



DATASHEET

¿Está tu planta a salvo de ciberataques?

La digitalización, los sistemas de control automático y otras innovaciones tecnológicas se utilizan habitualmente para optimizar las plantas de procesos industriales. Estos sistemas de control industrial (ICS) pueden utilizarse para optimizar la eficiencia y la producción.

Sin embargo, estos mismos sistemas diseñados para optimizar los procesos son tan vulnerables como cualquier otro sistema digital. Un ciberataque puede acarrear consecuencias medioambientales, así como lesiones o incluso víctimas mortales, y no sólo pérdidas económicas. La escala de las consecuencias puede ser sustancial y a menudo es el resultado de una actividad delictiva que tiene como objetivo las vulnerabilidades de estos sistemas automatizados. El alcance de los daños que pueden producirse cuando las organizaciones no establecen protecciones cibernéticas sólidas puede ser considerable. Estos daños pueden ser financieros, de contaminación tanto al aire o al agua, de peligro a la salud y seguridad de los empleados, etc. Dichos efectos pueden llegar a ser de muy largo alcance.

Dados los riesgos y las consecuencias subsiguientes, las organizaciones deben comprender que las ciberamenazas son tan importantes como los riesgos de seguridad “tradicionales”, y que los ciberataques pueden manipular las medidas de seguridad convencionales que han implantado en el proceso. Las alarmas pueden desactivarse, los controles pueden manipularse y las señales en las que confían los trabajadores para garantizar la seguridad son vulnerables a la manipulación mediante ciberataques.

Importancia de la ciberseguridad y la protección

Históricamente, los principales medios de comunicación se han centrado en la protección de los ordenadores, las redes informáticas y las transmisiones de datos. Sin embargo, dado que los ICS son igual de vulnerables a los ciberataques, las consecuencias pueden ser mucho más devastadoras que la violación de datos personales de la que se suele informar. Por lo tanto, las organizaciones necesitan barreras que sean completamente autónomas, junto con barreras para proteger la transmisión de datos.

A la hora de considerar la posibilidad y las consecuencias de un ciberataque a una planta, una parte importante de cualquier trabajo de evaluación de riesgos cibernéticos debe consistir en estudiar cómo poner las cosas fuera de alcance:

- > ¿Has identificado las áreas vulnerables a los ciberataques?
- > ¿Has identificado los accidentes graves que podría causar un ciberataque?
- > ¿Dispones de salvaguardas claramente definidas que requieran controles (ciberseguridad) para impedir el acceso remoto?
- > ¿Dónde están sus barreras independientes?
- > ¿Puedes responder con seguridad a las preguntas sobre salud, seguridad y medio ambiente?

Si no puedes responder positivamente a las preguntas anteriores, la ciberseguridad de su planta debe ser de máxima prioridad, dados los resultados potencialmente devastadores de un ataque.

DEKRA Cybersafe PS

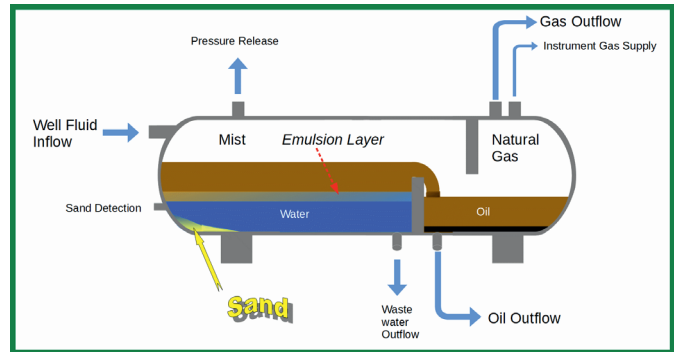
Los principales puntos a tener en cuenta a la hora de evaluar el riesgo de ciberataque son:

- > La necesidad de establecer los Riesgos de Accidentes Graves (Major Accident Hazards) que podría provocar un ciberataque;
- > La obligación de destacar todas las salvaguardas y barreras válidas que impidan tal devastación;
- > La necesidad de elaborar una lista de todas las salvaguardas independientes ciber-críticas;
- > La necesidad de elaborar un listado de todos los Riesgos de Accidentes Graves (MAH) para los que no existen salvaguardas independientes y para los que se debe confiar únicamente en los sistemas de protección informática.

