



Sistemas de control relacionados con la seguridad para maquinaria

Principios, normas e implementación
(Revisión 5 de la serie Safebook)

LISTEN.
THINK.
SOLVE.™

**Rockwell
Automation**

Sistemas de seguridad para maquinaria industrial

Índice

Capítulo 1	Reglamentos Directivas y legislación de la UE, Directiva de maquinaria, Directiva de uso de equipo de trabajo, Regulaciones de EE.UU., Administración de Salud y Seguridad Ocupacional, Regulaciones canadienses	2
Capítulo 2	Normas ISO (Organización Internacional de Normalización), IEC (Comisión Electrotécnica Internacional), Normas Europeas Armonizadas (EN), Normas OSHA, Normas ANSI, Normas canadienses, Normas australianas	18
Capítulo 3	Estrategia de seguridad Evaluación de riesgos, determinación de límites de máquina, identificación de tareas y riesgo, estimación de riesgo y reducción de riesgo, diseño inherentemente seguro, sistemas y medidas de protección, evaluación, formación técnica, equipo de protección personal, normas	22
Capítulo 4	Implementación de medidas de protección Prevención de arranques imprevistos, bloqueo-etiquetado de seguridad, sistemas de aislamiento de seguridad, prevención de acceso, resguardos de aislamiento fijos, detección de acceso y tecnologías y sistemas de seguridad	34
Capítulo 5	Cálculo de la distancia de seguridad Fórmulas, orientación y aplicación de soluciones de seguridad mediante cálculos de la distancia de seguridad para un control seguro de las piezas móviles potencialmente peligrosas.	56
Capítulo 6	Sistemas de control relacionados con la seguridad y seguridad funcional Introducción, ¿qué es la seguridad funcional? IEC/EN 62061 y (EN) ISO 13849-1:2008, SIL e IEC/EN 62061, PL y (EN) ISO 13849-1:2008, comparación de PL y SIL	60
Capítulo 7	Diseño de sistemas según (EN) ISO 13849 SISTEMA, arquitecturas de sistemas de seguridad (estructuras), tiempo de misión, tiempo medio antes de un fallo peligroso ($MTTF_p$), cobertura de diagnóstico (DC), fallo por causas comunes (CCF), fallo sistemático, nivel de rendimiento (PL), combinaciones y diseños de subsistemas, validación, puesta en servicio de equipos, exclusión de fallos	66
Capítulo 8	Diseño de sistemas según IEC/EN 62061 Diseño de subsistemas – IEC/EN 62061, influencia del intervalo de prueba de calidad, influencia del análisis de fallo por causas comunes, metodología de transición para categorías, limitaciones arquitectónicas, B10 y B10d, fallo por causas comunes (CCF), cobertura de diagnóstico (DC), tolerancia a fallos de hardware, gestión de la seguridad funcional, probabilidad de fallo peligroso (PFH_p), intervalo de prueba de calidad, fracción de fallos seguros (SFF), fallo sistemático	87
Capítulo 9	Sistemas de control relacionados con la seguridad, consideraciones adicionales Descripción general, categorías de sistemas de control, fallos no detectados, clasificación de componentes y sistemas, consideraciones de fallo, exclusiones de fallo, categorías de parada según IEC/EN 60204-1 y NFPA 79, requisitos de sistemas de control de EE.UU., normas de robots: EE.UU. y Canadá	98
Capítulo 10	Ejemplos de aplicación Ejemplo de aplicación del uso de la calculadora del nivel del rendimiento SISTEMA con la biblioteca de productos Rockwell Automation SISTEMA.	110
Capítulo 11	Productos, herramientas y servicios Productos, tecnologías, herramientas y servicios disponibles de Rockwell Automation.	138



Capítulo 1: Reglamentos

Directivas y legislación de la Unión Europea

Esta sección se proporciona como guía para las personas encargadas de la seguridad de máquinas, especialmente sistemas protectores de resguardos y sistemas de protección en la Unión Europea. Ha sido concebida para diseñadores y usuarios de equipo industrial.

Con el objeto de promover el concepto de un mercado abierto dentro del Área Económica Europea (EEA) (que comprende todos los estados miembros de la UE y tres países adicionales) todos los estados miembros están obligados a promulgar legislación que defina los requisitos de seguridad esenciales para la maquinaria y su uso.

La maquinaria que no cumpla estos requisitos no podrá suministrarse a o dentro de los países de la EEA.

Hay varias directivas europeas que pueden aplicarse con la seguridad de máquinas y equipos industriales, pero las dos que tienen la relevancia más directa son:

1 La Directiva de maquinaria

2 El uso de equipos de trabajo por parte de los trabajadores según la Directiva de trabajo

Estas dos directivas están directamente relacionadas con los Requisitos Esenciales de Seguridad y Salud (RESS) de la directiva de máquinas, y pueden usarse para confirmar la seguridad del equipo indicada en la Directiva de uso de equipos de trabajo.

Esta sección trata aspectos de ambas directivas, y se recomienda enfáticamente que las personas relacionadas con el diseño, el suministro, la compra o el uso de equipo industrial a o dentro de la EEA y también algunos otros países europeos se familiaricen con sus requisitos. La mayoría de suministradores y usuarios de maquinaria simplemente no podrán suministrar ni operar maquinaria en estos países a menos que cumplan con estas directivas.

Hay otras directivas europeas que pueden ser pertinentes a la maquinaria. La mayoría son especializadas en su aplicación y, por lo tanto, no se incluyen en esta sección, pero es importante anotar que, cuando sea pertinente, sus requisitos también deben cumplirse. Los ejemplos son: La Directiva de compatibilidad electromagnética 2014/30/CE y la Directiva ATEX 2014/34/UE.

Directiva de maquinaria

La Directiva de maquinaria abarca el suministro de nueva maquinaria y de otros equipos junto con componentes de seguridad. Es un delito suministrar maquinaria dentro de la UE a menos que se cumplan las disposiciones y los requisitos de la Directiva.

La definición más amplia de “maquinaria” dada dentro de la Directiva es la siguiente: Conjunto de partes o componentes vinculados entre sí, de los cuales al menos uno es móvil, asociados para una aplicación determinada, provisto o destinado a estar provisto de un sistema de accionamiento distinto de la fuerza humana o animal, aplicada directamente.



Etiqueta CE en la máquina

La actual Directiva de maquinaria (2006/42/EC) ha reemplazado la versión anterior (98/37/EC) a fines de 2009. Ésta aclara y enmienda, pero no introduce cambios radicales a sus requisitos esenciales seguridad y salud (RESS). Introduce algunos cambios para tomar en cuenta los cambios en tecnología y métodos. Extiende su alcance para cubrir algunos tipos adicionales de equipos (por ej., cabrestantes en obras de construcción). Ahora existe un requisito explícito para una evaluación de riesgos, y para cuya determinación se

aplican los requisitos esenciales de seguridad y salud (RESS), y existen cambios a los procedimientos de evaluación de cumplimiento normativo para equipo del Anexo IV. Puede encontrar información detallada y orientación sobre la definición y el resto de los aspectos de la Directiva de maquinaria en el sitio web oficial de la UE:

http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

Disposiciones clave de la Directiva original (98/37/EC) entraron en vigencia para maquinaria el 1 de enero de 1995, y para componentes de seguridad el 1 de enero de 1997.

Las disposiciones de la actual Directiva (2006/42/EC) entraron en vigencia el 29 de diciembre de 2009. Es responsabilidad del fabricante o de su representante autorizado asegurar que el equipo suministrado cumpla con la Directiva. Esto incluye:

- Asegurar que se cumpla con los requisitos esenciales de seguridad y salud (RESS) aplicables incluidos en el Anexo I de la Directiva
- Preparar un expediente técnico
- Realizar la evaluación de conformidad adecuada
- Dar una “Declaración CE de conformidad”
- Colocar la etiqueta CE donde corresponda
- Proporcionar instrucciones para el uso seguro



Requisitos esenciales de seguridad y salud



El Anexo 1 de la Directiva proporciona una lista de los requisitos esenciales de seguridad y salud (denominados RESS) que debe cumplir la maquinaria donde sea pertinente. El propósito de esta lista es asegurar que la maquinaria sea segura y que esté diseñada y construida de manera que pueda usarse, regularse y que pueda recibir mantenimiento en todas las fases de su vida útil sin poner en riesgo a los operadores. El texto a continuación ofrece una descripción general rápida de algunos de los requisitos habituales, aunque es importante tener en cuenta todos los

RESS recogidos en el Anexo 1. Deberá llevarse a cabo una evaluación de riesgos para determinar qué RESS son aplicables a los equipos en cuestión.

Los requisitos esenciales de seguridad y salud (RESS) en el Anexo 1 proporcionan una jerarquía de medidas para eliminar riesgos:

(1) Diseño inherentemente seguro. Siempre que sea posible, el diseño debe evitar peligros. En los casos en que esto no sea posible, deberán usarse **(2) dispositivos de protección adicionales**, por ej., resguardos con puntos de acceso enclavados, barreras inmateriales tales como barreras optoelectrónicas, tapetes de seguridad, etc. Cualquier otro riesgo que no pueda eliminarse mediante los métodos anteriores deberá eliminarse mediante **(3) equipo de protección personal y/o formación técnica**. El suministrador de la máquina deberá especificar lo apropiado.

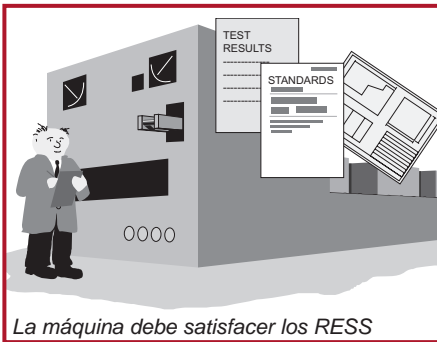
Deberán usarse materiales idóneos de construcción y operación. Deberán proporcionarse iluminación e instalaciones de manejo adecuadas. Los controles y los sistemas de control deberán ser seguros y fiables. Las máquinas no deberán poder ponerse en marcha en forma intempestiva y deberán contar con uno o más dispositivos de parada de emergencia. Se deberá dar consideración a instalaciones complejas donde los procesos aguas arriba o aguas abajo puedan afectar la seguridad de una máquina. El fallo de una fuente de alimentación eléctrica o de un circuito de control no deberá causar una situación peligrosa. Las máquinas deberán ser estables y capaces de soportar tensiones previsibles. No deberá haber bordes ni superficies expuestas que puedan causar lesiones al personal.

Deberán usarse resguardos o dispositivos de protección para evitar riesgos tales como los causados por piezas móviles. Éstas deberán ser de construcción robusta y difíciles de omitir. Los resguardos fijos tienen que instalarse mediante métodos que hagan necesario el uso de herramientas para su retirada y las uniones deberán ser prisioneras. Los resguardos móviles deben estar enclavados. Los resguardos regulables deben tener la capacidad de ser regulados de inmediato, sin necesidad de usar herramientas.

Deberán evitarse los peligros eléctricos y otros riesgos asociados a las fuentes de energía, incluidos los relativos a la energía almacenada. Deberá haber riesgo mínimo de lesiones por temperatura, explosión, ruido, vibración, polvo, gases o radiación. Deberán tomarse las provisiones apropiadas al realizar el mantenimiento y el servicio. Deberán proporcionarse suficientes indicaciones y dispositivos de advertencia. La maquinaria deberá proporcionarse con instrucciones para la instalación, el uso, la regulación, etc. con toda seguridad.

Evaluación de conformidad

El diseñador u otra persona responsable deberá mostrar pruebas que verifiquen la conformidad con los requisitos esenciales de seguridad y salud (RESS). Este archivo debe incluir toda la información pertinente, como resultados de pruebas, esquemas, especificaciones, etc.



Un Norma Armonizada Europea (EN) listado en el Diario Oficial de la Unión Europea bajo la Directiva para maquinarias, y cuya fecha de suspensión de presunción de conformidad no ha caducado, otorga presunción de conformidad con algunos de los RESS. (Muchas normas recientes listados en el Diario Oficial incluyen una referencia cruzada que identifica los RESS que abarca la normativa). Por lo tanto, cuando el equipo cumple con dichas Norma Armonizada Europea actuales, la tarea de demostrar conformidad con los requisitos

esenciales de seguridad y salud (RESS) queda considerablemente simplificada, y el fabricante también se beneficia de mayor certeza legal. Estas normas no son requisito legal; sin embargo, su uso se recomienda enfáticamente ya que probar la conformidad por métodos alternativos puede ser extremadamente complejo. Estas normas apoyan la Directiva de maquinaria y son producidas por el CEN (Comité Europeo de Normalización) en cooperación con ISO y CENELEC (Comité Europeo de Normalización Electrotécnica) en cooperación con IEC.

Deberá realizarse una evaluación de riesgos detallada y documentada para asegurar que se hayan eliminado todos los posibles riesgos en la máquina. De manera similar es responsabilidad del fabricante de la máquina asegurar que se cumplan todos los requisitos esenciales de seguridad y salud (RESS), incluso aquellos que no abarcan las normas EN armonizadas.



Expediente técnico

El fabricante o su representante autorizado debe preparar un expediente técnico para proveer prueba de conformidad con los requisitos esenciales de seguridad y salud (RESS). Este archivo debe incluir toda la información pertinente, como resultados de pruebas, esquemas, especificaciones, etc.

No es esencial que toda la información esté disponible permanentemente en copia impresa, pero debe ser posible disponer del expediente técnico completo para inspección a pedido de una autoridad competente (agencia designada por un país de la UE para monitorizar la conformidad de la maquinaria).

Como mínimo, la siguiente documentación debe incluirse en un expediente técnico:

1. Esquemas generales del equipo, incluidos esquemas del circuito de control.
2. Esquemas detallados, notas de cálculo, etc., que se requieran para verificar la conformidad de la maquinaria con los requisitos esenciales de seguridad y salud (RESS).
3. Documentación de la evaluación de riesgos, incluida una lista de los requisitos de salud y seguridad esenciales aplicables a la maquinaria y una descripción de las medidas de protección implementadas
4. Lista de normas y otras especificaciones técnicas utilizadas, que indique los requisitos esenciales de seguridad y salud que abarca.
5. Descripción de los métodos adoptados para eliminar los riesgos que presenta la máquina.
6. En caso de que fuera relevante, cualquier informe técnico o certificados obtenidos de alguna instalación de prueba u otra entidad.
7. Si se declara conformidad con alguna norma europea armonizada, cualquier informe técnico que proporcione resultados de las pruebas correspondientes.
8. Copia de las instrucciones de la máquina.
9. Cuando sea pertinente, declaración de incorporación de la maquinaria parcialmente completada y las instrucciones de ensamblaje relevantes de la misma.
10. Cuando sea pertinente, copias de la declaración CE de conformidad de la maquinaria u otros productos incorporados a la maquinaria.
11. Una copia de la declaración de conformidad CE

En el caso de fabricación en serie, detalles de las medidas internas (sistemas de calidad, por ejemplo) para asegurar que toda la maquinaria producida esté en conformidad:

- El fabricante debe realizar la investigación o las pruebas necesarias de componentes, conexiones o maquinaria completa para determinar si por su diseño y construcción puede instalarse y ponerse en servicio con toda seguridad.
- No es necesario que el expediente técnico exista como archivo único permanente, pero debe ser posible archivarlo para que esté disponible en un plazo razonable. Deberá estar disponible durante diez años después de la producción de la última unidad.

No es necesario que el expediente técnico incluya planos detallados ni información específica respecto a los subensamblajes usados en la fabricación de la máquina, a menos que sean esenciales para verificar la conformidad con los requisitos esenciales de seguridad y salud (RESS).

Evaluación de conformidad para máquinas listadas en el Anexo IV



Algunos tipos de equipo están sujetos a medidas especiales. Estos equipos aparecen en el Anexo IV de la directiva, e incluyen máquinas peligrosas tales como máquinas para trabajo de madera, prensas, máquinas de moldeo por inyección, equipo subterráneo, mecanismos de elevación para mantenimiento de vehículos, etc.

El Anexo IV también incluye ciertos componentes de seguridad, como dispositivos de protección, diseñados para detectar la presencia de personas (por ej., barreras optoelectrónicas) y unidades lógicas para asegurar las funciones de seguridad.

En el caso de máquinas del Anexo IV que no estén en conformidad total con las normas europeas armonizadas, el fabricante o su representante autorizado debe aplicar los siguientes procedimientos:

1. Examen CE de tipo. Se debe preparar un expediente técnico y un ejemplo de la máquina para ser presentado ante un organismo notificado (laboratorio de pruebas) para examen CE de tipo. Si pasa el examen se otorga un certificado de examen CE de tipo para la máquina. La validez del certificado debe ser revisada cada cinco años con el organismo notificado.



2. Aseguramiento de calidad total. Se debe preparar un expediente técnico, y el fabricante debe operar un sistema de calidad aprobado para diseño, fabricación, inspección final y pruebas. El sistema de calidad debe asegurar la conformidad de la maquinaria con las disposiciones de esta Directiva. El sistema de calidad debe ser auditado periódicamente por un organismo notificado.



En el caso de las máquinas que no estén incluidas en el Anexo IV o de aquellas si lo estén, pero cumplan plenamente las normas europeas armonizadas relevantes, el fabricante o su representante autorizado dispondrán de la opción de preparar la documentación técnica y autoevaluar y declarar el cumplimiento normativo del equipo. Se deben realizar revisiones internas para asegurar que el equipo fabricado mantenga la conformidad.

Entidades notificadas

Existe una red de organismos notificados que se comunican entre sí y trabajan con un criterio común en toda la UE. Los gobiernos (no la industria) designarán los organismos notificados y la información sobre las organizaciones elegidas para tal fin se podrá obtener en:

<http://ec.europa.eu/growth/tools-databases/nando/>

Procedimiento de la Declaración CE de conformidad



La etiqueta CE debe ser aplicada a todas las máquinas suministradas. Las máquinas deben también suministrarse con una Declaración CE de conformidad.

La etiqueta CE indica que la máquina cumple con todas las Directivas Europeas aplicables y que se han realizado los procedimientos apropiados de evaluación de conformidad. Es un delito colocar la etiqueta CE para la directiva de maquinaria, a menos que la máquina satisfaga los requisitos esenciales de seguridad y salud (RESS) correspondientes.

La Declaración CE de conformidad debe contener la siguiente información:

- Razón social y dirección completa del fabricante y, cuando corresponda, representante autorizado.
- Nombre y dirección de la persona autorizada para compilar el expediente técnico, quien debe estar establecido en la comunidad (en el caso de un fabricante fuera de la UE, éste puede ser el “representante autorizado”);
- Descripción e identificación de la maquinaria, incluida la denominación genérica, el modelo, el tipo, el número de serie y el nombre comercial;
- Una declaración expresa de que la maquinaria cumple todas las disposiciones pertinentes de esta Directiva y, cuando corresponda, una declaración similar sobre el cumplimiento de otras directivas y/o disposiciones relevantes por parte de la maquinaria.
- En caso necesario, una referencia a las normas armonizadas utilizadas;
- En caso necesario, la referencia a otras normas técnicas y especificaciones utilizadas;
- (En el caso de máquinas del anexo IV) de ser necesario, el nombre, la dirección y el número de identificación del organismo notificado que ha llevado a cabo el examen CE de tipo al cual se hace referencia en el anexo IX, y el número del certificado del examen CE de tipo;
- (En el caso de máquinas del anexo IV), de ser necesario, el nombre, la dirección y el número de identificación del organismo notificado que haya aprobado el sistema de aseguramiento de calidad total al que se hace referencia en el anexo X;
- Lugar y fecha de la declaración;
- Identidad y firma de la persona apoderada para redactar la declaración en nombre del fabricante o del representante autorizado.

Declaración CE de incorporación de máquinas parcialmente completadas

Se debe emitir una DECLARACIÓN DE INCORPORACIÓN junto con el equipo en los casos en que éste sea suministrado para ensamblaje con otros ítems para formar una máquina completa en un futuro. La etiqueta CE no debe usarse. La declaración debe indicar que el equipo no debe ponerse en servicio mientras no se haya declarado la conformidad de la máquina a la cual ha sido incorporado. Debe prepararse un expediente técnico y la maquinaria parcialmente completada debe suministrarse con información que contenga la descripción de las condiciones que deben cumplirse para incorporarla correctamente en la maquinaria final, con el objeto de no afectar la seguridad.

Esta opción no está disponible para equipos que pueden funcionar independientemente o que modifican la función de una máquina.



La Declaración de incorporación debe contener la siguiente información:

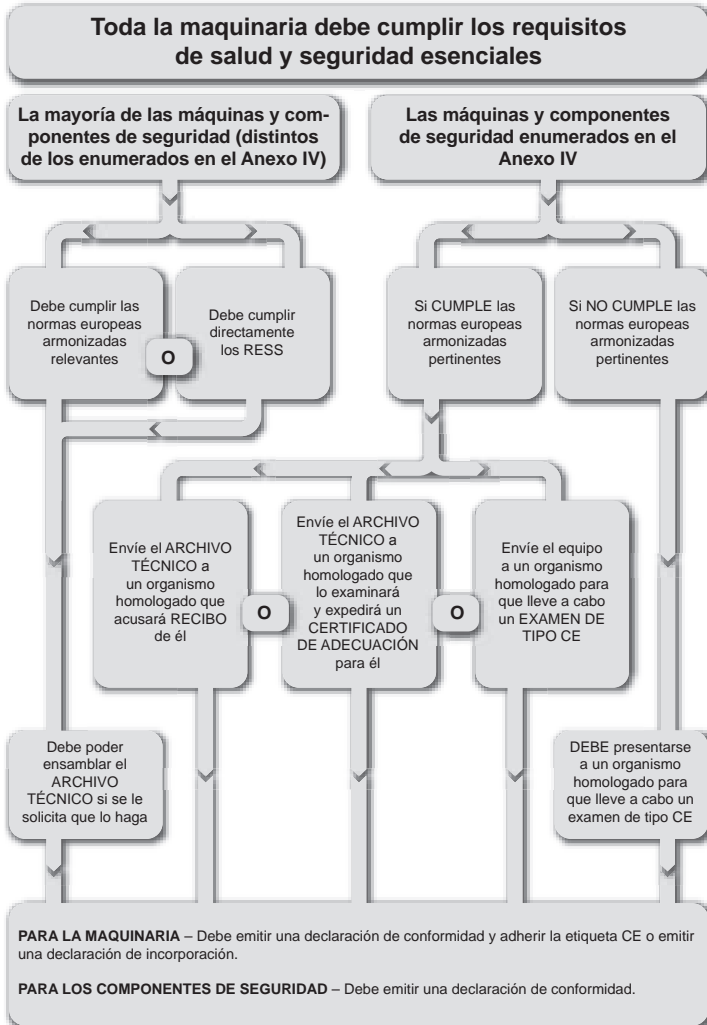
- Razón social y dirección completa del fabricante de la maquinaria parcialmente completada y, de ser necesario, del representante autorizado;
- Nombre y dirección de la persona autorizada para compilar la documentación técnica pertinente, quien debe estar establecida en la comunidad (en el caso de fabricantes fuera de la UE esta persona puede ser “el representante autorizado”);
- Descripción e identificación de la maquinaria parcialmente completada incluida la denominación genérica, la función, el modelo, el tipo, el número de serie y el nombre comercial;
- Un párrafo que declare qué requisitos esenciales de esta Directiva se aplican y cumplen, y que la documentación técnica pertinente es compilada de acuerdo con la parte B del anexo VII, y, de ser necesario, un párrafo que declare la conformidad de la maquinaria parcialmente completada con otras Directivas pertinentes;
- El compromiso de transmitir, en respuesta a una solicitud justificada por las autoridades nacionales, la información pertinente relativa a la maquinaria parcialmente completada. Esto incluye el método de transmisión sin menoscabo de los derechos de propiedad intelectual del fabricante de la maquinaria parcialmente completada;
- Un párrafo que indique que la maquinaria parcialmente completada no debe ser puesta en servicio mientras la maquinaria final a la cual ha sido incorporada no haya sido declarada en conformidad con las provisiones de esta Directiva, de ser necesario;
- Lugar y fecha de la declaración;
- Identidad y firma de la persona apoderada para redactar la declaración en nombre del fabricante o del representante autorizado.

Maquinaria suministrada desde fuera de la UE – Representantes autorizados

Si un fabricante con sede fuera de la UE (o del Espacio Económico Europeo [EEA]) exporta maquinaria a la UE, deberá designar a un representante autorizado.

Un representante autorizado es cualquier persona natural o legal establecida en la Comunidad Europea que haya recibido un mandato por escrito del fabricante de cumplir en su nombre todas o parte de las obligaciones y formalidades relacionadas con la Directiva de maquinaria.

La Directiva de uso de equipos de trabajo de la UE (Directiva Social)



Si bien la Directiva de maquinaria se dirige a los proveedores, esta Directiva (2009/104/CE) se dirige a los usuarios de la maquinaria. Abarca todos los sectores industriales e impone deberes generales a los usuarios, junto con requisitos mínimos para la seguridad del equipo de trabajo. Todos los países de Unión Europea están promulgando sus propias formas de legislación para implementar esta Directiva.



Por ejemplo, en Reino Unido se aplica con la designación Reglamento sobre el suministro y uso de equipos de trabajo (con frecuencia abreviada como P.U.W.E.R.). La forma de implementación puede variar de un país a otro, pero el efecto de la Directiva es el mismo.

Los artículos de la Directiva proporcionan detalles de qué tipos de equipo y lugares de trabajo cubre por la Directiva.

También imponen deberes generales a los usuarios, como implementar sistemas seguros de trabajo y proporcionar equipos idóneos y seguros que deben recibir el mantenimiento adecuado. Los operadores de las máquinas deben recibir información y formación técnica adecuadas para poder usar la máquina con toda seguridad.

Las máquinas nuevas (y la maquinaria de segunda mano proveniente de países fuera de la UE) suministradas después del 1 de enero de 1993, deben satisfacer las directivas para productos pertinentes, por ej., la Directiva de maquinaria (sujeto a arreglos de transición). Los equipos de segunda mano procedentes de la UE que se suministren por primera vez en el lugar de trabajo deberán cumplir de inmediato los requisitos mínimos que figuran en el anexo de la Directiva

Nota: La maquinaria existente o de segunda mano que sea significativamente reacondicionada o modificada se clasifica como equipo nuevo, de manera que el trabajo que se realice en la misma debe asegurar el cumplimiento con la Directiva de maquinaria (aunque sea para el propio uso de la compañía).

La idoneidad del equipo de trabajo es un requisito importante de la Directiva y resalta la responsabilidad del empleador de llevar a cabo un proceso adecuado de evaluación de riesgos.

Es un requisito que la maquinaria reciba el servicio de mantenimiento apropiado. Esto normalmente significa que debe haber un programa rutinario y planificado de mantenimiento preventivo. Se recomienda usar un registro y mantenerlo actualizado. Esto es especialmente importante en casos en los que el mantenimiento y la inspección del equipo contribuyen con la seguridad y a la integridad continua de un dispositivo o sistema de protección.

El anexo de la Directiva U.W.E. establece los requisitos mínimos aplicables a los equipos de trabajo.

Si el equipo cumple con las directivas del producto pertinentes, por ej., la Directiva de maquinaria, cumple automáticamente con los requisitos de diseño de máquina dados en la sección de requisitos mínimos del Anexo.

Los Estados miembros pueden aprobar leyes relativas al uso de equipos de trabajo que superen los requisitos mínimos de la Directiva.

Puede encontrar información detallada sobre el uso de la Directiva de equipos de trabajo en el sitio web oficial de la UE:

<https://osha.europa.eu/en/legislation/directives/3>

Regulaciones de los EE.UU.

Esta sección presenta algunas de las regulaciones sobre seguridad de resguardos para máquinas industriales en los EE.UU. Éste es sólo un punto de inicio; los lectores deben investigar más a fondo los requisitos de sus aplicaciones específicas y tomar medidas para asegurar que sus diseños, usos y procedimientos de mantenimiento y prácticas cumplan con sus propias necesidades, así como con los códigos y las regulaciones locales y nacionales.

Hay muchas organizaciones que promueven la seguridad industrial en los Estados Unidos. Éstas incluyen:

1. Corporaciones que usan requisitos establecidos y establecen sus propios requisitos internos;
2. La OSHA (Occupational Safety and Health Administration);
3. Organizaciones industriales como la National Fire Protection Association (NFPA), la Robotics Industries Association (RIA) y la Association of Manufacturing Technology (AMT), o el ANSI, que publica una lista de normas consensuadas reconocidas; y los proveedores de productos y soluciones de seguridad como Rockwell Automation.

Occupational Safety and Health Administration (OSHA)

En los Estados Unidos, uno de los principales impulsores de la seguridad industrial es la OSHA. La OSHA fue establecida en 1971 por una Ley del Congreso de los EE.UU. El propósito de esta ley es proporcionar condiciones de trabajo saludables y de seguridad, y preservar los recursos humanos. La ley autoriza que el Secretario de Trabajo establezca normas de seguridad y salud ocupacional obligatorios aplicables a los negocios que afectan el comercio interestatal. Esta Ley se aplica con respecto al empleo realizado en un lugar de trabajo en un estado, el Distrito de Columbia, el Estado Asociado de Puerto Rico, las Islas Vírgenes, Samoa Americana, Guam, el territorio de las Islas del Pacífico, la Isla Wake, la Plataforma Continental Exterior, la Isla Johnson y la zona del canal.

El Artículo 5 de la Ley establece los requisitos básicos. Cada empleador debe proporcionar a cada uno de sus empleados empleo y un lugar de empleo sin peligros reconocidos que causen o pudieran causar la muerte o lesiones físicas graves a sus empleados; y debe cumplir con las normas de seguridad y de salud ocupacional promulgados bajo esta Ley.



El Artículo 5 también establece que cada uno de los empleados debe cumplir con las normas de seguridad y de salud ocupacionales, y con todas las reglas, las regulaciones y las órdenes emitidas de conformidad con esta Ley, que sean aplicables a sus propias acciones y conducta.

La ley de OSHA establece que la responsabilidad corresponde tanto al empleador como al empleado. Esto es muy diferente de la Directiva para maquinarias que requiere que los proveedores pongan en el mercado máquinas que no representen peligro. En los EE.UU., un proveedor puede vender una máquina sin ninguna protección. El usuario debe añadir la protección para que la máquina sea segura. Si bien ésta era una práctica común cuando se aprobó la Ley, la tendencia es que los proveedores proporcionen máquinas con protección incorporada, ya que diseñar la seguridad incorporada en la máquina es mucho más económico que añadir la protección después de que la máquina ha sido diseñada y construida. La intención de las normas ahora es tratar que el proveedor y el usuario se comuniquen mutuamente los requisitos de protección, de modo que las máquinas fabricadas sean no sólo seguras sino más productivas.

El Secretario de Trabajo tiene la autoridad de promulgar como norma de seguridad o de salud ocupacional cualquier estándar de consenso y cualquier estándar federal, a menos que la promulgación de dicho estándar no resulte en seguridad o salud mejorada para los empleados designados específicamente.

OSHA lleva a cabo esta tarea publicando reglamentos en el Título 29 del Código de Reglamentos Federales (29 CFR). Las normas pertinentes a las máquinas industriales son publicadas por OSHA en la Parte 1910 de 29 CFR. Se pueden consultar de forma gratuita en el sitio web de la OSHA www.osha.gov. A diferencia de la mayoría de las normas voluntarias, las normas de la OSHA son leyes.

Algunas de las secciones importantes pertinentes con la seguridad de la máquina son:

- A – Generalidades
- B – Adopción y extensión de normas federales establecidas
- C – Disposiciones de seguridad y salud generales
- H – Materiales peligrosos
- I – Equipo de protección personal
- J – Controles ambientales generales – incluye bloqueo-marcado de seguridad
- O – Maquinaria y resguardos de máquina
- R – Sectores especiales
- S – Especificaciones eléctricas

Algunas normas de OSHA se refieren a normas voluntarias. El efecto legal de incorporar por referencia es que el material se trata como si fuera publicado en su totalidad en el Registro Federal. Cuando una norma de consenso nacional se incorpora por referencia en una de las subpartes, la norma adquiere validez jurídica.

Por ejemplo, NFPA 70, norma voluntaria conocida como Código Eléctrico Nacional de los EE.UU., se referencia en la Subparte S. Esto hace que los requisitos de la norma NFPA 70 sean obligatorios.

29 CFR 1910.147, en la Subparte J, abarca el control de energía peligrosa. Esto se conoce como norma de bloqueo-marcado de seguridad. La norma voluntaria equivalente es ANSI Z244.1. En resumen, esta norma requiere que la alimentación eléctrica de la máquina se bloquee durante las tareas de servicio o mantenimiento. El propósito es evitar la activación o puesta en marcha intempestiva de la máquina, misma que podría resultar en lesiones a los empleados.

Las empresas deberán establecer un programa de bloqueo y etiquetado de seguridad y emplear procedimientos para instalar dispositivos de bloqueo o etiquetado adecuados en los dispositivos de aislamiento de la energía o, de lo contrario, para inhabilitar las máquinas o equipos y evitar que reciban alimentación, arranquen o liberen la energía almacenada de forma imprevista, evitando así posibles lesiones a los empleados.

Los cambios, ajustes y otras actividades de mantenimiento de poca importancia que se desarrollan durante las operaciones de fabricación normales están cubiertas por ANSI Z244 “Medidas alternativas” cuando son rutinarias, repetitivas y forman parte integral del uso del equipo de producción, siempre que el trabajo se lleve a cabo con medidas alternativas que ofrezcan una protección eficaz. La OSHA respalda esta disposición directamente en la “excepción de mantenimiento de menor importancia de la OSHA”. Las medidas alternativas incluyen dispositivos de protección como barreras optoelectrónicas, tapetes de seguridad, enclavamiento de puertas protectoras y otros dispositivos similares conectados a un sistema de seguridad. El reto para el diseñador y para el usuario de la máquina es determinar cuáles son las tareas “menores” y “de rutina, repetitivas e integrales”. Este aspecto se puede cubrir durante la evaluación de riesgos.

La Subparte O abarca “Maquinaria y resguardos de máquina”. Esta subparte enuncia requisitos generales para todas las máquinas, así como requisitos para algunas máquinas específicas. Cuando se constituyó la OSHA en 1971, adoptó muchas normas ANSI existentes. Por ejemplo, B11.1 en el caso de prensas de potencia mecánica fue adoptada como 1910.217.

1910.212 es la norma general de OSHA para máquinas. Establece que debe proporcionarse uno o más métodos de resguardos de máquina para proteger al operador y a otros empleados en el área de la máquina contra peligros tales como los creados por el punto de operación, puntos de atrapamiento, piezas giratorias, rebabas que salen disparadas y chispas. Siempre que sea posible, los resguardos deben incorporarse a la máquina, o deben fijarse de alguna otra manera si por alguna razón no es posible incorporarlos a la misma. El resguardo no debe representar un peligro de accidente por sí mismo. Además, se precisará una herramienta para su extracción en caso de que el resguardo deba ser retirado.

El “punto de operación” es el área de la máquina donde se realiza el trabajo relacionado con el material procesado. Debe protegerse el punto de operación de una máquina cuya operación expone a un empleado a sufrir lesiones. El dispositivo protector debe cumplir con las normas vigentes o, en ausencia de normas específicas aplicables, debe estar diseñado y construido para evitar que el operador tenga ninguna parte de su cuerpo en



la zona de peligro durante el ciclo de operación.

La Subparte S (1910.399) establece los requisitos eléctricos de OSHA. Una instalación o equipo será aceptable para la Subsecretaría de Trabajo y estará autorizado dentro del sentido de esta Subparte S si un laboratorio de ensayo reconocido a escala nacional (NRTL) acepta, certifica, registra, etiqueta o determina por cualquier otro medio que es seguro.

¿Qué es el equipo? Es un término general que incluye materiales, conexiones, dispositivos, artefactos, accesorios y similares, usados como parte de una instalación eléctrica o en conexión con ésta.

¿Qué significa “Listado”? El equipo estará “registrado” si pertenece a uno de los tipos señalados en una lista que: (a) haya sido publicada por un laboratorio de ensayo reconocido a escala nacional (NRTL) que lleve a cabo inspecciones periódicas de la producción de dichos equipos y (b) declare que dicho equipo cumple normas reconocidas a escala nacional o se ha probado y demostrado que es seguro para un uso específico.

A partir de agosto de 2009, las siguientes compañías son reconocidas por OSHA como laboratorios de prueba reconocidos a nivel nacional:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- Aprobaciones legales FM LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

La autoridad competente (AHJ) tendrá la última palabra sobre los requisitos. Por ejemplo, algunos estados como Nueva York, California e Illinois exigen requisitos adicionales.

Algunos estados han adoptado sus propias OSHA locales y puede que exijan requisitos adicionales a los requisitos de la OSHA estadounidense/federal. Veinticuatro estados, Puerto Rico y las Islas Vírgenes tienen planes estatales aprobados por OSHA, y han adoptado sus propias normas y políticas de cumplimiento. En su mayor parte, estos estados adoptan normas idénticas a las federales de la OSHA. Sin embargo, algunos estados han adoptado distintas normas aplicables a este tema, o pueden tener políticas

de cumplimiento diferentes. Las empresas deben reportar el historial de incidentes a la OSHA. OSHA compila las tasas de incidentes, transmite la información a las oficinas locales, y utiliza esta información para priorizar las inspecciones. Los impulsores de inspección clave son:

- Peligro inminente
- Catástrofes y fatalidades
- Quejas de empleados
- Sectores altamente peligrosos
- Inspecciones locales planificadas
- Inspecciones de seguimiento
- Programas nacionales y de enfoque local

El incumplimiento de las normas de la OSHA puede resultar en multa. El detalle de las multas es:

- Grave: hasta \$7000 por falta
- No graves: a discreción, pero no más de \$7000
- Repetitivas: hasta \$70.000 por falta
- Intencionadas: hasta \$70.000 por falta
- Faltas que resultan en muerte: multas adicionales
- No corregir la falta \$7000/día

Regulaciones canadienses

En Canadá, la seguridad industrial se rige a nivel de provincias. Cada provincia tiene sus propias normativas que se deben mantener y respetar. Por ejemplo, Ontario ha establecido la Ley de Salud y Seguridad Ocupacional que establece los derechos y los deberes de todas las partes en el lugar de trabajo. Su principal propósito es proteger a los trabajadores contra peligros de seguridad y salud en el trabajo. La ley establece procedimientos para resolver los peligros en el lugar de trabajo y para hacer cumplir la ley cuando el cumplimiento no se realiza voluntariamente.

Dentro de la Ley está la regulación 851, sección 7 que define la revisión de las normas de seguridad y salud antes del arranque. Esta revisión es un requisito obligatorio en Ontario para cualquier maquinaria nueva, reconstruida o modificada, y un ingeniero profesional debe generar el informe respectivo.



Capítulo 2: Normas

Esta sección aborda algunas de las normas nacionales e internacionales típicas que son relevantes para la seguridad de máquinas. No tiene el objeto de ser una lista completa, sino de proporcionar información sobre asuntos de seguridad de maquinaria que están sujetos a normalización. Esta sección debe leerse junto con la sección de Normativa.

Muchos países del mundo están trabajando para lograr la armonización global de normas. Esto se observa de manera especial en el área de seguridad de la máquina. Dos organizaciones rigen las normas globales de seguridad de maquinaria: ISO e IEC. Las normas regionales y de los países todavía existen y apoyan los requisitos locales, pero muchos países se están dirigiendo al uso de normas internacionales producidas por ISO e IEC.

Por ejemplo, las normas EN (Norma Europea) se usan en todos los países de la EEA. Todas las nuevas normas EN están en línea con las normas ISO e IEC, y en la mayoría de casos tienen texto idéntico. En Estados Unidos ya se alude también con frecuencia a las normas IEC e ISO.

La IEC abarca asuntos electrotécnicos y la ISO trata otros asuntos. La mayoría de países industrializados son miembros de IEC y de ISO. Las normas de seguridad de maquinaria son escritas por grupos de trabajo formados por expertos de muchos países.

En la mayoría de países las normas pueden considerarse como voluntarias, mientras que las regulaciones son legalmente obligatorias. Sin embargo, las normas generalmente se usan como interpretación práctica de las regulaciones. Por lo tanto, el entorno de las normas y de las regulaciones está estrechamente vinculado.

ISO (International Organization for Standardization)

ISO es una organización no gubernamental formada por las entidades de normas nacionales de la mayoría de los países del mundo (157 países al momento de impresión de este documento). Una secretaría central situada en Ginebra, Suiza, coordina el sistema. ISO genera normas para diseñar, fabricar y usar maquinaria de manera más eficiente, segura y limpia. Estas normas también facilitan y permiten que sea más justo el comercio entre países. Las normas de la ISO pueden identificarse por las letras ISO.

Las normas para máquinas ISO están organizadas de la misma manera que las normas EN, en tres niveles: Tipo A, B y C (consulte la sección posterior en Normas Europeas Armonizadas EN).

Para obtener más información visite el sitio web de ISO: www.iso.org.

IEC (International Electrotechnical Commission)

La IEC prepara y publica normas internacionales para tecnologías eléctricas, electrónicas y otras afines. A través de sus miembros, la IEC promueve la cooperación internacional en todos los temas de normalización electrotécnica y asuntos relacionados, tales como la evaluación de conformidad con las normas electrotécnicas.

Para obtener más información visite el sitio web de IEC: www.iec.ch

Normas Europeas Armonizadas de EN

Estas normas son comunes a todos los países de la EEA, y son producidas por las organizaciones de normalización europea CEN y CENELEC. Su uso es voluntario, pero el diseño y la fabricación de equipos conforme a sus especificaciones es la manera más directa de demostrar cumplimiento con los requisitos esenciales de seguridad y salud (RESS) de la directiva de maquinaria.

Están divididas en 3 tipos: Normas A, B y C.

Tipo A. NORMAS: Abarcan aspectos aplicables a todo tipo de máquinas.

Tipo B. NORMAS: Subdivididas en 2 grupos.

NORMAS Tipo B1: Abarcan aspectos específicos de seguridad y ergonomía de maquinaria.

NORMAS Tipo B2: Abarcan componentes y dispositivos de protección.

NORMAS Tipo C: Abarcan tipos o grupos específicos de máquinas.

Cabe destacar que el cumplimiento de una norma C presupone automáticamente la conformidad con los RESS contemplados por esa norma. En ausencia de una norma tipo C adecuada, pueden usarse las normas tipos A y B como prueba parcial o total de conformidad con los requisitos esenciales de seguridad y salud (RESS), indicando el cumplimiento con las secciones pertinentes.

