Manual de seguridad en máquinas

Schneider Electric

Sencillamente,
una **única marca** y un único
proveedor de **ahorro energético**

Schneider Electric

Nuestra oferta de productos, soluciones y servicios.

+

El asesoramiento profesional de nuestros expertos.

=

Hasta el **30%** de **ahorro energético**

El sello de la **Eficiencia Energética**

Nuestros sellos de EE le ayudan a tomar la decisión correcta

El sello de soluciones de Eficiencia Energética indica el ahorro potencial que puede esperar de cada solución.

Este símbolo distingue los productos básicos para la Eficiencia Energética.

Consulte la Guía de Soluciones de Eficiencia Energética en:

www.schneiderelectric.es/eficienciaenergetica

Manual de seguridad en máquinas

Introducción

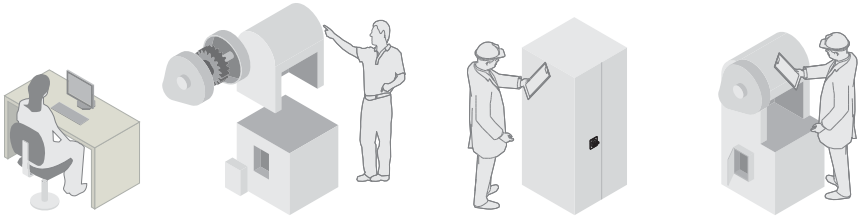
Existen diferentes guías sobre legislación de seguridad en maquinarias que tienden a presentar una visión distorsionada de los requisitos de dicha legislación.

La finalidad de este manual es aportar información actualizada y objetiva para ayudar a los fabricantes de máquinas y usuarios para que puedan ofrecer a las personas que trabajan con éstas, que sean seguras, legales y eficientes. No pretende ser una guía exhaustiva sobre el cumplimiento de la legislación en seguridad, ni sustituir a las normativas pertinentes, sino servir de guía a través de los pasos lógicos e indicar las fuentes de información relevantes.

Importancia de la seguridad

Además de la obligación moral de evitar dañar a cualquier persona, existen leyes que exigen que las máquinas sean seguras, así como importantes motivos económicos para evitar accidentes.

La seguridad debe tenerse en cuenta desde la fase de diseño y estar presente en todas las etapas del ciclo de vida de la máquina: el diseño, la fabricación, la instalación, el ajuste, el funcionamiento, el mantenimiento y su posterior desmontaje y eliminación.



Diseño/fabricación | Instalación | Ajuste/funcionamiento | Mantenimiento

Nuevas máquinas - la Directiva de Máquinas

El objetivo principal de la Directiva de Máquinas 2006/42/CE, que entró en vigor el 29 de diciembre de 2009, consiste en obligar a los fabricantes a que garanticen un nivel mínimo de seguridad para las máquinas y los equipos vendidos en la Unión Europea.

Las máquinas deberán cumplir con los requisitos esenciales de salud y seguridad enumerados en el Anexo I de la Directiva, con lo que se establece un nivel mínimo común de protección en toda el área económica europea.

Los fabricantes de máquinas o sus representantes autorizados dentro de la UE deberán asegurarse de que la máquina cumple con las directivas, de que se presente el Expediente técnico si así lo solicitan las autoridades pertinentes, de que la máquina presente el Marcado CE y de que se firme una Declaración de Conformidad antes de introducir la máquina al mercado dentro de la UE.

Máquinas existentes - la Directiva sobre equipos de trabajo

El usuario debe cumplir las obligaciones definidas por la Directiva sobre uso de equipos de trabajo 89/655/CEE, que en la mayoría de los casos puede cumplirse al utilizar la maquinaria que cumple con la normativa pertinente.

Se aplica al suministro de todos los equipos de trabajo, incluido el equipo móvil y de elevación, en todos los lugares de trabajo y en todas las situaciones laborales.

Estas obligaciones requieren que todos los equipos sean los indicados para su uso y que se inspeccionen y mantengan cuanto sea necesario para garantizar que lo sigan siendo.

El coste de los accidentes

Algunos de los costes son obvios, como la baja por enfermedad de los empleados lesionados, mientras que otros costes son más difíciles de identificar. La autoridad ejecutiva de salud y seguridad en el Reino Unido (HSE) expuso un ejemplo de un accidente con una máquina taladradora por el que la empresa incurrió en unos costes de 45.000 libras (≈ 51.300 €) (HSE INDG355). Sin embargo, esto no incluye algunos de los costes menos obvios y que en ocasiones pueden ascender al doble de la cifra inicial. En un accidente analizado por Schneider Electric en el Reino Unido, cuyo resultado fue una lesión reversible del trabajador, costó al empresario alrededor de 90.000 libras (≈ 102.600 €), de las cuales, el seguro sólo cubría 37.000 libras (≈ 42.200 €).
El impacto financiero total puede incluir un aumento en las primas del seguro, pérdida de la producción, pérdida de clientes e incluso pérdida de reputación.

Algunas medidas para reducir los riesgos pueden aumentar la productividad; por ejemplo, el uso de barreras inmateriales para proteger los puntos de acceso de las máquinas puede facilitar el acceso para la carga y la descarga; con la colocación de dispositivos de aislamiento se pueden desactivar ciertas partes de la máquina para repararlas mientras el resto de las partes sigue productiva.

Las normativas se aplican a todos los empresarios, a los trabajadores autónomos y a cualquier persona que tenga control en el suministro de equipos de trabajo.

Marco legal

Directiva CE:

- Instrumento legal para armonizar la legislación de los Estados miembros europeos.
- Define los requisitos esenciales de salud y seguridad.
- Los conceptos se transponen en las leyes nacionales (ley, decreto, orden, normativas).

Norma:

- Una norma es una especificación técnica aprobada por un organismo de normalización reconocido para su aplicación continua o repetida, cuyo cumplimiento no es obligatorio.

Norma armonizada:

- Una norma se convierte en armonizada cuando se publica en todos los Estados miembros.

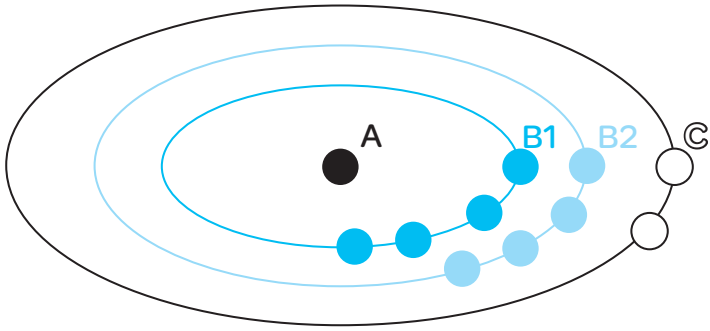
Presunción de conformidad:

Cuando un producto cumple una norma europea armonizada, cuya referencia se publica en el Diario Oficial de la Unión Europea para una Directiva específica, y que cubre uno o más de los requisitos de seguridad esenciales, se supone que el producto cumple con esos requisitos de seguridad esenciales de la Directiva. Se puede acceder a una lista de estas normas en la dirección http://www.newapproach.org/Directives/DirectiveList.asp.

Es necesario asegurar el cumplimiento del resto de requisitos esenciales de salud y seguridad, así como de aquellos para los que se da una Presunción de conformidad por el uso de una norma específica.

Normas de tipo A, B y C:

Las normas europeas de Seguridad para Máquinas forman la siguiente estructura:



Normas de tipo A

- (Normas básicas de seguridad) aportan conceptos básicos, principios de diseño y aspectos generales que pueden aplicarse a todas las máquinas;

Normas de tipo B

- (Normas de seguridad genéricas) que tratan sobre un aspecto de la seguridad o un tipo de dispositivo de seguridad que puede utilizarse en una amplia gama de máquinas:
  - Normas de tipo B1 sobre aspectos particulares de la seguridad (por ejemplo, distancias de seguridad, temperatura de superficies, ruido);
  - Normas de tipo B2 sobre dispositivos de seguridad (por ejemplo, mando bimanual, dispositivos de enclavamiento, dispositivos de protección sensibles a la presión, protectores);

Normas de tipo C

- (Normas de seguridad para máquinas) relativas a requisitos de seguridad específicos para una máquina o un grupo de máquinas determinado.

Si una norma de tipo C se desvía de una o más disposiciones tratadas en una norma de tipo A o en una norma de tipo B, la norma de tipo C tiene prioridad.

Algunos ejemplos de estos tipos de normas son los siguientes:		
EN ISO 12100-1	A	Seguridad de las máquinas - Conceptos básicos, principios generales para el diseño. Parte 1: Terminología básica, metodología.
EN ISO 12100-2	A	Seguridad de las máquinas - Conceptos básicos, principios generales para el diseño. Parte 2: Principios técnicos.
EN ISO 14121-1	A	Seguridad de las máquinas. Evaluación del riesgo. Parte 1: Principios.
EN 574	B	Dispositivos de mando a dos manos.
EN ISO 13850	B	Parada de emergencia - Principios de diseño.
EN IEC 62061	B	Seguridad funcional de sistemas de control electrónicos programables, electrónicos y eléctricos relativos a la seguridad.
EN ISO 13849-1	B	Seguridad de maquinaria - Partes de los sistemas de mando relativos a la seguridad. Parte 1 Principios generales para el diseño.
EN 349	B	Distancias mínimas para evitar el aplastamiento de partes del cuerpo humano.
EN SO 13857	B	Seguridad de maquinaria - Distancias de seguridad para evitar que las extremidades inferiores y superiores lleguen a zonas de peligro.
EN IEC 60204-1	B	Seguridad de maquinaria - Equipo eléctrico de máquinas - Parte 1: requisitos generales.
EN 999 ISO 13855	B	Posicionamiento de los equipos de protección en función de las velocidades de aproximación de partes del cuerpo humano.
EN 1088 ISO 14119	B	Dispositivos de enclavamiento asociados a resguardos - Principios de diseño y selección.
EN IEC 61496-1	B	Equipos de protección electrosensibles Parte 1: Requisitos generales y ensayos.
EN IEC 60947-5-5	B	Aparamenta de baja tensión - Parte 5-5: Aparatos y elementos de conmutación para circuitos de mando - Aparato de parada de emergencia eléctrica con enclavamiento mecánico.
EN 842	B	Señales visuales de peligro - Requisitos generales, diseño y ensayos.
EN 1037	B	Prevención de una puesta en en marcha intempestiva.
EN 953	B	Resguardos - Requisitos generales para el diseño y construcción de resguardos fijos y móviles.
EN 201	C	Maquinaria de plásticos y caucho - Máquinas de moldeo por inyección - Requisitos de seguridad.
EN 692	C	Máquinas-Herramienta - Prensas mecánicas - Requisitos de seguridad.
EN 693	C	Máquinas-Herramienta - Prensas hidráulicas - Requisitos de seguridad.
EN 289	C	Máquinas de plástico y caucho - Seguridad - Máquinas de moldeo por soplado indicadas para la producción de artículos huecos - Requisitos de diseño y construcción.
EN 422	C	Máquinas de moldeo por soplado para la producción de piezas huecas - Requisitos de diseño y construcción.
EN ISO 10218-1	C	Robots para entornos industriales - Requisitos de seguridad - Parte 1: Robot.
EN 415-4	C	Seguridad de las máquinas de embalaje - Parte 4: paletizadoras y despaletizadoras.
EN 619	C	Equipos y sistemas de manipulación continua - Requisitos de seguridad y EMC para equipos de manipulación mecánica de cargas de unidad.
EN 620	C	Equipos y sistemas de manipulación continua - Requisitos de seguridad y EMC de cintas transportadoras fijas para material a granel.

Responsabilidades del fabricante

Los fabricantes que introduzcan al mercado máquinas en el Área Económica Europea deben cumplir con los requisitos de la Directiva de Máquinas. Adviértase que al indicar “introducir al mercado” se incluye el caso de una organización que suministre una máquina para sí misma, es decir, fabricar o modificar máquinas para su propio uso o importar máquinas dentro del Área Económica Europea.

Responsabilidades del usuario

- Los usuarios de las máquinas deben asegurarse de que las máquinas recién adquiridas llevan el Marcado CE e incluyen la Declaración de Conformidad con la Directiva de Máquinas. Las máquinas deben utilizarse según las instrucciones del fabricante.

  Las máquinas existentes que fueron puestas en servicio antes de la entrada en vigor de la Directiva de Máquinas no tienen que cumplir con ella, aunque deberán ser seguras y aptas para su propósito.

- La modificación de las máquinas puede considerarse como fabricación de una nueva máquina, aunque sea para uso interno y la empresa que modifique la máquina debe ser consciente de que podría necesitar emitir una Declaración de conformidad y de incluir el Marcado CE.

