

ABB Drives

Guía técnica n.º 10 Seguridad funcional

ABB Drives

Guía técnica n.º 10

Seguridad funcional

© Copyright 2014 ABB. Todos los derechos reservados.

Las especificaciones pueden cambiar sin previo aviso.

3AUA0000163173 REV E 9.9.2014 #17230

Contenido

Limitación de responsabilidad	6
Acerca de esta guía.....	7
Parte 1 – Teoría y marco normativo	8
Seguridad y seguridad funcional.....	9
Directiva de Máquinas	10
Jerarquía del sistema de normas armonizadas europeo	11
Parte 2 – Normativa de Máquinas	14
Dos normas – IEC e ISO.....	14
Normas para la minimización de riesgos.....	15
Normas para sistemas de seguridad electrónicos.....	15
Normas de seguridad específicas para productos (normas Tipo C)	17
Norma específica para sistemas de convertidor relacionados con la seguridad	18
Funciones de seguridad normalizadas.....	18
Parte 3 – Pasos a seguir para cumplir con los requisitos de la Directiva de Máquinas	22
PASO 1: Gestión de la seguridad funcional.....	23
PASO 2: Evaluación de riesgos	24
PASO 3: Reducción de riesgos	26
PASO 4: Establecimiento de los requisitos de seguridad	28
PASO 5: Implementación de un sistema de seguridad funcional	32
PASO 6: Verificación del sistema de seguridad funcional	34
PASO 7: Validación de un sistema de seguridad funcional.....	38
PASO 8: Documentación de un sistema de seguridad funcional.....	38
PASO 9: Demostración de la conformidad.....	39
Glosario.....	40
Índice	42

Limitación de responsabilidad

Este documento es una guía informativa que pretende servir de ayuda a usuarios, especificadores y fabricantes de maquinaria, así como al personal implicado, para una mejor comprensión de los requisitos de la Directiva de Máquinas de la UE y las medidas necesarias para respetar dicha directiva con sus normas armonizadas.

Esta guía se ha elaborado a título informativo.

La información y los ejemplos de esta guía únicamente están destinados a un uso general y no ofrecen todos los detalles necesarios para implementar un sistema de seguridad.

ABB Oy Drives no acepta por ello ninguna responsabilidad por lesiones o daños directos o indirectos derivados del uso de la información contenida en este documento. El fabricante de la maquinaria siempre es responsable de la seguridad del producto y de su idoneidad conforme a las leyes vigentes. ABB se exime de cualquier responsabilidad derivada del uso de este documento.

Nota: parte del contenido de esta guía técnica son extractos de las normas ISO/IEC que están protegidas bajo copyright por la Comisión Electrotécnica Internacional (IEC) o por la Organización internacional para la estandarización (ISO).

Acerca de esta guía

Esta guía presenta la Directiva de Máquinas y las normas que es necesario considerar a la hora de diseñar una máquina con el objetivo de garantizar la seguridad funcional.

El propósito de este documento es explicar, en términos generales, cómo se lleva a cabo el proceso para cumplir con los requisitos de la Directiva de Máquinas y obtener el marcado CE. El marcado CE indica que la maquinaria cumple los requisitos de la Directiva.

Nota:

Este documento solo proporciona una descripción general del proceso para cumplir con los requisitos esenciales de la Directiva de Máquinas. El fabricante de la maquinaria sigue siendo el responsable último de la seguridad y la conformidad del producto.

El documento se divide en tres partes:

- Parte 1 – Teoría y marco normativo: presenta la idea subyacente a la seguridad funcional y cómo cumplir con la Directiva de Máquinas. También presenta la Directiva de Máquinas y explica la jerarquía del sistema de normas armonizadas europeo.
- Parte 2 – Normativa de máquinas - Presenta los dos sistemas de normas y enumera algunas normas de seguridad importantes y funciones de seguridad.
- Parte 3 – Pasos a seguir para cumplir con los requisitos de la Directiva de Máquinas: presenta nueve pasos para facilitar el proceso de cumplimiento de los requisitos esenciales de la Directiva de Máquinas.

Parte 1 – Teoría y marco normativo

Las leyes nacionales de los países miembros de la Unión Europea exigen que las máquinas cumplan los Requisitos Esenciales de Seguridad y Salud (EHSR, Essential Health and Safety Requirements) definidos en la Directiva de Máquinas y en sus normas armonizadas. Esto significa que todas las máquinas nuevas deben cumplir los mismos requisitos legales para su comercialización en cualquier país de la UE. Estas mismas normas gozan de reconocimiento en muchas regiones extracomunitarias, por ejemplo mediante tablas de equivalencias, lo que facilita el comercio de máquinas y su envío entre países dentro de la UE e incluso fuera de sus fronteras.

¿Por qué es necesario que las máquinas cumplan estos requisitos? Porque su cumplimiento contribuye a evitar accidentes y los daños asociados. Además, la conformidad con la Directiva de Máquinas y las normas armonizadas correspondientes garantiza a los fabricantes de maquinaria que han cumplido sus obligaciones al diseñar y entregar máquinas seguras de conformidad con las leyes nacionales.

Para los fabricantes, la mejora e innovación en las estrategias de seguridad se está convirtiendo en una forma de mejorar su productividad y competitividad en el mercado. El objetivo tradicional de los sistemas de seguridad convencionales ha sido lograr una seguridad operacional completa y satisfacer los requisitos legales. Esto se ha llevado a cabo con la incorporación de componentes mecánicos y eléctricos auxiliares, incluso en detrimento de la productividad. Los operadores pueden, en determinadas circunstancias, anular estos sistemas en un intento de aumentar la productividad, lo que puede provocar accidentes.

Los sistemas de seguridad modernos permiten garantizar la seguridad de los procesos y del operario a la vez que se mantiene la productividad. Un ejemplo de ello sería mantener una máquina en funcionamiento a velocidad baja para preservar la seguridad operativa. Gracias a las soluciones de seguridad modernas, la seguridad puede integrarse como parte de la funcionalidad de la máquina; las soluciones de seguridad ya no son ideas de última hora para cumplir las normas.

Los sistemas de seguridad pueden implementarse de manera eficaz siguiendo procesos definidos que permiten lograr unas prestaciones de seguridad concretas y el uso de subsistemas certificados a modo de bloques modulares para la creación de los sistemas de seguridad. El cumplimiento de las normas de seguridad se da por supuesto en el sector industrial, y algunos subsistemas certificados, como los convertidores de frecuencia, se están convirtiendo en una

auténtica exigencia del mercado. La seguridad de las máquinas se encuentra entre las áreas que registran un mayor crecimiento en el ámbito de la automatización industrial.

Seguridad y seguridad funcional

El objetivo de la seguridad es proteger a las personas y al medio ambiente frente a los accidentes y, en el caso que nos ocupa, frente a la maquinaria. Los sistemas de seguridad funcional cumplen esta función al reducir la probabilidad de que se produzcan situaciones indeseadas, minimizándose el número de incidentes al operar la maquinaria. Las normas de seguridad la definen como la no existencia de riesgos inaceptables. Los niveles de riesgo aceptables son definidos por medio de la reducción de riesgo requerida en las normas de seguridad de máquinas. Los fabricantes de maquinaria siempre deberían usar el mismo criterio de aceptabilidad (el más estricto) en todos los sectores del mercado, sin importar las diferencias regionales.

La forma más efectiva de eliminar riesgos es evitarlos mediante el diseño de máquinas intrínsecamente más seguras. Pero si no fuera posible o práctico reducir los riesgos en esta fase, a menudo la mejor opción es el uso de protecciones fijas o de seguridad funcional. Siempre que existe un sistema que permite realizar una parada de una máquina de manera rápida y segura o hacerla funcionar a baja velocidad durante periodos de tiempo concretos con el objetivo de reducir los riesgos, es posible obtener un aumento de la productividad y del tiempo de funcionamiento de la máquina, así como un comportamiento del sistema de seguridad menos brusco. Del mismo modo, se cumple con las obligaciones legales y se garantiza la seguridad de las personas y del entorno.

En el caso de las máquinas, la seguridad funcional suele ser sinónimo de sistemas fiables que monitorizan las aplicaciones de la máquina, llegando a asumir el control si el funcionamiento seguro se viera comprometido. Un sistema de seguridad es aquel que implementa las funciones de seguridad necesarias. Los sistemas de seguridad funcional están diseñados para detectar situaciones peligrosas o peticiones del usuario para garantizar seguridad y para llevar la máquina o proceso a un estado seguro como, por ejemplo un paro de emergencia.

La supervisión puede incluir la velocidad, la parada, el sentido de rotación y el reposo. Cuando el sistema de seguridad ejecuta una función de seguridad activa, por ejemplo la supervisión de la velocidad de arrastre, y el comportamiento del sistema se desvía de su objetivo (por ejemplo, el sistema funciona demasiado deprisa), el sistema de seguridad detecta la desviación y actúa para devolver la máquina a un estado de funcionamiento seguro. Esto se lleva a cabo, por ejemplo, parando la máquina de manera segura y disminuyendo el par del eje del motor.

Un sistema de seguridad no forma parte del funcionamiento estándar de una máquina, pero cualquier fallo en el mismo aumentará inmediatamente los riesgos relacionados con la operación de la máquina (la máquina podría estar funcionando normalmente, pero la función de seguridad no está disponible y puede ocurrir una situación peligrosa).

Directiva de Máquinas

La Directiva de Máquinas, junto con las normas armonizadas que la desarrollan, define los Requisitos Esenciales de Seguridad y Salud (EHSR) para maquinaria en el marco de la Unión Europea. Los requisitos EHSR se enumeran en el Anexo I de la Directiva de Máquinas.

