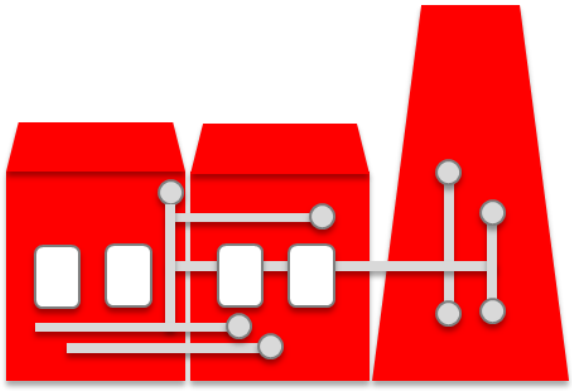
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

TEMA 1. INTRODUCCIÓN A LOS SISTEMAS DE CONTROL Y AUTOMATIZACIÓN Y A LA PROBLEMÁTICA DE SEGURIDAD ASOCIADA

1.2. Introducción a la problemática de seguridad



Curso avanzado de ciberseguridad en sistemas de control y automatización industrial

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1.2 INTRODUCCIÓN A LA PROBLEMÁTICA DE SEGURIDAD

1.2.1 Polisemia de la palabra "Seguridad" dentro del mundo de la industria

La palabra **seguridad** proviene de la palabra latina *securitas*. Nos podemos referir a la seguridad como la ausencia de riesgo o, también, a la falta de confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo al que haga referencia. Este problema nos surge cuando hablamos de seguridad dentro de los sistemas de control industrial.

En español traducimos como seguridad dos palabras diferentes provenientes del inglés: *Safety* y *Security*. Estas dos palabras son utilizadas dentro de los sistemas de control industrial para definir conceptos diferentes.

Figura 13. Safety vs. Security.

1.2.1.1 Safety

Se define la palabra inglesa *safety* como la condición de estar protegidos contra eventos accidentales: control de peligros naturales, accidentes, errores humanos, etc. Por lo tanto, debemos asociar la seguridad proveniente de *safety* con todas aquellas medidas que ayudan a evitar la ocurrencia de un accidente.

Así, dentro de los sistemas de control industrial se asocia la palabra *safety* con la prevención de daños a nivel de equipamiento, instalaciones, personas o la misma sociedad, que pudieran impactar accidentalmente en las actividades o elementos relacionados: operación, automatización, control y supervisión del proceso industrial.

Por ejemplo, los sistemas que utilizan tuberías para el transporte o distribución (sistemas de agua, gas…) disponen de mecanismos que detectan la presión dentro de las mismas para abrir válvulas de escape en casos de sobrepresión y, de esta forma, evitar la rotura de la canalización.

Otro ejemplo serían los detectores de falta de las líneas de distribución eléctrica. Estos sistemas comprueban que las líneas eléctricas tienen flujo de energía y, por lo tanto, las subestaciones están funcionando correctamente. Cuando el detector de falta detecta el fallo de suministro, se encarga de que la subestación quede alimentada por otra línea de distribución.

Tradicionalmente, las personas encargadas de la seguridad desde el punto de vista de *safety* han sido los ingenieros industriales y los ingenieros de control, ya que estos son los encargados de reducir el riesgo de accidentes y, como se ha visto anteriormente, las medidas de *safety* pueden estar basadas en sistemas electrónicos (*safety systems*) similares a los utilizados en el control, automatización y supervisión de procesos.

1.2.1.2 Security

El concepto *security* se puede definir como el grado de resistencia o de protección frente a daños intencionados. Se aplica a cualquier activo vulnerable y valioso, como una persona, vivienda, comunidad, nación u organización. En definitiva, *security* está relacionado con la prevención de eventos malintencionados, potencialmente dañinos como sabotajes, robos, ciberataques, etc., y abarca todas aquellas medidas específicas para prevenir un incidente malintencionado y mitigar los posibles daños.

En el ámbito de las organizaciones, la palabra *security* suele identificarse con los cuerpos de seguridad como policía, militares, seguridad privada, etc., que son los que han utilizado históricamente el término. Hoy en día también se asocia con los ingenieros informáticos para hablar de *information security* (seguridad de la información) o ciberseguridad, es decir, con la seguridad de los sistemas computacionales y del ciberespacio.