Evaluación de riesgos

Para que una máquina u otro equipo sean seguros, es necesario evaluar los riesgos que pueden resultar de su uso. La evaluación y la reducción de riesgos de las máquinas se describen en EN ISO 14121-1.

Existen diversas técnicas para la evaluación de riesgos y no se puede afirmar que ninguna sea “la correcta” para realizar la evaluación. La Normativa local especifica algunos principios generales pero no puede especificar exactamente qué debe hacerse en cada caso. Sería deseable que la norma indicara un valor o ‘puntuación’ para cada riesgo y un valor objetivo para el valor máximo que no debe superarse, pero no es el caso por varios motivos. La puntuación que se asignaría a cada riesgo, así como el nivel de riesgo que se puede tolerar, depende de una serie de estimaciones y variará en función de la persona que realice la evaluación, así como del entorno. Por ejemplo, los riesgos que pueden ser razonables en una fábrica que emplea a trabajadores cualificados pueden ser inaceptables en un entorno en el que esté presente el resto de personas, incluidos niños. Los porcentajes históricos de accidentes e incidentes pueden resultar indicadores útiles, pero no sirven de indicación certera de los porcentajes de accidentes que pueden producirse.

Identificar los límites de la máquina

- Es decir ¿qué se está evaluando?, ¿qué velocidades, cargas, sustancias, etc. pueden estar implicadas? Por ejemplo, ¿cuántas botellas moldea por soplado un extrusor por hora?, ¿cuánto material se procesa y a qué temperatura? Recuerde que debe incluirse el uso indebido predecible, como el uso posible de una máquina fuera de su especificación. ¿Cuál es la vida útil esperada de la maquinaria y su aplicación?, ¿de qué modo se desmontará y eliminará al final de su vida útil?

Identificar los peligros

- ¿Qué aspectos de la máquina podrían causar daños a las personas? Deberá tenerse en cuenta la posibilidad de atrapamientos, aplastamientos, cortes de herramientas, bordes afilados en la máquina o en el material que se procese. También deberán tenerse en cuenta otros factores como la estabilidad de la máquina, el ruido, la vibración y la emisión de sustancias o las radiaciones, así como las quemaduras de superficies calientes, sustancias químicas o fricción debido a altas velocidades. Esta fase debe incluir todos los peligros que puedan estar presentes durante el ciclo de vida de la máquina, incluida la construcción, la instalación, el desmontaje y eliminación.

  A continuación se ilustran ejemplos de peligros típicos, aunque no pretende ser una lista exhaustiva. Se puede obtener una lista más detallada en EN ISO 14121-1.

¿Quién puede sufrir daños por los peligros identificados y cuándo?

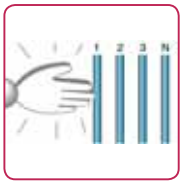
- ¿Quién interactúa con la máquina, cuándo y por qué? De nuevo, recuerde que debe preverse el uso indebido, incluida la posibilidad de que una persona no cualificada utilice la máquina y que podría encontrarse en el lugar de trabajo, es decir, no sólo operarios de las máquinas, sino personal de limpieza, de seguridad, visitantes y resto de personas.

Pinchazo, perforación, cizallamiento, amputación, corte

Aprisionamiento, atrapamiento, succión, enganche

Golpes

Aplastamiento



Electrocución

Proyección de sustancias peligrosas

Quemaduras

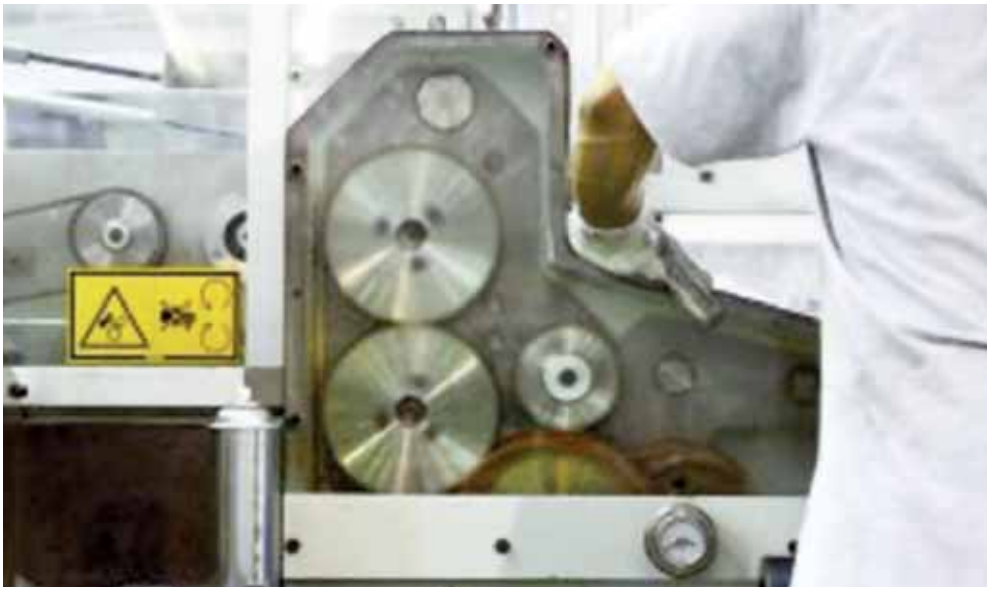
A continuación se indican ejemplos de peligros típicos, aunque no se trata de una lista exhaustiva. Se puede obtener una lista más detallada en EN ISO 14121-1.

Establezca prioridades de los riesgos según su nivel de gravedad

- EN ISO 14121-1 describe esta fase en la Estimación de riesgos. Esto se puede realizar multiplicando el posible daño procedente del peligro por la exposición a éste, teniendo en cuenta que puede estar expuesta más de una persona.

  Es difícil estimar el daño potencial, dada la posibilidad de que todos los accidentes pueden causar víctimas mortales. Aunque normalmente hay más de una posible consecuencia, una siempre será más posible que el resto. Deberán tenerse en cuenta todas las consecuencias posibles, no sólo la peor.

  El resultado del proceso de Evaluación de riesgos debe ser una tabla de los diferentes riesgos que existen en la máquina, junto a la indicación de la gravedad de cada uno. No hay una única "clasificación de riesgos" o "categoría de riesgos" para una máquina, sino que cada riesgo debe tenerse en cuenta por separado. Tenga en cuenta que la gravedad sólo puede ser una estimación, pues la Evaluación de riesgos no es una ciencia exacta. Tampoco se trata de un fin en sí mismo: la finalidad de la Evaluación de riesgos es que sirva de guía para la reducción de los mismos.



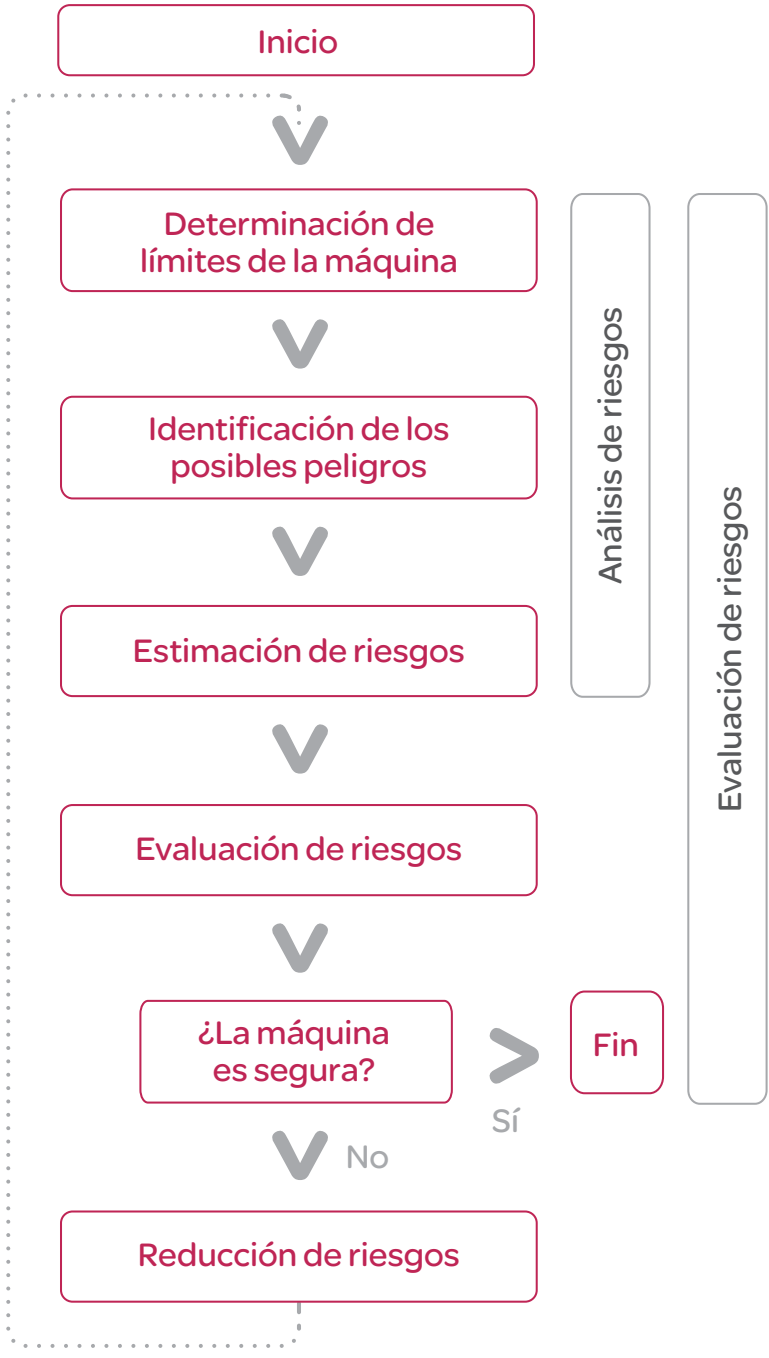
Reducción de riesgos

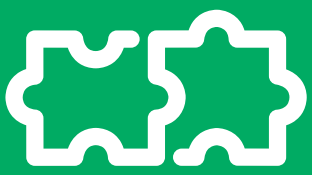
- La reducción de riesgos se incluye en la norma EN ISO 12100-2.

La reducción de riesgos se define en términos de eliminación del riesgo: “el objetivo de las medidas adoptadas debe ser eliminar cualquier riesgo a lo largo de la vida útil previsible de la máquina, incluidas las fases de transporte, montaje, desmontaje, desactivación y desmontaje”.

En general, si se puede reducir un riesgo, deberá reducirse. No obstante, deberá atenuarse según las realidades comerciales y las normativas, que utilizan palabras como “razonable” para indicar que puede que no sea posible eliminar algunos riesgos sin un coste desproporcionado.

El proceso de la evaluación de riesgos es iterativo, es decir, los riesgos deben identificarse, establecerse prioridades entre ellos, cuantificarse, diseñar medidas para reducirlos (primero mediante un diseño seguro y luego con protecciones) y después de este proceso se debe repetir para evaluar si los riesgos individuales se han reducido hasta un nivel tolerable y que no se han introducido riesgos adicionales. En el siguiente capítulo, se analizará el diseño seguro y la protección.


Inicio
Determinación de límites de la máquina
Identificación de los posibles peligros
Estimación de riesgos
Evaluación de riesgos
¿La máquina es segura?
Sí
No
Fin
Reducción de riesgos
Análisis de riesgos
Evaluación de riesgos

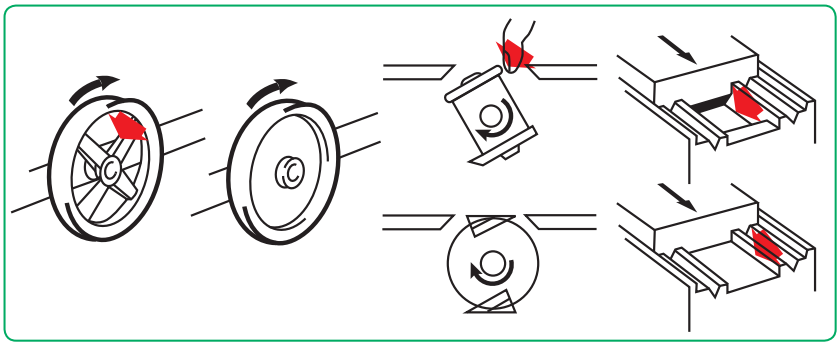


Diseño seguro y protección

Medidas de diseño inherentemente seguro
(según EN ISO 12100-2 capítulo 4)

- Algunos riesgos pueden evitarse con medidas sencillas: ¿se puede eliminar la acción que genera el riesgo? La eliminación a veces puede lograrse mediante la automatización de algunas tareas, como la carga de la máquina. ¿Se puede eliminar el peligro? Por ejemplo, el uso de un disolvente no inflamable para las tareas de limpieza puede eliminar el peligro de incendio asociado a los disolventes inflamables. Esta fase se conoce como **diseño inherentemente seguro**, y es el único modo de **reducir un riesgo a cero**.

