

tec.nicum news

Lo último sobre el Reglamento de Máquinas

Edición 2026.01

Página 2
Editorial
La seguridad en tiempos de cambio

Página 3
Nuevo Reglamento de Máquinas de la UE
Lo que deben saber fabricantes y usuarios

Página 6
El Cyber Resilience Act (CRA) y la seguridad OT
Impacto en la ingeniería mecánica y la automatización

Página 9
Automatización segura en la práctica
Las tecnologías clave

Página 11
Caso práctico
JBT Marel | maquinaria TREIF

Página 15
Certificaciones UL
El mercado norteamericano

Página 16
Robots humanoides
Nuevos retos para la seguridad de máquinas

Página 20
LOTO digital
Mantenimiento fiable sin montañas de papeleo

tec.nicum



Seguridad en tiempos de cambio: aprovechar oportunidades, asegurar el futuro

Estimados lectores:

La automatización industrial vive un momento de cambio profundo. Nuevos requisitos normativos, tecnologías de comunicación innovadoras y una digitalización creciente están transformando no solo máquinas e instalaciones, sino también lo que se exige a fabricantes, integradores y usuarios.

Con el nuevo Reglamento de Máquinas, obligatorio desde enero de 2027, y la Cyber Resilience Act, temas como la seguridad funcional y la ciberseguridad se entrelazan aún más. Las empresas tienen el reto de adaptar a tiempo sus productos y procesos a los requisitos futuros. Al mismo tiempo, esto abre la oportunidad de replantear la seguridad de forma integral y ganar ventaja competitiva.

En el artículo “Automatización segura en la práctica” vemos cómo los diseños de máquinas modernos pueden ser seguros y flexibles en el futuro. Tecnologías como la Safety Fieldbox, IO-Link Safety y Single Pair Ethernet sientan las bases de una automatización potente, integral y preparada para el futuro.

Nuestro caso práctico sobre las máquinas TREIF de JBT Marel demuestra que los conceptos de seguridad innovadores ya se aplican con éxito hoy. El ejemplo de los sistemas de corte modernos muestra cómo las soluciones de seguridad inteligentes pueden unir productividad y facilidad de uso.

Otro tema central de este número es la digitalización de los procesos de seguridad. Con Digital LOTO, la gestión digital de la consignación gana cada vez más importancia. Sobre todo ante las crecientes exigencias de documentación, transparencia y eficiencia, la digitalización ofrece un gran potencial para más seguridad en el día a día.

La rápida evolución de la robótica también plantea nuevas preguntas. Los robots humanoides y los sistemas con IA generan grandes expectativas de flexibilidad y rendimiento. Al mismo tiempo, las estrategias de seguridad deben seguir el ritmo para generar la confianza necesaria en el uso seguro de estas tecnologías. Por eso, la combinación de seguridad funcional e inteligencia artificial tendrá un papel clave en el futuro.

También vemos los requisitos del mercado norteamericano. Para muchas empresas, la certificación UL sigue siendo decisiva para entrar en mercados internacionales y marca el camino de su competitividad global.

Y por último, nos alegra contarle que los seminarios de nuestra academy tienen ahora una oferta aún más amplia. Transmitir conocimiento y desarrollar competencias siguen siendo claves para afrontar con éxito los retos de un mundo tecnológico cada vez más complejo.

Esperamos que disfrute de la lectura, que le aporte nuevas ideas para su trabajo diario y muchas propuestas para construir un futuro industrial seguro.

Su equipo de redacción de tec.nicum news

Lo que fabricantes y usuarios de máquinas deben saber

El nuevo Reglamento de Máquinas de la UE (UE) 2023/1230

RESUMEN RÁPIDO

El 20 de enero de 2027 empieza a aplicarse el Reglamento (UE) 2023/1230, que trae unas normas totalmente nuevas para fabricantes, importadores y usuarios de máquinas. Sustituye a la Directiva de Máquinas 2006/42/CE, vigente desde 2009, y sin peros: no hay transición gradual, sino una fecha de corte estricta. Quien no esté preparado se arriesga a no poder comercializar máquinas conforme a la ley. Es hora de hacer un repaso.

Autor: Tobias Keller
Head of Administration,
tec.nicum

1. Del borrador al reglamento: el proceso

La Directiva de Máquinas 2006/42/CE ha sido durante mucho tiempo la base de la seguridad de las máquinas en Europa. Pero el mundo ha cambiado: en 2006, la digitalización, la conectividad, la inteligencia artificial (IA) y la ciberseguridad apenas se tenían en cuenta, si es que se tenían. Además, las diferencias en la transposición de la directiva al derecho nacional de cada Estado miembro han provocado interpretaciones distintas y distorsiones de la competencia.

La Comisión Europea respondió con un nuevo enfoque: en lugar de revisar la directiva, optó por un reglamento. Así, las nuevas normas se aplican de forma directa y uniforme en los 27 Estados miembros sin necesidad de transposición nacional. El Parlamento Europeo aprobó el reglamento por amplia mayoría el 18 de abril de 2023 y el Consejo Europeo dio su visto bueno el 22 de mayo de 2023. Se publicó en el Diario Oficial de la UE el 29 de junio de 2023 y entró formalmente en vigor el 19 de julio de 2023.

El reglamento será obligatorio para los fabricantes desde el 20 de enero de 2027, exactamente 42 meses después de su entrada en vigor. En Alemania, la llamada ley de aplicación del Reglamento de Máquinas (Maschinen-DG) sustituirá también al anterior reglamento nacional de aplicación (9. ProdSV).

2. Qué cambia de fondo

Un reglamento en lugar de una directiva: se acabó el margen nacional

El cambio más importante es formal, pero tiene grandes consecuencias prácticas. Un reglamento de la UE es directamente aplicable, mientras que una directiva primero debe transponerse al derecho nacional. Hasta ahora, los Estados miembros podían interpretar y aplicar la Directiva de Máquinas de forma distinta. Eso se ha acabado. El Reglamento de Máquinas (UE) 2023/1230 se aplica de forma uniforme en toda la UE y es, por tanto, una gran ventaja para la seguridad jurídica y el mercado único. →



El nuevo Reglamento de Máquinas de la UE crea un marco jurídico moderno para la comercialización de máquinas en Europa.

Por primera vez: ciberseguridad e inteligencia artificial

Quizá la novedad técnica más importante es que, por primera vez, el nuevo reglamento trata de forma explícita los riesgos de ciberseguridad de los sistemas de mando de seguridad y del software crítico para la seguridad. Los fabricantes deben proteger las máquinas y su software frente a accesos no autorizados y manipulaciones. Además, se introducen requisitos para funciones de seguridad basadas en IA, en línea con la Ley de IA de la UE, que llega casi al mismo tiempo. Quien use IA en funciones de seguridad de máquinas tendrá que tener en cuenta ambas normativas. Las máquinas autónomas y teledirigidas también tendrán su propia regulación.

La evaluación de riesgos incluye el software

El principio de la evaluación de riesgos sigue siendo el mismo, pero su alcance se amplía. Una novedad es la obligación explícita de evaluar también los riesgos del software de la máquina, incluidas las actualizaciones previstas tras la comercialización. Los fabricantes deben decidir en la fase de diseño qué actualizaciones van a publicar y analizar de antemano sus riesgos. Esto supone un cambio de paradigma: la responsabilidad por la seguridad de la máquina ya no termina al entregarla.

Claridad sobre la "modificación sustancial"

Un punto que ha generado mucha discusión queda ahora regulado: el reglamento establece con precisión cuándo una modificación de una máquina existente es una "modificación sustancial" y exige por tanto un nuevo procedimiento de evaluación de la conformidad. Esto afecta directamente a los usuarios que hacen modificaciones o retrofits. En caso de duda, asumen antes su responsabilidad como fabricantes, incluidos el marcado CE y la documentación técnica.

Más control por terceros para máquinas de alto riesgo

Para seis categorías de productos con un riesgo especialmente alto (anexo I del RM), es obligatorio que intervenga un organismo notificado en la evaluación de la conformidad. Además, se endurecen las obligaciones de importadores y distribuidores y se amplía la obligación de las autoridades de notificar defectos de seguridad. También se amplía la definición de componente de seguridad, que ahora incluye de forma explícita el software y los componentes digitales con funciones de seguridad.

