

«Zones and Conduits» en las redes de automatización: la Security protege la Safety

La Safety es lo primero

Ostfildern, julio de 2026 – **El Reglamento de máquinas lo establece como obligatorio: la Industrial Security debe proteger las funciones relevantes para la seguridad frente a la manipulación; es decir, la protección (Security) es un requisito previo para el correcto funcionamiento de la seguridad funcional (Safety). Pero ¿cómo se puede proteger una red de automatización de forma integral? Normas como la IEC 62443-3-2 y la futura EN 50742 marcan el camino a seguir: segregar los sistemas en zonas y controlar las conexiones, un principio que se refleja en todas las recomendaciones actuales de asociaciones y expertos. Pilz está convencido de que la separación sistemática entre la Safety y la denominada automatización estándar es la clave para una seguridad eficaz de las máquinas, basada en el principio de «Defence-in-Depth» y aplicada mediante el enfoque de «Zones and Conduits» (zonas y canales de comunicación).**

Una casa puede estar construida de forma sólida y segura: con paredes resistentes, materiales ignífugos, una instalación eléctrica fiable y sistemas de alarma que funcionen correctamente. Esta seguridad estructural es un ejemplo de la Safety de las máquinas, en las que las contramedidas de diseño, los sensores y los mecanismos de protección tienen por objeto evitar riesgos no deseados. Sin embargo, una casa así solo seguirá siendo segura si no se producen intervenciones deliberadas. Los sistemas de control de calefacción

manipulados, los circuitos eléctricos saboteados o los sistemas de alarma desactivados pueden convertir un edificio, por muy seguro que sea su diseño, en un riesgo. Incluso en el ámbito de la maquinaria, el mejor diseño en materia de seguridad resulta ineficaz si se alteran o se desactivan sin autorización los componentes relevantes para la seguridad.

En este contexto, la Security asume el rol de protección exterior: puertas resistentes, accesos controlados, conexiones vigiladas y barreras contra intrusiones no deseadas. La Security no protege contra los accidentes en sí, sino contra la anulación de los mecanismos de protección, por ejemplo, por parte de personas que acceden mediante la selección no autorizada de modos de funcionamiento o mediante acciones no autorizadas. Solo así la Safety sigue siendo eficaz y fiable: «Security for Safety».

Desde los requisitos normativos hasta la propuesta de solución

El Reglamento de máquinas (UE) 2023/1230 convierte, por primera vez, la Security en requisito obligatorio para el correcto funcionamiento de la Safety en máquinas e instalaciones: las funciones de seguridad no deben verse afectadas por manipulaciones, ya sean intencionadas o no. A esto es precisamente a lo que se refiere la norma EN 50742, actualmente en fase de elaboración, que contribuirá a concretar los requisitos básicos de Security del Reglamento de máquinas. La norma define los detalles técnicos para la protección contra la corrupción y establece requisitos claros para el hardware, el software y los datos que pueden afectar a las funciones relevantes para la seguridad. La norma abarca todo el ciclo de vida, desde el desarrollo hasta la operación y la puesta fuera de servicio. Además, la serie de normas IEC 62443, ya existente, desempeña un rol fundamental, ya que describe la ciberseguridad

sistemática para los sistemas de automatización y control industrial. Ofrece un marco estructurado para el análisis de riesgos, la «Defence-in-Depth» y el principio de segmentación («Zones and Conduits»), y la norma EN 50742 la reconoce expresamente como un enfoque alternativo o complementario para la protección de la seguridad. En conjunto, estas normas constituyen el núcleo normativo de «Security for Safety»: exigen que la integridad digital de una máquina se considere un requisito previo para su seguridad funcional y se proteja en consecuencia.

Por qué «Zones and Conduits» aumenta la seguridad de las máquinas

Volviendo al esquema de la casa: la sala de calderas representa una zona, mientras que la conexión con el gateway de la casa inteligente representa la ruta de conexión correspondiente. Si se manipula esta conexión, se puede afectar a toda la instalación, incluso si la sala está perfectamente protegida. Por lo tanto, lo decisivo no es solo la protección de cada una de las zonas, sino también la seguridad de las conexiones que las unen. Es precisamente aquí donde entra en juego el principio de «Zones and Conduits». Las zonas se separan claramente entre sí y las transiciones entre ellas se diseñan de forma controlada. Al igual que en una casa, donde las puertas y las llaves asignadas determinan quién puede acceder a cada lugar, en una planta industrial la protección interna (Safety) y la protección externa contra la manipulación (Security) se complementan de forma estructurada.

De este modo se crea un concepto de protección que sigue el principio de «Defence-in-Depth»: la seguridad no se consigue mediante una única barrera, sino a través de varias capas de protección dispuestas en serie. Cuando se supera un obstáculo, la

siguiente resiste. Las zonas conforman estos espacios escalonados, y los Conduits constituyen los pasillos controlados que los unen. De este modo se evita que una única vulnerabilidad ponga en peligro todo el sistema, sobre todo cuando se trata de la Safety y, por tanto, de la protección de las personas.

