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

Por Daniel DesRuisseaux
Director del Programa de Ciberseguridad Industrial

Schneider Electric
www.schneider-electric.com.ar

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

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

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

Introducción

Durante los últimos diez años se ha observado un aumento exponencial de los ciberataques a los sistemas de control industrial (ICS). La industria ha respondido a las amenazas contra la ciberseguridad creando normas para ayudar a los usuarios finales y los fabricantes de equipos a brindar seguridad para los sistemas de control industrial. En la actualidad existen varias normas clave disponibles en el mercado. La norma IEC 62443 fue desarrollada por los comités de ISA99 e IEC para mejorar la seguridad, la disponibilidad, la integridad y la confidencialidad de los componentes o los sistemas usados para automatización y control industriales. La

serie de estándares IEC 62443 puede usarse en todos los segmentos de control industrial, y fue aprobada en muchos países. En su evolución, se ha ido convirtiendo en una norma clave para la industria, y *Schneider Electric* está creando su estrategia de ciberseguridad en torno a ella.

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

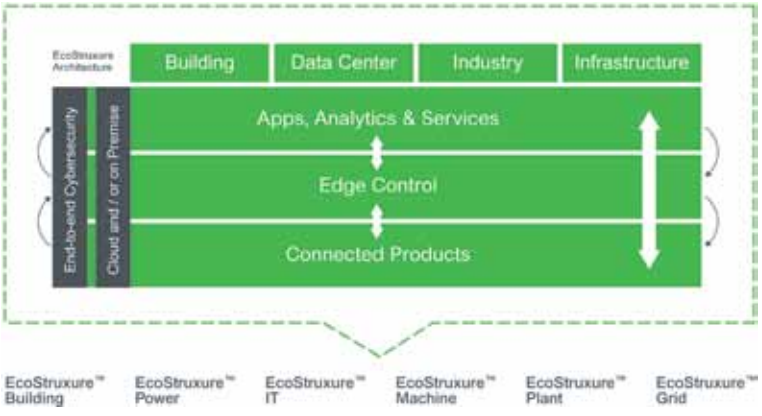

Figura 1

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

Tabla 1

EcoStruxure

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

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

Conceptos de ciberseguridad

