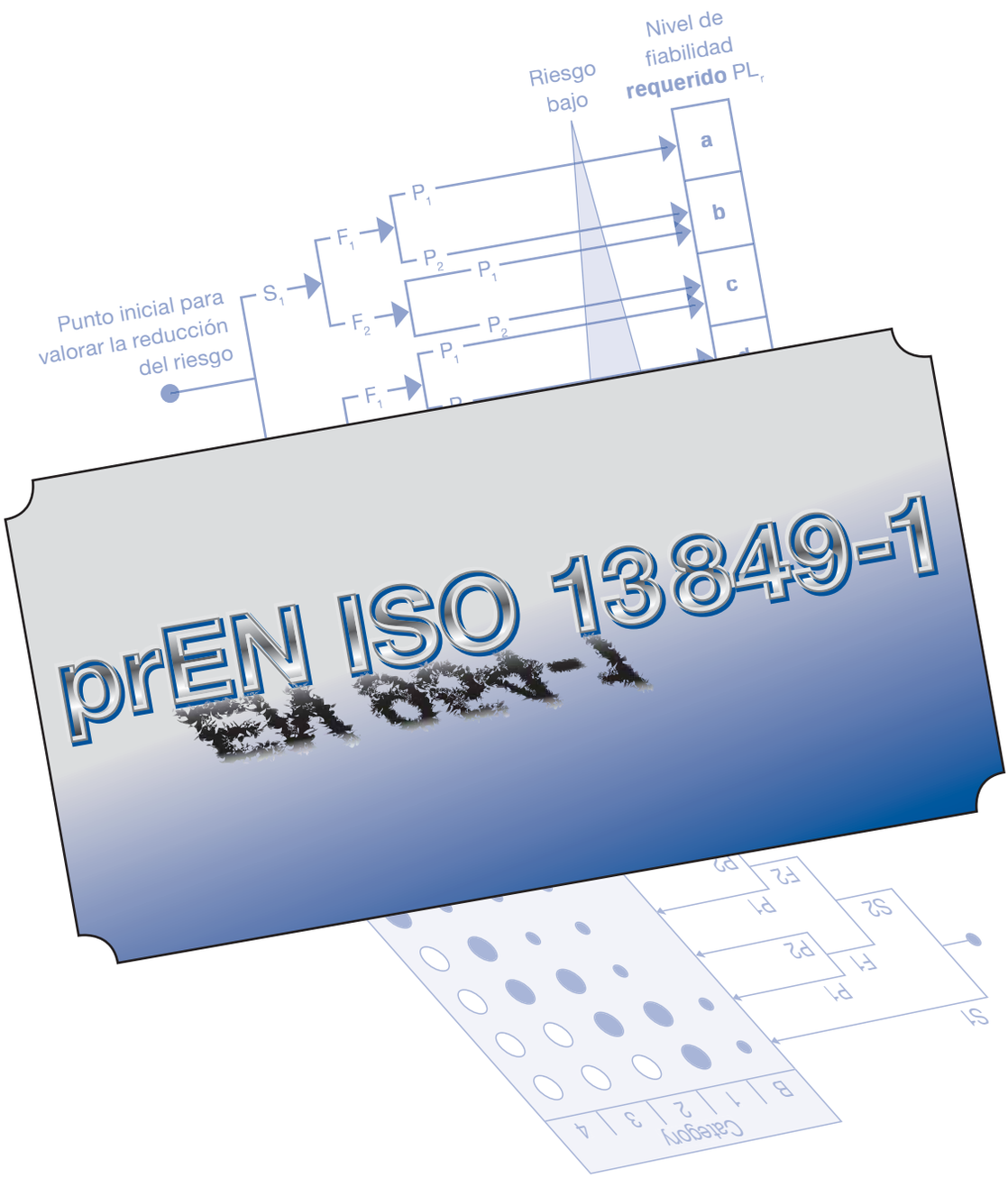
Una nueva visión en la seguridad de las máquinas:

prEN ISO 13849-1 –
Partes de los sistemas de mando relativas a la seguridad



SCHMERSAL Elan®

SCHMERSAL

Wuppertal/Wettenberg, marzo de 2006

Estimado cliente de SCHMERSAL:
Estimado cliente de Elan:

El presente folleto reproduce en detalle la presentación central de la conferencia que Elan celebró en 2005 para tratar la retirada de la norma EN 954-1 y los nuevos criterios de la norma revisada EN ISO 13849-1. Uno de los principales objetivos al publicar este folleto es demostrar la avanzada competencia que el Grupo Schmersal posee en el campo de la seguridad de las máquinas, como proveedor de dispositivos de conmutación y sistemas de seguridad concebidos para proteger a personas, máquinas y equipos. Deseamos además proporcionar a nuestros clientes información adicional sobre aspectos técnicos y normativas con el fin de ser vuestra compañía preferida a la hora de implantar componentes de seguridad y sistemas de mando de maquinas.