Se han concertado acuerdos para lograr la colaboración entre CEN/CENELEC y entidades tales como ISO e IEC. Eventualmente, esto debe resultar en la implementación de normas comunes en todo el mundo. En la mayoría de casos una norma EN tiene una contraparte en IEC o ISO. En general los dos textos son iguales y cualquier diferencia regional se expresa en referencia con la norma.

Para obtener una lista completa de las normas de seguridad de maquinaria de EN visite:

<http://ec.europa.eu/growth/single-market/european-standards/>



Normas de los EE.UU.

Normas de OSHA

Siempre que sea posible, OSHA promulga normas de consenso nacional o normas federales establecidas como normas de seguridad. Las disposiciones obligatorias (es decir la palabra implica obligatorio) de las normas, incorporadas por referencia, tienen el mismo vigor y efecto que las normas listadas en la Parte 1910. Por ejemplo, la norma de consenso nacional NFPA 70 se lista como documento de referencia en el Apéndice A de la Subparte S-Eléctrica de la Parte 1910 de 29 CFR. NFPA 70 es una norma voluntaria desarrollada por la National Fire Protection Association (NFPA). NFPA 70 se conoce también como Código Eléctrico Nacional (NEC). Por incorporación, todos los requisitos mandatorios del NEC son mandatorios de OSHA.

Normas de ANSI

El American National Standards Institute (ANSI) sirve como administrador y coordinador del sistema de normalización voluntaria del sector privado de los Estados Unidos. Es una organización de miembros privada y sin fines de lucro, que cuenta con el apoyo de un grupo diverso de organizaciones de los sectores privado y público.

ANSI no desarrolla normas, sino que facilita el desarrollo de éstas mediante el establecimiento de consenso entre los grupos calificados. ANSI también asegura que los grupos calificados sigan los principios de apertura y consenso, y los procedimientos debidos.

Estas normas están categorizadas como normas de aplicación o como normas de construcción. Las normas de aplicación definen el modo de aplicar los medios de protección a la maquinaria. Algunos ejemplos incluyen ANSI B11.1, que proporciona información sobre el uso de resguardos de máquina en prensas mecánicas y ANSI/RIA R15.06, que describe el uso de dispositivos de seguridad para protección de robots.

National Fire Protection Association (NFPA)

La National Fire Protection Association (NFPA) se organizó en 1896. Su misión es reducir el efecto de los incendios en la calidad de vida promoviendo códigos y normas con base científica, así como investigación y educación sobre incendios y aspectos relacionados con la seguridad. La NFPA auspicia muchas normas para ayudar a llevar a cabo su misión. Dos normas muy importantes relacionadas con la seguridad industrial y con la protección son el Código Eléctrico Nacional (NEC) y la Normativa Eléctrica para Maquinaria Industrial.

La National Fire Protection Association ha actuado como patrocinador de la NEC desde 1911. El documento del código original fue desarrollado en 1897 como resultado de los esfuerzos unidos de diversos intereses aliados en temas seguridad, electricidad y arquitectura. Desde entonces la NEC se ha actualizado muchas veces, y el contenido de su normativa se revisa cada tres años.

El Artículo 670 del NEC abarca algunos detalles sobre maquinarias industriales y refiere al lector a la Normativa Eléctrica para Maquinaria Industrial, NFPA 79.

NFPA 79 se aplica a los equipos, aparatos o sistemas eléctricos/electrónicos de las máquinas industriales. El propósito de NFPA 79 es proporcionar información detallada para la aplicación de equipos, aparatos o sistemas eléctricos/electrónicos suministrados como parte de máquinas industriales que promueven la seguridad personal y de la propiedad. NFPA 79, adoptada oficialmente por ANSI en 1962, es muy similar en contenido a la Norma IEC 60204-1.

Las máquinas que no están incluidas en las normas específicas de la OSHA, no deben representar ninguna fuente de peligro reconocida que pudiera causar la muerte o lesiones personales graves. Estas máquinas deben diseñarse y mantenerse de manera que se satisfagan o se superen los requisitos de las normas industriales aplicables. NFPA 79 es una norma que se aplicaría a las máquinas no específicamente cubiertas por las normas de OSHA.

Normas canadienses

Las normas CSA reflejan un consenso nacional de productores y usuarios, entre ellos fabricantes, consumidores, vendedores minoristas, sindicatos y organizaciones profesionales y entidades gubernamentales. Las normas son ampliamente usadas por la industria y el comercio, y a menudo son adoptadas en sus regulaciones por los gobiernos municipales, provinciales y federales, particularmente en los campos de salud, seguridad y construcción, así como medioambientales.

Las personas, las compañías y las asociaciones en todo Canadá demuestran su apoyo al desarrollo de normas de la CSA ofreciendo de manera voluntaria su tiempo y conocimientos para el trabajo que realiza el Comité de la CSA y apoyando los objetivos de la Asociación. El total de miembros de la CSA está formado por más de 7000 voluntarios de comités y 2000 asociados.

El Standards Council of Canada es la entidad coordinadora del Sistema de Normas Nacionales, una federación de organizaciones independientes y autónomas que trabajan para el desarrollo y la mejora de la normalización voluntaria a favor de los intereses nacionales.

Normas australianas

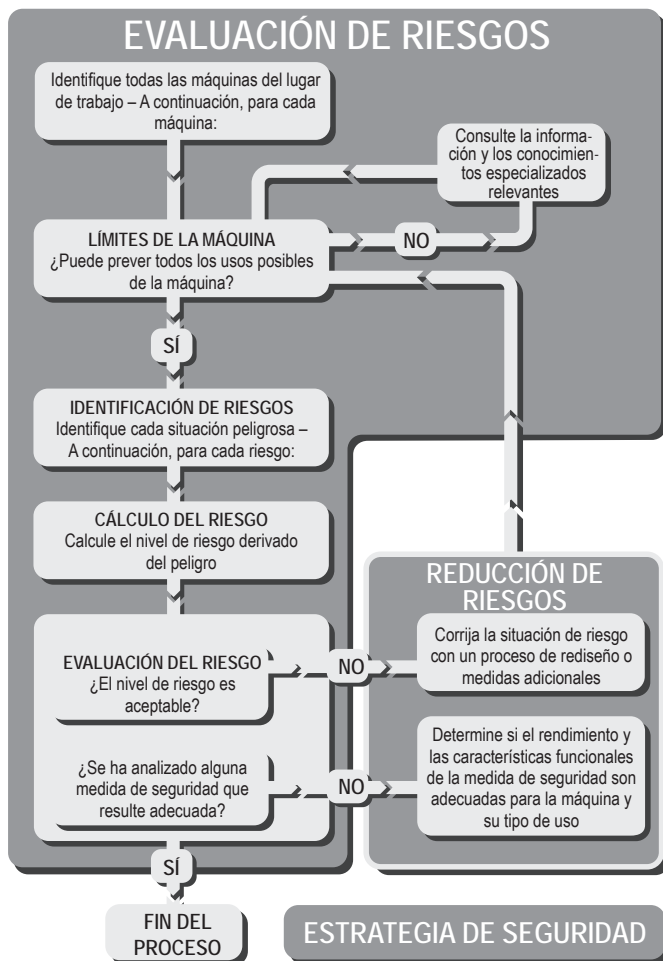
La mayoría de estas normas están ampliamente adaptadas a las normas ISO/IEC/EN equivalentes Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Teléfono: +61 2 8206 6000
Correo electrónico: mail@standards.org.au – Sitio web: www.standards.org.au



Capítulo 3: Estrategia de seguridad

Desde un punto de vista puramente funcional, es mejor que una máquina realice su tarea de procesar material de la manera más eficiente posible. Pero para que una máquina sea viable, también debe ser segura. De hecho, la seguridad debe ser una consideración principal.

Para desarrollar una estrategia de seguridad adecuada existen dos pasos que funcionan coordinadamente, como se muestra a continuación.



EVALUACIÓN DE RIESGOS basada en el claro entendimiento de los límites y de las funciones de la máquina y las tareas que pueden requerirse en la máquina durante el transcurso de su vida útil.

Luego se procede a la **REDUCCIÓN DE RIESGOS**, de ser necesario, y se seleccionan medidas de seguridad en base a la información derivada de la etapa de evaluación de riesgos. La manera en que esto se ha realizado es la base de la **ESTRATEGIA DE SEGURIDAD** de la máquina.

El seguimiento de este enfoque sistemático garantiza que se tengan en cuenta todos los aspectos y que el principio predominante no se pierda en los detalles. Todo el proceso debe documentarse. Esto no sólo asegura un trabajo más minucioso, sino que también permite que los resultados estén disponibles para que sean verificados por terceros.

Esta sección se aplica tanto a los fabricantes como a los usuarios de la máquina. El fabricante debe asegurar que su máquina pueda usarse de manera segura. La evaluación de riesgos debe comenzar en la fase de diseño de la máquina y debe considerar todas las tareas previsibles que deberán realizarse en la máquina. Esta estrategia basada en tareas en las etapas tempranas de la evaluación de riesgos es muy importante. Por ejemplo, puede haber la necesidad frecuente de ajustar las piezas móviles de la máquina. En la fase de diseño debe ser posible diseñar medidas que permitan realizar este procedimiento de manera segura. Si éstas se omiten en una etapa temprana puede ser difícil o imposible implementarlas en una etapa posterior. Como resultado, los ajustes de las piezas móviles probablemente todavía necesiten realizarse, aunque tendrían que realizarse de manera arriesgada o ineficiente (o ambas). Una máquina cuyas tareas han sido consideradas en su totalidad durante la evaluación de riesgos es una máquina más segura y más eficiente.

El usuario necesita asegurar que las máquinas en su entorno de trabajo sean seguras. Incluso si una máquina ha sido declarada segura por el fabricante, el usuario de la máquina debe realizar una evaluación de riesgos para determinar si el equipo es seguro en su propio entorno. A menudo las máquinas se usan en circunstancias no previstas por el fabricante. Por ejemplo, una máquina fresadora usada en el taller de un colegio necesita consideraciones adicionales con respecto a una que se usa en una sala de herramientas industriales. También cabe la posibilidad de que máquinas que son seguras por separado se combinen de un modo potencialmente inseguro.

También debe recordarse que si una compañía usuaria adquiere dos o más máquinas independientes y las integra en un proceso, ellos resultan ser los fabricantes de la máquina combinada.

Por lo tanto, consideremos ahora los pasos esenciales para obtener una estrategia de seguridad apropiada. Lo siguiente puede aplicarse a una instalación de fábrica existente o a una sola máquina nueva.



Evaluación de riesgos

Es un error considerar la evaluación de riesgos como una carga. Es un proceso útil que proporciona información vital y que permite que el usuario o el diseñador tomen decisiones lógicas acerca de las maneras de lograr la seguridad.

Hay varias normas que abarcan este tema. (EN) ISO 12100 Seguridad de maquinaria – Principios generales de diseño – Los apartados sobre la evaluación de riesgos y la reducción del riesgo contienen las pautas más aplicadas a escala global. También se encuentra disponible un informe técnico ISO: ISO/TR 14121-2. Ofrece orientación práctica y ejemplos de métodos para la evaluación de riesgos.

Con independencia de la técnica que se utilice para llevar a cabo una evaluación de riesgos, un equipo multidisciplinar normalmente obtendrá un resultado con una mayor cobertura y mejor equilibrio que una sola persona.

La evaluación de riesgos es un proceso reiterativo; se realiza en distintas etapas del ciclo de vida de la máquina. La información disponible varía de acuerdo con la etapa del ciclo de vida. Por ejemplo, una evaluación de riesgos realizada por un constructor de máquinas tiene acceso a cada detalle de los mecanismos de la máquina y a los materiales de construcción, pero probablemente una suposición sólo aproximada del entorno de trabajo en que se usa la máquina. Una evaluación de riesgos realizada por el usuario de la máquina no necesariamente tendría acceso a los detalles técnicos minuciosos, pero tiene acceso a todos los detalles del entorno de trabajo de la máquina. Lo ideal es que el resultado de una acción repetitiva sirva de aporte al siguiente proceso.

Determinación de límites de la máquina

Implica la recopilación y análisis de información relativa a los componentes, mecanismos y funciones de una máquina. También es necesario considerar todos los tipos de interacción humana con la máquina y el entorno donde funciona la máquina. El objetivo es obtener un entendimiento claro de la máquina y sus usos.

En los casos en que máquinas independientes estén vinculadas ya sea mecánicamente o por sistemas de control, éstas deben considerarse como una sola máquina, a menos que estén “zonificadas” por medidas de protección apropiadas.

Es importante considerar todas las limitaciones y las etapas de la vida de una máquina, incluidas la instalación, la puesta en servicio, el mantenimiento, el desmantelamiento, el correcto uso y la operación, así como las consecuencias del mal uso o mal funcionamiento razonablemente previsible.

Identificación de tareas y peligros

Todos los peligros de la máquina deben identificarse y listarse en términos de su naturaleza y ubicación. Los tipos de peligro incluyen trituración, corte, enredo, expulsión de piezas, vapores, radiación, sustancias tóxicas, calor, ruido, etc.

Los resultados del análisis de tareas deberán compararse con los resultados de la identificación de riesgos. De este modo se comprobará si existe una posibilidad de convergencia de un riesgo y una persona (es decir, una situación peligrosa). Todas las situaciones peligrosas deben listarse. Puede que el mismo riesgo dé lugar a diferentes tipos de situaciones peligrosas en función de la naturaleza de la persona o la tarea. Por ejemplo, la presencia de un técnico de mantenimiento muy diestro y con alta formación técnica puede tener diferentes implicaciones que la presencia de un encargado de limpieza no calificado y sin conocimientos de la máquina. En esta situación, si cada caso es listado y tratado por separado puede ser posible justificar diferentes medidas de protección para el técnico de mantenimiento que para el encargado de limpieza. Si los casos no se listan y tratan por separado, entonces debe utilizarse el peor de los casos, y el técnico de mantenimiento y el encargado de limpieza quedan cubiertos por la misma medida de protección.

Algunas veces es necesario llevar a cabo una evaluación de riesgos general sobre una máquina existente que ya tiene medidas protectoras (por ejemplo, una máquina con piezas móviles peligrosas protegida por una puerta de resguardo enclavada). Las piezas móviles constituyen un peligro potencial que puede convertirse en un peligro real en el caso de fallo del sistema de enclavamiento. A menos que el sistema de enclavamiento ya haya sido validado (por ejemplo, por medio de una evaluación de riesgos o diseño conforme a una norma apropiada), su presencia no debe considerarse.

Estimación de riesgos

Éste es uno de los aspectos más fundamentales de la evaluación de riesgos. Existen muchas formas de abordar este asunto y las páginas a continuación describen los principios básicos.

Cualquier máquina que tenga un potencial de situaciones peligrosas presenta un riesgo de evento peligroso (es decir, daño). Cuanto mayor sea el riesgo, más importante es hacer algo al respecto. En un peligro el riesgo podría ser tan pequeño que podríamos tolerarlo y aceptarlo, pero en otro peligro el riesgo podría ser tan alto que necesitaríamos tomar medidas extremas para brindar protección. Por lo tanto, para tomar una decisión respecto a “si hacer algo y qué hacer para evitar el riesgo”, necesitamos cuantificarlo.

El riesgo a menudo se considera únicamente en términos de la severidad de la lesión en caso de accidente. Debe tenerse en consideración la gravedad de la lesión potencial Y la probabilidad de su ocurrencia para calcular la magnitud de riesgo presente.



ISO TR 14121-2 "Evaluación del riesgo – Orientación práctica y ejemplos de métodos" muestra distintos métodos para la clasificación del riesgo. Existen diferencias en la terminología y los sistemas de puntuación, pero todos los métodos guardan relación con los principios establecidos en (EN) ISO 12100. El texto a continuación pone de relieve los principios de cuantificación del riesgo básicos y tiene como objetivo ofrecer ayuda con independencia de la metodología utilizada. Por lo general sigue los parámetros indicados en la herramienta híbrida de la cláusula 6.5 de ISO TR 14121-2.

Los siguientes factores se tienen en consideración:

- GRAVEDAD DE UNA LESIÓN POTENCIAL.
- PROBABILIDAD DE SU OCURRENCIA.

La probabilidad de su ocurrencia incluye como mínimo dos factores:

- FRECUENCIA DE EXPOSICIÓN.
- PROBABILIDAD DE LESIÓN.

Con frecuencia, el propio factor de probabilidad se divide en otros factores como:

- PROBABILIDAD DE OCURRENCIA.
- POSIBILIDAD DE EVITACIÓN.

Use todos los datos y las experiencias disponibles. Puesto que está tratando con todas las etapas de la vida útil de la máquina, y para evitar excesiva complejidad, base sus decisiones en el peor de los casos para cada factor. También es importante usar el sentido común. Las decisiones deben tener en consideración lo que es factible, realista y posible. Es aquí donde es valioso el enfoque de un equipo que incluya miembros de diversas áreas.

En esta etapa normalmente no se tendría en cuenta ninguno de los sistemas de protección existentes. Si esta estimación de riesgos muestra que se requiere un sistema de protección, existen algunas metodologías mostradas posteriormente en este capítulo que pueden ser útiles para determinar las características requeridas.

Gravedad de una lesión potencial

Para esta consideración daremos por hecho que el accidente o incidente ha ocurrido. Un estudio cuidadoso de la fuente de peligro revela cuál es la lesión más grave posible.

Recuerde: Para esta consideración estamos suponiendo que una lesión es inevitable y sólo estamos preocupados por su gravedad. Debe suponer que el operador está expuesto al movimiento o proceso peligroso. La gravedad de la lesión deberá evaluarse en función de los factores establecidos en la metodología elegida.

Por ejemplo, los siguientes:

- Defunción, pérdida de un ojo o brazo
- Efecto permanente; por ejemplo, pérdida de los dedos
- Efecto reversible y necesidad de atención médica
- Efecto reversible y necesidad de primeros auxilios

Frecuencia de la exposición

La frecuencia de exposición responde a la pregunta de con qué frecuencia está expuesto al peligro el operador o la persona a cargo de mantenimiento. La frecuencia de la exposición al riesgo podrá clasificarse en función de los factores establecidos en la metodología elegida.

Por ejemplo, los siguientes:

- Superior a una vez cada hora
- Entre una vez cada hora y una vez al día
- Entre una vez al día y una vez cada dos semanas
- Entre una vez cada dos semanas y una vez al año
- Inferior a una vez al año

Probabilidad de lesiones

Debe suponer que el operador está expuesto al movimiento o proceso peligroso. La probabilidad de que se produzca un evento peligroso podrá clasificarse en función de los factores establecidos en la metodología elegida. La probabilidad de ocurrencia se podrá clasificar teniendo en cuenta las características de la máquina, el comportamiento humano previsto y otros factores.

Por ejemplo, los siguientes:

- Insignificante
- Improbable
- Posible
- Probable
- Probabilidad muy alta

Posibilidad de evitación

Teniendo en cuenta la interacción de las personas con la máquina y otras características, como la velocidad de movimiento al arrancar, la posibilidad de evitar lesiones se podrá clasificar en función de los factores señalados en la metodología elegida.

Por ejemplo, los siguientes:

- Probable
- Posible
- Imposible



Una vez abordados todos los encabezados, los resultados se introducirán en el diagrama o la tabla de la cuantificación del riesgo que se esté utilizando. Esto dará lugar a una especie de estimación cuantificada de los riesgos sobre los diferentes peligros de la máquina. Esta información se podrá utilizar después para determinar qué riesgos tienen que reducirse para lograr un nivel de seguridad aceptable.

Reducción de riesgos

Ahora debemos considerar cada máquina y sus riesgos respectivos, y tomar medidas para solucionar todos sus peligros.

Jerarquía de medidas de reducción de riesgos

Existen tres métodos básicos que deben considerarse y usarse en el siguiente orden:

1. Eliminación o reducción de los riesgos en la mayor medida posible (diseño y fabricación de la maquinaria inherentemente seguros).
2. Instalación de medios de protección y adopción de medidas de protección complementarias en relación con los riesgos que no puedan eliminarse con el diseño.
3. Suministro de información para un uso seguro, incluidas señales de advertencia. También información sobre cualquier riesgo residual y si se necesita alguna formación o equipo de protección personal concreto.

Cada medida de la jerarquía debe considerarse, empezando por la más importante, y usarse siempre que sea posible. Esto generalmente resulta en el uso de una combinación de medidas.

Supresión del riesgo (diseño inherentemente seguro)

En la fase de diseño de la máquina es posible evitar muchos de los posibles peligros simplemente mediante una consideración cuidadosa de factores tales como materiales, requisitos de acceso, superficies calientes, métodos de transmisión, puntos de atrapamiento, niveles de voltaje, etc.

Por ejemplo, si no se requiere acceso a un área peligrosa, la solución es protegerla dentro del cuerpo de la máquina o por algún tipo de resguardo de aislamiento fijo.

Sistemas y medidas de protección

Si se requiere acceso, entonces las cosas se complican un poco. Es necesario asegurar que sólo pueda obtenerse acceso mientras la máquina esté en condición de seguridad. Se requieren medidas de protección tales como puertas de resguardo enclavadas y/o sistemas de disparo. La selección del dispositivo o sistema depende significativamente de las características de operación de la máquina. Se trata de un aspecto extremadamente importante, ya que un sistema que dificulte la eficiencia de las máquinas será propenso a sufrir retiradas u omisiones no autorizadas.

Unas de las interacciones entre las personas y la maquinaria más completas y con mayor implicación se produce durante el mantenimiento, la resolución de problemas y la reparación. En el caso de las intervenciones rutinarias y de poca importancia, se podrán emplear medidas de protección basadas en el sistema relacionado con la seguridad (véase la descripción más adelante) para garantizar la seguridad. No obstante, en todas las normas queda absolutamente claro que, para cualquier tipo de intervención, como las operaciones de mantenimiento, reparación, desmontaje o trabajos en los circuitos eléctricos importantes, deberán suministrarse y emplearse equipos que garanticen el aislamiento y disipación de la energía (en ocasiones, incluida la fuerza gravitacional) en la máquina. De este modo se podrá suprimir el riesgo de un arranque imprevisto y la exposición a fuentes de energía. Este aspecto está cubierto por muchas normativas y reglamentos distintos. Por ejemplo, véase el texto anterior en “Regulaciones de los EE.UU.” que describe las normas sobre “bloqueo-etiquetado de seguridad”. La norma europea e ISO EN 1037 y las normas ISO 14118 “Prevención de un arranque imprevisto” también establecen requisitos. En lo que respecta a la tecnología eléctrica, IEC/EN 60204-1 y NFPA 79 también contienen pautas y requisitos. Naturalmente, es obligatorio disponer de un sistema que funcione adecuadamente y que garantice el seguimiento de los procedimientos correctos.

La sección a continuación describe algunas implementaciones típicas.

Prevención de puesta en marcha intempestiva

Muchas normas abarcan la prevención de una puesta en marcha intempestiva. Algunos ejemplos incluyen ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 y AS 4024.1603. Estas normas tienen un tema en común: el método primario de evitar la activación inesperada es desconectar la energía del sistema y bloquear el sistema en estado desactivado. El objetivo es permitir un acceso seguro de las personas a las zonas peligrosas de una máquina.

Bloqueo-etiquetado

Los nuevos equipos deben fabricarse con dispositivos de aislamiento de la energía enclavables. Los dispositivos se aplican a todos los tipos de energía, tales como eléctrica, hidráulica, neumática, de gravedad y láser. Bloqueo significa aplicar un bloqueo a un dispositivo aislador de energía. El bloqueo sólo debe ser retirado por quien lo haya puesto o por un supervisor bajo condiciones controladas. Cuando varias personas deben trabajar en la máquina, cada persona debe aplicar sus bloqueos a los dispositivos de aislamiento de energía. Cada bloqueo debe ser identificable a quien lo haya puesto.

En los EE.UU. el etiquetado de seguridad es una alternativa al bloqueo de máquinas antiguas si nunca se instaló un dispositivo bloqueable. En este caso la máquina se desactiva y se coloca una etiqueta para advertir a todo el personal que no arranque la máquina mientras el portador de la etiqueta esté trabajando en ella. A partir de 1990, las máquinas modificadas deben actualizarse para incluir un dispositivo aislador de energía bloqueable.



Un dispositivo aislador de energía es un dispositivo mecánico que evita físicamente la transmisión o la liberación de energía. Estos dispositivos pueden ser un interruptor automático, un desconectador, un interruptor operado manualmente, una combinación de conector/socket o una válvula de operación manual. Los dispositivos de aislamiento eléctrico deben desconectar las fases de alimentación de suministro sin conexión a tierra y ningún polo debe funcionar independientemente.

El propósito del bloqueo y etiquetado de seguridad es evitar el arranque inesperado de la máquina. El arranque inesperado puede ser resultado de varias causas: Un fallo del sistema de control; una acción inapropiada en un control de arranque, sensor, contactor o válvula; restauración de la alimentación eléctrica después de una interrupción, o alguna otra influencia interna o externa. Después de realizar el procedimiento de bloqueo o etiquetado de seguridad, debe verificarse la disipación de energía.

Sistemas de aislamiento de seguridad

Los sistemas de aislamiento de seguridad ejecutan la desactivación ordenada de una máquina, y también proporcionan un método fácil de bloquear la alimentación eléctrica a una máquina. Este método funciona bien para sistemas de fabricación y máquinas de mayor tamaño, especialmente cuando varias fuentes de energía están ubicadas a nivel de entresuelo o en lugares distantes.

Interruptores de corte de carga

Para el aislamiento local de dispositivos eléctricos es posible colocar interruptores justo antes del dispositivo que necesita aislarse y bloquearse. Los interruptores de carga referencia boletín 194E son un ejemplo de un producto con capacidad de aislamiento y bloqueo.

Sistemas con atrapamiento de llave

Los sistemas con atrapamiento de llave son otro método para implementar un sistema de bloqueo. Muchos sistemas con atrapamiento de llave comienzan con un dispositivo aislador de energía. Cuando el interruptor es desactivado por la llave “primaria”, se desconecta la energía eléctrica a la máquina simultáneamente de todos los conductores de alimentación sin conexión a tierra. La llave primaria puede retirarse y llevarse a un lugar donde se requiera acceso a la máquina. Es posible añadir varios componentes para configuraciones de bloqueo más complejas.

Medidas alternativas al bloqueo

El bloqueo y el etiquetado de seguridad deben usarse durante las tareas de servicio o mantenimiento de las máquinas. Las intervenciones en la máquina durante las operaciones de fabricación normales están cubiertas por medidas de protección, como los sistemas de enclavamiento de las puertas de resguardo. La diferencia entre las operaciones de servicio/mantenimiento y las operaciones normales de producción no siempre es clara.

Algunos ajustes menores y tareas de servicio que se llevan a cabo durante las operaciones de producción normales no necesariamente requieren que se bloquee la máquina. Algunos ejemplos son carga y descarga de materiales, cambios y ajustes menores en las herramientas, niveles de lubricación de servicio y retirar el material de desecho. Estas tareas deben ser rutinarias, repetitivas e integrales al uso del equipo de producción, y el trabajo se debe realizar usando medidas alternativas, tales como medidas eficaces de protección. Las medidas de protección incluyen dispositivos como resguardos de enclavamiento, barreras optoelectrónicas y tapetes de seguridad. Si se emplean con dispositivos de salida y lógica de seguridad adecuados, los operadores podrán acceder de forma segura a las zonas peligrosas de la máquina durante las tareas de producción normales y las intervenciones de poca importancia.

La seguridad de la máquina en este caso depende del uso apropiado y de la correcta operación del sistema de protección incluso en condiciones de fallo. Ahora debe considerarse la correcta operación del sistema. Dentro de cada tipo es posible que haya una variedad de tecnologías con diversos grados de rendimiento de la monitorización, detección o prevención de fallos.

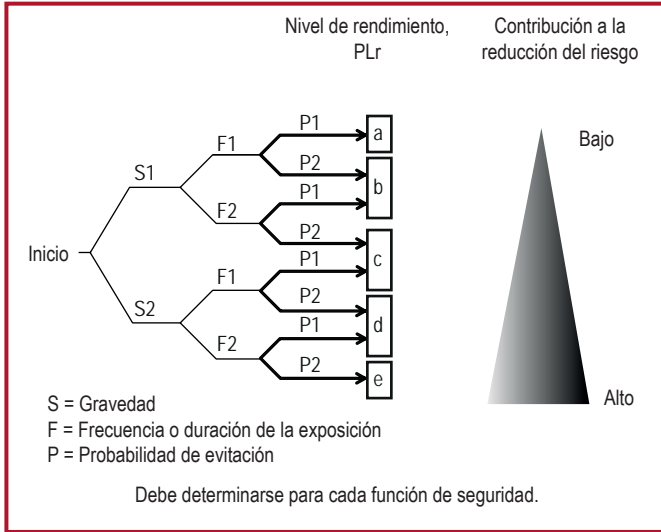
En condiciones ideales, todo sistema de protección sería perfecto sin posibilidades de fallo ni condiciones peligrosas. Sin embargo, en el mundo real, estamos restringidos por los límites actuales de conocimientos y materiales. Otra restricción muy real son los costes. Teniendo en cuenta estos factores, es evidente que necesitamos una forma de establecer una relación entre el alcance de las medidas de protección y el nivel de riesgo obtenido en la etapa de cálculo de riesgo.

Independientemente del tipo de dispositivo de protección seleccionado debe recordarse que un sistema de control relativo con la seguridad puede contener muchos elementos, entre ellos el dispositivo protector, el cableado, el dispositivo de conmutación de alimentación eléctrica y algunas veces partes del sistema de control operativo de la máquina. Todos estos elementos del sistema (incluidos los resguardos, el montaje, el cableado, etc.) deben tener características de rendimiento apropiadas pertinentes a sus principios y tecnología de diseño. IEC/EN 62061 y (EN) ISO 13849-1 clasifican niveles jerárquicos de rendimiento para los componentes relacionados con la seguridad de los sistemas de control y sus anexos incluyen métodos de evaluación de riesgos para determinar los requisitos de integridad de un sistema de protección.



Sistemas de seguridad para maquinaria industrial

(EN) ISO 13849-1:2015 incluye un gráfico de riesgo mejorado en su Anexo A.



IEC 62061 también proporciona un método en su Anexo A, el cual tiene el formato mostrado a continuación.

Evaluación de riesgos y medidas de seguridad										N.º de documento:		
Producto: _____										Parte de:		
Expedido por: _____										<input type="checkbox"/> Evaluación de riesgos previa		
Fecha: _____										<input type="checkbox"/> Evaluación de riesgos intermedia		
Zona negra = medidas de seguridad necesarias Zona gris = medidas de seguridad recomendadas										<input type="checkbox"/> Evaluación de riesgos de seguimiento		
Consecuencia	Gravedad Se	Clase CI					Frecuencia y duración, Fr	Probabilidad de evento peligroso, Pr	Evitación Av			
		3-4	5-7	8-10	11-13	14-15						
Fallecimiento, pérdida de un ojo o brazo		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hora	5	Común	5		
Permanente, pérdida de los dedos			OM	SIL 1	SIL 2	SIL 3	> 1 h – <= día	5	Probable	4		
Reversible, atención médica				OM	SIL 1	SIL 2	> 1 día – <= 2 semanas	4	Posible	3	Imposible	5
Reversible, primeros auxilios					OM	SIL 1	> 2 semanas – <= 1 año	3	Improbable	2	Posible	3
							> 1 año	2	Insignificante	1	Probable	1

N.º ser.	N.º riesgo	Riesgo	Se	Fr	Pr	Av	CI	Medida de seguridad	Seguro

Comentarios

El uso de cualquiera de los métodos anteriores debe proporcionar resultados equivalentes. Cada método está diseñado para considerar el contenido detallado de la norma a la cual pertenece.

En ambos casos es muy importante que se use la orientación provista en el texto de la norma. La tabla o el gráfico de riesgos no debe usarse de manera aislada o excesivamente simplista.

Evaluación

Después de seleccionar la medida de protección y antes de implementarla, es importante repetir la estimación de riesgo. Éste es un procedimiento que a menudo se omite. Puede darse el caso de que si instalamos una medida de protección, el operador de la máquina pudiese sentir que está total y completamente protegido contra el riesgo previsto.

Puesto que ya no tiene la concientización original del peligro puede intervenir en la máquina de manera diferente. Quizás quede expuesto al peligro con mayor frecuencia o acceda al interior de la máquina repetidamente. Esto significa que si la medida de protección falla, exista mayor riesgo que el previsto anteriormente. Éste es el riesgo real que debemos calcular. Por lo tanto, la estimación de riesgo debe repetirse teniendo en cuenta cualquier cambio previsto en la manera en que el personal pueda intervenir en la máquina. El resultado de esta actividad se usa para verificar si las medidas de protección propuestas son, de hecho, apropiadas. Para obtener mayor información se recomienda leer el Anexo A del IEC/EN 62061.

Formación técnica, equipo protector personal, etc.

Es importante que los operadores tengan la formación técnica necesaria en los métodos de trabajo seguro de una máquina. Esto no significa que deban omitirse otras medidas. No es aceptable simplemente indicarle a un operador que no debe acercarse a las áreas peligrosas (como alternativa de protección).

También puede ser necesario que el operador use equipos como guantes especiales, gafas de protección, máscaras, etc. El diseñador de la maquinaria debe especificar el tipo de equipo requerido. El uso de equipo de protección personal generalmente no constituye el método de protección principal, sino que complementa las medidas indicadas anteriormente. Normalmente también se necesitarán señales y marcas que faciliten la concienciación sobre los posibles riesgos residuales.



Capítulo 4: Implementación de las medidas protección

Cuando la evaluación de riesgos muestra que una máquina o que un proceso tiene el riesgo de causar lesiones personales, la fuente de peligro debe eliminarse o minimizarse. La manera de hacer esto depende del tipo de máquina y de la fuente de peligro. Las medidas de protección del sistema de control de seguridad, junto con los resguardos, evitan el acceso a un riesgo o el movimiento peligroso en una zona de riesgo cuando el acceso está disponible. Más adelante se explicarán ejemplos típicos de medidas de protección de sistemas de control de seguridad, incluidos resguardos enclavados, barreras optoelectrónicas, tapetes de seguridad, controles bimanuales e interruptores habilitantes.

Los sistemas y los dispositivos de parada de emergencia están asociados con sistemas de control relacionados con la seguridad, pero no son sistemas de protección directa, sólo deben considerarse como medidas de protección complementarias.

Cómo evitar el acceso con resguardos de aislamiento fijos

Si la fuente de peligro se encuentra en una parte de la máquina que no requiere acceso, debe contar con un resguardo fijo permanente en la maquinaria. Estos tipos de resguardos requieren siempre herramientas para su desinstalación. Los resguardos fijos deben 1) resistir su entorno de operación, 2) contener proyectiles si es necesario y 3) no crear peligros mediante bordes puntiagudos, por ejemplo. Es posible que los resguardos fijos tengan aberturas donde el resguardo se acopla con la maquinaria o debido a un envoltente tipo malla.

Las ventanillas permiten supervisar el rendimiento del equipo de una forma cómoda. Es preciso prestar atención a la selección del material utilizado, ya que las interacciones químicas con los fluidos de corte, los rayos ultravioleta y el mero envejecimiento podrían hacer que el material de las ventanillas se deteriorase con el tiempo.

El tamaño de las aberturas debe impedir que el operador llegue al peligro. Las tablas O-10 de U.S. OSHA 1910.217 (f) (4), ISO 13854, D-1 de ANSI B11.19, 3 de CSA Z432 y AS4024.1 dan orientación sobre la distancia apropiada a las piezas de riesgo a la que debe estar una abertura específica.

Detección de acceso

Se pueden utilizar medidas de protección para detectar el acceso a una zona de peligro. Cuando se selecciona la detección como método de reducción de riesgos, el diseñador debe entender que debe usarse un sistema de seguridad completo; el dispositivo de protección, por sí mismo, no proporciona la reducción de riesgo necesaria. Este sistema de seguridad generalmente consta de tres bloques: 1) un dispositivo de entrada que detecta el acceso al peligro, 2) un dispositivo lógico que procesa las señales del dispositivo detector, verifica el estado del sistema de seguridad y activa o desactiva los dispositivos de salida, y 3) un dispositivo de salida que controla el accionador (por ejemplo, un motor).

Implementación de las medidas protección

Dispositivos de detección

Muchos dispositivos alternativos están disponibles para detectar la presencia de una persona que entra o que está dentro del área peligrosa. La mejor opción para una aplicación en particular depende de una serie de factores.

- Factores ambientales que podrían influir en la fiabilidad del detector
- Frecuencia de acceso;
- Tiempo de parada del peligro;
- Importancia de completar el ciclo de la máquina, y
- Contención de proyectiles, fluidos, nebulizaciones, vapores, etc.

Los resguardos móviles seleccionados de manera adecuada pueden enclavarse para proporcionar protección contra proyectiles, fluidos, nubes tóxicas y otros tipos de peligros, y a menudo se usan cuando el acceso al peligro es poco frecuente. Los resguardos enclavados también se pueden bloquear para impedir el acceso hasta que la máquina se haya detenido por completo o cuando no sea conveniente detener el equipo a mitad del ciclo.

Los dispositivos de detección de presencia, como las barreras optoelectrónicas, los tapetes y los escáneres láser, proporcionan un acceso rápido y sencillo a la zona peligrosa y, en consecuencia, muchas veces se seleccionan cuando los operadores deben acceder a esta con frecuencia. Estos tipos de dispositivos no proporcionan protección contra proyectiles, nubes tóxicas, fluidos u otros tipos de peligros.

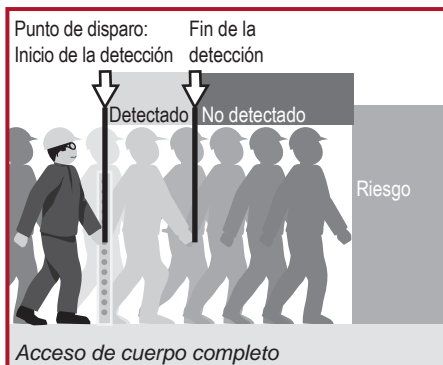
La mejor selección de medida de protección es un dispositivo o sistema que proporcione la máxima protección con la mínima obstrucción a la operación normal de la máquina. Deberán tenerse en cuenta todos los aspectos del uso de la máquina, ya que la experiencia ha puesto de manifiesto que si un sistema es difícil de utilizar, es más probable que se retire u omite.

Dispositivos de detección de presencia

IEC 62046 ofrece orientación práctica para la aplicación de dispositivos detectores de presencia. Se recomienda su uso. Cuando se decide cómo proteger una zona o un área, es importante comprender claramente qué funciones de seguridad se requieren exactamente. En general habrá por lo menos dos funciones.

- Desactivar o desconectar la alimentación eléctrica cuando una persona entra al área de peligro.
- Evitar activar o conectar la alimentación eléctrica cuando una persona está en el área de peligro.

Puede que a primera vista parezcan lo mismo; no obstante, a pesar de que obviamente están vinculadas y con frecuencia se logran con el mismo equipo, en realidad son dos funciones de seguridad distintas. Para lograr el primer punto, necesitamos usar alguna forma de dispositivo de disparo. En otras palabras, un dispositivo que detecte que una parte de una persona ha pasado más allá de un punto específico y que proporcione una señal para desconectar la alimentación eléctrica. Si la persona puede entonces continuar pasado este punto de disparo y su presencia ya no es detectada, entonces puede que no se logre el segundo punto (evitar la activación).



La imagen muestra un ejemplo de acceso de cuerpo completo con una barrera optoelectrónica instalada en vertical como dispositivo de activación. Las puertas de resguardo enclavadas también pueden considerarse como dispositivo sólo de disparo, cuando no haya nada que evite que la puerta se cierre después de la entrada.

Si el acceso de todo el cuerpo no es posible y, por lo tanto, una persona no puede continuar más allá del punto de disparo, su presencia siempre es detectada y se logra el segundo punto (evitar la activación). Para aplicaciones con acceso parcial del cuerpo, los mismos tipos de dispositivos realizan detección de presencia y de disparo. La única diferencia es el tipo de aplicación.

Los dispositivos de detección de presencia se usan para detectar la presencia de personas. La familia de dispositivos incluye barreras ópticas de seguridad, barreras de seguridad de un único haz, escáneres láser de seguridad y tapetes de seguridad. Para la instalación de cualquier dispositivo de detección de presencia, el tamaño de la zona de detección y la ubicación del dispositivo deberán tener en cuenta la distancia de seguridad necesaria.

Barreras optoelectrónicas de seguridad

Las barreras optoelectrónicas de seguridad son detectores fotoeléctricos de presencia diseñados específicamente para proteger al personal contra lesiones relacionadas al movimiento peligroso de la máquina. Las barreras optoelectrónicas, también denominadas AOPD (Active Opto-electronic Protective Devices, dispositivos de protección optoelectrónicos activos) o ESPE (Electro Sensitive Protective Equipment, equipos de protección electrosensibles), ofrecen un grado de seguridad óptimo al tiempo que pueden permitir un incremento de la productividad. Son ideales para aplicaciones en las que el personal debe obtener acceso fácilmente y con frecuencia a un punto de operación que presenta algún tipo de peligro. Las barreras optoelectrónicas están diseñadas y probadas para cumplir con las normas IEC 61496-1 y -2.

Escáneres láser de seguridad

Los escáneres láser de seguridad usan un espejo giratorio que desvía los pulsos de luz sobre un arco, creando un plano de detección. El ángulo de rotación del espejo

Implementación de las medidas protección

determina la ubicación del objeto. Mediante una técnica de “tiempo de vuelo” de un haz reflejado de luz invisible, el escáner también puede detectar la distancia a la que el objeto se encuentra del escáner. Al tomar la distancia medida y la ubicación del objeto, el escáner de láser determina la posición exacta del objeto.

Tapetes de seguridad para el suelo, sensibles a la presión

Estos dispositivos se usan para proporcionar resguardo a cierta área del suelo alrededor de una máquina. Se coloca una matriz de tapetes interconectados alrededor del área de peligro, y la presión aplicada al tapete (por ej., la pisada de un operador) causa que la unidad controladora del tapete desactive la alimentación eléctrica al punto de peligro. Las alfombras sensibles a la presión se utilizan con frecuencia en zonas cerradas que contienen varios equipos, sistemas de fabricación flexibles o celdas robóticas. Cuando es preciso obtener acceso a la celda (para la configuración o “aprendizaje” del robot, por ejemplo), impiden los movimientos peligrosos si el operador abandona la zona segura. Es importante evitar cualquier movimiento del tapete o tapetes con un sistema de fijación adecuado y seguro.

