Información general

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

Los conceptos de seguridad holísticos se enfocan en la cuestión del acceso para garantizar seguridad y protección industrial en las máquinas

Seguridad integral mediante gestión personalizada de permisos

Ostfildern, febrero de 2023 – **Cuando queremos proteger algo valioso, utilizamos puertas, candados y llaves para restringir el acceso. Lo mismo es aplicable al bien más preciado: nuestra seguridad en todas sus manifestaciones. Los entornos industriales exigen proteger por una parte, a las personas (seguridad) y por otra, a la máquina y los datos sensibles (protección industrial). Una seguridad deficiente puede tener diversas consecuencias, desde errores de manejo y accidentes hasta ciberataques de efectos devastadores. Un sistema Identification and Access Management completo que controla claramente los permisos de intervención y acceso contribuye a establecer un concepto de seguridad holístico y procesos eficientes.**

Una visión habitual en entornos de producción: resguardos que indican a las personas claramente que tras las puerta protectora se oculta una zona peligrosa que exige obrar con precaución. A través de un Human Machine Interface (HMI) o de una clave, las personas pueden acceder al proceso que se ejecuta tras la valla de protección. Pero, ¿y si la persona no está cualificada o autorizada para ello y pone en peligro además a otras personas? También pueden manipular el proceso una persona malintencionada, ya sea en la propia máquina o a través de acceso remoto. Por lo que respecta a la autorización de acceso, queda claro que la seguridad y la protección industrial están estrechamente vinculadas. Y lo que es más: La protección industrial preserva la integridad de la seguridad en la propia máquina. Ofrece protección, por ejemplo, contra entradas y accesos no autorizados desde el exterior a máquinas o instalaciones de producción y protección contra falsificación, pérdida y acceso no autorizado a datos sensibles del proceso y de la máquina. Esto incluye tanto ataques explícitos como incidencias de protección involuntarias.

La seguridad y la protección industrial van de la mano

Para empresas usuarias de máquinas e instalaciones es necesario asignar claramente las tareas y autorizaciones, es decir, establecer un Identification and Access Management. Incluye por una parte, medidas organizativas como instrucciones de trabajo o controles periódicos de los procesos y por otra, la integración de soluciones de seguridad adecuadas en el entorno de producción. La omisión de este tipo de medidas puede comportar que los responsables de la empresa tengan que responder personalmente de las consecuencias de posibles accidentes o fallos de producción. Hasta ahora, las soluciones de protección tenían carácter voluntario y en muchos lugares no se veía necesidad de actuación. Sin embargo, la legislación ya se ha percatado de que la seguridad y la protección van mano en mano. Por ello, el nuevo reglamento de máquinas establece como obligatorias las medidas de seguridad.

Modos de funcionamiento aumentan la seguridad

Existen varias normas C en las que se establece que los distintos modos de funcionamiento deben incluir también las correspondientes funciones de seguridad. Estos modos de funcionamiento pueden ser, por ejemplo, un modo automático, la intervención manual en condiciones restringidas o el modo de servicio. En la EN ISO 16090-1 relativa a centros de mecanizado y máquinas especiales se establecen por lo menos dos de estos modos de funcionamiento como requisito obligatorio para la seguridad funcional. Lo importante es que haya un solo modo de funcionamiento seleccionado y activo cada vez y que se visualice de manera clara.

Impedir accesos anónimos

Sin embargo, ¿cómo se decide qué personas pueden tener acceso en un modo de funcionamiento determinado o incluso modificar este modo de funcionamiento? Para ello se definen diferentes grupos de personas que tienen contacto con la máquina (por ejemplo, personal operador, de limpieza o de mantenimiento). A continuación, los trabajadores se asignan a los grupos en función de su cometido y capacitación. Según el tamaño de la empresa, las autorizaciones y permisos de acceso se pueden asignar también a grupos de usuarios diferentes o, por ejemplo, a un tipo de máquina que se utiliza a nivel corporativo. En una evaluación de riesgos, los expertos en seguridad calculan y evalúan el riesgo del acceso anónimo para cada peligro. A continuación se definen medidas para reducir el riesgo según el estado de la técnica y lo establecido en las normas armonizadas.

