ZVEI:
Die Elektroindustrie

Seguridad de las máquinas

Guía para la interpretación y aplicación de las Normas EN 62061 y EN ISO 13849-1

2ª Edición

Fachverband Automation

PIE DE IMPRENTA

Seguridad de las máquinas

Guía para la interpretación y aplicación de las Normas EN 62061 y EN ISO 13849-1

ZVEI – Asociación alemana de la industria electrotécnica y electrónica
Lyoner Straße 9
60528 Frankfurt am Main

Departamento de sistemas y dispositivos industriales de conmutación y control
Comité tecnico de sistemas de seguridad en automatización

Autor: Dr. Markus Winzenick

Tel: +49 69 6302-426
Fax: +49 69 6302-319
Mail: winzenick@zvei.org
www.zvei.org/automation

Junio 2012

Seguridad de las máquinas

¿ Es usted constructor o integrador de maquinaria ?
¿ Remodela o re-ensambla usted máquinas ?

¡ Lo que se ha de considerar en futuro sobre la seguridad funcional !

Interpretación y aplicación de las Normas sobre la seguridad funcional de la maquinaria EN 62061 y EN ISO 13849-1

1. *Procedimiento básico para responder a los requisitos de la Directiva de la Maquinaria (2006/42/CE)*

¿ Que es lo que debo hacer para poder introducir en el mercado europeo una máquina que cumpla los requisitos de las directivas ?

La Directiva de la Maquinaria (2006/42/CE) exige que las máquinas no presenten ningún peligro (Evaluación de riesgos según Norma EN ISO 12100). Ya que el riesgo nulo no existe en el campo de la técnica, es necesario reducir los riesgos hasta alcanzar un riesgo residual aceptable. Cuando la seguridad de la máquina depende de los sistemas de mando el objetivo general consiste en diseñar estos sistemas, de tal manera que la probabilidad de fallos funcionales sea suficientemente reducida. Si esto no es practicable, esos posibles fallos no deben provocar la pérdida de la función de seguridad. Para poder cumplir con esta exigencia es conveniente hacer uso de las normas harmonizadas por la Comisión Europea y que se publican en el Diario Oficial de la Union Europea. (Presunción de conformidad). Solo de esta manera se pueden evitar costes elevados y es fuerzos suplementarios para probar la conformidad en casos de accidentes o daños.

En este documento se comparan las dos Normas EN 62061 y EN ISO 13849-1 proporcionando también al lector ayuda para su selección

2. *¿ Porqué la Norma EN 954-1 no es válida ?*

En el pasado, las partes de los sistemas mando relativas a la seguridad (SRP/CS) se diseñaban de acuerdo con la norma EN 954-1. (SRP/CS = ingles: safety related parts of the control system)

Esta norma se basaba en una clasificación por categorias, que depende de los riesgos a cubrir. Las categorias especificaban el comportamiento de un sistema ante un fallo (aproximación determinista). Debido al uso generalizado de la electrónica y expecialmente de los sistemas electrónicos programables, esta simple categorización, basada unicamente en la estructura de un sistema de mando, ya no es suficiente para determinar la reducción de riesgo necesaria. La norma tampoco permitía la consideración de las probabilidades de los fallos (aproximación probabilistica).

Las dos Normas sucesoras, EN 62061 y EN ISO 13849-1 ponen remedio a esos problemas.

3. Objeto y campo de aplicación de las dos normas

EN ISO 13849-1: *Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales de diseño.*

Esta Norma se aplica a las partes de los sistemas de mando relativas a la seguridad (SRP/CS), incluyendo el diseño del soporte lógico (software) de cualquier tipo de máquina, independientemente de la tecnología y del tipo de energía utilizadas (eléctrica, hidráulica, neumática, mecánica, etc.).

La Norma EN ISO 13849-1 también contiene requisitos específicos para SRP/CS que utilízan sistemas electrónicos programables.