Bordes sensibles a la presión

Estos dispositivos son tiras que pueden montarse al borde de una pieza móvil, como una mesa o una puerta eléctrica de una máquina que presente un riesgo de trituración o corte.

Si la pieza móvil golpea al operador (o viceversa), el borde sensible flexible se oprime e inicia un comando para desactivar la fuente de energía del peligro. Los bordes sensibles también pueden usarse para resguardar maquinaria cuando existe el riesgo de atrapamiento. Si un operador queda atrapado en la máquina, el contacto con el borde sensible desactiva la alimentación eléctrica a la máquina.

Las barreras optoelectrónicas, los escáneres, las alfombras y los bordes sensibles también se clasifican como “dispositivos de activación”. No restringen el acceso, lo “detectan”. Se basan totalmente en su capacidad de detección y conmutación para ofrecer seguridad. Generalmente son adecuados sólo para maquinarias que se detienen razonablemente rápido después que se desconecta la alimentación eléctrica. Puesto que un operador puede caminar o entrar directamente al área peligrosa, obviamente es necesario que el tiempo requerido para que el movimiento se detenga sea menor que el tiempo requerido para que el operador entre en contacto con la zona peligrosa.

Interruptores de seguridad

Si el acceso al equipo es poco frecuente o cabe la posibilidad de proyección de un componente, se suelen preferir los resguardos móviles (accionables). El resguardo se enclava con el suministro de energía de la pieza de peligro de manera que asegure que cada vez que la puerta de resguardo no esté cerrada, se desactive la alimentación eléctrica de la zona de peligro.

Este método requiere el uso de un interruptor de enclavamiento acoplado a la puerta de resguardo. El control de la fuente de energía de la zona de peligro es controlado a través de la sección de conmutación de la unidad. La fuente de energía es generalmente eléctrica, pero podría ser también neumática o hidráulica. Cuando se detecta movimiento (abertura) de la puerta de resguardo, el interruptor de enclavamiento inicia



un comando para aislar el suministro de energía ya sea directamente o mediante un contactor de alimentación eléctrica (o válvula).

Algunos interruptores de enclavamiento también incorporan un dispositivo de enclavamiento que enclava la puerta de resguardo en posición cerrada y no permite que se abra mientras la máquina no esté en condición segura.

En la mayoría de las aplicaciones, la solución más fiable y económica es la combinación de un resguardo móvil y un interruptor de enclavamiento con o sin bloqueo del resguardo. (EN) ISO 14119 ofrece orientación práctica para la selección de todos los tipos de dispositivo de enclavamiento de resguardo. Se recomienda su uso.

Existe una amplia variedad de opciones de interruptores de seguridad:

- **Interruptores de seguridad con enclavamiento de lengüeta** – estos dispositivos requieren la inserción y extracción en el interruptor de un accionador con forma de lengüeta para su funcionamiento
- **Interruptores de enclavamiento de bisagra** – estos dispositivos se colocan sobre el pasador de la bisagra de una puerta de resguardo, y utilizan la acción de abertura del resguardo para el accionador.
- **Interruptores de enclavamiento con bloqueo** – En algunas aplicaciones se requiere bloquear el resguardo cerrado o retardar la abertura del resguardo. Los dispositivos adecuados para este requisito se conocen como interruptores de enclavamiento con bloqueo de resguardo. Estos dispositivos son apropiados para máquinas con retardo al paro, pero también pueden ofrecer un aumento significativo del nivel de protección a la mayoría de tipos de máquinas.
- **Interruptores de enclavamiento sin contacto** – estos dispositivos no requieren contacto físico para actuar con algunas versiones que incorporan una función de codificación para aumentar la resistencia a las intrusiones.
- **Dispositivos de enclavamiento de posición (interruptor de final de carrera)** – El accionamiento operado por levas generalmente toma la forma de un interruptor de final de carrera (o posición) positivo y una leva lineal o giratoria. Generalmente se usan en resguardos deslizantes.
- **Dispositivos de enclavamiento con atrapamiento de llave** – Las llaves de bloqueo mecánico pueden realizar enclavamiento de control así como enclavamiento de la alimentación eléctrica. Con el “enclavamiento de control” un dispositivo de enclavamiento inicia un comando de parada a un dispositivo intermedio, el cual desactiva un dispositivo subsiguiente para desconectar la energía del accionador. Con el “enclavamiento de la alimentación eléctrica”, el comando de parada interrumpe directamente el suministro de energía a los accionadores de la máquina.

Interfaces hombre-máquina

Función de parada – En los EE.UU., Canadá, Europa y a nivel internacional existe armonización de normas con respecto a la descripción de las categorías de parada para máquinas o sistemas de fabricación.

Implementación de las medidas protección

NOTA: estas categorías difieren de las categorías de ISO 13849-1. Consulte las normas NFPA 79 e IEC/EN 60204-1 si desea más información. Las funciones de parada pertenecen a tres categorías:

Categoría 0 es una parada mediante desconexión inmediata de la alimentación eléctrica a los accionadores de la máquina. Esto se considera parada no controlada. Con la alimentación eléctrica desconectada, la acción de freno que requiere alimentación eléctrica no es eficaz. Esto permite que los motores giren libremente y que paren por inercia en un largo período de tiempo. En otros casos, las máquinas que retienen accesorios puede dejar caer material, ya que requieren alimentación eléctrica para retener el material. También se pueden emplear medios de detención mecánicos (frenos) que no necesiten alimentación con una parada de categoría 0. Las paradas categoría 0 tienen prioridad sobre las paradas categoría 1 ó 2.

Categoría 1 es a una parada controlada con alimentación eléctrica disponible para los accionadores de la máquina para lograr la detención. Luego, cuando se realiza la parada, la alimentación eléctrica se desconecta de los accionadores. Esta categoría de parada permite que el freno energizado detenga rápidamente el movimiento peligroso, y luego la alimentación eléctrica puede desconectarse de los accionadores. Este tipo de parada puede redundar en una parada más rápida y controlada que permita un reinicio en menor tiempo. NOTA: La edición 2016 de IEC/EN 60204-1 ampliará los tipos de parada de categoría 1.

Categoría 2 es una parada controlada con alimentación eléctrica disponible a los accionadores de la máquina. Una parada de producción normal se considera parada categoría 2.

Estas categorías de parada deben aplicarse a cada una de las funciones de parada, cuando es la acción tomada por los dispositivos de control de seguridad en respuesta a una señal de entrada, debe utilizarse la categoría 0 ó 1. Las funciones de parada deben anular las funciones de arranque relacionadas. La selección de la categoría de parada de cada una de las funciones de paro debe determinarse mediante una evaluación de riesgos.

Función de parada de emergencia

La función de parada de emergencia debe funcionar como parada de categoría 0 o de categoría 1, según lo determine una evaluación de riesgos. Debe ser iniciada por una sola acción humana. Al ejecutarse debe anular todas las demás funciones y los modos de operación de la máquina. El objetivo es desconectar la alimentación eléctrica tan rápidamente como sea posible, sin crear peligros adicionales. Siempre que exista el peligro de que un operador corra algún riesgo con una máquina, debe haber facilidades para el acceso rápido a un dispositivo de parada de emergencia. El dispositivo de paro de emergencia debe estar siempre operativo y disponible. Los paneles del operador deben contener como mínimo un dispositivo de paro de emergencia. Se pueden utilizar dispositivos de paro de emergencia adicionales en otras ubicaciones en función de las necesidades. Los dispositivos de paro de emergencia adoptan diversas formas. Los botones pulsadores y los interruptores accionados por cable constituyen ejemplos de los tipos de dispositivos más populares



Hasta hace poco, los circuitos de parada de emergencia requerían componentes electromecánicos cableados. Los últimos cambios en normas como IEC 60204-1 y NFPA 79 permiten utilizar PLC de seguridad y otras formas de lógica electrónica conformes con los requisitos de normas como IEC 61508 en los circuitos de paro de emergencia.

Los dispositivos de parada de emergencia se consideran equipo de protección complementaria. No se consideran dispositivos de protección primaria porque no evitan el acceso a piezas peligrosas o no detectan el acceso a piezas peligrosas. Dependen de la interacción humana.

Si desea más información sobre los dispositivos de paro de emergencia, lea ISO/EN 13850, IEC 60947-5-5, NFPA 79 e IEC 60204-1, AS4024.1, Z432-94.

Pulsadores de paro de emergencia

Si se utiliza un botón pulsador como dispositivo de paro de emergencia, este tendrá que ser de tipo hongo, de color rojo y con fondo amarillo. Cuando se accione el dispositivo de paro de emergencia, deberá bloquearse. No deberá ser posible generar el comando de paro si esto no ocurre. El reinicio del dispositivo de paro de emergencia no debe provocar una situación peligrosa. Debe utilizarse una acción independiente y deliberada para volver a arrancar la máquina.

Una de las últimas tecnologías que se aplica a los dispositivos de paro de emergencia es la técnica de automonitorización. Se añade un contacto adicional en la parte posterior del botón de parada de emergencia, para monitorizar si otros bloques de contacto siguen estando presentes. Esto se conoce como bloque de contactos automonitorizados. Consta de un contacto accionado por resorte que se cierra cuando el bloque de contactos se encaja en su lugar en el panel.

Interruptores accionados por cable

Para maquinarias tales como transportadores, generalmente es más conveniente y eficaz usar como dispositivo de parada de emergencia un dispositivo accionado por cable a lo largo del área peligrosa. Estos dispositivos usan una cuerda de acero conectada a los interruptores de accionamiento por cuerda, de manera que al tirar de la cuerda en cualquier dirección y en cualquier punto a lo largo de su longitud se acciona el interruptor y se corta la alimentación eléctrica a la máquina.

Los interruptores accionados por cable deben detectar tanto el tiro como la holgura excesiva en el cable. La detección de la holgura permite controlar que el cable no se haya cortado y esté listo para su uso.

El recorrido del cable afecta el rendimiento del interruptor. Para distancias cortas, el interruptor de seguridad se monta en un extremo y un resorte de tensión se monta en el otro. Para distancias mayores debe montarse un interruptor de seguridad en ambos extremos del cable para asegurar que una acción única por parte del operador inicie

Implementación de las medidas protección

un comando de parada. El uso de hembrillas correctamente ubicadas para el apoyo y guía del cable es esencial. La fuerza de tiro del cable necesaria no debe superar los 200 N (45 lbs) ni una distancia de 400 mm (15,75 in) en una posición central entre dos hembrillas. Es importante seguir las instrucciones del fabricante para lograr un rendimiento operativo adecuado.

Control de mandos bimanuales

El uso de los controles con las dos manos (llamados también controles bimanuales) es un método común para evitar el acceso mientras la máquina está en condición peligrosa. Dos controles deben operarse concurrentemente (a 0,5 s uno de otro) para arrancar la máquina. Esto asegura que ambas manos del operador estén ocupadas en una posición segura (por ej., en los controles) y, por lo tanto, no puedan estar en el área peligrosa. Los controles deben operarse continuamente durante condiciones peligrosas. La operación de la máquina debe detenerse cuando se suelta cualquiera de los controles. Si se suelta uno de los controles, el otro control también debe soltarse para que pueda arrancar la máquina. Esto impide la posibilidad de manipular uno de los controles para omitir el mando bimanual y accionarlos con una sola mano.

Un mando bimanual depende en gran medida de la integridad de su sistema de control y monitorización para detectar cualquier fallo, por lo tanto, es importante que este aspecto esté diseñado según la especificación correcta. El rendimiento de un sistema de un mando bimanual está caracterizado en tipos por ISO 13851 (EN 574) como se muestra, y están relacionados con las categorías de ISO 13849-1. Los tipos más comúnmente usados para seguridad de maquinaria son IIIB e IIIC. La siguiente tabla muestra la relación de los tipos con respecto a las categorías de rendimiento de seguridad.

Requisito	Tipos				
	I	II	III		
			A	B	C
Accionamiento asíncrono			X	X	X
Use de la categoría 1 (de ISO 13849-1)	X		X		
Use de la categoría 3 (de ISO 13849-1)		X		X	
Use de la categoría 4 (de ISO 13849-1)					X

Tabla de requisitos de ISO 13851

La separación en el diseño físico debe impedir la operación incorrecta (por ej., con la mano y el codo). Esto puede realizarse mediante distancia o protectores. La máquina no debe ir de un ciclo a otro sin soltar y presionar ambos botones. Esto proporciona una función "antirrepetición" que impide la posibilidad de que se bloqueen los dos botones y la máquina funcione de manera continua. Soltar cualquiera de los botones debe causar que la máquina se detenga.



El uso del control de dos manos debe considerarse con cautela, ya que generalmente permite la exposición a algún tipo de riesgo. El control de dos manos sólo protege a la persona que los utiliza. El operador protegido debe ser capaz de observar todos los accesos a la pieza peligrosa, ya que otro personal quizás no esté protegido.

ISO 13851 (EN 574) ofrece orientación adicional sobre el mando bimanual.

Dispositivos de validación

Los dispositivos habilitantes son controles que en ocasiones forman parte de una estrategia que permite a los operadores acceder a una zona peligrosa con el motor de riesgo funcionado a una velocidad segura, únicamente mientras mantienen el dispositivo habilitante en la posición de accionamiento. Los dispositivos de validación utilizan tipos de interruptores de dos o tres posiciones. Los tipos de dos posiciones están desactivados cuando no se opera el accionador y están activados cuando se opera el accionador. Los interruptores de tres posiciones se encuentran inactivos mientras no se accionan (posición 1), activos cuando se mantienen en la posición central (posición 2) e inactivos cuando el accionador se desplaza más allá de la posición intermedia (posición 3). Además, al volver de la posición 3 a la 1, el circuito de salida no debe cerrarse al pasar por la posición 2.

Los dispositivos habilitantes deben utilizarse en combinación con otras funciones de seguridad. Un ejemplo típico es el paso del movimiento a un modo lento seguro controlado. Al usar un dispositivo de validación, una señal debe indicar que el dispositivo de validación está activo.

Dispositivos lógicos

Los dispositivos lógicos desempeñan un papel central en la pieza relacionada con la seguridad del sistema de control. Los dispositivos lógicos realizan la verificación y la monitorización del sistema de seguridad, y permiten que la máquina arranque o ejecutan comandos para parar la máquina.

Hay una gama de dispositivos lógicos disponibles para crear una arquitectura de seguridad que satisfaga los requisitos de complejidad y funcionalidad de la máquina. Los relés de seguridad cableados de monitorización son más económicos para máquinas de menor tamaño que requieren un dispositivo lógico dedicado para completar la función de seguridad. Se prefieren relés de seguridad para monitorización modulares y configurables cuando se requiere un número grande y diverso de dispositivos de protección y control mínimo de zona. En el caso de las máquinas de tamaño medio a grande y con características más complejas, puede que sea preferible el uso de sistemas de seguridad programables con E/S distribuidas.

Relés de control de seguridad (MSR)

Los módulos de relé de control de seguridad (MSR) desempeñan un papel clave en muchos sistemas de seguridad. Estos módulos generalmente comprenden dos o más

Implementación de las medidas protección

relés con guía positiva con circuitos adicionales para asegurar el rendimiento de la función de seguridad.

Los relés con guía positiva han sido diseñados para impedir el cierre simultáneo de los contactos normalmente cerrados y normalmente abiertos. Algunos relés de control de seguridad disponen de salidas de estado sólido relacionadas con la seguridad.

Los relés de control de seguridad realizan muchas verificaciones en el sistema de seguridad. En el momento del encendido realizan autoverificaciones de sus componentes internos. Cuando se activan los dispositivos de entrada, el MSR compara los resultados de las entradas redundantes. Si es aceptable, el MSR comprueba los accionadores externos conectados a sus salidas. Si están bien, el MSR espera una señal de restablecimiento para activar sus salidas. Por lo tanto, un MSR correctamente seleccionado y configurado puede proporcionar detección de fallos del sistema mediante la comprobación de su entrada conectada y los dispositivos de salida. También puede proporcionar funciones de enclavamiento contra reinicio/arranque.

La selección del relé de seguridad apropiado depende de una serie de factores: el tipo de dispositivo que controle, el tipo de reinicio, el número y tipo de las salidas, etc.

Tipos de entradas de los relés de control de seguridad (MSR)

Los distintos tipos de dispositivos de protección proporcionan diferentes clases de entradas a un relé de control de seguridad. Por este motivo es importante comprobar que sean compatibles. A continuación se incluye un breve resumen de los tipos de entradas habituales y de las características de detección de fallos cruzados necesarias.

Enclavamientos electromecánicos, algunos enclavamientos sin contacto y dispositivos de paro de emergencia: Contactos mecánicos, un solo canal con un contacto normalmente cerrado o doble canal, ambos normalmente cerrados. El MSR debe admitir canales sencillos o dobles y proporcionar funciones de detección de fallos cruzados para los sistemas de doble canal.

Algunos enclavamientos sin contacto y dispositivos de paro de emergencia: Contactos mecánicos, doble canal, uno normalmente abierto y uno normalmente cerrado. El MSR debe ser capaz de procesar diversas entradas.

Dispositivos con salidas de estado sólido: Barreras optoelectrónicas, escáneres láser y algunos enclavamientos de resguardo sin contacto disponen de dos salidas de surtidor y llevan a cabo su propia detección de fallos cruzados. El MSR debe poder obviar el método de detección de fallos cruzados de los dispositivos.

Tapetes sensibles a la presión: Los tapetes crean un cortocircuito entre doble canal. El MSR debe estar específicamente diseñado o poder configurarse para esta aplicación.

Bordes sensibles a la presión: Algunos bordes están diseñados como tapetes de 4 cables. Algunos son dispositivos de dos cables que crean un cambio en la resistencia. El MSR debe ser capaz de detectar un cortocircuito o el cambio de resistencia.



Detección de movimiento del motor: Mide la fuerza de un motor mientras reduce su velocidad. El MSR debe tolerar altas tensiones, así como detectar bajas tensiones a medida que el motor desacelera.

Mando bimanual: El MSR debe detectar flujos de impulsos provenientes de diversos sensores redundantes.

Control con las dos manos: El MSR debe detectar entradas diversas normalmente abiertas y normalmente cerradas, y proporcionar temporización de 0,5 s y lógica de secuenciamiento.

Los relés de control de seguridad deben estar específicamente diseñados o poder configurarse para interactuar con cada uno de estos tipos de dispositivo, ya que cuentan con características eléctricas distintas. Algunos MSR se pueden configurar completamente como relés de distintos tipos. Algunos MSR pueden hacer conexión con varios tipos de entradas, pero una vez que el dispositivo se ha seleccionado, el MSR sólo puede hacer interfaz con dicho dispositivo. El diseñador deberá seleccionar o configurar un MSR compatible con el dispositivo de entrada.

Impedancia de entrada

La impedancia de entrada de los relés de control de seguridad determina cuántos dispositivos de entrada pueden conectarse al relé y a qué distancia máxima pueden montarse. Por ejemplo, puede que un relé de seguridad tenga una impedancia de entrada permitida máxima de 500 ohmios. Si la impedancia de entrada es superior a 500 ohmios, no activará sus salidas. El usuario debe tener cuidado para asegurarse de que la impedancia de entrada permanezca bajo la especificación máxima. La longitud, el tamaño y el tipo de cable usado afecta la impedancia de entrada.

Número de dispositivos de entrada

El proceso de evaluación de riesgos debe emplearse para determinar el número de dispositivos de entrada que deben conectarse a una unidad de relé de control de seguridad MSR y la frecuencia con la que deben comprobarse los dispositivos de entrada. Para garantizar que los dispositivos de paro de emergencia y los enclavamientos de puerta se encuentren operativos, será preciso comprobar que funcionen en los intervalos regulares que determine la evaluación de riesgos. Por ejemplo, un MSR de entrada de doble canal conectado a una compuerta enclavada que debe abrirse en cada ciclo de la máquina (por ej., varias veces al día) quizás no necesite verificarse. Esto se debe a que la abertura del resguardo hace que el MSR se autoverifique, así como sus entradas y sus salidas (de acuerdo con la configuración) para determinar si tiene fallos individuales. A mayor frecuencia de abertura del resguardo, mayor integridad del proceso de verificación.

Otro ejemplo podría ser el de los dispositivos de paro de emergencia. Dado que normalmente estos únicamente se utilizan en caso de emergencia, lo más probable es que apenas se usen. Por lo tanto, deberá establecerse un calendario para accionar los paros de emergencia y confirmar su eficacia de una forma programada. Este tipo de activación del sistema de seguridad se denomina prueba funcional. Un tercer ejemplo podría ser el de las puertas de acceso para los ajustes del equipo, que, al igual que los paros de emergencia, probablemente se utilizarán con poca frecuencia. En este caso

Implementación de las medidas protección

también debería establecerse un calendario para accionar la función de comprobación de una forma programada.

La evaluación de riesgos ayuda a determinar si los dispositivos de entrada necesitan verificarse y con qué frecuencia. A mayor nivel de riesgo se requiere mayor integridad del proceso de verificación. Y mientras menos frecuente sea la verificación “automática”, más frecuente debe ser la verificación “manual” impuesta.

Detección de fallos cruzados de entrada

En los sistemas de doble canal, el sistema de seguridad debe detectar los fallos de cortocircuito de canal a canal de los dispositivos de entrada, también denominados fallos cruzados. Esto lo realiza un dispositivo detector o el relé de control de seguridad.

Los relés de control de seguridad basados en microprocesadores, como las barreras optoelectrónicas, los escáneres láser y los sensores sin contacto avanzados, detectan estos cortocircuitos de distintas formas. Una de las más comunes es la detección de fallos cruzados mediante las pruebas de impulsos. Las señales de entrada al MSR se impulsan con mucha rapidez. El pulso del canal 1 es offset del pulso del canal 2. Si se produce un cortocircuito, los pulsos ocurren concurrentemente y son detectados por el dispositivo.

Los relés de control de seguridad electromecánicos emplean una técnica diferente: una entrada de activación y una entrada de desactivación. Un cortocircuito del canal 1 al canal 2 hace que el dispositivo de protección contra sobrecorriente se active y el sistema de seguridad se desactive.

Salidas

Los MSR vienen con diversos números de salidas. Los tipos de salidas ayudan a determinar qué MSR debe usarse en aplicaciones específicas.

La mayoría de los MSR tiene por lo menos 2 salidas de seguridad de operación inmediatas. Las salidas de seguridad de los MSR se caracterizan por estar normalmente abiertas. Tienen clasificación de seguridad debido a la redundancia y verificación interna. Un segundo tipo de salida son las salidas retardadas. Las salidas retardadas normalmente se utilizan en las paradas de categoría 1, en las que la máquina necesita tiempo para ejecutar la función de parada antes de permitir acceso a la zona peligrosa. Los MSR también tienen salidas auxiliares. Generalmente éstas se consideran normalmente cerradas.

Especificaciones de salida

Las especificaciones de salida describen la capacidad que tiene el dispositivo de protección de conmutar las cargas. Normalmente, las especificaciones de los dispositivos industriales se describen como resistivas o electromagnéticas. Una carga resistiva puede ser un elemento calefactor. Las cargas electromagnéticas son típicamente relés, contactores o solenoides con una gran característica inductiva de la carga. El Anexo A de la norma IEC 60947-5-1 describe las capacidades nominales de las cargas.



Letra de designación: La designación es una letra seguida por un número, por ejemplo A300. La letra se refiere a la corriente térmica convencional incluida y si dicha corriente es directa o alterna. Por ejemplo, A representa 10 amperes de corriente alterna. Los números se refieren a la tensión de aislamiento nominal. Por ejemplo, 300 representa 300 V.

Utilización: La utilización describe los tipos de carga que el dispositivo es capaz de conmutar. Las utilizaciones relevantes a IEC 60947-5 se muestran en la siguiente tabla.

Utilización	Descripción de la carga
AC-12	Control de cargas resistivas de estado sólido con aislamiento por optoacopladores
AC-13	Control de cargas de estado sólido con aislamiento de transformador
AC-14	Control de pequeñas cargas electromagnéticas (menos de 72 VA)
AC-15	Cargas electromagnéticas mayores de 72 VA
DC-12	Control de cargas resistivas de estado sólido con aislamiento por optoacopladores
DC-13	Control de cargas electromagnéticas
DC-14	Control de cargas electromagnéticas que tienen resistencias en el circuito

Corriente térmica, Ith: La corriente térmica incluida convencional es el valor de corriente usado para las pruebas de subida de temperatura del equipo cuando está instalado en un envolvente especificado.

Tensión nominal de funcionamiento Ue y corriente Ie: La corriente y la tensión nominales de funcionamiento especifican el poder de corte y establecimiento de los elementos de conmutación en condiciones de funcionamiento normales. Los productos Allen-Bradley Guardmaster normalmente tienen una capacidad de 125 VCA, 250 VCA y 24 VCC.

VA: Las especificaciones de VA (Tensión x Amperaje) indican las especificaciones de los elementos de conmutación cuando se cierra el circuito y cuando se abre el circuito.

Ejemplo 1: Una clasificación A150, AC-15 indica que los contactos pueden establecer un circuito de 7200 VA. A 120 V CA, los contactos pueden establecer un circuito de corriente de entrada al momento del arranque de 60 amperios. Puesto que AC-15 es una carga electromagnética, los 60 amperes tienen una corta duración al momento del arranque de la carga. La abertura del circuito es sólo 720 VA porque la corriente de mantenimiento de la carga es 6 A, o sea la corriente nominal o de consumo.

Ejemplo 2: Una clasificación N150, DC-13 indica que los contactos pueden establecer un circuito de 275 VA. A 125 V CA, los contactos pueden establecer un circuito de 2,2 amperios. Las cargas electromagnéticas de CC no tienen una corriente de entrada

Implementación de las medidas protección

al momento del arranque como las cargas electromagnéticas de CA. La apertura del circuito también es de 275 VA porque la corriente de mantenimiento de la carga electromagnética es 2,2 A, o sea la corriente nominal de funcionamiento.

Rearme de la máquina

Si, por ejemplo, se abre un resguardo enclavado en una máquina en operación, el interruptor de enclavamiento de seguridad detiene la máquina. En la mayoría de casos es imperativo que la máquina no se vuelva a arrancar inmediatamente cuando se cierra el resguardo. Una manera común de lograr esto es usar una configuración de arranque con contactor de enclavamiento.

Presionar y soltar el botón de inicio momentáneamente activa la bobina de control del contactor, lo cual cierra los contactos de alimentación eléctrica. Siempre que la alimentación está fluyendo a través de los contactos de alimentación, la bobina de control se mantiene activada (enclavada eléctricamente) mediante los contactos auxiliares del contactor, los cuales están mecánicamente vinculados a los contactos de alimentación. Una interrupción de la alimentación principal o del suministro del control resulta en la desactivación de la bobina y en la apertura de los contactos auxiliares y la alimentación principal. El enclavamiento de resguardo está cableado al circuito de control del contactor. Esto significa que el rearmado puede lograrse sólo cerrando el resguardo y luego realizando el encendido por medio del botón de arranque normal, lo cual restablece el contactor y arranca la máquina.

El requisito para las situaciones de enclavamiento normal queda claro en ISO 12100 (extracto):

“Cuando el resguardo está cerrado las zonas peligrosas de la máquina pueden funcionar, pero al cerrar el resguardo no se inicia el funcionamiento automáticamente”.

Muchas máquinas ya tienen contactores sencillos o dobles que funcionan como se describe anteriormente (o tienen un sistema que logra el mismo resultado). Cuando se acopla un enclavamiento a una maquinaria existente, es importante determinar si la configuración de control de alimentación eléctrica cumple con estos requisitos, y tomar las medidas adicionales necesarias.

Funciones de rearme

Los relés de control de seguridad Guardmaster de Allen-Bradley están diseñados con restablecimiento manual monitorizado o rearme automático/manual.

Restablecimiento manual monitorizado

Un reinicio manual monitorizado requiere un cambio de estado del circuito de restablecimiento una vez que se ha cerrado la puerta o se ha restablecido el dispositivo de paro de emergencia. Los contactos auxiliares normalmente cerrados unidos mecánicamente de los contactores de conmutación de alimentación eléctrica



están conectados en serie con un botón pulsador momentáneo. Después de que el resguardo se abre y se cierra nuevamente, el relé de seguridad no permite que la máquina sea reiniciada hasta que haya un cambio de estado en el pulsador de rearme. Esta disposición cumple el cometido de los requisitos de reinicio manual adicional establecidos en (EN) ISO 13849-1; es decir, la función de reinicio garantiza que ambos contactores estén inactivos, que los dos circuitos de enclavamiento (y, en consecuencia, los resguardos) estén cerrados y (porque se requiere un cambio de estado) que el accionador de reinicio no se haya omitido o bloqueado (manipulado) por cualquier medio. Si estas verificaciones son satisfactorias, la máquina puede volverse a arrancar con los controles normales. (EN) ISO 13849-1 señala el cambio de estado de activo a inactivo ("flanco descendente").

El interruptor de restablecimiento debe ubicarse en un lugar que proporcione buena visibilidad de la fuente de peligro, de manera que el operador pueda verificar que el área esté despejada antes de la operación.

Rearme automático/manual

Algunos relés de seguridad tienen restablecimiento automático/manual. El modo de restablecimiento manual no se monitoriza y el restablecimiento se produce cuando se presiona el botón. No se detecta si el interruptor de restablecimiento está en cortocircuito u obstruido. Con este enfoque puede que no sea posible cumplir los requisitos para el reinicio manual adicional establecidos en (EN) ISO 13849-1, salvo que se empleen medios adicionales.

Alternativamente, la línea de restablecimiento puede conectarse en puente, permitiendo así el restablecimiento automático. Entonces el usuario debe proporcionar otro mecanismo para impedir el arranque de la máquina al cerrar la puerta.

Un dispositivo de restablecimiento automático no requiere acción de conmutación manual, pero después de la desactivación, siempre conduce una verificación de integridad del sistema antes de restablecer el mismo. Un sistema de restablecimiento automático no debe confundirse con un dispositivo sin capacidad de restablecimiento. En este último, el sistema de seguridad se habilita inmediatamente después de la desactivación, pero no se lleva a cabo la verificación de integridad del sistema.

El interruptor de restablecimiento debe ubicarse en un lugar que proporcione buena visibilidad de la fuente de peligro, de manera que el operador pueda verificar que el área esté despejada antes de la operación.

Resguardos de control

Un resguardo de control detiene el funcionamiento de la máquina cuando se abre el resguardo e inicia directamente el funcionamiento nuevamente cuando se cierra el resguardo. El uso de resguardos de control sólo se permite bajo estrictas condiciones, ya que cualquier arranque inesperado o incapacidad de parar puede ser extremadamente peligroso. El sistema de enclavamiento debe tener la más alta

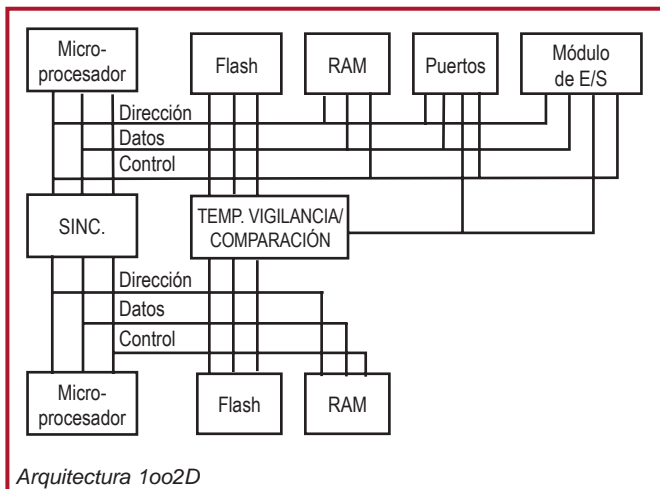
Implementación de las medidas protección

fiabilidad posible (a menudo se aconseja usar enclavamiento de resguardo). El uso de resguardos de control únicamente se puede plantear en maquinaria con la que no exista la posibilidad de que un operador o alguna parte de su cuerpo permanezca o llegue a la zona peligrosa mientras el resguardo esté cerrado. El resguardo de control debe ser el único acceso al área de peligro.

Controladores programables de seguridad

La necesidad de aplicaciones de seguridad flexibles y escalables impulsó el desarrollo de PLC/controladores de seguridad. Los controladores de seguridad programables proporcionan a los usuarios el mismo nivel de flexibilidad de control en una aplicación de seguridad al que están acostumbrados con los controladores programables estándar. Sin embargo existen diferencias extensas entre los PLC estándar y de seguridad. Los PLC de seguridad vienen en varias plataformas para acomodar la capacidad de escalado, los requisitos funcionales y de integración de los sistemas de seguridad complejos.

Se usan múltiples microprocesadores para procesar las E/S, la memoria y las comunicaciones de seguridad. Los circuitos de temporizador de control (watchdog) realizan análisis de diagnósticos. Este tipo de arquitectura se conoce como 1oo2D, debido a que cualquiera de los dos microprocesadores puede realizar la función de seguridad, y los diagnósticos extensos se realizan para asegurar que ambos microprocesadores estén operando de manera sincronizada.



Además, cada circuito de entrada se prueba internamente repetidas veces cada segundo para asegurar que funcione correctamente. Puede que solo pulse el dispositivo de paro de emergencia una vez al mes; pero cuando lo haga, el circuito interno se habrá probado de forma continua.

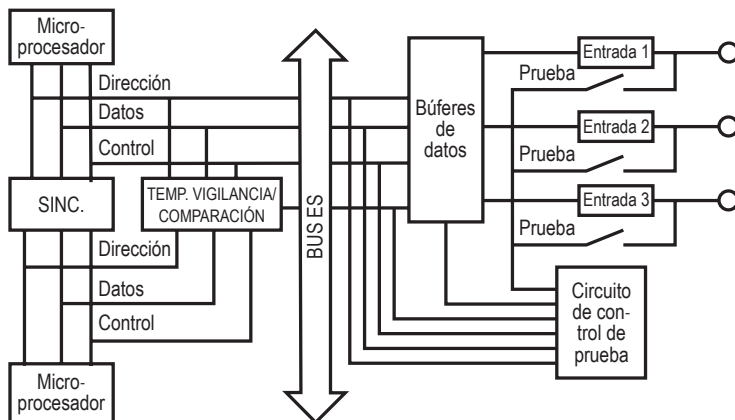


Diagrama de bloques del módulo de entrada de seguridad

Las salidas del PLC de seguridad son electromecánicas o de estado sólido con clasificación de seguridad. Al igual que los circuitos de entrada, los circuitos de salida se prueban múltiples veces cada segundo para asegurar que puedan desactivar la salida. Si uno de los tres falla, la salida es desactivada por los otros dos, y el fallo es reportado por el circuito de monitorización interno.

Cuando utilice dispositivos de seguridad con contactos mecánicos (dispositivos de paro de emergencia, interruptores de puerta, etc.), el usuario podrá aplicar señales de prueba de impulsos para detectar fallos cruzados.

Software

Los PLC de seguridad se programan de manera similar a los PLC estándar. Todos los diagnósticos adicionales y la verificación de errores mencionados anteriormente son realizados por el sistema operativo, por lo tanto, el programador no tiene conocimiento de lo que está sucediendo. La mayoría de los PLC de seguridad cuentan con instrucciones especiales para escribir el programa para el sistema de seguridad, y estas instrucciones tienden a simular la función de los relés de seguridad homólogos. Por ejemplo, la instrucción de paro de emergencia actúa en gran medida como un MSR. A pesar de que la lógica detrás de cada una de estas instrucciones es compleja, los programas de seguridad parecen relativamente sencillos porque el programador simplemente conecta estos bloques. Estas instrucciones, junto con otras instrucciones lógicas, matemáticas, de manipulación de datos, etc., cuentan con certificación de terceros para asegurar que su operación sea coherente con las normas vigentes.

Los bloques de funciones son métodos predominantes para las funciones de seguridad de programación. Además de los bloques de función y lógica de escalera, los PLC de seguridad también proporcionan instrucciones de aplicación de seguridad certificadas. Las instrucciones de seguridad certificadas proporcionan un comportamiento específico de la aplicación.

Implementación de las medidas protección

Hay bloques de funciones certificados disponibles para hacer interfaz con casi todos los dispositivos de seguridad. Una excepción a esta lista es el borde de seguridad que utiliza tecnología resistiva.

Los PLC de seguridad generan una “firma” que proporciona la capacidad de realizar el seguimiento de los cambios realizados. Esta firma generalmente es una combinación del programa, la configuración de entradas y salidas, y un sello de hora. Al finalizar y validar el programa, el usuario debe registrar esta firma como parte de los resultados de validación para referencia futura. Si el programa necesita modificación, es necesario revalidar y registrar una nueva firma. El programa también se puede bloquear con una contraseña para evitar cambios no autorizados.

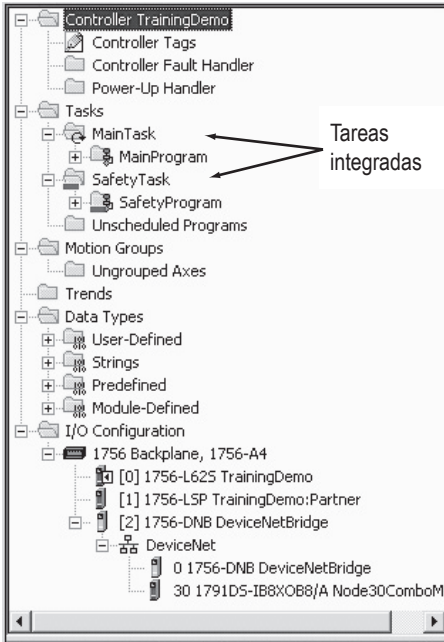
El cableado se simplifica con los programas lógicos, en comparación con los relés de control de seguridad. A diferencia del cableado que debe conectarse a terminales específicos en los relés de control de seguridad, los dispositivos de entrada se conectan a cualquier terminal de entrada de seguridad y los dispositivos de salida se conectan a cualquier terminal de salida de seguridad. Luego los terminales son asignados mediante el software.

Controladores de seguridad integrada

Las soluciones de control de seguridad ahora proporcionan integración completa dentro de una sola arquitectura de control, donde las funciones de seguridad y las funciones de control estándar residen y trabajan juntas. La posibilidad de ejecutar funciones secuenciales de alta velocidad, de movimiento, de accionamiento, de proceso, de lotes y de seguridad SIL 3 en un controlador ofrece ventajas considerables. La integración de los controles de seguridad y de control estándar ofrece la oportunidad de utilizar herramientas comunes y tecnologías que reducen los costes asociados con el diseño, la instalación, la puesta en servicio y el mantenimiento. La capacidad de utilizar hardware de control común, E/S de seguridad distribuidas o dispositivos en redes de seguridad y dispositivos de interfaz de hombre-máquina (HMI) comunes reducen los costes de adquisición y mantenimiento, así como también el tiempo de desarrollo. Todas estas características aumentan la productividad y la velocidad relacionada con la resolución de problemas, y reducen los costes de formación técnica gracias a la homogeneidad.

El siguiente diagrama muestra un ejemplo de la integración del control y la seguridad. Las funciones de control estándar no relacionadas con la seguridad residen en la tarea principal. Las funciones relacionadas con la seguridad residen en la tarea de seguridad.

Todas las funciones relacionadas al control estándar y con la seguridad están aisladas unas de otras. Por ejemplo, los tags de seguridad pueden ser leídos directamente por la lógica estándar. Los tags de seguridad se pueden intercambiar entre los controladores GuardLogix a través de EtherNet/IP, ControlNet o DeviceNet. Los datos de tags de seguridad pueden ser leídos directamente por dispositivos externos, interfaces de hombre-máquina (HMI), ordenadores personales (PC) y otros controladores.



1. La lógica y los tags estándar actúan del mismo modo que ControlLogix.
2. Datos de tag estándar, de programa o bajo el alcance del controlador y dispositivos externos, HMI, PC, otros controladores, etc.
3. Dado que es un controlador integrado, GuardLogix proporciona la capacidad de mover (asignar) datos de tag estándar a tags de seguridad para su uso dentro de la tarea de seguridad. De este modo se permite a los usuarios leer información de estado desde el lado estándar de GuardLogix. Estos datos no deben usarse para controlar directamente una salida de seguridad.
4. La lógica estándar puede leer directamente tags de seguridad.
5. La lógica de seguridad puede leer o escribir tags de seguridad.
6. Los tags de seguridad se pueden intercambiar entre los controladores GuardLogix a través de EtherNet/IP.
7. Los dispositivos externos, HMI, PC, otros controladores, etc., pueden leer datos de tags de seguridad, de programa o bajo el alcance del controlador. Tenga en cuenta que cuando estos datos se utilizan al margen de la tarea de seguridad, se consideran datos estándar, no datos de seguridad.

Implementación de las medidas protección

Redes de seguridad

Las redes de comunicación de la planta tradicionalmente han proporcionado a los fabricantes la capacidad de mejorar la flexibilidad, aumentar los diagnósticos, aumentar las distancias, reducir los costes de instalación y cableado, facilitar el mantenimiento y en general mejorar la productividad de sus operaciones de fabricación. Los mismos motivos han llevado a la implementación de redes de seguridad industrial. Estas redes de seguridad permiten a los fabricantes distribuir E/S de seguridad y dispositivos de seguridad alrededor de su maquinaria con un único cable de red para comunicaciones de ES estándar y de seguridad, reduciendo los costes de instalación al tiempo que se mejora el diagnóstico y se pueden utilizar sistemas de seguridad de mayor complejidad. También permiten comunicaciones seguras entre los PLC de seguridad/controladores y permiten a los usuarios distribuir su control de seguridad entre varios sistemas inteligentes.

Las redes de seguridad han sido diseñadas para detectar errores de transmisión e iniciar una función de reacción ante fallos adecuada. Los errores de comunicación que se detectan incluyen: inserción de mensajes, pérdida de mensajes, corrupción de mensajes, retardo de mensajes, repetición de mensajes y secuencia incorrecta de mensajes.

En la mayoría de las aplicaciones, cuando se detecta un error, el dispositivo pasa a un estado de desactivación conocido, normalmente denominado “estado de seguridad.” La entrada de seguridad o el módulo de comunicación de salida se encargan de detectar estos errores de comunicación y de pasar al estado de seguridad si es oportuno.