Facilidad de manejo previne manipulación

A la hora de implementar las medidas, es importante asegurar la facilidad de manejo y uso durante el funcionamiento para los usuarios a fin de excluir cualquier manipulación. Los constructores de máquinas deben tener en cuenta este requisito ya durante el proceso de desarrollo. Sistemas de manejo intuitivos y fáciles de usar para el usuario evitan que se neutralicen las medidas de seguridad o errores de manejo de la máquina. Un sistema de seguridad bien concebido favorece además procesos eficientes sin tiempos de parada innecesarios. El tema "Neutralización de dispositivos de protección" es uno de los puntos centrales de la EN ISO 14119. La norma define los principios para el diseño y la selección de sistemas de protección de puertas y proporciona directrices concretas para evitar manipulaciones.

Concepto de seguridad personalizado

Para que la apertura voluntaria o accidental de las puertas de acceso no genere situaciones de peligro, están protegidas mediante

un sistema de protección de puertas seguro. En el centro de la estrategia de la seguridad está la protección del operario frente a movimientos peligrosos de la máquina. Según si se trata de una máquina "stand-alone" o de complejas instalaciones concatenadas, se requiere un concepto de seguridad diseñado a medida. En máquinas con marcha en inercia peligrosa es fundamental contar con un bloqueo, mientras que cuando hay puertas transitables se requiere obligatoriamente un sistema de desbloqueo de alineación.

Protección a medida de puertas protectoras

Un sistema de protección de puertas de estructura modular como Pilz PSENmlock integra en un solo sistema la supervisión segura de puertas protectoras con el bloqueo seguro y dispone además de funciones de seguridad como parada de emergencia, desbloqueo de alineación y un bloqueo mecánico contra nueva puesta en marcha. Brinda flexibilidad e inteligencia descentralizada para la protección de aplicaciones muy diversas. Una solución a medida es una combinación específica de sensores, desbloqueo de alineación, tiradores/manijas y unidad de mando y pulsadores. Los usuarios configuran su solución de protección de puertas según los requerimientos de cada aplicación. Para satisfacer los requisitos de la protección industrial se consideran ahora los accesos y los permisos.

Un sistema para la seguridad y la protección industrial

En la práctica, la protección contra accesos no autorizados se puede realizar con un sistema de selección de modos de funcionamiento y autorización de acceso. Conjuga seguridad de las máquinas (Safety) y protección industrial (Industrial Security): la selección del modo de funcionamiento y la regulación de la autorización de acceso a la máquina. Los dispositivos del grupo de

productos Pilz PITmode constituyen una solución de este tipo, pues permiten conmutar entre modos definidos y gestionar la autorización de accesos. El manejo es intuitivo: cada usuario recibe un transpondedor con un código personal que permite la autenticación del usuario y evita manipulaciones.

Gestión selectiva de accesos y modos de funcionamiento

Puede elegirse entre diversas variantes de PITmode para diseñar el concepto de seguridad a medida. PITmode es un dispositivo compacto "Todo en uno" que ocupa poco espacio de instalación al incorporar los pulsadores de selección de modos de funcionamiento y una unidad de evaluación. El sistema modular PITmode fusion, por otra parte, está compuesto por la unidad de evaluación PITreader con tecnología RFID y servidor web integrado, así como de la unidad de evaluación segura Safe Evaluation Unit (SEU). Otra de las variantes es PITmode flex: PITreader se utiliza junto con un control Pilz y un bloque de software para la evaluación segura. La estructura modular facilita la integración de la autorización de acceso y la selección de modos de funcionamiento en el diseño de paneles de mandos instalados. Esto permite utilizar los pulsadores existentes para seleccionar el modo de funcionamiento y simplifica así el manejo al usuario. La identificación con el transpondedor es por medio de la unidad de lectura PITreader. PITmode y PITmode fusion ofrecen selección funcional segura de modos de funcionamiento y autorización de acceso hasta PL d.