EN 62061: *Seguridad funcional de sistemas de mando eléctricos, electrónicos y programables de máquinas.*

Esta Norma proporciona requisitos de seguridad y orientaciones sobre los principios para el diseño, integración y validación de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad (SRP/CS) de las máquinas

Esta Norma no proporciona requisitos para partes de sistemas de mando de que no sean eléctricas o electrónicas (por ejemplo hidráulica, neumática, electromecánica, etc.)

4. Resumen de la EN ISO 13849-1

La Norma EN ISO 13849-1 se basa en las conocidas categorías de la EN 954-1:1996, considerando también funciones de seguridad completas e incluyendo todos los elementos integrados para realizar las funciones definidas.

La Norma EN ISO 13849-1 añade la consideración del aspecto cuantitativo de las funciones de seguridad a la aproximación puramente qualitativa de la EN 954-1 para definir Niveles de prestación (PL = performance level).

Para las partes o componentes integrados se necesitan, dependiendo del tipo de componente, los valores de las caracteristicas siguientes:

- Categoría (requisitos estructurales)
- PL : Nivél de prestación (PL = performance level)
- $MTTF_d$: Tiempo media hasta que ocurra un fallo peligroso (ingles: mean time to dangerous failure)
- B_{10d} : Número de ciclos hasta que el 10% de los componentes falla peligrosamente

- DC : Cobertura del diagnóstico (inglés: diagnostic coverage)
- CCF : Fallo de causa común (inglés: common cause failure)
- T_M : Duración de la misión (inglés: mission time)

La Norma describe como puede ser calculado el nivel de prestación (PL), para las partes de los mandos relativos a la seguridad (SRP/CS), basándose en arquitecturas determinadas (en ingles: designated architectures), para la duración prevista de la misión.

En caso de desviacíon, la Norma EN ISO 13849, indíca como referencia a la Norma IEC 61508. Para la combinación de varias SRP/CS, la primera da indicaciones de como estimar el nivel de prestación global.

Para más informaciones respectivas a la validación, EN ISO 13849-1 da referencia a la Parte 2 que ya fue publicada a finales del año 2003. Esta parte contiene informaciones y datos relativos a la consideración de fallos, al mantenimiento, a la documentación técnica y las informaciones para el uso. El periodo de transición en el cual las dos Normas EN 954-1 y EN ISO 13849-1 podían usarse alternativamente acabó en el 31 de diciembre del 2011.

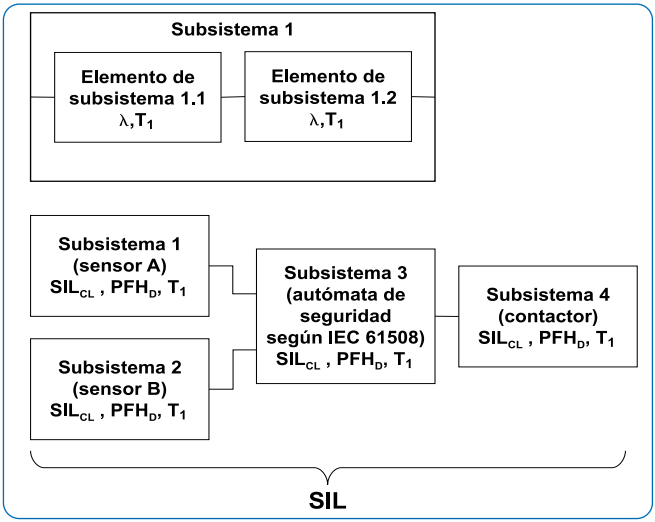
5. *Resumen de la EN 62061*

La Norma EN 62061 es una norma para un sector específico, derivada de la IEC 61508. Esta Norma describe la realización de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad. La norma considera el ciclo de vida completo, desde la fase de diseño hasta la la puesta fuera de servicio y esta basada en una aproximación tanto qualitativa como quantitativa.

La capacidad de prestación está definida por el **nivel de integridad de la seguridad o SIL** (inglés: safety integrity level).