El objetivo de la Directiva de Máquinas es garantizar que una máquina es segura, y que se ha diseñado y fabricado de forma que pueda ser utilizada, configurada y sometida a mantenimiento a lo largo de todas las fases de su vida útil, minimizando los riesgos para las personas y el entorno.

Los EHSR establecen que, en el proceso de búsqueda de soluciones para el diseño y la fabricación de máquinas seguras, los fabricantes de maquinaria tienen la obligación de aplicar los siguientes principios en el orden establecido (también conocido como método de los 3 pasos, EN ISO 12100):

1. Eliminar o minimizar los peligros en la medida de lo posible teniendo en cuenta los aspectos de seguridad durante las fases de diseño y fabricación de la máquina (diseñar máquinas intrínsecamente seguras).
2. Aplicar las medidas de protección necesarias para hacer frente a los peligros que no es posible eliminar.
3. Informar a los usuarios acerca de los riesgos aún existentes a pesar de la aplicación de todas las medidas de protección posibles, y especificar los requisitos relativos a la formación o al equipo de protección necesarios.

El cumplimiento de los EHSR de la Directiva de Máquinas permite al fabricante etiquetar la máquina con el marcado CE. El marcado CE indica que el fabricante garantiza que su producto cumple todas las normas relativas a la libre circulación de bienes, así como los requisitos esenciales de las Directivas europeas correspondientes, en este caso la Directiva de Máquinas.

Nota:

Es posible que existan otras directivas de obligado cumplimiento, por ejemplo la Directiva de Baja Tensión y la Directiva EMC. Esta guía sólo cubre los requisitos de la Directiva de Máquinas.

Nota:

La etiqueta del mercado CE conforme a la Directiva de Máquinas sólo puede aplicarse a una máquina completa y no a los componentes que la forman. Por lo tanto, el fabricante del producto, o el representante del fabricante, es el responsable del marcado CE, y no el fabricante del componente que está incluido en el producto final.

Como excepción, los componentes de seguridad a ser usados en las funciones de seguridad de la máquina, llevan el marcaje CE de acuerdo a la Directiva de Máquinas, del fabricante o representante del componente en Europa.

El fabricante de la máquina es responsable de llevar a cabo las evaluaciones de riesgos correspondientes, siguiendo los pasos indicados en la Parte 3, y de garantizar el cumplimiento de los requisitos. El fabricante de componentes es responsable de efectuar las pruebas de prestaciones de seguridad (nivel SIL/PL) en la función de seguridad del componente en cuestión, siempre que se use correctamente.

En este caso, un componente de seguridad podría ser un relé de seguridad o un convertidor de frecuencia con funciones de seguridad integradas.

Jerarquía del sistema de normas armonizadas europeo

El Comité Europeo de Normalización (CEN) y el Comité Europeo de Normalización Electrotécnica (CENELEC) redactan las normas Europeas “EN”, que pueden ser usadas como normas armonizadas en todos los países miembros de la UE. Todas las normas armonizadas llevan el prefijo “EN” (no todas las normas EN son armonizadas).

En la página web de la Comisión Europea, <http://ec.europa.eu>, puede encontrarse una lista de las normas armonizadas.

La mayoría de las normas armonizadas hacen referencia a una o más directivas. Para garantizar que se siguen los requisitos esenciales de la Directiva de Máquinas, es aconsejable aplicar las normas europeas armonizadas correspondientes. El diseño de máquinas conforme a estas normas permite a los fabricantes demostrar que cumplen con la Directiva de Máquinas y, en general, no requiere la certificación de terceros.

Nota:

Tenga en cuenta las excepciones para las máquinas enumeradas en el Anexo IV de la Directiva de Máquinas.

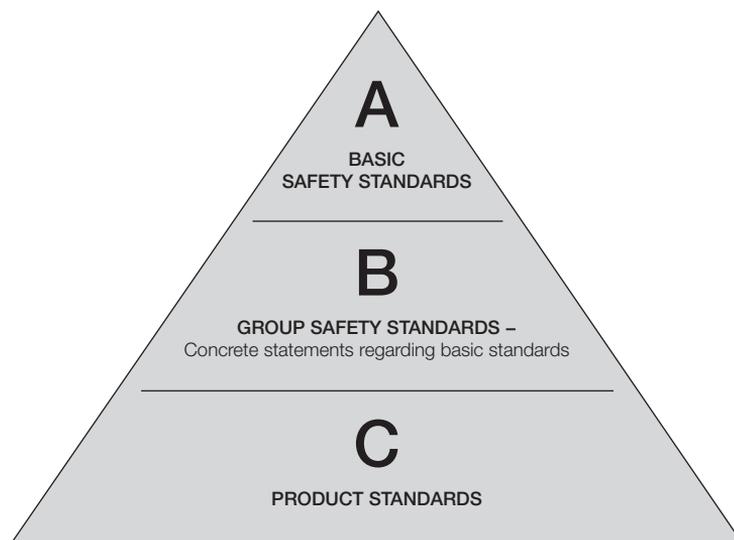


Figura 1-1 Jerarquía de las normas armonizadas europeas

- Las normas del Tipo C son específicas para una máquina o clase de máquina. Si existe una norma del Tipo C para una máquina, las normas asociadas del Tipo B, y posiblemente las del Tipo A, pasan a ser secundarias. Al diseñar funciones de seguridad, las normas del Tipo C definen requisitos adicionales obligatorios para las máquinas a las que están destinadas. Sin embargo, si no existe una norma del Tipo C para la máquina, las normas del Tipo A y del Tipo B proporcionan ayuda para el diseño y la fabricación de máquinas que cumplan los requisitos de la Directiva de Máquinas.
- Las normas del Tipo B tratan sobre los requisitos de seguridad comunes en el diseño de la mayoría de máquinas. Estas normas proporcionan información sobre los posibles riesgos y el modo de gestionarlos, con la ayuda de un proceso de reducción de riesgos. Las normas del Tipo B se dividen en dos grupos, B1 y B2. Las normas del Tipo B1 tratan los aspectos de seguridad concretos y las normas del Tipo B2 se encargan de los equipos de seguridad en general. Las normas del Tipo B1 son, por ejemplo, las EN 62061:2005 y EN ISO 13849-1:2008. Las normas del Tipo B2 incluyen normas para definir los paros de emergencia, como la EN ISO 13850:2008.
- Los estándares de tipo A manejan conceptos básicos, terminología y principios de diseño. Estos estándares, por sí mismos, no son suficientes para asegurar la conformidad con la Directiva de Máquinas. El único estándar de tipo A armonizado bajo la Directiva de Máquinas es el estándar básico de seguridad para la evaluación y reducción de riesgos, EN ISO 12100.

Nota:

La aplicación de normas armonizadas no es obligatoria, pero ofrecen recomendaciones y orientación para cumplir los requisitos de la Directiva de Máquinas, que sí deben cumplirse.

Parte 2 – Normativa de Máquinas

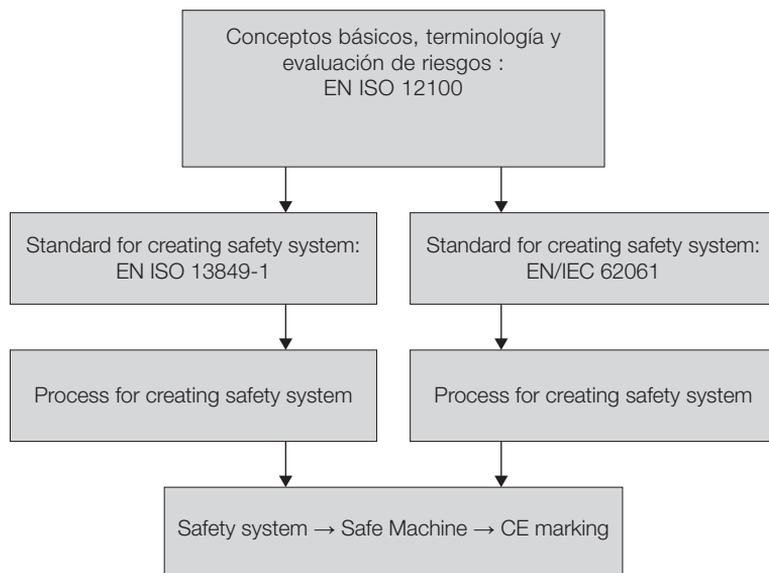


Figura 2-1 Introducción de las normas

Dos normas – IEC e ISO

Es posible seguir dos normas alternativas para implementar los sistemas de seguridad funcional de conformidad con la Directiva de Máquinas: la norma de la Organización Internacional para la Normalización (ISO) y la norma de la Comisión Electrotécnica Internacional (IEC).

El uso como referencia de cualquiera de estas normas ofrece unos resultados muy similares, y tanto los niveles de integridad de la seguridad (SIL) como los niveles de prestaciones (PL) son, de hecho, comparables. Para más información, véase la tabla comparativa en la Parte 3, paso 6.

Nota:

Corresponde al fabricante de la máquina decidir qué norma de creación de sistemas de seguridad usará (EN ISO 13849-1 o EN/IEC 62061), y a continuación deberá seguir la norma elegida durante todo el proceso para garantizar la coherencia con dicha norma.

Las normas CEN se basan en las normas ISO y básicamente son para equipos mecánicos (las nuevas normas se numeran en la serie 1xxxx), mientras que las norma CENELEC se basan en las IEC (las nuevas normas se numeran en la serie 6xxxx).

Nota:

Las normas ISO son presentadas en este documento como EN ISO, usando la notación de la lista de estándares armonizados. Las normas basadas en IEC son presentadas con EN/IEC, mostrando ambos prefijos, aunque los estándares IEC IEC se muestran sólo con el prefijo EN en la lista de estándares armonizados (p.e. EN 62061).