En los sistemas de automatización y control y los sistemas de información relacionados se hace uso del término *security,* tanto en el ámbito de la seguridad lógica, donde se utilizarían elementos como cortafuegos, antivirus, etc., como en el ámbito de la seguridad física, donde se utilizan cámaras de vigilancia, sensores de presencia, etc. para proteger estos mismos sistemas, las máquinas físicas y otras infraestructuras frente a ataques en el ámbito de lo físico.

1.2.2 Introducción a las vulnerabilidades comunes y factores de riesgo en los sistemas de control

Las vulnerabilidades comunes representan los problemas que más ampliamente se encuentran en los sistemas de control y automatización, mientras que los factores de riesgos potencian la probabilidad de explotar dichas vulnerabilidades.

De la relación entre las vulnerabilidades y los factores de riesgo pueden surgir los posibles ataques a los sistemas de control y automatización industrial.

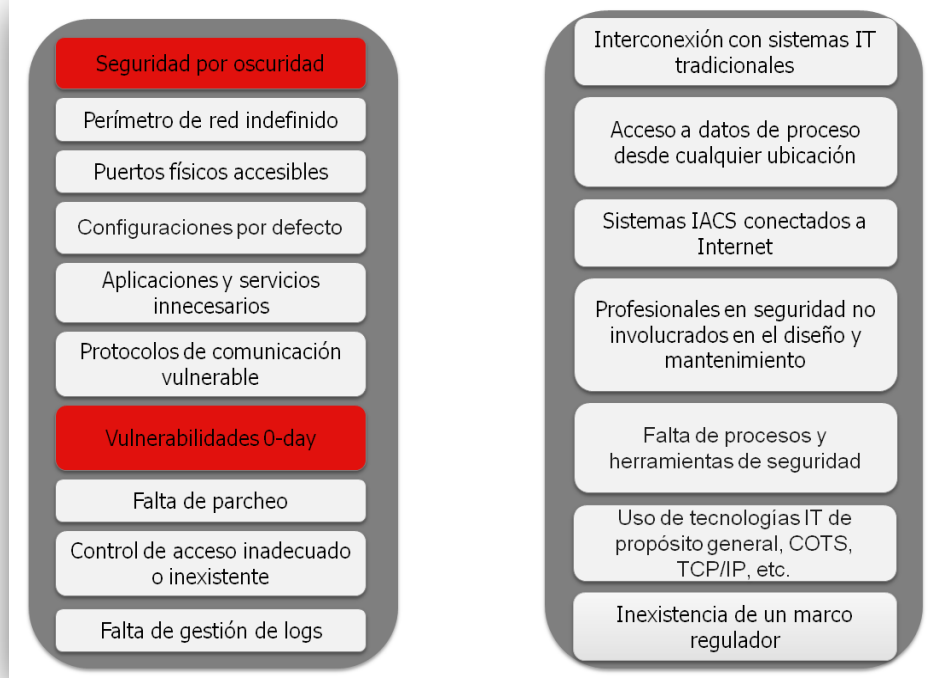


Figura 14. Relación seguridad por oscuridad – Vulnerabilidades de 0-Day.

La Figura 14 recoge la relación entre dos vulnerabilidades. La seguridad por oscuridad u ocultamiento, consistente en el profundo desconocimiento desde la perspectiva de seguridad del funcionamiento de muchas de las aplicaciones y protocolos que se utilizan en los sistemas de control y automatización. Esto ha venido motivado por el aislamiento en el que se ha trabajado con estos sistemas, tanto desde el punto de vista de la interconectividad con sistemas terceros como por el tipo de personal que los ha manipulado tradicionalmente. Esta seguridad por oscuridad ha derivado en la inexistencia de una comunidad que se dedique a realizar pruebas de forma continua sobre las aplicaciones y los protocolos industriales, y en consecuencia a la prevalencia de vulnerabilidades de tipo 0-day o sin parche para su corrección sobre estos sistemas.

