Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Alemania/Germany
www.pilz.com

Protección para empresas, máquinas y productos

Seguridad y Protección Industrial (Industrial Security): todo de un mismo proveedor

Ostfildern, octubre de 2025 - **Los incidentes de protección ya no solo afectan a los sistemas informáticos, sino cada vez más también al entorno de producción (OT). En el ámbito de la protección industrial se consideran incidentes tanto los ataques dirigidos como las manipulaciones inconscientes. El objetivo de la protección industrial en la producción es garantizar la disponibilidad de máquinas e instalaciones y la integridad y confidencialidad de los datos y procesos de las máquinas. Sin embargo, el principal objetivo de protección es la seguridad funcional. En última instancia, si las empresas no tienen soberanía sobre sus datos, están en juego la empresa y la seguridad de sus empleados: sin protección (Security) no hay seguridad (Safety) y sin seguridad no hay protección de las personas.**

En la UE se ha constatado esta situación de amenaza creciente y se ha adaptado la legislación en consecuencia: a nivel de las empresas, la **Directiva NIS 2** exige medidas para garantizar un alto nivel común de ciberseguridad en la Unión, por ejemplo, a través de un sistema de gestión de seguridad de la información.

El **Reglamento UE de Máquinas 2023/1230** establece ahora la protección contra manipulación de máquinas e instalaciones y exige medidas de protección industrial para las partes de máquinas que afectan a la seguridad funcional.

La **Ley de Ciberresiliencia (CRA)** exige medidas de protección para los productos con elementos digitales. Esto incluye controles,

sistemas E/S y diversos componentes que se montan en las máquinas.

Empresas, máquinas y productos: fabricantes y usuarios de máquinas deben afrontar retos y marcos jurídicos diferentes en cada uno de los niveles.

Seguridad de vanguardia

Independientemente de que la legislación convierta la protección industrial en un requisito obligatorio, hay una serie de buenas razones para abordar el tema y buscar asesoramiento en una fase temprana. Los procesos y condiciones establecidos para el funcionamiento de las máquinas pueden favorecer la manipulación si no se revisan periódicamente. La larga vida útil de muchas máquinas, por ejemplo, favorece en muchos casos la obsolescencia de los sistemas asociados y que llegue un momento en el que no correspondan a los estándares de protección actuales. Estos sistemas tienen brechas de seguridad que no se pueden cerrar porque el proveedor ha dejado de proporcionar actualizaciones de la protección. Muchas veces tampoco es posible implementar la protección contra software malicioso (malware) en los equipos terminales porque éstos han quedado obsoletos y podría afectar a su rendimiento, con el consiguiente riesgo de paradas de la producción.

Paso a paso hacia una mayor protección industrial

El objetivo es garantizar que las operaciones empresariales sigan estando protegidas, pero las empresas tienen que superar varios retos para lograrlo: desde la identificación de las normativas aplicables, la detección y solución de vulnerabilidades en los sistemas hasta la concienciación y formación de los empleados y posterior implantación de controles. Al ser la protección un "objetivo

móvil", se requiere además una verificación periódica del estado de protección industrial de la maquinaria. Es importante tener claras las responsabilidades dentro de la empresa y un planteamiento sistemático que incluya la adquisición de los conocimientos necesarios.

La empresa de automatización Pilz ha hecho suyos estos requisitos y preparado para fabricantes y usuarios de máquinas de todo el mundo una oferta de servicios que considera todos los aspectos relativos a la protección de personas y máquinas desde una perspectiva holística. Los expertos de Pilz conocen los requisitos legales y de normalización vigentes y los tienen en cuenta en su asesoramiento. La oferta se completa con cursos de formación que amplían o actualizan los conocimientos de protección en las empresas. La aplicación práctica se implementa también por medio de las soluciones de productos Pilz, como la gama Identification and Access Management - I.A.M. para más seguridad y protección industrial.

Sentar las bases adecuadas

Los especialistas en construcción de máquinas e instalaciones necesitan conocimientos básicos sólidos, sobre todo por lo que respecta a legislación y normativa aplicable, para garantizar la protección industrial (Industrial Security) en las propias máquinas. Los expertos de Pilz transmiten estos conocimientos en el curso de formación "Fundamentos de protección industrial (Industrial Security)". Los participantes se familiarizan con las amenazas para la protección, las medidas de protección adecuadas y las mejores prácticas en el contexto de la seguridad de máquinas y redes. Esto permite también a principiantes en el tema de la protección saber qué medidas pueden utilizar para proteger eficazmente las máquinas contra ciberataques y manipulación a nivel de producción.

