Ciberseguridad industrial

Introducción a la ciberseguridad industrial



Introducción a la ciberseguridad industrial

Índice

Presentación 3
Objetivos 3
1. Introducción 4
1.1. Evolución de la conectividad en la automatización industrial 4
1.2. Ciberseguridad en sistemas de control y automatización industrial (IACS).... 6
1.3. Diferencias entre la cultura de los IACS y la cultura IT 16
Resumen 21
Referencias bibliográficas 22

Introducción a la ciberseguridad industrial

Presentación

En este tema: “Introducción a la ciberseguridad industrial” dentro de la asignatura de Ciberseguridad industrial, el alumno va a conocer qué es la ciberseguridad en el entorno de las organizaciones industriales, realizando un repaso acerca de la historia de la automatización industrial en cuanto a tecnologías de comunicaciones, conectividad e interconexión de sistemas de control industrial. A continuación se expondrán los motivos que hacen necesario proteger estas comunicaciones y los sistemas de control industrial.



Objetivos

Los objetivos que se pretenden alcanzar en este tema son los siguientes:

- Introducir al alumno en los conceptos esenciales de comunicaciones y conectividad en el entorno industrial.
- Introducir al alumno en los conceptos de protección de los sistemas de control industrial.

Introducción a la ciberseguridad industrial

1. Introducción

Los sistemas de control industrial, o ICS (industrial control systems) de sus siglas en inglés, han evolucionado a lo largo de los años hasta alcanzar un nivel de interconexión muy alto y con requerimientos de conectividad cada vez más exigentes. Este aumento de la conectividad provoca de manera ineludible que se expongan a riesgos cada vez más importantes y de graves consecuencias. Es por ello que la protección de estos sistemas se convierte en un punto de vital importancia para las organizaciones industriales.

1.1. Evolución de la conectividad en la automatización industrial

Los **sistemas de control industrial** nacieron inicialmente como sistemas aislados para controlar un proceso específico o realizar una tarea concreta. Estos sistemas no tenían comunicación con otros sistemas, ni tenían relaciones de interconexión más allá de un interfaz hombre-máquina para ofrecer información o insertar una consigna o comando a la máquina.

Posteriormente surgió la necesidad de interconectar procesos entre sí, y lo primero que se ideó fue el intercambio de información mediante entradas y salidas digitales y de ese modo compartir información de estados para tomar decisiones al respecto.

Los sistemas de control industrial y sus tecnologías fueron evolucionando, dando lugar a la aparición de **buses de campo** que podían comunicar señales de entrada/salida con una unidad central (autómata programable) mediante un solo cable de comunicaciones y un protocolo de intercambio de información. De este modo, se consiguió la descentralización del control respecto a los sensores y actuadores, lo que hizo posible grandes avances sobre todo en la industria de proceso.

Mediante estos buses de campo también se establecieron las primeras conexiones entre diferentes máquinas, cada una de ellas con su control independiente, y de ese modo poder compartir información de los procesos.

Estos buses de campo, como por ejemplo **PROFIBUS**, estaban basados en tecnologías de comunicación serie que utilizaban cables de cobre. Y por supuesto los anchos de banda que podían alcanzar no podían ser muy grandes si queríamos tener una fiabilidad en las comunicaciones, ya que las ondas electromagnéticas y las corrientes inducidas producen muchas interferencias en ellos provocando fallos en las comunicaciones. Por lo tanto, estos sistemas tenían algunas limitaciones que no empezaron a destacar hasta que empezaron a aumentar los requerimientos de los procesos en cuanto a volumen de información a transmitir.

Por esa razón, en los años 90 del siglo XX se introdujo el estándar de Ethernet en la industria. El estándar Ethernet se estableció muy rápido en los entornos corporativos de oficina donde el aumento de la conectividad empezó a tomar una gran importancia: Internet e Intranet, correo electrónico, bases de datos conectadas, etc. En la industria se adoptó el mismo estándar, pero adaptado a las condiciones del entorno, es decir, con unas particularidades en la construcción de los componentes de red y en los

componentes pasivos para que fuesen capaces de soportar las condiciones de la industria; y se le bautizó como **Ethernet industrial**.

Los primeros componentes de red Ethernet industrial eran hubs y switches que utilizaban los mismos estándares que los equipos de entorno ofimático, salvo con una característica en su diseño capaces de soportar los entornos más agresivos en cuanto a temperatura, humedad, vibración, etc. Y poco a poco fueron adaptando la tecnología a las necesidades de los sistemas de control industrial.