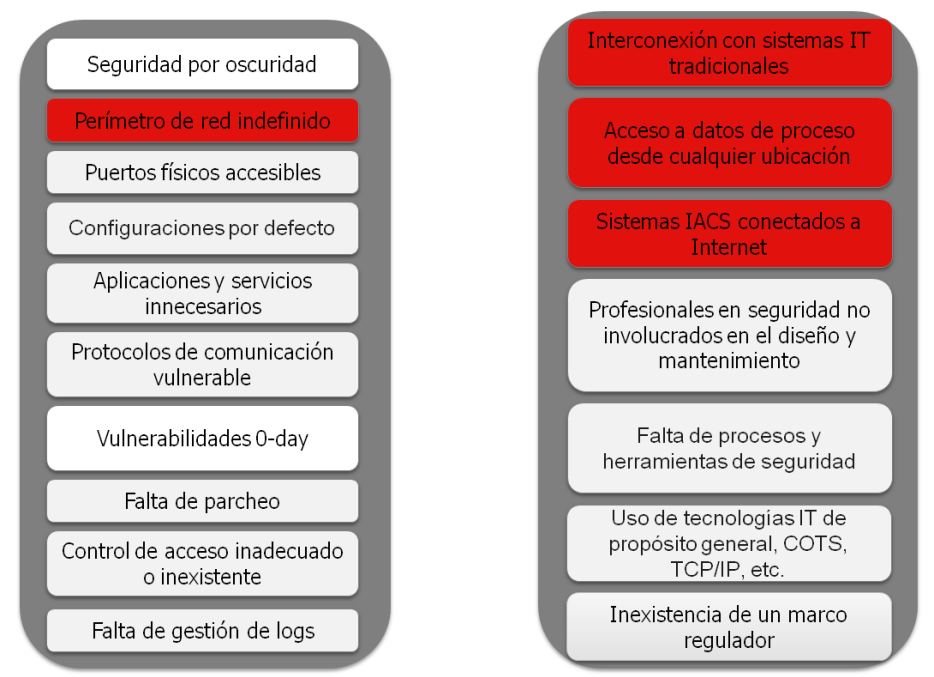


Figura 15. Problemas derivados de las interconexiones.

Si se juntan los factores de riesgos relacionados con la creciente interconexión de los sistemas de control y automatización con otros sistemas y el exterior, resulta en la potenciación de la vulnerabilidad de perímetro de red indefinido, como muestra la Figura . Los sistemas de control se conectan cada vez más con los sistemas IT tradicionales, ya que distintos aspectos de estos sistemas se controlan ahora desde la parte corporativa. Además, la información de estado de estos sistemas es requerida por más personas, desde empleados a altos directivos; y la variedad de soportes en los que se presenta va en aumento, equipos personales, teléfonos móviles, tabletas, etc. A esto se suma que, en la mayoría de los casos, los fabricantes se encuentran a miles de kilómetros de distancia y sin embargo han de realizar labores de mantenimiento y/o soporte. Esto suele motivar que estos sistemas se conecten a Internet, permitiendo estos accesos de forma económica para la empresa operadora. Todas esas conexiones hacen que el perímetro de los sistemas de control se desdibuje, en una clara contraposición a los sistemas de control y automatización clásicos donde todo estaba correctamente acotado y limitado.