Las redes de seguridad de versiones anteriores estaban vinculadas a un tipo de medio físico o a un esquema de acceso a medio físico; por lo tanto, los fabricantes debían usar cables específicos, tarjetas de interfaz de red, encaminadores, puentes, etc., que también se convertían en parte de la función de seguridad. Estas redes estaban limitadas en el sentido que sólo aceptaban comunicación entre dispositivos de seguridad.

Esto significaba que los fabricantes tenían que usar dos o más redes para su estrategia de control de máquina (una red para el control estándar y otra para el sistema de control relacionado con la seguridad), lo cual aumentaba los costes de instalación, formación técnica y piezas de repuesto.

Las redes de seguridad modernas permiten que un solo cable de red se comunique con los dispositivos de control de seguridad y estándar. El protocolo CIP Safety (protocolo industrial común) es un protocolo estándar abierto publicado por ODVA (Asociación de proveedores de Open DeviceNet) que permite comunicaciones de seguridad entre dispositivos de seguridad en las redes DeviceNet, ControlNet y EtherNet/IP. Puesto que CIP Safety es una extensión del protocolo CIP estándar, los dispositivos de seguridad y los dispositivos estándar pueden residir en la misma red. Los usuarios también pueden hacer conexión en puente entre redes que contienen dispositivos de seguridad, lo cual les permite subdividir los dispositivos de seguridad para realizar ajustes finos en los tiempos de respuesta de seguridad, o simplemente facilitar la distribución de



los dispositivos de seguridad. Puesto que el protocolo de seguridad es únicamente responsabilidad de los dispositivos finales (PLC de seguridad/controlador, módulo de E/S de seguridad, componente de seguridad), se usan cables estándar, tarjetas de interfaz de red, encaminadores y puentes, lo cual elimina accesorios especiales de conexión en red y permite apartar estos dispositivos de la función de seguridad.

Dispositivos de salida

Relés de control de seguridad y contactores de seguridad

Los contactores y los relés de control se utilizan para desconectar la alimentación eléctrica del accionador. Se añaden características especiales a los contactores y relés de control para permitir su uso con fines de seguridad.

Los contactos auxiliares mecánicamente vinculados se utilizan para comunicar el estado de los contactores y relés de control a un dispositivo lógico de control. El uso de contactos unidos mecánicamente ayuda a asegurar la función de seguridad. Para cumplir con los requisitos de los contactos mecánicamente unidos, los contactos normalmente cerrados y normalmente abiertos no pueden estar simultáneamente en el estado cerrado. La normativa IEC 60947-4-1 define los requisitos para los contactos mecánicamente unidos. Si los contactos normalmente abiertos se soldaran, los contactos normalmente cerrados se abrirían por lo menos 0,5 mm. Por el contrario, si los contactos normalmente cerrados se soldaran, entonces los contactos normalmente abiertos permanecerían abiertos.

Los sistemas de seguridad sólo deben arrancar en lugares específicos. Los relés de control y los contactores estándar permiten que se actúe manualmente sobre el contactor. En los dispositivos de seguridad no se puede actuar manualmente ya que están protegidos.

En los relés de control de seguridad, el contacto normalmente cerrado es accionado por el vínculo mecánico principal. Los contactores de seguridad utilizan un módulo aditivo de contactos para ubicar los contactos mecánicamente unidos. Si el bloque de contactos se cayera de la base, los contactos mecánicamente unidos permanecerían cerrados. Los contactos mecánicamente unidos están permanentemente adheridos al relé de control de seguridad o al contactor de seguridad. En los contactores de mayor tamaño, un módulo aditivo de contactos es insuficiente para reflejar con precisión el estado del vínculo mecánico más ancho. Se utilizan contactos de espejo que se ubican a cada lado del contactor.

El tiempo de desconexión de los relés de control o contactores desempeña un papel en el cálculo de la distancia de seguridad. A menudo se coloca un supresor de sobretensión en la bobina para aumentar la vida útil de los contactos que accionan la bobina. En el caso de las bobinas alimentadas con CA, el tiempo de desconexión no se ve afectado. En el caso de las bobinas alimentadas con CC, el tiempo de desconexión aumenta. El aumento depende del tipo de supresión seleccionado.

Implementación de las medidas protección

Los contactores y relés de control se han diseñado para conmutar cargas importantes de entre 0,5 A y más de 100 A. El sistema de seguridad opera con baja corriente. La señal de respuesta generada por el dispositivo lógico del sistema de seguridad puede oscilar entre unos miliamperios y decenas de miliamperios, normalmente a 24 VCC. Los relés de control de seguridad y los contactores de seguridad usan contactos bifurcados con recubrimiento de oro para conmutar de manera fiable esta baja corriente.

Protección contra sobrecarga

Las normas eléctricas requieren protección contra sobrecarga de motores. Los diagnósticos provistos por el dispositivo de protección contra sobrecarga mejoran no sólo la seguridad del equipo sino también la seguridad del operador. Las tecnologías disponibles hoy en día pueden detectar condiciones de fallo como sobrecarga, pérdida de fase, fallo de tierra, bloqueo, atasco, baja carga, desequilibrio de corriente y sobretensión. La detección y comunicación de condiciones anómalas antes de la activación ayuda a incrementar el tiempo de producción y a evitar condiciones peligrosas imprevistas para los operadores y trabajadores de mantenimiento

Variadores y servos

Los variadores y servos con clasificación de seguridad pueden usarse para evitar el riesgo de movimiento mecánico al ejecutar paradas de seguridad, así como paradas de emergencia.

Los variadores de CA logran la clasificación de seguridad con canales redundantes para desconectar la alimentación eléctrica al circuito de control de la compuerta. La lógica externa o integral, en función del tipo de variador, controla los canales redundantes. Este enfoque redundante permite que el variador de seguridad se aplique en circuitos de parada de emergencia sin necesidad de un contactor.

El servo logra un resultado en cierto modo similar al de los variadores de CA que emplean señales de seguridad redundantes para ejecutar la función de seguridad "desconexión de par segura".

Sistemas de conexión

Los sistemas de conexión añaden valor al reducir los costes de instalación y de mantenimiento de los sistemas de seguridad. Los diseños deben tener en cuenta aspectos tales como un solo canal, doble canal, doble canal con indicación y múltiples tipos de dispositivos.

Cuando se necesita una conexión en serie de enclavamientos de doble canal, un bloque de distribución puede simplificar la instalación. Con la clasificación IP67, estos tipos de cajas pueden montarse en la máquina en lugares remotos. Cuando se requiere un conjunto diverso de dispositivos puede usarse una caja ArmorBlock Guard I/O. Las entradas pueden ser configuradas mediante software para aceptar varios tipos de dispositivos.



Capítulo 5: Cálculo de la distancia de seguridad

Las piezas peligrosas deben estar en un estado de seguridad antes de que el operador entre en contacto con ellas. Para el cálculo de la distancia de seguridad, existen dos grupos de normas. En este capítulo, estas normas se agrupan de la siguiente manera:

ISO EN: (EN ISO 13855)

US CAN (ANSI B11.19, ANSI RIA R15.06 y CAN/CSA Z434-03)

Fórmula

La distancia de seguridad mínima depende del tiempo requerido para procesar el comando de parada y cuánto puede penetrar el operador en la zona de detección antes de ser detectado. La fórmula usada en todo el mundo tiene el mismo formato y los mismos requisitos. Las diferencias son los símbolos usados para representar las variables y las unidades de medición.

Las fórmulas son:

ISO EN: $S = K \times T + C$

US CAN: $D_s = K \times (T_s + T_c + T_r + T_{bm}) + D_{pf}$

Donde: D_s y S son la distancia segura mínima de la zona de peligro hasta el punto de detección más cercano

Direcciones de aproximación

Al calcular la distancia de seguridad cuando se utilizan barreras optoelectrónicas o un escáner de zona, es preciso tener en cuenta el ángulo de enfoque al dispositivo de detección. Se consideran tres tipos de aproximación:

Normal – aproximación perpendicular al plano de detección

Horizontal – aproximación paralela al plano de detección

En ángulo – aproximación en ángulo a la zona de detección.

Constante de velocidad

K es una constante de velocidad. El valor de la constante de velocidad depende de los movimientos del operador (por ej., velocidad de las manos, velocidad al caminar y longitud del paso al caminar). Este parámetro se basa en datos de investigación que muestran que es razonable suponer una velocidad de las manos de 1600 mm/seg (63 pulg./s) de un operador mientras el cuerpo está estacionario. Deben tenerse en cuenta las circunstancias de la aplicación real. Como guía general, la velocidad

Cálculo de la distancia de seguridad

de aproximación varía de 1600 mm/s (63 pulg./s) a 2500 mm/seg (100 pulg./s). La constante de velocidad apropiada debe ser determinada por la evaluación de riesgos.

Tiempo de parada

T representa el tiempo de parada general del sistema. El tiempo total en segundos comienza a partir del inicio de la señal de parada hasta el momento en que deja de haber peligro. Este tiempo puede desglosarse en sus partes incrementales (Ts, Tc, Tr y Tbm) para facilitar el análisis. Ts es el tiempo de parada de la máquina/equipo en el peor de los casos. Tc es el tiempo de parada del sistema de control en el peor de los casos. Tr representa el tiempo de respuesta del dispositivo de protección, incluso su interfaz. Tbm representa el tiempo de parada adicional permitido por el monitor de freno antes de que detecte deterioro del tiempo de parada más allá de los límites predeterminados por los usuarios finales. Tbm se usa para prensas mecánicas con revolución parcial. Ts + Tc + Tr generalmente son medidos por un dispositivo de medición de tiempo de parada si los valores son desconocidos.

Factores de penetración de profundidad

Los factores de penetración de profundidad son representados por los símbolos C y Dpf. Es el máximo recorrido hacia el peligro antes de la detección por parte del dispositivo de protección. Los factores de penetración de profundidad cambian según el tipo de dispositivo y de aplicación. Compruebe la norma correspondiente para determinar el mejor factor de penetración de profundidad posible. En el caso de aproximación normal a una barrera optoelectrónica o escáner de área cuya sensibilidad objeto sea menor a 64 mm (2,5 pulg.), las normas ANSI y IAs canadienses usan:

$Dpf = 3,4 \times (\text{sensibilidad objeto} - 6,875 \text{ mm})$, pero no menos de cero.

En el caso de aproximación normal a una barrera optoelectrónica o escáner de área cuya sensibilidad objeto sea menor a 40 mm (1,57 pulg.), las normas ISO y EN usan:

$C = 8 \times (\text{sensibilidad objeto} - 14 \text{ mm})$, pero no menos de 0.

Estas dos fórmulas tienen un punto de cruce a 19,3 mm. En el caso de sensibilidades de objeto menores a 19 mm, la aproximación US CAN es más restrictiva, puesto que la barrera optoelectrónica o el escáner de área debe colocarse más alejado del peligro. En el caso de sensibilidades de objetos de más de 19,3 mm, la norma ISO EN es más restrictiva. Los constructores de máquinas que deseen construir una máquina para uso en todo el mundo, deben usar las condiciones en el peor de los casos de ambas ecuaciones.

Aplicaciones de aproximación horizontal

Cuando se usan sensibilidades de objetos más grandes, las normas US CAN e ISO EN difieren ligeramente en el factor de penetración de profundidad y en la sensibilidad del objeto. El valor de ISO EN es 850 mm, donde el valor de US CAN es 900 mm. Las normas también difieren en la sensibilidad del objeto.



Aplicaciones de aproximación vertical

Ambas normas concuerdan en que la altura mínima del haz más bajo debe ser 300 mm, pero difieren con respecto a la altura mínima del haz más alto. ISO EN establece 900 mm, mientras que US CAN establece 1200 mm. El valor para el haz más alto parece ser irrelevante. Al considerar una aplicación de alcance a través, la altura del haz más alto tiene que ser mucho más alta para adaptarse a un operador de pie. Si el operador puede alcanzar por arriba del plano de detección, entonces se aplican los criterios de alcanzar por arriba.

Uno o varios haces

Los haces individuales o múltiples son definidos en más detalle por las normas ISO EN. Las siguientes figuras muestran las alturas “prácticas” de múltiples haces arriba del suelo. La penetración de profundidad es 850 mm en la mayoría de los casos y 1200 mm para el uso de haz individual. En comparación, la aproximación US CAN toma esto en consideración mediante los requisitos de alcanzar al otro lado. Siempre debe tenerse en consideración si es necesario pasar por encima, por debajo o alrededor de uno o múltiples haces.

# Haces	Altura por encima del suelo – mm (in)	C – mm (in)
1	750 (29,5)	1200 (47,2)
2	400 (5,7), 900 (35,4)	850 (33,4)
3	300 (11,8), 700 (27,5), 1100 (43,3)	850 (33,4)
4	300 (11,8), 600 (23,6), 900 (35,4), 1200 (47,2)	850 (33,4)

Cálculos de distancia

En el caso de aproximación normal a las barreras optoelectrónicas, el cálculo de la distancia de seguridad para ISO EN y US CAN es parecido, pero existen diferencias. Para la aproximación normal a las barreras optoelectrónicas verticales en las que la sensibilidad del objeto es como máximo 40 mm, el enfoque ISO EN requiere dos pasos. Primero, calcular S usando 2000 como la constante de velocidad.

$$S = 2000 \times T + 8 \times (d - 14)$$

La distancia mínima a la que puede estar S es 100 mm.

Un segundo paso puede usarse cuando la distancia es mayor que 500 mm. Entonces, el valor de K puede reducirse a 1600. Cuando se usa K = 1600, el valor mínimo de S es 500 mm.

La aproximación de US CAN utiliza un método de un paso: $D_s = 1600 \times T * D_{pf}$

Esto da lugar a diferencias superiores al 5% entre las normas cuando el tiempo de respuesta es inferior a 560 ms.

Cálculo de la distancia de seguridad

Aproximaciones en ángulo

La mayoría de las aplicaciones de barreras optoelectrónicas y escáneres se instalan en plano vertical (aproximación normal) u horizontal (aproximación en paralelo). Estas instalaciones nos son consideradas angulares si están dentro de $\pm 5^\circ$ del diseño propuesto. Cuando el ángulo excede $\pm 5^\circ$, deben tenerse en cuenta los riesgos potenciales (por ej., distancias más cortas) de aproximaciones previstas. En general, los ángulos por encima de 30° con respecto al plano de referencia (por ejemplo, suelo) deberían considerarse normales y aquellos por debajo de 30° deberían considerarse paralelos.

Tapetes de seguridad

Con los tapetes de seguridad, la distancia de seguridad debe tener en cuenta el ritmo de los pasos y la zancada de los operadores. Suponiendo que el operador está caminando y los tapetes de seguridad están instalados sobre el suelo. El primer paso del operador sobre el tapete es un factor de penetración de profundidad de 1200 mm o 48 in. Si el operador debe subir a una plataforma, el factor de penetración de profundidad se puede reducir en un factor del 40% de la altura del escalón. Es importante fijar el tapete o tapetes firmemente para impedir que se muevan.

Ejemplo

Ejemplo: Un operador utiliza una aproximación normal a una barrera optoelectrónica de 14 mm, conectada a un relé de control de seguridad conectado a un contactor alimentado con CC con un supresor de diodo. El tiempo de respuesta del sistema de seguridad, T_r , es $20 + 15 + 95 = 130$ ms. El tiempo de parada de la máquina, $T_s + T_c$, es 170 ms. No se usa monitor de freno. El valor D_{pf} es 1 pulgada y el valor C es cero. El cálculo sería como se indica a continuación:

$$D_{pf} = 3,4 (14 - 6,875) = 1 \text{ in (24,2 mm)} \quad C = 8 (14-14) = 0$$

$$\begin{aligned} D_s &= K \times (T_s + T_c + T_r + T_{bm}) + D_{pf} & S &= K \times T + C \\ D_s &= 63 \times (0,17 + 0,13 + 0) + 1 & S &= 1600 \times (0,3) + 0 \\ D_s &= 63 \times (0,3) + 1 & S &= 480 \text{ mm (18,9 pulg.)} \\ D_s &= 18,9 + 1 \\ D_s &= 19,9 \text{ pulg. (505 mm)} \end{aligned}$$

Por lo tanto, si se trata de un equipo que se va a utilizar en cualquier parte del mundo, la barrera óptica debe instalarse a una distancia de seguridad mínima de 20 pulgadas o 508 mm del peligro.



Capítulo 6: Sistemas de control relativos con la seguridad

Introducción

¿Qué es un sistema de control de seguridad (con frecuencia abreviado SRCS)? Es la parte del sistema de control relativa con la seguridad de una máquina que evita que se presente una condición peligrosa. Puede ser un sistema dedicado independiente o puede estar integrado al sistema de control normal de la máquina.

Su complejidad puede variar desde un sistema simple, como un interruptor de enclavamiento de puerta de resguardo y un interruptor de parada de emergencia conectados en serie, a una bobina de control de un contactor de alimentación eléctrica, y hasta un sistema complejo con dispositivos simples y complejos que se comunican a través de software y hardware.

Los sistemas de control relativos con la seguridad están diseñados para realizar funciones de seguridad. Los sistemas de control relativos con la seguridad (SRCS) deben continuar funcionando correctamente en todas las condiciones previsibles. Por lo tanto ¿qué es una función de seguridad?; ¿cómo diseñamos un sistema que logre seguridad?, y cuando lo hayamos hecho, ¿cómo lo demostramos?

Función de seguridad

Los componentes del sistema de control de la máquina relacionados con la seguridad implementan una función de seguridad para mantener el equipo bajo control en un estado de seguridad con respecto a un peligro específico o un conjunto de estos. Un fallo de la función de seguridad puede resultar en el aumento inmediato de los riesgos de usar el equipo, es decir, una condición peligrosa.

Una “situación peligrosa” se da cuando una persona puede verse expuesta a un riesgo. Una condición peligrosa no implica que la persona sufra daño. La persona expuesta puede tener capacidad de reconocer el peligro y evitar ser lesionada. La persona expuesta podría no ser capaz de reconocer el peligro, o el peligro puede ser causado por un arranque inesperado. La tarea principal del diseñador del sistema de seguridad es evitar condiciones peligrosas y los arranques inesperados.

La función de seguridad a menudo puede describirse con requisitos de múltiples partes. Por ejemplo, la función de seguridad iniciada por un resguardo de enclavamiento tiene tres partes:

1. Los peligros protegidos por el resguardo no podrán funcionar hasta que este esté cerrado.
2. La apertura del resguardo hará que el peligro se detenga si está activo en el momento de la apertura.
3. Y el cierre del resguardo no reiniciará el peligro que proteja.

Sistemas de control relacionados con la seguridad y seguridad funcional

Al establecer la función de seguridad para una aplicación específica, la frase “punto peligroso” debe cambiarse al nombre del punto peligroso específico. El origen del peligro no debe confundirse con los resultados de este. La trituration, los cortes y las quemaduras son resultados de un peligro. Algunos ejemplos de origen de un peligro incluyen motores, arietes, cuchillos, antorchas, bombas, láser, robots, efectores terminales, solenoides, válvulas, otros tipos de accionadores o riesgos mecánicos que impliquen los efectos de la gravedad.

Al tratar los sistemas de seguridad se utiliza la frase “al imponer o antes de que se imponga una demanda sobre una función de seguridad”. ¿Qué es una demanda impuesta sobre una función de seguridad? Algunos ejemplos de demanda impuesta sobre una función de seguridad incluyen la apertura de un resguardo enclavado, la ruptura de una barrera optoelectrónica, una pisada sobre un tapete de seguridad o la presión de un paro de emergencia. Un operador demanda que se detenga el punto peligroso o que permanezca desenergizado si ya está detenido.

Las partes relacionadas con la seguridad del sistema de control de la máquina ejecutan la función de seguridad. La función de seguridad no es ejecutada por un solo dispositivo, por ejemplo solamente el resguardo. El enclavamiento del resguardo envía un comando a un dispositivo lógico el cual, a su vez, inhabilita un accionador. La función de seguridad se inicia con el comando y termina con la implementación.

El sistema de seguridad debe diseñarse con un nivel de integridad acorde con los riesgos de la máquina. Los riesgos más altos requieren niveles de integridad mayores para asegurar el rendimiento de la función de seguridad. Los sistemas de seguridad de máquinas se pueden clasificar en niveles de rendimiento según su capacidad para garantizar la acción de su función de seguridad o, dicho de otro modo, su nivel de integridad de seguridad funcional.

Seguridad funcional de sistemas de control

¿Qué es la seguridad funcional?

La seguridad funcional forma parte del requisito de seguridad global y depende del correcto funcionamiento del proceso o equipo como respuesta a sus entradas. La IEC TR 61508-0 proporciona el siguiente ejemplo para ayudar a aclarar el significado de la seguridad funcional. “Por ejemplo, un dispositivo de protección frente a un exceso de temperatura que emplee un detector térmico en los bobinados de un motor eléctrico para desactivar el motor antes de que se sobrecaliente es un ejemplo de seguridad funcional. Sin embargo, proporcionar aislamiento especial para resistir altas temperaturas no es un ejemplo de seguridad funcional (aunque es un ejemplo de seguridad y podría proteger precisamente contra el mismo peligro).”

Como otro ejemplo comparemos una protección basada en hardware con un resguardo con enclavamiento. El resguardo basado en hardware no se considera “seguridad funcional” aunque puede proteger contra el acceso al mismo punto peligroso que una puerta con enclavamiento. La puerta con enclavamiento es un ejemplo de seguridad



funcional. Si se abre el resguardo, el enclavamiento actúa como “entrada” para un sistema que alcanza un estado de seguridad. De manera similar se utiliza equipo de protección personal (PPE) como medida de protección para ayudar a aumentar la seguridad del personal. El equipo de protección personal no se considera seguridad funcional.

La seguridad funcional es un término que se introdujo en IEC 61508:1998. Desde entonces, en ocasiones el término se ha asociado únicamente a sistemas de seguridad programables. Esto es un concepto erróneo. La seguridad funcional cubre una amplia gama de dispositivos usados para crear sistemas de seguridad. Dispositivos tales como enclavamientos, barreras optoelectrónicas, relés de seguridad, PLC de seguridad, contactores de seguridad y variadores de seguridad se interconectan para formar un sistema de seguridad, el cual realiza una función específica relacionada con la seguridad. Esto es seguridad funcional.

Por lo tanto, la seguridad funcional de un sistema de control eléctrico es muy importante para el control de peligros que surgen de las piezas en movimiento de la maquinaria.

Se necesita dos tipos de requisitos para lograr seguridad funcional:

- La función de seguridad.
- La integridad de seguridad.

La evaluación de riesgos desempeña un papel clave en el desarrollo de los requisitos de seguridad funcional. El análisis de peligros y tareas lleva a los requisitos funcionales de seguridad (es decir, la función de seguridad). La cuantificación de riesgos produce los requisitos de integridad de seguridad (por ejemplo, la integridad de seguridad o el nivel de rendimiento).

Cuatro normas de seguridad funcional importantes para sistema de control para maquinaria son:

1. IEC/EN 61508 “Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad”

Esta norma contiene los requisitos y las disposiciones aplicables al diseño de complejos sistemas y subsistemas electrónicos y programables. La norma es genérica; por lo tanto, no está restringida al sector de máquinas.

2. IEC/EN 62061 “Seguridad de maquinaria – Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad”

Esta norma es la implementación específica para maquinarias de IEC/EN 61508. Proporciona requisitos aplicables al diseño de nivel del sistema de todos los tipos de seguridad de maquinaria relacionada con sistemas de control eléctricos y también al diseño de subsistemas o dispositivos no complejos. Requiere que los subsistemas programables o complejos satisfagan los requisitos de la norma IEC/EN 61508

Sistemas de control relacionados con la seguridad y seguridad funcional

3. (EN) ISO 13849-1 “Seguridad de maquinaria – Componentes de los sistemas de control relacionados con la seguridad”

Esta norma está destinada a proporcionar una ruta de transición directa desde las categorías de la norma anterior EN 954-1.

4. IEC 61511 “Seguridad funcional – Sistemas de seguridad instrumentados para el sector de la industria de procesos”

Esta norma constituye la implementación de IEC/EN 61508 específica para el sector de procesos

Las normas de seguridad funcional representan un paso importante más allá de los requisitos existentes conocidos, tales como control fiable y sistemas de categorías ISO 13849-1:1999 (EN 954-1:1996) previas.

Las categorías no han desaparecido por completo; todavía se utilizan en la actual (EN) ISO 13849-1.

IEC/EN 62061 y (EN) ISO 13849-1

IEC/EN 62061 y (EN) ISO 13849-1 cubren los sistemas de control eléctricos relacionados con la seguridad. Es posible que finalmente se combinen en una sola norma con terminología común. Ambas normas producen los mismos resultados pero emplean métodos diferentes. Su propósito es proporcionar a los usuarios una opción para seleccionar el más idóneo para su situación. Un usuario puede decidir usar cualquiera de las normas, y ambas están armonizadas bajo la Directiva Europea de Maquinarias. Los resultados de las dos normas proporcionan niveles de prestaciones de seguridad o integridad comparables. Las metodologías de cada norma tienen diferencias apropiadas para usuarios específicos.

La metodología descrita en IEC/EN 62061 tiene el propósito de permitir funcionalidad de seguridad compleja que puede ser implementada por arquitecturas de sistemas que antes eran no convencionales. La metodología de (EN) ISO 13849-1 tiene como objetivo proporcionar una vía más directa y menos complicada para la funcionalidad de seguridad más convencional implementada por arquitecturas de sistemas convencionales.

Una distinción importante entre estas dos normas es la aplicabilidad a varias tecnologías. IEC/EN 62061 es más adecuada para los sistemas eléctricos. (EN) ISO 13849-1 se puede aplicar a los sistemas neumáticos, hidráulicos, mecánicos y eléctricos.

Informe técnico conjunto sobre IEC/EN 62061 y (EN) ISO 13849-1

Se ha preparado un informe conjunto sobre las normas IEC y ISO para ayudar a los usuarios de ambas normas.



Explica la relación entre las dos normas y explica cómo se puede extraer la equivalencia entre PL (nivel de rendimiento) de (EN) ISO 13849-1 y SIL (nivel de integridad de seguridad) de IEC/EN 62061 en los sistemas y subsistemas.

Para mostrar que ambas normas dan resultados equivalentes, el informe muestra un ejemplo de sistema de seguridad calculado según las metodologías de ambas normas. El informe también aclara una serie de aspectos que han sido objeto de varias interpretaciones. Quizás uno de los aspectos más importantes es el de exclusión de fallo.

En general, si se requiere un nivel de rendimiento e para que un sistema de control relacionado con la seguridad implemente una función de seguridad, no es normal recurrir únicamente a exclusiones de fallos para lograr dicho nivel de rendimiento. Esto depende de la tecnología utilizada y del entorno de funcionamiento previsto. Por lo tanto, es esencial que el diseñador tenga especial cuidado con el uso de las exclusiones de fallos a medida que aumenta el requisito de PL.

En general, el uso de las exclusiones de fallos no se puede aplicar a los aspectos mecánicos de los interruptores de posición electromecánicos para lograr un nivel de rendimiento e en el diseño de un sistema de control relacionado con la seguridad. Esas exclusiones de fallos que se pueden aplicar a condiciones de fallo mecánico concretas (por ejemplo, desgaste/corrosión, fractura) se describen en la Tabla A.4 de ISO 13849-2.

Por ejemplo, un sistema de enclavamiento de puerta que tiene que lograr un nivel de rendimiento e deberá incorporar una tolerancia de fallo mínima de 1 (por ejemplo, dos interruptores de posición mecánicos convencionales) para poder llegar a él, ya que normalmente no es justificable excluir fallos tales como accionadores de interruptor averiados. No obstante, puede que sea aceptable excluir fallos, como cortocircuitos del cableado dentro de un panel de control diseñado de conformidad con las normas relevantes.

SIL e IEC/EN 62061

IEC/EN 62061 describe tanto la magnitud de riesgo que debe reducirse como la capacidad del sistema de control de reducir dicho riesgo en términos de SIL (nivel de integridad de seguridad). Existen tres SIL que se emplean en el sector de la maquinaria, siendo el SIL 1 es el más bajo y el SIL 3 el más alto.

Puesto que el término SIL se aplica de la misma manera en otros sectores industriales, tales como productos petroquímicos, generación de energía y ferrocarriles, IEC/EN 62061 es muy útil cuando la maquinaria se usa dentro de dichos sectores. En otros sectores, como la industria de procesos, pueden producirse riesgos de mayor magnitud, por lo que IEC 61508 y la norma IEC 61511 específica para el sector de procesos incluyen SIL 4.

Sistemas de control relacionados con la seguridad y seguridad funcional

El SIL se aplica a una función de seguridad. Los subsistemas que conforman el sistema que implementa la función de seguridad deben tener la capacidad SIL apropiada. Esto algunas veces se conoce como límite de declaración de SIL (SIL CL). Se requiere un estudio completo y detallado de IEC/EN 62061 para poder aplicarlo correctamente.

PL y (EN) ISO 13849-1

(EN) ISO 13849-1 no utiliza el término SIL; en su lugar, habla de PL (nivel de rendimiento). En muchos aspectos PL puede relacionarse con SIL. Existen cinco niveles de rendimiento, PLa es el más bajo y PLe es el más alto.

Comparación de PL y SIL

Esta tabla muestra la relación aproximada entre PL y SIL cuando se aplica a estructuras de circuitos típicos.

PL (Nivel de rendimiento)	PFH _D (Probabilidad de fallos peligrosos por hora)	SIL (Nivel de integridad de seguridad)
a	$\geq 10^{-5}$ a $< 10^{-4}$	Ninguno
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$	1
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $< 10^{-6}$	2
e	$\geq 10^{-8}$ a $< 10^{-7}$	3

Correspondencia aproximada entre PL y SIL

IMPORTANTE: La tabla anterior se proporciona como orientación general y NO debe usarse para fines de conversión. Deben referenciarse los requisitos totales de las normas. Las tablas del Anexo K contienen información más detallada.



Capítulo 7: Diseño del sistema según (EN) ISO 13849

Se necesita un estudio completo y detallado de (EN) ISO 13849-1 antes de poder aplicarla correctamente. La siguiente es una descripción general breve:

Esta norma proporciona requisitos para el diseño y la integración de las piezas relacionadas con la seguridad de los sistemas de control e incluye algunos aspectos de software. La norma aplica a un sistema relacionado con la seguridad, pero también puede ser aplicada a las piezas que componen el sistema.

Herramienta de cálculo PL del software SISTEMA

SISTEMA es una herramienta de software para la implementación de (EN) ISO 13849-1. Su uso simplifica en gran medida los aspectos de cuantificación y cálculo de la implementación de la norma.

SISTEMA son las siglas de “Safety Integrity Software Tool for the Evaluation of Machine Applications” (herramienta de software de integridad de la seguridad para la evaluación de aplicaciones de máquinas) y el IFA la revisa y actualiza con regularidad. Requiere la introducción de varios tipos de datos de seguridad funcional, como se describe posteriormente en esta sección. Los datos se pueden introducir manual o automáticamente mediante la biblioteca de datos SISTEMA del fabricante.

La biblioteca de datos SISTEMA de Rockwell Automation está disponible para descarga, junto con un vínculo al sitio de descarga de SISTEMA, en:
www.rockwellautomation.com, en Solutions & Services > Safety Solutions.

Descripción general de (EN) ISO 13849-1

La descripción general que se incluye a continuación tiene como objetivo ofrecer una visión global de las disposiciones básicas de (EN) ISO 13849-1. También incluye alguna mención a su revisión, publicada a principios de 2106. Es esencial estudiar la propia norma en detalle.

Esta norma tiene una amplia aplicabilidad, ya que puede aplicarse a todas las tecnologías, incluidas eléctrica, hidráulica, neumática y mecánica. A pesar de que ISO 13849-1 se puede aplicar a sistemas complejos, también remite al lector a IEC 61508 para los componentes integrados de software complejos.

Los resultados de ISO 13849-1 son niveles de rendimiento [PL a, b, c, d o e]. El concepto de categoría original se mantiene, pero existen requisitos adicionales que deben cumplirse antes de poder declarar un PL en un sistema.

Los requisitos pueden enumerarse de manera básica de la siguiente forma:

- Arquitectura del sistema. Básicamente refleja las categorías a las que nos hemos acostumbrado

Diseño del sistema conforme con (EN) ISO 13849

- Se requiere fiabilidad de información para las partes que constituyen el sistema
- Se requiere cobertura de diagnóstico [DC] del sistema. Representa la eficacia de la supervisión de fallos en el sistema
- Protección contra fallo por causa común
- Protección contra fallos sistemáticos
- Requisitos específicos para el software cuando sea pertinente

Más adelante examinaremos con mayor detenimiento estos factores, pero antes será útil tener en cuenta la intención y el principio básicos de la norma en su totalidad. En este punto queda claro que existen consideraciones adicionales que hay que aprender, pero los detalles tendrán más sentido una vez que hayamos comprendido el objetivo de la norma y sus razones.

En primer lugar, ¿por qué necesitamos la norma? Es obvio que la tecnología utilizada en los sistemas de seguridad de la máquina ha progresado y cambiado de manera considerable a lo largo de los últimos diez años. Hasta hace relativamente poco, los sistemas de seguridad dependían de equipos simples con modos de fallo predecibles y previsibles. En la actualidad se utilizan cada vez más dispositivos electrónicos programables y complejos en los sistemas de seguridad. Esto nos ha dado ventajas en términos de costes, flexibilidad y compatibilidad, aunque también ha causado que las normas pre-existentes ya no sean adecuadas. Para poder saber si un sistema de seguridad es lo suficientemente bueno, necesitamos conocer más acerca de él. Por este motivo, las normas sobre seguridad funcional piden más información. Dado que, con la integración de subsistemas precalificados, los sistemas de seguridad emplean un enfoque más similar a una “caja negra”, dependemos en mayor medida de su conformidad con las normas. Por lo tanto esas normas necesitan ser capaces de interrogar adecuadamente la tecnología. Para ello, deben abordar los factores básicos de confiabilidad, detección de fallos e integridad arquitectónica y sistemática. Ese es el objetivo de (EN) ISO 13849-1.

Con el objeto de trazar un curso lógico a través de la norma es necesario considerar dos tipos de usuarios fundamentalmente diferentes: Los diseñadores de subsistemas relacionados con la seguridad, y los diseñadores de sistemas relacionados con la seguridad. En general, el diseñador del subsistema [normalmente un fabricante de componentes de seguridad] estará sujeto a un nivel de rigor superior. Debe proporcionar la información requerida para que el diseñador del sistema pueda asegurar que el subsistema tenga la integridad adecuada para el sistema. Esto normalmente requiere pruebas, análisis y cálculos. Los resultados se expresan en formato de datos requeridos por la norma.

El diseñador del sistema [normalmente un integrador o diseñador de máquinas] utilizará los datos del subsistema para efectuar algunos cálculos relativamente sencillos como parte del proceso de determinación del nivel de rendimiento [PL] global alcanzado por el sistema.



Determinación de la función de seguridad

Necesitamos decidir cuál es la función de seguridad. Es evidente que la función de seguridad deberá ser adecuada a la tarea requerida. ¿De qué manera nos ayuda la norma?

Es importante darse cuenta de que la funcionalidad requerida sólo puede determinarse considerando las características que prevalecen en la aplicación actual. Esto puede considerarse como la etapa de diseño del concepto de seguridad. No puede ser completamente cubierta por la norma porque la norma no conoce todas las características de una aplicación específica. Esto generalmente también se aplica al fabricante de máquinas que produce la máquina, pero que no necesariamente conoce las condiciones exactas de uso.

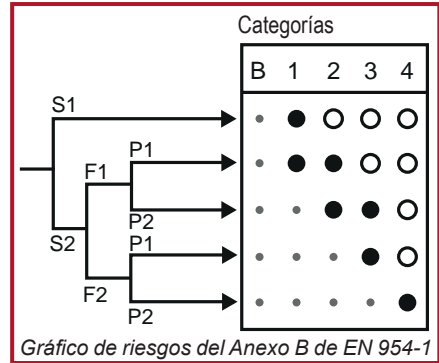
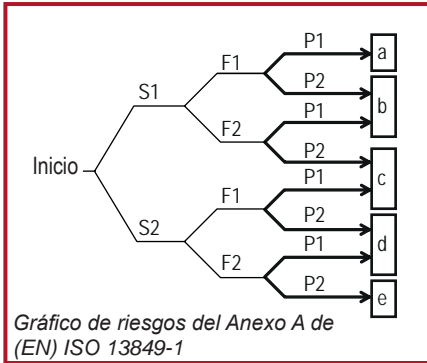
La norma ofrece ayuda con una larga lista de funciones de seguridad de uso común (por ejemplo, función de paro relacionada con la seguridad iniciada por la protección, función de silenciamiento, función de inicio/reinicio) y algunos de los requisitos normalmente asociados. Estudio de (EN) ISO 12100: "Principios de diseño básicos y evaluación del riesgo" se recomienda para su aplicación en esta etapa. ISO TR 22100-2 ofrece orientación práctica sobre la relación entre el proceso de evaluación del riesgo de la máquina de ISO 12100 y el proceso de asignación del nivel de rendimiento de (EN) ISO 13849-1. Existe un amplio conjunto de normas específicas para máquinas que recogen requisitos de funciones de seguridad para equipos concretos. Dentro de las normas EN europeas se denominan normas tipo C, y algunas de ellas tienen equivalentes exactos en las normas ISO. ISO TR 22100-1 proporciona información adicional sobre la relación entre las normas ISO 12100 y C.

Evidentemente la etapa de diseño del concepto de seguridad dependerá del tipo de máquina y también de las características de la aplicación y el entorno donde se utilice. El constructor de la máquina debe anticipar estos factores para poder diseñar un concepto de seguridad. Las condiciones previstas [es decir, anticipadas] de uso deben aparecer en el manual del usuario. El usuario de la máquina debe revisar que coincidan con las condiciones de uso reales.

El nivel de rendimiento r se emplea para indicar que la función de seguridad requiere el nivel de rendimiento en cuestión y este se determina durante la evaluación de riesgos. Para determinar el PLR, la norma proporciona un gráfico de riesgos dentro del cual se ingresan los factores de gravedad de lesión de la aplicación, la frecuencia de exposición y la posibilidad de evitarla.

La salida es el PLR. Los usuarios de la antigua EN 954-1 estarán familiarizados con este enfoque, pero tenga en cuenta que dentro de (EN) ISO 13849-1, la línea S1 ahora se subdivide mientras que el gráfico de riesgo antiguo no lo hacía. La versión de 2015 ofrece la posibilidad de reducir el rendimiento r un nivel en algunas circunstancias en función de la probabilidad de ocurrencia previsible.

Diseño del sistema conforme con (EN) ISO 13849



Por lo tanto, ahora disponemos de una descripción de la funcionalidad de seguridad y del nivel de rendimiento requerido [PLr] de los componentes del sistema de control relacionados con la seguridad [SRP/CS] que se utilizará para implementar esta funcionalidad. Ahora necesitamos diseñar el sistema y comprobar que cumpla el PLr.

Uno de los factores importantes para decidir qué norma aplicar [(EN) ISO 13849-1 o EN/IEC 62061] radica en la complejidad de la función de seguridad. En la mayoría de los casos, para la maquinaria, la función de seguridad será relativamente sencilla y (EN) ISO 13849-1 será la vía más adecuada. Información de fiabilidad, cobertura del diagnóstico [DC], [categoría] de la arquitectura del sistema, fallo por causa común y, donde sea pertinente, se utilizan requisitos para software para evaluar los PL.

Ésta es una descripción simplificada con el solo propósito de dar una descripción general. Es importante comprender que deben aplicarse todas las provisiones proporcionadas en el texto de la norma. Sin embargo, hay ayuda a la mano. La herramienta software SISTEMA está disponible para ayudar con los aspectos de cálculo y documentación. Ello también produce un expediente técnico.

SISTEMA se encuentra disponible en diferentes idiomas, incluido el alemán y el inglés. IFA, el desarrollador de SISTEMA, es una reputada institución del campo de la investigación y el ensayo con sede en Alemania. Está particularmente involucrada en la solución de problemas técnicos y científicos relacionados con la seguridad en el contexto de prevención y seguros contra accidentes estatutarios en Alemania. Trabaja en conjunto con agencias de seguridad y salud ocupacional en más de 20 países.

Los expertos del IFA, junto con sus colegas de BG, han desempañado un papel importante en la redacción de (EN) ISO 13849-1 e IEC/EN 62061.

La "biblioteca" de datos de componentes de seguridad de Rockwell Automation para uso con SISTEMA está disponible en: www.rockwellautomation.com, en *Solutions & Services > Safety Solutions*.

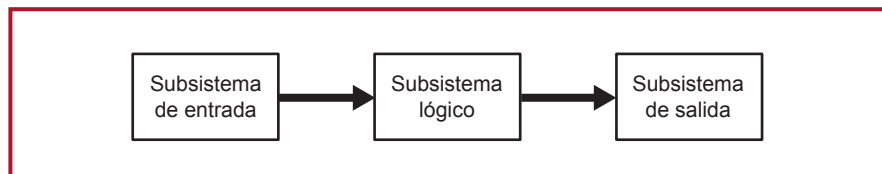


Sistemas de seguridad para maquinaria industrial

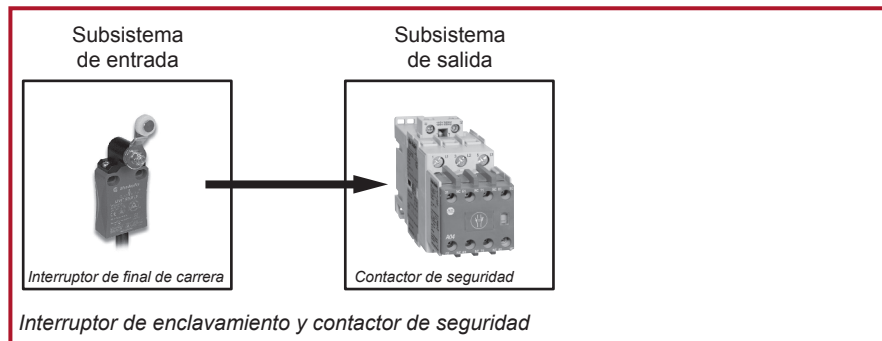
Con independencia del modo en el que se calcule el PL, es importante partir de la base adecuada. Necesitamos ver nuestro sistema de la misma manera que la norma; entonces empecemos con eso.

Estructura del sistema

Cualquier sistema puede ser dividido en componentes básicos del sistema o “subsistemas”. Cada subsistema tiene su propia función discreta. La mayoría de los sistemas pueden ser divididos en tres funciones básicas: entrada, solución lógica y actuación [algunos sistemas simples quizás no tengan solución lógica].