Normas para la minimización de riesgos

Las normas de seguridad básica para la minimización de riesgos incluyen:

- **EN ISO 12100:2010**
(Seguridad de las máquinas. Principios generales para el diseño)

EN ISO 12100 proporciona a los diseñadores la terminología básica, un marco general y una guía, incluyendo una estrategia para la reducción del riesgo (método de los tres pasos).

Nota:

Cualquier otra referencia a estas normas en este documento siempre se aplica a las versiones de estas normas mencionadas arriba.

Normas para sistemas de seguridad electrónicos

A continuación se enumeran las normas para sistemas de seguridad electrónicos:

- **EN ISO 13849-1:2008/AC:2009** (Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño),
- **EN ISO 13849-2:2012** (Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 2: Validación)
- **EN/IEC 62061:2005+AC:2010** (Seguridad de las máquinas. Seguridad funcional de sistemas de mando eléctricos, electrónicos y programables relativos a la seguridad),
- **IEC 61508:2010** (Seguridad funcional de sistemas de mando eléctricos, electrónicos y programables relativos a la seguridad), y
- **EN/IEC 60204-1:2006+AC:2010** (Seguridad de las máquinas. Equipamiento eléctrico de las máquinas. Requisitos generales).

Nota:

Cualquier otra referencia a estas normas en este documento siempre se aplica a las versiones de estas normas mencionadas arriba.

La norma EN ISO 13849-1 es una norma que facilita instrucciones para que los diseñadores fabriquen máquinas seguras. Dichas

instrucciones incluyen recomendaciones para el diseño, la integración y la validación de los sistemas. Esta norma puede utilizarse para partes de los sistemas de mando relativas a la seguridad y varios tipos de maquinaria, con independencia de la tecnología o la fuente de energía utilizada. Esto incluye también los requisitos específicos para componentes relacionados con la seguridad que cuentan con sistemas electrónicos programables. Esta norma cubre la totalidad de la función de seguridad en todos los dispositivos incluidos (es decir, una cadena de seguridad completa como por ejemplo sensor-lógica-actuador).

La norma define cómo se determina el Nivel de prestaciones (PL) y se verifica el PL alcanzado en un sistema. El PL describe la forma en que un sistema de seguridad es capaz de llevar a cabo una función de seguridad en situaciones predecibles. Existen cinco posibles niveles de prestaciones: a, b, c, d y e. El nivel "e" representa la mayor fiabilidad de seguridad y el nivel "a", la menor.

EN ISO 13849-2 especifica el proceso de validación de las funciones de seguridad diseñadas conforme a EN ISO 13849-1.

EN/IEC 62061 es una norma para el diseño de sistemas eléctricos de seguridad. Se trata de una norma específica para el sector de maquinaria dentro del marco de la norma IEC 61508. EN/IEC 62061 incluye recomendaciones para el diseño, la integración y la validación de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad para máquinas. Esta norma cubre toda la cadena de seguridad, por ejemplo sensor-lógica-actuador. No es necesario certificar los subsistemas individuales si la función de seguridad en su conjunto cumple los requisitos definidos. No obstante, se recomienda encarecidamente el uso de subsistemas certificados a modo de bloques modulares, ya que esto puede representar un ahorro de esfuerzos considerable en el proceso de diseño y de verificación.

Nota:

Al contrario que la norma EN ISO 13849-1, EN/IEC 62061 no incluye los requisitos para equipos de mando no eléctricos relativos a la seguridad para maquinaria.

Esta norma define cómo determinar el Nivel de Integridad de la Seguridad (SIL) para completar funciones de seguridad. En cambio, para la subsistemas de seguridad se utiliza el Límite de Reclamaciones del Nivel de Integridad de la Seguridad (SIL CL). El SIL y el SIL CL son una representación de la capacidad de la reducción de riesgos de las funciones y subsistemas de seguridad. Existen cuatro niveles SIL posibles: 1, 2, 3 y 4. "SIL 4" corresponde al nivel más alto de integridad de la seguridad y "SIL 1", al más bajo. En el caso de la maquinaria, sólo se utilizan los niveles de 1 a 3.

La **IEC 61508** es una norma de seguridad funcional básica. Esta cubre el ciclo de vida de los sistemas que contengan componentes eléctricos y/o electrónicos y/o electrónicos programables usados para llevar a cabo funciones de seguridad. La IEC 61508 no es una norma armonizada, pero es la más importante que describe los requisitos y los métodos empleados en el diseño de sistemas de mando relacionados con la seguridad que incluyen hardware y software complejo. La IEC 61508 se utiliza normalmente en el diseño de subsistemas de seguridad certificables. Las normas EN ISO 13849-1 y EN/IEC 62061 se basan en los principios establecidos en IEC 61508.

La **EN/IEC 60204-1** proporciona recomendaciones y requisitos para equipos eléctricos de máquinas con el objetivo de mejorar su seguridad y utilización.

Normas de seguridad específicas para productos (normas Tipo C)

Las normas de seguridad específicas para productos, conocidas como normas del Tipo C, se encargan de una máquina o clase de máquinas concreta y se basan en una presunción de conformidad respecto a los EHSR cubiertos por la norma.

Hay que tener en cuenta que:

- Los requisitos especificados en las normas del Tipo C normalmente prevalecen sobre los requisitos establecidos por las normas de seguridad general EN/IEC 62061, EN ISO 13849-1, etc.).
- Las normas del Tipo C pueden establecer requisitos SIL/PL para algunas funciones de seguridad específicas. Al menos deben cumplirse estos requisitos, independientemente de los resultados de la evaluación del análisis de riesgos (aunque siempre es necesario realizar evaluaciones de riesgo).

Nota:

Incluso si las listas de posibles peligros que pueden afectar a la máquina, creadas durante la evaluación de riesgos, y la norma del Tipo C son idénticas, la norma puede que no tenga en cuenta todos los EHSR pertinentes. La norma siempre debe inspeccionarse minuciosamente para determinar qué peligros podrían haberse excluido de la lista.

Norma específica para sistemas de convertidor relacionados con la seguridad

La norma específica para sistemas de convertidor relacionados con la seguridad es:

- **EN/IEC 61800-5-2:2007** (Convertidores eléctricos de velocidad ajustable. Requisitos de seguridad funcional).

Nota:

Cualquier otra referencia a esta norma en este documento sólo se aplica a la versión de esta norma mencionada arriba.

EN/IEC 61800-5-2 facilita especificaciones y recomendaciones para sistemas de convertidor usados en aplicaciones relacionadas con la seguridad. Se trata de una norma de producto que presenta aspectos relativos a la seguridad dentro del marco de la IEC 61508 e introduce requisitos para sistemas de convertidor cuando se usan como subsistemas en sistemas de seguridad.

Funciones de seguridad normalizadas

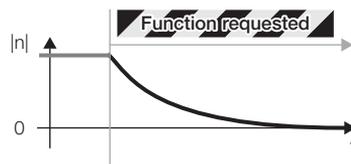
La norma EN/IEC 61800-5-2 define funciones de seguridad para sistemas con convertidores de frecuencia. Un convertidor de frecuencia puede ofrecer una o más de estas funciones. A continuación se muestran algunos ejemplos:

Safe torque off (STO)

Cuando está activado esta función lleva la máquina a un estado sin par de manera segura y/o evita que arranque accidentalmente.

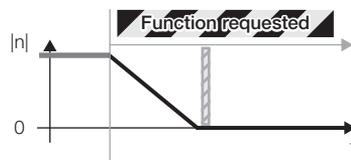
Nota:

El Safe torque off no protege contra riesgos eléctricos.



Paro seguro 1 (SS1, Safe Stop 1)

Cuando está activado la función SS1 para el motor de manera segura, iniciando la función STO por debajo de una velocidad determinada o tras un límite de tiempo definido.



Paro seguro 2 (SS2, Safe Stop 2)

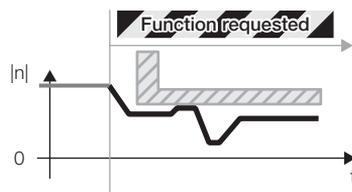
Cuando está activado la función SS2 para el motor de manera segura, iniciando la función SOS por debajo de una velocidad determinada o tras un límite de tiempo definido.

Paro de funcionamiento seguro (SOS, Safe Operating Stop)

Cuando está activada esta función mantiene el motor en un estado de reposo seguro, a la vez que mantiene el par del motor.

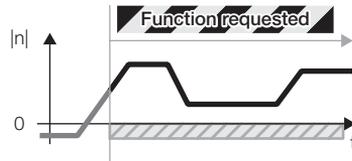
Velocidad limitada con seguridad (SLS, Safely-limited speed)

Cuando está activada la función SLS evita que el motor supere el límite de velocidad especificado.



Direccionamiento seguro (SDI, Safe direction)

Cuando está activada esta función evita que el eje del motor gire en un sentido no deseado.

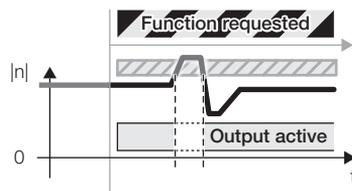


Control seguro de frenos (SBC, Safe brake control)

La función SBC proporciona una salida segura para controlar frenos (mecánicos) externos.

Monitorización de velocidad segura (SSM, Safe speed monitor)

Cuando está activada la función SSM proporciona una salida segura que indica que la velocidad está por debajo del límite de velocidad especificado.



Véase la norma EN/IEC 61800-5-2 para más ejemplos sobre funciones de seguridad.

Nota:

Las funciones SOS, SLS y SDI de las funciones mencionadas son funciones de monitorización, esto es, monitorizan de manera segura que el movimiento o el paro están dentro de los límites definidos. Si estas funciones detectan que el movimiento está fuera de los límites, activan una función de reacción de fallo, que típicamente es el Safe torque off (STO).