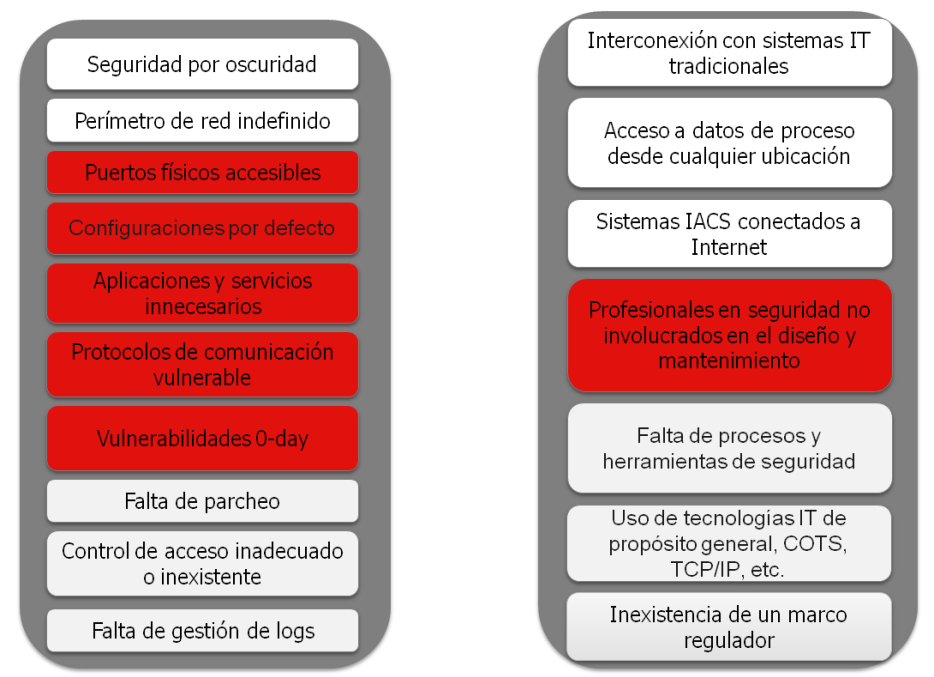


Figura 16. Relación entre la implicación de profesionales de seguridad y vulnerabilidades comunes.

En las fases de diseño y desarrollo de nuevos dispositivos y aplicaciones para los sistemas de control y automatización, los expertos en seguridad no han sido involucrados tradicionalmente, lo que ha favorecido la aparición de muchas vulnerabilidades, como muestra la Figura 16. La ausencia de estos profesionales implica que los sistemas se sigan diseñando pensando más en las funcionalidades operativas que en su seguridad, lo que se traduce habitualmente en deficiencias básicas; por ejemplo, la existencia de puertos físicos fácilmente accesibles que simplifiquen la operación pero sin la posibilidad de deshabilitarlos. También suele ser habitual la utilización de configuraciones genéricas para realizar un mantenimiento más simple, al configurarse de igual manera dispositivos análogos. Al igual que sucedía con los puertos físicos ocurre con los servicios y aplicaciones de los equipos, que no se aseguran ni se limitan a los estrictamente necesarios. A la hora de crear nuevos protocolos para los sistemas de control y automatización sigue primando la funcionalidad más que la seguridad, como han demostrado los nuevos protocolos creados en torno a las redes inteligentes, a los que no se les ha podido integrar seguridad por fallos en su especificación. En definitiva, todos estos problemas surgidos por una falta de personal de seguridad en los nuevos productos se traducen en la aparición de vulnerabilidades de tipo 0-day.

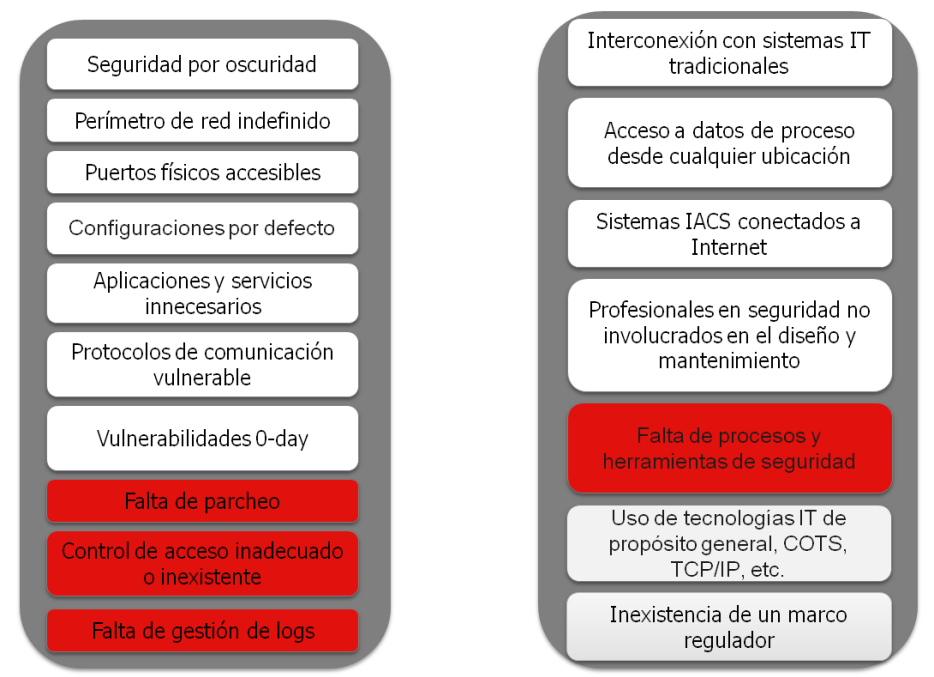


Figura 17. Problemas derivados de la falta de herramientas.