A través de la cualificación "CESA - Certified Expert for Security in Automation", Pilz ofrece un curso de experto de dos días de duración que proporciona a los participantes conocimientos pormenorizados sobre protección según la normativa más reciente, especialmente en relación con la serie de normas IEC 62443 ("Redes de comunicación industriales - Seguridad TI para redes y sistemas"). A su vez, se abordarán medidas prácticas para la reducción de riesgos, como el control del acceso, el aumento de la seguridad de la red a través de medios técnicos, así como medidas organizativas para reducir los riesgos de protección. Los participantes aprenderán a aplicar correctamente la normativa y a demostrar que sus sistemas de automatización cumplen los requisitos de ciberseguridad. Una vez superado el examen, los participantes reciben el certificado "CESA - Certified Expert for Security in Automation" de TÜV NORD, reconocido en todo el mundo.

Llevar los conocimientos teóricos a la práctica

Sobre la base de los fundamentos teóricos y los cursos de formación, el siguiente paso para reforzar la protección industrial es la aplicación de procesos estructurados y orientados en la práctica. El asesoramiento en el campo de tecnología operativa (Operational Technology, OT) establece la transición de la base teórica a las estrategias realizables. A través de un procedimiento escalonado, los servicios de protección industrial identifican los puntos vulnerables de los sistemas complejos y desarrollan medidas para reducir los riesgos. El resultado es un concepto de seguridad holístico.

Cuatro pasos para una mayor protección industrial (Industrial Security)

El proceso de protección de OT comprende cuatro fases: análisis de los requisitos de protección, evaluación de riesgos de protección

industrial, concepto de protección industrial y verificación del sistema de protección industrial.

En el análisis de las necesidades de protección, la empresa estudia los requisitos de protección de cada uno de los "activos" de la máquina o instalación y sus objetivos de protección. En la siguiente fase de evaluación de riesgos se analizan los distintos riesgos y la probabilidad de que ocurran, teniendo en cuenta además todas las subsecciones y el ciclo de vida completo del sistema. El siguiente paso es crear un concepto detallado de protección industrial con estrategias y medidas de defensa y mitigación de los riesgos ocasionados por ataques, manipulaciones y manejo incorrecto. A esto se suma la definición de políticas, normas y directrices con el fin de asegurar la seguridad de funcionamiento y de diseño del sistema. En la última fase, la verificación del sistema de protección industrial, se comprueba la eficacia de las contramedidas implementadas.

Asegurar la disponibilidad de las máquinas

El proceso de los servicios de protección industrial ayuda a mitigar o evitar los ciberataques. Disminuye además el número de incidentes de protección de provocados de manera no intencionada. Esto, a su vez, aumenta la disponibilidad de la máquina y, en última instancia, reduce costes y asegura la rentabilidad.

Este enfoque protege con medidas de protección adecuadas principalmente a las personas que trabajan en la máquina. Porque un incidente de protección puede convertirse en un obstáculo para las medidas de seguridad. Una barrera fotoeléctrica instalada, por ejemplo, delante de la maquinaria garantiza tiene la misión de evitar que el operario entre en una zona peligrosa. Si un intruso puede influir en el control y el mecanismo correspondiente, no podrá

garantizarse la función de protección de la barrera fotoeléctrica de seguridad. Aquí, la protección protege la seguridad.

Por tanto, si hablamos de la implementación en la propia máquina, es ventajoso y conveniente considerar conjuntamente la seguridad y la protección. Y es que sin protección no hay seguridad y, sin seguridad, las personas quedan desprotegidas.

Regulación transparente: ¿quién puede hacer qué en la máquina?

La seguridad de una máquina y de sus operadores depende de la regulación del acceso, ya sea de personas o de redes. Los puntos de acceso deberán estar protegidos contra la entrada no autorizada, por ejemplo, para que no puedan permanecer personas en la zona peligrosa mientras la máquina esté en funcionamiento. Y es que incluso la operación o el mantenimiento bienintencionado de una instalación - ya sea in situ o a través de una red - pueden tener consecuencias fatales.

