

tec.nicum

news

Tendencias, normas y soluciones para la seguridad de las máquinas

Edición 2025.02

Página 2
Editorial

Página 3
El Cyber Resilience Act y el nuevo Reglamento Europeo de Máquinas

Página 6
IO-Link Safety: el camino hacia la próxima generación de máquinas seguras

Página 10
Acceso al mercado de aparamenta de seguridad en Corea del Sur: certificación KC

Página 11
Tiepner GmbH: seguridad de máquinas en la construcción de máquinas especiales

Página 14
Nuevas cortinas y rejillas ópticas de seguridad con certificación ATEX

Página 15
tec.nicum, excellence in safety

Página 17
El programa de seminarios 2026 de tec.nicum academy

tec.nicum



mrl.news sigue siendo su brújula para el cambio: práctica, comprensible y orientada al futuro.

Estimados lectores:

Desde hace muchos años, mrl.news es una fuente fiable de información sobre la Directiva de Máquinas, el marco normativo central que ha marcado de forma decisiva la seguridad de las máquinas en Europa. Pero, igual que el entorno en el que se diseñan, operan y conectan las máquinas, las normas y la base jurídica también evolucionan constantemente.

En 2027, la actual Directiva de Máquinas 2006/42/CE será sustituida en la práctica por el nuevo Reglamento de Máquinas, el Reglamento (UE) 2023/1230. A primera vista parece un cambio formal, pero en realidad es un cambio de fondo. Como todos los reglamentos de la UE, el Reglamento de Máquinas se aplicará de forma directa y uniforme en todos los Estados miembros sin necesidad de transponerlo al derecho nacional.

Lo hemos hablado, sopesado y estudiado alternativas. Y hemos tomado una decisión consciente: mrl.news sigue siendo mrl.news. Porque este título es más que unas siglas. Representa conocimiento experto, orientación en el derecho de máquinas y una revista que desde hace años informa, clasifica y da impulso con fiabilidad.

El nuevo Reglamento de Máquinas aporta más claridad y carácter vinculante, pero también plantea nuevos retos, sobre todo en aspectos de seguridad digital, inteligencia artificial, software y sistemas conectados.

Como su partner en todo lo relacionado con la seguridad de las máquinas, también le acompañaremos en esta nueva etapa. En este y en los próximos números de mrl.news le mostraremos de forma práctica qué cambia para los fabricantes de maquinaria y de componentes. En la página 3 encontrará un primer artículo sobre ello.

Hay algo que no cambia: nuestro objetivo es compartir conocimiento, orientar y diseñar juntos soluciones seguras para las personas, las máquinas y el futuro.

Un saludo,
su equipo de redacción de
mrl.news

Seguridad jurídica de cara al futuro

La Cyber Resilience Act y el nuevo Reglamento de Máquinas de la UE

¿Qué requisitos se derivan de la Cyber Resilience Act (CRA) y del nuevo Reglamento de Máquinas de la UE para los fabricantes de maquinaria y de componentes?

El nuevo Reglamento de Máquinas (RM), obligatorio en todos los Estados miembros de la UE desde el 20 de enero de 2027, regula también, entre otras cosas, los requisitos para la construcción de maquinaria que se derivan de la Cyber Resilience Act (CRA) de la UE.

La CRA, que entró en vigor el 10 de diciembre de 2024, debe aplicarse por completo a partir del 11 de diciembre de 2027. Pero hay obligaciones de notificación de vulnerabilidades e incidentes cibernéticos que empiezan ya el 11 de septiembre de 2026.

El objetivo de la CRA es aumentar la resiliencia de la UE frente a ciberataques contra sistemas, productos y procesos digitales (hardware y software). Instalaciones y máquinas, y los procesos económicos asociados, ya están expuestos a muchos ataques a través de interfaces digitales locales o de redes IT. En la construcción de maquinaria, estos ataques suelen ir contra la integridad y la disponibilidad de los procesos de producción más que contra la obtención de datos e información de esos procesos.

La seguridad funcional de máquinas e instalaciones es especialmente vulnerable, porque los sistemas de seguridad deben llevar la máquina a un estado seguro incluso ante pequeñas alteraciones, es decir, la máquina tiene que pararse. Por eso el impacto económico de estos ciberataques es tan grave.



Obligaciones del fabricante

La CRA obliga a los fabricantes a desarrollar y fabricar los productos según los requisitos esenciales del anexo I del reglamento.

Los requisitos esenciales incluyen (anexo I, parte 1):

- El producto solo puede comercializarse sin vulnerabilidades conocidas
- Configuración segura por defecto
- Suministro de actualizaciones de seguridad
- Protección frente a accesos no autorizados
- Un diseño con una superficie de ataque limitada (“security by design”)

Además, se exige elaborar documentación técnica de hardware y software y respetar un deber de diligencia al integrar componentes de terceros. Por supuesto, esto también vale para los módulos de software integrados en componentes o máquinas.

Además, los fabricantes deben gestionar las vulnerabilidades de forma continua. Tienen que cerrar las brechas de seguridad durante todo el ciclo de vida del producto, y como mínimo cinco años. También deben ofrecer actualizaciones de software durante al menos diez años.

