realiza un análisis referido a la envergadura y capacidad de las empresas, sus necesidades y particularidades respecto de la ciberseguridad y el motivo de sus respuestas disímiles.

Otro de los temas que se trata en el estudio, y que está en permanente discusión en las distintas organizaciones, es el de la responsabilidad respecto a la ciberseguridad industrial.

En este aspecto, se consultó a las empresas lo siguiente: ¿quién/es tiene/n en su organización la responsabilidad de proteger, en materia de ciberseguridad, los sistemas de automatización y control industrial? El documento grafica la respuesta involucrando a los distintos roles, desde seguridad física, pasando por los distintos actores de las áreas de TI y de TO. Las respuestas todavía muestran la supremacía de las áreas de TI en ocuparse de temas vinculados a la seguridad de las redes industriales, y muy pocas empresas encuestadas, solo el 3,2 por ciento, ha identificado al responsable de seguridad en los sistemas de automatización y control industrial (CISO) como responsable de la materia.

Otra pregunta realizada en la encuesta dentro de este punto fue: ¿cómo participan las distintas áreas de la organización en los aspectos de ciberseguridad? Teniendo en cuenta todas las áreas de la empresa, desde TI, hasta las áreas financieras, pasando por TO y recursos humanos, entre otras, de las respuestas se observa cómo el área TI tiene la mayor participación, seguida de las áreas de TO y las áreas de seguridad de la información y seguridad informática.

En cuanto a concienciación de las áreas del negocio, se consultó lo siguiente: ¿los responsables del negocio están sensibilizados con las normas y los riesgos de la seguridad de las redes industriales? Las respuestas muestran que únicamente el diez por ciento (10%) de los gestores afirma estar muy sensibilizado frente a estos riesgos. De lo anterior se puede concluir que queda todavía un camino largo por recorrer en términos de esfuerzo de concienciación a nivel directivo.

Grado de capacitación en ciberseguridad industrial

Con respecto a la capacitación, la consulta fue: ¿cuál es el grado de capacitación de su organización en ciberseguridad industrial? En este aspecto, se confirma lo que se sospechaba, y es que las empresas industriales argentinas invierten más en la capacitación de los departamentos que están directamente relacionados con la tecnología y la seguridad de la información (TI y SI) que en la capacitación de los responsables del mantenimiento de las TO, siendo que estas tecnologías son las que sostienen los procesos productivos que son el corazón de los negocios, y que TI y SI existen para dar soporte al resto de la organización.

A continuación el documento trata dos temas que considero centrales: evaluación de riesgos y gestión de incidencias de seguridad.

» Evaluación de riesgos: se consultó ¿si la empresa había realizado evaluaciones del nivel de

Figura 3. Accesos remotos en Argentina

Figura 2. Nivel de implementación de gestión de incidencias de seguridad en Argentina

riesgo de los sistemas de automatización y control? Los datos indican que cerca de la mitad de las industrias no ha realizado ningún tipo de evaluación de riesgos, lo cual es tremendamente preocupante, en particular por la magnitud y nivel crítico de las empresas que han participado en este estudio.

» Gestión de incidencias de seguridad: la pregunta fue cómo era el proceso de gestión de incidencias de seguridad en las redes de automatización de la empresa. En este caso, el resultado fue que solo un 12,9 por ciento de las empresas estudiadas afirma tener un proceso de gestión de incidencias de ciberseguridad industrial desarrollado y en aplicación. No es de extrañar este pobre resultado cuando en la mayoría de las empresas tampoco existe este proceso de gestión en las áreas de TI y SI.

Hasta aquí el documento se ocupó de los aspectos organizativos y de gestión. A continuación, el estudio se ocupa de los aspectos técnicos de la ciberseguridad industrial. Los temas planteados son las conexiones de redes, los accesos remotos, el uso de normas y patrones y las medidas de ciberseguridad industrial.

Sobre el tema de conexiones a redes se consultó si las redes de automatización de la empresa estaban segmentadas y protegidas. La mayor cantidad de respuestas representó a aquellas empresas que reconocen una conexión entre la red corporativa y la de automatización, pero disponen de un *firewall* entre estas redes. Sin embargo, existe un muy preocupante 12,9 por ciento de empresas que mantiene sus redes directamente conectadas, lo que representa un enorme riesgo de incidencias de seguridad.

Con respecto a los accesos remotos la consultas fue si la red industrial posee accesos remotos. La figura 3 muestra las respuestas y lo dice todo, donde nuevamente lo preocupante es el diez por ciento (10%) de empresas que desconoce si su red industrial posee accesos remotos.

Otra pregunta sobre la misma temática fue si la red industrial posee dispositivos conectados a Internet, independientemente de los mecanismos de protección aplicados. Como era de suponer, siguiendo la tendencia de la convergencia de las redes, una amplia mayoría de las empresas estudiadas (más del sesenta por ciento —60%—) afirma tener dispositivos que están conectados a Internet de forma permanente o temporal, y lo preocupante es que más del diez por ciento (10%) de las empresas desconoce este tema, con lo cual obviamente tampoco se ocupa de su protección.

Respecto de normas, estándares y marcos de trabajo, las preguntas fueron si se estaban teniendo en cuenta alguno de estos documentos, y cuáles, en lo que se refiere a ciberseguridad industrial. Casi la mitad de las empresas tienen en cuenta las ISO 27000, pero muchas de ellas solo utilizan esta familia pero ninguna específica para el ámbito industrial.

Finalmente, dentro de los aspectos técnicos se consultó qué medidas de ciberseguridad industrial ya había implantadas en las empresa. Todas las empresas estudiadas afirman tener implantado algún tipo de medida de ciberseguridad industrial, pero se aprecia que las medidas específicas de ciberseguridad industrial (*gateways* unidireccionales, *whitelisting* o control de aplicaciones industriales) todavía presentan un uso bastante limitado, posiblemente porque su implementación depende de departamentos de TI con poca experiencia en el mundo industrial.

El último ítem de este estudio se refirió a cuestiones a futuro y se denominó "Mercado de la ciberseguridad industrial". En él se incluyeron los siguientes temas: previsión de nuevas actividades de ciberseguridad industrial, requisitos para nuevos proyectos, contratación de proyectos de ciberseguridad industrial, y certificaciones profesionales.

En los tres primeros aspectos, en mayor o menor medida, casi todas las empresas han aportado su granito de arena en el tema. En lo que sí coincidieron más del noventa por ciento (90%) de las empresas encuestadas es en la importancia de la formación y la capacitación profesional en el área de la ciberseguridad industrial.

Hasta aquí se ha expuesto una breve síntesis del estudio, mencionando solo aquellos aspectos que consideré más relevantes para este artículo. Dado el escaso recurso del espacio para exponer todos los gráficos y el escaso recurso del tiempo para leer todos los análisis, dejamos esta tarea al lector interesado en profundizar en los distintos ítems y conocer más detalles.

A continuación, y para concluir con este documento, señalaré sucintamente algunas de las conclusiones que se expresan en el estudio.

Conclusiones

De las conclusiones que expresa el documento rescato la que tiene que ver con los recursos humanos y con las regulaciones.

Posiblemente, la falta de regulaciones sea uno de los principales causantes de la falta de incentivos para que prospere el tema de ciberseguridad en el área industrial.

En cuanto a los recursos humanos, se aprecia una falta de concienciación en las áreas de decisiones de las organizaciones y una menor formación de las áreas de TO respecto de las de TI en este tema. Por eso la importancia de organizaciones como CCI y AADECA, que trabajan activamente en estos aspectos.

Destaco la labor de Nora Alzúa, Susana Asensio, Claudio Caracciolo, Miguel García-Menéndez y José Valiente, responsables de la generación, gestión y elaboración del documento. Para aquellos interesados en profundizar sobre el estudio, el mismo se puede acceder desde el link: *https://www.cci-es.org/estudioCI_argentina* ❖

Dos empresas se alían para abordar nuevos desafíos

Schneider Electric y *Claroty* se asociaron para abordar los desafíos de seguridad y ciberseguridad en la infraestructura industrial mundial

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

En agosto pasado, la empresa *Schneider Electric*, referente a nivel mundial de gestión de energía y automatización, anunció su alianza con *Claroty*, una empresa israelí de tecnología operacional (TO), acaecida para abordar los desafíos de seguridad y ciberseguridad que puede presentar el uso de nuevas tecnologías en la infraestructura industrial.

Bajo los términos del acuerdo, *Claroty* comercializará su solución de monitoreo y detección de redes TO, ICS en tiempo real a los clientes de *Schneider Electric* a través del Programa de Colaboradores de Automatización (CAPP, por sus siglas en ingles) de la compañía.

La plataforma *Claroty* protege proactivamente los sistemas de control industrial y monitorea continuamente las redes industriales en busca de amenazas cibernéticas. Con acceso remoto seguro, los propietarios de activos pueden emplear políticas para controlar el acceso remoto de empleados y terceros a sistemas críticos y registrar las sesiones. La detección continua de amenazas crea un inventario detallado de los activos de la red industrial, identifica configuraciones erróneas, monitorea el tráfico entre activos y encuentra anomalías que pueden indicar la presencia de un agente malintencionado. Las alertas ricas en contexto proporcionan al personal de planta y de seguridad información útil para una investigación, respuesta y recuperación eficientes.

Esta alianza añade un componente clave a las ofertas de ciberseguridad de extremo a extremo de *Schneider Electric* por proteger tanto los productos conectados como las ofertas de control *edge* dentro de la arquitectura y plataforma de sistemas abiertos e interoperables de *Schneider Electric, EcoStruxure*, habilitada para IoT. Con innovación en todos los niveles a través de productos conectados, control edge y aplicaciones, análisis y servicios, dicha arquitectura permite el diseño escalable y el funcionamiento de sistemas con la mejor ciberseguridad integrada en cada nivel.

Una característica clave de la plataforma *Claroty* es su capacidad para explorar el nivel más profundo de protocolos de red industriales sin afectar negativamente a el sistema. Esto permite a los usuarios finales identificar con seguridad las anomalías mientras protegen las redes industriales complejas y sensibles. El software tradicional de seguridad de TI a menudo utiliza consultas activas o requiere una huella en la red, lo que en última instancia puede interrumpir las operaciones. Sin embargo, la plataforma presentada utiliza un enfoque de monitoreo pasivo para inspeccionar el tráfico de manera segura sin el riesgo de interrupción.

Acerca de *Claroty*

Claroty es la segunda *startup* de la fundición *Team8*, de Israel, que orienta su actividad a las disciplinas de TI y TO. La empresa tiene una organización de investigación de seguridad de ICS de élite que comprende el uno por ciento (1%) superior del uno por ciento de expertos en seguridad cibernética de la Unidad 8200 de la Fuerza de Defensa de Israel. ❖

Aspectos de seguridad de la digitalización

Protección de instalaciones de producción industrial en transición

Andrés Gregorio Gorenberg, *andres.gorenberg@siemens.com*
Siemens Argentina, *www.siemens.com*

Hoy día, las compañías y los operadores de plantas han aprendido que deben protegerse contra ciberataques. Sin embargo, este hecho ya conocido está tomando más popularidad en el contexto de las nuevas normas de seguridad para la industria y las primeras reglamentaciones legales, como regulaciones sobre seguridad informática para infraestructuras críticas. En este sector, es necesaria la implementación o el cumplimiento de las normas de seguridad informática, teniendo en cuenta cómo las amenazas potenciales se incrementaron considerablemente en solo unos años.

Ante la creciente digitalización de las empresas y las redes que se encuentran en prácticamente todas las áreas, se abre un potencial económico al cual los países desarrollados e industrializados no pueden renunciar. Sin embargo, al mismo tiempo, la digitalización crea nuevas amenazas que deben tratarse rápida- y sistemáticamente. El notable aumento de ciberataques más profesionales y dirigidos en los últimos años –los denominados APT (amenazas persistentes avanzadas)– también ha motivado a las legislaturas a sancionar normativas adecuadas en los países.

El ejemplo de Alemania

Con la aprobación del Parlamento alemán de la Ley de Seguridad Informática –que aumenta la seguridad de los sistemas informáticos– que entró en vigencia en julio de 2015, los operadores de infraestructuras críticas (KRITIS) en Alemania están obligados a tomar ciertas medidas. Para algunas de las infraestructuras críticas que se registraron, la ley estipula un requisito de generación de informes sobre incidentes relacionados con la seguridad a partir de noviembre de 2016, así como también normas mínimas de seguridad informática a partir de mayo de 2017. Si un operador de infraestructura crítica sufriere fallas que debieran informarse, la Oficina Federal de Seguridad Informática de Alemania (BSI) también podrá requerir la participación de los fabricantes de productos y sistemas informáticos correspondientes. Esto incluye, por ejemplo, la rápida eliminación de los puntos débiles detectados.

Las normas de seguridad informática deberán encaminarse hacia la modernización. En consecuencia, las normas de seguridad deberán revisarse mediante auditorías cada dos años. El término legal "de última tecnología" (*state of the art*, en inglés) se utiliza porque, según la experiencia, los desarrollos técnicos generalmente superan la legislación. Por este motivo, se ha convertido en una buena práctica durante años en algunas ramas del Derecho hablar "de última tecnología" en las leyes, en lugar de intentar establecer requisitos técnicos específicos ya incluidos. "De última tecnología" en cierto momento histórico para un área correspondiente puede determinarse, por ejemplo, a través de las normas nacionales o internacionales existentes, como las DIN o IEC, o mediante modelos que se

Andrés Gregorio Gorenberg
Ingeniero Eléctrico por la Universidad Tecnológica Nacional desde 1995 y diplomado en Organización Estratégica de Negocios (Universidad de Chile, 2016), Negociación Avanzada (Universidad Austral, 2008), Management (ITBA, 2010) y Business Intelligent and Data Mining (UTN, 2014). Actualmente, se desempeña como Factory Automation Manager en Siemens, empresa en la que trabaja desde hace más de veinte años y en la que ocupa cargos con responsabilidades regionales en Sudamérica.

hayan probado con buenos resultados en la práctica, las denominadas "buenas prácticas". Debido a que las medidas técnicas necesarias pueden diferir según la situación específica, es casi imposible describir concluyente y universalmente qué significa "de última tecnología".

Respecto de la seguridad, la norma IEC 62443 es la principal en el entorno industrial, la cual, a veces, también se adapta o se utiliza como referencia en otras áreas, como en el caso del uso ferroviario. Es una norma reconocida internacionalmente, y la más abarcadora de todas. Está dirigida a operadores, integradores de sistemas y fabricantes de sistemas de automatización por igual. Al hacerlo, las distintas partes de la norma cubren procesos, tecnologías y funciones personales. Se aclara que, para que la protección sea la adecuada, es indispensable contar con un análisis de riesgos para definir e implementar medidas adecuadas. Mantener este grado de protección a largo plazo tiene la misma importancia, por ejemplo, a través de la revisión regular de la eficacia de las medidas utilizadas.

Certificado *TÜV SÜD* internacional según la norma IEC 62443-4-1

Por primera vez, la norma IEC 62443 también ofrece una base para la certificación de la ciberseguridad en los sistemas industriales de automatización y control. Uno de los primeros proveedores, *TÜV SÜD* declaró llevar a cabo pruebas y certificaciones conforme con IEC 62443. La certificación de los procesos de desarrollo y fabricación entre los fabricantes de productos se realiza según la parte 4-1 de la norma IEC 62443, es decir, la norma IEC 62443-4-1. Las funciones de seguridad de los productos pueden evaluarse de acuerdo con IEC 62443-3-3. En agosto de 2016, *TÜV SÜD* le otorgó a *Siemens* el certificado internacional según IEC 62443-4-1, mediante el cual se confirmó el cumplimiento con los requisitos de seguridad del proceso de desarrollo integral de los productos de automatización y unidades de disco de la empresa en siete sitios de desarrollo en Alemania.

La seguridad absoluta nunca ha existido en la era informática. El objetivo es encontrar medidas de seguridad adecuadas que intenten reducir el riesgo hasta un nivel aceptable. En otras palabras, se deberían aumentar los esfuerzos para protegerse de potenciales atacantes de modo que excedan los beneficios potenciales; no hay un vínculo económico. Según los niveles de seguridad (NS) definidos, la norma IEC 62443 brinda una guía para la seguridad necesaria respecto de los riesgos existentes.

La clave del concepto es el nivel de protección, el cual es producto del grado de seguridad y madurez. El grado de madurez indica la confiabilidad de los procesos de seguridad en una empresa, y se basa en las normas IEC 62443-2-4 e ISO 27001. A mayor madurez de una empresa, mayor el grado de seguridad. Este se refiere, a su vez, a las soluciones técnicas utilizadas conforme con la norma IEC 62443-3-3. La matriz consultada para la definición del nivel de protección establece que, para un mayor nivel de protección, es necesario un mayor grado de seguridad (una mejor solución de seguridad, técnicamente hablando), así como también un mayor grado de madurez (una mejor madurez de procesos).

Implementación de medidas de protección efectivas

Llevar todo esto a la práctica requiere una adaptación o mejora de sistemas, productos, soluciones y, también, de servicios mediante la incorporación de funciones y propiedades de seguridad, así como de procesos y directivas. Esto significa la implementación de una defensa multicapa o, para decirlo en la jerga de seguridad, una estrategia de protección total.

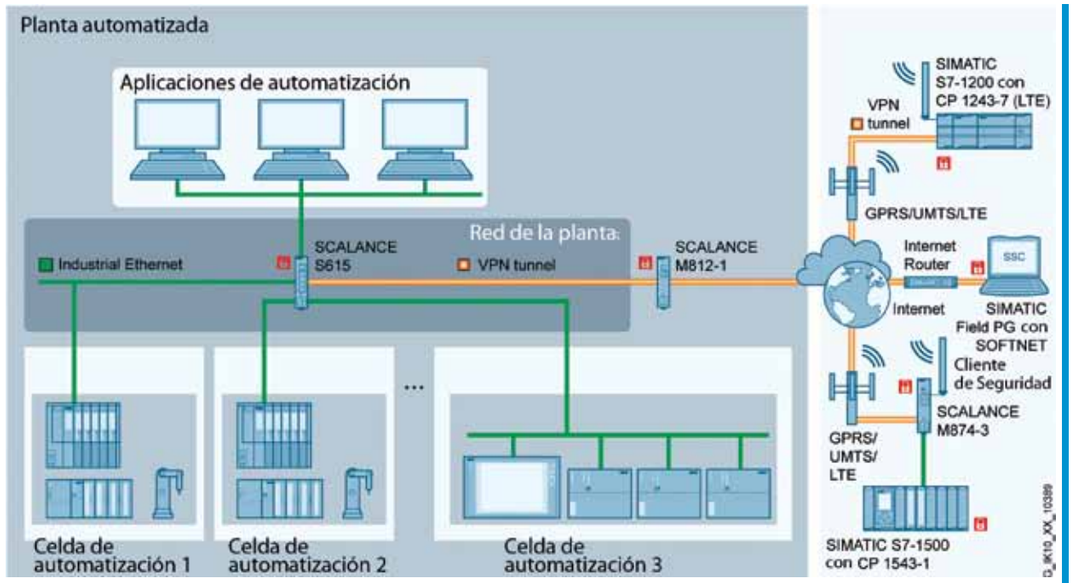


Imagen 1. Ejemplo de implementación de sistemas de ciberseguridad para producción y acceso remoto

Esto no solo significa que hay varias medidas de seguridad conectadas en cadena, sino que también se emplean distintas tecnologías. Por ejemplo: el acceso a las redes se controla mediante firewalls, tal como los que proporcionan los dispositivos de seguridad de nivel industrial de la familia de productos de automatización (como ejemplo la línea *Scalance S*, de *Siemens*). Al hacer esto, el acceso desde el exterior se reduce, lo cual también podría implementarse utilizando una zona desmilitarizada (ZDM). Una ZDM pone a disposición los datos de la red protegida; de este modo, se evita un acceso directo a la red de automatización desde afuera. Aquí los permisos de acceso deberían asignarse según la premisa *Need2Connect* (necesidad de conectarse), es decir, solo deberían concederse los accesos que sean absolutamente necesarios.

Para aumentar aún más la protección, en particular en redes más grandes, la segmentación de seguridad de las redes habla por sí misma: a través de un firewall o componentes especiales, se protegen varias celdas de automatización, tal como lo hacen los procesadores de comunicación de seguridad para los sistemas de automatización como, por ejemplo, los *Simatic S7*. En caso de que un hacker acceda a la red, se deberá sortear otro obstáculo para ingresar a la celda de automatización.

Los componentes de automatización representan en sí el siguiente obstáculo. En el caso de los PLC como ser los *Simatic*, los dispositivos HMI y los sistemas SCADA, poseen funciones de seguridad integradas (como la protección por contraseña), lo cual reduce aún más el riesgo de accesos no autorizados.