Operaciones de emergencia

La norma EN/IEC 60204-1 define dos operaciones de emergencia: la desconexión de emergencia y el paro de emergencia.

Desconexión de emergencia

La función de desconexión de emergencia desconecta la alimentación a un sistema, o a parte de este, si surge el riesgo de descarga eléctrica.

Esta función requiere el uso de componentes de conmutación externos y no puede lograrse con funciones del convertidor como la función **Safe torque off (STO)**.

Paro de emergencia

La función de paro de emergencia debe operar de manera que cuando se active, se detenga el movimiento peligroso de la maquinaria y se inhabilite el arranque de la máquina en cualquier caso, incluso tras el rearme. El rearme del paro de emergencia sólo permite arrancar de nuevo la máquina.

Esta función puede detener cualquier movimiento peligroso llevando a cabo las siguientes acciones:

- tasa de deceleración óptima hasta detención completa de la máquina
- utilizando una de las dos categorías de paro de emergencia, 0 o 1, o
- una secuencia de desconexión predefinida.

Paro de emergencia, paro categoría 0 significa que se interrumpe inmediatamente la alimentación al motor. Es equivalente a la función **Safe torque off (STO)**, definida por la norma EN 61800-5-2.

Paro de emergencia, paro categoría 1 significa que la velocidad de la máquina desciende hasta el reposo mediante una deceleración controlada, y a continuación se interrumpe la alimentación al motor. Es equivalente a la función **Paro seguro 1 (SS1)**, definida por la norma EN 61800-5-2.

Con su actuación, la función de paro de emergencia no debe crear ningún peligro adicional o requerir de ninguna acción adicional del operador de la máquina.

Nota:

La norma EN ISO 13850:2008 presenta los principios de diseño de una función de paro de emergencia.

Prevención de arranque inesperado

Una de las condiciones más importantes de las máquinas seguras es garantizar que una máquina permanezca parada cuando haya personas presentes en una zona peligrosa.

La función **Safe torque off** se puede usar para implementar de manera efectiva la función de prevención de arranque inesperado, efectuando por lo tanto paros seguros cortando la alimentación al motor pero manteniéndola en los circuitos principales de mando del convertidor. La función de prevención de arranque inesperado requiere, por ejemplo, de un interruptor que pueda bloquearse además de la función STO.

Los principios y requisitos de la función de prevención de arranque inesperado se describen en la norma EN 1037:1995+A1 2008. Otra norma que cubre la prevención de arranque inesperado es la ISO 14118:2000.

Parte 3 – Pasos a seguir para cumplir con los requisitos de la Directiva de Máquinas

La Directiva de Máquinas exige que la maquinaria sea segura. Sin embargo, nunca es posible eliminar por completo los riesgos. El objetivo es minimizar el riesgo.

La conformidad con la Directiva de Máquinas se consigue si:

- se cumplen los requisitos establecidos en las normas armonizadas, o
- un organismo autorizado efectúa un examen para la aprobación de la máquina.

El proceso de cumplimiento de los EHSR de la Directiva de Máquinas usando las normas armonizadas puede dividirse en nueve pasos:

- **Paso 1: Gestión de la seguridad funcional.** Gestionar la seguridad funcional a lo largo del ciclo de vida de la máquina.
- **Paso 2: Evaluación de riesgos.** Análisis y evaluación de riesgos.
- **Paso 3: Reducción de riesgos.** Eliminar o minimizar los riesgos mediante el diseño y la documentación.
- **Paso 4: Establecimiento de los requisitos de seguridad.** Definir la funcionalidad y las prestaciones de seguridad necesarias para eliminar el riesgo o reducirlo hasta un nivel aceptable.
- **Paso 5: Implementación del sistema de seguridad funcional.** Diseño y creación de las funciones de seguridad.
- **Paso 6: Verificación del sistema de seguridad funcional.** Garantizar que el sistema de seguridad cumple los requisitos definidos.
- **Paso 7: Validación del sistema de seguridad funcional.** Revisar el sistema de seguridad implementado contra la evaluación de riesgos y para asegurarse de que el sistema de seguridad realmente sirve para reducir los riesgos como se espera.
- **Paso 8: Documentación del sistema de seguridad funcional.** Documentar el diseño y elaborar documentación para el usuario.
- **Paso 9: Proporción del cumplimiento.** Demostrar la conformidad de la máquina con los EHSR de la Directiva de Máquinas mediante evaluaciones de conformidad y documentos técnicos.

Cada uno de estos pasos se explica con más detalle en los capítulos siguientes.

Actualización de la maquinaria existente

Las siguientes cuestiones deben considerarse al actualizar los requisitos de seguridad para máquinas existentes:

- Máquinas que ya poseen el marcado CE: los nuevos componentes que se añadan a la máquina también deben poseer el marcado CE de acuerdo con las directivas relevantes tales como la Directiva de Baja Tensión y CEM (también los componentes de seguridad de acuerdo con la Directiva de Máquinas). Deberá definirse en cada caso cómo se aplican los nuevos componentes al sistema antiguo de conformidad con la Directiva de Máquinas.
- Máquinas que no poseen el marcado CE: el nivel de seguridad de la máquina puede mantenerse sustituyendo viejos componentes por nuevos que posean el marcado CE.

Por último, queda a criterio de la autoridad correspondiente decidir si el cambio ha sido suficientemente amplio como para requerir una actualización del nivel de seguridad.

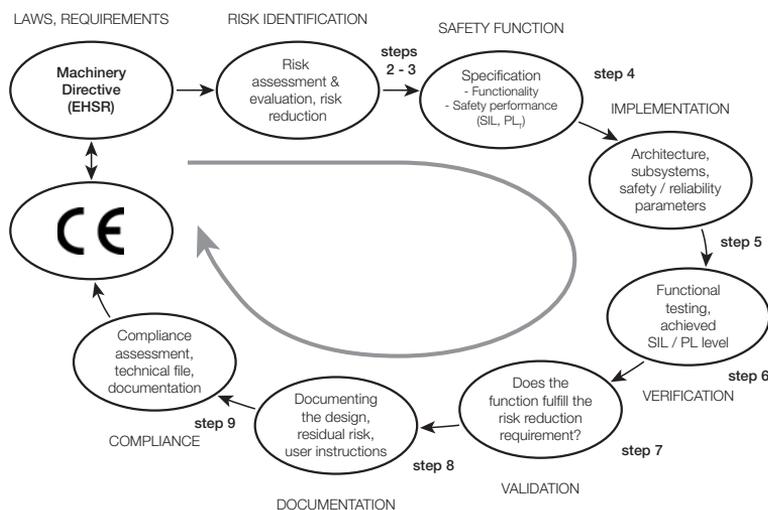


Figura 3-1 Diagrama de flujo para el cumplimiento de los requisitos de la Directiva de Máquinas

PASO 1: Gestión de la seguridad funcional

Para lograr la seguridad funcional requerida, es necesario implementar tanto un sistema de gestión de proyectos como de gestión de calidad que cumpla, por ejemplo, con las normas IEC 61508 o ISO 9001. El sistema de gestión se puede especificar en la forma de un plan de seguridad.

Plan de seguridad

En la norma EN/IEC 62061 se especifica un plan de seguridad para el proceso que permite cumplir con los requisitos de la Directiva de Máquinas. Este plan debe ser creado y documentado para cada sistema de seguridad, y actualizarse siempre que sea necesario.

Plan de seguridad:

- identifica todas las actividades pertinentes,
- describe la política y la estrategia para cumplir con los requisitos de seguridad funcional,
- identifica las responsabilidades,
- identifica o establece los procedimientos y los recursos para la documentación,
- describe la estrategia de gestión de la configuración, e
- incluye planes de verificación y validación.

Nota:

Aunque las actividades enumeradas anteriormente no se especifican exhaustivamente en la norma EN ISO 13849-1, es necesario llevar a cabo actividades similares para cumplir en su totalidad con los requisitos de la Directiva de Máquinas.

Una vez se ha creado el plan de seguridad (conforme a la norma EN/IEC 62061), se inicia la evaluación de riesgos.

PASO 2: Evaluación de riesgos

La evaluación del riesgo es un proceso que analiza y valora los riesgos, que son considerados como una combinación de las consecuencias del daño y la probabilidad de que se produzca este daño ante la exposición a un peligro.

Nota:

Según la nueva Directiva de Máquinas 2006/42/CE, es obligatorio documentar y llevar a cabo una evaluación de riesgos de la máquina.

La Directiva de Máquinas 2006/42/CE exige a los fabricantes llevar a cabo evaluaciones de riesgos, cuyos resultados deben tenerse en cuenta a la hora de diseñar una máquina. Cualquier riesgo que se considere como "elevado" debe reducirse a un nivel aceptable mediante cambios en el diseño o aplicando las medidas de seguridad apropiadas. Los estándares EN 62061 y EN ISO 13849-1 proporcionan métodos numéricos para la evaluación de riesgos y niveles de reducción.

El proceso de evaluación de riesgos proporciona a los diseñadores los requisitos para que conciban una maquinaria intrínsecamente segura. La evaluación de los riesgos en la fase de diseño es muy importante, pues siempre resulta más efectivo que proporcionar instrucciones al usuario acerca de cómo operar el equipo de forma segura.

Conforme a la norma EN ISO 12100-1, la evaluación de riesgos consta de dos partes: el análisis de riesgos y la valoración de riesgos. Por análisis de riesgos entendemos identificar y estimar los

riesgos, mientras que la valoración de riesgos se refiere a decidir si el riesgo es aceptable, o si es necesaria una reducción del mismo. La valoración de riesgos se lleva a cabo sobre la base de los resultados del análisis de riesgos. Las decisiones referentes a la necesidad de reducir los riesgos se toman de acuerdo con el procedimiento de valoración de riesgos.