Pilz aplica este enfoque de forma sistemática bajo el lema «Security for Safety»: la Safety es el objetivo de protección prioritario de Security. Lo más importante es la protección de la Safety, que a su vez protege a las personas. Por eso, Pilz separa la Safety del control general de las máquinas —lo que se conoce como «automatización estándar»— y reduce así la exposición de las funciones relevantes para la seguridad. Cuanto más claramente se separen funcionalmente estos «tesoros», menos medidas de seguridad adicionales serán necesarias para protegerlos de forma fiable.

Las ventajas de este enfoque se hacen evidentes a lo largo de todo el ciclo de vida de una máquina. Si se separan la Safety y las funciones estándar, al actualizar estas últimas no es necesario recertificar ni adaptar simultáneamente las funciones de seguridad, lo que reduce considerablemente las tareas de mantenimiento y servicio. Además, los controladores de seguridad clásicos requieren actualizaciones críticas para la seguridad con mucha menos frecuencia que los controladores de automatización, por lo que esta separación evita muchas intervenciones innecesarias. La separación también ofrece ventajas desde el punto de vista tecnológico: un microcontrol de seguridad como PNOZmulti 2 se puede combinar libremente con productos de distintos fabricantes de sistemas de control, mientras que los sistemas integrados suelen estar vinculados a tecnologías específicas. Asimismo, las soluciones de Safety

independientes aumentan los obstáculos para los atacantes, ya que los sistemas independientes deben ser comprometidos uno por uno, lo que complica considerablemente la manipulación. Además, una automatización estándar puede estar conectada a Internet cuando sea necesario, mientras que las funciones de Safety propiamente dichas permanecen aisladas, lo que reduce drásticamente la superficie de ataque de las funciones de Safety.

Además, esta separación entre la automatización de la seguridad Safety y la de Security, con niveles de protección óptimamente ajustados para cada caso, aumenta la eficiencia gracias a una mejor planificación de las medidas de seguridad, mantenimiento y ampliación. Los cambios en el programa de automatización no requieren entonces intervenir en la parte relacionada con la seguridad, lo que reduce considerablemente el esfuerzo de programación y adaptación. Al mismo tiempo, esta separación tiene un efecto positivo en los costes de software y asistencia técnica, ya que los sistemas independientes suelen conllevar menos gastos de licencia y de servicio.

Protección mediante la separación: competencia mediante la formación

La clara separación entre la Safety y la automatización estándar no solo garantiza la solidez técnica, sino que también reduce los errores de manejo y las necesidades de formación. Dado que las funciones relacionadas con la seguridad se ejecutan en hardware propio y están claramente delimitadas desde el punto de vista organizativo, permanecen protegidas incluso si se realizan cambios en el programa de automatización. Los errores en el funcionamiento diario no ponen en peligro la Safety y permiten atribuir las responsabilidades con mayor claridad.

Para ayudar a las empresas a implementar esta arquitectura, Pilz ofrece un amplio programa de formación y servicios. Entre ellos se incluyen los cursos «Fundamentos de Industrial Security» y «CESA – Certified Expert for Security in Automation», así como los Industrial Security Services. No solo explican cómo se pueden desarrollar conceptos sólidos de «Security-for-Safety» a partir de los distintos bloques, sino que van mucho más allá: muestran cómo gestionar sistemáticamente los riesgos de Security y desarrollar conceptos de seguridad integrales, cómo clasificar los requisitos de la norma IEC 62443, cómo estructurar la arquitectura de una red de máquinas segura y cómo evaluar y mejorar continuamente la eficacia de las contramedidas adoptadas.

Una ventaja decisiva de este enfoque es que el personal operativo del usuario final no necesita tener un conocimiento profundo de los temas de Security, ya que la protección de las funciones de Safety queda garantizada por el diseño arquitectónico. Por lo tanto, los cursos de formación están dirigidos principalmente a quienes toman decisiones en materia de Security o diseñan sistemas, mientras que los operarios pueden seguir trabajando de forma segura sin necesidad de formación adicional en el ámbito de la Industrial Security. De este modo se establece una distribución de funciones adaptada a la práctica, que simplifica el funcionamiento de la instalación y, al mismo tiempo, aumenta de forma sostenible el nivel de protección.

Más seguridad gracias a una estructura clara y a los conocimientos adecuados

Una estrategia eficaz de «Security for Safety» no se consigue con medidas aisladas, sino mediante una arquitectura bien planificada, responsabilidades claras y un desarrollo específico de las

competencias. Ahí es precisamente donde entra en juego Pilz. Con su enfoque sistemático en la «Defence-in-Depth» y una clara separación entre la Safety y la automatización estándar, Pilz sienta las bases para la creación de máquinas resistentes, y lo complementa con formación y asesoramiento orientados a la práctica, para que las empresas puedan seguir este camino con confianza. De este modo se consigue un nivel de seguridad que no solo cumple con los requisitos normativos, sino que aporta un valor añadido tangible en el día a día: más sencillo, más robusto y con una eficacia duradera.

((Caracteres: 9640))

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