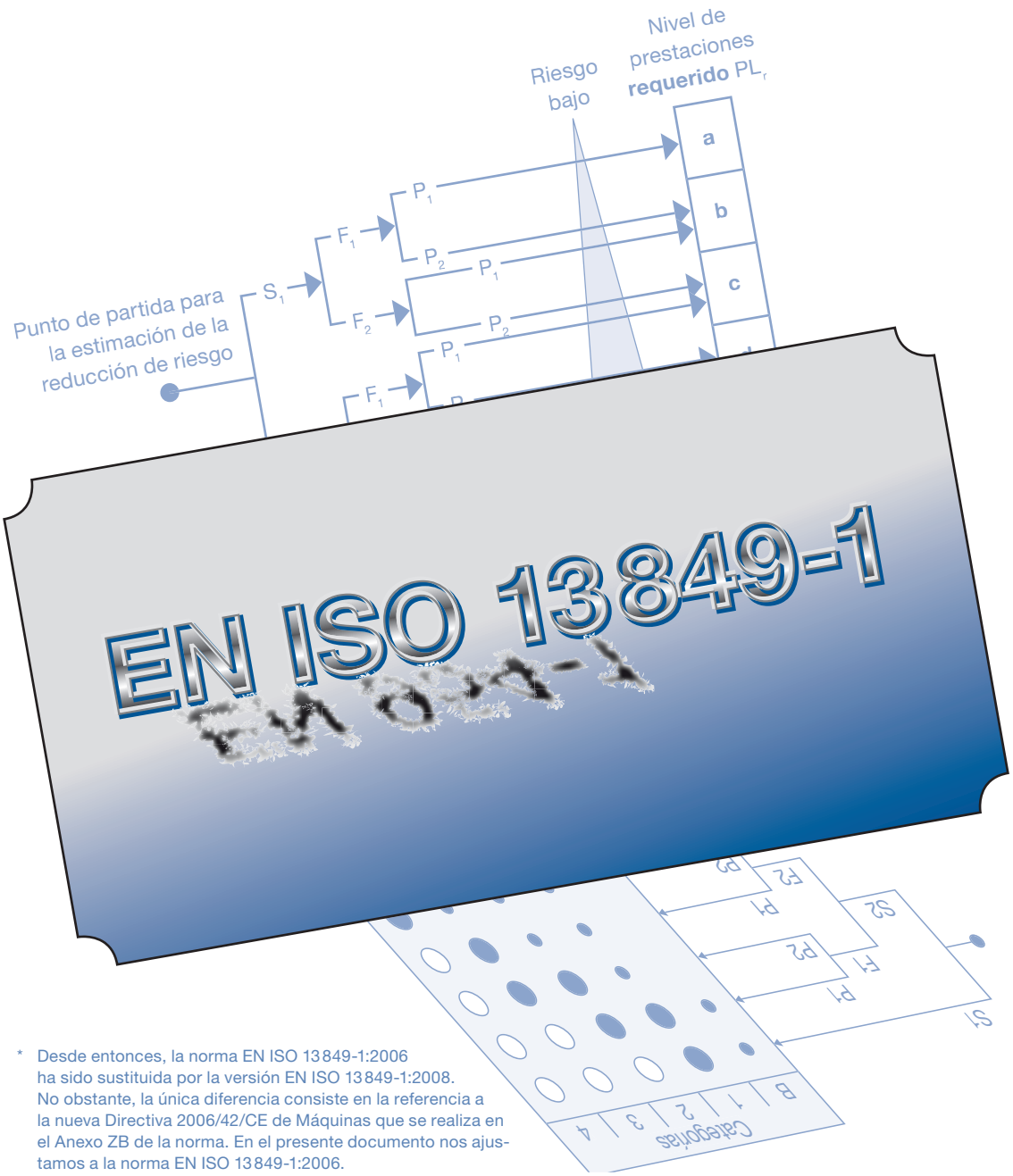
Antecedentes específicos sobre EN ISO 13 849-1:2006*

para personal técnico y de ventas de Schmersal/Elan y clientes interesados



* Desde entonces, la norma EN ISO 13849-1:2006 ha sido sustituida por la versión EN ISO 13849-1:2008. No obstante, la única diferencia consiste en la referencia a la nueva Directiva 2006/42/CE de Máquinas que se realiza en el Anexo ZB de la norma. En el presente documento nos ajustamos a la norma EN ISO 13849-1:2006.

SCHMERSAL

Explicación de las abreviaturas utilizadas frecuentemente

- CC: Categoría de control (B, 1, 2, 3, 4): actualmente la categoría ya condiciona decisivamente (de forma determinista) la calidad relativa a seguridad de las SRP/CS. Las CC B y CC 1 están relacionadas con la calidad del componente utilizado, mientras que las categorías superiores exigen componentes (canales) adicionales que sean capaces de compensar el fallo de componentes específicos.
- CCF: Fallo de causa común: Fallos provocados por una causa común, en los que diversos componentes que procesan de forma simultánea y repetida la misma pieza fallan al mismo tiempo por motivos de seguridad. Por ejemplo, un coche en el que los cuatro frenos fallen al mismo tiempo.
- DC: Cobertura del diagnóstico:
  Nivel de cobertura del diagnóstico, es decir, la capacidad de detección de defectos, que normalmente es automática.
- $MTTF_d$: Tiempo medio hasta un fallo peligroso:
  Tiempo medio hasta un fallo peligroso de un componente o dispositivo. Esta información no debe confundirse con la vida útil garantizada[1].
- PFH/PFH_d: Probabilidad de un fallo peligroso por hora[2].
- PL: Nivel de prestaciones (EN ISO 13 849-1:2006)
  Existe una escala de 5 PL (a, b, c, d, e), en la que la calidad relativa a la seguridad va en aumento de “a” hasta “e” en función del nivel creciente de riesgo que deba cubrirse.
- SIL: Nivel de integridad de la seguridad (EN IEC 62 061:2005)
  Existe una escala de 3 SIL (1, 2, 3), en la que la calidad relativa a la seguridad va en aumento de “1” a “3” en función del nivel creciente de riesgo que deba cubrirse.
- SILCL: Límite de reclamación SIL (IEC 62 61:2005)
  SIL máximo que puede utilizarse en un subsistema en función de las restricciones estructurales y de la integridad de fallos sistemática.
- SRP/CS: Parte de un sistema de mando relativa a la seguridad
  Sub-PL/sub-SIL: PL o SIL a nivel de subsistema. Un subsistema es un sistema capaz de realizar una función de seguridad de forma adecuada en relación con una tarea parcial (por ejemplo, un módulo de entrada que detecte las entradas de forma segura).
- SRB: Módulo de relé de seguridad.
- Valor B_{10d}: Número de ciclos hasta que haya sufrido fallos peligrosos un 10% de los componentes de una muestra aleatoria de al menos 7 prototipos. Este concepto hace referencia a los componentes afectados por desgaste, es decir, a los componentes mecánicos, neumáticos y electromecánicos.
- Valor T_{10d}: Valor guía de recambio preventivo (10 % del valor $MTTF_d$ en años, calculado utilizando el valor B_{10d}). Con este último valor (B_{10d}) aproximadamente el 63 % de todos los componentes han sufrido fallos peligrosos. Se asume que se dará una tasa constante de fallos peligrosos dentro del tiempo T_{10d}.

[1] El índice “d” significa fallo peligroso. Por ejemplo: un transistor falla y no se apaga (es decir, se genera una situación de peligro en cuanto a seguridad funcional de la máquina), por oposición a “no se enciende” (no es peligroso en cuanto a seguridad funcional de la máquina, aunque afecte al funcionamiento). Véase también la entrada (la entrada = el parágrafo) “Tasas de fallos” en la sección de glosario.

[2] En el caso de este valor no suele diferenciarse el tipo de fallo mediante el uso del índice “d” (peligroso), es decir, normalmente se considera que tanto un valor PFH como un valor PFH_d significan fallo peligroso.

Prólogo

Con la entrada en vigor de las normas EN ISO 13 849-1:2006 y EN IEC 62 061:2005, el diseño de las partes de un sistema de mando relativas a la seguridad adquiere toda una nueva dimensión: en el futuro, el diseño de SRP/CS implicará una combinación de enfoques deterministas[1] y probabilistas[2]. A esto hay que añadir algunos requisitos nuevos, de igual importancia, que se engloban bajo los términos “Fallos sistemáticos” y *“Software”* (véanse también las páginas 82 y siguientes, así como las entradas “Anexo G” y “Software” del glosario). El presente documento pretende proporcionarle antecedentes sobre la cuestión de la “nueva normalización de las SRP/CS”, que le serán útil en su trabajo diario.

En lo que concierne a la combinación de enfoques deterministas y probabilistas en el diseño de SRP/CS a que asistiremos en el futuro, existen algunos requisitos nuevos que nuestros clientes deberán tener en cuenta. Por otra parte, los clientes también gozarán de un mayor margen de configuración. Como fabricante de componentes de seguridad, nos vemos directamente afectados por estos cambios y debemos expresar nuestra opinión al respecto.

Aunque, por motivos prácticos, recomendamos a nuestros clientes que en el futuro basen la configuración de SRP/CS en la norma EN ISO 13 849-1:2006 (y en la filosofía de PL subyacente a la misma), en este documento también tendremos en cuenta la filosofía SIL en todos los ámbitos en que proceda considerarla como una alternativa de acuerdo con EN IEC 62 061:2005. Debido a la existencia de desacuerdos relativos a competencia entre los comités de normalización, lo cierto es que ambas normas están compitiendo por suceder a EN 954-1:1996. No obstante, en caso de decantarse por la norma EN ISO 13 849-1:2006, ello no será problemático, ya que en esencia los PL y SIL son compatibles entre sí y la “idea” subyacente es, en gran medida, la misma (véase también la entrada “Normas” del glosario). Sencillamente, nos parece que la norma EN IEC 62 061:2005 se adecua mejor que EN ISO 13 849-1:2006 a determinados casos específicos.

El siguiente folleto se ha elaborado partiendo de una primera edición editada a mediados de 2008. No obstante, la presente edición ha sido reelaborada a fondo, delimitada con mayor precisión y ampliada; como la anterior, se divide en varias secciones centradas en diferentes aspectos, algunos de los cuales son específicos de Schmersal/Elan, mientras que otros están relacionados con principios básicos y antecedentes. Véase en este sentido el Índice, páginas 4 y siguientes. Además, en la Sección 7 (a partir de la página 93) también encontrará un breve glosario con información adicional relativa a la nueva normalización de las SRP/CS. Si desea información sobre la filosofía subyacente a la norma EN ISO 13 849-1:2006, empiece por la Sección 6, páginas 81 y siguientes.

En este punto, me gustaría agradecer a todos aquellos colegas que, con su participación activa, propuestas y críticas, han contribuido a la creación de este folleto.

Wuppertal/Wettenberg, abril de 2009

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG, Wuppertal
Director de Schmersal tec.nicum

(1) Determinista (D): ambos términos se utilizan en filosofía de la ciencia; D significa la determinación y predeterminación inequívocas de hechos a partir de causas (definibles y reproducibles), como por ejemplo la tolerancia a los fallos a partir de la redundancia (las tolerancias y la coincidencia son irrelevantes).

(2) Probabilista: Clasificación de los hechos en función de su nivel de certidumbre = cálculo de probabilidad/teoría de la probabilidad (área de las matemáticas).

Índice

Parte 1: Antecedentes ..... Página 9

Parte 2: Información (base para realizar cálculos según EN ISO 13849-1:2006 y EN IEC 62061:2005) ..... Página 15

Dispositivos únicos sencillos del programa Schmersal/Elan ..... Página 21
– Dispositivos únicos sencillos del programa Schmersal/Elan ..... Página 22
– Información específica de dispositivo ..... Página 25
– Excurso: Cuestiones relativas a la arquitectura o la categoría de control ..... Página 29
– Excurso: Detección de fallos en el caso de dispositivos únicos sencillos con función de seguridad ..... Página 32

Dispositivos con funciones de seguridad más complejas ..... Página 35
– Dispositivos con funciones de seguridad más complejas ..... Página 36
– Dispositivos con funciones de seguridad más complejas del programa Schmersal/Elan ..... Página 38
– Combinaciones de dispositivos ..... Página 41
– Dispositivos de sistema bus de seguridad ASi-SaW con interfaz ASi-SaW ..... Página 42

Parte 3: Combinación de varios sub-PL en un PL global ..... Página 45

Cómo calcular el PL de un subsistema (un sub-PL) ..... Página 53
– Introducción/prefacio ..... Página 54
– Ejemplos ..... Página 56
– Cómo calcular un sub-PL con dispositivos del programa Schmersal/Elan ..... Página 63

Parte 4: Excurso ..... Página 67

Detección de fallos ..... Página 68

Influencia de la definición de la función de seguridad sobre el cálculo del PL – ejemplos ..... Página 70

Parte 5: Ejemplos de conexión del informe del BGIA ..... Página 73

1) Ejemplo de conexión 8.2.34 del BGIA: control de una puerta ó guarda con procesamiento de señal mediante módulo SRB o PLC de seguridad (el caso clásico) ..... Página 74

2) Ejemplo de conexión 8.2.29 del BGIA: conexiones en serie o en cascada ..... Página 75

3) Ejemplo de conexión 8.2.28 del BGIA: conexiones en serie o en cascada ..... Página 76

4) Ejemplo de conexión 8.2.18 del BGIA: bloqueo de una puerta ó guarda con procesamiento de señal mediante módulo SRB o PLC de seguridad (canal 1) y PLC estándar (canal 2) ..... Página 77

5) Ejemplo de conexión 8.2.19 del BGIA: cierre de la puerta de una guarda ..... Página 78

Parte 6: Presentación general de las características y aplicación de norma EN ISO 13849-1:2006 ..... Página 81

Objetivo de la normalización de SRP/CS ..... Página 82

Nivel de prestaciones (1) ..... Página 85

Nivel de prestaciones (2) ..... Página 87

Nivel de prestaciones (3) ..... Página 92

Parte 7: Glosario/ Información adicional relativa a algunos términos y palabras clave ..... Página 93

– Adición de probabilidades de fallo ..... Página 94
– Análisis del gráfico del riesgo conforme a EN ISO 13849-1:2006 ..... Página 94
– Análisis del gráfico del riesgo conforme a EN IEC 62061:2006 ..... Página 94
– Análisis del valor T_{10d} ..... Página 94
– Anexo E ..... Página 95
– Anexo G (conforme a EN ISO 13849-1:2006) ..... Página 96
– Anexo K (conforme a EN ISO 13849-1:2006) ..... Página 96
– Arquitecturas ..... Página 98
– Arquitecturas designadas ..... Página 99

– BGIA ..... Página 99
– Bibliografía ..... Página 99
– Buenas prácticas de ingeniería (BPI) ..... Página 100

– Cableado ..... Página 100
– Cálculos (cálculos de PL) ..... Página 100
– Categorías de control ..... Página 101
– Categorías de control/categoría de control 2 ..... Página 102
– CCF (fallo de causa común), medidas contra CCF, gestión de CCF ..... Página 103
– Circuito conmutado de reinicio ..... Página 104
– Circuito de retroalimentación ..... Página 104
– Cobertura del diagnóstico DC ..... Página 105
– Compatibilidad SIL ↔ PL/PL ↔ SIL ..... Página 105
– Comprobación/intervalo de comprobación ..... Página 105
– Conexiones en serie ..... Página 106
– Conexiones en serie de dispositivos electromagnéticos ..... Página 106
– Curva de la bañera ..... Página 106

– Detección de defectos DC ..... Página 107
– Detección de defectos (externa) ..... Página 107
– Directiva de Máquinas (DM) ..... Página 108
– Disco del BGIA ..... Página 108
– Distribución exponencial ..... Página 109
– Duración de misión (vida útil) ..... Página 109

– Entrada en vigor ..... Página 110
– Equipos de ensayo ..... Página 110
– Estimación de PL y SIL ..... Página 110
– Exclusión de defectos ..... Página 110
– Exclusión de defectos: conexión/cableado ..... Página 111
– Exclusión de defectos en caso de dispositivos activados de forma manual ..... Página 111
– Exclusión de defectos en caso de dispositivos de enclavamiento ..... Página 111

– Fallos ..... Página 112
– Fallos (fallos aleatorios) ..... Página 112
– Fallos (fallos sistemáticos) ..... Página 112
– Fiabilidad del hardware, $MTTF_d$ ..... Página 113
– Fórmula de simetrización ..... Página 113
– Función de seguridad ..... Página 113

– Gestión de CCF/medidas contra CCF ..... Página 113
– Gráfico de barras ..... Página 114
– Gráfico de resultado PL ..... Página 114
– Gráfico de resultados PL ..... Página 114
– Gráfico del riesgo, evaluación del riesgo ..... Página 114

– Informe 2/08 del BGIA ..... Página 114
– Interruptor de control adicional ..... Página 115

– Límite de reclamación SIL (SILCL) ..... Página 115
– Límite máximo ..... Página 115

– Método del recuento de partes ..... Página 115
– Modificación 1 de EN 1088:1996 ..... Página 115
– Modo en baja solicitación ..... Página 116
– $MTTF_d$, fiabilidad del hardware ..... Página 116

– Nivel de cable ..... Página 116
– Nivel de prestaciones ..... Página 116
– Normas C (tipo C) ..... Página 116
– Normas ..... Página 117
  – Normas (de tipo) A, B y C ..... Página 117
  – EN 954-1:1996 ..... Página 117
  – EN 954-2 ..... Página 117
  – EN ISO 13849-1:2006 ..... Página 117
  – EN ISO 13849-2:2003 ..... Página 118

– EN IEC 62 061:2005 ..... Página 118
– EN IEC 61 508:2001 ..... Página 118
– EN ISO 13 849-1:2006 → EN IEC 62 061:2006 (comparación) ..... Página 119
– EN ISO 13 849-1/EN IEC 62 061:2005 (comparación con EN 954-1:1996) ..... Página 120

– Objetivo de la normalización de SRP/CS ..... Página 121

– Periodo de transición ..... Página 121
– PFD (probabilidad de fallo en solicitación) ..... Página 121
– PL – Nivel de prestaciones ..... Página 122
– PL_r = Nivel de prestaciones requerido ..... Página 122
– Prestaciones probadas ..... Página 122

– Reinicialización ..... Página 122
– Riesgo, análisis del riesgo, valoración del riesgo ..... Página 122

– SIL (Nivel de integridad de la seguridad) ..... Página 123
– SISTEMA ..... Página 124
– Software ..... Página 125

– Tasas de fallos ..... Página 126
– Tecnología de fiabilidad (ingeniería de fiabilidad) ..... Página 128

– Uso probado ..... Página 129

– Valores B_{10d} ..... Página 129

Parte 8: Fragmento de nuestro folleto "Nuevo enfoque de la seguridad de máquinas: EN ISO 13 849-1:2006 – partes de un sistema de mando relativas a la seguridad" ..... Página 131

Ejemplo de la norma incluido en el Anexo I de EN ISO 13 849-1:2006

Datos editoriales ..... Página 137

La información contenida en este folleto ha sido elaborada a nuestro mejor saber y entender. No obstante, excepto cuando existan disposiciones legales en sentido contrario y de obligado cumplimiento, asumimos que no existe ningún tipo de responsabilidad por los eventuales errores y confusiones. El usuario de esta información no queda exento de su responsabilidad en el sentido de comprobar la información y recomendaciones que presentamos para su propio uso. Esperamos comprendan este mensaje y le den la atención debida.

Antecedentes específicos

Antecedentes (1)

(Para más información: véase sección 6, página 81 y siguientes)

Dicho de forma sencilla, de acuerdo con los requisitos previstos de cara al futuro por la nueva norma EN ISO 13849-1:2006[1] relativa al diseño de SRP/CS, un nivel de prestaciones consiste en la consideración de varios factores determinantes. Actualmente este concepto está aceptado a nivel internacional como una forma de determinar la seguridad y fiabilidad de los sistemas de mando y medición, es decir, los factores pertinentes para la integridad de la seguridad de un sistema. En oposición a las prácticas habituales en ingeniería mecánica, un nivel de prestaciones (PL, *performance level*) constituye un enfoque multidimensional. No obstante, en vez de técnicas de modelado complejo, la norma EN ISO 13849-1:2006 hace uso de un método simplificado en el que se tienen en cuenta 4 variables auxiliares.

Ahora bien, debemos tener claro que, de forma adicional, los niveles de prestaciones, con independencia del nivel de que se trate, están sujetos a requisitos fundamentales (requisitos básicos), es decir, medidas destinadas a prevenir y controlar defectos y fallos sistemáticos, mientras que la clasificación PL (PL “a” hasta “e”) está relacionada esencialmente con la prevención y el control de defectos y fallos aleatorios (véase también la entrada “Fallos” del glosario).

- El punto de partida para determinar un PL consiste en definir las diversas funciones de
- seguridad de una máquina o los sistemas de mando de la máquina.

- A continuación, debe establecerse el nivel de prestaciones requerido, PL_r, en relación con la función de seguridad en cuestión. El nivel de prestaciones (“a” hasta “e”) debe seleccionarse a partir de la norma correspondiente (norma de producto) o utilizando una evaluación del gráfico del riesgo.

- Así pues, el nivel de prestaciones refleja la cantidad de medidas necesaria para minimizar el riesgo.

a) Debe reducirse un nivel muy reducido de riesgo
b) Debe reducirse un nivel reducido de riesgo
c) Debe reducirse un nivel mayor de riesgo
d) Debe reducirse un nivel elevado de riesgo
e) Debe reducirse un nivel importante de riesgo

- La eficacia de las medidas (requeridas) se expresa como un valor PFH_d (valor de la probabilidad media residual máxima tolerada de que se dé un fallo peligroso). El valor PFH_d también constituye el punto de referencia para los niveles de integridad de la seguridad (SIL) internacionales, reconocidos en las normas EN IEC 61508:2000 o EN IEC 62061:2005.

- De acuerdo con EN ISO 13849-1:2006, actualmente la estimación (cálculo) del nivel de prestaciones se realiza a partir de 4 parámetros específicos (variables auxiliares):

[1] Con efectos a partir de 2010 como máximo. La norma EN 954-1:1996 (o ISO 13849-1:1999) dejará de ser aplicable en diciembre de 2009.

1. La arquitectura, que en esencia equivale a la consideración de las categorías de control y con la que ya estamos familiarizados por la norma EN 954-1:1996 (ISO 13849-1:1999), ha sido adoptada en EN ISO 13849-1:2006;

2. La evaluación de la fiabilidad de los equipos, expresada como el tiempo medio hasta un fallo peligroso ($MTTF_d$) en años (una hipótesis estadística del periodo de tiempo en que el equipo funcionará sin fallos desde el punto de vista de la seguridad, en ausencia de fallos aleatorios);

3. La evaluación (probabilidad) de la eficacia de las medidas de detección de defectos en la SRP/CS o sección de la SRP/CS, expresada como cobertura del diagnóstico, DC, de forma porcentual;

4. La evaluación de las medidas contra los denominados fallos de causa común o de modo común (CCF = fallos de causa común = fallos que podrían interrumpir simultáneamente la capacidad multicanal de un sistema de seguridad).

- A continuación, puede establecerse el nivel de prestaciones (PL) alcanzado utilizando una gráfica de barras o el Anexo K de la norma EN ISO 13849-1:2006, y comparándolo y validándolo con el PL_r requerido en relación con la función de seguridad en cuestión.

Conclusión esquemática

Nivel de prestaciones PL_r
Referencia: Consideración de la norma C o del gráfico del riesgo

→

Probabilidad de fallos peligrosos por hora (PFH_d)

→

PL			Nivel de integridad de la seguridad (SIL)
a	$\geq 10^{-5} \ldots < 10^{-4}$	=	Sin equivalente
b	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	≙	SIL 1
c	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$		
d	$\geq 10^{-7} \ldots < 10^{-6}$	≙	SIL 2
e	$\geq 10^{-8} \ldots < 10^{-7}$	≙	SIL 3

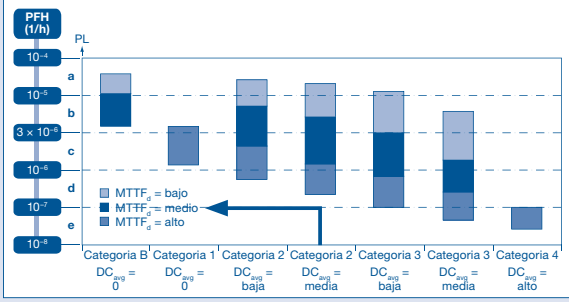
Arquitectura designada (categoría de control):
Consideración anterior de EN 954-1:1996

Fiabilidad de equipos
(Tiempo medio hasta un fallo peligroso): Fuente: Información de fabricante o consulta de las normas u otras fuentes, como por ejemplo manuales MIL

Cobertura del diagnóstico DC (prestaciones en la detección de fallos peligrosos a tiempo): Anexo E de EN ISO 13849-1:2006 o información del fabricante

Fallo de causa común – Gestión de CCF:
> 65 puntos (siempre puede asumirse en el caso de los dispositivos de seguridad) (remítase también a la entrada "CCF" del glosario)

Gráfico de barras



Representación numérica con arreglo a EN ISO 13849-1:2006, Anexo K

Tabla K.1 – Descripción numérica de la figura 5 de EN ISO 13849-1:2006 [3] – Anexo K (informativo)

$MTTF_d$ para cada canal años	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = nula		DC_{avg} = nula		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = alta	
3	$3,80 \times 10^{-5}$	a			$2,59 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	a	$1,28 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b		
3,3	$3,48 \times 10^{-5}$	a			$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	a	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b		
3,6	$3,17 \times 10^{-5}$	a			$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b		
3,9	$2,93 \times 10^{-5}$	a			$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b		
4,3	$2,65 \times 10^{-5}$	a			$1,78 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b		
4,7	$2,43 \times 10^{-5}$	a			$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b		
5,1	$2,24 \times 10^{-5}$	a			$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b		
5,6	$2,04 \times 10^{-5}$	a			$1,33 \times 10^{-5}$	a	$9,67 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c		
6,2	$1,84 \times 10^{-5}$	a			$1,19 \times 10^{-5}$	a	$8,60 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c		
6,8	$1,68 \times 10^{-5}$	a			$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c		
7,5	$1,52 \times 10^{-5}$	a			$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c		
8,2	$1,39 \times 10^{-5}$	a			$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c		
[illegible]	[illegible]	[illegible]			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		

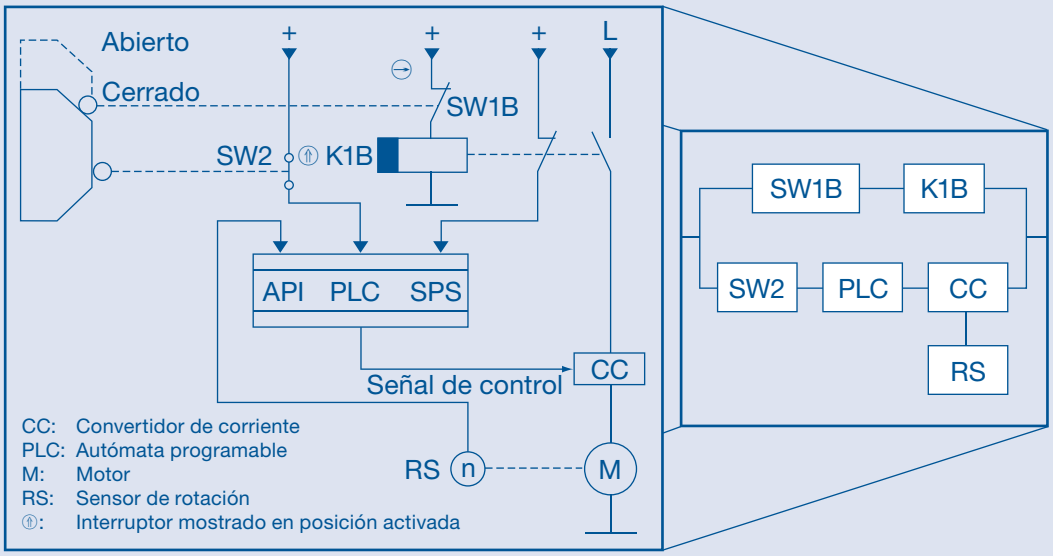
- En esencia, este folleto se centra en la información relativa al cálculo (estimación) del nivel de prestaciones tal como deberá utilizarse en el futuro en virtud de la norma EN ISO 13849-1:2006, y en este sentido hace referencia principalmente al denominado método sub-PL.

  Nota: Debe considerarse que las palabras “cálculo” y “estimación”, utilizadas con frecuencia en este documento en relación con los niveles de prestaciones (PL), poseen el mismo significado. La norma EN ISO 13849-1:2006 hace referencia de forma frecuente a estimación. Estimación no debe confundirse con “adivinar” (por el contrario, se trata de un término matemático relativo a variables auxiliares en combinación con desigualdades); ahora bien, en sentido contrario, tampoco es necesaria una precisión de cálculo total. Lo más importante es poseer la dirección o magnitud adecuada.

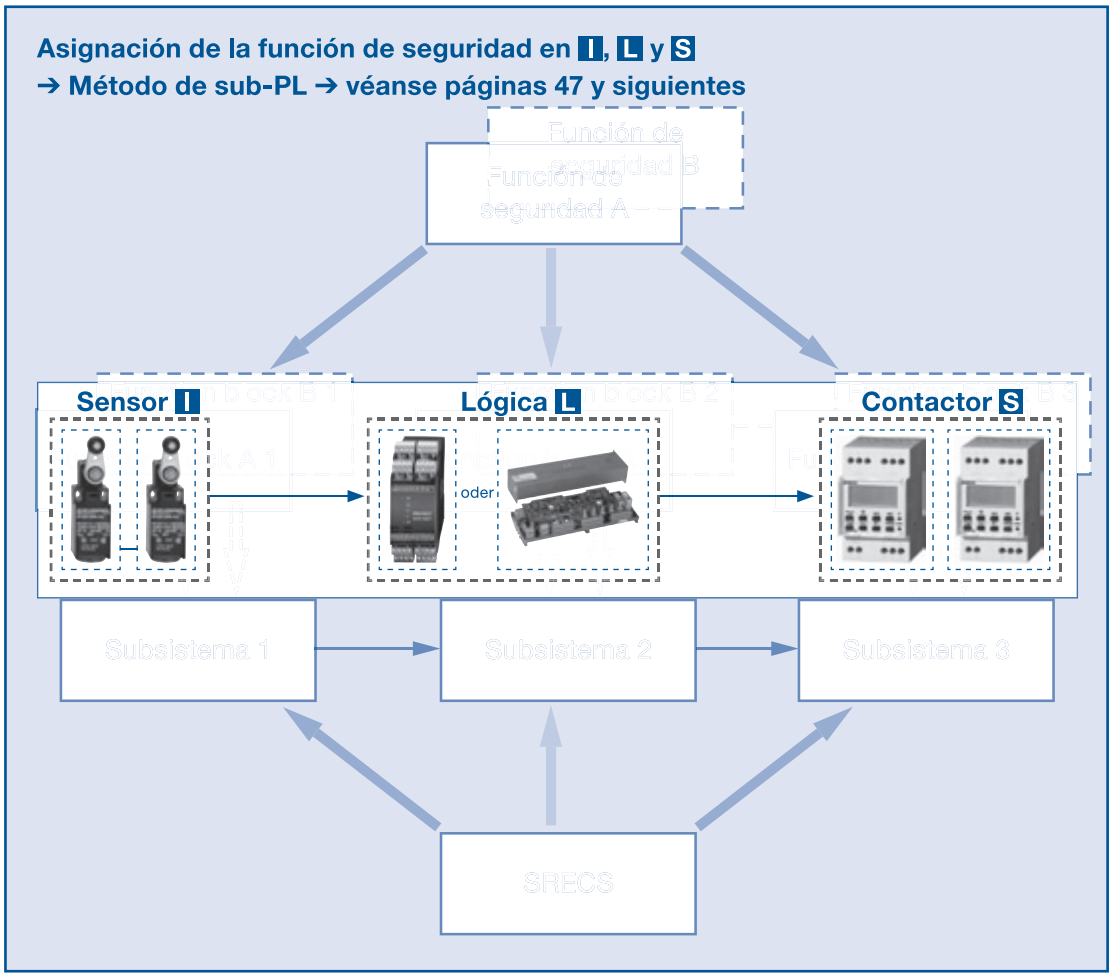
- En principio existen dos posibilidades para calcular el nivel de prestaciones (PL) de una función de seguridad:

  La primera posibilidad consiste en el denominado método de bloques, de acuerdo con el Anexo B de EN ISO 13849-1:2006, y constituye un análisis de toda la SRP/CS. A título ilustrativo, en el Anexo B de EN ISO 13849-1:2006 (véase apéndice tras el glosario, páginas 131 y siguientes) puede encontrarse un análisis global utilizando el método de bloques. Se recomienda utilizar este método sobre todo en el caso de SRP/CS complejas interrelacionadas y en casos especiales (como alternativa al método de subsistemas).

Análisis total de una función de seguridad ➔ Método de bloques ➔ Ejemplo estándar



La segunda posibilidad es el método de subsistemas, diseñado como una simplificación (también denominado en lo sucesivo “análisis de sub-PL” o “método de sub-PL”), que se realiza de acuerdo con la denominada tabla de combinación (Tabla 11 de EN ISO 13849-1:2006, véanse páginas 45 y siguientes). Véase también Anexo H de la norma. La ventaja del método de subsistemas es, por una parte, que los dispositivos y sistemas que conforman un subsistema ya están disponibles en el mercado y han sido evaluados por el fabricante en lo que concierne al sub-PL (o sub-SIL) y la PFH_d correspondiente, de forma que en estos casos no es necesario realizar ningún cálculo; y, por otra parte, si debemos estimar un sub-PL por nosotros mismos, la estimación (cálculo) es considerablemente más sencilla (menos compleja).



- Los sub-PL o sub-SIL* constituyen la base para la modularización de una SRP/CS total en sub-SRP/CS (= partes o subsistemas), que derivarán de bloques funcionales (normalmente bloques funcionales relativos a los niveles de entrada, procesamiento de señal y salida = **I** de entrada + **L** de lógica + **S** de salida). Véase la figura anterior. Como ya se ha indicado anteriormente, esta diferenciación permite simplificar el cálculo posterior de los PL globales (o SIL globales) utilizando la tabla de combinación (véanse páginas 45 y siguientes).

- Partiendo de la gama de productos de Schmersal/Elan (así como de las gamas de productos de nuestros competidores), y en lo que concierne al enfoque de sub-PL o sub-SIL, cabe diferenciar dos tipos de dispositivos, los “dispositivos únicos sencillos con función de seguridad” y los “dispositivos con funciones de seguridad más complejas”.

- Esta división en dos grupos no implica ninguna valoración, es decir, ambos tipos de dispositivos son capaces de realizar su función de seguridad respectiva en la SRP/CS con el mismo nivel de calidad; tan solo varía su uso (véanse páginas 15 y siguientes).

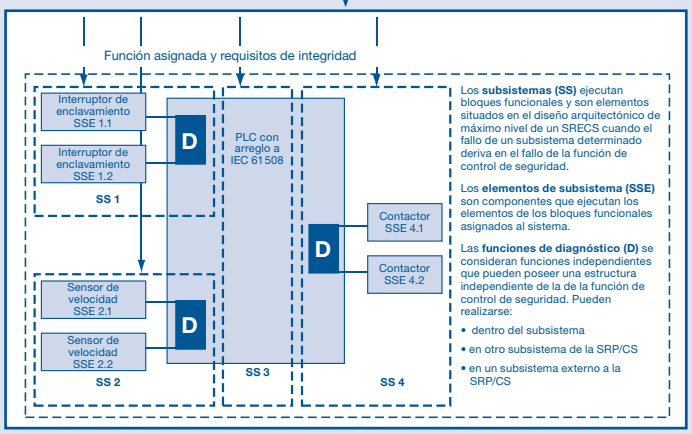
(1) En adelante se utilizarán las expresiones sub-PL y sub-SIL en el mismo sentido, ya que la norma EN IEC 62061:2005 describe el método de análisis de subsistemas como el preferente.

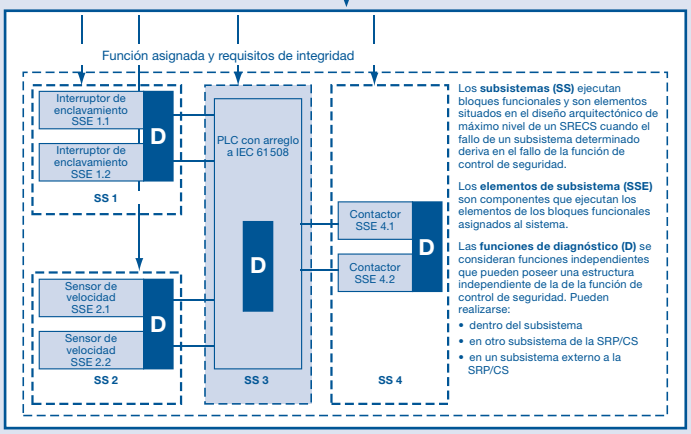
- La diferencia fundamental entre ambos grupos es la arquitectura del dispositivo, que es diferente. Para empezar, existen arquitecturas (véase figura, a la izquierda) con “sistema de diagnóstico externo” (automático) y arquitecturas (véase figura, a la derecha) con “sistema de autodiagnóstico” (automático) (véanse también en relación con este punto las páginas 15 y siguientes). En este contexto, “automático” significa, en ambos casos, “realizado esencialmente por el sistema” o “sin intervención de la voluntad humana”.

Dispositivos únicos sencillos con función de seguridad

Dispositivos con funciones de seguridad más complejas

Diferencia: Diagnóstico externo frente a autodiagnóstico





Los dispositivos únicos sencillos con función de seguridad (también denominados elementos de seguridad parciales o SSE) se caracterizan de forma específica por el hecho de no poseer una capacidad integrada de detección de defectos, sino que se requieren otras partes de la SRP/CS para realizar esta función (diagnóstico externo). Véase también la disposición independiente de **D** *en el anterior esquema. Juntos (uno o varios SSE +* **D***) constituyen un subsistema adecuado para un cálculo de sub-PL (superior). En el caso de los PL inferiores basta con realizar una evaluación de la fiabilidad de los equipos de los dispositivos únicos sencillos (SSE).*

Los dispositivos con función de seguridad más compleja ya se suministran con una arquitectura que posee todas las características necesarias para un sub-PL (superior), y en concreto una capacidad propia de detección de defectos (autodiagnóstico). En este sentido, véase también la asignación directa de **D** *en el anterior esquema, es decir, SSE y* **D** *ya conforman una unidad (un subsistema, normalmente con un sub-PL superior).*

Información (de base para realizar cálculos en el sentido de EN ISO 13849-1:2006 y EN IEC 62061:2005)

Información (de base para realizar cálculos en el sentido de EN ISO 13849-1:2006 y EN IEC 62061:2005)

- Todos los fabricantes deberán ampliar gradualmente su información técnica, si no lo han hecho ya, para que incluya información en el sentido de EN ISO 13849-1:2006 y EN IEC 62061:2005, o bien ser capaces de comunicar esta información previa solicitud. Además de la información de fabricante existen otras fuentes disponibles (empezando por EN ISO 13 849-1:2006 [Anexo C] y la propia norma EN IEC 62061:2005, así como la norma SN 29000 y los manuales MIL [relativamente desfasados], etc.). No obstante, en ambas normas se indica con total claridad que debe utilizarse información del fabricante siempre que sea posible.

- La información variará dependiendo del tipo de dispositivo. En primer lugar, estos pueden dividirse en función de sus componentes (como por ejemplo componentes electrónicos), o dispositivos únicos sencillos (como por ejemplo dispositivos de conmutación de seguridad sencillos) o dispositivos con funciones de seguridad más complejas, entre los que se incluyen las combinaciones de dispositivos.

- En adelante no volverá a hacerse mención de los componentes. Por otra parte, la diferencia básica reside en el hecho de que los dispositivos con funciones de seguridad más complejas y las combinaciones de dispositivos ya se suministran con una arquitectura específica integrada orientada a la seguridad (en otras palabras, con CC 2 o superior) y cuentan con su propia capacidad de detección de defectos (en este sentido, podría decirse que son “inteligentes”). También podría hablarse de capacidad de autodiagnóstico. Por tanto, los dispositivos con funciones de seguridad más complejas poseen un sub-PL o sub-SIL superior integrado.

- Por otra parte, los dispositivos únicos sencillos, como por ejemplo los interruptores de seguridad sencillos, tienden a poseer una arquitectura sencilla (como máximo de 2 canales) y, más concretamente, no poseen capacidad de autodiagnóstico. En estos dispositivos los fallos se detectan a través de otras partes SRP/CS, situadas corriente arriba o corriente abajo con respecto a los dispositivos únicos sencillos, como por ejemplo mediante un módulo SRB con interruptores AZ16. Así pues, en este caso también podría hablarse de diagnóstico externo. En la normativa los dispositivos únicos sencillos también se denominan “elementos parciales o de subsistema”.

- En general, los dispositivos únicos sencillos (sin diagnóstico externo adicional) poseen un sub-PL o sub-SIL bajo (dependiendo de la probabilidad de fallo, PL “c” o SIL 1 como máximo); no obstante, es posible optimizarlos hasta un sub-PL “e” o un sub-SIL 3 introduciendo las adiciones pertinentes (véase: “capacidad de canal múltiple”) y complementándolos con medidas adicionales de detección de defectos (véase: “diagnóstico externo”). En este caso, puede ser necesaria la adición de una estructura/diseño de 2 canales[1].

[1] Explicado de forma sencilla, esto significa que (dejando a un lado las excepciones) los interruptores sencillos, incluso cuando sean de dos canales desde el punto de vista eléctrico, no pueden poseer una categoría superior a 1 y un sub-PL superior a “c” o un sub-SIL superior a 1. Tan solo es posible asignar categorías, PL o SIL superiores a este tipo de interruptores cuando existe una inteligencia corriente abajo que también detecte fallos, es decir, cuando se combinen con una capacidad de 2 canales o similar. En relación con este punto véase también las páginas 23 y siguientes y 29 y siguientes.

- Algunos ejemplos típicos de dispositivos únicos sencillos serían válvulas y cilindros en tecnología de fluidos (hidráulica, neumática), relés de contactor y auxiliares, dispositivos de control de parada de emergencia, interruptores de posición, dispositivos de enclavamiento, incluidos interruptores de seguridad magnéticos, Interruptores de validación, etc.
  En el futuro, en general se especificará un valor de fiabilidad, expresado como un B_{10d} (capacidad de conmutación máxima) en relación con los dispositivos de este tipo, ya que se ven afectados por el desgaste habitual producido por el uso, así como, cuando proceda, un valor $MTTF_d$ (expresado en años) en relación con los dispositivos nuevos.

Conclusión esquemática:
División del programa Schmersal/Elan en dos grupos

Dispositivos únicos sencillos con función de seguridad	**Dispositivos con funciones de seguridad más complejas**
• Como norma: 1 canal (en ocasiones 2 canales) • Independiente: PL “c” o SIL 1 como máximo • Sin diagnóstico • Para un PL superior: + arquitectura superior + diagnóstico externo necesario	• Como norma: 2 canales • Capacidad de autodiagnóstico • Optimizado para sub-PL superiores

- Como ya se ha indicado, también puede obtenerse un (sub-)PL “d” o (sub-)PL “e” en los denominados dispositivos únicos sencillos cuando también se incorporen medidas de detección de defectos recibidas de otras partes de la SRP/CS; en caso de no contar con las características integradas necesarias para cumplir los requisitos de una arquitectura de 2 canales, podría requerirse también la redundancia de los dispositivos. En estos análisis, en esencia esto no implica más que la combinación de los dispositivos que ya conocemos por EN 954-1:1996 como por ejemplo, módulos de relé de seguridad, cuyos circuitos de entrada y retroalimentación actúan como comparaciones a prueba de errores que detectan cualquier defecto o fallo en los niveles I u O.

Interruptores de seguridad con activación independiente

Interruptores de imán de seguridad

Dispositivos de bloqueo por solenoide de seguridad en metal y plástico

Sistemas con bloqueo de llave

Interruptores de posición con función de seguridad

Equipos de parada de emergencia

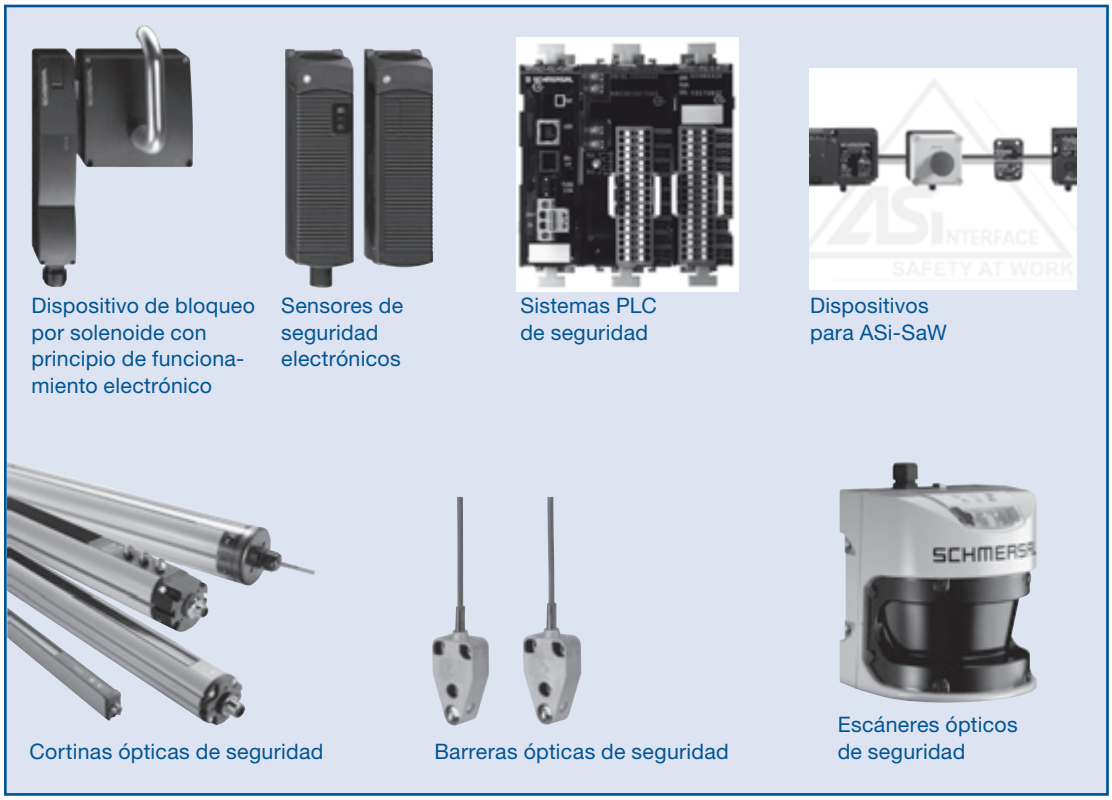
Interruptores de validación

Interruptor de seguridad de tracción por cable

Interruptores de pedal de seguridad

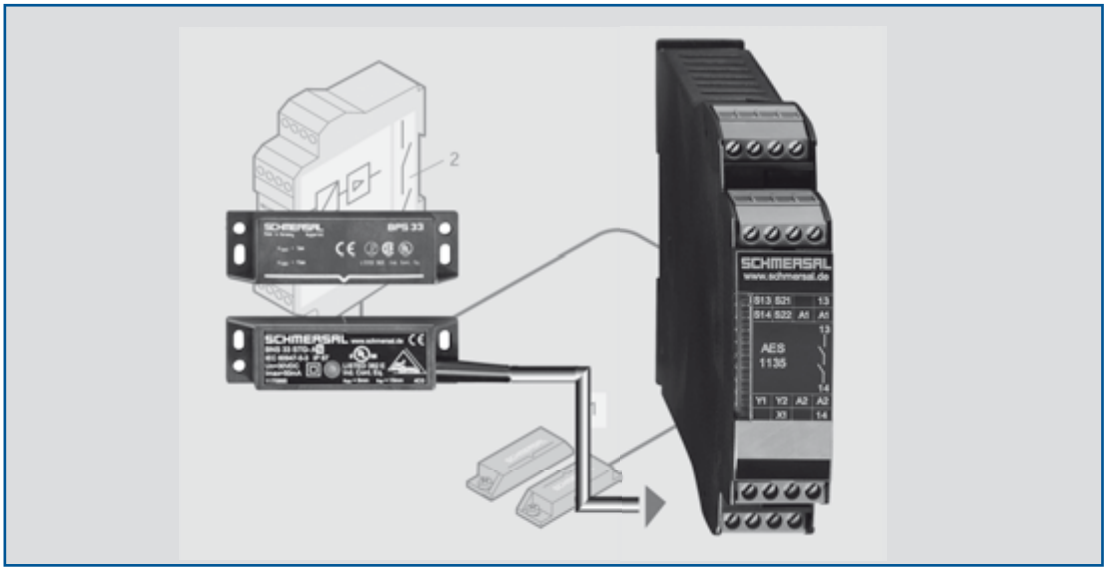
Aclaración: En otras normas y otros contextos del ámbito de la ingeniería de fiabilidad se utilizan otras expresiones para la probabilidad de fallos, como por ejemplo valores λ o FIT. Estas pueden convertirse con facilidad en valores $MTTF_d$ utilizando el valor inverso. Los denominados valores MTBF (= tiempo medio entre fallos) pueden equipararse a valores MTTF a efectos de la norma EN ISO 13849-1:2006, aunque no debe pasarse por alto el índice “d”, que significa “peligroso” o “fallo peligroso”. De acuerdo con EN ISO 13849-1:2006, en general pueden identificarse los valores sin “d” de acuerdo con un ratio 50:50 (en el que tan solo es pertinente uno de cada dos fallos), es decir, que un valor $MTTF_d$ es dos veces más elevado que el valor MTTF (para todos los fallos posibles). Esta misma correlación se da entre los valores B_{10d} y B_{10}.