A continuación se resume la presentación de los ingenieros Thomas Börner y Karl-Heinz Büllesbach, empleados del Berufsgenossenschaftliches Institut für Arbeitsschutz – BGIA (Instituto de Seguridad y Salud de los Organismos de Seguros y Prevención de Riesgos Laborales) de Sankt Augustin, Alemania. Ambos trabajan en la unidad de electrónica del departamento técnico de protección de maquinas y sistemas de mando, una actividad íntimamente relacionada con el tema que nos ocupa. Los datos del presente documento se basan en la presentación en PowerPoint de los dos ingenieros, por lo que a ellos corresponde la propiedad intelectual de los mismos.

Tanto el BGIA, como las compañías de seguros y prevención de riesgos laborales del sector de la maquinas han mostrado un gran interés en el desarrollo de la norma revisada EN ISO 13849-1. Esta iniciativa esta destinada a las pequeñas y medianas empresas que fabriquen o utilicen máquinas y sistemas de mando, a las que se quiere ofrecer una orientación lo más simple y exhaustiva posible para su futura ejecución en todos los sistemas de mando relativos a la seguridad.

La aplicación de la norma prEN ISO 13849-1 es actualmente objeto de una gran controversia que afecta a un grupo concreto de normas.

La norma específica del sector IEC EN 62061 (derivada de la IEC EN 61508) también compite para reemplazar la EN 954-1, especialmente en el sector de los sistemas eléctricos, electrónicos y electrónicos programables con funciones de seguridad.

De todos modos, la gama de productos del grupo Schmersal ya está en disposición de cumplir las especificaciones de ambas normas futuras. Si tiene usted alguna duda relativa a este tema, consúltenos.

Para mayor claridad, hemos dividido la presentación “prEN ISO 13894-1: Una nueva visión de la seguridad de las máquinas” en diferentes apartados, que, a su vez, están subdivididos, para que el lector pueda profundizar en aquellos temas que sean de su interés.

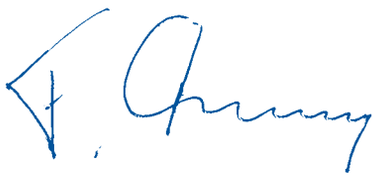
Le agradecemos por anticipado su comprensión respecto al uso de abreviaturas (las cuales son inevitables). De todos modos, se adjunta un glosario para facilitar la comprensión (véase la página desplegable).

Aunque hemos intentado que el resumen sea claro y comprensible, es posible que sólo hayamos conseguido este objetivo en parte, dada la complejidad del tema. Asimismo, es posible que queden algunas dudas por resolver.

Pese a todo ello, deseamos que la lectura de este documento le resulte interesante y esperamos trabajar con usted en un futuro.

Atentamente,

Heinz Schmersal
Consejero delegado
K.A. Schmersal Holding GmbH & Co. KG



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

Una nueva visión en la seguridad de las máquinas:
prEN ISO 13849-1 – Partes de los sistemas de mando relativas a la seguridad

Índice

Edición
Elan Schaltelemente GmbH & Co. KG
Im Ostpark 2
35435 Wettenberg
Teléfono +49 (0)641 9848-0
Fax +49 (0)641 9848-420
E-Mail: info@elan.schmersal.de
Internet: www.elan.de

Texto
Friedrich Adams
SCHMERSAL Holding GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
E-Mail: fadams@schmersal.de

Producción
Werbe-Grafik Heinz Flick, 35075 Gladenbach/
Druckteam Peter Bork, 35435 Wettenberg

Una nueva visión en la seguridad de las máquinas:
prEN ISO 13849-1 – Partes de los sistemas de mando relativas a la seguridad

Introducción

Cuando dentro de unos años la norma EN 954-1[1] sea sustituida, lo cual a estas alturas se da por sentado, se producirá una especie de cambio paradigma. En el futuro se reducirá la importancia en el enfoque determinista, en la ejecución de partes relacionadas con la seguridad de los sistemas de control de las máquinas, y aparecerán visiones probabilísticas.

