Seguridad funcional en máquinas e instalaciones

La Directiva Europea sobre Máquinas, puesta en práctica

EN 954-1
EN ISO 13849-1

EN 62061

Safety Integrated

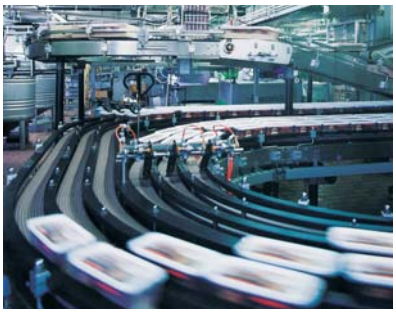
Answers for industry.

SIEMENS

Nuevas normas regulan a los fabricantes de máquinas

Normas a nivel mundial, amplias reglamentaciones

Contenido


En nuestra calidad de partner en todas las cuestiones relacionadas con la seguridad, nuestras prestaciones no se limitan a ofrecer productos y sistemas de seguridad, sino también a consultoría en todo lo relacionado con normas y reglamentos internacionales, para lo que disponemos del know-how más actual. Para los fabricantes de maquinaria y los operadores de plantas ofrecemos una amplia oferta de cursos de formación y servicios que cubre todo el ciclo de vida de plantas y máquinas cumpliendo con los requisitos de seguridad.

Para minimizar los riesgos inevitables hasta un nivel tolerable en la construcción de una máquina, es vital evaluar y, dado el caso, limitar adecuadamente todos los posibles riesgos. La evaluación de los riesgos, por un lado, permite optimizar paso a paso la máquina en cuanto a la seguridad. Por otro lado, servirá de prueba en caso de que se produzca algún daño. A partir de la correcta documentación de esa medida, se podrán evaluar el desarrollo y los resultados del proceso de minimización de los riesgos, a la vez que supondrá la base del manejo seguro de la máquina – siendo responsabilidad del usuario la formación adecuada de su personal operario. En el momento de establecer configuraciones de varias máquinas, o bien modificando o ampliando las máquinas existentes, el usuario se hará constructor de máquinas a sí mismo.

La Directiva de "Máquinas" se puede cumplir de distintas maneras, a saber: Encargando la certificación de la máquina a un organismo de pruebas, cumpliendo las normas armonizadas, o bien por medio del certificado de seguridad ampliado, realizando las pruebas adecuadas y presentando la correspondiente documentación. En cada caso, la marca CE con el correspondiente certificado de seguridad constituye la prueba visible del cumplimiento de la directiva mencionada. Además, la Directiva base sobre la seguridad en el trabajo de la UE requiere que toda máquina lleve esa marca.

Evitar accidentes, impedir daños secundarios

Partiendo de las consecuencias físicas o psíquicas que puedan sufrir las personas en accidentes con máquinas o instalaciones, cabe decir que son tolerables los posibles daños materiales – aúnque los tiempos de inactividad del material pueden dar lugar a importantes pérdidas económicas. Pero siempre que se produzca el peor de los casos, las causas de un accidente se deben analizar con todo detalle. Y si resulta que se haya incumplido alguna de las directivas aplicables, eso puede llevar a la reclamación de indemnización por daños y perjuicios por un importe no despreciable, a la vez que se perjudica la reputación de la empresa responsable – con consecuencias graves. De lo contrario, cumpliendo cada una de las normas relevantes, es de suponer que también se cumplan los requisitos de las directivas aplicables (efecto de presunción).

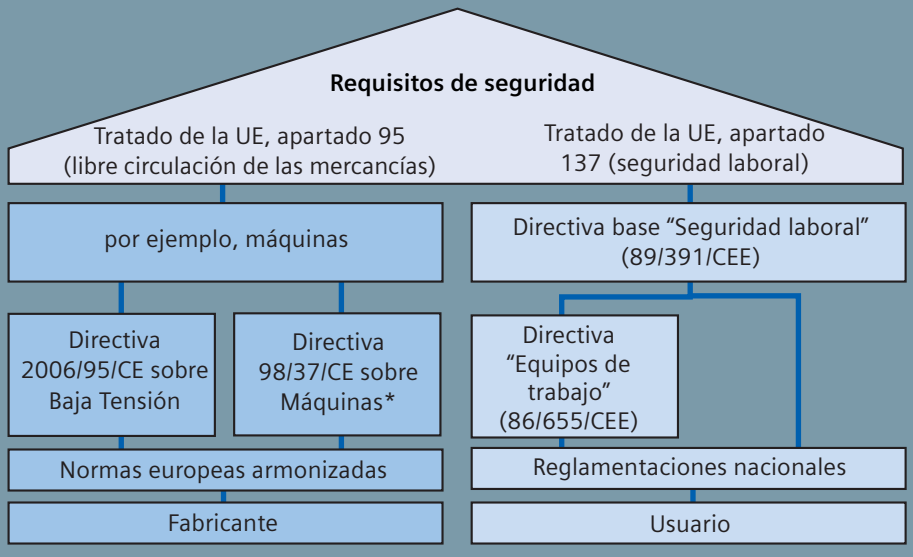
A continuación se describe paso a paso cómo usted podrá asegurar la fiabilidad operacional de su máquina en todo momento.

Requisitos básicos de seguridad en la industria de fabricación y proceso

Objetivo:
Protección personal, material y del medio ambiente

Resultado:
Marca CE como prueba de seguridad de la máquina

CE



* De momento, es de aplicación obligatoria la Directiva sobre Máquinas 98/37/CE. Como muy tarde, será reemplazada por la nueva Directiva sobre Máquinas 2006/42/CE a finales de 2009.

La armonización de las normas y reglamentaciones nacionales sobre la realización técnica de máquinas es el producto de la consolidación del Mercado Europeo:

- Se establecieron los requisitos básicos que por un lado se dirigen a los fabricantes – en materia del libre comercio (artículo 95), y por otro, a los usuarios (explotadores) – en materia de seguridad laboral (artículo 137).
- En consecuencia, cada uno de los países miembros de la EU incorporaron obligatoriamente la Directiva "Máquinas" al derecho nacional, tal y como exige el tratado europeo. En Alemania, por ejemplo, la mencionada Directiva se traduce en la ley sobre la seguridad en máquinas GSG.

Con el fin de asegurar plena conformidad con una directiva, es aconsejable aplicar las correspondientes normas armonizadas europeas. De esa manera, se otorga el efecto de presunción y tanto el fabricante como el usuario tendrán seguridad jurídica en lo relativo a las reglamentaciones nacionales y la Directiva EU de que se trate.

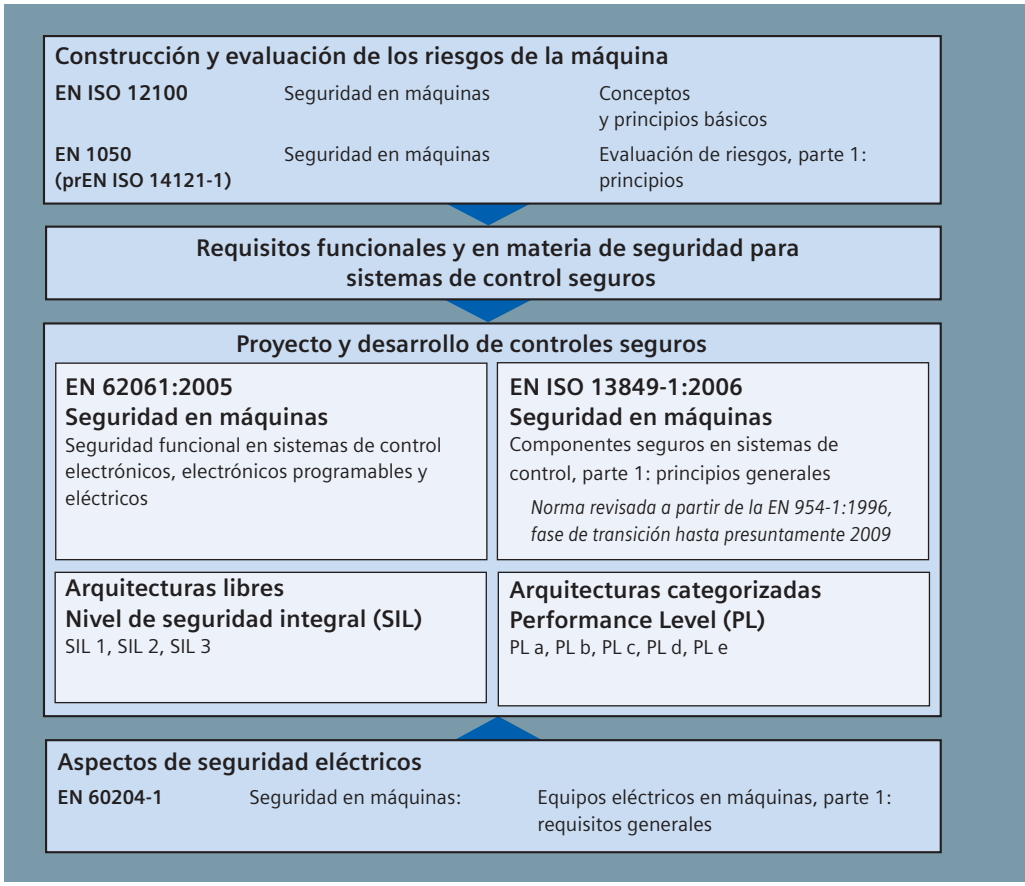
Con la marca CE, el fabricante de la máquina documentará el cumplimiento de todas las reglamentaciones y normas del libre comercio. Y como las Directivas Europeas son reconocidas en todos los países del mundo, su aplicación facilita las exportaciones a los países miembros de la CEE.