La gestión de vulnerabilidades incluye (anexo I, parte 2):

- Notificación, corrección y documentación de vulnerabilidades
- Elaboración de una SBOM (documentación del historial de versiones de software de todos los componentes)
- Revisión periódica de la ciberseguridad
- Obligaciones de notificación a ENISA y CSIRT (agencias de la UE)

Obligaciones de notificación en caso de brechas de seguridad

Para que los usuarios puedan cerrar una vulnerabilidad lo antes posible, por ejemplo con una actualización de software, hay que informar a los usuarios y a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en cuanto se conozca una vulnerabilidad explotable activamente.



Las obligaciones de notificación del fabricante incluyen (artículo 14):

- Notificar a ENISA y CSIRT cualquier vulnerabilidad explotada activamente o incidente en cuanto se tenga conocimiento
- Notificación con información y, si hace falta, medidas correctoras en un plazo de 72 horas
- Informe final sobre las vulnerabilidades explotadas y los incidentes:
  - Descripción, gravedad y efectos del ataque
  - Posibles causas y autores
  - Actualizaciones de seguridad y medidas correctoras para los usuarios afectados

La obligación de notificación entra en vigor 21 meses después de la entrada en vigor del reglamento CRA, es decir, en septiembre de 2026.

Cumplir los objetivos de protección y definir el nivel de seguridad:

Para cumplir los requisitos, el fabricante de la máquina puede apoyarse en distintas normas.

Los requisitos normativos de ciberseguridad están, entre otras, en la IEC 62443. Define objetivos de protección y niveles de seguridad, así como procedimientos para cumplir los requisitos de ciberseguridad en sistemas de automatización industrial. La norma evalúa los requisitos técnicos de sistemas (IEC 62443-3-3) y de productos (IEC 62443-4-2) mediante los llamados security levels (SL). Los distintos niveles indican la resistencia frente a atacantes potenciales con diferentes conocimientos y recursos.

El fabricante de componentes y máquinas debe analizar qué nivel o qué propiedades de seguridad necesita un componente o una máquina para resistir los ataques potenciales identificados.

A partir de esta evaluación de riesgos hay que implantar mecanismos de control adecuados frente a accesos no autorizados. Pueden ser sistemas de autenticación, de gestión de identidades o de accesos que garanticen la integridad de los datos almacenados, transmitidos o procesados de otro modo, sean personales o no, y que protejan comandos, programas y configuraciones contra la manipulación.

Por eso la IEC 62443 es una buena guía para que fabricantes y usuarios de máquinas apliquen la ciberseguridad de forma eficaz.

También está el proyecto de norma IEC 63208 sobre los aspectos de ciberseguridad de los componentes. El borrador final (FDIS) está disponible desde mayo de 2025 y se espera que se apruebe como muy tarde a principios de 2026.

La IEC 63208 retoma el sistema de la IEC 62443 y amplía los requisitos de ciberseguridad a la aparamenta de baja tensión con capacidad de comunicación.

Cyber Resilience Act de la UE (CRA 2024/2847)

Entrada en vigor: 10 de diciembre de 2024
Notificaciones desde: 11 de septiembre de 2026
Aplicación obligatoria: 11 de diciembre de 2027

Reglamento de Máquinas de la UE (RM 2023/1230)

Entrada en vigor: 19 de julio de 2023
Aplicación obligatoria: 20 de enero de 2027

IEC 62443 Seguridad IT para sistemas de automatización industrial (IACS)

Parte 3-3: requisitos del sistema y niveles SL
Parte 4-2: requisitos para componentes
Fecha: 2019 / 2020

FDIS_IEC 63208 Aparamenta de baja tensión y sus componentes. Aspectos de seguridad

Fecha: borrador final 2025-05

Reglamentos y normas de la UE de un vistazo.

Soluciones para la construcción de maquinaria

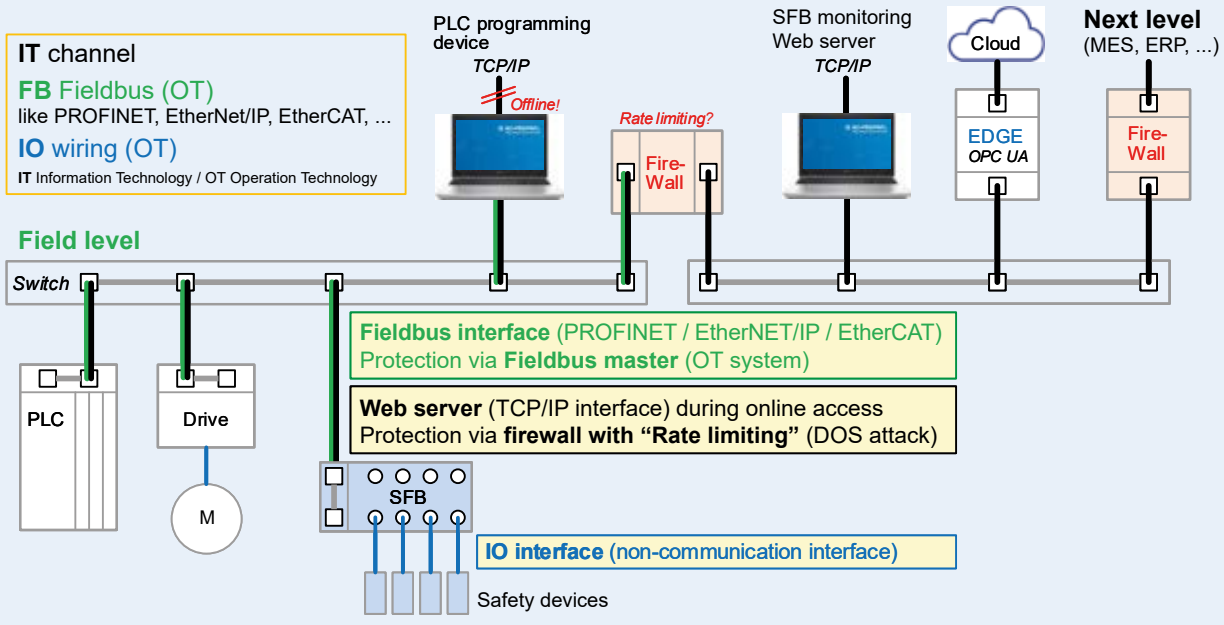
Como primer paso, conviene crear un esquema del sistema de la máquina para analizar la topología de red. Hay que tener en cuenta tanto el área OT de los buses de campo de la máquina como su integración en la red IT de la planta y de las instalaciones de producción.