Estas medidas reducen los riesgos de accesos no autorizados y de pérdida de datos, pero solo si todas las funciones de seguridad se implementan correctamente, los dispositivos están bien configurados, y no se encuentran puntos débiles visibles, de modo que ni siquiera los denominados “ataques de canal lateral” puedan prosperar.

Seguridad en el diseño

Para lograr esto, deberán tomarse las medidas adecuadas durante el desarrollo y la fabricación de productos para detectar y eliminar posibles debilidades durante las primeras etapas. Varias normas de seguridad ahora también exigen estas medidas, tal como se mencionó. Este enfoque, conocido como seguridad en el diseño, se deberá considerar para el desarrollo del producto desde el principio. Esto significa que los aspectos de seguridad ya se toman en cuenta en las especificaciones de los requisitos, la arquitectura y la programación, y que los análisis de riesgos se realizan y todo se encuentra verificado y evaluado.

Sin embargo, la experiencia también ha demostrado que no es posible evitar todos los puntos débiles, en particular, con productos con software. Por este motivo, es indispensable detectar los puntos débiles durante las operaciones para que puedan resolverse enseguida, y notificar a los usuarios afectados de forma rápida y precisa. Para que esto funcione sin inconvenientes, deberán establecerse procesos adecuados, y las responsabilidades de cada uno y las personas de contacto deberán definirse claramente.

Durante los últimos años, empresas como *Siemens* han incorporado y optimizado las medidas y los procesos mencionados. Esto se extiende hasta la calidad de los productos y sistemas de escala industrial, incluyendo los aspectos de seguridad. Evitar los puntos débiles ya durante el desarrollo y la fabricación, y eliminarlos de inmediato durante las operaciones contribuye en gran medida a minimizar riesgos y a mejorar continuamente la seguridad de los sistemas de automatización y comunicación industriales.

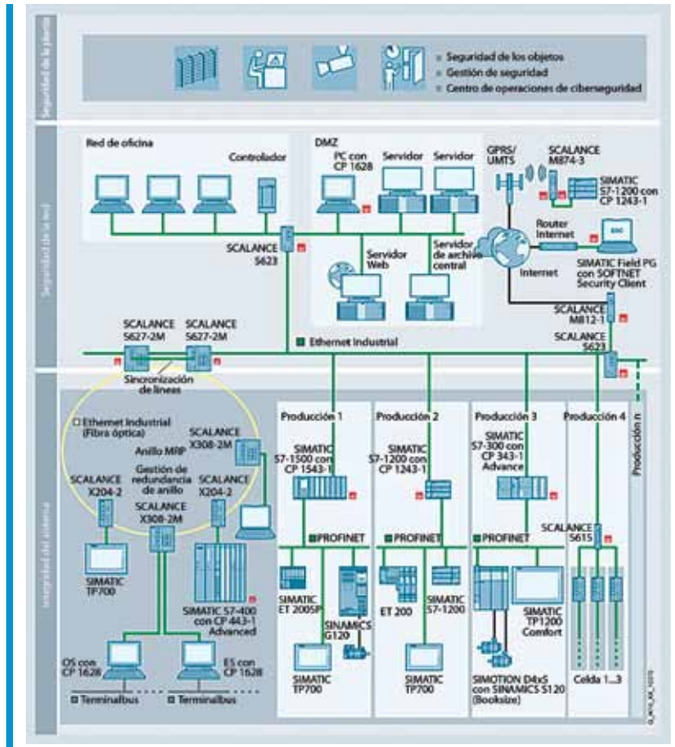


Imagen 2. Aspectos de seguridad: comunicación segura, protección de acceso a la red y segmentación de redes con productos con seguridad integrada

La seguridad como requisito previo para la digitalización

Sin duda, la evolución de la ingeniería y las prácticas de digitalización abren un nuevo panorama a los sistemas de producción, sin embargo, los requisitos de seguridad y las amenazas aumentan con la digitalización. La buena noticia es que las opciones de protección para las instalaciones industriales y sus sistemas de automatización están mejorando cada vez más también. Esto es crucial para mantener y mejorar la productividad en el futuro. Durante el proceso de digitalización de las empresas, la seguridad cibernética es uno de los aspectos que cobrará cada vez más importancia y para lo cual se deberá invertir en mejorar los conocimientos y las tecnologías apropiadas para lograrlo. ❖

SRS: la base de una gestión exitosa de SIS

Roberto E. Varela
robertoe.varela@gmail.com

La especificación de requisitos de seguridad (SRS) es un documento requerido por la norma IEC 61511 [1] y define los requisitos generales, funcionales y de integridad de las funciones instrumentadas de seguridad (SIF) y de los sistemas instrumentados de seguridad (SIS). Debe ser clara, concisa, completa y consistente. Con una especificación desarrollada según los lineamientos de la norma, se reducirá la probabilidad de ocurrencia de errores sistemáticos, se comprenderán mejor los peligros potenciales, los riesgos que estos implican, se reducirán las fallas aleatorias, se detallarán las SIF requeridas con su correspondiente nivel de integridad (SIL), se evitarán funciones innecesariamente complejas o muy simplificadas y se validará apropiadamente el SIS.

Introducción

La norma IEC 61511 no incluye un ejemplo de cómo debe ser desarrollada la SRS, solo indica qué debe especificarse y cuáles son los atributos del sistema que deben incluirse. Recordemos que las normas de seguridad funcional son normas de desempeño, no prescriptivas. No es un libro de cocina con recetas. Cada usuario, empresa o establecimiento debe desarrollar su propia SRS.

IEC 61511 indica que la SRS debe ser escrita de tal modo que sea una ayuda para la comprensión e interpretación de sus requisitos por aquellos que deben utilizar la información contenida en ella en cualquier fase del ciclo de vida de seguridad. Deben incluirse tanto los requisitos de seguridad para el equipamiento como para el programa de aplicación.

La norma no especifica si la SRS es un documento único o una colección de varios documentos. Es importante tener en cuenta que la documentación contenida en la SRS debe cubrir todos los aspectos que deben considerarse durante el ciclo de vida de seguridad: diseño y arquitectura de la SIF/SIS, confiabilidad, disponibilidad, sistemas de soporte, instalación, pruebas y mantenimiento, especificación del equipamiento, programa de aplicación, seguridad de acceso al sistema, interfaz de operación, ingeniería y mantenimiento.

Contenido de la SRS

Muchas empresas y organizaciones relacionadas con seguridad en procesos han desarrollado especificaciones SRS, tanto en formato narrativo, como en formularios que contienen toda la información requerida por la norma IEC 61511.

La responsabilidad del desarrollo y revisión de una buena especificación SRS incluye un equipo de profesionales y técnicos de las áreas de proceso, instrumentación, operación y mantenimiento con experiencia y conocimiento del alcance de las normas de seguridad funcional.

La información debe estar estructurada de manera tal de considerar:

- Requisitos no funcionales generales aplicables al SIS en su conjunto, tales como normas, guías de diseño, condiciones ambientales como temperatura, humedad, contaminantes, puesta a tierra, interferencias RFI/EMI, vibración, descarga electrostática, clasificación eléctrica de área, inundaciones, tormentas eléctricas, etcétera.
- Requisitos funcionales generales aplicables a todas las funciones de seguridad del sistema instrumentado de seguridad, por ejemplo, definición de estado seguro; entradas de proceso y punto de disparo; salidas a proceso y su acción; relación entre entradas y salidas; consideración de parada manual; consideración de bypasses; tiempo de respuesta; modos operativos (normal cerrado, normal abierto); modos de falla; acciones del operador; requerimientos de interfaz de operación, mantenimiento e ingeniería; etcétera.
- Requisitos de integridad de la seguridad aplicables a todas las funciones de seguridad del sistema instrumentado de seguridad, tales como SIL requerido; cobertura de diagnósticos; requisitos de mantenimiento e intervalo de prueba funcional; modo de demanda; restricciones de arquitectura; votación.

Los requisitos de seguridad del programa de aplicación son derivados de la SRS y de la arquitectura seleccionada del SIS. Estos requisitos forman parte de la SRS en un capítulo separado. Los datos requeridos para desarrollar la especificación del programa de aplicación son los requisitos de seguridad especificados para cada SIS; los requisitos resultantes de la arquitectura del SIS y del manual de seguridad, tales como limitaciones y restricciones del equipamiento y del software embebido.

Los requisitos de seguridad del programa de aplicación estarán suficientemente detallados para permitir el diseño e implementación para alcanzar la seguridad funcional requerida y que pueda llevarse a cabo una evaluación de seguridad funcional.

Conclusión

La norma internacional de seguridad funcional para IEC 61511 es reconocida como una "buena práctica de ingeniería" para la implementación de SIS en el sector de la industria de procesos. Cumpliendo los requisitos de la norma, pueden minimizarse los efectos de los errores humanos en las distintas etapas del ciclo de vida, tal como los muestra el estudio realizado por el *Health and Safety Executive* del Reino Unido en su publicación "Out of control" [2].

La SRS debe consolidar toda la información proveniente de las etapas precedentes del ciclo de vida. Además, contendrá toda la información necesaria para cumplimentar los requisitos de la fase mandatoria de validación del SIS previa a la puesta en servicio de la planta y a la incorporación de los materiales peligrosos, en caso de una planta nueva. La validación se basa en el contenido de la SRS, no en ningún otro documento de diseño intermedio o de menor nivel, de manera tal que los errores cometidos en la creación de esos documentos detallados de diseño sean detectados durante la validación. ❖

Roberto Varela
Roberto Eduardo Varela es ingeniero químico (Universidad Nacional de La Plata), especialista en seguridad, higiene y protección ambiental, ingeniero en seguridad funcional (*TÜV Rheinland*) – SIS, especialista y consultor SIS, especialista en estudios de confiabilidad y autor e instructor de cursos sobre seguridad funcional.
Autor del Libro: "SIS – Evolución, diseño y aplicación", Editorial *Control*, 2003.

Referencias

[1] IEC 61511. Edición 2.0. Partes 1, 2 y 3. Seguridad funcional: sistemas instrumentados de seguridad para el sector de la industria de procesos
[2] "Out of Control: Why Control Systems go Wrong and How to Prevent Failure" Reino Unido: Sheffield, Heath and Safety Executive, 2° edición 2003

Adiós a un pionero de la industria nacional

AADECA, *www.aadeca.org*

La noticia del fallecimiento de Higinio "Gino" Ridolfi apenó a la industria, sobre todo aquella asociada a la metalmecánica, el control y la automatización. Fue quien fundó *Automación Micromecánica*, una de las empresas argentinas más respetadas del sector.

Nació en Junín, el 24 de septiembre de 1928. Hijo de Adela y Alejandro Ridolfi, dos inmigrantes italianos que habían llegado al país unos años antes. La muerte inesperada del *pater familiae* culminó con la vuelta de la madre y sus dos pequeños a la Italia natal, en donde Gino y su hermano Carlos recibieron educación técnica de excelencia en una reconocida institución en Vicenza.

En 1948, juntos decidieron volver a Argentina, en donde rápidamente fueron valorados por sus capacidades técnicas: Gino se desempeñó como director de las empresas *Famag* y *Merex*.

Con el deseo de hacer germinar un proyecto propio, los hermanos compraron un torno y empezaron su proyecto de producción. En la década de 1960, ambos ya casados, pudieron comprar una casa en Villa Domínico, y así nació *Automación Micromecánica*.

Tras la Segunda Guerra Mundial, Estados Unidos y los países de Europa ya desarrollaban elementos neumáticos de aire comprimido para procesos industriales, pero en Argentina eso era aún un terreno inexplorado. Los Ridolfi pusieron manos a la obra, investigaron el tema y lograron finalmente desarrollar productos propios: equipos para tratar el aire; válvulas y cilindros. Mientras Carlos creaba productos, Higinio comenzaba a proyectar el mercado.

Los años fueron pasando, la empresa afianzó su crecimiento. Y la década de 1970 estuvo signada por la salida al mundo: la competencia a nivel internacional. Luego, en los años '80 y '90, por la adaptación a las nuevas regulaciones, de esta manera, *Automación Micromecánica* fue una de las primeras PyME argentinas en certificar ISO 9001 y 14001. Durante los primeros años del siglo XXI, la empresa consolidó su presencia en el mundo, con exportaciones a más de veinticinco países, con una fuerte visión de alcanzar el liderazgo en América Latina.

Notable emprendedor, Gino Ridolfi no solo se destacó puertas adentro de su propia empresa, sino que además participó activamente en gran cantidad de organizaciones empresariales como ser en la Unión Industrial de Avellaneda, en el Organismo Argentino de Acreditación, en AAFMHA y en ADIMRA. Asimismo, a lo largo de esa trayectoria, conquistó numerosos reconocimientos y premios tanto a nivel personal como para la empresa: Premio a la Innovación (Fundación Banco de Galicia); Premio Nacional a la Calidad, 1996; Premio de Calidad a los Mejores Proveedores del Mercosur, Grupo *Volkswagen*, 2000; Premio Carlos Pellegrini, 2004, y Premio Exportar durante tres ediciones.

"Lo recordaremos siempre como un trabajador incansable, con gran capacidad para adaptarse a entornos cambiantes, produciendo a partir de su espíritu creador y de la confianza como valores irrenunciables", reza el comunicado de ADIMRA tras recibir la noticia. AADECA se suma a su memoria. ❖

IEC 62443 y las acciones de *Yokogawa*

Yokogawa, *www.yokogawa.com.ar*

De cara al acelerado incremento global del cibercrimen, este es un problema acuciante como para alentar la ciberseguridad en sistemas de control de procesos utilizados en infraestructuras importantes para la sociedad tales como plantas de energía, gas y petroquímicas. Como parte de los esfuerzos internacionales por la estandarización de la seguridad bajo estas circunstancias, la Comisión Electrotécnica Internacional (IEC), una organización de estandarización internacional, estableció la norma IEC 62443 en 2010, que define los lineamientos del control de seguridad para organizaciones involucradas con sistemas de control de procesos.

Los estándares de certificación y evaluación del Instituto de Cumplimiento de la Seguridad de la Sociedad Internacional de Automatización (ISCI) y de la Asociación de Usuarios de Automatización de Procesos (WIB) tenderán a reflejarse en IEC 62443, y los operarios de sistemas de control de procesos tienden a incluir el cumplimiento de IEC 62443 dentro de sus requisitos.

En base a lo establecido más arriba, los expertos en seguridad de *Yokogawa* están activamente involucrados en el desarrollo de estándares internacionales de tecnología de seguridad para sistemas de control de procesos, incluyendo IEC 62443. La empresa ofrece actividades de producción para el cliente, estables y seguras en base a tales estándares a fin de ofrecer productos, servicios y soluciones con un valor agregado.

Este artículo hace un repaso de la norma internacional IEC 62443 y describe las actividades de *Yokogawa* referidas a ella.

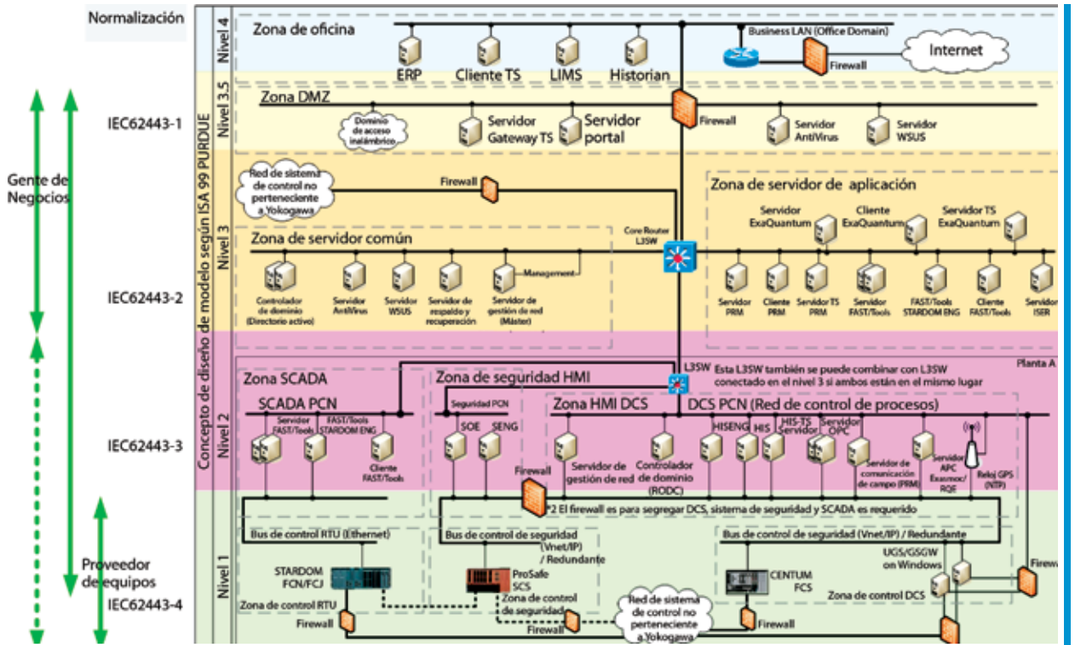


Figura 1. Vista general de las normas de seguridad IEC 62443

Repaso de IEC 62443

IEC 62443 define los lineamientos del control de seguridad para proveedores que fabrican componentes para sistemas de control de procesos, integradores que construyen tales sistemas integrando los componentes, operarios que operan los sistemas, y todas las organizaciones involucradas con los sistemas de control de procesos. IEC 62443 está compuesta por una serie de cuatro estándares:

- IEC 62443-1: definición de términos, conceptos, etc., de toda la norma
- IEC 62443-2: gestión de seguridad para organizaciones
- IEC 62443-3: normas de seguridad para construir sistemas
- IEC 62443-4: normas de seguridad para equipamiento y dispositivos de control

La mayoría de las series IEC 62443 están basadas en los requisitos ISA 99, y solamente IEC 62443-2-4 está basada en WIB.

A continuación, las relaciones simplificadas entre *Yokogawa* y las cuatro series de normas anteriores:

- IEC 62443-1: referencia a términos y modelos en varios documentos de *Yokogawa*
- IEC 62443-2: provisión de servicios de gestión de seguridad para clientes
- IEC 62443-3: provisión de un servicio de integración para diseñar e implementar los controles de seguridad necesarios para los sistemas de control que se entregarán a los clientes
- IEC 62443-4: referencia (seguimiento) a los requisitos y normas de seguridad para elementos de control provistos a los clientes

Acciones de *Yokogawa* para obtener certificaciones

Ya están desarrollados los esquemas de certificación basados en la norma internacional de seguridad IEC 62443 y *Yokogawa* se ha involucrado activamente para obtenerlos. La empresa ofrece acciones de producción para el cliente estables y seguras para que obtengan certificaciones de terceros, ofrece productos, servicios y soluciones con un valor agregado.

Certificación EDSA

ISCI presentó la certificación de valuación de la seguridad de un dispositivo integrado (EDSA) para los componentes integrados en equipos de control, para proveedores de equipos que fabrican componentes para sistemas de control de procesos.

Yokogawa obtuvo su certificación como primera proveedora de dispositivos en Japón en enero de 2014 por el sistema instrumentado de seguridad *ProSafe-RS*, y en julio de ese mismo año, para el sistema de control de producción integrado *Centum VP*.

Nótese, como se dijo antes, que la norma EDSA de ISCI sigue a IEC 62443-4.

Certificación CSMS

IEC 62443-2-1 de IEC 62443-2 define los requisitos de gestión de seguridad para organizaciones que utilizan sistemas de control de procesos. En abril de 2014, el Ministerio de Economía, Comercio e Industria de Japón presentó un esquema de certificación de gestión de seguridad basado en IEC 62443-2-1, denominado CSMS (sistema de gestión de ciberseguridad para IACS [sistemas de control y automatización industrial]).

La certificación CSMS apunta a dos tipos de operadores: un integrador que construye sistemas de control de procesos y un operador que hace las operaciones utilizando esos sistemas. *Yokogawa Solution Service* obtuvo su certificación como primera integradora en Japón.

Ciclo de vida seguro

Yokogawa provee las soluciones para implementar seguridad para el ciclo de vida completo basada en la estrategia de "defensa en profundidad".

El enfoque se basa en normas de seguridad internacionales tales como IEC 62443 y la serie SP del Instituto Nacional de Normalización y Tecnología (NIST, de Estados Unidos), e implementa controles técnicos, operacionales y gerenciales para asegurar la información. Aquellas implican un enfoque efectivo para garantizar la seguridad, el rendimiento necesario de las utilidades de producción, y los preparativos para mantener la salud de los sistemas de control de procesos que están en su base.