  Al eliminar la transmisión del final del rodillo en un transportador se reducirá la posibilidad de que alguien quede atrapado en el rodillo. Al sustituir las poleas rayadas por discos uniformes se pueden reducir los peligros de amputaciones. Si se evitan los bordes afilados, las esquinas y las protuberancias, se pueden evitar cortes y rasguños. Si se aumenta la distancia mínima, se pueden evitar aplastamientos de partes del cuerpo, si se reduce la distancia máxima se puede eliminar la posibilidad de introducción de partes del cuerpo. Si se reducen las fuerzas, las velocidades y las presiones, se pueden reducir los riesgos de lesiones.



Eliminación de zonas cortantes mediante medidas de diseño inherentemente seguro Fuente: BS PD 5304

- Tenga cuidado para no sustituir un peligro por otro. Por ejemplo, las herramientas accionadas con aire evitan los peligros asociados a la electricidad, pero pueden introducir otros por el uso de aire comprimido, como la inyección de aire en el cuerpo y el ruido de un compresor.

Las normas y la legislación determinan una clara jerarquía para los controles.
La principal prioridad es la eliminación de los peligros o la reducción de los riesgos hasta un nivel tolerable, mediante medidas de diseño inherentemente seguro.

Protección y medidas protectoras complementarias
(según EN ISO 12100-2 capítulo 5)

- Cuando no es posible aplicar un diseño inherentemente seguro, el siguiente paso es **la protección**. Esta medida puede incluir, por ejemplo, protecciones fijas, protecciones de enclavamiento, detección de presencia para evitar arranques inesperados, etc.

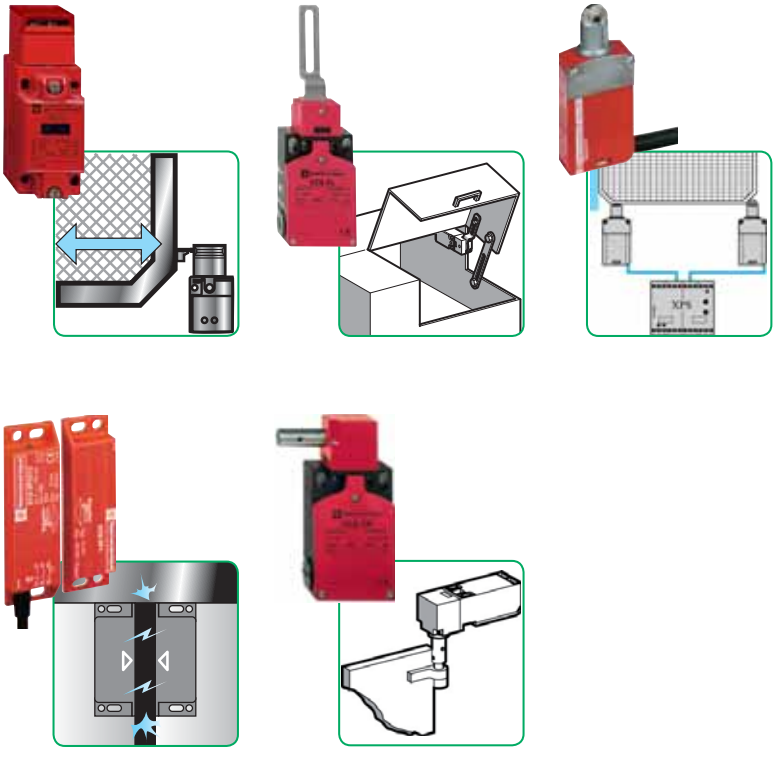
  La protección debe evitar que las personas entren en contacto con los peligros, o bien reducir los peligros a un nivel seguro, antes de que la persona pueda entrar en contacto con ellos.

  Las protecciones en sí mismas pueden ser fijas para cercar o distanciar un peligro, o bien móviles para que puedan cerrarse automáticamente o se accionen o se enclaven eléctricamente.

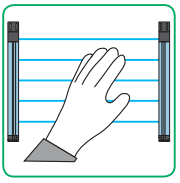
Entre los dispositivos de protección típicos utilizados como parte del sistema de protección se incluyen los siguientes:

- Interruptores de enclavamiento para detectar la posición de las protecciones móviles para el interbloqueo del control, normalmente para permitir tareas como la carga/descarga, la limpieza, la configuración, el ajuste, etc.

  Se protege a los operarios al detener la máquina cuando el actuador se retira del cabezal del interruptor, cuando se acciona la palanca o el pulsador, cuando la protección se abra o la bisagra de la protección gira 5°, normalmente en máquinas con baja inercia (es decir, con tiempos rápidos de parada).



Barreras inmateriales para detectar la aproximación a áreas peligrosas



- Por los dedos, las manos o el cuerpo (resolución de hasta 14 mm, 30 mm y más de 30 mm).

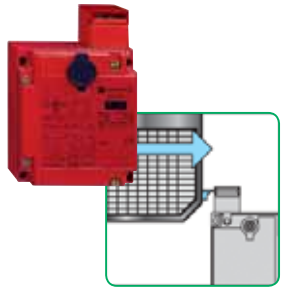
Las barreras inmateriales normalmente se utilizan en aplicaciones de manutención, packaging, cintas transportadoras, en las tareas de almacenamiento y otras aplicaciones. Se han diseñado para la protección de las personas que operen o trabajen en la cercanía de las máquinas, deteniendo los movimientos peligrosos de las partes en el momento en el que se corten los haces de luz.
Hacen posible la protección de las personas y permiten al mismo tiempo un acceso libre a las máquinas. La ausencia de puertas y protecciones reduce el tiempo necesario para cargar, inspeccionar o realizar ajustes y facilita el acceso.

Tapices de seguridad para detectar la presencia de personas

- Al aproximarse, permanecer en el área de peligro o subir hasta ella.

Los tapices de seguridad normalmente se emplean frente o alrededor de máquinas o robots potencialmente peligrosos. Proporcionan una zona de protección entre los operarios de la máquina y los movimientos peligrosos. Se han diseñado principalmente para garantizar la seguridad del personal y servir de complemento a los productos de seguridad como las barreras inmateriales y permitir así el acceso libre para la carga y descarga de las máquinas. Funcionan detectando a las personas cuando entran en contacto con el tapiz y provocan la parada del movimiento peligroso.

Enclavamientos por electroimán (protecciones eléctricas) para evitar la apertura de las protecciones

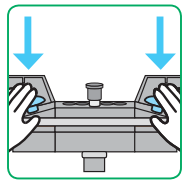


- Durante fases peligrosas de funcionamiento. A diferencia de los enclavamientos sin electroimán, se utilizan en cargas de alta inercia, es decir, en los casos en los que el tiempo de detención es largo y es preferible permitir el acceso únicamente cuando se haya detenido el movimiento peligroso. Se utilizan a menudo en un circuito con temporización (en el que se conoce y define el tiempo de detención de la máquina) o en la parada real de velocidad cero (en la que el tiempo de parada puede variar) para permitir el acceso únicamente cuando se den condiciones seguras.

  Los dispositivos de enclavamiento deben seleccionarse e instalarse para reducir al mínimo la posibilidad de fallos y defectos y la protección general no debe impedir las tareas de producción. Entre los pasos que se deben adoptar para lograrlo se incluyen los siguientes:

  - fijación de los dispositivos con seguridad en un lugar (fijo) y que sea necesario el uso de una herramienta para retirarlo o ajustarlo;
  - dispositivos o sistemas codificados, por ejemplo, mecánicamente, eléctricamente, magnéticamente u ópticamente;
  - obstrucción física o blindaje para evitar el acceso al dispositivo de interbloqueo cuando la protección esté abierta;
  - el soporte de los dispositivos debe ser suficientemente rígido como para mantener el funcionamiento correcto.

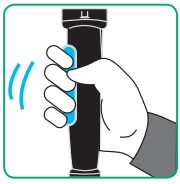
Mandos bimanuales e interruptores de pedal



- Se utilizan para garantizar que el operario se encuentra lejos del área de peligro al realizar movimientos peligrosos (por ejemplo, recorrido descendente en aplicaciones de prensa).

  Sirven de protección principalmente al operario de la máquina. Se puede proporcionar protección complementaria para el personal con otras medidas, como la colocación de barreras inmateriales.

Mandos de validación para permitir el acceso en condiciones específicas de riesgo reducido



- Para funciones de mantenimiento, puesta en marcha, ajuste, etc. (por ejemplo, avance lento), con una posición central y 2 posiciones de “no funcionamiento” (totalmente liberado o apretado).

Supervisión de señales de seguridad – sistemas de control

- Las señales de los dispositivos de protección normalmente se controlan con relés de seguridad, controladores de seguridad o autómatas de seguridad (denominados normalmente “dispositivos de resolución de lógica de seguridad”), que a su vez se utilizan para accionar (y a veces supervisar) dispositivos de salida, como contactores.

  La elección del dispositivo de resolución de lógica dependerá de muchos factores, incluido el número de entradas de seguridad que se van a procesar, el coste, la complejidad de las funciones de seguridad en sí mismas, la necesidad de reducir el cableado mediante descentralización con un bus de campo como el sistema AS-Interface Safety at Work o SafeEthernet, o incluso la necesidad de enviar señales de seguridad o datos en largas distancias a través de máquinas de gran tamaño o entre máquinas en grandes centros. El uso actual tan habitual de dispositivos electrónicos complejos y software en los controladores de seguridad y los autómatas de seguridad en parte ha contribuido a la evolución de las normativas relacionadas con los sistemas de control eléctricos relacionados con la seguridad.

Dos de las normas disponibles en el momento de publicación del presente documento son EN ISO 13849-1 (que substituirá directamente a la EN 954-1) y EN IEC 62061.

Relé de seguridad

Controlador de seguridad

Autómata de seguridad compacto

Autómata de seguridad modular

- La protección por lo general incluirá el uso de algún tipo de sistema de control y la Directiva de Máquinas destaca diversos requisitos sobre las prestaciones del sistema de control. En especial, indica que “Los sistemas de control deben diseñarse y montarse de modo que se evite la generación de situaciones peligrosas”. La Directiva de Máquinas no especifica el uso de ninguna norma determinada, pero el uso de un sistema de control que cumpla los requisitos de las normas armonizadas es una forma de demostrar el cumplimento de este requisito de la Directiva de Máquinas. Dos de las normas disponibles en el momento de publicación del presente documento son EN ISO 13849-1 (que sustituirá a la EN 954-1) y EN IEC 62061.

Medidas protectoras complementarias - Parada de emergencia

- Aunque las paradas de emergencia son necesarias para todas las máquinas (la Directiva de Máquinas tan sólo permite dos excepciones específicas) no se consideran un medio fundamental para la reducción de riesgos. Se consideran “medidas protectoras complementarias”. Se utilizan únicamente como **sistema complementario en caso de emergencia**. Deben ser robustas, fiables y estar disponibles en todas las posiciones en las que pueda ser necesario accionarlas.

  EN IEC 60204-1 define las siguientes tres categorías de funciones de parada:

  - Categoría de parada 0: parada mediante la interrupción inmediata de la alimentación de los accionadores de la máquina (parada no controlada);
  - Categoría de parada 1: una parada controlada, en la que se mantienen alimentados los accionadores para que puedan detener la máquina e interrupción de la alimentación cuando se ha obtenido la parada;
  - Categoría de parada 2: una parada controlada con alimentación en los accionadores de la máquina.

- La categoría de parada 2 normalmente no se considera la indicada para paradas de emergencia.

  Las paradas de emergencia en la maquinaria deben ser “antifraudes”. Es decir, su diseño debe garantizar que aunque se pulse el botón muy lentamente o se tire del cable, si el contacto que normalmente está cerrado se abre, el mecanismo debe enclavarse. Esto evita “usos fraudulentos”, que pueden derivar en situaciones peligrosas. También debe darse lo contrario, es decir, que el enclavamiento no debe producirse a menos que se abra el contacto de NC. Los dispositivos de parada de emergencia deben cumplir con EN IEC 60947-5-5.

Riesgos residuales

- Una vez que se han reducido al máximo los riesgos mediante el diseño y mediante la protección, deberá repetirse la evaluación de riesgos para comprobar que no se han introducido nuevos riesgos (por ejemplo, las protecciones eléctricas pueden introducir peligros de enganches) y para estimar que se han reducido los riesgos hasta un nivel aceptable. Incluso después de realizar varias veces el procedimiento de evaluación y de reducción de riesgos, es posible que existan riesgos residuales.