- Por otra parte, el fabricante construye los dispositivos con funciones más complejas (subsistemas y superiores) de forma que puedan evaluarse independientemente desde el punto de vista de la seguridad, sin intervención de ninguna otra parte de la SRP/CS. En este caso, la información del fabricante es un sub-PL o un sub-SIL (con el valor PFH_d correspondiente, respectivamente). Algunos ejemplos típicos de dispositivos con funciones de seguridad más complejas son módulos de relé de seguridad, sensores de seguridad basados en microprocesador, PLC de seguridad, sistemas bus de seguridad y similares.



Aclaración: en el caso de los valores PFH no es especialmente común diferenciar mediante el uso del índice “d”, es decir, en general se utilizan los valores PFH y PFH_d de forma indistinta.

- Las combinaciones de dispositivos equivalen a dispositivos con funciones de seguridad más complejas, como por ejemplo la combinación de interruptores de seguridad magnéticos BNS con módulos de evaluación AES especiales, de esta forma, combinándolos, constituyen una función de seguridad completa e independiente a la que puede asignarse un sub-PL o un sub-SIL superior.



Ejemplo de combinación de dispositivos BNS/AES

- ADVERTENCIA: problema: en caso de mezclarse dispositivos únicos sencillos y dispositivos con funciones de seguridad más complejas en una SRP/CS, como por ejemplo un interruptor de seguridad en el nivel de entrada y un SPS de seguridad en el nivel de la lógica, el resultado podría ser que haya valores $MTTF_d$ (o valores B_{10d} de los que pueda derivarse el valor $MTTF_d$) correspondientes a un subsistema (en este ejemplo, el subsistema del "nivel de entrada", véase página 22 f.), y PFH_d en relación con el otro subsistema (en este ejemplo el subsistema del "nivel de la lógica"). Es posible que deba convertirse uno de los dos valores (cuando estos deban sumarse). En este caso puede ser de ayuda el Anexo K de EN ISO 13849-1:2006 (por desgracia, solo hasta una $MTTF_d$ de 100 años; véase la entrada "Anexo K" del glosario), o bien puede realizarse una estimación/extrapolación aproximada de las cifras del Anexo K o el cálculo inverso simplificado de un valor PFH_d para convertirlo en un valor $MTTF_d$ ($1/PFH_d$: 8,760) (véase también página 50 y las entradas pertinentes del glosario).

- Tras este problema se esconde el hecho de que, en realidad, además de requisitos deterministas, lo que subyace al PL obtenido tras considerar los cuatro parámetros mencionados desde una perspectiva de probabilidad matemática es un valor PFH_d. Dicho de otro modo, el valor PFH_d es el valor "de mayor categoría" (con el que pueden describirse los dispositivos con funciones de seguridad más complejas), mientras que el valor $MTTF_d$ no es más que un aspecto parcial en el marco del análisis diferenciado de dispositivos únicos sencillos, a los que posteriormente se añaden la arquitectura (categoría de control), la detección de defectos (DC) y la gestión de CCF, y que entonces, en su conjunto, pueden describirse mediante un valor PFH_d. El fundamento matemático de este hecho ha sido establecido por el BGIA[1].

[1] BGIA: Instituto Alemán de Salud y Seguridad Ocupacionales del sector de los seguros legales de accidente de Alemania (véase glosario).

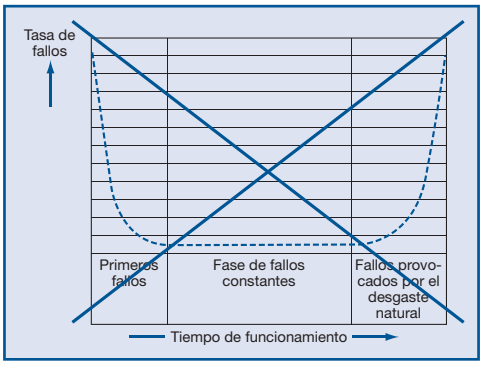
Dispositivos únicos sencillos del programa Schmersal/Elan

Cálculo del valor B_{10d}

- En general, en el futuro deberá especificarse la información sobre fiabilidad relativa a la seguridad en forma de valor B10d en relación con los dispositivos de este tipo. La arquitectura (categoría de control), el sistema de detección de defectos (DC) y el sistema de gestión de CCF (véase la entrada “CCF” del glosario) llevan asociada una actividad de planificación de proyectos para el cliente (y sus asesores).

- El valor B_{10d} es una especie de “valor bruto” para calcular un valor $MTTF_d$ en relación con los dispositivos que, debido a su tecnología, están sujetos a un desgaste natural por el número de ciclos de conmutación y, posiblemente, por la carga de conmutación.

- El cálculo del valor B_{10d} es necesario porque, con un coeficiente constante de fallos y defectos aleatorios durante la duración de la misión, no se considera que la denominada curva de bañera sea de aplicación con total exactitud a los dispositivos afectados por un desgaste natural (véanse las entradas “valor B_{10d}”, “Curva de bañera” y “Duración de la misión” del glosario). Esto significa que, después de los primeros fallos de los componentes afectados por desgaste natural, la tasa de fallos no es constante en el tiempo, sino que en general aumenta. Dicho de otro modo, la tasa de fallos varía a lo largo del tiempo.

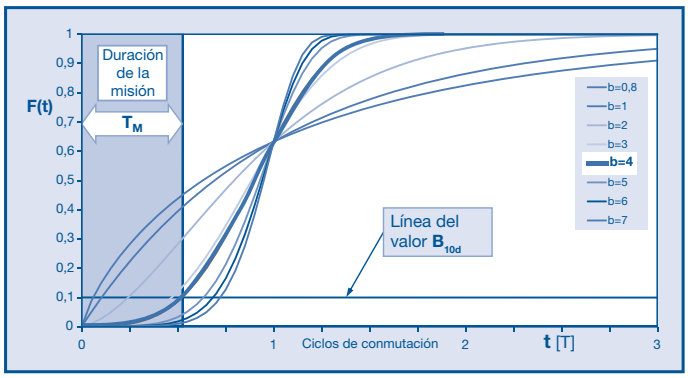


- Estas son las fórmulas de conversión de un valor B_{10d} en un valor $MTTF_d$:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad n_{op} = \frac{d_{op} \times h_{op} \times 3.600 \frac{s}{h}}{t_{cycle}}$$

n_{op} = número medio de operaciones por año
d_{op} = número medio de días de utilización por año
h_{op} = número medio de horas de utilización por día
t_{cycle} = tiempo medio entre el comienzo de dos ciclos sucesivos del componente en segundos (es decir, 4 × por hora = 1 × por 15 minutos = 900 s)

- De forma adicional, debe establecerse un valor T_{10d} en el caso de las tecnologías afectadas por desgaste natural (10 % del MTTFd derivado del valor B_{10d}). El valor T_{10d} es un indicador de la sustitución preventiva del componente (donde T_{10d} < 20 años). El porcentaje del 10 % se explica por el hecho de que se asume una pauta de fallo constante (al igual que la pauta de fallo de la curva de bañera). Con el valor B_{10d}, por el contrario, de forma similar al valor $MTTF_d$, ha generado fallos peligrosos en torno al 63 % de los componentes de una muestra aleatoria. Véase también la entrada “Distribución exponencial” del glosario.



Ejemplo de cálculo de valor $MTTF_d$:

- Un interruptor de control de puerta de guarda puede poseer un valor B_{10d} de 2.000.000.

- La aplicación con protección mecánica en el que se utiliza puede funcionar 200 días (d_{op}) al año con 2 turnos (h_{op}), y la puerta de guarda se abre 2 veces por hora. Esto genera un número de ciclos de trabajo por año de 200 (d_{op}) × 16 (h_{op}, 2 turnos) × 2 (solicitaciones/hora) o (t_{ciclo} = 1.800) = 8.400 n_{op}.

- Por tanto, esto resulta en un valor $MTTF_d$ de 2.381 años[1] (2.000.000: 0,1 × 8.400 = 2.381).

- El valor T_{10d} (238 años) es irrelevante en este ejemplo, ya que supera con mucho la vida útil asumida (duración de la misión) de un sistema de mando de maquinaria (20 años) en la norma EN 13 849-1:2006.

Origen de los datos

- Cuando no se indique otra cosa: EN ISO 13 849-1:2006 e Informe 2/2008 del BGIA (véase entrada “Informe 2/08 del BGIA” del glosario).

Cuestiones relativas a la arquitectura o la categoría de control

- La cuestión o en algunos casos el problema de a qué categoría de control corresponde un dispositivo único sencillo seguirá igual en el futuro, ya que las categorías de control siguen siendo una característica significativa del PL.

- Por tanto, de esta forma se resuelve el “viejo” debate de si un dispositivo con contactos de seguridad redundantes (contacto de apertura positiva o comparable) es suficiente para una arquitectura con un sistema de protección contra fallos, tal como se exige en relación con las categorías de control 3 y 4, o si deben incluirse dos dispositivos (capacidad física de 2 canales).

- El mero uso de un dispositivo con contactos de seguridad redundantes implica asumir la existencia de exclusión de defectos en el sistema de activación mecánico (el mecanismo de activación), es decir, poder excluir la posibilidad de que se den fallos peligrosos, como por ejemplo a causa del desgaste natural, daños, suciedad, etc.

[1] La limitación de los valores $MTTF_d$ a un máximo de 100 años no es de aplicación en este caso, ya que en principio está referido a un valor único. El redondeo o uso del límite de 100 años por canal tan solo tiene lugar al final del análisis del PL, junto con otros valores $MTTF_d$. ADVERTENCIA: en contraposición a lo anterior, en el software SISTEMA (véase entrada “SISTEMA” del glosario) el análisis de cada subsistema ya genera redondeo o uso del límite máximo. Por este motivo, al objeto de evitar un redondeo excesivo, se recomienda utilizar la misma arquitectura de la SRP/CS en el subsistema específico de SISTEMA (= varios subsistemas de acuerdo con la definición estipulada en la presente, pero con la misma arquitectura).

- Los enfoques de exclusión de defectos también son aceptables en virtud de la norma EN ISO 13849-1:2006, de acuerdo con su Artículo 7.3, así como en virtud de EN ISO 13849-2: 2003. Por otra parte, en su Artículo 3.3 la norma requiere que la evaluación de las probabilidades de fallo en una SRP/CS comience donde se genera la señal de seguridad, es decir, en el rodillo del interruptor de posición, y finalice en el contacto de los elementos de activación.

- En todos los casos el análisis debe realizarse con la máxima atención.

- En lo que concierne a nuestros dispositivos, puede encontrarse asesoramiento en la siguiente lista de dispositivos, bajo el epígrafe “capacidad de 1 o 2 canales” y en la sección “Cuestiones relativas a la arquitectura o la categoría de control” del excurso incluido en las páginas 29 y siguientes. En última instancia, no obstante, la cuestión de la exclusión de defectos depende de la evaluación del cliente y de las condiciones de aplicación.

Cobertura del diagnóstico

- Dependiendo del procesamiento de señal posterior, hasta un 99 % (véanse también páginas 32 f. y 68 f.).

Medidas CCF
(Medidas contra fallos de causa común)

- Medidas CCF (medidas contra fallos de causa común): la evaluación independiente plantea algunas dificultades. Por el contrario, una evaluación contextualizada en la que se integren los dispositivos únicos sencillos en la SRP/CS es mejor, sobre todo porque en este caso, también, se plantea la cuestión de si se ha ejecutado la eventual función de dos canales y cómo (es decir, si utilizar redundancia eléctrica o física).

- No obstante, los dispositivos únicos sencillos de la gama Schmersal/Elan ya poseen integrada la puntuación mínima requerida de 65, de la cual una proporción corresponde al subsistema en que se utilizan (véase entrada “CCF” del glosario, tabla a partir de 3). Esto es así porque deben cumplirse la norma de producto de la serie EN IEC 60947-5, los requisitos medioambientales y de seguridad correspondientes, la compatibilidad EM de los dispositivos, etc. A esto hay que añadir los puntos (posiblemente prorrateados) de las unidades de análisis “1. separación física entre los recorridos de la señal”[1] y, cuando proceda, “2. diversidad”[2].

- Importante: las medidas CCF deben analizarse y evaluarse exclusivamente partiendo de la categoría de control 2, ya que las SRP/CS de la CC 2 poseen varios canales (ya se trate de una capacidad clásica de dos canales o de una capacidad de un canal + canal de prueba).

- Para más información: véase entrada “CCF” del glosario.

[1] Los contactos individuales de los dispositivos están separados galvánicamente. Deben cumplirse también los demás requisitos relativos a la protección o separación de la disposición de los cables.
[2] Por ejemplo, y dependiendo del enfoque adoptado, combinaciones de contacto NC/contacto NO.

Información específica de dispositivo

(Véase también el catálogo en línea de Schmersal en www.schmersal.net)

- Nota (1): cuando en lo sucesivo se haga referencia a contactos NC, esto siempre significará contactos de apertura positiva, exceptuando los interruptores magnéticos de seguridad. En el caso de los contactos de apertura positiva, se entiende que la información es independiente de la carga precisamente debido a esta característica de seguridad especial. Véase la entrada “Exclusión de defectos” del glosario.
- Nota (2): Resulta legítimo plantearse la pregunta de por qué, en ocasiones, los valores B_{10d} resultan ser tan diferentes a pesar de que los productos correspondientes, exceptuando los interruptores magnéticos de seguridad, posean contactos de apertura positiva. El motivo es que también deben considerarse otros defectos generadores de situaciones peligrosas, como por ejemplo el desgaste de los elementos mecánicos de la función escalón de un dispositivo de control de parada de emergencia o la capacidad de rearme (sin quedarse enganchado) de un botón pulsador. En el caso de los denominados interruptores de clase 2, el valor estándar se ha visto influido por la reducida vida útil experimentada en marcas competidoras en el pasado.

Dispositivos de control de parada de emergencia

- Valor B_{10d} (independiente de la carga): 100.000 (contacto NC)
- Capacidad de 1 o 2 canales: dependiendo de la arquitectura designada (categoría de control)
- ALTERNATIVA: exclusión de defectos como parte del valor B_{10d} (véanse páginas 29 y 75)
- Nota (1): de acuerdo con la norma, cuando se dé una carga máxima de un dispositivo de control de parada de emergencia, puede asumirse un valor B_{10d} de tan solo 6.050; en caso contrario, de 100.000. No estamos de acuerdo con el enfoque adoptado en la norma en relación con nuestros dispositivos por la siguiente razón: el valor B_{10d} de 6.050 es un valor de comprobación mínimo de EN IEC 60 947-5-5 relativo a la función correcta del mecanismo de cierre de un dispositivo de control de parada de emergencia según el punto 7.3. Tan solo se presta atención a este valor mínimo. Por el contrario, la norma no se interesa por el número de ciclos de conmutación que tendría lugar antes de que fallase el mecanismo de cierre. Ahora bien, en nuestros laboratorios de pruebas hemos comprobado que nuestros dispositivos alcanzan un número mínimo de 100.000 ciclos de funcionamiento correctos.
- Nota (2): Recomendamos conseguir una capacidad de 2 canales en dispositivos de control de parada de emergencia utilizando dos elementos de contacto (véase: redundancia física).

Interruptor de seguridad de tracción por cable

- Véanse dispositivos de parada de emergencia

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Interruptor de validación / botón pulsador de 3 posiciones

- Valor B_{10d} (independiente de la carga): 100.000 (contacto NC)
- Capacidad de 1 o 2 canales: dependiendo de la arquitectura designada (categoría de control)
- ALTERNATIVA: exclusión de defectos como parte del valor B_{10d}

Interruptor de pedal de seguridad (versión 3 posiciones con rearme)

- Véase interruptor de validación/botón pulsador de 3 posiciones

Dispositivos de accionamiento a dos manos (combinaciones contacto NC-contacto NO)

- Valor B_{10d}: 20.000.000 (contacto NC)[1]
  1.000.000 (contacto NO)[2]
  100.000 (contacto NO)[3]

[1] Independiente de la carga
[2] Con carga óhmica o casi óhmica y sobredimensionamiento, es decir, ≤ 10 % de la potencia nominal
[3] Con carga inductiva y sobredimensionamiento (≤ 10 % de la potencia nominal)

Nota: En combinación con módulos SRB a dos manos y similares, las restricciones [1] a [3] no son de aplicación o son cubiertas por el módulo SRB.

Interruptor de posición con activación integrada (denominado interruptor de tipo 1)

- Valor B_{10d}: 20.000.000 (contacto NC)[1]
  1.000.000 (contacto NO)[2]
  100.000 (contacto NO)[3]

[1] Independiente de la carga
[2] Con carga óhmica o casi óhmica y sobredimensionamiento, es decir, ≤ 10 % de la potencia nominal
[3] Con carga inductiva y sobredimensionamiento (≤ 10 % de la potencia nominal)

- Capacidad de 1 o 2 canales: para dispositivos bipolares únicos dependiendo de la norma C, o cuando se requiera exclusión de defectos en virtud de EN ISO 13849-2:2003 (véase nota al pie de la página 16, y página 29 f.).

Interruptor de posición con actuador separado (denominado interruptor de tipo 2)

- Valor B_{10d}: 2.000.000 (contacto NC)[1]
  1.000.000 (contacto NO)[2]
  100.000 (contacto NO)[3]

[1] Independiente de la carga
[2] Con carga óhmica o casi óhmica y sobredimensionamiento, es decir, ≤ 10 % de la potencia nominal
[3] Con carga inductiva y sobredimensionamiento (≤ 10 % de la potencia nominal)

- Capacidad de 1 o 2 canales: para dispositivos bipolares únicos dependiendo de la norma C, o cuando se requiera exclusión de defectos en virtud de EN ISO 13849-2:2003 (véase nota al pie de la página 16, y página 29 f.).

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Interruptor de posición con actuador separado y bloqueo por solenoide de guarda

- Valor B_{10d}: véase más arriba (interruptor de posición con activación independiente)
- Capacidad de 1 o 2 canales: previa consideración de la exclusión de defectos (véase nota al pie de la página 16 y la página 29 f.), un dispositivo único puede cumplir los requisitos de capacidad de 2 canales (= SK 3, PL “d” como máximo), pero tan solo en la versión con mecanismo de bloqueo a prueba de errores[1] (= CC 3). El Informe 2/08 del BGIA también hace referencia a esta posibilidad y prevé un segundo interruptor que haría las veces de sistema adicional de protección durante el funcionamiento (no obstante, esto también puede conseguirse de otras formas).

  [1] En combinación con un dispositivo de enclavamiento, se entiende por mecanismo de bloqueo a prueba de errores que el mecanismo de bloqueo no puede adoptar la posición de bloqueo mientras la puerta de guarda esté abierta, es decir, que pueden excluirse los “dispositivos de enclavamiento neumáticos”. Por este motivo, cuando existan requisitos de seguridad mayores también puede prescindirse de un segundo sensor.

- En la CC 3 debe tenerse en cuenta:
  - control de la posición de la puerta de guarda = canal 1
    control de la posición de cierre (bloqueo de guarda) = canal 2 o
  - control de la posición de la puerta de guarda = mecánico mediante mecanismo de bloqueo a prueba de errores
    control de la posición de cierre (bloqueo de guarda) (contacto de seguridad 1) = canal 1 (eléctrico)
    control de la posición de cierre (bloqueo de guarda) (contacto de seguridad 2) = canal 2 (eléctrico)
- Otros aspectos: véase la información anterior y el ejemplo de conexión del BGIA incluido en la página 78

Interruptor de seguridad magnético[1]

- Valor B_{10d} (dependiente de la carga):

20.000.000	(con una carga del 20 %)
400.000	(con una carga del 100 %)
7.500.000	(con una carga del 40 %)[2]
2.500.000	(con una carga del 60 %)[2]
1.000.000	(con una carga del 80 %)[2]

  [2] Valores propios tras consultar al BGIA

- Capacidad de 1/2 canales: es posible contar con capacidad de 2 canales en un dispositivo único (exceptuando BNS 30, 300 y 333 = 1 canal).
- Combinaciones de dispositivos BNS/AES o módulos SRB con capacidad BNS: se trata de una combinación de dispositivos (véase página 41) que representa un subsistema (con sub-PL o sub-SIL y valor PFHd). En este caso no procede tener en cuenta el valor B10d ni la reducción progresiva del valor en función de la carga, como antes, es decir, que podemos asumir 20.000.000 porque los contactos de relé de láminas de los sensores están conmutados con una carga máxima del 20%. Dicho de otro modo: esta consideración adicional tan solo es de aplicación cuando existe procesamiento de señal alternativo. De esto no cabe concluir que no vaya a “funcionar” si se utilizan módulos de otros fabricantes, sino más bien que la combinación debe comprobarse (límites de corriente y voltaje, carga de conmutación, etc.).
- En combinación con módulos AES (u otros sistemas adecuados de procesamiento de señal), el cálculo puede realizarse, en caso necesario, para un único BNS con un valor PFH_d de $2{,}5 \times 10^{-11}$ (a 0,1 h^{-1}) (exceptuando los BNS 30, 300 y 333 = $1{,}21 \times 10^{-6}$ a 0,1 h^{-1}, 1 canal, PL “c” como máximo).

[1] En la norma EN ISO 13849-1:2006, los interruptores de seguridad magnéticos se incluyen (con sujeción al desgaste natural) bajo los “interruptores de proximidad”.

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Interruptor de seguridad de bisagra (gama TESF)

- Valor B_{10d} (independiente de la carga): 2.000.000[1]

  [1] Con un ángulo de conmutación de seguridad máximo de 8°. Puede considerarse un valor mayor cuando, desde el punto de vista de la seguridad, pueda tolerarse un ángulo de conmutación más amplio.
- Capacidad de 1 o 2 canales: la capacidad de 2 canales también es posible en dispositivos únicos cuando se utilice exclusión de defectos en el eje que introduzca el movimiento de rotación (instalación protegida, activación sin tensión).
- Nota: en el caso de los interruptores de seguridad de bisagra TVS 521, el valor B_{10d} debe considerarse haciendo referencia a los valores relativos a interruptores de tipo 1.

Dispositivos con interfaz ASi-SaW

- Véanse páginas 42 y siguientes.

Sistemas de transferencia de llave

- Valor $MTTF_d$: 150 años[1]

  [1] La norma EN ISO 13849-1:2006 permite adoptar un enfoque simplificado con un valor $MTTF_d$ global de 150 años para todos los sistemas mecánicos. Para el interruptor de llave de un sistema SHGV recomendamos asumir la exclusión de defectos en relación con el contacto de apertura positiva y asumir un valor B_{10d} de 1.000.000 (con carga óhmica o casi óhmica y sobredimensionamiento, es decir, al 10 % de la potencia nominal) o 100.000 (en caso de carga inductiva y sobredimensionamiento, es decir, al 10 % de la potencia nominal) en relación con el contacto NO.
- capacidad de 1/2 canales: véase interruptor de posición con activación independiente y dispositivo de enclavamiento

Botón de rearme/restauración

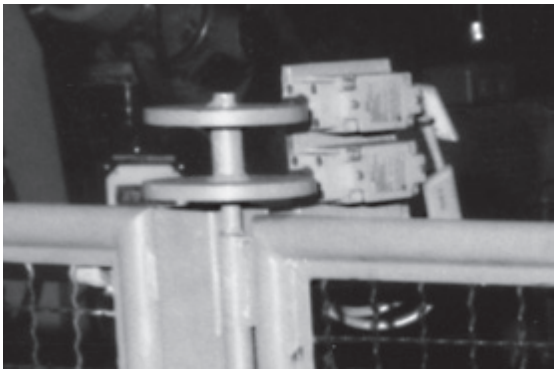
- Con el objetivo de no hacer demasiado complejo el diseño de otros análisis relativos al PL (como por ejemplo la protección ante movimientos peligrosos), estos dispositivos también pueden considerarse en el marco de una función de seguridad independiente de “protección ante inicio/reinicio inesperados”. Esta puede incluir cualquier otro aspecto que deba tenerse en cuenta, sobre todo si las señales de parada se producen como una PARADA de categoría 2 (apagado controlado sin desconectar la alimentación de los mecanismos de transmisión; véase EN IEC 60204-1).
- Son de aplicación los valores B_{10d} relativos a contactos NO (véase, por ejemplo, la página 26).
- Además, actualmente, en el Artículo 5.2.2 de EN ISO 13849-1:2006 existe un requisito inequívoco en el sentido de que la función de rearme manual tan solo puede efectuarse liberando el elemento de transmisión en su posición activada (encendido). Dicho de otro modo, los botones de rearme/restauración deben llevar asociado un sistema de detección de flanco de bajada.
- Esta medida de seguridad sirve para detectar defectos relacionados con el botón o su uso.
- Cuando la detección de flanco de bajada se lleva a cabo con circuitos autocontrolados, la exclusión de defectos es aceptable.

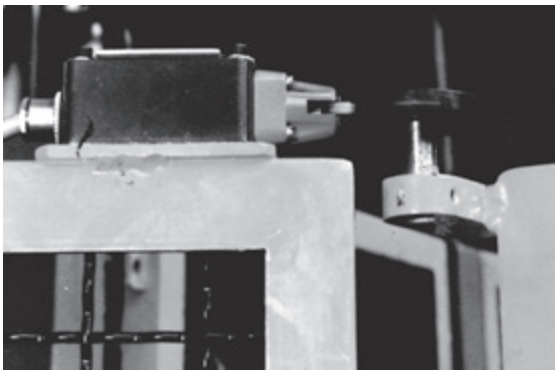
¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

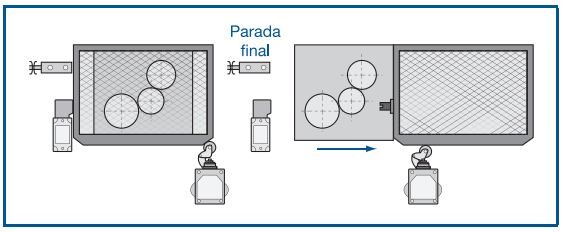
- La cuestión ya se planteaba con la aplicación de EN 954-1:1996: de acuerdo con los requisitos asociados a las categorías de control 3 o 4, ¿debe ejecutarse la estructura a prueba de 1 fallo (con tolerancia a 1 fallo) de una SRP/CS utilizando una redundancia física, como por ejemplo, en los dispositivos de enclavamiento de dispositivos de protección móviles, por medio de dos interruptores, o cumple también estos requisitos un dispositivo de enclavamiento único con dos contactos de seguridad (internos) (capacidad eléctrica de 2 canales)?

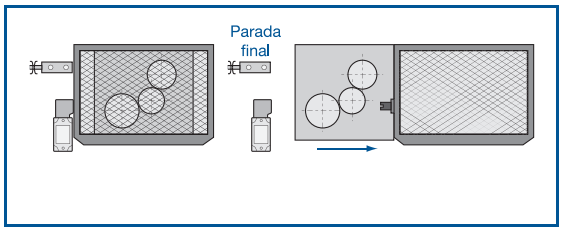
- En este contexto, los dispositivos de conmutación de seguridad activados de forma manual, como por ejemplo dispositivos de control de parada de emergencia o los Interruptores de validación, deben considerarse una excepción desde un primer momento. De cualquier forma, en este caso tan solo resulta relevante una capacidad eléctrica de 2 canales. Si nos ajustamos al Informe BGIA (véase entrada “Informe BGIA” del glosario), podemos terminar asignando un sistema de detección de defectos a todos estos dispositivos, ya que normalmente se diseñan con contactos de apertura positiva cuando la frecuencia de activación previsible se sitúa dentro del intervalo del valor B_{10d}. No obstante, la disposición del cableado, etc., debe ser la “correcta”. En este caso, el operador se responsabiliza de la eventual detección de defectos, y debe quedar convencido de que el dispositivo en cuestión no está dañado antes de trabajar con él.

- En el caso de los interruptores electromagnéticos, el punto fundamental es el mecanismo de activación de los contactos eléctricos, que generaría la pérdida de la función de seguridad de los dispositivos en caso de fallo. En este caso, la norma es valorar la elevada improbabilidad de que se dé un fallo peligroso de estas características.









Para ilustrar la cuestión: ejemplos de soluciones de 2 interruptores frente a soluciones de 1 interruptor (arriba: en una puerta giratoria; abajo: en una puerta corredera).

- Esta cuestión tampoco se resuelve en EN ISO 13 849-1:2006 (en el sentido de proporcionar una “receta”). Por una parte tenemos la Nota 1 del Artículo 3.3 de la norma. De acuerdo con ella, una combinación de SRP/CS empieza en el punto en que se genera la señal (es decir, en el rodillo de un interruptor de posición) y finaliza en los contactos de los elementos de control de potencia (es decir, en el elemento de control de potencia de un contactor).

Por otra parte, de acuerdo con el Artículo 7.3 de la Norma, en determinadas circunstancias es posible realizar exclusiones de defectos.

- Lo ideal es abordar la cuestión desde la norma C (norma de producto) “competente” que corresponda, como es el caso de determinadas funciones de seguridad de prensas de imprimir, por ejemplo (basta con la capacidad eléctrica de 2 canales de un interruptor), o en el caso de prensas de metal (en este caso se requiere de forma explícita una solución de 2 interruptores).

- En casos dudosos recomendamos lo siguiente a los clientes:
  - En caso de duda, proporcionar siempre una capacidad física de 2 canales (una solución de 2 interruptores) para los niveles de prestaciones “d” y “e” (o para las categorías de control 3 y 4).
  - Como excepción a lo anterior, pueden utilizarse sin un segundo interruptor los interruptores magnéticos de seguridad de la gama BNS con salidas de 2 canales, los interruptores de bisagra de la serie de modelos TESF y todos los dispositivos de enclavamiento sin contacto, con o sin cierre, de la “familia CSS” de Schmersal, siempre que se cumpla la adición AMD 1 de EN 1088:1996 (véase entrada “AMD 1” del glosario). El dispositivo AZM 200 cuenta con una función adicional de seguridad durante el funcionamiento integrada a través de un sistema de mando de doble posición.
  - En los interruptores sencillos, y en especial en los interruptores de posición de tipo 1 (con elementos de activación integrados), debería proporcionarse por norma una redundancia física en las arquitecturas de 2 canales, ya que una influencia externa negativa puede afectar de forma directa a la función del mecanismo de leva de 1 canal.
  - El nivel de prestaciones “e” no admite concesión alguna, ni siquiera en previsión de la revisión prevista de EN ISO 13 849-2:2003 (fuente: nueva Tabla D.8 del borrador de la revisión). Básicamente, esto significa que, en el caso de un PL “e”, tan solo puede utilizarse una solución de 2 interruptores en todos los dispositivos electromecánicos.
  - Por el contrario, de acuerdo con EN ISO 13 849-2:2003, Anexo A, Artículo A.5, en el nivel de prestaciones “d” pueden utilizarse exclusiones de defectos en el caso de los interruptores de seguridad con activación independiente cuando puedan garantizarse las condiciones previstas en la siguiente tabla. De forma adicional, recomendamos que también se tengan en cuenta los aspectos de la siguiente sección (“Dispositivos de enclavamiento con sistema de cierre”), cuando proceda.

Defecto asumido	Exclusión de defecto	Observaciones
Desgaste/ corrosión	Sí, cuando se hayan seleccionado de forma minuciosa los materiales, el (sobre)dimensionamiento, el proceso de fabricación, el proceso de tratamiento y una lubricación adecuada en función de la vida útil especificada (véase también Tabla A.2).	Véase ISO 13849-1:2006, 7.2
Problemas de ajuste/piezas flojas	Sí, cuando se hayan seleccionado de forma minuciosa los materiales, el proceso de fabricación, los elementos de sujeción y el proceso de tratamiento en función de la vida útil especificada (véase también Tabla A.2).	
Rotura	Sí, cuando se hayan seleccionado de forma minuciosa los materiales, el (sobre)dimensionamiento, el proceso de fabricación, el proceso de tratamiento y una lubricación adecuada en función de la vida útil especificada (véase también Tabla A.2).	
Deformación por sobrecarga	Sí, cuando se hayan seleccionado de forma minuciosa los materiales, el (sobre) dimensionamiento, el proceso de fabricación y el proceso de tratamiento en función de la vida útil especificada (véase también Tabla A.2).	
Rigidez/ atascos	Sí, cuando se hayan seleccionado de forma minuciosa los materiales, el (sobre)dimensionamiento, el proceso de fabricación, el proceso de tratamiento y una lubricación adecuada en función de la vida útil especificada (véase también Tabla A.2).	

– La tabla A.2 de la página 30 afecta a los denominados principios de seguridad comprobados que deben aplicarse de forma adicional.

– En determinadas circunstancias puede prescindirse de la capacidad física de 2 canales en el caso de dispositivos de enclavamiento con bloqueo, es decir, que el sistema de bloqueo de seguridad individual puede ser suficiente si se garantizan las siguientes condiciones (lo mismo para la tabla mencionada anteriormente):

  a) Debe incluir un dispositivo con un mecanismo de bloqueo a prueba de fallos (véase página 27) y un sistema de evaluación de la señal de 2 canales (1 × posición de la puerta, 1 × control del mecanismo de bloqueo).
  b) Únicamente aplicaciones con nivel de prestaciones “d” (o categoría de control 3) como máximo; además, debe intervenir una fuente de peligro visible.
  c) La interacción entre el mecanismo de activación y el dispositivo no debe estar sometida a tensiones (sin margen de movimiento), por ejemplo en relación con un sistema de manilla de seguridad.
  d) El mecanismo de activación debe poseer una forma óptima para su ejecución y estar construido a partir de una pieza de metal perforado (sin resortes, etc.).
  e) El lugar de instalación de los dispositivos debe seleccionarse de forma que no puedan entrar partículas de suciedad o similares en el mecanismo de articulación.
  f) Deben respetarse las fuerzas de bloqueo máximas y los principios derivados de las “buenas prácticas de ingeniería” (véase glosario).
  g) Deben proporcionarse medidas adicionales para minimizar la posibilidad de eludir el sistema con arreglo a AMD 1 de EN 1088:1996. Además, el segundo interruptor puede integrarse en las medidas que vayan a realizarse si no hay alternativas.
  h) Se recomienda la realización de una prueba de inicio automática para detectar eventuales fallos. Esta medida está concebida para mantener las previsiones de cambio de señal de los dispositivos (no obstante, dependiendo de la aplicación, el sistema de mando operativo también comprobaría los cambios de señal derivados de una función correcto de los dispositivos en el transcurso del funcionamiento = modificación de señal mínima en relación con una unidad de tiempo lógica).

Al margen de esto, la norma general es que no debe utilizarse un dispositivo de enclavamiento como parada final, y debe respetarse tanto la norma EN 953:1997[1] como el correspondiente dispositivo de procesamiento de señal de 2 canales.

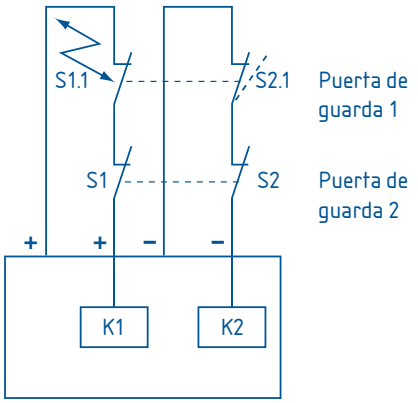
[1] DIN EN 953:1997-11: Seguridad de Máquinas – Guardas – Requisitos generales para el diseño y la construcción de guardas fijas y móviles

Excurso: Detección de fallos en el caso de dispositivos únicos sencillos con función de seguridad

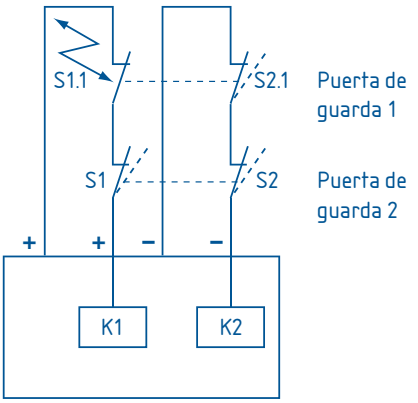
- Tal como se ha mencionado anteriormente, la detección (diagnóstico) de fallos en dispositivos únicos sencillos con función de seguridad debe proporcionarse a través de otras partes de la SRP/CS, situadas corriente arriba o corriente abajo de los dispositivos únicos sencillos (normalmente a nivel del procesamiento de señal **L**). La cobertura del diagnóstico conseguida depende de la función de detección de defectos (véase EN ISO 13 849-1:2006, Anexo E).

- En el caso de los módulos de relé de seguridad (combinaciones de relé de seguridad), PLC de seguridad, etc. (que se ajusten a los requisitos del sub-PL “e”), puede conseguirse una DC del 99 % con una conexión 1:1 de 2 canales (conexión paralela); por el contrario, en el caso de las conexiones en serie (conexiones en cadena tipo serie/paralelo) tan solo se alcanza una DC del 60 % en determinadas circunstancias, y no puede excluirse la posibilidad de una acumulación de defectos. La DC de otros mecanismos de detección de defectos debe evaluarse de forma individual.

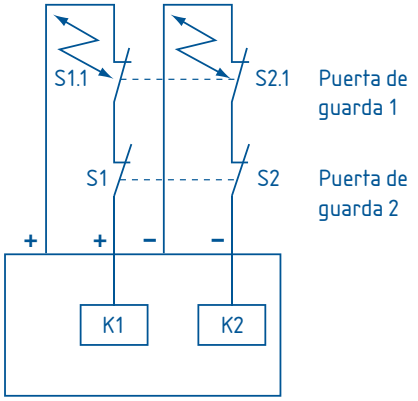
- Peor escenario de análisis de defectos con la conexión en serie de dispositivos electromecánicos:



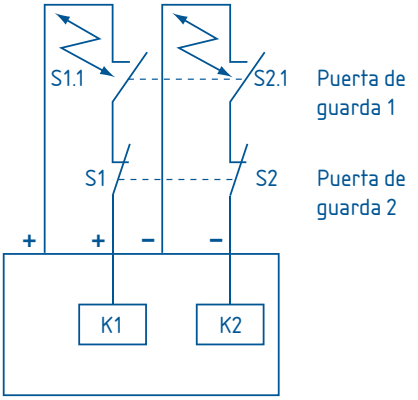
Primer defecto:
- Cortocircuito por el contacto S1.1 (puerta de guarda 1)
- La puerta de guarda 1 está abierta
- El módulo desconecta el canal 1
- Obstrucción del funcionamiento (reacción de seguridad correcta, restauración imposible)



Eliminación del defecto:
- La puerta de guarda 1 sigue abierta
- El módulo desconecta el canal 2
- Reinicio posible



Acumulación de defectos:
- Segundo defecto en la puerta de guarda 1
- Cortocircuito por S2.1



Situación peligros:
- La puerta de guarda 1 está abierta
- El módulo no se desconecta

- La cobertura del diagnóstico del 60% en conexiones en serie de dispositivos electromecánicos sencillos se basa en una estimación de probabilidad matemática de más de 2 puertas de guarda. Cuando, por el contrario, tan solo haya dos dispositivos de protección, se recomienda la conexión paralela en el nivel **L** (conexión 1:1). En ningún caso debe utilizarse la conexión en serie en dispositivos electromecánicos sin medidas adicionales ajustadas a un PL “e” o una CC 4.

- Es posible estimar una cobertura del diagnóstico superior a 60% (y por tanto, potencialmente, un PL “e” o una CC 4) en conexiones en serie de dispositivos electromecánicos cuando, por ejemplo, se incorporen las señales de retroalimentación de forma adicional al SPS operativo, cuya certeza en forma de una señal adecuada se incorpore a su vez al recorrido activador del nivel **L**. Véase también la página 76 del Excurso en este sentido (ejemplo de conexión 8.2.28 del BGIA).

- Es posible utilizar exclusión de defectos en conexiones en serie de dispositivos de control de parada de emergencia (en relación con este punto, véase ejemplo de conexión 8.2.29 del BGIA en la página 75).

- La citada restricción de la DC del 60 % en caso de conexiones en serie (conexiones de cadena tipo margarita) tan solo es de aplicación, como ya se ha indicado, a los circuitos ejecutados con tecnología eléctrica tradicional. En el caso de conexiones en serie ejecutadas con una tecnología diferente, como por ejemplo a través de dispositivos ASi-SaW o dispositivos basados en microprocesador de la “familia” CSS de Schmersal, se consigue una cobertura del diagnóstico del 99 % gracias a su inteligencia adicional.

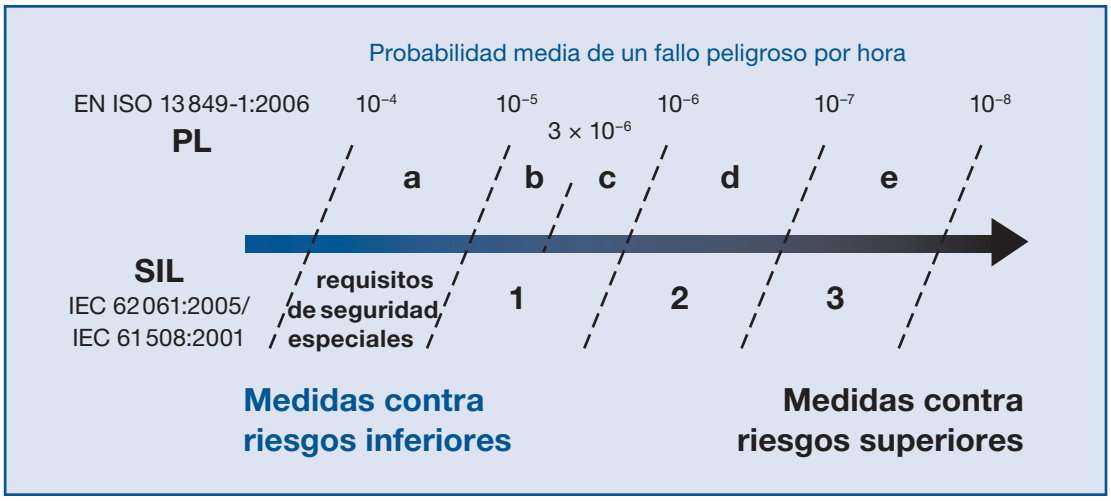
- Para más información (incluida la detección de defectos en dispositivos únicos sencillos en el nivel **O**), véanse la página 55 y el Excurso de la página 68 f.

Dispositivos con funciones de seguridad más complejas

Preludio

- Normalmente, este tipo de dispositivos se suministra con un sub-SIL y un valor PFH_d correspondiente, ya que los dispositivos han sido diseñados y certificados partiendo de EN IEC 61 508-1/-7:2001, en parte debido al uso de tecnología de microprocesador a la que no es de aplicación EN 954-1:1996, y en parte por otros motivos.

- Ya se sabe que, debido a la compatibilidad de las dos nuevas normas en materia de SRP/CS, un SIL puede convertirse a un PL y viceversa (véase tabla de conversión). El SIL y el PL se basan en el valor PFH_d, a partir del cual también puede obtenerse un valor $MTTF_d$ de bloque si se desea.



ADVERTENCIA: las anteriores clasificaciones de PFH_d corresponden a un PL global (o SIL global). Los subsistemas tan solo pueden "consumir" proporciones (recomendación: un máximo de 20% en cada uno de los niveles **I** y **L**, para que el nivel **O** tenga >60 %).

- Puede utilizarse el Anexo K de EN ISO 13 849-1:2006 para convertir un valor PFH_d en un valor $MTTF_d$ (valores PFH_d correspondientes como máximo a una $MTTF_d$ de 100 años almacenado). No obstante, de acuerdo con el Informe 2/08 del BGIA, puede calcularse un valor $MTTF_d$ de bloque de forma muy simplificada (solo posible en esta dirección) a partir de un valor PFH_d, invirtiendo este último. Por ejemplo: $1/PFH_d$: 8.760 = $MTTF_d$ de bloque (con PL o SIL superiores, normalmente de varios cientos de años). Véase también página 50.

- Nota: Salvo algunas excepciones, un valor $MTTF_d$ de bloque siempre es superior a un valor $MTTF_d$ único que refleje exclusivamente una fiabilidad estadística de equipos, mientras que en el valor PFH_d (y, al invertirlo, en el $MTTF_d$ de bloque) también se tienen en cuenta y evalúan todas las demás medidas, y en especial las medidas de detección de defectos o cobertura del diagnóstico. Así pues, un valor $MTTF_d$ de 30 años unido a todas las demás medidas requeridas para un PL "e" se corresponde con un valor $MTTF_d$ de bloque de aproximadamente 1.200 años.

- Este último valor puede ser necesario cuando se mezclen valores $MTTF_d$ y PFH_d en una cadena **I** + **L** + **O** (entrada, lógica, salida).

- En determinados dispositivos de protección (véanse fichas de datos de dispositivos), el subsistema **L** puede no ser de aplicación en algunos casos cuando el sensor del nivel **I** actúe directamente utilizando salidas OSSD[1] en el nivel **O**, por ejemplo (en SRP/CS estructuradas sencillas) en el caso de que el sensor también posea una interfaz para un circuito de retroalimentación (denominada función EDM[2] y, normalmente, para el botón de rearme/restauración. En estos casos puede omitirse un módulo SRB, un PLC de seguridad o similares.

[1] OSSD = dispositivos de conmutación de señales de salida = parte relativa a la seguridad de un dispositivo de protección, es decir, una cortina óptica de seguridad o sensor de la “familia” CSS de Schmersal conectada al sistema de mando de la máquina y que pasa a estado APAGADO cuando la parte del sensor se activa durante el funcionamiento normal especificado.

[2] EDM = control de dispositivos externos = un dispositivo de protección, es decir, una cortina óptica de seguridad o sensor de la “familia” CSS de Schmersal, que controla el estatus de otras partes de la SRP/CS.

Dispositivos con funciones de seguridad más complejas del programa Schmersal/Elan[1]

(véase también el catálogo de Schmersal en línea, en www.schmersal.net)

[1] Los valores PFH_d indicados son en su mayoría valores calculados durante la certificación del dispositivo (Asociación de Seguros de Responsabilidad Patronal [BG], Autoridad de Inspección Técnica [TÜV], etc.) de acuerdo con EN IEC 61 508:2001.

Sensores de seguridad CSS 180[2]

- Sub-SIL 3, sub-PL “e”, PFH_d $6{,}1 \times 10^{-9}$

Sensores de seguridad CSS 34[2]

- Sub-SIL 3, sub-PL “e”, PFH_d $3{,}6 \times 10^{-9}$

Interruptor de seguridad AZ 200[2]

- Sub-SIL 3, sub-PL “e”, PFH_d $4{,}0 \times 10^{-9}$

Dispositivo de bloqueo por solenoide electrónico AZM 200

- Sub-SIL 3, sub-PL “e”, PFH_d $4{,}0 \times 10^{-9}$

Dispositivo de bloqueo por solenoide electrónico MZM 100[2]

- Sub-SIL 3, sub-PL “e”, PFH_d $4{,}3 \times 10^{-9}$

[2] En relación con los sensores de seguridad y los bloqueos de guarda sin contacto de la “familia” CSS de Schmersal: deben tenerse en cuenta los requisitos de medidas adicionales para reducir el riesgo de manipulación (AMD 1 de EN 1088:1996) al utilizar estos dispositivos (exceptuando los dispositivos de bloqueo AZM 200 AZM 200, debido a su doble sistema de control de la posición). Un ejemplo sería la fijación permanente de la pieza de unión (con tornillos protegidos contra manipulación, instalación oculta o técnicas similares). Véase también la entrada “AMD 1” del glosario.

La cobertura del diagnóstico del 99% en estos dispositivos (dispositivos de la “familia” CSS de Schmersal) no se ve afectada en el caso de conexiones en serie, debido a que estos dispositivos ejecutan rutinas de autocontrol.

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Módulos de relé de seguridad (arquitectura: CC 4)[1)]

- Sub-SIL 3, sub-PL “e”, valor PFH_d dependiente de la carga de conmutación y los ciclos de trabajo de acuerdo con lo siguiente: valor mínimo (véase análisis incremental) de $9{,}54 \times 10^{-8}$ o $MTTF_d$ de 30 años[(2)].

(1) Información de detección de defectos (para la cobertura del diagnóstico) relativa a las partes de la SRP/CS corriente arriba y corriente abajo (dispositivos únicos sencillos en los niveles I u O): véanse páginas 32 f. y 50.
(2) Se requiere una inspección adicional porque los relés son componentes sujetos a desgaste natural. Valores B_{10d} usados como base de cálculo (con porcentaje de carga): 20.000.000 (20%), 7.500.000 (40%), 2.500.000 (60%), 1.000.000 (80%), 400.000 (100%).

