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

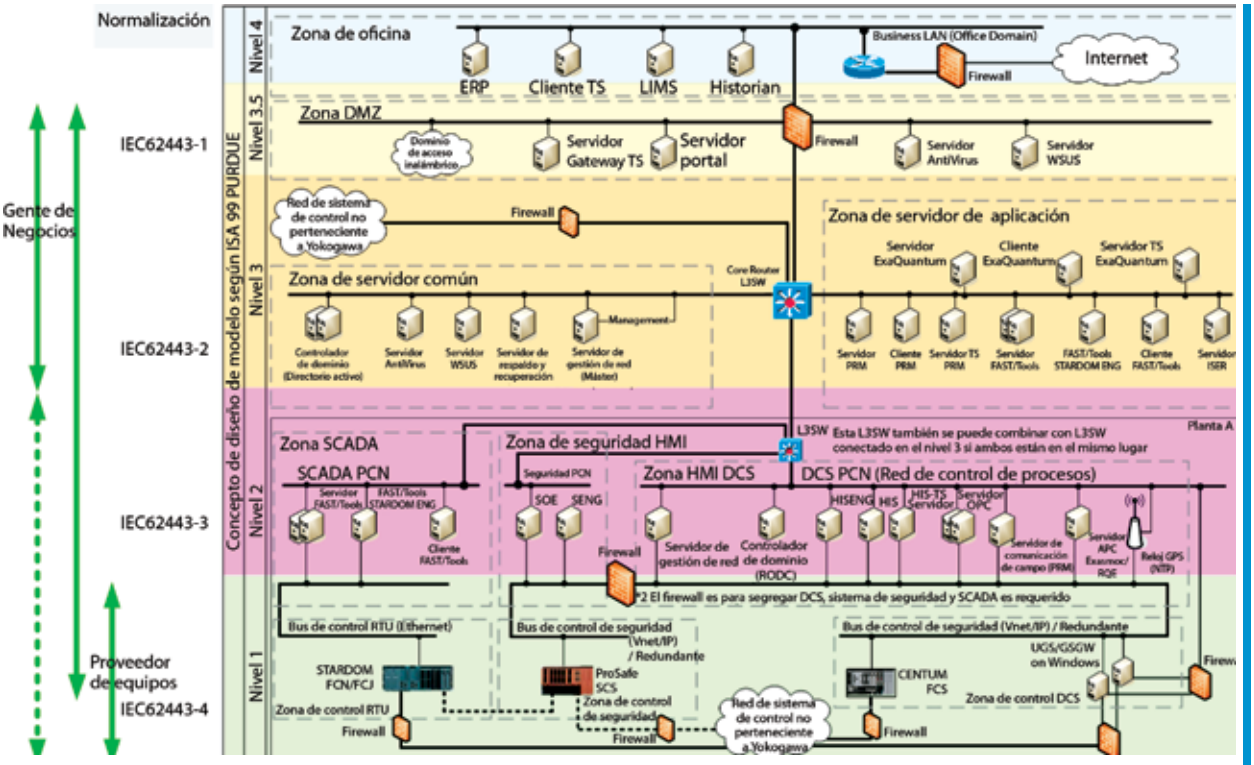

Figura 1. Vista general de las normas de seguridad IEC 62443

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.

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.

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.

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

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)

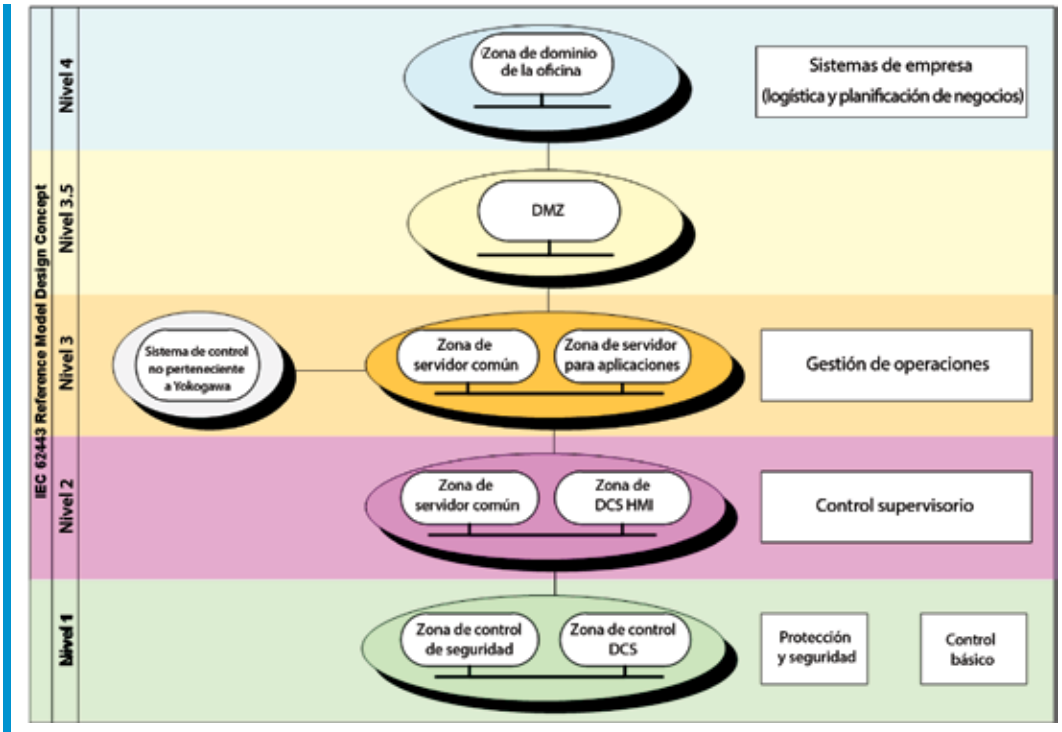

Figura 3. Conceptos de diseño para el modelo de referencia según IEC 62443

- 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. ❖