Yokogawa acompaña a sus clientes en sus acciones sobre la seguridad a través del ciclo de vida de los sistemas de control de procesos, para mejorar los controles de seguridad, prevenir y mitigar amenazas contra la ciberseguridad, y estar preparados para una recuperación rápida en caso de emergencia.

Figura 2. Solución de soporte para implementar el ciclo de vida de seguridad

Productos para sistemas

Evaluación de la seguridad en el desarrollo de software

Yokogawa lleva a cabo un proceso de desarrollo estricto. Esto implica que puede identificar y remover las vulnerabilidades de la seguridad en todos los procesos, incluyendo diseño, codificación, testeo y documentación.

Además, la empresa obtuvo la certificación EDSA para productos de sistemas. Los puntos de evaluación de esta certificación incluyen la seguridad en el desarrollo de software (SDSA), por lo cual demuestra que la empresa sigue un proceso de desarrollo seguro.

Seguridad integrada Vnet/IP

Vnet/IP, la red de control de *Yokogawa* utilizada en *Centum VP* y *ProSafe-RS* cuenta con funciones de control de seguridad integradas.

Vnet/IP es una red de control redundante dual para automatización de procesos basada en Ethernet gigabit, que combina confiabilidad y actuación en tiempo real para las operaciones de planta. Implementa controles de seguridad contra amenazas a la ciberseguridad, tales como escuchas ilegales, falsificaciones y burlas de datos. También determina la autenticidad de los paquetes de comunicación a partir de un método de autentificación en base a una clave secreta compartida y decide si recibir o no ciertos paquetes. Dicha clave secreta compartida se modifica periódicamente para impedir ataques sucesivos e intentos de adivinar la clave.

Soporte para la integración del sistema

Diseño del sistema

IEC 62443-1-1 describe una serie de modelos que se pueden utilizar para diseñar controles de seguridad apropiados.

- Modelo de referencia: refiere a expresiones acerca de fabricación integrada o sistema de producción como una serie de niveles lógicos, desde un punto de vista general.
- Nivel del modelo de referencia: refiere a las funciones y actividades basadas en el modelo jerárquico funcional de IEC 62264-1, desde el proceso (nivel 0) hasta la empresa (nivel 4)

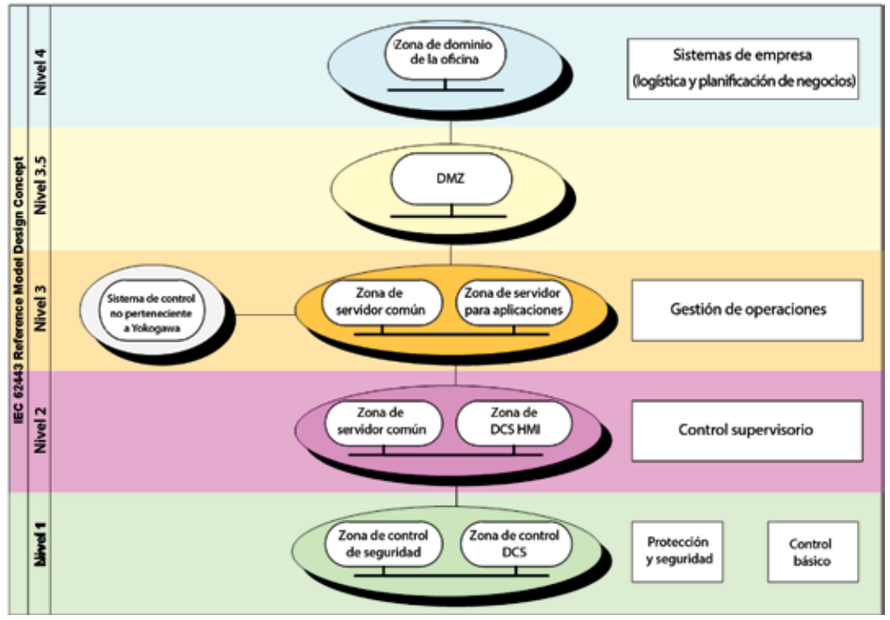


Figura 3. Conceptos de diseño para el modelo de referencia según IEC 62443

- Modelo de zona: refiere a un conjunto de elementos del modelo de referencia de acuerdo a características definidas, provee un contexto para la definición de una política, procedimiento, y pasos a seguir, y se aplica a las instalaciones.
- Zona: refiere a las instalaciones físicas agrupadas lógicamente, tanto como a instalaciones de aplicación e información que comparten requisitos comunes de seguridad.

En base a lo dicho, *Yokogawa* diseña una red basada en el modelo de referencia Purdue. La configuración del sistema se muestra en la figura 3.

Cada zona presenta requisitos de seguridad diferentes. Por lo tanto, *Yokogawa* recomienda que los usuarios construyan zonas diversas, como segmentos de red diferentes, e implementen un control de acceso apropiado, por ejemplo, instalando switches de capa 3 y firewalls entre las zonas.

Fortalecimiento de la PC (herramienta de seguridad TI)

Los productos de sistema IA de *Yokogawa* incluyen herramientas de seguridad TI como estándar. Dicha herramienta elimina las funciones de *Windows* que no son necesarias para los productos de la empresa y además presentan vulnerabilidades e incrementan la dependencia del sistema operativo.

Por ejemplo, la función de control de acceso para los usuarios y grupos de *Windows* se puede usar para controlar las herramientas de *Centum VP* y acceder a sus carpetas y archivos. De esta forma, se puede implementar un control de seguridad; en el caso de que el usuario se loguee en el sistema como operario, puede usar la pantalla y las herramientas de operario, pero no las de ingeniería. Además, se pueden configurar DCOM y firewall de *Windows* para restringir el uso de los tipos y puertos de comunicación.

También se puede implementar el control de malware restringiendo el uso de dispositivos de almacenamiento externo como memorias USB.

Los usuarios podrán configurar su seguridad ellos mismos, a través de la herramienta IT Security de *Yokogawa*, que contribuye a implementar la "Operación de un programa de seguridad IACS" según IEC 62443-2-2.

Autentificación de usuario y gestión de privilegio de la operación y función de monitoreo

Con la función de control y operación de *Centum VP*, se puede configurar la seguridad según el usuario. Tal función presenta los modos de autentificación de *Centum* y de *Windows*, que provee opciones flexibles para dicha tarea.

Centum VP brinda funciones de monitoreo y operación de planta que son sofisticadas y flexibles, tales como autentificación de usuario, restricción de la operación y rango de monitoreo, y restricción de operaciones, a fin de prevenir problemas causados por los errores operacionales y asegurar la protección de los sistemas. Los usuarios de *Centum VP* en general están reunidos en cuatro grupos: operario, ingeniero de sistema, ingeniero de recetas y usuarios de los paquetes de reportes, y por lo tanto la función de restricción de acceso se puede aplicar a cada uno. Los operarios se dividen en tres roles: solo monitoreo, monitoreo y operación, y mantenimiento, y entonces se pueden aplicar restricciones para cada rol.

Esto contribuye a implementar la gestión y autentificación definidas en "Establecer un programa de seguridad IACS" según IEC 62443-2-1.

Gestión del historial de operaciones

Centum VP puede almacenar los registros de operación de cada usuario. Además, la función de gestión del historial puede grabar una operación en detalle, por ejemplo, operación de la función de monitoreo y operación, mantenimiento de los archivos de definición de reporte, ingeniería, y mantenimiento. *ProSafe-RS* también presenta una función de gestión del historial de operaciones. Esta función permite determinar quién y cuándo llevó a cabo qué operación, en el caso de que ocurra algún suceso.

Esto contribuye a implementar la gestión de cuentas y autentificación definidas en "Establecer un programa de seguridad IACS" según IEC 62443-2-1.

Soporte para gestión de la seguridad

Evaluación y consulta

Yokogawa provee una evaluación de control de la seguridad y servicio de consulta, identifica debilidades específicas y vulnerabilidades potenciales en los sistemas de control de proceso instalados e implementa medidas de seguridad que el cliente necesita.

Además, como se mencionó más arriba, la empresa obtuvo su certificación CSMS basada en IEC 62443-2-1 como integradora que construye sistemas de control de procesos. La empresa japonesa brinda servicios de consulta para ayudar a construir el ciclo de vida de seguridad y obtener certificaciones de acuerdo a estas normas.

Implementación de controles de seguridad en puntos finales

Yokogawa provee controles de seguridad apropiados para proteger los sistemas de control de procesos instalados en contra de las amenazas de ciberseguridad.

- Instalación de software antivirus y programas de actualización de la seguridad: se instala un software antivirus diseñado por *Yokogawa* y los programas de actualización necesarios para evitar la invasión e infección de programas maliciosos tales como virus.
- Listas blancas: se previene la ejecución de programas maliciosos como malware, incluyendo binarios permitidos y scripts como exe y dll o Java en la lista blanca, e inhabilitando la ejecución de programas que no están en la lista.
- USB Port Lock: el camino por el cual muchas amenazas se introducen directamente dentro, por ejemplo, en el HMI de los sistemas de control de procesos es, en muchos casos el de los dispositivos de almacenamiento auxiliares tales como una memoria USB que se puede conectar a los puertos USB. El camino de infección que parte de un puerto USB puede bloquearse física y teóricamente a través de capas bloqueadoras y modificando la configuración de la PC.

Soporte y mantenimiento

Yokogawa provee servicios de soporte y mantenimiento para mantener los controles de seguridad de los sistemas funcionando correctamente y actualizarlos para cubrir vulnerabilidades en operaciones normales. La empresa también brinda entrenamiento para ayudar a los clientes a implementar su propio ciclo de vida de seguridad. A esto se le pueden sumar consultas y evaluaciones adicionales según se necesite.

Por otro lado, ofrece un servicio de recuperación para minimizar el tiempo de parada de los sistemas de control de proceso de los clientes en caso de que ocurrieran problemas inesperados del sistema como un virus o falla del hardware. Además de los miembros que realizan el mantenimiento normal de los sistemas, hay otros que se dedican a responder los incidentes de seguridad para implementar una recuperación rápida que minimice el daño, y proponen medidas para que no vuelva a ocurrir.

Laboratorios de seguridad

Yokogawa invierte constantemente en sus recursos humanos y técnicos para mantener su alto nivel de competencia en el área de seguridad.

La empresa cuenta con laboratorios de seguridad en Singapur, Tokio (Japón), Bangalore (India) y Houston (Estados Unidos), en donde ingenieros de sistemas y expertos en ciberseguridad colaboran para aplicar las últimas tecnologías de ciberseguridad en los sistemas de *Yokogawa* y así ayudar a los clientes a proteger sus sistemas de las crecientes y cada vez más sofisticadas amenazas a la ciberseguridad.

Los laboratorios también investigan las últimas tecnologías acerca de seguridad y las implicaciones reales de la ciberseguridad para diversos entornos industriales, y desarrollan medidas y soluciones al respecto mejor adaptadas para los diferentes

Figura 4. Laboratorio de seguridad de *Yokogawa*

sectores, aplicaciones y configuraciones del sistema. Además, desarrolla, valida y muestra nuevos procedimientos y herramientas para los ingenieros de sistema y especialistas en seguridad de la propia empresa.

Otro rol importante de los laboratorios es actualizar constantemente los estándares y prácticas de seguridad de *Yokogawa*, incluyendo numerosos documentos y procedimientos de trabajo, que se preparan en base a normas internacionales, entre ellas, IEC 62443.

Resumen

El cibercrimen global ha crecido rápidamente, y las técnicas de ataque avanzaron y se complejizaron. Para asegurar la prevención y mitigación de los riesgos de los sistemas de control de procesos, es esencial que los clientes cultiven una cultura de la seguridad en todos sus departamentos y mejoren sus actividades sobre la seguridad en base a normas internacionales como IEC 62443.

La solución de ciclo de vida de la seguridad provista por *Yokogawa*, que obtuvo las certificaciones EDSA y CSMS, atiende estas cuestiones y garantiza actividades productivas protegidas y estables. ❖

Conocimientos y competencias: dos valores que pueden ser certificados

Ricardo A. Vittoni, Risknowlogy South America, *ricardovittoni@risknowlogy.com*

Ricardo Vittoni
Licenciado en Higiene y Seguridad en el Trabajo (Univesidad de Morón, 2008) y reconocido como Functional Safety Expert (*TÜV Rheinland*, 2006 y *TÜV SÜD*, 2009), se desempeña desde el año 2008 como responsable para Latinoamérica de la empresa *Risknowlogy* (Suiza). Es autor e instructor de cursos de aplicación de la seguridad funcional en procesos y en máquinas y está calificado como instructor para profesionales de ingeniería en SIS, con los avales de *TÜV Rheinland, TÜV Süd y Risknowlogy.*

Los sistemas instrumentados de seguridad (SIS) están normados por IEC 61511. Esta norma establece que "las personas, departamentos u organismos involucrados en actividades del ciclo de vida de seguridad deben ser competentes para realizar las actividades de las que son responsables". Ser competente significa tener los conocimientos y las competencias (aptitudes, habilidades y destrezas) adecuados para ejecutar una tarea específica, y todo profesional que trabaje en el ciclo de vida de un SIS debe poder demostrarlo en forma inobjetable para cumplir con los requisitos de la norma. En este artículo se explican brevemente qué son conocimientos y qué es competencia, y se plantea la importancia de que un profesional que se desempeña en el ciclo de vida de un SIS pueda obtener una certificación con validez internacional, que demuestre que es competente para las tareas que tendrá que realizar.

Conocimientos y competencias

Estos dos conceptos parecen equivalentes a primera vista. Es decir, podría parecer que una persona que tiene conocimientos es competente para realizar una tarea. Sin embargo, aunque los conocimientos son necesarios, no son suficientes para hacer a una persona competente.

Para obtener conocimientos, nuestra cultura ha desarrollado la educación formal, y la capacitación por medio de cursos de especialización, ambos medios sensiblemente mejorados con el advenimiento de la tecnología, que permite incorporar los conocimientos con la ayuda de medios audiovisuales e informáticos. No obstante, no es sino hasta su implementación práctica que una persona comienza a hacerse capaz de aplicar lo aprendido. En este momento adquiere un valor: sabe hacerlo.

Conocimientos = Educación formal + Capacitación

Pongamos como ejemplo un cuerpo de bomberos. Sus miembros reciben capacitación específica sobre sustancias inflamables, sobre los distintos tipos de fuego y sobre los diferentes medios para extinguirlos en condiciones ambientales diversas. Luego realizan tareas de adiestramiento, en las cuales ponen en práctica todo lo aprendido durante la capacitación, hasta hacerse diestros en el control de un incendio. Finalmente, para estar seguros de que en cualquier situación que se les pueda presentar, podrán apagar el fuego y salir con vida, realizan entrenamientos periódicos, poniendo en práctica, una y otra vez, con todas las variantes posibles, lo aprendido en la capacitación teórica y en el adiestramiento práctico. Finalmente, la participación activa en incendios reales les permite ir perfeccionando cada vez más su pericia, aunando su habilidad y la experiencia.

Podríamos decir, entonces, que recién luego de un buen tiempo de estar entrenando en forma sistemática, y haber extinguido varios incendios reales, el cuerpo de bomberos tendrá las competencias específicas y necesarias. Habrá entonces ganado un valor: desarrollar su trabajo con total profesionalismo y real efectividad.

Como vemos en este ejemplo, la competencia desarrollada es posterior al conocimiento adquirido, es la asimilación profunda de los conocimientos teóricos y el afianzamiento de estos gracias a la actuación (práctica en casos reales), una y otra vez, a lo largo del tiempo.

Competencia = Conocimiento + Adiestramiento + Entrenamiento + Actuación

Ser competente, fundamental en el ciclo de vida de un SIS

La norma internacional que regula el ciclo de vida completo de un SIS, esto es: la especificación, el diseño, la construcción, la operación, el mantenimiento y el desguace del SIS, es la norma IEC 61511. Ella expresa claramente: "Las personas, departamentos u organismos involucrados en actividades del ciclo de vida de seguridad deben ser competentes para realizar las actividades de las que son responsables". (IEC 61511-1:2016, cláusula 5.2.2.2).

Esto significa que serán muchas y diferentes las personas involucradas en el ciclo de vida de un SIS. Asimismo, desde la etapa inicial de especificación (identificación de peligros y evaluación de riesgos, asignación de capas de protección a funciones de seguridad, especificación de requisitos de seguridad), pasando por la etapa de diseño, ingeniería y construcción, siguiendo por la etapa de operación y mantenimiento, hasta finalizar con el desguace del SIS, los conocimientos y competencias requeridos serán muchos y diferentes, así como serán también diferentes las múltiples tareas involucradas en este ciclo de vida.

Pero, ¿es acaso comparable la exigencia de competencia en las personas que desempeñan alguna actividad en el ciclo de vida de un SIS, con la exigencia que se tiene, por ejemplo, para los miembros de un cuerpo de bomberos? La respuesta es sí, pues un SIS es un conjunto de funciones de seguridad (o de capas de protección) destinadas fundamentalmente a proteger a las personas, y también al medioambiente (que es como proteger a las personas que vivirán en el futuro), de los eventuales daños que sustancias peligrosas, o las condiciones físico-químicas en que éstas evolucionan, pudieran producirles.

Surge entonces una pregunta fundamental: si es tan importante que las personas sean competentes para desempeñarse en el ciclo de vida de un SIS, ¿cómo se puede demostrar la competencia de cada una de esas personas?

Certificación de conocimientos y competencias

Es bien sabido por todos nosotros que, cuando necesitamos comprobar, por ejemplo, que una persona tiene una serie de conocimientos específicos, será generalmente suficiente con tomarle un examen y pedirle un certificado de sus conocimientos. Pero para hacerlo, la persona que corrige el examen, o la que firma el certificado, debe haber demostrado previamente tener, al menos, los mismos conocimientos que están dando como válidos, lo cual nos lleva a plantearnos, nuevamente, cómo podemos tener certeza de que la persona que corrige el examen, o la que firma el certificado, es competente para hacerlo. Este dilema se resuelve generalmente con la creación de los cuerpos colegiados, y es así que tenemos

ingenieros, arquitectos, médicos, etcétera, que han demostrado sus conocimientos al ser sometidos a una junta examinadora de una determinada y reconocida universidad.

Lamentablemente, no existe una Facultad de SIS, ni una de Seguridad Funcional en ninguna universidad del mundo, pero existen, en cambio, organizaciones que reúnen profesionales de larga trayectoria en la materia, que son reconocidas a nivel internacional por su idoneidad, como las TÜV (Rheinland, SÜD), en Alemania; la ISA y el CSFE Governance Board, en Estado Unidos; *Sintef*, en Noruega, y algunas organizaciones privadas con presencia global, como *Exida* y *Risknowlogy*, por nombrar algunas. Serán, entonces, estas organizaciones las que podrán examinar a los profesionales destinados a realizar tareas del ciclo de vida de un SIS, y emitir, con un juicio acertado, certificados que demuestren que estas personas tienen los conocimientos necesarios para ello.

Pero, ¿solo los conocimientos pueden ser certificados? ¿Se puede tomar un examen para comprobar las competencias? Seguramente no, pues que una persona responda correctamente una pregunta solo demuestra que tiene conocimientos, según lo que analizamos anteriormente. Será necesario, entonces, someter a cada profesional, y al trabajo realizado por él durante varios años, a evaluación y juzgamiento (*assessment*, en inglés), para determinar si posee también las aptitudes, habilidades, destrezas y experiencia que hacen a la competencia. Serán también dichas organizaciones las que podrán emitir los certificados correspondientes.

Dentro de los roles que pueden ser certificados por sus conocimientos y competencias para actuar en el ciclo de vida de un SIS, podemos mencionar los siguientes:

- Operadores de planta
- Técnicos de mantenimiento
- Ingenieros de diseño
- Facilitadores de HAZOP, de LOPA, de desarrollo de especificaciones, etcétera
- Verificadores
- Auditores

Importancia del reconocimiento internacional

Pero nuevamente, ¿qué garantía podemos tener de que los criterios usados por cada una de esas organizaciones son equivalentes y útiles para cualquier SIS instalado en cualquier parte del mundo? Bueno, para eso existe, en principio, la norma IEC 61511, que establece los lineamientos básicos del ciclo de vida de un SIS, pero existe también la norma ISO/IEC 17024, que se emite "con el objetivo de lograr y promover un punto de referencia aceptado a nivel mundial para las organizaciones que operan la certificación de personas". Según esta norma, "la certificación de personas es un medio de garantizar que la persona certificada cumple con los requisitos del esquema de certificación", y que "la confianza en los respectivos esquemas de certificación se logra por medio de un proceso de evaluación aceptado a nivel mundial, vigilancia posterior y reevaluaciones periódicas de la competencia de las personas certificadas".