Se permite el manual de instrucciones digital

El Reglamento de Máquinas introduce un enfoque práctico y que ahorra recursos al permitir que el manual de instrucciones, las instrucciones de montaje y la declaración UE de conformidad se entreguen solo en formato digital. Aun así, los usuarios deberían guardar copias locales de estos documentos. No basta con depender del acceso online, porque los enlaces a la documentación del fabricante pueden dejar de funcionar.

3. Plazos clave de un vistazo

Fecha	Evento
2023-06-29	Publicación del Reglamento (UE) 2023/1230 en el Diario Oficial de la UE
2023-07-19	Entrada en vigor formal del reglamento (se permite la aplicación voluntaria)
2025-01-20	La Comisión Europea encarga a CEN/CENELEC finalizar las normas
Fin de 2026	Publicación prevista de las hEN en el DOUE; decisión de ejecución con la lista de normas
2027-01-20	**Fecha de corte:** la Directiva 2006/42/CE deja de aplicarse. Solo vale el RM (UE) 2023/1230. Sin aplicación en paralelo.

4. Situación de la normalización: el tiempo corre

Las normas armonizadas dan a los fabricantes una caja de herramientas práctica. Quien aplica una de estas normas puede suponer, en general, que cumple los requisitos legales ("presunción de conformidad"). Pero justo aquí está ahora uno de los mayores retos del nuevo Reglamento de Máquinas.

Todas las normas armonizadas hasta ahora con la Directiva de Máquinas (hay varios cientos) deben revisarse a la luz de los nuevos requisitos del RM y modificarse si hace falta. El 20 de enero de 2025, la Comisión Europea dio el mandato final de normalización a CEN y CENELEC. El calendario es ambicioso: CEN/CENELEC debía presentar un borrador del programa de trabajo conjunto como muy tarde en julio de 2025; las normas armonizadas debían aprobarse a principios de 2026 y publicarse en el Diario Oficial de la UE a finales de 2026, poco antes de la fecha límite del 20 de enero de 2027. Los comités técnicos trabajan en las normas desde febrero de 2025. Según CEN/CENELEC, los resultados de unos dos tercios de →

todas las normas armonizadas se habían enviado a la Comisión Europea a mediados de 2025. Ahora mismo no está claro si todas se publicarán a tiempo. Pero el reglamento prevé "especificaciones comunes" como alternativa si las normas armonizadas no están disponibles para el 20 de enero de 2027.

Las nuevas normas que se publiquen antes de la fecha límite de 2027 deben cumplir los requisitos tanto de la antigua Directiva de Máquinas como del nuevo reglamento. Por eso, tal como están las cosas, tendrán dos anexos normativos: el actual anexo ZA (para la Directiva) y un nuevo anexo ZB (para el RM). Además, la Comisión Europea está elaborando unas directrices. El grupo de redacción se reunió por primera vez en enero de 2025 y los primeros borradores estaban listos a principios de 2026. Un tema secundario con relevancia práctica: la sentencia "Malamud" del TJUE (marzo de 2024) exige que las normas armonizadas, como parte del Derecho de la UE, sean de acceso gratuito. Ya se han creado las primeras "plataformas de lectura".

5. Conclusión: actuar ya, no esperar

El 20 de enero de 2027 está más cerca de lo que parece. Quien siga trabajando con la Directiva de Máquinas debería empezar ya a adaptar sus procesos al nuevo Reglamento de Máquinas. Las evaluaciones de riesgos deben incluir software y ciberseguridad, la documentación técnica debe actualizarse y hay que estudiar pronto si puede hacer falta una certificación por terceros.

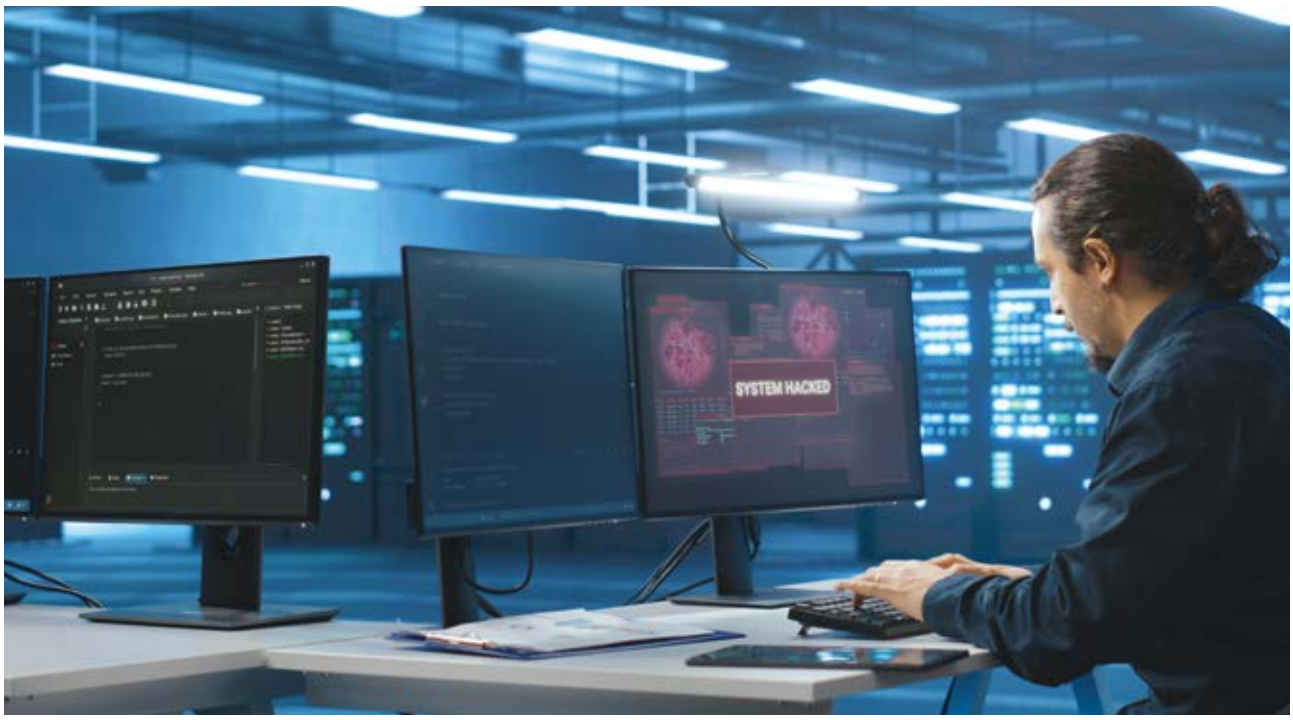
Los fabricantes con proyectos complejos que no se entregarán hasta después de la fecha límite deberían empezar ya a aplicar el nuevo reglamento. Así se ahorran muchas correcciones costosas después. Ya se puede y está permitido cumplir de forma voluntaria y anticipada los requisitos del Reglamento de Máquinas, por ejemplo aplicando antes los nuevos requisitos de ciberseguridad.

El nuevo Reglamento de Máquinas no es un simple documento administrativo. Es la respuesta a un mundo transformado por la tecnología, con máquinas conectadas, inteligentes y cada vez más autónomas. Quien entienda y aplique pronto los requisitos no solo tendrá seguridad jurídica, sino también una ventaja competitiva real. ■

Nota sobre la normalización:
La publicación de la lista de normas armonizadas del RM en el Diario Oficial de la UE está prevista para finales de 2026. Hasta entonces se pueden seguir aplicando las normas armonizadas de la Directiva de Máquinas 2006/42/CE, siempre que su contenido cumpla los requisitos del RM. Las organizaciones deben seguir de cerca las publicaciones de CEN/CENELEC y de la Comisión Europea.



Las empresas que actúan pronto ganan seguridad en la planificación, evitan prisas innecesarias y adaptan a tiempo sus productos a los nuevos requisitos.



Impacto en la construcción de maquinaria y la automatización

La Cyber Resilience Act (CRA) y la seguridad OT

Autor: Tobias Keller
Head of Administration, tec.nicum

1. ¿Qué es la Cyber Resilience Act?

