25.05.2023

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

Nota de prensa

Thomas Pilz: Seguridad y Protección para la automatización digital

Ostfildern, 25.05.2023 - **(vale la palabra hablada)**

Thomas Pilz

La seguridad llega ahora a la industria y a la fabricación de máquinas por ley.

Actualmente se está produciendo un profundo cambio en las normas y leyes de seguridad del sector industrial. Esta tendencia viene impulsada por el auge de temas como la protección y la inteligencia artificial (IA). Tanto en el ámbito de la industria en general como en el de la fabricación de máquinas e instalaciones en particular, hay tres nuevos requisitos legales relacionados con la protección, a saber: la Directiva NIS2 de la UE, el nuevo Reglamento de Máquinas y la Ley de Ciberresiliencia.
Al igual que en la conferencia de prensa del año pasado, hoy me centraré en el tema de la protección y les mostraré qué consecuencias tendrá para toda la industria.

NIS2: Más obligaciones y más sanciones para más empresas

NIS (Network and Information Security) 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 sucesora de esta directiva es la NIS2, que entró en vigor a principios de 2023 y que los Estados miembros de la UE deben haber transpuesto a su ordenamiento jurídico para otoño de 2024. Además, la nueva directiva afecta también a los sectores de la fabricación de máquinas y la automoción, entre otros; en concreto, se aplica a empresas con más de 50 empleados o un volumen anual de negocios superior a 10 millones de euros. Según la Asociación Alemana de Construcción de Máquinas e Instalaciones (VDMA, por sus siglas en alemán), esto afecta a unas 9000 empresas de toda Europa. En el futuro, estas empresas tendrán que demostrar que adoptan medidas técnicas, operativas y organizativas para protegerse contra los incidentes de seguridad. Esto incluye, en primer lugar, el análisis de riesgos de los sistemas existentes en entornos de producción, es decir, la tecnología operativa (TO). A continuación, se deben desarrollar e implantar procesos específicos, como la protección mediante contraseña o el cifrado, así como impartir formación a los empleados. Los incidentes de ciberseguridad deben notificarse a las autoridades competentes en un plazo de 24 horas. Otra novedad es la inclusión explícita de las cadenas de suministro. En resumen, la NIS2 afecta ahora a más empresas, amplía las obligaciones y prevé sanciones más estrictas. Las empresas que no tomen medidas se enfrentan a graves sanciones.

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

En septiembre de 2022, la Comisión Europea presentó un proyecto de reglamento cuyo objetivo es aumentar la ciberseguridad de los productos. En concreto, esta ley está dirigida a los fabricantes de productos con elementos digitales, lo que incluye tanto productos de hardware como de software (y firmware). Además, se aplica tanto a los productos de consumo como a los destinados a aplicaciones industriales, como los sistemas de control de máquinas. Según la Ley de Ciberresiliencia, a partir de ahora solo podrán comercializarse aquellos productos que garanticen un nivel adecuado de ciberseguridad. Además, los fabricantes están obligados a informar a los clientes sobre las deficiencias de seguridad lo antes posible y a subsanarlas. Por tanto, la normativa afecta a todo el ciclo de vida de un producto. Esto significa que ahora los fabricantes deberán ofrecer actualizaciones de software más allá del periodo de garantía habitual para protegerse de futuras amenazas. Esperamos que el reglamento se adopte para finales de 2024.

Nuevo Reglamento de Máquinas: la ciberseguridad como obligación

La tercera nueva normativa en materia de seguridad es el Reglamento de Máquinas de la UE, que se publicará próximamente. Al tratarse de un reglamento, no es necesario transponerlo antes a la legislación nacional. Los fabricantes de máquinas disponen de 42 meses para cumplir los nuevos requisitos. Este Reglamento de Máquinas sustituye a la anterior Directiva relativa a las máquinas y se diferencia de ella en que introduce la obligatoriedad de la ciberseguridad. Mientras que la anterior Directiva relativa a las máquinas se limitaba a mencionar la seguridad, el nuevo Reglamento incluye la protección de la seguridad como uno de sus objetivos en el apartado "Protection against corruption" (Protección contra la corrupción) de los "Essential health and safety requirements EHSR" (Requisitos básicos de seguridad y de protección de la salud). Además, establece que las funciones de seguridad de la máquina no deben verse perjudicadas por falsificaciones involuntarias o intencionadas. Hasta el momento, se sabe que el cumplimiento de la Ley de Ciberresiliencia conlleva una presunción de conformidad con el Reglamento de Máquinas.

