WHITE PAPER

Ciberseguridad y Seguridad de Procesos: Un enfoque integrador de la gestión de riesgos

Un nuevo mundo de interconectividad

Para muchos de nosotros, la interconectividad, la digitalización, los sistemas de control automático y otros avances tecnológicos impregnan tanto nuestro trabajo como nuestro ocio. Lo que quizá pasemos por alto es que las mismas herramientas que utilizamos a diario para "optimizar" nuestra vida privada también se han adaptado para optimizar los procesos industriales de todo tipo. Hoy en día, casi todas las plantas de proceso tienen sistemas de control industrial (SCI) integrados en los distintos niveles de digitalización de la empresa, desde los dispositivos de campo (instrumentos, actuadores, relés...) hasta los servidores corporativos de más alto nivel.

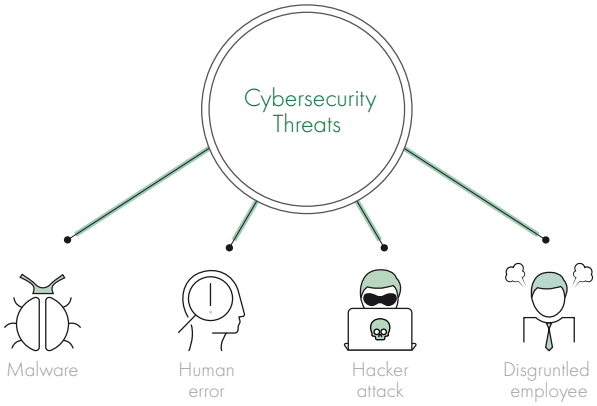
Estos sistemas pueden utilizarse para supervisar y controlar a distancia los lugares de trabajo, adquiriendo y transmitiendo datos sin necesidad de que el personal se desplace largas distancias. Los dispositivos que componen un SCI pueden abrir y cerrar válvulas y disyuntores, recoger datos de los sistemas de sensores y supervisar el entorno local. Dentro de una misma planta, un SCI puede controlar de forma centralizada las distintas fases de la producción, recopilar y compartir datos para acceder rápidamente a ellos y encontrar y remediar fallos reduciendo su impacto global. La eficiencia no es la única ventaja de un sistema automatizado. La salud y la seguridad de los trabajadores también se benefician de la capacidad de estos sistemas para detectar el peligro de forma rápida y fiable.

Sin embargo, ningún sistema es invulnerable. Todos hemos experimentado averías en la tecnología que utilizamos en nuestra vida personal. En un contexto industrial, un mal funcionamiento de la tecnología puede provocar pérdidas financieras, daños a los activos, consecuencias medioambientales e incluso lesiones a personas o pérdida de vidas. La escala de las consecuencias puede ser masiva y también puede ser el resultado de una actividad delictiva que tiene como objetivo las vulnerabilidades de estos cibersistemas automatizados y centralizados.

Enfrentarse a los inconvenientes de la digitalización

El alcance de los daños que pueden producirse cuando las organizaciones no establecen protecciones cibernéticas sólidas y resistentes es mucho mayor que el que puede sufrir un solo usuario individual de tecnología. Cuando una planta falla o tiene problemas financieros, cuando el aire o el agua se contaminan, o la salud y la seguridad de los empleados se ven comprometidas, los efectos son de gran alcance. Dado que es mucho lo que está en juego, los líderes de la industria deben entender que las ciberamenazas son tan potentes como los riesgos de seguridad a los que se han enfrentado tradicionalmente y que pueden, de hecho, secuestrar las medidas de seguridad convencionales que han puesto en marcha. Las alarmas pueden desactivarse de forma centralizada, los controles pueden manipularse, las señales en las que confían los trabajadores para garantizar la seguridad son vulnerables a la manipulación en la era cibernética.

El error humano, culpable de muchos accidentes industriales, sigue desempeñando un papel en los desastres relacionados con la informática. Los empleados o contratistas pueden conectar inadvertidamente una máquina infectada al sistema, conectarse a una red no segura, descargar el programa equivocado o instalar un malware. La novedad es el aumento del potencial de los ataques a distancia. Un empleado descontento que conozca el sistema puede estar motivado por la venganza. Los piratas informáticos pueden entrar en la red para obtener beneficios económicos o políticos. Los que buscan una ventaja competitiva pueden robar secretos o paralizar la producción. Otros ciberdelincuentes pueden querer interrumpir las infraestructuras críticas, desde las centrales nucleares hasta el suministro de agua o las redes eléctricas. Ya sea a pequeña o gran escala, simple o sofisticada, los riesgos que plantea el avance de la tecnología exigen la atención de los líderes de la industria.