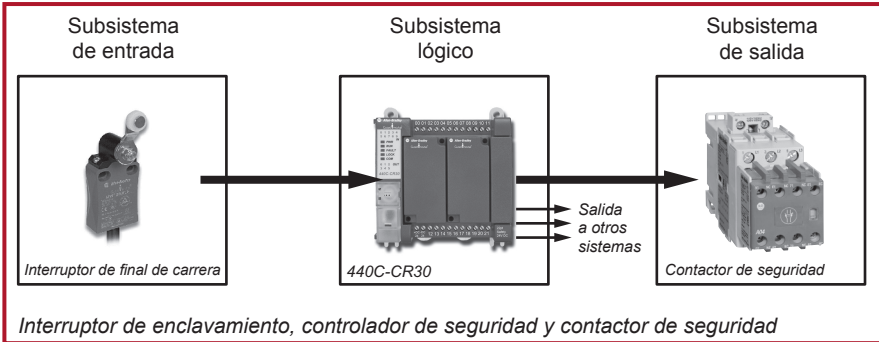


Los grupos de componentes que implementan estas funciones son los subsistemas.

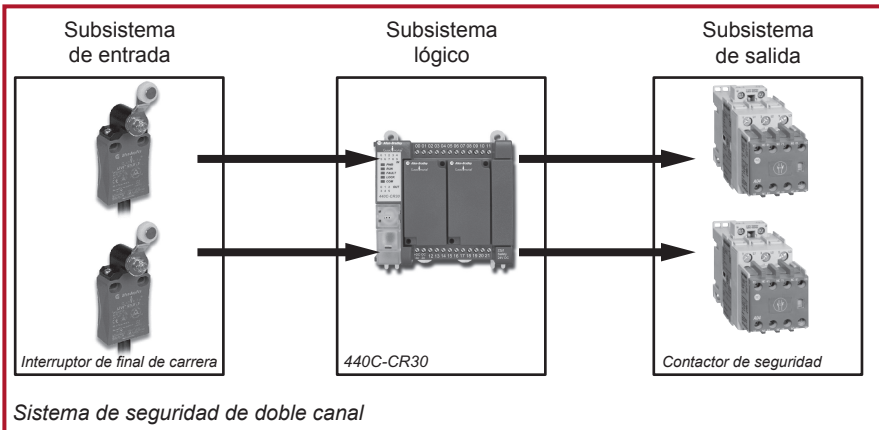


Arriba se muestra un ejemplo sencillo de sistema eléctrico de canal individual. Sólo comprende subsistemas de entrada y de salida.

Diseño del sistema conforme con (EN) ISO 13849



El sistema anteriormente mostrado es un poco más complejo porque también se necesita cierta lógica. El controlador de seguridad tendrá tolerancia a fallos (por ejemplo, doble canal) a escala interna, pero el sistema global seguirá limitado a un estado de canal individual como consecuencia del interruptor de final de carrera y los subsistemas de contactor individuales. Un sistema de canal individual fallará si falla uno de sus subsistemas de canal individual; no tendrá “tolerancia a fallos”.

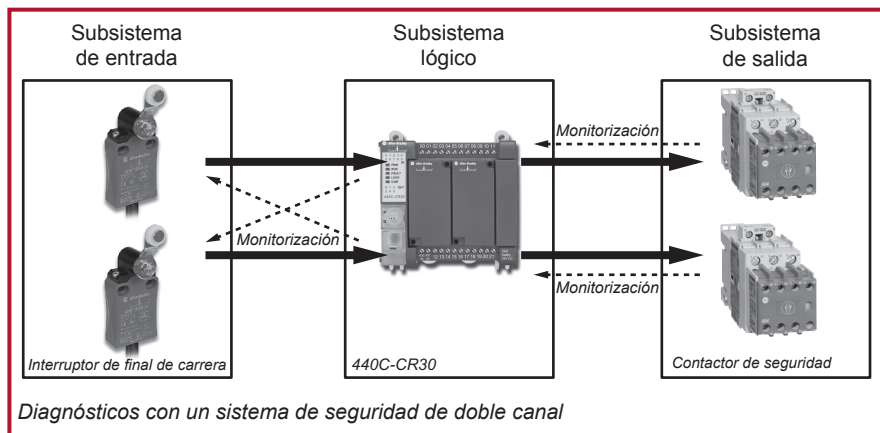


Arriba se muestra un sistema de doble canal [también denominado redundante o “con tolerancia a fallos”]. Cada subsistema cuenta con dos canales y puede tolerar un fallo individual sin perjuicio de la función de seguridad. Esta función de seguridad requeriría dos fallos, uno en cada canal antes del subsistema, para que el sistema fallara. Obviamente un sistema de doble canal tiene menos probabilidad de fallar y entrar en condición peligrosa que un sistema de canal individual. Pero podemos hacerlo aún más fiable [en términos de su función de seguridad] si incluimos medidas de diagnóstico para detección de fallos. Por supuesto, después de haber detectado el fallo también debemos reaccionar al mismo y poner el sistema en estado de seguridad. El siguiente



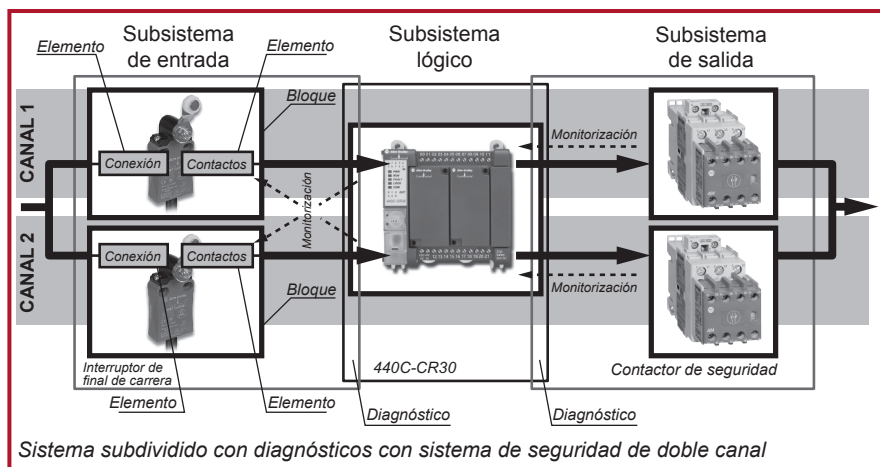
Sistemas de seguridad para maquinaria industrial

diagrama muestra la inclusión de las medidas de diagnóstico logradas por las técnicas de monitorización.



Generalmente [aunque no siempre] el sistema comprende doble canal en todos sus subsistemas. Por lo tanto, podemos ver que en este caso cada subsistema tiene dos "subcanales". La norma describe estos como "bloques". Un subsistema de doble canal tiene un mínimo de dos bloques, y un subsistema de canal individual tiene un mínimo de un bloque. Es posible que algunos sistemas comprendan una combinación de bloques de doble canal y de canal individual.

Si deseamos investigar el sistema en mayor profundidad debemos ver las partes que componen los bloques. La herramienta SISTEMA utiliza el término "elementos" para estas partes de los componentes.



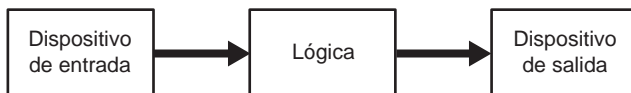
Diseño del sistema conforme con (EN) ISO 13849

El subsistema de interruptores de final de carrera se muestra subdividido hasta su nivel de elemento. El subsistema del contactor de salida se subdivide hasta su nivel de bloque. El subsistema lógico no se subdivide porque el fabricante ya lo ha calificado y validado con un PL determinado. El controlador lógico lleva a cabo la función de control tanto de los interruptores de final de carrera como de los contactores. Por lo tanto, los cuadros que representan los subsistemas de interruptor de final de carrera y contactor tienen una pequeña superposición con el cuadro del subsistema lógico.

Este principio de subdivisión del sistema se puede reconocer en la metodología establecida en (EN) ISO 13849-1 y en el principio de estructura del sistema básico de la herramienta SISTEMA. Sin embargo, es importante notar que existen algunas diferencias sutiles. La norma no es restrictiva en su metodología, pero en el caso del método de estimación del PL simplificado, normalmente el primer paso consiste en dividir todo el sistema en canales y después en bloques dentro de cada canal. Con SISTEMA normalmente es más cómodo dividir el sistema en subsistemas y después cada subsistema en bloques. La norma no describe de manera explícita el concepto de subsistema, pero su uso como se da en SISTEMA proporciona un enfoque más comprensible e intuitivo. Por supuesto no se afecta el cálculo final. SISTEMA y la norma utilizan los mismos principios y las mismas fórmulas. Es interesante notar que el enfoque de subsistema también se utiliza en EN/IEC 62061.

El sistema que hemos estado utilizando como ejemplo es sólo uno de los cinco tipos básicos de arquitecturas de sistemas que designa la norma. Cualquier persona que esté familiarizada con el sistema de categorías reconocerá nuestro ejemplo como representativo de la categoría 3 o 4.

La norma emplea cinco categorías originales de la anterior EN 954. Las denomina categorías de arquitecturas designadas. Los requisitos para las categorías son casi [pero no del todo] idénticas a aquellas que aparecen en EN 954-1. Las categorías de arquitecturas designadas están representadas por las siguientes figuras. Es importante notar que éstas pueden aplicarse a un sistema completo o a un subsistema. Los diagramas no tienen que considerarse necesariamente una estructura física; su objetivo es más bien ofrecer una representación gráfica de requisitos conceptuales.



Categoría B de arquitectura designada

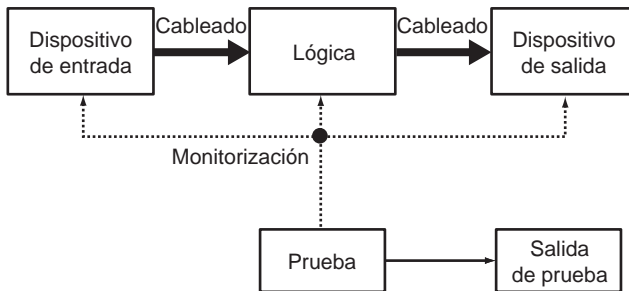
La categoría de arquitectura designada B debe emplear principios de seguridad básicos [véase el anexo de (EN) ISO 13849-2]. El sistema o subsistema puede fallar en el caso de un fallo único.

Consulte los requisitos completos en (EN) ISO 13849-1.



Categoría 1 de arquitectura designada

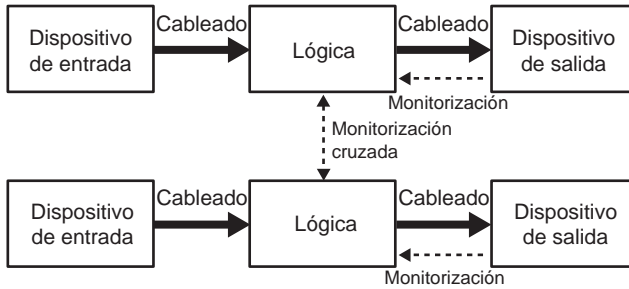
La categoría 1 de arquitectura designada tiene la misma estructura que la categoría B, e igualmente puede fallar en caso de un fallo único. No obstante, dado que debe emplear también principios de seguridad de eficacia probada [véase el anexo de (EN) ISO 13849-2] es menos probable que para la categoría B. Consulte los requisitos completos en (EN) ISO 13849-1.



Categoría 2 de arquitectura designada

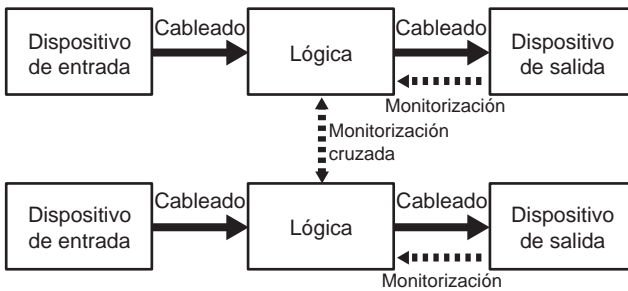
La categoría de arquitectura designada 2 debe emplear principios de seguridad básicos [véase el anexo de (EN) ISO 13849-2]. También debe haber monitorización de diagnóstico a través de una prueba funcional del sistema o del subsistema. Ésta debe ocurrir durante la puesta en marcha y luego periódicamente con una frecuencia equivalente a por lo menos cien pruebas por cada demanda sobre la función de seguridad. La enmienda de 2015 admite como requisito alternativo que la función de seguridad pase al estado de seguridad antes del tiempo de seguridad del proceso. Puede que el sistema o subsistema aún falle si se produce un único fallo entre las pruebas funcionales, pero esto suele ser menos probable que con la categoría 1. Tenga en cuenta que para la categoría 2 empleada para PLd deberá haber dos dispositivos de salida de señal ya que, en caso de que se produzca una detección de fallo, la salida de prueba deberá iniciar un estado de seguridad. Consulte los requisitos completos en (EN) ISO 13849-1.

Diseño del sistema conforme con (EN) ISO 13849



Categoría 3 de arquitectura designada

La categoría de arquitectura designada 3 debe emplear principios de seguridad básicos [véase el anexo de (EN) ISO 13849-2]. También existe el requisito de que el sistema o subsistema no debe fallar en el caso de un fallo único. Esto significa que el sistema debe tener tolerancia a fallo único con respecto a su función de seguridad. La forma más habitual de cumplir este requisito consiste en emplear una arquitectura de doble canal como la que se ha mostrado anteriormente. Además de ello, también se requiere que, siempre que sea posible, se detecte el fallo único. Este requisito es igual al requisito original de la categoría 3 de EN 954-1. En ese contexto el significado de la frase “siempre que sea posible” resultó ser de alguna manera problemática. Implicaba que la categoría 3 podía cubrir todo, desde un sistema con redundancia pero sin detección de fallos [con frecuencia denominada de forma descriptiva “redundancia estúpida”] hasta un sistema redundante donde se detectaran todos los fallos únicos. Este problema se corrige en (EN) ISO 13849-1 con el requisito de estimar la calidad de la cobertura de diagnóstico [DC]. Podemos observar que, cuanto mayor es la fiabilidad [MTTF_p] del sistema, menor es la DC que necesitamos. No obstante, en todos los casos, la DC tiene que ser como mínimo del 60% para las arquitecturas de la categoría 3.



Categoría 4 de arquitectura designada



La categoría de arquitectura designada 4 debe emplear principios de seguridad básicos [véase el anexo de (EN) ISO 13849-2]. Tiene un diagrama de requisitos similares para la categoría 3, pero demanda mayor monitorización, es decir, mayor cobertura de diagnóstico. Esto se ilustra con líneas punteadas más gruesas que representan las funciones de monitorización. En esencia, la diferencia entre las categorías 3 y 4 radica en que en la categoría 3 deben detectarse la mayoría de los fallos, pero en la categoría 4 deben detectarse todos los fallos individuales peligrosos y las combinaciones de fallos peligrosas. En la práctica, normalmente esto se logra con un alto nivel de diagnóstico para garantizar que todos los fallos relevantes se detecten antes de que pueda producirse una acumulación. La DC tiene que ser como mínimo del 99%.

Datos de fiabilidad

(EN) ISO 13849-1 emplea datos de fiabilidad cuantitativos como parte del cálculo del PL alcanzado por los componentes del sistema de control relacionados con la seguridad. La primera pregunta que esto genera es, ¿de dónde obtenemos esta información? Es posible utilizar datos de manuales de fiabilidad reconocida, pero la norma aclara que la fuente de preferencia es el fabricante. Por ello, Rockwell Automation facilita la información relevante a través de la biblioteca de datos para SISTEMA. Antes de continuar debemos considerar qué tipos de datos se requieren y también entender cómo se producen.

El tipo fundamental de datos requeridos como parte de la determinación de PL en la norma [y en SISTEMA] es el valor PFH_d [la probabilidad de fallo peligroso por hora]. Son los mismos datos que se utilizan en IEC 61508 y están representados por la abreviatura PFH_d empleada en IEC/EN 62061.

PL (Nivel de rendimiento)	PFH_d (Probabilidad de fallos peligrosos por hora)	SIL (Nivel de integridad de seguridad)
a	$\geq 10^{-5}$ a $< 10^{-4}$	Ninguno
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$	1
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $< 10^{-6}$	2
e	$\geq 10^{-8}$ a $< 10^{-7}$	3

La tabla anterior muestra la relación entre PFH_d y PL y SIL. En el caso de algunos subsistemas, puede que el fabricante proporcione la PFH_d . Esto facilita el cálculo. El fabricante usualmente tiene que llevar a cabo cálculos relativamente complejos y/o pruebas en sus subsistemas para poder proveerlo. En caso de que esta no se encuentre disponible, (EN) ISO 13849-1 nos ofrece un enfoque simplificado alternativo basado en el promedio $MTTF_d$ [tiempo medio antes de un fallo peligroso] de un canal individual. El PL [y en consecuencia la PFH_d] de un sistema o subsistema se puede calcular mediante la metodología y las fórmulas de la norma. Puede hacerse de manera aún más conveniente utilizando SISTEMA.

Diseño del sistema conforme con (EN) ISO 13849

NOTA: Es importante saber que, en el caso de un sistema de doble canal (con o sin diagnóstico), no es correcto utilizar la $1/PFH_d$ para determinar el $MTTF_d$ que exige (EN) ISO 13849-1. La norma requiere el $MTTF_d$ de un canal individual. Se trata de un valor muy diferente del $MTTF_d$ de la combinación de ambos canales de un subsistema de dos canales. Si se conoce la PFH_d de un subsistema de dos canales, simplemente se podrá introducir directamente en SISTEMA

MTTF_d de un canal individual

Representa el tiempo medio promedio antes de la ocurrencia de un fallo que podría ocasionar el fallo de la función de seguridad. Se expresa en años. Se trata de un valor medio de los $MTTF_d$ de los “bloques” de cada canal y se puede aplicar a un sistema o un subsistema. La norma proporciona esta fórmula que se emplea para calcular la media de todos los $MTTF_d$ de cada elemento empleado en un canal individual o subsistema.

En esta etapa, el valor de SISTEMA se vuelve evidente. Los usuarios no invierten tiempo consultando tablas y cálculos de fórmulas debido a que estas tareas son realizadas por el software. Los resultados finales pueden ser impresos en formato de informe de múltiples páginas.

$$\frac{1}{MTTF_d} = \sum_{j=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{dj}}$$

Fórmula D1 de (EN) ISO 13849-1

En la mayoría de los sistemas de doble canal, ambos canales son idénticos; en consecuencia, el resultado de la fórmula representa cualquiera de los canales.

Si los canales del sistema o del subsistema son diferentes, la norma proporciona una fórmula para ello.

$$MTTF_d = \frac{2}{3} \left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Esto, en efecto, promedia los dos promedios. Para simplificar, también se permite usar el valor de canal en el peor de los casos.



La norma agrupa el $MTTF_D$ en estos tres intervalos:

Denotación del $MTTF_D$ de cada canal	Intervalo del $MTTF_D$ de cada canal
Bajo	3 años \leq $MTTF_D$ < 10 años
Mediano	10 años \leq $MTTF_D$ < 30 años
Alto	30 años \leq $MTTF_D$ < 100 años

Niveles del $MTTF_D$

Tenga en cuenta que (EN) ISO 13849-1 limita el $MTTF_D$ que se puede utilizar de un canal individual de un subsistema a un máximo de 100 años, aunque puede que los valores reales obtenidos sean mucho más altos

Tal y como veremos más adelante, el intervalo del promedio del $MTTF_D$ obtenido se combinará después con la categoría de arquitectura designada y la cobertura de diagnóstico [DC] para proporcionar una clasificación de PL preliminar. El término preliminar se utiliza aquí porque aún se debe cumplir con otros requisitos, incluida la integridad sistemática y las medidas contra fallo por causa común, cuando sea pertinente.

Métodos de determinación de datos

Ahora necesitamos profundizar una etapa más en el modo en el que un fabricante determina los datos en forma de PFH_D o $MTTF_D$. Entender esto es esencial al tratar con los datos de los fabricantes. Los componentes pueden agruparse en tres tipos básicos:

- Mecánico (electromecánico, mecánico, neumático, hidráulico, etc.)
- Electrónico (por ej., estado sólido)
- Software

Existe una diferencia fundamental entre los mecanismos de fallo común de estos tres tipos de tecnología. En forma básica puede resumirse de la siguiente manera:

Tecnología mecánica:

El fallo es proporcional respecto a la fiabilidad inherente y a la tasa de uso. Mientras mayor es la tasa de uso, mayor es la probabilidad de que una de las piezas de los componentes se degrade y falle. Note que ésta no es la única causa de fallo, pero a menos que limitemos el tiempo/ciclos de operación, será la predominante. Es evidente que un contactor que tiene un ciclo de conmutación de una vez cada diez segundos opera de manera más fiable durante un tiempo mucho más corto que un contactor idéntico que opera una vez por día.

Diseño del sistema conforme con (EN) ISO 13849

Los dispositivos tecnológicos físicos generalmente comprenden componentes diseñados de manera individual para uso específico. Los componentes se conforman, moldean, funden, mecanizan, etc. Se combinan con acoplamientos, resortes, imanes, bobinados eléctricos, etc. hasta formar un mecanismo. Debido a que las piezas de los componentes en general no tienen ningún historial de uso en otras aplicaciones, no podemos encontrar datos fiables preexistentes. El cálculo de la PFH_D o el $MTTF_D$ del mecanismo normalmente se basa en las pruebas. Tanto EN/IEC 62061 como (EN) ISO 13849-1 abogan por un proceso de ensayo denominado ensayo $B10_D$.

En el ensayo $B10_D$, varias muestras de dispositivo [normalmente un mínimo de diez] se prueban en condiciones convenientemente representativas. La media de ciclos operativos alcanzada antes de que el 10% de las muestras fallen y pasen a la condición peligrosa se conoce como valor $B10d$. En la práctica, normalmente todas las muestras fallan y pasan a un estado de seguridad, pero en este caso la norma determina que el valor $B10d$ [peligroso] se pueda considerar el doble del valor $B10$.

Tecnología electrónica:

No existe un desgaste físico asociado a las piezas móviles. Dado un entorno de funcionamiento acorde con las características eléctricas y de temperatura especificadas, el fallo predominante de un circuito electrónico será proporcional a la fiabilidad inherente de sus componentes constituyentes [o la ausencia de ellos]. Existen muchas razones para los fallos de componentes por separado: imperfecciones introducidas durante la fabricación, sobretensiones excesivas, problemas de conexión mecánica, etc. En general, los fallos en los componentes electrónicos pueden deberse a la carga, el tiempo y la temperatura, pero es difícil predecirlos con un análisis y parecen tener una naturaleza aleatoria. Por lo tanto, la prueba de un dispositivo electrónico en condiciones de prueba de laboratorio no necesariamente revela patrones típicos de fallo a largo plazo.

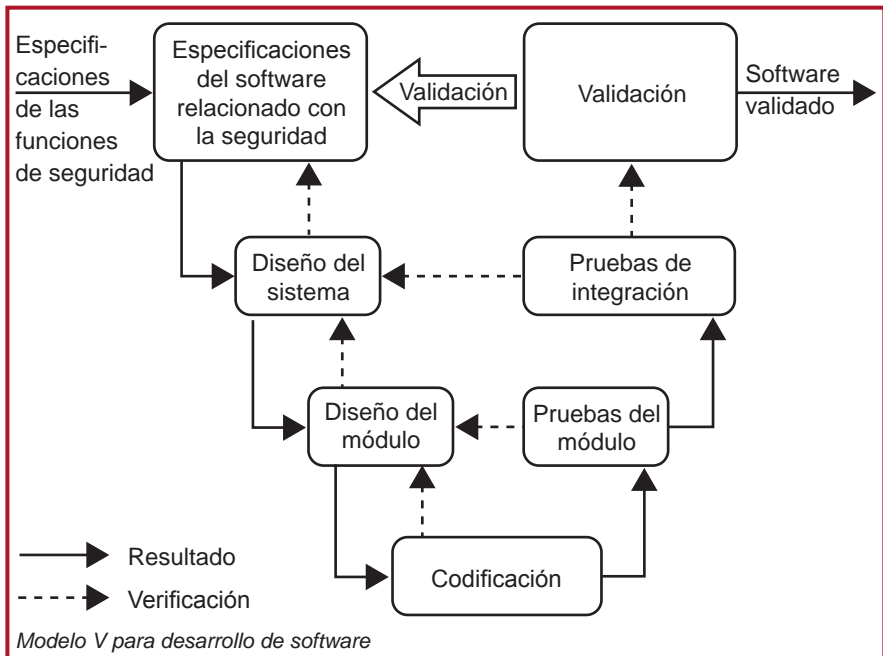
Para poder determinar la fiabilidad de los dispositivos electrónicos es común el uso de análisis y cálculo. Podemos encontrar buenos datos para los componentes individuales en los manuales de datos de fiabilidad. Podemos utilizar el análisis para determinar qué modos de fallo de componentes son peligrosos. Es una práctica aceptable y habitual calcular la media de los modos de fallo de los componentes como un 50% seguros y un 50% peligrosos. Esto normalmente resulta en datos relativamente conservadores.

IEC 61508 proporciona fórmulas que pueden usarse para calcular la probabilidad total de fallo peligroso [PFH o PFD] del dispositivo, es decir, el subsistema. Las fórmulas son bastante complejas y toman en cuenta [de ser aplicable] la fiabilidad del componente, el potencial de fallos por causa común [factor beta], la cobertura de diagnóstico [DC], el intervalo de prueba funcional y el intervalo de prueba de calidad. La conveniente es que este cálculo complejo normalmente lo realiza el fabricante del dispositivo. Tanto EN/IEC 62061 como (EN) ISO 13849-1 admiten subsistemas calculados de este modo según IEC 61508. La PFH_D resultante se podrá utilizar directamente en el Anexo K de (EN) ISO 13849-1 o en la herramienta de cálculo SISTEMA.



Software:

Los fallos del software son de naturaleza inherentemente sistemática. Estos fallos se deben al modo en el que se diseña, escribe o compila. Por lo tanto, todos los fallos son causados por el sistema bajo el cual es producido, no por su uso. Por esto, para controlar los fallos debemos controlar ese sistema. Tanto IEC 61508 como (EN) ISO 13849-1 establecen requisitos y metodologías para ello. No necesitamos entrar en detalles aquí, excepto decir que éstas utilizan el modelo clásico V. El software incorporado es una tarea para el diseñador del dispositivo. El enfoque habitual consiste en desarrollar software integrado de conformidad con los métodos formales establecidos en IEC 61508 parte 3. En lo que respecta al código de aplicación, el software con el que interactúa el usuario, la mayoría de los dispositivos de seguridad programables cuentan con rutinas o bloques de funciones “certificados”. Esto simplifica la tarea de validación para el código de aplicación, pero debe recordarse que el programa de aplicación completo aún necesita ser validado. La manera en cómo están vinculados y parametrizados los bloques debe ser correcta y válida para la tarea prevista. (EN) ISO 13849-1 e IEC/EN 62061 contienen pautas para este proceso.



Diseño del sistema conforme con (EN) ISO 13849

Cobertura de diagnóstico

Ya hemos mencionado este tema cuando consideramos las categorías 2, 3 y 4 de la arquitectura designada. Dichas categorías requieren alguna forma de prueba de diagnóstico para verificar si la función de seguridad sigue estando funcionando. El término “cobertura de diagnóstico” [normalmente abreviado como DC] se utiliza para caracterizar la eficacia de esta prueba. Es importante darse cuenta de que la cobertura de diagnóstico no está basada sólo en el número de componentes que pueden fallar de manera peligrosa. Tiene en cuenta la tasa total de fallos peligrosos. El símbolo λ se usa para “tasa de fallo”. La cobertura de diagnóstico expresa la relación de las tasas de ocurrencia de los dos siguientes tipos de fallos peligrosos:

Fallo peligroso detectado [λ_{dd}], es decir, aquellos fallos que causarían o podrían causar la pérdida de la función de seguridad, pero que se detectan. Después de la detección, una función de reacción al fallo ocasiona que el dispositivo o sistema pase al estado de seguridad.

Fallo peligroso [λ_d], es decir, todos aquellos fallos que podrían llegar a causar la pérdida de la función de seguridad. Esto incluye tanto los fallos que son detectados como aquellos que no lo son. Naturalmente, los fallos realmente peligrosos son aquellos que no se detectan [denominados λ_{du}]

La cobertura de diagnóstico se expresa mediante la fórmula:

$DC = \lambda_{dd}/\lambda_d$, expresada como porcentaje.

Este sentido del término DC es común a (EN) ISO 13849-1 y EN/IEC 62061. No obstante, el modo en el que se obtiene difiere. La segunda norma propone el uso de un cálculo basado en el análisis del modo de fallo, pero también permite el uso del método simplificado en forma de datos históricos, tal y como establece (EN) ISO 13849-1. Varias técnicas de diagnóstico típicas se enumeran junto con el porcentaje de cobertura de diagnóstico que se considera se obtenga según su uso. En algunos casos, se requiere igualmente el juicio racional, por ejemplo en algunas técnicas la cobertura de diagnóstico obtenida es proporcional a la frecuencia con que se realiza la prueba. A veces se argumenta que este enfoque es bastante impreciso. Sin embargo, el cálculo de la cobertura de diagnóstico puede depender de muchas variables diferentes, e independientemente de cualquiera de las técnicas que se utilice, el resultado en general realmente sólo puede describirse como aproximado.

También es importante entender que las tablas de (EN) ISO 13849-1 se basan en amplias investigaciones llevadas a cabo por el IFA con resultados obtenidos mediante el empleo de técnicas de diagnóstico conocidas en aplicaciones reales. Para simplificar, la norma divide la cobertura de diagnóstico en cuatro rangos básicos.

<60% = ninguna
 60% a <90% = baja
 90% a <99% = media
 ≥99% = alta



Este enfoque de usar rangos en vez de valores porcentuales individuales también puede considerarse más realista en términos de la precisión que se puede lograr. La herramienta SISTEMA utiliza los mismos datos históricos que la norma. A medida que aumenta el uso de electrónica compleja en dispositivos relacionados con la seguridad, la cobertura de diagnóstico se convierte en un factor más importante. Es probable que el trabajo futuro en las normas trate de aclarar este tema. Mientras tanto, el uso del análisis racional de ingeniería y sentido común debería ser suficiente para llevar a la correcta elección del rango de cobertura de diagnóstico.

Fallo por causas comunes

En la mayoría de los sistemas o de los subsistemas de doble canal [es decir, tolerantes a fallo único], el principio de diagnóstico está basado en la premisa de que no habrá fallos peligrosos en ambos canales al mismo tiempo. El término “al mismo tiempo” puede expresarse con más exactitud como “dentro del intervalo de prueba de diagnóstico”. Si el intervalo de prueba del diagnóstico es razonablemente corto [por ej., menor de ocho horas] es razonable asumir que dos fallos no relacionados e independientes tienen baja probabilidad de ocurrir dentro de ese tiempo. Sin embargo, la norma deja en claro que debemos pensar cuidadosamente acerca de si las posibilidades de fallo son realmente independientes y no relacionadas. Por ejemplo, si un fallo en un componente puede ocasionar de manera previsible fallos de otros componentes, entonces la totalidad resultante de fallos se considera un fallo único.

Es además posible que un evento que ocasione el fallo de un componente pueda también causar el fallo de otros componentes. Esto se denomina “fallos por causa común”, normalmente abreviado como CCF. El grado de propensión de los CCF normalmente se describe como el factor beta (β). Es muy importante que los diseñadores de sistemas y subsistemas estén al tanto de las posibilidades de fallos por causa común. Existen muchos tipos diferentes de fallos por causa común y, correspondientemente, muchas distintas formas de evitarlos. (EN) ISO 13849-1 marca un proceso razonable entre los extremos de la complejidad y la simplificación excesiva. Al igual que EN/IEC 62061 adopta un enfoque que es esencialmente cualitativo. Ofrece una lista de medidas eficaces para evitar los fallos por causa común.

Núm.	Medida contra CCF	Puntaje
1	Separación/segregación	15
2	Diversidad	20
3	Diseño/aplicación/experiencia	20
4	Evaluación/análisis	5
5	Competencia/formación	5
6	Condiciones ambientales	35

Puntaje para fallos por causa común

Diseño del sistema conforme con (EN) ISO 13849

Se debe implementar una cantidad suficiente de estas medidas para el diseño de un sistema o subsistema. Se puede aducir, con cierta justificación, que el uso de esta lista puede no ser adecuada para evitar todas las posibilidades de fallos por causa común. Sin embargo, si el propósito de la lista se considera de manera apropiada, es claro que el espíritu de este requisito es hacer que el diseñador analice las posibilidades de fallos por causa común e implemente medidas apropiadas para evitarlos, basadas en el tipo de tecnología y las características de la aplicación prevista. El uso de la lista aplica la consideración de algunas de las técnicas más fundamentales y eficaces, tales como diversidad de modo de fallo y habilidades de diseño. La herramienta SISTEMA del IFA también requiere la implementación de las tablas de consulta CCF de la norma y las proporciona en un formato cómodo.

Fallos sistemáticos

Ya hemos hablado sobre los datos de fiabilidad de la seguridad cuantificada en forma de $MTTF_D$ y la probabilidad de un fallo peligroso. Sin embargo, esto no es todo. Cuando nos referimos a esos términos estábamos pensando acerca de fallos que parecían ser de naturaleza aleatoria. De hecho, IEC/EN 62061 se refiere de manera específica a la abreviatura PFH_D como la probabilidad de un fallo de hardware aleatorio. Pero existen algunos tipos de fallos conocidos colectivamente como “fallos sistemáticos” que pueden atribuirse a errores cometidos en el proceso de diseño o fabricación. El ejemplo clásico de esto es un error en el código del software. La norma proporciona medidas en el Anexo G para evitar estos errores [y por consiguiente los fallos]. Estas medidas incluyen disposiciones tales como el uso de materiales adecuados y técnicas de fabricación, revisión, análisis y simulación por ordenador. También existen eventos y características previsibles que pueden ocurrir en el entorno de operación que pueden causar fallo a menos que su efecto sea controlado. EL Anexo G también proporciona medidas para esto. Por ejemplo, es fácilmente previsible que puede haber pérdidas ocasionales de alimentación eléctrica. Por lo tanto, la desactivación de los componentes debe resultar en un estado de seguridad del sistema. Estas medidas pueden parecer simplemente de sentido común, y en realidad lo son, sin embargo son esenciales. El resto de los requisitos de la norma no tienen sentido a menos que se dé debida consideración al control y se eviten los fallos sistemáticos. En ocasiones esto requerirá el mismo tipo de medidas empleadas para el control de los fallos de hardware aleatorios [para lograr la PFH_D requerida] como la prueba de diagnóstico automático y el hardware redundante.

Exclusión de fallos

Una de las principales herramientas de análisis para sistemas de seguridad es el análisis de fallos. El diseñador y el usuario deben entender cómo se desempeña el sistema de seguridad en presencia de fallos. Hay muchas técnicas disponibles para realizar el análisis. Algunos ejemplos son análisis de árbol de fallos, modos de fallo, análisis de efectos y criticidad, análisis de árbol de eventos, y análisis de carga y fuerza.



Durante el análisis es posible que se descubran algunos fallos que no pueden detectarse con pruebas automáticas de diagnóstico sin un coste económico excesivo. Además, la probabilidad de que estos fallos se produzcan se puede reducir en gran medida gracias al diseño, la fabricación y los métodos de ensayo de mitigación. Bajo estas condiciones puede excluirse mayor consideración de los fallos. Exclusión de un fallo significa descartar la ocurrencia de un fallo porque la probabilidad de que se produzca dicho fallo del SRCS es insignificante.

(EN) ISO 13849-1 permite la exclusión de fallos en función de la improbabilidad técnica de ocurrencia, la experiencia técnica generalmente aceptada y los requisitos técnicos relativos a la aplicación. (EN) ISO 13849-2 ofrece ejemplos y justificaciones de la exclusión de determinados fallos de los sistemas eléctricos, neumáticos, hidráulicos y mecánicos. La exclusión de fallos debe declararse con justificaciones detalladas provistas en la documentación técnica.

No siempre es posible evaluar un sistema de control relacionado con la seguridad sin asumir que determinados fallos se pueden excluir. Para obtener información detallada sobre las exclusiones de fallos, consulte ISO 13849-2.

A medida que aumenta el nivel de riesgo, la justificación para exclusión de fallos es más rigurosa. En general, cuando se requiere un nivel de rendimiento e para que un sistema de control relacionado con la seguridad implemente una función de seguridad, no es normal recurrir a las exclusiones de fallos para lograr dicho nivel de rendimiento. Esto depende de la tecnología utilizada y del entorno de funcionamiento previsto. Por lo tanto, es esencial que el diseñador tenga especial cuidado con el uso de las exclusiones de fallos a medida que aumenta el requisito de PL.

Nivel de rendimiento (PL)

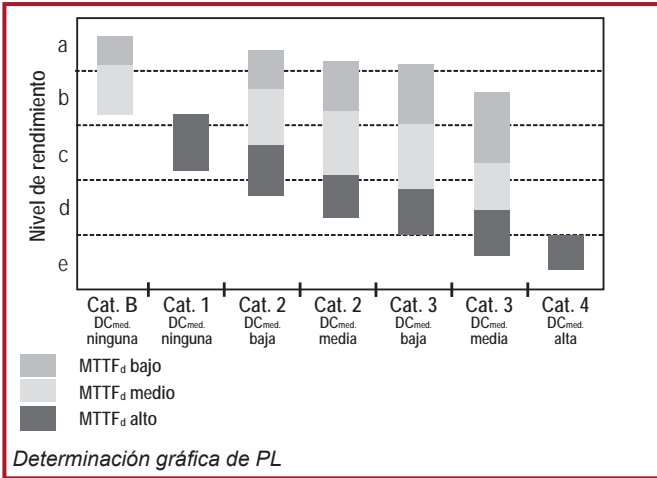
El nivel de rendimiento es un nivel discreto que especifica la capacidad de las piezas relacionadas con la seguridad de un sistema de control para realizar una función de seguridad.

Para evaluar el nivel de rendimiento logrado por la implementación de cualquiera de las cinco arquitecturas designadas, se requieren los siguientes datos del sistema (o subsistema):

- $MTTF_D$ (tiempo medio antes de un fallo peligroso de cada canal)
- DC (cobertura de diagnóstico).
- Arquitectura (la categoría)

El siguiente diagrama muestra un método gráfico para determinar el nivel de rendimiento a partir de una combinación de estos factores. La tabla del Anexo K muestra los resultados tabulares de los distintos modelos Markov que sentaron la base de este diagrama. Consulte la tabla cuando necesite determinaciones más precisas.

Diseño del sistema conforme con (EN) ISO 13849



También deben lograrse otros factores para satisfacer el nivel de rendimiento requerido. Estos requisitos incluyen las disposiciones para fallos de causa común, fallos sistemáticos, condiciones ambientales y tiempo de misión. Si se conoce la PFH_D del sistema o subsistema, las tablas del Anexo K se pueden utilizar para obtener el PL.

Diseño y combinaciones de subsistemas

Los subsistemas que cumplen un PL se pueden combinar en un sistema utilizando la tabla a continuación.

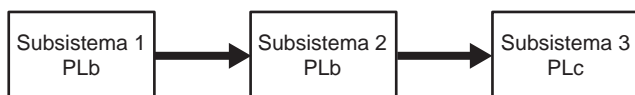
PL _{bajo}	N _{bajo}	PL
a	>3	no permitido
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Cálculo del nivel de rendimiento para subsistemas combinados en serie



El uso de esta tabla procedente de la norma no es obligatorio; simplemente tiene como objetivo proporcionar un método alternativo de peor de los casos muy sencillo cuando se desconocen los valores PFHd. El PL del sistema se puede calcular por otros métodos, incluida la herramienta SISTEMA. La lógica detrás de la tabla es clara. Primero, que el sistema sólo puede ser tan bueno como su subsistema más débil. Segundo, cuanto más subsistemas haya, mayor es la posibilidad de fallo.

En el sistema del siguiente diagrama, los niveles de rendimiento más bajos están en los subsistemas 1 y 2. Ambos son PLb. Por lo tanto, al usar esta tabla podemos leer horizontalmente b (en la columna PLlow), hasta 2 (en la columna Nlow) y encontrar el nivel de rendimiento del sistema como b (en la columna PL). Si todos los subsistemas tuvieran el nivel PLb, el nivel de rendimiento logrado sería PLa.



Combinación de subsistemas en serie como sistema PLb

Validación

La validación de las funciones de seguridad incluye y supera la verificación de los niveles de rendimiento conseguidos. El objetivo consiste en validar que la función de seguridad implementada cumpla de hecho los requisitos de seguridad globales de la maquinaria. La validación desempeña un papel importante en todo el proceso de desarrollo y puesta en servicio del sistema de seguridad. ISO/EN 13849-2:2012 establece los requisitos de validación. Requiere un plan de validación y describe la validación mediante técnicas de prueba y análisis tales como análisis de árbol de fallos y modos de fallos, análisis de efectos y criticidad. La mayoría de estos requisitos se aplican al fabricante del subsistema y no al usuario del subsistema.

Puesta en servicio de la máquina

En la etapa de puesta en servicio del sistema o de la máquina debe llevarse a cabo la validación de todas las funciones de seguridad en todos los modos de operación, y deben cubrirse todas las condiciones anormales previsibles. También deben considerarse las combinaciones de entradas y las secuencias de operación. Este procedimiento es importante porque siempre es necesario verificar que el sistema sea idóneo para las características de operación y ambientales reales. Algunas de estas características pueden ser distintas de las previstas en la etapa de diseño.

Diseño del sistema de acuerdo con IEC/EN 62061

Capítulo 8: Diseño del sistema de acuerdo con IEC/EN 62061

IEC/EN 62061, “Seguridad de máquinas – Seguridad funcional de sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad” es la implementación específica de máquinas de IEC/EN 61508. Proporciona requisitos aplicables al diseño de nivel de sistema para todos los tipos de sistemas de control eléctrico relacionados con la seguridad de las máquinas y también para el diseño de subsistemas o dispositivos no complejos.

La evaluación de riesgos resulta en una estrategia de reducción de riesgos que a su vez identifica la necesidad de funciones del sistema de control relacionado con la seguridad. Estas funciones deben documentarse y deben incluir:

- especificación de requisitos funcionales;
- especificación de los requisitos de integridad de seguridad.