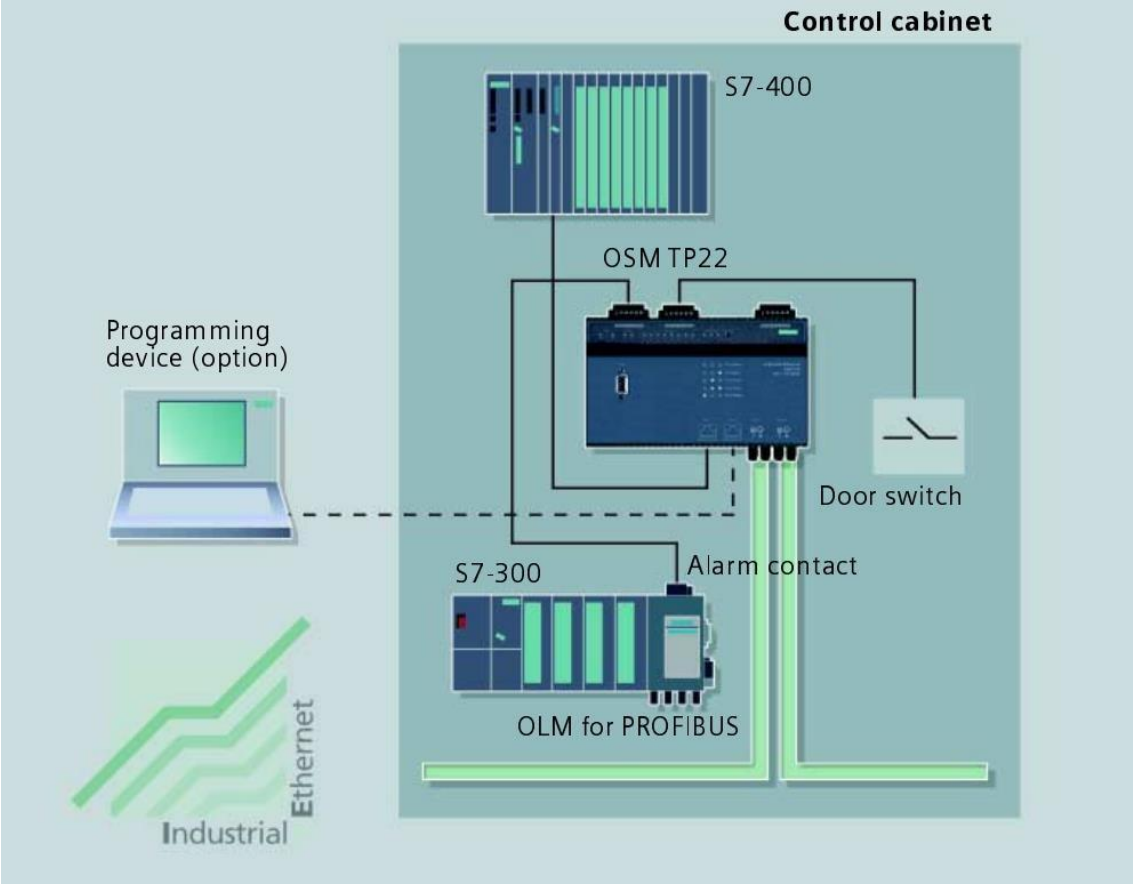


Figura 1. Primeros switches industriales basados en tecnología Ethernet Industrial. Fuente: <www.siemens.com>

Debido a ello, aparecieron en los años 2000 los primeros buses de campo basados en Ethernet industrial, como por ejemplo PROFINET, que aportaban todas las ventajas en cuanto a eficiencia y flexibilidad a los sistemas de control. La tecnología de Ethernet industrial ya se venía utilizando para conectar autómatas programables entre sí, o sistemas de interfaz hombre-máquina (HMI), como los SCADA o las pantallas de operador, con los autómatas programables. Pero los buses de campo requerían de una característica para ser eficientes: el determinismo.

Con el paso del tiempo, la tecnología de Ethernet industrial se impuso como la tecnología predominante en los sistemas de control industrial haciendo prácticamente desaparecer al resto de tecnologías de comunicaciones basadas en buses serie.

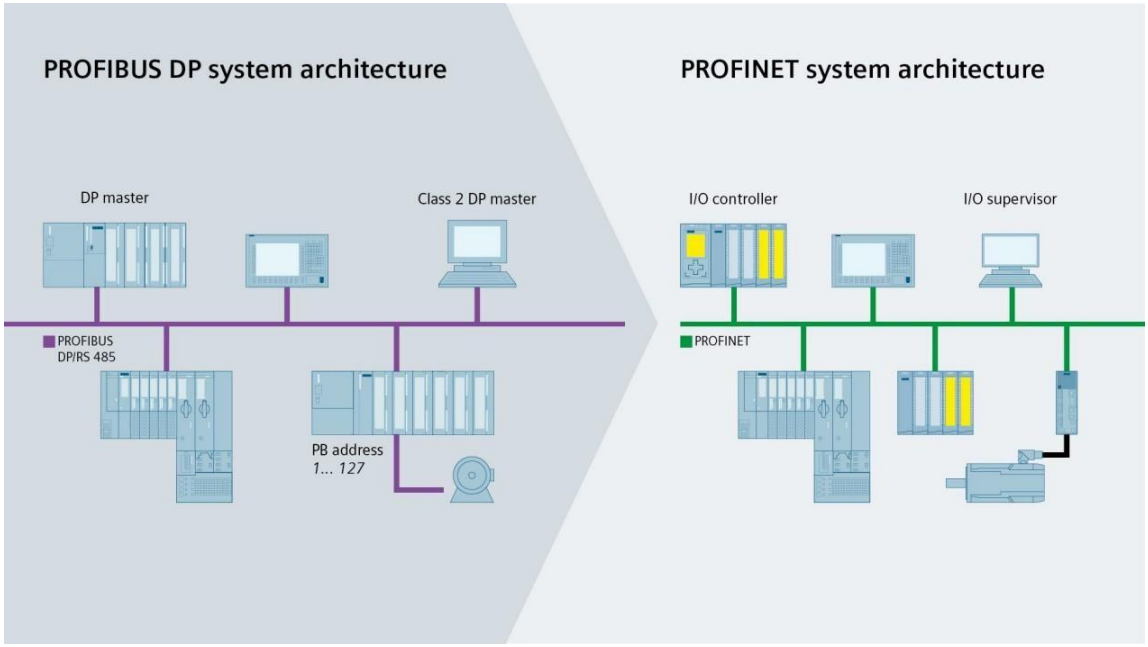


Figura 2. Evolución de tecnología de buses de campo basados en par de cobre a tecnología basada en Ethernet Industrial. Fuente: <www.siemens.com>

Al convertirse en tecnología predominante, las posibilidades que ofrece fueron aumentando mediante las innovaciones y, en consecuencia, las necesidades de interconexión de los sistemas tanto horizontal como verticalmente crecieron exponencialmente.

Con la aparición del concepto de Industria 4.0, las organizaciones han tenido la necesidad de conectar los sistemas de control industrial con los sistemas de gestión empresarial para obtener todo el potencial, por un lado, de los datos, y por otro lado de la automatización de todos los procesos empresariales: gestión de pedidos, gestión de la producción, gestión energética, gestión de materias primas, gestión de la logística, etc.

En conclusión, hemos pasado de una situación en la que las máquinas estaban aisladas y realizaban tareas limitadas a un programa determinado, a estar totalmente conectadas tanto horizontal como verticalmente (incluso a Internet); con los riesgos que esto conlleva si hablamos en términos de ciberseguridad.

1.2. Ciberseguridad en sistemas de control y automatización industrial (IACS)

Debido a la transformación digital de los sistemas de automatización industrial, se requiere una integración de los sistemas cada vez mayor, grandes volúmenes de datos y la adopción de estándares abiertos para proporcionar el acceso directo necesario en todos los niveles. La enorme cantidad de oportunidades y beneficios, tanto en la fabricación discreta como en las industrias de procesos, prometidas por estos cambios ha llevado al mercado a hablar desde hace tiempo de una nueva revolución industrial y el comienzo de lo que se denomina “Industria 4.0”.