Dos normas compiten por la sucesión de la EN 954-1: la primera es la prEN ISO 13849[2], diseñada especialmente para ser una continuación de la EN 954-1. La segunda es la IEC EN 62061[3], una derivada de la IEC EN 61508[4] específica del sector.

La teoría probabilista se mantendrá en el futuro en ambas normas (por lo menos en cuanto a la noción genérica de ingeniería de fiabilidad), independientemente de la decisión que se tome. En cambio, la norma EN 954-1 se basa esencialmente en el estudio de las estructuras.

En el presente artículo, basado en la conferencia de Elan de 2005, nos concentraremos en la prEN ISO 13849-1, la probabilística. Es decir, la teoría basada en el cálculo y establecimiento de modelos probabilísticos tiene una importancia mucho mayor en las normas IEC EN 61508 e IEC EN 62061. En cambio, en la prEN ISO 13849-1 se ha intentado conseguir un delicado equilibrio entre el pensamiento determinista y el probabilista, simplificando los nuevos elementos a un nivel necesario y practicable para el usuario medio (véase la Figura 1).

1) EN 954-1: 1997-03: Partes relacionadas con la seguridad de los sistemas de control de las máquinas. – Parte 1: Principios generales para el diseño (corresponde asimismo a la ISO 13849-1: 1999-11)

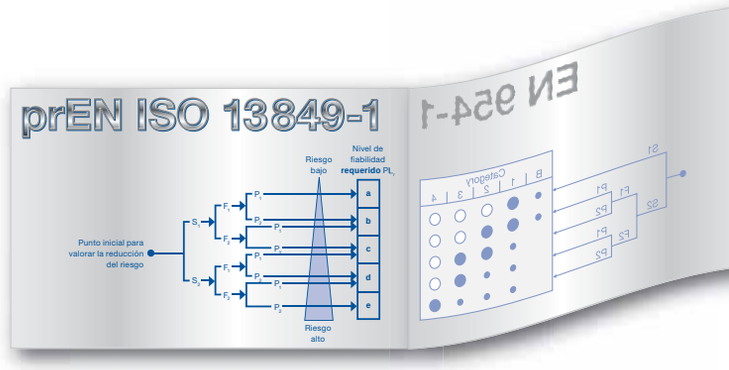
2) prEN ISO 13849-1: 2004-06: Partes relacionadas con la seguridad de los sistemas de control de las máquinas – Parte 1: Principios generales para el diseño.
ATENCIÓN: Este borrador no es idéntico a la versión definitiva. Actualmente están en preparación las versiones definitivas en cada país.

3) IEC EN 62061: 2005-10: Seguridad de las máquinas – seguridad funcional de los sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad

4) IEC EN 61508: 2002-11: Seguridad funcional de los sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad

- Parte 1: Requisitos generales
- Parte 2: Requisitos de los sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad
- Parte 3: Requisitos del software
- Parte 4: Términos y abreviaturas
- Parte 5: Ejemplos para calcular el nivel de integridad de seguridad
- Parte 6: Principios de aplicación de las normas IEC 61508-2 e IEC 61508-3
- Parte 7: Detalles de aplicación de procedimientos y medidas