Toda la siguiente información va dirigida a los fabricantes de máquinas, así como a los usuarios que modifiquen o dejen modificar componentes con relevancia para la seguridad de sus máquinas.

Normas básicas en el desarrollo de funciones de control

Objetivo:
Cumplir los requisitos de seguridad aplicables con el fin de tener seguridad jurídica y cumplir las reglamentaciones de exportación, minimizando adecuadamente los posibles riesgos.

Resultado:
Desarrollo de medidas de protección adecuadas aplicando las normas armonizadas y, con ello, obtener conformidad con los requisitos de seguridad de la Directiva Máquinas a partir del efecto de presunción.

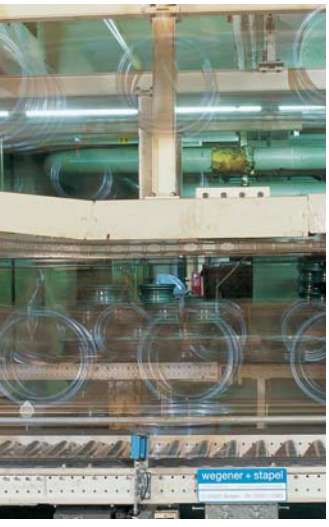


La seguridad en máquinas requiere protección ante variedad de riesgos. Ello se puede conseguir de la siguiente manera:

- Construcción a partir de los principios de minimización de riesgos y evaluación de los mismos en el caso concreto (EN ISO 12100-1, EN 1050)
- Sistemas de protección, dado el caso utilizando controles seguros (seguridad funcional según EN 62061 o EN ISO 13849-1)
- Seguridad eléctrica (EN 60204-1)

A continuación se detalla la **seguridad funcional**. Ese concepto se refiere a los componentes de la máquina o instalación cuya seguridad depende de la correcta función de los correspondientes sistemas de control o dispositivos de protección. Para ello, están disponibles las siguientes dos normas:

- EN 62061:2005 – parte de la norma europea base IEC 61508
- EN ISO 13849-1:2006 – norma revisada a partir de la EN 954-1, que no cubre las categorías actuales.



Paso a paso:

Proyecto y desarrollo de controles seguros

La norma EN 62061

La norma EN 62061 "Seguridad en máquinas – Seguridad funcional de sistemas de mando eléctricos, electrónicos y programables" especifica una serie de requisitos, a la vez que incluye recomendaciones sobre el proyecto, la integración y evaluación de sistemas de control eléctricos, electrónicos y electrónicos programables seguros (SRECS) en máquinas. Es la primera norma que regula toda la cadena de seguridad, desde el sensor hasta el actuador. Ahora, para alcanzar un nivel de seguridad integral, como por ejemplo SIL 3, ya no basta con certificar adecuadamente los distintos equipos involucrados, sino que es imprescindible demostrar que el sistema de seguridad global cumple todos los requisitos de seguridad especificados.

No obstante, la norma no incluye ninguna especificación sobre las capacidades de los elementos de control seguros no eléctricos – por ejemplo hidráulicos, neumáticos o electromecánicos.

Nota:
Siempre que los elementos de control seguros no eléctricos sean supervisados por medio de una unidad de control adecuada, pueden despreciarse en la evaluación de seguridad a partir de los requisitos aplicables.

La norma EN ISO 13849-1

La norma EN ISO 13849-1 "Seguridad de las máquinas – Seguridad funcional de sistemas de mando eléctricos, electrónicos y programables, parte 1: principios generales" considera las categorías conocidas de la norma EN 954-1, edición 1996, incluyendo todas las funciones de seguridad y equipos integrados en los circuitos seguros.

Asimismo, más allá de los criterios de calidad de la EN 954-1, la EN ISO 13849-1 evalúa la cantidad de las funciones de seguridad existentes a partir de los niveles de rendimiento (PL), basados en las categorías anteriores. La norma describe la determinación del PL de los componentes seguros en sistemas de control, considerando para ello las arquitecturas designadas y la vida útil prevista en el caso concreto. En casos de discrepancia, hace referencia a la norma IEC 61508. Y para las combinaciones de componentes seguros formando sistemas de control complejos, ofrece la información adecuada para determinar el PL resultante.

La norma EN ISO 13849-1 cubre cualquier componente seguro en sistemas de control (SRP/CS) y todo tipo de máquina, independientemente de la tecnología y forma energética de que se trate (eléctrica, hidráulica, neumática, mecánica, etc).

En 2009 concluirá la transición de la norma EN 954-1 a la EN ISO 13849-1. Hasta ese momento, aplicarán las dos normas sin restricción alguna.

Plan de seguridad según EN 62061 – hilo conductor en el desarrollo de máquinas seguras

Siguiendo un procedimiento sistemático a lo largo de la vida útil del producto, se determinan y traducen fiablemente todos los aspectos y reglamentaciones relativas a la seguridad en el desarrollo y el funcionamiento de una máquina. El plan de seguridad (Safety Plan) le servirá de guía al usuario en todas las fases – hasta la modernización y actualización. El esquema y la aplicación obligatoria del plan de seguridad se especifican en la norma EN 62061.

La norma requiere seguir un procedimiento sistemático en el desarrollo de un sistema de seguridad (SRECS), incluyendo la documentación adecuada de todas las actividades en el plan de seguridad: desde el análisis y la evaluación de los riesgos que se desprendan de la máquina, el proyecto y la realización del SRECS hasta la validación, siendo obligatorio actualizar el plan de seguridad continuamente en el proceso del desarrollo del SRECS.

El plan de seguridad documentará los siguientes temas y actividades:

- **Proyecto y procedimiento para todas las actividades en el desarrollo de un sistema SRECS.**
  Por ejemplo:
  - Especificación de la función de control segura (SRCF)
  - Proyecto e integración del SRECS
  - Validación del SRECS
  - Elaboración de la documentación destinada a los usuarios del SRECS
  - Documentación de la información relativa al desarrollo del SRECS (documentación de proyecto)
- **Estrategia para obtener seguridad funcional**
- **Responsabilidades en la ejecución y supervisión de las actividades**

Las actividades descritas no se describen explícitamente en la norma ISO 13849-1:2006 – aunque son vitales para la correcta aplicación de la Directiva "Máquinas".

1° paso:
Estrategia para minimizar los riesgos, según EN ISO 12100-1, apartado 1

Objetivo:
Minimizar los riesgos

Resultado:
Definir y especificar las medidas de protección

El primer objetivo en la minimización de los riesgos consiste en localizar, evaluar y finalmente controlar los peligros realizando las protecciones adecuadas.

Para ello, la EN ISO 12100-1 recomienda el siguiente proceso iterativo:

1. Determinar los límites físicos y temporales de la máquina
2. Localizar, valorar y evaluar los posibles riesgos
3. Valorar el riesgo que supondrán los peligros y situaciones de peligro en cada caso concreto
4. Evaluar el riesgo y determinar las medidas de protección
5. Eliminación o minimización de los riesgos a partir del método de tres etapas: diseño constructivo con seguridad inherente, medidas de protección técnicas e información para usuarios

La norma EN 1050 (prEN ISO 14121-1) incluye información detallada sobre los pasos 1 a 4.

Los riesgos localizados determinan los requisitos de seguridad. El plan de seguridad según la norma EN 62061 servirá de guía en el siguiente procedimiento:
Por cada peligro localizado, se especificará una función de seguridad, incluyendo la especificación de pruebas – ver “Validación”.

2° paso:
Análisis de riesgos

Objetivo:
Determinar y evaluar la función de protección a partir de los riesgos

Resultado:
Determinar el nivel de seguridad integral necesario

Los factores de riesgo (Se, Fr, Pr y Av) constituyen los valores base en las dos normas. Dichos factores de riesgo se evalúan de diferentes maneras. Según EN 62061, se determina el nivel de seguridad integral requerido (SIL), según EN ISO 13849-1 el Performance Level (PL).

Riesgo, según el peligro localizado	=	Gravedad de la lesión **Se**	y	Frecuencia y duración **Fr** Probabilidad **Pr** Posibilidad de evitar el peligro **Av**

En el ejemplo "Parada segura del husillo en el momento de abrir la cubierta de seguridad" se evalúa el riesgo a partir de las dos normas.