La Cyber Resilience Act (CRA) es el Reglamento (UE) 2024/2847, que entró en vigor el 10 de diciembre de 2024. Su objetivo es que los productos con elementos digitales (PDE) sean ciberseguros durante todo su ciclo de vida, desde el desarrollo hasta la distribución y la retirada.

La CRA se aplica a todos los fabricantes, importadores y distribuidores que comercializan en la UE hardware o software con capacidad de red o conectividad digital. En la construcción de maquinaria, esto significa que en cuanto una máquina, un control, un sensor o un accionamiento está conectado o se puede conectar, entra en juego la CRA.

Calendario

Oct. 2024: CRA publicada en el Diario Oficial de la UE
Dic. 2024: entrada en vigor
Sept. 2026: obligación de notificar vulnerabilidades explotadas activamente
Dic. 2027: aplicación completa de todos los requisitos de la CRA

2. Relevancia para la construcción de maquinaria y la automatización

Los componentes clásicos de máquinas, como PLC, sistemas SCADA, robots industriales, paneles HMI, accionamientos en red y gateways IIoT, entran en el ámbito de la CRA si tienen capacidad de red. Es decir, prácticamente todos los productos modernos de Industria 4.0 están afectados.

Obligaciones clave para los fabricantes de máquinas

- Secure by Design: la ciberseguridad debe integrarse desde la fase de desarrollo, no añadirse a posteriori
- Gestión de vulnerabilidades: hay que ofrecer actualizaciones de seguridad durante todo el ciclo de vida del producto (al menos 5 años)
- Evaluación de la conformidad: distintos procedimientos según la clase de riesgo (estándar, clase I, clase II), hasta ensayos obligatorios por terceros
- SBOM (Software Bill of Materials): documentación completa de todos los componentes de software y sus dependencias
- Obligación de notificar: las vulnerabilidades explotadas activamente deben notificarse a ENISA en 24 horas →

3. Seguridad OT frente a seguridad IT: una diferencia clave

Por primera vez, la CRA trata también de forma explícita la tecnología operativa (OT), es decir, los sistemas de control industrial y los equipos de campo. Hay diferencias de fondo con la seguridad IT clásica:

Criterio	Seguridad IT	Seguridad OT
Objetivo de protección	Confidencialidad, integridad, disponibilidad (CIA)	Disponibilidad, integridad, confidencialidad (AIC): ¡orden inverso!
Paradas	Actualizaciones a corto plazo posibles	Parada = pérdida de producción; actualizaciones solo en ventanas de mantenimiento
Ciclos de vida	3–5 años	15–30 años (las máquinas suelen ser más antiguas que los sist. operativos)
Conectividad	Totalmente conectado	A menudo aisladas (air gap) o conectadas indirectamente
Protocolos	Estándar TCP/IP	Profibus, PROFINET, Modbus, OPC UA, EtherCAT
Parches	Distribución inmediata posible	Hace falta validación, ensayos y aprobación del fabricante

4. El triángulo normativo: CRA, NIS 2 y Reglamento de Máquinas

En la construcción de maquinaria se entrelazan tres normativas de la UE que juntas forman un marco completo de ciberseguridad:

Cyber Resilience Act (UE) 2024/2847	**Directiva NIS 2** (UE) 2022/2555 / NIS2UmsuCG	**Reglamento de Máquinas** (UE) 2023/1230
Foco: producto ■ Obligaciones para fabricantes de productos conectados ■ Marcado CE para PDE ■ Aplicable desde diciembre de 2027	**Foco: usuarios** ■ Obligaciones para empresas de sectores críticos (incluida la fabricación) ■ SGSI, obligaciones de notificación, gestión de riesgos ■ En Alemania: NIS2UmsuCG / nueva BSIG desde diciembre de 2025	**Foco: máquina** ■ Sustituye a la antigua Directiva de Máquinas (2006/42/CE) ■ Ciberseguridad como nuevo requisito esencial (RESS) ■ Aplicable desde julio de 2027

Contexto: la CRA y el Reglamento de Máquinas se aplican a nivel de producto (fabricantes), mientras que NIS 2 se aplica a nivel de organización (usuarios). Las organizaciones que fabrican y operan máquinas pueden estar sujetas a las tres normativas a la vez. Los productos conformes con la CRA facilitan a los usuarios cumplir NIS 2. →



5. Qué significa para el sector alemán de maquinaria

Con unas 6.500 empresas de maquinaria y más del 70 por ciento de su producción destinada a la exportación, Alemania está especialmente afectada. La VDMA calcula que la mayor parte del sector entra en la CRA. Hay que actuar a varios niveles:

Medidas inmediatas hasta 2026

- Análisis de carencias: ¿qué productos son PDE? ¿Qué clase de riesgo se aplica?
- Crear procesos para notificar vulnerabilidades en 24 horas (obligatorio desde septiembre de 2026)
- Crear procesos SBOM: tener una visión de todos los componentes open source y de terceros usados

A corto plazo, hasta 2027

- Integrar el ciclo de desarrollo seguro (SDL) en el proceso de ingeniería
- Desarrollar arquitecturas de seguridad específicas para OT: segmentación de red, defensa en profundidad, con la IEC 62443 como marco de referencia
- Alinear la CRA y el Reglamento de Máquinas: integrar la ciberseguridad en la evaluación de la conformidad CE
- Revisar la cadena de suministro: los proveedores también deben cumplir la CRA (responsabilidad en toda la cadena)

Conclusión

La Cyber Resilience Act supone un cambio de paradigma: la ciberseguridad se convierte en una característica del producto, comparable al marcado CE para la seguridad mecánica. Para el sector alemán de maquinaria es un reto considerable, pero también una oportunidad: quien invierta pronto asegurará el acceso al mercado y ventajas competitivas.

La clave está en combinar la CRA (seguridad del producto), NIS 2 (obligaciones de los usuarios) y el Reglamento de Máquinas (seguridad de la máquina). La seguridad OT no es solo un tema de IT: requiere métodos, normas (IEC 62443, ISA/IEC 62443) y conocimientos propios, que el sector de la maquinaria tiene que desarrollar. ■



Automatización segura en la práctica: Safety Fieldbox (SFB), IO-Link/IO-Link Safety y Single Pair Ethernet en Schmersal

RESUMEN RÁPIDO

Safe Automation 4.0:
En Schmersal, la SFB, IO-Link/IO-Link Safety y, en el futuro, Single Pair Ethernet forman una plataforma integrada para la construcción modular de máquinas. Reducen el cableado, mejoran el diagnóstico y permiten una comunicación segura basada en IP directamente desde el sensor. El resultado son diseños de máquina flexibles y preparados para el futuro.

Autor: Volker Heinzer
Strategic Product Manager – Industrial Communication Systems and Industry 4.0



"Con la SFB, IO-Link Safety y Single Pair Ethernet llevamos de forma sistemática la técnica de seguridad al futuro digital. Estas tecnologías abren nuevas posibilidades para los diseños de máquinas y simplifican por igual el diseño, la puesta en marcha y el funcionamiento."

El sector de la maquinaria vive un cambio tecnológico profundo. Las crecientes exigencias de flexibilidad, los diseños modulares y la digitalización cada vez mayor de la fabricación requieren nuevas soluciones de comunicación, sobre todo en seguridad funcional. Como fabricante de componentes y sistemas de seguridad, Schmersal desarrolla tecnologías que simplifican el diseño y hacen posibles nuevos conceptos de automatización segura. **El foco está en tres tecnologías clave: la Safety Fieldbox (SFB), IO-Link/IO-Link Safety y, en el futuro, Single Pair Ethernet (SPE).**

La Safety Fieldbox (SFB): seguridad descentralizada para máquinas modulares

Las máquinas modulares y las líneas de producción flexibles necesitan una arquitectura fácil de adaptar y de ampliar rápido. Aquí la Safety Fieldbox (SFB) de Schmersal ofrece una ventaja decisiva. Como periferia de seguridad descentralizada, permite implementar las funciones de seguridad directamente en el módulo de la máquina, sin armarios centrales, sin largos cableados en paralelo y sin estructuras de cableado complejas.