El enfoque del valor B_{10d} tan solo concierne al nivel de salida conectado O. No debe considerarse el nivel de entrada I (carga < 20 %).

Análisis incremental:
En los siguientes casos se genera un $PFH_d < 9{,}54 \times 10^{-8}$ ($< 2{,}47 \times 10^{-8}$) o $MTTF_d > 30$ años (> 100 años):
≤ 6,5 (1,9) millones de ciclos de conmutación por año (n_{op}/año) y carga del 20 %
≤ 2,5 (0,75) millones de ciclos de conmutación por año (n_{op}/año) y carga del 40 %
≤ 0,6 (0,18) millones de ciclos de conmutación por año (n_{op}/año) y carga del 60 %
≤ 0,3 (0,09) millones de ciclos de conmutación por año (n_{op}/año) y carga del 80 %
≤ 0,1 (0,03) millones de ciclos de conmutación por año (n_{op}/año) y carga del 100 %

Pueden calcularse valores PFH_d de $MTTF_d$ “mejores” con un número de ciclos de conmutación más reducido.

- Resulta razonable calcular un valor PFH_d de $\leq 5 \times 10^{-9}$ (y con un valor PFH_d de $\leq 1{,}3 \times 10^{-8}$ con una carga de conmutación de hasta el 80 %) con un número medio de ciclos de trabajo de ≤ 100 × por día (≤ 36.500 n_{op}/año) y una carga de conmutación de hasta el 60 %.
- Por ejemplo, en el Informe 2/08 del BGIA se asume un valor PFH_d de $2{,}31 \times 10^{-9}$ en el caso de los módulos de relé de seguridad (en otro caso de $2{,}69 \times 10^{-9}$). Existen otros ejemplos (por ejemplo, con SIEMENS) con un valor PFH_d de 1×10^{-9}. En este caso, pueden calcularse números de ciclos de funcionamiento y/o cargas de conmutación claramente más favorables en comparación con la evaluación anterior.

Módulos de relé de seguridad (arquitectura: CC 3)

- Sub-SIL 3, sub-PL “e”, $PFH_d < 8{,}84 \times 10^{-8}$[(1)] o $MTTF_d > 62$ años (incluido PL “d” o SIL 2)
- Observaciones adicionales: véase lo indicado anteriormente (según proceda) (módulos SRB con arquitectura CC 4).

Relé temporizado de seguridad AZS 2305

- Sub-SIL 2, sub-PL “d”, PFH_d $2{,}5 \times 10^{-8}$

Monitores de parada de seguridad FWS 1205, 1206 y 2xxx

- (En función de los circuitos) como máximo Sub-PL “d”, sub-SIL 2, sub-PL “d”, PFH_d: $8{,}8 \times 10^{-9}$

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Controladores de seguridad ESALAN-Compact[1]

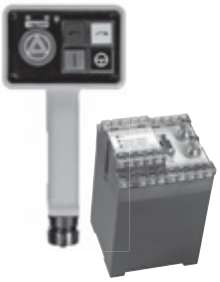
- Sub-SIL 3, sub-PL “e”, PFH_d 0,14 × 10^{-7} o $MTTF_d$ de 193 años (para salidas de semiconductor) o 0,15 × 10^{-7} o $MTTF_d$ de 192 años (para salidas de relé)

[1] Información de detección de defectos (para la cobertura del diagnóstico) relativa a las partes de la SRP/CS corriente arriba y corriente abajo (dispositivos únicos sencillos en los niveles I u O): véanse páginas 32 f. y 50.

PLC de seguridad PROTECT PSC[1]

- I/O de 2 canales: Sub-SIL 3, sub-PL “e”, PFH_d 1,27 × 10^{-8} (entrada de 2 canales → salida de 2 canales) 1,64 × 10^{-8} (2 × entradas de 2 canales → salida de 2 canales, por ejemplo en modo de funcionamiento “muting”)
- I/O de 1 canal: a demanda.

[1] Información de detección de defectos (para la cobertura del diagnóstico) relativa a las partes de la SRP/CS corriente arriba y corriente abajo (dispositivos únicos sencillos en los niveles I u O): véanse páginas 32 f. y 50.



Sistemas inalámbricos ESALAN

- Sub-SIL 3, sub-PL “e”, PFH_d 5,5 × 10^{-9}

Barreras, rejillas y cortinas ópticas de seguridad (Tipo 4)

- Sub-SIL 3, sub-PL “e”, PFH_d (por ejemplo SLG(C) 420) 7,42 × 10^{-9}

Aclaración: tan solo es de aplicación a las versiones suministradas con salidas OSSD[1] y función EDM[2] (por tanto, sin dispositivo de evaluación adicional o módulo SRB)

[1] OSSD = dispositivos de conmutación de señales de salida = parte relativa a la seguridad de un dispositivo de protección, es decir, una cortina óptica de seguridad o sensor de la “familia” CSS de Schmersal conectada al sistema de mando de la máquina y que pasa a estado APAGADO cuando la parte del sensor se activa durante el funcionamiento normal especificado.

[2] EDM = control de dispositivos externos = un dispositivo de protección, es decir, una cortina óptica de seguridad o sensor de la “familia” CSS de Schmersal, que controla el estatus de otras partes de la SRP/CS.

Barreras, rejillas y cortinas ópticas de seguridad (Tipo 2)

- Sub-SIL 2, sub-PL “d”, PFH_d (por ejemplo SLG(C) 220) 3,59 × 10^{-8}

Escáner de láser de seguridad

- Sub-SIL 2, sub-PL “d”, PFH_d 7,3 × 10^{-8}
- Duración de la misión: 11 años

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

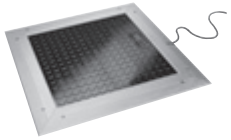
Combinaciones de dispositivos

Interruptores magnéticos de seguridad BNS / módulos de control AES

- Combinación de versiones de BNS/AES, modelos AES 1xxx (exceptuando 1102 y 1112, así como (véase más adelante) 1337): sub-PL “d”, sub-SIL 2, valor PFH_d en función de los ciclos de trabajo, de acuerdo con lo siguiente: sub-PL “d”; sub-SIL 2, valor PFH_d en función de los ciclos de trabajo, de acuerdo con lo siguiente: 1×10^{-8} a 6 h^{-1}, 9×10^{-9} a 1 h^{-1} y $8{,}4 \times 10^{-9}$ a 0,1 h^{-1}
- Combinación de BNS/AES del modelo AES 1337:
  Sub-PL “e”, sub-SIL 3, valores PFH_d previa solicitud
- Combinación de BNS/AES del modelo AES 2xxx: sub-PL “d”, sub-SIL 2, valor PFH_d en función de los ciclos de trabajo: $1{,}8 \times 10^{-9}$ a 0,1 h^{-1}
- Combinación de versiones BNS/AES de los modelos 1102, 1112, 6112 y 7112: sub-PL “c”, sub-SIL 1, valor PFH_d en función de los ciclos de trabajo: $1{,}21 \times 10^{-6}$ o $MTTF_d$ de 75 años a 5,280 n_{op}/año

Perfiles de seguridad

- A demanda



Alfombras de seguridad

- A demanda

Topes de seguridad

- A demanda

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Observación preliminar

Al considerar una estimación del PL, la función de seguridad respectiva (véanse página 70 y siguientes) y la cadena son

- el dispositivo de conmutación de seguridad, incluida la interfaz integrada ASi-SaW (es decir, el interruptor magnético BNS 260 AS)

o bien

- el “dispositivo de conmutación de seguridad” más la “conexión de interfaz ASi-SaW” externa (es decir, el dispositivo de control de parada de emergencia + el tubo ASi)

más

- el monitor ASM ASi-SaW. A los efectos del método del subsistema, esto se corresponde con los niveles **I** y **L**.

A esto hay que añadir la evaluación del nivel de salida **O**.

En el caso de dispositivos únicos sencillos en el nivel **O**, la interfaz de circuito de retroalimentación del monitor ASM ASi-SaW de la detección de defectos también hace las veces de función de seguridad, como módulo de relé o SPS de seguridad. Por tanto, en función de la calidad relativa a seguridad de la señal de retroalimentación, puede obtenerse una cobertura del diagnóstico de hasta el 99% (en este sentido, véase página 55).

Nota sobre el nivel **I**: la cobertura del diagnóstico del 99 % del sistema bus de seguridad ASi-SaW no se ve afectada ni siquiera en caso de conexión en serie de dispositivos únicos sencillos, es decir, que sigue siendo del 99 % porque las rutinas de control del ASi-SaW incorporan (supervisan) cada parte por separado.

Nota 2: el nivel de prestaciones de una función de seguridad viene determinado por la teoría del eslabón más débil de la cadena, es decir, que un dispositivo de conmutación de seguridad único que tan solo pueda evaluarse como un canal y, por tanto, alcance un sub-PL “c” como máximo, determinará el PL global. La mayor calidad del sistema electrónico ASi-SaW no mejora el PL.

Nota 3: en caso de dispositivos únicos sencillos con conexión de interfaz ASi-SaW externa, recomendamos considerar los dos componentes del sistema como un subsistema. En función de los ciclos de trabajo[1], en general esto supone un sub-PL “c” en los dispositivos únicos sencillos de 1 canal y, por norma, siempre un sub-PL “e” en dispositivos/conjuntos de dispositivos de 2 canales. En caso necesario, debe cuantificarse el subsistema mediante un valor PFH (véase página 50).

[1] No es necesario tener en cuenta el efecto de la carga de conmutación.

Interruptores magnéticos de seguridad

- Valor B_{10d}: 2.000.000[1]
  [1] Funcionamiento con carga reducida (<20 %)
- Capacidad de 1 o 2 canales, capacidad de 2 canales también posible en un dispositivo único
- Versión BNS 260 AS:
  Sub-PL “e”, valor PFH_d $6{,}21 \times 10^{-9}$ (con n_{op}/año de 525.600) o $3{,}35 \times 10^{-9}$ (con n_{op}/año de 24.000)
- Versión BNS 36 AS:
  Sub-PL “e”, valor PFH_d $1{,}24 \times 10^{-8}$ (con n_{op}/año de 525.600) o $4{,}03 \times 10^{-9}$ (con n_{op}/año de 24.000)
- Versión BNS 16 AS:
  similar a BNS 36 AS

Interruptores de posición con activación independiente
(denominado interruptor de clase 2)

- Valor B_{10d}: 2.000.000[1]
  [1] Funcionamiento con carga reducida (<20 %)
- Capacidad de 1 o 2 canales con interruptores de seguridad: con un dispositivo único depende de la norma C o de la exclusión de defectos necesaria con arreglo a EN ISO 13849-2:2003
- Versión AZ 16 AS:
  Sub-PL “c”[2], sub-SIL 1[2] (con exclusión de defectos facilitada por el cliente con PL “d” como máximo[2], sub-SIL 2[2]), valor PFH_d: PFH_d/interruptores de seguridad (se basará en una evaluación en función del usuario) + PFH_d/sistema electrónico ASi-SaW ($<1 \times 10^{-8}$), por ejemplo, con 100 años de $MTTF_d = 3{,}47 \times 10^{-8}$, con 200 años = $2{,}19 \times 10^{-8}$, con 500 años aproximadamente $0{,}55 \times 10^{-8}$, etc.

[2] con $MTTF_d$ “alta”

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Interruptores de posición con activación independiente y dispositivo de enclavamiento (denominado interruptor de clase 2)

- Valor B_{10d}: 2.000.000[1]

  [1] Funcionamiento con carga reducida (< 20 %)
- Capacidad de 1 o 2 canales: véanse páginas 26 f. y 29 y siguientes (dispositivos con activación independiente y sistema de cierre sin interfaz ASi-SaW)
- Versión AZM 162 AS:
  Máx. sub-PL “d”[2], SIL 2[2], valor PFH_d: PFH_d/interruptores de seguridad (se basará en una evaluación en función del usuario) + PFH_d/sistema electrónico ASi-SaW ($<1 \times 10^{-8}$), por ejemplo, con 100 años de $MTTF_d = 3{,}47 \times 10^{-8}$, con 200 años = $2{,}19 \times 10^{-8}$, con 500 años aproximadamente $0{,}55 \times 10^{-8}$, etc.

  [2] con $MTTF_d$ “alta”
- Versión AZM 170 AS:
  Máx. sub-PL “d”[2], SIL 2[2], valor PFH_d: PFH_d/interruptores de seguridad (se basará en una evaluación en función del usuario) + PFH_d/sistema electrónico ASi-SaW ($<1 \times 10^{-8}$), por ejemplo, con 100 años de $MTTF_d = 3{,}47 \times 10^{-8}$, con 200 años = $2{,}19 \times 10^{-8}$, con 500 años aproximadamente $0{,}55 \times 10^{-8}$, etc.

  [2] con $MTTF_d$ “alta”
- Versión AZ 200 AS:
  Sub-PL “e”, sub-SIL 3, valor PFH_d: 4×10^{-9}
- Versión MZM 100 AS:
  Sub-PL “e”, sub-SIL 3, valor PFH_d: $<5 \times 10^{-9}$

Monitores ASi-SaW

- Versión ASM:
  Sub-PL “e”, sub-SIL 3, valor PFH_d: $9{,}1 \times 10^{-9}$
- Versión ASM G2:
  Sub-PL “e”, sub-SIL 3, valor PFH_d: $5{,}4 \times 10^{-9}$

Conexiones de interfaz ASi-SaW externas

- Versión ASi/Opto-Tube:
  Aportación al sub-PL “e”, aportación al sub-SIL 3, valor PFH_d: $<1 \times 10^{-8}$

¡Más información o respectivamente información actualizada en el catálogo online www.schmersal.net!

Combinación de varios sub-PL en un PL global

Combinación de varios sub-PL en un PL global

- Referencia: véanse páginas 12 y siguientes, así como páginas 53 y siguientes.

- En comparación con el método de bloques, la combinación de varios sub-PL (normalmente, sub-PL correspondientes a los niveles **I**, **L** y **O**) en un PL global en relación con una SRP/CS constituye un proceso muy sencillo.

- La norma EN ISO 13849-1:2006 incluye la denominada tabla de combinación (tabla 11 de la norma). En primer lugar, la tabla refleja la teoría del eslabón más débil de la cadena, aunque, cuando procede, también tiene en cuenta la adición de probabilidades de fallo residuales, es decir, que a partir de una determinada longitud de cadena, los valores de fiabilidad PFH_d o $MTTF_d$ podrían situarse por debajo de un valor límite crítico y afectar al PL global.

- En el lado izquierdo de la tabla puede leerse el número total de sub-PL_{bajo} ($> N_{bajo} \leq N_{bajo}$), es decir, el número del sub-PL más bajo, mientras que el PL global resultante puede leerse en el lado derecho. Una de las características de la tabla de combinación es que, a partir de un número determinado de sub-PL_{bajo}, se da una reducción de nivel. Esto se debe a la acumulación de probabilidades de fallo residuales (cuanto más larga sea la cadena, más elevado será el riesgo residual de fallo).

- ADVERTENCIA: la reducción en un PL no es obligatoria cuando, en un caso específico, las probabilidades de fallo residuales sean mejores que las asumidas por los autores de la norma al elaborar la tabla 11. En este caso se asume el valor medio.

PL_{bajo}	N_{bajo}	→	PL
a	>3	→	ninguno, no autorizado
	≤3	→	a
b	>2	→	a
	≤2	→	b
c	>2	→	b
	≤2	→	c
d	>3	→	c
	≤3	→	d
e	>3	→	d
	≤3	→	e

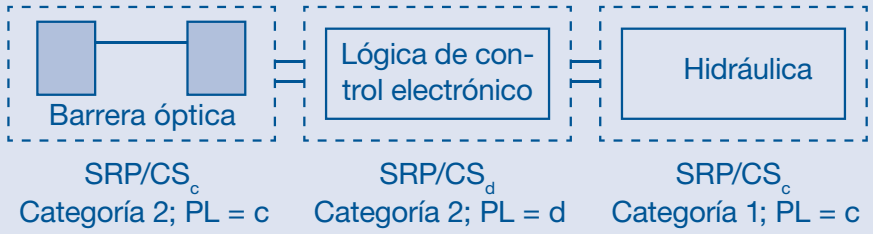
- Dicho de otro modo, en casos específicos debe calcularse lo siguiente:
  a) el sub-PL más bajo (PL_{bajo}) de la SRP/CS; y
  b) el número de sub-PL más bajos (N_{bajo}) presentes; y
  c) el PL global resultante.

- En un PL global “a” se toleran como máximo tres sub-PL_{bajo}, en los PL globales “b” y “c” se toleran como máximo dos sub-PL_{bajo} y en los PL globales “d” y “e” se toleran tres sub-PL sin que se produzca ninguna reducción de nivel, o viceversa: cuando en la SRP/CS pertinente haya más sub-PL_{bajo}, el PL global descenderá un nivel (por ejemplo: 3 × sub-PL “c” produce un PL global “b”).

- Importante: los sub-PL “superiores” de una SRP/CS no se contabilizan al utilizar la tabla de combinación (teoría del eslabón más débil). Esto mismo es de aplicación a los subsistemas y partes de una SRP/CS en los que se haya utilizado exclusión de defectos.

- Consejo: para poder utilizar la tabla de combinación también en circuitos complejos (sin demasiados problemas de reducción de nivel), se recomienda analizar de forma más minuciosa los circuitos en cuestión. En este caso, el objetivo consiste en analizar tan solo los subsistemas relevantes desde el punto de vista de la seguridad. Por tanto, no cabría analizar aquellas partes del subsistema que no estén relacionadas con la seguridad (por ejemplo, no todos los mecanismos de transmisión de un sistema tienen por qué plantear riesgos), y, por otra parte, los conjuntos de circuitos complicados también pueden incluir varias funciones de seguridad (véase también, en relación con este punto, el Excurso de la página 70 y siguientes).

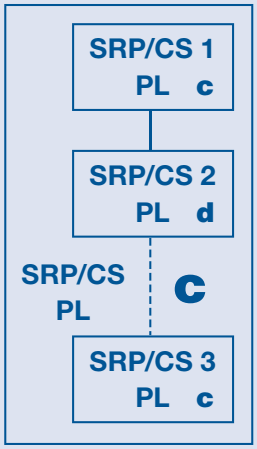
- **Ejemplo 1**
  (2 × sub-PL “c” = PL global “c”)



Ejemplo 1:

I	L	O	PL_{Ist}
PL “c”	PL “d”	PL “c”	PL “c”

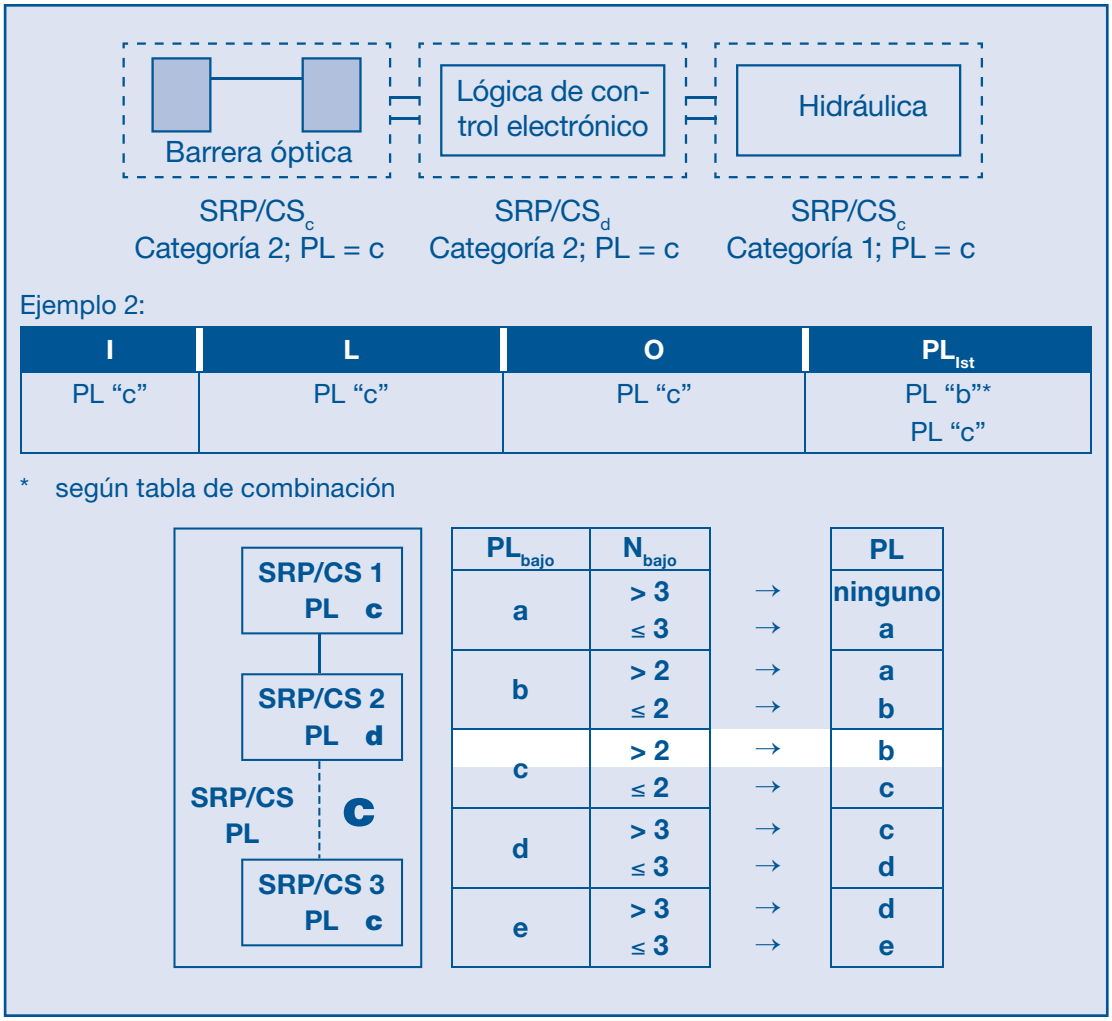
* según tabla de combinación
** véase siguiente figura



PL_{bajo}	N_{bajo}		PL
a	> 3	→	ninguno
	≤ 3	→	a
b	> 2	→	a
	≤ 2	→	b
c	> 2	→	b
	≤ 2	→	c
d	> 3	→	c
	≤ 3	→	d
e	> 3	→	d
	≤ 3	→	e

Este caso es el del ejemplo de uso de la tabla de combinación incluido en la norma. Se asume la existencia de una SRP/CS compuesta por 2 subsistemas con un PL “c” y un subsistema con un sub-PL “d”. En este caso, el sub-PL más bajo es “c”, que está presente dos veces, es decir, que la SRP/CS en su conjunto sigue poseyendo un PL “c”. La parte de la SRP/CS con un sub-PL “d” no se tiene en cuenta (porque es “superior”).

- **Ejemplo 2**
  Este ejemplo (3 × sub-PL “c”) pone de manifiesto el procedimiento en caso de reducción de nivel por ser necesario un PLr superior, en caso de que no se pueda o desee corregir este hecho.



Una SRP/CS puede componerse de tres subsistemas con 3 × sub-PL “c”. Según la tabla de combinación, esto produce una reducción del nivel hasta un PL global de “b”. En este caso deberían tenerse en cuenta los valores PFH_d individuales de cada subsistema, es decir, habría que sumarlos y comparar el resultado con el valor PFH_d requerido para el PL global “c”. En el anterior ejemplo, este valor es $\geq 1 \times 10^{-6} \ldots \leq 3 \times 10^{-6}$).

Cuando el valor PFH_d total se encuentre dentro del intervalo pertinente, no procede reducir el nivel, ya que los valores individuales son mejores que los asumidos por el legislador como modelo.

Cuando vaya a utilizarse este enfoque de forma simplificada con valores $MTTF_d$, el valor objetivo en relación con el PL global debería ser siempre “>30 años” ($MTTF_d$ “alta”).

La parte superior de la siguiente figura ilustra la posibilidad de que los valores no sean suficientes para alcanzar un PL “c”, mientras que en la parte inferior (variación 2) puede conseguirse un PL “c”.

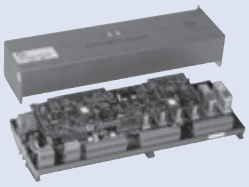
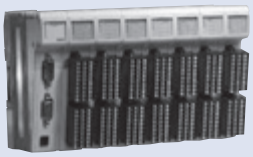
Suma y comparación de valores $MTTF_d/PFH_d$

- $MTTF_d$: >30 años (peor escenario)
- PFH_d: $>10^{-6} \ldots <3 \times 10^{-6}$

	I	L	O	PL_{Ist}	Comentarios
Alter-nativa 1:					
$MTTF_d$	50 años +	50 años +	50 años ≙	17 años	No es suficiente
PFH_d	$2{,}24 \times 10^{-6}$ +	$2{,}24 \times 10^{-6}$ +	$2{,}24 \times 10^{-6}$ ≙	$6{,}72 \times 10^{-6}$	
Alter-nativa 2:					
$MTTF_d$	200 años +	100 años +	100 años ≙	40 años	Justo suficiente
PFH_d	$\approx 0{,}7 \times 10^{-6}$ +	$1{,}14 \times 10^{-6}$ +	$1{,}14 \times 10^{-6}$ ≙	3×10^{-6}	

- **Ejemplo 3**
  Este ejemplo debe considerarse al margen de la tabla de combinación de EN ISO 13 849-1:2006, es decir, el "eslabón más débil de la cadena", y los valores PFH_d de la SRP/CS se consideran desde el principio. Este análisis corresponde, por ejemplo, a la norma EN IEC 62 061:2005.

Ejemplo 3:

I	L	O	SRP/CS
AZM 200	ESALAN-Compact	Sistema de transmisión con función de seguridad	PL_{Ist}
			Σ
PL "e"	PL "e"	PL "d"	PL "d"*
$4{,}3 \times 10^{-9}$ +	$0{,}5 \times 10^{-9}$ +	10×10^{-9}	= $14{,}8 \times 10^{-9}$ PFH_d**

* Determinado por el eslabón "más débil" de la cadena

** Comparar con el valor PFH_d límite, por ejemplo $>10^{-7} \ldots <10^{-6}$ con un PL "d"

- En cualquier otro caso (cuando haya un número de subsistemas sustancialmente superior al indicado en la tabla 11 de EN ISO 13 849-1:2006) deben tenerse en cuenta todos los subsistemas. Más concretamente, procede sumar sus probabilidades de fallo residuales (es decir, los valores PFH_d individuales) y compararlas con el valor PFH_d máximo aceptable en relación con el PL correspondiente; es decir, en este caso la norma es que el eslabón más débil (el sub-PL más bajo) determina el PL global. De forma alternativa también pueden sumarse valores $MTTF_d$, aunque en este caso el objetivo siempre debería ser un valor superior a 30 años.

- **Ejemplo**
  Una SRP/CS puede componerse de 6 subsistemas.
  – El sub-PL más bajo determina el PL global.
  – La suma de los valores PFH_d de los subsistemas debe situarse dentro de la categoría PL_r.

Nivel de prestaciones (PL)	Probabilidad media de fallo peligroso por hora (PFH_d)	máx. 1 fallo peligroso (tolerado) por
a	$\geq 10^{-5} \ldots < 10^{-4}$	10.000 horas
b	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	100.000 horas
c	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$	333.000 horas
d	$\geq 10^{-7} \ldots < 10^{-6}$	1.000.000 horas
e	$\geq 10^{-8} \ldots < 10^{-7}$	10.000.000 horas

PFH_d de subsistema 1 con PL "e"	I	p.e. 5×10^{-9}
+ PFH_d de subsistema 2 con PL "d"	I	p.e. 10×10^{-9}
+ PFH_d de subsistema 1 con PL "e"	L	p.e. 1×10^{-9}
+ PFH_d de subsistema 1 con PL "d"	O	p.e. 10×10^{-9}
+ PFH_d de subsistema 1 con PL "d"	O	p.e. 10×10^{-9}
+ PFH_d de subsistema 1 con PL "d"	O	p.e. 10×10^{-9}
= PL global = PL_{bajo} = "d"		**p.e. $4{,}6 \times 10^{-8}$**

¿De dónde deben extraerse los valores PFH_d en vez de robarlos?

- En caso de utilizarse en subsistemas dispositivos con funciones de seguridad más complejas a las que ya se haya asignado un sub-PL (o sub-SIL), normalmente los valores PFH_d también estarán disponibles en forma de información del fabricante. Para poder obtener un valor PFH_d a partir de estimaciones propias de sub-PL, podemos remitirnos al Anexo K de EN ISO 13849-1:2006, aunque tan solo llega a un valor $MTTF_d$ de 100 años. En caso de valores $MTTF_d$ superiores, tan solo es posible convertirlos a un valor PFH_d estimado de forma minuciosa (o prudente) (no olvide que se trata de una función logarítmica). En la actualidad se está elaborando una ampliación del Anexo K de EN ISO 13849-1:2006 (para valores $MTTF_d > 100$ años). Actualmente tan solo se dispone de cifras no oficiales: véase la entrada "Anexo K" del glosario).

- De acuerdo con la información facilitada por el BGIA, también es posible calcular la mitad del valor PFH_d de la categoría de PL correspondiente, cuando esto resulte útil (atención: función logarítmica), en el supuesto de que dispongamos de información relativa al PL de un subsistema pero no de la información de PFH_d correspondiente.

- Para facilitar adicionalmente los cálculos, parece razonable sumar los valores $MTTF_d$ y $MTTF_d$ de bloque ($PFH_d = 1/PFH_d : 8.760$) de acuerdo con el método de recuento de partes. En este caso, si queremos evitar una reducción de nivel, debemos obtener un $MTTF_d > 30$ años por canal como mínimo. Véase información incluida anteriormente.

Observaciones finales sobre el método del subsistema

- Como ya se ha mencionado en varias ocasiones, el método del subsistema está relacionado con la opción de cálculo simplificado de un PL global que se ofrece en la norma.

- No obstante, en casos específicos, esta simplificación puede conllevar que, al aplicar el método del subsistema, obtengamos una estimación de PL global inferior a la que tendríamos si utilizásemos el método de bloques. Más concretamente, esto se debe al uso sistemático de la filosofía del eslabón más débil en la cadena de subsistemas. Por el contrario, con el método de bloques los parámetros específicos pertinentes se consideran en su conjunto (con el valor $MTTF_d$) o como una media (con la cobertura del diagnóstico DC), es decir, que hasta cierto punto es posible compensar los valores individuales más bajos con otros valores más elevados.

- Ejemplo: una función de seguridad se compone de un subsistema con un sub-PL “c” y de varios otros subsistemas con sub-PL “e” (= PL global “c” aplicando el método del subsistema y de acuerdo con la filosofía del eslabón más débil de la cadena de subsistemas). Por otra parte, si utilizamos el método de bloques para obtener una estimación global, es posible que obtengamos un PL global de “d”, dependiendo de la configuración de los valores individuales. Este resultado se situaría dentro del margen de maniobra previsto en la norma.

- Los principios matemáticos subyacentes a la norma también pueden generar resultados absurdos (paradojas). Por ejemplo, los aumentos de valores $MTTF_d$ pueden producir aritméticamente una DC_{avg} inferior debido al suministro de equipos de mejor calidad, incluso cuando las partes individuales de la SRP/CS estén sujetas a la misma cobertura del diagnóstico. También podrían darse casos en sentido inverso. Por este motivo, se recomienda realizar las correcciones pertinentes haciendo uso tanto del sentido común como de los conocimientos profesionales.

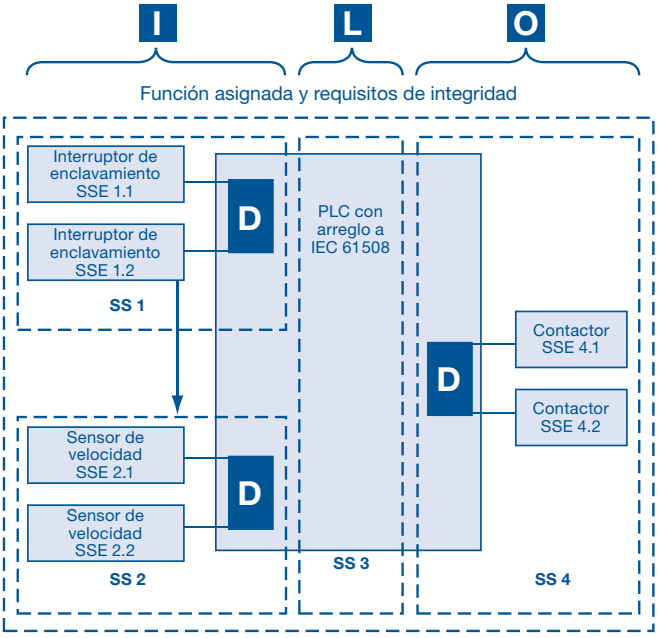
Confusión, ¡pero de alto nivel!

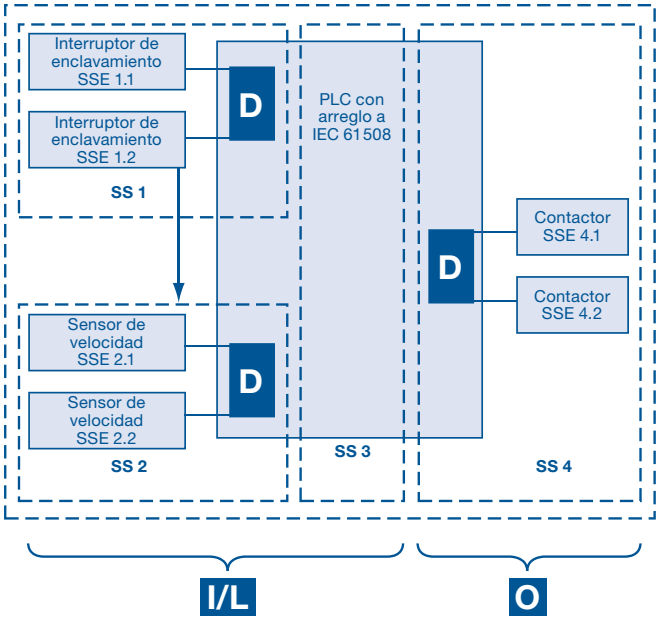
¿Cómo calcular el PL de un subsistema (un sub-PL)?

- ADVERTENCIA: los siguientes ejemplos de conexión están relacionados fundamentalmente con el nivel de entrada, es decir, con qué sub-PL o sub-SIL puede conseguirse en la SRP/CS en relación con dispositivos únicos sencillos combinados con un procesamiento de señal corriente abajo.
- En los módulos SRB normalmente es de aplicación una cobertura del diagnóstico DC del 99 % (debido a la comprobación de los dos relés de canal con direccionamiento positivo); esta DC del 99 % también es de aplicación a los PLC de seguridad (debido a la comparación cruzada de datos altamente dinámica de los dos sistemas de microordenador del dispositivo). El sistema de mando de 2 canales es un prerequisito. Los dos valores de DC derivan del Anexo E de EN ISO 13849-1:2006.
- En el caso de dispositivos electromagnéticos conectados en serie que se sitúen corriente arriba con respecto al nivel de entrada de un módulo SRB o PLC de seguridad, debe considerarse una cobertura del diagnóstico alternativa. En este caso, hasta nuevo aviso, utilizaremos una DC limitada del 60 % = “baja” (véase página 32 f.).
- Cualquier otro tipo de procesamiento de señal corriente abajo de dispositivos únicos sencillos requiere una evaluación especial (véase también el Anexo E de EN ISO 13849-1:2006). En este caso, no debe olvidarse que en una SRP/CS pueden utilizarse varias medidas de exclusión de defectos (por ejemplo mediante módulos SRB, PLC de seguridad etc., así como medidas relativas a equipos de ensayo [TE], como por ejemplo PLC operativos). Véase el ejemplo de la página 76.

Existen dos posibilidades para obtener un sub-PL:

- La primera posibilidad consiste en obtener un sub-PL para la función “dispositivo único sencillo + diagnóstico” (a través del procesamiento de señal posterior). En este caso se consideraría la parte del conjunto de circuitos de conmutación de un módulo SRB o un PLC de seguridad que realice la función de detección de defectos en el nivel de entrada, para que el análisis tan solo concierna al nivel **I**. Todos los elementos posteriores (niveles **L** + **O**) deben ser objeto de un análisis de sub-PL independiente. Esto es lo que la norma trata de explicar con la siguiente figura (véase figura, etiquetas de la parte superior).





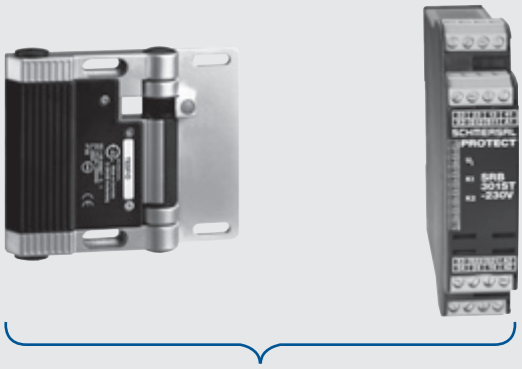
- La segunda posibilidad consiste en obtener un sub-PL para la combinación de dispositivos “dispositivo único sencillo + módulo SRB o PLC de seguridad”, de forma que se combinen los niveles **I** + **L** (véase figura, etiquetas de la parte inferior). No obstante, en el caso de módulos SRB, esto también requeriría conocimientos relativos al nivel de salida **O** para poder realizar una estimación aproximada del valor B_{10d}, ya que el relé está sujeto a desgaste natural.

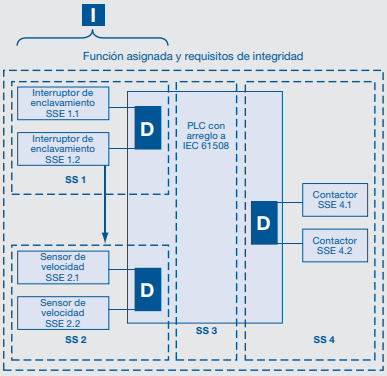
Las siguientes observaciones son de aplicación al margen de que se opte por la primera o por la segunda posibilidad:

- Se requiere una evaluación más diferenciada en relación con la cobertura del diagnóstico del circuito de retroalimentación de los elementos de activación situados corriente abajo (normalmente esto corresponde al cliente). Aunque las medidas ya mencionadas (DC: 99%, véase más arriba) también tendrían efecto en este caso, la DC obtenida con dispositivos únicos sencillos en el subsistema del “nivel de salida” **O** depende de la calidad de la señal de retroalimentación desde el punto de vista de la seguridad. Aunque puede asumirse una DC del 99% en el caso de contactores con contactos con direccionamiento positivo, este porcentaje será inferior cuando la señal se origine en contactos con direccionamiento positivo. Entre otras cosas, dependerá de si el nivel de salida se incorpora al proceso normal, y con qué frecuencia, y por tanto debe comprobarse en condiciones normales de funcionamiento (es decir, no en condiciones críticas para la seguridad). Estos análisis los debe realizar el propio cliente, con la ayuda del Anexo E de la norma EN ISO 13849-1:2006 (DC = >60 % ... <99 %).
- Recuerde que la cobertura del diagnóstico puede incrementarse cuando puedan incorporarse en el análisis las señales de retroalimentación derivadas de la parte operativa del sistema de mando (véase la mención a “equipos de ensayo” en este documento). En el Anexo E de EN ISO 13 849-1:2006 se incluye información relativa a la eficacia de estas medidas adicionales.
- Cuando se utilice exclusión de defectos en relación con un subsistema completo (véase página 32 f.), como por ejemplo en el caso de dispositivos de seguridad activados de forma manual (parada de emergencia, Interruptores de validación, etc.), no es necesario analizar el subsistema (véase la sección “Ejemplos de conexión del BGIA”, en la página 76). No obstante, se recomienda hacer uso de la máxima prudencia en este caso.

Ejemplo 1[1]

Debe protegerse una puerta de guarda de una valla de seguridad que rodea un sistema robótico haciendo uso de un interruptor TESF. Se produce el siguiente procesamiento de señal con un módulo de relé de seguridad de la gama SRB PROTECT, con una CC 4.





Ejercicio: ¿de qué sub-PL dispone el nivel de entrada del "interruptor TESF"?

Los interruptores TESF son dispositivos únicos sencillos con su propia función de diagnóstico. El diagnóstico tiene lugar en el módulo SRB corriente abajo. Por tanto, se realiza un análisis tanto del propio interruptor TESF como de la función de diagnóstico del módulo SRB, que se aplica a la detección de defectos en el nivel de entrada (interruptor TESF). Por consiguiente, esta función constituye (solo en **I**) la base de nuestro análisis de sub-PL (en el Ejemplo 3 se abordan las combinaciones de dispositivos **I** + **L**).

Aspecto 1:
¿de qué arquitectura se dispone (qué exclusiones de fallos deben considerarse)?

- Desde un punto de vista físico, un interruptor TESF es un interruptor, pero con dos contactos NC de apertura positiva independientes (canales). La realización del movimiento giratorio de la puerta de guarda en la activación de pistón de ambos canales tiene lugar utilizando un mecanismo de 1 canal (eje activador), pero en el interior del dispositivo, es decir, con protección y sin tensiones. Utilizamos exclusión de defectos en esta pequeña parte de 1 canal. Dicho de otro modo: la arquitectura del interruptor TESF es de 2 canales.

- La instalación de la conexión entre el interruptor TESF y el módulo SRB goza de protección o se realiza con cable protegido independiente (con exclusión de defectos en el cableado, de lo contrario se requiere control cruzado del módulo SRB).

- La conexión del interruptor TESF con el módulo SRB se realiza mediante conexión 1:1 de 2 canales siguiendo un ejemplo de conexión relativo a la CC 4 (sin conexión en serie).

POR TANTO: la arquitectura del subsistema **I** lleva asociada una CC 4.

[1] Posteriormente se realiza el análisis y la validación del PL_r requeridos anteriormente cuando, en retrospectiva, $PL_{Ist} > PL_r$; ≥ no se considera.

Aspecto 2: ¿de qué fiabilidad de equipo $MTTF_d$ se dispone?

Los interruptores TESF son dispositivos únicos sencillos sujetos a desgaste natural y, por tanto, llevan asociado un valor B_{10d} de 2.000.000. De acuerdo con el ejemplo de cálculo de la página 23, esto resulta en un valor $MTTF_d$ de 2.381 años por canal.

POR TANTO, se dispone de una fiabilidad de equipo $MTTF_d$ “alta”.

Aspecto 3: ¿de qué cobertura del diagnóstico DC se dispone?

La función de detección de defectos del interruptor TESF está sujeta al siguiente SRB PROTECT con una DC del 99 % (véase página 32 f.)

POR TANTO, se dispone de una cobertura del diagnóstico “alta”.

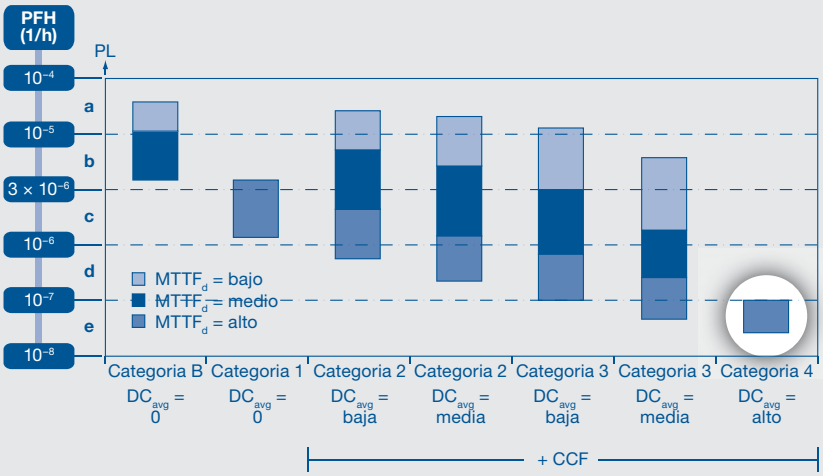
Aspecto 4: ¿qué medidas CCF se han tomado?

Siempre podemos asumir >65 puntos en los componentes de seguridad incorporados e instalados correctamente. Para más información, véase la entrada “CCF” del glosario.

POR TANTO: se han tomado suficientes medidas CCF (CCF: OK).

Resumen de acuerdo con el gráfico de barras

- Arquitectura (CC): 4
- $MTTF_d$: alta
- DC: alta
- CCF: OK



POR TANTO: Nivel de prestaciones “e”

Ejemplo 2[1]

Igual que el anterior, pero con varios interruptores TESF en serie.

Ejercicio: ¿de qué sub-PL dispone el nivel de entrada del “interruptor TESF”?

Se asume que, en un punto específico en el tiempo X, tan solo se requiere la función de seguridad de un interruptor TESF (de forma que en un momento determinado tan solo hay abierta una puerta de guarda). Por tanto, existe un número respectivo de funciones de seguridad correspondiente al número de interruptores TESF de la valla de seguridad, por ejemplo tres dispositivos realizarán tres funciones de seguridad diferentes.

Dicho de otro modo: no debe sumarse la probabilidad de fallos residual de los interruptores TESF. Como resultado, el análisis de sub-PL debe basarse en la combinación “1 × interruptor TESF/diagnóstico SRB”.

En todo lo demás: véase el ejemplo anterior, Ejemplo 1.

Aspecto 1:
¿de qué arquitectura se dispone (qué exclusiones de fallos deben considerarse)?

- En primer lugar: ver ejemplo anterior Ejemplo 1, aunque debido a la conexión en serie no pueden detectarse todos los fallos, es decir, que no puede excluirse la posibilidad de una acumulación de fallos. Por tanto, se trata de una arquitectura sin potencial de autocontrol total (2 canales, pero con detección de defectos limitada).

POR TANTO: la arquitectura del subsistema lleva asociada una CC 3.

[1] Posteriormente se realiza el análisis y la validación del PL_r requeridos anteriormente cuando, en retrospectiva, $PL_{Ist} > PL_r$; ≥ no se considera.

Aspecto 2: ¿de qué fiabilidad de equipo $MTTF_d$ se dispone?

Todos los interruptores TESF conforman una función de seguridad.

Para calcular el valor $MTTF_d$ asumimos que todas las puertas de guarda están abiertas 2 × por hora, es decir, que queda un valor $MTTF_d$ de 2.381 años. Si asumiésemos que, de forma opcional, la exigencia de 2 × por hora hace referencia a todas las puertas de guarda del perímetro, los valores MTTFd aumentarían de forma significativa de nuevo (no obstante, debido al límite de 100 años por canal, esto no afectaría en modo alguno al PL).

En todo lo demás: véase el ejemplo anterior.

POR TANTO, se dispone de una fiabilidad de equipo $MTTF_d$ “alta”.

Excurso: cuando deban considerarse varios interruptores TESF en relación con una función de seguridad porque siempre haya abierta más de una guarda durante el funcionamiento, deben sumarse los valores $MTTF_d$ de los dispositivos (aplicando el método de recuento de partes). En este caso, el resultado de la suma determinará la clasificación de $MTTF_d$. No obstante, se apreciará que, debido a las elevadas $MTTF_d$ individuales, sería necesario un mayor número de dispositivos para llegar a una reducción de categoría, como por ejemplo a un valor $MTTF_d$ “medio”. En este caso la cobertura del diagnóstico del 60 % no se ve modificada.

Aspecto 3: ¿de qué cobertura del diagnóstico DC se dispone?

Dado que en las conexiones en serie de dispositivos únicos sencillos no puede excluirse la posibilidad de una acumulación de fallos, tras consultar al BGIA asumimos una DC “baja” (véase página 32 f.) cuando ninguna otra medida resulte efectiva, como por ejemplo la realización de una función adicional de detección de defectos a través de un equipo de ensayo externo (véase: “Integración del PLC en condiciones de funcionamiento normales”) o la realización de exclusiones de fallos.

En todo lo demás: véase el ejemplo anterior.

POR TANTO, se dispone de una cobertura del diagnóstico “baja”.

Aspecto 4: ¿qué medidas CCF se han tomado?

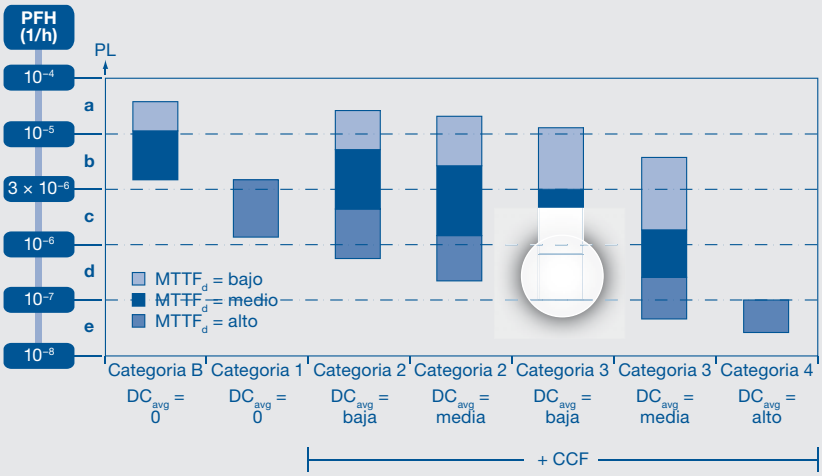
Véase ejemplo anterior.