Los requisitos funcionales incluyen detalles como la frecuencia de operación, el tiempo de respuesta requerido, los modos de operación, los ciclos de servicio, el ambiente de operación y las funciones de reacción ante fallo. Los requisitos de integridad de seguridad se expresan en niveles llamados niveles de integridad de seguridad (SIL). Según la complejidad del sistema, algunos o todos los elementos indicados en la siguiente tabla deben considerarse para determinar si el diseño del sistema cumple con las especificaciones del nivel de integridad de seguridad requerido.

Elemento para consideración de SIL	Símbolo
Probabilidad de fallos peligrosos por hora	PFH_b
Tolerancia a fallos de hardware	HFT
Fracción de fallo no peligroso	SFF
Intervalo de prueba de calidad	T_1
Intervalo de prueba de diagnóstico	T_2
Probabilidad de fallos por causa común	β
Cobertura de diagnóstico	DC

Elementos para consideración del nivel de integridad de seguridad

Subsistemas

El término “subsistema” tiene un significado especial en IEC/EN 62061. Es la subdivisión de primer nivel de un sistema en piezas que, si llegaran a fallar, causarían un fallo de la función de seguridad. Por lo tanto, si se usan dos interruptores redundantes en un sistema, ninguno de los interruptores individuales es un subsistema. El subsistema podría comprender ambos interruptores y cualquier otra función de diagnóstico de fallo asociada.



Probabilidad de fallos peligrosos por hora (PFH_D)

IEC/EN 62061 emplea los mismos métodos básicos señalados en la sección sobre (EN) ISO 13849-1 para determinar índices de fallos en los componentes. Las mismas disposiciones y los mismos métodos aplican a componentes electrónicos y “mecánicos”. En IEC/EN 62061 no se tiene en cuenta el $MTTF_D$ en años. La tasa de fallos por hora (λ) se calcula directamente o se obtiene o deriva a partir del valor B10 mediante la siguiente fórmula:

$$\lambda = 0,1 \times C/B10 \text{ (donde } C = \text{número de ciclos de operación por hora)}$$

Existe una diferencia importante entre las normas en la metodología para determinar la PFH_D total de un subsistema o sistema. Se debe llevar a cabo el análisis de componentes para determinar la probabilidad de fallo de los subsistemas. Se proporcionan fórmulas más simples para el cálculo de arquitecturas de subsistemas comunes (descritos más adelante en el texto). Cuando estas fórmulas no sean apropiadas será necesario utilizar métodos de cálculo más complejos, tales como los modelos Markov. Las probabilidades de fallo peligroso (PFH_D) de cada subsistema se suman para determinar la PFH_D total del sistema. La tabla 3 de la norma se puede utilizar para determinar qué nivel de integridad de seguridad (SIL) es adecuado para ese intervalo de PFH_D .

SIL (Nivel de integridad de seguridad)	PFH_D (Probabilidad de fallos peligrosos por hora)
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$

Probabilidades de fallo peligroso para niveles de integridad de seguridad (SIL)

El fabricante normalmente facilitará los datos de la PFH_D de un subsistema. Los datos de los componentes y sistemas de seguridad de Rockwell Automation se encuentran disponibles en:

www.rockwellautomation.com, en *Solutions & Services > Safety Solutions*

IEC/EN 62061 también indica que los manuales de datos de fiabilidad pueden usarse cuando corresponde.

Para dispositivos electromecánicos de baja complejidad, el mecanismo de fallo generalmente está vinculado al número y a la frecuencia de operaciones, y no sólo al tiempo. Por lo tanto, los datos para estos componentes se obtendrán de algún tipo de prueba (por ejemplo, el ensayo B10 que se describe en el capítulo sobre (EN) ISO 13849-1). En tal caso se necesitará información basada en la aplicación, como el número previsto de operaciones anuales, para convertir el B10d o datos similares en PFH_D .

Diseño del sistema de acuerdo con IEC/EN 62061

NOTA: En general lo siguiente es verdadero (tomando en cuenta un factor para cambiar años a horas):

$$PFH_D = 1/MTTF_D$$

No obstante, es importante saber que, en el caso de un sistema de doble canal (con o sin diagnóstico), no es correcto utilizar la $1/PFH_D$ para determinar el $MTTF_D$ que exige (EN) ISO 13849-1. La norma requiere el $MTTF_D$ de un canal individual. Se trata de un valor muy diferente del $MTTF_D$ de la combinación de ambos canales de un subsistema de dos canales.

Restricciones de arquitecturas

La característica esencial de la norma IEC/EN 62061 es que el sistema de seguridad está dividido en subsistemas. El nivel de integridad de seguridad del hardware que se puede declarar para un subsistema está limitado no solo por la PFH_D , sino también por la tolerancia a fallos de hardware y la fracción de fallos seguros de los subsistemas. La tolerancia a fallos de hardware es la capacidad del sistema de ejecutar su función en presencia de fallos. Una tolerancia a fallos de cero significa que la función no se realiza cuando se produce un fallo. Una tolerancia a fallo de uno permite que el subsistema realice su función en presencia de un solo fallo. La fracción de fallos no peligrosos es la porción de la tasa de fallos totales que no resulta en un fallo peligroso. La combinación de estos dos elementos se conoce como restricción arquitectónica, y su salida es el límite de declaración del nivel de integridad de seguridad (SIL CL). La siguiente tabla muestra la relación de las restricciones de arquitecturas con respecto al límite de declaración del nivel de integridad de seguridad (SIL CL). Un subsistema (y, en consecuencia, su sistema) deben cumplir los requisitos de PFH_D y las limitaciones arquitectónicas junto con otras disposiciones relevantes de la norma.

Fracción de fallo no peligroso (SFF)	Tolerancia a fallos de hardware		
	0	1	2
<60%	No permitido a menos que se apliquen excepciones específicas	SIL 1	SIL 2
60% – <90%	SIL 1	SIL 2	SIL 3
90% – <99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

Restricciones de arquitecturas con respecto al SIL

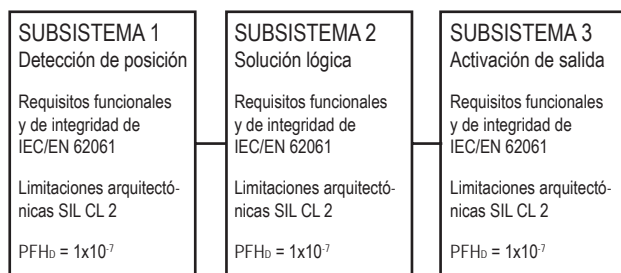
Por ejemplo, la arquitectura de un subsistema que posee tolerancia a un único fallo y tiene una fracción de fallos seguros del 75% estará limitada a una clasificación igual o inferior a SIL 2 con independencia de la probabilidad de un fallo peligroso. Cuando se



combinan los subsistemas, el nivel de integridad de seguridad obtenido por el SRCS está limitado a ser menor o igual que el límite de declaración del nivel de integridad de seguridad (SIL CL) más bajo de cualquiera de los subsistemas involucrados en la función de control relacionada con la seguridad.

Realización del sistema

Para calcular la probabilidad de fallo peligroso, cada una de las funciones de seguridad debe desglosarse en bloques de funciones, los cuales luego se ejecutan como subsistemas. La implementación de diseño de sistema de una función de seguridad típica incluye un dispositivo de detección conectado a un dispositivo lógico conectado a un accionador. Esto crea una configuración de subsistemas en serie. Como ya hemos visto, si podemos determinar la probabilidad de fallo peligroso para cada subsistema y conocer su SIL CL, entonces la probabilidad de fallo del sistema se calcula con mayor facilidad sumando la probabilidad de fallos de los subsistemas. Este concepto se muestra a continuación.



$$= PFH_b^1$$

$$= 1 \times 10^{-7}$$

$$= 3 \times 10^{-7} \text{ es decir, adecuado para SIL 2}$$

$$+ PFH_b^2$$

$$+ 1 \times 10^{-7}$$

$$+ PFH_b^3$$

$$+ 1 \times 10^{-7}$$

Si, por ejemplo, queremos alcanzar un nivel SIL 2, el límite de declaración del nivel de integridad de seguridad (SIL CL) mínimo de cada subsistema deberá ser SIL 2 y la suma de la PFH_b del sistema no deberá superar el límite permitido en la tabla anterior sobre la "Probabilidad de fallos peligrosos para los SIL".

Diseño del subsistema – IEC/EN 62061

Si un diseñador de sistema utiliza componentes ensamblados en subsistemas según IEC/EN 62061, las cosas se facilitan mucho porque no se aplican los requisitos específicos para el diseño de subsistemas. Estos requisitos son cubiertos, en general, por el fabricante del dispositivo (subsistema) y son mucho más complejos que los requeridos para el diseño a nivel de sistema.

IEC/EN 62061 requiere que los subsistemas complejos, como los PLC de seguridad, cumplan con las especificaciones de IEC 61508 u otras normas adecuadas. Esto significa que, para dispositivos que usan componentes complejos electrónicos o programa-

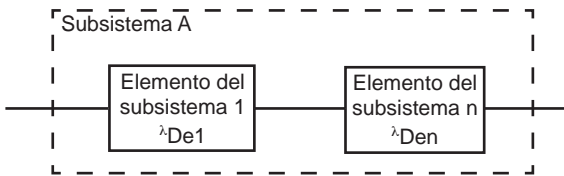
Diseño del sistema de acuerdo con IEC/EN 62061

bles, está en pleno vigor la norma IEC 61508. Esto puede ser un proceso muy difícil y laborioso. Por ejemplo, la evaluación de la PFH_D alcanzada por un subsistema puede conllevar un proceso muy complicado con el empleo de técnicas como la elaboración de modelos Markov, los diagramas de bloques de fiabilidad o el análisis del árbol de fallos.

IEC/EN 62061 proporciona requisitos para el diseño de subsistemas de menor complejidad. Normalmente esto incluye componentes eléctricos relativamente simples, como interruptores con enclavamiento y relés de control de seguridad electromecánicos. Los requisitos no son tan laboriosos como los de IEC 61508, pero pueden ser bastante complicados.

IEC/EN 62061 proporciona cuatro arquitecturas lógicas de subsistema con las fórmulas asociadas que se pueden utilizar para evaluar la PFH_D alcanzada por un subsistema de baja complejidad. Estas arquitecturas son representaciones puramente lógicas y no deben considerarse arquitecturas físicas. En los siguientes cuatro diagramas se muestran las cuatro arquitecturas lógicas de subsistemas, incluidas sus fórmulas.

Para la arquitectura de subsistema básica mostrada a continuación, las probabilidades de fallos peligrosos simplemente se suman.



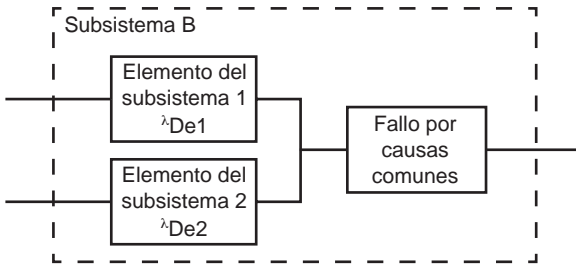
Arquitectura lógica de subsistema A

$$\lambda_{DssA} = \lambda_{De1} + \dots + \lambda_{Den}$$

$$PFHD_{ssA} = \lambda_{DssA}$$

λ Lambda se utiliza para designar el índice de fallos. Las unidades del índice de fallos son fallos por hora. λ_D , Lambda sub D es el índice de fallos peligrosos. λ_{DssA} , Lambda sub DssA es el índice de fallos peligrosos del subsistema λ . Lambda sub DssA es la suma de las tasas de fallos de los elementos individuales, e1, e2, e3, hasta e incluyendo "en". La probabilidad de fallos peligrosos se multiplica por 1 hora para crear la probabilidad de fallo durante una hora.

El siguiente diagrama muestra un sistema tolerante a un solo fallo sin función de diagnósticos. Cuando la arquitectura incluye tolerancia a un solo fallo, existe el potencial de fallos por causa común y debe tomarse en consideración. La derivación de los fallos por causa común se describe brevemente en este capítulo.



Arquitectura lógica de subsistema B

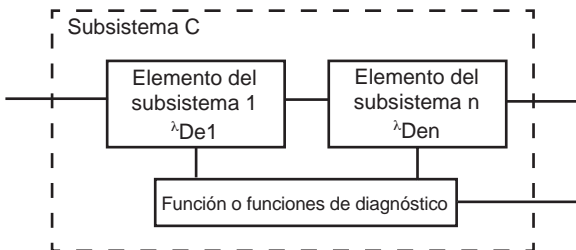
$$D_{ssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$
$$PFHD_{ssB} = \lambda D_{ssB}$$

La fórmula de esta arquitectura tiene en cuenta la disposición en paralelo de los elementos del subsistema y añade estos dos elementos de la tabla anterior "Elementos para la consideración SIL".

β – probabilidad de fallos por causa común (Beta)

T1 – intervalo de prueba de calidad o vida útil, el menor de los dos. La prueba de calidad está diseñada para detectar fallos y la degradación del subsistema de seguridad de modo que el subsistema pueda restaurarse a una condición de operación. En la práctica, normalmente esto implica una sustitución (al igual que el término equivalente "tiempo de misión" en (EN) ISO 13849-1).

El siguiente diagrama muestra la representación funcional de un sistema tolerante a cero fallos con una función de diagnósticos. La cobertura de diagnósticos se usa para reducir la probabilidad de fallos de hardware peligrosos. Las pruebas de diagnóstico se realizan automáticamente. La definición de cobertura de diagnóstico es la misma que se indica en (EN) ISO 13849-1; es decir, la relación entre el índice de fallos peligrosos detectados y el índice de fallos peligrosos totales.



Arquitectura lógica de subsistema C

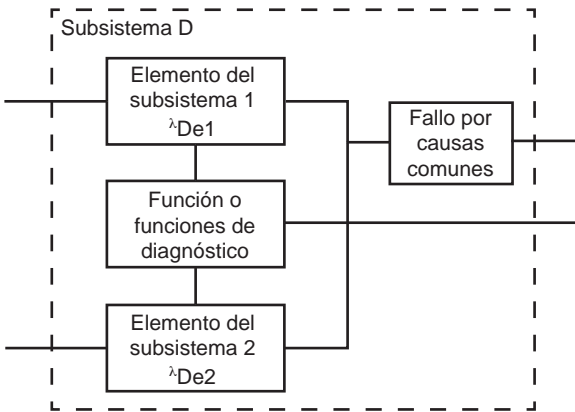
Diseño del sistema de acuerdo con IEC/EN 62061

$$\lambda_{DssC} = \lambda_{De1} (1-DC1) + \dots + \lambda_{Den} (1-DCn)$$

$$PFHD_{ssC} = \lambda_{DssC} C$$

Estas fórmulas incluyen la cobertura de diagnósticos, DC, para cada elemento del subsistema. Las tasas de fallos de cada uno de los subsistemas se reducen por la cobertura de diagnóstico de cada subsistema.

A continuación se muestra el cuarto ejemplo de una arquitectura de subsistemas. Este subsistema es tolerante a un solo fallo e incluye una función de diagnóstico. El potencial de fallos por causa común también debe considerarse en los sistemas tolerantes a un solo fallo.



Arquitectura lógica de subsistema D

Si los elementos del subsistema son diferentes se usan las siguientes fórmulas:

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De1} \times \lambda_{De2} \times (DC1 + DC2)] \times T2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC1 - DC2)] \times T1/2 \} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFHD_{ssD} = \lambda_{DssD}$$

Si los elementos del subsistema son los mismos se usan las siguientes fórmulas:

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times T2/2 + [\lambda_{De}^2 \times (1-DC)] \times T1 \} + \beta \times \lambda_{De}$$

$$PFHD_{ssD} = \lambda_{DssD}$$

Observe que ambas fórmulas usan un parámetro adicional, T2, el intervalo de diagnóstico. Esta es sólo una revisión periódica de la función. Ésta es una prueba menos completa que la prueba de calidad.



Por ejemplo, presuponga estos valores en el ejemplo en el que los elementos del subsistema son idénticos:

$$\beta = 0,05$$

$$\lambda_{De} = 1 \times 10^{-6} \text{ fallos/hora}$$

$$T1 = 87.600 \text{ horas (10 años)}$$

$$T2 = 2 \text{ horas}$$

$$DC = 90\%$$

PFHD_{ssD} = 5,790E-8 fallos peligrosos por hora. Esto estaría dentro del rango requerido para SIL 3.

Efecto del intervalo de prueba de calidad

IEC/EN 62061 señala como opción recomendada un intervalo de prueba de calidad (PTI) de 20 años (aunque no es obligatoria). Ahora veremos las repercusiones del intervalo de prueba de calidad sobre el sistema. Si recalculamos la fórmula con T1 a 20 años nos da el resultado **PFHD_{ssD}** = 6,58E-8. Todavía se encuentra dentro del intervalo requerido para el SIL 3. El diseñador deberá tener en cuenta que este subsistema debe combinarse con otros subsistemas para calcular el índice de fallos peligrosos global.

Repercusiones del análisis de fallos por causas comunes

Ahora veremos las repercusiones de los fallos por causas comunes sobre el sistema. Imagine que adoptamos medidas adicionales y nuestro valor β (Beta) mejora al 1% (0,01) mientras que el intervalo de prueba de calidad sigue siendo de 20 años. El índice de fallos peligrosos mejorará a 2,71E-8, lo que implica que el subsistema será más adecuado para su uso en un sistema SIL 3.

Fallos por causa común (CCF)

Los fallos por causa común suceden cuando múltiples fallos que son resultado de una sola causa producen un fallo peligroso. La información sobre fallos por causa común generalmente sólo la requiere el diseñador del subsistema, generalmente el fabricante. Se emplea como parte de las fórmulas facilitadas para la estimación de la **PFH_o** de un subsistema. Generalmente no se requiere a nivel de diseño del sistema.

El Anexo F de IEC/EN 62061 proporciona un enfoque sencillo para el cálculo de CCF. La siguiente tabla muestra un resumen del proceso de puntaje.

Diseño del sistema de acuerdo con IEC/EN 62061

N.º	Medida contra CCF	Puntaje
1	Separación/segregación	25
2	Diversidad	38
3	Diseño/aplicación/experiencia	2
4	Evaluación/análisis	18
5	Competencia/formación	4
6	Condiciones ambientales	18

Puntaje para medidas contra fallos por causa común

Se otorgan puntos para emplear medidas específicas contra fallos por causa común (CCF). Los puntos se suman para determinar el factor de fallos por causa común, el cual se muestra en la siguiente tabla. El factor beta se usa en modelos de subsistemas para "regular" la tasa de fallos.

Puntaje total	Factor de fallos por causas comunes (R)
<35	10% (0,1)
35 – 65	5% (0,05)
65 – 85	2% (0,02)
85 – 100	1% (0,01)

Factor beta para fallos por causa común

Cobertura de diagnósticos (DC)

Las pruebas automáticas de diagnóstico se emplean para reducir la probabilidad de fallos peligrosos de hardware. Lo ideal sería poder detectar todos los fallos de hardware peligrosos, pero en la práctica, el valor máximo está establecido en el 99% (también se puede expresar como 0,99)

La cobertura de diagnósticos es la relación de la probabilidad de fallos peligrosos detectados comparado con la probabilidad de todos los fallos peligrosos.

$$DC = \frac{\text{Probabilidad de fallos peligrosos detectados, } \lambda_{DD}}{\text{Probabilidad de fallos peligrosos totales, } \lambda_{D\text{Total}}}$$

El valor de la cobertura de diagnóstico oscilará entre cero y el 99%.



Tolerancia a fallos de hardware

La tolerancia a fallos de hardware representa el número de fallos que un subsistema puede sostener antes de que se produzca un fallo peligroso. Por ejemplo, una tolerancia a fallos de hardware de 1 significa que 2 fallos causarían una pérdida de la función de control de seguridad, pero no un solo fallo.

Gestión de la seguridad funcional

La norma proporciona requisitos para el control de gestión y las actividades técnicas necesarias para lograr un sistema de control eléctrico relacionado con la seguridad.

Intervalo de prueba de calidad

El intervalo de prueba de calidad representa el tiempo después del cual un subsistema debe verificarse o reemplazarse totalmente para asegurar que quede en condición “como nuevo”. En la práctica, en el sector de máquinas, esto se realiza mediante el reemplazo. Por lo tanto, el intervalo de prueba de calidad normalmente es igual a la vida útil. (EN) ISO 13849-1 lo denomina como tiempo de misión.

Una prueba de calidad es una comprobación que permite detectar fallos y deterioro en un SRCS, de modo que este pueda recuperar un estado prácticamente “como nuevo”. La prueba de calidad debe detectar el 100% de los fallos peligrosos, incluida la función de diagnóstico (si la hubiera). Los distintos canales deben probarse independientemente.

A diferencia de las pruebas de diagnóstico que son automáticas, las pruebas de calidad generalmente se realizan manualmente y fuera de línea. Por ser automáticas, las pruebas de diagnóstico se realizan a menudo en comparación con las pruebas de calidad que se hacen con poca frecuencia. Por ejemplo, los circuitos que van a un interruptor de enclavamiento en un resguardo pueden probarse automáticamente para detectar condiciones de cortocircuito y circuito abierto con pruebas de diagnóstico (por ej., impulsos).

El intervalo de prueba de calidad debe ser declarado por el fabricante. Algunas veces el fabricante proporciona un rango de distintos intervalos de prueba de calidad. Lo más habitual es simplemente cambiar el subsistema por uno nuevo en lugar de llevar a cabo una prueba de calidad.

Fracción de fallo no peligroso (SFF)

La fracción de fallo no peligroso es similar a la cobertura de diagnóstico, pero también toma en consideración cualquier tendencia inherente de fallo a un estado de seguridad. Por ejemplo, cuando se funde un fusible hay un fallo, pero es muy probable que el fallo sea un circuito abierto que, en la mayoría de casos sería un fallo “no peligroso”. SFF es (la suma de la tasa de fallos “no peligrosos” más la tasa de fallos peligrosos detectados) dividido entre (la suma de la tasa de fallos “no peligrosos” más la tasa de

Diseño del sistema de acuerdo con IEC/EN 62061

fallos peligrosos detectados y no detectados). Cabe señalar que los únicos tipos de fallo que deben tenerse en cuenta son aquellos que podrían tener alguna repercusión sobre la función de seguridad.

El fabricante normalmente declarará el valor SFF si es relevante.

La fracción de fallo no peligroso (SFF) puede calcularse mediante la siguiente ecuación:

$$SFF = (\sum \lambda S + (\sum \lambda DD)) / ((\sum \lambda S + (\sum \lambda D))$$

donde

- $\sum S$ = el índice de fallos seguros,
- $\sum \lambda S + \sum \lambda D$ = el índice de la totalidad de los fallos,
- λDD = el índice de fallos peligrosos detectados,
- λD = el índice de la totalidad de los fallos peligrosos.

Fallo sistemático

El estándar tiene requisitos para el control y la prevención de fallos sistemáticos. Los fallos sistemáticos difieren de los fallos de hardware aleatorios, que son fallos que se producen con aleatoriedad, normalmente como consecuencia de algún tipo de deterioro de los componentes del hardware. Los tipos típicos de posibles fallos sistemáticos son errores de diseño de software, errores de diseño de hardware, errores de especificación de requisitos y procedimientos de operación. Algunos ejemplos de los pasos necesarios para evitar un fallo sistemático son:

- correcta selección, combinación, configuraciones, ensamblaje e instalación de componentes;
- uso de buenas prácticas de ingeniería;
- seguir las especificaciones del fabricante y las instrucciones de instalación;
- asegurar la compatibilidad entre componentes
- soportar las condiciones ambientales;
- uso de materiales adecuados



Capítulo 9: Sistemas de control relacionados con la seguridad, consideraciones adicionales

Descripción general

Este capítulo estudia los principios y consideraciones estructurales generales que deberían tenerse en cuenta durante el diseño de un sistema de control relacionado con la seguridad.

Categorías de sistemas de control

Las “categorías” de los sistemas de control tienen su origen en la anterior EN 954-1:1996 (ISO 13849-1:1999). No obstante, todavía se utilizan con frecuencia para describir la estructura de los sistemas de control de seguridad y siguen siendo parte integral de (EN) ISO 13849-1 como arquitecturas designadas. La descripción y los requisitos de las categorías ya se han tratado con anterioridad en esta publicación en “Descripción general de (EN) ISO 13849-1”. El objetivo de esta sección consiste en proporcionar orientación sencilla, aunque práctica, para la implementación de las estructuras de categorías.

Categoría B

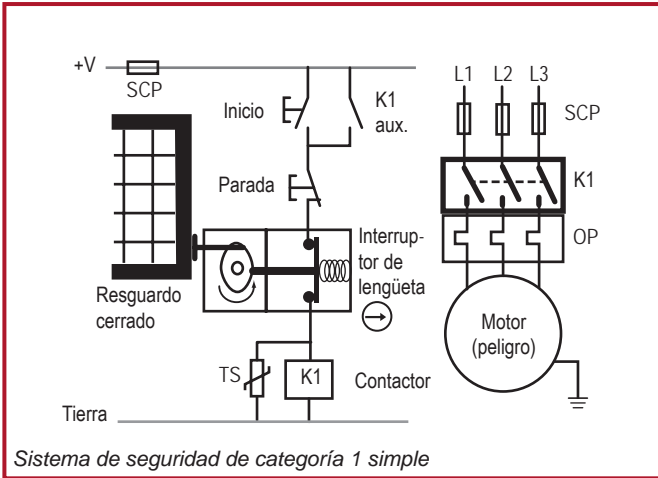
La categoría B debe considerarse la base sobre la que se construyen todas las otras categorías. No tiene ninguna estructura o disposición especial más allá de los principios de seguridad básicos señalados en los Anexos A a D de (EN) ISO 13849-2. Estos indican las buenas prácticas generales en el diseño y la selección de materiales.

Categoría 1

La categoría 1 requiere el uso de componentes y principios de seguridad de eficacia demostrada.

Aquí se muestra un sistema típico cuyo objetivo es alcanzar la categoría 1. El enclavamiento y el contactor desempeñan las funciones principales en la desconexión de la alimentación eléctrica del motor cuando es preciso acceder a la zona de peligro. El enclavamiento de lengüeta cumple los requisitos de IEC 60947-5-1 para los contactos de acción de apertura directa, tal y como indica el símbolo de la flecha dentro del círculo. Con unos componentes de eficacia demostrada, la probabilidad de que la alimentación eléctrica se desconecte es mayor para la categoría 1 de lo que lo sería para la categoría B. El uso de componentes de eficacia demostrada tiene como objetivo minimizar la posibilidad de que se pierda la función de seguridad, pero debe tenerse en cuenta que un único fallo todavía puede dar lugar a la pérdida de la función de seguridad.

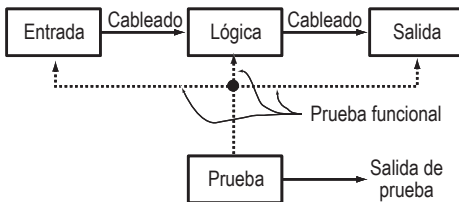
Sistemas de control relacionados con la seguridad, consideraciones adicionales



La categoría 1 tiene como fin evitar fallos mediante diseños sencillos con componentes altamente fiables. Si este tipo de prevención no reduce por sí sola el riesgo en una medida suficiente, deberá utilizarse la detección de fallos. Las categorías 2, 3 y 4 se basan en la detección de fallos o averías, con unos requisitos cada vez más exigentes para alcanzar niveles de reducción del riesgo más altos.

Categoría 2

Además de cumplir con los requisitos de la categoría B y usar principios de seguridad de eficacia probada, el sistema de seguridad debe someterse a pruebas para cumplir con la categoría 2. Las pruebas deben diseñarse para detectar fallos en las partes relacionadas con la seguridad de los sistemas de control. Si no se detecta ningún fallo, se permite el funcionamiento de la máquina. Si se detectan fallos, una función de reacción ante fallos deberá garantizar que la máquina permanezca en un estado seguro.



El equipo que realiza la prueba puede ser una parte integral del sistema de seguridad o una pieza independiente del equipo.



Las pruebas deben realizarse:

- cuando la máquina se pone en marcha,
- antes de la iniciación del peligro, y
- periódicamente fuera necesario por la evaluación de riesgos.

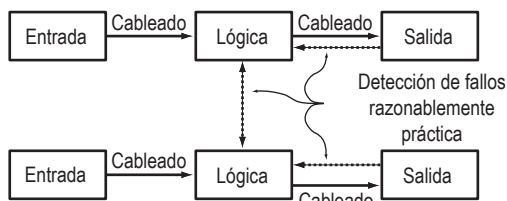
Nota: (EN) ISO 138491-1 presupone una relación entre la prueba y la demanda de la función de seguridad de 100:1 o una prueba a demanda de la función de seguridad con la capacidad de detectar un fallo y detener la máquina en menos tiempo del que se tarda en llegar al peligro.

En esencia, los subsistemas y sistemas de seguridad deben activarse para probar que su función de seguridad siga funcionando correctamente. Esto puede ser difícil o imposible de aplicar con tecnologías con características mecánicas. Un enfoque de categoría 2 suele ser más relevante para la tecnología electrónica. Para el nivel de rendimiento d, deberá existir una salida de prueba capaz de iniciar un estado de seguridad en caso de que se detecte un fallo.

Categoría 3

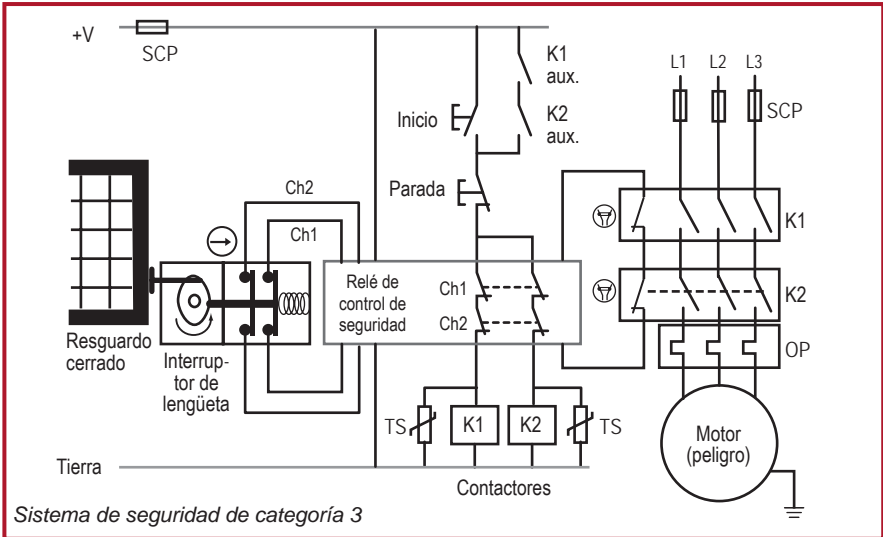
Además de cumplir con los requisitos de la categoría B y con los principios de seguridad de eficacia probada, la categoría 3 requiere resultados satisfactorios de la función de seguridad en presencia de un fallo individual. El fallo debe ser detectado durante o antes de que se imponga la siguiente demanda sobre la función de seguridad, siempre que sea razonablemente práctico.

Puede que algunos fallos, como los fallos cruzados, que no provocan una pérdida inmediata de la función de seguridad, no se detecten. Esto significa que, para la categoría 3, una acumulación de fallos no detectados puede provocar la pérdida de la función de seguridad.



Aquí se presenta un diagrama de bloques para explicar los principios de un sistema de categoría 3. La redundancia combinada con la monitorización cruzada y la monitorización de salida se utiliza para garantizar el rendimiento de la función de seguridad

Sistemas de control relacionados con la seguridad, consideraciones adicionales



Aquí se muestra un ejemplo de un sistema de categoría 3. El interruptor de seguridad con enclavamiento de lengüeta tiene conjuntos de contactos redundantes. Internamente el relé de control de seguridad (MSR) tiene circuitos redundantes que realizan control cruzado entre sí. Un conjunto redundante de contactores desconecta la alimentación eléctrica del motor. El MSR supervisa los contactores a través de los contactos mecánicamente vinculados.

La detección de fallos debe plantearse para cada componente del sistema de seguridad. ¿Cuáles son los modos de fallo de un interruptor de lengüeta de doble canal? ¿Cuáles son los modos de fallo del MSR? ¿Cuáles son los modos de fallo de los contactores K1 y K2? ¿Cuáles son los modos de fallo del cableado?

En el caso de los circuitos de categoría 3 es una práctica habitual utilizar interruptores de seguridad con enclavamiento de lengüeta sencillos con conjuntos de contactos eléctricos redundantes. Esto significa que debe excluirse la posibilidad de que se produzca un fallo de un único componente dentro de la conexión de activación. Si este fallo no se puede excluir, significa que un único fallo puede provocar la pérdida de la función de seguridad. Es muy importante que cualquier exclusión de fallos esté plenamente justificada.

El relé de control de seguridad (MSR) proporciona diagnóstico de fallos para el interruptor de seguridad con enclavamiento de lengüeta y para los contactores. El MSR también puede facilitar otras funciones, como el reinicio manual. En lo referente a su arquitectura interna, los relés de control de seguridad normalmente son PLe o SIL 3.

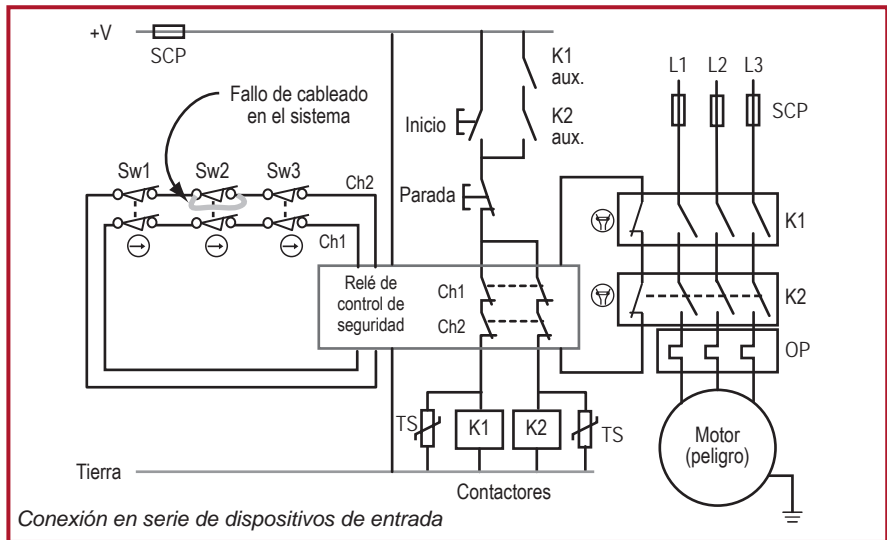
Los dos contactores deben contar con protección frente a sobrecargas y cortocircuitos. La probabilidad de que el contactor falle con contactos soldados es pequeña, aunque no



es imposible. Los contactores también pueden fallar si sus contactos de interruptor de alimentación permanecen cerrados porque el inducido se ha bloqueado. Si un contactor falla y pasa a un estado peligroso, el segundo contactor seguirá funcionando y desconectará la alimentación eléctrica del motor. El MSR detecta el contactor en fallo durante el siguiente ciclo de la máquina. Cuando la puerta esté cerrada y se pulse el botón de inicio, los contactos mecánicamente vinculados del contactor en fallo permanecerán abiertos y el MSR no podrá cerrar sus contactos de seguridad, revelando así el fallo

Fallos no detectados

Con una estructura de sistema de categoría 3 puede haber algunos fallos que no pueden ser detectados pero no deben, por sí mismos, ocasionar la pérdida de la función de seguridad. Si es posible detectar los fallos, necesitaremos saber si, en algunas circunstancias, estos se podrían enmascarar o eliminarse de forma accidental mediante el funcionamiento de otros dispositivos dentro de la estructura del sistema.



Aquí se muestra un método ampliamente usado para conectar múltiples dispositivos a un relé de control de seguridad. Cada dispositivo dispone de dos contactos de acción de apertura directa normalmente cerrados. Este método ahorra costes de cableado ya que los dispositivos de entrada están conectados en serie. Supongamos que ocurre un fallo de cortocircuito en uno de los contactos en Sw2 como muestra en la figura. ¿Puede detectarse este fallo?

Si se abre el interruptor Sw1 (o Sw3), ambos canales Cn1 y Cn2 son circuitos abiertos y el MSR desconecta la alimentación eléctrica del área de peligro. Si Sw3 se abre y luego se cierra nuevamente, el fallo en sus contactos no es detectado porque no hay cambio

Sistemas de control relacionados con la seguridad, consideraciones adicionales

de estado en el MSR: ambos canales Cn1 y Cn2 permanecen abiertos. Si Sw1 (o Sw3) se cierra después, el peligro puede reiniciarse presionando el pulsador de arranque. Bajo estas circunstancias el fallo no ocasiona pérdida de la función de seguridad, pero no es detectado, permanece en el sistema y un fallo subsiguiente (un cortocircuito en el segundo contacto del Sw2) puede ocasionar la pérdida de la función de seguridad.

Si solo Sw2 fue abierto y cerrado, sin operación de los otros interruptores, el Cn1 se abre y el Cn2 permanece cerrado. El MSR desactiva el peligro porque Ch1 está abierto. Cuando se cierra Sw2, el motor no puede arrancar cuando se presiona el botón de arranque porque no se abre Cn2. El fallo es detectado. Sin embargo, si por alguna razón, el Sw1 (o Sw3) se abre y se cierra, el circuito de ambos canales Cn1 y Cn2 se abre y luego se cierra. Esta secuencia simula el borrado del fallo y provoca el rearme no intencionado en el MSR.

Esto plantea la duda de qué DC podría declararse para los conmutadores por separado dentro de esta estructura cuando se aplica (EN) ISO 13849-1 o IEC 62061. Hasta la publicación de ISO TR 24119 (noviembre de 2015: evaluación de la conexión serial del enmascaramiento de fallo en los dispositivos de enclavamiento asociados a resguardos con contactos libres de potencial) no existían unas pautas definitivas específicas sobre este aspecto, pero era habitual presuponer una DC del 60% si los conmutadores se probaban por separado en periodos adecuados para revelar fallos. Si previsiblemente uno (o varios) de los conmutadores no se iban a probar nunca por separado, se podía alegar que su DC debía describirse como cero. ISO TR 24119 proporciona directrices detalladas para la determinación de la DC para los dispositivos de enclavamiento de resguardos con contactos libres de tensión conectados en serie. La tabla a continuación ofrece una descripción general básica. Es esencial estudiar el documento en su totalidad para determinar la DC máxima real permitida para cualquier arquitectura y aplicación concreta.

Número de resguardos móviles utilizados con frecuencia ¹	Número de resguardos móviles adicionales	Probabilidad de enmascaramiento	Cobertura de diagnóstico	PL máximo que se puede conseguir
0	2 a 4	Bajo	Mediano	PL d
	5 a 30	Mediano	Bajo	PL d
	>30	Alto	Ninguno	PL c
1	1	Bajo	Mediano	PL d
	2 a 4	Mediano	Bajo	PL d
	≥5	Alto	Ninguno	PL c
>1	--	Alto	Ninguno	PL c

¹ Frecuencia de conmutación superior a una vez por hora

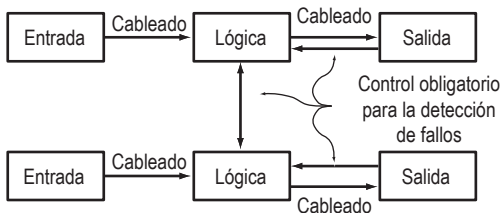


La conexión en serie de contactos electromecánicos se limita a un PLd máximo y, en algunos casos, se puede restringir a un PLc máximo. Tenga en cuenta que, en cualquier caso, si los fallos previsiblemente se enmascararán (por ejemplo, múltiples resguardos móviles se abrirán al mismo tiempo como parte del funcionamiento o servicio normal), la DC se limitará a ninguno.

Cabe destacar que estas características de una estructura de categoría 3 siempre han requerido atención, pero las normas sobre seguridad funcional hacen especial hincapié en ellas.

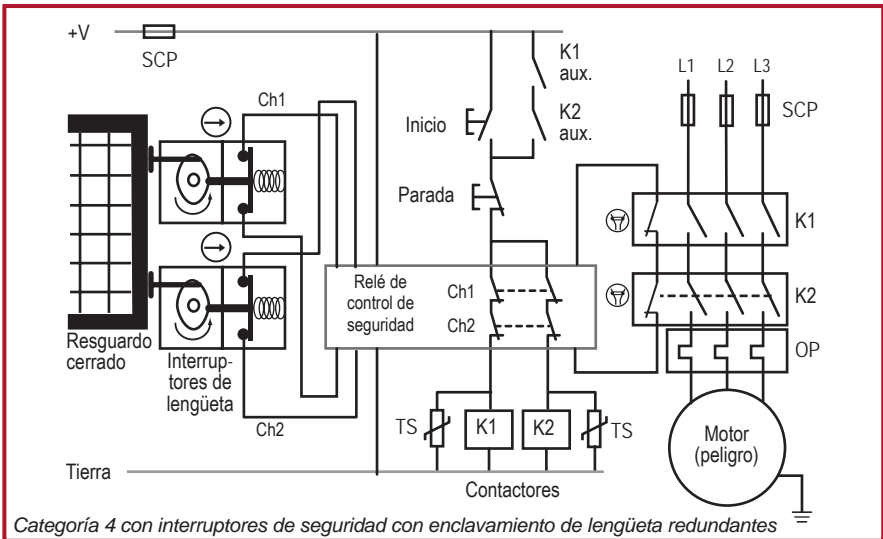
Categoría 4

Al igual que la categoría 3, la categoría 4 exige que el sistema de seguridad cumpla los requisitos de la categoría B, emplee principios de seguridad de eficacia demostrada y ejecute la función de seguridad en presencia de un único fallo. A diferencia de la categoría 3, en la que la acumulación de fallos puede causar la pérdida de la función de seguridad, la categoría 4 requiere resultados de la función de seguridad en presencia de la acumulación de fallos. En la práctica, normalmente esto se logra con un alto nivel de diagnóstico para garantizar que todos los fallos relevantes se detecten antes de que pueda producirse una acumulación. Cuando plantee una acumulación de fallos teórica, puede que baste con dos fallos, aunque en algunos diseños puede que sea necesario tener en cuenta tres fallos.