Sin embargo, esta tendencia tiene un lado no tan positivo al conllevar un aumento de los riesgos por un ciberincidente. Esta integración de gran alcance, los grandes volúmenes de información crecientes y los estándares universales facilitan mucho el acceso de los atacantes y el malware a los sistemas. Los estudios sobre recientes incidentes muestran que no solo se reconocen las redes OT y las áreas de producción como objetivos lucrativos para los ataques, sino que las personas detrás de estos ataques se están volviendo cada vez más agresivas en sus tácticas, utilizando herramientas más efectivas y aplicando más recursos a los ataques. Y la razón de esta nueva situación es que existe una industria de ciberdelincuencia con muchos recursos y gran financiación.

La realidad actual es que los sistemas industriales también enfrentan ataques implementados profesionalmente. La guerra cibernética ya está sobre nosotros. La nueva situación de amenaza exige un replanteamiento fundamental de la seguridad de la información, la protección del acceso y todo el proceso de establecimiento de conceptos de seguridad industrial. Los atacantes están mejorando su arsenal y nunca ha sido más importante para los proveedores y operadores de sistemas de automatización y producción asumir la amenaza que representan.

Afortunadamente, es completamente posible implementar una defensa lo suficientemente eficaz como para minimizar los riesgos hasta un nivel aceptable por las organizaciones industriales. Si bien el 100% de la seguridad está fuera de discusión (no existe básicamente), ciertamente hay formas y medios de reducir el riesgo a un nivel aceptable como hemos comentado. Controlar el riesgo de esta manera requiere un concepto de seguridad integral que tenga en cuenta las diferentes características y la naturaleza profesional de los ataques y que además promueva una fuerte cooperación entre las diversas partes involucradas, es decir, operadores de sistemas de automatización, integradores, fabricantes de máquinas y proveedores. Todos los actores deben estar involucrados en el ciclo de vida de la ciberseguridad industrial para alcanzar el éxito.

Las medidas organizativas y técnicas deben coordinarse cuidadosamente: un concepto de seguridad integral se basa en las personas, los procesos y la tecnología al unísono para lograr el nivel de protección necesario.

1.2.1. Descripción general del concepto de seguridad industrial

Todos los aspectos, desde el nivel operativo hasta el nivel de campo y desde el control de acceso físico hasta la protección de redes y terminales, deben abordarse simultáneamente para proteger los sistemas industriales contra ciberataques internos y externos. El enfoque más adecuado para esto es un concepto de defensa en profundidad de acuerdo con las recomendaciones establecidas en el estándar IEC 62443, el estándar más aceptado para la seguridad en la automatización industrial.

Los elementos de seguridad de la planta, seguridad de la red industrial e integridad del sistema forman la base del concepto de ciberseguridad industrial. En este enfoque se consideran todos los factores clave, incluida la protección del acceso físico y las medidas organizativas, como las directrices y los procesos, así como las medidas técnicas para proteger las redes industriales y los sistemas contra el acceso no

autorizado, el espionaje y la manipulación. La protección en múltiples niveles y el efecto combinado de diferentes medidas de protección proporciona un alto grado de seguridad, reduciendo el riesgo de ataques exitosos y, en última instancia, mejorando la disponibilidad y productividad de la planta.

"Defensa en Profundidad", *Defense-in-Depth* en inglés, es un concepto de defensa muy antiguo que ahora se aplica en ciberseguridad para diseñar las arquitecturas de protección. Podemos imaginar un castillo medieval donde el elemento más vulnerable se encontraba en el interior del mismo (el señor del castillo) y para protegerle se implementaban diferentes medidas, de modo que el atacante no pudiese acceder al elemento vulnerable derribando una sola medida, sino que tenía que ir derribando una a una para llegar al objetivo. Por ejemplo, volviendo al ejemplo del castillo, podríamos implementar un foso profundo con agua, un puente levadizo, una torre de vigilancia, un muro de piedra, una guarnición de arqueros en torres, etc.

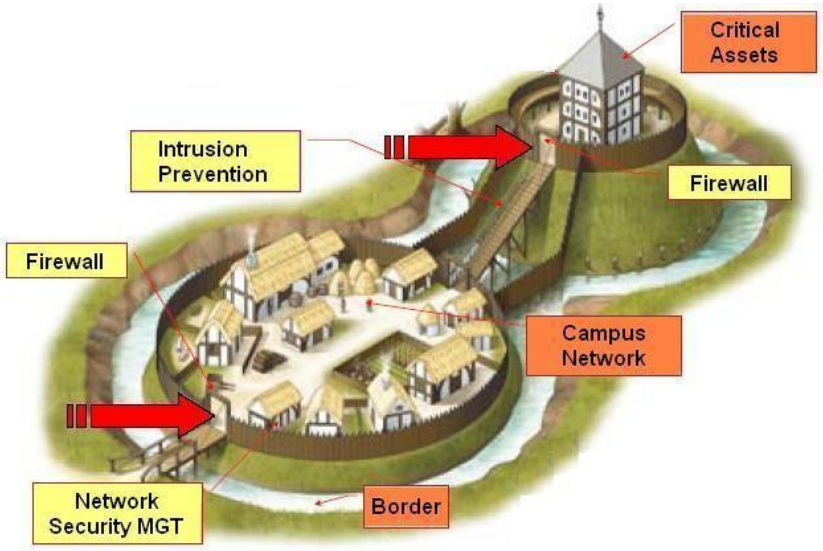


Figura 3. Técnica de "Defensa en Profundidad" aplicada a un castillo medieval. Fuente: <www.nigesecurityguy.files.wordpress.com>

Esta técnica, también denominada técnica de capas de cebolla, hace que un atacante encuentre muy complicado alcanzar su objetivo en una única acción de ataque. Lo que ofrecerá más tiempo a una organización industrial a detectar el ataque y a mitigar sus efectos.

Está metodología puede dividir las diferentes técnicas en tres grupos: seguridad de planta, seguridad de red e integridad del sistema. Los veremos detenidamente a continuación.