POR TANTO se han tomado suficientes medidas CCF (CCF: OK).

Resumen de acuerdo con el gráfico de barras

- Arquitectura (CC): 3
- $MTTF_d$: alta
- DC: baja
- CCF: OK

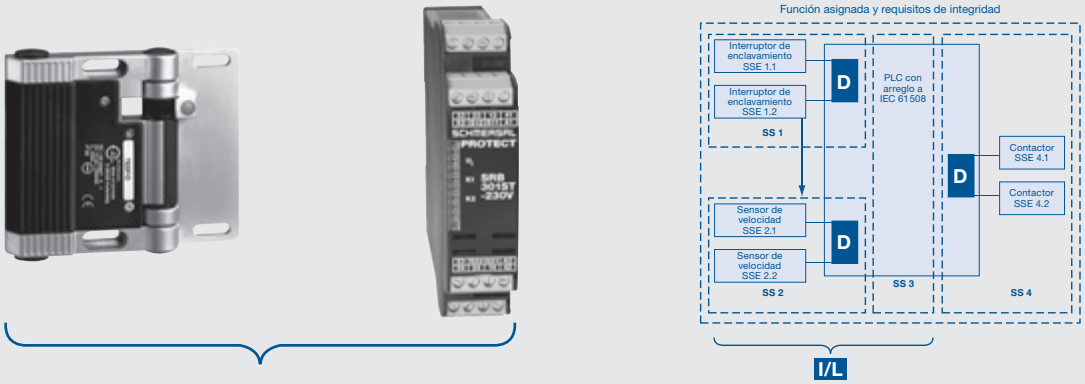
POR TANTO: Nivel de prestaciones “d”



Ejemplo 3[1]

Ejercicio

Combinamos el nivel de entrada y el nivel de procesamiento de señal, es decir, la parte de la SRP/CS hasta el nivel de contacto activador del módulo SRB, para crear una combinación de dispositivos.



Aspecto 1: ¿de qué arquitectura se dispone (qué exclusiones de fallos deben considerarse)?

De forma adicional al interruptor TESF con diagnóstico SRB del nivel de entrada I , debe analizarse el nivel de procesamiento de señal **L** del propio módulo SRB.

En el caso de un módulo SRB, este nivel se corresponde con un dispositivo con funciones de seguridad más complejas ya evaluado y con un sub-PL (o sub-SIL) incorporado (en nuestro ejemplo, con sub-PL “e” o sub-SIL 3).

POR TANTO, no es necesario realizar análisis individuales de la arquitectura, la $MTTF_d$[2], la DC y las medidas CCF en relación con el módulo SRB (porque ya están reflejadas en el sub-PL o sub-SIL). En este caso se asume que la frecuencia de conmutación y la carga de conmutación del relé no afectan a una $MTTF_d$ “alta”.

[2] Debería realizarse un análisis aproximado para comprobar si el número de ciclos de trabajo y la carga de conmutación afectan a la clasificación de $MTTF_d$ por utilizarse tecnología sujeta a desgaste natural en el relé. También debe tenerse en cuenta la carga de conmutación en el nivel de activación de los módulos SRB. No obstante, esta tan solo sería crítica con un número elevado de ciclos de trabajo y una carga de conmutación alta (véanse valores B_{10d} de los relés).

[1] Posteriormente se realiza el análisis y la validación del PL_r requeridos anteriormente cuando, en retrospectiva, $PL_{Ist} > PL_r$; ≥ no se considera.

Resumen

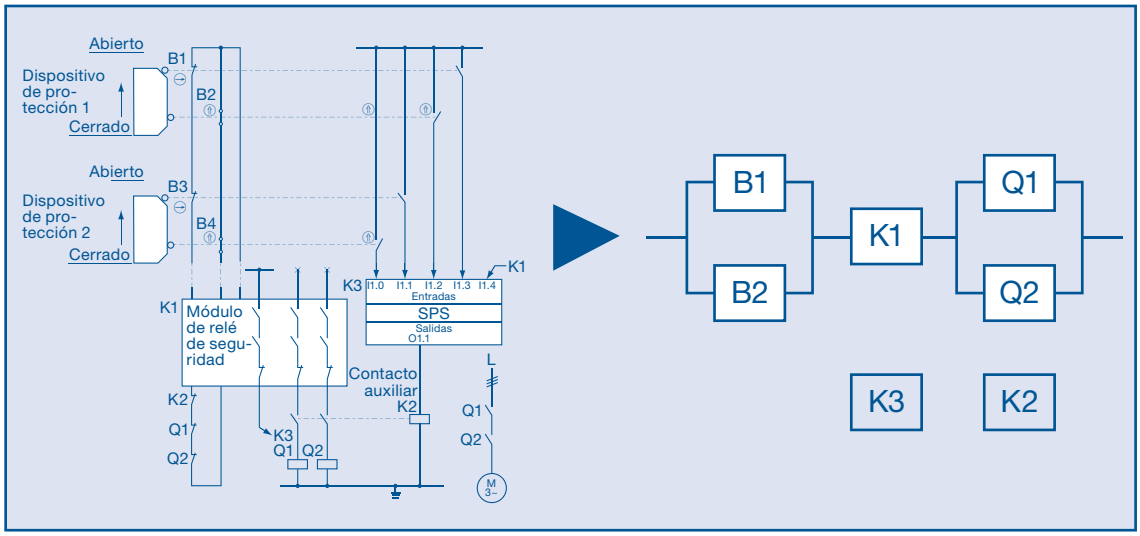
De acuerdo con la tabla de combinación (véanse páginas 45 y siguientes), con la conexión 1:1 se obtiene un sub-PL “e” en relación con la combinación de dispositivos* en su conjunto (2 × “e” sigue siendo “e”), y en caso de conexión en serie un sub-PL “d” (determinado por el eslabón más débil de la cadena).

No obstante, también sería razonable combinar los niveles I y L en un subsistema de “clasificación superior” [teniendo en cuenta un valor B_{10d} adicional en relación con el relé del módulo SRB, véase[2]].

[1] Debería realizarse un análisis aproximado para comprobar si el número de ciclos de trabajo y la carga de conmutación afectan a la clasificación de $MTTF_d$ por utilizarse tecnología sujeta a desgaste natural en el relé. También debe tenerse en cuenta la carga de conmutación en el nivel de activación de los módulos SRB. No obstante, esta tan solo sería crítica con un número elevado de ciclos de trabajo y una carga de conmutación alta (véanse valores B_{10d} de los relés).

¿Cómo calcular un sub-PL con dispositivos del programa Schmersal/Elan?

Como es lógico, las siguientes medidas (con las consideraciones adicionales pertinentes) deben ir precedidas de un análisis de la conexión (véanse páginas 70 y siguientes) y de la transferencia de la conexión a un diagrama de bloque.



Sub-PL del nivel de entrada I

- Cableado:
  Exclusión de defectos conforme a EN ISO 13 849-2:2003 o control cruzado (véase también la entrada “Exclusión de defectos: conexión/cableado” del glosario).

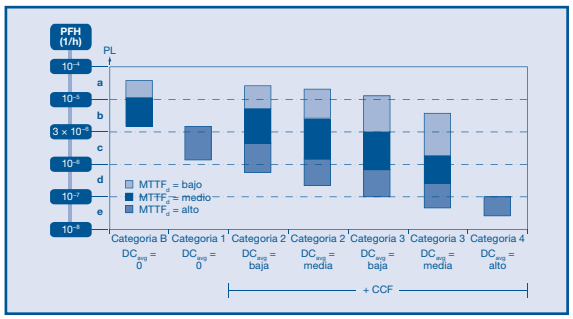
- Definición de la arquitectura, es decir, qué categoría de control se consigue en el nivel de entrada (véase figura anterior).

- Definición del valor $MTTF_d$ por canal (normalmente mediante una consideración de valor B_{10d}, véanse páginas 22 y siguientes)

- Definición de la DC de los módulos SRB y del PLC de seguridad:
  – 99 % con conexión 1:1
  – 60 % con conexión en serie (independiente de la definición de la función de seguridad)
  – cuando proceda, incorporar la cobertura del diagnóstico de un TE (véase página 32 f.)

- Gestión de CCF:
  >65 puntos (véase entrada “CCF” del glosario)

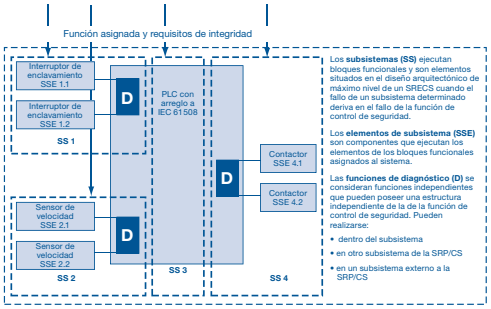
  = Sub-PL de acuerdo con el resultado del diagrama (véase figura) o con el Anexo K de EN ISO 13 849-1:2006



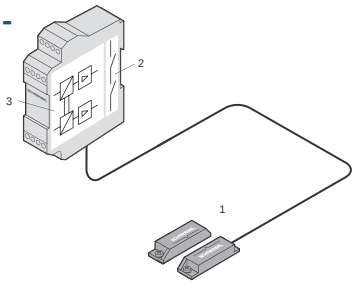
Conclusión esquemática

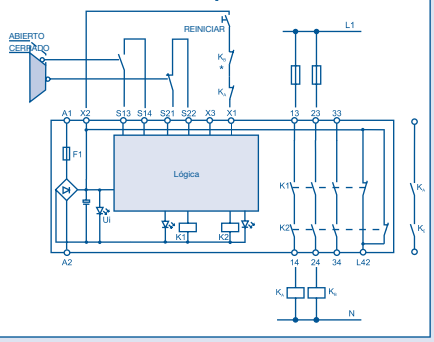
Estimación de sub-PL modular (diferenciada)

Necesaria cuando se realicen diagnósticos (y por tanto haya cobertura del diagnóstico correspondiente a la detección de defectos, DC) en una parte posterior o subsiguiente de la SRP/CS

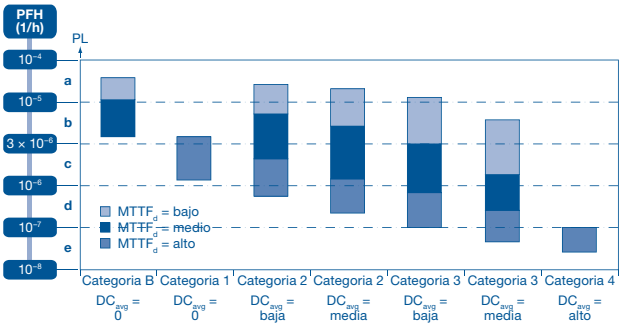


por ejem-plo:





Sub-PL



Arquitectura designada (categoría de control):
- ¿1 canal?
- ¿2 canales?
- ¿Prestaciones de CC 4?[1]

Fiabilidad de equipo $MTTF_d$: Calcular mediante un análisis del valor B_{10d} cuando proceda

Cobertura del diagnóstico DC:
- ≥99 % con conexión 1 : 1[2]
- 60 % con conexión en serie
- La DC (como se ha mencionado) se realiza a través de SRB o controladores de seguridad con CC 4

Medidas contra fallos de causa común (CCF): >65 puntos

[1] remítase a los ejemplos de conmutación de los sistemas SRB o PLC
[2] ATENCIÓN: DC de 99 % tan solo en el circuito de retroalimentación, cuando las señales sean generadas por contactores con contactos con direccionamiento positivo, de lo contrario inferior (véase Anexo E de EN ISO 13849-1:2006)

Sub-PL del nivel lógico (nivel de procesamiento de señal) L

- Sub-PL o sub-SIL: véase dispositivo correspondiente. Como ya se ha descrito, esto afecta a dispositivos con funciones de seguridad más complejas que ya posean un sub-PL o sub-SIL integrado.

Sub-PL del nivel de salida O

- Procedimiento similar al nivel de entrada (no obstante, para más información sobre posibles valores de DC diferentes, véase EN ISO 13849-1:2006, Anexo E). Por tanto, esto es competencia del cliente.

Excurso

Excurso: detección de fallos

La detección de fallos posee una importancia especial en una SRP/CS por dos motivos:

- Aunque en las arquitecturas de canal múltiple un primer defecto puede no ser crítico desde el punto de vista de la seguridad (debido a la redundancia o a la tolerancia de fallos del equipo), es necesario detectar los fallos y que estos generen un obstáculo operativo que evite la acumulación de defectos. En caso de producirse nuevos fallos tras un fallo no detectado, esto podría conducir a una situación de peligro inaceptable par este tipo de arquitecturas.

- Por suerte, sin embargo, también en el caso de arquitecturas sencillas, no todas las situaciones peligrosas derivadas de un fallo provocan de forma directa un accidente, y en este sentido la detección de fallos tiene el efecto de evitar el riesgo de que se den situaciones peligrosas repetitivas.

- En el Anexo E de EN ISO 13849-1:2006 se enumeran las medidas habituales de detección de fallos y el alcance del efecto deseado, en forma de cobertura del diagnóstico (clasificadas en medidas para la unidad de entrada, la lógica y la unidad de salida).

- Para no tener que realizar el cálculo uno mismo, la norma EN ISO 13849-1:2006 incluye tablas de consulta con medidas típicas y evaluaciones porcentuales (debe realizarse una estimación cuando sea necesario).

Medida	Cobertura del diagnóstico (DC)
Dispositivo de entrada	
Estímulo cíclico de comprobación mediante cambio dinámico de las señales de entrada	90 %
Comprobación, por ejemplo utilización de contactos normalmente abiertos y normalmente cerrados, guiados mecánicamente	99 %
Control cruzado de señales de entradas sin comprobación dinámica	0 % a 99 %, dependiendo de la frecuencia con la que la aplicación cambia

Medida	Cobertura del diagnóstico (DC)
Lógica	
Control indirecto (por ejemplo, control mediante un presostato, control eléctrico de la posición de los actuadores)	90 % a 99 %, dependiendo de la aplicación
Control directo (por ejemplo, control eléctrico de la posición de los distribuidores de mando, control de los dispositivos electromagnéticos mediante elementos de contacto unidos mecánicamente)	99 %

Medida	Cobertura del diagnóstico (DC)
Dispositivos de salida	
Control de salidas mediante un canal sin comprobación dinámica	0 % a 99 %, dependiendo de la frecuencia con la que la aplicación cambia la señal
Control cruzado de señales de salida sin comprobación dinámica	0 % a 99 %, dependiendo de la frecuencia con la que la aplicación cambia la señal
Control cruzado de señales de salida con comprobación dinámica, sin detección de cortocircuitos (para I/O múltiples)	90 %

- De forma adicional las medidas o combinación de medidas para la detección de fallos (y por tanto del efecto deseado de cobertura del diagnóstico) depende en gran medida de la arquitectura de la SRP/CS.

- No existe la posibilidad de detección de fallos en arquitecturas sencillas de un canal (= DC 0), ya que no hay ninguna “inteligencia” corriente abajo o de categoría superior que pueda realizar esta función.

- La mejor opción para el nivel de entrada I es una capacidad de 2 canales y un procesamiento de señal posterior mediante módulos SRB o PLC de seguridad en combinación con una conexión 1:1 (o comparable), ya que en este caso tiene lugar una denominada comparación a prueba de fallos, en la que se comprueba la coherencia de los canales (por ejemplo, cerrar ambos canales en caso de “disposición de los contactos NC” durante la inicialización de la máquina). Por tanto, esto corresponde a una DC del 99 % (véase Anexo E de EN ISO 13 849-1:2006). En el caso de las arquitecturas sencillas de 1 canal, como es lógico, no se dispone de esta referencia comparativa. Al mismo tiempo, como es evidente, la capacidad de 2 canales también cubre el denominado requisito de tolerancia a 1 fallo de las categorías de control 3 y 4; véase entrada “Categorías de control” del glosario.

- También ofrecen posibilidades de comprobación la capacidad eléctrica de 2 canales o la inclusión de señales de retroalimentación del PLC (con comprobación posterior) o bien, típicamente en los contactores corriente abajo, la lectura inversa de las señales de retroalimentación en el recorrido de reinicio del SRP/CS. Por tanto, un circuito de retroalimentación de contactos con direccionamiento positivo también genera una DC del 99 %.

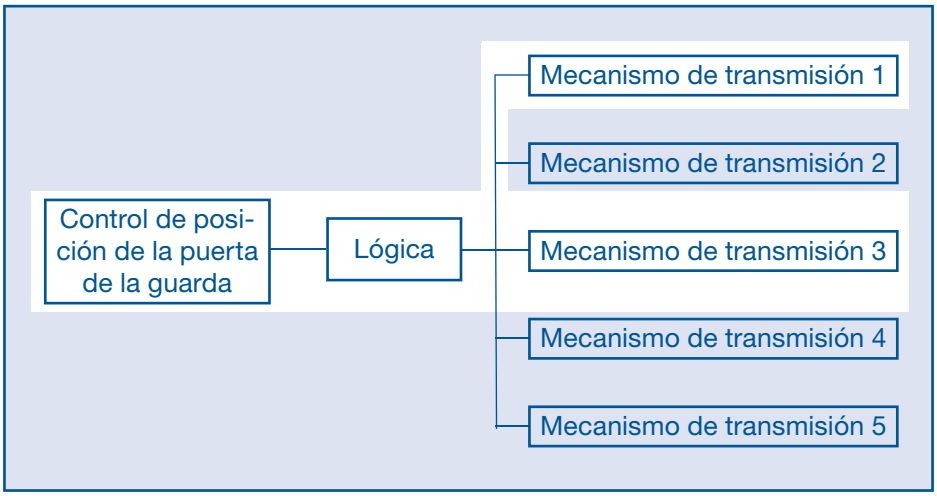
- Para más información sobre la cobertura del diagnóstico: véanse páginas 32 f. y 68 f.

Excurso: Influencia de la definición de la función de seguridad sobre el cálculo del PL – ejemplos

- La definición de qué es una función de seguridad y qué equipos físicos y quizás software se enmarcarían en dicha definición condiciona el alcance del análisis del PL. Lo más importante es saber qué partes del sistema de mando se ven implicadas cuando se produce una solicitud de la función de seguridad y por tanto son “responsables” de la función de protección para las personas. Esto se explica en mayor detalle mediante los siguientes ejemplos (fuente: Informe 2/2008 del BGIA, véase glosario).

Ejemplo 1: Función de seguridad “apagado al abrirse la puerta de una guarda”

- Al abrirse la puerta de la guarda, el operador de la máquina accede a una zona peligrosa en la que cinco mecanismos de transmisión controlan los movimientos de una máquina. La apertura de la puerta de la guarda provoca el apagado de los cinco mecanismos de transmisión con la mayor rapidez posible.



- Por consiguiente, los PL de los siguientes bloques (los respectivos bloques llevan asignadas probabilidades de fallo de la instalación eléctrica) están relacionados al realizar el cálculo posterior del PL de la función de seguridad:
  – Control de posición de la puerta de una guarda, incluidos los componentes mecánicos
  – Lógica
  – Mecanismo de transmisión x (x = 1, 2, ... 5)

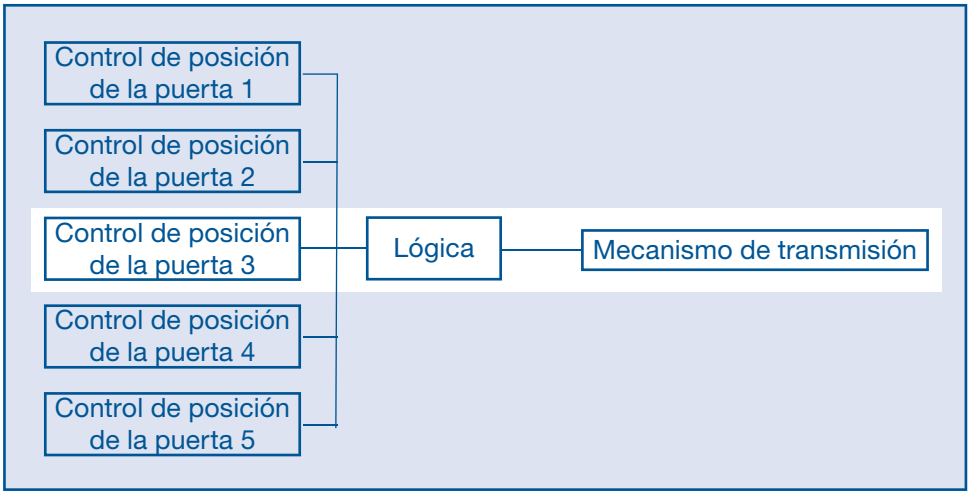
- El resultado puede ser un PL que ya no sea suficiente para la aplicación, aunque quizás tan solo los mecanismos de transmisión 1 y 3 activen movimientos peligrosos para el operador y los demás se apaguen meramente por motivos “funcionales”. En este caso, se recomienda considerar únicamente los movimientos de la función de seguridad que supongan un peligro real.

Ejemplo 2: Función de seguridad “apagado al abrirse una puerta de guarda”

- Una valla con cinco puertas protege un movimiento peligroso. La apertura de una de las puertas provoca el apagado. A efectos del cálculo posterior del PL, cada puerta constituye el componente de su propia función de seguridad, SF1 a SF5, que se compone de los siguientes bloques (los respectivos bloques llevan asignadas probabilidades de fallo de la instalación eléctrica):

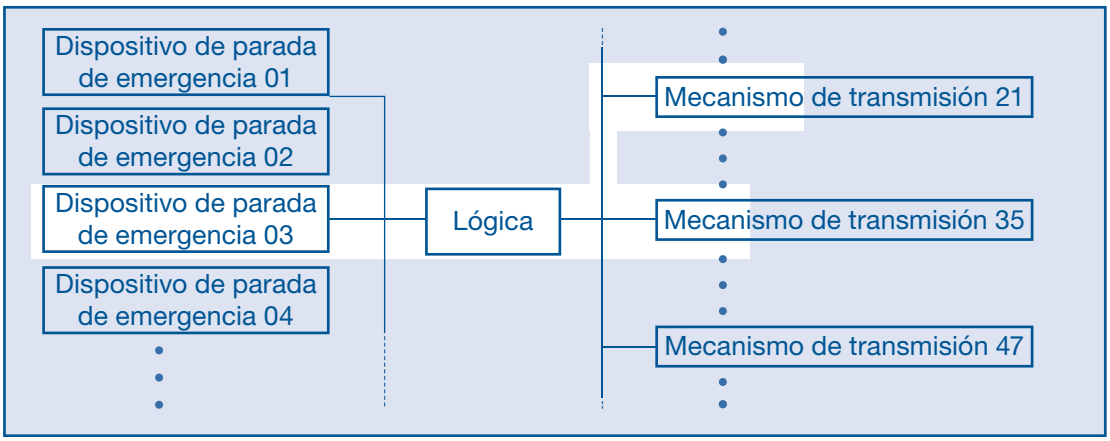
– Control de posición de las puertas x (x = 1, 2, ... 5), incluidos los componentes mecánicos
– Lógica
– Mecanismo de transmisión

- En la figura se muestra el diagrama de circuito funcional y los bloques de la función de seguridad SF3:



Ejemplo 3: Función de seguridad “parada de emergencia de una máquina en su totalidad”

- Una máquina de grandes dimensiones tiene instalados 20 dispositivos de parada de emergencia, cuya activación apaga los 50 mecanismos de transmisión existentes con la mayor rapidez posible. En este caso, ¿qué componentes deben tenerse en cuenta al realizar la función de seguridad? No puede preverse qué dispositivo de parada de emergencia se activará para ejecutar la función de seguridad. Dado que el operador tan solo activa un único dispositivo de parada de emergencia a la vez, se definen las funciones de seguridad SF1 a SF20. Aunque no se conoce la ubicación de la persona sometida a la situación de peligro al activarse la parada de emergencia, con independencia de su ubicación no todos los 50 mecanismos de transmisión generarán una situación de peligro. Por este motivo, debe considerarse el escenario menos favorable para que estén representadas todas las situaciones imaginables. Este viene determinado por el peor PL, y por tanto depende, entre otras cosas, del número de mecanismos de transmisión en la cadena de seguridad que generen movimientos peligrosos en la ubicación menos favorable, así como de los respectivos PL individuales.



- En el cálculo posterior del PL relativo a la función de seguridad deben tenerse en cuenta los valores PL de los siguientes bloques:
  - Dispositivo de parada de emergencia 03
  - Lógica
  - Mecanismo de transmisión 21
  - Mecanismo de transmisión 35
  - Mecanismo de transmisión 47

- Los ejemplos ponen de manifiesto que, al definir una función de seguridad, se recomienda adoptar una “perspectiva local” que tenga en cuenta lo siguiente:
  - ¿En qué ubicación se encontrarán las personas en el momento considerado?
  - ¿Qué movimientos son peligrosos en la ubicación de la persona o personas?
  - ¿Qué dispositivos de protección debe activar la función de seguridad? Cuando proceda, debe considerarse el uso de varios dispositivos de protección alternativos.

Observaciones desde la perspectiva de Schmersal/Elan, sobre todo en relación con el Ejemplo 2:

- En el futuro deberemos adoptar un nuevo enfoque[1] de acuerdo con el cual una conexión eléctrica en serie puede componerse de varias funciones de seguridad y la evaluación del PL o SIL hace referencia a la función de seguridad única. Esto quiere decir (véase siguiente ejemplo) que la conmutación de 5 puertas de guarda en serie puede suponer la consideración individual de 5 funciones de seguridad y, por tanto, 5 evaluaciones individuales.

[1] Aunque en realidad este también se incluía en EN 954-1, en esta norma no se formuló de forma clara.

- En este ejemplo se asume que, en un momento específico, tan solo se solicita la función de seguridad de forma simultánea desde un dispositivo de protección por parte de un operador, es decir, que tan solo se abre de forma simultánea uno de los 5 dispositivos de protección o tan solo se activa un dispositivo de control de parada de emergencia en una serie de varios dispositivos de control de parada de emergencia.

- Este enfoque simplifica de forma considerable el uso de la nueva normativa, ya que la cadena de SRP/CS objeto de análisis se “acorta”. Sin embargo, esto tan solo es posible cuando existe una independencia real entre las funciones de seguridad individuales, es decir, que no podría adoptarse, por ejemplo, en el caso de una puerta doble.

- Debe considerarse el riesgo de eliminar un fallo en conexiones en serie de dispositivos electromagnéticos en SRP/CS (véase entrada “Conexiones en serie” del glosario, y las referencias a este concepto en el presente documento) en el marco de la función de seguridad correspondiente. Hasta nuevo aviso, presuponemos que en este caso tan solo puede asumirse un valor de DC “bajo” (= 60 %).

- Nuestro argumento anterior de que es posible conectar en serie hasta 31 dispositivos de la familia CSS sin reducción de la clasificación (véase: Suma de probabilidades de fallo residuales) ya no es tan estricto. Lo considerado hasta ahora implica que ahora puede conectarse en serie una cantidad considerablemente mayor de interruptores CSS. No obstante, sin lugar a dudas, el argumento relativo a la detección de fallos integral en conexiones en serie sigue siendo válido.

- Ahora bien, existen diferentes formas posibles de abordar la cuestión de las “conexiones en cascada o en serie” (véanse ejemplos 8.2.29 y 8.2.28).

Ejemplos de conexión del Informe del BGIA[1]

[1] Para un informe más completo: véase Informe 2/08 del BGIA. Se han seleccionado los siguientes ejemplos para que nuestra gama de productos quede reflejada en la mayor medida posible. En total, el Informe del BGIA incluye 37 ejemplos de conexión. ADVERTENCIA: las notas incluidas a continuación han sido recortadas y simplificadas en gran medida.

Además debe recordarse que, en el caso de exclusiones de defectos en contactos de apertura positiva, el Informe del BGIA requiere la realización de un análisis específico. Aunque el "contacto con cierre normal" no se considera parte de la cuantificación (exclusión de defectos), deberá realizarse un análisis del valor B_{10d}.

Recomendación 1: no consideramos que la distinción mencionada realizada por el BGIA resulte útil para nuestro tipo de dispositivos, ya que no aporta a nuestros clientes prácticamente nada. O se considera la exclusión de defectos o no (véase más arriba). Los contactos de apertura positiva no constituyen más que uno de los aspectos a considerar.

Recomendación 2: debe descartarse la exclusión de defectos desde el principio cuando la estimación indique que el uso del dispositivo reside en la zona superior de su valor B_{10d} (en el caso de los interruptores de posición, por ejemplo, en caso de varios cientos de miles de ciclos de trabajo por año; en cualquier caso, por debajo de esta cifra estaremos normalmente en un intervalo de $MTTF_d > 100$ años).

Recomendación 3: seguimos sintiéndonos incómodos a la hora de recomendar exclusiones de defectos en su totalidad en relación con interruptores de posición sencillos (basta con pensar, por ejemplo, en el desgaste natural del rodillo de la transmisión o en la aparición de burbujas en la leva) (a menos que la norma C correspondiente acepte de forma expresa una exclusión de defectos). No obstante, en relación con este punto recomendamos consulten las páginas 29 y siguientes.

Recomendación 4: véase también la entrada "Exclusión de defectos" del glosario.

Un caso especial (exclusión de defectos como parte del B_{10d} en su conjunto) sería el de los dispositivos de control de parada de emergencia (véase discusión anterior de este punto).

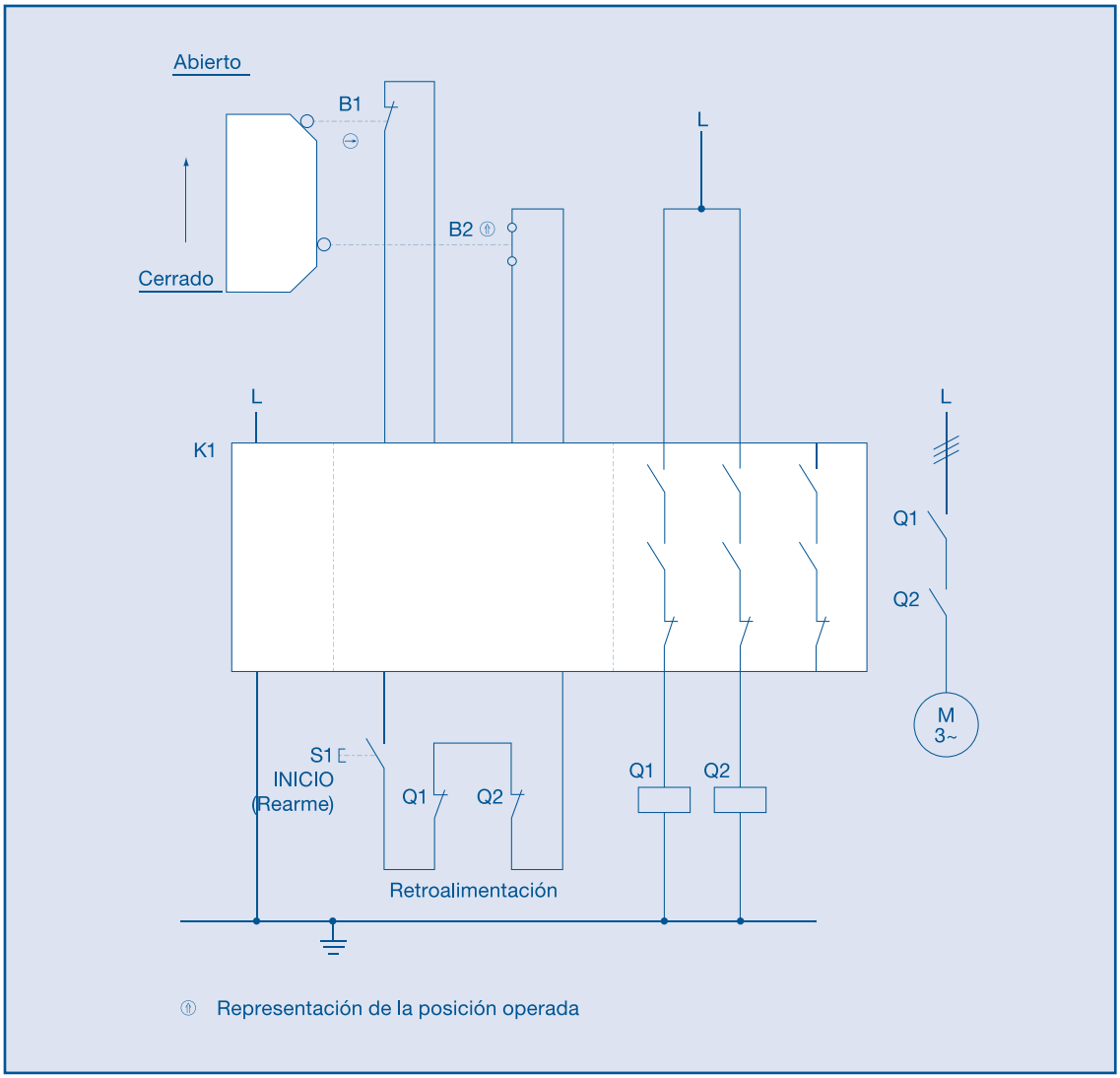
1) Ejemplo de conexión 8.2.34 del BGIA: control de la puerta de una guarda con procesamiento de señal posterior mediante módulo SRB o PLC de seguridad *(el caso clásico)*

Observaciones

- Conexión de entrada de 2 canales
- Detección de fallos (diagnóstico externo) en el SRB mediante comprobación utilizando relé con direccionamiento positivo = DC del 99 % o en el PLC de seguridad mediante comparación cruzada de datos = DC del 99 % (fuente: Anexo E de EN ISO 13 894-1:2006)
- Módulo SRB o PLC de seguridad con sub-PL “e”
- Conexión de salida de 2 canales con circuito de retroalimentación de contactos con transmisión positiva.
- Deben tenerse en cuenta todas las demás “normas” relativas a la aplicación, la conexión y el cableado.

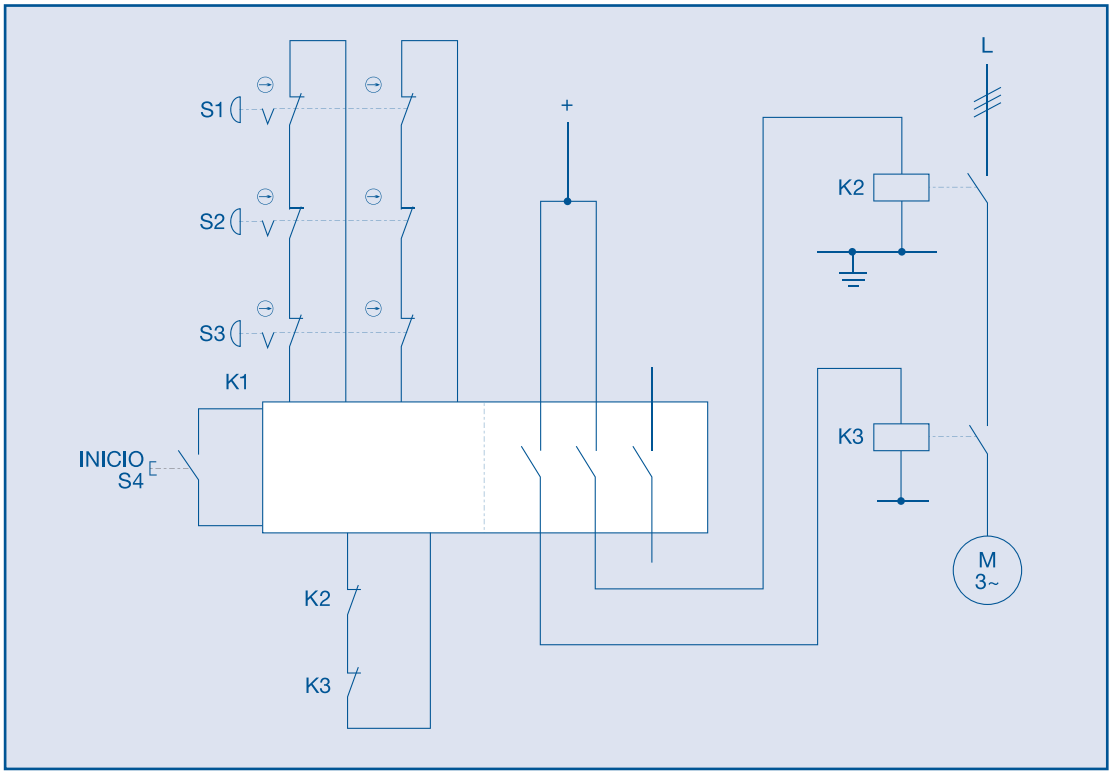
Resultado: asumiendo un valor $MTTF_d$ alto se obtiene un PL “e” en relación con la combinación (CC 4, $MTTF_d$ “alta”, DC del 99 %, falta de sensibilidad a los fallos CCF). El valor $MTTF_d$ deriva del análisis del valor B_{10d} (véase discusión anterior de este punto).

Ejemplo de conexión:



2) Ejemplo de conexión 8.2.29 del BGIA: conexiones en serie o en cascada

- El BGIA obtiene un PL “e” en caso de conexión en cascada de dispositivos de control de parada de emergencia porque la exclusión de defectos se realiza en relación con los dispositivos en su conjunto.



Observaciones

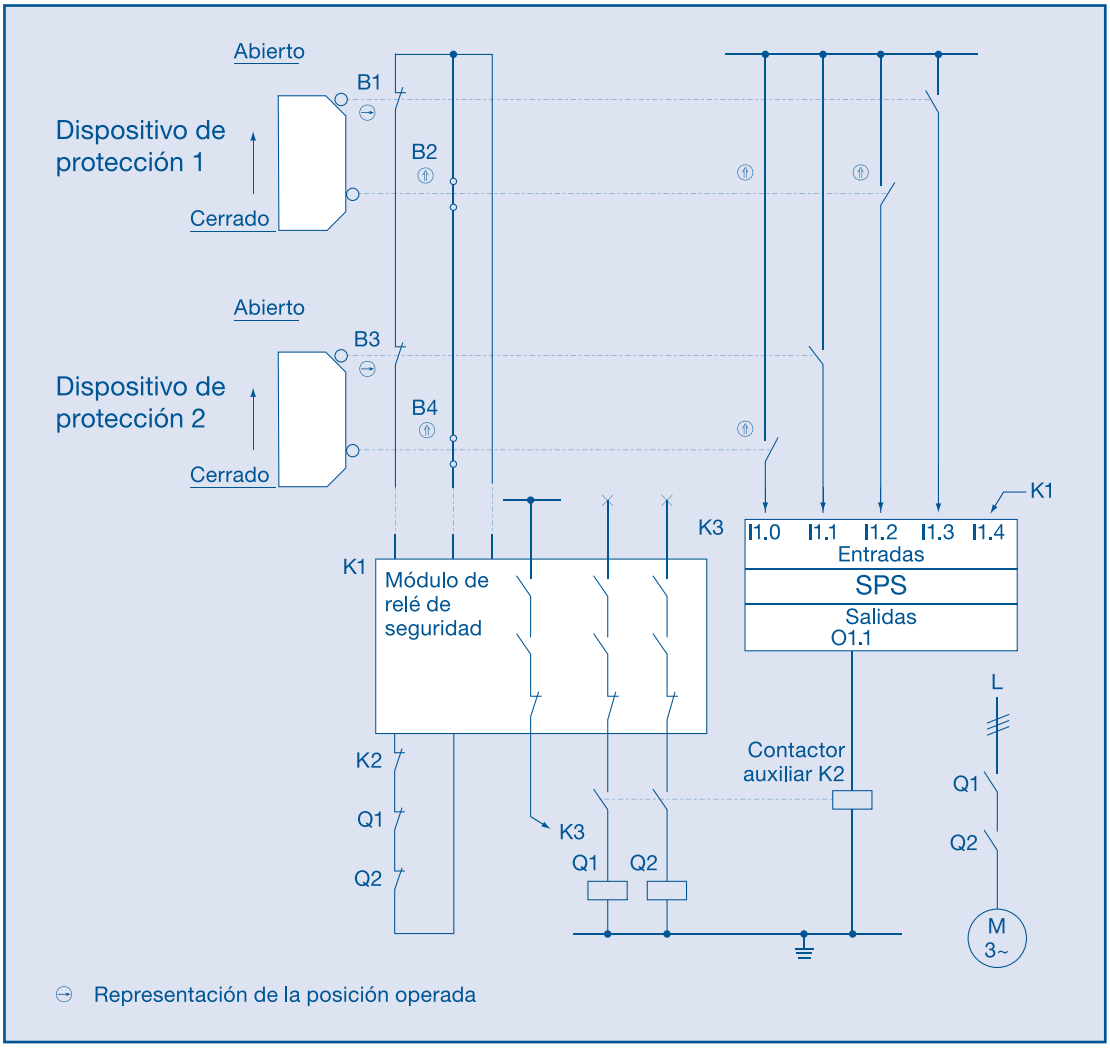
- Exclusión de defectos en S1, S2 y S3, cableado incluido
- Conexión de entrada de 2 canales
- Módulo SRB (o similar) con PL “e”
- Resultado: asumiendo un valor $MTTF_d$ alto para el módulo SRB, se obtiene en el ejemplo un PL “e” a pesar de la conexión en serie.

El BGIA no recomienda utilizar los datos de conmutación indicados anteriormente en relación con dispositivos operados por máquinas.

3) Ejemplo de conexión 8.2.28 del BGIA: conexiones en serie o en cascada

- A pesar de la conexión en serie de dispositivos electromagnéticos, en el siguiente ejemplo se obtiene un PL “e”, en el que se incorpora un PLC operativo a la SRP/CS para conseguir una detección de fallos adicional.

- En la terminología de la EN ISO 13 849- 1:2006, el PLC operativo de detección de fallos también se denomina “equipo de ensayo”. En el ejemplo de conexión del BGIA destaca el hecho de que esta posibilidad, unida al módulo de seguridad, permite obtener el efecto deseado de una DC del 99 %.



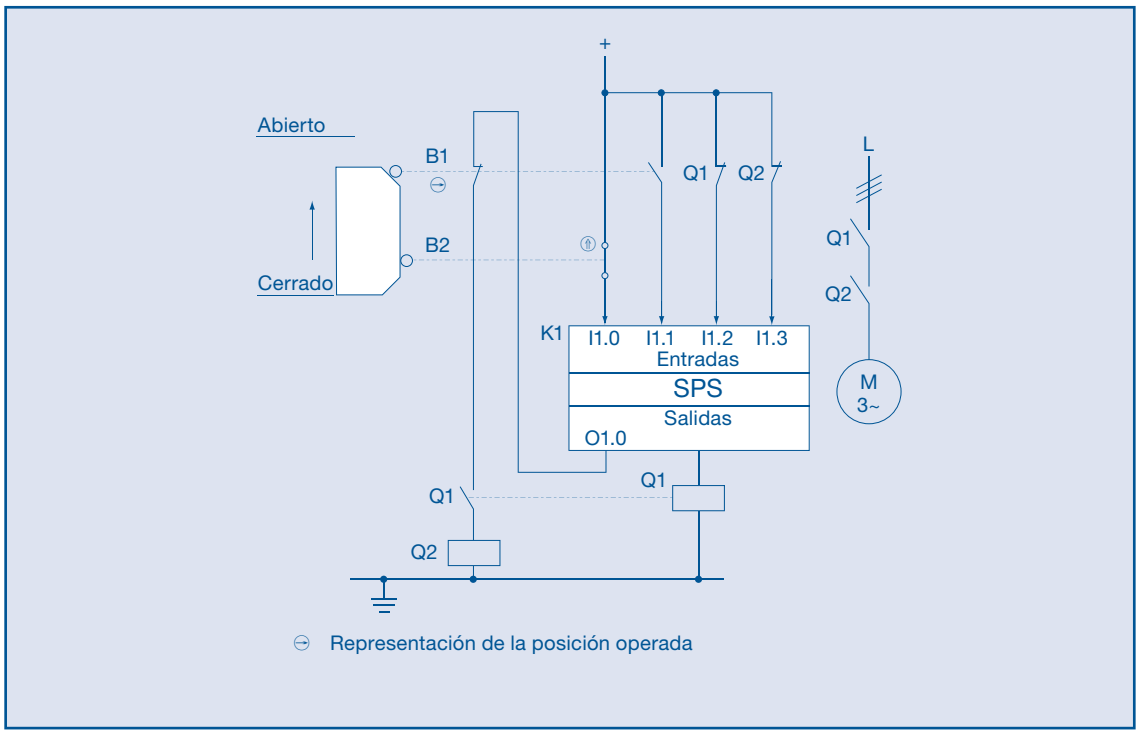
4) Ejemplo de conexión 8.2.18 del BGIA: bloqueo de una puerta ó guarda con procesamiento de señal mediante módulo SRB o PLC de seguridad (canal 1) y PLC estándar (canal 2)

Este ejemplo pone de manifiesto la posibilidad de trabajar sin SRB o PLC de seguridad (circuito básico – habitual en prensas de impresión de grandes dimensiones u otras máquinas similares).

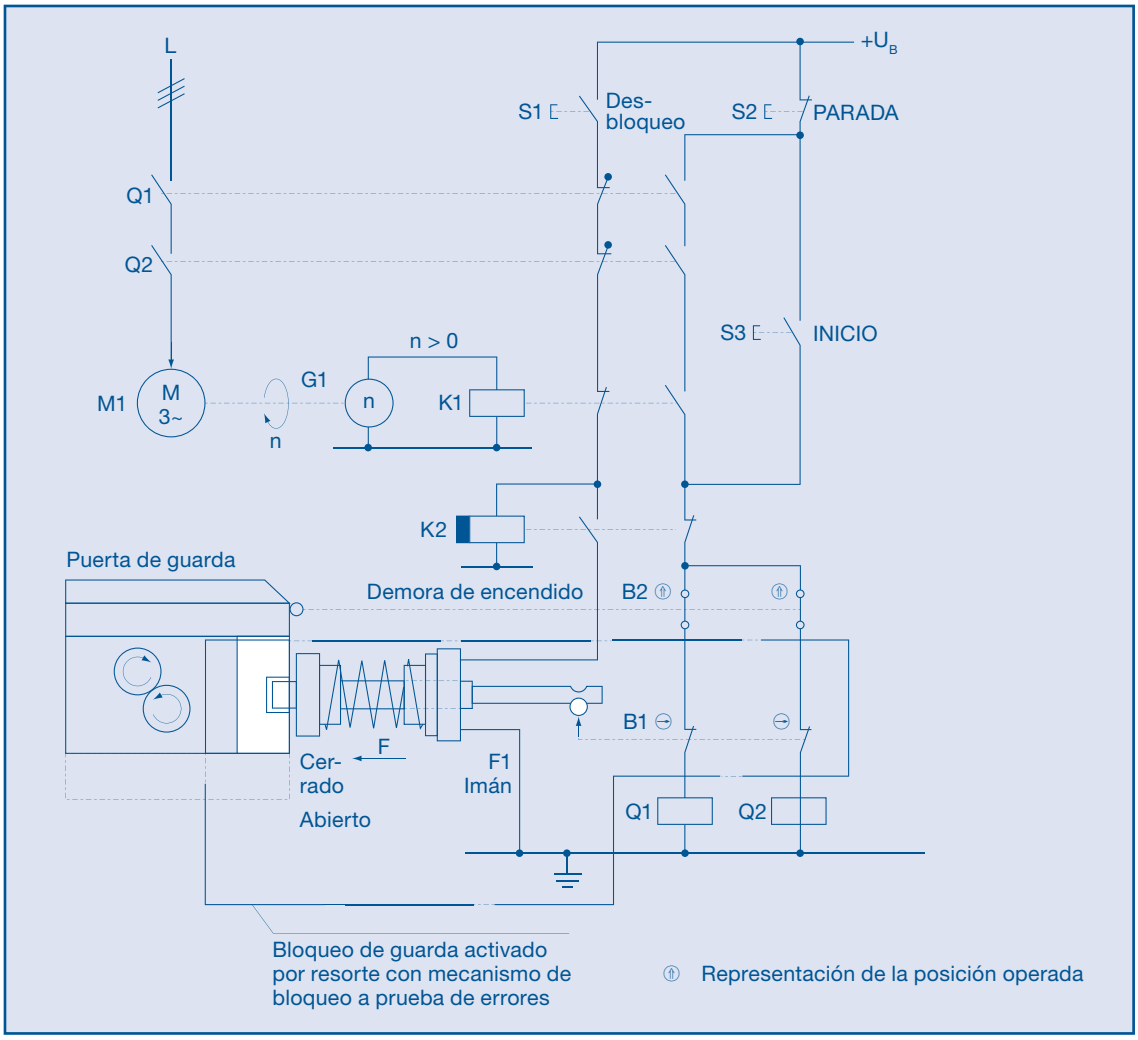
Observaciones

- Conexión de entrada de 2 canales, ruta de cable protegida/separada
- Se calcula un valor $MTTF_d$ “alto” analizando el valor B_{10d} correspondiente a los dos interruptores de posición, B1 y B2.
- “Canal 1” de procesamiento de señal directamente a través de un contactor (Q2); “canal 2” a través de un SRS estándar con contactor posterior Q1. La arquitectura posee una CC 3.
- Cobertura del diagnóstico: la posición de B1 se transmite adicionalmente al PLC y se compara su coeficiente de verosimilitud con B2 (DC = 99 %). La posición de los contactores (con transmisión positiva) también se transmite al PLC a través del circuito de retroalimentación (DC = 99%). El propio PLC es comprobado en este proceso (DC = 60 %). Por tanto, se obtiene una DC_{media} de 62 %.
- Deben tenerse en cuenta todas las demás “normas” relativas a la aplicación, la conexión y el cableado.