Determinación del SIL requerido (asignación SIL)

Frecuencia y/o duración de la exposición **Fr**	
≤ 1 h	5
> 1 h – 1 día	5
> 1 día – 2 semanas	4
> 2 semanas – 1 año	3
> 1 año	2

Probabilidad de la situación peligrosa **Pr**	
frecuentemente	5
probable	4
posible	3
poco frecuente	2
despreciable	1

Posibilidad de evitar el peligro **Av**	
imposible	5
posible	3
probable	1

Consecuencias	Gravedad de la lesión **Se**	Clase **Cl = Fr + Pr + Av**				
		3–4	**5–7**	**8–10**	**11–13**	**14–15**
Muerte, pérdida de ojos, brazos	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, pérdida de dedos de la mano	3	otras medidas		SIL 1	SIL 2	SIL 3
Reversible, tratamiento médico	2				SIL 1	SIL 2
Reversible, primeros auxilios	1					SIL 1

Ejemplo

Peligro	Se	Fr	Pr	Av		Cl	Medidas de seguridad	Seguro
Husillo rotativo	3	5	4	3	=	**12**	Vigilar cubierta de protección con **SIL 2**	sí, aplicando SIL 2

Procedimiento

1. Determinar la importancia de daños Se:	Permanente, pérdida de dedos de la mano
2. Determinar frecuencia Fr, probabilidad Pr y posibilidad de evitar el peligro Av:	– Acceso al área de peligro: una vez al día, Fr = 5 – Probabilidad probable, Pr = 4 – Posibilidad de evitar el peligro: posible, Av = 3
3. Suma Fr + Pr + Av = clase Cl	Cl = 5 + 4 + 3 = 12
4. Punto de intersección línea importancia de daños Se y columna Cl = SIL requerido	SIL 2

Con ello, se requiere SIL 2

Determinar el PL requerido (con esquema de riesgos)

La validación del riesgo se efectúa a partir de parámetros idénticos:

Parámetros de riesgo

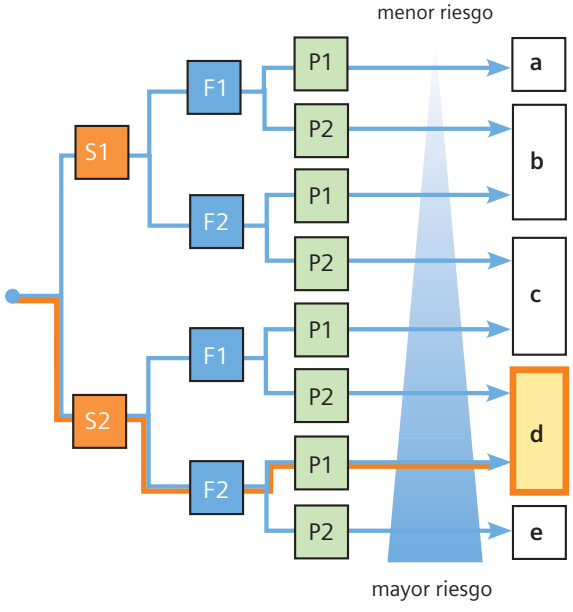
S = Importancia de lesiones
- S1 = lesión de menor importancia (por regla general, reversible)
- S2 = lesión grave (irreversible) y hasta la muerte

F = Frecuencia y/o tiempo de exposición al peligro
- F1 = muy poca o poca frecuencia y/o corta exposición
- F2 = mayor frecuencia hasta permanente y/o larga exposición

P = Posibilidad de evitar el peligro o minimización de daños
- P1 = posible en ciertas condiciones
- P2 = apenas posible

a, b, c, d, e = objetivos de seguridad a nivel de rendimiento P2

Performance Level (PL) requerido



Procedimiento

1. Determinar la importancia de daños S:	S2 = lesión grave (irreversible) y hasta la muerte
2. Determinar la frecuencia y/o tiempo de exposición al peligro F:	F2 = mayor frecuencia hasta permanente y/o larga exposición
3. Determinar la posibilidad de evitar el peligro o minimizar los daños P:	P1 = posible en ciertas condiciones

Con ello, se requiere un Performance Level PL d

3° paso:

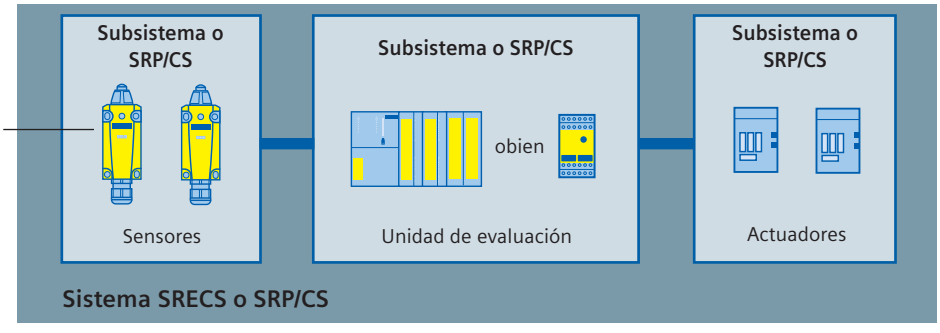
Configuración del circuito de seguridad y determinación del nivel de seguridad

Objetivo:
Función de control y determinación del nivel de seguridad integral

Resultado:
Calidad de la función de control seleccionada

Aunque las dos normas utilizan diferentes métodos de evaluación de una misma función de seguridad, se pueden comparar los correspondientes resultados. Asimismo, utilizan conceptos y definiciones semejantes.
Ambas normas consideran la cadena de seguridad global de una manera comparable, determinando una función de seguridad como sistema.

Configuración de una función de seguridad



SRP/CS: Componentes seguros del sistema de control, según EN ISO 13849-1
SRECS: Sistema de control seguro eléctrico, según EN 62061

Ejemplo:

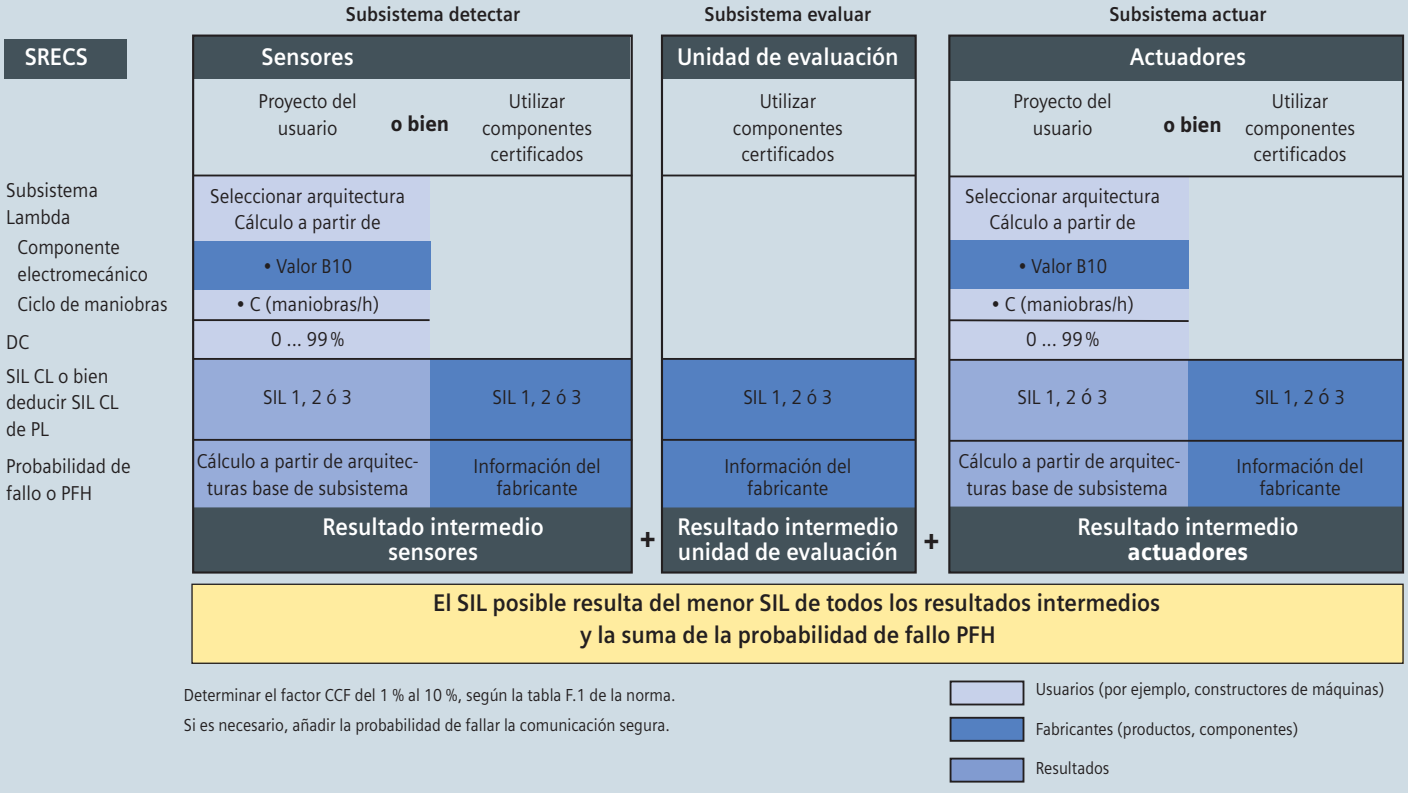
- Requisitos: Parada segura del husillo giratorio en el momento de abrir la cubierta de seguridad.
- Solución: La cubierta de seguridad se vigila con dos interruptores de posición (sensores). Para la desconexión del husillo se integran dos contactores de carga (actuadores). La unidad de evaluación consistirá en un sistema de control seguro (CPU, F-DI, F-DO) o un aparato de maniobra seguro.

La tecnología de conexión entre los subsistemas se tendrá en consideración.

Procedimiento común y simplificado:

1. Considerar cada subsistema o SRP/CS para obtener resultados “intermedios”. Existen dos opciones:
   a. Utilizar componentes certificados con la correspondiente información del fabricante (por ejemplo SIL CL, PFH o PL).
   b. Calcular las tasas de fallo de los elementos de subsistemas o componentes a partir de la arquitectura seleccionada (uno o dos canales). A continuación, se calculará la probabilidad de fallar el subsistema o el SRP/CS.
2. Evaluar los resultados intermedios relativos a los requisitos estructurales (SIL CL o PL) y sumar la probabilidad de fallo/PFH.