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

Niveles de seguridad garantizados

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

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

Defensa en profundidad

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

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

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

Controles de compensación

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

Visión general

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

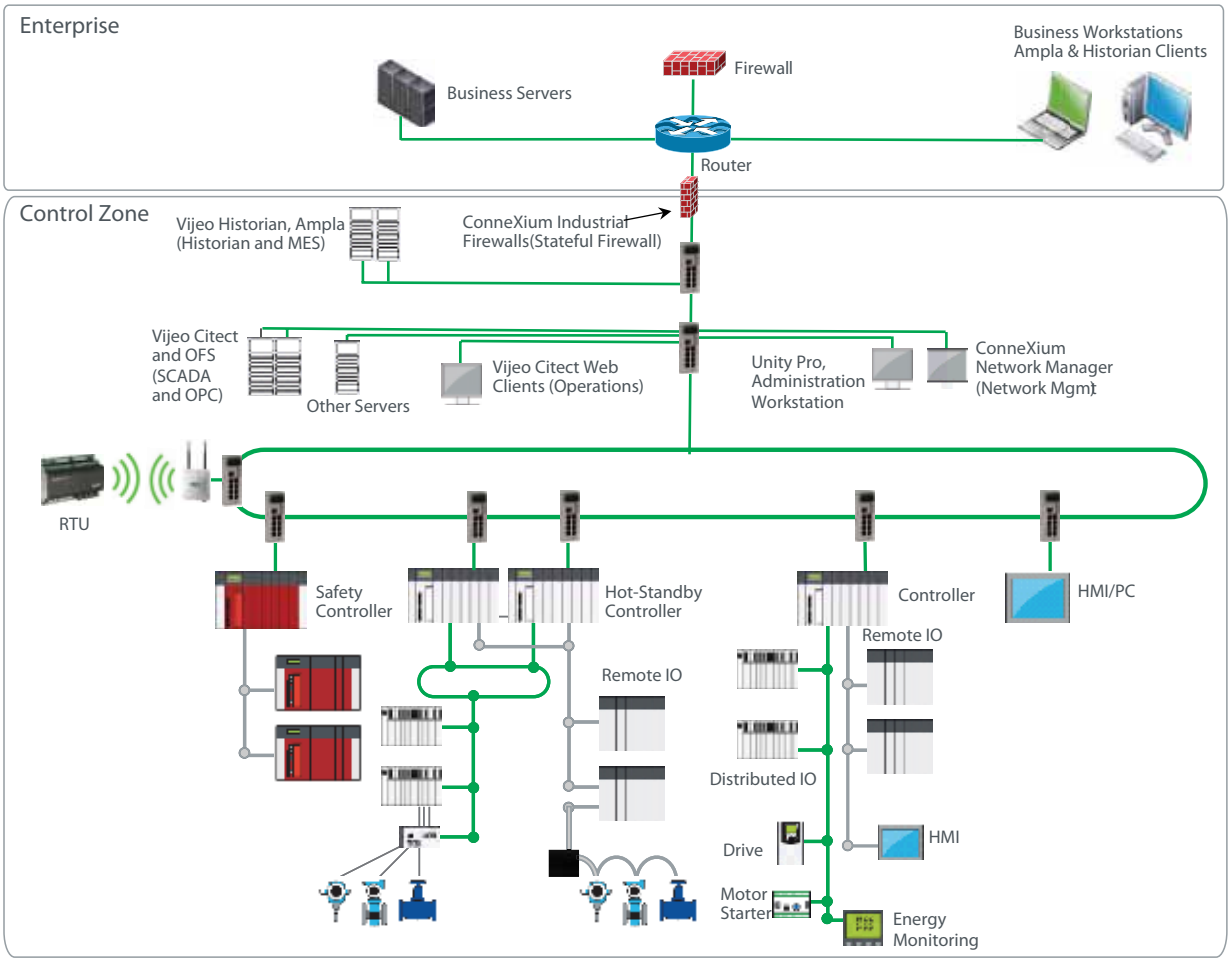

Figura 2

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

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

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

A lo largo de este informe, la red de referencia que se acaba de presentar se modificará para ilustrar cambios que permitan satisfacer los requisitos de cada uno de los niveles de seguridad según IEC 62443. El foco de este informe serán los tres primeros niveles de seguridad, ya que en ellos se incluye la gran mayoría de las aplicaciones industriales, en particular, los requisitos de sistema según se

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

Tabla 2. Requisitos clave estipulados para SL1

especifican en el estándar de sistema IEC 62443-3-3. Se presentará cada uno de los niveles de seguridad (SL) conjuntamente con una descripción de los cambios necesarios. Para simplificar la presentación, en este informe se presupone que cuando se eleva el nivel de seguridad, se lo eleva para toda la red (no se configurarán segmentos de red específicos con niveles de seguridad diferentes).