En este sentido es fundamental disponer de un Identification and Access Management (I.A.M.) como elemento que regule claramente los permisos y accesos a máquinas e instalaciones en la empresa. Esto incluye medidas organizativas y especificaciones, así como las funciones de seguridad pertinentes. Un sistema de autorización de acceso como PITreader de Pilz representa el componente de producto idóneo. Permite a los usuarios cumplir los requisitos de protección de trabajadores, responsabilidad civil, máxima productividad y protección de datos.

Solo un enfoque holístico de la seguridad y la protección puede garantizar una protección integral de las personas y las máquinas. El hecho de que una empresa adopte medidas de protección ya no es

una cuestión que queda a discreción de la empresa. Ahora es un requisito legal. En el sector de la construcción de máquinas, la protección industrial (Industrial Security) no es solo responsabilidad del Departamento de Informática, sino que debe ser un elemento integrado desde el diseño hasta la construcción. Implantar la protección a posteriori es laborioso y suele afectar a la facilidad de uso, la funcionalidad y la productividad.

((Caracteres: 9.784))

((Cuadro:))

Resumen de la legislación de la UE en materia de protección industrial (Industrial Security):

Sobre todo en Europa, los legisladores están respondiendo a la situación de amenaza con una serie de leyes. Tanto es así que Europa tiene la normativa más estricta del mundo en este ámbito. Pero la coordinación con otros países ya está en marcha, y esas leyes también llegarán allí. Por tanto, cabe esperar una uniformización de la protección industrial (Industrial Security) en todo el mundo.

NIS 2: más obligaciones para las empresas

La NIS (Seguridad de las redes y de la información) es una Directiva de la Unión Europea para reforzar la ciberseguridad. Esta directiva está en vigor desde 2016 y hasta ahora se aplicaba a los proveedores de servicios esenciales, como la energía, el transporte, la banca, las infraestructuras de los mercados financieros, el sector sanitario, el suministro y la distribución de agua potable y las

infraestructuras digitales. Los proveedores de estos sectores debían tomar "medidas de seguridad adecuadas" y notificar los incidentes graves de seguridad. La nueva Directiva NIS 2 ((UE) 2022/2555 ... sobre medidas para un alto nivel común de ciberseguridad en la Unión) obligará en el futuro a un número significativamente mayor de empresas a adoptar medidas de gestión de riesgos de ciberseguridad. La NIS 2 amplía los sectores e incluye, por ejemplo, la industria manufacturera/productora, incluidos los constructores de máquinas y los fabricantes de equipos eléctricos.

Se exigen análisis de riesgos y conceptos de seguridad para sistemas de información, así como la protección de la cadena de suministro y la seguridad del personal. Incluye también conceptos de control de acceso y la gestión de instalaciones, además de cursos de formación obligatorios para directivos.

La Directiva fue aprobada a finales de 2022 por el Parlamento Europeo y el Consejo de la UE. Como todas las Directivas UE, la NIS 2 no es directamente efectiva y vinculante en los distintos Estados miembros de la UE, sino que debe ser transpuesta a derecho nacional en cada Estado. Las empresas deberían preocuparse por cumplir la NIS 2 lo antes posible y llevar a cabo una evaluación completa de la protección de la empresa. Esto incluye, por ejemplo, el establecimiento de un sistema de gestión de la seguridad de la información (SGSI). En este contexto, resulta útil la certificación conforme a la norma de seguridad de la información ISO 27001.

Los aerogeneradores como ejemplo de aplicación de la NIS 2: los requisitos de la NIS 2 afectan también al sector de la construcción de máquinas, como los fabricantes de instalaciones para la generación de energía (por ejemplo, aerogeneradores). Por su parte, el fabricante del aerogenerador necesitará soluciones de

automatización, controles o sensores. Además, a partir de cierto tamaño, los fabricantes de componentes eléctricos también entran en el ámbito de aplicación de la NIS 2. Puesto que la NIS 2 establece que también hay que tener en cuenta a los proveedores, una empresa como Pilz deberá preocuparse por garantizar la seguridad de las cadenas de suministro y establecer requisitos para sus proveedores. Por tanto, la NIS 2 abarca toda la cadena de suministro.

El nuevo Reglamento de Máquinas: sin protección no hay Marcado CE

La Directiva de Máquinas 2006/42/CE reviste especial importancia en el contexto de la seguridad funcional de las máquinas.

Para poder importar máquinas en Europa, los fabricantes de máquinas siempre han tenido que realizar un procedimiento de evaluación de la conformidad y obtener el Marcado CE al final del proceso.