Las funciones de seguridad, identificadas durante la evaluación de riesgos, se dividen en funciones de seguridad parciales y son a su vez asociadas a componentes reales cono sistemas parciales, subsistemas y elementos de subsistemas. La Norma considera tanto el soporte material (hardware) como el soporte lógico (software).

Un sistema de mando relativo a la seguridad (SRP/CS) se compone de varios subsistemas. La seguridad de un subsistema se define por sus parámetros „límite de respuesta" (SILCL, límite de tolerancia o aptitud máxima) y „PFH_d".



Parámetros de seguridad de los subsistemas:

- SILCL : Límite de respuesta SIL (inglés: SIL claim limit)
- PFH_d : Probabilidad media de que se produzca un fallo peligroso por hora (1/h)
- T_1 : Tiempo de servicio (inglés: lifetime)

Los subsistemas a su vez pueden estar compuestos de elementos (de subsistemas) con estructuras diferentes, con los los parámetros necesarios para calcular el valor PHFD correspondiente al subsistema.

Parámetros de los elementos de subsistemas:

- λ : tasa de fallos (inglés : failure rate) para los elementos sensibles al desgaste se utiliza e valor B_{10}
- SFF : tasa o fracción de averías seguras (que no llevan a la perdida de la función de seguridad – en inglés: safe failure fraction)

Para los elementos electromecánicos el fabricante indicará la tasa de fallos en forma del valor B_{10} relacionado con el número de ciclos. Tomando el cuenta la frequencia de actuación o corte de la aplicación se deberá calcular la tasa de fallos y el tiempo máximo de utilización.

Cuando el subsistema se diseña / construye a partir de elementos de subsistema se han de definir los siguientes parámetros internos.

- T_2 : Intervalo entre verificaciones (tests) de diagnóstico (inglés: diagnostic test intervall)
- β : Vulnerabilidad a los fallos por causa común (ingles: suscetibility to common cause failure)
- DC : Cobertura del diagnóstico: Medida de la efectividad del diagnóstico. (inglés: diagnostic coverage)

El valor PFH_D total de un sistema de mando relativo a la seguridad se calcula sumando los valores PFH_D de cada subsistema integrante.

Para realizar un sistema de mando relativo a la seguridad, el usuario de la Norma tiene las posibilidades siguientes:

- Utilizar componentes y subsistemas que cumplen los requisitos de una de las Normas EN 954-1, IEC 61508 o EN 62061. La Norma indíca como integrar ese tipo de elementos para realizar una función de seguridad
- Diseñar sus propios subsistemas
  - – Subsistemas electrónicos programmables y subsistemas complejos. Aplicación de la Norma IEC 61508
  - – Aparatos simples y subsistemas. Aplicación de la Norma EN 62061

La Norma presenta un sistema completo para la realización de sistemas de mando relativos a la segurida ya sean eléctricos, electrónicos o electrónicos programables. La EN 62061 es Norma Harmonizada desde diciembre del año 2005.

Para sistemas de mando de seguridad no eléctricos se aplica EN ISO 13849-1.

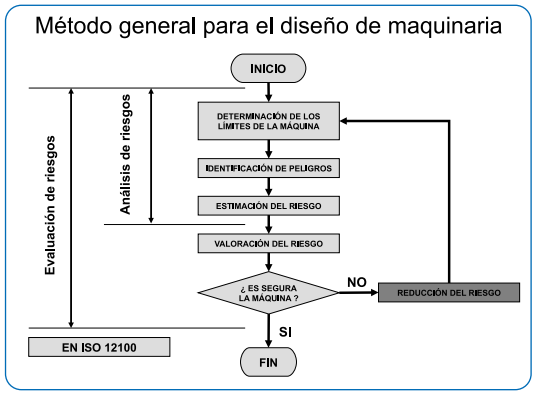
6. *Paso a paso hasta la función de seguridad. Procedimiento básico*

1er Paso – Evaluación de riesgos según EN ISO 12100

En general se considera que cualquier peligro existente en una máquina llevará, antes o despues a causar un daño si no se toman medidas para evitarlo.