Normalmente tiene sentido segmentar las distintas áreas de red y protegerlas en los puntos de transición con cortafuegos. Además, el acceso al área OT a través de las interfaces IT para programación y servicio debe protegerse y, si hace falta, permitirse solo offline. ■

Udo Weber
Product Manager de técnica de seguridad del Grupo Schmersal y miembro del comité conjunto DIN “Principios de seguridad – sistemas de mando”



Esquema del sistema de una máquina





Los primeros productos IO-Link Safety de Schmersal estarán disponibles hacia finales del primer semestre de 2026: el sensor de seguridad RSS362 (derecha) y el enclavamiento con bloqueo AZM42 (izquierda). Otros productos, como el maestro IO-Link Safety y el sensor RSS262, están en desarrollo.

Comunicación segura en la Industria 4.0

IO-Link Safety: abriendo camino a la próxima generación de máquinas seguras

Con IO-Link Safety hay por primera vez un sistema de comunicación normalizado e independiente del fabricante para la seguridad funcional. Amplía las posibilidades de la Industria 4.0 con una comunicación segura punto a punto entre sensores, actuadores y controladores.



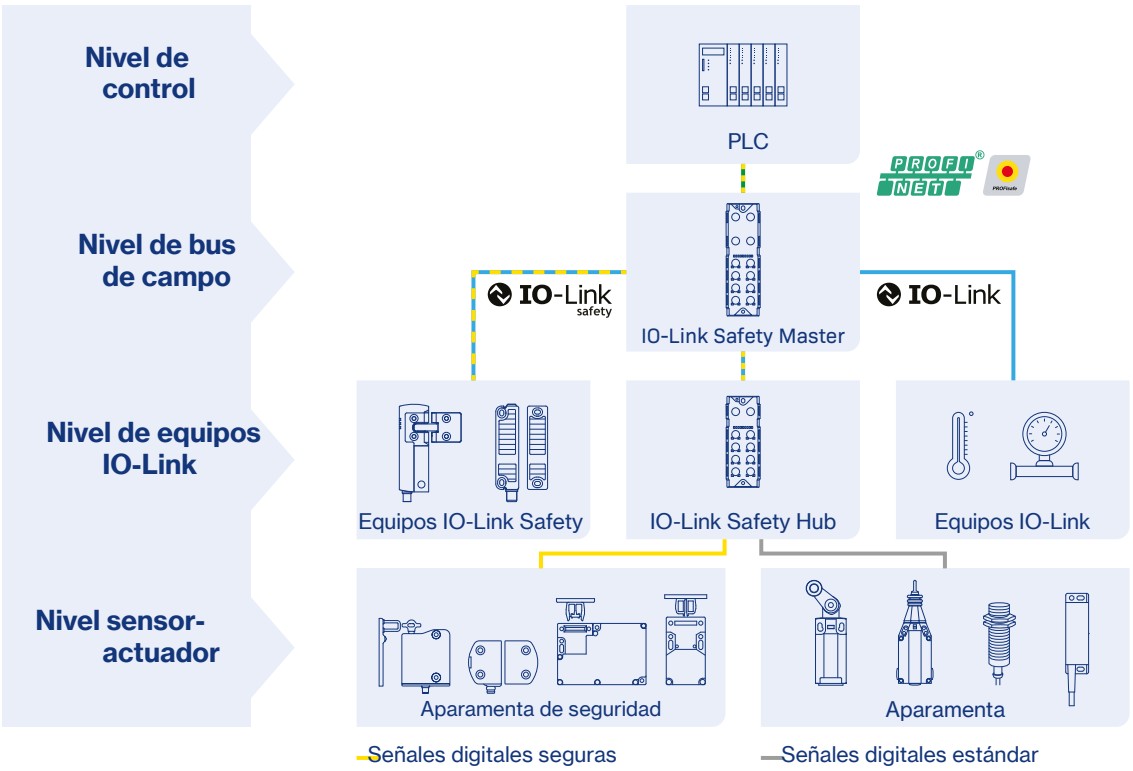
En esta entrevista, Volker Heinzer, Strategic Product Manager del Grupo Schmersal, explica hasta dónde ha llegado la tecnología, qué oportunidades ofrece y por qué tendrá un papel clave en la seguridad de las máquinas.