De esta forma, las organizaciones mencionadas anteriormente podrán certificar los conocimientos y las competencias de las personas que deban actuar en el ciclo de vida de un SIS, usando esquemas de certificación que estén de acuerdo, por ejemplo, con los criterios establecidos por ISO-IEC 17024. Las certificaciones así emitidas serán reconocidas internacionalmente, y un profesional certificado en Argentina, por ejemplo, podrá ser contratado en cualquier país del mundo, sin tener que volver a demostrar sus conocimientos y competencias antes de realizar su trabajo.

Tomemos el ejemplo del señor John Doe (figura 1):

- John Doe es un profesional independiente, que se ha capacitado en seguridad y salud ocupacional, y en el uso práctico de la norma IEC 61511.
- Luego de trabajar seis años en tareas del ciclo de vida de un SIS, siguiendo los lineamientos de IEC 61511, obtuvo su certificación como profesional de seguridad funcional (FSP).
- Luego de reunir otros cinco años de práctica como FSP, obtuvo su certificación de competencias como profesional certificado en verificación SIL y cálculos de confiabilidad.

Conclusiones

Se ha analizado qué son los conocimientos y qué las competencias, llegando a la conclusión de que, mientras los primeros son necesarios, solo la aplicación de esos conocimientos en forma práctica y continuada, a lo largo del tiempo, permitirá desarrollar las competencias adecuadas.

Se ha visto que la norma IEC 61511, que regula los SIS, requiere que todas las personas que trabajen en el ciclo de vida de seguridad sean competentes, es decir, que tengan, para cada tarea que deban realizar, dos valores fundamentales: conocimientos y competencias.

Se ha establecido que una de las formas prácticas de saber cuándo una persona es competente es someterla a una examinación de sus conocimientos, y a una evaluación y juzgamiento de sus competencias, por una organización de reconocida trayectoria en la materia que emita certificados apropiados.

Se han mencionado los roles principales dentro del ciclo de vida de un SIS que pueden certificados.

Se ha establecido la importancia de contar con una norma de alcance internacional, como la ISO-IEC 17024, que permita la certificación de las personas de acuerdo a un esquema de certificación homologado en todo el mundo.

Conocimientos y competencias, dos valores que pueden ser certificados, para estar seguros de que los SIS sean, realmente, sistemas de protección que logren mantener a salvo a las personas y al medioambiente de los peligros inherentes a la industria de procesos. ❖

Figura 1. Profesional con conocimientos y competencias certificados

Seguridad: la clave para un desarrollo exitoso de IIoT

Fabrice Jadot
Scheneider Electric
www.schneider-electric.com.ar

Palabras clave:
Automatización, ciberseguridad, IIoT, innovación en todos los niveles, PLC, desarrollo seguro del ciclo de vida, protocolos seguros, seguridad

La Internet industrial de las cosas (IIoT) es un tema candente de los últimos años. Una cuestión clave que impactará sobre su aceptación definitiva es la seguridad. Un ataque exitoso a un sistema IIoT podría resultar en la pérdida de datos relevantes, interrupción de operaciones y destrucción de los sistemas. Esto resultará en el daño a la marca y la reputación, pérdida económica y daño a la infraestructura crítica. Peor aún, podría dañarse el ambiente, o lastimar y perder una vida humana. Una solución segura de IIoT comprende una variedad de elementos que incluye productos seguros, protocolos seguros, una red segura, monitorización de seguridad permanente y empleados con experiencia en ciberseguridad.

Protocolos de seguridad

Los sistemas IIoT presentan nuevas técnicas de conexión que requerirán protocolos de comunicación seguros. Es importante tener en cuenta dos conceptos clave a la hora de discutir protocolos de seguridad, encriptado e integridad/autenticidad de los datos. El encriptado se puede usar para asegurar protocolos, pero puede anular otras aplicaciones de seguridad como sistemas de detección de intrusión. La integridad y autenticidad de los datos se puede proveer sin encriptado, y son compatibles con sistemas de detección de intrusión.

Los sistemas tradicionales utilizaban protocolos de comunicación inseguros. Los protocolos de comunicación evolucionan para incorporar mejoras de seguridad: DNP3 se convierte en DNPV5, OPC-UA, Modbus evoluciona hacia Modbus Seguro y EtherNET/IP se convierte en EtherNET/IP Seguro. Es necesario seleccionar protocolos seguros para mejorar la solución de seguridad.

Permeabilidad de la confianza en el ciclo de vida de IIoT

La confianza en el ciclo de vida de IIoT se refiere tanto a la integridad de cada elemento en un sistema como a la integridad de los datos generados por el sistema. La confianza impacta sobre la cadena de suministro, la instalación, la configuración, el uso regular y un eventual desmantelamiento; requiere de un monitoreo constante para asegurar que se preserva la integridad durante todo el ciclo de vida del producto.

Recurramos a un ejemplo para ilustrar la permeabilidad de un modelo de confianza. Supongamos un usuario final que adquiere un PLC con características de seguridad. El vendedor del PLC adquiere los microprocesadores y la memoria de vendedores de componentes que envían sus productos a los sitios de fabricación. El software del producto se puede desarrollar en las instalaciones de desarrollo del vendedor o adquirir de otros socios. Los productos se fabrican y envían hacia los depósitos. El equipamiento puede luego enviarse a distribuidores o integradores de sistemas antes de llegar hasta el usuario final. En este ejemplo, encontramos muchas organizaciones manipulando el hardware/software. Existe un potencial de problemas de seguridad que se pueden introducir en cualquiera de esas locaciones. Los usuarios finales deben confiar en la totalidad de la cadena de suministro que provee los componentes del sistema. La permeabilidad de la confianza entre los operadores del sistema y los proveedores es clave para la seguridad de los sistemas de IIoT.

Fabrice Jadot
Jefe de la Oficina de Tecnología para Industria en *Scheneider Electric*, empresa en la que trabaja desde 1997. Desde 2015 es miembro de ODVA, una asociación internacional que reúne miembros de empresas líderes en automatización.

Ser experto en ciberseguridad

Un desafío que enfrentan muchos usuarios finales industriales es la experiencia en ciberseguridad. El personal industrial desarrolló competencias focalizadas en optimizar los procesos. Las pequeñas y medianas empresas en particular quizá presenten dificultades internas para adquirir habilidades en ciberseguridad. Los vendedores de equipos e integradores de sistemas pueden sacar ventaja y ofrecer una opción rentable de experiencia en seguridad. Los proveedores, efectivamente, mezclan el control industrial y la experiencia en ciberseguridad, muchos consultores TI carecen de experiencia OT. Los proveedores también tendrán experiencia para guiar a los usuarios finales durante la elección de datos del proceso que deberían ser relevantes.

Otra cuestión clave es el entrenamiento para operar apropiadamente el sistema una vez activado. Deben seguirse algunos consejos para operar, monitorear y actualizar los procesos de forma efectiva. Una guía acerca de las políticas de seguridad apropiadas para la empresa también es importante.

Consideraciones sobre la nube

Los servicios en la nube permiten que se utilice potencia informática externa para analizar y controlar la infraestructura OT. En una arquitectura en la nube, se almacena y analiza la información de miles de dispositivos, y a ella se accede desde un servidor. La infraestructura de la nube se puede colocar dentro de la red corporativa, o fuera y operada por un tercero asociado. Muchos usuarios finales están implementando un modelo de nube interno. Los datos obtenidos de IIoT se almacenarían y acumularían en los equipos de una red corporativa. Contener los datos en equipamiento interno conectado a una red controlada por el usuario final ayuda a salvaguardar datos potencialmente críticos.

Recurrir a un tercero asociado genera una cantidad de cuestiones de confianza que pueden impactar en la seguridad y privacidad. La información debe estar protegida tanto respecto de privacidad como de seguridad. Por ejemplo, unas credenciales robadas podrían permitir que los atacantes accedan a datos importantes. Aún más, se pueden propagar los ataques a nubes de otros clientes de ese socio.

Productos seguros y lidiar con el equipamiento existente

El primer concepto clave involucra sistemas de seguridad. El ciclo de vida del producto tiene un gran impacto en la seguridad de las aplicaciones industriales. A diferencia de los entornos TI, en los sistemas de control industrial, los productos pueden permanecer activos y en servicio durante treinta años. Es ingenuo asumir que los usuarios finales actualizarán todos sus componentes antiguos cuando implementen IIoT. Además, los sistemas IIoT incluirán dispositivos finales tradicionales que fueron desarrollados antes de la llegada de los nuevos estándares de seguridad junto con dispositivos finales nuevos con características de seguridad integradas.

Comencemos observando los desafíos que implican los dispositivos tradicionales. La mayoría de las instalaciones industriales contiene equipamiento que ya quedó anticuado desde una perspectiva de seguridad TI. Un equipamiento tradicional está más expuesto a un ataque que uno con las últimas versiones de seguridad integradas. Hay dos opciones disponibles para mitigar esto. La elección de una de las dos está impulsada por la aplicación:

- Limitar la comunicación solamente a la recolección de datos. Esta es la opción más segura pero quizá no es viable para todas las aplicaciones.
- Restringir el acceso a dispositivos. Note que esto requerirá monitorear la integridad de las comunicaciones para asegurar que los datos no se modificaron durante su viaje entre dispositivos. Esta opción es más práctica, dado que limitar el acceso a la recolección de datos no es compatible con muchas aplicaciones.

Los dispositivos que han sido desarrollados más recientemente incluirán cuestiones de seguridad. En este caso quizá se pueden operar sin necesidad de construir un sistema de seguridad alrededor de ellos.

Consideraciones cuando se adquiere equipamiento

Si los clientes optan por actualizar su equipamiento, seleccionar uno con firma de firmware y software es importante para la asegurar el parcheo seguro. Debería también inclinarse hacia productos con un ciclo de vida de desarrollo seguro (SDL). La mayoría de las organizaciones cuenta con un proceso bien definido para crear, lanzar y mantener productos. Sin embargo, el crecimiento apremia y los riesgos asociados a productos inseguros condujo a que se prestara más atención a la necesidad de integrar la seguridad dentro del proceso de desarrollo. Se debería pedir a los posibles proveedores que den una prueba de que los centros de desarrollo están certificados según estándares tales como IEC 62443-4-1. La certificación de un tercero acerca de un proceso de desarrollo puede otorgar una garantía de que los productos fueron desarrollados según prácticas seguras, reduciendo la posibilidad de introducir algún riesgo.

Conclusión

Conectar los dispositivos entre sí y a la nube abre la puerta a un proceso inteligente que potencialmente conduce a mejoras significativas en productividad y eficiencia. Las herramientas para implementar con éxito IIoT están en su lugar ahora, pero el cambio será evolución vs. revolución. Los usuarios finales sopesarán el valor de la nueva funcionalidad contra el riesgo de realizar cambios a su sistema de control que impedirá un cambio rápido. La seguridad será un factor clave. Cuando se implementa un IIoT, deberán considerarse el diseño del sistema, las características del producto, los procesos de desarrollo seguros, y la experiencia en la implementación. ❖

Cuantificación de los beneficios de la optimización del portafolio de inversiones frente a la priorización en las organizaciones con gran inversión de activos

I. Tamimi y Dr. P. Beullens (Universidad de Southampton) S. Sadnicki (Copperleaf)
ibrahimissam3@gmail.com; p.beullens@soton.ac.uk; ssadnicki@copperleaf.com
MDE Network

Palabras clave
Planificación y gestión de inversión de activos, análisis de decisiones, optimización, priorización, beneficios cuantificados de la gestión de activos

Resumen

A lo largo de los años, muchas organizaciones han tomado decisiones de inversión sobre la base de un proceso convencional de clasificación y priorización. Al priorizar, se determina un puntaje fijo para cada inversión; esto puede ser una medida del rendimiento financiero de la inversión (por ejemplo, valor actual neto) o posiblemente una medida del riesgo que la inversión mitigará para la organización (puntaje del riesgo). Durante la priorización, el portafolio de inversiones se clasifica según ese puntaje fijo y luego se seleccionan las inversiones que pueden ejecutarse dentro de los límites del presupuesto. La optimización matemática que utiliza la programación lineal puede mejorar los resultados de la optimización y alcanzar resultados con valores más altos, respetando a la vez múltiples limitaciones (por ejemplo, tolerancia financiera, de nivel de servicio, de recursos, de tiempo, de dependencias entre proyectos y de riesgo).

Si bien distintas organizaciones han reportado beneficios importantes al usar las técnicas de optimización, los resultados son específicos a cada contexto operativo. Este estudio busca generalizar los resultados y cuantificar el valor obtenido al usar técnicas de optimización en los portafolios de inversiones de activos.

Contexto

En los últimos años, el análisis de decisiones *(Decision Analytics)* se ha convertido en una disciplina. Según un estudio de investigación de *Sloan Management Review* del MIT, las compañías que incorporan el análisis en su cultura tienen más éxito en la nueva era digital, y el 87 por ciento de los encuestados fomentan el uso del análisis en sus organizaciones para tomar mejores decisiones [1]. Aunque la palabra 'optimización' quizás se use demasiado en el ámbito laboral, "vamos a optimizar nuestros procesos", el uso de la verdadera optimización matemática es menos frecuente a pesar de proveer el mayor valor en el espectro del análisis descriptivo-predictivo-prescriptivo y proporciona la mayor ventaja competitiva [2].

Para las organizaciones que realizan grandes inversiones de activos, el proceso de planificación de inversión de activos es el candidato principal para los métodos de optimización. A nivel del proyecto (o de intervención de los activos), cada proyecto potencial tiene generalmente un impacto en múltiples indicadores clave de rendimiento (KPI) o medidas de valor de la organización, lo que genera un requisito de análisis de múltiples criterios para la toma de decisiones (MCDA). Cuando los proyectos potenciales se incluyen en los portafolios de inversión, las organizaciones quieren determinar qué inversiones hacer y el momento para hacer esas inversiones y proporcionar así, el mayor valor a la organización.

Una manera de abordar el problema es mediante un proceso convencional de clasificación y priorización. En su forma más básica, esto implica ordenar una lista de riesgos de activos o proyectos potenciales en *Excel*. No obstante, la priorización no puede manejar la naturaleza de múltiples criterios y otras complejidades (por ejemplo, opciones y dependencias del proyecto) del proceso de planificación de inversión de activos y, como consecuencia, cualquier priorización generalmente resulta en soluciones por debajo del nivel óptimo. Por el contrario, la optimización matemática y, en particular, la programación lineal entera mixta (MILP), determina la solución óptima para maximizar el valor según todas las limitaciones del portafolio.

Este estudio prueba el beneficio de la optimización MILP sobre la priorización convencional mediante la investigación de la mejora en el valor del portafolio. Esta es una pregunta importante para los clientes que elaboran un caso de negocio para invertir en herramientas avanzadas para apoyar sus procesos de planificación de inversión de activos. En este estudio, hemos definido el objetivo estadístico de la siguiente manera: "Las organizaciones que optimizan (en oposición a las que priorizan) sus portafolios de inversión de activos pueden proporcionar un x por ciento más de valor con la misma cantidad de gasto".

Revisión bibliográfica

En general, falta evidencia documentada de los beneficios tangibles de las técnicas avanzadas de gestión de activos. El problema de la optimización del portafolio de inversión no es diferente.

Copperleaf tiene múltiples ejemplos puntuales de su base actual de clientes [3]. Por ejemplo:

- Una organización obtuvo 42 millones de dólares adicionales al valor de su portafolio a través de técnicas de optimización.
- Otra organización demostró una mejora del seis por ciento (6%) al comparar un portafolio optimizado contra el mismo portafolio priorizado.

La tesis doctoral de Wijnia de 2016 [4] proporciona más ejemplos que incluyen diversos problemas relacionados, tales como la optimización de un único activo, la asignación del presupuesto anual y la optimización de todo un sistema. Wijnia encuentra consistentemente una mejora del veinte por ciento (20%) en relación con el valor del riesgo basado en la optimización.

Lógicamente, existen dudas sobre confiar en la evidencia de las anécdotas de una o dos organizaciones similares. Esto hace que se necesite un resultado generalizado de manera que otras organizaciones que realicen grandes inversiones de activos puedan considerar los beneficios potenciales disponibles dentro de su contexto específico.

Metodología

El Centro de Investigación Operativa, Ciencia de la Administración y Ciencia de la Información de la Universidad de Southampton (Inglaterra), llevó adelante este estudio como parte de la tesis de Maestría en Ciencias del autor.

En primer lugar, el investigador construyó una metodología para generar portafolios de

inversiones representativos. Se utilizaron datos de inversiones reales proporcionados por diversas organizaciones con gran inversión de activos para garantizar que los portafolios fueran lo más representativos posibles de los portafolios de inversión potenciales de una organización con gran inversión de activos. Se evaluaron dos situaciones:

- Un algoritmo de priorización tradicional
- Optimización MILP

Después de repetirlo varias veces, los resultados obtenidos son efectivamente una simulación Montecarlo de priorización y optimización del portafolio de inversión que puede analizarse para obtener resultados generales sobre la diferencia en el valor general entre las dos técnicas.

Diseño de factores

Naturalmente, existen muchos factores que afectan la naturaleza del proceso de optimización del portafolio. Estos factores tendrán un impacto en la magnitud de la proporción de mejora del valor sobre el método de priorización. Hemos tomado en cuenta varios de estos factores al completar el análisis y resaltamos otros elementos que se verían beneficiados a partir de una mayor investigación.

Hemos incluido los siguientes factores claves:

- Cantidad de inversiones dentro del portafolio. Las inversiones pueden considerarse como cualquier proyecto o actividad de intervención llevado a cabo para proporcionar valor a la organización. El portafolio es un conjunto de inversiones.
- Posibilidad de que las inversiones tengan múltiples alternativas. Las alternativas son diferentes opciones de inversión para mitigar el mismo riesgo o para satisfacer la misma necesidad (por ejemplo, renovación, reemplazo o cambio en el esquema de mantenimiento, etcétera).
- Duración de un período limitado (por ejemplo, optimización para producir el plan de inversión del año siguiente o un plan de negocio regulatorio de cinco años).
- Otros factores para investigación futura son:
- Inversiones con gasto plurianual (en lugar de proyectos para un solo año).
- La 'aspereza' del límite presupuestario del período (por ejemplo, qué porcentaje del portafolio potencial puede ejecutarse durante el período limitado).
- La cantidad de limitaciones del portafolio (por ejemplo, limitaciones financieras, de nivel de servicio y recursos).
- Dependencias entre las inversiones (por ejemplo, que la ejecución de una alternativa de inversión sea en una fecha posterior a otra alternativa de inversión relacionada).

Se eligió un experimento factorial para reducir la cantidad de pruebas requeridas y ayudar a entender las interacciones entre diferentes factores. A los tres factores elegidos, se les asignaron los siguientes 'niveles':

- Cantidad de inversiones dentro del portafolio
  - Nivel 'bajo' de mil inversiones
  - Nivel 'alto' de mil inversiones
- Cantidad de alternativas de inversión:
  - Todas las inversiones con una y solo una alternativa de inversión
  - Las inversiones tienen las mismas probabilidades de tener una, dos o tres alternativas de inversión.
- Duración del período limitado
  - Un plan anual con una limitación de un año
  - Un plan de cinco años con limitaciones de cinco años

Estos factores se combinaron para proporcionar ocho (2^3) observaciones. Por ejemplo, la observación n.° 1 tenía un portafolio de cien inversiones, cada una de las cuales consideraba una alternativa única para un plan anual.

Se generaron otras características para cada inversión/portafolio de inversión:

- El costo de la inversión siguió una distribución de probabilidad predeterminada y pronosticado dentro de un solo año.
- Se simuló el riesgo mitigado por cada inversión mediante la generación de una condición inicial y una de impacto para un activo de muestra. La degradación del activo fue simulada usando una muestra de la curva de degradación de condición (que provoca un aumento de la probabilidad de falla a lo largo del tiempo).
- La combinación de la condición inicial con la degradación del activo proporciona un riesgo base que cambia con el tiempo. De manera similar, el efecto de la condición del impacto proporciona un perfil de riesgo residual después de la intervención. Por lo tanto, el valor de la inversión es el nivel del riesgo mitigado (el delta entre los perfiles de riesgo base y residual).
- La 'aspereza' del problema de optimización se mantuvo constante, independientemente de la combinación de los factores mencionados anteriormente.

Mediante la simulación de degradación del activo, se capturó una importante característica de los portafolios de inversión de activos: los riesgos de los activos cambian con el tiempo y, por lo tanto, diferir una inversión provocaría la mitigación de un nivel de riesgo distinto. Esta naturaleza del valor de la inversión basada en el tiempo puede calcularse dinámicamente dentro de algoritmos de optimización avanzados, algo que no se captura de forma habitual en los algoritmos de priorización. Investigaciones futuras podrían considerar la diferencia entre la optimización dinámica y estática del valor.