Las medidas de seguridad destinadas a reducir riesgos, son aplicadas por los fabricantes de maquinaria y por los usuarios. Las medidas de seguridad tomadas durante la fase de diseño son preferibles a aquellas tomadas por el usuario ya que, generalmente, son más eficaces.

El diseñador de maquinaria debe respetar el orden indicado a continuación, tomando en cuenta la experiencia del uso de máquinas similares y si fuese posible, el intercambio de informaciónes con posibles clientes.



- Definir los límites de la máquina incluyendo el uso previsto
- Identificar los peligros, situaciones y sucesos peligrosos asociados con la máquina
- Estimar el riesgo de cada peligro o cada situación o suceso peligroso
- Valoración del riesgo y decisión sobre la necesidad de reducir el riesgo

2° Paso – Definición de las medidas destinadas a reducir los riesgos determinados

El objetivo es la máxima reducción de los riesgos que han sido determinados, teniendo en cuenta diferentes factores. El proceso es iterativo, ya que puede ser necesario repetir este paso para reducir el riesgo de manera adecuada aun cuando la tecnologia disponible ha sido aplicada de manera óptima.

Este proceso ha de realizarse teniendo en cuenta y en el orden siguiente:

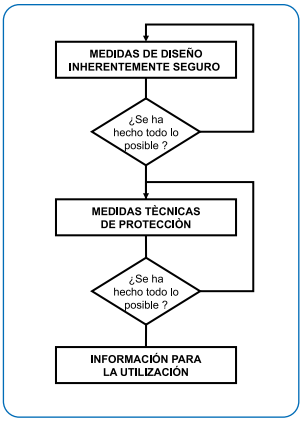
– la seguridad de la máquina en todas las fases de su vida útil

– la aptitud de la máquina para realizar la función deseada

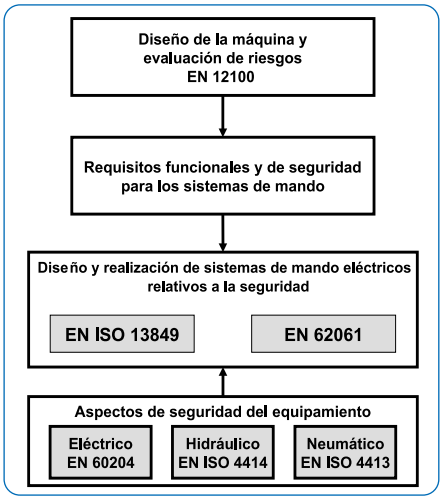
– la facilidad de uso de la máquina

Solamente después se pueden tomar en consideración los costes de fabricación, servicio y demontaje de la máquina.

El análisis y el proceso de reducción del riesgo exige que los peligros sean eliminados o los riesgos reducidos utilizando las siguientes medidas preventivas en el orden dado



– Eliminar el peligro o reducir el riesgo mediante un diseño inherentemente seguro
– Reducir el riesgo mediante dispositivos de protección y medidas suplementarias
– Reducir el riesgo mediante la información al usuario sobre el riesgo residual y de las medidas personales de protección a tomar por el usuario



3er Paso – Reducción del riesgo mediante la aplicación de medidas de mando

Si para reducir el riesgo se utilizan sistemas de mando, el diseño de las partes de los sistemas de mando que desempeñen la función de seguridad debe ser parte integral del diseño de la máquina. Esas partes deberán proveer la función de seguridad con un PL o SIL adecuado a la reducción de riesgo requerida.

4° Paso – Realización de las medidas de mando con la ayuda de EN ISO 13849-1 o de EN 62061

1) Determinación del nivel de prestaciónes requerido

EN ISO 13849-1

Determinación del nivel de prestaciónes requerido

S = Gravedad de la lesión

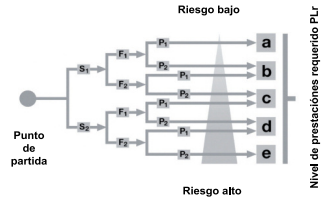
S1 = Lesión leve (normalmente reversible)
S2 = Lesión grave (normalmente irreversible · incluyendo la muerte)