Fuente: Beuth Verlag GmbH, 10772 Berlín; www.beuth.de



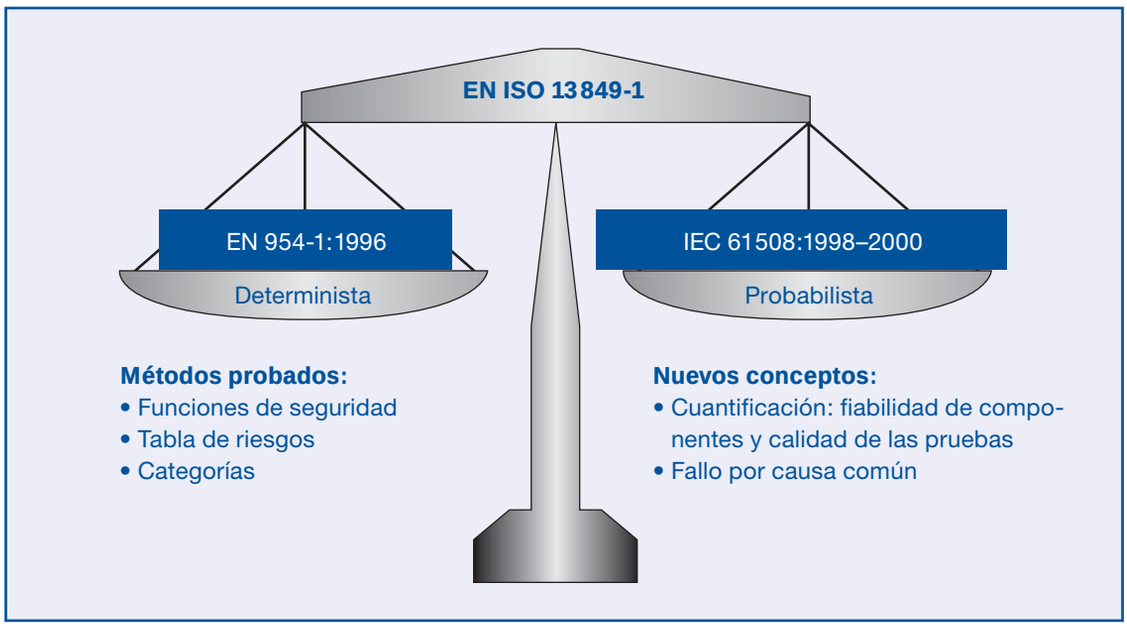


Figura 1: Equilibrio entre determinismo y probabilismo

Sin ánimo de ofender a los autores de la norma prEN ISO 13849-1, nos permitimos decir que se trata de una versión “light” de la IEC EN 61508. Y decimos “light” porque la característica particular de la prEN ISO 13849-1 es su intento de tener en cuenta los intereses de la mayoría de los clientes a los que se dirige, es decir, las pequeñas y medianas empresas de maquinaria y sistemas de mando, permitiendo simplificaciones y generalizaciones adecuadas y justificables en cuanto a la seguridad. A ello se suma el objetivo evidente de limitar los esfuerzos añadidos que implica la visión probabilista.

Por ejemplo, si nos centramos en el desarrollo de componentes electrónicos complejos basados en microprocesadores con funciones de seguridad, ya sean controladores de programas almacenados, sistemas de bus o escáneres láser, la norma prEN ISO 13849-1 es de poca utilidad. En estos casos sería mejor utilizar la IEC EN 61508.

Antecedentes de la retirada de la norma EN 954-1

A la pregunta de si la retirada de la EN 954-1 tiene sentido y responde a las incidencias de los accidentes de maquinaria, es decir, si los accidentes industriales pueden ser causados por las limitaciones y lagunas de la EN 954-1, la respuesta es un “no” rotundo.

Por lo menos, esa es la respuesta desde el punto de vista alemán, si bien ello no quiere decir que la norma EN 954-1 no sea mejorable y no admita críticas. Lo que se pone en duda es la necesidad de una sustitución total por otra norma que no suponga una compatibilidad absoluta y automática.

Por otro lado, durante muchos años ha existido una discusión extremadamente controvertida sobre la precisión de las perspectivas y normas de la EN 954-1, especialmente en otros estados miembros de la Unión Europea, pero también en círculos alemanes.

- Desde un punto de vista teórico, las críticas se basan esencialmente en el hecho de que la EN 954-1 “sólo” presenta medidas destinadas a reducir el riesgo en una gama de distintos niveles, con lo que se genera un único nivel de riesgo residual en todas las categorías[1]. Ello significa que el riesgo para el operador de la máquina es teóricamente constante, independientemente de que una SRP/CS[2] (parte relacionada con la seguridad de los sistemas de control de las máquinas) se ejecute de acuerdo con la categoría 1, 2, 3 o 4, y que no se diferencia, por ejemplo, entre el riesgo que supone una lesión leve (reversible) o grave (irreversible). Además, esta visión deriva de la falta de una categoría común en la norma EN 954-1.

  Los críticos exigen que a mayor nivel de riesgo se requieran medidas más estrictas para reducir el riesgo residual.