Método según EN 62061



Nota: El procedimiento exacto para determinar la seguridad integral se describe en el ejemplo de aplicación de la norma EN 62061.
Ver también: http://support.automation.siemens.com/WW/view/de/2399647

Subsistema "detectar" – Sensores

En el caso de los componentes certificados, el fabricante de los mismos proporciona los valores necesarios (SIL CL y PFH). Utilizando los componentes electromecánicos en el proyecto del usuario, se pueden determinar los niveles SIL CL y PFH de la siguiente manera.

Determinación del SIL CL
En el ejemplo se puede tomar como base el SIL CL 3, pues la arquitectura se corresponde con la categoría 4, según EN 954-1, y se dispone del correspondiente diagnóstico.

Cálculo de las tasas de fallo λ de los componentes del subsistema "interruptor de posición"
Con el valor B10 y las maniobras C se puede calcular la tasa global de fallos de un componente electromecánico según EN 62061, apartado 6.7.8.2.1:

$\lambda = 0{,}1 * C/B10 = 0{,}1 * 1/10.000.000 = 10^{-8}$
C = Ciclo de maniobras por hora (duty cycle), según usuario
Valor B10 = información del fabricante (ver anexo, página 18 – tabla valores B10)

La tasa de fallos λ cubre los factores no peligrosos (λ_S) y peligrosos (λ_D):

$\lambda = \lambda_S + \lambda_D$
$\lambda_D = \lambda$* Cuota de fallos peligrosos en %
$= 10^{-8} * 0{,}2 = 2 * 10^{-9}$
(ver anexo, página 18 – tabla valores B10)

Determinación de la probabilidad de fallos peligrosos PFH_D a partir de la arquitectura

La norma EN 62061 especifica cuatro arquitecturas de subsistemas (arquitecturas base de subsistema A–D). El cálculo de la probabilidad de fallo PFH_D se realizará a partir de las fórmulas previstas en dicha norma para cada una de las arquitecturas.

Cálculo de la tasa de fallos peligrosos λ_D en el caso de subsistemas bicanales con diagnóstico (arquitectura base de subsistema D) y elementos idénticos:

$\lambda_D = (1 - \beta)^2 * \{[\lambda_{De}^2 * DC * T2] + [\lambda_{De}^2 * (1 - DC) * T1]\} + \beta * \lambda_{De}, = \approx 2*10^{-10}$
$PFH_D = \lambda_D * 1\ h \approx 2*10^{-10}$
λ_{De} = tasa de fallos peligrosos para un componente del subsistema

Suponiendo en el ejemplo:

ß = 0,1	supuesto conservador, valor máximo según norma
DC = 0,99	debido a discrepancia y vigilancia de cortocircuito
T2 = 1/C	debido a la evaluación del programa de seguridad
T1 = 87.600 h (10 años)	vida útil del componente

Subsistema “evaluar” – Unidad de evaluación:

En el caso de los componentes certificados, el fabricante proporciona los valores necesarios:

Valores ejemplares:
SIL CL = SIL 3
$PFH_D = < 10^{-9}$

Subsistema “actuar” – Actuadores:

En el caso de los componentes certificados, el fabricante proporciona los valores necesarios:

Valores ejemplares:
SIL CL = SIL 2
$PFH_D = 1{,}29*10^{-7}$

Siempre que el usuario desarrolle el subsistema “actuar”, el procedimiento se corresponde al subsistema “detectar”.

Determinación de la seguridad integral de las funciones de seguridad

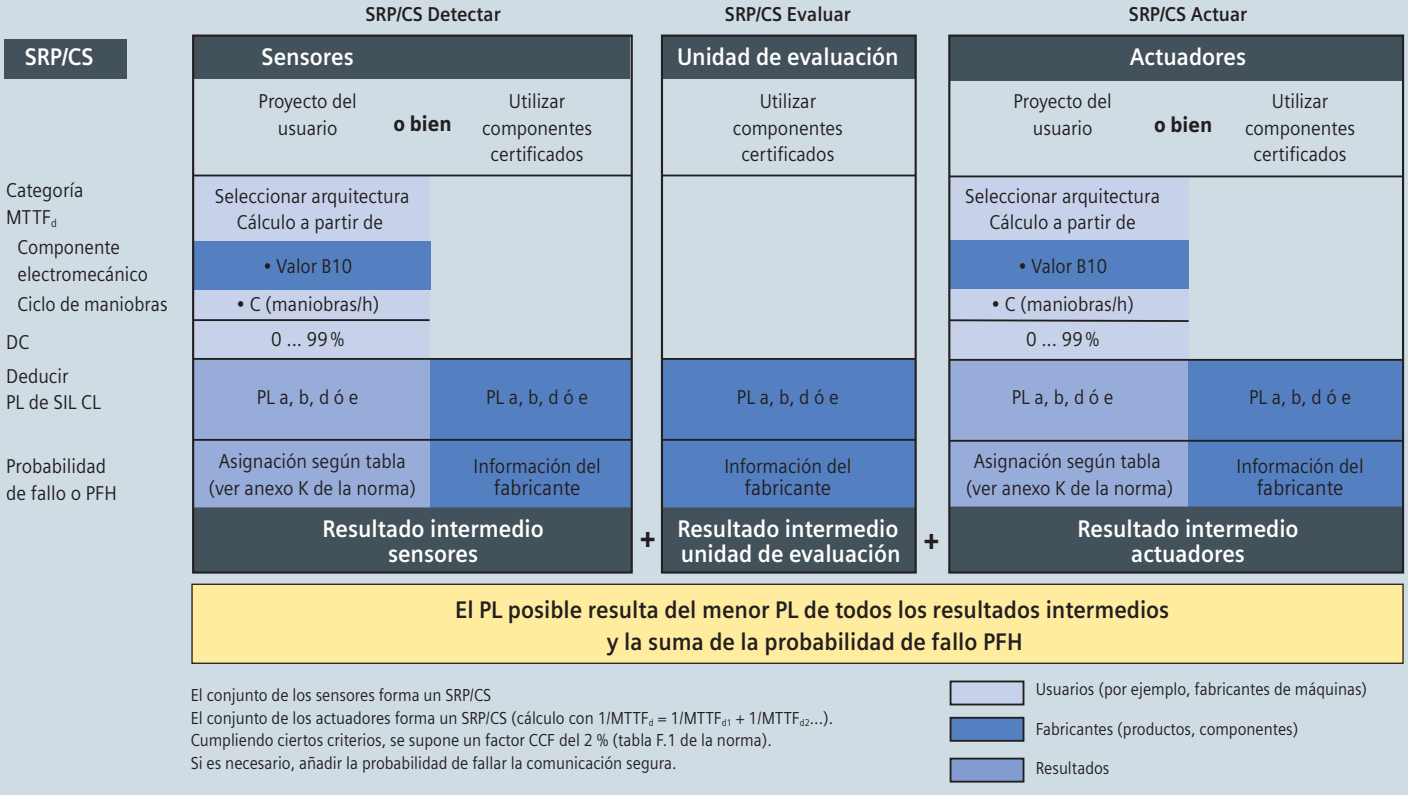
Se determinará el mínimo nivel SIL (SIL CL) entre todos los subsistemas del sistema de control seguro (SRCF):

SIL CL Mn = mínimo (SIL CL (subsistema 1)) .....SIL CL (subsistema n)
= SIL CL 2

Suma de las probabilidades de fallos peligrosos (PFH_D)
de los subsistemas
$PFH_D = PFH_D$ (subsistema 1) + ... + PFH_D (subsistema n) = $1{,}30*10^{-7}$
$= <10^{-6}$ equivale SIL 2

Resultado: La función de seguridad cumple los requisitos SIL 2

Método según EN ISO 13849-1



SRP/CS "detectar" – Sensores

En el caso de los componentes certificados, el fabricante de los mismos proporciona los valores necesarios (PL, SIL CL o PFH_D). El SIL CL y el PL se traducen entre sí a partir de la probabilidad de fallo, ver "Aplicación SIL y PL".
Utilizando los componentes electromecánicos proyecto del usuario, se pueden determinar los niveles PL y PFH_D de la siguiente manera.

Cálculo de las tasas de fallo de los componentes SRP/CS "interruptor de posición"
A partir del valor B10 y el ciclo de maniobras n_{op}, el usuario puede calcular la tasa de fallo $MTTF_d$ del componente electromecánico:

$MTTF_d = B10_d/0{,}1 * n_{op} = 0{,}2 * 10^8$ horas = 2.300 años, equivale $MTTF_d$ = alta

con n_{op} = maniobras por año (información del usuario)

$n_{op} = (d_{op} * h_{op} * 3.600\ s/h) / t_{ciclo}$

suponiendo en base al uso proyectado del componente:

- h_{op} funcionamiento medio en horas/día;
- d_{op} funcionamiento medio en días/año;
- t_{ciclo} promedio entre dos ciclos consecutivos del componente (por ejemplo, conmu tar una válvula) en segundos/ciclo.