Un nuevo estándar para seguridad y comunicación

IO-Link Safety se basa en la probada tecnología IO-Link y traslada sus principios a la seguridad funcional. Así se crea por primera vez un estándar uniforme en el nivel más bajo de la automatización, que facilita integrar componentes de seguridad. “IO-Link Safety es muy importante para nosotros, porque es una tecnología clave para el futuro de la seguridad de las máquinas”, explica Volker Heinzer. En una industria cada vez más conectada y automatizada, es importante diseñar soluciones de seguridad flexibles, escalables y capaces de dar datos. La ventaja decisiva: IO-Link Safety da transparencia hasta el nivel de campo. Sensores y actuadores no solo transmiten señales de seguridad, sino que también intercambian datos de diagnóstico y parámetros adicionales. Esto abre nuevas posibilidades de mantenimiento, monitorización de estado y optimización de procesos: un paso real hacia “Safety meets Smart Factory”.

Normalización a nivel internacional

Un hito importante fue la normalización de IO-Link Safety en la IEC 61139-2, que establece que el sistema cumple los requisitos de seguridad más altos, hasta PL e (EN ISO 13849-1) o SIL 3 (IEC 61508/62061). “La publicación de la primera versión de las IO-Link Safety Extensions en 2017 abrió el camino a soluciones de seguridad independientes del fabricante”, dice Heinzer. Hasta entonces, el ámbito de la seguridad estaba muy marcado por interfaces propietarias. IO-Link Safety crea una base común en la que equipos →



Representación esquemática de la arquitectura de un sistema IO-Link Safety.

de distintos fabricantes pueden trabajar juntos de forma interoperable. Así, en el futuro los usuarios podrán combinar con flexibilidad componentes de seguridad de distintos proveedores sin atarse a un sistema concreto. Esto hace la seguridad de las máquinas no solo más eficiente, sino también más económica y preparada para el futuro.

Valor añadido con la comunicación bidireccional

La comunicación bidireccional es una de las ventajas clave de IO-Link Safety. Mientras que las conexiones de seguridad convencionales suelen permitir solo transmisiones de señal simples, IO-Link Safety permite un intercambio de información en ambos sentidos. Es decir, los controladores no solo reciben datos de los sensores, sino que también pueden devolverles parámetros, órdenes y configuraciones. “Esto mejora mucho las posibilidades de diagnóstico”, subraya Heinzer. La capacidad de comunicación de sensores y actuadores abre además nuevos campos de aplicación, como el mantenimiento predictivo o la monitorización de procesos. Otra ventaja práctica es el menor trabajo de instalación. En lugar de cables de ocho hilos, con IO-Link Safety suelen bastar cables estándar de tres hilos con conectores M12. Esto reduce costes de material e instalación, evita errores de cableado y acelera la puesta en marcha. Para los fabricantes de máquinas supone una ganancia de eficiencia notable.

Integración en el mundo de la Industria 4.0

IO-Link Safety no es solo una solución de seguridad, sino un elemento clave de la transformación digital. La tecnología encaja sin problemas en los entornos modernos de Industria 4.0, en los que los datos se recogen, analizan y usan en todos los niveles. “Poder obtener información adicional del nivel de campo da más flexibilidad y transparencia en la producción”, afirma Heinzer. Así, IO-Link Safety impulsa procesos de fabricación inteligentes y adaptativos que se ajustan de forma dinámica a las necesidades de producción.

Retos en el camino hacia la aplicación práctica

Además de las muchas ventajas, Heinzer también ve retos: “Tenemos que asegurar que todo el ecosistema de IO-Link e IO-Link Safety siga siendo interoperable.” Esto vale tanto para el desarrollo de equipos como para la integración de sistemas. La implantación exige entender a fondo la tecnología y supone al principio un trabajo de desarrollo adicional. Las empresas sin experiencia previa con IO-Link deben prepararse para cierto cambio de mentalidad. “Al principio puede haber costes iniciales más altos”, reconoce Heinzer, “pero se amortizan rápido con el ahorro y la eficiencia a largo plazo.” →

Schmersal lanza al mercado los primeros productos IO-Link Safety

Buenas noticias para todos los usuarios: Schmersal presentará pronto sus dos primeros productos IO-Link Safety, el enclavamiento con bloqueo AZM42 y el sensor de seguridad RSS362. Esto convierte a la empresa en una de las pioneras de la integración IO-Link Safety y subraya su papel de liderazgo en seguridad funcional. Ambos equipos amplían el sistema de instalación IO-Link Safety de Schmersal para aplicaciones de seguridad industrial y ofrecen comunicación segura bidireccional mediante un cable de 3 hilos. Así se pueden realizar aplicaciones seguras hasta performance level e, categoría 4 o SIL 3, con mucha flexibilidad y una integración sencilla en sistemas existentes.

AZM42: bloqueo con valor añadido digital

Ya en su versión original, el enclavamiento con bloqueo AZM42 es una de las soluciones de seguridad más compactas y potentes para la construcción de maquinaria. En la nueva versión se han reducido aún más las distancias al montar dos equipos uno al lado del otro, y la función de enclavamiento y bloqueo hasta PL e, cat. 4, SIL 3 está en un solo equipo. La interfaz IO-Link Safety amplía el bloqueo con numerosas funciones de Industria 4.0. Además de las funciones de seguridad conocidas, el AZM42 ofrece ahora datos de estado y diagnóstico en tiempo real, incluida información sobre la tensión de alimentación, la temperatura y la calidad de la señal RFID. El sistema también cuenta los ciclos de apertura de puerta y de bloqueo y detecta, por ejemplo, si se supera la distancia entre sensor y actuador.