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

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

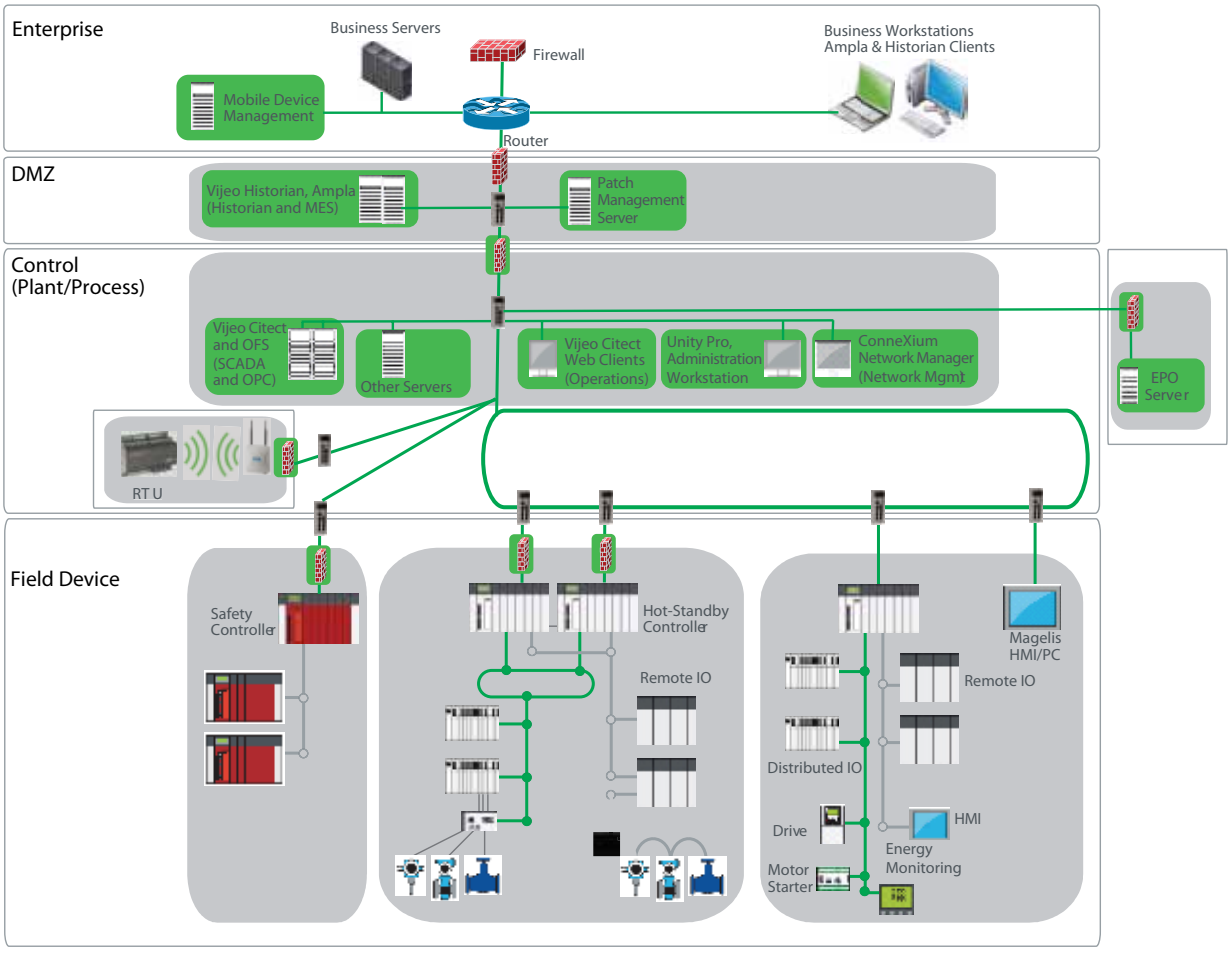

Figura 3

Nivel de seguridad SL1

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

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

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

Las zonas son:

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

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

Nivel de seguridad SL2

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

Es importante notar que algunos de los requisitos son mejoras de los estipulados para SL1, y otros son nuevos. Por ejemplo, en SL1, el sistema debe autentificar y autorizar a los usuarios humanos. En SL2, el sistema debe además autentificar y autorizar los dispositivos y los procesos de software. En SL1, el sistema debe detectar, informar y evitar la ejecución de software malicioso. En SL2, el sistema debe

detectar, informar y evitar la ejecución de software malicioso en todos los puntos de entrada y salida de la zona. En algunos casos, se agregan nuevos requisitos, como la capacidad de admitir certificados de autentificación.