La SFB se comunica por PROFINET / PROFIsafe, EtherNet/IP / CIP Safety o EtherCAT / FSoE, integra entradas y salidas seguras y paneles de mando con parada de emergencia segura, y permite integrar señales de E/S estándar mediante módulos de ampliación opcionales (port extenders).

Para los diseñadores, esto supone una gran simplificación:

- La funcionalidad de seguridad se vuelve modular, escalable y totalmente digital
- Se reduce el cableado, se minimizan las fuentes de error y la puesta en marcha es mucho más rápida
- Los módulos de máquina se pueden entregar preconfigurados y combinar con flexibilidad en campo

Sobre todo en aplicaciones con configuraciones de máquina que cambian a menudo, como máquinas de embalaje o células de montaje, la SFB ofrece una solución de seguridad realmente plug-and-play.

IO-Link e IO-Link Safety: transparencia hasta el sensor

Mientras IO-Link demuestra desde hace tiempo sus ventajas como estándar de comunicación consolidado en campo, Schmersal da el siguiente paso lógico con IO-Link Safety. Así, por primera vez es posible una comunicación continua y bidireccional también con los equipos de seguridad.

Las ventajas para el diseño y el funcionamiento son considerables:

Integración de equipos más sencilla

IO-Link reduce las variantes de componentes y permite la parametrización automática en los cambios de producto y la configuración al sustituir componentes en el servicio técnico. Los equipos ya no tienen que →

ajustarse a mano: lo hace automáticamente el control o el módulo de la máquina.

Transparencia y diagnóstico

Con IO-Link, además del estado “puerta cerrada y bloqueo activado”, hay una placa de características electrónica y muchos datos de estado y diagnóstico, como temperatura, intensidad de la señal RFID, estados de fallo y avisos. Además, los datos de funcionamiento, como contadores de ciclos, de fallos y de horas de servicio, dan información valiosa para el mantenimiento predictivo. La configuración y parametrización seguras, junto con comandos de sistema propios, permiten integrar funciones totalmente nuevas.

Conceptos de seguridad flexibles

Con IO-Link Safety, la técnica de seguridad también pasa a definirse por software. Los parámetros de los equipos, los niveles de seguridad o las configuraciones se pueden transmitir de forma digital y documentar de forma centralizada. Esto simplifica tanto la validación según ISO 13849 como la ampliación posterior de las máquinas. Schmersal lanzará sus primeros equipos y componentes con IO-Link e IO-Link Safety ya en el segundo semestre del año, un paso importante hacia una comunicación continua hasta el nivel de sensores y actuadores.

Single Pair Ethernet (SPE): el camino hacia una infraestructura unificada

El volumen creciente de datos de sensores, actuadores y componentes de seguridad exige canales de comunicación potentes. Single Pair Ethernet (SPE) ya se considera el “Industrial Ethernet de próxima generación”, y Schmersal adapta activamente su técnica de seguridad a esta tecnología de futuro.

SPE ofrece ventajas importantes:

Ethernet hasta el sensor

Con un solo par trenzado se consigue una comunicación IP de extremo a extremo, del sensor a la nube. Es decir: se acabaron las islas de bus de campo y los cambios de medio.

Grandes distancias y gran ancho de banda

Con un alcance de hasta 1.000 metros en campo y una alta velocidad de datos, SPE es ideal para grandes instalaciones, intralogística o la industria de procesos.

Menos variedad de cables y conectores

SPE sienta las bases para conectores compactos y conceptos de sensor innovadores en la técnica de seguridad.

Conceptos de seguridad de futuro

Combinado con protocolos de comunicación seguros, crea una plataforma unificada y potente para transmitir señales seguras y no seguras. Para los diseñadores de máquinas, esto significa seguridad en la planificación a largo plazo y la posibilidad de diseñar ya hoy sistemas compatibles con las futuras arquitecturas Ethernet.

Sinergias de la interacción entre tecnologías

Las mayores ventajas surgen de la interacción de las tres tecnologías:

- La SFB se convierte en un nodo de seguridad modular
- IO-Link Safety la completa con una comunicación de equipos flexible y segura
- Single Pair Ethernet aporta la columna vertebral IP para flujos de datos potentes en tiempo real

El resultado es una arquitectura perfecta para conceptos de máquina modernos y escalables: modular, flexible, eficiente, digital y segura en todo momento. Los diseñadores ganan en menor complejidad, los técnicos en una puesta en marcha más sencilla y los desarrolladores en nueva libertad para diseñar funciones de seguridad.

Ventajas prácticas en el diseño

Menos variantes, menos esfuerzo

IO-Link y los nodos SFB modulares reducen la variedad de equipos y simplifican la documentación y el cableado.

Puesta en marcha más rápida

La parametrización digital, la detección automática y un mejor diagnóstico reducen mucho los tiempos de instalación y de servicio.

Nuevos diseños de máquina

SPE y los conceptos de seguridad descentralizados abren nuevos enfoques para unidades de producción móviles, flexibles y conectadas.

Preparados para el futuro

Los proyectistas ya pueden preparar hoy las máquinas para futuras arquitecturas de seguridad basadas en Ethernet. Schmersal ya no ve la técnica de seguridad como componentes sueltos, sino como un sistema integrado, desde la técnica de conexión y la periferia descentralizada hasta la integración digital. ■

Cortar en lonchas y en dados: rápido, preciso y seguro
Controlador de seguridad OEM en máquinas de corte industrial

RESUMEN RÁPIDO

Breve perfil de JBT Marel y las máquinas TREIF

Desde hace más de 75 años, el nombre TREIF es sinónimo de máquinas para cortar alimentos. La empresa de Oberlahr (Westerwald), que forma parte de JBT Marel desde principios de 2025, desarrolla y fabrica, entre otras cosas, slicers (lonchas finas), dicers (cubos) y porcionadoras de muy distintas capacidades. El foco está en maquinaria para la industria alimentaria. Pero, como también hay una amplia gama de cortadoras para el comercio, sobre todo panaderías, las máquinas TREIF también son conocidas por los consumidores.

JBT Marel desarrolla y fabrica una gama muy amplia de máquinas, equipos y sistemas para el procesado de alimentos (carne, aves, pescado, platos preparados, etc.). La planta de Oberlahr tiene un alto grado de integración vertical, incluida la fabricación de cuchillas, y emplea a unas 370 personas. Gracias a su capacidad de innovación y su fuerte presencia en el mercado, la empresa se considera uno de los "hidden champions" del sector de maquinaria e instalaciones y está presente en todo el mundo con filiales y socios de ventas.

Autor: Dirk Plastwich

Systems and Solutions Sales Representatives
Functional Safety Engineer (TÜV Rheinland Certified)

Con su conocida gama TREIF, JBT Marel fabrica en Oberlahr (Westerwald) sistemas de corte industrial y usa en todas sus gamas un control de seguridad compacto a medida, también en la nueva TREIF PUMA, que saldrá al mercado en breve. Esta solución tiene ventajas claras, no solo para el fabricante de la máquina, sino también para los operarios.

Filetes, pastel de carne, chuletas: la "TREIF PUMA" de JBT Marel corta alimentos a gran velocidad, con mucha precisión y gran flexibilidad. Por eso esta serie se usa en todo el mundo, sobre todo en muchas plantas cárnicas. En la planta de Oberlahr (Westerwald) se prepara ahora la producción en serie de la nueva generación de PUMA. **(Figura 1)**



Image 1: Shortly before market launch: The new generation of the Puma series will set new standards for the fast and precise cutting of meat.

Compacto y a medida: el (pequeño) controlador de seguridad

Incluso con el rendimiento máximo de 260 cortes por minuto y con frecuentes cambios manuales de producto, los operarios no tienen que preocuparse por la seguridad durante el corte. La seguridad es una prioridad absoluta para los diseñadores, como demuestra el concepto de manejo que veremos más adelante. Además, la nueva TREIF PUMA, como su predecesora y la mayoría de máquinas TREIF que fabrica JBT Marel, lleva un controlador de seguridad compacto PROTECT SELECT OEM. (Figura 2) Schmersal programa y valida el controlador según las especificaciones y requisitos del cliente, en este caso JBT Marel. Se entrega como controlador de seguridad totalmente programado y validado, con una selección de programas de aplicación. Las configuraciones de E/S, combinaciones de aparamenta de seguridad y señales adecuadas para cada tipo de máquina se eligen mediante los programas de aplicación del PROTECT SELECT OEM, según el concepto de seguridad desarrollado para las máquinas TREIF.