Pista: La herramienta de diseño de seguridad funcional de ABB es una herramienta PC que proporciona un modo conveniente de llevar a cabo la evaluación de riesgo numéricamente de acuerdo con los estándares de maquinaria EN/IEC 62061 o EN ISO 13849-1.

Nota:

La valoración de riesgos debe ser realizada de forma independiente para cada peligro.

Los cuatro pasos de la valoración de riesgos:

1. Determinar los límites y el uso previsto de la máquina.
Estos límites son:
 - límites de uso
 - límites espaciales
 - límites ambientales o medioambientales
 - límites de vida útil
2. Identificar los peligros que podría generar la máquina.
3. Estimar los riesgos identificados uno a uno.
 - Gravedad del riesgo (consecuencias potenciales)
 - Probabilidad del riesgo (frecuencia, probabilidad, evitabilidad)
4. Evaluar el riesgo: ¿Es necesario reducir el riesgo?
 - Sí: Aplicar medidas para la reducción de riesgos y volver al Paso 2 del análisis de riesgos.

Nota:

El método de los tres pasos para la reducción de riesgo de acuerdo con la EN ISO 12100 se presenta en el próximo capítulo.

- **NO:** Se ha cumplido el objetivo de reducción de riesgos y el proceso se da por terminado.

Documente el proceso de evaluación de riesgos y los resultados obtenidos para cada peligro.

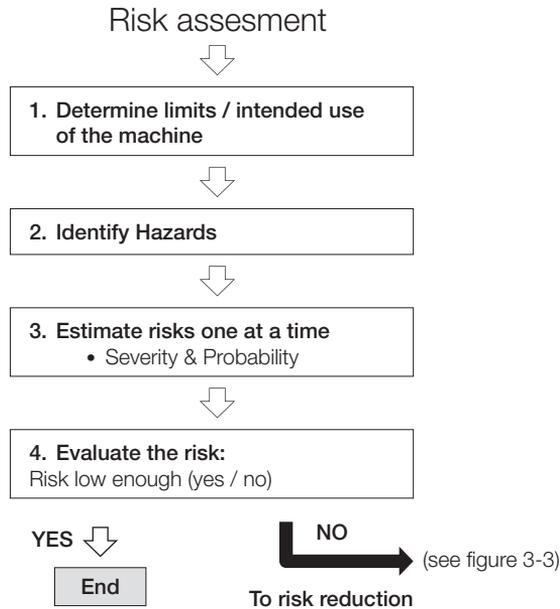


Figura 3-2 Evaluación y valoración de riesgos conforme a EN ISO 12100

Una vez se ha llevado a cabo la evaluación de riesgos, existen dos opciones dependiendo del resultado de la evaluación:

Opción 1

Si la evaluación concluye que la reducción de riesgos no es necesaria, entonces la máquina ha alcanzado el nivel adecuado de seguridad requerido por la Directiva de Máquinas.

Nota:

Los riesgos restantes deben documentarse en los manuales de operación y mantenimiento correspondientes. Siempre existe algún riesgo residual.

Opción 2

Si la evaluación revela que el riesgo continúa siendo inaceptable, se inicia el proceso de reducción del riesgo.

PASO 3: Reducción de riesgos

La forma más efectiva de minimizar riesgos es hacerlo durante la fase de diseño, por ejemplo, modificando el diseño de la máquina o el proceso de trabajo. Si esto no fuera posible, deben reducirse los riesgos y asegurarse su conformidad con los requisitos de la Directiva de Máquinas mediante la aplicación de sus normas armonizadas.

Si la evaluación de riesgos concluye que es necesario reducir el riesgo, se crea una estrategia de minimización de riesgos. La norma EN ISO 12100-1 divide el método para la reducción de riesgos en tres pasos principales (método de los tres pasos):

Método de los 3 pasos

1. Medidas de diseño intrínsecamente seguras: creación de un diseño más seguro, modificación del proceso, eliminación del riesgo mediante el diseño.
2. Medidas de protección y salvaguarda complementarias: funciones de seguridad, protección fija.
3. Información para el uso (gestión del riesgo residual):
 - dispositivos, señales y signos de aviso en la máquina y
 - en las instrucciones de funcionamiento.

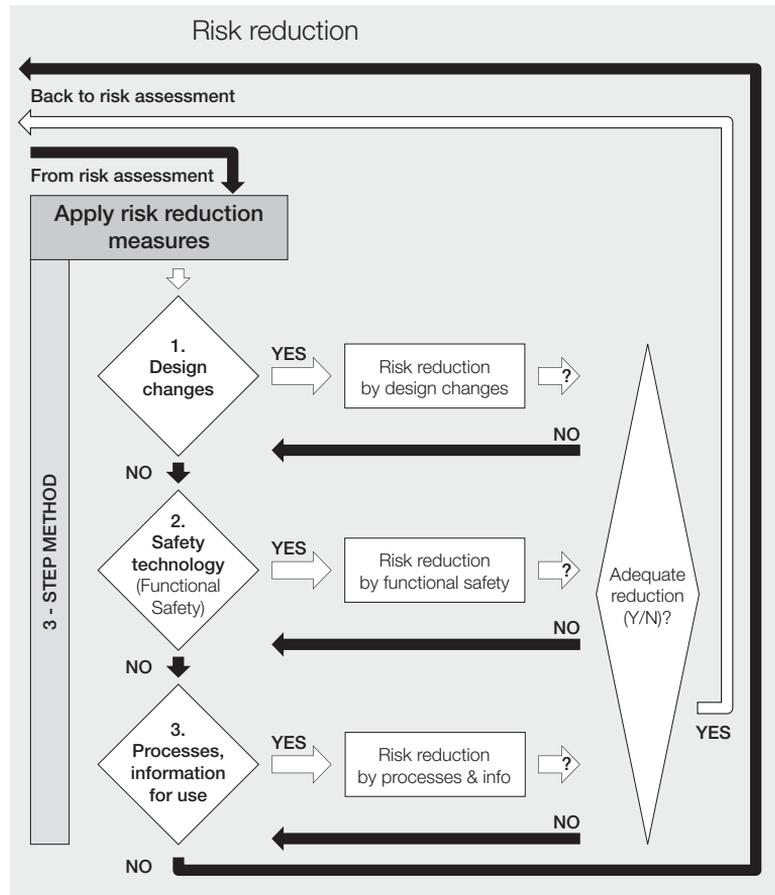


Figura 3-3 Método de reducción de riesgos en 3 pasos conforme a EN ISO 12100-1

El riesgo residual es aquel que persiste una vez se han tenido en cuenta e implementado todas las medidas de protección. Las medidas tecnológicas por sí mismas nunca son capaces de conseguir eliminar totalmente los riesgos, por lo que siempre existirá algún riesgo residual.

Estos riesgos deben documentarse en las instrucciones de funcionamiento.

La parte de la reducción de riesgos correspondiente al usuario incluye información proporcionada por el diseñador (fabricante). Las medidas de reducción de riesgos tomadas por una organización o usuario son:

- Las medidas de reducción más comunes adoptadas por la organización:
 - implementación de procesos de trabajo seguros
 - supervisión de los trabajos
 - sistemas de permisos de trabajo seguros
- La disposición y el uso de protecciones adicionales
- El uso de equipos de protección personal
- La formación del personal
- Asegurarse de que las instrucciones de seguridad y de funcionamiento han sido leídas y se actúa conforme a ellas.

Los diseñadores siempre deben recoger la valiosa información facilitada por los usuarios al definir medidas de protección.

Tras poner en práctica la reducción de riesgos, es obligatorio revisarla para garantizar que se toman las medidas adecuadas para reducir el riesgo a un nivel apropiado. Esto puede hacerse repitiendo el proceso de evaluación de riesgos.

Los pasos restantes que figuran a continuación describen la opción 2 del método de los 3 pasos: protecciones mediante una solución de seguridad funcional.

PASO 4: Establecimiento de los requisitos de seguridad

Una vez se ha llevado a cabo la reducción de riesgos correspondiente a la introducción de cambios en el diseño, es necesario especificar las protecciones adicionales. Las soluciones de seguridad funcional pueden usarse en los peligros restantes como medida adicional de reducción de riesgos.

Funciones de seguridad

Una función de seguridad es una función de una máquina cuyo fallo puede provocar un aumento inmediato del riesgo. Explicado de forma sencilla, es una medida que debe tomarse para reducir las probabilidades de que tenga lugar un evento indeseado durante una exposición a un peligro. Una función de seguridad no es parte del funcionamiento de la máquina en sí. Esto significa que si la función de seguridad falla, la máquina sigue funcionando normalmente, pero el riesgo de lesión asociado a su funcionamiento aumenta.

La definición de una función de seguridad siempre incluye dos componentes:

- **Acción requerida** (lo que debe hacerse para reducir el riesgo) y
- **prestaciones de seguridad** (SIL o PL, Nivel de Integridad de la Seguridad y Nivel de Prestaciones, respectivamente).

Nota: Es importante también especificar los requerimientos de tiempo de la función de seguridad, p.e. el máximo tiempo permitido para llevar el sistema a un estado seguro.

Para poder seleccionar correctamente los componentes de seguridad es necesario especificar el medio del sistema de seguridad.

Nota: Es obligatorio especificar, verificar (prestaciones de seguridad y funcionalidad) y validar la función de seguridad para cada uno de los peligros identificados.

Ejemplo de función de seguridad:

Requisito: un eje en giro desprotegido puede lesionar a una persona que se acerque demasiado.

Acción: para evitar que alguna persona resulte herida, el motor debe pararse en un máximo de un (1) segundo tras la apertura de la puerta de seguridad.

Una vez se ha definido la función de seguridad que ejecuta la acción, se determina el nivel de seguridad que requiere para ello.