Suponiendo en el ejemplo:

DC "alto" debido a discrepancia y vigilancia de cortocircuito
Categoría 4

Resultado: Se obtiene un Performance Level PL e con una probabilidad de fallo de $2{,}47*10^{-8}$

(del anexo K de la norma EN ISO 13849-1:2006)

SRP/CS "evaluar" – Unidad de evaluación

En el caso de los componentes certificados, el fabricante proporciona los valores necesarios:

Valores ejemplares:
SIL CL = SIL 3, equivale PL e
$PFH_D = < 10^{-9}$

SRP/CS "actuar" – Actuadores

En el caso de los componentes certificados, el fabricante proporciona los valores necesarios:

Valores ejemplares:
SIL CL = SIL 2, equivale PL d
$PFH_D = 1{,}29*10^{-7}$

Siempre que el usuario desarrolle el SRP/CS "actuar", el procedimiento se corresponde al SRP/CS "detectar".

Determinación de la seguridad integral de las funciones de seguridad
Se determinará el mínimo nivel PL entre todos los SRP/CS del sistema de control seguro (SRCF):

PL Mn = mínimo (PL (SRP/CS 1)) .....PL (SRP/CS n) = PL d

Suma de las probabilidades de fallos peligrosos (PFH_D) der SRP/CS
$PFH_D = PFH_D$ (SRP/CS 1) + ... + PFH_D (SRP/CS n) = $1{,}74*10^{-7} = <10^{-6}$ equivale PL d

Resultado: La función de seguridad cumple los requisitos PL d

Determinación del Performance Level a partir de la categoría, DC y $MTTF_d$

Aunque las dos normas utilizan diferentes métodos de evaluación de una misma función de seguridad, se pueden comparar los correspondientes resultados.
Procedimiento simplificado para evaluar el PL basado en SPR/CS:

Categoría	B	1	2	2	3	3	4
DC_{avg}	sin	sin	bajo	medio	bajo	medio	alto
$MTTF_d$ / canal							
bajo	a	sin cubrir	a	b	b	c	sin cubrir
medio	b	sin cubrir	b	c	c	d	sin cubrir
alto	sin cubrir	c	c	d	d	d	e

Utilizar SIL y PL

Las funciones de seguridad se pueden validar, según lo indicado anteriormente, de dos maneras diferentes. Los niveles SIL y PL se pueden comparar el uno con el otro a partir de la probabilidad de fallos peligrosos, ver siguiente tabla.

SIL y PL son comparables

Nivel de seguridad integral SIL	Probabilidad de fallos peligrosos por hora (1/h)	Performance Level PL
–	$\geq 10^{-5}$ hasta $< 10^{-4}$	a
SIL 1	$\geq 3 \times 10^{-6}$ hasta $< 10^{-5}$	b
SIL 1	$\geq 10^{-6}$ hasta $< 3 \times 10^{-6}$	c
SIL 2	$\geq 10^{-7}$ hasta $< 10^{-6}$	d
SIL 3	$\geq 10^{-8}$ hasta $< 10^{-7}$	e

4° paso:
Validación a partir del plan de seguridad

Objetivo:
Comprobar la correcta introducción de los requisitos de seguridad especificadas

Resultado:
Prueba documentada del cumplimiento de los requisitos de seguridad

La validación consiste en comprobar si el sistema de seguridad (SRECS) cumple o no los requisitos de la especificación SRCF a partir del plan de seguridad.
Se requiere el siguiente procedimiento:

- Determinar y documentar las responsabilidades.
- Documentar todas las pruebas.
- Validar cada SRCF, realizando las pruebas o el análisis adecuado.
- Validar la seguridad integral sistemática del SRECS.

Proyecto

Se elaborará el plan de seguridad. La validación se desarrollará a partir de ese documento

Pruebas

Se comprobarán todas las funciones de seguridad, según la especificación y tal y como se describe en el 1° paso.

Documentación

La documentación formará parte integral del proceso de investigación en casos de daños debidos a fallos. El contenido de la lista de documentos se detalla en la Directiva sobre Máquinas. La lista comprende, entre otras:

- Análisis de riesgos
- Evaluación de peligros
- Especificación de las funciones de seguridad
- Componentes de hardware, certificados, etc.
- Esquemas de circuitos
- Protocolos de pruebas
- Documentación del software, incluyendo códigos, certificados, etc.
- Información sobre el uso, incluyendo instrucciones de seguridad y las restricciones que haya

Una vez finalizada la validación, se puede elaborar el certificado de conformidad CE para la protección realizada.

CE

Ventajas a todos los niveles: Seguridad de un mismo proveedor

Sea para registrar, mandar y señalizar, evaluar o actuar, con la gama de productos Safety Integrated, Siemens es el único fabricante que puede realizar cualquier función de seguridad deseada en la industria. Tecnología de seguridad completa y de un mismo proveedor, integrada y homogénea a partir de Totally Integrated Automation. Para los usuarios, esto significa: un uso seguro, fiable y rentable de las instalaciones.

Reducir los costes, integrando la tecnología de seguridad

Safety Integrated constituye la aplicación consecuente de la tecnología de seguridad a partir del concepto de Totally Integrated Automation – nuestra amplia gama de productos y sistemas homogéneos e integrados para soluciones de automatización, que es única en su género. Es decir, todas las funciones seguras se integrarán en el sistema de automatización estándar para formar un sistema global integrado. Las ventajas del fabricante de la máquina y del usuario consisten en una importante reducción de los costes en todas las fases de la vida útil.

Con nuestros productos y sistemas para el uso en sistemas convencionales y seguros, así como los correspondientes servicios adicionales y ofertas de formación, todo de un mismo proveedor, puede estar seguro: Safety Integrated siempre ofrece una solución rápida y – sobre todo – económica.

Independientemente de que:

- se opte por una solución convencional, una solución basada en un sistema de bus, o un control/accionamiento (**nivel de flexibilidad**) y/o
- se trate de una simple función de parada de emergencia, una simple cadena de circuitos de seguridad, o bien de operaciones altamente dinámicas (**nivel de complejidad**).

SIRIUS – Valores B10 estándar de componentes electromecánicos

La siguiente tabla incluye los valores B10 estándares de los componentes SIRIUS, incluyendo las tasas de fallos peligrosos, según ISO 13849-2 (anexo D), ISO/FDIS 13849-1:2005 (anexo C) y DIN EN 62061 (anexo D, tipos de falta en componentes eléctricos/electrónicos). Para información más detallada, consulte la norma Siemens SN 31920.

Familia de productos Siemens SIRIUS (componentes electromecánicos)	Valor B10 (maniobras, a título de ejemplo)	Tasa de fallos peligrosos
Dispositivos de parada de emergencia (con contactos de apertura positiva) • desbloqueo giratorio • desbloqueo tirando	 100.000 30.000	 20 % 20 %
Interruptores de tirón por cable para dispositivos de parada de emergencia (con contactos de apertura positiva)	1.000.000	20 %
Interruptores de posición estándar (con contactos de apertura positiva)	10.000.000	20 %
Interruptores de posición con actuador en unidad independiente (con contactos de apertura positiva)	1.000.000	20 %
Interruptores de posición con mecanismo de retención (con contactos de apertura positiva)	1.000.000	20 %
Interruptores de bisagra (con contactos de apertura positiva)	1.000.000	20 %
Interruptores de posición con actuador en unidad independiente (con contactos de apertura positiva)	1.000.000	20 %
Pulsadores (sin bloqueo, con contactos de apertura positiva)	10.000.000	20 %
Contactores/arrancadores con contactos de apertura forzosa (en 3RH) o contactos de espejo (en 3RT), resp.	1.000.000	75 %

Conceptos relativos a la seguridad funcional

Fallo (failure)
Pérdida de la capacidad de funcionar adecuadamente una unidad.

β, Beta:
Factor de falta a consecuencia de una causa común.
Factor CCF: common cause failure factor.
(0,1 – 0,05 – 0,02 – 0,01)

B10
El valor B10 de los componentes sometidos al desgaste es la frecuencia de maniobras: se corresponde al nivel en que un 10 % de las unidades sometidas a la prueba de vida útil hayan fallado. A partir del valor B10 y el ciclo de maniobras se puede calcular la tasa de fallo de componentes electromecánicos.

CCF (common cause failure)
Fallo a consecuencia de una causa común (por ejemplo cortocircuito).
Fallo de varias unidades por una sóla incidencia, sin que se trate de fallos provocadas recíprocamente entre las unidades.

**DC (diagnostic coverage),
nivel de coincidencia de diagnóstico**
Reducción de la probabilidad de fallos peligrosos de hardware que resulta de las pruebas de diagnóstico automatizadas.

Tolerancia a fallos
Capacidad de un SRECS (sistema de control seguro eléctrico), subsistema o elemento de subsistema de mantener operativa una función requerida en condiciones de fallo (resistencia a fallos).

Seguridad funcional
Componente de la seguridad global de una máquina y el sistema de control de la misma que depende de la correcta función del SRECS (sistema de control seguro eléctrico), sistemas seguros en otras tecnologías y sistemas externos de protección.

**Fallo peligroso
(dangerous failure)**
Cada fallo que se produzca en la máquina o la alimentación de energía y que supone algún peligro.

**Categorías B, 1, 2, 3 ó 4
(arquitecturas previstas)**
Esas categorías consideran factores cualitativos y cuantitativos (como, por ejemplo $MTTF_d$, DC y CCF). Aplicando un procedimiento simplificado, considerando las categorías arquitecturas previstas, se puede validar el PL (Performance Level) alcanzado.

λ, Lambda
Tasa de fallo que se compone de las tasas de fallos no críticos (λ_S) y peligrosos (λ_D).