Primero seis, ahora siete programas de aplicación en un solo controlador

Desde hace varios años, los ingenieros usan este controlador de seguridad específico de OEM en las máquinas TREIF. Mike Vogelsberg, jefe de desarrollo de software e ingeniería eléctrica: "Antes teníamos distintos modelos de control para cada gama." →



Figura 2: la unidad de control de las nuevas cortadoras PUMA. A la derecha de la imagen: el controlador de seguridad compacto PROTECT SELECT OEM.

Desde que pasamos a PROTECT SELECT, la gestión del stock es mucho más sencilla y las funciones de seguridad se ajustan perfectamente a nuestras necesidades, en todas las gamas. Tras la instalación solo hay que dar de alta el controlador y elegir las aplicaciones correspondientes."

Al principio había seis programas de aplicación, escritos por especialistas en software de Schmersal. Sus funciones incluyen, por ejemplo, la coordinación segura de la vigilancia y el manejo de la tapa protectora, el avance (pinza), la cinta de salida y la cuchilla, así como posiciones de mantenimiento definidas. También se tiene en cuenta desde el punto de vista de la seguridad la apertura opcional de la tapa por muelle, no eléctrica, que permite cargar más rápido el nuevo material de corte.

Para la nueva generación de controles PUMA, los programadores de Schmersal han "programado" ahora una séptima aplicación en el controlador. Y, si hace falta, se pueden añadir fácilmente más funciones o programas para nuevos requisitos. Así, este tipo de controlador de seguridad está preparado para el futuro y se puede usar en distintas gamas.

La amplia conectividad del PROTECT SELECT OEM (18 entradas digitales seguras y dos analógicas seguras, seis salidas seguras) abre muchos escenarios de aplicación. Una interfaz unidireccional permite procesar señales y mejora la usabilidad, a la vez que reduce el cableado.

De serie en todas las máquinas: Safe Torque Off

Una aplicación que se usa en todas las máquinas con PROTECT SELECT OEM es la función de parada de emergencia "Safe Torque Off". Los programas de aplicación se eligen fácilmente según la necesidad o durante la instalación, porque una sola versión del controlador de seguridad compacto PROTECT SELECT OEM cubre una amplia gama de máquinas. Mike Vogelsberg: "Usamos el PROTECT SELECT OEM no solo en porcionadoras como la TREIF PUMA, sino también, entre otras, en dicers, máquinas que cortan bacon y jamón en cubos, y en las cortadoras de pan autoservicio de los supermercados, que llevan enclavamientos con bloqueo. Solo nuestras máquinas más complejas, con funciones de seguridad especialmente sofisticadas que suelen requerir funciones de accionamiento seguras como Safe Limited Speed, llevan un PLC de seguridad adecuado."

Estrecha colaboración en la fase de programación

Al definir las aplicaciones necesarias y asignar entradas y salidas, los expertos en seguridad de Schmersal trabajaron estrechamente con el equipo de desarrollo de TREIF; los programadores de Schmersal visitaron varias veces la planta de Oberlahr. El resultado: la lógica del programa se adapta perfectamente a las funciones de la máquina, se han trasladado los códigos de varios controles usados antes y también se ha hecho una pequeña modificación de hardware. Un examen de tipo del software formó parte de los servicios de Schmersal.

Cortes higiénicos y precisos: la nueva PUMA

Más estandarización a nivel de accionamientos y de máquina fue un objetivo clave del equipo de diseño de Mike Vogelsberg en el desarrollo de la nueva generación PUMA, un enfoque que ya ha dado buenos resultados en seguridad de máquinas. "Los accionamientos tienen control de velocidad. El operario introduce el grosor de las lonchas y la cadencia por minuto, y la máquina se ajusta sola." El control coordina los accionamientos, y el modo de funcionamiento del controlador de seguridad compacto se coordina a su vez con las señales de funcionamiento.

Manejo: lo más intuitivo posible, y con la nueva serie H

En el manejo de la PUMA y de otras máquinas, los diseñadores siguen el principio de "menos es más". Mike Vogelsberg: "Las máquinas se usan a menudo en empresas pequeñas. No suelen manejarlas electricistas, sino personal de plantas cárnicas o de panaderías. Por eso el objetivo es que el manejo sea lo más sencillo e intuitivo posible." Se consigue con una pantalla táctil **(figura 3)** y unos pocos elementos físicos de mando. TREIF usa para ello la serie H de elementos de mando de Schmersal. **(Figuras 4 y 5)** Esta serie se lanzó hace poco y cumple también estándares de higiene muy altos. Justo lo que se exige a las máquinas TREIF, como explica Mike Vogelsberg: "Lo probamos todo. Lo montamos con mucho cuidado para asegurar que aguanta →



Figura 3: todo a la vista: la pantalla táctil de la PUMA.

limpiezas frecuentes e intensas, y literalmente probamos muchas cosas hasta que se rompen. Pero siempre hemos estado satisfechos con los interruptores de la anterior serie N de Schmersal, así que ahora pasaremos poco a poco a la serie sucesora." Según Vogelsberg, las slicers en particular tienen requisitos de higiene muy altos: "Estas máquinas cortan a menudo productos crudos que se comen tal cual, sin cocinar. Las naves son más frías y los estándares de higiene, más altos."

En el punto de mira: diseño a prueba de manipulaciones

Al desarrollar tanto los resguardos como la HMI (interfaz persona-máquina) de las máquinas TREIF, la resistencia a la manipulación es clave, ya que si se puentean los resguardos el riesgo de lesión es alto. Por eso, por ejemplo, los imanes de los sensores de seguridad están ocultos y se exige un ciclo de prueba al encender las máquinas: hay que abrir y cerrar una vez el resguardo para comprobar que la función de parada de seguridad actúa correctamente con el resguardo abierto. El controlador de seguridad compacto OEM también vigila este ciclo.

Las ventajas de una solución de seguridad a medida



Figura 4: ergonómica e higiénica: la unidad de mando de los sistemas TREIF.

Figura 5: los elementos de mando de la serie H de Schmersal (aquí un interruptor principal) cumplen el estándar de higiene más alto.

En resumen, los responsables de la gama TREIF lo tienen claro: la estandarización basada en el principio "un controlador para todo" ahorra costes, reduce la complejidad y simplifica la gestión del stock, mientras que la versión OEM incluye todas las funciones necesarias para un funcionamiento seguro. Las variantes necesarias para los distintos tipos y series de máquinas están integradas en el controlador; el programa de aplicación correspondiente se activa en la instalación con botones de selección y la pantalla táctil.

En TREIF también están satisfechos con los "aspectos blandos": según Mike Vogelsberg, la colaboración continua funciona bien. Por eso las nuevas generaciones de máquinas llevarán cada vez más aparamenta higiénica de la serie H de Schmersal, además de la versión OEM específica para TREIF del controlador de seguridad compacto. ■



Figura 6: Mike Vogelsberg, jefe de desarrollo de software e ingeniería eléctrica, en el centro técnico de la gama TREIF, delante de la slicer "LevelUp", que como la PUMA está a punto de salir al mercado.



Desde 2023, la Safety Fieldbox forma parte de la gama de Schmersal de unos 13.000 productos con certificación UL.

Conforme a norma, fiable y preparada para el futuro.

Certificación UL de la aparamenta de seguridad

RESUMEN RÁPIDO

La certificación UL de un vistazo

- Requisito previo para muchas aplicaciones en Norteamérica
- Requisitos adicionales a los de las normas IEC
- Foco en seguridad de producto, materiales e instalación
- Evaluación del producto y de la fabricación
- Auditorías periódicas del centro de producción

Autor: Jörg Eisold, Dipl.-Ing. (FH)

Responsable de Normas, Comités y Asociaciones

La aparamenta de seguridad es un componente clave de las máquinas modernas. Ya sean interruptores de posición, sensores optoelectrónicos o sistemas de seguridad RFID, deben funcionar de forma fiable y, sobre todo, estar homologados para usarse en todo el mundo.