Los sistemas de control y automatización tradicionales estaban aislados, pero hoy en día sus relaciones con otros sistemas y procesos están creciendo de forma exponencial. Este rápido crecimiento implica que aún no existen todos los procesos organizativos y herramientas de seguridad específicas que ayuden a solucionar o mitigar las vulnerabilidades y deficiencias como las anteriormente descritas. Por ejemplo, la aplicación de parches en estos entornos no ha sido una práctica habitual, siguiéndose la máxima "si funciona, mejor no tocarlo". Anteriormente, cuando los sistemas estaban aislados el nivel de riesgo de esta mala praxis era inferior. Sin embargo, hoy en día, y debido a la creciente interconexión con otros sistemas corporativos, Internet, etc., es una cuestión fundamental a tener en cuenta. Algo similar ocurre con el control de acceso a estos sistemas. Tradicionalmente el acceso se realizaba en local desde las propias instalaciones, por lo que contar con una seguridad física adecuada era necesario. Hoy día sin embargo, los accesos se realizan desde cualquier ubicación, incluso utilizando Internet. Por otro lado, la gestión de logs y eventos de seguridad en estos entornos se ha limitado a eventos como "indisponibilidad de algún equipo telegestionado". Sin embargo, el registro de accesos y uso, cambios de configuraciones y otros eventos ha sido, y continúa siendo, prácticamente inexistente, en parte motivado por que muchos dispositivos no generan eventos útiles desde el punto de vista de la seguridad.

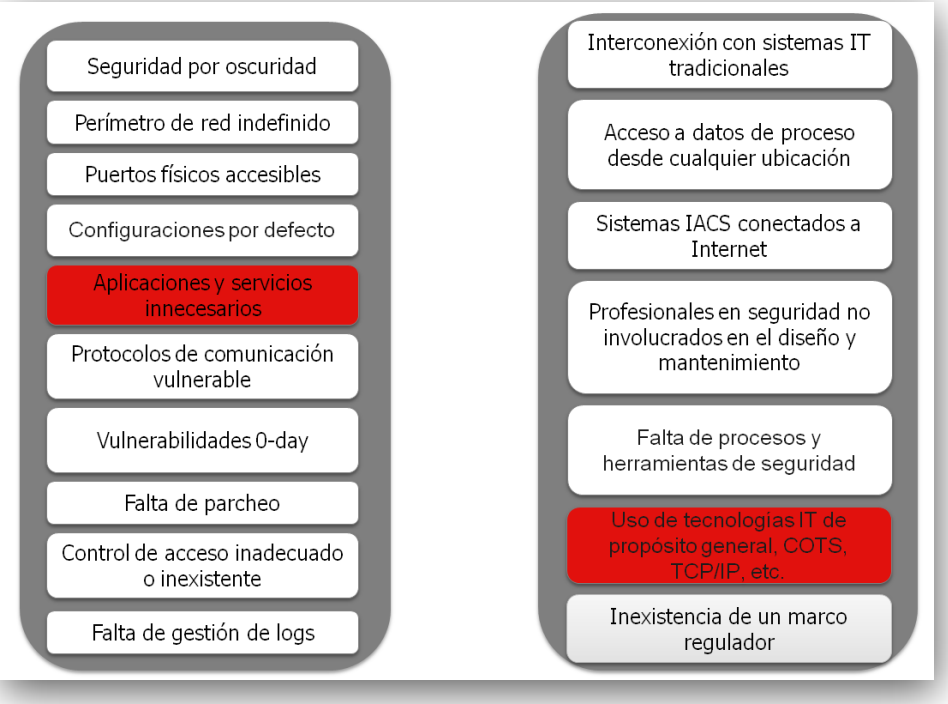


Figura 18. Relación entre uso de tecnologías IT y servicios innecesario en OT.