AZM42

RSS362: sensor de seguridad con diagnóstico inteligente

Con el RSS362, Schmersal lanza ahora la versión compatible con IO-Link Safety de su sensor de seguridad sin contacto basado en RFID, ya introducido con éxito. También aquí se han reducido mucho las distancias entre dos equipos. Las funciones de seguridad conocidas siguen siendo lo principal, completadas con un amplio paquete de datos de diagnóstico y funcionamiento. El RSS362 también informa del número de ciclos de conmutación, de la tensión de alimentación, de la temperatura y la calidad de la señal RFID y de la alineación del sensor con el actuador. Estos datos se pueden transmitir al control mediante la comunicación IO-Link Safety y usarse allí para muchas tareas, como el mantenimiento predictivo.



RSS362

Igual que el AZM42, el RSS362 admite comunicación segura bidireccional: el controlador también puede enviar al sensor datos de configuración, parámetros u órdenes de forma segura. Así se pueden programar actuadores nuevos sin intervención física. Gracias a la función de almacenamiento de datos, las configuraciones de ambos equipos se guardan automáticamente y se restauran al sustituirlos. Esto simplifica mucho el mantenimiento. La configuración y parametrización offline también permite preparar los equipos en el PC de la oficina, una ventaja real en mantenimiento y en producción en serie.

Heinzer: “Con estos dos productos demostramos que IO-Link Safety no es solo un concepto teórico, sino que ya ha llegado a la práctica.” →



Además de las funciones de seguridad conocidas, el AZM42 ofrece ahora datos de estado y diagnóstico en tiempo real.

Aplicaciones prácticas y valor añadido para el usuario

Integrar IO-Link Safety en los componentes de seguridad abre nuevas posibilidades a usuarios y fabricantes de máquinas. El acceso a datos adicionales permite ajustar de forma dinámica los intervalos de mantenimiento, localizar antes las causas de fallos y evitar paradas no planificadas. Además, IO-Link Safety facilita la estandarización de arquitecturas y una puesta en marcha rápida. Su diseño modular permite ampliar con más flexibilidad las soluciones de seguridad en el futuro, una ventaja decisiva ante entornos de producción cada vez más complejos.

Perspectivas: IO-Link Safety como estándar del sector

El mercado de IO-Link crece rápido: más de 500 empresas de todo el mundo forman ya parte del consorcio IO-Link, entre ellas muchos proveedores líderes de automatización. “Igual que IO-Link ha crecido exponencialmente en importancia en los últimos años, IO-Link Safety también tendrá un papel central en la próxima generación de máquinas e instalaciones seguras”, está convencido Heinzer. Para Schmersal esto significa desarrollo continuo, estrecha colaboración en el consorcio IO-Link y una apuesta clara por las tecnologías de seguridad basadas en datos. Con el AZM42 y el RSS362, la empresa es uno de los primeros proveedores en llevar a la producción en serie equipos compatibles con IO-Link Safety, una señal clara para el mercado.



Conclusión: la seguridad se vuelve digital, conectada e inteligente

IO-Link Safety marca un punto de inflexión en la técnica de seguridad industrial. La vía de comunicación normalizada une funcionalidad y seguridad en una plataforma y crea la base para sistemas inteligentes que se vigilan a sí mismos. Para fabricantes y usuarios de máquinas, las ventajas son claras: menos costes de instalación, más transparencia, diagnóstico más rápido y una flexibilidad sin precedentes. “IO-Link Safety tendrá un papel central en la próxima generación de máquinas e instalaciones seguras, y Schmersal estará en primera línea”, concluye Heinzer, subrayando la determinación de la empresa de dar forma activa a este cambio tecnológico e impulsar soluciones de seguridad innovadoras. ■

Volker Heinzer
Strategic Product Manager de sistemas de comunicación industrial e Industria 4.0 en el Grupo Schmersal

Seguridad de producto ensayada

Acceso al mercado de Corea del Sur para aparamenta de seguridad: la certificación KC

La **Korea Certification (KC)** es un instrumento central para garantizar la seguridad de los productos en Corea del Sur. Allí es obligatoria para muchos aparatos eléctricos y electrónicos. La certificación KC también es obligatoria, en determinadas condiciones, para algunos productos de seguridad como pulsadores de parada de emergencia, dispositivos de bloqueo, controladores de seguridad o relés de seguridad, y garantiza que los productos funcionen de forma segura y fiable según las normas coreanas. La normativa nacional aplicable se basa en parte en las normas IEC internacionales, aunque las normas coreanas tienen algunas particularidades que difieren de las IEC.

La Korean Agency for Technology and Standards (KATS) se encarga de su aplicación. La certificación KC se introdujo ya en 2009 para agrupar en un sistema unificado las numerosas marcas de ensayo que había en Corea del Sur.

Los fabricantes extranjeros tienen requisitos especiales adicionales: deben nombrar un representante autorizado con sede en Corea y algunos documentos técnicos deben estar en coreano.