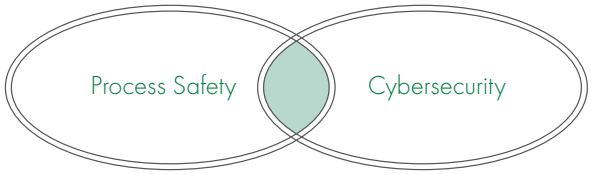
En este contexto, las autoridades de seguridad plantean dos preguntas principales a sus clientes y socios industriales. En primer lugar, si se produce un ciberataque, ¿qué medidas de seguridad lo impiden? En segundo lugar, cuando un ciberataque tiene éxito, ¿cuál es el riesgo final para las personas?
DEKRA puede ayudar ampliamente en ambas cuestiones, pero es importante destacar la diferencia esencial entre ellas: una se ocupa de la prevención de ataques y la otra identifica los riesgos finales no deseados para las personas.

Los hackers (piratas informáticos) son noticia

Durante 2018, los hackers han acaparado los mayores titulares con ataques a instituciones financieras y políticas, pero las infraestructuras también han sido víctimas. Además del sonado asalto al Servicio Nacional de Salud Británico en abril, un ciberataque accedió a las redes eléctricas estadounidenses durante el verano. No se registraron daños, pero los autores pudieron obtener información vital que podría utilizarse para infligir mayores daños en el futuro.
Hasta ahora, los resultados de la mayoría de los casos publicados de ciberataques dirigidos a la industria se han limitado a los daños económicos. En 2017, el virus petya estuvo detrás de una caída del 3% en las cifras de ventas trimestrales de una gran empresa y supuso una pérdida de 110 millones de libras para otra compañía.
Sin embargo, es fácil imaginar resultados mucho peores. Los espías corporativos podrían aprovechar las debilidades de la red para robar secretos, sabotear la producción e infligir daños duraderos a los competidores. Los terroristas podrían atacar las plantas que utilizan sustancias peligrosas como parte de un ataque a la población civil, causando explosiones, contaminando el aire o los suministros de agua y cobrando vidas humanas. No es un riesgo que merezca la pena correr. Requieren un análisis sistemático y una respuesta proporcionada.

Ciberprotección con herramientas de Seguridad de Procesos

Por muy aterradores que sean estos escenarios, es importante darse cuenta de que la industria puede aprovechar muchas de las herramientas que ya emplea como parte de la gestión de la Seguridad de Procesos en la lucha contra las ciberamenazas. Tanto la Seguridad de Procesos como la ciberseguridad tienen como objetivo prevenir o mitigar los eventos que implican una pérdida de control de los materiales peligrosos y las fuentes de energía. Reconocer y aprovechar este solapamiento es clave a la hora de crear ciberdefensas sólidas.
El enfoque basado en el riesgo que constituye el núcleo del ciclo



de vida de la seguridad de los procesos puede aplicarse con éxito a la ciberseguridad en el contexto de los procesos industriales. Los marcos de medición de riesgos utilizados tradicionalmente en la Seguridad de Procesos funcionan igualmente bien para la ciberseguridad. Al mismo tiempo, cada disciplina tiene un ciclo de vida distinto que requiere una gestión continua, y cada una afecta a aspectos múltiples y superpuestos de los procesos industriales.

Una fórmula para calcular los riesgos

El principio general utilizado en la seguridad de los procesos para evaluar el riesgo puede aplicarse universalmente, dondequiera que se produzcan situaciones peligrosas. Esencialmente, el nivel de riesgo es un producto de las consecuencias producidas por el peligro multiplicado por la probabilidad de que esas consecuencias se produzcan.