Integridad/prestaciones de seguridad

La integridad de la seguridad mide las prestaciones de una función de seguridad. Ayuda a cuantificar la probabilidad de que active la función de seguridad cuando así se solicita. La integridad de la seguridad que requiere una función se determina durante la evaluación de riesgos y se representa mediante el Nivel de Integridad de la Seguridad (SIL) o el Nivel de prestaciones (PL) alcanzado, en función de la norma utilizada.

Las dos normas usan diferentes técnicas de evaluación para la función de seguridad, aunque sus resultados son comparables. Los términos y las definiciones son similares en ambas normas.

Determinación del SIL requerido (EN/IEC 62061)

El proceso para determinar el SIL es el siguiente:

1. Determine la gravedad de las consecuencias de un evento peligroso.
2. Determine el valor numérico para la frecuencia y el tiempo durante el cual la persona está expuesta al peligro.

Pista: La determinación del SIL requerido puede ser cómodamente hecho con la herramienta PC de diseño de seguridad funcional (FSDT) de ABB.

3. Determina el valor de la probabilidad de que una situación de riesgo ocurra cuando se está expuesta a ella.
4. Determina el valor de la posibilidad de prevenir o limitar el alcance de los daños.

Ejemplo:

Los parámetros utilizados para determinar los valores numéricos se presentan en el siguiente ejemplo de una tabla de asignación del SIL.

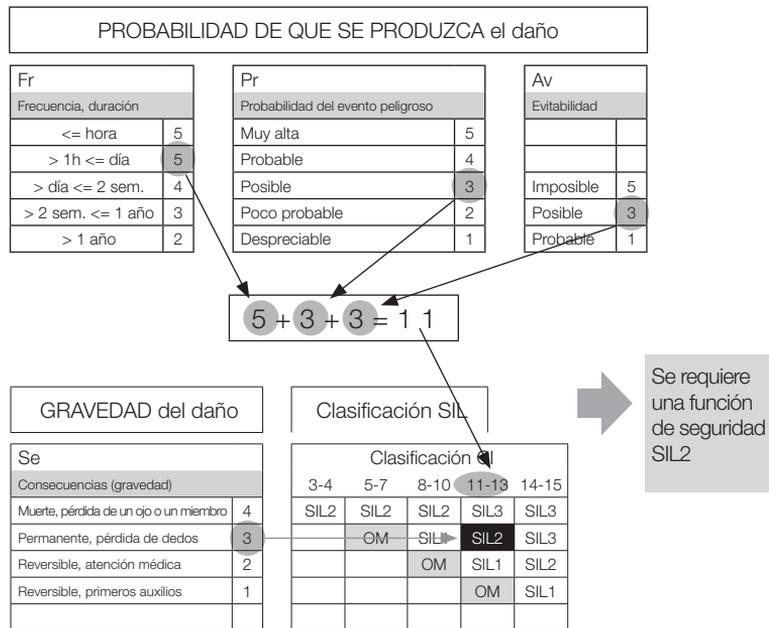


Figura 3-4 Ejemplo de una tabla de asignación del SIL (basado en la EN/IEC 62061, figura A.3)

En este ejemplo, el análisis de peligros se lleva a cabo para un eje en giro desprotegido.

1. Gravedad (Se) = 3. La consecuencia del peligro es una lesión permanente, con posible pérdida de dedos.
2. Frecuencia (Fr) = 5. Una persona está expuesta al peligro varias veces al día.
3. Probabilidad (Pr) = 3. Es posible que el peligro se haga realidad.
4. Evitabilidad (Av) = 3. El peligro es evitable.
 - 5 + 3 + 3 = 11, con la consecuencia determinada, siendo igual a un SIL 2.

Las tablas utilizadas para determinar estos valores forman parte de la norma.

Tras haber definido el SIL requerido, es posible iniciar la implementación del sistema de seguridad.

Determinación del PL requerido (EN ISO 13849-1)

Para determinar el PL requerido, seleccione una de las alternativas de entre las siguientes categorías y cree una "ruta" hasta el PL requerido en el gráfico.

1. Determine la gravedad del daño.

Los parámetros de la gravedad son:

S1 Leve, lesión normalmente reversible

S2 Grave, lesión normalmente irreversible, incluida la muerte

2. Determine la frecuencia y la duración de la exposición al peligro.

Los parámetros de la frecuencia y la duración son:

F1 Entre poco probable y frecuente y/o exposición breve

F2 Entre frecuente y continua y/o exposición larga

3. Determine la posibilidad de evitar el peligro o de limitar el daño ocasionado.

Los parámetros relacionados con la posibilidad de evitar y de limitar el daño son:

P1 Posible bajo ciertas condiciones

P2 Prácticamente imposible

Pista:

La determinación del SIL requerido puede ser cómodamente hecho con la herramienta PC de diseño de seguridad funcional (FSDT) de ABB.

Ejemplo:

El nivel de prestaciones resultante se representa por a, b, c, d y e en el ejemplo siguiente del gráfico de riesgos del PL.

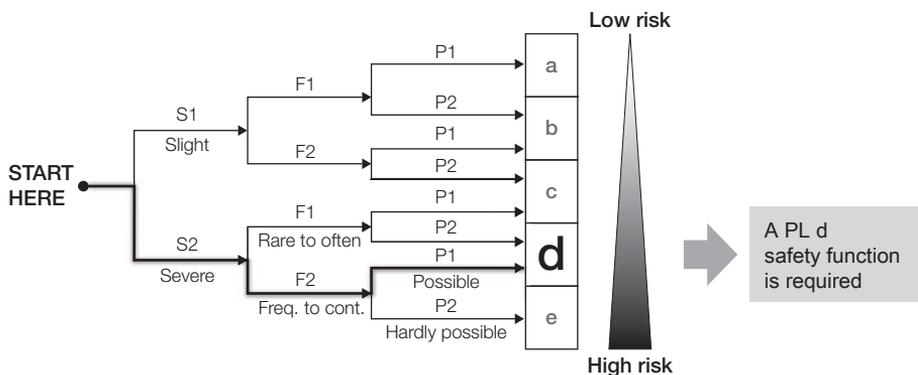


Figura 3-5 Ejemplo del gráfico de riesgos del PL (basado en la EN ISO 13849-1, figura A.1)

En este ejemplo, el análisis de peligros se lleva a cabo para un eje en giro desprotegido.

- La consecuencia del peligro es una lesión grave e irreversible.
Gravedad = S2.
- Una persona está expuesta al peligro varias veces al día.
Frecuencia = F2.
- Es posible evitar o limitar el daño ocasionado por el peligro.
Posibilidad = P2.

La ruta lleva a un valor de PL requerido (PLr) d. Las tablas utilizadas para determinar estos valores forman parte de la norma. Tras haber definido el PL requerido, es posible iniciar la implementación del sistema de seguridad.

PASO 5: Implementación de un sistema de seguridad funcional

Cuando se pretende diseñar y fabricar una función de seguridad, la idea es planear y fabricar la función de seguridad para que satisfaga el SIL/PL requerido que se especifica en el capítulo previo. El uso de subsistemas certificados en los sistemas de seguridad funcional puede ahorrar mucho trabajo a los diseñadores de dichos sistemas. La implementación de funciones de seguridad resulta más conveniente una vez se han realizado algunos cálculos de seguridad y fiabilidad y los subsistemas están certificados.

Nota:

Si no se utilizan subsistemas certificados, puede ser necesario llevar a cabo cálculos de seguridad para cada subsistema. Las normas EN/IEC 62061 y EN ISO 13849-1 incluyen información sobre el proceso y los parámetros de cálculo necesarios.

Pista:

La selección de una adecuada arquitectura de una función de seguridad que cumpla los cálculos de seguridad requeridos y la verificación SIL/PL puede llevarse a cabo convenientemente con la herramienta de PC denominada herramienta de diseño de seguridad funcional (FSDT).

Los procesos de implementación y verificación son iterativos y se desarrollan en paralelo. La idea es usar la verificación como herramienta durante la implementación para asegurarse de que se alcanza la seguridad funcional y el nivel SIL/PL requeridos con el sistema implementado. Para más información sobre los procesos de verificación, véase el paso siguiente.

ABB dispone de una herramienta PC de diseño de seguridad funcional (FSDT) para establecer un objetivo de SIL/PL para una función de seguridad, así como para diseñar, verificar el SIL/PL alcanzado y documentar la función de seguridad.

Los pasos generales para la implementación de un sistema de seguridad funcional son:

1. Definir los requisitos de seguridad como SIL o PL conforme a la norma EN/IEC 62061 o a la EN ISO 13849-1.

2. Seleccionar la arquitectura del sistema que va a utilizarse para el sistema de seguridad.

Las normas EN ISO 13849-1 y EN/IEC 62061 ofrecen arquitecturas básicas con fórmulas de cálculo.

- la categoría B, 1, 2, 3 o 4 de acuerdo con la norma EN ISO 13849-1, o
- la arquitectura designada A, B, C o D de acuerdo con la norma EN/IEC 62061 para los subsistemas y para el sistema en su conjunto.

Para obtener más información sobre las arquitecturas designadas, consulte las normas pertinentes.

3. Fabricar el sistema a partir de subsistemas de seguridad: sensor/interruptor, entrada, lógica, salida y actuador.

Adopte una de estas acciones:

- use subsistemas certificados (recomendado) o
- lleve a cabo cálculos de seguridad para cada subsistema.

El nivel de seguridad del sistema en su conjunto se establece sumando todos los niveles de seguridad de los subsistemas.

4. Instalar el sistema de seguridad.

Es necesario que el sistema se instale de forma adecuada para evitar un posible fallo común a causa de un cableado indebido, por razones medioambientales o por otros factores. Un sistema de seguridad que no realiza su tarea correctamente por culpa de una instalación deficiente carece de utilidad, e incluso puede llegar a suponer un riesgo.