Resultado: el sistema de conmutación posee un PL “d” (véase diagrama de bloque: CC 3, $MTTF_d$ “alta”, DC “baja”, CCF OK).



(5) Ejemplo de conexión 8.2.19 del BGIA: cierre de la puerta de guarda



Observaciones

- A modo de explicación: el circuito se realiza sin nivel de control piloto (módulo SRB, PLC de seguridad o similar) con control directo del mecanismo de activación, y le corresponde un PL “d”.

- Este ejemplo no se ha incluido por la elegancia de la conexión, sino porque respalda nuestro argumento sobre las circunstancias en que puede asignarse un CC 3 al sistema de bloqueo de la guarda. En combinación con un módulo SRB correspondiente, podría obtenerse incluso una combinación de dispositivos con CC 4 y PL “e”.

- Advertencia: Control de detención de 1 canal

- Comentario del BGIA: la posición del perno de retención se controla a través de un interruptor de posición integrado, B1, mientras que el interruptor B2 controla la posición de la puerta de guarda para aumentar la seguridad contra la manipulación. El dispositivo de enclavamiento ofrece un mecanismo de bloqueo a prueba de fallos.

- Por tanto: canal 1, “control de posición de la puerta de guarda”: mecanismo de bloqueo a prueba de fallos + contacto(s) de seguridad para el control de la posición de la puerta de guarda; canal 2: “control de la posición del perno de retención”: 2 canales eléctricos.

- Cuando la protección contra la manipulación se consigue de otra forma, este ejemplo de conexión respalda nuestra opinión de que, en determinadas circunstancias, es posible utilizar un dispositivo de enclavamiento con mecanismos a prueba de fallos (es decir, sin un segundo interruptor adicional) para alcanzar la CC3 (véanse páginas 29 y siguientes).

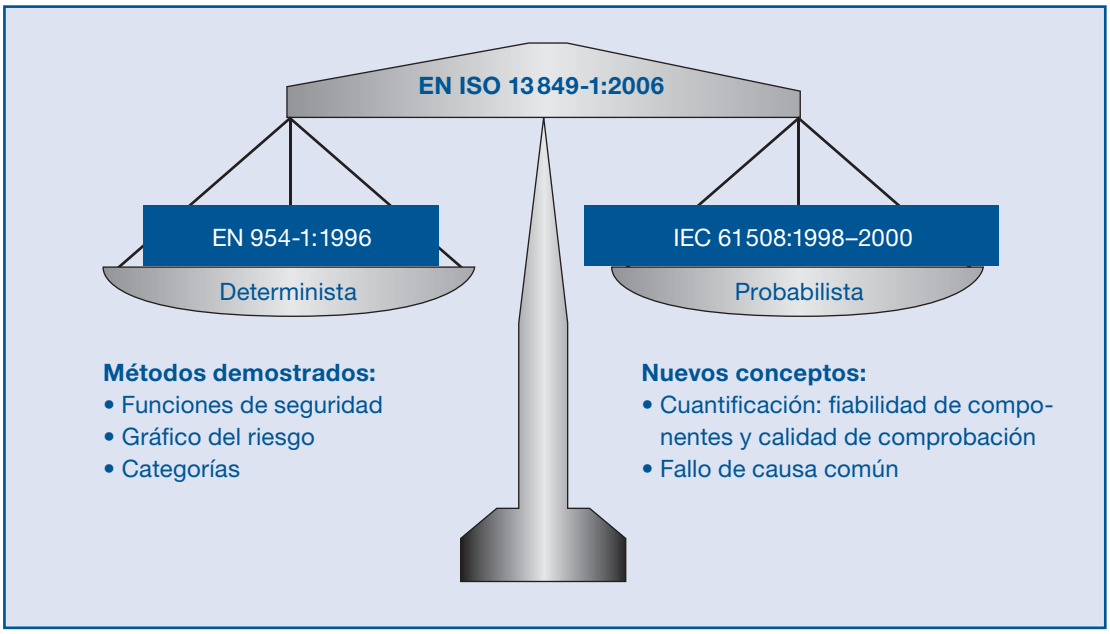
Presentación general de las características y uso de EN ISO 13849-1:2006

Objetivo de la normalización de las SRP/CS

- La normalización de las SRP/CS tiene por objetivo la introducción de medidas adicionales que permitan mantener la función de protección personal de una SRP/CS también en caso de fallo (o, mejor dicho, reducir los estados peligrosos derivados de un fallo a un riesgo residual aceptable).

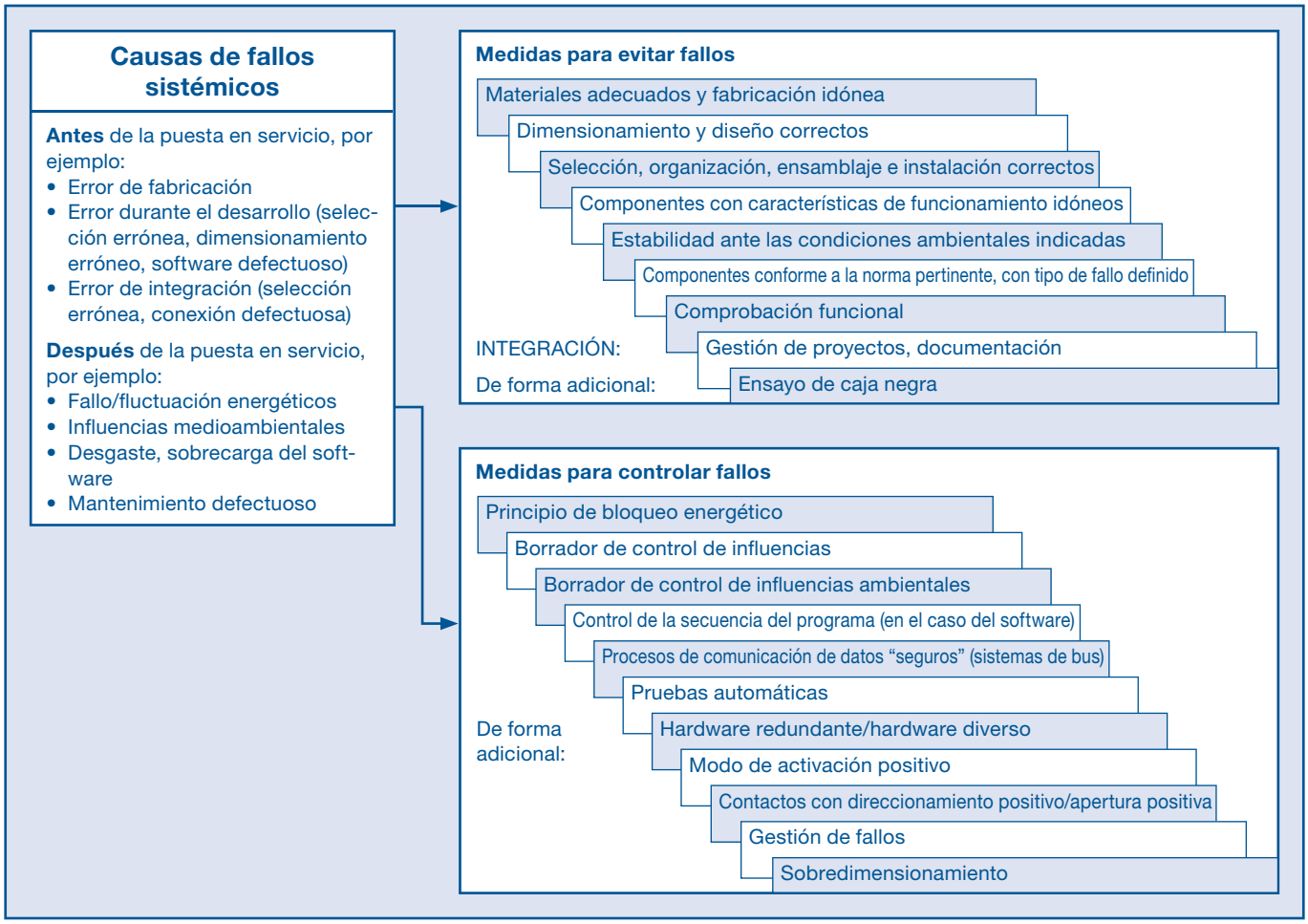
- Los fallos se producen por defectos y problemas en el hardware y el software de los SRP/CS utilizados, en la medida en que sean pertinentes para la seguridad.

- ¡Advertencia! Matiz semántico: los fallos (por ejemplo, en componentes = antes la función era correcta) generan defectos (= estado permanente del dispositivo); no obstante, una SRP/CS también puede presentar defectos desde un primer momento (fallo de diseño = fallo sistemático). Los estados peligrosos derivados de problemas (temporales) pueden equipararse a fallos.



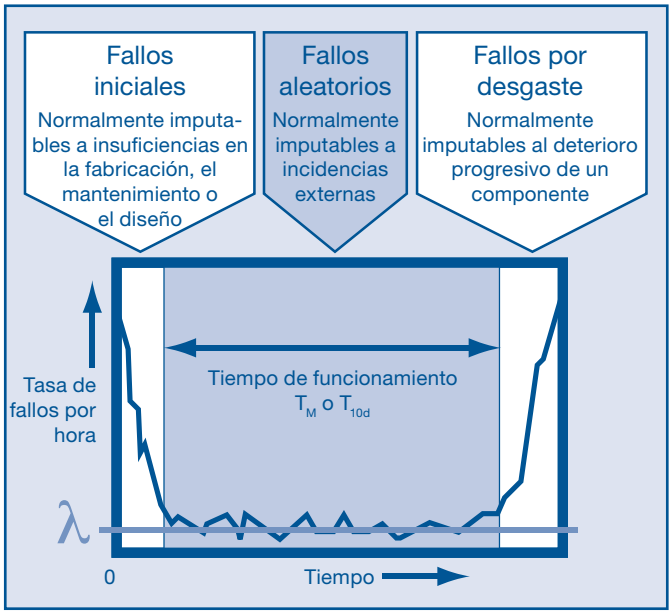
- Existen dos tipos de medidas adicionales: las que sirven para reducir el riesgo de defectos o fallos sistemáticos, y las que tienen por objetivo reducir los defectos o fallos aleatorios.

- Los defectos y fallos sistemáticos ya están presentes en el momento de la entrega. Hacen referencia de forma determinista a una causa específica y tan solo pueden ser eliminados modificando el diseño o el proceso de fabricación, el procedimiento de funcionamiento, la documentación u otros factores pertinentes. Esto significa que están relacionados con problemas de diseño básicos, lagunas en las especificaciones, fallos de razonamiento, defectos del software, etc. En estos casos la redundancia u otras medidas similares no son efectivas.



- En el Anexo G de EN ISO 13849-1:2006 y en EN ISO 13849-2:2003 pueden encontrarse medidas contra defectos y fallos sistemáticos.

- Por el contrario, a los defectos y fallos aleatorios tan solo puede asignarse una probabilidad estadística (estos son los fallos provocados, por ejemplo, por el envejecimiento del producto o por una avería aleatoria de los componentes). Dicho de otro modo: cuanto más reducida sea la probabilidad de fallo, más elevada será la seguridad funcional. La probabilidad de defectos y fallos aleatorios constituye un factor exclusivamente estadístico, y aunque permite extraer conclusiones en torno a la seguridad global de un producto en un ámbito en cuestión, no permite alcanzar conclusiones relativas a la seguridad de un producto específico. Véase también la figura de la curva de bañera.



- Los defectos aleatorios no existen en el momento de la entrega, sino que derivan de defectos del hardware y se producen de forma aleatoria durante el funcionamiento. Algunos ejemplos de defectos y fallos aleatorios son cortocircuitos, interrupciones, desplazamientos de componentes, fatiga de los materiales u otros similares. Aunque este tipo de fallos y defectos se dan de forma aleatoria (como ya se ha indicado), es posible asignarles una probabilidad estadística.

- Las medidas contra defectos y fallos aleatorios son la redundancia, la detección de defectos, etc., es decir, todo lo que asociamos de forma directa (e incompleta) con la categoría de control (CC), el nivel de prestaciones (PL) y el nivel de integridad de la seguridad (SIL). Decimos “incompleta” porque las medidas contra fallos y defectos sistemáticos constituyen un prerrequisito básico obligatorio de la CC, el PL o el SIL.

- Los denominados fallos de causa común, fallos de varias unidades (canales) con la misma función por una misma causa, constituyen un tipo específico de factor a tener en cuenta.

- Los defectos y fallos aleatorios tan solo se producen en el hardware, mientras que en el caso del software se asumen exclusivamente fallos y defectos sistemáticos. No obstante, esta teoría es controvertida, sobre todo en el caso de niveles críticos más elevados, como por ejemplo en la construcción de aeronaves.

- Actualmente se estima que la proporción de accidentes con maquinaría atribuidos a fallos aleatorios del hardware es reducida. Se habla de un porcentaje máximo de entre el 10 y el 15 % del total de accidentes. Según otras estimaciones, el porcentaje es aún menor. En contraposición, la mayor parte de los accidentes puede atribuirse a deficiencias sistemáticas y, no lo olvidemos, como consecuencia de la manipulación de dispositivos de protección.

Nivel de prestaciones (1)

- Definición de la norma (EN ISO 13849-1:2006): nivel discreto utilizado para especificar la aptitud de las partes de los sistemas de mando relativas a la seguridad para desempeñar una función de seguridad.

- Dicho de forma sencilla: calidad global orientada a la seguridad de una SRP/CS, teniendo en cuenta la arquitectura de la SRP/CS (= perspectiva determinista) y la fiabilidad de la SRP/CS (perspectiva probabilista). Se tienen en cuenta, en esencia, los aspectos relacionados con la fiabilidad relativa a la seguridad, la resistencia a fallos y defectos, la tolerancia de defectos, el comportamiento en caso de defectos, la detección de defectos, la posibilidad de evitar la acumulaciones de defectos y la posibilidad de evitar los defectos sistemáticos.

- El PL requerido (PL_r a … e) deriva de la consideración del gráfico del riesgo, de la función de seguridad respectiva o de la norma C en cuestión.

- Desde una perspectiva de probabilidad matemática, la probabilidad media de un fallo peligroso por hora (PFH_d) conlleva un nivel de prestaciones (PL) de acuerdo con la siguiente tabla:

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

Nota: Además de la probabilidad media de un fallo peligroso por hora (PFH_d) se requieren algunas otras estimaciones.

- La nota incluida bajo la tabla aclara el hecho (véase más arriba) de que no solo se tienen en cuenta los requisitos de probabilidad matemática.

- Para tener una idea aproximada, los valores PFH_d también pueden interpretarse como sigue:

Nivel de prestaciones (PL)	Número máximo de fallos tolerados: 1 fallo peligroso por
a	1 fallo peligroso por 10.000 horas
b	1 fallo peligroso por 100.000 horas
c	1 fallo peligroso por 333.000 horas
d	1 fallo peligroso por 1.000.000 horas
e	1 fallo peligroso por 10.000.000 horas

- Como es lógico, si la probabilidad media de un fallo peligroso por hora (PFH_d) da como resultado un PL, también pueden especificarse subsistemas con valores PFH_d a los que se asigna un sub-PL específico. Algunos ejemplos típicos de esta situación serían todos los dispositivos con funciones de seguridad más complejas, en los que normalmente se especifica este límite de fallos de forma adicional con la clasificación de PL o SIL.

- En este caso puede apreciarse con total claridad que, en última instancia, el intervalo de PL compartido (o EN ISO 13 849-1:2006) y el SIL (o EN IEC 62 061:2005 y EN IEC 61 508-1/-7: 2001) se corresponden sencillamente con los valores PFH_d.

- Cuando exista información relativa a sub-PFH_d, se recomienda que los valores respectivos tan solo requieran una parte específica del valor global designado como valor máximo en la clasificación de PL o SIL correspondiente, es decir, ≤ 20 % en relación con el nivel de entrada **I**, por una parte, y el nivel de la lógica **L**, por otra, de la SRP/CS, de forma que quede más del 60 % para el nivel de salida **O**, que según la experiencia constituye el eslabón más débil de la cadena.

- Si desea verse así, los siguientes parámetros, que se definen y explican en mayor detalle en la sección (2) y que se utilizan para establecer un PL o sub-PL, no son más que una simplificación que permite evitar los complejos cálculos matemáticos que subyacen en realidad a los valores PFH_d.

- Si se utiliza el método del subsistema para estimar el PL (véanse páginas 45 y siguientes), algunos de los cálculos indicados a continuación no serán necesarios o serán más sencillos. En este documento se utiliza el denominado método de bloques (véanse páginas 131 y siguientes).

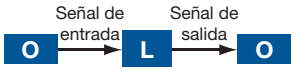
Nivel de prestaciones (2)

Un PL se compone de:

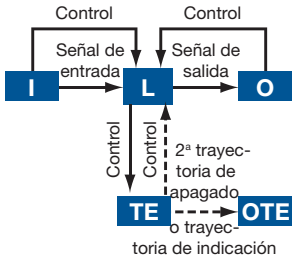
- **Arquitectura** (= categoría de control)
  Explicación breve: la arquitectura de una SRP/CS (1 canal, 1 canal con comprobación, 2 canales con comprobación mutua, 2 canales con autocontrol) en relación con la cadena **I** (entrada) + **L** (lógica = procesamiento de la señal) + **O** (salida); EN ISO 13849-1:2006 recomienda arquitecturas específicas, relativas a las categorías de control conocidas, además de ofrecer la posibilidad de poder realizar exclusiones de defectos de conformidad con EN ISO 13849-2:2003. Aunque en EN ISO 13849-1:2006 también se "permiten" otras arquitecturas, en ellas no puede utilizarse el método de cálculo simplificado tal cual, sino que debe recurrirse a cálculos matemáticos de mayor precisión con la inversión de tiempo que ello conlleva.

  - Debe designarse (1):
    - Categoría de control B … 4 (arquitecturas designadas: clasificación de las partes de sistemas de mando relativas a la seguridad en función de su resistencia a defectos y de su comportamiento posterior en caso de darse un defecto.
  - De acuerdo con EN 13849-2:2003, las exclusiones de defectos siguen siendo importantes o necesarias.

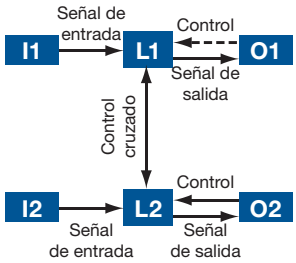
  Categorías B y 1:

  Categoría 2:

  Categorías 3 y 4:

  - Advertencia: La CC 2 se ha modificado. Véase el parágrafo "Categoría de control 2" en el glosario.

- Además de tenerse en cuenta las arquitecturas de una SRP/CS de acuerdo con lo anterior, en los requisitos de una categoría de control también se incluye el cumplimiento de los denominados principios de seguridad (a) básicos y (b) de ensayo y comprobación óptimos. Los principios de seguridad básicos están relacionados con los requisitos técnicos vigentes y deben tenerse en cuenta como fundamento básico (a partir de la categoría de control B); de forma adicional, los principios de seguridad de ensayo y comprobación óptimos también son de aplicación a partir de la categoría de control 1. Esto no debe confundirse con el requisito de utilizar componentes testeados y comprobados de forma óptima (que también son de aplicación en la CC 1). En los Anexos A-D de EN ISO 13849-1:2003 ("Validación de una SRP/CS") pueden encontrarse una descripción de en qué consisten estos diferentes requisitos. Véase también el parágrafo "Categorías de control" del glosario.

- **Fiabilidad del hardware** (= $MTTF_d$/tiempo medio hasta un fallo peligroso)
  Explicación breve: el tiempo medio, expresado en años (y), hasta producirse un fallo (aleatorio) peligroso en un canal de la SRP/CS; los valores de $MTTF_d$ específicos por canal del hardware utilizado deben determinarse, sumarse (utilizando el método del recuento de partes) y compararse con las especificaciones incluidas en la norma en relación con los niveles "bajo", "medio" y "alto". Los valores de $MTTF_d$ se basan en información del fabricante o en información procedente de elaboraciones de referencia pertinentes, como por ejemplo SN 29500.

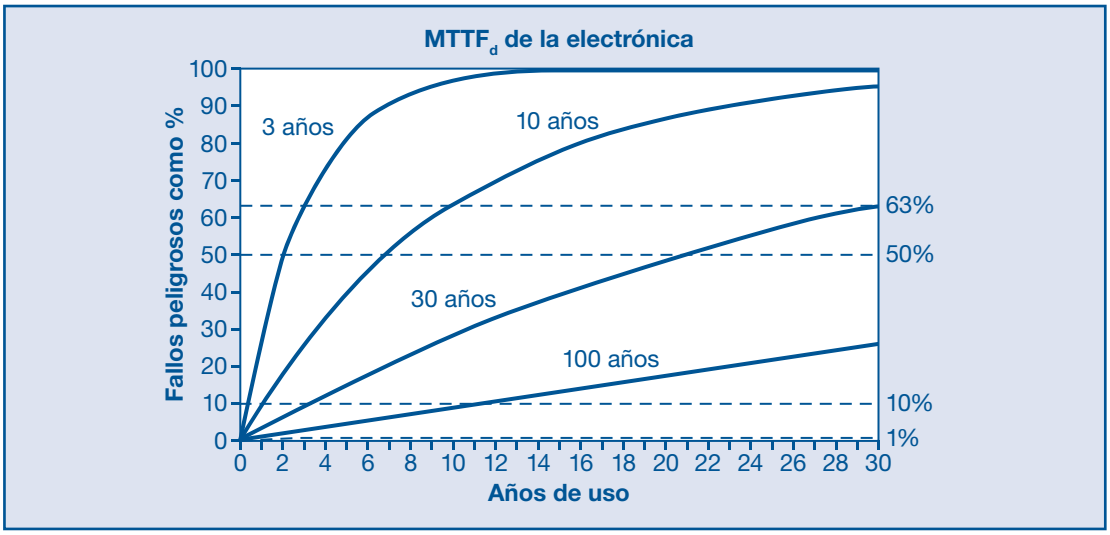
- Debe designarse (2):
  – $MTTF_d$ por canal como la suma de los $MTTF_d$ específicos de **I** + **L** + **O** dividido en tres grupos: "bajo", "medio" y "alto"

Denominación	Intervalo de $MTTF_d$
bajo	3 años ≤ $MTTF_d$ < 10 años
medio	10 años ≤ $MTTF_d$ < 30 años
alto	30 años ≤ $MTTF_d$ ≤ 100 años

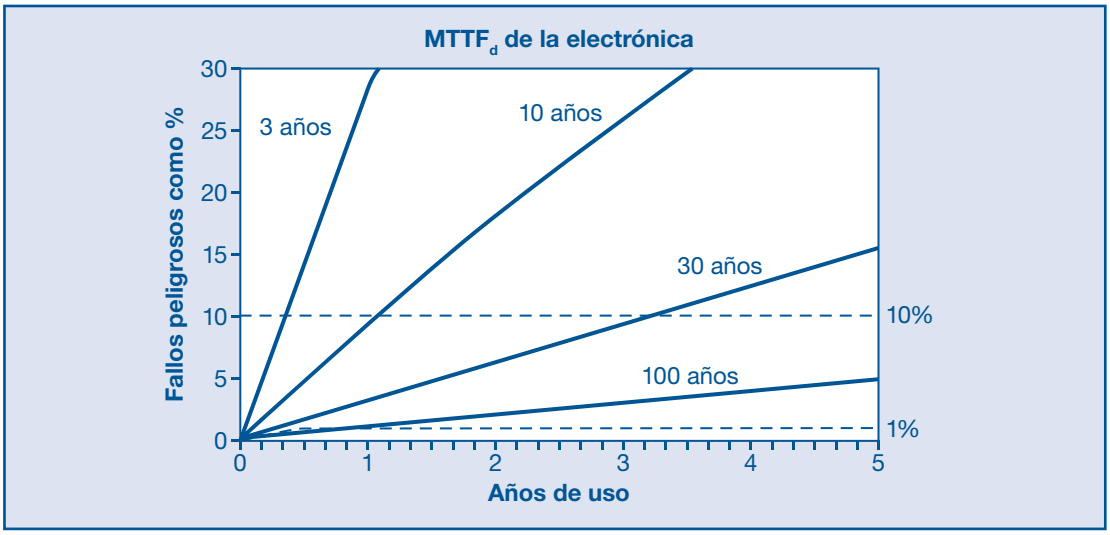
- Expresado de forma sencilla: calidad estadística del hardware orientado a la seguridad (derivada de la fiabilidad).
- En EN ISO 13849-1:2006 se utiliza el denominado método del recuento de partes para calcular los valores $MTTF_d$.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}}$$

ADVERTENCIA: la información de $MTTF_d$ tan solo constituye una indicación estadística de la probabilidad de supervivencia de un volumen elevado de productos (la indicación es del tipo de: en este punto en el tiempo tan solo "sobrevive" un 37 %). El valor recíproco $1/MTTF_d$ es la probabilidad de fallo por hora, también denominada λ o valor FIT (para 10^{-9} fallos). La teoría de probabilidad matemática subyacente es la distribución exponencial (véase glosario).



Las curvas muestran (de arriba a abajo) el porcentaje de fallos peligrosos como una función del $MTTF_d$ de los componentes. De arriba a abajo: 3 años, 10 años, 30 años, 100 años. También se indica (horizontalmente) la línea del 63 %, en la que coinciden el número de años de uso y el valor $MTTF_d$. Las otras líneas se corresponden con los porcentajes 50 %, 10 % y 1 %.



Las curvas muestran (de arriba a abajo) el porcentaje de fallos peligrosos como una función del MTTF$_d$ de los componentes. Se muestra el intervalo específico de los 5 primeros años de uso. De arriba a abajo: 3 años, 10 años, 30 años, 100 años. También se indican (horizontalmente) las líneas del 10 % y del 1 %.

- **Cobertura del diagnóstico** (= DC en %)
  Explicación breve: nivel, basado en la probabilidad, de la eficacia deseada del diagnóstico (→ detección de defectos), que expresa la relación existente entre los defectos peligrosos detectados y el número total de defectos peligrosos. No obstante, esta relación se ve también ponderada por el valor de MTTF$_d$ del componente en cuestión. Esto significa que la calidad de control de los componentes con un MTTF$_d$ amplio no tiene por qué ser tan elevada como la de los componentes con un MTTF$_d$ más reducido. A título ilustrativo, un 90% significa una probabilidad del 90 % de detectar defectos peligrosos (a tiempo) y del 10% de no descubrirlos (a tiempo) (a tiempo = detección antes de ocurrir la denominada probabilidad de segundo defecto). En el Anexo E de EN ISO 13849-1:2006 pueden encontrarse sugerencias de evaluación de diferentes medidas en los niveles **I**, **L** y **O**; es posible calcular una DC$_{avg}$ media en relación con una SRP/CS global aplicando una fórmula específica (“avg” significa “promedio”).

- Debe designarse (3):
  – La DC$_{avg}$ de la SRP/CS global (dividida en 4 grupos: “nula”, “baja”, “media” y “alta”) = resultado de la eficacia de las DC individuales de **I**, **L** y **O**

Denominación	Intervalo de valores
nula	DC < 60 %
baja	60 % ≤ DC < 90 %
media	90 % ≤ DC < 99 %
alta	99 % ≤ DC

Debe designarse (3) (continuación):

- Expresado de forma sencilla: eficacia/fiabilidad de las medidas de detección de defectos expresada como un porcentaje (cálculo de la DC_{avg} aplicando la fórmula)

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_S}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

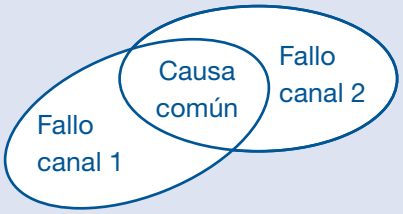
- Información de apoyo en EN ISO 13849-1:2006: véase el Anexo E de EN ISO 13849-1:2006

$$DC = \frac{\Sigma \lambda_{dd}}{\Sigma \lambda_d} \qquad \frac{\text{Probabilidad de fallos peligrosos detectados}}{\text{Probabilidad de fallos peligrosos totales}}$$

- **Gestión de fallos de causa común** (o “CCF”)
  Explicación breve: medidas para evitar fallos en los dos canales de una SRP/CS de forma simultánea debido a una causa común, por ejemplo solapamiento de ambos canales por una influencia ajena, sobrecalentamiento, sobretensión por descarga (pulsación de sobretensión) con salidas redundantes de semiconductor, aceite contaminado en el caso del sistema hidráulico o demasiado agua en el aire en el caso del sistema neumático; es decir, una única causa elimina la capacidad de canal múltiple (normalmente, la redundancia).
  El Anexo de EN ISO 13849-1:2006 incluye una tabla con medidas contra fallos de causa común. A cada medida se asigna una puntuación. Se recomienda implantar medidas que posean una puntuación de >65 de 100 puntos posibles.

- Debe designarse (4):
  – Medidas contra CCF (asignación SÍ/NO, tan solo a partir de la categoría de control 2): fallo derivado de una causa común: fallos de varias unidades como consecuencia de un único hecho; por tanto, estos fallos no poseen efectos recíprocos.

- Asignación de las medidas en **I**, **L** y **O** de acuerdo con la tabla de consulta (debe alcanzarse una puntuación mínima de 65 puntos de 100 puntos posibles).



N°	Medida contra CCF	Puntuación
1	Desconexión/separación	
	Desconexión física entre los caminos de las señales	15
2	Diversidad	
	Uso de diferentes tecnologías/principios de diseño	20
3	Diseño/aplicación/experiencia	
3.1	Protección contra sobretensión, sobrepresión, sobreintensidad, etc.	15

- De forma adicional, en la SRP/CS hay medidas contra fallos y defectos sistemáticos. Véase la entrada “Fallos (fallos sistemáticos)” del glosario.

Resultado

- Puede utilizarse un gráfico de resultados (fig. 1), del que puede deducirse el PL alcanzado, o bien, cuando se requiera un resultado más preciso, en el Anexo K de EN ISO 13 849-1: 2006 (Fig. 2) se ofrece una asignación numérica precisa entre los parámetros de PFH_d y de PL.

Tabla de resultados

- $MTTF_d$ limitado a 100 y
- Dependencia en función de CC, DC, CCF y $MTTF_d$
- Asignación más precisa (según Anexo K)
- Pueden utilizarse “solapamientos” en el caso de cálculos precisos

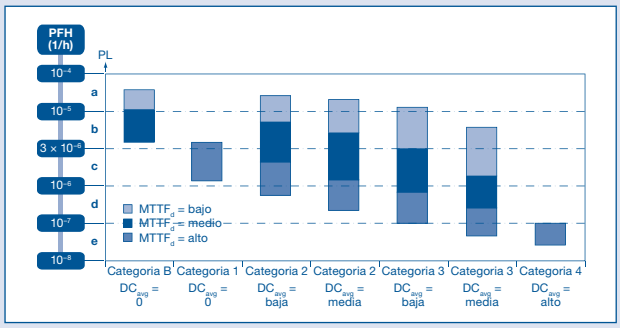


Fig. 1: Gráfico de barras

Representación numérica

- Véase Anexo K de EN ISO 13 849-1:2006

Tabla K.1 – Descripción numérica de la figura 5 (de EN ISO 13 849-1:2006 [D] – Anexo K [informativo])

	Probabilidad media de un fallo peligroso por hora (1/h) y nivel de prestaciones correspondiente (PL)														
$MTTF_d$ por canal	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
Años	DC_{avg} = nula		DC_{avg} = nula		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = alta	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}78 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}08 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}02 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}02 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

Figura 2: Anexo K de EN ISO 13 849-1:2006

Nivel de prestaciones (3)

- De acuerdo con la norma, la evaluación debe realizarse preferiblemente haciendo uso de información del fabricante.

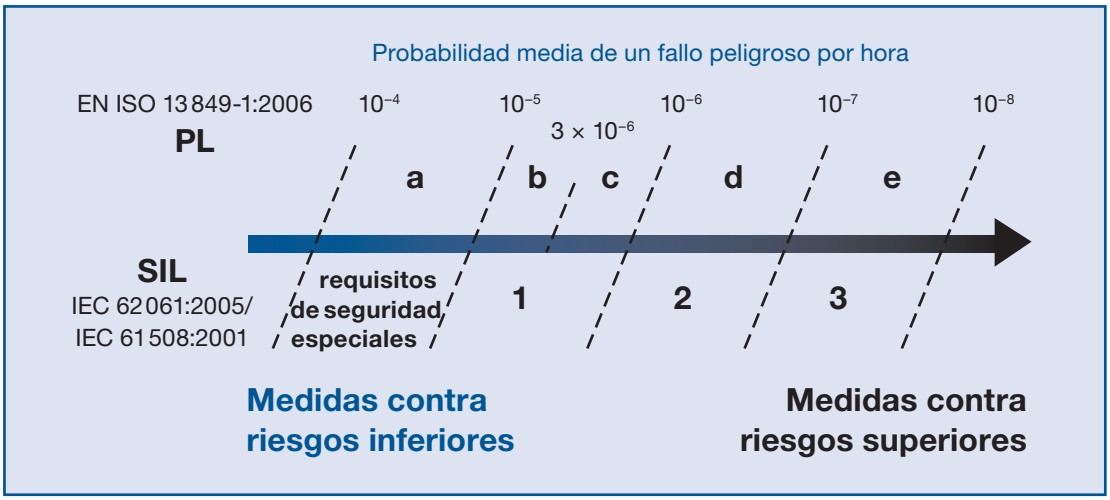
- Un PL puede establecerse de dos formas:

  – Se divide la función de seguridad (cadena I + L + O) en bloques (partes de componentes individuales desde una perspectiva funcional y lógica) que se valoran en relación con los aspectos que definen el PL y se evalúan de forma conjunta (en parte analíticamente, en parte matemáticamente). Esta solución se denomina método de bloques en EN ISO 13849-1:2006 y se describe de forma detallada en el Anexo B de la norma.

  – La SRP/CS global se divide en subsistemas derivados de bloques funcionales. Se determina un sub-PL para cada subsistema y se suman para obtener un PL global (véanse páginas 45 y siguientes).

- Los sub-PL tienen la ventaja de que el fabricante de la máquina puede utilizar un procedimiento simplificado para determinar el PL global, que en este caso viene determinado por el sub-PL inferior. Además, el valor de $MTTF_d$ debe corresponderse con la clasificación “alta” o utilizarse la tabla de combinación (véanse página 45 y parágrafo “Cálculos (cálculos de PL)” del glosario.

- En lo que concierne a los resultados y al efecto deseado de los mismos, un PL y un nivel de integridad de la seguridad (SIL) son lo mismo. En este sentido, también existe una tabla de compatibilidad (por ejemplo, PL “e” = SIL 3, etc.), aunque existen diferentes métodos de cálculo en función del caso en cuestión.



- ADVERTENCIA: las anteriores clasificaciones de PFH_d son de aplicación a un PL global (o SIL global). Tan solo pueden “utilizarse” proporciones en relación con los subsistemas (recomendación: como máximo un 20% para I y L, de forma que O disponga de >60 %).

Glosario –
información adicional relativa a algunos términos y palabras clave

Adición de probabilidades de fallo

- Cuando se dispone de valores de $MTTF_d$, la adición por canal se produce utilizando el método de recuento de partes, es decir, se suman los valores recíprocos $1/MTTF_d$. A continuación, el resultado se convierte de nuevo en un valor de $MTTF_d$ global y se compara con las especificaciones de la norma relativas a los niveles "bajo" (3 y … 10 y), "medio" (10 y … 30 y) y "alto" (30 y … 100 y). Existe un límite de $MTTF_d$ de 100 años por canal (no obstante, pueden asumirse valores más elevados dentro de un canal).

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d\,i}}$$

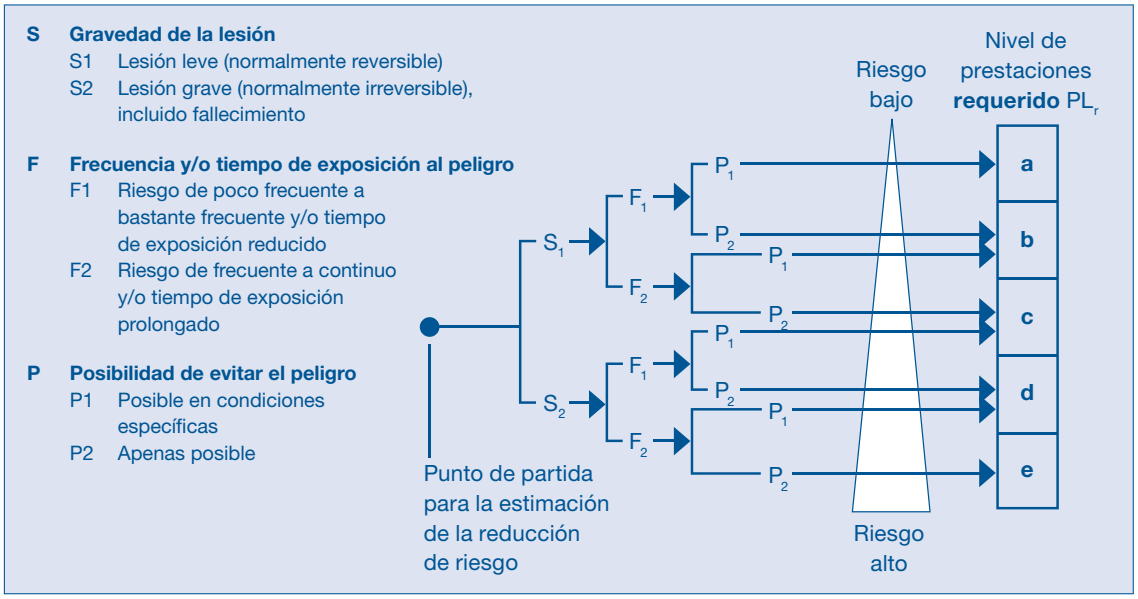
- Existe una denominada fórmula de simetrización para los canales con valores de MTTFd diferentes:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

- Aunque los valores PFHd pueden sumarse simplemente (es decir, $1 \times 10^{-9} + 1 \times 10^{-9} = 2 \times 10^{-9}$), la subclasificación más baja condiciona los niveles PL o SIL globales. Los valores PFH_d más elevados no pueden compensar en modo alguno las limitaciones sobre el nivel de integridad de la seguridad (véase sección pertinente) derivadas de las denominadas restricciones de la arquitectura.

Análisis del gráfico del riesgo conforme a EN ISO 13849-1:2006

- Establece el PL_r (= PL que debe aplicarse para conseguir la reducción de riesgo requerida para cada función de seguridad).
- Aunque los parámetros de análisis ya conocidos por la valoración del riesgo de EN 954-1:1996 (ISO 13849-1:1999) se mantienen en la norma EN ISO 13849-1:2006, en esta ocasión el resultado, en vez de conllevar el requisito de obtener una categoría de control, genera un nivel de prestaciones PL_r que debe conseguirse de acuerdo con lo siguiente:



- Una de las ventajas del nuevo gráfico del riesgo es que, ahora, existe una definición normativa de la distinción entre los parámetros F1 y F2, es decir: F1 se aplica a las frecuencias que impliquen una permanencia en la zona peligrosa de 1 × hora o más, y F2 a las frecuencias que impliquen una permanencia en la zona peligrosa de > 1 × hora.

- La segunda ventaja es que, en el futuro, el análisis de los parámetros siempre generará un PL_r inequívoco, mientras que en la anterior norma era posible llegar con varias permutaciones a dos categorías de control (aplicables de forma discrecional) sin que se proporcionase ninguna orientación adicional para tomar esta decisión.

Análisis del gráfico del riesgo conforme a EN IEC 62061:2006

- Establece los requisitos de integridad de la seguridad de la SRP/CS en forma de nivel de integridad de la seguridad (SIL).
- Está relacionado con una derivada adaptada a la construcción de máquinas y extraída del gráfico del riesgo conforme a EN IEC 61508:2001, de acuerdo con lo siguiente.

- En relación con lo anterior, la norma EN IEC 62061:2006 sigue reconociendo el denominado límite de reclamación de SIL (SILCL = límite de reclamación de SIL), relacionado con el SIL máximo (según la definición de la norma) que puede reivindicarse en relación con un sistema de SRP/CS en relación con las restricciones estructurales y la integridad de la seguridad sistemática. En este sentido, el límite de reclamación de SIL es importante para la evaluación global (validación), ya que el SILCL inferior (en su calidad de eslabón más débil de la cadena) condiciona el SIL que puede alcanzar una SRP/CS en su totalidad.

(1) Cuando la permanencia sea menor a 10 minutos, el valor puede reducirse al siguiente nivel. Esto no es de aplicación a la frecuencia de exposición ≤1 h, que no debe reducirse de nivel en ningún caso.

Gravedad del daño **S**	

(1)

Frecuencia y/o permanencia **F**	
≤1 hora	5
>1 hora … ≤1 día	5
>1 día … ≤2 semanas	4
>2 semanas … ≤1 año	3
>1 año	2

(2)

Probabilidad de que se dé un suceso peligroso **W**	
frecuente	5
probable	4
posible	3
poco frecuente	2
insignificante	1

Posibilidad de prevención **P**	
imposible	5
posible	3
probable	1

Efectos	Gravedad del daño **S**	Clase **K = F + W + P**				
		3–4	**5–7**	**8–10**	**11–13**	**14–15**
Muerte, pérdida de ojo o brazo	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, pérdida de dedos	3			SIL 1	SIL 2	SIL 3
Reversible, atención médica	2	Otras medidas			SIL 1	SIL 2
Reversible, primeros auxilios	1					SIL 1

Análisis del valor T_{10d}

- El análisis del valor T_{10d} constituye otra de las novedades de la norma EN ISO 13849-1:2006. El valor T_{10d} se corresponde con el 10 % del valor B_{10d} y, al convertirlo a años (y), debe considerarse como una información relativa a la sustitución preventiva de los dispositivos afectados por desgaste. Con el valor T_{10d} se asume que se dará una pauta de fallo constante en el dispositivo correspondiente durante el periodo de tiempo en cuestión (similar a la sección media de la “curva de bañera”).
- Como es evidente, la información relativa a la sustitución preventiva de un dispositivo tan solo tiene sentido en relación con valores de MTTF en que el ratio del 10 % se sitúe dentro de la duración de la misión prevista de la SRP/CS de 20 años.
- El análisis del valor T_{10d} no puede sustituir las inspecciones periódicas de los equipos de trabajo de acuerdo con la Directiva CE de Utilización de Equipos de Trabajo ni, en Alemania, la normativa relativa a seguridad ocupacional (BetrSichV).
- Véase también el término “valores B_{10d}”.

Anexo E

- Estimación de la cobertura del diagnóstico (DC) en funciones y módulos.
- Véase término “Detección de defectos” y las páginas 32 f. y 68 f.

Anexo G (conforme a EN ISO 13849-1:2006)

- Las medidas contra fallos sistemáticos se encuentran entre las más importantes para la seguridad de las SRP/CS. Las deficiencias en este ámbito apenas pueden compensarse utilizando otras medidas.

ISO/FDIS 13849-1:2006 (E)

Anexo G
(informativo)

Fallos sistemáticos

G.1 Generalidades

La Norma ISO 13849-2 proporciona una lista completa de medidas que se deberían aplicar contra los fallos sistemáticos, tales como los principios básicos de seguridad y los principios de eficacia probada.

G.2 Requisitos para controlar los fallos sistemáticos

Se deberían aplicar las medidas siguientes:

– Utilizar la desenergización (véase la Norma ISO 13849-2).

  Las partes del sistema de mando relativas a la seguridad (SRP/CS) se deberían diseñar de manera que sea posible obtener o mantener un estado de seguridad de la máquina en caso de pérdida de la alimentación de energía.

– Medidas para controlar los efectos de los cortes de tensión, variaciones de tensión, sobretensiones, caídas de tensión.

  Se debería predeterminar el comportamiento de las SRP/CS en respuesta a los cortes de tensión, las variaciones de tensión, las sobretensiones y las caídas de tensión, de manera que las SRP/CS puedan obtener o mantener un estado de seguridad de la máquina (véase también la Norma IEC 60204-1 y A.8 de la Norma IEC 61508-7-2000).

– Medidas para controlar o evitar los efectos del medio ambiente físico (por ejemplo, la temperatura, la humedad, el agua, las vibraciones, el polvo, las sustancias corrosivas, las interferencias electromagnéticas y sus efectos).

- En este sentido, las medidas destinadas a evitar y controlar los fallos sistemáticos vuelven a considerarse, de forma adicional, en el Anexo G de EN ISO 13849-1:2006, a nivel informal.
- Decimos que “se consideran de forma adicional” porque las normas EN 954-1:1996 (ISO 13849-1:1999) y, en particular, EN ISO 13849-2:2003 (concebidas originalmente como EN 954-2), ya incluyen requisitos deliberados a los que se da continuidad y que se mejoran en el Anexo G.
- En la norma EN IEC 62061:2005 también se incluyen las mismas consideraciones en relación con este tema.
- El Anexo G se divide en 4 grupos. El grupo G.1 es sencillamente una referencia cruzada a las consideraciones pormenorizadas de EN ISO 13849-2:2003 (véase más arriba). El grupo G.2 está relacionado con las medidas de control de fallos sistemáticos, el G.3 con las medidas para evitar fallos sistemáticos y el G.4 con las medidas para evitar fallos sistemáticos durante la integración de una SRP/CS.

Anexo K (conforme a EN ISO 13849-1:2006)

- El Anexo K responde a un doble objetivo:
  – En primer lugar, de las áreas de solapamiento del gráfico de barras puede deducirse con mayor precisión, por ejemplo, a partir de qué valor de $MTTF_d$ se consigue un PL “e” con una arquitectura acorde a la CC 3 y una cobertura del diagnóstico media (a partir de 62 años), etc. Para más información: véase extracto de la tabla incluido a continuación.
  – Del Anexo K también puede deducirse la probabilidad media de un fallo peligroso por hora (o el valor PFH_d) que corresponde a una configuración específica. Por ejemplo, un PL “d” con una arquitectura acorde a la CC 3, un valor de $MTTF_d$ por canal de 56 años y una cobertura del diagnóstico media corresponde con un valor PFH_d de $1{,}03 \times 10^{-7}$/h.

(1) Dado que las medidas contra CCF son obligatorias a partir de la CC 2, no se enumeran por nombre en el Anexo K, sino que se consideran ya dadas.