En junio de 2023 se publicó el nuevo Reglamento de Máquinas, que recoge las especificaciones adaptadas al estado actual de la técnica. Al tratarse de un reglamento, no es necesario transponerlo antes a la legislación nacional. Los fabricantes de máquinas tienen hasta el 20 de enero de 2027 para adecuarse a los nuevos requisitos, que deberán cumplir a partir de la fecha límite.

Este Reglamento de Máquinas sustituye a la anterior Directiva de máquinas y se diferencia de ella en que introduce la obligatoriedad de la ciberseguridad. Mientras la Directiva de Máquinas se limitaba a consideraciones sobre la seguridad, el Reglamento incluye el objetivo de protección industrial en el apartado "Protection against corruption"

(Protección contra la corrupción) de los "Essential health and safety requirements (EHSR)" (Requisitos esenciales de salud y seguridad): las funciones de seguridad de la máquina no deben verse mermadas por una falsificación involuntaria o deliberada.

Esta nueva vía para obtener el Marcado CE plantea una serie de problemas e interrogantes para los fabricantes y empresas usuarias de máquinas, que tendrán que revisar sus actuales conceptos de seguridad y protección.

Ley de Ciberresiliencia: protección en todo el ciclo de vida del producto

Además del análisis de la empresa y de las máquinas, es imprescindible implementar también medidas de protección directamente en los dispositivos (p. ej., controles). En septiembre de 2022, la Comisión Europea presentó un borrador de reglamento cuyo objetivo es aumentar la ciberseguridad de los productos. El "Cyber Resilience Act" (CRA) está dirigido a fabricantes de productos que contienen elementos digitales (hardware y software) diseñados para comunicarse con otros productos. Esto afecta tanto a los productos del segmento B2C, como los teléfonos inteligentes (smartphones) y robots aspiradores, como a los del segmento B2B, como controles y sensores, así como a productos de software puro, como sistemas operativos, o la propia máquina.

La obligación de los fabricantes de notificar las vulnerabilidades explotadas se aplicará a partir del 11/09/2026. A partir del 11/12/2027, los productos con elementos digitales tendrán que cumplir los requisitos del CRA para poder comercializarse en la UE.

La CRA es un Reglamento de la UE y, en consecuencia, será directamente aplicable en los Estados miembros de la UE

El impacto real del CRA dependerá de los criterios que se utilicen finalmente para clasificar los productos. Según el CRA, solo podrán comercializarse productos que garanticen un nivel adecuado de ciberseguridad, y esto durante el ciclo de vida completo de un producto. La protección comienza, por tanto, en la fase de desarrollo del producto. Hace ya algunos años que Pilz basa sus procesos de desarrollo también en la normativa IEC 62443-4-1 "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements", como demuestra el hecho de que SecurityBridge se ha desarrollado según criterios manifiestamente seguros.

((Caracteres: 6.062))

Pilz – The Spirit of Safety

Pilz es proveedor mundial de productos, sistemas y servicios de técnicas de automatización. Como pionero en automatización segura, Pilz garantiza la seguridad de las personas, de las máquinas y del medio ambiente. Además de la sede central en Ostfildern (Stuttgart), esta empresa familiar fundada en 1948 cuenta hoy con 2.500 empleados en 42 filiales y sucursales distribuidas por todos los continentes.

El líder tecnológico ofrece una gama de soluciones de automatización completas para seguridad (Safety) y protección industrial (Industrial Security) a pie de máquina. El abanico incluye sensores, tecnología de control y accionamiento y sistemas para comunicación, diagnóstico y visualización industrial. Una oferta internacional de servicios que incluye asesoramiento, ingeniería y cursos de formación que completan la oferta. Las soluciones de Pilz se emplean no solo en la construcción de máquinas e instalaciones, sino también en muchos otros sectores, como la intralogística, el embalaje, la tecnología ferroviaria y la robótica.

www.pilz.com

Pilz en las redes sociales:

En nuestros canales de redes sociales ofrecemos información general sobre la empresa y las personas que trabajan en Pilz e informamos sobre temas de actualidad del mundo de las técnicas de automatización.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contacto para la prensa:

Martin Kurth

Prensa corporativa y especializada
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Prensa corporativa y especializada
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Prensa especializada

Tel: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle

Prensa especializada

Tel.: +49 711 3409-7147
e.roessle@pilz.de