- Asimismo, como se menciona en la segunda crítica, los requisitos de la EN 954-1 no reflejan adecuadamente la complejidad creciente en los sistemas automatizados de las fábricas, es decir, en cuanto al análisis del número de “eslabones de la cadena” y de los diversos niveles de interconexión, no tiene suficientemente en cuenta si la SRP/CS se encuentra en una máquina individual, en un dispositivo complejo con múltiples conexiones o en un sistema de producción integrado. Asimismo, podría decirse que: **A mayor complejidad –> mayor nivel de riesgo residual –> ¡mayores medidas requeridas para controlar el riesgo residual!**

  La falta de consideración de la complejidad de la SRP/CS es, sin duda, un aspecto a tener en cuenta.

- Por otro lado, el argumento de que la EN 954-1 ya no refleja el estado actual de la tecnología es incuestionable, sobre todo porque, aunque no excluye explícitamente las tecnologías basadas en microprocesadores programables, no define ningún requisito referente a las mismas.

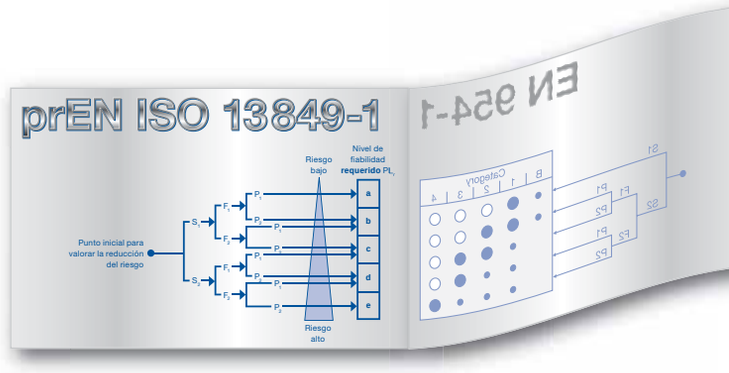
Esta representación de las críticas, que no pretende ser exhaustiva, sirve simplemente para comprender mejor el contexto de esta polémica, sin tener que entrar a fondo en el tema (véase también la Figura 2).

Críticas:

- Aunque es aplicable a sistemas programables y a electrónicas complejas, no presenta requisitos detallados.
- Los requisitos para la consideración de los valores de fiabilidad son inadecuados.
- La exclusión de defectos en la categoría 1 produce una falta de jerarquía para determinar el alcance de la reducción del riesgo.
- En la tabla de riesgos no existe una relación directa entre reducción del riesgo y categoría, y no se tiene en cuenta la complejidad.

Figura 2: Algunas críticas a la actual EN 954-1

1) Compárese también con la norma CR 954-100 – Principios de uso y aplicación de la norma EN 954.1
2) En adelante, nos referiremos a las partes relacionadas con la seguridad de los sistemas de control de las máquinas con las siglas SRP/CS, del inglés “safety-related part of a control system”.