F = Frecuencia y/o duración de la exposición al peligro

F1 = Raro a bastante frecuente y/o corta duración de la exposición
F2 = Frecuente a continuo y/o larga duración de la exposición

P = Posibilidad de evitar el peligro o de limitar el daño

P1 = Posible en determinadas condiciones
P2 = Raramente posible



EN 62061

Estimación del riesgo y determinación del nivel de integridad de la seguridad (SIL)

Frequencia y duración DI > 10min / Dc < 10min	Fr (DI/Dc)	Probabilidad del evento peligroso	Pr	Posibilidad de evitar o reducir el daño	Av
≤ 1 / hora	5 / 5	Alta	5	Imposible	5
> 1 / hora - ≤ 1 / día	5 / 4	Probable	4	Posible	3
> 1 / día - ≤ 2 / semana	4 / 3	Posible	3	Probable	1
> 2 / semana - ≤ 1 / año	3 / 2	Rara	2		
> 1 / año	2 / 1	Despreciable	1		

Daño, consequencias y gravedad	S	Clase K = Fr+Pr+Av				
		3-4	5-7	8-10	11-13	14-15
Muerte, pérdida de un ojo o un brazo	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, pérdida de varios dedos	3		MA	SIL 1	SIL 2	SIL 3
Reversible con atención médica	2			MA	SIL 1	SIL 2
Reversible, primeros auxilios	1				MA	SIL 1
MA = Medidas Adicionales						

2) Especificación

La especificación de los requisitos funcionales ha de describir detalladamente cada función de seguridad a realizar. A este efecto, han de definirse las interacciones y los interfaces con otras funciones de mando y las reacciones requeridas ante un fallo. Para esto ha de determinarse el PL o SIL necesario.

3) Diseño de la arquitectura del sistema de mando

Una parte del proceso de reducción de riesgos consiste en determinar las funciones de seguridad de la máquina. Esto comprende las funciones de seguridad realizadas por los sistemas de mando, como por ejemplo, la prevención de la puesta en marcha intempestiva. Cuando se definan las funciones de seguridad, han de tenerse siempre en cuenta los diferentes modos de operación de la máquina (por ejemplo : modo automático o modo de reglaje) que puedan exigir medidas de protección diferentes en función de un modo específico (por ejemplo la aplicación de una velocidad reducida en el modo de reglaje y la de un mando bimanual durante el modo automático). Una función de seguriad puede realizarse por una o más partes del mando relativas a la seguridad (SRP/CS) y diferentes funciones de seguridad pueden estar repartidas en varias partes del mando relativas a la seguridad (por ejemplo : unidades de lógica o elementos de transmisión de energía).

4) Determinacíon del nivel de prestaciones alcanzado

EN ISO 13849-1

Para cada SRP/CS o combinación de SRP/CS que desempeñen una función de seguridad, es necesario efectuar una evaluación del PL alcanzado.

El PL de una SRP/CS depende de los parámetros siguientes:

- El valor $MTTF_d$ o B_{10d} de los componentes individuales
- El valor DC de la cobertura del diagnóstico
- La medidas tomadas contra Fallos de causa común CCF
- La estructura
- El comportamiento ante un defecto
- El soporte lógico relativo a la seguridad (software)
- Los fallos sistemáticos
- La aptitud a ejecutar la función de seguridad ante las condiciones del medio ambiente previstas
- La aplicación de principios de seguridad de eficacia probada

EN 62061

La selección y el diseño de las SRP/CS deberá responder a los requisitos siguientes:

- Requisitos para la integridad de la seguridad de los componentes materiales (hardware) que comprenden
- Los limites estructurales respectivos a la integridad de la seguridad del soporte material
- Los requisitos para la probabilidad de fallos aleatorios peligrosos del soporte material.

Asi como los siguientes requisitos para la integridad sistemática

- Requisitos para evitar los fallos
- Requisitos para la controlar los fallos sistemáticos

La EN 62061 describe también los requisitos para la realización de los programas de aplicación.