1.2.2. Seguridad de la planta

La seguridad de la planta establece las condiciones necesarias para garantizar que las medidas técnicas de seguridad de IT implementadas no puedan eludirse por otros medios físicos. Las medidas de seguridad de la planta incluyen infraestructura de protección de acceso físico como barreras, tornos de acceso, cámaras de vigilancia y

lectores de tarjetas. Las medidas organizativas incluyen, sobre todo, un proceso de gestión de la seguridad para garantizar la seguridad de una planta.

1. **Protección de acceso físico**

   Aquí se pueden cubrir los siguientes puntos:

   a. Medidas y procesos que eviten el acceso de personas no autorizadas a las plantas.

   b. Separación física de diferentes áreas de producción con autorizaciones de acceso diferenciadas.

   c. Protección de acceso físico para componentes críticos de automatización (por ejemplo, los armarios de control cerrados de forma segura mediante una llave).

   Las directrices relativas a las medidas de protección del acceso físico también influyen en la cuestión de qué medidas de seguridad de IT se requieren y en qué grado. Si, por ejemplo, el acceso a un área en particular ya está estrictamente limitado a personas autorizadas seleccionadas, las interfaces de acceso a la red o los sistemas de automatización no necesitan estar protegidos de manera tan robusta como sería el caso en áreas de acceso general.

2. **Gestión de la seguridad**

   Las medidas organizativas adecuadas y la introducción de procesos de seguridad eficaces son vitales para la seguridad de la planta. Las medidas organizativas deben estar estrechamente coordinadas con las medidas técnicas, ya que la eficacia de cada una depende en gran medida de la eficacia de la otra; de hecho, la mayoría de los objetivos de seguridad solo se pueden lograr mediante una combinación de medidas organizativas y técnicas.

   Las medidas organizativas incluyen el establecimiento de un proceso de gestión de la seguridad. El primer paso para determinar qué medidas es probable que se requieran en una situación determinada es analizar los riesgos específicos que existen e identificar cuáles no se pueden tolerar. La importancia de un riesgo identificado a este respecto depende del daño asociado con su materialización, así como de su probabilidad de ocurrencia. No realizar un análisis de riesgos adecuado y determinar los objetivos de seguridad es más que probable que resulte en que ambas medidas implementadas sean ineficaces o innecesariamente caras y, por otro lado, existirán algunas vulnerabilidades que no se identifiquen y, por lo tanto, que no se aborden.

   El análisis de riesgos identificará objetivos de seguridad que forman la base de medidas organizativas y técnicas específicas. Las medidas deben revisarse después de su implementación ya que debe ser un proceso de mejora continua. El riesgo debe evaluarse nuevamente de vez en cuando o después de cambios materiales en caso de que la situación de amenaza o los factores subyacentes

hayan cambiado. El análisis de riesgos proporciona la base del procedimiento para implementar medidas de protección y, en su caso, de seguimiento.

3. **Servicios de seguridad de la planta**

   Los servicios de seguridad especiales pueden ayudar a los operadores en muchos aspectos con el diseño de entornos de producción seguros. Este proceso asistido se extiende desde un análisis del riesgo (evaluar la seguridad) y el diseño y realización de una operación de producción segura (implementar la seguridad) hasta la monitorización continua del estado de seguridad de la planta (gestionar la seguridad).

   La evaluación de riesgos aporta transparencia en cuanto al estado de la seguridad de una planta e identifica las vulnerabilidades, proporcionando así una base sobre la cual se puede derivar el riesgo correspondiente. Las medidas necesarias se compilan en un plan de acción (hoja de ruta) que muestra cómo se puede elevar el estado de seguridad de una planta a un nuevo nivel superior. Un ejemplo es realizar una evaluación según IEC 62443, que establece las acciones necesarias para que una planta específica cumpla con dicho estándar. Los servicios de escaneo se pueden utilizar como alternativa o en combinación para lograr transparencia en los dispositivos informáticos existentes en el activo, así como también las vulnerabilidades, incluidas las verificaciones contra niveles de seguridad predefinidos.

   El siguiente paso es implementar las medidas propuestas para cerrar las brechas identificadas. Los recursos que abarcan tanto hardware (como firewalls) como software (como antivirus, listas blancas y detección de anomalías) se utilizan para este propósito. También se incluyen instrucciones y pautas claras sobre seguridad de IT en el entorno industrial. En última instancia, las soluciones de seguridad solo pueden funcionar correctamente si los empleados han sido formados y capacitados en consecuencia. La concienciación y la comprensión de los empleados deben promoverse continuamente a través de talleres, capacitación basada en la web o medidas equivalentes.

   Otro aspecto clave de los servicios de ciberseguridad en esta área es el apoyo de los proveedores a las organizaciones ofreciendo la monitorización continua de las plantas industriales y las máquinas de producción, así como la gestión de vulnerabilidades y parches, logrando así transparencia en el aumento de ciberamenazas.

   En conclusión, la estrategia de defensa en profundidad crea una base adecuada para mejorar la seguridad en las plantas industriales.

1.2.3. Seguridad de la red

Un elemento central del concepto de seguridad industrial es la seguridad de la red. Comprende principalmente la protección de las redes de automatización contra el acceso no autorizado, así como el control de todas las interfaces hacia otras redes, como el conducto a la red corporativa. En particular, las pasarelas de mantenimiento remoto a Internet deben protegerse en este contexto. La protección de las

comunicaciones contra la interceptación y manipulación mediante la transmisión de datos cifrados y la autenticación del nodo de comunicación también están dentro del alcance de la seguridad de la red.

1. **Asegurar interfaces a otras redes**

   Las interfaces con otras redes se pueden monitorizar y proteger mediante firewalls y, cuando corresponda, mediante la configuración de una zona desmilitarizada (DMZ). Una DMZ es una red en la que los mecanismos técnicos de seguridad protegen el acceso a datos, dispositivos, servidores y servicios dentro de esta área. Los sistemas instalados dentro de la DMZ están protegidos de otras redes por cortafuegos que controlan el acceso. Esta separación permite proporcionar datos de redes internas (por ejemplo, la red de automatización) en redes externas sin tener que admitir el acceso directo a la red de automatización. Una DMZ generalmente está diseñada para que tampoco permita el acceso a la red de automatización, lo que significa que la red de automatización permanece protegida incluso si un atacante obtiene el control de un sistema dentro de la DMZ.