Y ahora, la pregunta es: ¿quién tiene que ocuparse de qué?

¿Qué consecuencias tendrán estas nuevas normativas? Para ilustrar cómo se relacionan los sectores entre sí, utilizaré como ejemplo el de la generación de energía. Hasta ahora, la Directiva NIS solo había afectado al sector de la electricidad. Ahora, la nueva NIS2 afecta también al sector de la construcción de máquinas, como los fabricantes de equipos para generar energía (por ejemplo, aerogeneradores). A su vez, el fabricante del aerogenerador necesita soluciones de automatización, sistemas de mando o sensores, por ejemplo, de Pilz. Además, a partir de cierto tamaño, los fabricantes de componentes eléctricos también entran en el ámbito de aplicación de la NIS2. Y puesto que la NIS2 establece que también hay que tener en cuenta a los proveedores, una empresa como Pilz también debe preocuparse por garantizar la seguridad de las cadenas de suministro y establecer normas para sus proveedores. Por tanto, la NIS2 abarca toda la cadena de suministro.

Desde tiempos inmemoriales, los fabricantes de máquinas han tenido que someterse al procedimiento de evaluación de la conformidad para poder importar máquinas en Europa, al final del cual se obtiene el Marcado CE. Ahora, con el nuevo Reglamento, los fabricantes deben demostrar que sus máquinas también están protegidas contra la manipulación. Por último, el fabricante de los componentes eléctricos estará sujeto a las normas que establecerá la Ley de Ciberresiliencia.

En resumen, el hecho de que una empresa adopte medidas de seguridad ya no es una cuestión que queda a discreción de la empresa, sino que es una obligación establecida por ley. Ahora, las empresas deberían preocuparse por cumplir la NIS2 lo antes posible y llevar a cabo una evaluación completa de la seguridad de la empresa. Esto incluye, por ejemplo, el establecimiento de un sistema de gestión de la seguridad de la información (SGSI) con certificación ISO 27001.

En el sector de la construcción de máquinas, la protección industrial no es solo responsabilidad del Departamento de Informática, sino que debe ser un elemento integrado desde el diseño hasta la construcción. Implantar la seguridad a posteriori siempre lleva mucho tiempo y suele afectar a la facilidad de uso, la funcionalidad y la productividad. Cuando se trata de evaluar riesgos, no solo hay que tener en cuenta la seguridad, sino también la protección. Sin protección no hay marcado CE.

Y para los fabricantes de productos con elementos digitales, la serie de normas IEC 62443 ofrece una buena orientación. Por ejemplo, la norma IEC 62443-4-1 describe los requisitos para el proceso denominado "Security Development Lifecycle" (ciclo de vida de desarrollo de seguridad).

La UE se ha situado a la cabeza en materia de legislación de seguridad y Europa tendrá la normativa más estricta del mundo. Pero la coordinación con otros países ya está en marcha, y esas leyes también llegarán allí. Actualmente, Australia, por ejemplo, se mantiene en contacto con la UE y probablemente seguirá las normas europeas. Por tanto, cabe esperar una uniformización de la protección industrial en todo el mundo.

Thomas Pilz

Estándares de comunicación abiertos como tarea histórica

Los productos de Pilz se distinguen por su compatibilidad y por su facilidad de manejo. Nuestro objetivo es ofrecer productos que estén siempre a la última, que sean fáciles de manejar y que se puedan integrar en cualquier arquitectura de automatización.