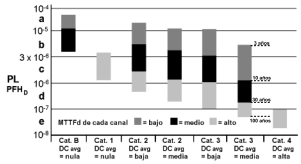
Parámetros de seguridad de los subsistemas son:

- SILCL : Límite de respuesta SIL (inglés: SIL claim limit)
- PFH_d : Probabilidad media de que se produzca un fallo peligroso por hora (1/h)
- T_1 : Tiempo de servicio

EN ISO 13849-1

Performance level (PL)	Probabilidad media de un fallo peligroso por hora (1/h)
a	$\geq 10^{-5}$ a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
e	$\geq 10^{-8}$ a $< 10^{-7}$

Relación entre las categorías, el $MTTF_d$ de cada canal la DC_{avg}, y el PL



Nota:
el valor PFH es indispensable para determinar el nivél de prestaciones (PL) pero además se necesita tener en cuenta las medidas para evitar fallos, como CCF y categorías, así como el DC.

EN IEC 62061

Probabilidad media de un fallo peligroso por hora (1/h)	SIL (IEC 61508)
$\geq 10^{-6}$ a $< 10^{-5}$	1
$\geq 10^{-7}$ a $< 10^{-6}$	2
$\geq 10^{-8}$ a $< 10^{-7}$	3

Parámetros de seguridad de los subsistemas:

- λ: tasa de fallos
- B_{10d} : para los elementos sensibles al desgaste
- T_1 : Tiempo de servicio
- T_2 : Intervalo de test diagnóstico
- β: Vulnerabilidad a los fallos de causa común
- DC : Cobertura del diagnóstico
- SFF : tasa o fracción de averías seguras (que no llevan a la perdida de la función de seguridad (en inglés: safe failure fraction)

SFF	HFT 0	HFT 1	HFT 2
< 60 %	inaceptable	SIL 1	SIL 2
60 % a < 90 %	SIL 1	SIL 2	SIL 3
90 % a < 99 %	SIL 2	SIL 3	SIL 3
≥ 99 %	SIL 3	SIL 3	SIL 3

EN ISO 13849-1	EN IEC 62061

Performance level (PL)	SIL
a	—
b	1
c	
d	2
e	3

Nota:
la tabla describe la relación entre los dos conceptos de las Normas (PL y SIL). Para la evaluación de un SRP/CS la comparaciòn de los valores PFHd por sí sola no es suficiente.

5) Verificación

El PL de una SRP/CS debe satisfacer el "nivel de prestaciones requerido" para cada función individual de seguridad.

Los PL de las SRP/CS combinadas para realizar una función de seguridad deben alcanzar o superar el "nivel de prestaciones requerido" para esa función.

Cuando se combinan SRP/CS para realizar una función de seguridad se puede utilizar la tabla 11 de la Norma para estimar el PL resultante.

La probabilidad de un fallo peligroso de cada una de las funciones de mando relativas a la seguridad (SRCF), debida a un fallo aleatorio peligroso, debe ser igual o inferior al valor límite de fallos determinado por la especificación de los requisitos de seguridad.

El SIL total alcanzado por los SRECS (sistemas de mandos electricos relativos a la seguridad) dentro de los límites estructurales es siempre menor o igual al SILCL más bajo de todos los subsistemas que participan en la realización de la función de seguridad.

6) Validación

El diseño de una función de seguridad ha de ser validado. En la validación se revisa la aptitud de la función de seguridad para la aplicación. La validación puede realizarse por análisis o por ensayo. (por ejemplo: simulando deliberadamente defectos individuales o multiples).