Autenticación sencilla – también a distancia

Para seleccionar el modo de funcionamiento, el usuario introduce su transpondedor directamente en el PITmode y acciona el pulsador asignado al modo de funcionamiento o la tecla correspondiente en el HMI. Se dispone del permiso necesario, el

usuario podrá acceder al proceso. Esto funciona también cuando un empleado del servicio técnico intenta acceder a distancia a una máquina: el mantenimiento remoto no podrá comenzar hasta que una persona a pie de máquina habilite la oportuna autorización en el sistema. Una vez finalizados los trabajos de mantenimiento, se bloquea el acceso antes de que vuelva a arrancar la máquina. De este modo se excluyen manipulaciones por personas no autorizadas o la posibilidad de que queden puertos abiertos accidentalmente tras el mantenimiento. Las empresas usuarias aumentan su protección industrial al poder controlar quién accede al proceso y con qué autorización.

Solución completa para gestión de accesos

Si solo hay que gestionar los accesos, PITreader se puede usar como sistema de autorización de acceso de forma aislada o junto con un control Pilz. Junto con el microcontrol configurable PNOZmulti 2, el administrador configura las autorizaciones de acceso a máquinas e instalaciones utilizando la función "arrastrar y soltar" en la herramienta de configuración correspondiente PNOZmulti Configurator. A través de la unidad de lectura PITreader, se transferirán a continuación a la llave transpondedor RFID. La variante PITreader S tiene integrado el estándar OPC UA y se puede usar también con controles de otros fabricantes que no sean Pilz. Como ya se ha mencionado, los dispositivos PITmode pueden integrarse fácilmente en paneles de mando existentes.

Elección entre llave, tarjeta o sticker

La variante PITreader card unit aumenta la flexibilidad para empresas usuarias y operadores: permite usar tarjetas y sticker RFID compatibles junto con o en lugar de una llave transpondedor RFID. Las empresas que utilicen tarjetas RFID-compatibles pueden

seguir usándolas en combinación con PITreader card unit: con una sola tarjeta, el usuario podrá ejecutar varias funciones. La ventaja fundamental de los transpondedores RFID – ya sea en forma de llave, tarjeta o sticker – es la posibilidad de concentrar varias funciones en un solo transpondedor y unificar así un llavero mecánico completo. Mucho más cómodo para el usuario, que solo tiene que llevar el medio de identificación. Los administradores, por otra parte, ahorran tiempo y trabajo de gestión y conservación de llaves.

Una ventaja en términos de protección

Se han tenido en cuenta también aspectos de protección relacionados con la autenticación de usuarios, cualificación y protección contra acceso. Si se produjera un accidente o incidencia de protección en la máquina aun habiendo aplicado todas las medidas de seguridad, la lectura de la llave RFID permitiría saber si se realizaron modificaciones y conocer los autores. Si se desea esta función opcional, el sistema de control registra en el Audit Trail interno seguro (log de eventos) tanto la autenticación como la hora de acceso.

La clave: una administración detallada

Los administradores son muy meticulosos a la hora de gestionar permisos que garanticen seguridad y protección industrial durante el ciclo de vida completo de la aplicación. Unas herramientas de software de Pilz para la organización de usuarios y transpondedores simplifican la tarea de administración. Bajo una discreta llave RFID pueden esconderse complejas matrices de autorización o especificaciones gestionadas a nivel corporativo. Los administradores utilizan el servidor web PITreader integrado para programar los transpondedores RFID asociados a PITmode o

PITreader y almacenar en ellos los datos y permisos de los usuarios. Puesto que los principales ajustes se realizan directamente en la unidad de lectura, se agiliza la puesta en marcha y la configuración de interfaces.