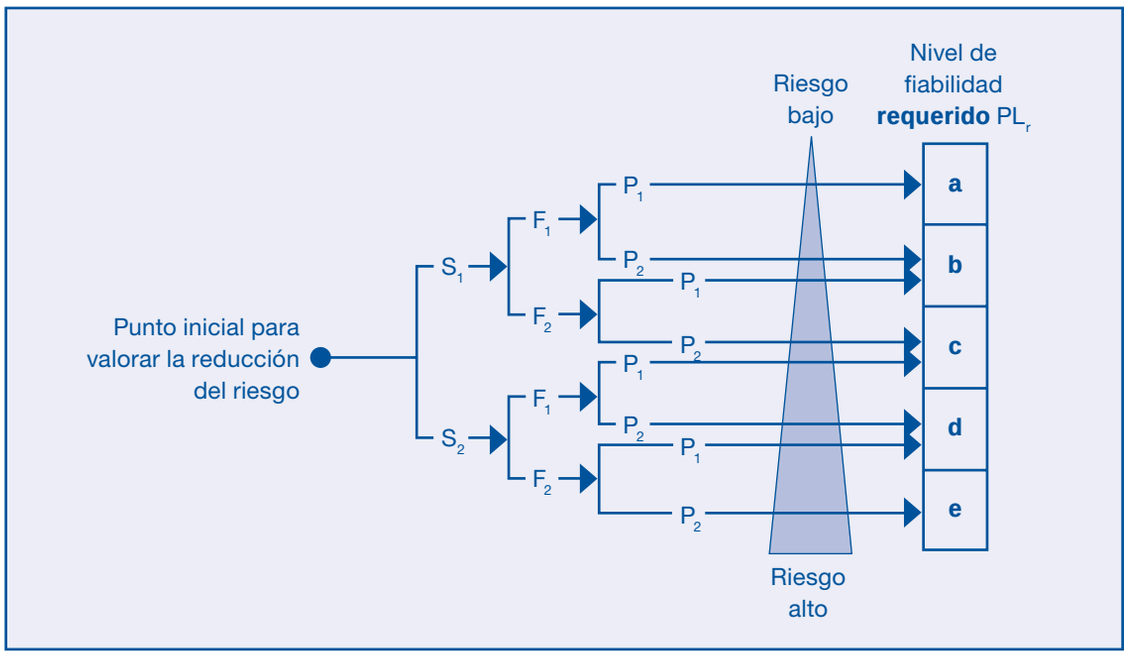


Figura 3: Reducción del riesgo y nivel de fiabilidad requeridos. S = gravedad de la lesión, F = frecuencia y/o duración de la exposición al riesgo, P = posibilidad de reducir el riesgo.

Nueva tabla de riesgos

Antecedentes
La norma prEN ISO 13849-1 también utiliza una tabla de riesgos (véase Figura 3); sin embargo, la consideración de los parámetros de riesgo ya no se traducen en categorías de control, como en la EN 954-1, sino en los denominados niveles de fiabilidad (PL).

El PL, nivel de fiabilidad, designa la capacidad de una parte relacionada con la seguridad de los sistemas de control de las máquinas (SRP/CS) de ejecutar una función de seguridad para alcanzar la reducción del riesgo deseado, un enfoque que incluye aspectos cuantitativos y cualitativos.

Los parámetros de riesgo individuales de la norma prEN ISO 13849-1 (gravedad de la lesión, frecuencia y duración de la exposición, etc.) no se modifican respecto a los de la norma EN 954-1.

Ejecución
El nivel de fiabilidad correspondiente (subdividido desde PL “a” hasta PL “e”) refleja los diferentes riesgos residuales, expresados como la probabilidad de fallo grave por hora o PFH_d[1] (véase también la Figura 4).

Por tanto, el enfoque de la nueva norma tiene en cuenta la probabilidad residual, es decir, incluye ingeniería de fiabilidad o una combinación de las visiones determinista y probabilista.

Los grados del PL se han seleccionado para que se ajusten a los niveles de integridad de seguridad (SIL) de la IEC EN 61508, y puedan asociarse a las categorías de control de la EN 954-1, si bien la coincidencia no es exacta (como ya hemos indicado); por ejemplo, la categoría 1 corresponde (aunque no exactamente) al PL “b”, la categoría 2, al PL “c”, etc.