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

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

Nivel de seguridad SL3

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

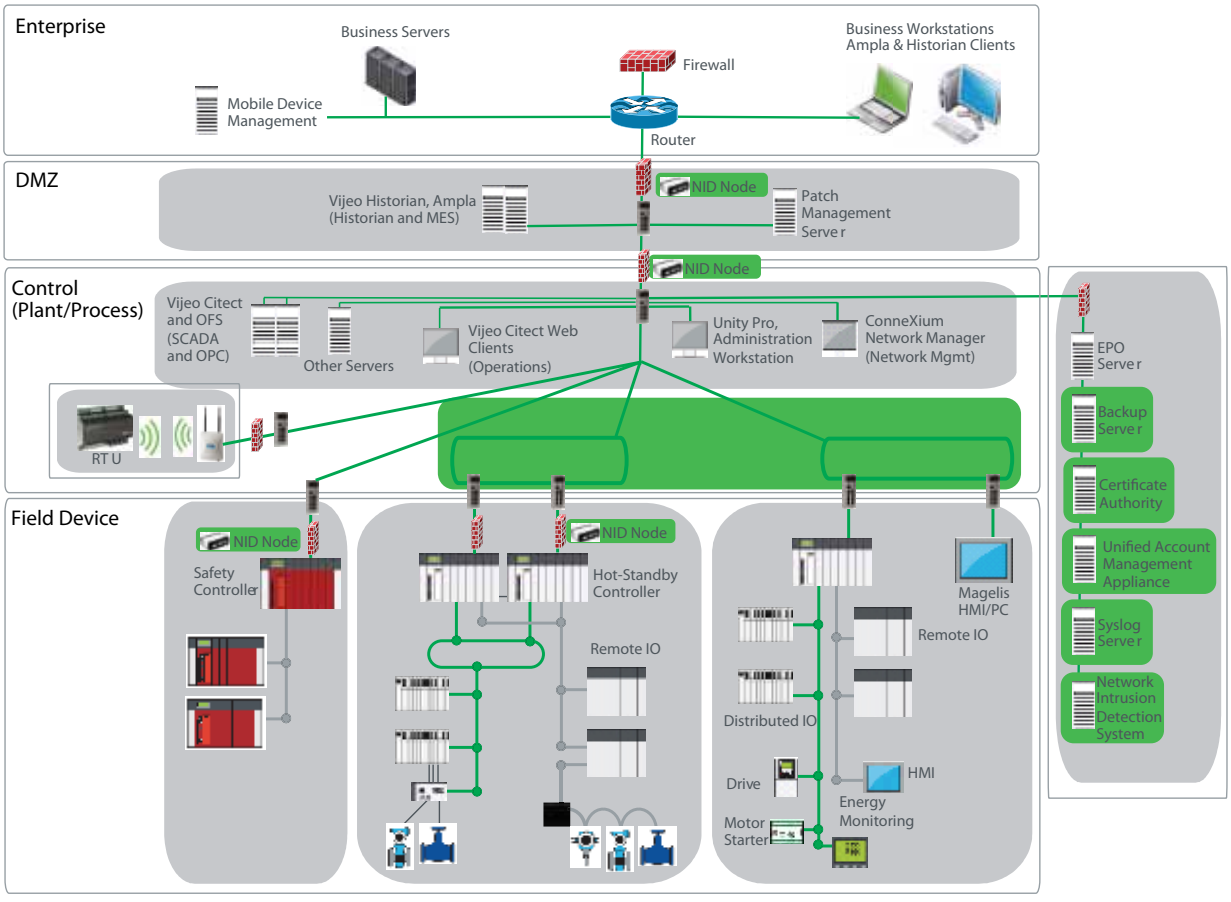

Figura 4

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

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

Certificación del producto y del sistema

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

» Usuarios finales. Por lo general, los usuarios finales evalúan los productos de los fabricantes en base a criterios entre los que se incluyen el contenido de características, el precio y los

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

Tabla 3.

términos de la entrega. La especificación de características puede ser un proceso complejo. La norma IEC 62443 simplifica el proceso de definición de requisitos de seguridad al permitir que los usuarios finales especifiquen un nivel de seguridad como objetivo, en lugar de detallar una lista complicada de características individuales. Los usuarios finales sabrán las características exactas disponibles en los equipos en base a su cumplimiento con los estándares establecidos en IEC 62443.