Priorización

El modelo de priorización está diseñado como un algoritmo codicioso. Una de las desventajas inherentes del estudio de priorización es que se debe seleccionar un factor para clasificar todas las inversiones, a pesar de saber que el espacio de decisión es mucho más complejo. Para este estudio, elegimos clasificar las inversiones según la magnitud del nivel de riesgo inicial. Este es un enfoque común entre los servicios públicos que aún tienen que implementar técnicas de optimización avanzadas; se clasifican todos los riesgos y se seleccionan las intervenciones asociadas hasta agotar el dinero disponible (priorización de línea de corte). Los enfoques alternativos incluyen una clasificación basada en el riesgo neto (por ejemplo, nivel de riesgo inicial, nivel de riesgo posterior a la intervención); riesgo/dólar, riesgo neto/dólar; un puntaje ponderado de diversos factores; o VAN de la inversión (donde el riesgo monetizado es un componente).

Además, si una inversión tiene múltiples alternativas, el algoritmo de priorización elige la alternativa con el nivel más bajo de riesgo posterior a la intervención dado que solo una alternativa puede avanzar hacia el proceso de priorización clasificado. Cuando las inversiones o las alternativas tengan la misma clasificación, se selecciona la opción de menor costo.

Las inversiones se planifican dentro de los límites monetarios según el orden de la lista. A su vez, por cada año restringido, el algoritmo desciende en la lista hasta que ninguna de las inversiones restantes pueda incluirse dentro de la limitación. A cualquier inversión que no se seleccione el primer año, las fechas de inicio se trasladan un año y el proceso se repite por cada período con restricciones. Otra desventaja frecuente del algoritmo de priorización es que la 'clasificación de riesgo' estática no se actualiza a medida que las inversiones se trasladan en el tiempo; en realidad, la clasificación

Portafolio OBS13P8	Priorización	Optimización
Beneficio de la mitigación del riesgo de seguridad ($k)	212.029	215.500
Beneficio de la mitigación del riesgo ambiental ($k)	63.609	64.650
Beneficio de la mitigación del riesgo financiero ($k)	21.203	21.550
Total costo de la inversión ($k)	174.562	170.361
Valor total del portafolio ($k)	122.279	131.339
Porcentaje de mejora		7,4%

Tabla 1. Valor del portafolio de muestra para una simulación única

Tamaño del portafolio: cien inversiones	Inversiones con alternativa única	Inversiones con alternativa variable
Período de planificación de un año	6,6%	14%
Período de planificación de cinco años	8,6%	20,2%

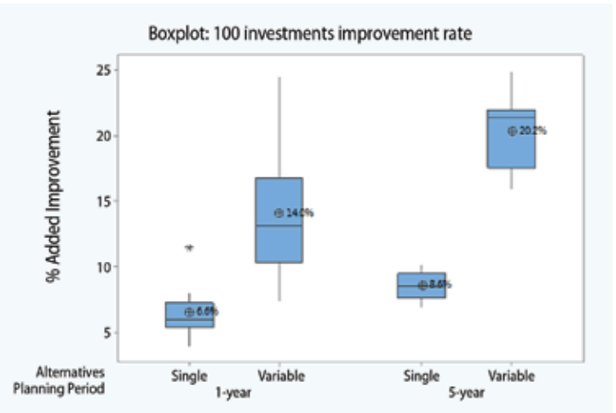


Figura 1. Gráfico de caja y mejora porcentual promedio para las observaciones con portafolios de cien inversiones.

puede cambiar debido al deterioro de los activos en diferentes proporciones.

Optimización

En la optimización (realizada con *Copperleaf C55*), se monetizaron todos los riesgos, y la mitigación de riesgos anual se incluyó en el cálculo del VAN de la inversión. Luego se utilizó un algoritmo de programación lineal entera mixta (MILP) para maximizar el valor del portafolio respetando diversas limitaciones (en este caso, una restricción financiera única). Cabe destacar que, dado que el motor de optimización consideró diferentes alternativas de inversión y una posible postergación de las inversiones, el valor de la inversión se recalculó de forma dinámica.

Simulación Montecarlo

En cada una de las ocho observaciones (combinaciones en el diseño factorial), repetimos el análisis varias veces. Se llevaron a cabo un total de sesenta simulaciones: diez por cada portafolio cuando la cantidad de inversiones era de cien, y cinco por cada portafolio cuando la cantidad de inversiones era de mil.

Resultados

Se generaron datos por cada ciclo de simulación. En particular, hemos registrado el valor total del portafolio, dividido por mitigación de riesgo y costo neto de inversión, para el portafolio priorizado y el optimizado.

Los resultados para uno de los portafolios se muestran a continuación. En este ejemplo, observamos que el algoritmo de optimización selecciona un portafolio con 7,4 por ciento más del valor total que el algoritmo de priorización (ver tabla 1).

Al combinar los resultados de la simulación Montecarlo, podemos generar un factor promedio de mejora para cada uno de los ocho factores de observación. En la figura 1, se muestran las observaciones donde los portafolios generados contenían cien inversiones.

El diagrama de caja ilustra:

- El valor promedio (según la tabla correspondiente)
- La línea de valor de la mediana trazada a través de la caja
- La caja de rango intercuartílico; cincuenta por ciento (50%) medio de los datos
- Los 'bigotes' superiores e inferiores que muestran el veinticinco por ciento (25%) superior e inferior de los datos (sin incluir los valores atípicos)
- Un valor atípico (*) que está por fuera de los bigotes

Luego se completó el mismo análisis con portafolios con mil inversiones. Los resultados se muestran en la figura 2.

Comentario sobre los resultados

Los resultados muestran que la optimización siempre produce un valor del portafolio más alto con las mismas limitaciones monetarias comparado al modelo de priorización. Esto es constante en el rango de siete a veinte por ciento (7-20%).

En segundo lugar, la ventaja de la optimización se intensifica a medida que aumenta la complejidad. Por ejemplo (teniendo en cuenta los portafolios de mil inversiones):

- La presencia de múltiples alternativas de proyectos duplicará el beneficio de optimización

Tamaño del portafolio: mil inversiones	Inversiones con alternativa única	Inversiones con alternativa variable
Período de planificación de un año	6,6%	13.3%
Período de planificación de cinco años	10,3%	20,3%

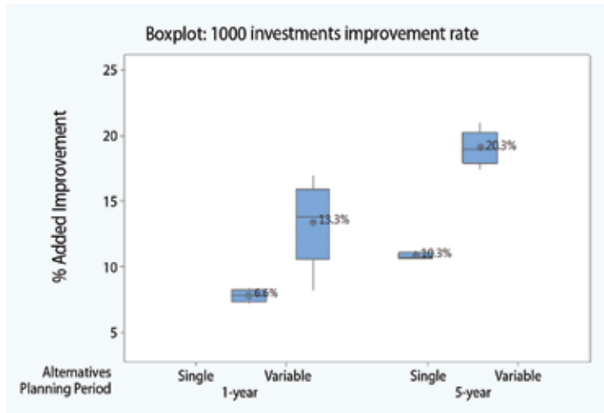


Figura 2. Gráfico de caja y mejora porcentual promedio para las observaciones con portafolios de mil inversiones

- Para el período de planificación de un año, la tasa de mejora aumenta del 6,6 al 13,3 por ciento
- Para el período de planificación de cinco años, la tasa de mejora aumenta del 10,3 al 20,3 por ciento
- Una restricción de varios años aumenta el beneficio de optimización en aproximadamente cincuenta por ciento (50%)
- Para las alternativas únicas, la tasa de mejora aumenta del 6,6 al 10,3 por ciento
- Para las alternativas múltiples, la tasa de mejora aumenta del 13,3 al 20,3 por ciento

Un análisis factorial completo (que se completó con MATLAB) confirma que los dos factores mencionados anteriormente tienen un efecto sobre el beneficio de optimización, pero el tamaño del portafolio (es decir, la cantidad de inversiones) no afecta los resultados. Esto puede parecer ilógico a primera vista. No obstante, el fundamento de este hallazgo probablemente se deba al hecho de que la 'aspereza' se mantuvo constante a pesar del aumento en la cantidad de inversiones. Si el presupuesto total se mantuviera independiente de la cantidad de inversiones, probablemente habría tenido un impacto significativo.

En la actualidad, se continúa investigando para mejorar nuestro entendimiento acerca de las diferencias entre la priorización y la optimización para escenarios de usuarios particulares que incluyen inversiones plurianuales. Se recomienda ampliar las investigaciones sobre el análisis de otros factores (específicos del sector) posiblemente importantes (por ejemplo, cuando las alternativas de inversión tienen interdependencias) o cuando el ajuste del problema puede estar sujeto a actualizaciones periódicas (por ejemplo, actualizaciones del conjunto de inversiones o presupuestos disponibles).

Conclusiones

En resumen, los resultados muestran que la optimización proporciona una mejora significativa constante frente a la priorización al construir planes de inversión. Las organizaciones pueden tener mayor confianza en que la implementación de técnicas de optimización avanzadas ofrecerán un beneficio significativo.

En particular, nuestro análisis respalda la conclusión de que las organizaciones que optimizan (en lugar de priorizar) sus portafolios de inversión de activos pueden proporcionar entre siete y veinte por ciento (7-20%) más de valor de sus portafolios cuando se enfrentan a las mismas limitaciones financieras. El mayor factor de mejora se aplica a las organizaciones que consideran las inversiones con múltiples alternativas en un plan de inversión plurianual.

Se recomienda continuar investigando para evaluar el impacto de otros factores identificados. ❖

Menciones

Los autores agradecen al Centro de Investigación Operativa, Ciencia de Administración y Ciencia de la Información de la Universidad de Southampton y, en particular, a Pete Becque por desarrollar el alcance del proyecto junto con *Copperleaf*.

Referencias

[1] "The Analytics Mandate, Data & Analytics Global Executive Study and Research Project", MIT Sloan *Management Review* (2014)
[2] T. H. Davenport & J. G. Harris. *Competing on Analytics, The New Science of Winning*, Figure 1-2, page 8. (2007)
[3] The ROI of C55, *Copperleaf White Paper* (2016)
[4] Y.C. Wijnia. *Processing Risk in Asset Management – Exploring the Boundaries of Risk Based Optimization Under Uncertainty for an Energy Infrastructure Asset Manager*, PhD Thesis, TU Delft, NL (2016)

Adquisición, registro y reportes dinámicos de datos

Darío Zyngierman,
Afcon Control &Automation
darioZ@afcon-inc.com
www.afcon-inc.com

Afcon Pulse Historian es la evolución de *Afcon* en materia de registradores de datos de alto rendimiento. Permite almacenar información en un sistema de bases de datos relacional y consultarla fácilmente. Se pueden generar diariamente grandes volúmenes de información del sistema de control del cliente, ya sea de la industria de automatización, piso de planta, gestión de edificios, detección de incendios, control de acceso y seguridad, etc.

A la información que almacena *Pulse Historian* se puede acceder fácilmente desde los sistemas empresariales, y visualizar mediante el *PulseSupremeReport*, desarrollado por *Afcon* y ya incorporado en el producto. El sistema cuenta con un amplio rango de capacidades para informar y analizar datos históricos o en tiempo real, que permiten la visualización e incrementar la eficiencia operacional y energética.

Afcon Pulse Historian ofrece métodos avanzados para acceder a la información y *Business Intelligen*t (BI) simplifica la generación de informes y preserva recursos de tecnología informática (TI), dando lugar a una toma de decisiones con mayor rapidez y seguridad.

Sistema de procesamiento de datos altamente organizado y escalable

El sistema reúne tanto datos históricos como en tiempo real, y los convierte en información útil, permitiendo mayor escalabilidad y despliegue de escenarios.

Más allá del tamaño de la operación, es capaz de recolectar y almacenar todos los datos importantes procesados y generados diariamente por el sistema de control del cliente. Puede desarrollarse en una sola instalación o planta y luego crecer hasta convertirse en una solución de múltiples niveles y sitios. Así, fortalece el almacenamiento de datos tanto local como a nivel corporativo facilitando los requerimientos más exigentes de informes y análisis de datos.

Por su capacidad de configurar arquitecturas de varios niveles, ofrece la flexibilidad que se necesita en las redes de infraestructuras modernas, permitiendo la continuidad de los negocios junto con la facilidad de uso que se espera.

Optimización y visibilidad de procesos

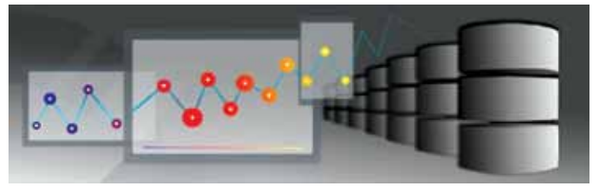
Construido específicamente para la adquisición escalable, almacenamiento y acceso de información industrial, *Afcon Pulse Historian* mejora la visibilidad, provee un contexto para los datos en crudo, y reúne la información dispersa geográficamente.

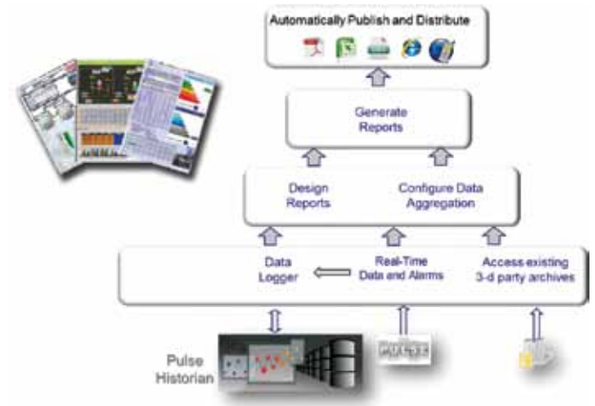
Es posible comparar resultados de producciones pasadas, analizar los datos anteriores a un evento específico y diseñar series de producción optimizadas. Puede generar y distribuir informes automáticamente y compartir información con toda la empresa por medio del *SupremeReport*. El sistema soporta un sistema de reportes modernos, que pueden crearse rápidamente, lo que provee a las empresas múltiples beneficios.

Alto rendimiento

Afcon Pulse Historian optimiza la información de la planta, captura los datos de una forma mucho más rápida que los sistemas de bases de datos estándar y entrega resultados en tiempo real de datos con resoluciones del orden de los milisegundos.

Está diseñado para gestionar el continuo de valores ocurridos en un periodo de tiempo, lo que difiere radicalmente del estilo de información aislada de una típica base de datos. Combina una veloz recolección de datos con extensiones de periodos de tiempo con una base de datos SQL asignada para optimizar el rendimiento tanto de almacenamiento como de acceso a los datos. Además, incorpora *Business Intelligent*, desarrollado por la misma empresa, que reduce los requisitos de almacenamiento a la vez que preserva los datos importantes.





Integración sencilla mediante software

El sistema forma parte del software *SCADA/HMI Afcon Pulse*, una solución de software industrial de alto rendimiento que incluye SCADA/HMI, análisis avanzados, sistemas avanzados de distribución e informes, gestión de eventos/procedimientos, aplicaciones móviles, y más. Responde a un amplio rango de desafíos operacionales para diversas industrias.

Afcon Pulse Historian suma habilidades de recolección de datos y toma información de múltiples sensores y sistemas. Está basada en el hecho de que *Afcon Pulse* soporta más de 150 drivers nativos y estándares de fabricación propia, así como OPC. ❖

Protección de compresores: la válvula anti-surge

Gerardo Ramírez Herrera
GE Oil & Gas – Flow & Process Technologies, *www.geoilandgas.com*

Introducción

Dado el auge de la industria de gas, principal combustible de plantas de generación eléctrica, así como materia prima para otros negocios como la industria del etileno, los compresores que le dan movimiento para transportarlo a lo largo del país, así como también para suministrarlo a los complejos procesadores y transformadores, son de vital importancia y parte fundamental de la industria en general. Mantener protegidos a estos equipos críticos es una necesidad, tanto por su propio costo, como también por lo cuantioso de las posibles pérdidas de la producción. La válvula de control automático anti-surge juega un papel preponderante en la protección de los compresores de gas, al prevenir el fenómeno conocido como "surge" del compresor con sus efectos destructivos.

La transmisión de gas natural a través de los gasoductos tendidos a través del país requiere de un proceso de compresión para poder moverlo y que llegue a los puntos de destino; dependiendo de la orografía y distancias a recorrer, podría requerir de estaciones de recompresión. Estos gasoductos se construyen en diferentes tamaños como 8, 12, 24 o 36 pulgadas, y mayores aún, dependiendo del volumen que necesitan los grandes consumidores. Típicamente, los compresores son impulsados por un motor basado en una turbina de gas, y en ocasiones, los gases de escape de estas turbinas se utilizan para calentar un volumen de agua y así generar vapor, el cual se puede recalentar y utilizar para dar movimiento a una turbina de vapor, a la cual se acopla un generador eléctrico, resultando con esto una central de cogeneración eléctrica.

Los compresores de gas pueden elevar la presión hasta niveles mayores a los 200 kilos por centímetro cuadrado (kg/cm^2) y mover volúmenes de gas hasta de más de mil metros cúbicos por minuto (m^3/min), con velocidades incluso mayores a las 20.000 revoluciones por minuto (rpm). Asimismo, después de la transportación del gas natural, cuando este es la materia prima de alguna planta de transformación industrial, como un complejo de producción de etileno, también será necesaria otra compresión a fin de alimentarlo eficientemente a todos los procesos que se llevan a cabo en dicha planta.

La protección del compresor implica ciertas aplicaciones de las válvulas de control automático, consideradas en el ámbito de servicio severo, las cuales son verdaderas especialidades en el campo de la instrumentación y control automático de plantas industriales. Estas aplicaciones pueden ser:

- Válvula de control anti-surge
- Válvula de reciclado del compresor
- Válvula de desvío caliente (*hot by-pass*)
- Válvula de paro rápido
- Válvula de desvío frío (*cold by-pass*)
- Válvula de descarga de venteo

Descripción

Los compresores están diseñados para operar entre el cincuenta y el cien por ciento de su capacidad nominal. Cuando por alguna circunstancia el compresor no genera el flujo suficiente para mantener la presión en la línea y operar con flujos arriba del cincuenta por ciento de su capacidad, se está en riesgo de originar la reversa del flujo a través del compresor, debido al volumen acumulado en la tubería o en la planta; esta situación se conoce como "surge del compresor". Debido a que el flujo en reversa golpea violentamente a los impulsores que están girando a alta velocidad, puede causar serios daños al equipo. Si esta situación no se corrige de inmediato, el surge se puede repetir en lapsos de 0,5 a tres segundos.