  Excepto en el caso de máquinas diseñadas según una norma armonizada específica (norma tipo C), el diseñador es quien deberá determinar si el riesgo residual es tolerable o si deben tomarse más medidas de seguridad y ofrecer información sobre dichos riesgos residuales, mediante letreros de advertencia, instrucciones de uso, etc. Las instrucciones además deberán especificar las medidas necesarias, como el uso de equipos de protección individual (EPI) o procedimientos de trabajo especiales, pero todo ello no es tan fiable como las medidas implementadas por el diseñador.

Seguridad funcional

Seguridad funcional

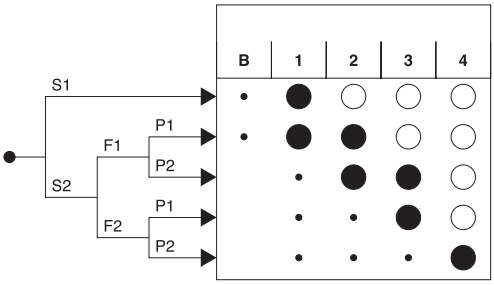
- La IEC ha publicado una serie de preguntas frecuentes relacionadas con la Seguridad funcional en la dirección http://www.iec.ch/zone/fsafety/

  En los últimos años se han publicado una serie de normas relativas al concepto de seguridad funcional. Entre los ejemplos se incluyen IEC 61508, IEC 62061, IEC 61511, ISO 13849-1 e IEC 61800-5-2, que se han adoptado en Europa y se han publicado como EN.

  La seguridad funcional es un concepto relativamente nuevo que sustituye a las antiguas "Categorías" de comportamiento ante condiciones de fallo que se definían en EN 954-1 y se describían erróneamente como "Categorías de seguridad".

Un recordatorio de los principios de EN 954-1

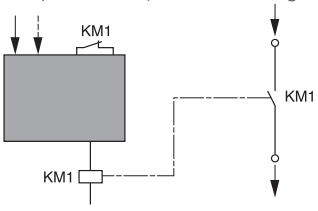
- Los usuarios de EN 954-1 conocerán el anterior "gráfico de riesgos" que muchos empleaban para diseñar las partes relacionadas con la seguridad de los circuitos de control eléctricos para las categorías B, 1, 2, 3 o 4. El usuario debía evaluar subjetivamente la gravedad de las lesiones, la frecuencia de la exposición y la posibilidad de evitar el peligro con términos que iban de leve a grave, inusual a frecuente y de posible a prácticamente imposible, y así determinar la categoría necesaria para cada parte relacionada con la seguridad.



- El concepto es que cuanto más dependa la reducción de riesgos del sistema de control de máquinas de seguridad * (SRECS), más resistente a los fallos deberá ser (como cortocircuitos, contactos soldados, etc).

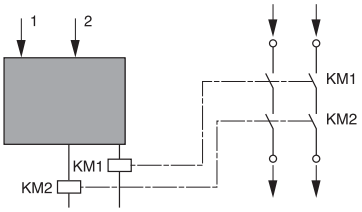
  El comportamiento de las categorías según las condiciones de fallo se definía del siguiente modo:

  - Los circuitos de control de categoría B son básicos y pueden causar pérdidas en la función de seguridad debido a un fallo.
  - La categoría 1 también puede llevar a una pérdida de la función de seguridad, pero con menos probabilidad que la categoría B.
  - Los circuitos de categoría 2 detectan fallos mediante una prueba periódica en intervalos pertinentes (la función de seguridad puede perderse entre las pruebas periódicas).

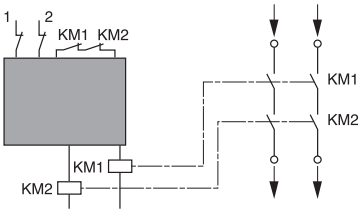


*El sistema de control de seguridad de la máquina se denomina:
- SRP/CS Partes de los sistemas de mando relativas a la seguridad según la norma EN ISO 13849-1.
- SRECS Sistema de control eléctrico relacionado con la seguridad según la norma EN IEC 62061.

- Los circuitos de categoría 3 garantizan la función de seguridad en presencia de un único fallo, por ejemplo, empleando dos canales (redundantes), pero se puede producir una pérdida de la función de seguridad si se acumulan varios fallos.



- Los circuitos de categoría 4 garantizan que la función de seguridad siempre se encuentra disponible incluso en el caso de uno o más fallos, normalmente empleando la redundancia de entrada y de salida, junto a un bucle de retorno para la supervisión continua de las salidas.



- La seguridad funcional es **“parte de la seguridad general relacionada con la EUC* y el sistema de control de EUC que depende del funcionamiento correcto de los sistemas relacionados con la seguridad de E/E/PE**, otros sistemas tecnológicos relacionados con la seguridad y las instalaciones de reducción de riesgos externos”**.
  Tenga en cuenta que se trata de un atributo del equipo bajo control y del sistema de control, no de ningún componente en particular ni de un tipo específico de dispositivo. Se aplica a todos los componentes que contribuyen al rendimiento de la una función de seguridad, incluidos por ejemplo, interruptores de entrada, dispositivos de resolución de lógica, como autómatas y PC Industriales (incluido el software y el firmware) y dispositivos de salida, como los contactores y los variadores de velocidad.

* EUC equivale a Equipment Under Control, equipo bajo control.
**Nota E/E/PE equivale a Electrical/Electronic/Programmable Electronic (eléctrico/electrónico/electrónico programable).

También debe recordarse que las palabras “funcionamiento correcto” significan que la función es correcta, no sólo lo que se esperaba, lo que significa **que las funciones deben seleccionarse correctamente**. Antes, se tendía a elegir componentes especificados según una categoría superior de EN 954-1, en lugar de componentes de categoría inferior que en realidad podrían disponer de funciones más idóneas. Esto quizás se debía a la creencia errónea de que las categorías eran jerárquicas, de modo que, por ejemplo, la categoría 3 siempre sería “mejor” que la categoría 2, etc. Las normas de seguridad funcional están ideadas para que los diseñadores se centren más en las funciones que son necesarias para reducir cada riesgo individual y en el rendimiento necesario para cada función, en lugar de basarse únicamente en componentes determinados.

¿Qué normas se aplican a la función de seguridad?

- En el momento de publicación del presente documento, la norma EN 954-1 dejará de estar en vigor a partir del 31 de diciembre de 2011. Las alternativas disponibles son EN IEC 62061 y EN ISO 13849-1.

  El rendimiento de cada función de seguridad se especifica como el nivel de integridad de la seguridad ó SIL (Safety Integrity Level) en el caso de EN IEC 62061 o nivel de prestaciones ó PL (Performance Level) en el caso de EN ISO 13849-1.

  En ambos casos, la arquitectura del circuito de control que ofrece la función de seguridad es un factor, pero a diferencia de EN 954-1 estas nuevas normas requieren que se tenga en cuenta la fiabilidad de los componentes seleccionados.

EN IEC 62061

- Es importante tener en cuenta cada función al detalle: EN IEC 62061 requiere que se establezca una especificación de requisitos de seguridad o SRS (Safety Requirements Specification). Esto incluye una especificación funcional (qué hace, en detalle) y una especificación de la integridad de la seguridad, que define la probabilidad de que la función se desarrolle en condiciones específicas.
  Un ejemplo que se utiliza a menudo es “detener la máquina cuando la protección esté abierta”, que necesita una consideración más detallada de la especificación funcional inicial. Por ejemplo, ¿se detendrá la máquina al eliminar la tensión de la bobina de un contactor o reduciendo la velocidad con un variador de velocidad? ¿Es necesario que la protección quede cerrada hasta que se hayan detenido los movimientos peligrosos? ¿Deberá desactivarse el resto de equipos, aguas arriba o aguas abajo? ¿Cómo se detendrá la apertura de la protección?
  La especificación de integridad de la seguridad debe tener en cuenta los fallos aleatorios de hardware, así como los fallos sistemáticos. Los fallos sistemáticos son los relativos a una causa específica y sólo se pueden evitar al eliminar dicha causa, normalmente modificando el diseño. En la práctica, la mayoría de fallos ‘en el mundo real’ son sistemáticos y se producen por una especificación incorrecta.
  Como parte del proceso de diseño normal, esta especificación debe dar lugar a la selección de medidas de diseño idóneas, por ejemplo, las protecciones pesadas y mal alineadas pueden provocar daños en los interruptores de enclavamiento, a menos que se instalen amortiguadores y pasadores de alineación, los contactores deben estar protegidos debidamente contra sobrecargas.
  ¿Con qué frecuencia se abrirán las protecciones? ¿Cuáles pueden ser las consecuencias de un fallo en la función? ¿Cuáles serán las condiciones ambientales (temperatura, vibración, humedad, etc.)?
  En EN IEC 62061, un requisito de integridad de la seguridad se expresa como un valor de fallo objetivo de la probabilidad de un fallo peligroso por hora de cada función de control relacionada con la seguridad o SRCF (Safety related control function). Esto se puede calcular a partir de los datos de fiabilidad de cada componente o subsistema y se relaciona con el nivel de SIL, tal y como se muestra en la Tabla 3 de la norma:

Nivel de integridad de la seguridad (SIL)	Probabilidad de un fallo peligroso por hora PFH_D
3	$>10^{-8}$ hasta $<10^{-7}$
2	$>10^{-7}$ hasta $<10^{-6}$
1	$>10^{-6}$ hasta $<10^{-5}$

Tabla 1: Relación entre SIL y PFH_D.

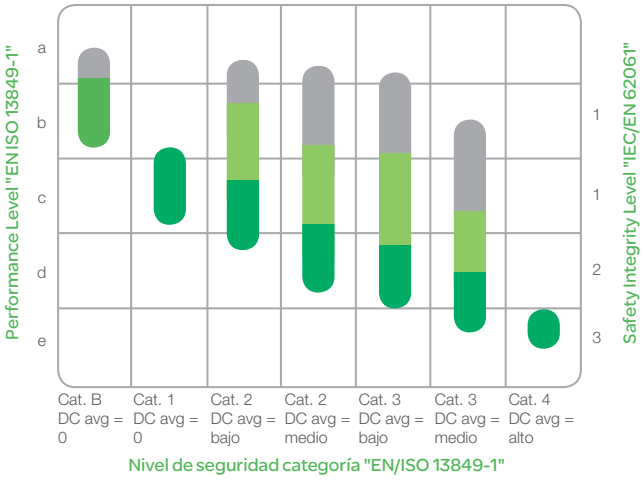
EN ISO 13849-1

- EN ISO 13849-1 emplea una combinación del tiempo medio hasta que se produce un fallo peligroso $MTTF_d$ (Mean Time To Dangerous Failure), la cobertura de diagnóstico DC (Diagnostic Coverage) y la arquitectura (categoría) para determinar el nivel de prestaciones PL (Performance Level) con los siguientes niveles (a, b, c, d, e). Un método simplificado del PL estimado se incluye en la Tabla 7 de la norma. Las categorías son las mismas que las de EN 954-1, que se explican en el Anexo 2.

Categoría	B	1	2	2	3	3	4
DC_{avg}	Ninguna	Ninguna	Baja	Media	Baja	Media	Alta
$MTTF_d$ de cada canal							
Bajo	a	No cubierto	a	b	b	c	No cubierto
Medio	b	No cubierto	b	c	c	d	No cubierto
Alto	No cubierto	c	c	d	d	d	e

Tabla 2: Procedimiento simplificado para evaluar el PL logrado por SRP/CS.

- En la tabla anterior puede observarse que sólo se puede utilizar una arquitectura de categoría 4 para lograr el nivel PLe máximo, pero que se pueden lograr niveles PL inferiores con otras categorías en función de la combinación de $MTTF_d$ y la DC de los componentes utilizados.



- $MTTF_d$ para cada canal = bajo
- $MTTF_d$ para cada canal = medio
- $MTTF_d$ para cada canal = alto

* En varias aplicaciones la consecución del Performance Level c por la categoría 1 puede no ser suficiente.
En este caso una categoría superior, p. ej. 2 o 3, puede ser elegida.

Índice	Rango de $MTTF_d$
Bajo	3 años ≤ $MTTF_d$ < 10 años
Medio	10 años ≤ $MTTF_d$ < 30 años
Alto	30 años ≤ $MTTF_d$ ≤ 100 años

Tabla 3: Niveles de $MTTF_d$.

- Para la estimación del tiempo medio hasta que se produce un fallo peligroso $MTTF_d$ de un componente, se puede pueden utilizar los siguientes datos, en orden de preferencia:

  1. Datos del fabricante ($MTTF_d$, B10 o $B10_d$).
  2. Métodos en los Anexos C y D de EN ISO 13849-1.
  3. Elegir 10 años.

- La cobertura del diagnóstico DC es una medida de cuántos fallos peligrosos detectará un sistema de diagnóstico. El nivel de seguridad puede aumentar cuando los subsistemas se prueben internamente mediante autodiagnóstico.