5. Comprobar la funcionalidad del sistema.

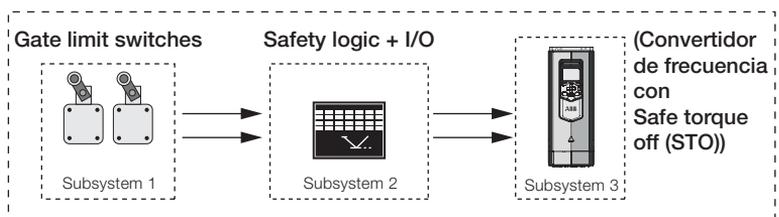


Figura 3-6 Estructura de una función de seguridad

PASO 6: Verificación del sistema de seguridad funcional

La verificación del sistema de seguridad funcional demuestra y garantiza que el sistema de seguridad implementado cumple con los requisitos especificados para el sistema en la fase de requisitos de seguridad.

La verificación no debe llevarse a cabo tras el proceso de implementación, sino de manera paralela a éste como un proceso iterativo, de modo que se garantice que la implementación genere en efecto un sistema que cumplirá los requisitos especificados.

Además de verificar si se ha conseguido el SIL o PL del sistema, también es necesario verificar el correcto funcionamiento del sistema de seguridad efectuando pruebas de funcionalidad.

Verificación del SIL del sistema de seguridad (EN/IEC 62061)

Para verificar los niveles de integridad de la seguridad se debe comprobar que las prestaciones de seguridad de la función de seguridad creada, es decir su capacidad de reducción de riesgos, sean iguales o mayores al objetivo de prestaciones requerido fijado durante la valoración de riesgos. Se recomienda el uso de subsistemas certificados, ya que su fabricante ya ha definido valores para determinar la integridad de seguridad sistemática (SILCL) y la probabilidad de fallos peligrosos por hora (PFH_d).

Pista: La verificación del SIL alcanzado puede ser llevada a cabo convenientemente con la herramienta PC de diseño de seguridad funcional (FSDT) de ABB.

Para verificar el SIL de un sistema de seguridad en que se utilizan subsistemas certificados:

1. Determine la integridad de seguridad sistemática del sistema mediante los valores del límite de solicitud de SIL (SILCL, SIL Claim Limit) definidos para los subsistemas.

El SILCL es el valor máximo del SIL para el que el subsistema resulta estructuralmente adecuado. El SILCL es un indicador para la determinación del SIL alcanzado: el SILCL de todo el sistema no puede ser mayor que el SILCL del subsistema de menor entidad.

2. Calcule la integridad de seguridad aleatoria del hardware para el sistema mediante los valores de Probabilidad de fallo peligroso por hora (PFH_d, Probability of a dangerous Failure per Hour) definidos para los subsistemas. Habitualmente, los fabricantes de subsistemas certificados facilitan valores de PFH_d para sus sistemas.

La PFH_d es el valor de fallo aleatorio del hardware que se utiliza para determinar el SIL.

3. Utilice la lista de comprobación de Fallos por Causa Común (CCF) para asegurarse de que se han tenido en cuenta todos los aspectos necesarios a la hora de crear los sistemas de seguridad.

Las tablas con listas de comprobación de CCF pueden consultarse en la norma EN/IEC 62061, Anexo F.

Calcule los puntos según la lista y compare el resultado final con los valores enumerados en la norma EN/IEC 62061 Anexo F, y con los resultados de la Tabla F.2 en el factor CCF (β). Este valor se utiliza para estimar el valor de probabilidad de PFH_d .

4. Determine el SIL alcanzado con ayuda de la tabla correspondiente.

Ejemplo de verificación del SIL (Los datos de cálculo son ficticios):

Verificación del sistema de seguridad funcional de un eje en giro:

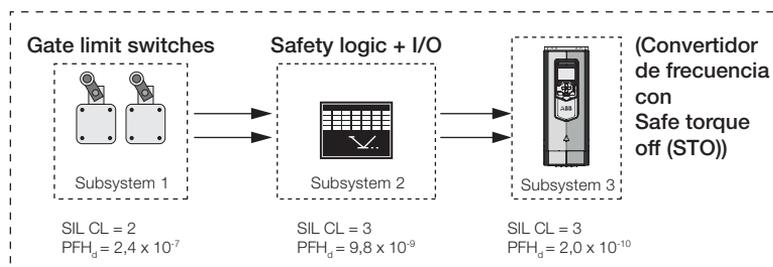


Figura 3-7 Ejemplo de verificación del SIL (basado en EN/IEC 62061, tabla 3)

- Integridad de seguridad sistemática:
 $SIL\ CL_{sist} \leq (SIL\ CL_{subsistema})_{mínimo} \rightarrow$ Límite de solicitud de SIL 2
- Integridad de seguridad aleatoria del hardware:
 $PFH_d = PFH_{d1} + PFH_{d2} + PFH_{d3} = 2,5 \times 10^{-7} < 10^{-6}$
 = El sistema cumple con el SIL 2.

Tabla para determinar el SIL de acuerdo con el valor de PFH_d obtenido para todo el sistema de seguridad (en modo continuo/alta demanda):

SIL	Probabilidad de fallos peligrosos por hora (1/h)
SIL 1	$\geq 10^{-6}$ hasta $< 10^{-5}$
SIL 2	$\geq 10^{-7}$ hasta $< 10^{-6}$
SIL 3	$\geq 10^{-8}$ hasta $< 10^{-7}$

Tabla 3-1 Tabla para determinar el SIL (basado en EN/IEC 62061, tabla 3)

Verificación del PL del sistema de seguridad (EN ISO 13849-1)

Para verificar el nivel de prestación, compruebe que el PL de la función de seguridad correspondiente concuerda con el PLr requerido. Si la función de seguridad está formada por varios subsistemas, sus niveles de prestaciones deben ser iguales o mayores que el nivel de prestaciones requerido para dicha función de seguridad. Se recomienda el uso de subsistemas certificados, pues ya tendrán definidos sus valores de prestaciones de seguridad.

Pista:

La verificación del PL alcanzado puede ser llevada a cabo convenientemente con la herramienta PC de diseño de seguridad funcional (FSDT) de ABB.

Nota:

De acuerdo con la EN ISO 13849-1 se usa el MTTFd para definir el PL y el PFHd para un subsistema. Sólo se usa el PFHd para determinar el PL del sistema completo.

Para verificar el PL de un sistema de seguridad en que se utilizan subsistemas certificados:

1. Determine la susceptibilidad del sistema a Fallos por Causa Común (CCF) mediante la lista de comprobación de CCF.

Las tablas con listas de comprobación de CCF pueden consultarse en la norma EN ISO 13849-1:2008, Anexo I. La puntuación mínima requerida es de 65 puntos.

2. Determine el PL alcanzado con ayuda del gráfico de barras y utilizando los valores establecidos para:

- Categoría
- Tiempo medio hasta fallo peligroso ($MTTF_d$)
- Cobertura del diagnóstico (DC)

El $MTTF_d$ es el tiempo medio que transcurre hasta que tiene lugar un fallo peligroso. DC hace referencia al número de fallos peligrosos que pueden detectarse mediante diagnóstico.

Encontrará más información relativa a los detalles de los cálculos en la norma EN ISO 13849-1.

3. Introduzca los valores resultantes en el gráfico de PL, a partir del cual puede determinarse el PL obtenido.

Ejemplo de verificación del PL:

Verificación del sistema de seguridad funcional de un eje en giro:

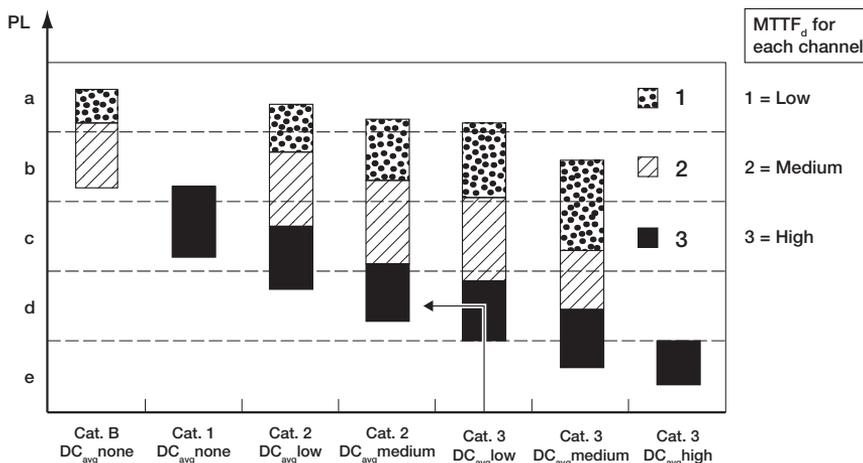


Figura 3-8 Ejemplo de verificación del PL

Para determinar el PL conseguido definido en el ejemplo anterior:

- la arquitectura designada es de la Categoría 3,
- el valor de $MTTF_d$ es alto y
- el valor medio de DC es bajo.

= el sistema cumple el valor PL d.

Tabla para determinar el PL de acuerdo con el valor de PFH_d obtenido para todo el sistema de seguridad:

PL	Probabilidad de fallos peligrosos por hora (1/h)
a	$\geq 10^{-5}$ hasta $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ hasta $< 10^{-5}$
c	$\geq 10^{-6}$ hasta $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ hasta $< 10^{-6}$
e	$\geq 10^{-8}$ hasta $< 10^{-7}$

Tabla 3-2 Tabla para determinar el PL (basado en la EN ISO 13849-1 tabla 3)

Comparación de los valores de SIL y de PL

Aunque los métodos de evaluación son diferentes para cada norma, los resultados de la evaluación son comparables en función del fallo aleatorio de hardware.