Existen otros fenómenos de surge, como el golpe de ariete, que es un fenómeno en una tubería, causado al presentarse súbitamente una obstrucción en una línea de líquido, generalmente por un cierre imprevisto, ya sea parcial o total de una válvula. Esta obstrucción genera sobrepresión repentina en la línea básicamente por la naturaleza propia de un caudal incompresible. Los resultados del golpe de ariete pueden ser desastrosos para la tubería y los soportes, pudiendo resultar incluso en severas fallas mecánicas. Este indeseable efecto se

Figura 1. Estaciones de compresión para estaciones de gas natural: protección anti-surge, medición y regulación de caudal

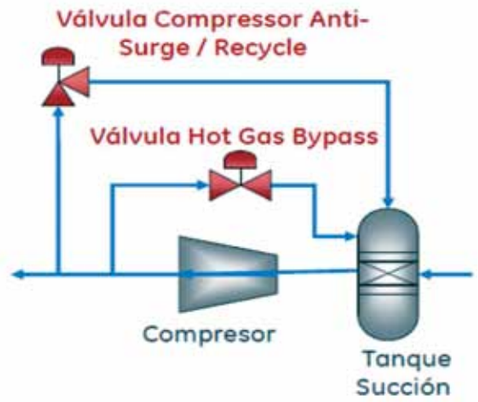


Figura 2. Esquema válvula retorno anti-surge y válvula desvío para variaciones de carga

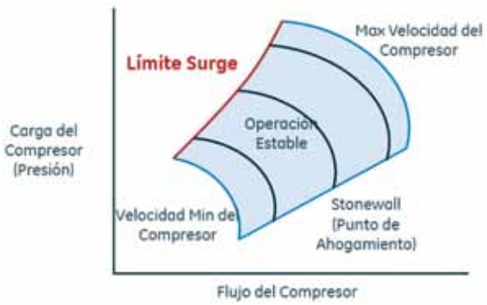


Figura 3

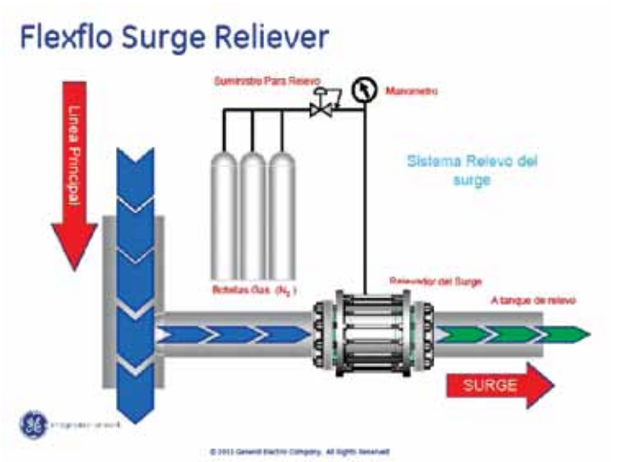


Figura 4. Operación del compresor

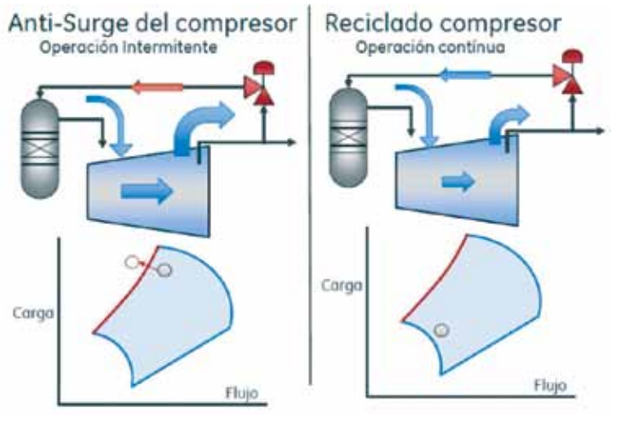


Figura 5. Diagrama simple de modos de operación intermitente y continua del compresor

debe prevenir mediante el uso de un dispositivo actuado por piloto que tiene la virtud de abrir en forma casi instantánea al detectar cierta sobrepresión en la línea, desviando el flujo hacia un tanque de alivio del surge.

Protección de los compresores

La función de la válvula anti-surge es proteger al compresor de las condiciones dañinas del surge, así como también proporcionar una vía de recirculación durante la puesta en servicio de la planta o de las estaciones de compresión, así como durante periodos de baja carga o demanda de gas. Los retos a que se enfrenta esta aplicación son:

- Manejo de grandes flujos, requiriendo válvulas de altos coeficientes de flujo (Cv)
- Ruido y vibración altos
- Velocidad de respuesta muy rápida, sistema exageradamente dinámico
- Control proporcional preciso y de alto desempeño
- Alta hermeticidad del sello en el asiento (clase alta de fuga)

Debido a que una situación de surge es intermitente, ya que ocurre ocasionalmente por fallas en el sistema de suministro del gas, en operación normal de la planta, la válvula anti-surge funciona como mera recirculación de excesos de flujo, así como para mantener al compresor trabajando por encima de su velocidad mínima.

Cálculo y selección de la válvula de control

De acuerdo a los volúmenes y presiones que se manejan en la transmisión del gas o que requiere la planta procesadora, se hace el dimensionamiento y selección de la válvula anti-surge. Por tanto, los

Gas and Vapor Flow Equations

volumetric flow

$$C_v = \frac{q}{N_7 F_p p_1 Y}\sqrt{\frac{G_g T_1 Z}{x}}$$

or

$$C_v = \frac{q}{N_9 F_p p_1 Y}\sqrt{\frac{M T_1 Z}{x}} \quad *$$

mass flow

$$C_v = \frac{w}{N_6 F_p Y \sqrt{x p_1 \gamma_1}} \quad *$$

or

$$C_v = \frac{w}{N_8 F_p p_1 Y}\sqrt{\frac{T_1 Z}{x M}} \quad *$$

Gas expansion factor

$$Y = 1 - \frac{x}{3 F_k x_T}$$

Pressure drop ratio

$$x = \frac{\Delta p}{p_1}$$

Ratio of specific heats factor

$$F_k = \frac{k}{1.40}$$

The IEC 534-2 equations are identical to the above ISA equations (marked with an *) except for the following symbols :

k (ISA) corresponds to γ (IEC)
γ_1 (ISA) corresponds to ρ_1 (IEC)

Nomenclature

C_v = valve flow coefficient
F_k = ratio of specific heats factor, dimensionless
F_P = piping geometry factor (reducer correction)
p_1 = upstream pressure
p_2 = downstream pressure
q = volumetric flow rate
N = numerical constant based on units (see table below)
G_g = gas specific gravity. Ratio of gas density at standard conditions
T_1 = absolute inlet temperature
M = gas molecular weight
x = pressure drop ratio, $\Delta p/p_1$ Limit $x = F_k x_T$
Z = gas compressibility factor
Y = gas expansion factor, $Y = 1 - \frac{x}{3 F_k x_T}$
x_T = pressure drop ratio factor
γ_1 = (Gamma) specific weight (mass density), upstream conditions
w = weight (mass) flow rate
k = gas specific heat ratio

Numerical Constants for Gas and Vapor Flow Equations

Constant		Units Used in Equations				
	N	w	q*	p, Δp	γ_1	T_1
N_6	2.73	kg/h	-	kPa	kg/m³	-
	27.3	kg/h	-	bar	kg/m³	-
	63.3	lb/h	-	psia	lb/ft³	-
N_7	4.17	-	m³/h	kPa	-	K
	417.0	-	m³/h	bar	-	K
	1360.0	-	scfh	psia	-	R
N_8	0.948	kg/h	-	kPa	-	K
	94.8	kg/h	-	bar	-	K
	19.3	lb/h	-	psia	-	R
N_9	22.5	-	m³/h	kPa	-	K
	2250.0	-	m³/h	bar	-	K
	7320.0	-	scfh	psia	-	R

*q is in cubic feet per hour measured at 14.73 psia and 60°F, or cubic meters per hour measured at 101.3 kPa and 15.6° C.

Table 3

Masoneilan DRESSER VALVE DIVISION

Figura 6. Página 13 del Manual de cálculo OZ1000 Masoneilan

datos mínimos necesarios para efectuar cálculo son los siguientes:

- Flujo o flujos para las distintas velocidades de operación del compresor (F)
- Presión de entrada a la válvula es la presión de descarga del compresor (P1)
- Presión de salida de la válvula es la presión en el punto de succión (P2)
- Temperatura (T)
- Peso molecular del gas (MW)
- Factor de compresibilidad (Z)
- Relación de calores específicos (Cp/Cv)
- Tamaño y cédula de las tuberías de entrada y salida

Mediante el programa de cálculo y selección de válvulas de control ValSpeQ, propiedad de *General Electric*, que se basa en la nomenclatura y ecuaciones de ANSI/ISA, estándar S75-01.01 y del IEC estándar 60534-2-1, se efectúan las corridas de cálculo necesarias para determinar las características necesarias de la válvula para manejar adecuadamente los flujos, caídas de presión, velocidades del fluido en la salida, estimación del ruido resultante, así como los materiales de construcción y forma de los internos, a fin de hacer una selección compatible y eficiente de acuerdo con todos los datos de proceso entregados por la compañía encargada de la ingeniería.

La capacidad de flujo, representada por el coeficiente de flujo Cv, en su definición básica es el número de galones por minuto que fluyen a través de una restricción con una caída de presión de una libra por pulgada cuadrada, a condiciones estándar, esto es, a 60 grados farenheit y a nivel del mar. Es un coeficiente adimensional que fue desarrollado por la compañía *Masoneilan* en 1944 y ha sido revisado y modificado para las distintas condiciones en las instalaciones industriales, llegando así actualmente a ser como se muestra en la copia de la página 13 del manual de cálculo OZ1000 de Masoneilan, reproducida en la figura 6. Cabe mencionar que las ecuaciones de cálculo para los diferentes estados de los fluidos también han sido revisadas y perfeccionadas continuamente. Asimismo, la teoría y ecuaciones para efectuar la predicción del ruido e encuentran en el manual de control de ruido, también de *Masoneilan OZ3000*.

Asimismo, el estándar IEC-534-8-3 es la base de las ecuaciones y nomenclatura para la predicción de ruido aerodinámico.

Consideraciones generales y recomendaciones para el diseño y selección de la válvula de control

Clase de fuga por los internos, definida por el estándar ANSI/FCI 70.2 normalmente se solicita como IV o VI.

Nivel estimado de ruido: normalmente se requiere que su valor no exceda 85 decibeles A para operación continua. Asimismo, es recomendable que el nivel de presión del sonido nunca exceda 105 decibeles A, dado el riesgo de daños mecánicos en los equipos que esto supondría. Se pueden utilizar internos, así como también dispositivos externos para atenuación de ruido, tales como cajas concéntricas multiperforadas, pilas de discos, cartuchos. ❖

Combinación de software de monitoreo y firewall industrial: el sistema inmune para las redes de producción

Hernán López
Phoenix Contact
hlopez@phoenixcontact.com
www.phoenixcontact.com

El nivel de seguridad de las redes de producción se puede incrementar rápida y sencillamente combinando software para monitoreo de la red y dispositivos de seguridad industrial. Esta combinación crea un nuevo estándar de seguridad en aplicaciones industriales e infraestructuras de redes críticas

La seguridad de acceso es un tema de creciente importancia en tiempos de Industria 4.0. Por eso, *Security Matters* y *Phoenix Contact* han reunido su experiencia en una sociedad tecnológica. El nivel de seguridad en las redes de producción puede mejorar de forma significativa y sencilla combinando software para monitorear la red con aplicaciones de seguridad industrial. La solución mancomunada configura nuevos estándares, tanto para la fabricación, como para infraestructuras críticas.

Hoy en día, más y más máquinas y sistemas intercambian información entre sí local y globalmente. La cantidad creciente de comunicaciones conduce a que se incrementen los requisitos de seguridad en la red. Los operadores deben, entonces, preguntarse a sí mismos qué información debe transmitirse, a qué máquina y cuándo. Sobre todo cuando se trata de sistemas de producción que se han expandido, o se han integrado completamente en la red tras cierta cantidad de años. La respuesta a esta pregunta resulta ser difícil y consume demasiado tiempo. *Security Matters* y *Phoenix Contact* han conformado una sociedad tecnológica para proveer a los usuarios un soporte eficiente, integrado y profesional.

Por una parte, *Security Matters* fue fundada en la ciudad alemana de Eindhoven en 2009, es una compañía innovadora, activa en el campo de seguridad TI y está especializada en la detección de anomalías en las redes industriales. *Silent Defense* es un componente esencial de su portafolio de productos. Esta plataforma para monitoreo de red está disponible en el mercado desde 2013.

Por otra parte, como una de las líderes e innovadoras en el mercado en ingeniería eléctrica, electrónica y automatización, *Phoenix Contact* opera, entre otras cosas, su propio centro de excelencia para ciberseguridad localizado en Berlín. Respaldada por su experiencia en la temática, la empresa provee productos a medida y soluciones de red que satisfacen requisitos industriales específicos. Los routers del rango de productos *FL mGuard* son el núcleo de la línea de producto de protección (ver figura 1).

Figura 1. Los dispositivos de protección FL mGuard se utilizan también en entornos de producción

Identificación simultánea de errores y diagnóstico de ataques

En 2016, *Security Matters* y *Phoenix Contact* decidieron combinar sus productos de protección, generando así un valor añadido para los usuarios. Para proveer una solución para monitorear la red, *Silent Defense* da soporte a los usuarios con análisis y fortalecimiento de su red. La capacidad de visualizar la red en tiempo real, llevar a cabo tests definidos por el usuario y monitorear de forma automática la comunicación de red son solo algunas de las funciones que distinguen este sistema de monitoreo. *Silent Defense* se puede usar para diagnosticar ciberataques y también para identificar errores operacionales (ver figura 2).

Los routers industriales *FL mGuard* de *Phoenix Contact* están diseñados para operar sin ventiladores y brindar protección y rendimiento confiables en una carcasa metálica compacta que se puede montar en riel DIN. Además de proveer un

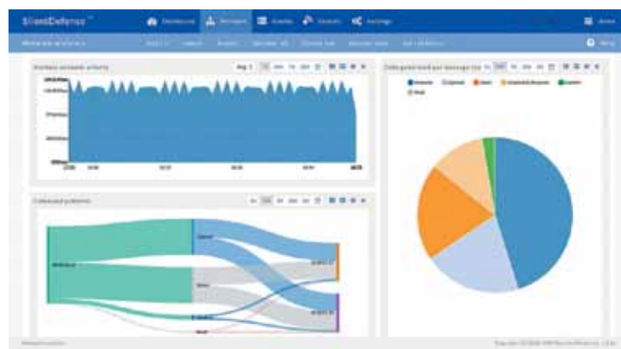


Figura 2. La visualización en tiempo real de la comunicación de red en el tablero de análisis de la red

túnelVPN seguro, los dispositivos son capaces de varias funciones firewall específicas de la industria. Esto incluye un firewall de usuario, un firewall condicional para activar reglas de firewalls específicas, así como inspección para la investigación a fondo de cualquier paquete de datos transmitido a través de OPC clásico o Modbus/TCP.

Esto habilita que el concepto de defensa-en-profundidad, basado en los estándares internacionales ISA 99 e IEC 62443, se pueda implementar profesionalmente en las aplicaciones. Gracias al concepto de seguridad descentralizada, las plantas productivas quedan protegidas de forma segura contra el sabotaje y los malos funcionamientos asociados en un proceso de producción (ver figura 3).

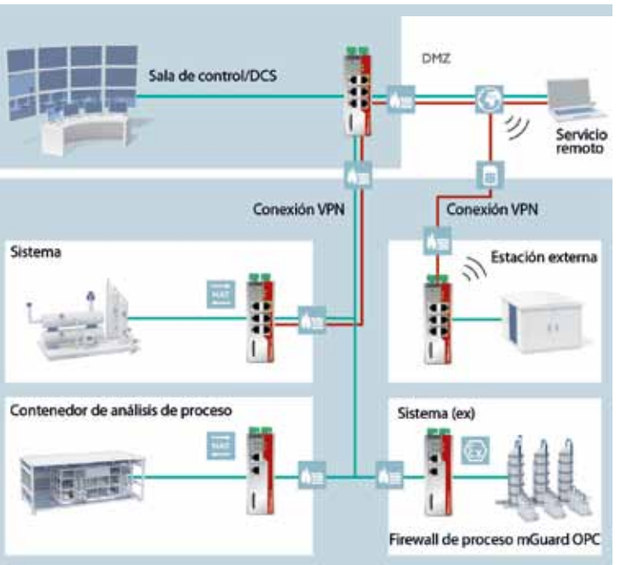


Figura 3. Las plantas de producción se pueden proteger con routers de seguridad de forma descentralizada

Detección inmediata de cambios menores en la red

Cuando se combinan en la práctica *Silent Defense* y *FL mGuard*, hay un beneficio adicional para los usuarios. Por ejemplo, *Security Consulting* de *Phoenix Contact* utiliza el software para monitorear la red a fin de analizar en detalle el intercambio de datos en redes industriales complejas. El operador del sistema tiene de esta forma un panorama exacto sobre qué participantes en la red de producción están enviando qué contenido a qué otros participantes, así como cuándo y cómo se envía. La comunicación no autorizada es visible y puede ser apagada. Un ciberataque espectacular no representa el mayor riesgo para muchas compañías, sino los innumerables pequeños cambios autoinducidos en el sistema que se van agregando a lo largo del tiempo e implican un riesgo mayor para la disponibilidad de la red de fabricación.

Los ejemplos abundan. Un controlador, por ejemplo, se intercambia por un dispositivo de reemplazo que está programado de alguna forma diferente al PLC original. Durante una actualización del sistema, el proveedor del producto utiliza un protocolo para tiempo de sincronización más débil que el que se usaba antes. Los nuevos dispositivos agregados intentan alcanzar un servidor externo utilizando puertos TCP desconocidos. Establecer la conexión con un servidor no disponible inunda la red de producción con datos. La lista de ejemplos es interminable.

Transmisión directa de datos de configuración registrados en el firewall

Después de que *Silent Defense* analiza las relaciones comunicacionales en la red de producción y se apagan las conexiones no deseadas, el segundo paso importante que sigue es proteger la red utilizando firewalls de la gama *Fl mGuard*. El aspecto innovador de esta solución es la interacción de hardware y software insitu para el usuario. Las relaciones comunicacionales que fueron identificadas como correctas se transmiten directamente como registros de datos de configuración de firewall en el dispositivo de protección instalado en un sistema descentralizado. Esto hace que definir las reglas de firewall sea mucho más fácil y evita reglas de firewall descuidadamente mantenidas o defectuosas. Los empleados responsables en particular prefieren dejar que los paquetes de datos no identificados o desconocidos pasen por el firewall en las redes de producción que son complejas y han crecido a lo largo de los años, antes que correr el riesgo de que el sistema quizá no fabrique más. Esta práctica, sin embargo, implica un riesgo de protección grande e innecesario. Con la solución descripta en esta nota, los requisitos de usuario se implementan ahora de forma profesional, garantizando una elevada disponibilidad del sistema y a la vez, alta protección de la red de producción contra acceso no autorizado y acciones dañinas.

Ajuste dinámico de mediciones de seguridad

Los proyectos piloto iniciales están dando el próximo paso innovador. Si *Silent Defense* se instala de forma permanente en el lugar del usuario, este tiene la opción de ajustar de forma dinámica las medidas de protección. Si, por ejemplo, los hackers están utilizando un link de comunicación ya existente para un ataque, el firewall *FL mGuard* puede cambiar la configuración esencialmente en tiempo real siguiendo la aprobación de un empleado responsable o *Silent Defense* puede ser usado para hacer esto automáticamente. De esta manera, las conexiones no deseadas se pueden detener rápida y fácilmente, a la vez que una transmisión de datos deseada va a permitirse específicamente después.

La sociedad tecnológica entre *Security Matters* y *Phoenix Contact*, por lo tanto, ha conducido a un salto innovador en la protección industrial y está configurando nuevos estándares en el área de calidad. El software *Silent Defense* y el router

Familia de productos de Ethernet industrial, de *Phoenix Contact*

FL mGuard forman una simbiosis y crean un claro beneficio para el usuario. Por lo tanto, es irrelevante si se utiliza en una aplicación de infraestructura crítica o en una aplicación en uno de los muchos sectores industriales.

Funciones para equipos de seguridad

El nuevo firmware 8.4 para dispositivos de protección en la gama de productos de *FL mGuard* expande el rango de utilidades de estos dispositivos, entre otras cosas, con el Inspector Modbus TCP y el firewall basado en nombres DNS. El Inspector Modbus TCP, una inspección de paquete profunda para Modbus/TCP, se puede usar para proveer protección detallada para conexiones que usan el estándar industrial ampliamente adoptado. Los derechos de acceso se pueden configurar tanto a nivel de puertos y direcciones IP como para códigos de función y registros utilizados dentro del protocolo Modbus. Por ejemplo, el usuario puede definir qué participantes Modbus están habilitados para solo leer valores y cuáles para sobreescribirlos. Más aún, los derechos de acceso se pueden definir de forma precisa de acuerdo con el registro.

El firewall basado en nombres DNS permite crear derechos de acceso a firewall que incluso estén basados en direcciones IP y nombres DNS. Esto hace que las creaciones de configuraciones sean más sencillas en escenarios en donde las direcciones IP frecuentemente cambian. La nueva versión de firmware 8.4 está lista para descargar en el área de descarga de su respectiva página de producto. ❖

Monitoreo y control remoto vía SMS y GPS

Nuevo módulo de comunicación para *Logo! V8*

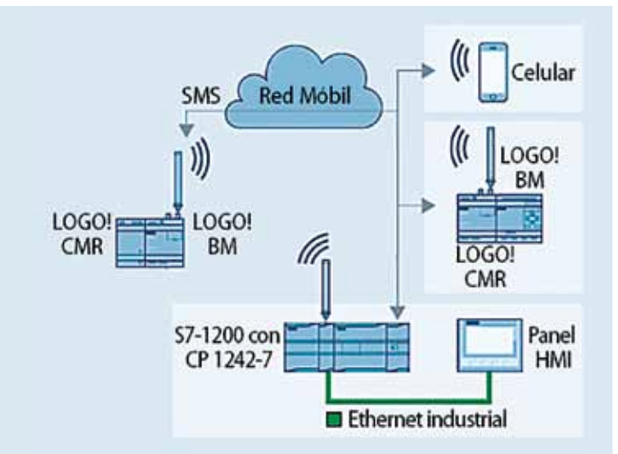
Siemens, *www.siemens.com*

A *Logo! V8* puede adicionarse un nuevo módulo de comunicación, el *CMR2020*, con el que se puede controlar o enviar información de estado y avisos vía mensajería de texto a teléfonos celulares. Una vez que la tarjeta SIM ha sido insertada, el módulo se convierte en un nodo más de la red de telefonía móvil. De esta forma, los usuarios pueden configurar diferentes comandos para acceso remoto, así como el disparo de mensajes de texto, lo cual permite trasmitir información de diagnóstico y avisos a números de teléfono previamente definidos.