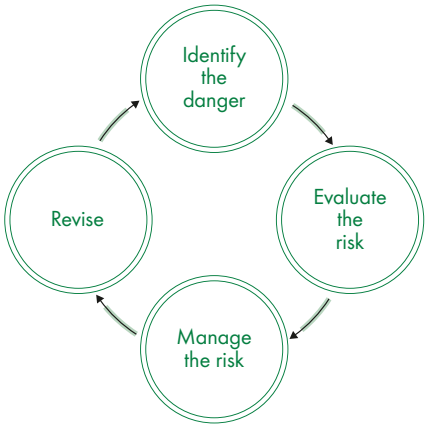
Risk = Consequences + Probability

En un contexto cibernético, tal vez el peligro sea que los sensores utilizados para indicar los niveles peligrosos de ciertas sustancias se desactiven como resultado de la piratería informática, el mal funcionamiento técnico o un error del usuario. Las consecuencias podrían ser daños en la maquinaria u otros equipos o incluso lesiones del personal. En el peor de los casos, podría producirse una explosión que causara lesiones o la muerte de personas y liberara toxinas en el medio ambiente. Las consecuencias variarían, por supuesto, en función de las particularidades de la planta en cuestión, al igual que el tercer elemento, la probabilidad. Se refiere a la probabilidad de que se produzca un incidente. En la seguridad de los procesos, se trata de un número real que va de 0 a 1. Si un suceso es casi seguro, la probabilidad asignada se acerca a 1; si es prácticamente imposible, casi 0.

El ejemplo anterior demuestra la complejidad de los riesgos industriales y subraya la importancia de la cooperación entre los equipos de EHS, IT y operaciones a la hora de enfrentarse a las ciberamenazas. Ya no hay líneas de demarcación bien definidas entre estas divisiones: el éxito de una de ellas en la lucha contra los peligros depende de las otras.

Interconectividad significa interdependencia

El ciclo de vida de la Seguridad de Procesos se suele conceptualizar como cuatro fases que se repiten continuamente.



Sin embargo, la simplicidad del gráfico desmiente la complejidad de la tarea. Por ejemplo, la identificación de peligros tiene que ir más allá de lo superficial para ser eficaz, y esto requiere experiencia y conocimientos. La gestión actual de la seguridad de los procesos utiliza herramientas como HAZID, HAZOP, CHAZOP y FMEA para facilitar este paso, y estas herramientas exigen la aportación de profesionales con un profundo conocimiento de los procesos en cuestión. Cuando los procesos se automatizan o digitalizan, no sólo los responsables de salud y seguridad y los supervisores de operaciones deben tener un lugar en la mesa, sino también los expertos en cibernética. DEKRA integra activamente las evaluaciones.

Lo mismo ocurre con la segunda fase, la evaluación del riesgo. También en este caso, los especialistas en seguridad de procesos han desarrollado instrumentos como el SIL y el LOPA para evaluar el riesgo, que pueden adaptarse para su uso en un contexto cibernético, a fin de garantizar la independencia adecuada, tal como exige la norma. Para evaluar la resistencia de una red cibernética a los ataques, es necesario investigar sus puntos débiles y de acceso. Las herramientas de seguridad de procesos pueden ayudar en estos esfuerzos.

Gestionar los riesgos significa reducir su impacto y frecuencia. Una vez más, la cooperación entre disciplinas es esencial para una gestión eficaz de los riesgos, ya que los procesos industriales están cada vez más entrelazados con las redes cibernéticas. Las soluciones diseñadas por equipos interdisciplinares procedentes de EHS, operaciones y IT serán sin duda más sólidas frente a los nuevos peligros tecnológicos que los enfoques monodisciplinares.

La fase final, de revisión o examen, puede incluir auditorías, programas de formación, investigación de accidentes y otras formas de consolidación. Impulsa el ciclo de vida a medida que sale a la luz nueva información sobre puntos ciegos internos o desarrollos y avances externos. Con los rápidos cambios que se están produciendo en la tecnología, este es un paso especialmente importante para un sistema de ciberseguridad sólido y resistente.

El HAZOP con un giro cibernético se convierte en una evaluación de ciberseguridad

Una de las herramientas más populares de Evaluación de Riesgos del Proceso (PHA) utilizada para identificar los riesgos (fase 1 del ciclo de vida de la seguridad del proceso) es el estudio de Peligros y Operabilidad (HAZOP). DEKRA utiliza el conocido enfoque y estilo HAZOP para crear una evaluación de ciberseguridad del proceso. Esta evaluación no sólo analiza las causas, sino también las salvaguardas contra determinados peligros. Presta especial atención a la independencia de las salvaguardas en cuanto a su vulnerabilidad a los ciberataques, así como a la identificación del riesgo final para las personas.