Tabla K.1 – Descripción numérica de la figura 5 (de EN ISO 13849-1:2006 [D] – Anexo K [informativo])

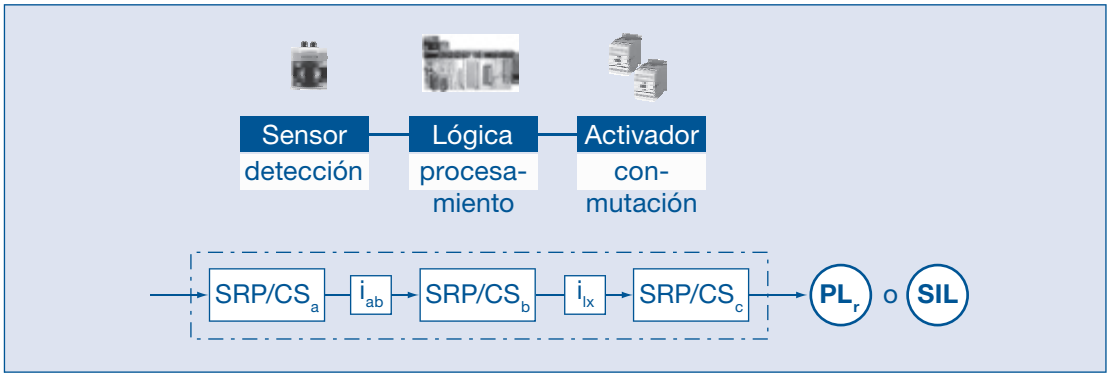
	Probabilidad media de un fallo peligroso por hora (1/h) y nivel de prestaciones correspondiente (PL)													
$MTTF_d$ por canal	**Cat. B**	**PL**	**Cat. 1**	**PL**	**Cat. 2**	**PL**	**Cat. 2**	**PL**	**Cat. 3**	**PL**	**Cat. 3**	**PL**	**Cat. 4**	**PL**
Años	DC_{avg} = nula		DC_{avg} = nula		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = baja		DC_{avg} = media		DC_{avg} = alta	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}88 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}13 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}78 \times 10^{-7}$	d		
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}08 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}38 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}08 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e

- A efectos prácticos, el valor PFH_d representa el ámbito de aplicación de EN IEC 61 508-2001 o EN IEC 62 061:2005, ya que estas normas expresan la probabilidad de fallo residual de una SRP/CS en esta unidad. También podría decirse que el Anexo K constituye un reflejo claro de la forma en que EN IEC 61 508:2001 influyó sobre la preparación de EN ISO 13 849-1:2006. No obstante, el valor PFH_d no constituye un enfoque exclusivamente probabilista.
- La tabla del Anexo K se basa en numerosos cálculos realizados por el Instituto Alemán de Salud y Seguridad Ocupacionales (BGIA) del Sector de los Seguros Legales de Accidente de Alemania, sito en St. Augustin, durante la planificación de la norma utilizando los modelos Markov.
- Por desgracia, las cifras del Anexo K tan solo llegan a un valor de $MTTF_d$ de 100 años por canal, a pesar de que la conversión de valores “más elevados” sería en ocasiones deseable para realizar análisis dentro de un canal. No obstante, estos valores pueden extrapolarse de forma simplificada mediante un cálculo logarítmico. De acuerdo con el Informe 2/08 del BGIA, puede calcularse un valor de $MTTF_d$ de bloque de forma muy simplificada (tan solo posible en esta dirección) a partir de un valor PFH_d, y calculando el valor recíproco, es decir, $1/PFH_d$: 8.760 = $MTTF_d$ de bloque (en el caso de PL o SIL más elevados, normalmente varios cientos de años).
- Desde su emisión se han actualizado de forma no oficial las cifras del Anexo K (denominadas valores básicos), aunque esto tan solo es de aplicación a arquitecturas acordes a la categoría de control 4. El uso de estas cifras tan solo es compatible con EN ISO 13 849-1:2006 en relación con subsistemas (para poder conmutar más subsistemas en serie). La limitación de una SRP/CS global a 1×10^{-8} no se ve afectada por este hecho.
- En el caso de otras arquitecturas, la recomendación, en caso necesario, sigue siendo una extrapolación prudente que tenga en cuenta la escala logarítmica doble o haga uso de las variables auxiliares $MTTF_d$ y $MTTF_d$ de bloque.
- A continuación se muestran las cifras actualizadas (con una CC 4, una DC “alta” y CCF >65 puntos):

$MTTF_d$ (y) = PFH_d (por hora)			
100 = $2{,}47 \times 10^{-8}$	240 = $9{,}81 \times 10^{-9}$	560 = $4{,}11 \times 10^{-9}$	1.300 = $1{,}75 \times 10^{-9}$
110 = $2{,}23 \times 10^{-8}$	270 = $8{,}67 \times 10^{-9}$	620 = $3{,}70 \times 10^{-9}$	1.500 = $1{,}51 \times 10^{-9}$
120 = $2{,}03 \times 10^{-8}$	300 = $7{,}76 \times 10^{-9}$	680 = $3{,}37 \times 10^{-9}$	1.600 = $1{,}42 \times 10^{-9}$
130 = $1{,}87 \times 10^{-8}$	330 = $7{,}04 \times 10^{-9}$	750 = $3{,}05 \times 10^{-9}$	1.800 = $1{,}26 \times 10^{-9}$
150 = $1{,}61 \times 10^{-8}$	360 = $6{,}44 \times 10^{-9}$	820 = $2{,}79 \times 10^{-9}$	2.000 = $1{,}13 \times 10^{-9}$
160 = $1{,}50 \times 10^{-8}$	390 = $5{,}94 \times 10^{-9}$	910 = $2{,}51 \times 10^{-9}$	2.200 = $1{,}03 \times 10^{-9}$
180 = $1{,}33 \times 10^{-8}$	430 = $5{,}38 \times 10^{-9}$	1.000 = $2{,}27 \times 10^{-9}$	2.300 = $9{,}85 \times 10^{-10}$
200 = $1{,}19 \times 10^{-8}$	470 = $4{,}91 \times 10^{-9}$	1.100 = $2{,}07 \times 10^{-9}$	2.400 = $9{,}44 \times 10^{-10}$
220 = $1{,}08 \times 10^{-8}$	510 = $4{,}52 \times 10^{-9}$	1.200 = $1{,}90 \times 10^{-9}$	2.500 = $9{,}06 \times 10^{-10}$

Arquitecturas

- Definición de la norma (EN 62 061:2005): configuración específica de los elementos del hardware y el software en una SRP/CS:
  Las arquitecturas de SRP/CS se componen del nivel de entrada **I** (compuesto por sensores y dispositivos de control orientados a la seguridad), el nivel lógico **L** (procesamiento de la señal) y el nivel de salida **O** (con las señales de control de los movimientos peligrosos desencadenados por salidas como los contactores). También forman parte de la arquitectura el número de canales (es decir, la categoría de control) y los equipos de control internos y externos.
- Para determinar un PL o SIL (global) debe considerarse toda la cadena, es decir, la conexión en serie **I** + **L** + **O**.



- De nuevo, en este caso un nivel puede ser el resultado de una conexión en serie en la medida en que derive de la función de seguridad.
- Las arquitecturas de EN ISO 13 849-1:2006 son especialmente importantes cuando se las denomina “arquitecturas designadas”. Estas arquitecturas hacen referencia a las categorías de control ya conocidas por EN 954-1:1996 y actualizadas en EN ISO 13 849-1:2006.
- A este respecto, la denominación “arquitecturas designadas” implica que, si se desea utilizar la norma EN ISO 13 849-1:2006, no se permite una desviación significativa con respecto a las mismas (es decir, una desviación sustancial de las categorías de control) (con la excepción de las exclusiones de defectos). De lo contrario, sería necesario evaluarlas de conformidad con EN IEC 61 508:2001, EN IEC 62 061:2005 u otras normas específicas (como, por ejemplo, EN IEC 61 496 en el caso de los AOPD[1]). En este contexto, sin embargo, las arquitecturas no deberían considerarse como diagramas de circuito, sino como diagramas esquemáticos funcionales. En este sentido, mientras mantengamos las características y estructura principales de las “arquitecturas designadas”, el hecho de que tengamos tres bloques en un canal, o más o menos bloques, no es relevante.
- Esta restricción se explica por cálculos de probabilidad matemática que se tuvieron en cuenta durante la elaboración de EN ISO 13 849-1:2006 y que se basan en las categorías de control conocidas.
- Véase también el término “categorías de control”.

[1] AOPD= Dispositivos de protección optoelectrónicos activos

B

Arquitecturas designadas

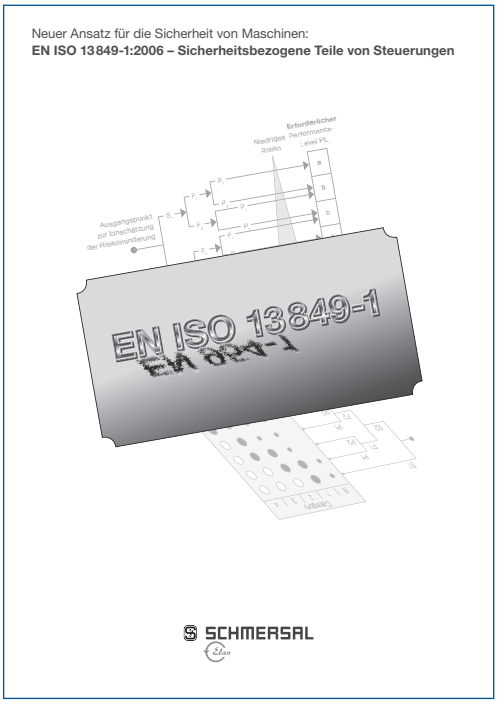
- Véanse parágrafos “Arquitecturas” y “Categorías de control”.

BGIA

- El BGIA, Instituto Alemán de Salud y Seguridad Ocupacionales del Sector Alemán de los Seguros Legales contra Accidentes, es un instituto de investigación y comprobación de las aseguradoras legales de accidentes en Alemania. Su domicilio social se encuentra sito en St. Augustin, cerca de Bonn.
- El BGIA presta respaldo a las aseguradoras legales de accidentes en Alemania y a sus entidades, haciendo hincapié en cuestiones de carácter científico-técnico relativas a salud y seguridad ocupacionales, mediante:
  - Estudios, investigación y desarrollo
  - Inspección de productos y muestras de materiales
  - Mediciones operativas y servicio de consulta
  - Participación en la normalización y formulación de normativa
  - Facilitación de información profesional y conocimiento especializado
- De forma adicional, el BGIA actúa en nombre de fabricantes y sociedades en el marco de:
  - La inspección y certificación de productos
  - La certificación de la gestión de la calidad

Bibliografía

- En la actualidad, tanto EN ISO 13 849-1:2006 como EN IEC 62 061:2005 ofrecen una gran cantidad de bibliografía, publicada tanto por editoras como por fabricantes de componentes de seguridad, en ocasiones de forma gratuita.
- Nuestro folleto informativo “Nuevo enfoque de la seguridad de máquinas: EN ISO 13 849-1:2006 – SRP/CS”, puede descargarse en www.schmersal.com (enlace: seguridad y normativa), es una de las primeras fuentes de información (y sigue siendo una de las más exhaustivas).
- También existen explicaciones relativas a la aplicación de las normas EN 62 061 y EN ISO 13 849-1 en un folleto publicado por la división de automoción de la Asociación Alemana de Fabricantes Eléctricos y Electrónicos (ZVEI) (puede descargarse en www.zvei.org).
- Por último, pero no por ello menos importante, cabe mencionar el Informe 2/08 del BGIA en relación con este tema (véase sección pertinente).



Buenas prácticas de ingeniería (BPI)

- Término original procedente de la planificación y funcionamiento de sistemas farmacéuticos. El significado específico de este término en el ámbito del diseño de SRP/CS, en el marco de la norma EN ISO 13849-1:2006, implica que deben tenerse en cuenta los siguientes puntos:
  - los requisitos de las normas de producto respectivas (véase tabla D.2 de EN ISO 13849-1:2006);
  - los requisitos de las normas A (EN ISO 12100-1/-2, EN ISO 14121-1/-2); y
  - los principios de seguridad básicos y demostrados, así como el uso de componentes de seguridad probados (CC 1) (Anexos A–D de EN ISO 13849-2:2003).
- También forman parte de los GEP la selección de dispositivos adecuados a la vista de la aplicación y las condiciones ambientales, así como considerar la información del fabricante (palabra clave: instrucciones de uso).
- La idea subyacente es evitar defectos y fallos sistemáticos que no (o apenas) se vean influidos por las características de diseño que contribuyen al PL (o SIL).
- Véase también el término “Fallos”.

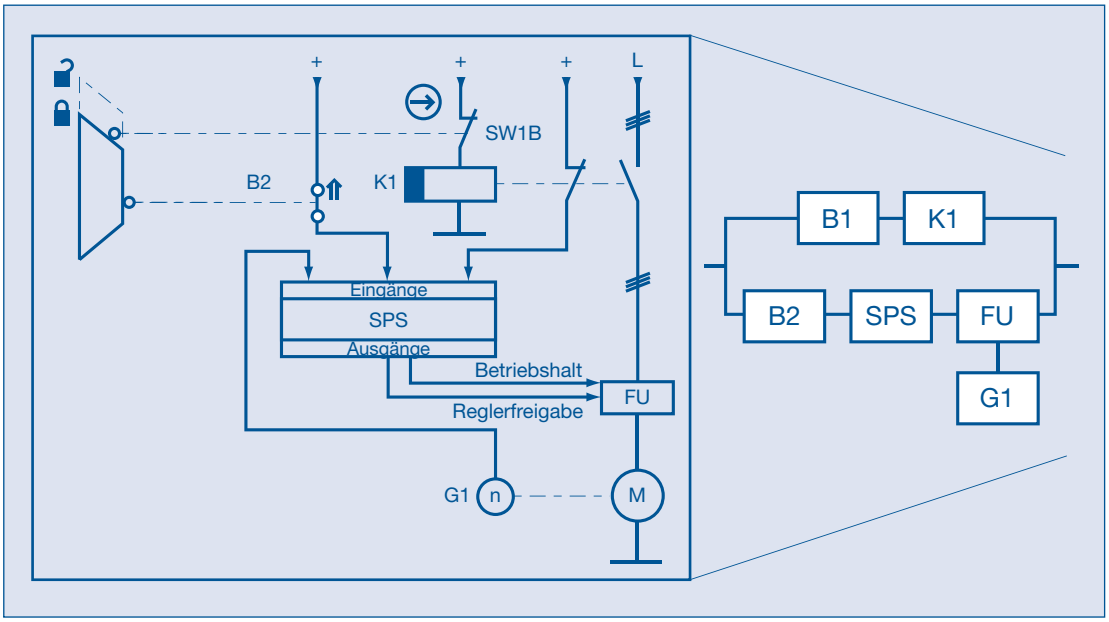
C

Cableado

Véase “Exclusión de defectos: conexión/cableado”.

Cálculos (cálculos de PL)

- De acuerdo con EN ISO 13849-1:2006, existen dos métodos fundamentalmente diferentes para calcular (estimar) un nivel de prestaciones (PL):
  - El método 1 consiste en un análisis discreto, es decir, las partes del sistema de mando de la máquina relativas a la seguridad se determinan (identifican) y estructuran en un diagrama de bloques utilizando el método de bloques (véase ejemplo).



  - Se establece la contribución relativa a $MTTF_d$, DC y CCF de cada bloque específico y, partiendo de fórmulas específicas y tablas de consulta, se contrasta con los valores globales respectivos. A continuación se realiza una valoración basada en la figura titulada “Relación entre las categorías, la DC_{avg}, el $MTTF_d$ de cada canal y el PL” de la norma EN ISO 13849-1:2006 (véase gráfico de barras en el lugar citado).
  - En la norma EN ISO 13849-1:2006, este método también se describe como el método de bloques, y se explica de forma detallada en el Anexo B. En el folleto, páginas 131 y siguientes, puede encontrarse un ejemplo extraído de la norma.

– El método 2 consiste en el análisis de subsistemas en relación con los cuales ya se ha designado o estimado un nivel de prestaciones PL (= sub-PL) y en la aplicación de la denominada tabla de combinación. El PL global se ve condicionado de forma fundamental por el sub-PL inferior (“a” < “b” < “c” < “d” < “e”) y por la cantidad de subsistemas (véase figura); esto significa que el PL global no se ve afectado hasta un número determinado de PL_{bajo}, mientras que a partir de un número específico de PL_{bajo} se reduce la categoría en un nivel debido a la adición de “riesgos residuales/probabilidades de defectos residuales” (véase el ejemplo de la norma). No obstante, la reducción de categoría no es necesaria cuando (como parte de un cálculo adicional sencillo), la suma de los valores de $MTTF_d$ individuales de la SRP/CS produce un valor global “alto” (>30 años) o un valor PFH_d correspondiente.

Cálculo del PL para la conmutación en serie de SRP/CS

PL_{baja}	N_{baja}	→	PL
a	>3	→	nulo, no permitido
	≤3	→	a
b	>2	→	a
	≤2	→	b
c	>2	→	b
	≤2	→	c
d	>3	→	c
	≤3	→	d
e	>3	→	d
	≤3	→	e

- En la norma EN IEC 62 061:2005 se ofrece un método similar (que funciona con $SIL_{subsistemas}$).
- Véanse también las páginas 45 y siguientes del folleto.

Categorías de control

- Terminología de EN 954-1:1996, en el futuro denominadas “arquitecturas designadas” (EN ISO 13 849-1:2006). Están relacionadas con los requisitos de seguridad aplicables a las SRP/CS con independencia de la tecnología, y se dividen en 5 niveles (categorías B, 1, 2, 3 y 4). Los niveles oscilan desde requisitos sencillos a requisitos complejos, como por ejemplo la seguridad/redundancia de 1 defecto y el autocontrol.
- De forma adicional a los requisitos relativos a la arquitectura, también forman parte de los requisitos de las categorías de control el cumplimiento de los denominados principios de seguridad básicos (a partir de la CC B) y, a partir de ahí (desde la CC 1), la consideración de los denominados principios de eficacia probada. Esto no debe confundirse con el requisito de utilizar componentes de eficacia probada (que solo es de aplicación a la CC 1). En los Anexos A–D de EN ISO 13 849-1:2003 (“Validación de una SRP/CS”) puede encontrarse una descripción de en qué consisten estos diferentes requisitos.
- Las categorías de control reflejan la resistencia a fallos de una SRP/CS y el comportamiento en caso de defecto.
- En la siguiente tabla se incluye una descripción breve de los requisitos asociados a las 5 categorías de control.

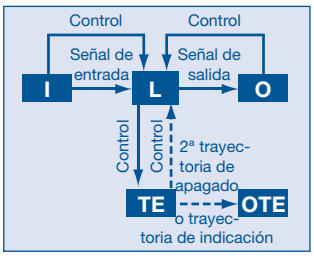
(1) No se pretende que las categorías deban utilizarse en ningún orden o clasificación jerárquica específicos en relación con los requisitos de seguridad.
(2) La aceptabilidad o no de la pérdida total o parcial de la función o funciones de seguridad como consecuencia de defectos se determina a partir de la valoración del riesgo.

Cat.[1]	Resumen de requisitos	Comportamiento del sistema[2]	Principios para obtener la seguridad
B	Las partes de sistemas de mando relativas a la seguridad y/o sus dispositivos de protección, así como sus componentes, se deben diseñar, construir, seleccionar, montar y combinar de acuerdo con las normas pertinentes de manera que puedan soportar las influencias esperadas.	Si se produce un defecto, este puede conducir a la pérdida de la función de seguridad.	Se caracterizan principalmente por la selección de los componentes.
1	Se deben aplicar los requisitos de B. Se deben utilizar componentes de eficacia probada y principios de seguridad de eficacia probada.	La aparición de un defecto puede conducir a la pérdida de la función de seguridad, pero la probabilidad de que se produzca dicho defecto es menor que en la categoría B.	
2	Se deben aplicar los requisitos de B y utilizar los principios de seguridad de eficacia probada. La función de seguridad debe ser comprobada a intervalos adecuados por el sistema de mando de la máquina.	• La aparición de un defecto puede conducir a la pérdida de la función de seguridad en el intervalo entre dos comprobaciones. • Mediante la comprobación se detecta la pérdida de la función de seguridad.	Se caracterizan principalmente por la estructura.
3	Se deben aplicar los requisitos de B y utilizar los principios de seguridad de eficacia probada. Las partes relativas a la seguridad se deben diseñar de manera que: • un solo defecto en cualquiera de estas partes no conduzca a la pérdida de la función de seguridad, y • siempre que se realicen pruebas de forma adecuada, se detecte dicho defecto.	• Cuando se produce un solo defecto, la función de seguridad se desempeña siempre. • Algunos defectos se detectan, pero no todos. • La acumulación de defectos no detectados puede conducir a la pérdida de la función de seguridad.	Se caracterizan principalmente por la estructura.
4	Se deben aplicar los requisitos de B y utilizar los principios de seguridad de eficacia probada. Las partes relativas a la seguridad se deben diseñar de manera que: • un solo defecto en cualquiera de estas partes no conduzca a la pérdida de la función de seguridad, y • se detecte dicho defecto en el momento de, o antes de, la siguiente solicitación de la función de seguridad, pero si esta detección no es posible, una acumulación de defectos no detectados no debe conducir a la pérdida de la función de seguridad	• Cuando se produce un solo defecto, la función de seguridad se desempeña siempre. • Los defectos se detectan a tiempo para impedir la pérdida de la función de seguridad.	Se caracterizan principalmente por la estructura.

Categorías de control/categoría de control 2

- En este documento no se tratarán en profundidad los requisitos y el contenido de las categorías de control, ya que se las conoce desde hace muchos años por la norma EN 954-1:1996. En el parágrafo “Categorías de control” puede encontrarse una presentación general.
- Como excepción a lo anterior, deseamos hacer mención del hecho de que, en la norma EN ISO 13849-1:2006, se han incrementado los requisitos de la categoría de control 2. En la práctica, a partir de ahora esta categoría será una especie de categoría de control 3 “edulcorada”.
- Explicación de fondo: dada la posibilidad de que el fallo de una función de seguridad en la CC 2 pase desapercibido en los intervalos entre comprobaciones, la frecuencia de comprobación constituye un factor crítico. Además, el propio equipo de control y comprobación podría fallar antes que el canal de la función. Por este motivo, en la cuantificación se requiere:
  – que el valor de $MTTF_d$ del equipo de control y comprobación (TE) no sea inferior a la mitad del valor de $MTTF_d$ de la lógica L y

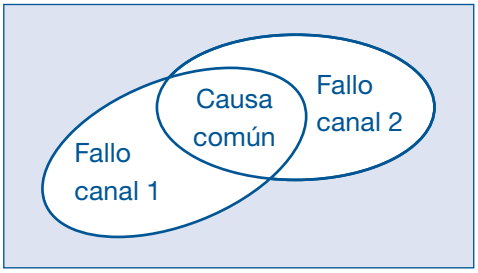
– que la frecuencia de control y comprobación sea como mínimo 100 veces superior a la tasa de solicitación media del equipo de seguridad o a la tasa de fallos peligrosos;
– a esto hay que añadir el requisito de un segundo camino de apagado (a través del equipo de control y comprobación).



- En particular, el ratio requerido de 1:100 de la tasa de solicitación con respecto a la frecuencia de control y comprobación implica que las estructuras de CC 2 con tecnología electromecánica (sin inteligencia de control y comprobación propia) deben desempeñar tareas apenas realizables. El motivo que explica el aumento de los requisitos de la categoría de control 2 es que en el futuro podrá conseguirse un nivel de prestaciones “d” en relación con un valor de $MTTF_d$ “alto” y una DC “media”. Debemos recomendar a nuestros clientes que contemplen opciones de diseño alternativas para este nivel de criticidad. Si con el tiempo obtenemos información relativa a nuevas opciones de diseño, se lo haremos saber.
- Por otra parte, hasta un PL “c” sería suficiente un valor de $MTTF_d$ “alto” y una arquitectura de categoría de control 1 (1 canal, pero ejecutado con componentes de seguridad de eficacia probada). Esto significa que puede seguir utilizándose tecnología electromecánica para el intervalo de riesgo medio típico (es decir, un PL “c”). Así pues, a pesar del aumento de los requisitos de la CC 2, no existe ninguna diferencia significativa en comparación con la situación actual de la tecnología de seguridad.

CCF (fallo de causa común), medidas contra CCF, gestión de CCF

- Definición de la norma (EN ISO 13 849-1:2006): fallo de varios elementos que resultan de un solo suceso y que no son consecuencia unos de otros (no debe confundirse con fallos similares).
- El CCF se basa en un análisis de defectos muy específico y tiene por objetivo garantizar que se introducen medidas adecuadas para evitar fallos que afecten a más de un canal de la SRP/CS al mismo tiempo y que, por tanto, puedan derivar en la inoperancia de la función de protección de un sistema a pesar de contar con varios canales.
- El CCF también se denomina factor β en la terminología utilizada en las normas EN IEC 62 061:2005 y EN IEC 61 508:2001. Estos fallos específicos también se describen en otros lugares como “fallos de modo común”.



- Un ejemplo típico de CCF son los efectos de la radiación electromagnética, como por ejemplo un pulso de sobretensión que afecte a las salidas de semiconductores realizadas de forma redundante, con el resultado negativo simultáneo y coincidente de que ya no es posible desconectar los transistores de ambos canales. Otros ejemplos serían la ausencia de medidas de filtrado con tecnología de fluidos o defectos derivados de las condiciones climáticas, como por ejemplo la humedad.
- En la tabla F.1, EN ISO 13 849-1:2006 enumera medidas habituales contra CCF (véase la siguiente figura) y evalúa cada medida asignándole una puntuación. EN ISO 13 849-1:2006 considera que se han adoptado medidas suficientes contra los riesgos de CCF cuando la suma de las puntuaciones correspondientes a las medidas adoptadas genera una puntuación de más de 65 puntos (de un máximo de 100); en este caso, puede colocarse una marca de visto bueno junto a la puntuación de “gestión de CCF”.

- Deben garantizarse medidas adecuadas contra CCF en todos los casos a partir de la categoría de control 2.

Proceso de puntuación y cuantificación de las medidas contra los CCF

Nº	Medida contra los CCF	Puntuación
1	**Separación/aislamiento**	
	Separación física entre los caminos de las señales	15
2	**Diversidad**	
	Utilizar diferentes tecnologías/principios de diseño o principios físicos	20
3	**Diseño/aplicación/experiencia**	
3.1	Protección contra sobretensión, sobrepresión, sobreintensidad, etc.	15
3.2	Utilización de componentes de eficacia probada	5
4	**Evaluación/análisis**	
	¿En el diseño se tienen en cuenta los resultados de un análisis de los modos de fallo y sus efectos para evitar los fallos de causa común durante el desarrollo?	5
5	**Competencia/formación**	
	¿Han sido formados los diseñadores para entender las causas y consecuencias de los fallos de causa común?	5
6	**Medio ambiente**	
6.1	Protección de la contaminación y de las perturbaciones electromagnéticas (CEM) contra los CCF de conformidad con las normas pertinentes.	25
6.2	Otras influencias: ¿se han tenido en cuenta los requisitos relativos a la inmunidad contra todas las influencias ambientales pertinentes, tales como la temperatura, los choques, las vibraciones, la humedad (por ejemplo, tal como se especifica en las normas pertinentes)?	10
	Total	100

Circuito conmutado de reinicio

- Normalmente se incluyen aquí las señales de reinicio/rearme manuales (y, en casos excepcionales, automáticas) del nivel **L**.
- El operador debe asegurarse por anticipado de que es posible reiniciar de forma segura el sistema de mando de la máquina.
- La norma EN ISO 13849-1:2006 estipula de forma inequívoca que en el futuro se requerirá un cambio por flanco para el reinicio. Remítase también a la página 28.
- En el nivel **O** suelen fusionarse el circuito conmutado de reinicio y el circuito de realimentación.

Circuito de realimentación

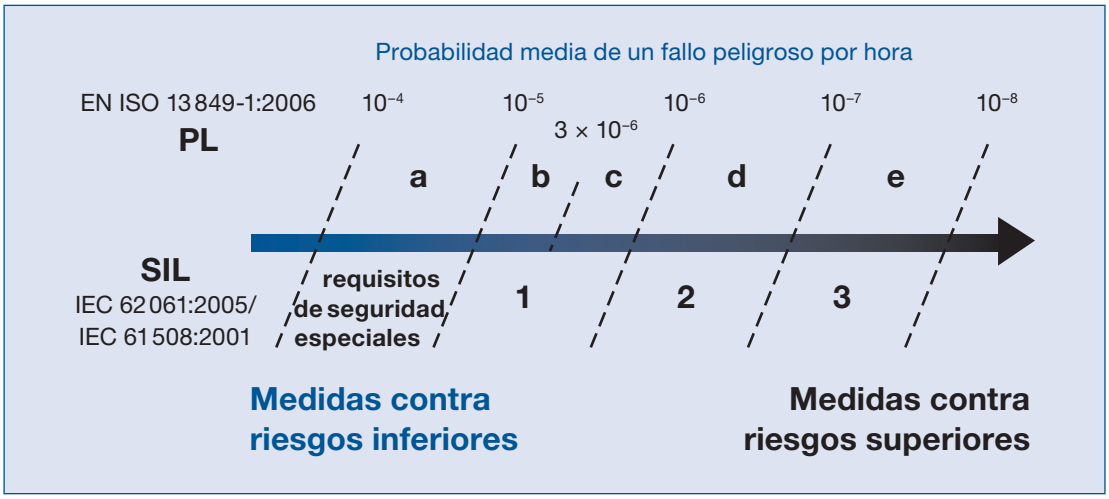
- Medida para detectar defectos en el nivel de salida **O** cuando estos sean realizados por dispositivos únicos sencillos, como por ejemplo contactores.
- El resultado de comprobación de otras medidas también puede “verterse” en este caso para garantizar que el controlador de la máquina tan solo puede reiniciarse una vez que las partes de la SRP/CS en cuestión funcionan correctamente.
- La cobertura del diagnóstico (DC) puede ser de hasta el 99% dependiendo de la calidad de las señales de realimentación.
- Véase también la página 55.

Cobertura de diagnóstico, DC

- Véase sección 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”, así como páginas 32 f. y 68 f.

Compatibilidad SIL ↔ PL /PL ↔ SIL

- Dado que la norma EN IEC 61 508-2001 se encuentra por detrás de las dos normas nuevas relativas a SRP/CS, la información de SIL y PL de ambas normas es compatible, es decir, un PL puede expresarse de forma simplificada como un SIL, y un SIL de forma simplificada como un PL. En este caso, un criterio de medición común es la probabilidad de un fallo peligroso por hora (PFH_d), de acuerdo con lo siguiente:



- Aunque el procedimiento mencionado anteriormente es aplicable de forma global, también puede utilizarse en relación con subsistemas o sistemas parciales, en cuyo caso se cuenta con la ventaja específica, por ejemplo, de que los dispositivos calificados con SIL pueden integrarse en análisis de PL de acuerdo con EN ISO 13 849-1:2006 y, a la inversa, los dispositivos calificados con PL en análisis de SIL de acuerdo con EN IEC 62 061:2005.
- Cuando se realicen cálculos sin utilizar la tabla de combinación (tabla 11 de EN ISO 13 849-1:2006), en los subsistemas se recomienda utilizar como máximo un 20 % del PFH_d global para los niveles **I** y **L**, de forma que quede > 60 % para el nivel **O** (que, de acuerdo con la experiencia, constituye el eslabón más débil de la cadena).
- Observación: en relación con la conversión de valores de $MTTF_d$ en valores PFH_d, y viceversa: véase término “Anexo K” de EN ISO 13 849-1:2006.

Comprobación/intervalo de comprobación

- Comprobación repetitiva/inspección recurrente de la SRP/CS realizada para detectar defectos de forma que, en caso necesario, pueda reinstaurarse el sistema en su estado inicial (“como nuevo”) o lo más cerca posible de este. En este caso, el recuento se inicia utilizando una nueva duración de la misión.
- Algunos usos típicos de las comprobaciones y los intervalos de comprobación son los productos químicos y la ingeniería de procesos; otro ejemplo sería el mantenimiento de aeronaves.
- Este tema apenas afecta a nuestros dispositivos (exceptuando el análisis del valor T_{10d} en los dispositivos sujetos a desgaste).
- Esto no afecta a la obligación impuesta sobre el empleador de llevar a cabo inspecciones periódicas de los equipos de trabajo en aplicación de la Directiva CE de Utilización de Equipos de Trabajo, o bien, en Alemania, a las obligaciones provenientes de las disposiciones en materia de seguridad ocupacional (BetrSichV).

Conexiones en serie

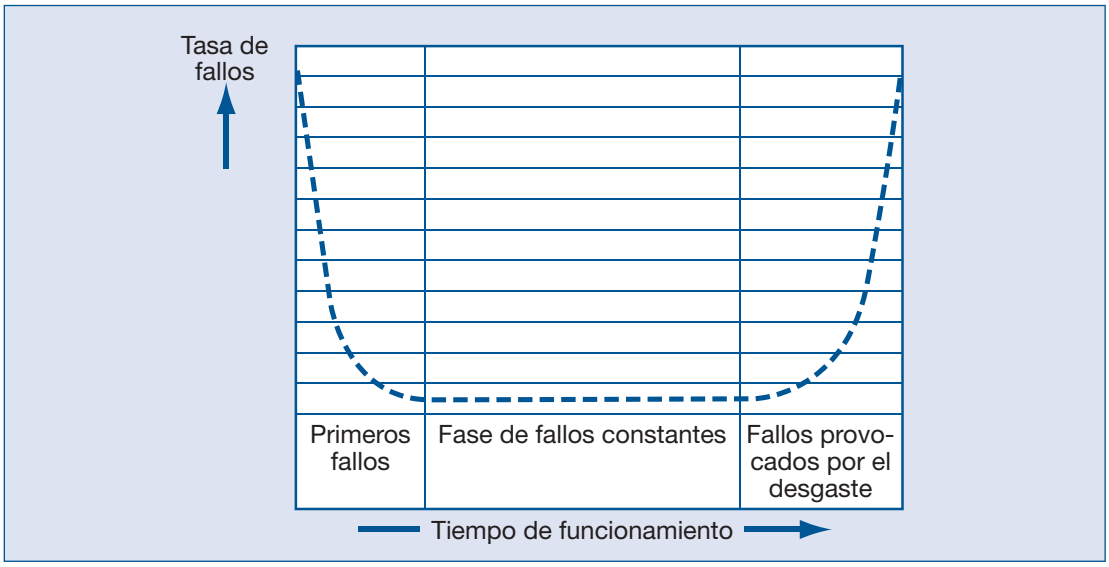
- La longitud de una conexión en serie (y, por tanto, el alcance relativo de la probabilidad residual de defectos, mayor cuanto más larga sea la conexión) viene determinada por la definición de la función de seguridad (véase también página 32 f.).
- De acuerdo con esta perspectiva, pueden conectarse en serie más de 31 dispositivos CSS, por ejemplo, sin que ello lleve asociado una reducción de los niveles SIL o PL, siempre que haya varias funciones de seguridad, independientes entre sí, que protejan el número de dispositivos.
- No obstante, el argumento de la detección total de defectos (DC ≥ 99 %) en la "familia" CSS sigue siendo totalmente válido.

Conexiones en serie de dispositivos electromecánicos

- En el pasado, argumentamos que las conexiones en serie de dispositivos electromecánicos tan solo constituyen una categoría de control 3. La calificación como CC 4 no es posible porque no es posible detectar todos los defectos de la conexión en serie, y en determinadas circunstancias no puede excluirse una acumulación de defectos (véase figura de la página 32 f.).
- Aunque no hay ninguna variación en lo relativo a este criterio, es decir, no se permite que un módulo SRB o un SiSPS posean una cobertura del diagnóstico "alta" (≥ 99 %) en caso de conexión en serie, en el futuro también podrá obtenerse un PL "d" con una arquitectura de CC 3. Tras consultar al BGIA, recomendamos realizar los cálculos partiendo de una DC del 60 % (véase sección pertinente de la presente, en particular la página 32 f.).
- Ahora bien, también es posible contar con conexiones en serie con un PL "e" cuando los contactos de la conexión en serie del PLC en condiciones de funcionamiento normales se contrasten y evalúe su verosimilitud en ese punto (véase ejemplo de conexión 8.2.28 del BGIA, página 76), o bien cuando puedan realizarse exclusiones de defectos en el nivel de entrada (véase ejemplo de conexión 8.2.29 del BGIA, página 75).

Curva de la bañera

- Representación de diagrama de la vida útil del dispositivo/tasa de fallos de (típicamente) los componentes electrónicos y los dispositivos y sistemas con tasas de fallos constantes en la fase II. Al tener en cuenta la fase I (primeros fallos) y la fase III (final de la vida útil), la representación de diagrama produce una curva de aspecto similar a una bañera.
- Véanse también los términos "Distribución exponencial" y "Tasas de fallos".
- Productos típicos: sensores de seguridad electrónicos, dispositivos de protección opto-electrónicos (AOPD), PLC de seguridad, sistemas de bus, etc.
- No es posible utilizar tasas de fallos con "comportamiento de curva de bañera" de forma sistemática en relación con una SRP/CS, ya que, con frecuencia, los componentes, dispositivos y sistemas se utilizan con tecnologías a las que no es de aplicación la tasa de fallos constante de la fase II, como por ejemplo tecnología de fluidos, ingeniería eléctrica y mecánica. En estos casos debería realizarse un análisis del valor B_{10d} (véase sección pertinente) de forma previa al cálculo de los valores de $MTTF_d$.



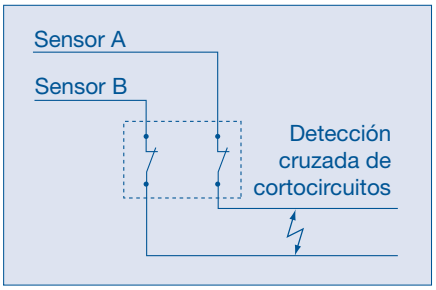
D

Detección de defectos, DC

- Véase la parte 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”, así como las páginas 32 f. y 68 f.

Detección de defectos (externa)

- Cuando se utilizan dispositivos únicos sencillos dentro de una SRP/CS, la responsabilidad relativa a detecciones de defectos recae en otras partes de la SRP/CS situadas aguas arriba o aguas debajo de los dispositivos únicos sencillos (normalmente, en el procesamiento de la señal de la unidad lógica o en un equipo de control y comprobación especial).
- En estos casos, es necesario saber qué medidas de detección de defectos son efectivas y, por supuesto, la aplicación de los dispositivos únicos sencillos debe ser correcta, es decir, deben ir integrados en la lógica (por ejemplo, contactores aguas abajo, preferentemente con contactos forzados y circuito de realimentación).
- Cuando proceda, debe consultarse qué medidas de detección de defectos son efectivas en relación con las partes aguas arriba y aguas debajo de la SRP/CS. Además, también deben cumplirse todos los requisitos de las categorías de control, como por ejemplo los relativos a la disposición del cableado, etc.
- En teoría, se crea un subsistema o sistema parcial propio.
- Véase también la página 32 f.
- Puede asumirse una cobertura del diagnóstico de 99% en relación con el nivel de entrada cuando se utilicen módulos de relé de seguridad, en la medida en que estos sean compatibles con la CC 4, el PL e o el SIL 3 (medida de la tabla E: control de unidades electromecánicas con contactos forzados). No obstante, en el nivel de salida la cobertura del diagnóstico depende de forma fundamental del tipo de salida.



- Cuando, por ejemplo, el control de un contactor se realice mediante contactos forzados de direccionamiento positivo con circuito de realimentación, también puede conseguirse una DC del 99 %.

- Puede asumirse una cobertura del diagnóstico del 99% en el nivel de entrada en relación con los PLC de seguridad, los sistemas bus de seguridad, etc. (debido, en este caso, a la denominada comparación cruzada de datos) (siempre que, al igual que antes, exista compatibilidad con CC 4, PL e o SIL 3). Lo anterior es de aplicación también al nivel de salida (véase: módulos de relé de seguridad).
- ADVERTENCIA: las versiones indicadas anteriormente no son de aplicación a todas las variantes como por ejemplo a las conexiones en serie de interruptores electromecánicos de seguridad, ya que la función lógica no siempre detecta determinados defectos que pueden producirse dentro de una cadena. En este caso, para conseguir una cobertura del diagnóstico del 99 %, deben incorporarse dispositivos con una conexión 1:1; de lo contrario, se requerirán medidas adicionales (por ejemplo un equipo de control y comprobación externo).
- Para más información sobre la detección de defectos en conexiones en serie, y más concretamente en el caso de la conexión en serie de dispositivos electromecánicos, véase la página 32 f.

Directiva de Máquinas (DM)

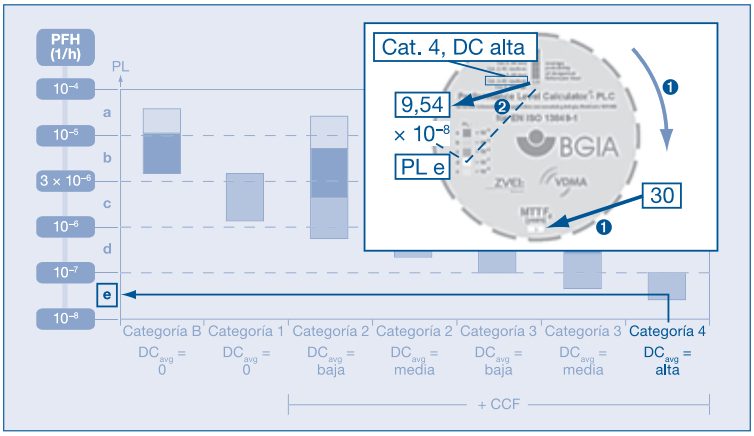
- La Directiva de Máquinas de la CE (DM) constituye la base legal de los requisitos de seguridad funcional de maquinaria en la Unión Europea y los demás países de la AELC, incluyendo, Islandia, Liechtenstein, Noruega y Suiza, así como Turquía en vistas de su acceso previsto a la UE.
- Al igual que con todas las directivas comunitarias, el contenido de la DM debe trasponerse a los respectivos derechos nacionales. En el caso de la DM, en Alemania esto se ha realizado en el marco de la Ley de Seguridad de Productos y Equipos (GPSG), en forma de la denominada Ordenanza de Máquinas (= 9. GPSG-VO).
- La necesidad de las partes de los sistemas de mando relativas a la seguridad (= SRP/CS) procede de los principios generales (palabra clave: análisis de riesgos o, en el futuro, valoración del riesgo), así como de los requisitos del punto 1.2.1 (palabra clave: seguridad y fiabilidad de los sistemas de mando) del Anexo 1[1] de la DM.
- La necesidad de las SRP/CS se explica adicionalmente en el punto 9.4 “Función de mando en caso de defecto” de EN IEC 60 204-1:2005[2], donde se hace referencia en última instancia (en lo que concierne a la definición concreta) a la competencia de EN ISO 13 849-1:2006 y EN IEC 62 061:2005. El concepto graduado se basa en los principios generales de la DM.

[1] Véase la DM 2006/42/CE, vigente desde el 29-12-2009, o la DM 98/37/CEE vigente en la actualidad

[2] Elektrische Ausrüstung von Maschinen (equipos eléctricos de máquinas); fuente: Beuth-Verlag, Berlín

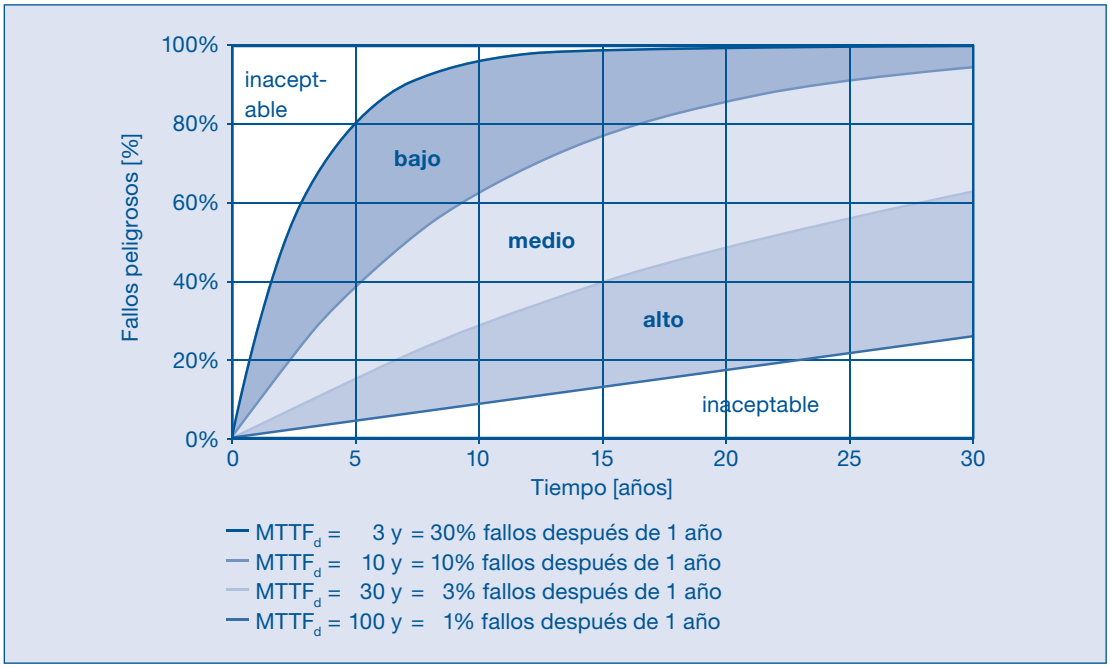
Disco del BGIA

- Una herramienta de apoyo elaborada por el BGIA en la que se muestra la relación existente, por una parte, entre el PL y el PFH_d, y, por otra, entre el $MTTF_d$, la DC y los CCF. En esencia, constituye una reproducción del Anexo 6 de EN ISO 13 849-1:2006.



Distribución exponencial

- La distribución exponencial es una distribución de probabilidad constante a lo largo del conjunto de números reales positivos con una distribución de vida útil típica; se expresa, por ejemplo, en valores de MTTF o MTBF, y se utiliza para estimar la vida útil de los componentes, dispositivos etc. cuando no es necesario tener en cuenta los efectos del envejecimiento (desgaste).
- Se utiliza un análisis ascendente del valor B_{10d} con relación a los componentes y dispositivos afectados por desgaste.
- Un valor de $MTTF_d$ asume/significa que:
  – un 63 % de todas las unidades ha sufrido fallos peligrosos;
  – un 37 % de todas las unidades sigue funcionando correctamente.
- En la norma EN ISO 13849-1:2006 se dividen los valores de $MTTF_d$ en tres grupos por canal:



Duración de misión (vida útil)

- Los modelos de probabilidad matemática que subyacen a la norma EN ISO 13849-1:2006 presuponen una duración de la misión de 20 años. Una excepción a esto es el análisis de los valores B_{10d} o T_{10d} en relación con las sustituciones preventivas de dispositivos que puedan ser necesarias. En contraposición, las denominadas comprobaciones, intervalos de comprobación y similares desempeñan una función de menor importancia en el ámbito de la ingeniería en lo que concierne a los niveles PL y SIL.

Entrada en vigor

- La norma EN ISO 13 849-1:2006 entró en vigor en el otoño de 2006. Aunque IEC EN 62 061:2005 ya goza de vigencia, es posible que la norma EN 954-1:1996 (y ISO 13 849-1:1999) pueda seguir aplicándose hasta diciembre 2009 (con presunción de conformidad con la Directiva de Máquinas de la CE).
- Para más información, véase también el término “Periodo de transición”.

Equipos de control y comprobación

- Los equipos de control y comprobación se utilizan para la detección de defectos (cobertura del diagnóstico) en SRP/CS. Pueden implantarse en los canales de una SRP/CS, por ejemplo en el SPS de seguridad o en el módulo SRB. También pueden funcionar como equipo de control y comprobación externo, sin integración en los canales de una SRP/CS, por ejemplo como parte de las funciones del SPS operativo. En este caso existen algunos requisitos adicionales sobre el equipo de control y comprobación, aunque normalmente estos no suponen un obstáculo insalvable. Véase también, en este sentido, el ejemplo de conexión 8.2.28 del BGIA (página 76).

Estimación de PL y SIL

- Tanto EN ISO 13 849-1:2006 como EN IEC 62 061:2005 utilizan de forma consciente el término “estimación” en relación con la determinación de niveles PL y SIL para dejar bien claro que, en el caso de los requisitos cuantitativos (probabilistas), no se trata de calcular un valor preciso y absoluto.
- En el caso de una SRP/CS sencilla, en el marco de los PL “a” a “c”, la norma EN ISO 13 849-1:2006 incluso llega a estipular que es suficiente una estimación cualitativa (véase punto 4.5.1).
- El hecho de que una estimación sea suficiente se explica por el afán de simplificación perseguido por ambas normas y por el enfoque determinista en la categoría de control, que sigue desempeñando un papel importante. En particular, a esto debe añadirse el hecho de que, en la práctica, los fallos aleatorios, contra los que se dirigen de forma específica las medidas cuantitativas (probabilistas), tan solo están implicados entre un 10 y un 15 % de los accidentes producidos en la construcción de máquinas. De acuerdo con otras estimaciones, esta proporción es incluso menor.

Exclusión de defectos

- La exclusión de defectos constituye un punto medio entre los requisitos técnicos de seguridad (el análisis de defectos requerido) y la posibilidad teórica de que se dé un defecto.
- Tal como indica su nombre, durante la valoración de seguridad (FMEA) se excluyen determinados casos de fallos o defectos en una SRP/CS (su incidencia no se acepta/no se permite que se acepte).
- Así pues, las exclusiones de defectos permiten simplificaciones (parcialmente sustanciales) en el diseño de la arquitectura de una SRP/CS, por ejemplo en cuestiones relativas a la necesidad de un diseño redundante o en cuestiones concernientes al diseño de los cables de conexión en una SRP/CS; no obstante, la posibilidad de la exclusión de defectos no debe utilizarse de forma arbitraria y subjetiva. Por el contrario, el análisis realizado debe ir acompañado de justificaciones matizadas y documentos escritos.
- Debe distinguirse entre el uso de exclusiones de defectos respaldado por las prácticas vigentes del sector o su uso a título individual (sin este respaldo).
- Se considera que los Anexos A–D de EN ISO 13 849-2:2003 constituyen la expresión definitiva de las prácticas vigentes del sector en el ámbito de la seguridad de máquinas. En ellos se establece qué exclusiones de defectos pueden admitirse de forma automática en función de la tecnología (mecánica, hidráulica, neumática o eléctrica), cuáles tan solo son admisibles en determinadas circunstancias, y cuáles son inadmisibles.

- La posibilidad de la exclusión de defectos se describe en la norma EN ISO 13849-1:2006 como sigue: La exclusión de defectos se puede basar en:
  - la improbabilidad técnica de que ocurran determinados defectos;'
  - la experiencia técnica generalmente admitida, que se puede utilizar independientemente de la aplicación considerada; y
  - los requisitos técnicos relativos a la aplicación y el riesgo específico estudiado.
- Al excluirse defectos debe aportarse una descripción detallada en los documentos técnicos.
- La siguiente demarcación es pertinente para las exclusiones de defectos: la combinación de partes de un sistema de mando relativas a la seguridad empieza en el punto en que se generan las señales de seguridad (incluido, a título ilustrativo, el accionador y el rodillo de un interruptor de posición) y finaliza en las salidas de los elementos de control eléctrico (incluidos, a título ilustrativo, los contactos principales de un contactor).
- Véanse también las páginas 29 y siguientes.