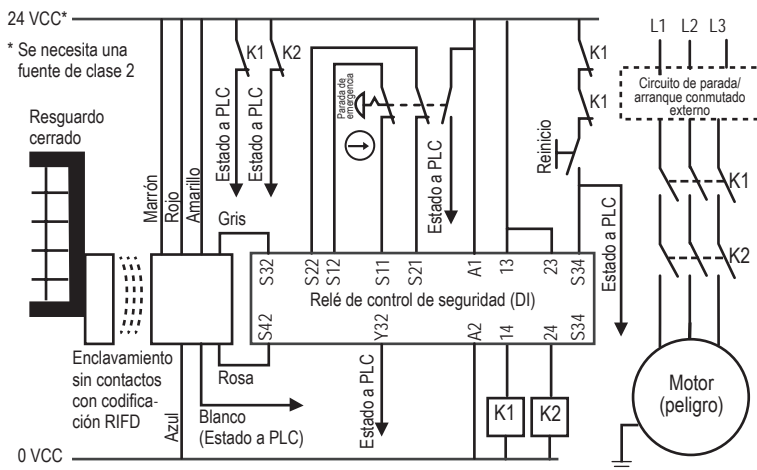


Aquí se muestra el diagrama de bloques para la categoría 4. Se necesita la supervisión de ambos dispositivos de salida y la monitorización cruzada. La categoría 4 tiene una cobertura de diagnóstico superior a la de la categoría 3.

Sistemas de control relacionados con la seguridad, consideraciones adicionales



Hasta hace relativamente poco tiempo, el uso de los interruptores de enclavamiento de lengüeta sencillos con dos canales eléctricos se planteaba para los circuitos de la categoría 4. Para poder utilizar un enclavamiento de lengüeta sencillo en un circuito de doble canal es necesario excluir los posibles puntos de fallo único en la lengüeta de accionamiento mecánica y la conexión del interruptor. No obstante, el informe técnico conjunto ISO TR 23849 ha aclarado que este tipo de exclusión de fallos no debe utilizarse en sistemas PLe o SIL 3. Si el diseñador del sistema de seguridad prefiere utilizar enclavamientos de tipo lengüeta, se pueden emplear dos interruptores distintos para cumplir los requisitos de la categoría 4.



Categoría 4 con enclavamiento sin contactos electrónicos accionado por RFID

La tecnología contemporánea tiene enfoques distintos para lograr una arquitectura de categoría 4 (y PLe/SIL 3). El uso de una electrónica compleja ha permitido integrar la tolerancia a fallos de una forma rentable y ha hecho posible un alto grado de cobertura de diagnóstico en un único dispositivo. El dispositivo de enclavamiento que se muestra no solo cumple los requisitos de la categoría 4, sino que también ofrece un nivel de resistencia a la manipulación (anulación) extremadamente alto mediante el uso de la codificación RFID. También se puede conectar en serie a otros dispositivos similares sin que se rebaje la categoría o la cobertura de diagnóstico.

PL (nivel de rendimiento) para la clasificación del sistema y los componentes

Las (categorías de) arquitecturas designadas de (EN) ISO 13849 se pueden utilizar como parte de las clasificaciones de PL de los componentes (dispositivos) de seguridad, así como clasificaciones de PL del sistema. Esto genera alguna confusión que puede aclararse al comprender los componentes y sus capacidades. Al estudiar los ejemplos anteriores, descubrimos que un componente como un interruptor de enclavamiento clasificado con la categoría 1 se puede utilizar solo en un sistema de la categoría 1. También puede formar parte de un sistema de categoría 3 ó 4 si dos de los componentes se usan junto con una función de diagnóstico proporcionada por un relé de control de seguridad.

Algunos componentes tales como los relés de control de seguridad y los controladores de seguridad programables tienen sus propios diagnósticos internos y se verifican para asegurar resultados correctos. Por lo tanto, pueden clasificarse como componentes de seguridad para cumplir con las categorías 2, 3 ó 4 sin ninguna medida adicional.

Consideraciones y exclusiones de fallos

El análisis de seguridad requiere un análisis extenso de fallos y comprender perfectamente los resultados del sistema de seguridad en presencia de fallos. ISO 13849-1 e ISO 13849-2 contienen información detallada sobre las consideraciones y las exclusiones de fallos.

Si un fallo da lugar a un fallo en otro componente, el primer fallo y todos los fallos posteriores se considerarán un único fallo.

Si dos o más fallos se producen como resultado de una misma causa, los fallos se consideran un solo fallo. Esto se conoce como fallos por causa común.

La aparición de dos o más fallos independientes al mismo tiempo se considera altamente improbable y por eso no se tiene en cuenta en este análisis.

Exclusiones de fallos

(EN) ISO 13849-1 e IEC 62061 permiten el uso de exclusiones de fallos cuando se determina la clasificación de un sistema de seguridad si se puede demostrar que la aparición del fallo es extremadamente improbable. Es importante que donde se utilicen las exclusiones de fallos, éstas sean justificadas de manera apropiada y válidas para la vida útil prevista del sistema de seguridad. Mientras mayor sea el nivel de riesgo protegido por el sistema de seguridad más estricta será la justificación requerida para la exclusión del fallo. Esto siempre ha causado confusión acerca de cuándo se pueden o no se pueden usar ciertos tipos de exclusiones de fallo. Como ya hemos visto en este capítulo, recientes normas y documentos de orientación han aclarado algunos aspectos de este tema.

En general, cuando se requiere un nivel de rendimiento e o SIL 3 para que un sistema de seguridad implemente una función de seguridad, ISO TR 23849 explica que no es normal recurrir a las exclusiones de fallos para lograr este nivel de rendimiento. Esto depende de la tecnología utilizada y del entorno de funcionamiento previsto. Por lo tanto, es esencial que el diseñador tenga especial cuidado con el uso de las exclusiones de fallos a medida que aumenta el PL o SIL. Por ejemplo, la exclusión de fallos no se aplica a los aspectos mecánicos de los interruptores de posición electromecánicos y a los interruptores operados manualmente (por ej., un dispositivo de parada de emergencia) para poder obtener un sistema PLe o SIL 3. Esas exclusiones de fallos que se pueden aplicar a condiciones de fallo mecánico concretas (por ejemplo, desgaste/corrosión, fractura) se describen en la Tabla A.4 de ISO 13849-2. Por lo tanto, un sistema de enclavamiento de resguardo que tiene que lograr un PLe o SIL 3 debe incorporar una tolerancia de fallo mínima de 1 (por ej., dos interruptores de posición mecánicos convencionales) para poder llegar a este nivel de rendimiento ya que no es normalmente justificable excluir fallos, tales como, accionadores de conmutación averiados. No obstante, puede que sea aceptable excluir fallos, como cortocircuitos del cableado dentro de un panel de control diseñado de conformidad con las normas relevantes.



Categorías de parada de acuerdo con IEC/EN 60204-1 y NFPA 79

El hecho de que el término “categoría” en lo que respecta a los sistemas de control relacionados con la seguridad tenga distintos sentidos resulta tan desafortunado como confuso. Hasta ahora hemos discutido las categorías que se originaron en EN 954-1. Son una clasificación del rendimiento de un sistema de seguridad bajo condiciones de fallo.

También existe una clasificación denominada “categorías de parada” que tiene su origen en IEC/EN 60204-1 y NFPA 79. Existen tres categorías de parada.

Categoría de parada 0 requiere desconexión inmediata de la alimentación eléctrica a los accionadores. Esto algunas veces se considera como una parada no controlada porque en algunas circunstancias el movimiento puede requerir cierto tiempo para detenerse debido a que el motor puede estar libre para parar por inercia.

Categoría de parada 1 requiere mantener la alimentación eléctrica para aplicar el freno hasta lograr la parada y luego desconectar la alimentación eléctrica del accionador. Nota: Consulte IEC 60204-1 si desea obtener información sobre las categorías de parada 1a y 1b.

Categoría de parada 2 permite que no se desconecte la alimentación eléctrica del accionador.

Tome nota de que sólo las categorías de parada 0 ó 1 pueden usarse en las paradas de emergencia. La elección de la categoría a usar debe ser definida por medio de una evaluación de riesgos.

Todos los ejemplos de circuitos mostrados hasta ahora en este capítulo han usado una categoría de parada 0. Se logra una categoría de parada 1 con una salida con retardo a la desconexión final de la alimentación eléctrica. Un resguardo enclavado con bloqueo de resguardo generalmente forma parte de un sistema de parada de categoría 1. Esto mantiene el resguardo bloqueado en posición cerrada hasta que la máquina llega a un estado seguro (por ejemplo, parado).

La detención de una máquina sin tener debidamente en cuenta el controlador programable puede afectar al reinicio y podría redundar en daños en la máquina y la herramienta. No se puede confiar sólo en un PLC estándar (no relacionado con la seguridad) para una tarea de parada relacionada con la seguridad; por lo tanto, es necesario considerar otros enfoques.

A continuación se indican dos posibles soluciones para las paradas de categoría 1:

1. Relé de seguridad con mando de anulación retardada

Se usa un relé de seguridad con salidas tanto de accionamiento inmediato como de acción con retraso. Las salidas de accionamiento inmediato se conectan a las entradas del dispositivo programable (por ejemplo, PLC o habilitación del variador) y las salidas de acción con retraso se conectan a un contactor principal. Cuando se activa el interruptor de enclavamiento de resguardo conmutan las salidas de acción inmediata en de relé de

seguridad. Éstas indican al sistema programable que realice una parada con la secuencia correcta. Una vez transcurrido un tiempo breve, aunque suficiente, para permitir este proceso, la salida retardada del relé de seguridad cambia y aísla el contactor principal.

Nota: Cualquier cálculo para determinar el tiempo total de parada debe tomar en cuenta el período de retardo de la salida del relé de seguridad. Esto es especialmente importante cuando se usa este factor para determinar la posición de los dispositivos según el cálculo de la distancia de seguridad.

2. PLC de seguridad

Las funciones lógicas y de temporización necesarias se pueden implementar cómodamente utilizando un PLC de seguridad como GuardLogix.

Requisitos del sistema de control de seguridad en los EE.UU.

Control fiable

El más alto nivel de reducción de riesgos establecido en las normas para robots de los EE.UU. y Canadá se logra mediante sistemas de control de seguridad que cumplen con los requisitos de control fiable. Los sistemas de control relacionados con la seguridad con control fiable son arquitecturas de doble canal con monitorización. La función de paro del robot no debe evitarse mediante el fallo de un componente individual, incluso la función de monitorización.

La función de monitorización genera una orden de parada al detectarse un fallo. Si un peligro permanece después que se detiene el movimiento, debe proporcionarse una señal de alarma. El sistema de seguridad debe permanecer en estado de seguridad hasta que se corrige el fallo. Preferiblemente, el fallo se debe detectar al momento en que se genera. Si esto no puede realizarse, entonces el fallo debe detectarse durante el siguiente ciclo del sistema de seguridad. Los fallos del modo común deben tomarse en cuenta si existe probabilidad significativa de que ocurra dicho tipo de fallo.

Los requisitos canadienses difieren de los requisitos de los EE.UU. en dos requisitos adicionales. Primero, los sistemas de control relacionados con la seguridad son independientes de los sistemas normales de control de programa. Segundo, el sistema de seguridad no debe neutralizarse ni omitirse sin detección.

Comentarios sobre el control fiable

El aspecto más importante de un control fiable es la tolerancia a fallos únicos y la monitorización (detección de fallos). Los requisitos establecen cómo el sistema de seguridad debe responder en presencia de “un fallo único”, “cualquier fallo único”, o “un fallo de cualquier componente individual”.

Deben tenerse en cuenta tres conceptos muy importantes en relación con los fallos: (1) no todos los fallos se detectan, (2) la adición de la palabra “componente” plantea dudas sobre el cableado, y (3) el cableado forma parte integral del sistema de seguridad. Los fallos del cableado pueden causar en la pérdida de la función de seguridad.



El propósito de la fiabilidad del control claramente es el resultado de la función de seguridad en presencia de un fallo. Si se detecta el fallo, entonces el sistema de seguridad debe ejecutar una acción de seguridad, proporcionar notificación sobre el fallo y detener el funcionamiento de la máquina hasta que el fallo sea corregido. Si no se detecta el fallo, entonces la función de seguridad debe realizarse bajo demanda.

Capítulo 10: Ejemplos de aplicación

Descripción general: funciones de seguridad prediseñadas para máquinas

Las funciones de seguridad de maquinaria, con independencia de si se trata de mecanismos de paro de emergencia, protección o detección de presencia, requieren múltiples elementos, incluido un sensor o dispositivo de entrada, un dispositivo lógico y un dispositivo de salida. Estos elementos juntos proporcionan un nivel de protección calculado en función del nivel de rendimiento, como se explica en (EN) ISO 13849-1.

En este capítulo hemos seleccionado una de las muchas funciones de seguridad prediseñadas para máquinas desarrolladas por Rockwell Automation. Cada uno de estos documentos proporciona orientación sobre una función de seguridad específica basada en los requisitos funcionales, la selección de equipos y el nivel de rendimiento exigido, incluida la configuración y el cableado, la configuración, el plan de verificación y validación y el cálculo del nivel de rendimiento.

Las funciones de seguridad prediseñadas son gratuitas y se pueden descargar del sitio web de Rockwell Automation.

www.rockwellautomation.com, en Solutions & Services > Safety Solutions.

Las funciones de seguridad a continuación se basa en un interruptor de enclavamiento de control de puerta con un relé de seguridad configurable. Los productos utilizados son: SensaGuard con codificación RFID, interruptor de enclavamiento de seguridad sin contactos conectado a un relé de seguridad configurable Guardmaster 440C-CR30. Los dispositivos de salida utilizados son contactores de seguridad 100S-C. La clasificación de seguridad alcanzada por esta función de seguridad prediseñada es: CAT. 4, PLe según (EN) ISO 13849-1.

El número de publicación del documento original es: SAFETY-AT133C-EN-P

Descripción de la seguridad funcional

Una barrera fija protege a los trabajadores del movimiento peligroso. Cuando es necesario, el acceso a la zona peligrosa se produce a través de una puerta oscilante. Un enclavamiento sin contactos SensaGuard, conectado a las entradas del relé de seguridad configurable 440C-CR30, controla la puerta. El relé 440C-CR30 controla dos contactores de seguridad 100S-C que, conectados en serie, controlan la alimentación del motor que acciona el movimiento peligroso. Cada vez que esta puerta monitorizada se abre, el sistema de seguridad desconecta la alimentación

eléctrica del motor. El motor y el movimiento peligroso que acciona mantienen la inercia hasta que se detienen (parada de categoría 0). El motor no se podrá volver a arrancar si la puerta monitorizada está abierta. Una vez que se haya cerrado la puerta, se podrá arrancar el motor de nuevo pulsando y soltando el botón que reinicia el relé 440C-CR30 e iniciando después el arranque externo para restablecer la alimentación del motor controlada por los contactores 100S-C.

El interruptor SensaGuard supervisa el estado de la puerta (abierta o cerrada). El interruptor SensaGuard también controla los fallos en sus dos salidas de dispositivo de conmutación de señal de salida. El relé 440C-CR30 controla los fallos en las entradas procedentes del interruptor SensaGuard y supervisa el estado de las señales de restablecimiento y retroalimentación procedentes de los contactores 100S-C. El relé también controla los fallos en sus propias salidas. Estas salidas controlan los contactores 100S-C. El relé 440C-CR30 desactiva sus salidas y desconecta la alimentación eléctrica del motor cuando se detecta un fallo. No se reinicia si no se ha corregido el fallo.

Lista de materiales

Esta aplicación utiliza estos productos.

Número de catálogo	Descripción	Cantidad
440N-Z21S16B	Interruptor SensaGuard, plástico de 18 mm, 2 x PNP, 0,2 A máx., salida de seguridad, cable de 10 m	1
800FP-R611	800F de reinicio, plástico redondo (tipo 4/4X/13, IP66), azul, R, empaquetado estándar	1
2080-IQ4OB4	Módulo de combinación de salida/entrada digital de cuatro canales	1
1761-CBL-PM02	Cable; relé de seguridad configurable 440C-CR30 con un ordenador personal, cable de impresora	1
440C-CR30-22BBB	Relé de seguridad configurado por software Guardmaster 440C-CR30, PLe SIL 3, 22 E/S de seguridad, puerto serial incorporado, puerto de programación USB, 2 ranuras enchufables, 24,0 V CC	1
100S-C23EJ23BC	Contactador de seguridad MCS 100S-C, 23 A, 24 V CC (con bobina eléctrica), contacto bifurcado	2

Descripción general del sistema

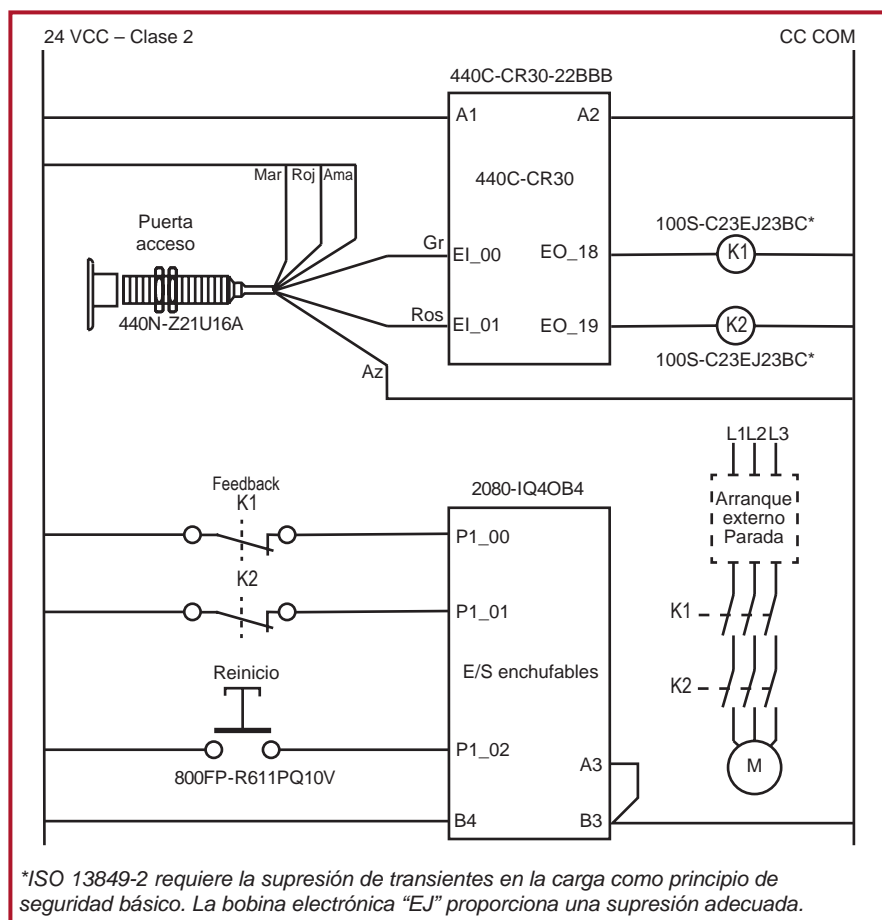
El interruptor de enclavamiento SensaGuard se utiliza para confirmar que la puerta de resguardo encuentre cerrada, en un estado seguro. El movimiento peligroso cesa o se



Sistemas de seguridad para maquinaria industrial

evita siempre que la puerta no esté cerrada. Además de controlar el estado de la puerta de resguardo, el interruptor SensaGuard supervisa todas las condiciones de fallo de sus salidas. El relé de seguridad configurable 440C-CR30 también detecta fallos de cable abierto, fallos en un único canal o cortocircuitos a 0 V en sus entradas de interruptor SensaGuard.

El relé de seguridad configurable 440C-CR30 supervisa todas las condiciones de fallo en las salidas sometidas a pruebas de impulsos que accionan las bobinas del contactor de seguridad. El relé de seguridad configurable 440C-CR30 que controla las señales de respuesta en SMF2 confirma el correcto estado de seguridad de los contactores K1 y K2 durante la puesta en marcha.



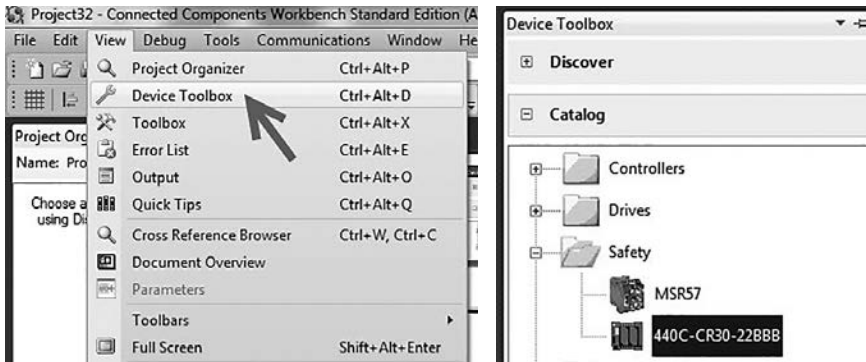
Configuración

El relé 440C-CR30 se configura mediante el software Connected Components Workbench™, versión 6.01 o posterior. La descripción detallada de cada paso está fuera del alcance de este documento. Se presupone el conocimiento del software Connected Components Workbench.

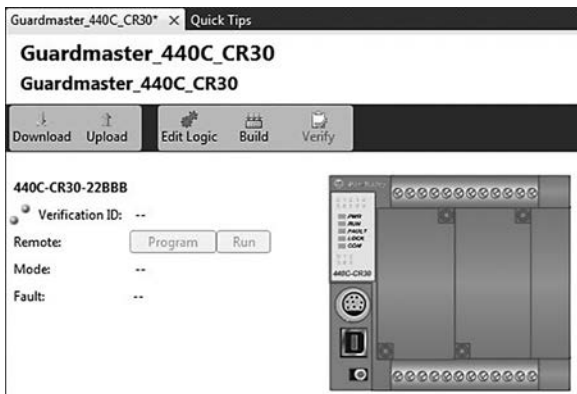
Configuración del relé 440C-CR30

Siga estos pasos para configurar el relé Guardmaster 440C-CR30 en el software Connected Components Workbench.

1. En el software Connected Components Workbench, seleccione View y después Device Toolbox. Una vez en Device Toolbox, seleccione 440C-CR30-22BBB.

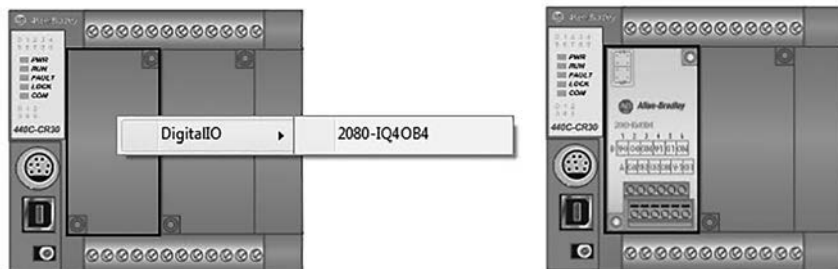


2. En Project Organizer, haga doble clic en Guardmaster_400C_CR30*.



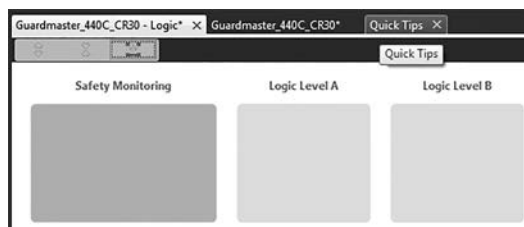
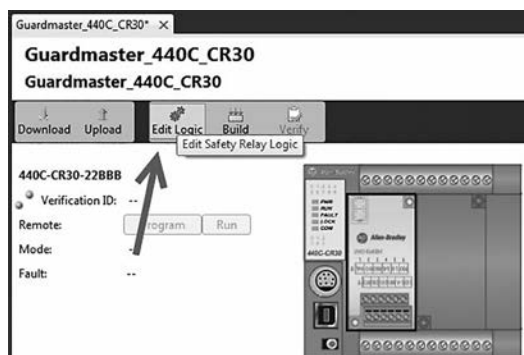


3. Para añadir el módulo de E/S enchufable solicitado en este circuito, haga clic con el botón derecho en el espacio del módulo enchufable izquierdo y seleccione el módulo 2080-IQ4OB4.

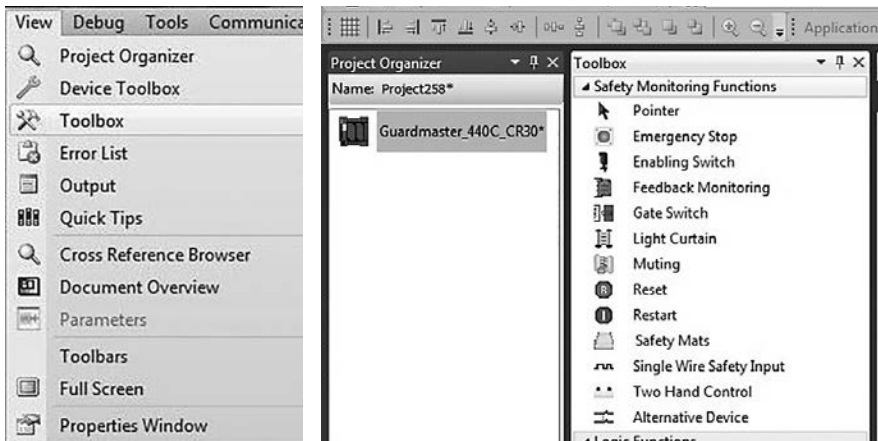


SUGERENCIA: El módulo de E/S aparecerá en el gris estándar porque no es un módulo de E/S de seguridad. Esto es posible en esta aplicación porque no se utiliza para conectar señales de seguridad. Las entradas como las de retroalimentación y el botón de reinicio no se consideran estrictamente señales de seguridad. El uso de E/S estándar para estas señales que no son de seguridad puede reservar el número limitado de entradas y salidas de seguridad para las señales de seguridad reales.

4. Haga clic en el botón Edit Logic para abrir el área de trabajo de Connected Components Workbench. Aparecerá un espacio disponible en blanco.



5. En el menú desplegable View, seleccione Toolbox. Aparecerá Toolbox.



Configuración de las entradas

Toolbox no enumera ninguna función de control de seguridad SensaGuard. Siga estos pasos para crear una.

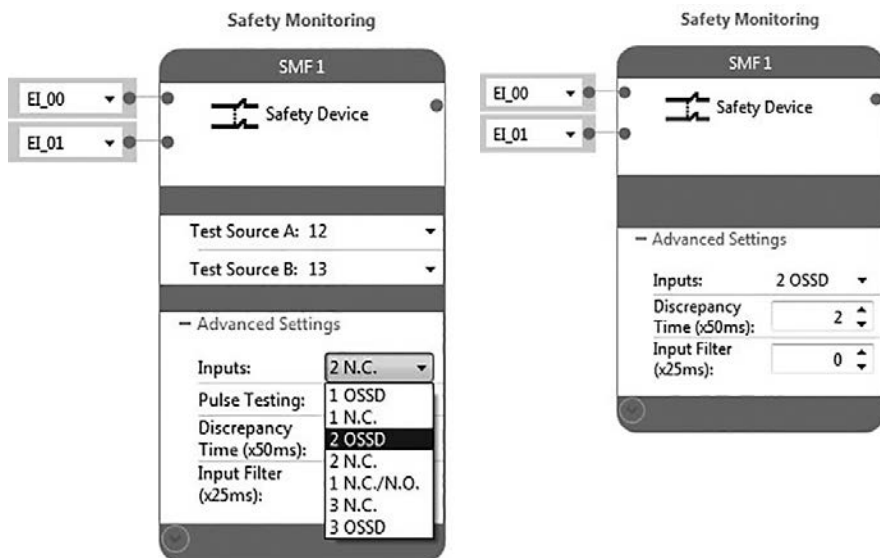
1. Seleccione Alternative Device. Arrástrelo hasta el bloque verde en la columna Safety Monitoring y suéltelo.



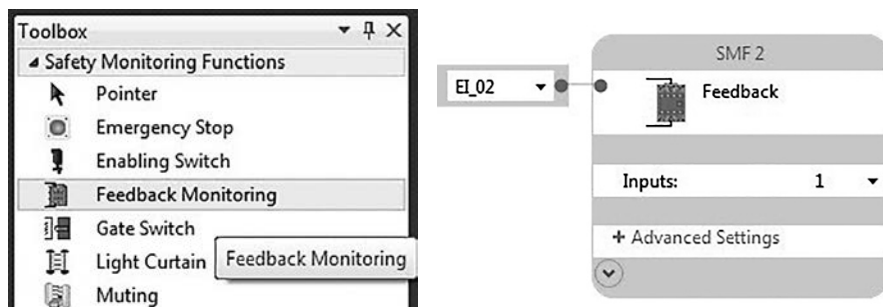


El software Connected Components Workbench asignará automáticamente las dos primeras entradas disponibles, EI_00 y EI_01, al dispositivo. Déjelas asignadas. El software Connected Components Workbench asignará automáticamente el nombre de función SMF 1 a este bloque. De manera predeterminada, el software presupondrá que se trata de un dispositivo electromecánico y le asignará fuentes de prueba. El interruptor SensaGuard cuenta con dos salidas de dispositivo de conmutación de señal de salida y no requiere fuentes de prueba.

2. Para configurar el bloque correctamente, abra Advanced Settings y seleccione 2 OSSD en el menú desplegable Inputs. El bloque resultante tendrá el aspecto de la imagen.

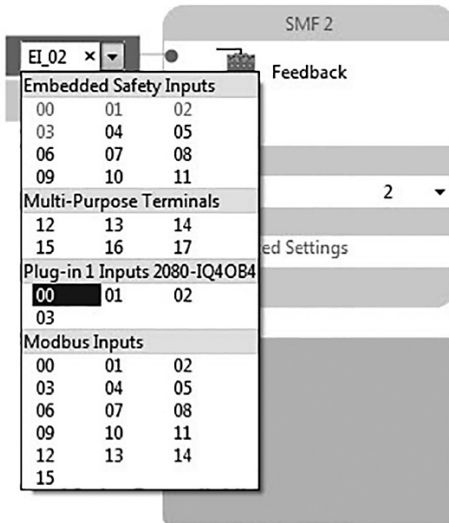


3. Haga clic en una función de control de seguridad Feedback Monitoring, arrástrela y suéltela en el bloque Safety Monitoring situado debajo del bloque SensaGuard en el área de trabajo.

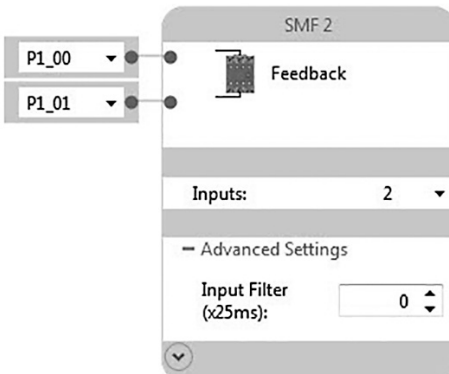


Tenga en cuenta que el software Connected Components Workbench la asignará al terminal de entrada EI_02, el siguiente terminal de entrada de seguridad disponible. El software dará por hecho que se trata de una entrada sencilla y asignará automáticamente el nombre de función SMF 2 a este bloque.

4. Dado que el circuito requiere dos entradas, una de cada contactor, cambie el número de entradas a 2, una para el contacto normalmente cerrado de cada contactor 100S.

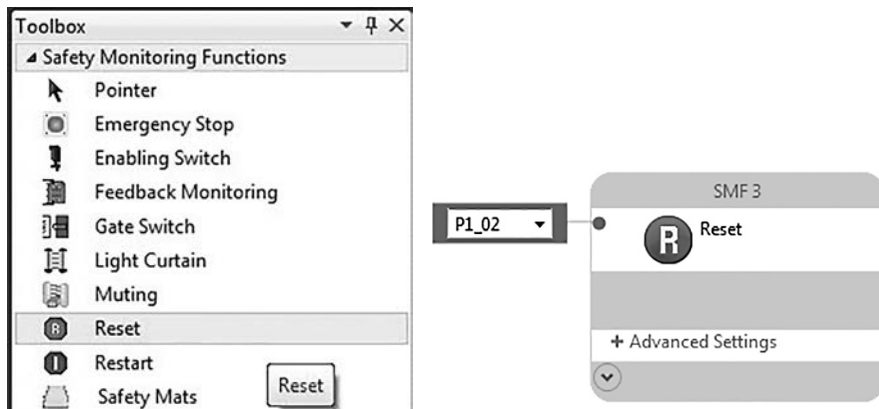


5. Asigne las entradas a los terminales enchufables PI_00 y PI_01. Esto evitará un uso innecesario de las entradas de seguridad para las señales de retroalimentación.





- Haga clic en una función de control de seguridad Reset, arrástrela y suéltela en el bloque Safety Monitoring situado debajo del bloque Feedback Monitoring en el área de trabajo.

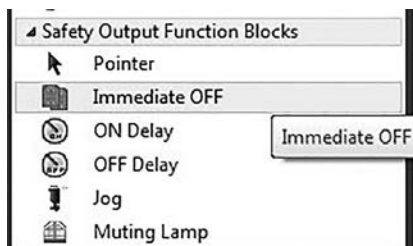


El software Connected Components Workbench asignará automáticamente el nombre de función SMF 3 a este bloque. Vuelva a asignar la entrada Reset al terminal enchufable PI_02.

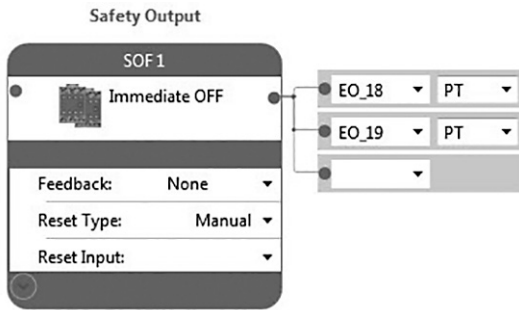
Configuración de las salidas

Para configurar las salidas, siga estos pasos.

- Haga clic en Immediate OFF en la sección Safety Output Function Blocks de Toolbox y arrástrelo.

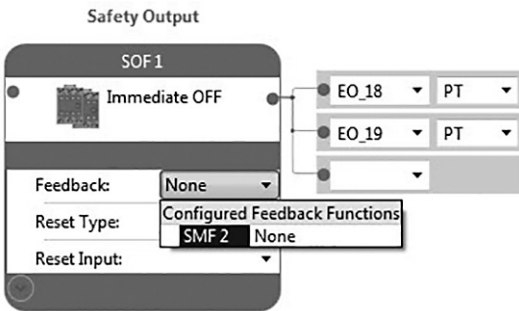


2. Suéltelo en el bloque superior de la columna Safety Output en el área de trabajo.

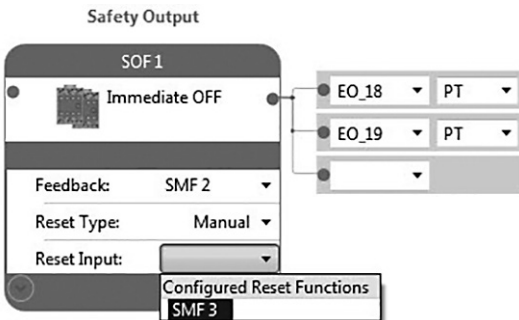


El software Connected Components Workbench asignará automáticamente los terminales de salidas EO_18 y EO_19. La opción de prueba de impulsos (PT) es el valor predeterminado para estos terminales. El valor predeterminado para la opción Reset Type es Manual. Deje estos ajustes configurados con sus valores predeterminados.

3. Seleccione SMF 2 en el menú desplegable Feedback.

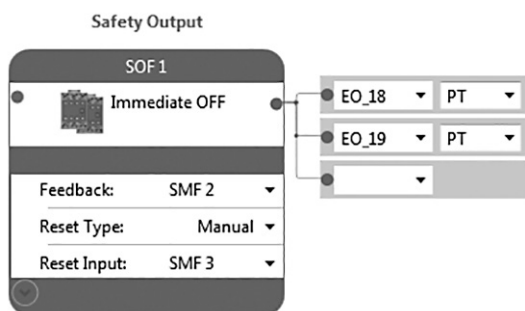


4. Seleccione SMF 3 en el menú desplegable Reset Input.





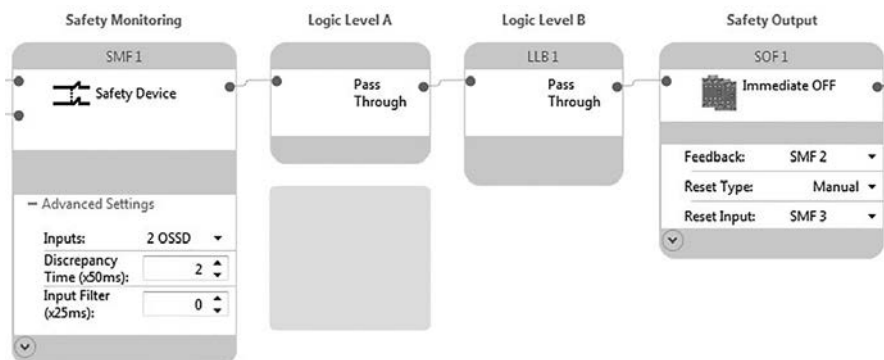
La configuración de la salida de seguridad se habrá completado.



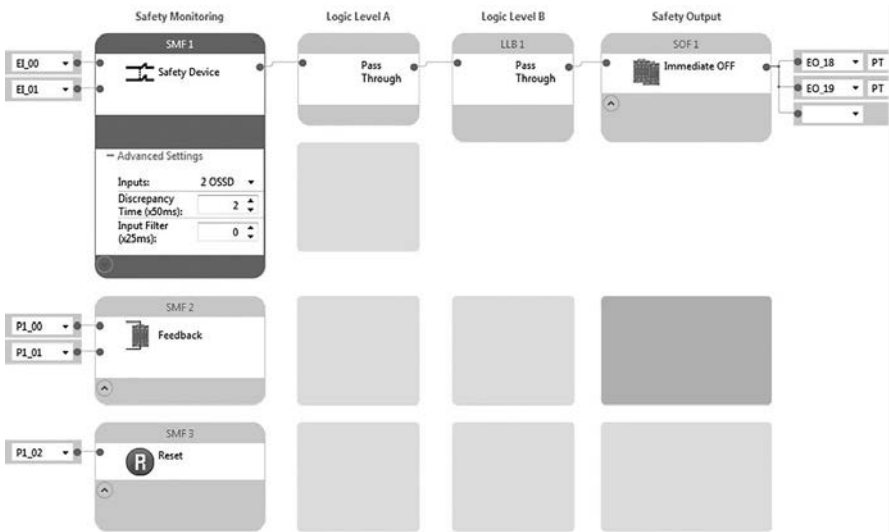
Configuración de la lógica

La sección Logic determina la respuesta de las salidas de seguridad a las entradas de control de seguridad. En este caso, la salida de seguridad sigue a la entrada de control de seguridad directamente.

1. Haga clic en el punto azul a la derecha del bloque de entrada SensaGuard Safety Monitoring. Se volverá gris.
2. Haga clic en el punto azul a la izquierda del bloque Safety Output para conectar la lógica.

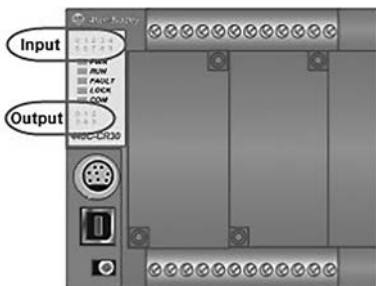


La lógica completada tendrá este aspecto.



Configuración de los indicadores de estado

El relé de seguridad configurable 440C-CR30 cuenta con diez leds indicadores de estado de entrada y seis leds indicadores de estado de salida que el usuario puede configurar. En muchos casos, pueden resultar muy útiles para instalar, poner en servicio, supervisar y resolver los problemas del sistema del relé de seguridad configurable 440C-CR30. No influyen en el funcionamiento del sistema en modo alguno y no es necesario configurarlos. No obstante, su configuración es sencilla y se recomienda utilizarlos.





1. Haga clic en Guardmaster_440C_CR30*.



2. Seleccione LED Configuration.

440C-CR30-22BBB

Verification ID: --
Remote:
Mode: --
Fault: --



LED	Type Filter	Value
0	Not Used	Not Used
1	Not Used	Not Used
2	Not Used	Not Used
3	Not Used	Not Used
4	Not Used	Not Used

3. En Type Filter, seleccione Terminal Status para LED 0.

LED	Type Filter	Value
0	Terminal Status	Not Used
1	Not Used	Not Used
2	Safety Monitoring Function Status	Not Used
3	Safety Output Function Status	Not Used
4	Not Used	Not Used
5	Not Used	Not Used

- Para LED 0, seleccione Terminal 00 en el menú desplegable Value. El indicador de estado LED 0 quedará configurado de modo que muestre el estado del terminal 00.

LED	Type Filter	Value
0	Terminal Status	Terminal 00
1	Not Used	Terminal 00
2	Not Used	Terminal 01
3	Not Used	Terminal 02
4	Not Used	Terminal 03
5	Not Used	Terminal 04

- Asigne los siguientes cuatro leds de entrada (1..4) del mismo modo. Los leds indicadores de estado de entrada quedarán configurados.

LED	Type Filter	Value	
0	Terminal Status	Terminal 00	
1	Terminal Status	Terminal 01	SensaGuard OSSD 1 Status
2	Safety Monitoring Function Status	SMF 1	SensaGuard OSSD 2 Status
3	Safety Monitoring Function Status	SMF 2	SensaGuard Status
4	Safety Monitoring Function Status	SMF 3	Feedback Status
5	Not Used	Not Used	Reset Status

- Asigne los tres leds de salida como se indica.