Índice	Cobertura del diagnóstico
Nula	DC < 60%
Baja	60% ≤ DC < 90%
Media	90% ≤ DC < 99%
Alta	99% ≤ DC

Tabla 4: Niveles de cobertura de diagnóstico.

- Los fallos de causa común CCF (Common Cause Failures) se producen cuando un efecto externo (como un daño físico) hacen que una serie de componentes no puedan utilizarse, independientemente del $MTTF_d$. Entre los pasos que deben adoptarse para reducir los CCF se incluyen los siguientes:
  - Diversidad en los componentes utilizados y modos en los que se accionan.
  - Protección contra la polución.
  - Separación.
  - Compatibilidad electromagnética mejorada.

¿Qué norma utilizar?

- A menos que una norma C especifique un nivel de SIL o un nivel de PL, el diseñador puede elegir entre utilizar EN IEC 62061 o EN ISO 13849-1, o cualquier otra norma. Tanto EN IEC 62061 como EN ISO 13849-1 son normas armonizadas que aportan una Presunción de conformidad con los requisitos esenciales de la Directiva de Máquinas, siempre que se apliquen. Sin embargo, debe recordarse que sea cual sea la norma elegida, debe emplearse en su totalidad y no pueden mezclarse en un mismo sistema.

  Se están realizando trabajos conjuntos entre IEC e ISO, para producir un Anexo común para las dos normas con el objetivo de crear una única norma.

  EN IEC 62061 es quizás más completo en lo que respecta a responsabilidades de especificación y gestión, mientras que EN ISO 13849-1 se ha diseñado para permitir una transición más sencilla a partir de EN 954-1.

Certificación

- Algunos componentes se encuentran disponibles con certificación para un SIL ó PL específicos. Debe recordarse que estos certificados son sólo una indicación del nivel máximo SIL o el nivel máximo PL que puede lograr un sistema utilizando ese componente en una configuración específica y no son una garantía de que un sistema completo cumplirá un nivel SIL o un nivel PL específicos.

Ejemplos prácticos de sistemas de control según normas

Quizás el mejor modo de comprender la aplicación de EN IEC 62061 y EN ISO 13849-1 es mediante los ejemplos prácticos de las siguientes páginas.

Para ambas normas utilizaremos el ejemplo en el que la apertura de una protección deba hacer que se detengan las partes móviles de una máquina y en caso contrario, la posible lesión resultante puede ser un brazo roto o la amputación de un dedo.

Ejemplo práctico utilizando la norma EN IEC 62061

Seguridad de máquinas - Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables.

- Los sistemas de control eléctricos relativos a la seguridad en máquinas o SRECS (Safety-related electrical control systems) desempeñan una función cada vez más importante a la hora de garantizar la seguridad general de las máquinas y cada vez se utilizan con más frecuencia con tecnología electrónica compleja. Esta norma es específica del sector de las máquinas dentro del marco de trabajo de EN IEC 61508.

  Aporta normas para la integración de subsistemas diseñados según EN ISO 13849-1. No especifica los requisitos operativos de los componentes de control no eléctricos en las máquinas (por ejemplo: hidráulico, neumático).

Concepto funcional de seguridad

- El proceso comienza con el análisis de los riesgos (EN ISO 14121-1) para poder determinar los requisitos de seguridad. Una característica particular de EN IEC 62061 es que insta al usuario a realizar un análisis de la arquitectura para realizar las funciones de seguridad y a que tenga en cuenta las subfunciones y analice sus interacciones antes de tomar decisiones sobre un hardware para el sistema de control de seguridad, denominado sistema de control eléctrico relacionado con la seguridad o SRECS (safety related electrical control system).

  Debe establecerse y documentarse un plan de seguridad funcional para cada proyecto de diseño. Debe incluir lo siguiente:

  Una especificación de los requisitos de seguridad para las funciones de seguridad (SRCF) que conste de dos partes:

  - Una descripción de las funciones e interfaces, modos de operación, prioridades de funcionamiento, frecuencia de la operación, etc.
  - Especificación de los requisitos de integridad de la seguridad para cada función, expresados en términos de nivel de integridad de la seguridad o SIL (Safety Integrity Level).
  - La Tabla 1 a continuación indica los valores máximos de fallos para cada SIL.

Nivel de integridad de la seguridad (SIL)	Probabilidad de un fallo peligroso por hora PFH_D
3	$>10^{-8}$ hasta $<10^{-7}$
2	$>10^{-7}$ hasta $<10^{-6}$
1	$>10^{-6}$ hasta $<10^{-5}$

  - El proceso de diseño estructurado y documentado para los sistemas de control eléctricos (SRECS),
  - Los procedimientos y recursos para la grabación y el mantenimiento de la información adecuada,
  - El proceso para la gestión y la modificación de la configuración, teniendo en cuenta la organización y el personal autorizado,
  - La verificación y el plan de validación.

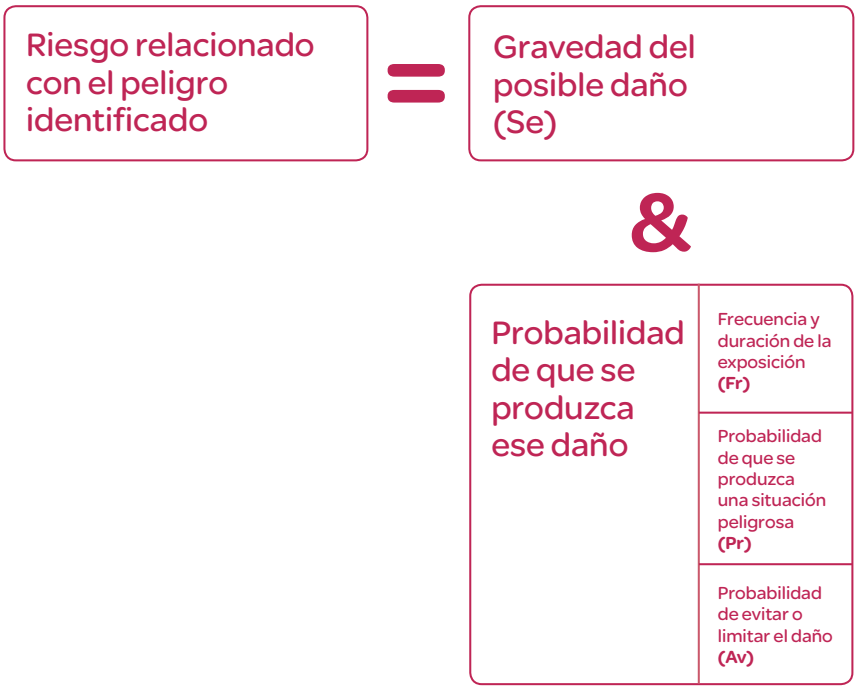
- La ventaja de este enfoque es que puede ofrecer un método de cálculo que incluye todos los parámetros que pueden afectar a la fiabilidad de los sistemas de control. El método consiste en asignar un nivel de integridad de la seguridad o SIL a cada función, teniendo en cuenta los siguientes parámetros:
  - La probabilidad de un fallo peligroso de los componentes (PFH_D),
  - El tipo de arquitectura (A, B, C o D), es decir:
    - Con o sin redundancia,
    - Con o sin funciones de seguridad, lo que hace posible controlar algunos de los fallos peligrosos,
  - Fallos de causa común CCF (Common Cause of Failures), incluidos;
    - Cortocircuitos entre canales,
    - Sobretensión,
    - Pérdida de alimentación eléctrica, etc.,
  - La probabilidad de errores de transmisión peligrosos en los que se emplee comunicación digital,
  - Interferencias electromagnéticas (EMI).

- El diseño de un sistema se divide en 5 pasos, tras haber establecido el plan de seguridad funcional:
  1. En función de la evaluación de los riesgos, asignar un nivel de integridad de la seguridad (SIL) e identificar la estructura básica del sistema de control eléctrico (SRECS), describir cada función relacionada (SRCF),
  2. Desglosar cada función en una estructura de bloques de funciones o FB (function block),
  3. Enumerar los requisitos de seguridad para cada bloque de funciones y asignar los bloques de funciones a los subsistemas dentro de la arquitectura,
  4. Seleccionar los componentes de cada subsistema,
  5. Diseñar la función de diagnóstico y comprobar que se alcanza el nivel de integridad de seguridad especificado (SIL).

- En nuestro ejemplo, plantearemos una función que corte la alimentación de un motor cuando se abra una protección. Si la función falla, el operario de la máquina podría romperse un brazo o amputarse un dedo.

Paso 1 - Asignar un nivel de integridad de la seguridad (SIL) e identificar la estructura del sistema de control eléctrico relacionado con la seguridad (SRECS)

- En función de la evaluación de riesgos realizada según EN ISO 14121-1, se realiza la estimación del nivel de SIL necesario para cada función de control relacionada con la seguridad (SRCF) y se desglosa en parámetros, tal y como se muestra en la siguiente ilustración.



Gravedad Se

- La gravedad de las lesiones o el daño en la salud se pueden estimar teniendo en cuenta las lesiones reversibles, las lesiones irreversibles o la defunción.

  En la siguiente tabla se muestra la clasificación recomendada.

Consecuencias	Gravedad (Se)
Irreversible: muerte, pérdida de un ojo o un brazo	4
2 Irreversible: extremidad(es) rota(s), pérdida de dedo(s)	3
Reversible: necesidad de asistencia médica	2
Reversible: necesidad de primeros auxilios	1

Probabilidad de que se produzca el daño

- Cada uno de los tres parámetros Fr, Pr, Av se estima por separado, usando el caso menos favorable. Se recomienda emplear un análisis de tareas para garantizar que la estimación de la probabilidad de que se produzca el daño se tiene en cuenta correctamente.

Frecuencia y duración de la exposición Fr

- El nivel de la exposición está relacionado con la necesidad de acceder a la zona peligrosa (funcionamiento normal, mantenimiento, ...) y el tipo de acceso (alimentación manual, ajuste, ...).
  Luego se puede estimar la frecuencia media y la duración de la exposición.

  En la siguiente tabla se muestra la clasificación recomendada:

Frecuencia de exposición	Duración > 10 min
Fr < 1 h	5
1 h < Fr < 1 día	5
1 día < Fr < 2 semanas	4
2 semanas < Fr < 1 año	3
Fr > 1 año	2

Probabilidad de que se produzca una situación peligrosa Pr

- Deben tenerse en cuenta dos conceptos básicos:

  La capacidad de previsibilidad de las situaciones peligrosas en las diferentes partes de la máquina en sus distintos modos de funcionamiento (normal, mantenimiento, solución de problemas), prestando especial atención a los reinicios inesperados;

  El comportamiento de las personas que interactúan con la máquina, como el estrés, el cansancio, la inexperiencia, etc.

Probabilidad de que se produzca	Probabilidad (Pr)
Muy alta	5
Probable	4
Posible	3
Raramente	2
Insignificante	1

Probabilidad de evitar o limitar el daño Av

- Este parámetro está relacionado con el diseño de la máquina. Tiene en cuenta lo repentinamente que pueda producirse la situación peligrosa, la naturaleza del peligro (corte, temperatura, eléctrico), la posibilidad física de evitar el peligro y la posibilidad de que una persona identifique una situación peligrosa.

Probabilidades de evitar o limitar el daño (Av)	
Imposible	5
Raramente	3
Probable	1

Asignación de SIL:

- La estimación se realiza con la ayuda de la siguiente tabla.

En nuestro ejemplo, el grado de gravedad (Se) es 3 porque existe el riesgo de amputación de un dedo; este valor se muestra en la primera columna de la tabla. Los demás parámetros deben añadirse juntos para seleccionar una de las clases (las columnas verticales de la siguiente tabla), lo que da como resultado:

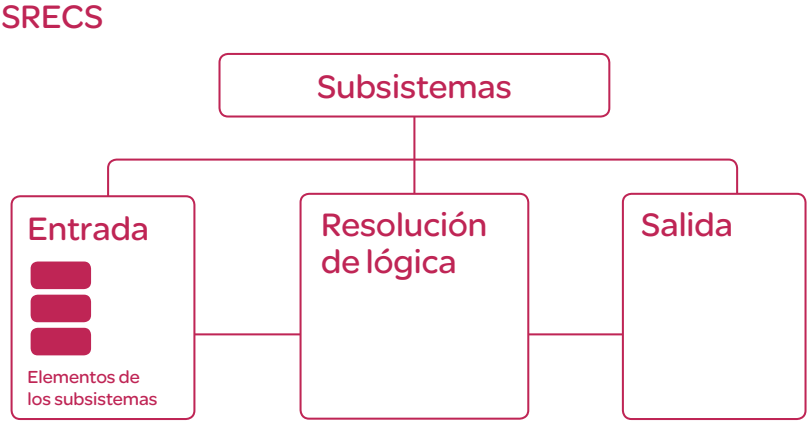
Fr = 5 acceso varias veces al día
Pr = 4 situación peligrosa probable
Av = 3 probabilidad de evitar casi imposible

Por lo tanto, una clase **Cl = 5 + 4 + 3 = 12**
El sistema de control eléctrico relacionado con la seguridad (SRECS) de la máquina debe realizar esta función con un nivel de integridad de SIL 2.