**$MTTF$ / $MTTF_d$
(Mean Time To Failure/Mean Time To Failure dangerous)**
Tiempo medio hasta que se produce un fallo o fallo peligroso. En el caso de los elementos de construcción, el MTTF se puede determinar a partir de un análisis de los datos de campo o predicciones. Siendo constante la tasa de fallo, el promedio de funcionamiento sin fallar es de $MTTF = 1 / \lambda$, siendo Lambda λ la tasa de fallo del equipo. (según las estadísticas, es de suponer que transcurrido el MTTF hayan fallado un 63,2 % de los componentes afectados.)

Performance Level (PL)
Nivel de cumplimiento que especifica la capacidad de los componentes seguros de un sistema de control de ejecutar una función segura en condiciones previsibles: desde PL “a” (máxima probabilidad de fallar) hasta PL “e” (mínima probabilidad de fallar).

PFH_D (Probability of dangerous failure per hour)
Probabilidad de un fallo peligroso por hora.

Proof-Test, prueba repetitiva
Prueba repetitiva que permite detectar pérdidas en el rendimiento del SRECS y los correspondientes subsistemas, de manera que se podrá restablecer, al menos en la mayor medida posible, el estado de nuevo de los mismos.

SFF (safe failure fraction)
Tasa de fallos no críticos en la tasa global de fallos de un subsistema que no provocan fallos peligrosos.

**SIL (Safety Integrity Level)
nivel de seguridad integral**
Nivel discreto (un de tres posibles) que determina los requisitos de seguridad integral en funciones de control seguros asignadas al SRECS, siendo el SIL 3 el nivel superior y el SIL 1 el inferior.

**SIL CL (Claim Limit),
requisito límite SIL**
SIL máximo admisible en un subsistema SRECS, según las restricciones estructurales y la seguridad integral sistemática.

Función de seguridad
Función integral de una máquina, cuya pérdida puede aumentar los riesgos globales de la máquina.

**SRCF (Safety-Related Control Function),
función de control**
Función de control segura ejecutada por el SRECS con nivel de integridad determinado, destinada a mantener el estado seguro de la máquina y evitar un aumento de los riesgos.

**SRECS (Safety-Related Electrical
Control System)**
Sistema de control eléctrico seguro de una máquina, destinado a mantener el estado seguro de la máquina.

**SRP/CS (Safety-Related Parts of
Control System)**
Componente seguro del sistema de control que actúa sobre señales de entrada seguras y genera señales de salida seguras.

Subsistema
Componente de la arquitectura SRECS a nivel superior, provocando la pérdida de cualquier subsistema el fallo de la función de control segura.

Elemento de subsistema
Componente del subsistema que consiste en un módulo o conjunto de módulos.

Productos	SIMATIC Sensors Barreras fotoeléctricas	SIMATIC Sensors Cortinas fotoeléctricas	SIMATIC Sensors Escáneres láser	SIRIUS Interruptores de protección, interr. de bisagra, interr. de carrera corta, interr. magnéticos (sin contacto)
Homologación	Cat. 2 y 4 según EN 954-1 o bien tipo 2 y 4 según IEC/EN 61496	Cat. 2 y 4 según EN 954-1 o bien tipo 2 y 4 según IEC/EN 61496 SIL 2 y 3 según IEC/EN 61508 certificado NRTL	Hasta cat. 3 según EN 954-1 o bien tipo 3 según IEC/EN 61496 certificado NRTL	Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 Hasta PL e según EN ISO 13849-1
Aplicación/ funciones de seguridad	Sistemas de protección sin contacto para la protección de acceso a zonas y puntos peligrosos y entradas a los mismos	Sistemas de protección sin contacto para la protección de zonas peligrosas: • Particularmente inmune a perturbaciones y con alta disponibilidad gracias a circuitos integrados de desarrollo específico (ASICs) y métodos inteligentes de evaluación • Funciones avanzadas: Blanking, Muting, Control de ciclo	Sistemas de protección sin contacto para la protección de zonas peligrosas en instalaciones móviles y estacionarias • Protección horizontal y vertical • Parametrización flexible de campos de protección	Control mecánico de dispositivos de seguridad, bloqueo de puertas de seguridad
Posibilidades de comunicación de seguridad		AS-Interface (ASIsafe) y PROFIBUS con perfil PROFIsafe	AS-Interface (ASIsafe) y PROFIBUS con perfil PROFIsafe	AS-Interface (ASIsafe)

				
SIRIUS Pulsadores parada de emerg., interruptores de tirón, pupitres de mando a 2 manos, pedales, columnas de señalización y lámparas para empotrar	**Módulos seguros ASIsafe**	**DP/AS-i F-Link (ASIsafe Solution PROFIsafe)**	**SIMATIC Mobile Panel 277F IWLAN**	**SIRIUS Módulos de seguridad 3TK28**
Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 Hasta PL e según EN ISO 13849-1	Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 Hasta PL e según EN ISO 13849-1 NFPA 79, certificado NRTL	Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 Hasta PL e según EN ISO 13849-1 NFPA 79, certificado NRTL	Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508	Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 Hasta PL e según EN ISO 13849-1 NFPA 79, certificado NRTL
Aplicaciones de PARADA DE EMERGENCIA en la industria manufacturera y de procesos; señalización de estados en máquinas e instalaciones	Detección segura del estado de dispositivos de protección de efecto mecánico y sin contacto físico para aplicaciones de seguridad en automatización manufacturera (excepción: variadores seguros)	Pasarela segura entre las señales ASIsafe y el telegrama PROFIsafe para aplicaciones de seguridad en automatización manufacturera	Para manejo y visualización (HMI) a pie de proceso de líneas de producción con aplicaciones de seguridad crítica, ejecución de tareas relevantes para la seguridad como p. ej. eliminación de anomalías en líneas en marcha Funciones de seguridad: • Pulsador de parada de emergencia • Dos pulsadores de validación (decha./izda.) • Delimitación por transponder y medida de distancia para inicio de sesión y manejo seguros	Vigilancia de dispositivos de protección como p. ej. aparatos de parada de emergencia, interruptores de posición y sensores de actuación sin contacto físico; vigilancia segura de movimientos (p. ej. vigilancia segura de parada)
AS-Interface (ASIsafe)	AS-Interface (ASIsafe)	AS-Interface (ASIsafe) y PROFIBUS con perfil PROFIsafe	PROFINET con perfil PROFIsafe	

Evaluar

Monitor de seguridad ASIsafe (ASIsafe Solution local)

Hasta cat. 4 según EN 954-1
Hasta SIL 3 según IEC 61508
Hasta PL e según EN ISO 13849-1
NFPA 79, certificado NRTL

Para todo tipo de aplicaciones de seguridad en automatización manufacturera:
- Detección segura del estado de dispositivos de protección de efecto mecánico y sin contacto físico incl. desconexión en 1–2 circuitos de habilitación
- Posibilidad de control activo de salidas distribuidas como p. ej. válvulas seguras o arrancadores de motor
- Acoplamiento de dos redes ASIsafe

AS-Interface (ASIsafe Solution local)

Sistema modular de seguridad SIRIUS 3RK3

Hasta cat. 4 según EN 954-1
Hasta SIL 3 según IEC 61508/62061
Hasta PL e según EN ISO 13849-1

Sistema de seguridad modular parametrizable para todo tipo de aplicaciones de seguridad en automatización manufacturera:
- Evaluación segura del estado de dispositivos de protección de efecto mecánico y sin contacto físico
- Función de diagnóstico integrada
- Vigilancia integrada de prueba de señales y tiempo de discrepancia

Diagnóstico vía PROFIBUS

Safety Unit TM121 C

Hasta cat. 3 según EN 954-1
Hasta SIL 2 según IEC 61508
NFPA 79, certificado NRTL (Canadá)

Dispositivo compacto para vigilar movimientos, por ejemplo en prensas y conformación de metales

Funciones de seguridad:
- Mando a dos manos y con pedal
- Parada de emergencia, cortina fotoeléctrica
- Vigilancia de puertas y rejillas de seguridad
- Selectores seguros de modo de operación
- Control de válvulas de seguridad
- Control de movimiento

RS232

PLCs SIMATIC

Hasta cat. 4 según EN 954-1
Hasta SIL 3 según IEC 61508
NFPA 79, certificado NRTL

Sistemas de seguridad escalables
- ET 200S F-CPU
- S7-300F
- S7-400F

Funciones de seguridad:
- Función integrada de diagnóstico y rutina de autotest
- Al aparecer un fallo, la aplicación puede pasarse flexiblemente a un estado seguro y mantenerla en el mismo
- Coexistencia de programas estándar y de seguridad en una CPU
- Bloques de seguridad certificados por el TÜV, también para aplicaciones con prensas y calderas
- Software: STEP 7 FUP, KOP, S7 Distributed Safety

PROFINET/PROFIBUS con perfil PROFIsafe

Periferia SIMATIC

Hasta cat. 4 según EN 954-1
Hasta SIL 3 según IEC 61508
NFPA 79, certificado NRTL

Sistemas de periferia escalables y redundantes
- ET 200eco
- ET 200M
- ET 200S
- ET 200pro

Funciones de seguridad:
- Vigilancia integrada de prueba de señales y tiempo de discrepancia
- Un mismo sistema de periferia descentralizada con módulos de E/S estándar y de seguridad
- Configuración de la visualización de los tiempos de prueba de señales y de discrepancia usando STEP 7