1) PFH = probabilidad de fallo por hora

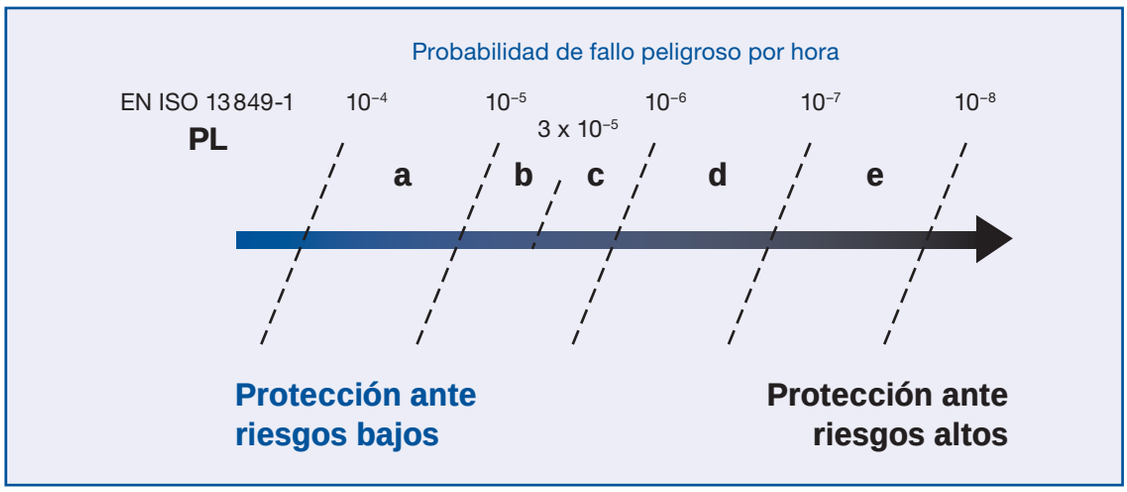


Figura 4: Definición del PL, como fiabilidad relativa a la seguridad

Aplicación

- Deben tenerse en cuenta todas y cada una de las funciones de seguridad de la máquina que surjan a partir de un análisis de riesgos, como, por ejemplo, la parada de emergencia, el enclavamiento de resguardos móviles, etc. El denominado PL_r es el producto de la consideración de la gráfica de riesgo (la letra "r" significa "requerido")[1].
- El PL es una consideración global, y siempre se refiere a la cadena de sensores (detección), al componente lógico (proceso) y al accionador (interruptor).

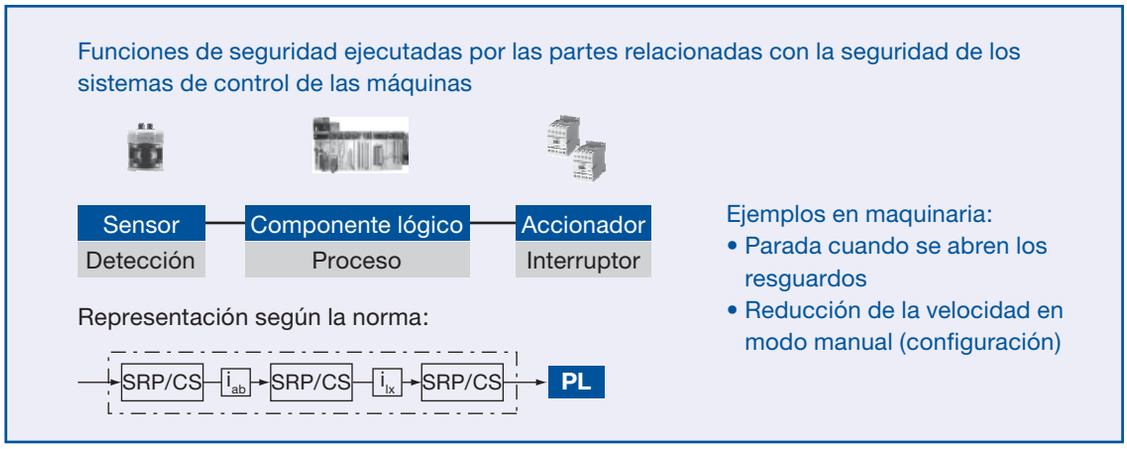


Figura 5: Función de seguridad y SRP/CS

1) La sistemática de la norma distingue entre PL_r y PL. PL_r se refiere al nivel de fiabilidad estimado necesario una vez considerado el riesgo (es decir, se trata de un valor deseado concreto). PL se refiere al resultado del análisis (es decir, se trata del valor real).

Nuevos aspectos a tener en cuenta
El resultado de la combinación de los enfoques determinista y probabilista (el equilibrio al que nos hemos referido anteriormente) es que para la determinación del PL hay que tener en cuenta los siguientes aspectos (véase también la Figura 6):

1. La categoría de control (de forma aproximada, como ya hemos mencionado) contenida en la norma, es denominada de forma predominante “arquitectura designada”.

2. El “$MTTF_d$” (tiempo medio hasta el fallo peligroso).

3. La “cobertura de diagnóstico” (DC).

4. La denominada “gestión de fallos por causas comunes” (CCF).

Asimismo, existen medidas para contrarrestar los fallos de sistema, un prerrequisito ya presente en la norma prEN ISO 13849-1 y que aparece en el Anexo G. Su origen es la teoría del fallo en la ingeniería de fiabilidad, que distingue entre fallos coincidentes (véase $MTTF_d$) y sistemáticos, entre otros (véase la Figura 7).

Los fallos sistemáticos tienen causas deterministas no coincidentes, y sólo pueden eliminarse mediante modificaciones en el diseño, la producción, las secuencias de operación o factores similares.

El Anexo G sugiere las siguientes medidas:

- Una selección de las contenidas en la norma EN ISO 13849-2.
- La protección ante las influencias procedentes del entorno.
- Medidas informáticas típicas (control y revisión de programas, etc.)
- Protección de las comunicaciones de datos.