Tal como muestra la Figura 18, el uso cada vez más habitual dentro del ámbito industrial de tecnologías IT típicas de entornos corporativos, como el correo electrónico, el DNS, herramientas de mensajería instantánea, Ethernet, la pila TCP/IP, o sistemas operativos comerciales como Windows, suponen que los sistemas de control y automatización queden expuestos a ataques habituales contra estas tecnologías y los atacantes dispongan de múltiples herramientas en las que apoyarse.

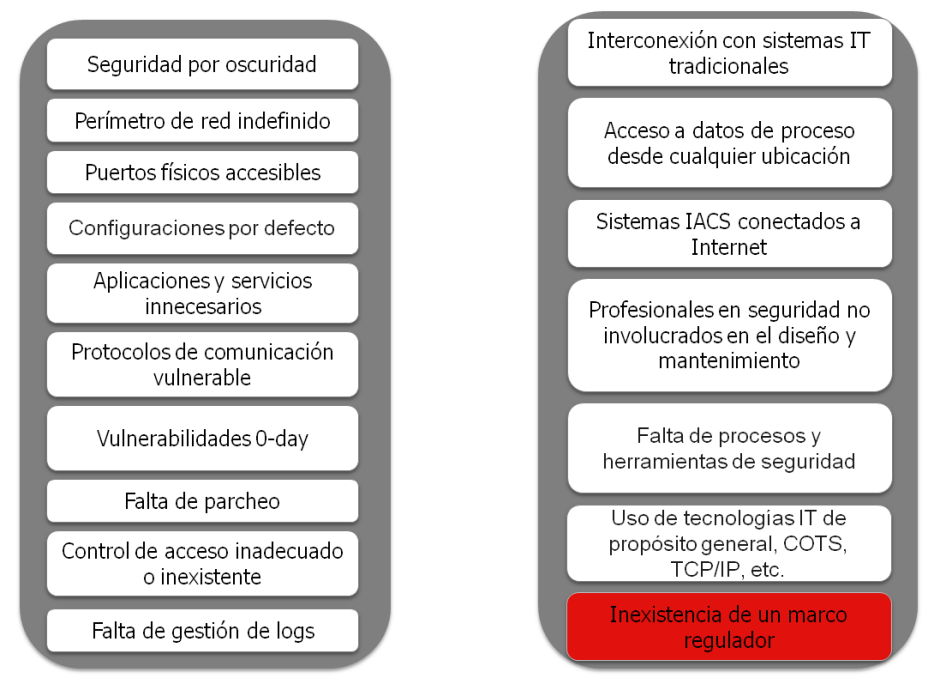


Figura 19. Falta de normativa.

Finalmente, la 19 refleja el riesgo que supone la inexistencia de un marco regulador que obligue específicamente al cumplimiento de ciertas medidas de seguridad dentro de los sistemas de control y automatización. Esto no favorece en absoluto la mejora de la seguridad de los mismos y hace que las vulnerabilidades tanto técnicas como organizativas sigan creciendo cada día.

1.2.3 Aproximación a la protección de los sistemas de control y automatización

La protección a nivel lógico de los sistemas de control y automatización frente a eventos de seguridad intencionados o accidentales viene limitada por un conjunto de restricciones que condicionan las técnicas y estrategias de protección a aplicar, debiendo ser éstas, a veces, distintas de las elegidas en la protección de los sistemas de información que se encuentran en el entorno corporativo o de oficina. Particularmente, su propia idiosincrasia les confiere características únicas con las que no cuentan los sistemas corporativos, aun a pesar de ser también sistemas informáticos. Adicionalmente, la naturaleza del proceso o actividad que controlan, o la del propio personal que los diseña y mantiene, impone también limitaciones relevantes a la hora de abordar su protección.

En cualquier caso, las medidas de protección que se van a aplicar en los sistemas de control y automatización van a aprovechar las herramientas, procesos y tecnologías de seguridad existente en el ámbito de TI, pero teniendo en cuanta que su aplicación a estos sistemas no puede ser directa por las características especificas que tienen estos entornos.