- PROFIBUS con perfil PROFIsafe: todos los sistemas
- PROFINET con perfil PROFIsafe: ET 200S, ET 200pro

Actuar

Arrancadores de motor para **• ET 200S (IP20)** **• ET 200pro (IP65)**	**Variadores para** **• ET 200S** **• ET 200pro FC**	**Variadores** **1) SINAMICS G120** **2) SINAMICS G120D**	**Sistema de accionamiento SINAMICS S120**	**SINUMERIK 840D**
Hasta cat. 4 según EN 954-1 Hasta SIL 3 según IEC 61508 NFPA 79, certificado NRTL	Hasta cat. 3 según EN 954-1 Hasta SIL 2 según IEC 61508 NFPA 79, certificado NRTL	Hasta cat. 3 según EN 954-1 Hasta SIL 2 según IEC 61508 NFPA 79 y 85, certificado NRTL	Hasta cat. 3 según EN 954-1 Hasta SIL 2 según IEC 61508 NFPA 79, certificado NRTL	Hasta cat. 3 según EN 954-1 Hasta SIL 2 según IEC 61508 NFPA 79, certificado NRTL
Para todo tipo de aplicaciones de seguridad en automatización manufacturera y tareas de accionamiento descentralizadas como en transportadores, manutención o aparatos de elevación • Arranque y desconexión seguros con aparellaje convencional y estático • Protección de motor integrada • Desconexión selectiva de seguridad (ET 200S)	Accionamientos centrales (variador) integrados en sistema usando motores asíncronos normalizados sin encóder Funciones de seguridad integradas y autónomas: • Desconexión segura de par • Parada segura 1 • Limitación segura de velocidad	1) Variadores modulares y centrales de seguridad 2) Variadores descentralizados para motores asíncronos normalizados sin encóder Funciones de seguridad integradas y autónomas: • Desconexión segura de par • Parada segura 1 • Limitación segura autónomas: de velocidad • Control seguro de frenos (sólo G120)	Potente sistema de accionamiento para aplicaciones de control de movimiento en máquinas e instalaciones, p. ej. máquinas de envasado y embalaje o de transformación de plásticos, estampadoras, prensas, manipuladores, etc.) Funciones de seguridad: • Desconexión segura de par • Parada segura 1 y 2 • Parada operativa segura • Limitación segura de velocidad • Control seguro de frenos	Control numérico con funciones de seguridad integradas en control y accionamientos para máquinas-herramienta, p.ej. para la protección en el modo de mantenimiento con puerta de seguridad abierta Funciones de seguridad: • Desconexión de par y parada seguras • Limitación segura de velocidad • Finales de carrera y levas seguras • Lógica programable segura • Gestión segura de frenos • Prueba de aceptación integrada
• PROFIsafe: PROFIBUS/PROFINET con perfil PROFIsafe • Solution Local: aplicación de seguridad local	PROFIBUS/PROFINET con perfil PROFIsafe	PROFIBUS/PROFINET con perfil PROFIsafe	PROFIBUS con perfil PROFIsafe	PROFIBUS con perfil PROFIsafe

Siemens AG
Industry Sector
Low-Voltage Controls and Distribution
Apartado de correos 48 48
90026 NÜRNBERG
ALEMANIA

www.siemens.com/safety-integrated

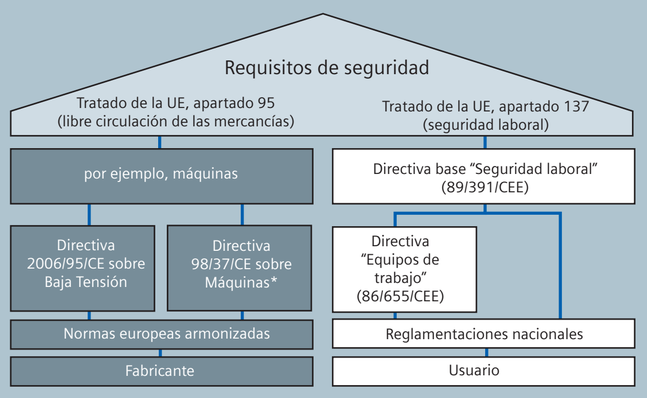
Reservadas las modificaciones 02/09
Referencia E20001-A230-M103-V1-7800
Dispo 27610
WÜ/17261 XX03.52.9.03 PA 02093.0
Impreso en Alemania

E20001-Y290-M103-V1-7800

Seguridad funcional en máquinas e instalaciones

La Directiva Europea sobre Máquinas – puesta en práctica

Normas base para funciones de control seguras



** De momento, es de aplicación obligatoria la Directiva sobre Máquinas 98/37/CE. Como muy tarde, será reemplazada por la nueva Directiva sobre Máquinas 2006/42/CE a finales de 2009.*

Normas armonizadas (efecto de presunción)

Normas base en el desarrollo de funciones de control

Construcción y evaluación de los riesgos de la máquina

EN ISO 12100	Seguridad de máquinas	Conceptos y principios base
EN 1050 (prEN ISO 14121-1)	Seguridad de máquinas	Evaluación de riesgos, parte 1: principios

Requisitos funcionales y en materia de seguridad para sistemas de control seguros

Proyecto y desarrollo de controles seguros

EN 62061:2005 **Seguridad de máquinas** Seguridad funcional en sistemas de control electrónicos, electrónicos programables y eléctricos	**EN ISO 13849-1:2006** **Seguridad de máquinas** Componentes seguros en sistemas de control, parte 1: principios generales *Norma revisada a partir de la EN 954-1:1996, fase de transición hasta presuntamente 2009*
Arquitecturas libres **Nivel de seguridad integral (SIL)** SIL 1, SIL 2, SIL 3	**Arquitecturas categorizadas** **Performance Level (PL)** PL a, PL b, PL c, PL d, PL e

Aspectos de seguridad eléctricos

EN 60204-1	Seguridad de máquinas:	Equipos eléctricos en máquinas, parte 1: requisitos generales

Proyecto y desarrollo de controles seguros

Estrategia para minimizar los riesgos, según EN ISO 12100-1

Determinación de medidas de minimización de riesgos en un proceso iterativo:

1. Especificar los límites de la máquina
2. Localizar, valorar y evaluar los posibles riesgos
3. Valorar el riesgo que supondrán los peligros y situaciones de peligro en cada caso concreto
4. Evaluar el riesgo y determinar las medidas de protección
5. Eliminación o minimización de los riesgos a partir del método de tres etapas: diseño constructivo con seguridad inherente, medidas de protección técnicas e información para usuarios

La norma EN 1050 (prEN ISO 14121-1) incluye información detallada sobre los pasos 1 a 4.

Aplicable en el caso de los sistemas de control eléctricos, electrónicos y electrónicos programables seguros (SRECS) de máquinas

EN 62061:2005 **(parte de la norma europea base IEC 61508)**

Aplicable en el caso de los elementos de sistemas y todo tipo de máquina, independientemente de la tecnología y forma de energía (eléctrica, hidráulica, neumática, mecánica, etc.)

EN ISO 13849-1:2006 **(norma revisada a partir de la EN 954-1:1996, fase de transición hasta presuntamente 2009)**

Plan de seguridad

Estrategia para la realización de las funciones de seguridad, responsabilidades, mantenimiento ...

Análisis de riesgos

Riesgo, según el peligro localizado Importancia del daño = Importancia del daño **Se** y

Frecuencia y perduración	**Fr**
Probabilidad	**Pr**
Posible evitación	**Av**

Determinación del SIL requerido

(asignación SIL)

Frecuencia y/o perduración **Fr**		Probabilidad de la situación peligrosa **Pr**		Posible evitación **Av**	
≤ 1 h	5	frecuentemente	5		
> 1 h–1 día	5	probable	4		
> 1 día–2 semanas	4	posible	3	imposible	5
> 2 semanas–1 año	3	poco frecuente	2	posible	3
> 1 año	2	despreciable	1	probable	1

Consecuencias	Alcance de daños **Se**	Clase **Cl = Fr + Pr + Av**				
		3–4	5–7	8–10	11–13	14–15
Muerte, pérdida de ojos, brazos	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, pérdida de dedos de la mano	3	otras medidas		SIL 1	SIL 2	SIL 3
Reversible, tratamiento médico	2				SIL 1	SIL 2
Reversible, primeros auxilios	1					SIL 1

Procedimiento
1. Determinar la importancia de daños Se
2. Determinar frecuencia Fr, probabilidad Pr y evitación Av
3. Suma Fr + Pr + Av = clase Cl
4. Punto de intersección línea importancia de daños Se y columna Cl = SIL requerido

Determinación del PL requerido

(con esquema de riesgos)

Parámetros de riesgo

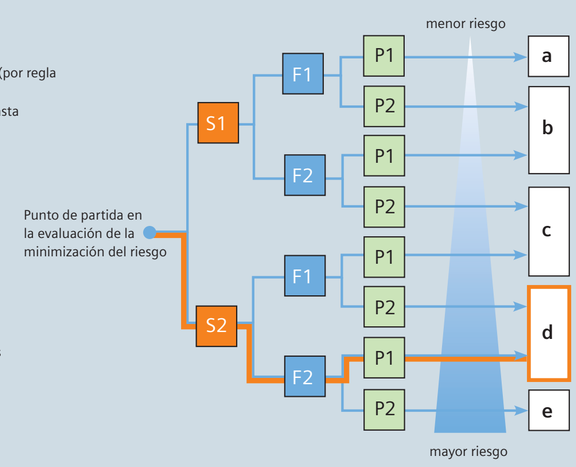
S = Importancia de lesiones
- S1 = lesión de menor importancia (por regla general, reversible)
- S2 = lesión grave (irreversible) y hasta la muerte