A través del mismo módulo, también se puede utilizar una antena GPS que ayuda, por ejemplo, a rastrear la posición actual de un contenedor controlado por *Logo!* alrededor del mundo o monitorear el envío en camiones. También permite la sincronización de hora y fecha basada en la información del servidor NTP de la red móvil o de la señal GPS. Esto evita realizar mantenimientos adicionales para el ajuste del reloj.

Estos equipos se pueden implementar, por ejemplo, en la construcción de sistemas de control para domótica, para las seguridades y alarmas de una casa, puertas de garaje, y otros, de manera que ante una irregularidad se puede enviar un mensaje de texto; para control de iluminación de empresas, comercios e instalaciones industriales o sistemas de riego de parques, estadios u ornamentos. Los *Logo!* son adecuados para las tareas de control efectivas en la industria, tales como el control de la bomba o un control de nivel.

La conexión del módulo se puede efectuar de forma rápida y sencilla a través de la interfaz Ethernet. Así como comandos de programación, el usuario puede guardar una lista de números de teléfono autorizados para controlar y recibir valores de procesos, datos de diagnóstico y avisos. Los mensajes de texto están protegidos por contraseña. Utilizando las dos entradas y las dos salidas, el módulo de comunicación se puede implementar en tareas de control simples de forma independiente sin un módulo básico de *Logo!* ❖



Esquema de funcionamiento para aplicaciones de telecontrol. Con el módulo *CMR2020* se puede enviar y recibir mensajes SMS con otros Logo! como también con otros dispositivos en comunicación nativa Simatic, por ejemplo con el *S71200*. Todos pueden integrarse transparentemente con redes y dispositivos de telefonía celular. Asociado a dispositivos móviles, el módulo *CMR2020* es capaz de transmitir su posición geográfica gracias a las funciones de comunicación GPS, de este modo provee innovadoras soluciones para sistemas de seguimiento satelital y automatización.

Nota del editor: La nota de producto aquí publicada puede leerse, o bien de forma independiente, o bien como la segunda parte de la nota titulada "Entendiendo un poco más telecontrol y teleservicio", de Andrés Gorenberg, publicada en *AADECA Revista 3* (Nov-Dic, 2016, págs. 38-41) y disponible en *www.editores.com.ar*

¡Nuestros profesionales por fin tendrán su día!

Diego Maceri, Presidente de AADECA, *www.aadeca.org*

Muchas profesiones celebran su día: Día del Médico, Día del Biólogo, Día del Químico y Día del Ingeniero, por mencionar sólo algunos. Nuestra especialidad conjuga una amplia diversidad de disciplinas tales como procesos, electrónica, electricidad, neumática, hidráulica, mecánica, termodinámica, informática. También involucra a una gran cantidad de profesionales tanto ingenieros como técnicos,académicos y científicos, así como muchos otros profesionales idóneos en la materia, que juntos integramos este rubro de suma trascendencia para el desarrollo tecnológico e industrial.

Es por eso que aprovechando la celebración del "Día del Instrumentista" que se lleva a cabo los 25 de Noviembre - celebración basada en una tradición de instrumentistas de varios polos industriales de nuestro país – el Consejo Directivo de AADECA ha comenzado a trabajar desde hace un tiempo para formalizar dicho día como el "Día del Profesional de Instrumentación, Automatización y Control".

Por tal motivo, esta propuesta se estará presentando en el Honorable Congreso de la Nación para institucionalizarlo a nivel nacional.

Uno de los objetivos principales de la Asociación es la difusión y jerarquización de nuestro rubro, con lo cual cada acción que realizamos está orientada en ese sentido. Entendemos que cada rubro o sector tiene su día especial y es tarea de la Asociación llegar a los fueros más altos para que el trabajo de nuestros profesionales sea aún más reconocido.

Desde hace casi 50 años tenemos nuestra Asociación Profesional, nuestro Congreso Académico, nuestras Jornadas y Foros, una Sede para juntarnos, y desde hace más de un año también nuestra propia Revista. Sólo nos falta el reconocimiento de nuestro día. Y como nos gustan los desafíos, ya iniciamos el camino para lograrlo.

Esperamos que en este 2018, año en que se celebra nuestro Congreso y Foro bianual, ya estemos en condiciones de anunciar formalmente:

25 de noviembre

"Día del Profesional de la Instrumentación, Automatización y Control"

Sistemas de control de Yokogawa en el futuro

Naoki Ura y Koichi Oya
Yokogawa, *www.yokogawa.com.ar*

Introducción

Han pasado más de cuarenta años desde que *Yokogawa* lanzara el primer sistema de control distribuido (DCS) en 1975. Ahora, muchos clientes reflexionan acerca del rol de los sistemas de control como productores de bienes, diferente de los bienes generales de los consumidores y los bienes de lujo. Específicamente, los clientes quieren continuar operando sus plantas de forma segura y proteger la productividad, y a la vez responder a los cambios en el mercado, y tratan de identificar cómo los sistemas de control y sus vendedores pueden ayudarlos a satisfacer tales requisitos, y qué cosas deben pagar para eso.

Como vendedora de sistemas de control, *Yokogawa* tiene una responsabilidad para responder tales preguntas de los clientes. Bajo estas circunstancias, las expectativas de los clientes sobre la empresa cambian. El rol de *Yokogawa* pasará de ser un vendedor que solamente ofrece hardware y software para un sistema de control, a un socio del cliente que le soluciona sus problemas en toda la planta. Este artículo presenta cómo evolucionan los productos para sistemas de control de *Yokogawa* como una plataforma para responder a las expectativas de los clientes.

Cambios en el ambiente de negocios que rodea a los clientes

En la industria energética, han crecido los sectores relacionados a varias nuevas fuentes de energía. Sin embargo, se espera que las industrias de gas y petróleo y petroquímica continúen jugando un rol importante durante los próximos veinte a treinta años dado que aún es muy alta la demanda de productos en estas industrias para construir infraestructura, especialmente en países emergentes. En estas industrias, la competición de productos en el mercado es cada vez más severa dada la aparición de los países que incluyen el BRIC, y también por otras razones. Por lo tanto, se requiere una producción altamente eficiente, óptima y diseñada a medida. Bajo estas circunstancias, está cambiando enormemente el ambiente de negocios que rodea a los clientes. Se describen a continuación esos cambios, sus impactos y las respuestas que requieren.

Cambios en las materias primas y en los bienes que se producen

Como resultado de la innovación tecnológica y las regulaciones en lo que a materias primas respecta, así como su procuración globalizada, en cada caso difieren las calidades, composiciones, precios y formas de provisión. Además, según los requisitos de usuario, se necesita producir varios productos en cantidades pequeñas. Deben introducirse equipamiento de producción y sistemas de instrumentación que puedan responder de forma flexible a los cambios en materias primas, y también se espera que crezcan la renovación de las plantas existentes y la introducción de nuevo equipamiento.

Cambios en la carga de producción

Dependiendo de los cambios en la demanda de los productos, quizá cambie enormemente la carga de producción de las plantas, y entonces debe mejorar la eficiencia en la producción. Como resultado, los operarios están forzados a operar la planta de forma más precisa que nunca, a la vez monitoreando un amplio rango de comportamientos de la planta. Sumado a la eficiencia en la producción, también es importante fortalecer la seguridad, identificar los problemas por adelantado, y realizar mejoras en base a un análisis de las causas de los problemas inmediatamente después de que estos hayan ocurrido.

Cambios en la actitud de los clientes para invertir en nuevas utilidades de producción

El retorno en la inversión en utilidades de producción es una cuestión estrictamente considerada en las plantas de los clientes. Por ejemplo, los clientes desean con ansias expandir sus oportunidades de producción maximizando el uso de sus equipamientos y minimizando las paradas de producción. Los clientes tienen ganas de que se reduzcan las detenciones imprevistas en la producción, aunque sea imposible hacerlo, y continuar a la vez con la producción dentro de límites seguros.

Cambios en las tareas de las personas a cargo de la producción

Por gestionar muchas plantas distribuidas de una forma integrada, muchos clientes responden de forma flexible a los cambios en la materias primas y demandas de producción. Sin embargo, en la práctica, es difícil asignar expertos a todas las plantas, pues su número es limitado. Mientras tanto, las operaciones de planta se automatizan de forma gradual, aunque no completamente.

Así, las tareas necesarias, especialmente las de los operadores de planta en cada una ellas, se reducen a tareas más complicadas y críticas que rara vez se ejecutan. Entre las tareas, que convencionalmente llevaban a cabo operadores en general, las más simples y repetitivas se automatizan, mientras que la no-rutinarias se dejan en manos de los operadores. Más todavía, operarios en general cada vez más deben tratar con tareas complicadas que antes correspondían a los expertos.

Por estas razones, es necesario minimizar la carga sobre los operadores, darles un guía sobre las respuestas correctas en tiempo real, y proveerles entrenamiento práctico de modo que puedan ejecutar sus tareas con seguridad. También es importante ofrecer entrenamiento sobre la marcha a un costo razonable y en tiempos cómodos. Además, se necesita un sistema que permita a los expertos asistir a los operadores desde lugares remotos.

Expectativas por la integración de operación y mantenimiento (O&M)

Desde los últimos años, los clientes demandan fuertemente una operación de planta que maximice los beneficios generados por las instalaciones optimizando su plan de mantenimiento en todas las actividades de producción. Para maximizar las capacidades de las instalaciones, los operadores necesitan identificar las perturbaciones de la planta, cambios en la demanda de producción, y otros factores. Además, necesitan entender las condiciones de cada equipamiento y dispositivo de la

planta, y tener los conocimientos y habilidades necesarias para usarlos de forma efectiva. A la vez, el personal de mantenimiento necesita entender las condiciones de operación de cada equipamiento y dispositivo de la planta, y mantenerlos, considerando su influencia en las actividades productivas. Por lo tanto, la información sobre integración de operación y mantenimiento (O&M) y su gestión es cada vez más importante. Durante la operación de la planta, es importante hacer un uso total de esa información, y tomar en consideración el impacto de las operaciones de operación y mantenimiento en la eficiencia de la producción durante toda la vida útil.

Requisitos del sistema de control del futuro

Para responder a los cambios en el entorno de negocios de los clientes y satisfacer sus expectativas, los sistemas de control necesitan mejorar desde cuatro puntos de vista fundamentales: esquemas para automatizar la operación de planta, esquemas que permitan a los operadores monitorear las operaciones de la planta y realizar acciones acordes, ingeniería para configurar el sistema entero para la planta de un cliente; y servicios de mantenimiento para asegurar operaciones estables y a largo plazo. Los requerimientos para cada uno de estos puntos se describen a continuación.

Control inteligente (requisitos de los esquemas para automatizar la operación de la planta)

Para mejorar la eficiencia energética de las plantas, es necesario operar cada proceso manteniendo los valores estables dentro de los límites y a la vez maximizando la eficiencia. El control avanzado de procesos (APC) es una tecnología conocida para este propósito. Para introducir APC en las plantas de los clientes, deben acortarse los tiempos de instalación y deben reducirse los costos. Además, es importante identificar con precisión las condiciones de los procesos de los clientes.

Por otro lado, cada unidad de proceso en una planta a menudo se opera a través de varios controladores autónomos y distribuidos que trabajan de forma cooperativa por cuestiones de confiabilidad y mantenimiento. En tanto que el proceso se complejiza, las relaciones entre estos controladores tienden a ser más fuertes. Además de los cambios en las materias primas o en la demanda de la producción, una planta está siempre afectada por los cambios en las condiciones exteriores tales como el clima, la temperatura y los procedimientos operativos, tanto como condiciones cambiantes debido al envejecimiento de las instalaciones, y demás. Entonces, el equilibrio óptimo entre los controladores y las unidades de proceso es fluctuante

Como consecuencia, se necesita una función que supervise y controle todas las unidades de proceso de manera integrada y a la vez maneje varios controladores en cada unidad de proceso. Esta función se llama control supervisor, que lleva a cabo control de tareas, control avanzado y control óptimo entre muchos controladores.

La parte izquierda de la figura 1 muestra el control supervisor en la gestión de producción y jerarquía de control. Se utilizan muchos controladores en cada proceso para controlarlos. El control supervisor en la capa por encima de la de los controladores, controla los procesos utilizando varios controladores.

Las funciones de control avanzado, incluyendo APC, en general operan para cada unidad de proceso, y no necesitan considerar el equilibrio de control entre los controladores. Las funciones de control supervisor tales como APC pueden mantener equilibrios de control como respuesta a numerosas fluctuaciones externas.

Más todavía, se requiere control de alta precisión utilizando tecnología de campo digital y de simulación. *Yokogawa* ofrece tales funciones de control, que operan de forma efectiva sobre una plataforma muy confiable que la empresa ha desarrollado durante cuarenta años. La relación entre control supervisor, control avanzado, control óptimo y tecnología de simulación se muestra en la parte derecha de la figura 1.

Operación inteligente (requisitos para esquemas con las que los operarios monitorean la operación de planta y actúan en consecuencia)

Debido a los cambios en el mercado y la integración O&M, el trabajo de los operarios en general se está complejizando. Muchos clientes reconocen claramente que uno de los factores importantes para prevenir los accidentes de planta, de los cuales hay numerosos casos hoy en día, es la interfaz humano-máquina (HMI). Los estándares internacionales ISA 101 (ANSI/ISA-101.01-2015, Interfaces humano-máquina para sistemas de automatización de procesos, ISA, 2015) e ISA 106 (ISA-TR 106.00.01-2013, Automatización de procedimientos para operaciones de proceso continuo – Modelos y terminología, ISA, 2013) discuten cómo debería ser HMI.

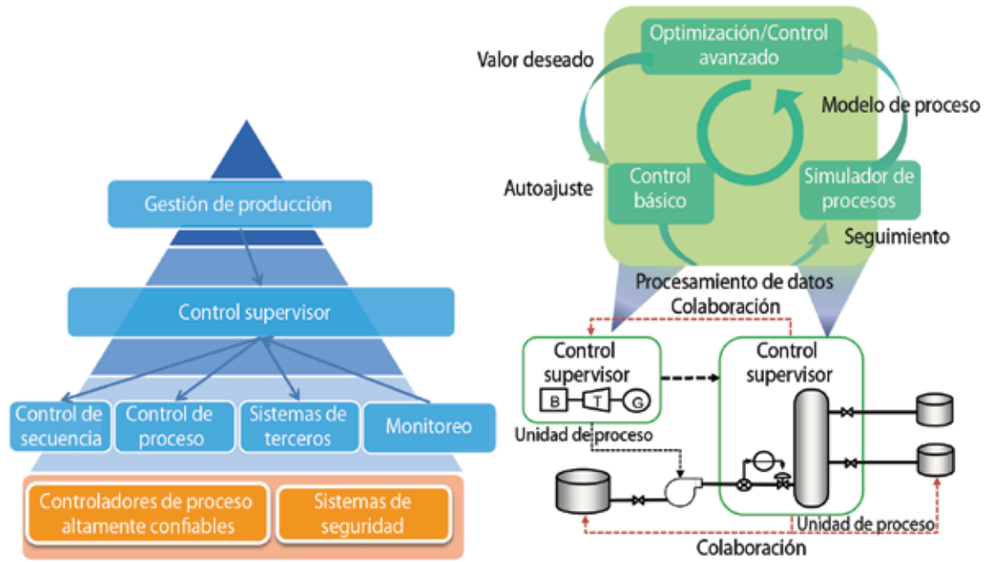


Figura 1. Control supervisor

La HMI es un medio importante que permite a las personas a cargo de monitorear la planta operarla y actuar en consecuencia, y entonces, se necesita ampliar el papel de la típica consola de HMI dedicada a los controladores de cada vendedor. Para lograr esto, además de la información convencional que incluye los datos de producción y de mantenimiento, es posible utilizar datos obtenidos por el control inteligente y las tecnologías digitales de campo y de simulación. Por utilizar esta rica cantidad de datos, la HMI se puede expandir como una herramienta que permite a las personas entender las condiciones de una planta con un solo vistazo, identificar las mediciones, y tomar acciones de forma protegida. La figura 2 muestra el funcionamiento y los contenidos que ayudan a las personas a tomar decisiones puntuales basadas en la información dada.

Yokogawa ofrecerá sistemas basados en ISA 101 que facilitan el diseño de la HMI e igualan los datos de diferentes fuentes y los convierten en información fácil de entender. Además, configurará

Figura 2. Funcionamiento para asistir a las personas en su trabajo

sistemas que permitan a los operarios compartir información protegida acerca de la situación actual con expertos en un lugar remoto, y editar automáticamente las mediciones provistas por los expertos como un procedimiento de operación estándar (SOP) electrónico que queda disponible para otros operarios en general. Además, combinando tecnología digital de campo, simulación y sus sistemas de control, brindará un entorno de entrenamiento que simula la operación de planta.

Ingeniería inteligente (requisitos de ingeniería para configurar un sistema entero para la planta de un cliente)

Dado que las plantas son cada vez más complicadas, rara vez se controlan solo con DCS de un solo vendedor, sino que en general combinan varios sistemas de diferentes vendedores. En los últimos años, DCS y sistemas de instrumentación seguros muy a menudo se combinan como un sistema llamado sistema integrado de control y seguridad (ICSS). La implementación y configuraciones de estos sistemas varían muy seguido durante el trabajo de ingeniería dependiendo del progreso del proyecto y los cambios en los requisitos del cliente. Además, el trabajo de ingeniería se divide en trabajo para cada unidad de proceso y cada sistema de control. En el sistema de control, se divide más entre trabajo de campo, y trabajo para implementar aplicaciones del sistema de control y para diseñar procesos. Como se muestra en la figura 3, los tiempos para la ingeniería de un sistema de control se pueden acortar llevando a cabo varias tareas en paralelo.

Considerando lo dicho, *Yokogawa* provee un entorno de ingeniería integrado en el que los resultados de varios sistemas y lugares se integran sin contradicciones, se gestionan sus modificaciones, y no solo se administra el historial de modificaciones sino que también se mantiene la consistencia entre las modificaciones del sistema. En particular,

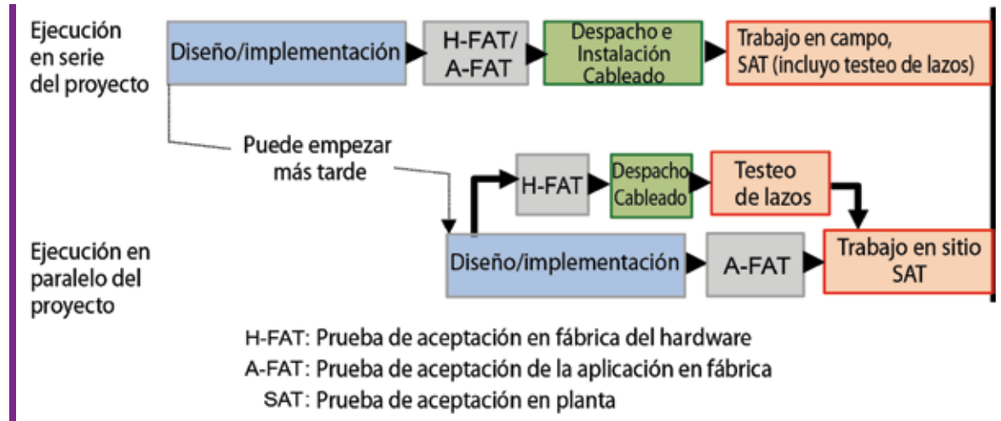


Figura 3. Ejecución en paralelo del trabajo de campo y diseño e implementación de aplicaciones del sistema de control

Yokogawa provee un sistema que permite la ejecución en paralelo del trabajo de ingeniería e instalación en el campo para el hardware implicado en entradas salidas (E/S), que debe manejarse junto con los dispositivos de campo, y el trabajo de diseño e implementación de aplicaciones de un sistema de control cuya ejecución requiere del consentimiento del cliente. Para lograr esto, las funciones de las herramientas de ingeniería para diseñar e implementar las aplicaciones deben mejorar drásticamente de modo tal que la información relacionada a esas tareas se pueda utilizar apropiadamente en cualquier momento.