Con SafetyBUS p, el primer sistema de bus de campo seguro, y con la Ethernet segura en tiempo real SafetyNET p, hemos dado forma al desarrollo de la comunicación industrial segura. Pero la era de las soluciones exclusivas para empresas ha terminado. Ahora nos comprometemos con todas nuestras fuerzas a crear estándares para toda la industria. ¡Estamos haciendo historia!

OPC UA

La industria se ha puesto de acuerdo en utilizar el protocolo de comunicación OPC UA (siglas en inglés de Open Platform Communications Unified Architecture, "arquitectura unificada de comunicaciones de plataforma abierta") para la conexión en red segura y genérica de instalaciones industriales. Este protocolo de comunicación proporciona una interfaz estandarizada (IEC 62541) para la comunicación entre distintas fuentes de datos en la industria. Como miembro de la OPC Foundation, los trabajadores de Pilz participan tanto en el consejo de dirección como en los equipos de trabajo técnicos del grupo Field Level Communication (FLC). La atención de Pilz se centra sobre todo en el grupo de trabajo que se ocupa del tema Safety, o seguridad (Safety over OPC UA).

En Pilz destacamos especialmente por nuestro conocimiento sobre el uso de la tecnología publisher-subscriber (pub/sub) en relación con los requisitos de los protocolos de bus de campo que funcionan con seguridad. Frente al modelo clásico de master/slave, el modelo pub/sub permite intercambiar datos directamente entre los participantes. Esto permite utilizar OPC UA incluso para tareas de automatización complejas y en instalaciones distribuidas. En Pilz somos especialistas en este ámbito, ya que nuestro SafetyNET p es el único sistema de bus de campo seguro basado en Ethernet que soporta pub/sub desde el principio.

Estamos avanzando a buen ritmo en nuestro trabajo sobre seguridad funcional. El grupo trabaja codo con codo con las autoridades verificadoras en la especificación prueba y los sistemas de prueba, así como en la certificación de pilas para OPC UA Safety. La versión 1.05 ya se ha lanzado.

IO-Link Safety
A nivel de sensores, la automatización ya ha dado un gran paso adelante en términos de flexibilidad. De hecho, el protocolo de comunicación IO-Link Safety está a punto de comercializarse. La comunicación punto a punto ofrece muchas ventajas, como la simplificación de la instalación (p. ej., a través de cableado estandarizado y la eliminación de cableados en paralelo), la parametrización automática con herramientas de ayuda y una mayor capacidad de diagnóstico.

Para poder utilizar IO-Link en tareas de automatización relativas a la seguridad, Pilz ha trabajado incansablemente dentro de la comunidad IO-Link para incorporar este protocolo junto con las pruebas y certificaciones asociadas. Varios expertos de Pilz dirigen los dos grupos de trabajo de IO-Link Safety (para marketing y tecnología).

Presentaremos los primeros sensores listos para el mercado en la SPS de noviembre. El objetivo de Pilz es ofrecer un sistema completo formado por sensores, accionadores y módulos Master. Esto facilita el uso del sistema por parte del cliente y aumenta el rendimiento.

Estamos convencidos de que, en el futuro, las soluciones de automatización se diferenciarán aún más por sus funcionalidades: ¿qué calidad tienen las interfaces de usuario, cuál es su facilidad de manejo y qué otras ventajas ofrecen? En este apartado existe un gran margen de innovación y potencial para nuevas aplicaciones.

Thomas Pilz
El futuro de la seguridad es dinámico
¿Qué implica una mayor digitalización para la protección de las personas y las máquinas? ¿Qué tecnologías cumplen los requisitos de seguridad? ¿Qué papel desempeñan las personas? Todos queremos saber qué nos deparará el futuro. Y lo primero de todo son buenas noticias: el ser humano será una pieza fundamental y su papel se verá incluso reforzado.