Cada fabricante debe comprobar en detalle qué esquema de certificación se aplica a cada producto. Los productos con certificación KC deben marcarse en consecuencia. Además de la etiqueta “KC”, cada fabricante recibe un número de certificado, que también debe figurar en el producto. ■

El proceso de certificación se desarrolla así:

1. **Solicitud** a un centro de ensayos acreditado en Corea.
2. **Entrega de la documentación técnica,** p. ej., esquemas eléctricos, listas de piezas, análisis de riesgos e informes de ensayo (los informes del esquema CB pueden reconocerse en parte).
3. **Ensayos de tipo** en laboratorios coreanos acreditados.
4. **Inspección inicial de la producción** (obligatoria en la primera solicitud).
5. **Emisión del certificado** y publicación en la base de datos KC.

Dipl.-Ing. (FH) Jörg Eisold
Responsable de Normas, Comités y Asociaciones,
K.A. Schmersal GmbH & Co. KG



El logotipo de la certificación KC.



La fabricación de herramientas y máquinas especiales para soldar plásticos es la especialidad de Tiepner GmbH desde hace más de 40 años.

Fig. 1: La instalación compacta fabrica tarjetas de plástico laminado que se usan, entre otras cosas, como tarjetas de cliente, carnés o tarjetas cheque. A la izquierda, Christian Höltge, gerente de Tiepner GmbH.

Jugar bien la carta
Seguridad en la construcción de máquinas especiales

Los operarios de las máquinas (especiales) totalmente automatizadas de Tiepner siempre están bien informados del proceso y del estado de funcionamiento en el circuito de seguridad. Lo garantizan puertas de seguridad que dejan ver bien cada estación y, en la máquina más reciente, manillas iluminadas que indican con colores, por ejemplo, si la puerta está liberada para abrirse. Una safety fieldbox simplifica la comunicación en el circuito de seguridad de la máquina, que produce hasta 15.000 tarjetas de identificación de plástico por hora. Tiepner aprovecha así dos de las últimas innovaciones de Schmersal y está totalmente satisfecha con el resultado.

Los clientes de Tiepner GmbH, en Dietfurt (Alto Palatinado), no ponen todos los huevos en la misma cesta. Al contrario: con una sola instalación Tiepner producen o procesan cada hora un número de cinco cifras de tarjetas de plástico, que se usan como tarjetas de identificación, chip, carné, cheque o cliente y están hechas de distintos plásticos, sobre todo PVC o policarbonato.

15.000 tarjetas por hora

Tiepner ha planificado, construido y entregado hace poco una instalación así, que fabrica de forma totalmente automática tarjetas en formato ID estándar **(ver fig. 1)**. El material de partida son pliegos laminados que se introducen en la instalación. Primero se separan los pliegos en varias estaciones, luego se alinean y se comprueba su grosor. Después, una estación troquela tres tarjetas de medidas normalizadas del cuerpo base. Cada tarjeta se deposita en uno de varios cargadores. Así, la instalación produce unas 15.000 tarjetas por hora, con o sin chip, en serie o personalizadas.

Salvo para retirar los cargadores, la máquina trabaja de forma automática, sin que un operario tenga que intervenir. Los operarios ven bien cada estación, y cada puerta de seguridad, con grandes ventanas, está asegurada con un enclavamiento con bloqueo.

Nuevo sistema de mando

Este concepto es estándar en todas las máquinas de Tiepner, igual que el hecho de que la aparamenta y los mandos de seguridad de los resguardos sean de Schmersal. En la instalación más reciente que presentamos aquí, Tiepner fue uno de los primeros usuarios de una nueva generación de sistemas de mando. El gerente Christian Höltge **(ver fig. 1)**: “Poco antes de empezar a diseñar esta máquina especial, Schmersal había lanzado una nueva serie de manillas de puerta iluminadas que señalizan el estado de funcionamiento de la máquina. Como damos mucha importancia a la transparencia en la interfaz persona-máquina, esta serie nos gustó enseguida. Encaja bien en nuestro concepto de mando.” →

Manillas de puerta que se iluminan en distintos colores

La nueva serie es el sistema de manillas de puerta DHS **(fig. 2)**, que une las funciones de una manilla robusta con la indicación de distintos estados de la máquina: las manillas se iluminan en una gran superficie con hasta siete colores. El propio usuario puede configurar qué color corresponde a cada función.



Fig. 2: las manillas del sistema DHS se iluminan en una gran superficie con hasta siete colores e indican el estado del resguardo.

Tiepner usa el sistema, por ejemplo, para indicar si se puede abrir el resguardo. Y si el control detecta una anomalía, el resguardo donde se ha detectado se ilumina en color.

Además, cada manilla de la serie DHS lleva un pulsador cuya función también se puede asignar libremente, por ejemplo como rearme o como petición de apertura del resguardo.

Transparencia en el resguardo

Desde el punto de vista del usuario, el sistema de manillas simplifica el manejo de la máquina. El usuario sabe en qué punto está, por ejemplo, en qué modo de funcionamiento (preparación o marcha a impulsos) está la máquina. Tiepner ha configurado el sistema para que con el pulsador también se pueda consultar si el enclavamiento con bloqueo ha liberado la puerta, es decir, si se puede abrir. Así no hace falta montar manillas ni pilotos adicionales.