2. **Concepto de segmentación de red y protección de célula**

   La segmentación de la red de la planta para crear celdas de automatización separadas protegidas por mecanismos técnicos de seguridad ayuda a minimizar aún más el riesgo y a aumentar la seguridad. La segmentación de la red implica proteger elementos de una red, como una subred, con un dispositivo de seguridad que los separa del resto de la red por motivos técnicos de seguridad. Los dispositivos dentro de una celda segmentada están protegidos contra el acceso no autorizado desde el exterior sin necesidad de ningún compromiso en términos de capacidad en tiempo real, rendimiento u otras funciones.

   El cortafuegos puede controlar los intentos de acceso desde y hacia la celda. Incluso es posible estipular qué nodos de red pueden comunicarse entre sí y, en su caso, qué protocolos pueden utilizar. Esto significa que los intentos de acceso no autorizados pueden bloquearse, en primer lugar, y también hace posible reducir la carga en la red, ya que solo aquellas comunicaciones que se desean y permiten explícitamente pueden continuar.

   La división de las celdas y la asignación de los dispositivos reflejan los requisitos de comunicación y protección de las estaciones de la red. Además, los dispositivos de seguridad pueden cifrar la transmisión de datos hacia y desde las células mediante un túnel VPN para proteger contra el espionaje y la manipulación de datos.

   Esto comprende la autenticación de los participantes de la comunicación y, en su caso, la autorización de los intentos de acceso. El concepto de protección de células se puede implementar y la comunicación entre las células se puede proteger mediante el uso de componentes como los firewalls industriales.

3. **Acceso remoto seguro**

   Cada vez es más común conectar plantas directamente a Internet y conectar plantas remotas a través de redes móviles (GPRS, UMTS, LTE). Esto se hace para permitir el mantenimiento remoto, usar aplicaciones remotas y también para facilitar la monitorización de máquinas instaladas en todo el mundo.

   Asegurar el acceso es particularmente importante en este contexto. Los atacantes pueden encontrar puntos de acceso no seguros de forma fácil y económica utilizando motores de búsqueda, como Shodan, escáneres de puertos o scripts automatizados.



Enlace

Enlace al motor de búsqueda Shodan:

<www.shodan.io>

Por lo tanto, es muy importante asegurarse de que los nodos de comunicación estén autenticados, la transmisión de datos esté cifrada y la integridad de los datos esté protegida, especialmente en el caso de plantas de infraestructura crítica. Incidentes como la intrusión de personas no autorizadas, el escape de datos confidenciales y la manipulación de parámetros o comandos de control pueden resultar en un daño enorme, incluso al medio ambiente y poner en peligro incluso al personal de la organización.

Los mecanismos de túnel VPN, que proporcionan las mismas funciones (autenticación, cifrado y protección de la integridad) requeridas, han demostrado ser particularmente efectivos en la industria y los routers industriales de comunicaciones móviles admiten la configuración de túneles VPN, lo que permite que los datos se envíen de forma segura a través de estas redes con protección contra el acceso no autorizado.

Normalmente, los dispositivos para su uso en comunicaciones seguras se autentican como nodos de comunicación fiables utilizando, por ejemplo, certificados y las direcciones IP o nombres DNS relevantes se aplican en las reglas del cortafuegos para permitir o bloquear el acceso.

1.2.4. Integridad del sistema

El tercer pilar de un concepto de seguridad equilibrado es la integridad del sistema. Los sistemas cuya integridad debe protegerse en este contexto comprenden componentes de control y automatización, sistemas SCADA y pantallas HMI.

Estos requieren protección contra el acceso no autorizado y el malware, o deben cumplir requisitos especiales en áreas como la protección de la experiencia.

1. **Protección de sistemas basados en PC en la red de la planta**

   Los sistemas de PC utilizados en la oficina suelen estar protegidos contra software malintencionado y cualquier debilidad detectada en su sistema operativo o software de aplicación se corrige mediante la instalación de actualizaciones o parches. También se pueden requerir medidas de protección equivalentes para PC industriales y sistemas de control basados en PC, dependiendo de cómo se utilicen.

   Los mecanismos de protección familiares del entorno de oficina, como el software antivirus, también se pueden utilizar en entornos industriales en principio, aunque es fundamental asegurarse de que no tengan un impacto adverso en la tarea de automatización, es decir, que se debe comprobar la compatibilidad.

   Las soluciones de listas blancas (*white-listing*) se pueden utilizar conjuntamente con el software antivirus. La lista blanca implica la creación de listas aprobadas en las que el usuario especifica explícitamente qué tareas y procesos se ejecutan en el ordenador. Cualquier intento por parte de un usuario o un paquete de malware de instalar un nuevo programa se rechaza, evitando el daño asociado.

   Por supuesto, los numerosos mecanismos de seguridad integrados proporcionados en los sistemas operativos Windows también están disponibles para su uso en sistemas de refuerzo en la medida necesaria. Estos incluyen no solo la administración de usuarios y la administración de derechos, sino también opciones como configuraciones finamente diferenciadas que utilizan políticas de seguridad.

2. **Protección del nivel de control**

   Los esfuerzos para proteger el nivel de control se centran en garantizar la disponibilidad de la solución de automatización. Los mecanismos de seguridad integrados en los componentes de automatización estándar proporcionan el punto de partida para proteger el nivel de control.

   Estos mecanismos se habilitan y configuran de acuerdo con el nivel de protección requerido para la máquina o planta en cuestión. La configuración de los mecanismos de seguridad de los componentes de automatización, así como el desarrollo de los programas de ingeniería para la solución de automatización, se realizan desde la herramienta de ingeniería. Sin embargo, la interconexión cada vez mayor y la integración de los mecanismos de IT en la tecnología de automatización están cambiando los requisitos de las plantas de producción en términos de protección de acceso y protección contra la manipulación, que son absolutamente esenciales para los sistemas de control modernos.