El ser humano como diseñador

Por ejemplo, en el proyecto "Fluide Produktion" (producción fluida) de la plataforma de investigación ARENA2036. Pilz trabaja con sus socios en el desarrollo y la aplicación de un concepto de producción ciberfísica centrado en el ser humano, especialmente para la producción de automóviles. El objetivo del proyecto es dividir las instalaciones de producción en módulos flexibles en cuanto a su ubicación para poder formar y desmontar unidades dinámicas en función de las necesidades. Los módulos se han diseñado centrándose en el papel del ser humano como diseñador activo de su entorno de producción.

De todos estos requerimientos nace la demanda de seguridad dinámica, es decir, una adaptación más flexible de las funciones de seguridad a los procesos de producción y los requisitos de protección asociados, que están en constante evolución. Esto permite, por ejemplo, que los robots o las plataformas móviles no tengan que desconectarse inmediatamente si una persona entra en el espacio de trabajo, sino que puedan seguir funcionando a una velocidad reducida (y, por tanto, menos peligrosa), o que incluso puedan ejecutar estrategias de evasión seguras. Las funciones de los controles se transferirán paulatinamente a sensores y accionadores inteligentes de sistemas distribuidos, que mejorarán la interacción entre los módulos de máquinas y entre personas y máquinas.

Seguridad en tiempo real

Las situaciones dinámicas de los futuros entornos de producción deben controlarse y autorizarse en tiempo real sin perder de vista la seguridad, de modo que la protección de las personas y las máquinas quede garantizada en todo momento. La expresión clave será "seguridad en tiempo real". Es posible que en el futuro haya diferentes máquinas —o activos en general— que compartan dispositivos de seguridad. Esto es lo que se conoce como "Shared Safety" (seguridad compartida), un concepto con el que estamos trabajando en la SmartFactory KL. En esta forma de concebir la seguridad, el clásico marcado CE como resultado de un procedimiento análogo de evaluación de la conformidad queda descartado. La información sobre todos los activos implicados debe estar disponible en tiempo de ejecución. Las palabras clave aquí son placa de características digital y capa de administración.

En el marco del proyecto "Fluide Produktion" (producción de fluidos) mencionado anteriormente, estamos trabajando otros temas de futuro, como la identificación de personas y objetos y, por tanto, la diferenciación entre ambos. Aquí es donde entra en juego el uso de la inteligencia artificial. Los algoritmos de IA pueden aprender a reconocer y evaluar los riesgos. En este sentido, el marcado CE constituye la protección básica. Pero pueden introducirse otras medidas para reducir al mínimo los riesgos, flexibilizar aún más la seguridad y aumentar la productividad.

Leyenda:

También encontrará textos e imágenes para descargar en www.pilz.com. Para acceder directamente a las páginas web pertinentes del centro de prensa, introduzca el siguiente código web en el campo de búsqueda de la página de inicio.: **237512**

Grupo Pilz

El grupo Pilz es un proveedor mundial de productos, sistemas y servicios de tecnología de automatización. En Ostfildern, la sede de esta empresa familiar, trabajan aproximadamente 2500 personas. Mediante las 42 filiales y sucursales que tiene en todo el mundo, Pilz vela por la seguridad de las personas, máquinas y medio ambiente. Este líder tecnológico ofrece soluciones completas de automatización que abarcan sensores, tecnología de control y accionamiento, incluyendo sistemas para la comunicación, el diagnóstico y la visualización industrial. Una oferta internacional de servicios que incluye asesoramiento, ingeniería y cursos de formación completa el programa. Las soluciones de Pilz se emplean no solo en la construcción de máquinas e instalaciones sino también en muchos otros sectores, como la energía eólica, la tecnología ferroviaria o la robótica.

www.pilz.com

Pilz en las redes sociales

En nuestros medios sociales ofrecemos información general relacionada con la empresa y las personas que trabajan en Pilz e informamos sobre los actuales desarrollos en el campo de la tecnología de automatización.

 https://www.facebook.com/pilzINT

 https://twitter.com/Pilz_INT

 https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

 https://www.linkedin.com/company/pilz

Contacto para la prensa

Martin Kurth
Prensa corporativa y especializada
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Prensa especializada
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de