Nivel de integridad de la seguridad SIL	Nivel de prestaciones PL
Sin correspondencia	a
1	b
1	c
2	d
3	e

Tabla 3-3 Comparación entre el SIL y el PL (basado en la EN ISO 13849-1 tabla 4)

PASO 7: Validación de un sistema de seguridad funcional

Es obligatorio validar cada función de seguridad para garantizar que reduce el riesgo conforme a lo requerido en la fase de evaluación de riesgos.

Para determinar la validez del sistema de seguridad funcional, cotéjelo con el proceso de evaluación de riesgos llevado a cabo al inicio del procedimiento para el cumplimiento de los EHSR de la Directiva de Máquinas (véase el Paso 2, página 24). El sistema es válido si realmente reduce los riesgos analizados y evaluados en el proceso de evaluación de riesgos.

PASO 8: Documentación de un sistema de seguridad funcional

Antes de que la máquina pueda cumplir con los requisitos de la Directiva de Máquinas, es necesario documentar su diseño y elaborar la documentación para el usuario pertinente.

La documentación debe redactarse con rigor. Debe ser exacta y concisa, pero al mismo tiempo informativa y fácil de entender por el usuario. La documentación para el usuario debe incluir todos los riesgos residuales y ofrecer las instrucciones apropiadas acerca de cómo operar la máquina de forma segura. Debe ser accesible y fácil de mantener. La documentación para el usuario se suministra con la máquina.

Si desea más información sobre la documentación requerida y su naturaleza, consulte los EHSR en el Anexo I de la Directiva de Máquinas.

PASO 9: Demostración de la conformidad

Antes de comercializar una máquina, el fabricante debe asegurarse de que se implementa de conformidad con las normas armonizadas. También debe probarse que la combinación de partes relativas a la seguridad cumple los requisitos definidos para cada función de seguridad.

Para probar la conformidad con la Directiva de Máquinas, debe demostrarse que:

- La maquinaria cumple los Requisitos Esenciales de Seguridad y Salud (EHSR) pertinentes definidos en la Directiva de Máquinas.
- La maquinaria cumple los requisitos de otras Directivas relacionadas.
- La conformidad con estos requisitos puede garantizarse si se cumple con lo estipulado en las normas armonizadas correspondientes.
- El documento técnico está actualizado y disponible.
El documento técnico demuestra que la máquina es conforme con las normas de la Directiva de Máquinas.

Nota:

El informe técnico tiene que estar disponible en un tiempo razonable porque puede ser requerido por, p.e. las autoridades, y la ausencia de un documento técnico es razón suficiente para dudar del cumplimiento de la máquina con los EHSR.

El documento técnico debe incluir el diseño, la fabricación y el funcionamiento de la maquinaria en la medida en que sea necesario para demostrar su conformidad. Si desea más información sobre el contenido del documento técnico, consulte el Anexo VII de la Directiva de Máquinas 2006/42/CE.

- Se han aplicado los procedimientos de evaluación de la conformidad.
Los requisitos especiales para las máquinas enumeradas en el Anexo IV de la Directiva de Máquinas se cumplen cuando es necesario.
- Se ha emitido la declaración de conformidad CE y se suministra con la máquina.

Una vez se ha establecido la conformidad, se coloca el marcado CE.

Se presupone que la maquinaria con el marcado CE, que además va acompañada de una declaración de conformidad CE, cumple los requisitos de la Directiva de Máquinas.

Glosario

CCF (Common Cause Failure), Fallo por causa común

Situación en la que varios subsistemas fallan a causa de un único evento. Todos los fallos son causados por este evento y no son consecuencia entre sí.

Daño

Daño a la salud o lesión física.

DC (Diagnostic Coverage), Cobertura del diagnóstico

Efectividad de la monitorización de los fallos de un sistema o subsistema. Es la relación entre la tasa de fallos peligrosos detectados y la tasa de fallos peligrosos totales.

EHSR (Essential Health and Safety Requirements), Requisitos Esenciales de Seguridad y Salud

Requisitos que la maquinaria debe satisfacer para ajustarse a la Directiva de Máquinas de la Unión Europea y obtener así el mercado CE. Estos requisitos se enumeran en el Anexo I de la Directiva de Máquinas.

EN

Siglas de Norma Europea ('EuroNorm'). Este prefijo se usa con los estándares europeos (o versiones europeas de los estándares IEC/ISO) de las organizaciones europeas CEN y CENELEC. Las normas armonizadas también llevan el prefijo EN.

Función de seguridad

Función diseñada para aumentar la seguridad de una máquina cuyo fallo puede provocar un aumento inmediato del riesgo.

IEC (International Electrotechnical Commission), Comisión Electrotécnica Internacional

Organización mundial para la normalización que se compone de todos los comités electrotécnicos nacionales.

www.iec.ch

ISO (International Organization for Standardization), Organización Internacional para la Normalización

Federación internacional de organismos nacionales de normalización.

www.iso.org

Marcado CE

Marca de conformidad obligatoria para la maquinaria y otros tipos de productos que se comercializan en el Área Económica Europea (EEA). Mediante la colocación del marcado CE en el producto, el fabricante garantiza que dicho producto cumple todos los requisitos esenciales de las Directivas Europeas pertinentes.

MTTF_d (Mean Time To dangerous Failure), Tiempo medio hasta un fallo peligroso

Previsión de tiempo medio hasta que se produce un fallo peligroso.

Norma armonizada

Norma europea que ha sido elaborada bajo el mandato de la Comisión Europea o de la Secretaría de la AELC con el propósito de ofrecer apoyo a los requisitos esenciales de una Directiva, y que es de obligado cumplimiento según la legislación de la UE.

Peligro

Fuente potencial de daños.

PFH_d (Probability of dangerous Failure per Hour), Probabilidad de fallo peligroso por hora

Probabilidad media de que se produzca un fallo peligroso en una (1) hora. La PFH_d es el valor que se utiliza para determinar el valor del SIL o del PL de una función de seguridad.

PL (Performance Level), Nivel de prestaciones

Niveles (a, b, c, d, e) que especifican la capacidad de un sistema de seguridad de efectuar una función de seguridad bajo condiciones previsibles.

Riesgo

Combinación de hasta qué punto es posible que se produzca el daño y lo grave que puede resultar.

SIL (Safety Integrity Level), Nivel de integridad de la seguridad

Niveles (1, 2, 3, 4) que especifican la capacidad de un sistema de seguridad eléctrico de efectuar una función de seguridad bajo condiciones previsibles. En el caso de la maquinaria, sólo se utilizan los niveles de 1 a 3.

SILCL (SIL Claim Limit), Límite de solicitud de SIL

Nivel máximo de integridad de la seguridad (SIL) que puede reclamarse para un sistema de seguridad eléctrico, teniendo en cuenta las restricciones en la arquitectura y la integridad de seguridad sistemática.

Subsistema

Componente de una función de seguridad que tiene su propio nivel de seguridad (SIL/PL) que afecta al nivel de seguridad de toda la función de seguridad. Si alguno de los subsistemas falla, también fallará toda la función de seguridad.

Índice

A	N
Actualización de maquinaria existente 22	Normas armonizadas 8, 12, 16, 22, 26, 38
Análisis de riesgos 10, 18, 24, 25	
Anexo IV 11, 12, 38	P
C	Parada de funcionamiento segura (SOS) 19
CEN 12, 16	Paro de emergencia 13, 21
CENELEC 12, 16	Paro seguro 1 (SS1) 19
Control seguro de frenos (SBC) 21	Paro seguro 2 (SS2) 19
D	Periodo de transición 14
Demostración de la conformidad 40	Plan de seguridad 23
Desconexión de emergencia 20	PL (Performance Level), Nivel de prestaciones 15, 17, 29, 30, 35, 37, 41
Direccionamiento seguro (SDI) 20	Prestaciones de seguridad 8, 10, 29, 34, 35
Directiva de Máquinas 8, 9, 11, 12, 22, 23, 26, 32, 37, 38	R
Directiva Europea sobre Maquinaria 98/37/CE 38	Reducción de riesgos 9, 13, 16, 24, 25, 26
Directiva Europea sobre Maquinaria 2006/42/CE 11, 24, 38	Riesgo residual 26, 27, 28, 38
Documentación del sistema de seguridad 37	S
E	Seguridad funcional 9, 23, 28
EHSR 8, 9, 10, 18, 22, 32, 37, 38, 40	SIL (Safety Integrity Level), Nivel de integridad de la seguridad 15, 18, 29, 34, 37, 41
EN/IEC 61800-5-2 18	Sistema de seguridad funcional 32, 33, 37
EN/IEC 62061 13, 14, 17, 24, 29, 32, 34	Sistema de seguridad validado 39
EN ISO 13849-1 13, 14, 16, 24, 30, 32, 35	V
Estándar tipo A 13	Velocidad limitada con seguridad (SLS) 20
Estándar tipo B 13	Verificación del sistema de seguridad 35
Estándar tipo C 13	
Evaluación de riesgos 12, 16, 18, 24, 26, 27, 29, 37	
F	
Funciones de seguridad 9, 10, 13, 14, 17, 18, 19, 27, 28, 32, 33, 37, 38, 40	
M	
Marcado CE 7, 10, 23, 26, 39, 40	
Monitorización de velocidad segura (SSM) 20	

Contacte con nosotros

Para obtener más información, póngase en contacto con su representante local de ABB o visite:

www.abb.es

www.abb.com/drivespartners

© Copyright 2014 ABB. Todos los derechos reservados.
Las especificaciones están sujetas a cambio sin previo aviso.

3AUA0000163173 REV E ES 9.9.2014 # 17290