7. Glosario

Abreviatura	Término ingles	Descripción
B_{10d}		Número de ciclos tras los cuales se produce un fallo peligroso en el 10% de los componentes.
λ	Failure Rate	Tasa de fallos por hora.
λ_s		Tasa de fallos que no causan peligro (seguros).
λ_d		Tasa de fallos que causan peligro.
CCF	Common Cause Failure	Un fallo por una causa común o fallos de unidades diferentes debidos a un solo suceso.
DC	Diagnostic Coverage	Cobertura del diagnóstico: Medida de la efectividad del diagnóstico, que se determina calculando la relación existente entre la tasa de fallos peligrosos detecta- dos y la tasa total de fallos peligrosos.
DC_{avg}	Average Diagnostic Coverage	Valor medio de DC.
	Designated Architecture	Arquitectura designada. Estructura de una SRP/CS con límites específicos de los valores de $MTTF_d$, DC y CCF.
HFT	Hardware Fault Tolerance	Número de fallos tras los cuales una Función de seguridad solicitada sigue desarollandose.
MTBF	Mean Time	Tiempo medio entre dos fallos consecutivos.
MTTF	Mean Time To Failure	Tiempo medio hasta un fallo.
$MTTF_d$	Mean Time To Dangerous Failure	Tiempo medio hasta un fallo peligroso.
MTTR	Mean Time To Repair	Tiempo medio hasta la reparación.
PFH	Probability Of Failure Per Hour	Probabilidad de fallo por hora.
PFH_D	Probability Of Dangerous Failure Per Hour	Probabilidad de fallo peligroso por hora.
PL	Performance Level	Nivel discreto que especifica la capacidad de componentes de seguridad de ejecutar una función de seguridad en condiciones previsibles.
PL_r	Performance Level required	PL requerido para una función de seguridad específica

Abreviatura	Término ingles	Descripción
SIL	Safety Integrity Level	Nivél de integridad de la seguridad
SILCL	Safety Integrity Claim Limit	Nivél máximo de integridad de la seguridad de un elemento (Aptitud)
SRCF	Safety Related Control Function	Función de seguridad
SRP/CS	Safety Related Parts of a Control System	Parte de un sistema de mando relacionado con la seguridad.
SRECS	Safety Related Electrical Control Systems	Sistema de mando eléctrico de una máquina cuyo fallo comporta un aumento inmediato del riesgo.
T_1	Lifetime	Tiempo de servicio asumido
T_2	Diagnostic Test Interval	Intervalo entre verificaciones (tests) de diagnóstico
T_M	Mission Time	Tiempo de servicio previsto
β	Susceptibility to Common Cause Failure	Vulnerabilidad a los fallos de cause común
C	Duty Cycle	Ciclos de actuación por hora de un elemento electromecánico
SFF	Safe Failure Fraction	Tasa de fallos no peligrosos (seguros)
Security		Término coloquial para describir un guardias o servicios de seguridad que protegen personas o valores mediante vigilancia.
Safety		Termino general utilizado para la seguridad funcional y la seguridad de maquinaria
Maschinen-sicherheit		La prevención y/o la reducción hasta un nivel tolerable por medio de medidas preventivas de los riesgos presentes en una máquina e identificados mediente análisis.
Funktionale Sicherheit		Concepto de la seguridad de la maquinaria relativo a los sistemas de mando que dependan del buen funcionamiento de partes o elementos específicos (SRP/CS) y de sistemas externos.

8. Preguntas frequentes

P: ¿ Existe una especificación SIL o PL para válvulas elctromagnéticas, relés o contactores ?

R: No. Componentes individuales no tienen PL o SIL

P: ¿ Cual es la diferencia entre Sil y SILCL ?

R: El SIL define la integridad de la seguridad de un sistema completo mientrals que el SILCL solo define la integridad de la seguridad de un subsistema

P: ¿ Que relación existe entre el PL y el SIL ?

R: El valor PFH_d puede usarse para establecer un relación entre PL y SIL (vease Paso 4º). Atención: la tabla no toma en cuenta los requisitos específicos a cada Norma referentes a la estructura autorizada, cobertura del diagnóstico y otros requisitos sistemáticos.