En primer lugar, nuestra evaluación de la ciberseguridad examina la causa de un determinado escenario, o los factores que contribuyen a una desviación de los procesos normales. Por ejemplo, si un peligro surge de un fallo tecnológico que afecta al bucle de control de temperatura automatizado de un reactor, la causa de este peligro se considera vulnerable a un ciberataque. Por el contrario, si un error humano provoca una carga incorrecta de catalizador en el reactor, la causa no es vulnerable a la cibermanipulación.

Nuestra evaluación de la ciberseguridad también tiene en cuenta las diferentes salvaguardas existentes para garantizar el funcionamiento normal, evaluando cada una de ellas por separado. Una salvaguarda es cualquier mecanismo destinado a evitar accidentes o a limitar los daños en caso de que se produzca un incidente. Una alarma de alta presión automatizada es un tipo de salvaguarda vulnerable a los ataques de los ciberdelincuentes, mientras que una válvula de alivio de presión o un disco de ruptura no lo son. En una situación de ciberataque, las pantallas en las que confían los operadores pueden ser manipuladas para ocultar el ataque real. Las alarmas requieren la acción del operador, y no sólo podría ser falsa la propia alarma, sino que el estado de la planta de proceso también podría ser inexacto. Por tanto, los sistemas de alarma son muy vulnerables a los ciberataques.

Si tanto las causas como las salvaguardas son vulnerables a los ciberataques, y no hay medidas de seguridad disponibles que sean resistentes a dichos ataques, entonces nuestra evaluación de la ciberseguridad de DEKRA se centra en las consecuencias. Daños potenciales para las personas y el medio ambiente. Cualquiera puede optar por incluir la evaluación del riesgo de un ciberataque sobre la producción, los activos y la reputación. En función de la gravedad de las consecuencias, puede determinarse el correspondiente nivel de seguridad (SL) utilizando las dos normas de la IEC que son normas europeas: EN 62443 y EN 61511.

Llegados a este punto, la evaluación de la ciberseguridad ha alcanzado su objetivo: la identificación de los posibles peligros y problemas operativos, en este caso los que pueden provocar un ciberataque. El mismo informe enumera todas las salvaguardas disponibles de acuerdo con la menor vulnerabilidad a los ataques. La generación y el diseño de las soluciones adecuadas tiene lugar en las fases posteriores del ciclo de vida de la Seguridad de Procesos.

Avanzando: Gestión integrada de la Seguridad de Procesos

Los sistemas de control industrial, al igual que las redes sociales y la banca en línea, son un hecho en la era digital. El reto es cómo aprovechar las ventajas y minimizar los riesgos. Hemos visto cómo la industria puede ampliar las metodologías probadas de Seguridad de Procesos para reforzar la resistencia a los ciberataques. De hecho, los riesgos cibernéticos pueden integrarse fácilmente en los análisis de peligros de procesos (PHA) de forma que se evite la duplicación innecesaria de esfuerzos o gastos. Se trata de adaptar inteligentemente las herramientas de PS existentes y reconocer la interdependencia de las IT, EHS y las preocupaciones operativas.

Un equipo interdisciplinario experimentado puede gestionar eficazmente la Seguridad de Procesos convencionales y, al mismo tiempo, identificar y analizar los escenarios cuyas causas y salvaguardas son vulnerables a los ciberataques: el marco ya existe. Recurrir a la ayuda de terceros expertos en Seguridad de Procesos, como el equipo de DEKRA, puede facilitar la integración de una dimensión cibernética en los sistemas de gestión de la seguridad de las organizaciones. Entre las muchas incertidumbres que conlleva la digitalización, una cosa es cierta: la industria no puede permitirse el lujo de descuidar las cuestiones de ciberseguridad.

Consultoría DEKRA

Consultoría DEKRA combina la ciencia basada en la evidencia, la tecnología de vanguardia y la experiencia de renombre internacional para crear soluciones de seguridad innovadoras para hoy y mañana. Nuestro objetivo es liderar la transformación de la seguridad en el lugar de trabajo y las prácticas empresariales, dentro de las operaciones y los procesos, así como en la dinámica y rápidamente cambiante era digital.

¿Desea obtener más información?

Contáctanos

DEKRA