Gravedad (Se)	Clase (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	**SIL 2**	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Estructura básica del SRECS

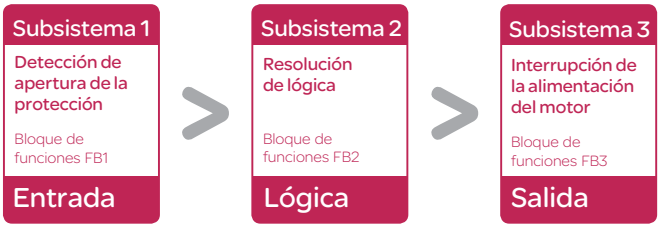
- Antes de entrar en detalle sobre los componentes de hardware que deben utilizarse, el sistema se desglosa en subsistemas. En este ejemplo, se necesitan 3 subsistemas para realizar las funciones de entrada, procesamiento y salida. La siguiente figura ilustra esta fase y utiliza la terminología empleada en la norma.



Paso 2 - Desglosar cada función en una estructura de bloques de funciones FB (function block)

- Un bloque de funciones (FB) es el resultado de un desglose detallado de una función relacionada con la seguridad.
  La estructura del bloque de funciones ofrece un concepto inicial de la arquitectura del sistema de control eléctrico relacionado con la seguridad (SRECS). Los requisitos de seguridad de cada bloque se derivan de la especificación de los requisitos de seguridad de la función correspondiente de control relacionada con la seguridad.

SRECS
SIL requerido= SIL2



Paso 3 - Enumerar los requisitos de seguridad para cada bloque de funciones y asignar los bloques de funciones a los subsistemas dentro de la arquitectura

- Cada bloque de funciones se asigna a un subsistema en la arquitectura del sistema SRECS. (La norma define 'subsistema' de forma que el fallo de cualquier subsistema producirá el fallo de una función de control relacionada con la seguridad.) A cada subsistema se puede asignar más de un bloque de funciones. Cada subsistema puede incluir elementos de subsistemas y si fuera necesario, funciones de diagnóstico para garantizar que se pueden detectar los fallos y tomar las medidas adecuadas.

  Estas funciones de diagnóstico se consideran funciones separadas; se pueden realizar dentro del subsistema o mediante otro subsistema. Los subsistemas deben alcanzar al menos la misma capacidad de SIL que la asignada a toda la función de control relacionada con la seguridad, cada uno con su propio SIL CL (SIL Claim Limit). En este caso, el SILCL de cada subsistema debe ser 2.

SRECS

Paso 4 - Seleccionar los componentes de cada subsistema

• Se seleccionan los productos mostrados a continuación.

Componente	Número de operaciones (B10)	% fallos peligrosos	Vida útil
Interruptores de posición de seguridad XCS	10.000.000	20%	10 años
Módulo de seguridad XPS AK	$PFH_D = 7.389 \times 10^{-9}$		
Contactor LC1 TeSys	1.000.000	73%	20 años

Los datos de fiabilidad se obtienen a través del fabricante.

La duración del ciclo en este ejemplo es de 450 segundos, por lo que el ciclo de trabajo **C** es de 8 operaciones por hora, es decir, la protección se abrirá 8 veces por hora.

Paso 5 - Diseño de la función de diagnóstico

- El nivel SIL logrado por los subsistemas depende no sólo de los componentes, sino también de la arquitectura seleccionada. Para este ejemplo, elegiremos arquitecturas B para las salidas del contactor y D para el interruptor de posición (véase el Anexo 1 de este manual para obtener una explicación de las arquitecturas A, B, C y D).

  En esta arquitectura, el módulo de seguridad realiza un diagnóstico automático y comprueba también los interruptores de posición de seguridad. Existen tres subsistemas para los que deben determinarse los SILCLs (SIL Clain Limits):

  SS1: dos interruptores de posición de seguridad en un sistema con una arquitectura tipo D (redundante);
  SS2: un módulo de seguridad SILCL 3 (determinado a partir de los datos, incluido PFH_D, proporcionado por el fabricante);
  SS3: dos contactores utilizados según una arquitectura de tipo B (redundante sin retorno de los contactos espejo)

  El cálculo tiene en cuenta los siguientes parámetros:

  B10: número de operaciones en las que el 10% de los componentes habrá fallado.
  C: Ciclo de trabajo (número de operaciones por hora).

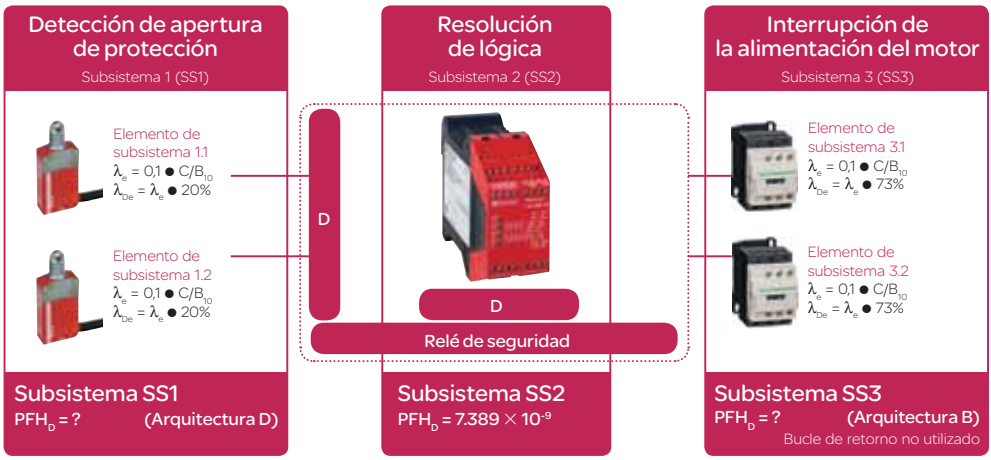
  λ_D: tasa de fallos peligrosos ($\lambda = \times$ proporción de fallos peligrosos).

  β: factor de fallo de causa común: véase el Anexo F de la norma.

  T1: Intervalo de test de prueba o vida útil, lo que sea menor, tal y como lo especifique el fabricante. La norma indica que los diseñadores deben emplear una duración de 20 años, para evitar el uso de un intervalo de test de prueba demasiado breve con el fin de mejorar el cálculo de SIL. Sin embargo, reconoce que puede ser necesario sustituir los componentes electromecánicos cuando se llegue a un número de operaciones específico. Por lo tanto, la cifra utilizada para T1 puede ser la duración indicada por el fabricante, o en el caso de los componentes electromecánicos, el valor de B10 dividido por la tasa de operaciones C.

  T2: intervalo de pruebas de diagnóstico.

  DC: Tasa de cobertura de diagnóstico = $\lambda_{DD} / \lambda_{Dtotal}$, la proporción entre la tasa de fallos peligrosos detectados y la tasa de fallos peligrosos totales.



- La tasa de fallos, λ, de un elemento de subsistema electromagnético se define como λe = 0,1 × C / B10, donde C es el número de operaciones por hora en la aplicación y B10 es el número esperado de operaciones en el que el 10% de los componentes habrá fallado. En este ejemplo, consideraremos que C = 8 operaciones por hora.

			SS1 2 interruptores de posición supervisados	SS3 2 contactores sin diagnóstico
Tasa de fallo de cada elemento λ_e	λ_e = 0.1 C/B_{10}			
Tasa de fallos peligrosos de cada elemento λ_{De}	λ_{De} = λ_e × proporción de fallos peligrosos			
DC			99%	No aplicable
Factor de fallo de causa común β			Peor caso asumido del 10%	
T1	T_1 = min (vida útil, B_{10}/C)		(10 000 000/8) = 1 250 000	(1 000 000/8) = 125 000
Intervalo de pruebas de diagnóstico T2			Cada demanda, es decir, 8 veces cada hora, = 1/8 = 0,125 h	No aplicable
Tasa de fallos peligrosos de cada subsistema	Fórmulas para la arquitectura B: $\lambda_{DSSB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) /2$	Fórmulas para la arquitectura D para subsistemas del mismo diseño: $\lambda_{DSSD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1\} + \beta \times \lambda_{De}$		$\lambda_{DSSB} = (1 - 0.9)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) /2$

- Examinando los contactores de salida en el subsistema SS3, debemos calcular el PFH_D. Para la arquitectura de tipo B (tolerante a un solo fallo, sin diagnóstico) la probabilidad de un fallo peligroso del subsistemas es:

$\lambda_{DSSB} = (1 - \beta)2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

[Ecuación B de la norma]

$PFH_{DSSD} = \lambda_{DSSB} \times 1h$

En este ejemplo, $\beta = 0.1$

$\lambda_{De1} = \lambda_{De2} = 0.73\ (0.1 \times C / 1\ 000\ 000) = 0.73\ (0.8/1\ 000\ 000) = 5.84 \times 10^{-7}$

T_1 = min (vida útil, B_{10}/C) = min (175 200, 1 000 000/8) = min (175 200, 125 000) = 125 000 h

$\lambda_{DSSB} = (1 - 0.1)^2 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 125\ 000 + 0.1 \times [(5.84 \times 10^{-7}) + (5.84 \times 10^{-7})] /2$

$= 0.81 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 125\ 000 + 0.1 \times 5.84 \times 10^{-7}$

$= 0.81 \times 3.41056 \times 10^{-13} \times 125\ 000 + 0.1 \times 5.84 \times 10^{-7}$

$= (3.453 \times 10^{-8}) + (5.84 \times 10^{-8}) = 9.29 \times 10^{-8}$

Puesto que $PFH_{DSSB} = \lambda_{DSSB} \times 1h$, PFH_D para los contactores en el Subsistema SS3 = 9.29×10^{-8}

- Está dentro de los límites de SILCL 2 y SILCL 3. Sin embargo, la Tabla 5 de la norma EN 62061 nos da unas limitaciones de arquitectura para lograr alcanzar un límite de SIL claim en particular, y en este caso la arquitectura B donde el porcentaje de fallo seguro es menor al 60% (la fracción de fallo seguro es del 27% para los contactores) y la tolerancia a fallos del hardware es 1, el estado máximo del límite SIL claim que puede ser alcanzado, es en realidad SILCL 1. Esto significa que el nivel SIL general de este sistema no puede ser mayor a 1. De forma que para alcanzar un SILCL mayor a 1 para los contactores, necesitamos tener una cobertura del diagnóstico adicional, en el caso de los contactores de Schneider Electric éste puede ser conseguido cableando los contactos espejo (contactos NC auxiliares) en el relé de seguridad, en la entrada EDM "external device monitoring", logrando así obtener una arquitectura de tipo D con un SFF >99% y un SILCL 3 (se adjuntan los cálculos a continuación).

Fracción de fallos seguros (SFF)	Tolerancia a fallos Hardware (HFT)		
	0	1	2
<60%	No permitido (para excepciones ver la nota 3)	SILCL 1	SILCL 2
60%-<90%	SILCL 1	SILCL 2	SILCL 3
90%-<99%	SILCL 2	SILCL 3	SILCL 3 (ver la nota 2)
>=99%	SILCL 3	SILCL 3 (ver la nota 2)	SILCL 3 (ver la nota 2)

Nota 1: Un fallo de tolerancia hardware N significa que el fallo N+1 puede provocar la pérdida de la función de control relativa a la seguridad.
Nota 2: Un límite SIL claim 4 no es considerado en esta norma. Para SIL 4 ver IEC 51508-1.
Nota 3: Ver 6.7.6.4 para subsistemas donde las exclusiones de fallo se aplican a fallos que pueden originar un fallo peligroso, ver 6.7.7.

Los contactores LC1D TeSys incluyen contactos espejo

- Para elementos del subsistema del mismo diseño.

$\lambda_{DSSD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC]\ T_2/2 + [\lambda_{De}^2 \times (1\text{-}DC)] \times T_1\} + \beta\ \lambda_{De}$

$PFH_{DSSD} = \lambda_{DSSD} \times 1h$

En este ejemplo, $\beta = 0.1$

$\lambda_{De} = 0.73\ (0.1 \times C / 1\ 000\ 000) = 5.84 \times 10^{-7}$

T_1 = min (vida útil, B_{10}/C) = min (175 200, 1 000 000/8) = min (175 200, 125 000) = 125 000 h

$T_2 = 1/C = 1/8 = 0.125$

DC = 0.99 (alcanzado mediante la realimentación de los contactos espejo de los contactores en el relé de seguridad para detectar soldaduras en el contactor).