Planta sostenible (requisitos de los servicios de mantenimiento para asegurar la operación a largo plazo)

Después de que sus plantas comienzan a operar, los clientes dan importancia a en tener continuidad de una producción estable y a largo plazo y a la vez mantener y mejorar la eficiencia. Por este motivo, *Yokogawa* ha preparado acuerdos de mantenimiento anuales, uno de los cuales provee el servicio de mantenimiento durante veinticinco años. Bajo este acuerdo, *Yokogawa* trabaja junto con los clientes para diseñar un plan de mantenimiento y llevarlo adelante, en donde se define el plan de reemplazos según se necesiten para los componentes del hardware que se deterioren y los de software que sean difíciles de mantener durante los siguientes veinticinco años; y a la vez minimiza la influencia sobre la operación de la planta. Así como para los componentes provistos por la empresa, tales como productos del sistema de control o dispositivos de campo, *Yokogawa* ofrece planes de mantenimiento a largo plazo.

Para dispositivos HMI, la política de diseño de *Yokogawa* es que estos sean capaces de operar y monitorear sobre controladores de un DCS por lo menos de una generación anterior, como solía ser. Gracias a esta política, los dispositivos HMI con un tiempo de vida relativamente corto se pueden reemplazar por nuevos sin suspender la operación de los controladores que actúan directamente sobre el proceso. Como resultado, esto permite que los sistemas de control se actualicen de acuerdo a la agenda de mantenimiento u operación del cliente. Nótese que *Yokogawa* permite un intercambio parcial del hardware por acoplamiento no directo de sus componentes, e incrementa la coexistencia y conectividad de múltiples piezas de software utilizando tecnología de virtualización.

Asimismo, así como para las computadoras y

sus sistemas operativos, sus tiempos de vida son relativamente cortos en comparación con otros componentes utilizados en los sistemas de control. *Yokogawa* ha forjado alianzas con vendedores de computadoras y también ha asegurado un soporte de mantenimiento más duradero que el que existe para las PC en el mercado, lo que le permite ofrecer plataformas que ya no sean afectadas por las políticas de soporte de *Microsoft Corporation* o del proveedor del sistema operativo. Dado que se incrementarán en el futuro los componentes de hardware y software del sistema de control que no sean de *Yokogawa*, son necesarias algunas medidas para que los clientes puedan usar el sistema de forma segura durante largo tiempo. *Yokogawa* expandirá sus configuraciones para una provisión más estable y soporte de mantenimiento de componentes que no sean de su marca.

Las condiciones actuales de aplicaciones, software y hardware sean o no de *Yokogawa*, y su historial de mantenimiento y modificaciones son información importante para el mantenimiento de todo el sistema durante un largo periodo. Sin embargo, muchos clientes no gestionan esta información de forma apropiada; quizá se disperse, pierda o no se mantenga actualizada. Utilizando las funciones de la ingeniería inteligente descriptas más arriba, *Yokogawa* ofrece un marco como se muestra en la figura 4, que fácilmente puede mantener esa información actualizada y asegurar el mantenimiento de los componentes en las plantas de los clientes, y a la vez referir a la información de mantenimiento de productos en *Yokogawa*.

Tecnologías clave para satisfacer los requisitos

El apartado anterior describía los requisitos para el sistema de control desde cuatro puntos de vista. Para satisfacer estos requisitos, se necesitan dos tecnologías clave, tecnologías de simulación de procesos y tecnologías digitales de campo, junto a una plataforma muy confiable y de alto rendimiento para sistemas de control.

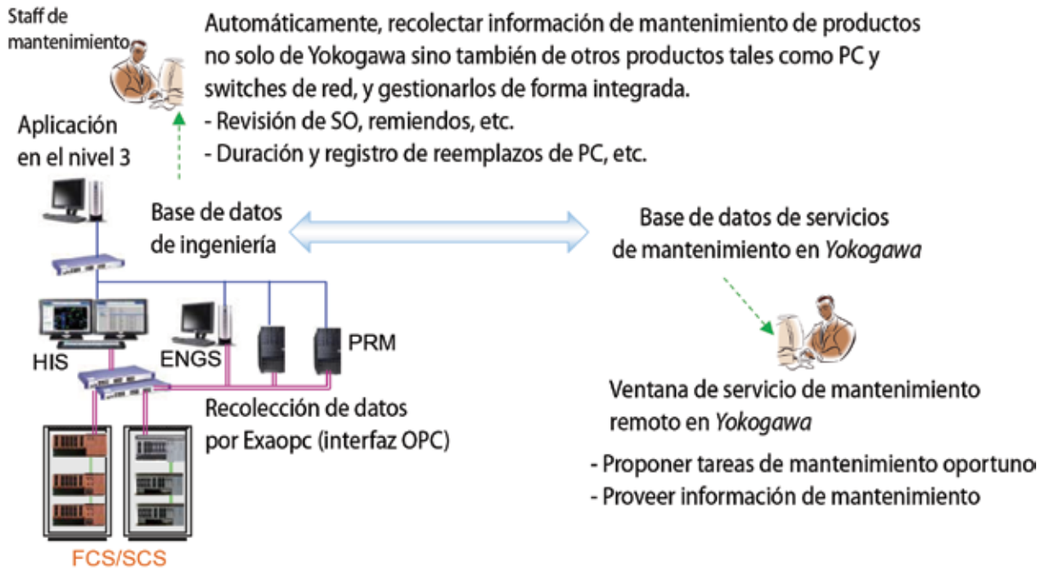


Figura 4. Gestión de la información de mantenimiento de los componentes del sistema

Tecnología digital de campo

La tecnología digital de campo ofrece varios valores añadidos a los clientes por permitir intercambio de datos en tiempo real entre el sistema de control y los dispositivos de campo con una inteligencia autónoma distribuida en toda la planta.

Gracias a la evolución de microprocesadores integrados en los dispositivos de campo, un sistema de control puede obtener datos precisos de un solo equipo. Mucho más, el intercambio de datos digitalizados entre un sistema de control y los dispositivos de campo permite que la comunicación sea inalámbrica. Esto hace posible colocar los equipos de campo en lugares en los que antes no se podía por cuestiones de cableado, y visualizar datos de proceso que de otra forma sería imposible. Dado que crece la cantidad de datos que se recolectan, es posible detectar cambios menores en la planta, identificar relaciones causales, y predecir los comportamientos futuros de la planta con mayor precisión. Además, los dispositivos que transmiten datos pueden mejorar su confiabilidad con una función de autodiagnóstico. Como respuesta, esto permite el control, mantenimiento y otras actividades basadas solo en datos confiables, contribuyendo así enormemente a reducir los costos y mejorar la seguridad, eficiencia y disponibilidad de la planta.

La tecnología digital de campo ayuda a reducir no solo los costos operacionales (OPEX) sino también los de capital (CAPEX) a la hora de construir un sistema de control. Con esta tecnología, la información contenida en equipos de campo remotos, tales como identificadores y configuraciones se puede obtener por comunicación y utilizarse para ingeniería y mantenimiento del sistema de control. Los cambios en la configuración de la planta, incluso el reemplazo de un equipo sin que se vean afectados los documentos de diseño, se pueden gestionar fácilmente con funciones de gestión centralizadas, permitiendo que el mantenimiento se realice rápidamente.

Más todavía, la tecnología digital de campo facilita el chequeo de validación de varios lazos al mismo tiempo. Esto incluye que los dispositivos en puntos finales se conecten al sistema de control de forma apropiada, que entreguen información de acuerdo a la instrucción del sistema, y que todo esté configurado apropiadamente en los equipos. Esto permite que las validaciones confiables de lazos se realicen más rápidamente en comparación con el método tradicional, y que la cantidad de trabajo requerida para arrancar una planta se pueda reducir. Convencionalmente, dos ingenieros, uno en el lugar del sistema de control y otro en campo, conducen las revisación del lazo uno por uno mientras intercambian información utilizando transceptores.

Tecnología de simulación de procesos

Al combinar tecnología de simulación con tecnología digital de campo y la ingeniería de los sistemas de control, el sistema de control de *Yokogawa* presenta varias ventajas para los clientes. Esto incluye reducción de los costos por crear modelos de proceso, mejorar la precisión de la predicción de comportamientos, y el seguimiento de las condiciones de operación a las situaciones reales actuales

Para los sistemas de control de *Yokogawa,* los modelos de proceso se desarrollan como sigue. Primero, en una etapa temprana de diseño e implementación, se aplican en cada modelo de proceso funciones de simulación fundamentales basadas en los modelos de proceso estandarizados. Luego, en tanto que progresa la ingeniería, el ajuste del modelo se repite y los modelos se mejoran. Como resultado, para el momento en que inicia la operación de planta, los modelos de proceso están listos para usar y solo se necesita un breve trabajo de identificación, que reduce enormemente el tiempo y los costos de construcción de modelos. Para lograr esto, es indispensable estrechar las funciones

de ingeniería del sistema de control y las funciones de simulación.

Antes de comenzar con la operación de planta, la simulación de procesos que utiliza modelos de proceso se puede utilizar para otros propósitos que el entrenamiento. Al simular el comportamiento de la planta del cliente sobre la base de sus requisitos desde el momento del diseño, *Yokogawa* y su cliente pueden compartir los comportamientos esperados después de iniciada la operación de la planta. Además, incluso antes de que la configuración de E/S del hardware se determine, la simulación de procesos se puede utilizar para depurar e inspeccionar las aplicaciones para compensar su inspección sobre el equipamiento real, mejorar su calidad y acortar el tiempo requerido para inspección luego del arranque de la planta.

Más todavía, luego de que se pone en marcha la planta, la simulación del proceso puede visualizar las condiciones internas en el equipamiento de producción y procesos que son difíciles de medir con sensores, y puede predecir el futuro con una simulación acelerada. Como resultado, esto puede provocar que el control lógico o los operarios tomen acciones preventivas antes de que los procesos actúen de forma anormal o antes de que las condiciones sean ineficientes.

Luego del arranque, es necesario cambiar los modelos de proceso en tiempo real para que respondan de forma más flexible a los cambios en las materias primas o demanda de la producción. Por ejemplo, los valores de proceso en una planta real se pueden incorporar dentro de un modelo para ajustar los parámetros y condiciones de operación en el modelo en tiempo real. Además, los resultados de simulación de respuestas a salto se pueden utilizar para las funciones de transferencia para control avanzado, o sintonía del PID para procesos simulados.

En todos los casos, la precisión de la simulación y la dependencia de los datos utilizados para la simulación deben estar asegurados. Utilizando activamente dispositivos de campo con tecnología digital, se pueden identificar y eliminar los datos inciertos provistos por dispositivos en falla y que pueden afectar adversamente la simulación, pueden ser detectados y eliminados. Además, los equipos de campo están evolucionando en lo que a cantidad de puntos medibles se refiere, tanto como la velocidad de medición, de modo que se incrementa la cantidad total de puntos medibles. Como resultado, el número de valores medidos disponibles excluyendo los de baja dependencia es suficiente para ajustar los modelos altamente precisos.

Conclusión

Yokogawa siempre dio prioridad al cliente y desarrolla productos en consideración de los valores que los clientes buscan. *Yokogawa* reconoce que los clientes compran sistemas de control que no son de su marca. Los clientes pagan dinero a *Yokogawa* no solo por el hardware, software y aplicaciones de sistemas de control sino también para sus servicios de mantenimiento, planes de actualización y trabajo real, y por las habilidades del staff de *Yokogawa*. La empresa continuará desarrollando y proveyendo las funciones necesarias para brindar un valor mayor al precio pagado. ❖

Nota del editor: la nota aquí reproducida fue originalmente escrita para la revista Y***okogawa Technical Report*** edición en inglés, N°.2 (2015), y traducida especialmente para ***AADECA Revista***.

AADECA

Glosario de siglas de la presente edición

AAFMHA: Asociación Argentina de Fabricantes de Máquina-Herramienta, Accesorios y Afines

ADACSI: Asociación de Auditoría y Control de Sistemas de Información

ADIMRA: Asociación de Industriales Metalúrgicos de la República Argentina

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

APC *(Advanced Process Control)*: control avanzado de procesos

APT *(Advanced Persistent Thread)*: amenaza avanzada persistente

BI *(Business Intelligent)*: negocios inteligentes

BRIC: Brasil, Rusia, India y China

BSI *(Bundesamt für Sicherheit in der Informationstechnik)*: Oficina Federal de Seguridad Informática, de Alemania

CAPEX *(Capital Expanditure)*: costos de capital

CAPP *(Collaborative Automation Partner Program)*: Programa de Colaboradores de Automatización

CCI: Centro de Ciberseguridad Industrial

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

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

CSFE *(Center for Seabees and Facilities Engineering)*: Centro para Instalaciones de Ingeniería

CSMS *(Cyber Security Management System for IACS)*: Sistema de Gestión de Ciberseguridad para IACS

DCOM *(Distributed Component Object Model)*: modelo de objetos de componentes distribuidos

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

DIN *(Deutsches Institut für Normung)*: Instituto Alemán de Normalización

DMZ *(Demilitarized Zone)*: Zona desmilitarizada

DNP *(Distributed Network Protocol)*: protocolo de red distribuida

DNS *(Domain Name System)*: sistema de nombres de dominio

EDSA *(Embedded Device Security Assurance)*: valuación de la seguridad de dispositivo integrado

EMI *(Electromagnetic Interference)*: interferencia electromagnética

E/S: entrada-salida

FSP *(Federation of Security Professionals)*: Federación de Profesionales de Seguridad

GPS *(Global Positioning System)*: sistema de posicionamiento global

HAZOP *(Hazard and Operability Analysis)*: análisis de peligros y operabilidad

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

IACS *(Industrial Automation Control System)*: sistema de automatización y control industrial

IAIA: Instituto de Auditores Internos de Argentina

ICSS *(Integrated Control Safety System)*: sistema integrado de control y seguridad

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

IIoT *(Industrial Internet of Things)*: Internet industrial de las cosas

I/O *(Input/Output)*: E/S

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

IP *(Internet Protocol)*: protocolo de Internet

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

ISCI *(ISA Security Compliance Institute)*: Instituto de Cumplimiento de la Seguridad de ISA

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

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

ITBA: Instituto Tecnológico de Buenos Aires

I+D: investigación y desarrollo

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

KRITIS *(Kritische Infrastrukturen)*: infraestructuras críticas

LOPA *(Layer of Protection Analysis)*: análisis funcional de operabilidad

MCDA *(Multiple Criteria Decision Analysis)*: análisis de múltiples criterios para la toma de decisiones

MILP *(Mixed Integer Linear Programming)*: programación lineal entera mixta

MIT *(Massachusetts Institute of Technology)*: Instituto Tecnológico de Massachusetts

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

NS: niveles de seguridad

ODVA *(Open DeviceNet Vendor Association)*: Asociación de Proveedores de Dispositivos

NTP *(Network Time Protocol)*: protocolo de tiempo de red

OLE *(Object Linking and Embedding)*: incrustación y enlazado de objetos

OPC *(OLE for Process Control)*: OLE para control de procesos

OPC UA *(OPC Unified Architecture)*: arquitectura unificada de OPC

OPEX *(Operating Expense)*: costos operacionales

OS *(Operating System)*: sistema operativo

OT *(Operational Technology)*: tecnología operacional

O&M: operación y mantenimiento

PC *(Personal Computer)*: computadora personal

PID: proporcional-integral-derivativo

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

PyME: pequeña y mediana empresa

RFI *(Radio-Frequency Interference)*: interferencia de radiofrecuencia

SDL *(Security Development Lifecycle)*: ciclo de vida de desarrollo de seguridad

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

SDSA *(Software Development Security Assessment)*: evaluación de la seguridad en el desarrollo de software

SI: seguridad de la información

SIF *(Safety Instrumented Functions)*: funciones instrumentadas de seguridad

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

SIM *(Subscriber Identity Module)*: módulo de identificación de suscripción

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

SO: sistema operativo

SOP *(Standard Operating Procedure)*: procedimiento de operación estándar

SQL *(Structured Query Language)*: lenguaje de consulta estructurada

SRS *(Security Requirements Specification)*: especificación de requisitos de seguridad

TCP *(Transmission Control Protocol)*: protocolo de control de transmisión

TI: tecnología de la información

TO: tecnología operacional

TR *(Technical Report)*: reporte técnico

USB *(Universal Serial Bus)*: bus de serie universal

UTN: Universidad Tecnológica Nacional

VAN: valor actual neto

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

ZDM: zona desmilitarizada

Control en el agua

Roberto Saco

Roberto Saco es un desatacado docente de las áreas de control y automatización en las universidades de Quilmes y de Buenos Aires. Asimismo, es socio activo de AADECA, institución que conoció durante el ejercicio de su vida profesional. Esa es una cara de Roberto, y acá se muestra otra. Desde 2007, practica kitesurf, un deporte relativamente nuevo, pero de auge creciente.

¿Qué es el kitesurf?

El kitesurf o kiteboard es un deporte que consiste en deslizarse planeando sobre el agua mediante una tabla (board) y un barrilete (kite) aprovechando la fuerza del viento. Es un deporte relativamente reciente y esta en constante auge. Actualmente se han subdividido distintas especialidades.

¿Hace cuánto tiempo lo practica? ¿Cómo empezó todo?

Lo practico desde el 2007. Anteriormente practicaba windsurf. Fue mientras practicaba windsurf que observé la práctica del kitesurf en los distintos lugares que frecuentaba (Punta Lara, Magdalena, Costa Atlántica, Chascomús). En la primavera del 2007 decidí tomar un curso y experimentar en el deporte. A partir de ahí me atrapó.

¿Qué sensaciones le produce hacer esta actividad?

Estar en el mar, río, laguna practicando este deporte me desconecta totalmente de mi rutina cotidiana. Durante esas dos horas (una en invierno) ingreso en un entorno extraño para muchos, "vuelo" sobre el agua. Mi concentración está solo en la posición y tensión del kite, dirección del viento, rumbo, planeo, planificando qué borde hacer o qué ola tomar, equivocándome, cayéndome al agua, aprendiendo de los errores y volviendo a probar. Cuando termino la práctica, generalmente, me quedo junto a amigos del deporte, compartiendo excelentes momentos.

¿Qué le diría a alguien que quiera imitarlo?

Que no lo dude. Que pruebe. El camino es tomar un curso básico, donde se provee el equipo y se aprende el uso de los sistemas de seguridad del kite. Muchos me preguntan si es un deporte peligroso, mi respuesta es: los deportes no son peligros, pero algunas personas sí. Mi consejo es alejarse lo más posible de las personas peligrosas. Además, utilizar los elementos de seguridad aconsejados.

¿Algo más que quiera agregar?

Los días ideales para la práctica de este deporte no son los días ideales que mucha gente busca cerca del mar, río, laguna, lago. La próxima vez que estén disfrutando de la playa y se tengan que ir, debido a que se vuela la sombrilla, la arena les golpea en la cara y se ponga fresco por el fastidioso viento lateral, tal vez nos crucemos, porque es en ese momento cuando suelo llegar a la playa, con mi tabla y mi kite a disfrutar del viento, el mar y las olas.

AADECA

CURSOS 2018

Proyectos Industriales

Generación Eléctrica

Ciberseguridad Industrial

Redes y Comunicaciones Industriales

Metrología

SCADA y DCS

PLC Nivel I y II

Turbinas en generación eléctrica

Control de Movimiento

Cursos In Company

y mucho más ...

ORGANIZA

AADECA

Asociación Argentina
de Control Automático

Para mayor información comuníquese por e-mail a
cursos@aadeca.org - tel. 011 4374-1684

aadeca.org

IO-Link - ¡Liberando el potencial!

¿Qué ventajas ofrecen los sistemas IO-Link de ifm?	Los sensores IO-Link de ifm ofrecen actualmente posibilidades completamente nuevas para los usuarios. Un ejemplo es la transmisión en ambos sentidos de datos cíclicos y acíclicos y de mensajes. Por otra parte, IO-Link ofrece todavía mucho más:
Sin influencia externa de la señal	La transmisión de datos está basada en una señal de 24V. Se hace innecesario el uso de cables apantallados y tomas a tierra.
Sin pérdidas de los valores de medición	La transmisión de valores de medición se lleva a cabo en su totalidad digitalmente. Se reemplaza así la transmisión y conversión de señales analógicas, procesos que suelen ser propensos a errores.
Sencilla sustitución de sensores	Todos los parámetros del sensor se almacenan en el maestro y se transmiten al nuevo equipo.
Protección contra manipulaciones	Ya no se producen errores de ajuste por parte de los operarios.
Identificación	Equipos de sustitución equivalentes. No se aceptan sensores erróneos.
Detección de rotura de cable/diagnóstico	Las roturas de cable o los cortocircuitos son detectados de inmediato.

Garantía 5 años en productos ifm

www.io-link.ifm
Tel: +54 (011) 5353-3436