Limitar el acceso a interfaces

Las posibilidades del Identification and Access Management llegan hasta la habilitación de puertos USB industriales especiales, una de las principales puertas de entrada para incidencias de protección. El sistema de autorización de acceso PITreader se combina con un elemento de manejo como PIT oe USB, que dispone de un interface Host USB 2.0 activable. Esta solución permite cargar programas, extraer datos y conectar un teclado o ratón, todo a prueba de manipulación. Porque el interface se activa exclusivamente si se dispone de la autorización pertinente, protegiendo así el flujo de datos de la producción. Junto con un cortafuegos industrial como Pilz SecurityBridge, que controla la comunicación de datos dentro de segmentos de automatización industriales, está asegurada la protección de las máquinas contra manipulación y accesos no autorizados.

Parques de maquinaria – seguridad y protección

Cuando existe necesidad de actualizar la tecnología del parque de maquinaria o una evaluación de riesgos ha determinado actuaciones necesarias, solo hay que reequipar el sistema de autorización de acceso PITreader: el dispositivo puede enchufarse directamente a las salidas normalizadas para interruptores de llave de 22,5 milímetros de diámetro. Con un control Pilz, la función de seguridad requerida se puede configurar directamente. En caso de utilizar un control ajeno, se usa PITmode fusion para integrar la evaluación de la autorización de acceso y la selección de modos de

funcionamiento. Dependiendo del formato de transpondedor usado, pueden utilizarse las tarjetas RFID existentes en la empresa para la autenticación.

Conclusión

Para preservar el bien más preciado —nuestra seguridad— es preciso diseñar conceptos de seguridad completos y actualizarlos periódicamente. En este sentido es fundamental disponer de un sistema de Identification and Access Management como elemento que regule claramente las autorizaciones y los accesos en una empresa. La solución es un concepto que incluya medidas organizativas y especificaciones, además de las funciones de seguridad requeridas. Un sistema de autorización de acceso como PITreader, completado con los componentes de software adecuados, es el componente de hardware idóneo para organizar usuarios y transpondedores. La incorporación de un sistema de protección de puertas, un control, el software correspondiente y funciones como la selección de modos de funcionamiento convierten la solución en un concepto integral de seguridad y protección industrial. Un concepto que es además fácil de manejar para el usuario: solo necesita tener a mano su llave personal.

Caracteres: 14.675

Ilustraciones

Fig. 1:

F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)

Pie de foto: Un completo sistema Identification and Access Management gestiona el acceso a la aplicación y garantiza con ello la integridad de las funciones y medidas de seguridad; seguridad y protección industrial incluidas.

Fig. 2:
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)

Pie de foto: PITmode fusion de Pilz es un sistema modular de selección de modos de funcionamiento y autorización de acceso que combina funciones de seguridad y protección industrial en un solo sistema.

Fig. 3:
F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg (Pilz GmbH & Co. KG)

Pie de foto: El sistema de autorización de acceso PITreader card unit de Pilz, con las tarjetas PITreader card y sticker PITreader RFID-compatibles, abre las puertas a nuevos formatos para la implementación de un sistema de autorización de acceso eficiente.

Fig. 4:
F_Press_PITreader_Webserver.jpg (© Pilz GmbH & Co. KG)

Pie de foto: Las llaves transpondedor RFID se cargan y programan en el PITreader. La asignación de las autorizaciones de acceso y la selección de los modos de funcionamiento tiene lugar a través del servidor web asociado.

Fig. 5:
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold_v0.jpg (© Pilz GmbH & Co. KG)

Pie de foto: La combinación flexible de sistema de protección de puertas PSENmlock con el módulo de tirador compatible (arriba a la izquierda), la unidad de pulsadores PITgatebox con sistema de autorización de acceso integrado PITreader (arriba a la derecha), el microcontrol configurable PNOZmulti 2 (abajo a la derecha) y la solución de diagnóstico Safety Device Diagnostics (abajo a la izquierda) proporciona una solución completa para protección de puertas con autorización de acceso.