Nota: el cableado de los contactores retorna al relé de seguridad con lo cual también cambia la Fracción de fallo seguro del subsistema del contactor desde un valor inferior al 60% a un valor superior al 99% (un fallo peligroso de uno de los contactores no permitirá un reinicio del sistema), por lo que se refiere a la tabla 5, será posible alcanzar hasta un SILCL3.

$\lambda_{DSSD} = (1 - 0.1)^2 \{[5.84 \times 10^{-7} \times 2 \times 0.99]\ 0.125\ /2 + [5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times (1\text{-}0.99)] \times 125\ 000\} + 0.1 \times 5.84 \times 10^{-7}$

$= 0.92\ (6.753 \times 10^{-13})\ 0.0625 + (6.753 \times 10^{-13} \times 0.1 \times 125\ 000) + 5.84 \times 10^{-8}$

$= (3.883 \times 10^{-14}) + (8.44 \times 10^{-9}) + (5.84 \times 10^{-8})$

$= 6.684 \times 10^{-8}$

A partir de $PFH_{DSSD} = \lambda_{DSSD} \times 1h$, el PFH_{DSSD} para el subsistema del contactor en arquitectura D es 6.684×10^{-8}. Esto significa que el subsistema tiene un SILCL3

Para los interruptores de posición en el subsistema SS1 los cuales están en una arquitectura D

- D.2 de la norma
  $PFH_{DSSD} = \lambda_{DSSD} \times 1h$
  $\lambda_e = 0{,}1 \bullet C / B10 = 0.1 \times 8/10\,000\,000 = 8 \times 10^{-8}$
  $\lambda_{De} = \lambda_e \times 0.2 = 1.6 \times 10^{-8}$
  DC = 99%
  β = 10% (peor caso)
  T_1 = min (vida útil, B_{10}/C) = min (87 600, 10 000 000/8) = min (87 600, 1 250 000) = 87 600
  T_2 = 1/C = 1/8 = 0.125 hora

- A partir de D.2; para elementos del mismo diseño:
  $\lambda_{DSSD} = (1 - 0.1)^2 \{[(1.6 \times 10^{-8})^2 \times 2 \times 0.99] 0.125/2 + [1.6 \times 10^{-8})^2 \times (1 - 0.99)] \times 87\,600\} + 0.1 \times 1.6 \times 10^{-8}$
  $= 2.566 \times 10^{-17} + 2.24 \times 10^{-13} + 1.6 \times 10^{-9}$
  $= 1.6 \times 10^{-9}$
  Puesto que $PFH_{DSSD} = \lambda_{DSSD} \times 1h$, PFH_D para los interruptores de posición en el Subsistema SS1 = 1.60×10^{-9}

- Ya sabemos que para el Subsistema SS2, PFH_D para el bloque de función del dispositivo de resolución de lógica (implementado mediante el relé de seguridad XPSAK) es 7.389×10^{-9} (datos del fabricante)

  El PFH_D general para el sistema de control eléctrico de seguridad (SRECS) es la suma del PFH_Ds de todos los Bloques de funciones y por lo tanto es:
  $PFH_{DSRECS} = PFH_{DSS1} + PFH_{DSS2} + PFH_{DSS3} =$
  $1.60 \times 10^{-9} + 7.389 \times 10^{-9} + 6.684 \times 10^{-8} = 7.58 \times 10^{-8}$

Todos los subsistemas tienen un SIL claim de SILCL3, además los cálculos anteriores dan un SIL general para el sistema dentro de los límites de SIL3.

Nivel de integridad de la seguridad (SIL)	Probabilidad de un fallo peligroso por hora PFH_D
3	$>10^{-8}$ hasta $<10^{-7}$
2	$>10^{-7}$ hasta $<10^{-6}$
1	$>10^{-6}$ hasta $<10^{-5}$

Tabla 1: Relación entre SIL y PFH_D

Ejemplo práctico utilizando la norma EN ISO 13849-1

Seguridad de las máquinas - Partes de los sistemas de mando relativas a la seguridad - Parte 1: Principios generales para el diseño

- Al igual que con EN IEC 62061, se puede considerar que el proceso incluye una serie de 6 pasos lógicos.
  PASO 1: Evaluación de riesgos e identificación de las funciones de seguridad necesarias.
  PASO 2: Determinar el nivel de prestaciones requerido (PLr) para cada función de seguridad.
  PASO 3: Identificar la combinación de las partes relacionadas con la seguridad que realizan la función de seguridad.
  PASO 4: Evaluar el nivel de prestaciones (PL) de todas las partes relacionadas con la seguridad.
  PASO 5: Comprobar que el PL del SRP/CS* de la función de seguridad es al menos igual al PLr.
  PASO 6: Comprobar que se cumplen todos los requisitos (véase EN ISO 13849-2).

* Parte del sistema de mando relativa a la seguridad (nombre del sistema de mando de seguridad de la máquina en la norma EN ISO 13849-1).

Para obtener más detalles, véase el Anexo 2 de este manual

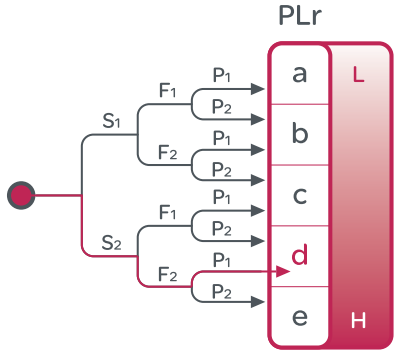
- PASO 1: Al igual que en el ejemplo anterior, necesitamos una función de seguridad para cortar la alimentación del motor cuando la protección se encuentre abierta.

- PASO 2: Mediante el "gráfico de riesgos" de la Figura A.1 de EN ISO 13849-1 y los mismos parámetros utilizados en el ejemplo anterior, el Nivel de prestaciones necesario es d (nota: PL = d se compara a menudo con SIL 2 como "equivalente").

  H = Alta contribución para reducir el riesgo por el sistema de control.

  L = Baja contribución para reducir el riesgo por el sistema de control.

  S = Gravedad de la lesión.
  S1 = Leve (lesión normalmente reversible).
  S2 = Grave (lesión normalmente irreversible, incluyendo la muerte).
  F = Frecuencia y/o tiempo de exposición al peligro.
  F1 = Raro a bastante frecuente y/o corta duración de la exposición.
  F2 = Frecuente a continuo y/o larga duración de la exposición.
  P = Posibilidad de evitar el peligro o limitar el daño.
  P1 = Posible en determinadas condiciones.
  P2 = Raramente posible.



- PASO 3: Se tendrá en cuenta la misma arquitectura básica que en el ejemplo anterior para EN IEC 62061, es decir, una arquitectura de categoría 3 sin retorno.

- PASO 4: El nivel PL de la SRP/CS se determina mediante la estimación de los siguientes parámetros: (véase el Anexo 2):
  - La CATEGORÍA (estructura) (véase punto 6 de EN ISO 13849-1). Tenga en cuenta que en este ejemplo, el uso de una arquitectura de **categoría 3 significa que no se utilizan los contactos espejo en los contactores**.
  - El $MTTF_d$ para cada componente (véanse los Anexos C y D de EN ISO 13849-1).
  - La Cobertura del diagnóstico (véase el Anexo E de EN ISO 13849-1).
  - Los Fallos de causa común (véase la tabla de puntuaciones en el Anexo F de EN ISO 13849-1).
- El fabricante facilita los siguientes datos de los componentes:

Ejemplo SRP/CS	B10 (operaciones)	$MTTF_d$ (años)	DC
Interruptores de posición de seguridad	10.000.000		99%
Módulo de seguridad XPSAK		154,5	99%
Contactores	1.000.000		0%

- Obsérvese que como el fabricante desconoce los detalles de la aplicación y en particular el número de ciclos de los dispositivos electromecánicos, sólo puede ofrecer datos de B10 o $B10_d$ de los componentes electromecánicos. Esto explica por qué ningún fabricante debe aportar una cifra de $MTTF_d$ para un dispositivo electromecánico.

- El $MTTF_d$ de los componentes se puede calcular con la siguiente fórmula:

  $MTTF_d = B10_d / (0.1 \times n_{op})$
  Donde n_{op} es el número medio de operaciones por año.

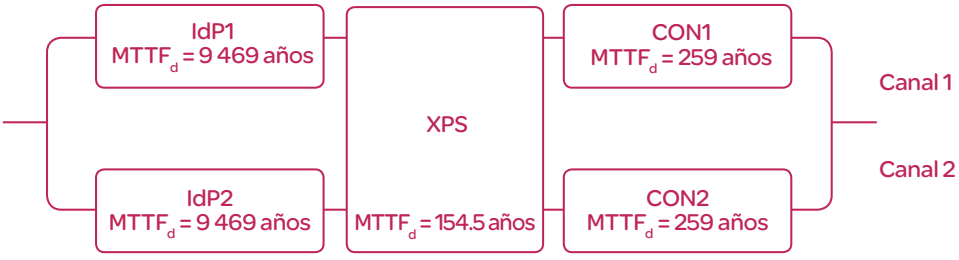
  B10 es el número de operaciones en las que el 10% de los componentes habrá fallado.
  $B10_d$ es el tiempo esperado en el que el 10% de los componentes habrá fallado en un modo "peligroso". Sin tener conocimientos específicos sobre el modo en el que se está utilizando un componente, y qué constituye un fallo peligroso, para un interruptor de posición, el % de fallo peligroso es un 20%, por lo que $B10_d$ = B10/20%
  Asumiendo que la máquina se utiliza durante 8 horas al día, durante 220 días al año, con un tiempo de ciclo de 120 segundos, n_{op} será 52 800 operaciones al año.

- Asumiendo que $B10_d$ = B10/20%, la tabla de resultados es la siguiente:

Ejemplo SRP/CS	B10 (operaciones)	$B10_d$	$MTTF_d$ (años)	DC
Interruptores de posición de seguridad	10 000 000	50 000 000	9 469	99%
Módulo de seguridad XPSAK			154.5	99%
Contactores	1 000 000	1 369 863	259	0%

- Los valores de $MTTF_d$ resaltados en rojo se han obtenido de los datos de la aplicación utilizando el número de ciclo y los datos de $B10_d$.

  El $MTTF_d$ de cada canal se puede calcular utilizando el método de recuento de partes en el Anexo D la norma.



En este ejemplo, el cálculo es idéntico para los canales 1 y 2:

$$\frac{1}{MTTF_d} = \frac{1}{9\,469 \text{ años}} + \frac{1}{154.5 \text{ años}} + \frac{1}{259 \text{ años}} = \frac{1}{95.85 \text{ años}}$$

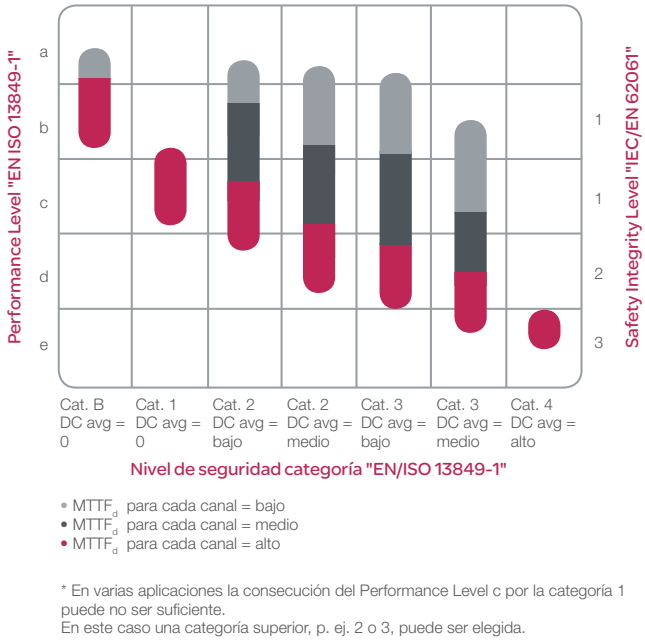
- El $MTTF_d$ de cada canal es por lo tanto de 95.85 años; es nivel "alto" según la Tabla 3.
  A partir de las ecuaciones en el Anexo E la norma, se puede determinar que DC_{avg} = 62.4%.

• PASO 5: Verificar que el nivel PL del sistema coincide con el PL requerido (PLr).

Teniendo en cuenta que disponemos de una arquitectura de categoría 3, un $MTTF_d$ alto y una Cobertura media del diagnóstico baja (DC_{avg}), se puede observar en la siguiente tabla (fig. 5 de la norma) que se ha alcanzado un PL=d, lo que cumple el nivel PLr=d requerido.