Probabilidad media de un fallo peligroso por hora (1/h)	Performance level (PL) ISO 13849-1	SIL (IEC 61508)
$\geq 10^{-5}$ a $< 10^{-4}$	a	ninguno
$\geq 3 \times 10^{-6}$ a $< 10^{-5}$	b	1
$\geq 10^{-6}$ a $< 3 \times 10^{-6}$	c	
$\geq 10^{-7}$ a $< 10^{-6}$	d	2
$\geq 10^{-8}$ a $< 10^{-7}$	e	3

P: ¿ Que grado de cobertura de diagnóstico se puede tener en cuenta cuanto se utilizan contactores o relés de guía forzada ?

R: Conforme a las dos Normas, se puede aceptar un DC de 99% para contactores o relés de guía forzada siempre que se realize una función de diagnóstico con reacción adecuada a los fallos o por lo menos con advertencia de peligro.

P: ¿ Es posible de obtener una tolencia a un solo fallo material (HFT = 1) con un único interruptor en un resguardo movil ?

R: No, ya que un fallo único llevaría a la perdida de la función de seguridad.

P: ¿ Se pueden obtener valores PFHd para componentes susceptibles al desgaste ?

R: No, pero el usuario puede calcular el valor MTTFd de un componente susceptible al desgaste a partir de su valor B_{10d} y del número de ciclos de activación del componente en la aplicacion específica.

P: ¿ Cual es la diferencia entre MTBF y MTTF ?

R: El MTBF define el tiempo medio entre dos fallos, mientras que el MTTF define el tiempo medio hasta el primer fallo.

P: ¿ Que significado tiene el índice „d" en la abreviación $MTTF_d$?

R: „d" significa – peligroso – por lo que $MTTF_d$ es el tiempo medio hasta la aparición de un fallo peligroso

P: ¿ Se puede aplicar la Norma EN ISO 13849-1 para integrar sistemas electrónicos programables complejos, por ejemplo : un autómata programable ?

R: Si, pero cuando el nivél de prestaciones requerido es PL „e" el soporte lógico (software) empotrado (sistema operativo) deberá cumplir los requisitos aplicables de la Norma IEC 61508-3

P: ¿ Que se debe hacer cuando el fabricante de un componente no suministra los valores de los parámetros necesarios ?

R: Las Normas EN ISO 13849-1 y EN IEC 62061 describen en sus anexos valores de referencia que pueden usarse substitutivamente. Preferentemente deben usarse los valores suministrados por el fabricante.

P: ¿ Puede aplicarse el cálculo de MTTFd según la Norma EN ISO 13849-1 para válvulas utilizadas en procesos industriales que solo son accionadas 1 o 2 veces al año ?

R: No, ya que la Norma no contempla los sistemas con baja demanda (low demand mode). En estos casos se necesitan medidas complementarias (por ejemplo „dinamización forzada" – actuación forzada de las válvulas aunque esto no sea neceasrio para el proceso) para la estimación del $MTTF_d$.

P: ¿ Puede aplicarse el cálculo de la tasa de fallos según la Norma EN ISO 62061 para válvulas utilizadas en procesos industriales que solo son accionadas 1 o 2 veces al año ?

R: No, vease la pregunta anterior

P: ¿ Es necesario certificar el programa de la aplicación (soporte lógico de la aplicación – software)? ¿ Mediante que Norma ?

R: No, ninguna de las Normas exige certificar el programa de la aplicación. En proyectos compleyos o de grandes dimensiones es recomendable puede ser necesario. Una comprobación puede ser necesaria para la verificación y la validación de funciones de seguridad. Informaciones al respecto se encuentran en EN ISO 13849-1 capítulo 4.6 y EN 62061 capítulos 6.9 y 6.10 así como en EN 61508-3.

P: ¿ Es posible usar cualquier componente que presente un valor MTTF para aplicaciones de seguridad?

R: No, además de los parámetros estadísticos como MTTF y B_{10} el componente ha de ser adecuado para la aplicación, cumplir requisítos mínimos de diseño y aplicar principios de seguridad.

Asociación alemana de la industria
electrotécnica y electrónica
Lyoner Straße 9
60528 Frankfurt am Main

Asociación profesional de automatización

Departamento de sistemas y dispositivos
industriales de conmutación y control

Comité tecnico de sistemas de seguridad
en automatización