Mientras que en Europa el marcado CE se basa en la serie de normas IEC 60947-5-x, el mercado norteamericano impone requisitos adicionales. Allí la regla es que, sin la certificación de un organismo de ensayo reconocido como UL (Underwriters Laboratories), el acceso al mercado es en muchos casos prácticamente imposible.

Aunque UL ha ido alineando sus normas con la serie IEC, aunque las normas converjan, las filosofías de seguridad siguen siendo distintas.

Las normas de la serie IEC 60947-5-x establecen cómo debe funcionar un equipo, incluidos parámetros eléctricos, propiedades mecánicas y condiciones ambientales. Esta base técnica se incorpora al marco de normas UL, por ejemplo como UL 60947-5-1 o UL 60947-5-2, pero se completa con requisitos nacionales. Además, los productos deben instalarse según el National Electrical Code (NEC), que impone restricciones adicionales.

Los requisitos nacionales adicionales se refieren, por ejemplo, al comportamiento frente al fuego del equipo, a los materiales usados y a la seguridad en caso de instalación incorrecta. Por eso, incluso productos técnicamente maduros que cumplen las normas IEC no son automáticamente conformes con UL. En los interruptores de seguridad convencionales según IEC 60947-5-1, el foco está en características como la apertura forzada, la robustez mecánica y la vida útil.

La certificación UL incluye varios aspectos adicionales, como la evaluación de distancias en el aire y líneas de fuga, la verificación de las propiedades de los materiales (p. ej., inflamabilidad) y ensayos en condiciones de carga y fallo propias de UL.

Un punto clave es usar materiales homologados (p. ej., plásticos con “UL Yellow Card”). Esto convierte la elección de materiales en un factor crítico del desarrollo. En los sensores sin contacto según IEC 60947-5-2, el foco se desplaza aún más hacia la aplicación. Mientras la norma IEC describe la función del sensor, como las distancias de conmutación o la CEM, UL considera el sistema completo, incluida la alimentación, el cable de conexión, la protección en el armario eléctrico y el entorno de funcionamiento. Así, el sensor no solo se evalúa por sí solo: también hay ensayos UL del sistema completo.

Con sensores de seguridad modernos, como los sistemas RFID, la complejidad aumenta. La IEC 60947-5-3 exige una respuesta definida ante fallos (comportamiento determinista), la vigilancia de estados internos y la integración de principios de seguridad funcional. Esto es un reto especial para la certificación UL, porque hay que evaluar funciones electrónicas y de software. Además, hay que demostrar un comportamiento seguro en caso de fallo. Por eso aquí tienen un papel clave tanto la seguridad funcional como la seguridad de producto clásica. Los requisitos adicionales deben tenerse en cuenta desde el principio del desarrollo, por ejemplo al elegir materiales y componentes homologados.

Otro aspecto importante es que UL no solo evalúa el producto, sino también el proceso de fabricación. El centro de producción figura también en el expediente UL del producto certificado. Para ello se hacen auditorías periódicas en cada centro de producción.

Una vez cumplidos todos los requisitos, realizados los ensayos necesarios y aportadas las pruebas formales, nada impide acceder al mercado norteamericano. ■

Seguridad en robots humanoides
Nuevos retos para los conceptos de seguridad y la seguridad funcional

RESUMEN RÁPIDO

Seguridad en robots humanoides:
Como muchos robots no estacionarios o interactivos, los robots humanoides trabajan directamente junto a las personas y usan cada vez más IA para reconocer su entorno y actuar de forma autónoma. Esto genera nuevos requisitos de seguridad que los diseños de máquinas clásicos solo cumplen en parte.

Riesgos clave:
- Riesgo de caída si falla la alimentación
- Colisiones por movimientos rápidos
- Comportamiento de la IA difícil de prever
- Ciberataques a sistemas conectados

Por eso ganan importancia la seguridad funcional, la fusión de sensores, las funciones de movimiento seguras y la ciberseguridad. Las normas existentes se están ampliando para cubrir mejor los sistemas robóticos con IA.

Autora: Katrin Wirz
Product Manager K.A. Schmersal GmbH & Co. KG



¿Qué es un robot humanoide?

Los robots humanoides están a punto de pasar del laboratorio a la aplicación industrial. Prometen una nueva forma de automatización: flexible, adaptable y lista para usarse de inmediato en entornos de trabajo humanos. **Pero al mismo tiempo surgen cuestiones de seguridad que los conceptos clásicos de la Directiva de Máquinas solo resuelven en parte.**

Los robots humanoides se caracterizan por su diseño parecido al humano y su capacidad de interactuar con el entorno. Suelen tener un torso, dos brazos, varios sensores y un medio de desplazamiento, con piernas o con sistemas alternativos.

Pero lo decisivo no es solo su forma, sino su función: están pensados para asumir tareas humanas e integrarse en entornos de trabajo existentes. Esta característica no distingue en lo esencial a los robots móviles de los robots industriales clásicos, que suelen trabajar en células cerradas y están optimizados para tareas concretas.

Las crecientes posibilidades de integrar inteligencia artificial (IA) refuerzan mucho esta tendencia. Los sistemas modernos pueden percibir su entorno, interpretar situaciones y tomar decisiones a partir de ellas. Así se alejan de los sistemas estrictamente deterministas y se acercan a procesos de decisión basados en cálculos de probabilidad. Esta nueva calidad abre por un lado posibilidades enormes, pero por otro trae nuevas incertidumbres, sobre todo en cuanto a la previsibilidad del comportamiento.

Ámbitos de aplicación y actores del mercado

El futuro papel de los robots inteligentes se verá sobre todo donde se necesite flexibilidad y capacidad de adaptación. En la producción industrial pueden asumir tareas que antes eran exclusivas de las personas, sin grandes modificaciones de las instalaciones existentes. Esto se considera una gran ventaja, sobre todo con la falta de personal cualificado, ya que los robots colaborativos pueden asumir tareas físicamente duras, monótonas o peligrosas. Además, hay oportunidades en logística, sanidad y servicios. Las aplicaciones van desde el apoyo en cuidados y tareas de servicio hasta intervenciones en entornos peligrosos, como operaciones de rescate. →

El mercado de la robótica humanoide está dominado ahora por varios actores internacionales. Empresas como Boston Dynamics y el Toyota Research Institute impulsan sobre todo el desarrollo de movimientos muy dinámicos y modelos de comportamiento basados en IA. Con el proyecto Optimus, Tesla apuesta por la escala industrial, mientras que empresas como SoftBank Robotics y Hanson Robotics se centran en la interacción social. Al mismo tiempo, empresas como Unitree Robotics y UBTECH desarrollan sistemas compactos y relativamente baratos. Todos estos enfoques comparten la combinación de actuadores avanzados, sensores potentes y una arquitectura de software cada vez más compleja.

Retos de seguridad y nuevas dimensiones del riesgo

La combinación de interacción física y control inteligente plantea nuevos retos de seguridad. A diferencia de los robots industriales clásicos, a menudo no es posible mantener una separación física entre "persona y máquina". Al contrario, los robots humanoides se usan precisamente para interactuar directamente con las personas, y el foco pasa del aislamiento a la colaboración segura.

Un riesgo clave está en el diseño mecánico de estos sistemas. Los robots humanoides, por ejemplo, suelen ser dinámicamente inestables y deben controlar su equilibrio de forma activa y continua. Una desconexión brusca o una pérdida de alimentación, como la que provoca el "Safe Torque Off (STO)", no lleva por tanto a un estado seguro, sino que puede provocar una caída. En ese momento, el robot se convierte en un objeto sin control con una energía cinética considerable, lo que supone un alto riesgo de lesión, sobre todo en sistemas grandes.

Además, hay riesgos importantes de colisión. Por su inercia y su masa, incluso robots pequeños pueden generar fuerzas que superan los umbrales de dolor normalizados. En los robots humanoides este riesgo aumenta por la gran movilidad de todo el cuerpo, incluidas piernas, torso y brazos. Además de los riesgos físicos, hay retos de software. Al mismo tiempo, se exige más en el reconocimiento de situaciones y contextos: un robot no solo debe reconocer que un objeto se mueve, sino también entender si es, por ejemplo, una herramienta o un peligro potencial.