Al igual que el ejemplo práctico de EN IEC 62061, sólo es necesario que **el cableado de los contactos espejo auxiliares normalmente cerrados de ambos contactores vaya a la entrada de supervisión de los dispositivos externos (EDM) del relé de seguridad para cambiar la arquitectura a categoría 4. Al hacerlo el cálculo del PL pasará de un nivel d a un nivel e.**

Teniendo en cuenta que disponemos de una arquitectura de categoría 4, un $MTTF_d$ alto y una Cobertura media del diagnóstico alta (DC_{avg}), al consultar la Tabla 7 de la norma se demuestra que el nivel de prestaciones resultante es PL=e, que coincide con el PLr.



* En varias aplicaciones la consecución del Performance Level c por la categoría 1 puede no ser suficiente.
En este caso una categoría superior, p. ej. 2 o 3, puede ser elegida.

• PASO 6: Validación – comprobar el funcionamiento y probar donde sea necesario (EN ISO 13849-2).

Fuentes de información

Legislación

- Directiva europea de máquinas 2006/42/CE.
- EN ISO 14121-1 Seguridad de las máquinas. Evaluación del riesgo - Parte 1: Principios.
- EN ISO 12100-1 Seguridad de las máquinas – Conceptos básicos, principios generales para el diseño - Parte 1: Terminología básica, metodología.
- EN ISO 12100-2 Seguridad de las máquinas. Conceptos básicos, principios generales para el diseño - Parte 2: Principios técnicos.
- EN IEC 60204 Seguridad de las máquinas. Equipo eléctrico de las máquinas. Requisitos generales.
- EN ISO 13850 Seguridad de las máquinas. Parada de emergencia. Principios de diseño.
- EN IEC 62061 Seguridad de las máquinas, Seguridad funcional de sistemas de control eléctricos, electrónicos y programables relativos a la seguridad.
- EN IEC 61508 Seguridad funcional de los sistemas eléctricos / electrónicos / electrónicos programables relacionados con la seguridad.
- EN ISO 13849-1 Seguridad de las máquinas - Partes de los sistemas de mando relativas a la seguridad - Parte 1: Principios generales para el diseño.

Documentos de Schneider Electric

- Schneider Electric “Soluciones de seguridad Preventa”.

Schneider Electric website

- www.oem.schneider-electric.com

Anexos - arquitecturas

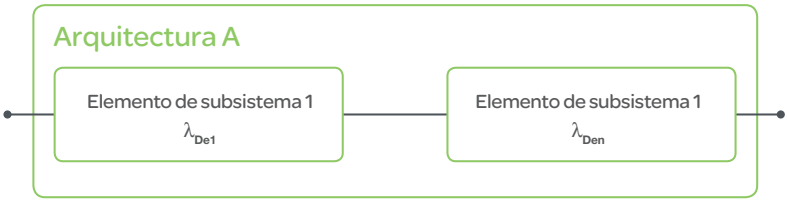
Anexo 1

Arquitecturas de EN IEC 62061

> Arquitectura A: Tolerancia a cero fallos, sin función de diagnóstico
Donde: λ_{De} es la tasa de fallos peligrosos del elemento

$$\lambda_{DSSA} = \lambda_{De1} + \ldots + \lambda_{Den}$$

$$PFH_{DSSA} = \lambda_{DSSA} \bullet 1h$$



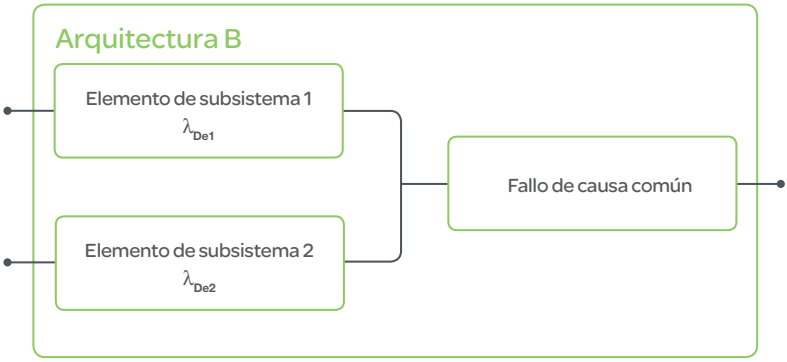
Representación lógica del subsistema

> Arquitectura B: Tolerancia a un único fallo, sin función de diagnóstico
Donde: T_1 es el intervalo de test de pruebas o la vida útil, la cifra que sea menor (Dato proporcionado por el proveedor o calcular para el producto electromecánico mediante: $T_1 = B_{10}/C$).

β es la susceptibilidad a fallos de causa común
(β se determina mediante la Tabla de puntuación F.1 de EN IEC 62061).

$$\lambda_{DSSB} = (1 - \beta)^2 \bullet \lambda_{De1} \bullet \lambda_{De2} \bullet T_1 + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DSSB} = \lambda_{DSSB} \bullet 1h$$



Representación lógica del subsistema

> Arquitectura C: Tolerancia a cero fallos, con una función de diagnóstico

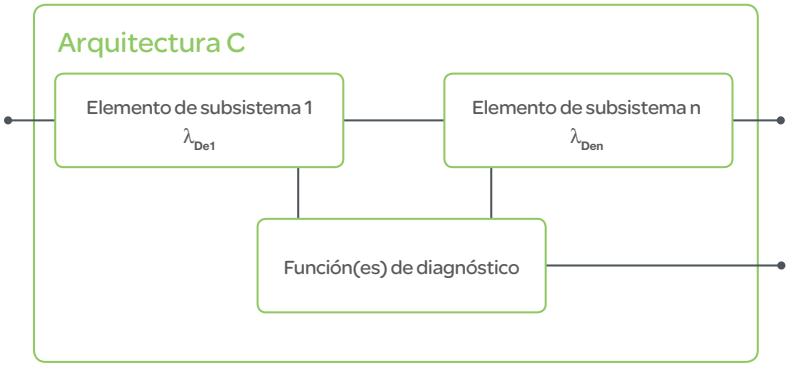
Donde: DC es la cobertura del diagnóstico = $\Sigma \lambda_{DD}/\lambda_D$

λ_{DD} es la tasa de fallos peligrosos detectados y λ_D es la tasa de los fallos peligrosos totales

La DC depende de la efectividad de la función de diagnóstico utilizada en este subsistema

$$\lambda_{DSSC} = \lambda_{De1} \bullet (1 - DC_1) + ... + \lambda_{Den} \bullet (1 - DC_n)$$

$$PFH_{DSSC} = \lambda_{DSSC} \bullet 1h$$



Representación lógica del subsistema

> Arquitectura D: Tolerancia a un único fallo, con una función de diagnóstico

Donde: T_1 es el intervalo de test de pruebas o la vida útil, lo que sea menor

T_2 es el intervalo de test de diagnóstico

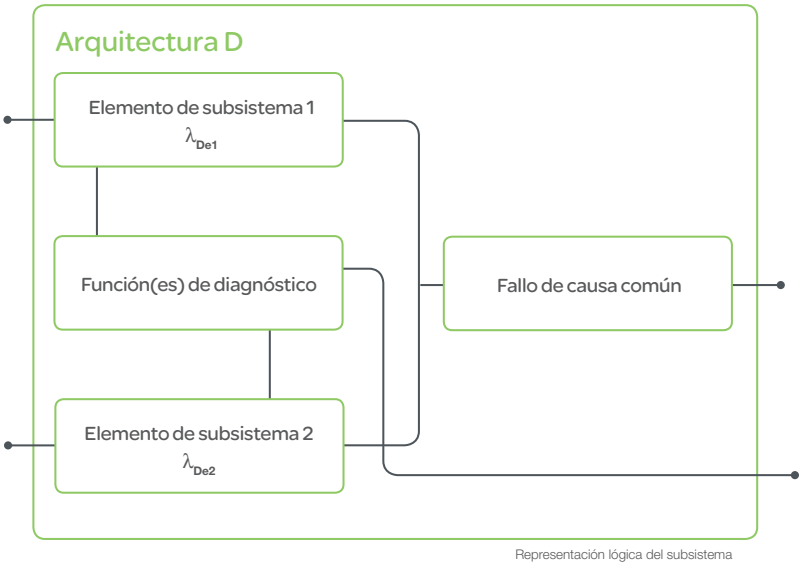
(Al menos igual al tiempo entre las demandas de la función de seguridad)

β es la susceptibilidad a los fallos de causa común

(Se determinará con la tabla de puntuaciones del Anexo F de EN IEC 62061)

DC es la cobertura del diagnóstico = $\Sigma \lambda_{DD}/\lambda_D$

(λ_{DD} es la tasa de fallos peligrosos detectados y λ_D es la tasa de los fallos peligrosos totales)



Representación lógica del subsistema

Para elementos del Subsistema de diseño distinto

λ_{De1} = tasa de fallos peligrosos del elemento del subsistema 1;
DC_1 = cobertura del diagnóstico del elemento del subsistema 1.
λ_{De2} = tasa de fallos peligrosos del elemento del subsistema 2;
DC_2 = cobertura del diagnóstico del elemento del subsistema 2.

$$\lambda_{DSSD} = (1-\beta)^2 \{[\lambda_{De1} \bullet \lambda_{De2} (DC_1 + DC_2)] \bullet T_2/2 + [\lambda_{De1} \bullet \lambda_{De2} \bullet (2-DC_1-DC_2)] \bullet T_1/2\} + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$
$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

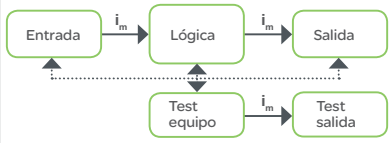
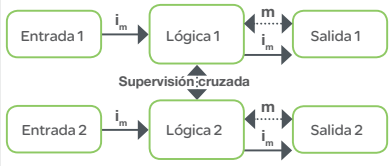
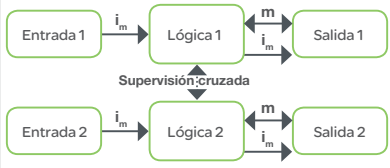
Para los elementos del Subsistema del mismo diseño

λ_{De} = tasa de fallos peligrosos de un elemento de un subsistema 1 o 2;
DC = cobertura del diagnóstico del elemento del subsistema 1 o 2.

$$\lambda_{DSSD} = (1-\beta)^2 \{[\lambda_{De}^2 \bullet 2 \bullet DC] T_2/2 + [\lambda_{De}^2 \bullet (1-DC)] \bullet T_1\} + \beta \bullet \lambda_{De}$$
$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

Anexo 2

Categorías en EN ISO 13849-1

Categoría	Descripción	Ejemplo
Categoría B	Cuando se produce un fallo, se puede perder la función de seguridad	
Categoría 1	Cuando se produce un fallo, se puede perder la función de seguridad, pero el $MTTF_d$ de cada canal en la Categoría 1 es superior al de la Categoría B. Por consiguiente, la pérdida de la función de seguridad es menos probable.	
Categoría 2	El comportamiento del sistema de Categoría 2 permite que: si se produce un fallo, puede producirse la pérdida de la función de seguridad entre los ciclos de comprobaciones; la pérdida de la función de seguridad se detecta mediante ciclos de comprobación.	
Categoría 3	El SRP/CS para la Categoría 3 debe diseñarse de modo que un único fallo en cualquiera de estas partes relacionadas con la seguridad no produzcan la pérdida de la función de seguridad. Siempre que sea razonablemente posible, este único fallo debe detectarse antes o en la siguiente demanda de la función de seguridad	
Categoría 4	El SRP/CS para la Categoría 4 debe diseñarse de modo que un único fallo en cualquiera de las partes relacionadas con la seguridad no produzca la pérdida de la función de seguridad, y este único fallo se detecte antes o en la siguiente demanda de las funciones de seguridad, es decir, de inmediato, al activar o al finalizar el ciclo de operación de la máquina. Si esta detección no es posible, una acumulación de fallos sin detectar no debe producir la pérdida de la función de seguridad.	

Make the most of your energy

> www.schneiderelectric.es

902·110·062

Soporte Técnico

en productos y aplicaciones

es-soportetecnico@es.schneider-electric.com

- > Elección
- > Asesoramiento
- > Diagnóstico

902·101·813

Servicio Posventa SAT

es-sat@es.schneider-electric.com

- > Reparaciones e intervenciones
- > Gestión de repuestos
- > Asistencia técnica **24** horas

> www.isefonline.es

Instituto Schneider Electric de Formación · Tel.: 934 337 003 · Fax: 934 337 039

Schneider Electric España, S.A.U.
Bac de Roda, 52, edificio A · 08019 Barcelona· Tel.: 93 484 31 00 · Fax: 93 484 33 07

ESMKT13009B11

Dep. legal: B. 12.677-2011

ESMKT13009B11