En este capítulo introductorio se van a mostrar algunas de las soluciones que se van a aplicar a los sistemas de control y automatización para su protección y las limitaciones en su utilización.

Una de las soluciones de seguridad que más se está integrando en los sistemas de control y automatización son los cortafuegos. Esta medida de seguridad se está utilizando tanto como solución de seguridad perimetral como en redes internas. Sin embargo, el uso de cortafuegos tradicionales viene limitado por su capacidad a la hora de interpretar los numerosos protocolos de telecontrol o telemedida, que son radicalmente distintos a los de los sistemas de TI habituales. Últimamente, ya están surgiendo soluciones de cortafuegos específicos para sistemas de control y automatización, que son capaces de comprender los protocolos industriales y, por tanto, ayudan a controlar mejor los flujos de comunicaciones.

Medidas complementarias a los cortafuegos, como IDS/IPS, también se están utilizando en los sistemas de control y automatización. La limitación de estas soluciones es similar al de los cortafuegos, ya que no comprenden muchos protocolos industriales. Además, el tiempo de análisis del tráfico, sobre todo en configuraciones in-line, puede incurrir en latencias no compatibles con la naturaleza de tiempo real de ciertos procesos industriales.

Siguiendo con la protección en las redes y las comunicaciones están las VPN de tipo Host-Host para asegurar las comunicaciones entre pares de dispositivos. La limitación en el uso de esta tecnología viene determinada por la cantidad de recursos computacionales que son necesarios en los procesos criptográficos, y que las hacen prácticamente inviables en la mayor parte de los dispositivos de automatización y control empotrados.

Las soluciones antivirus de los entornos de TI también son válidas en los sistemas de control y automatización, pero su uso se restringe a los sistemas, ya que los controladores y otros dispositivos empotrados no suelen utilizar sistemas operativos y aplicaciones comerciales que sean soportados por los antivirus. A esto se suman posibles sobrecargas durante el proceso de actualización de firmas y análisis de binarios, que pueden afectar al cumplimento con los parámetros de tiempo real. En relación con el proceso de actualización de firmas, la centralización del mismo también puede ser incompatible con ciertas buenas prácticas de filtrado, que impidan que las redes de control tengan acceso hasta consola central corporativa.

La última medida de protección de esta introducción son las auditorias técnicas de seguridad. Las auditorías técnicas de seguridad permiten conocer el estado de seguridad de un sistema, pero también suelen ser muy agresivas, llevándolos a veces a estados no controlados (p. ej. indisponibilidad). Estas consecuencias son inaceptables en un entorno de automatización y control, donde estos sistemas juegan un papel fundamental en el "core" del negocio. Es por ello que hay que buscar metodologías y técnicas de auditoría alternativas de riesgo nulo para los sistemas en producción

En el tema 6 se explicarán detalladamente los factores limitantes que afectan a la aplicación de herramientas y tecnologías de seguridad a los sistemas de control y automatización.

REFERENCIAS TÉCNICAS

Safety

http://en.wikipedia.org/wiki/Safety

Security

http://en.wikipedia.org/wiki/Security

Safety and Security in SCADA Systems Must be Improved through Resilience Based Risk Management. Stig O. Johnsen. 2013

Security vs. safety. Eirik Albrechtsen. 2003

GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480): SEGURIDAD EN SISTEMAS SCADA. Centro Criptológico Nacional. 2010.

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/480-SCADA/480-Seguridad_sistemas_SCADA-mar10.pdf

Ataque 0-day

http://en.wikipedia.org/wiki/Zero-day_attack

Logs

http://blog.s21sec.com/2009/11/logs.html

Guía para empresas: seguridad de los sistemas de monitorización y control de los procesos e infraestructuras (SCADA)

https://www.incibe.es/file/DqUev-29M3FtRjmJl-mD6A

ICS-CERT

https://ics-cert.us-cert.gov/

Safety and security

http://forum.wordreference.com/showthread.php?t=5489&langid=24

Seguridad: Safety o Security?

http://www.aena.es/csee/Satellite/SeguridadOperacionalNA/es/Page/1228215516978/1228215409300/

Buses de campo profibus y profinet

http://www.profibus.com

INSTITUTO NACIONAL DE CIBERSEGURIDAD