La solución Cyber SafePS de DEKRA ha sido diseñada para identificar los riesgos de ciberseguridad para la planta; destacar los diferentes tipos de salvaguardas, desde las vulnerables, hasta las aceptablemente seguras y robustas; permitir identificar las consecuencias potenciales; permitir a las organizaciones determinar soluciones efectivas. Nuestra evaluación Cyber SafePS identifica todas las barreras contra los ciberataques que son realmente independientes y guía a los clientes a través de la protección de las personas, el medio ambiente y los activos.

Entender el concepto

Casi todas las plataformas marinas tienen un separador de petróleo, gas y agua; la arena y los residuos del agua de mar se separan y se eliminan, dejando el gas y el petróleo para pasar a la planta de procesamiento.



En el ejemplo anterior, los posibles Riesgos de Accidentes Graves son:

- > El ciberataque podría cerrar las válvulas e impedir la extracción del líquido residual; el líquido llena el recipiente, lo bloquea y, de repente, todo el petróleo y el gas de la planta se detienen.
- > El ciberataque cierra la válvula anterior a la válvula de alivio de presión utilizada para liberar la presión; a alta presión, el recipiente podría romperse y explotar.
- > El ciberataque detiene el lavado de la arena, lo que permite que la arena permanezca con el petróleo.

Cada Riesgo de Accidente Grave cuenta con barreras y salvaguardas para prevenir accidentes y garantizar la seguridad. En el ejemplo, al hacer que la válvula situada debajo de la válvula de alivio de presión sea una de tipo manual, se evita el ciberataque al no poder accionarse desde la autopista del sistema de control.

Este enfoque es similar a la funcionalidad de los cortafuegos y sistemas de software que detienen los ciberataques. El ejemplo demuestra que las protecciones pueden ser sencillas; es posible que las presiones de las tuberías y los recipientes puedan ser ahora protecciones adicionales. Sin embargo, las plantas deben asegurarse de que haya diversidad de barreras para que ningún MAH dependa de una sola barrera; diversidad de salvaguardas = no sólo UNA barrera.

El sistema Cyber SafePS de DEKRA realiza el análisis, destacando el nivel de diversidad y defensa en profundidad que tienes en tu planta de procesos y muestra lo que debe identificarse como barreras y salvaguardas ciber-críticas. La solución también muestra automáticamente qué barreras ciber-críticas deben tener una alta integridad (clasificación SIL), además de proporcionarte el sencillo diagrama de red que exigen las normas.

El enfoque de DEKRA garantiza el equilibrio adecuado entre las barreras independientes y la protección de ordenadores y autopistas de datos, y nuestros expertos evalúan los riesgos para elaborar un Informe de Evaluación Cibernética. Este incluye programas que aseguran la identificación de todas las salvaguardas críticas, proporcionando a los clientes defensa en profundidad y diversidad según lo requerido por el HSE.

DEKRA Process Safety

DEKRA Process Safety es una empresa de consultoría en seguridad de procesos. Trabajando en colaboración con nuestros clientes, nuestro enfoque consiste en evaluar la seguridad de los procesos e influir en la cultura y seguridad organizacional con el objetivo de marcar la diferencia.

Nuestro objetivo es ayudar a nuestros clientes a crear una cultura de la atención y una mejora sostenible y cuantificable de los resultados en materia de seguridad. La amplitud y profundidad de nuestra experiencia en seguridad de procesos nos convierte en especialistas reconocidos en todo el mundo y en asesores de confianza. Ayudamos a nuestros clientes a comprender y evaluar sus riesgos, y trabajamos juntos para desarrollar soluciones pragmáticas. Nuestro enfoque práctico y de valor añadido integra la gestión especializada de la seguridad de procesos, la ingeniería y los ensayos. En colaboración con nuestros clientes, combinamos la experiencia técnica con la pasión por la preservación de la vida, la reducción de daños y la protección de activos.

Somos una unidad de servicios de DEKRA SE, líder mundial en seguridad desde 1925, con más de 45.000 empleados en 60 países y cinco continentes. Como parte de la principal organización mundial de expertos DEKRA, somos el socio global para un mundo seguro.

Tenemos oficinas en Norteamérica, Europa y Asia.

Para más información, visita <https://www.dekra.es/es/seguridad-de-procesos/>

Para contactarnos: <https://www.dekra.es/es/formulario-contacto/>

¿Quieres más información?

Contáctanos