Combinación con un bloqueo compacto

Todo el sistema de manillas está pensado para integrarse en perfiles de 40 mm, y se puede usar como unidad con el enclavamiento con bloqueo AZM40. Tiepner usa justo esta combinación y así reúne en una unidad compacta las funciones centrales de la seguridad de la máquina y de la interfaz persona-máquina: vigilancia de posición del resguardo, enclavamiento / bloqueo / apertura del resguardo e información sobre el estado de funcionamiento **(fig. 3)**.



Fig. 3: las manillas pueden combinarse como unidad con el enclavamiento con bloqueo compacto AZM40.

Los diseñadores de Tiepner y los usuarios de la primera máquina con este sistema están totalmente satisfechos. Christian Höltge: “El operario siempre está bien informado: ¿se puede abrir la puerta de seguridad? ¿En qué puerta ha detectado el control una anomalía? Esto da transparencia.”

Para funciones de mando adicionales se usa además un panel de mando independiente de la serie BDF 100 de Schmersal **(fig. 4)**. La serie BDF 100 incluye una selección de paneles de mando para funciones adicionales. Se montan con poco esfuerzo donde se puedan alcanzar rápido si hace falta, también como pulsador de parada de emergencia independiente **(fig. 5)**. Además, son muy compactos y encajan perfectamente en los perfiles de 40 mm del cerramiento de la máquina.





Fig. 4, izquierda: para funciones de mando adicionales se usa un panel de mando independiente de la serie BDF 100 de Schmersal (arriba en la imagen). **Fig. 5, derecha:** el pulsador de parada de emergencia independiente, también de la serie BDF 100, está montado a la vista y se alcanza rápido en caso de emergencia.

Estreno de la Safety Fieldbox

En la comunicación relativa a la seguridad, Tiepner usa por primera vez la Safety Fieldbox de Schmersal **(ver fig. 6)**. Las interfaces universales para conectores M12 de ocho polos permiten integrar en el circuito de seguridad enclavamientos con bloqueo electrónicos y electromecánicos, sensores, paneles de mando, cortinas ópticas o interruptores →



Fig. 7: como especialista en la producción de tarjetas de plástico, Tiepner también diseña y construye instalaciones más complejas que se encargan de pasos previos del proceso, como la producción del laminado, que tiene hasta ocho capas.

de seguridad. Los enclavamientos con bloqueo o las cortinas ópticas de seguridad solo necesitan una conexión M12.

Los paneles de mando con función de parada de emergencia y hasta tres elementos de mando y señalización no seguros



Fig. 6: la Safety Fieldbox simplifica la integración de la aparamenta de seguridad en el circuito de seguridad

también se pueden conectar directamente a un puerto de la Safety Fieldbox sin hardware adicional. Los datos se transmiten al control mediante un protocolo Ethernet seguro. Esto crea una buena base para modularizar la técnica de seguridad, también desde el punto de vista económico, porque esta interfaz universal es más barata que equipos individuales con interfaz de bus.

En instalaciones más grandes, varias fieldboxes conectadas entre sí también pueden simplificar la comunicación de seguridad.

Listo para conectar con cables preconfeccionados

Para Tiepner, instalar la aparamenta de seguridad en esta instalación fue especialmente fácil. Christian Höltge: “Indicamos las longitudes de cable al hacer el pedido y Schmersal nos suministró los cables preconfeccionados directamente. Eso nos ahorró aún más tiempo, y montar la fieldbox también costó muy poco.”

Conclusión: solución completa de seguridad

Así, en el diseño y la fabricación de esta máquina Tiepner ha optado por una solución completa para la seguridad. El especialista en tarjetas de plástico usa la serie DHS, una innovación de Schmersal que da transparencia en el resguardo, y la Safety Fieldbox simplifica la comunicación en el circuito de seguridad y la instalación de la aparamenta de seguridad. ■

Un especialista en la producción de tarjetas

Tiepner GmbH también diseña y fabrica instalaciones mucho más grandes que la descrita aquí. Sirven para producir el laminado del que se troquelan las tarjetas **(ver fig. 7)**. Hasta ocho láminas de policarbonato o PVC, en hojas o en bobina, se preparan primero una a una de forma totalmente automática, se recortan si hace falta y después se apilan. Unas cámaras ayudan a formar la pila, que también depende de la alineación exacta de la impresión. Después se troquelan las tarjetas. Tiepner fabrica también máquinas independientes y muy compactas solo para esta operación, como la descrita aquí.

Máxima exigencia

NUEVAS CORTINAS / REJILLAS ÓPTICAS DE SEGURIDAD CON CERTIFICACIÓN ATEX (PARA ZONA 1 / 2G Y ZONA 21 / 2D)



Schmersal ha ampliado su gama de dispositivos de protección optoelectrónicos para proteger de forma fiable accesos en atmósferas potencialmente explosivas. Con la nueva serie EX-SLC/SLG440, las cortinas y rejillas ópticas de seguridad ya están disponibles en versión Ex. Así se combinan los estándares de seguridad más altos con una calidad probada.

En muchas zonas de producción hay un mayor riesgo de explosión, por ejemplo en la industria química, en refinerías o en talleres de pintura donde se procesan recubrimientos inflamables. El polvo también puede suponer riesgo de explosión en industrias que procesan materiales a granel, como la industria de piensos o del reciclaje, los aserraderos o las plantas de cereales.