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

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

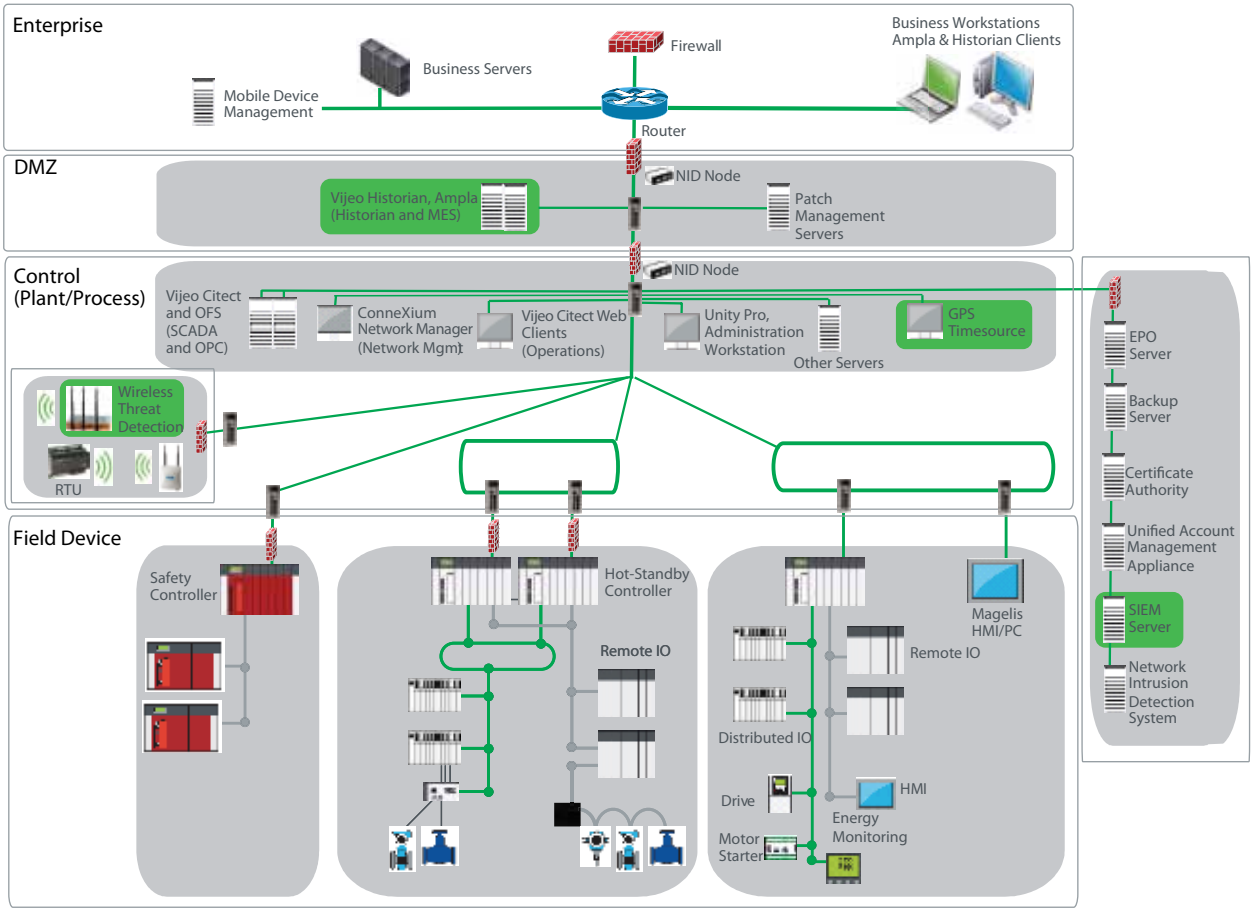

Figura 5

certificaciones de ciberseguridad en sus requisitos para adquisición de equipos

Conclusión

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

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

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

Tabla 4