   La protección de la propiedad intelectual es otro tema de creciente preocupación: los fabricantes de maquinaria invierten muchos recursos en el desarrollo de sus productos y no pueden permitirse el lujo de ver comprometida su *know-how,* patentado en muchos casos. Las funciones de protección de

know-how y protección contra copias proporcionadas por algunos autómatas programables de última generación brindan a los usuarios un soporte conveniente y sencillo también en esta área. La función de protección de *know-how* permite una protección muy específica de los módulos del programa para evitar el acceso a su contenido y la copia y modificación de algoritmos.

En algunos sistemas de control, la función de protección contra copias vincula los componentes del programa al número de serie de la tarjeta de memoria o CPU. Esto ayuda a evitar la copia de las máquinas, ya que los programas protegidos solo se pueden utilizar en las máquinas para las que están destinados. Estas funciones ayudan a los fabricantes de maquinaria a salvaguardar su inversión y mantener su ventaja tecnológica.

Otras funciones de seguridad como un *Stateful Inspection Firewall* y túnel VPN pueden estar integradas en los procesadores de comunicaciones de los autómatas programables.

La protección que brindan se extiende a los respectivos controladores conectados, a las redes subyacentes y, cuando sea necesario, a la comunicación entre ellos y, por lo tanto, complementa y mejora el concepto de protección a nivel de célula en una planta.

1.2.5. Conceptos de funciones y derechos de acceso

Defenderse contra las diversas amenazas planteadas y lograr un nivel adecuado de protección exige un concepto de defensa en profundidad que establezca múltiples obstáculos para que los posibles atacantes los superen. Por supuesto, no se puede permitir que estos obstáculos obstaculicen a los usuarios autorizados. En la práctica, es común establecer un sistema de derechos de acceso escalonados o categorías de derechos bajo los cuales algunos usuarios solo pueden acceder a unidades, dispositivos o aplicaciones específicas de la planta; por ejemplo, algunos tienen derechos de administrador y algunos solo tienen derechos de acceso de lectura o escritura.

La implementación de un concepto de seguridad, por lo tanto, ayuda no solo a defenderse contra ataques directos, sino también a instituir un concepto de autorización. Los conceptos de autorización están destinados a garantizar que el acceso esté restringido a personas autorizadas en función de los derechos específicos que se les asignan. Por lo general, esto implica definir roles, cada uno de los cuales confiere un conjunto específico de derechos, en lugar de crear un perfil de derechos separado para cada usuario. A los usuarios o grupos de usuarios se les asignan estos roles y, por lo tanto, reciben los derechos de acceso correspondientes. Por lo tanto, la gestión adecuada de los usuarios y los derechos es muy importante para la seguridad industrial.

Una configuración universal para todos los componentes de automatización facilita la gestión de usuarios en este caso, porque los roles y derechos de las diferentes personas involucradas se pueden definir y mantener de forma centralizada.

1.2.6. Desarrollo de productos con funciones de ciberseguridad

Cada vez más se exige a los proveedores de tecnología industrial un enfoque de seguridad desde el diseño. Esto significa considerar los aspectos de seguridad como parte del desarrollo y la producción de productos industriales. El estándar de seguridad IEC 62443 tiene un capítulo dedicado a este respeto dada la importancia que tiene en el ciclo de vida de la ciberseguridad.

Un producto de automatización debe ser monitorizado e integrado en un concepto de seguridad integral desde la creación del mismo hasta la producción y durante su uso, es decir, durante el ciclo de vida completo del producto. Los activos en este contexto pueden incluir código fuente, procesos de IT y máquinas de producción. El requisito de seguridad relacionado con los activos y la organización, con respecto a los procesos y métodos, se vuelve cada vez más difícil a medida que aumenta el nivel de seguridad deseado. El propietario del producto es responsable de especificar el nivel de seguridad que se aplicará al producto y los activos asociados.

Los requisitos de seguridad son particularmente altos cuando se desarrollan y fabrican productos de automatización que tienen funciones de seguridad. Las claves de seguridad utilizadas deben estar protegidas de forma fiable contra el acceso no autorizado en el almacenamiento. En el caso de una brecha de seguridad, por ejemplo, generar y distribuir nuevas claves sería una operación muy laboriosa. Los retrasos en la detección de la infracción, o una infracción que pasa completamente desapercibida, conllevarían altos riesgos de seguridad.

Estos productos estándar pueden reducir el riesgo para el usuario final gracias a las pruebas de vulnerabilidad, los análisis de riesgo y el trabajo de optimización del diseño asociado que se lleva a cabo durante el desarrollo de los mismos.

1.2.7. Resumen: seguridad industrial para plantas de producción

Incluso hace unos pocos años, la seguridad de las plantas de producción era un tema periférico. Las amenazas parecían bastante abstractas y teóricas y pocos fabricantes y operadores tenían mucho interés en los problemas involucrados.

Una serie de graves incidentes que se difundieron en los medios de comunicación lo cambiaron todo. De repente, quedó claro para todos que los sistemas de automatización y las plantas de producción también estaban en la lista de objetivos de los ciberataques, que eran vulnerables y que las posibles consecuencias podrían ser graves. Una combinación de la gran cantidad de casos registrados e investigaciones realizadas utilizando *honeypots* (trampas configuradas para engañar a los piratas informáticos para que expongan sus métodos y generen estadísticas de ataques) reveló el verdadero alcance de las amenazas planteadas.

El camino hacia la fábrica digital está asociado a numerosas tendencias, como el aumento de la interconexión, los volúmenes cada vez mayores de transmisión y almacenamiento de datos y la continua difusión de los estándares abiertos utilizados, que aumentan el riesgo de ciberataques. Evitar estos desarrollos solo por razones de

seguridad no es una solución, ya que este comportamiento resultaría en una competitividad cada vez menor y una contracción en los ingresos por ventas.

La defensa contra amenazas y ataques es, por tanto, un requisito previo fundamental para la transformación digital. Se recomienda a las empresas que realicen una revisión cuidadosa de la situación de seguridad de sus datos incluso sin la motivación del Reglamento General de Protección de Datos (RPGD) de la UE, que entró en vigor recientemente.

Los riesgos se pueden minimizar con éxito teniendo en cuenta los factores de seguridad durante las fases de diseño, desarrollo y producción, mediante la implementación de un concepto de seguridad integral para crear componentes robustos equipados con funciones de seguridad efectivas.

Pero la ingeniería y la tecnología por sí solas nunca pueden ser suficientes. Deben implementarse procesos y medidas organizativas y adaptarse los requisitos específicos relevantes.