Los aspectos de ciberseguridad y seguridad de los datos también ganan mucho peso. Los robots suelen procesar grandes cantidades de datos sensibles y están cada vez más conectados, por lo que pueden ser objetivo de ataques. Las estrategias de seguridad deben tener en cuenta no solo la integridad física, sino también la digital.

Conceptos de seguridad, normas y clasificación industrial

En este contexto surgen nuevas arquitecturas de seguridad que van más allá de los conceptos clásicos. Los enfoques modernos combinan varios niveles de protección. En el nivel más bajo están las funciones seguras de accionamiento y movimiento, que por ejemplo limitan velocidades y fuerzas o aportan mecanismos de amortiguación activos. Se completan con una vigilancia completa del entorno basada en la fusión de sensores, que capta el espacio de trabajo como un campo de seguridad tridimensional y lo evalúa de forma dinámica. Además, ganan importancia los sistemas de supervisión de nivel superior, que analizan el comportamiento de la propia IA y pueden intervenir en situaciones críticas.

Desde el punto de vista regulatorio, este campo tecnológico aún está en desarrollo. Normas existentes como ISO 12100, ISO 10218 e ISO 13482 son una base importante, pero su aplicación a sistemas humanoides es limitada. En particular, aspectos como la estabilidad dinámica, los procesos de decisión basados en IA y el funcionamiento seguro ante una pérdida de alimentación no están del todo cubiertos en los marcos existentes. Al mismo tiempo, ganan importancia marcos regulatorios generales como el nuevo Reglamento de Máquinas (UE) 2023/1230, que establece por primera vez requisitos explícitos para sistemas basados en software y con IA.

Seguridad funcional y evaluación sistemática de la seguridad

Un aspecto clave que va más allá de las consideraciones de seguridad clásicas es aplicar de forma coherente la seguridad funcional a los sistemas robóticos que interactúan. Mientras que normas como ISO 12100 dan un marco para la evaluación de riesgos, IEC 61508 e ISO 13849 aportan sobre todo la base metodológica para desarrollar sistemas relativos a la seguridad.

La seguridad funcional abarca el análisis, la especificación y la validación de las funciones de seguridad, incluida la demostración de su fiabilidad. Incluye componentes de hardware y software y cubre toda la arquitectura del sistema. Este enfoque es cada vez más importante en todos los robots, porque las funciones críticas para la seguridad ya no dependen solo de elementos de control clásicos, sino que se implementan cada vez más con software complejo y algoritmos de IA.

Un componente clave es la evaluación sistemática de los riesgos de fallo. Tiene en cuenta tanto los fallos aleatorios de hardware como los errores sistemáticos, por ejemplo en el software o en los modelos de IA. El objetivo es demostrar que el sistema completo alcanza niveles de seguridad definidos →

(p. ej., SIL o Performance Level) y que los fallos críticos ocurren con una probabilidad suficientemente baja.

Además, hace falta una visión integral del ciclo de vida. Las evaluaciones de seguridad no solo deben cubrir la fase de diseño, sino también el funcionamiento, el mantenimiento, las actualizaciones y el comportamiento de aprendizaje del sistema. Sobre todo en sistemas con IA, el comportamiento puede cambiar con el tiempo, lo que exige procesos continuos de evaluación y validación.

Los componentes semiconductores tienen un papel especialmente importante. Procesadores, chips de sensores y aceleradores de IA son la base técnica de la percepción, la decisión y la actuación. Los fallos en estos componentes pueden llevar directamente a situaciones críticas. Por eso hay que evaluar específicamente estos componentes, incluida su arquitectura, sus mecanismos de fallo y su integración en el sistema.

Además, ganan importancia las evaluaciones de seguridad específicas de la IA. Enfoques normativos como la ISO/PAS 8800 tratan el análisis sistemático de modelos de IA, incluida su robustez, su capacidad de generalización y sus posibles errores. El objetivo es integrar procesos de decisión no deterministas en un marco de seguridad robusto.

Además del análisis, el foco está en validar las medidas de reducción del riesgo. Entre ellas:

- Sensores y fusión de sensores para una percepción fiable del entorno
- Limitación de velocidad, fuerzas y áreas de trabajo
- Funciones de movimiento seguras y estrategias de parada controlada
- Visualización y simulación de zonas de peligro

Estas medidas no solo deben implantarse, sino también revisarse de forma sistemática y demostrar su eficacia.

Al fin y al cabo, la seguridad funcional está muy ligada a la ciberseguridad. Los sistemas humanoides conectados deben protegerse frente a manipulaciones y accesos no autorizados, por ejemplo según la IEC 62443. Solo combinando seguridad funcional y seguridad IT se puede aplicar una estrategia de protección completa.

Abrir nuevos mercados

Esto supone retos y oportunidades para las empresas de técnica de seguridad. El Grupo Schmersal, como proveedor consolidado de componentes y sistemas de seguridad, tiene un amplio conocimiento en seguridad funcional de máquinas. Estas capacidades pueden aplicarse en muchos ámbitos de las aplicaciones humanoides, como el procesamiento seguro de señales, el control de funciones de seguridad y la protección de áreas de trabajo. Al mismo tiempo, habrá que seguir desarrollando las tecnologías existentes para cumplir nuevos requisitos, como la vigilancia tridimensional del entorno o la evaluación de seguridad basada en IA.

En resumen, los robots móviles, incluidos los humanoides, ofrecen un gran potencial de innovación, pero exigen a la vez un cambio de paradigma en la seguridad de las máquinas. Los enfoques clásicos, como la desconexión segura o la separación física entre personas y máquinas, llegan a su límite. En su lugar, el foco pasa a enfoques de seguridad adaptativos y en varias capas que integran aspectos mecánicos, sensoriales y de IT. El éxito de esta tecnología dependerá en gran medida de si se logra un nivel de seguridad sólido sin renunciar a su potencial económico. ■

Fuentes:

- Fraunhofer IPA, Guidelines on the Safety of Humanoid Robots, septiembre de 2025
- White Paper, Out of the Cage: Advanced Functional Safety for Humanoids – Positron Safety AI Architecture, Synapticon GmbH, Dr.-Ing. Florian Weißhardt, Dr.-Ing. Tim Fröhlich, Dieter Volpert, 23 de enero de 2026
- Safety considerations for humanoid robots, 2026, Industriezeitschrift.de
- SGS-Société Générale de Surveillance SA (2026), folleto “Safety Assessment for Humanoid Robots”
- 1) Normas:

  ISO 12100: Seguridad de las máquinas. Principios generales para el diseño. Evaluación y reducción del riesgo
  ISO 10218: Robótica. Requisitos de seguridad, parte 1: robots industriales, parte 2: aplicaciones y células robotizadas
  ISO 13482: Robots y dispositivos robóticos. Requisitos de seguridad para robots de cuidado personal
  IEC 61508: Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad
  ISO 13849: Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad
  ISO/PAS 8800:2024: Vehículos de carretera. Seguridad e inteligencia artificial
  IEC 62443: Redes de comunicación industrial. Seguridad IT para redes y sistemas



Los robots humanoides abren nuevas posibilidades en la industria. Su uso exige normas y reglas de seguridad claras. La clave es una integración segura en los procesos existentes.

Consignación digital (lockout/tagout)

Mantenimiento fiable sin montañas de papeles

RESUMEN RÁPIDO

Puntos clave para los usuarios

- LOTO sigue siendo un proceso central del mantenimiento seguro, sobre todo al trabajar con fuentes de energía, energía residual y zonas peligrosas.
- tec.dloto no sustituye el bloqueo físico, pero hace mucho más sólidas la preparación, la autorización, la verificación y la liberación.
- Empezando por un código QR, la guía paso a paso, las imágenes de referencia, las fotos como prueba y las aprobaciones ayudan a reducir los fallos típicos de los procesos en papel.
- Los registros centralizados, los dashboards y los registros auditables dan a los responsables de seguridad más transparencia en el día a día.
- Como parte de la oferta de servicios de tec.nicum, la solución se integra de forma práctica en los procesos existentes de la planta, con apoyo de consultoría, formación, ingeniería e integración.

Autor: Tobias Keller

Head of Administration,
tec.nicum



Con tec.dloto, tec.nicum, la división de servicios del Grupo Schmersal, ofrece una solución digital que convierte los procedimientos LOTO tradicionales en procesos guiados, trazables y listos para auditoría.