Las cortinas y rejillas ópticas de seguridad **SLC/SLG440** se han desarrollado ahora también en versión Ex para estos ámbitos exigentes. Estos dispositivos de protección optoelectrónicos pueden usarse en atmósferas de gas y polvo especialmente explosivas, en las zonas **1 y 21**, para proteger zonas peligrosas.

Cortinas ópticas de seguridad EX-SLC440 para detección de dedos, manos y cuerpo

- Certificación ATEX para 2G / D, zona 1 / 21
- Protección de dedos y manos con resolución de 14 mm y 30 mm
- Protección de cuerpo con 2 a 4 haces
- Alcance: 0,3 a 20 m
- Estanca al polvo
- Apta para exteriores
- Carcasa protectora con tapas metálicas
- Montaje y manejo sencillos, con poco peso

CATEGORÍA ATEX			
Zona 1 Gas	**Zona 21** Polvo	**Zona 2** Gas	**Zona 22** Polvo
2G	**2D**	**3G**	**3D**
✓	✓	✓	✓



Pida el folleto o consúltelo online






excellence in safety

tec.nicum es la unidad de negocio del Grupo Schmersal para soluciones y servicios de seguridad de máquinas, instalaciones y en el trabajo.

Schmersal reestructuró su negocio de servicios en 2024. La oferta de servicios de seguridad de tec.nicum se ha ampliado mucho, sobre todo en digitalización y soluciones completas para la seguridad de las máquinas, y las actividades y competencias globales se han integrado más.

En abril de 2024, Schmersal fundó la nueva filial tec.nicum – Solutions & Services GmbH, que integró también omnicon engineering GmbH, adquirida por Schmersal en 2019. La sede de la nueva filial está en Kirkel-Limbach (Alemania).

Los cuatro pilares de la oferta de tec.nicum hasta ahora (academy, consulting, engineering e integration) se han completado con dos más: digitalisation y outsourcing.

digitalisation: tec.nicum ofrece cada vez más soluciones de software de nuevo desarrollo, como una nueva herramienta para hacer evaluaciones de riesgos, y nuevas tecnologías digitales como soluciones en la nube, aplicaciones IIoT, procedimientos de consignación digitalizados y herramientas de gestión energética.

outsourcing: tec.nicum ofrece a las empresas la posibilidad de externalizar por completo todas las tareas relacionadas con la seguridad de las máquinas, desde la planificación e instalación de armarios eléctricos hasta el diseño de soluciones de seguridad integrales. tec.nicum suministra al usuario soluciones plug & play listas para conectar.

Gracias a su red mundial de consultoría, los servicios de tec.nicum están disponibles en todo el mundo. tec.nicum ofrece a los clientes un asesoramiento competente e independiente de productos y fabricantes, y les acompaña en el diseño de seguridad de sus máquinas y líneas de producción.

tec.nicum
Schmersal Group

tec.nicum – Solutions & Services GmbH
Oficina de Kirkel
Friedrichstraße 65
66459 Kirkel-Limbach
Tel.: +49 6841 77780-0
E-mail: europe@tecnicum.com
Web: www.tecnicum.com

tec.nicum – Solutions & Services GmbH
Oficina de Wuppertal
Möddinghofe 30
42279 Wuppertal
Tel.: +49 202 6474-932
E-mail: europe@tecnicum.com
Web: www.tecnicum.com





La oferta de servicios de tec.nicum tiene seis áreas: academy (formación), consulting (consultoría), engineering (ingeniería técnica), integration (ejecución e implantación), digitalisation (soluciones de software y nuevas tecnologías digitales) y outsourcing (soluciones completas).

academy

Centro de formación

- Formaciones
- Formación a medida
- Seminarios in company
- Cursos certificados (mce.expert y FSE)

consulting

Análisis y documentación

- Soporte técnico
- Evaluaciones de riesgos
- Evaluación de la conformidad CE
- Evaluación de máquinas y líneas
- Documentación técnica

engineering

Ingeniería y diseño

- Proyectos técnicos
- Desarrollo conceptual de proyectos
- Diseño eléctrico y mecánico
- Dirección de proyectos

integration

Aplicación práctica

- Llave en mano
- Instalación
- Retrofit

digitalisation

Integración de software

- tec.**ps** (Product Service System)
- tec.**ssm** (Schmersal Smart Machine)
- tec.**cvs** (AI and Computational Vision Solutions)
- tec.**dloto** (Digital Lockout Tagout)
- tec.**ems** (Energy Monitoring System)

outsourcing

Soluciones en serie

- Productos plug & play
- Proyectos Engineer to Order
- Sistemas y armarios

tec.nicum

Imágenes: K.A. Schmersal GmbH & Co. KG (shutterstock.com, Annette Kradisch, fotógrafa del reportaje de Tiepner)

Este folleto está impreso en papel con certificación FSC®. La etiqueta de este producto garantiza una gestión responsable de los bosques del planeta.

Las emisiones de gases de efecto invernadero generadas en la producción de este folleto se han compensado invirtiendo en el proyecto “LAYA Estufas de leña energéticamente eficientes” en la India.





Edita:

tec.nicum

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
Tel.: +49 202 6474-932
europe@tecnicum.com
www.tecnicum.com