1.3. Diferencias entre la cultura de los IACS y la cultura IT

Algunos de los principios básicos de la seguridad de los sistemas de información que son susceptibles de ser aplicados de manera selectiva y adecuada a la seguridad de los sistemas de control y automatización industrial (IACS). Como requisito previo para esta adaptación, es importante examinar las diferencias en la cultura, los requisitos y los problemas operativos entre los sistemas de automatización y control y los sistemas de IT. Las áreas críticas que deben abordarse incluyen la seguridad, las demandas en tiempo real, el mantenimiento, la productividad, la capacitación y la mentalidad del personal.

Analizaremos estos temas relacionados entre sí para ayudarnos a comprender mejor cómo aplicar los principios de seguridad a los sistemas de control y automatización sin afectar negativamente su misión principal y en pleno reconocimiento de sus requisitos especiales.

1.3.1. Diferencias en cultura, filosofía y requisitos

Los principales avances en la seguridad de los sistemas y redes informáticos se han producido a través de la ruta de la tecnología de los sistemas de información, con orígenes en la informática y la ingeniería de software. Los principales actores son los administradores de sistemas de IT, los analistas de sistemas, los administradores de bases de datos, los ingenieros de software, los administradores de redes, los directores de información (CIO), etc. Por otro lado, una gran parte del personal que puebla el campo de los sistemas de control y automatización industrial tiene experiencia en ingeniería, con capacitación en áreas tales como ingeniería eléctrica, ingeniería química, ingeniería mecánica e ingeniería de sistemas de control industrial.

La motivación, los requisitos y el enfoque de cada uno de los grupos son, en muchos casos y en gran medida divergentes, con algunas áreas comunes superpuestas. Por ejemplo, los métodos de mejora de procesos y calidad de software ampliamente utilizados en el entorno de IT a menudo son ajenos a los ingenieros de control y, de

hecho, pueden considerarse engorrosos a la hora de implementar un sistema SCADA y algoritmos al control de procesos. Además, el desempeño de un proceso en una planta es crítico y un desempeño inadecuado en las áreas de producción puede resultar en enormes pérdidas financieras, daños al equipo y lesiones al personal. Estas graves consecuencias de los errores operativos no suelen ocurrir con frecuencia en las instalaciones de IT.

Del mismo modo, la seguridad es una preocupación fundamental en un entorno de producción y, en algunos casos, el mal funcionamiento del sistema de control puede provocar incendios o explosiones, e incluso daños a las personas. Por lo tanto, en un entorno de producción, la seguridad y el rendimiento suelen tener prioridad sobre la seguridad de la información, lo que no es el caso en un sistema de IT.

La lección que se puede aprender de estas comparaciones es que el conocimiento y los métodos de seguridad de los sistemas de información tradicionales proporcionan una base sólida para abordar la automatización industrial y la seguridad del sistema de control, aunque con modificaciones apropiadas y necesarias para abordar las características únicas de los sistemas de automatización y control.

Un punto de partida importante para incorporar estas modificaciones es la formación y la concienciación. En general, la mayoría de las universidades y los programas de certificación que abordan la seguridad informática y de redes se han centrado en gran medida en la seguridad informática. Los sistemas de automatización y control, que normalmente se encontraban en redes aisladas y eran relativamente pocos en comparación con los sistemas de IT, no se han considerado objetivos interesantes. Con el advenimiento de la amenaza del ciberterrorismo, esta situación ya no es así. Además, los sistemas SCADA y de control de procesos de la planta se están conectando ahora a grandes redes corporativas e incluso a redes públicas como Internet.

El *Certified Information System Security Professional* (CISSP) y las certificaciones relacionadas no abordan la seguridad de los sistemas de control y automatización industrial. Existen organizaciones, como ISA, que han abordado este problema y están satisfaciendo una necesidad crítica; y NIST ha generado publicaciones especiales que abordan directamente los sistemas de control y automatización industrial como veremos en el tema correspondiente. Sin embargo, es importante que la capacitación en seguridad relacionada con el control de líneas de producción, procesos industriales, transmisión y distribución eléctrica, plantas químicas, etc., pase a primer plano en universidades, institutos técnicos, gobiernos y organismos de certificación.

Para comprender cómo adaptar los métodos de seguridad de IT a la automatización industrial y la seguridad del sistema de control, es necesario identificar y comprender las amenazas a este último. Un impedimento para la divulgación completa de las amenazas es el hecho de que la mayoría de las instalaciones afectadas son de propiedad privada y estas organizaciones son reacias a publicitar las brechas de seguridad que podrían afectar negativamente su reputación y a su valor en los mercados bursátiles.

Las organizaciones también necesitan incentivos para invertir en la actualización de su infraestructura de automatización y control. Muchas instalaciones existentes han

estado en funcionamiento durante 10 o 20 años, y las inversiones en seguridad tienen que competir con otras iniciativas convincentes en una organización. A veces es difícil justificar una inversión que no tiene un retorno de la inversión medible. Aunque con sufrir un único ciberincidente, la inversión ya estaría amortizada.

1.3.2. Consideraciones para adaptar los métodos de seguridad de IT a los IACS

Para asegurar un IACS, hay problemas específicos que deben abordarse y que tienen en cuenta las diferencias entre los sistemas de IT y los IACS. Estos problemas incluyen lo siguiente:

- La informática forense no ha madurado y no se ha implementado ampliamente en los IACS en comparación con los sistemas de IT.
- La conexión en serie a sistemas proporciona un medio para inyectar comandos maliciosos en una red de control.
- El exceso de comprobación, cifrado, vigilancia, etc., puede interferir con la naturaleza determinista de los sistemas de control de procesos.
- En muchos entornos de IACS, los ingenieros de control tienen múltiples responsabilidades que, en muchos casos, violan el principio de seguridad de separación de funciones.
- La instalación de parches y actualizaciones en los sistemas de control de procesos puede generar situaciones graves, y a veces peligrosas, en las instalaciones de producción.
- Las disciplinas de diseño del ciclo de vida comunes en el campo de las IT no se utilizan ampliamente en los sistemas de control y automatización industrial.
- Los atajos de mantenimiento y puertas traseras instaladas en los sistemas de control y automatización para el mantenimiento remoto pueden ser puntos de entrada fáciles para modificar software y firmware críticos con consecuencias negativas.
- Muchos proveedores de IACS combinan mecanismos de seguridad (*security*) con mecanismos de seguridad (*safety*), lo que genera puntos únicos de falla y menos resiliencia que separar estas dos funciones lógica y físicamente.
- Muchas instalaciones de fabricación e instalaciones SCADA albergan sistemas heredados con tecnología obsoleta, memoria y potencia informática mínimas, y poca atención a la seguridad.
- La exploración de puertos de los sistemas de control y automatización puede provocar bloqueos y falta de disponibilidad del sistema.
- El acceso remoto a los sistemas de control y automatización a través de módems más antiguos o dispositivos inalámbricos sin seguridad representa una seria amenaza para la seguridad.