F = Frecuencia y/o perduración del peligro
- F1 = muy poca o poca frecuencia y/o corta exposición
- F2 = mayor frecuencia hasta permanente y/o larga exposición

P = Posible evitación del peligro o minimización de daños
- P1 = posible en ciertas condiciones
- P2 = apenas posible

a, b, c, d, e = objetivos de seguridad del Performance Level

Performance Level PL requerido



Configuración del circuito de seguridad y determinación del nivel de seguridad

SRECS	Subsistema detectar: Sensores	Subsistema evaluar: Unidad de evaluación	Subsistema actuar: Actuadores
	Proyecto del usuario **o bien** Utilizar componentes certificados	Utilizar componentes certificados	Proyecto del usuario **o bien** Utilizar componentes certificados
Subsistema Lambda	Seleccionar arquitectura Cálculo a partir de		Seleccionar arquitectura Cálculo a partir de
Componente electromecánico	• Valor B10		• Valor B10
Ciclo de maniobras	• C (maniobras/h)		• C (maniobras/h)
DC	0 ... 99 %		0 ... 99 %
SIL CL, o bien deducir SIL CL de PL	SIL 1, 2 ó 3 / SIL 1, 2 ó 3	SIL 1, 2 ó 3	SIL 1, 2 ó 3 / SIL 1, 2 ó 3
Probabilidad de falta o PFH	Cálculo a partir de arquitecturas base de subsistema / Información del fabricante	Información del fabricante	Cálculo a partir de arquitecturas base de subsistema / Información del fabricante
	Resultado intermedio sensores +	**Resultado intermedio unidad de evaluación** +	**Resultado intermedio actuadores**

El SIL posible resulta del menor SIL de todos los resultados intermedios y la suma de la probabilidad de fallo PFH

Determinar el factor CCF del 1 % al 10 %, según la tabla F.1 de la norma.
Si es necesario, añadir la probabilidad de fallar la comunicación segura.

SRP/CS	SRP/CS Detectar: Sensores	SRP/CS Evaluar: Unidad de evaluación	SRP/CS Actuar: Actuadores
	Proyecto del usuario **o bien** Utilizar componentes certificados	Utilizar componentes certificados	Proyecto del usuario **o bien** Utilizar componentes certificados
Categoría MTTF$_d$	*Seleccionar arquitectura Cálculo a partir de*		*Seleccionar arquitectura Cálculo a partir de*
Componente electromecánico	• Valor B10		• Valor B10
Ciclo de maniobras	• C (maniobras/h)		• C (maniobras/h)
DC	0 ... 99 %		0 ... 99 %
Deducir PL de SIL CL	PL a, b, c, d ó e / PL a, b, c, d ó e	PL a, b, c, d ó e	PL a, b, c, d ó e / PL a, b, c, d ó e
Probabilidad de falta o PFH	Asignación según tabla (ver anexo K de la norma) / Información del fabricante	Información del fabricante	Asignación según tabla (ver anexo K de la norma) / Información del fabricante
	Resultado intermedio sensores +	**Resultado intermedio unidad de evaluación** +	**Resultado intermedio actuadores** / **Resultado intermedio actuadores**

El PL posible resulta del menor PL de todos los resultados intermedios y la suma de la probabilidad de falta PFH

El conjunto de los sensores forma un SRP/CS.
El conjunto de los actuadores forma un SRP/CS (cálculo con $1/MTTF_d = 1/MTTF_{d1} + 1/MTTF_{d2}$ ...).
Cumpliendo ciertos criterios, se supone un factor CCF del 2 % (tabla F.1 de la norma).
Si es necesario, añadir la probabilidad de fallar la comunicación segura.

Usuarios (por ejemplo, constructores de máquinas)
Fabricantes (productos, componentes)
Resultados

SIL y PL son comparables

Nivel de seguridad integral SIL	Probabilidad de fallos peligrosos por hora (1/h)	Performance Level (PL)
–	$\geq 10^{-5}$ hasta $< 10^{-4}$	a
SIL 1	$\geq 3 \times 10^{-6}$ hasta $< 10^{-5}$	b
SIL 1	$\geq 10^{-6}$ hasta $< 3 \times 10^{-6}$	c
SIL 2	$\geq 10^{-7}$ hasta $< 10^{-6}$	d
SIL 3	$\geq 10^{-8}$ hasta $< 10^{-7}$	e

Validación a partir del plan de seguridad

Comprobar la correcta introducción de los requisitos de seguridad especificados		
Proyecto	Pruebas	Documentación

Marca CE (declaración de conformidad) CE

Fallo (failure)
Pérdida de la capacidad de funcionar adecuadamente una unidad.

β, **Beta**:
Factor de fallo a consecuencia de una causa común.
Factor CFF: common cause failure factor β (0,1 – 0,05 – 0,02 – 0,01)

B10
El valor B10 de los componentes sometidos al desgaste es la frecuencia de maniobras: se corresponde al nivel en que un 10 % de las unidades sometidas a la prueba de vida útil hayan fallado. A partir del valor B10 y el ciclo de maniobras se puede calcular la tasa de fallo de componentes electromecánicos.

CCF (common cause failure)
Fallo a consecuencia de una causa común (por ejemplo cortocircuito). Fallo de varias unidades por una sóla incidencia, sin que se trate de fallos provocados recíprocamente entre las unidades.

DC (diagnostic coverage), nivel de coincidencia de diagnóstico
Reducción de la probabilidad de fallos peligrosos de hardware que resulta de las pruebas de diagnóstico automatizadas.

Tolerancia a fallos
Capacidad de un SRECS (sistema de control seguro eléctrico), subsistema o elemento de subsistema de mantener operativa una función requerida en condiciones de fallo (resistencia a fallos).

Seguridad funcional
Componente de la seguridad global de una máquina y el sistema de control de la misma que depende de la correcta función del SRECS (sistema de control seguro eléctrico), sistemas seguros en otras tecnologías y sistemas externos de protección.

Fallo peligroso (dangerous failure)
Cada fallo que se produzca en la máquina o la alimentación de energía y que supone algún peligro.

Categorías B, 1, 2, 3 ó 4 (arquitecturas previstas)
Las categorías consideran factores cualitativos y cuantitativos (como por ejemplo $MTTF_d$, DC y CCF). Aplicando un procedimiento simplificado, considerando las arquitecturas previstas, se puede validar el Performance Level PL alcanzado.

λ, **Lambda**
Tasa de fallo que se compone de las tasas de fallos no críticos (λ_S) y peligrosos (λ_D).

MTTF / MTTF$_d$
(Mean Time To Failure/Mean Time To Failure dangerous)
Tiempo medio hasta que se produce un fallo o fallo peligroso. En el caso de los elementos de construcción, el MTTF se puede determinar a partir de un análisis de los datos de campo o predicciones. Siendo constante la tasa de fallo, el promedio de funcionamiento sin fallar es de MTTF = 1 / λ, siendo Lambda λ la tasa de fallo del equipo (según las estadísticas, es de suponer que transcurrido el MTTF hayan fallado un 63,2 % de los componentes afectados.)

Performance Level (PL)
Nivel discreto que especifica la capacidad de los componentes seguros de un sistema de control de ejecutar una función segura en condiciones previsibles desde PL "a" (máxima probabilidad de fallar) hasta PL "e" (mínima probabilidad de fallar).

PFH$_D$ (Probability of dangerous failure per hour)
Probabilidad de un fallo peligroso por hora.

Proof-Test, prueba repetitiva
Prueba repetitiva que permite detectar pérdidas en el rendimiento del SRECS y los correspondientes subsistemas, de manera que se podrá restablecer, al menos en la mayor medida posible, el estado de nuevo de los mismos.

SFF (safe failure fraction)
Tasa de fallos no críticos en la tasa global de fallos de un subsistema que no provocan fallos peligrosos.

SIL (Safety Integrity Level), nivel de seguridad integral
Nivel discreto (uno de tres posibles) que determina los requisitos de seguridad integral en funciones de control seguras asignadas al SRECS, siendo el SIL 3 el nivel superior y el SIL 1 el inferior.

SIL CL (Claim Limit), requisito límite SIL
SIL máximo admisible en un subsistema SRECS, según las restricciones estructurales y la seguridad integral sistemática.

Función de seguridad
Función integral de una máquina, cuya pérdida puede aumentar los riesgos globales de la máquina.

SRCF (Safety-Related Control Function), función de control
Función de control segura ejecutada por el SRECS con nivel de integridad determinado, destinada a mantener el estado seguro de la máquina y evitar un aumento de los riesgos.

SRECS (Safety-Related Electrical Control System)
Sistema de control eléctrico seguro de una máquina, destinado a mantener el estado seguro de la máquina.

SRP/CS (Safety-Related Parts of Control System)
Componente seguro del sistema de control que actúa sobre señales de entrada seguras y genera señales de salida seguras.

Subsistema
Componente de la arquitectura SRECS a nivel superior, provocando la pérdida de cualquier subsistema el fallo de la función de control segura.

Elemento de subsistema
Componente del subsistema que consiste en un módulo o conjunto de módulos.

Safety Integrated

Answers for industry.

SIEMENS