Cuadro: Protección digital para el mantenimiento Key-in-pocket

Además de autorizaciones de acceso, PITreader se puede usar junto con un control Pilz, como el microcontrol configurable PNOZmulti 2 o el sistema de automatización PSS 4000, como protección eficaz para el mantenimiento "Key-in-Pocket". Este sistema se encarga de que la máquina no pueda ponerse en marcha durante los trabajos de mantenimiento y de bloquear el acceso a personas no autorizadas. Sobre el terreno, el funcionamiento es el siguiente: uno o más operarios autorizados

para realizar tareas de mantenimiento se autentican para acceder a la instalación. Tras confirmarse la autenticación, el control Pilz almacena en una lista segura un Security-ID específico del usuario. Ahora ya se puede desconectar la máquina, abrir la puerta protectora y acceder a la máquina. Durante las tareas, las llaves RFID permanecen guardadas "en el bolsillo del pantalón" del respectivo usuario. Una vez finalizado el mantenimiento y después de salir de la zona peligrosa, todos los operarios cierran sesión, los ID de protección se eliminan de la lista segura del control Pilz y se puede volver a poner en servicio la máquina. A diferencia de una protección para el mantenimiento con llaves mecánicas, se puede entrar o salir de la instalación por cualquier puerta protectora. "Key-in-Pocket" ofrece al personal más flexibilidad y ahorro de tiempo para la realización de tareas de mantenimiento. La protección digital para mantenimiento se ha diseñado especialmente para máquinas con zonas peligrosas aisladas por vallas de protección. La empresa usuaria sabe en todo momento quién ha obtenido acceso a una determinada tarea y puede adjudicar permisos temporales.

1.578 caracteres

Fig. cuadro Key-in-pocket:
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

Pie de foto: la protección para el mantenimiento "Key-in-pocket" está compuesta por el sistema de autorización de acceso PITreader, la unidad de pulsadores PITgatebox y un control Pilz, como el microcontrol configurable PNOZmulti 2 o el sistema de automatización PSS 4000.

Cuadro: Asignar y actualizar autorizaciones

Las empresas que usan un sistema de autorización de acceso deben velar por la actualización y administración continua de las autorizaciones y los datos de los usuarios si quieren garantizar la seguridad. De esto se encarga el PIT Transponder Manager (PTM) de Pilz: en un panel de control gráfico, el administrador gestiona los ajustes y datos de los usuarios y las listas de bloqueo. Las autorizaciones específicas de cada usuario se escriben en unos pocos pasos en la llave transpondedor sobre la base de plantillas preconfiguradas y una función de importación.

En las empresas que tienen en servicio varios PITmode o PITreader, se utiliza el software PIT User Authentication Service (UAS) de Pilz para organizar estos dispositivos. Esta herramienta sirve para conectar con PITreader sistemas de gestión como PTM o software de administración de usuarios de terceros. PIT UAS contiene una base de datos central de autorizaciones para los

usuarios y permite importar y asignar datos del PTM a todos los PITreader. Los administradores pueden consultar el estado actual de todos los PITreader y visualizar una lista de diagnóstico. Obtienen así una visión general rápida aunque haya muchos dispositivos en uso.

1.218 caracteres

Fig. cuadro Administración de usuarios:
((imagen disponible en breve)).jpg (© Pilz GmbH & Co. KG)

Pie de foto: cuando se usan varias unidades de lectura PITreader en una empresa, los dispositivos se organizan con el User Authentication Service (UAS).

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 2.500 personas. A través de las 42 filiales y sucursales que tiene en todo el mundo, Pilz vela por la seguridad de personas, máquinas y medio ambiente.
Este líder tecnológico ofrece soluciones completas de automatización que abarcan sensores y tecnología de control y de 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 Pilz se emplean no solo en la construcción de máquinas e instalaciones, sino también en

muchos otros sectores, como la intralogística, la tecnología ferroviaria o la robótica.

www.pilz.com

Contacto para la prensa:

Martin Kurth

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

Sabrina Schilling

Prensa especializada

Tel: +49 711 3409-7147
s.schilling@pilz.de

Sabine Karrer

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

Hansjörg Sperling-Wohlgemuth
Dirección de congresos y conferencias
Tel: +49 711 3409-239
h.sperling@pilz.de

Jenny Skarman

Prensa especializada

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