- Existe una tendencia a aplicar los protocolos utilizados para los sistemas de IT a los sistemas de automatización y control industrial por su amplia disponibilidad, su menor costo y la existencia de personal capacitado. Sin embargo, en la mayoría de los casos, estos protocolos no fueron diseñados para sistemas de control de procesos deterministas y son vulnerables a muchos ataques existentes. Existe una gran dependencia de los proveedores que proporcionan software y hardware modificados para los IACS, lo que da como resultado implementaciones no estándar que son difíciles de mantener sin el apoyo de estos proveedores.

- Los mecanismos de autenticación débiles en muchos sistemas SCADA y sistemas de control de plantas en red los dejan vulnerables a los ataques.

Sin embargo, es importante examinar ahora algunas áreas temáticas críticas relacionadas para proporcionar una base para desarrollar soluciones de seguridad más específicas.

Las amenazas en IT y en los sistemas de control y automatización industrial provienen de diferentes fuentes con diferentes motivaciones. Es importante comprender estas fuentes de amenazas y sus características para contrarrestar cualquier actividad maliciosa de su parte.

Las categorías de terroristas, espionaje industrial y personas con información privilegiada son de particular interés en relación con los sistemas de control y automatización industrial. Tradicionalmente, las amenazas internas se han considerado una de las más peligrosas porque les dan a las personas internas la capacidad de eludir las medidas de protección. Sin embargo, las amenazas externas están aumentando y también son motivo de gran preocupación, en particular en relación con la infraestructura crítica y las plantas de procesamiento de recursos. Además, las amenazas a los sistemas de automatización pueden materializarse a partir de fuentes ambientales y estructurales.

1.3.3. Comparaciones del entorno IT y los IACS desde una perspectiva de estándares

Se puede obtener información valiosa sobre los contrastes y similitudes entre las áreas de enfoque de seguridad de los sistemas de IT y las de los sistemas de control y automatización industrial a partir de un ejemplo, utilizando estándares que representan cada una de las áreas. Como ejemplo podemos comparar dos documentos: ISO 27002, *Código de prácticas para la gestión de la seguridad de la información*, que se utilizará para representar las áreas de énfasis de seguridad de los sistemas de IT. Mientras que IEC 62443-2-1, *Seguridad para la industria Sistemas de control y automatización Parte 2-1: Establecimiento de un programa de seguridad de sistemas de control y automatización industrial*, se utilizará para ilustrar las principales preocupaciones de la seguridad del sistema de control y automatización.

En cada documento, hay áreas comunes abordadas por ambos estándares y otras áreas abordadas por un estándar y no por el otro.

Se desprende de los documentos que temas como la gestión de cambios, la seguridad del correo electrónico, las políticas de control de acceso, las firmas digitales, el cumplimiento y la planificación de la continuidad del negocio se encuentran entre las áreas consideradas críticas para los sistemas de IT que no se enfatizan en los estándares de los sistemas de control y automatización. Por el contrario, para los sistemas de automatización y control, los dominios importantes no cubiertos incluyen el análisis de la arquitectura de seguridad, el análisis cuantitativo y cualitativo, la gestión de la seguridad de la información y las pruebas de seguridad de la información. Las áreas de énfasis común incluyen la política de seguridad de la información, la evaluación de riesgos, la capacitación, la seguridad física de los medios, el acceso remoto, el registro de eventos y la protección contra el malware.

1.3.4. Conclusiones

Comprender los requisitos de seguridad de los sistemas de control y automatización industrial y cómo se relacionan con los sistemas de IT requiere un mapeo de estos requisitos con las tecnologías emergentes que se emplean en el control de los procesos de producción, así como la infraestructura crítica. Los avances en capacidad y sofisticación de los sistemas de control y automatización industrial requieren un enfoque de seguridad personalizado. Algunos de los factores que impulsan la seguridad de los sistemas de control y automatización industrial incluyen:

- La Smart Grid.
- Aplicaciones avanzadas de criptografía y gestión de claves.
- Sistemas de automatización avanzados.
- Relés de protección avanzada para sector eléctrico.
- Redes inalámbricas avanzadas, como 5G industrial.
- Procesamiento de alarmas.
- Disponibilidad de información energética en tiempo real.
- Seguridad entre sistemas de energía, transporte e IT.
- Redundancia en redes, equipos y sensores.
- La Industria 4.0.
- Digitalización de la industria.
- Internet de las Cosas (IoT).

Introducción a la ciberseguridad industrial

Resumen

En conclusión, la conectividad digital, como habilitador de la transformación digital de las corporaciones industriales, conlleva la aparición de nuevos riesgos que deben ser adecuadamente gestionados. Además, por las particularidades que encontramos en los sistemas de control industrial, estos riesgos deben ser gestionados de manera diferente a la que se gestiona en los entornos corporativos, utilizando estándares y mecanismos de protección diferentes. Aunque las amenazas sean las mismas, las consecuencias ante un ciberincidente son totalmente diferentes.

Referencias bibliográficas

IEC (International Electrotechnical Commission) and ISO (International Organization for Standardization). (2005). *Information Technology – Security Techniques – Code of Practices for Information Security Management*. ISO/IEC Standard 27002-2005. Suiza: Geneva 20.

ISA (International Society of Automation). (2009). *Security for Industrial Automation and Control Systems – Part 2-1: Establishing an Industrial Automation and Control Systems Security Program*. NC, Estados Unidos: Research Triangle Park.