El mantenimiento es el momento en que la seguridad de las máquinas se vuelve especialmente tangible. Se activan resguardos, se paran accionamientos, se desconectan fuentes de energía y se disipa la energía residual. Mientras que en producción la seguridad se garantiza con procedimientos fijos y dispositivos técnicos, la seguridad durante el mantenimiento, la limpieza, la resolución de averías o las modificaciones depende a menudo de una buena preparación y una aplicación coherente. Justo ahí entra en juego la consignación (lockout/tagout), y justo ahí se ve por qué una solución digital como tec.dloto es más que un software cómodo para los usuarios de instalaciones industriales.

Lockout/Tagout, LOTO para abreviar, es un procedimiento sistemático para controlar fuentes de energía peligrosas. “Lockout” es el bloqueo físico de un dispositivo de aislamiento de energía, como un interruptor principal, una válvula o un dispositivo de corte. “Tagout” completa ese bloqueo con una señalización clara: quién ha hecho el bloqueo, por qué, y que el equipo no debe volver a ponerse en marcha. El concepto de este procedimiento viene de la seguridad laboral anglosajona. Fue especialmente importante la norma estadounidense OSHA 29 CFR 1910.147, “The control of hazardous energy”, que desde finales de los años 80 establece requisitos de programas, procedimientos, formación e inspecciones periódicas para trabajos de mantenimiento y reparación.

El concepto de seguridad de fondo también está bien asentado en Europa y en Alemania, aunque no siempre se use el término “LOTO”. La ISO 14118 trata la prevención de la puesta en marcha inesperada de las máquinas y cubre distintas formas de energía: eléctrica, hidráulica y neumática, así como la energía cinética almacenada, por ejemplo por posición, presión o muelles. El reglamento alemán de seguridad operativa también exige que los equipos de trabajo puedan pararse y separarse de sus fuentes de energía de forma segura. El principio práctico es el mismo en todas partes: una máquina no debe arrancar de forma inesperada durante trabajos peligrosos, y la energía almacenada no debe liberarse sin control.

Por eso, un procedimiento LOTO estándar sigue una lógica clara. Primero se prepara el trabajo y se identifican todas las fuentes de energía relevantes. La máquina →

se para de forma ordenada, se separa de sus fuentes de energía y se asegura para que no pueda volver a conectarse. Después se disipa o se controla de forma fiable la energía residual. Solo se puede empezar a trabajar tras comprobar que la instalación está sin energía o en un estado seguro. Antes de volver a ponerla en marcha hay que revisar la zona de trabajo y la máquina, informar al personal correspondiente y retirar correctamente los dispositivos de bloqueo. Parece sencillo, pero en el día a día es propenso a errores, sobre todo con instalaciones complejas, cambios de turno, contratas, prisas o tareas de mantenimiento que cambian a menudo.

Principio básico de LOTO:
Preparar el trabajo, identificar las fuentes de energía, parar y aislar la máquina, bloquearla y señalizarla, descargar o asegurar la energía residual, verificar que está en estado seguro y, al terminar, liberarla de nuevo tras una comprobación.

Las soluciones manuales tradicionales suelen usar instrucciones impresas, formularios, etiquetas, candados personales y registros a mano. Los candados físicos siguen siendo imprescindibles para la protección in situ. Pero la parte organizativa suele ser menos fiable: los papeles se pierden, se vuelven ilegibles o ya no reflejan la situación actual. Las fotos se guardan en dispositivos privados o dispersos, las autorizaciones se dan por teléfono o e-mail y, en una auditoría, cuesta mucho reconstruir quién hizo qué paso y cuándo. Aún más crítica es la falta de visibilidad mientras se trabaja. Con procedimientos solo manuales, los mandos y responsables de seguridad a menudo solo saben después si un proceso se ha documentado completo y bien.



tec.dloto ataca justo estos puntos débiles. La solución de tec.nicum es una plataforma web y móvil para la gestión LOTO. Digitaliza el proceso de aislamiento de energía y guía a los usuarios por los pasos necesarios. El proceso empieza de forma práctica: el trabajador escanea un código QR en la máquina, inicia la solicitud LOTO y recibe instrucciones digitales paso a paso. Las imágenes de referencia ayudan a identificar sin dudas el punto de corte o el fusible correcto. Las fotos subidas y las comprobaciones documentan el estado real in situ. Los pasos críticos se pueden asegurar con flujos de aprobación antes de empezar el mantenimiento.



Así, una checklist se convierte en un proceso guiado. Cada acción queda registrada con fecha y hora, las acciones se asignan a cada usuario y el historial LOTO está disponible de forma consolidada. Esto da a responsables de seguridad, mandos y directores de planta una transparencia que con papel solo se consigue con mucho esfuerzo. Dashboards, seguimiento en vivo, notificaciones y una vista centralizada de las instalaciones muestran qué medidas LOTO están activas, qué autorizaciones están pendientes y dónde se está trabajando. Esto no solo reduce el estrés de las auditorías, sino que mejora la gestión diaria.

La ventaja frente a las soluciones manuales no está solo en no usar papel. La clave es que tec.dloto aporta compromiso al proceso. No es tan fácil saltarse pasos, las instrucciones obsoletas se sustituyen de forma centralizada y las responsabilidades quedan trazadas en el sistema. Donde antes había que juntar documentos dispersos, carpetas locales y acuerdos verbales, ahora se generan registros listos para auditoría, con fotos, fecha y hora y roles bien definidos. También es más fácil que personal nuevo o empresas externas se pongan al día, porque no solo reciben instrucciones, sino que el sistema les guía por el proceso. →



LOTO mejora la seguridad en los trabajos de mantenimiento. Las soluciones digitales hacen los procesos eficientes y trazables.

Esto supone un valor añadido importante para los clientes de tec.nicum. tec.nicum no ve tec.dloto como una herramienta IT aislada, sino como parte de una oferta de servicios completa en todo lo relacionado con la seguridad de máquinas y la seguridad laboral. tec.nicum – Solutions & Services GmbH forma parte del Grupo Schmersal y reúne servicios de las áreas academy, consulting, engineering, integration, digitalisation y outsourcing. Esto es importante porque un sistema LOTO eficaz no termina al comprar el software. Hay que adaptar los procesos a la planta, definir bien los roles, formar al personal y mantener los procedimientos según las necesidades de la operación. Justo ahí tec.nicum puede apoyar a sus clientes.

En la práctica, esto significa que las empresas no solo reciben una plataforma digital, sino también ayuda para montar un proceso LOTO sólido, escalable y verificable. tec.dloto admite acceso móvil, puede usarse en la nube o on-premise y facilita el arranque con cargas masivas y flujos de trabajo personalizables. Así, la solución crece con la organización. En el futuro se podrían añadir más módulos de seguridad, como funciones de permiso de trabajo. Para usuarios con varias líneas, plantas o equipos rotativos, esta escalabilidad es una ventaja clave.

Sobre todo en tareas críticas para la seguridad, la digitalización solo tiene sentido si facilita y hace más seguro el trabajo in situ. tec.dloto lo cumple porque no sustituye los principios básicos probados de la consignación, sino que asegura que se apliquen de forma coherente. La separación física y el bloqueo siguen siendo lo esencial. La solución digital asegura que la preparación, la aprobación, la verificación y la devolución se gestionen y documenten bien. Así se crea un vínculo práctico entre seguridad y salud, mantenimiento y cumplimiento normativo. ■

La conclusión es clara: LOTO no es un mero trámite, sino un elemento clave del mantenimiento seguro. Los métodos manuales pueden funcionar, pero exigen mucha disciplina. Con tec.dloto, tec.nicum ofrece a sus clientes un servicio que va más allá de la herramienta y hace este proceso más profesional, transparente y eficiente. Para los clientes significa menos papeleo, menos incertidumbre, verificaciones más rápidas y una base mucho mejor para gestionar con fiabilidad los trabajos críticos para la seguridad.

Imágenes: K.A. Schmersal GmbH & Co. KG, shutterstock.com,
JBT Marel para el caso práctico de las máquinas TREIF

Edita:

tec.nicum

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