Exclusión de defectos: conexión/cableado

- La norma EN ISO 13849-1:2006 favorece la asunción de que pueden realizarse exclusiones de defectos en relación con el cableado de una SRP/CS.
- A continuación se indican los requisitos para una exclusión de defectos:

Aceptación de defectos	Exclusión de defectos
Cortocircuito entre dos conductores cualquiera	Cortocircuitos entre conductores – instalados de forma permanente (instalación fija) y protegidos contra daños externos (por ejemplo mediante conducto para cable o conducto armado); o – protegidos en cables resguardados diferentes; o – incluidos en un espacio de instalación eléctrica[(1)]; o – protegidos de forma individual mediante un cable de tierra.
Cortocircuito entre un conductor y una parte conductora no protegida, la tierra, o una conexión de conductor de protección	Cortocircuitos entre un conductor y una parte no protegida en un espacio de instalación[1].
Interrupción de un conductor	No

(1) El prerrequisito es que tanto los cables como el espacio de instalación se ajusten a los requisitos aplicables (véase la norma EN 60204-1 [IEC 60204-1]).

- De forma alternativa, recomendamos a nuestros clientes que utilicen un equipo de procesamiento de señales con control cruzado adicional.

Exclusión de defectos en caso de dispositivos activados de forma manual

- Dispositivos de control de parada de emergencia, interruptores de validación, etc.; véanse páginas 29 y siguientes.

Exclusión de defectos en caso de dispositivos de enclavamiento

- Función física/eléctrica de 2 canales de interruptores de control con enclavamiento para dispositivos de protección móviles: véanse páginas 29 y siguientes.

Fallos

- Definición de la norma (EN ISO 13 849-1:2006): cese de la aptitud de una unidad (subsistema) para cumplir una función requerida.
- Uno de los objetivos importantes de la normalización en este ámbito consiste en reducir el riesgo de fallos en una SRP/CS que provoquen estados peligrosos.
- Las perturbaciones se equiparan a fallos.
- En la normalización relativa a SRP/CS se distingue entre fallos aleatorios y sistemáticos, así como entre fallos peligrosos (la información relativa a valores a menudo se identifica mediante un subíndice “d”) y fallos no peligrosos (que obstaculizan la disponibilidad de procesos). Estos últimos no se incluyen en el ámbito de aplicación de la normativa relativa a SRP/CS.
- El resultado de los fallos es la presencia de defectos en la SRP/CS. De acuerdo con las definiciones de la norma, los fallos son sucesos y los defectos estados. No obstante, también pueden producirse defectos sin que ocurran fallos de forma anterior. Deben adoptarse medidas también contra defectos, medidas que se abordan en particular en la norma EN ISO 13 849 2:2003.
- Dado que esta distinción entre lo que constituye un “fallo” y lo que significa un “defecto” está en gran parte relacionada con matices semánticos, en algunas partes de este folleto se utilizan ambos términos de forma indistinta.

Fallos (fallos aleatorios)

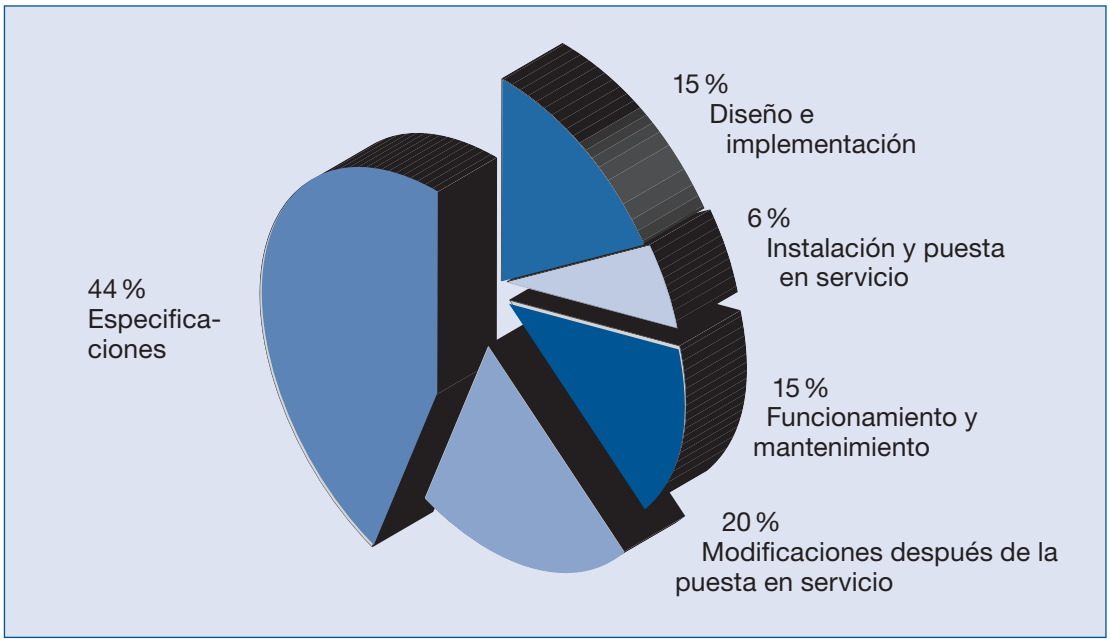
- En particular, el requisito de determinar la calidad global relativa a la seguridad de una SRP/CS en forma de PL o SIL tiene como objetivo reducir el riesgo residual de estados peligrosos originados por fallos peligrosos aleatorios.
- En el caso del hardware, se asume de forma fundamental que puede fallar tanto de forma aleatoria como sistemática. Por el contrario, el software tan solo sufre fallos sistemáticos.
- Es posible asignar una probabilidad estadística a los fallos aleatorios del hardware (debido al debilitamiento del producto por diversas causas, como por ejemplo la fatiga de los materiales). Dicho de otro modo: cuanto menor sea esta probabilidad, mayor será la seguridad funcional. Cuando proceda, puede prescindirse de otros elementos sin que ello afecte a la calidad global relativa a la seguridad.
- Normalmente, en la actualidad se estima que la proporción de accidentes derivados de fallos aleatorios del hardware es reducida. Se habla de un máximo de entre el 10 y el 15 % de todos los accidentes con máquinas. De acuerdo con otras estimaciones, el porcentaje es aún menor.
- La probabilidad de fallos aleatorios del hardware constituye un dato exclusivamente estadístico y no permite extraer conclusiones en torno a la calidad de un producto concreto.

Fallos (fallos sistemáticos)

- Definición de la norma (EN ISO 13 849-1:2006): fallo asociado de forma determinista a una cierta causa, que solamente puede ser eliminado mediante una modificación del diseño o del proceso de fabricación, de los procedimientos de trabajo, de la documentación o de otros factores apropiados.
- Los fallos sistemáticos pueden afectar tanto al hardware como al software.
- En el nuevo Anexo G de EN ISO 13 849-1:2006 vuelven a considerarse de forma adicional las medidas destinadas a evitar y controlar los fallos sistemáticos. Decimos que “se consideran de forma adicional” porque las normas EN 954-1:1996 (ISO 13 849-1:1999) y, en particular, EN ISO 13 849-2:2003 (concebidas originalmente como EN 954-2), ya incluyen requisitos deliberados a los que se da continuidad y que se mejoran en el Anexo G.
- También, también pueden encontrarse análisis detallados de este tema en la norma EN IEC 62 061:2005.

- En la actualidad, la causa de la mayor parte de los accidentes con máquinas se explica por fallos sistemáticos. Entre estos se incluyen la realización inadecuada de análisis FMEA y comprobaciones, la existencia de lagunas en el diseño y las especificaciones, así como los errores de razonamiento. A esto cabe añadir los accidentes derivados de la manipulación de dispositivos de protección (que, de acuerdo con las estimaciones, representan en Alemania aproximadamente un 25 %).
- Aunque no se haya incluido de forma precisa en el sistema propuesto en la norma, una valoración del riesgo (análisis de riesgos) exhaustiva debería formar parte del contexto de determinación del potencial de defectos sistemáticos. Véanse también EN ISO 12 100-1/ -2:2003 y EN ISO 14 121:2007 (antes EN 1050).
- De acuerdo con un estudio británico (véase figura), más del 60 % de todos los accidentes estudiados como parte de un estudio representativo podían atribuirse a causas ya presentes en la SRP/CS antes de la puesta en servicio.

(1) ¡Más del 60 % de los fallos están "integrados en los sistemas relativos a la seguridad" antes de su puesta en servicio!



Fiabilidad del hardware, $MTTF_d$

- Véase la parte 6, páginas 81 y siguientes: "Características y aplicación de EN ISO 13 849-1:2006".

Fórmula de simetrización

- Véase término "Adición de probabilidades de fallo".

Función de seguridad

- A una función de seguridad debe asignarse una clasificación de PL requerido de acuerdo con EN ISO 13 849- 1:2006 o un nivel SIL de acuerdo con EN IEC 62 061:2005. Según la definición (véase EN ISO 13 849-1:2006), se trata de una función de una máquina cuyo fallo podría dar lugar a un aumento inmediato del (de los) riesgo(s).
- Por tanto, la definición de la función de seguridad afecta de forma considerable a la determinación del PL o el SIL.
- Para más información: véanse páginas 70 y siguientes

Gestión de CCF/medidas contra CCF

- Véase "CCF (fallo de causa común), medidas contra CCF, gestión de CCF".

Gráfico de barras

- Véase sección pertinente de la presente y parte 6, página 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

Gráfico de resultado PL

- Véase también la parte 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

Gráfico de resultados PL (gráfico de barras)

- Véase sección pertinente de la presente y la sección 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

Gráfico del riesgo, evaluación del riesgo

- Las dos nuevas normas sobre SRP/CS incluyen un gráfico del riesgo utilizado como ayuda para determinar el nivel necesario de reducción del riesgo de la SRP/CS o los niveles PL o SIL correspondientes.
- Si pasamos por alto el análisis diferenciado de EN IEC 62 061:2005, los enfoques y resultados son en gran medida comparables. En algunos casos límite, la norma EN ISO 13 849-1:2006 puede ser algo “más estricta” (estipulando una clase de requisito más elevada).

Informe 2/08 del BGIA

- Este informe, titulado “Funktionale Sicherheit von Maschinensteuerungen – Anwendung der DIN EN ISO 13 849” (Seguridad Funcional de los Sistemas de Mando de Máquinas – Profundización en la norma DIN EN ISO 13 849), profundiza en el conocimiento de la norma EN ISO 13 849-1:2006.
- El informe ha sido publicado por el BGIA, Instituto Alemán de Salud y Seguridad Ocupacionales del Sector Alemán de los Seguros Legales contra Accidentes (DGUV), St. Augustin, y puede descargarse en www.dguv.de o solicitarse en formato papel al BGIA (o a nosotros).
- El informe posee aproximadamente 260 páginas y se divide en los siguientes capítulos:
  - Prólogo
  - Introducción
  - Presentación general del informe y la norma
  - Funciones de seguridad y su contribución a la reducción de riesgos
  - Diseño de sistemas de mando seguros
  - Verificación y validación
  - Ejemplos de conexión para SRP/CS
  - Bibliografía

  + 10 Anexos
- Cabe hacer mención, en particular, de los 37 ejemplos de conexión, aunque no se trate de “recetas”.
- Véanse también las páginas 73 y siguientes.
- Un ejemplo típico de CCF son los efectos de la radiación electromagnética, como por ejemplo un pulso de sobretensión que afecte a las salidas de semiconductores realizadas de forma redundante, con el resultado negativo simultáneo y coincidente de que ya no es posible desconectar los transistores de ambos canales. Otros ejemplos serían la ausencia de medidas de filtrado con tecnología de fluidos o defectos derivados de las condiciones climáticas, como por ejemplo la humedad.

- En la tabla F.1, EN ISO 13849-1:2006 enumera medidas habituales contra CCF (véase la siguiente figura) y evalúa cada medida asignándole una puntuación. EN ISO 13849-1:2006 considera que se han adoptado medidas suficientes contra los riesgos de CCF cuando la suma de las puntuaciones correspondientes a las medidas adoptadas genera una puntuación de más de 65 puntos (de un máximo de 100); en este caso, puede colocarse una marca de visto bueno junto a la puntuación de "gestión de CCF".
- Deben garantizarse medidas adecuadas contra CCF en todos los casos a partir de la categoría de control 2.

- En la tabla puede apreciarse que, en el caso de los dispositivos únicos sencillos, tan solo existe una posibilidad matizada de determinar completamente la puntuación de CCF de forma anticipada, ya que las unidades de análisis 1 y 2, en particular, constituyen áreas cuya configuración compete al cliente. Las unidades de análisis 3, etc., por el contrario, están sobre todo relacionadas con el diseño y son específicas del dispositivo, y ya proporcionan la puntuación mínima de 65 necesaria para los dispositivos únicos sencillos.

Interruptor de control adicional
- Véase página 29.

L

Límite de reclamación SIL (SILCL)
- El límite de reclamación SIL se corresponde con el SIL requerido en relación con una función de seguridad (la especificación objetivo derivada de un análisis de gráfico del riesgo o de una norma C).
- El límite de reclamación "SILCL" debe entenderse de forma similar al nivel de prestaciones requerido, PLr.
- Véase también el término "SIL".

Límite máximo
- Esto significa que no puede calcularse un valor de $MTTF_d$ de más de 100 años en relación con un PL global, para evitar que se realicen cálculos que ofrezcan resultados más ventajosos que los reales a causa exclusivamente del valor de $MTTF_d$ (es decir, que generen niveles PL por encima de "c"). Es posible realizar cálculos con valores por encima de los 100 años de $MTTF_d$ dentro de un canal, e incluso en ocasiones son necesarios de forma urgente (en el caso de conexiones en serie más largas).
- En este sentido, véase también la observación relativa a la herramienta de software SISTEMA en la página 23.

M

Método del recuento de partes
- Véase "Adición de probabilidades de fallo".

Modificación 1 de EN 1088:1996
- La Modificación 1 de EN 1088:1996[1], introducida como una adición a la norma, afecta a los requisitos de diseño destinados a minimizar las posibilidades de manipulación de los dispositivos de enclavamiento. Desde su emisión, la Modificación 1 ha derivado en la Edición EN 1088-10:2008.
- En este punto es necesario distinguir entre medidas que impiden la manipulación de forma sencilla (como hasta ahora) y las medidas adicionales diseñadas para dificultar dicha manipulación. Se proponen medidas de diversa índole en función del tipo de dispositivo de enclavamiento; de estas, y en esto consiste la verdadera novedad, se debe implantar al menos una.

[1] Dispositivos de enclavamiento asociados a dispositivos de seguridad – directrices de diseño y selección (www.beuth.de).

- En lo que concierne a los dispositivos con accionadores separados, se enmarcan en dichas medidas adicionales los siguientes elementos opcionales:
  - instalación oculta del dispositivo;
  - imposibilidad de liberar el accionador de forma sencilla, por ejemplo utilizando un ensamblaje con tornillos protegidos contra manipulación, remaches, soldadura, etc.;
  - codificación individual de los accionadores; o
  - introducción de medidas de control asociadas al sistema de mando, como por ejemplo pruebas de verosimilitud, pruebas de inicio o similares.
- A la vista de la posibilidad de que se produzca un accidente, debe prestarse la atención necesaria a los nuevos requisitos (ampliados). De acuerdo con las estimaciones, una cuarta parte de todos los accidentes laborales con máquinas en Alemania son causados por la manipulación de dispositivos de protección. Un estudio empírico encargado por diversas aseguradoras legales de accidentes (incluidas aseguradoras de accidentes del sector metalúrgico) y realizado por el Instituto alemán de Salud y Seguridad Ocupacionales (BGIA) en St. Augustin ha puesto de manifiesto este dato y otras informaciones y conclusiones de gran valor (descarga: www.dguv.de/bgia → Publikationen → BGIA-Reports 2005–2006).
- No obstante, la manipulación de los dispositivos de protección no es el único factor a tener en cuenta. Con frecuencia, tal como ha puesto de manifiesto el citado estudio, los operarios tienen motivos tanto objetivos como subjetivos para manipularlos si desean hacer su trabajo. Por este motivo, en el futuro se exigirá con mayor intensidad a los ingenieros encargados del diseño de máquinas que tengan en cuenta este hecho en el concepto de seguridad de una máquina, por ejemplo ofreciendo modos de funcionamiento adicionales diferentes del modo automático que sean igual de eficaces y seguros. En cualquier caso, en lo que concierne a la “manipulación de dispositivos de protección”, se trata también de la “cultura de seguridad” de la compañía que utilice la máquina.

Modo en baja solicitación
- Véase PFD.

$MTTF_d$, fiabilidad del hardware
- Véase sección pertinente de la presente (palabras clave: “riesgos de fallos”, “curva de bañera”, etc.), así como la sección 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

N

Nivel de cable
- Véase “exclusión de defectos: cableado”.

Nivel de prestaciones
- Véase sección pertinente de la presente (palabra clave “cálculos”, etc.), así como la sección 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

Normas C (tipo C)
- Estas normas, relacionadas con los requisitos de seguridad concretos aplicables a tipos específicos de máquinas (máquinas herramientas, centros de procesamiento, máquinas de embalaje, etc.), deben adaptarse al nuevo escenario normativo. Esto significa que, cuando se definan categorías de control en relación con la ejecución de funciones de seguridad determinadas, el redactor de la norma en cuestión debe adaptarlas al nivel de prestaciones requerido (= PL_r).

- En vista de los varios centenares de normas C existentes en la actualidad, no puede preverse que esto vaya a tener lugar a corto plazo (en los próximos meses). Por tanto, en un primer momento, el responsable de la SRP/CS debe realizar la conversión CC → PLr por sí mismo. No obstante, es posible que la entrada en vigor de la nueva Directiva de Máquinas CE 2006/42/CE incluya un proceso acelerado para esta conversión.
- Aunque, en parte, la conversión CC → PL_r puede realizarse de forma simplificada, en ocasiones deben volver a consultarse los parámetros de riesgo S, F y P (véase el parágrafo "Gráfico del riesgo" de acuerdo con EN ISO 13 849-1:2006); esto es así cuando el análisis del gráfico del riesgo actual da como resultado dos categorías de control aplicables de forma alternativa. En el futuro desaparecerá este tipo de ambigüedades.
- No obstante, es también concebible que algunos redactores de normas C puedan seguir exigiendo una categoría de control de forma adicional a la determinación de un PL_r por no considerar que en el futuro vaya a ser posible sustituir las estructuras anteriores de 2 canales por estructuras de 1 canal que lleven asociados valores de $MTTF_d$ y/o valores DC de una envergadura acorde.
- Las normas (de tipo) C constituyen un nivel propio en la matriz de la normativa de seguridad de máquinas, situado por encima de los niveles de las normas denominadas A y B. Las normas (de tipo) A estipulan los requisitos básicos de la seguridad de máquinas (directrices de diseño, valoración del riesgo etc.). El subgrupo B1 de las normas (de tipo) B también está relacionado con los diferentes aspectos relativos a seguridad (distancias de seguridad, dimensiones de cuerpos, etc.), mientras que el subgrupo B2 aborda los requisitos impuestos sobre los dispositivos de protección (dispositivos de enclavamiento, AOPD, etc.).

NORMAS

Normas (de tipo) A, B y C

- Véase normas C.

EN 954-1:1996

- Esta norma relativa a SRP/CS fue controvertida desde un primer momento y se retirará en diciembre de 2009.
- Queda sustituida por la norma EN ISO 13 849-1:2006.

EN 954-2

- Véase EN ISO 13 849-2:2003.

EN ISO 13 849-1:2006

- Nueva norma B1 sobre el tema: Partes de sistemas de mando relativas a la seguridad – Parte 1: Principios generales de diseño.
- Versión alemana: DIN EN 13 849-1:2007-07;
  fuente: Beuth-Verlag GmbH, Berlín, www.beuth.de
- Norma enumerada (armonizada) con presunción de conformidad bajo el marco de la Directiva de Máquinas CE desde mayo de 2007.
- Sustituye a EN 954-1:1996 (ISO 13 849-1:1999) (se retirará en noviembre de 2009).
- Modificaciones sustanciales:
  - Nivel de prestaciones (sustituye al análisis exclusivo de categorías de control)
  - Incorpora el desarrollo y la aplicación de los denominados sistemas electrónicos programables con función de seguridad (PES) a la tecnología de SRP/CS
  - Amplía (mediante un Anexo G propio) el análisis del control y la prevención de los fallos y defectos sistemáticos
- Norma alternativa a EN ISO 13 849-1:2006 (parcialmente): EN IEC 62 061:2005.

EN ISO 13849-2:2003

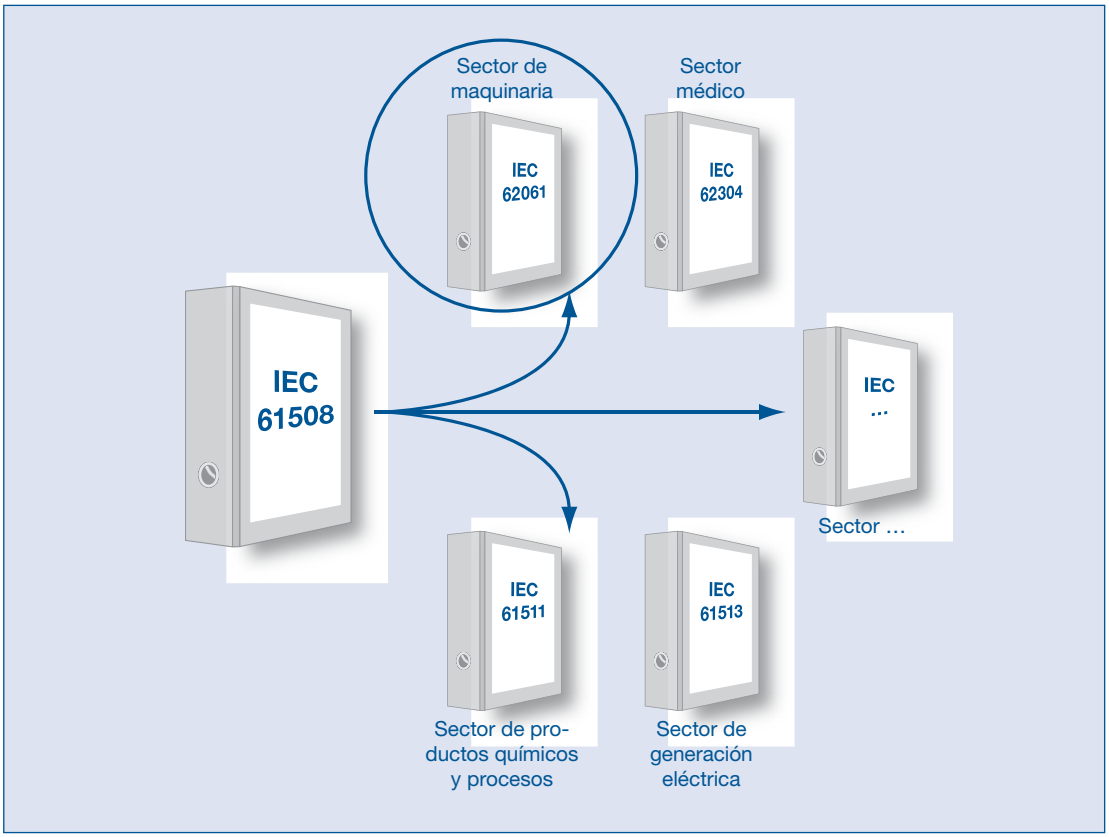
- Norma introducida originalmente como parte 2 de EN 954, concentrada especialmente en la “Validación de SRP/CS” (Partes de los sistemas de mando relativas a la seguridad – Parte 2: Validación)
- Versión alemana: DIN EN ISO 13849-2:2003-12;
  fuente: Beuth-Verlag GmbH, Berlín, www.beuth.de
- Sigue vigente (aunque está en curso de refundición) y actualmente complementa a EN ISO 13849-1:2006.
- La norma conserva su importancia para la configuración y el diseño de SRP/CS, también tras la entrada en vigor de la nueva parte 1 en forma de la norma EN ISO 13849-1:2006.
- Posee especial importancia en cuanto a las exclusiones de defectos admisibles y la lista de principios básicos y de eficacia probada, así como los componentes de seguridad de eficacia probada (véanse Anexos A–D, relativos a tecnología).

EN IEC 62061:2005

- Nueva norma B1 sobre el tema: Seguridad funcional de los sistemas eléctricos, electrónicos y programables relativos a la seguridad (sistemas E/E/PES)
- Norma específica del sector de la ingeniería derivada de EN (IEC) 61508:2001
- Versión alemana: DIN EN 62061 (VDE 0113-50):2005-10;
  fuente: Beuth-Verlag GmbH, Berlín, www.beuth.de
- Norma enumerada (armonizada) con presunción de conformidad bajo el marco de la Directiva de Máquinas CE desde diciembre de 2006.
- Debe considerarse una alternativa a EN 954-1:1996 y (sobre todo en el caso de los sistemas E/E/PES más complejos) también como una alternativa a EN ISO 13849-1:2006.
- Contenido principal:
  – analiza los sistemas de mando eléctricos relativos a la seguridad (SRECS) y los niveles de integridad de la seguridad (SIL)
  – refleja los requisitos de ingeniería de EN (IEC) 61508:2001, aunque de forma simplificada
- Remítase también al término “EN ISO 13849-1:2006 → EN IEC 62061:2005 (comparación)”

EN IEC 61508:2001

- Denominada “publicación de seguridad básica” sobre el tema: Seguridad funcional de los sistemas eléctricos/electrónicos/programables – Partes 1 a 7 (= 370 páginas)
- Versión alemana: DIN EN 61508-x:2001 (x = Partes 1 a 7);
  fuente: Beuth-Verlag GmbH, Berlín, www.beuth.de
- Norma IEC 1508 original (modificaciones 1998 + 2000); se adoptó en las especificaciones normativas europeas en 2001, pero sin armonización en el marco de la Directiva de Máquinas CE.
- El ámbito de validez de la norma abarca todas las fases de la vida de un producto/sistema y tiene en cuenta el denominado ciclo vital de seguridad (desde el diseño hasta el desmontaje). Se analizan todas las modalidades de sistemas relevantes para la seguridad (sistemas tolerantes a defectos, sistemas de apagado, etc.) y medidas de reducción del riesgo en c aso de fallo o error hasta los riesgos de catástrofe. Información de fondo: esta norma se creó con motivo del accidente con gas tóxico de Seveso.
- El efecto deseado de las medidas se expresa como un nivel de integridad de la seguridad (SIL) calculado a partir de un modelado matemático complejo de gran exigencia científica. Las denominadas normas sectoriales también surgieron en este contexto y simplifican los requisitos de la norma 61508:2001 de forma ajustada a los requisitos del grupo objetivo en cuestión.



- Dicho de forma muy sencilla, la norma EN IEC 61 508 constituye el modelo de la ingeniería de fiabilidad relativa a la seguridad e inspiró la norma EN ISO 13 849-1:2006.

EN ISO 13 849-1:2006 ↔ EN IEC 62 061:2005 (comparación)

- Ambas normas son normas enumeradas (armonizadas) con presunción de conformidad en el marco de la Directiva de Máquinas CE.
- Por desgracia existen solapamientos entre ambas normas (es decir, disposiciones duplicadas). Esto se debe a que ambas normas están relacionadas con la configuración de SRP/CS cuando se utilizan tecnologías eléctricas, electrónicas y programables (EN ISO 13 849-1:2006 en forma de nivel de prestaciones y EN IEC 62 061:2005 en forma de nivel de integridad de la seguridad).
- Estos solapamientos se explican por el hecho de que una de las normas fue creada a nivel ISO y la otra a nivel IEC (a nivel europeo, el nivel CEN o CENELEC). El legislador ISO reivindica que EN 954-1:1996 también era ya una norma ISO y, en este sentido, se atribuye competencia para revisar la norma (es decir, la norma sucesora), mientras que los legisladores IEC, remitiéndose a la Publicación de Seguridad Básica EN IEC 61 508:2001, consideran que poseen competencia sobre las denominadas tecnologías E/E/PES.
- Existe una línea divisoria muy clara en el caso de las tecnologías mecánica, hidráulica, neumática y eléctrica afectada por el desgaste (en relación con las cuales tan solo EN ISO 13 849-1:2006 incluye una normativa definitiva), por una parte, y las arquitecturas que se desmarcan de forma significativa de las arquitecturas designadas en EN 13 849-1:2006 (es decir, las categorías de control); (en este caso, EN IEC 62 061:2005 es “competente”, aunque se remite con mucha frecuencia a EN IEC 61 508:2001). Además, existe una referencia a la competencia de EN IEC 62 061:2005/61 508:2001 en relación con el desarrollo de PES con nivel de prestaciones “e”, siempre que no se utilice software diseñado de forma diferente. En cualquier otro aspecto, no dudamos en recomendar a nuestros clientes la norma EN ISO 13 849-1:2006.

- El motivo de esta recomendación es que EN ISO 13849-1:2006 trata de simplificar sistemáticamente la complejidad derivada de la conversión al nivel de prestaciones en la mayor medida posible para el usuario de ingeniería (el “coste” de esta simplificación es que tan solo podremos movernos en el marco de las arquitecturas designadas), mientras que EN IEC 62061:2005 ofrece más opciones (aunque remitiéndose con frecuencia a EN IEC 61508:2001). La filosofía de simplificación subyacente a EN IEC 62061:2005, en comparación con EN IEC 61508:2001, consiste en hacer posibles los SRP/CS con subsistemas.
- A pesar de todo, ambas normas son compatibles entre sí y pueden utilizarse de forma alternada o combinarse.

EN ISO 13849-1 / EN IEC 62061:2005 (comparación con EN 954-1:1996)

- Dejando a un lado su complejidad, la ventaja evidente de las dos nuevas normas relativas a SRP/CS es que, en el futuro, el usuario dispondrá de un mayor margen de configuración. Por ejemplo, en la norma EN ISO 13849-1:2006 existen 5 o quizás 6 posibilidades de configuración diferentes para el PL “c”. En el pasado tan solo habría habido la CC 2.

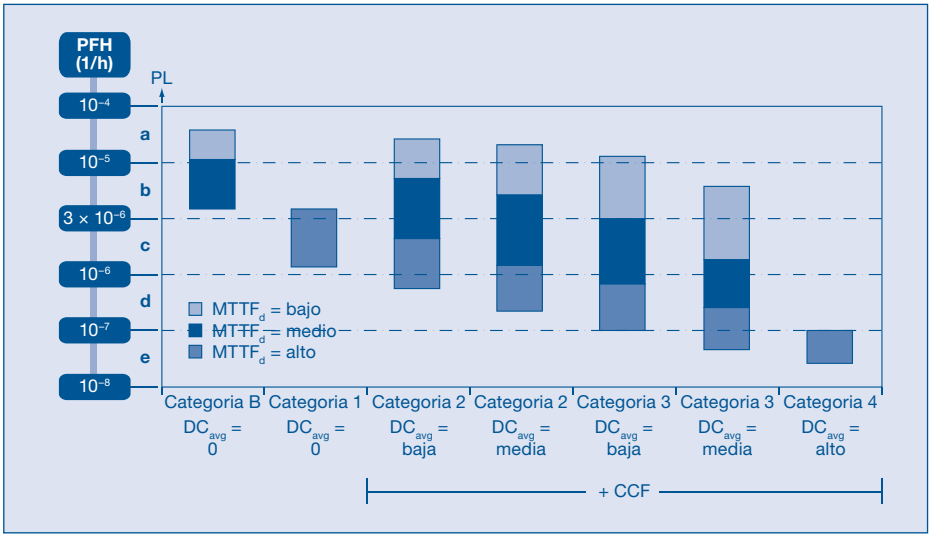
Nivel de prestaciones (PL)	**PL “a”**		**PL “b”**		
Arquitectura designada (CC)	CC B	CC 2	CC 2	CC 3	CC 3
Calidad de componentes ($MTTF_d$)	baja	baja	media	baja	baja
Cobertura del diagnóstico (DC)		baja	baja	media	baja
Gestión de CCF		sí	sí	sí	sí

Nivel de prestaciones (PL)	**PL „c“**				
Arquitectura designada (CC)	SK 1	SK 2	SK 2	SK 3	SK 3
Calidad de componentes ($MTTF_d$)	alta	alta	media	media	baja
Cobertura del diagnóstico (DC)		baja	media	baja	media
Gestión de CCF		sí	sí	sí	sí

Nivel de prestaciones (PL)	**PL „d“**			**PL „e“**
Arquitectura designada (CC)	SK 2	SK 3	SK 3	SK 4
Calidad de componentes ($MTTF_d$)	alta	alta	media/alta[1]	alta
Cobertura del diagnóstico (DC)	media	baja	media	alta
Gestión de CCF	sí	sí	sí	sí

[1] PL “e” con $MTTF_d$ “muy alto”

Redondeo a la baja de seguridad:



- Otra diferencia con EN 954-1:1996 es la incorporación del desarrollo y la aplicación de sistemas PES (SiSPS, sistemas bus de seguridad etc.), así como el análisis deliberado de defectos sistemáticos (incluidos CCF).

O

Objetivo de la normalización de SRP/CS

- Véase la sección 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

P

Periodo de transición

- La norma EN 954-1:1996 (y ISO 13 849-1:1999) se retirará en diciembre de 2009. De forma simultánea, la norma perderá su denominada presunción de conformidad (es decir, la consideración de que interpreta y materializa “de forma correcta” los objetivos de protección de la Directiva de Máquinas CE previstos por el legislador).
- Las máquinas y los sistemas de mando de máquinas utilizados por primera vez a partir de 2010 deberán tener en cuenta la nueva norma, y en caso de duda seguir ajustándose a la Directiva de Máquinas CE.
- ADVERTENCIA: esto también es de aplicación a las construcciones ya existentes que se comercialicen a partir de esa fecha.
- Siendo realistas, en algunos casos no será posible realizar una conversión a tiempo, sobre todo si tenemos en cuenta, por ejemplo, los plazos de producción de las máquinas y sistemas de maquinaria de grandes dimensiones. En el peor de los casos, cabe la posibilidad de que los tribunales deban pronunciarse en torno a la consideración de estos casos. En este supuesto, también se tendrá en cuenta, sin lugar a dudas, el hecho de que la norma EN 954-1:1996 no ha sido una “mala” norma o que EN ISO 13 849-1:2006 no es una norma “más segura” (sino que sencillamente adopta un enfoque diferente).
- Al margen de esto, las máquinas y sistemas de mando de máquinas que ya estén en uso están sujetas a la norma de “protección de los derechos adquiridos”.

PFD (probabilidad de fallo en solicitación)

- Análisis extraído de la norma EN IEC 61 508-1/-7:2001.
- Probabilidad de la integridad de seguridad de una SRP/CS, típica en los ámbitos de tecnología de procesos e ingeniería de procesos. El valor PFD constituye la contrapartida del valor PFH_d en la automatización de fábricas.
- Esta distinción es pertinente por el hecho de existir una frecuencia significativamente diferente en la solicitación de la función de seguridad. En el denominado modo en baja solicitación (típico en la tecnología de procesos y la ingeniería de procesos), la función de seguridad se solicita de forma muy escasa (frecuencia no mayor a una vez al año). Un ejemplo típico serían los sistemas de apagado de emergencia, que tan solo se activan cuando un proceso está fuera de control, lo que normalmente ocurre menos de una vez al año. Lo contario de lo anterior sería el denominado modo en alta solicitación (con valores PFH_d), que implica una solicitación de la función de seguridad (más) frecuente o continua (= más de una vez al año).
- La clasificación del nivel SIL en modo en baja solicitación es la siguiente[1]:

SIL	PFD	Fallos máximos aceptados del SIS
1	$\geq 10^{-2} \ldots < 10^{-1}$	1 fallo peligroso en 10 años
2	$\geq 10^{-3} \ldots < 10^{-2}$	1 fallo peligroso en 100 años
3	$\geq 10^{-4} \ldots < 10^{-3}$	1 fallo peligroso en 1.000 años
4	$\geq 10^{-5} \ldots < 10^{-4}$	1 fallo peligroso en 10.000 años

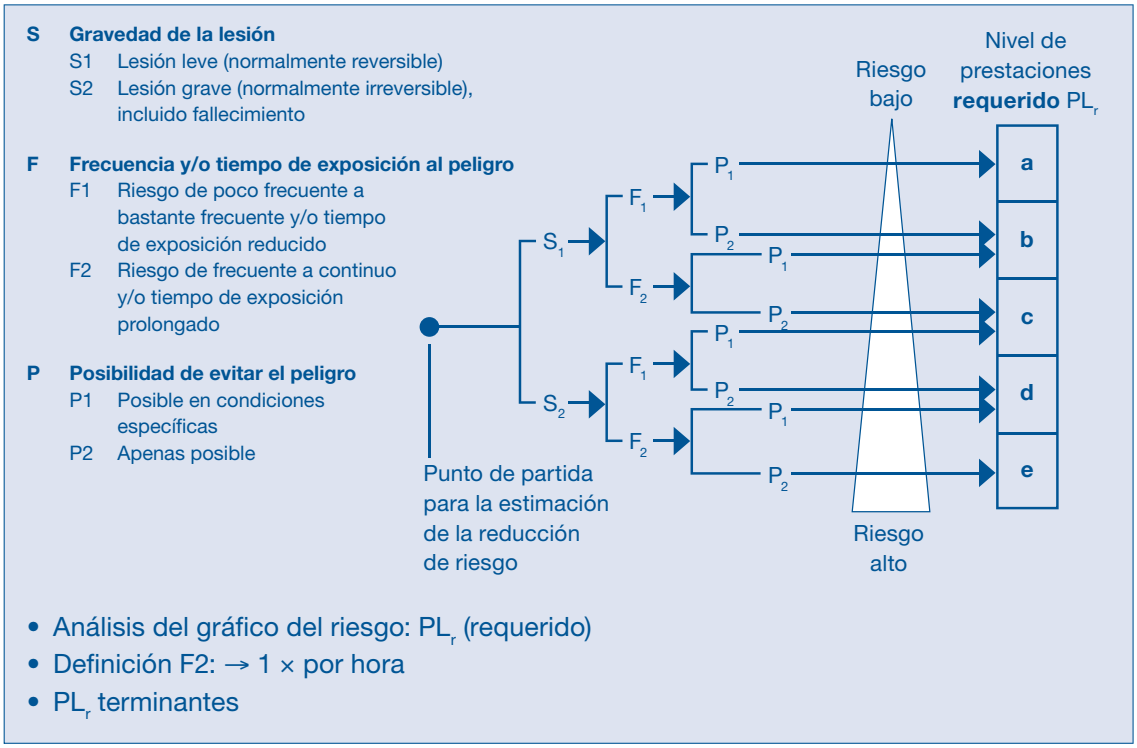
[1] El SIL 4 hace referencia a las funciones de seguridad con riesgo de varias muertes y consecuencias catastróficas y no se tiene en cuenta en ingeniería (automatización de fábricas).

PL – nivel de prestaciones

- Véase sección pertinente de la presente (palabra clave “estimaciones”, etc.), así como la parte 6, páginas 81 y siguientes: “Características y aplicación de EN ISO 13 849-1:2006”.

PL_r = requerido

- Definición de la norma (EN ISO 13 849-1:2006): nivel de prestaciones (PL) aplicado con el fin de conseguir la reducción de riesgo requerida para cada función de seguridad.
- Se trata, por así decirlo, de determinar el estado OBJETIVO a partir de la valoración del riesgo de una función de seguridad. Por tanto, debe obtenerse un $PL \geq PL_r$.
- El PL_r deriva de la norma C correspondiente o de un análisis de gráfico del riesgo relativo a la función de seguridad, es decir, se asigna un nivel de prestaciones (“a”, “b”, “c”, “d” o “e”) a una función de seguridad dependiendo de la gravedad asumida de las lesiones en caso de fallo, de la frecuencia y/o duración en la zona de riesgo, y de la posibilidad de evitar el peligro mediante una reacción personal.
- Véase el parágrafo “Análisis del gráfico del riesgo conforme a EN ISO 13 849-1:2006”.



Prestaciones probadas

- Un término del ámbito de la ingeniería mecánica de uso poco frecuente, que, en particular, se considera una medida sustitutiva del análisis de defectos y fallos sistemáticos.
- Véase EN IEC 61 508:2001.

R

Reinicialización

- Véase el término “Circuito conmutado de reinicio” y la página 28.

Riesgo, análisis del riesgo, valoración del riesgo

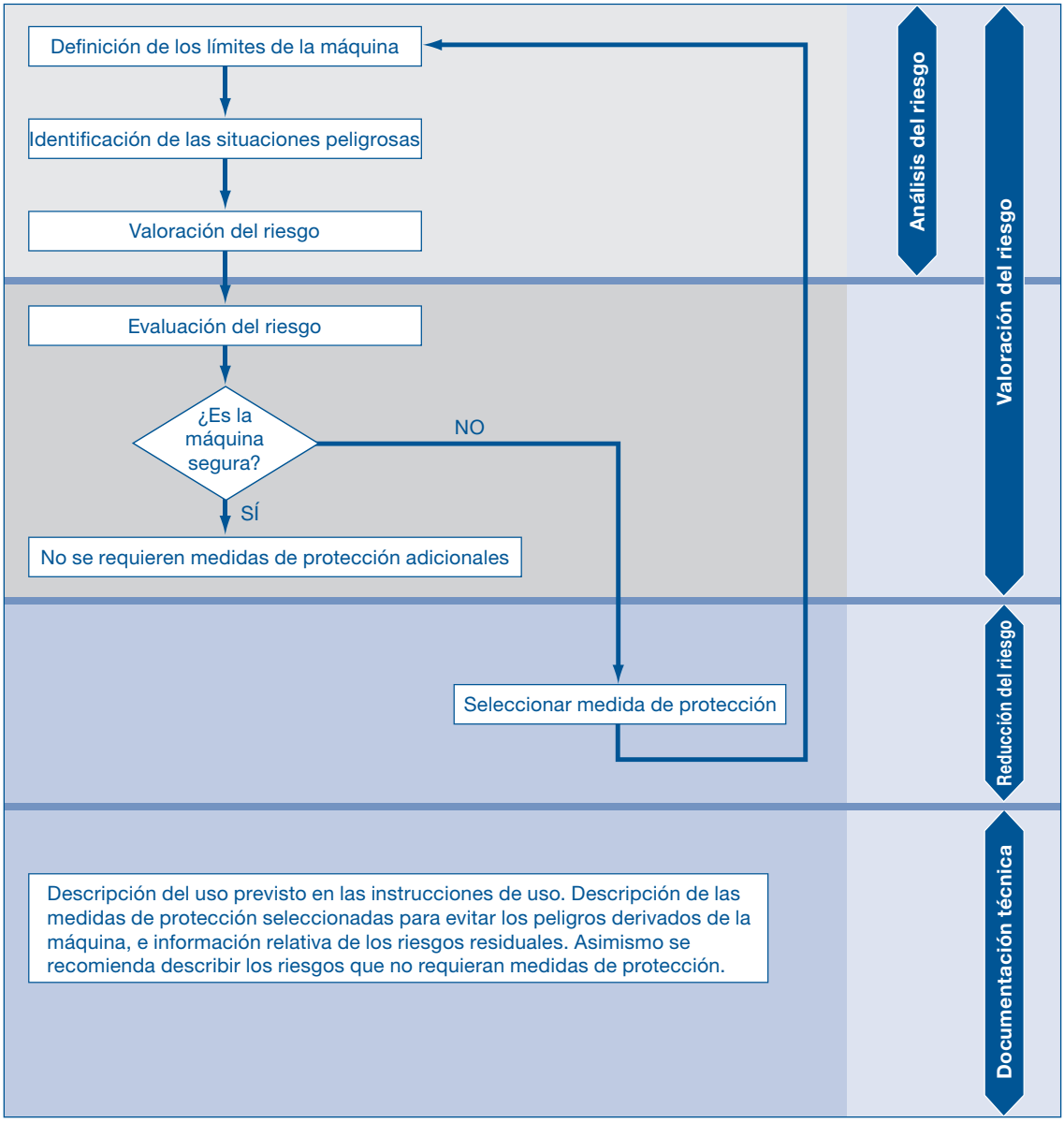
- Definición de riesgo en la norma: combinación de la probabilidad de que se produzca un daño y de la gravedad de dicho daño.
- Definición de análisis del riesgo en la norma: combinación de la especificación de los límites de la máquina, la identificación del peligro y la estimación del riesgo.

- Definición de valoración del riesgo en la norma: juzgar, conforme al resultado del análisis del riesgo, si los objetivos de reducción del riesgo se han alcanzado.
- Este conjunto de temas se desprende también de los requisitos legales de la Directiva de Máquinas CE (véase término “Directiva de Máquinas”).
- Las perspectivas del “riesgo y el análisis del riesgo” (también denominado evaluación de riesgos, análisis de peligros u otras expresiones similares) no constituyen la temática principal de ninguna de las dos nuevas normas relativas a SRP/CS; por el contrario, se presupone que esta fase ya se habrá realizado antes de utilizar una o las dos normas de SRP/CS.
- En particular, las normas EN ISO 12 100-1/-2:2004[1] y EN 1050:1995 (en el futuro, EN ISO 14 121:2007[2]) ofrecen asistencia en cuanto a su interpretación y realización.

[1] Seguridad de máquinas – términos básicos, principios generales de diseño –
-1: Parte 1: Terminología básica, metodología;
-2: Parte 2: Principios técnicos

[2] Seguridad de máquinas – valoración del riesgo –
-1: Parte 1: Principios

Ejemplo de un plan de evaluación del riesgo (fuente: SUVA/CH = Asociación de Aseguradoras de Accidentes Laborales de Suiza).

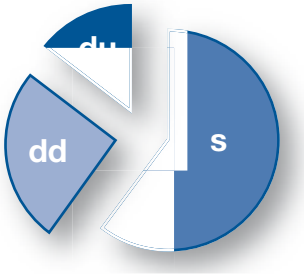


S

SIL (nivel de integridad de la seguridad)

- Clasificación de la calidad global relativa a la seguridad de una SRP/CS reconocida por las normas EN IEC 62 061:2005 y EN IEC 61 508-1/-7:2001 (similar a la filosofía de los niveles PL).

- Definición de la norma: nivel discreto para especificar los requisitos de integridad de la seguridad de la función de mando relativa a la seguridad. Se entiende por integridad de la seguridad la probabilidad de que las funciones de mando requeridas se realicen de forma satisfactoria en todas las condiciones especificadas, y en este sentido hace referencia al hardware, el software y la integridad de la seguridad sistemática. A pesar del uso del término "probabilidad", los niveles SIL no son puramente probabilistas.
- Un SIL viene determinado por las denominadas restricciones de la arquitectura y por la probabilidad de un defecto peligroso por hora (PFH_d).
- Las restricciones de la arquitectura existen con sujeción a la denominada fracción de fallo seguro (SFF), que combina el diagnóstico con el ratio de defectos considerados seguros. Dicho de forma más sencilla, cuando la SFF (es decir, el ratio de defectos reconocidos y/o seguros) es elevada, puede realizarse una construcción de 1 canal en función del SIL, y cuando la SFF es baja, en función también del SIL, la construcción deberá ser redundante (tolerancia de defectos del hardware).