LED	Type Filter	Value	
0	Terminal Status	Terminal 18	Output Channel 1 Status
1	Terminal Status	Terminal 19	Output Channel 2 Status
2	Safety Output Function Status	SOF 1	Safety Output Status
3	Not Used	Not Used	
4	Not Used	Not Used	

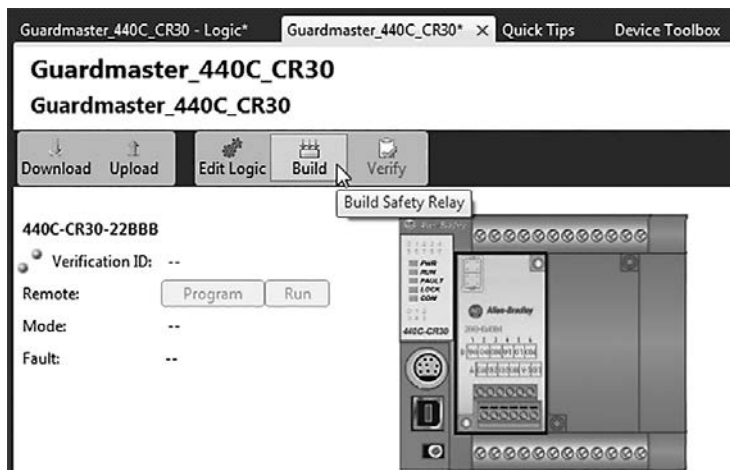
Confirmación de la validez de la generación de comandos

Siga estos pasos para confirmar la validez de la lógica con la función de generación de comandos del software Connected Components Workbench.

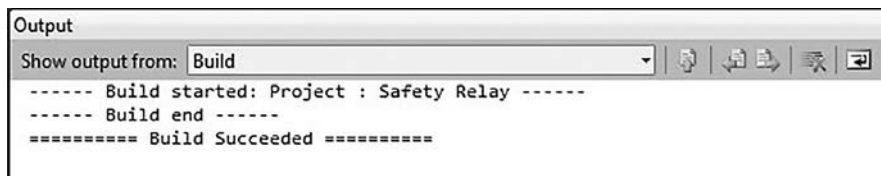
- Haga clic en Guardmaster_440C_CR30 en la barra por encima del área de trabajo.



2. Haga clic en Build.



El mensaje Build Succeeded le confirmará que la configuración es válida.



Si se detecta un error o una omisión durante una generación de comandos, aparecerá un mensaje donde se detallará el error para que pueda corregirlo. Una vez corregido el error, deberá llevar a cabo la generación de comandos de nuevo.

Almacenamiento y descarga del proyecto

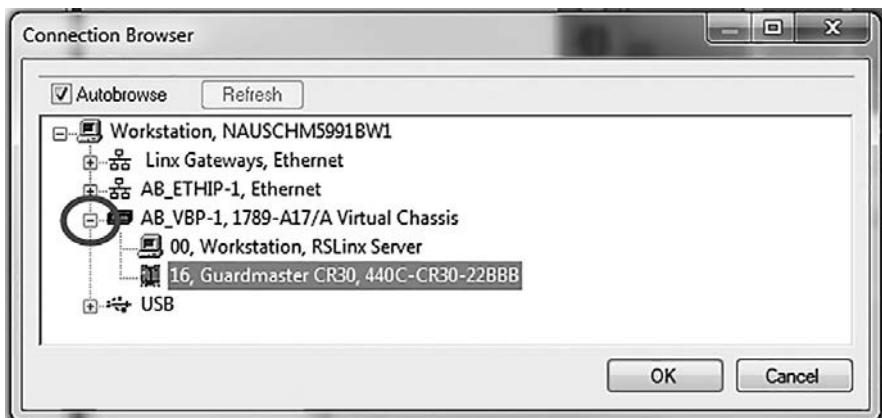
Siga estos pasos para guardar y descargar el proyecto.

1. En el menú File, seleccione Save as para guardar el proyecto.
2. En la ventana Project Organizer, haga doble clic en Guardmaster_440C_CR30 para abrir el área de trabajo.
3. Encienda el relé de seguridad 440C-CR30.
4. Conecte el cable USB al relé 440C-CR30.

5. Haga clic en Download.

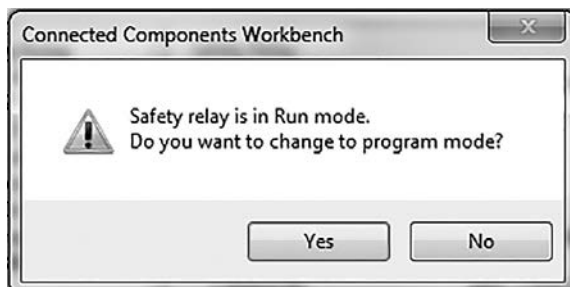


6. En Connection Browser, amplíe el elemento AB_VBP-1 Virtual Chassis y seleccione Guardmaster 440C-CR30-22BBB. Haga clic en OK.

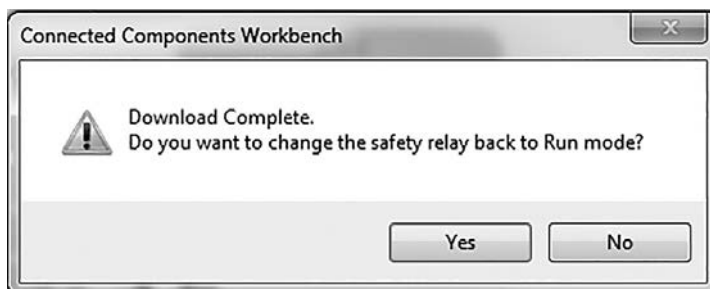




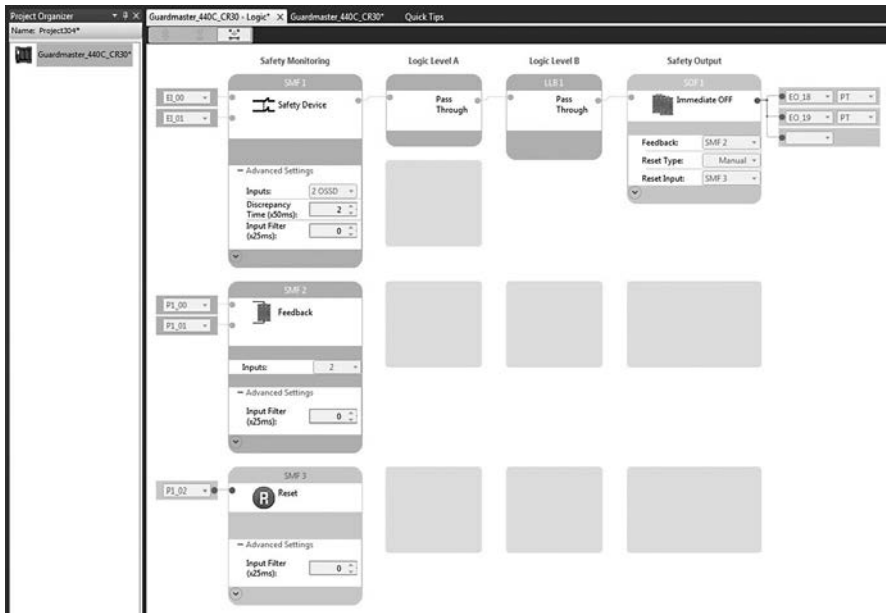
7. Haga clic en Yes para cambiar del modo de funcionamiento al de programación.



8. Cuando se haya completado la descarga, haga clic en Yes para cambiar del modo de programación al de funcionamiento.



9. Haga clic en Edit Logic para ver el diagnóstico en línea.



El verde indica que un bloque es verdadero o que una entrada o un terminal de salida está activo. El verde intermitente señala que una función de salida de seguridad está lista para su reinicio.

El modo de diagnóstico en línea del relé 440C-CR30 puede resultar muy útil durante el proceso de verificación.

10. Repase la información de las secciones Cálculo del nivel de rendimiento y Plan de verificación y validación antes de verificar la configuración

Cálculo del nivel de rendimiento

Si se implementa correctamente, esta función de parada relacionada con la seguridad puede alcanzar una clasificación de seguridad de categoría 4, nivel de rendimiento e (CAT. 4, PL_e), según ISO 13849-1: 2008, según la estimación de la herramienta de cálculo del nivel de rendimiento del software SISTEMA.

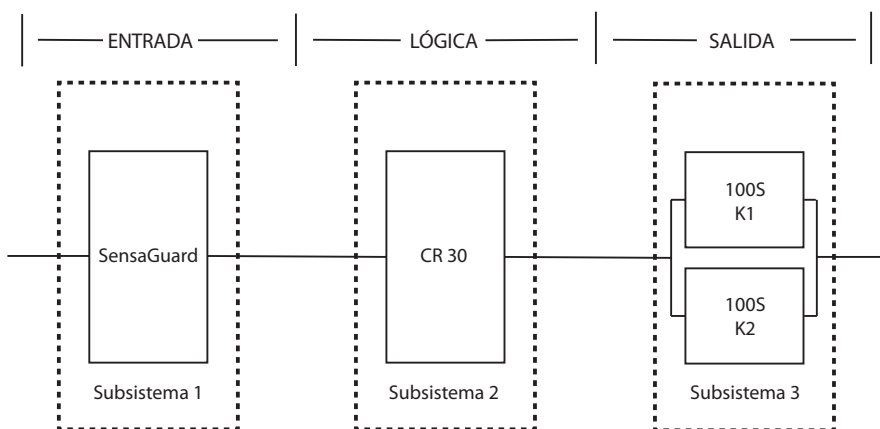
El nivel de rendimiento requerido (PL_r) mínimo determinado en la evaluación de riesgos para esta función de seguridad es PL_d.



Project		Safety functions				IFIA	
Status	Type	Name	Type	PLr	PL		
✓	SF	SensaGuard	Safety-related stop function initiated by safeguard	d	e		

Safety function		Subsystems										IFIA	
Status	Type	Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category				
✓	SB	Interlock Switch: SensaGuard	e	1.12E-9	not relevant	not relevant	not relevant	4	fulfilled				
✓	SB	CR 30	e	SE-8	not relevant	not relevant	not relevant	4	fulfilled				
✓	SB	100S Contactors	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled				

Esta parada relacionada con la seguridad iniciada por una función de seguridad de protección se puede modelar de este modo:



Puesto que se trata de dispositivos electromecánicos, los datos de los contactores de seguridad incluyen esta información:

- Tiempo medio antes de un fallo peligroso ($MTTF_d$)
- Cobertura de diagnóstico (DCavg)
- Fallo por causas comunes (CCF)

Las evaluaciones de seguridad funcional de los dispositivos electromecánicos incluyen estos aspectos:

- Frecuencia de funcionamiento
- Supervisión efectiva de sus fallos
- Especificación e instalación correctas

SISTEMA calcula el MTTFd con los datos B10d suministrados por los contactores, junto con la frecuencia de uso estimada que se haya introducido durante la creación del proyecto SISTEMA.

La DCavg (99%) de los contactores se selecciona en la tabla Dispositivo de salida de ISO 13849-1 Anexo E, control directo.

El valor CCF se genera mediante el proceso de puntuación señalado en el Anexo F de ISO 13849-1. El proceso de puntuación CCF completo debe llevarse a cabo cuando se implemente una aplicación de forma efectiva. Debe alcanzarse una puntuación mínima de 65.

Plan de verificación y validación

La verificación y la validación desempeñan un papel importante para evitar fallos durante el proceso de diseño y desarrollo del sistema de seguridad. ISO 13849-2 establece los requisitos de verificación y validación. La norma exige un plan documentado que confirme que se han cumplido todos los requisitos de seguridad funcional.

La verificación es un análisis del sistema de control de seguridad resultante. El nivel de rendimiento (PL) del sistema de control de seguridad se calcula para confirmar que el sistema cumple el nivel de rendimiento requerido (PLr) especificado. El software SISTEMA normalmente se utiliza para realizar cálculos y ayudar a cumplir los requisitos de ISO 13849-1.

La validación es una prueba funcional del sistema de control de seguridad cuyo objetivo es demostrar que el sistema cumple los requisitos de la función de seguridad especificados. El sistema de control de seguridad se prueba para confirmar que todas las salidas relacionadas con la seguridad responden correctamente a sus entradas de seguridad correspondientes. La prueba funcional incluye condiciones de funcionamiento normal además de inyección de fallos potenciales de los modos de fallo. Normalmente se utiliza una lista de verificación para documentar la validación del sistema de control de seguridad.

Antes de validar el sistema, confirme que el relé de seguridad configurable Guardmaster 440C-CR30 se haya cableado y configurado de conformidad con las instrucciones de instalación.



Lista de verificación y validación

Información general sobre la maquinaria	
Descripción	
Nombre de máquina/número de modelo	
Número de serie de la máquina	
Nombre del cliente	
Fecha de la prueba	
Nombre del responsable de la prueba	
Número de esquema	
Dispositivos de entrada	440N-Z21S16B
Relé de seguridad configurable	440C-CR30-22BBB
Variador de frecuencia variable	
Contactador de seguridad	100S-C23EJ23BC

Configuración del relé y cableado de seguridad			
Paso de la prueba	Verificación	Aprobación/rechazo	Cambios/modificaciones
1	Confirme que todas las especificaciones de los componentes sean adecuadas para la aplicación. Consulte los principios de seguridad básicos y los principios de seguridad de eficacia demostrada de ISO 13849-2.		
2	Inspeccione visualmente el circuito del relé de seguridad para confirmar que el cableado se ajuste al de los esquemas.		
3	Confirme que el relé de seguridad configurable 440C-CR30 tenga la configuración correcta y prevista.		

Verificación de funcionamiento normal: el sistema de seguridad responde correctamente a todas las entradas de interruptor de arranque, parada, reinicio, paro de emergencia y SensaGuard normales.

Paso de la prueba	Verificación	Aprobación/rechazo	Cambios/modificaciones
1	Confirme que no haya nadie en la zona protegida.		
2	Confirme que el movimiento peligroso se haya detenido.		
3	Confirme que la puerta esté cerrada.		
4	Conecte la alimentación eléctrica del sistema de seguridad.		
5	Confirme que los leds indicadores de estado de entrada Terminal 00, Terminal 01 y SMF1 del relé de seguridad 440C-CR30 estén iluminados en verde. Confirme que todos los indicadores de estado de salida estén apagados. Confirme que los leds indicadores de estado de encendido y funcionamiento estén iluminados en verde. Compruebe que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
6	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Confirme que los leds indicadores de estado de salida Terminal 18, Terminal 19 y SOF1 estén iluminados en verde. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
7	Confirme que el movimiento peligroso no se haya iniciado al encender el equipo.		

8	Presione y suelte el botón de arranque del variador. Confirme que se inicie el movimiento peligroso y que el equipo comience a funcionar.		
9	Pulse el botón de parada externo. El equipo debe detenerse de la forma normal configurada. El sistema de seguridad no debe responder.		
10	Presione y suelte el botón de arranque externo. Confirme que se inicie el movimiento peligroso y que el equipo comience a funcionar.		
11	Abra la puerta de resguardo. El sistema de seguridad debe activarse. El movimiento peligroso debe detenerse en menos de 0,7 segundos. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
12	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé de seguridad configurable 440C-CR30 no debe responder. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
13	Cierre la puerta de resguardo. La máquina no debe arrancar. El relé de seguridad 440C-CR30 no debe responder. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
14	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. La salida SOF1 del relé de seguridad 440C-CR30 debe activarse. El movimiento peligroso no debe iniciarse. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
15	Presione y suelte el botón de arranque externo. Confirme que el motor arranque y que el equipo comience a funcionar.		

Validación de una respuesta segura a un funcionamiento anómalo: el sistema de seguridad responde adecuadamente a todos los fallos previsible con el diagnóstico correspondiente.

Pruebas del relé de seguridad configurable 440C-CR30 y SensaGuard

Paso de la prueba	Verificación	Apro- bación/ rechazo	Cambios/ modificaciones
1	Mantenga la puerta de resguardo cerrada. Con el movimiento peligroso en marcha, retire el cable OSSD1 SensaGuard conectado al terminal E1_00 del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 debe activarse de inmediato. El led indicador de estado de fallo rojo en el relé debe parpadear. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
2	Vuelva a conectar el cable a E1_00. El relé de seguridad 440C-CR30 no debe responder. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 no debe responder. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
3	Abra y cierre la puerta de resguardo. El led de estado de fallo rojo debe estar apagado. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
4	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. La salida SOF 1 en el relé 440C-CR30 debe activarse. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		



5	Pulse el botón de arranque externo. La máquina debe empezar a funcionar. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench. Este paso es opcional en las siguientes pruebas de validación de SensaGuard (pasos 6 al 27).		
6	Con la puerta de resguardo cerrada, conecte OSSD 1 a 24 V DC. Después de aproximadamente 40 segundos, el interruptor SensaGuard se activará. El relé de seguridad 440C-CR30 se activa. El led indicador de estado de fallo rojo en el relé de seguridad 440C-CR30 debe parpadear. El indicador de estado en el interruptor SensaGuard parpadea en rojo. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
7	Desconecte OSSD 1 de 24 V DC. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
8	Desconecte y vuelva a conectar la alimentación eléctrica del interruptor SensaGuard. Aproximadamente cinco segundos después de que se haya restablecido la alimentación eléctrica del interruptor SensaGuard, su led de estado se quedará iluminado en verde fijo. El led indicador de estado de fallo rojo intermitente en el relé de seguridad 440C-CR30 se apaga. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
9	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
10	Conecte OSSD 1 a DC COM. El relé de seguridad 440C-CR30 se activa de inmediato. La columna luminosa roja Safe Stop se enciende. La columna luminosa ámbar Gate 1 se enciende. El led indicador de estado de fallo rojo en el relé de seguridad 440C-CR30 debe parpadear. El indicador de estado en el interruptor SensaGuard parpadea en rojo.		
11	Desconecte OSSD1 de DC COM. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden.		
12	Desconecte y vuelva a conectar la alimentación eléctrica del interruptor SensaGuard. Aproximadamente cinco segundos después de que se haya restablecido la alimentación eléctrica del interruptor SensaGuard, su led indicador de estado se quedará iluminado en verde fijo. La columna luminosa ámbar Gate 1 se apaga. La columna luminosa roja Safe Off permanece encendida. El led indicador de estado de fallo rojo intermitente en el relé de seguridad 440C-CR30 se apaga.		
13	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. La salida SOF 1 del relé de seguridad 440C-CR30 debe activar los contactores. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
14 a 27	Repita los pasos del 1 al 13 utilizando EI_01 en lugar de EI_00 y OSSD 2 en lugar de OSSD 1.		
28	Conecte OSSD 1 a OSSD 2 (terminal EI_00 al terminal EI_01). Después de aproximadamente 50 segundos, el interruptor SensaGuard se activará. El relé de seguridad 440C-CR30 se activa. El indicador de estado en el interruptor SensaGuard parpadea en rojo. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
29	Desconecte OSSD 1 de OSSD 2. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Ni el interruptor SensaGuard ni el relé de seguridad 440C-CR30 responden.		

30	Desconecte y vuelva a conectar la alimentación eléctrica del interruptor SensaGuard. Aproximadamente cinco segundos después de que se haya restablecido la alimentación eléctrica del interruptor SensaGuard, su led de estado se quedará iluminado en verde fijo. El led indicador de estado de fallo rojo intermitente en el relé de seguridad 440C-CR30 se apaga. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		
31	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. La columna luminosa roja Safe Stop debe estar apagada. La salida SOF1 en el relé de seguridad 440C-CR30 debe activar los contactores. Compruebe que todos los leds indicadores de estado funcionen correctamente y que el estado del relé de seguridad 440C-CR30 sea el correcto con el software Connected Components Workbench.		

Validación de una respuesta segura a un funcionamiento anómalo: el sistema de seguridad responda adecuadamente a todos los fallos previsibles con el diagnóstico correspondiente.

Contactora – Pruebas del relé de seguridad configurable 440C-CR30

Paso de la prueba	Verificación	Apro- bación/ rechazo	Cambios/ modificaciones
1	Con la máquina en funcionamiento, interrumpa la conexión entre el terminal EO_18 del relé de seguridad configurable 440C-CR30 y el terminal A1 de la bobina K1. El movimiento peligroso debe detenerse por inercia.		
2	Pulse el botón de parada externo. Restablezca la conexión. Pulse el botón de arranque externo para reanudar el movimiento peligroso.		
3	Con el movimiento peligroso en funcionamiento, conecte el terminal A1 de la bobina K1 a 24 V CC. Tras una espera de aproximadamente 18 segundos, el relé de seguridad 440C-CR30 debe activarse. K2 debe desactivarse. El movimiento peligroso se detiene por inercia. El led indicador de estado de fallo rojo en el relé de seguridad 440C-CR30 está encendido.		
4	Desconecte el terminal A1 de la bobina K1 de 24V CC. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 no debe responder.		
5	Desconecte y vuelva a conectar la alimentación eléctrica del relé de seguridad 440C-CR30. Responde. El led indicador de estado de fallo en el relé de seguridad 440C-CR30 está apagado.		
6	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Pulse el botón de arranque externo. El movimiento peligroso debe reanudarse.		
7	Con la máquina en funcionamiento, cortocircuite el terminal A1 de la bobina K1 de DC COM. El relé de seguridad 440C-CR30 debe activarse. El led indicador de estado de fallo rojo en el relé de seguridad 440C-CR30 está encendido.		
8	Desconecte el terminal A1 de la bobina K1 de DC COM. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 no debe responder.		
9	Desconecte y vuelva a conectar la alimentación eléctrica del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 responde. El led indicador de estado de fallo en el relé de seguridad 440C-CR30 está apagado.		
10	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Pulse el botón de arranque externo. El movimiento peligroso se reanuda.		
11 a 21	Repita los pasos del 1 al 10 utilizando EO_19 en lugar de EO_18, y K2 en lugar de K1.		
22	Conecte el terminal A1 de K1 al terminal A1 de K2. Tras una espera de aproximadamente 18 segundos, el relé de seguridad 440C-CR30 debe activarse. El movimiento peligroso se detiene por inercia. El led indicador de estado de fallo rojo en el relé de seguridad 440C-CR30 está encendido.		



23	Desconecte el terminal A1 de K1 del terminal A1 de K2. Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé de seguridad 440C-CR30 no debe responder.		
24	Desconecte y vuelva a conectar la alimentación eléctrica del relé de seguridad 440C-CR30. Responde. El led indicador de estado de fallo en el relé de seguridad 440C-CR30 está apagado.		
25	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. Pulse el botón de arranque externo. El movimiento peligroso debe reanudarse.		

Validación de una respuesta segura a un funcionamiento anómalo: el sistema de seguridad responde adecuadamente a todos los fallos previsibles con el diagnóstico correspondiente.

Retroalimentación del contactor – Pruebas del relé de seguridad configurable 440C-CR30

Paso de la prueba	Verificación	Aprobación/ rechazo	Cambios/ modificaciones
1	Con la máquina en funcionamiento, retire la conexión de retroalimentación K1 del terminal P1_00. La máquina debe seguir funcionando.		
2	Abra la puerta de resguardo. El sistema de seguridad debe activarse. El movimiento peligroso debe detenerse en menos de 0,7 segundos. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé 440C-CR30 sea el correcto con el software Connected Components Workbench.		
3	Cierre la puerta de resguardo. La máquina no debe arrancar. El relé 440C-CR30 no debe responder. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé 440C-CR30 sea el correcto con el software Connected Components Workbench.		
4	Pulse y suelte el botón de reinicio del relé de seguridad 440C-CR30. El relé 440C-CR30 no debe responder. Compruebe que los leds indicadores de estado funcionen correctamente y que el estado del relé 440C-CR30 sea el correcto con el software Connected Components Workbench.		
5	Restablezca la conexión en P1_00. Desconecte y vuelva a conectar la alimentación eléctrica del relé 440C-CR30. Pulse el botón de reinicio del relé 440C-CR30. Las salidas del relé 440C-CR30 deben activarse. Presione y suelte el botón de arranque externo. Confirme que el motor arranque y que el equipo comience a funcionar.		
6	Repita los pasos del 1 al 5 con la conexión de retroalimentación K2 en el terminal P1_01.		

Verificación de la configuración

El sistema debe comprobar la configuración de cada aplicación por separado con el comando Verify. Si no se verifica la configuración del relé de seguridad 440C-CR30, presentará un fallo después de 24 horas de funcionamiento.

ATENCIÓN: El proceso de verificación debe documentarse en el archivo técnico del sistema de seguridad.

Siga estos pasos para descargar y comprobar la configuración.

1. Compruebe que el relé 440C-CR30 esté encendido y conectado a su estación de trabajo a través del cable USB.
2. Confirme que en la esquina superior derecha de la pestaña Connected Components Workbench Project se indique la conexión del relé 440C-CR30. De lo contrario, haga clic en Connect to Device para establecer la conexión de software.



3. Haga clic en Verify.





4. Responda a todas las preguntas y marque cada casilla si se ha completado la operación. Haga clic en Generate.

Connected Components Workbench


- Have you followed installation instructions and precautions to conform to applicable safety standards?
- Have you verified that the electrical specifications of the sensor and inputs are compatible?
- Have you verified that the electrical specifications of the outputs and the actuators are compatible?
- Have you calculated the system's safety response time for each safety chain?
- Is the system response time in proper relation to the process tolerance time?
- Have probability (PFD/PFH/PLx) values been calculated according to the system's configuration?
- Have you performed all appropriate functional verification tests on the system?

Safety Verification ID:

IMPORTANTE: Todas las casillas deben estar marcadas para que se genere el identificador de verificación.

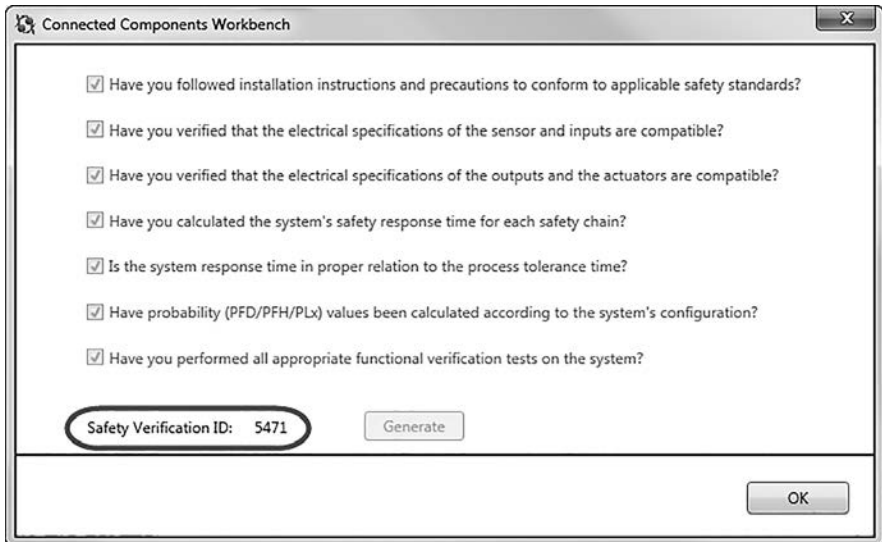
6. Haga clic en Yes para proceder a la verificación.

Connected Components Workbench

 Performing a Safety Verify will change the safety relay to Program mode.
Proceed with the Safety Verify?

7. Haga clic en Yes para cambiar al modo de funcionamiento.

8. Registre el identificador de verificación de seguridad en la documentación de la máquina.



Este proceso informa al relé 440C-CR30 de que las pruebas funcionales y la verificación del sistema se han completado. El identificador de verificación único se puede utilizar para determinar si se han realizado cambios en un archivo de configuración. Cualquier cambio en la configuración eliminará el identificador de verificación de seguridad. Las acciones de verificación posteriores generarán un identificador de verificación distinto. El identificador de verificación de seguridad únicamente se muestra en el software Connected Components Workbench durante la conexión con el relé 440C-CR30.



Capítulo 11: Productos, herramientas y servicios

Descripción general

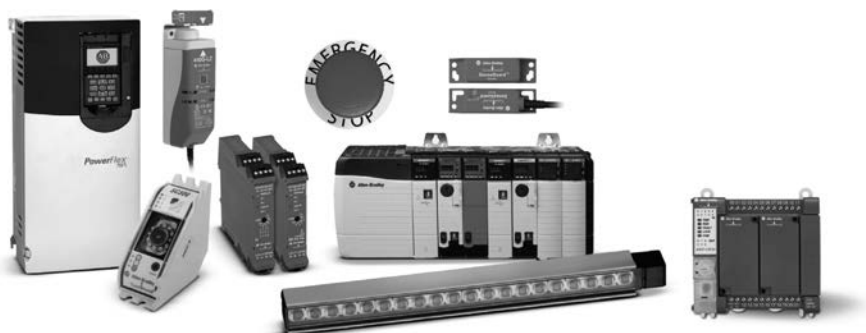
Rockwell Automation es un proveedor global líder en soluciones de alimentación eléctrica, control e información industrial que lleva más de 100 años ayudando a sus clientes en diversos sectores. Una parte de su cartera de automatización industrial la conforma un completo conjunto de tecnologías, herramientas y servicios de seguridad de máquinas.

Productos y tecnologías para sus aplicaciones

Rockwell Automation cuenta con la más amplia cartera entre los proveedores de soluciones de seguridad de máquinas y puede hacerse cargo de las tres partes de un sistema de seguridad (dispositivo de entrada, control lógico y elemento eléctrico final).



Los productos y tecnologías disponibles incluyen:



Productos, herramientas y servicios

Dispositivos de entrada de seguridad

- Dispositivos de seguridad de detección de presencia**
 Los dispositivos de seguridad de detección de presencia detectan la ubicación de objetos o personas cerca de zonas peligrosas. Éstas incluyen: barreras ópticas de seguridad, escáneres láser de seguridad, sensores de seguridad de detección de la mano, bordes y alfombras sensible a la presión
- Interruptores de seguridad con enclavamiento**
 Los interruptores de seguridad se han diseñado y fabricado de conformidad con los estándares globales de alta fiabilidad, estabilidad y calidad. Los interruptores de seguridad incluyen interruptores de final de carrera y enclavamiento e interruptores de paro de emergencia.
- Dispositivos de parada de emergencia y disparo**
 Los interruptores de paro de emergencia incluyen un conjunto de botones pulsadores de tipo hongo con contactos con guía positiva. Los interruptores habilitantes y los interruptores accionados por cable proporcionan la función de emergencia en una aplicación o están cableados para permitir el movimiento del operador dentro de la aplicación de seguridad.
- Interfaz del operador**
 Los dispositivos de interfaz del operador permiten al operador interactuar con la aplicación y ofrecen funciones de seguridad específicas adicionales.

Controladores lógicos de seguridad

- Relés de seguridad (monofuncionales o configurables)**
 Los relés de seguridad comprueban y supervisan un sistema de seguridad y permiten a la máquina iniciar o ejecutar comandos para detener el equipo. Los relés de seguridad monofuncionales son más económicos para máquinas de menor tamaño que requieren un dispositivo lógico específico para completar la función de seguridad. Se prefieren relés de seguridad para monitorización modulares y configurables cuando se requiere un número grande y diverso de dispositivos de protección y control mínimo de zona.
- Controladores de seguridad integrados**
 Los PLC de seguridad ofrecen las ventajas de los sistemas de PLC tradicionales para las aplicaciones de seguridad, sustituyendo los relés de lógica cableada que se necesitan normalmente para llevar los procesos automatizados a un estado de seguridad. Los PLC de seguridad permiten albergar tanto programas estándar como relacionados con la seguridad en un único chasis de controlador, lo que proporciona una gran flexibilidad en la programación, además de un entorno familiar y de utilización sencilla para los programadores. Las soluciones de controladores de seguridad ofrecen un control abierto e integrado que garantiza la seguridad de su maquinaria y protege sus activos.



- **Dispositivos E/S de seguridad**

Los productos de seguridad Guard I/O™ ofrecen todas las ventajas propias de las E/S distribuidas tradicionales, pero han sido diseñados para los sistemas de seguridad. Reducen los costes de cableado y el tiempo de puesta en marcha de las máquinas y celdas y se encuentran disponibles con diversas funciones para aplicaciones tanto dentro del armario como en la máquina.

Accionadores de seguridad

- **Arrancadores y contactores de seguridad**

El controlador de motores distribuido ArmorStart® ofrece una funcionalidad de seguridad de categoría 4 al tiempo que proporciona una solución de seguridad integrada en su instalación de seguridad DeviceNet™ On-Machine™. Los relés de control y los contactores de seguridad IEC ayudan a proteger a los trabajadores de los arranques de los equipos accidentales y de las pérdidas de la función de seguridad.

- **Variadores de CA PowerFlex®**

Los variadores PowerFlex se encuentran disponibles con funciones de seguridad. Los variadores de CA PowerFlex 525 incluyen desconexión de par segura integrada como característica estándar. La desconexión de par segura es una característica opcional para los variadores de CA PowerFlex de la serie 40P, 70, 700H, 700S y 750, que también son compatibles con la función de seguridad de monitorización de velocidad.

- **Controles de movimiento integrado Kinetix®**

Todos los servovariadores Kinetix 300, 6000, 6200, 6500 y 7000 cuentan con funcionalidad de seguridad integrada. Con la desconexión de par segura, una salida del variador se inhabilita para eliminar el par del motor sin desconectar la alimentación eléctrica de toda de la máquina. La función de seguridad de monitorización de velocidad permite a los usuarios reducir y controlar la velocidad de la aplicación con el fin de ayudar a los operadores a realizar algunos tipos de trabajo con seguridad sin necesidades de detener la máquina por completo.

Sistemas de conexión/redes

- **Sistemas de conexión “Quick Connect”**

Los t-port/bifurcadores, cajas de distribución y clavijas cortocircuitadoras de seguridad Guardmaster® son componentes de un sistema de desconexión rápida específico para la seguridad de máquinas.

- **GuardLink™**

GuardLink es un protocolo de comunicaciones basado en la seguridad que utiliza cableado estándar en una topología “troncal y de derivación” con conexiones “plug-and-play”. Permite la comunicación de los dispositivos de seguridad con fines de diagnóstico y control, como los comandos de reinicio y bloqueo a distancia en un único cable. Se pueden conectar hasta 32 dispositivos en un tramo de cable

Productos, herramientas y servicios

de hasta 1000 metros. Los dispositivos de seguridad Allen-Bradley con tecnología GuardLink permiten acceso a la información del sistema de seguridad a través de EtherNet/IP. GuardLink puede contribuir a simplificar la configuración del sistema, reducir el cableado e incrementar la información de diagnóstico con fines de mantenimiento y uso.

- **Seguridad a través de EtherNet/IP**

La red EtherNet/IP™ proporciona sistemas de red a nivel de toda la planta con tecnologías de conexión en red estándar de la industria abierta. Ofrece información y control en tiempo real en aplicaciones discretas, de procesos continuos, de lotes, de seguridad, de accionamiento, de movimiento y de alta disponibilidad. Las redes EtherNet/IP conectan dispositivos como los arrancadores de motor y los sensores a controladores y dispositivos HMI, así como al sistema global de la empresa. Admiten comunicaciones industriales y no industriales en una única infraestructura de red común.

Herramientas de ayuda

Una amplia gama de herramientas para lograr el cumplimiento normativo en materia de seguridad, reducir el riesgo de lesiones y mejorar la productividad.

Safety Automation Builder

Safety Automation Builder es una herramienta de software GRATUITA que ayuda a simplificar el diseño y la validación de los sistemas de seguridad de máquinas, reduciendo el tiempo y los costes. La integración con el software de evaluación de riesgos RASWin proporciona a los usuarios una gestión coherente, fiable y documentada del ciclo de vida de la seguridad funcional. Safety Automation Builder simplifica el diseño del sistema de seguridad, facilitando el cumplimiento normativo y contribuyendo a la reducción de costes a través de la orientación de los usuarios en el desarrollo de los sistemas de seguridad, incluido su diseño, la selección de productos y el análisis de seguridad para ayudar a satisfacer los requisitos de nivel de rendimiento de la seguridad de las máquinas establecidos en la norma global (EN) ISO 13849-1.

RASWin

El software RASWin ayuda a los usuarios a gestionar la progresión a lo largo del ciclo de vida de la seguridad funcional, organizando la información procedente de cada paso del proceso y la validación de la maquinaria. RASWin vincula los pasos del ciclo de vida de la seguridad para evitar fallos sistemáticos, incluidas las especificaciones de la función de seguridad, la asignación de los requisitos de nivel de rendimiento (PLr) y el cálculo del PLr, la validación del circuito de seguridad y la documentación.

Calculadora del nivel de rendimiento SISTEMA

La herramienta SISTEMA, desarrollada por el Instituto para la Seguridad y Salud Ocupacional del Seguro de Accidentes Sociales de Alemania (IFA), automatiza el cálculo del nivel de rendimiento alcanzado por los componentes relacionados



Sistemas de seguridad para maquinaria industrial

con la seguridad del sistema de control de una máquina según (EN) ISO 13849-1. Los datos para los productos de seguridad de maquinaria de Rockwell Automation ahora se encuentran disponibles en un formato de archivo de biblioteca para su uso con la herramienta de cálculo SISTEMA. La combinación de ambos elementos proporciona a los diseñadores de maquinaria y sistemas una completa ayuda que les ahorra tiempo en la evaluación de la seguridad según (EN) ISO 13849-1. Una función de exportación desde Safety Automation Builder permite importar fácilmente el diseño del sistema de seguridad a SISTEMA para recibir una verificación de otros fabricantes del nivel de rendimiento requerido.

Funciones de seguridad prediseñadas para máquinas

Las funciones de seguridad de maquinaria requieren múltiples elementos, incluido un dispositivo de entrada, un dispositivo lógico y un dispositivo de salida. Juntos, estos elementos proporcionan un nivel de protección calculado por el nivel de rendimiento señalado en (EN) ISO 13849-1. Rockwell Automation ha elaborado muchos documentos sobre funciones de seguridad, cada uno de los cuales proporciona orientación para una función de seguridad específica en función de los requisitos funcionales, la selección del equipo y el requisito de nivel de rendimiento. Estos incluyen implementación y cableado, configuración, plan de verificación y validación y cálculo del nivel de rendimiento.

Herramienta Safety Maturity Index

Safety Maturity Index™ es una completa herramienta de evaluación de las actuaciones en materia de cultura de la seguridad, procesos y procedimientos de cumplimiento normativo e inversiones de capital en tecnologías de la seguridad. Ayuda a las empresas a conocer su nivel de rendimiento actual y las medidas que pueden adoptar para aumentar la seguridad y la rentabilidad.

Unos servicios y experiencia que le serán de ayuda

Como principal proveedor mundial de soluciones de seguridad industrial, Rockwell Automation puede ayudarle a reducir las lesiones y los costes al tiempo que incrementa la productividad en todas las fases del ciclo de vida de la seguridad.

Nuestros experimentados trabajadores, cualificados en el ámbito de la seguridad (muchos de los cuales poseen certificaciones de seguridad de maquinaria TÜV Rheinland), prestan los servicios de seguridad. La plantilla de Rockwell Automation incluye técnicos, ingenieros y expertos en seguridad funcional con certificación TÜV que ayudan a nuestros clientes a lo largo de todo el ciclo de vida de la seguridad.

El ciclo de vida de la seguridad es un proceso claramente definido que ayuda a maximizar la productividad y a aumentar la seguridad mediante la identificación de las medidas necesarias para evaluar y mitigar los riesgos de la maquinaria. Le explicamos en qué consiste el ciclo de vida de la seguridad en este documento disponible para su descarga.

Productos, herramientas y servicios

Algunos de los servicios disponibles son:

- **Evaluaciones de seguridad**
Servicios que ayudan a evaluar el riesgo en la planta y que respaldan una toma de decisiones bien informada para aumentar la seguridad de los trabajadores y los equipos.
- **Servicios de diseño**
Diseño del circuito exhaustivo, correcta aplicación de los dispositivos y revisiones del diseño para aumentar el nivel de seguridad global.
- **Servicios de validación e instalación**
Comprobación de que los sistemas funcionen dentro de los parámetros y estándares definidos.
- **Formación en seguridad**
Exhaustivos programas de formación impartida por los mejores expertos del sector.
- **Servicios personalizados**
Compatibles con las configuraciones, plataformas, programas, tecnologías y aplicaciones específicas del cliente.

¿Por qué elegir Rockwell Automation?

La seguridad integrada junto con la automatización puede aumentar la productividad en muchas fases del proceso de producción, desde el diseño y prueba de los equipos hasta su modificación o desmantelamiento, pasando por la instalación, la puesta en marcha inicial, el uso y el mantenimiento. Todas las fases se pueden optimizar si se aplican soluciones de seguridad correctamente.

Como líder mundial en seguridad y automatización industrial e innovador tecnológico, Rockwell Automation disfruta de una posición privilegiada para ayudarle a desarrollar soluciones de fabricación más eficientes, seguras y productivas.

Rockwell Automation, después de muchos años de experiencia en el campo de la automatización y la seguridad, cuenta con un vasto conocimiento de las aplicaciones y pone en práctica los principios de las normas sobre seguridad más recientes, como ISO 12000, (EN) ISO 13849-1 e IEC 62061, lo que nos permite ayudarle con la selección, integración, formación y asistencia técnica de las soluciones de seguridad eléctrica, de los procesos y de las máquinas.



www.rockwellautomation.com

Oficinas corporativas de soluciones de potencia, control e información

Américas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europa/Medio Oriente/África: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia-Pacífico: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Argentina: Rockwell Automation S.A., Alem 1050, 5° Piso, CP 1001AAS, Capital Federal, Buenos Aires, Tel.: (54) 11.5554.4000, Fax: (54) 11.5554.4040, www.rockwellautomation.com.ar

Chile: Rockwell Automation Chile S.A., Luis Thayer Ojeda 166, Piso 6, Providencia, Santiago, Tel.: (56) 2.290.0700, Fax: (56) 2.290.0707, www.rockwellautomation.cl

Colombia: Rockwell Automation S.A., Edif. North Point, Carrera 7 N° 156 - 78 Piso 18, PBX: (57) 1.649.96.00 Fax: (57) 649.96.15, www.rockwellautomation.com.co

España: Rockwell Automation S.A., C/ Josep Pla, 101-105, 08019 Barcelona, Tel.: (34) 932.959.000, Fax: (34) 932.959.001, www.rockwellautomation.es

México: Rockwell Automation S.A. de C.V., Bosques de Cierulos N° 160, Col. Bosques de Las Lomas, C.P. 11700 México, D.F., Tel.: (52) 55.5246.2000, Fax: (52) 55.5251.1169, www.rockwellautomation.com.mx

Perú: Rockwell Automation S.A., Av Victor Andrés Belaunde N°147, Torre 12, Of. 102 - San Isidro Lima, Perú, Tel: (511) 441.59.00, Fax: (511) 222.29.87, www.rockwellautomation.com.pe

Puerto Rico: Rockwell Automation Inc., Calle 1, Metro Office # 6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, Fax: (1) 787.706.3939, www.rockwellautomation.com.pr

Venezuela: Rockwell Automation S.A., Edif. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, Fax: (58) 212.943.3955, www.rockwellautomation.com.ve