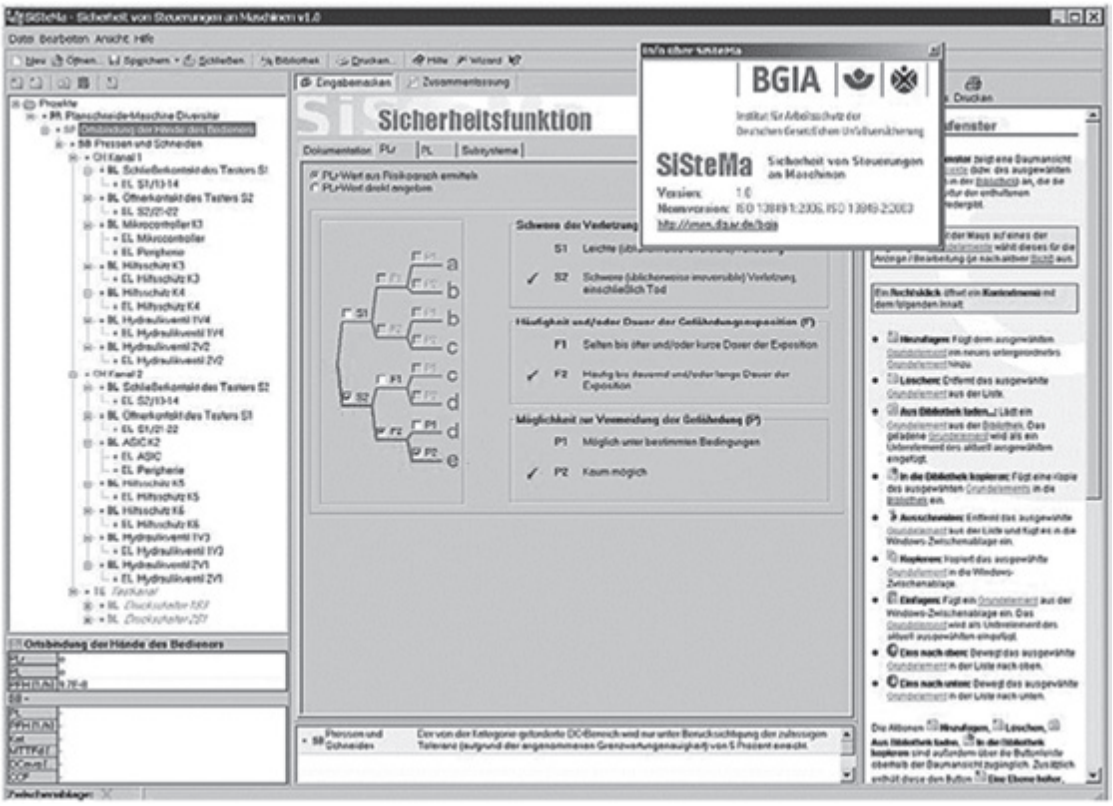
SFF: s = defectos considerados "seguros", dd = defectos "peligrosos detectados", du = defectos "peligrosos no detectados"

- A título ilustrativo, un SIL 2 requiere un valor PFH_d de entre 1×10^{-7} y 1×10^{-6} en un HWT 2 (3 canales) con SFF < 60 %, en un HWT 1 (2 canales) con SFF 60 … 90 %, o en un HWT 0 (1 canal) con SFF 90 … 99 %.
- Dependiendo del nivel de criticidad, la norma EN IEC 62 061:2006 distingue tres niveles de integridad de la seguridad para la construcción de máquinas. Otro factor decisivo en esta clasificación es un gráfico del riesgo (similar al utilizado en la norma EN ISO 13 849-1:2006).
- En lo que concierne a la probabilidad residual de defectos, no es posible afirmar que un SIL sea más estricto que un PL o viceversa. Más bien, digamos que los SIL ofrecen más posibilidades de configuración.
- En lo que concierne a los subsistemas o sistemas parciales de un SRP/CS, el citado documento también hace referencia a sub-PL o sub-SIL, términos relacionados con el reforzamiento de la seguridad, expresado en forma de SIL y PFH_d, en relación con un subsistema o sistema parcial.
- El SIL global de una SRP/CS se corresponde con el sub-SIL más bajo (teoría del eslabón más débil) y con el valor PFH_d que pueda obtenerse en relación con el mismo, que equivale a la suma de los valores PFH_d individuales correspondientes a los diferentes sub-SIL.
- En total, EN IEC 61 508:2001 reconoce 4 niveles SIL. El SIL 4 cubre los riesgos de muerte múltiple o efectos catastróficos, es decir, que no es pertinente para el sector de las máquinas. De forma adicional al valor PFH_d, la norma EN IEC 61 508:2001 también hace uso del denominado valor PFD (PFD = probabilidad de fallo en solicitación) cuando la solicitación de una función de seguridad es muy poco frecuente (> una vez por año), algo que es típico, por ejemplo, en el sector de los productos químicos y la tecnología de procesos.

SISTEMA

- Software basado en WINDOWS para realizar cálculos de PL de acuerdo con la norma EN ISO 13 849-1:2006, que ha sido desarrollado por el BGIA (Instituto Alemán de Salud y Seguridad Ocupacionales del Sector Alemán de los Seguros Legales contra Accidentes (DGUV), sito en St. Augustin, y que está a disposición de todos los interesados de forma gratuita.
- SISTEMA es un acrónimo de **SI**cherheit von **STE**uerungen an **MA**schinen (seguridad de los sistemas de mando en máquinas).

- La herramienta SISTEMA replica la estructura de las partes del sistema de mando relativas a la seguridad (SRP/CS) basándose en las denominadas arquitecturas designadas, y calcula valores de fiabilidad de forma detallada, incluido el nivel de prestaciones (PL) alcanzado. Los parámetros de riesgo para determinar el PL, es decir, la categoría, las medidas contra CCF, la calidad de los componentes ($MTTF_d$) y la calidad de comprobación (DC_{avg}), pueden registrarse siguiendo un proceso por pasos. Las consecuencias de cada modificación de parámetros sobre el sistema global pueden visualizarse de forma directa e imprimirse en forma de informe.
- Aunque la herramienta presta asistencia con los cálculos, en ningún caso puede sustituir una comprensión básica de la norma.
- SISTEMA puede descargarse en www.dguv.de/bgia/13849. Se solicita al usuario que se registre para aceptar los términos de la licencia y recibir eventuales actualizaciones.



Software

- El software integrado en los sistemas PES se aborda de forma especial tanto en EN ISO 13 849-1:2006 como en EN IEC 62 061:2005.
- Debe diferenciarse entre el software del sistema operativo del PES (= SRESW, que significa software integrado relativo a la seguridad) y el software de las aplicaciones de un PES (= SRASW, que significa software de aplicaciones relativo a la seguridad). Este último (SRASW) se divide a su vez en función del lenguaje de programación utilizado (FVL cuando se usen lenguajes de programación con variabilidad lingüística total y LVL cuando se usen lenguajes de programación con variabilidad limitada).
- En este folleto no se abundará más en el tema del “SRESW”.
- Es importante saber que la norma EN 13 849-1:2006 también facilita el desarrollo de sistemas PES (véase sección pertinente de la presente) y que la norma se hace eco de los requisitos SRESW hasta el PL “d”. Debe utilizarse la sección pertinente de EN IEC 61 508:2001 como base cuando se posea un PL “e”; de forma alternativa, el software SRESW puede desarrollarse por otros medios.
- También, en el futuro existirán requisitos adicionales aplicables al software SRASW que afectarán al usuario, por ejemplo al programador de un PLC de seguridad. Existen requisitos básicos que son de aplicación a todos los PL y requisitos adicionales a partir del PL “c”, que se dividen en FVL y LVL.

- **Definición de “software de usuario”:**
  Software instalado en la máquina de forma específica por el fabricante para la aplicación y que, en general, contiene secuencias lógicas, valores límite y rutinas para controlar las entradas, salidas, cálculos y decisiones respectivos con el objetivo de cumplir los requisitos de la SRP/CS.
- **Definición de FVL:**
  Tipo de lenguaje con la capacidad de implementar una amplia variedad de funciones y aplicaciones.
  – Ejemplo: C, C++, ensamblador
  – Observación 1: de acuerdo con IEC 61 511-1:2003, punto 3.2.80.1.3.
  – Observación 2: ejemplo típico de sistemas que utilizan FVL: sistemas integrados.
  – Observación 3: en el sector de la maquinaria se utiliza FVL en software integrado y, de forma ocasional, en software de aplicaciones.
- **Definición de LVL:**
  Tipo de lenguaje con la capacidad de combinar funciones de librería predefinidas y específicas de la aplicación con el objetivo de ejecutar las especificaciones de las funciones de seguridad.
  – Observación 1: de acuerdo con IEC 61 511-1:2003, punto 3.2.80.1.2.
  – Observación 2: en IEC 61 131-3 se incluyen ejemplos típicos de LVL (plano de contactos, diagrama de bloques de funciones).
  – Observación 3: ejemplo típico de sistema que utiliza LVL: PLC.

T

Tasas de fallos

- Los valores típicos de tasas de fallos citados en la norma EN ISO 13 849-1:2006 son valores de $MTTF_d$ (= tiempo medio hasta un fallo peligroso).
- En general, los valores de MTTF constituyen una característica estadística relativa a la fiabilidad de un objeto (al margen de su naturaleza) y ofrecen información en torno a la probabilidad de fallos aleatorios. Los fallos debidos a otros factores, como por ejemplo a una selección incorrecta, un dimensionamiento insuficiente, etc., se incluyen en el grupo de fallos sistemáticos y no se expresan en forma de valores de MTTF.
- Los valores de MTTF se basan en el periodo medio de vida útil o prestación de servicio de los objetos (hasta el fallo). La información relativa a la vida útil o la prestación de servicio se extrae de datos de comportamiento en servicio, extrapolaciones a partir de pruebas de esfuerzo, los denominados análisis FMED[1], etc.
- Las normas EN ISO 13 849-1:2006 y EN IEC 62 061:2005 tan solo se interesan por los fallos peligrosos, por ejemplo que un contacto no pueda cerrarse (= normalmente una perturbación en el caso de los sistemas de apagado, pero no peligroso) o abrirse (= normalmente peligroso en el caso de los sistemas de apagado). El ratio de fallos peligrosos con respecto a fallos no peligrosos se estima normalmente en 50:50. En este sentido, por tanto, un valor de $MTTF_d$ siempre es dos veces superior al valor de MTTF, que refleja todos los fallos posibles.
- Cuando se trata de varios objetos, se utiliza un valor de $MTTF_d$ para expresar la probabilidad matemática, en relación con la distribución exponencial, de que, tras extinguirse la vida útil del MTTFd, hayan producido fallos peligrosos el 63,2 % de los objetos afectados. Por tanto, se trata de un dato relativo a la probabilidad de supervivencia (véase ejemplo de la página 110).

[1] Análisis diagnóstico del modo y los efectos de fallos

- Ejemplo:

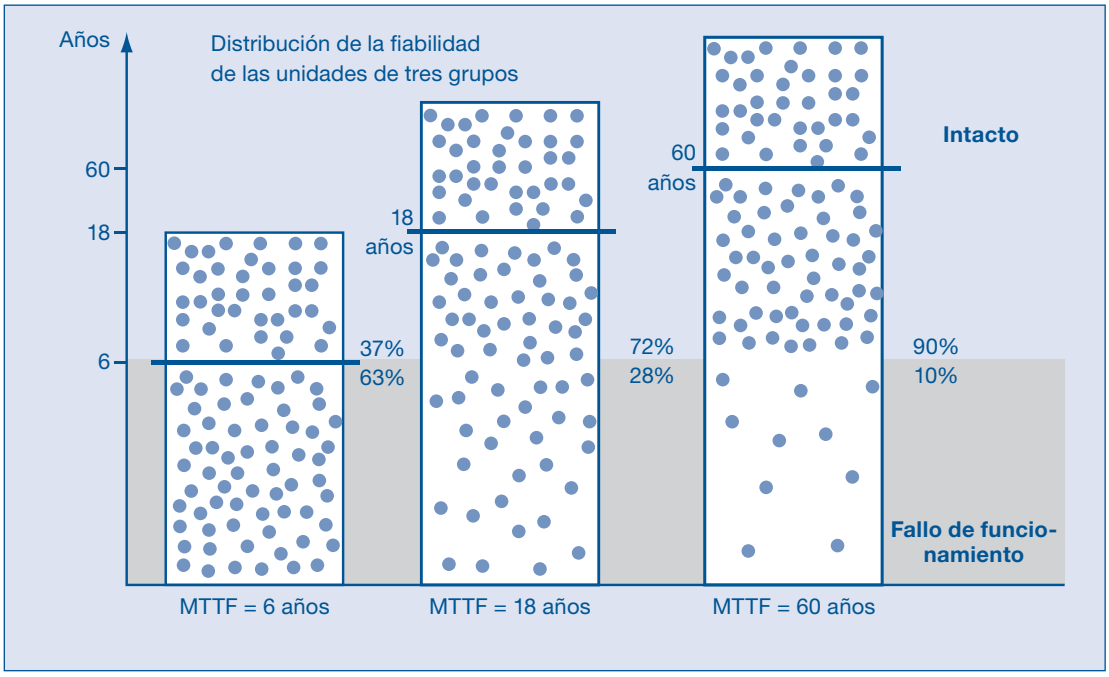


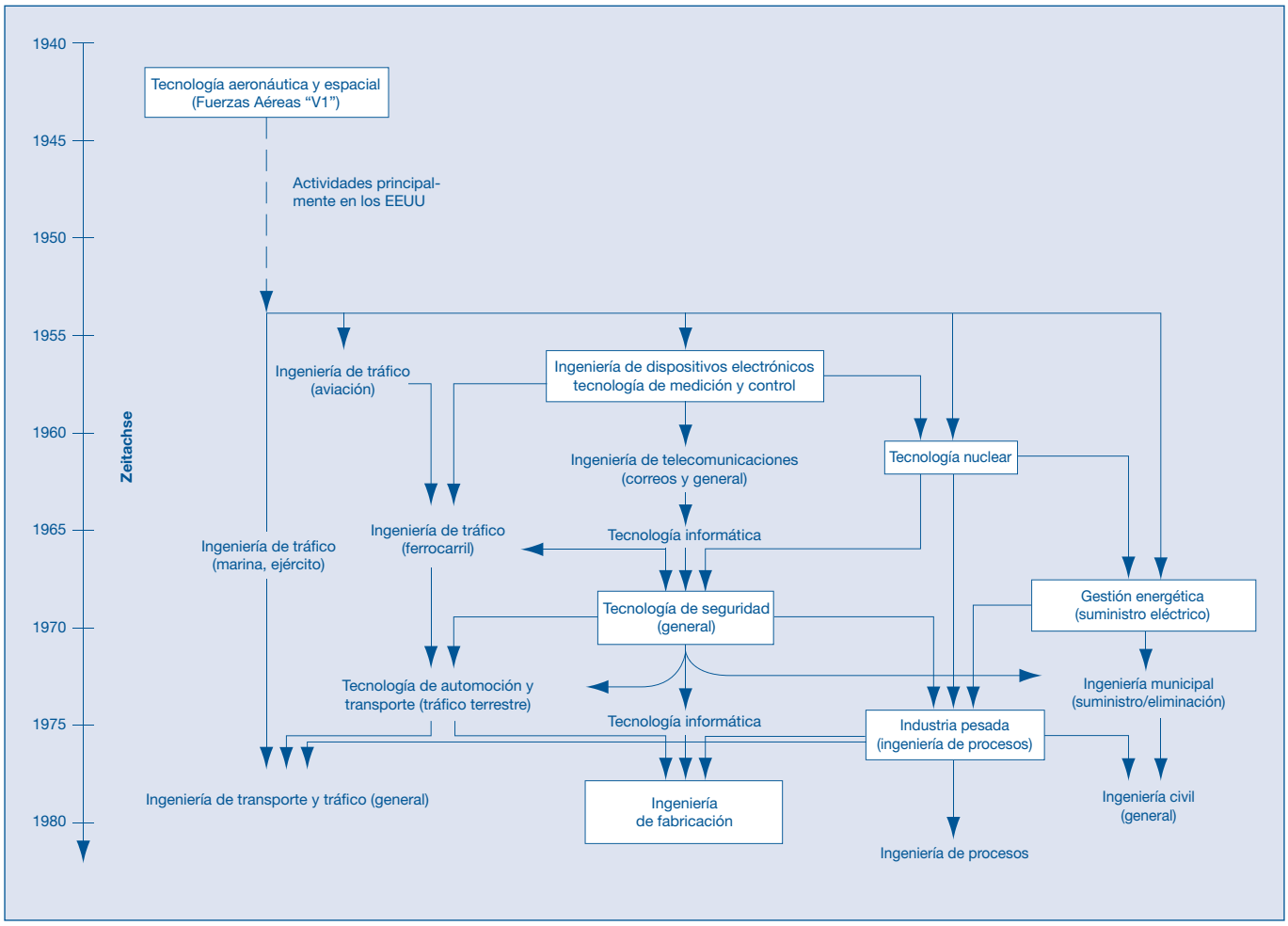
Ilustración de la vida útil media: se representan tres grupos con diferentes niveles de fiabilidad. Sus unidades (ilustradas en forma de puntos) sufren fallos en momentos aleatorios. La situación de los fallos en el tiempo se corresponde con la coordenada vertical. Los tiempos de los fallos se distribuyen sobre periodos de tiempo largos; por ejemplo, en el caso del primer grupo, hay unidades individuales que sobreviven durante 18 años, mientras que algunas fallan transcurrido tan solo un año. El 63% ya ha sufrido fallos tras 6 años (Fuente: "Einführung in die Methoden der Zuverlässigkeitsbewertung" [Introducción a los métodos de evaluación de la fiabilidad], Siemens AG, I&S IS ICS IT2).

- Por el contrario, los valores λ o FIT, las tasas de fallos con que "funciona" la norma EN IEC 62 061:2005, indican de media cuántos objetos fallan de forma aleatoria en una unidad de tiempo (= 1/tiempo en comparación con la "probabilidad de supervivencia" de los valores de MTTF o $MTTF_d$). Los valores FIT representan una tasa de fallos expresada en 10^{-9} por hora. Por tanto, se trata de un análisis temporal alternativo del mismo fenómeno. Por este motivo, en este caso los valores recíprocos de los valores λ o FIT son valores de MTTF o $MTTF_d$.
- Aunque los valores PFH_d también expresan la probabilidad de un fallo peligroso por hora, pueden aportar más al cálculo que un simple análisis de los fallos aleatorios del hardware. Por tanto, la conversión tan solo es permisible con reservas. Es posible en las estructuras de 1 canal (1/ $MTTF_d$ = PFH_d y viceversa). Además, los valores PFH_d pueden convertirse de forma muy simplificada en valores de $MTTF_d$ de bloque calculando el valor recíproco (1/ PFH_d: 8.760) (no permisible en sentido inverso).
- En el caso de los valores PFH_d, la distinción realizada mediante el subíndice "d" no es particularmente habitual, es decir, que tanto los valores PFH como los valores PFH_d suelen utilizarse en relación con fallos peligros.
- Los valores de MTBF o $MTBF_d$ constituyen una subcategoría de los valores de MTTF o $MTTF_d$. MTBF significa "tiempo medio entre fallos" y es el tiempo medio entre dos fallos en objetos reparables. La diferencia entre MTTF ($MTTF_d$) y MTBF ($MTBF_d$) tan solo es marginal y puede pasarse por alto en lo que concierne a las SRP/CS.
- En muchos otros ámbitos, como por ejemplo en productos químicos e ingeniería de procesos, ingeniería militar, aviónica, etc., la incorporación de tasas de fallos forma parte de las prácticas vigentes (palabra clave: ingeniería de fiabilidad).

- Existen numerosas fuentes y obras de referencia relativas a las tasas de fallos, como por ejemplo SN 29 500, los manuales MIL, etc.
- Si deseamos remitirnos a las fuentes generales para obtener información en torno a las tasas de fallos, es buena idea que nos preguntemos si un valor hace referencia a fallos peligrosos en el sentido de EN ISO 13 849-1:2006 (a menudo identificado con el subíndice “d”) o a todos los fallos posibles (este último valor debe convertirse; véase más arriba).
- Además, en la norma EN ISO 13 849-1:2006 se recomienda incorporar a los cálculos tan solo un 10 %, como máximo, de valores no verificados y procedentes de fuentes diferentes.
- En el caso de información no específica sobre tasas de fallos, por ejemplo en relación con componentes eléctricos, a menudo esta hace referencia a valores nominales que no tienen en cuenta el efecto de la temperatura (por ejemplo, el hecho de que la tasa de fallos se duplique por cada aumento de 20 °C de la temperatura), los ciclos de temperatura (calor ↔ frío) y otras influencias medioambientales. Es necesario introducir estas influencias en los cálculos adicionales (práctica típica en la norma EN IEC 61 508:2001) o utilizar una cifra global incluyendo tan solo un 10 % de tasas de fallos nominales en los cálculos adicionales (recomendación de EN ISO 13 849-1:2006).

Tecnología de fiabilidad (ingeniería de fiabilidad)

- La fiabilidad es una propiedad de los materiales evaluable empíricamente mediante un valor medible estadísticamente basado en las frecuencias observadas de fallo, o bien utilizando cálculos de probabilidad.
- En un sentido más amplio, los análisis de PL y SIL se enmarcan en la ciencia de la tecnología de fiabilidad (ingeniería de fiabilidad).
- Las primeras aplicaciones de la tecnología de fiabilidad se descubrieron, como a menudo en otros ámbitos, en el campo de la tecnología militar (a estas siguieron otras aplicaciones).



- El ámbito de la investigación en tecnología de fiabilidad se ocupa de la fiabilidad de los componentes y sistemas, así como de los métodos de análisis y salvaguarda de la fiabilidad. De forma simultánea a estas investigaciones se crean bases de datos de fiabilidad, además de investigarse métodos de planificación de ensayos y la evaluación estadística de datos relativos a fallos y ensayos de montacargas. Otros temas son el modelado realista de sistemas técnicos complejos, la simulación de la fiabilidad y la disponibilidad en las primeras fases de desarrollo. Se realizan cálculos de la vida útil del sistema y se determinan grupos de carga. Uno de los ámbitos de trabajo es la realización de análisis FMEA y la elaboración de documentación de acompañamiento del desarrollo.

U

V

Uso probado

- Véase: “Prestaciones probadas”.

Valores B_{10d}

- Definición de la norma: número de ciclos hasta que el 10 % de los componentes falla peligrosamente (los valores B_{10d} son de aplicación sobre todo a componentes mecánicos, fluidos y electromecánicos).
- ADVERTENCIA: otra característica de importancia → valor T_{10d}.
- Se entiende por número de ciclos el número de ciclos de conmutación a lo largo de la vida útil, es decir, el valor B_{10d} expresa un número máximo de ciclos de conmutación y constituye la base para realizar los cálculos necesarios del $MTTF_d$ en relación con los dispositivos de una SRP/CS afectados por desgaste. Entre estos se incluyen los componentes y dispositivos mecánicos, como por ejemplo resortes, dispositivos de control de fluidos como válvulas, y aparamenta electromecánica como contactores, relés, interruptores de posición, dispositivos de control de parada de emergencia, etc.
- Los componentes de este tipo poseen un patrón de fallos que viene determinado por el número de ciclos de conmutación realizados y, parcialmente, por la carga de conmutación, y por tanto se asume una distribución Weibull (de incremento constante) en relación con ellos, ya que la probabilidad de fallos varía en el tiempo.
- Las fórmulas para convertir un valor B_{10d} en un valor de $MTTF_d$ son las siguientes:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad n_{op} = \frac{d_{op} \times h_{op} \times 3.600 \frac{s}{h}}{t_{cycle}}$$

n_{op} = número medio de ciclos de conmutación por año
d_{op} = número medio de días de utilización por año
h_{op} = número medio de horas de utilización por día
t_{cycle} = exigencia media de la función de seguridad en segundos (por ejemplo, 4 × hora = 1 × 15 min. = 900 s)

- En el Anexo C (tabla C.1) de EN ISO 13 849-1:2006 se indican valores B_{10d} en relación con los tipos habituales de componentes afectados por desgaste, a los que a continuación debe aplicarse la anterior fórmula para calcular los valores de $MTTF_d$ por canal (puede utilizarse como base la información del fabricante en vez de los valores incluidos en la norma, de ser diferentes).
- Los componentes mecánicos e hidráulicos constituyen una excepción y no debe aplicárseles la fórmula de cálculo. Debido a la elevada fiabilidad de estos componentes, conocida y demostrada por la experiencia, el redactor de la norma recomienda que se asuma un valor $MTTF_d$ global de 150 años por canal (siempre que se respeten los principios de seguridad básicos y de eficacia probada descritos en la norma).

- Los valores B_{10d} correspondientes a interruptores de proximidad (basados en contacto de relé de láminas), contactores y relés conforman una segunda sección del Anexo C. En relación con los componentes de este tipo se especifican dos valores B_{10d}: el primero se utiliza cuando el componente se usa con una carga mínima (= 20 %) (B_{10d} = 20.000.000) y el segundo cuando el componente se usa con una carga máxima (B_{10d} = 400.000). Se permite la creación de valores intermedios, por ejemplo 7.500.000 (con una carga del 40 %), 2.500.000 (con una carga del 60 %) o 1.000.000 (con una carga del 80 %).
- Además, debe procurarse que, de acuerdo con EN IEC 60947-5-x, se exijan contactos de apertura positiva en relación con los dispositivos de parada de emergencia e interruptores de posición.
- Un prerrequisito para aplicar los valores B_{10d} de la norma son los denominados procesos de buenas prácticas de ingeniería, es decir, que el fabricante del componente:
  - confirme el uso de los principios de seguridad básicos y de eficacia probada de acuerdo con EN ISO 13849-2:2003 o las normas de producto correspondientes en relación con el diseño del componente; y
  - describa las condiciones de uso y aplicación adecuadas para el usuario (palabra clave: instrucciones de uso).
- De forma adicional, el responsable de la SRP/CS debe ajustarse a los principios de seguridad básicos y de eficacia probada de acuerdo con EN ISO 13849-2:2003 en relación con la instalación y el funcionamiento del componente.
- Existe otro factor que debe tenerse en cuenta en relación con los componentes afectados por desgaste, a saber, el denominado valor T_{10d}, que representa un valor relativo al mantenimiento preventivo de los componentes afectados por desgaste mediante su sustitución en el momento oportuno.

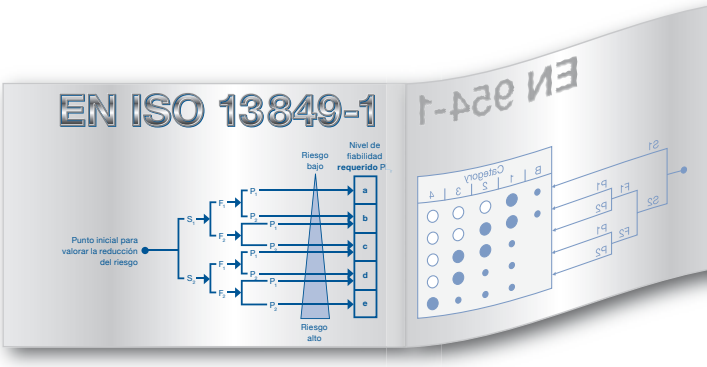
Extracto de la tabla C.1 de EN ISO 13849-1:2006: valores B_{10d} seleccionados de los componentes usados habitualmente en SRP/CS

	Principios básicos de seguridad y de eficacia probada de acuerdo con la Norma ISO 13849-2:2003	**Otras normas pertinentes**	**Valores típicos: $MTTF_d$ (años) o B_{10d} (ciclos)**
Componentes mecánicos	Tablas A.1 y A.2	–	$MTTF_d$ = 150
Componentes hidráulicos	Tablas C.1 y C.2	EN 982	$MTTF_d$ = 150
Componentes neumáticos	Tablas B.1 y B.2	EN 983	B_{10d} = 20.000.000
Relés y contactores auxiliares con carga ligera (carga mecánica)	Tablas D.1 y D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20.000.000
Relés y contactores auxiliares con carga máxima	Tablas D.1 y D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400.000
Interruptores de proximidad con carga ligera (carga mecánica)	Tablas D.1 y D.2	IEC 60947 EN 1088	B_{10d} = 20.000.000
Interruptores de proximidad con carga máxima	Tablas D.1 y D.2	IEC 60947 EN 1088	B_{10d} = 400.000
Contactores con carga ligera (carga mecánica)	Tablas D.1 y D.2	IEC 60947	B_{10d} = 20.000.000
Contactores con carga nominal	Tablas D.1 y D.2	IEC 60947	B_{10d} = 2.000.000
Interruptor de posición independiente de la carga[a]	Tablas D.1 y D.2	IEC 60947 EN 1088	B_{10d} = 20.000.000
Interruptor de posición (con accionador separado, dispositivo de seguridad con bloqueo) independiente de la carga [(1)]	Tablas D.1 y D.2	IEC 60947 EN 1088	B_{10d} = 2.000.000
Dispositivo de parada de emergencia independiente de la carga[(1)]	Tablas D.1 y D.2	IEC 60947 ISO 13850	B_{10d} = 100.000
Dispositivo de parada de emergencia con exigencias máximas de funcionamiento[(1)]	Tablas D.1 y D.2	IEC 60947 ISO 13850	B_{10d} = 100.000
Pulsador (por ejemplo, interruptores de validación), independiente de la carga[(1)]	Tablas D.1 y D.2	IEC 60947	B_{10d} = 100.000

[(1)] Si es posible la exclusión de defectos para la apertura positiva

Fragmento de nuestro folleto
“Nuevo enfoque de la seguridad de máquinas:
EN ISO 13849-1:2006 –
partes de un sistema de mando relativas a la seguridad”

En el ejemplo de conexión queda pendiente el análisis del valor B_{10d} en relación con los dispositivos afectados por desgaste. Suponemos que la información de fabricante, definida en relación con dicho análisis, ya se ha convertido de forma adecuada.



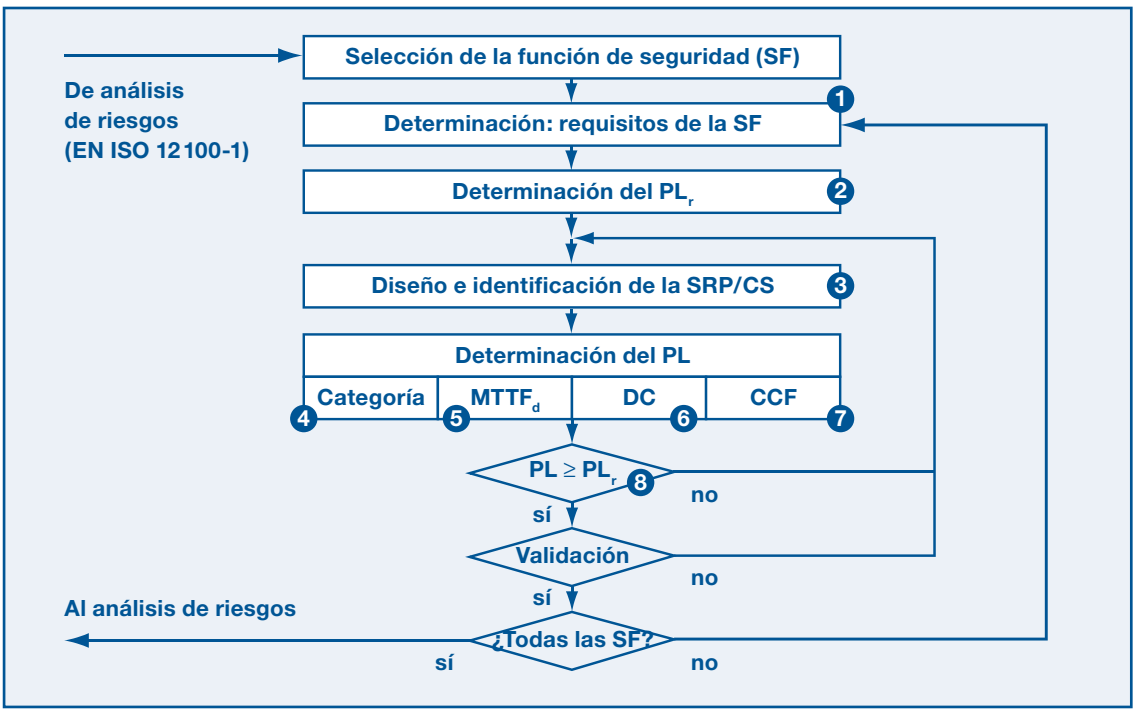


Figura 32: Proceso iterativo de diseño y desarrollo según la norma EN 13849-1

Ejemplo

En primer lugar, el proceso iterativo de diseño y desarrollo de la norma EN ISO 13849-1 coincide con la versión de la EN ISO 12100. En este caso, también se divide teóricamente en 8 pasos, empezando por la selección de una función de seguridad (1) y luego, siguiendo los pasos del (2) al (7), se determina si se ha conseguido el PL_r requerido (8).

El ejemplo mostrado (véase la Figura 33) se refiere al enclavamiento de resguardos móviles, es decir, a la función de detener el movimiento peligroso cuando el resguardo se abre, a no permitir un nuevo arranque hasta que éste se cierra, etc. (véase la norma EN 1088: seguridad de las máquinas – dispositivos de enclavamiento asociados a resguardos – principios de diseño y selección).

❶

Ejemplo:

- Enclavamiento de un resguardo

Función de seguridad

- Detención del movimiento peligroso cuando el resguardo se abre

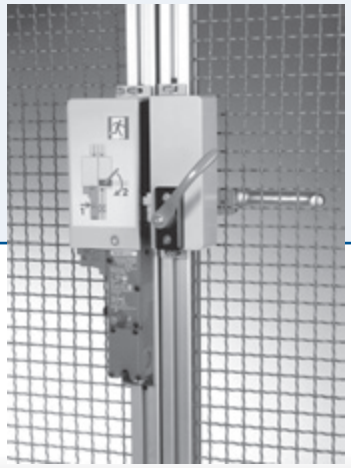


Figura 33: Selección y determinación de los requisitos de una función de seguridad

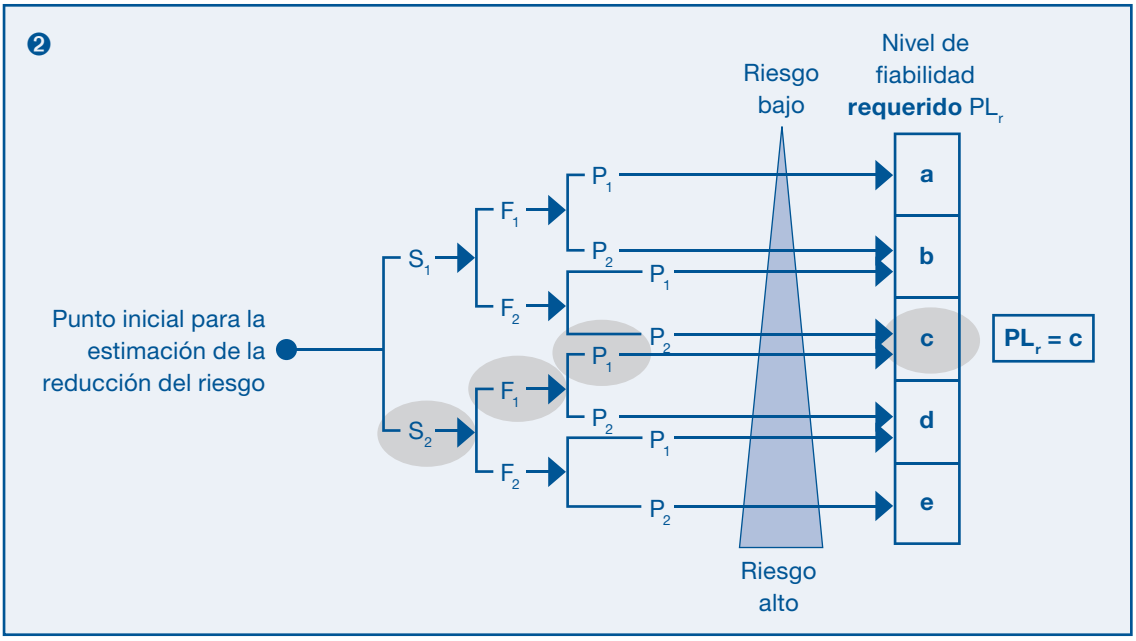


Figura 34: Determinación del PL_r

Según la norma EN ISO 13849-1, el nivel de prestaciones requerido, o PL_r, debe ser de “c” (véase la Figura 34).

La Figura 35 presenta una estructura de una SRP/CS (arquitectura designada).

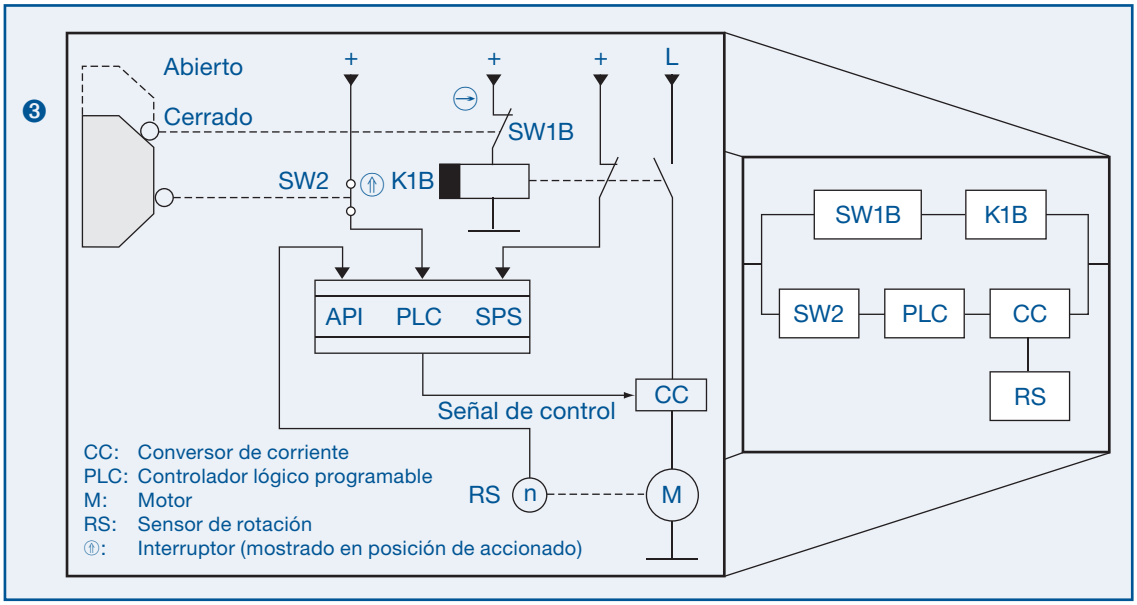
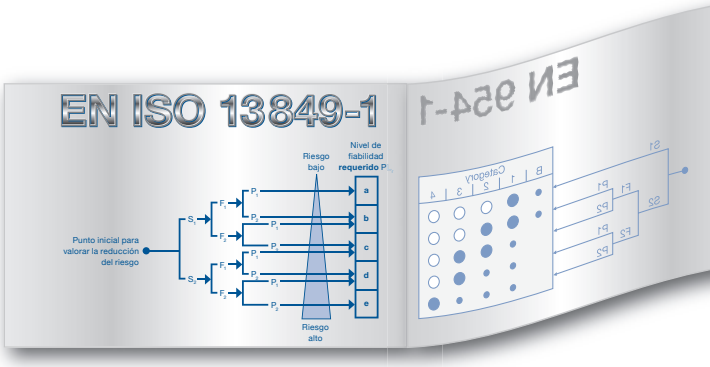


Figura 35: Diseño e identificación de una SRP/CS



A partir de la arquitectura designada de la Figura 35:

❹

- Cumple los requisitos de la categoría B ✔
- Un solo fallo no produce la pérdida de la SF ✔
- Detección de fallo parcial ✔
- Una acumulación de fallos no detectados no produce la pérdida de la SF (1º falla la SPS sin que se detecte, 2º falla el canal A) ✔

–> Puede obtenerse la categoría 3

Figura 36: Determinación de la categoría de PL

Como ambos canales del ejemplo presentan una construcción distinta (véase la estructura de la SRP/CS), deben determinarse primero los valores $MTTF_d$ correspondientes a los canales A y B y simetrizarlos.

❺

- **SW1B: contacto de apertura positiva:** Exclusión de defecto por la no apertura de los contactos, la no activación de los interruptores debida a fallo mecánico (ruptura de pistón, desgaste de palanca, desalineación)
- **K1B: $MTTF_d$ = 30 a (especificación) del fabricante)**

$$\frac{1}{MTTF_{d\,C1}} = \frac{1}{MTTF_{d\,K1B}} = \frac{1}{30\ a}$$

Canal 1: $MTTF_d$ = 30 a

Figura 37: Determinación del PL: $MTTF_d$ para el canal A

❺

- **SW2, SPS, CC: $MTTF_d$ = 20 a cada uno (especificación del fabricante)**

$$\frac{1}{MTTF_{d\,C2}} = \frac{1}{MTTF_{SW2}} + \frac{1}{MTTF_{PLC}} + \frac{1}{MTTF_{CC}} = \frac{3}{20\ a}$$

Canal 2: $MTTF_d$ = 6,7 a

- **$MTTF_d$ simetrizado para ambos canales:**

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

$MTTF_d$ = 20 a (medio)

Figura 38: Determinación del PL: $MTTF_d$ para el canal B y $MTTF_d$ total

A continuación se muestra el análisis de la cobertura de diagnóstico (DC):

❻

- DC_{K1B} 99%, “alta”, debido a los contactos eléctricos de activación positiva de la tabla del anexo E.1
- DC_{SW2} = 60%, “baja”, debido al control de las señales de entrada sin pruebas dinámicas
- DC_{PLC} = 30%, “ninguna”, debido a la baja eficacia de las autocomprobaciones
- DC_{CC} = 90%, “media”, debido a la menor distancia de desconexión, al estar el accionador supervisado por el controlador. Véase la tabla del anexo E.1

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_S}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

DC_{avg} = 67% (baja)

Figura 39: Determinación del PL: DC_{avg}

A continuación se muestra la determinación del nivel de gestión de CCF:

❼

CCF: Fallos de varias partes por causas comunes

• Separación de la vía de señal	15 puntos
• Diversificación	20 puntos
• Protección ante sobretensión o sobrepresión	0 puntos
• Componentes probados	5 puntos
• FMEA (análisis de modos y efectos de fallo)	5 puntos
• Competencia/formación del diseñador	0 puntos
• EMC o filtración de medio de presión y proteccion ante contaminación	25 puntos
• Temperatura, humedad, choques, vibraciones, etc.	10 puntos

Σ = 80 puntos > 65 puntos

Figura 40: Determinación del PL: CCF

Y, finalmente, la disposición en el diagrama de bloques, es decir, la verificación de si PL => PL_r (véase la Figura 41).

Notas: Naturalmente, la división meticulosa de cada uno de los pasos del ejemplo anterior es un tanto exagerada. Además, el ejemplo ilustra dos canales de diferente construcción tanto en el ámbito del sensor como en el del proceso lógico, por lo que parece más complejo que los que se suelen usar en la práctica.

De todos modos, es una muestra de la filosofía de los nuevos requisitos de la norma EN ISO 13849-1, aunque en el ejemplo no se ha tenido en cuenta el valor B_{10d} para el dispositivo de enclavamiento (como dispositivo electromecánico), que debería haberse incluido para una mayor precisión.

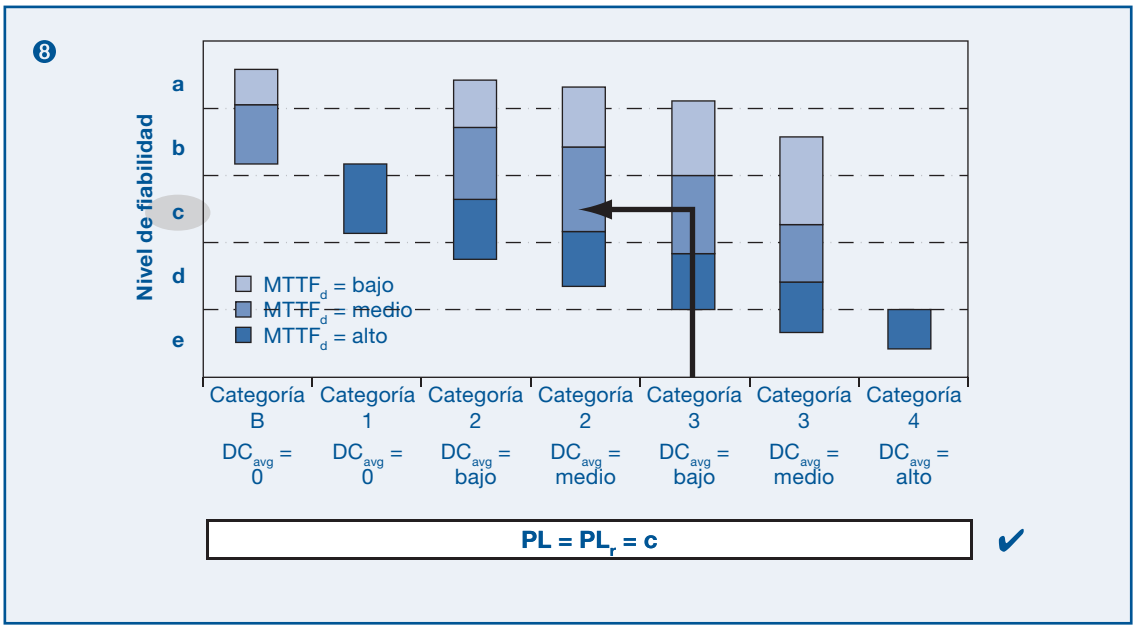


Figura 41: Determinación de si se ha conseguido que PL ≥ PL_r

Edición

K.A. Schmersal GmbH
Sistemas de conmutación de seguridad industrial
Möddinghofe 30
D-42279 Wuppertal
Alemania

Teléfono: +49 (0)202 6474-0
Fax: +49 (0)202 6474-100
E-Mail: info@schmersal.com
Internet: www.schmersal.com

Elan Schaltelemente GmbH & Co. KG
Im Ostpark 2
D-35435 Wettenberg
Alemania

Teléfono: +49 (0)641 9848-0
Fax: +49 (0)641 9848-420
E-Mail: info-elan@schmersal.com
Internet: www.elan.de

Texto

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG
Schmersal tec.nicum

E-Mail: fadams@schmersal.com

Producción

flick-werk – Werbe-Grafik Heinz Flick,
D-35075 Gladenbach, Alemania
Cityflair, S.L., E-08191 Rubí (Barcelona), España

Sistemas de seguridad

Seguridad en sistemas – Protección de hombre y máquina

Con frecuencia es inevitable que las personas tengan que intervenir en el proceso de trabajo de una máquina, por ejemplo, para cargar, descargar, limpiar, realizar labores de conservación y mantenimiento, etcétera. En estos casos, el operario debe tener garantizada su seguridad. Dicha seguridad entra dentro del ámbito de responsabilidad del propietario de la máquina, y así lo exigen también las normas y directivas internacionales sobre seguridad de las máquinas.

Con sus productos, el Grupo Schmersal aboga desde hace ya muchos años por la seguridad en el lugar de trabajo y ofrece actualmente a la industria mundial la mayor gama de dispositivos y sistemas de seguridad para la protección de hombre y máquina.

Bajo el lema “Seguridad en sistemas – Protección de hombre y máquina”, las empresas del Grupo Schmersal desarrollan y fabrican dispositivos de seguridad, que tiene como base la estructura de sistemas y se integra de forma óptima en los procesos de trabajo. En Schmersal estamos convencidos de que seguridad e incremento de la productividad no son conceptos opuestos.

La gama de productos extraordinariamente amplia de la que disponemos es fruto principalmente de nuestra política de desarrollo y gestión de productos orientada al cliente. Muchos productos han sido desarrollados para satisfacer los deseos concretos de los clientes y, por tanto, para aplicaciones específicas. Por otra parte, nuestra cartera de productos también se ha ampliado sustancialmente por el hecho de haber dejado de ser una empresa individual para convertirnos en un grupo empresarial de alto rendimiento.

Actualmente, el Grupo Schmersal es un consorcio de empresas que operan a nivel mundial y que, en calidad de centros de competencia, están especializadas en distintas áreas de dispositivos y sistemas de seguridad.

De esta forma, el Grupo Schmersal ofrece a sus clientes seguridad en sistemas y protección para hombre y máquina.

Más detalles

A su disposición 24 horas al día, el catálogo "on line", hojas de datos, instrucciones de montaje y conexionado, declaraciones de conformidad y mucho más en: www.schmersal.net

Documentación "on line" en seis lenguas
La información "on line" para nuestros clientes se pone al día de forma permanente. El Catálogo General, puede ser consultado en internet, en seis idiomas distintos. No sólo se encuentran los datos técnicos del programa de productos, si no también las aclaraciones a las exigencias de conformidad, los certificados de pruebas e incluso las instrucciones de montaje y conexionado, las cuales pueden ser bajadas.

Un servicio añadido
Los dibujos técnicos de los productos, están también incluidos en el Catálogo "on line", y están a disposición de los diseñadores, que pueden así bajarlos directamente, para ser incorporados directamente a su sistema CAD. La página Schmersal, contiene además, la necesaria información, puesta al dia, sobre artículos en general, comentarios técnicos referidos a la seguridad de la máquina, así como sobre las noticias que pueden afectar eventos y cursillos. Es muy conveniente dar una ojeada de forma regular!

Atención personalizada
Naturalmente, también pueden ustedes, llamar directamente, cuando necesiten información adicional sobre un tema concreto:

Tel.: (+34) 93 8970906

¡Le aconsejaremos con mucho gusto de forma personal!

Schmersal Ibérica, S.L.
Pol. Ind. La Masia
Camí de les Cabòries, Nave 4
08798 Sant Cugat Sesgarrigues
ESPAÑA
Teléfono: +34 93 8970906
Fax: +34 93 3969750
E-Mail: info-es@schmersal.com
Internet: www.schmersal.es

Schmersal Ibérica, S.L.
Apartado 30
2626-909 Póvoa de Sta. Iria
PORTUGAL
Teléfono: +351 21 9593835
Fax: +34 93 3969750
E-Mail: info-pt@schmersal.com
Internet: www.schmersal.pt

K.A. Schmersal GmbH
Sistemas de conmutación
de seguridad industrial

Möddinghofe 30
D-42279 Wuppertal
Apartado postal 24 02 63 09
D-42232 Wuppertal
ALEMANIA

Teléfono: +49 (0)202 6464-0
Fax: +49 (0)202 6474-100
E-Mail: info@schmersal.com
Internet: www.schmersal.com

Elan Schaltelemente GmbH & Co. KG

Im Ostpark 2
D-35435 Wettenberg
Apartado postal 11 09
D-35429 Wettenberg
ALEMANIA

Teléfono: +49 (0)641 9848-0
Fax: +49 (0)641 9848-420
E-Mail: info-elan@schmersal.com
Internet: www.elan.de

04.2010