Figura 7: Impedir y controlar errores sistematicos

Aplicación
- Deben tenerse en cuenta todas y cada una de las funciones de seguridad de la máquina que surjan a partir de un análisis de riesgos, como por ejemplo la parada de emergencia, el enclavamiento de resguardos móviles, etc. El denominado PL_r es el producto de la consideración de la gráfica de riesgo (la letra “r” significa requerido).

- El PL es una consideración global, y siempre se refiere a la cadena de sensores (detección), al componente lógico (proceso) y al accionador (interruptor) (véase la Figura 5).

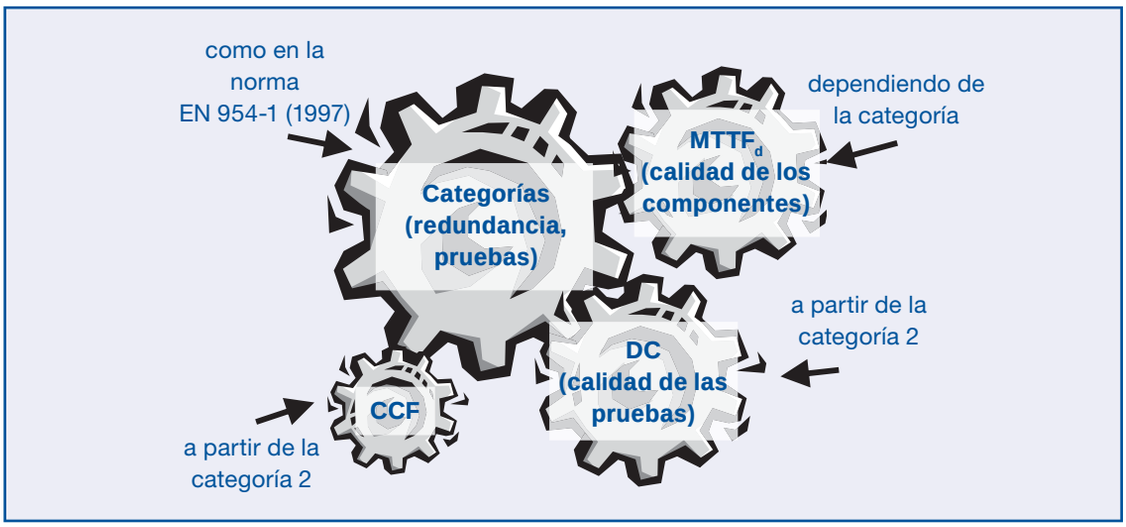


Figura 6: Extensión de los términos referidos a las categorías

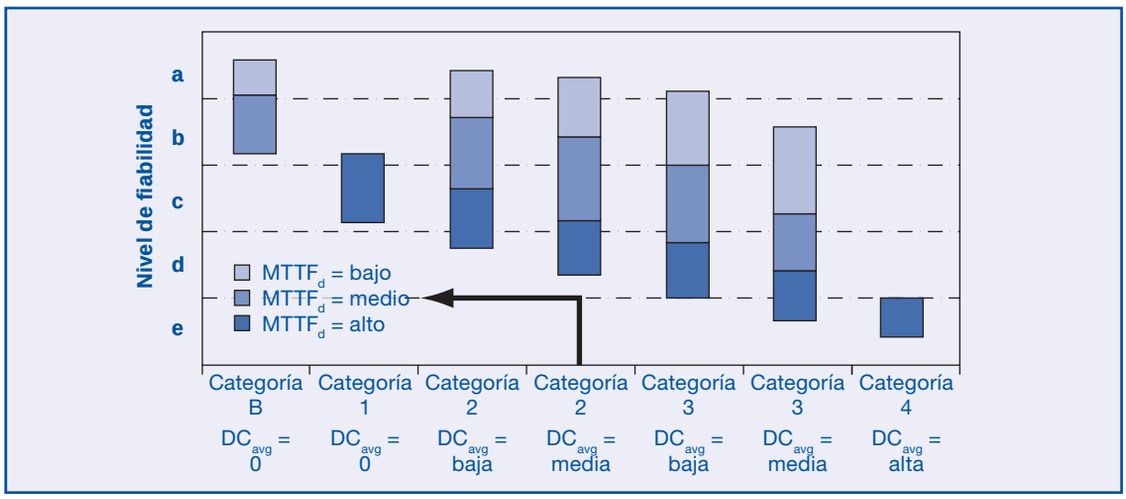


Figura 8: Determinación simplificada del Nivel de Fiabilidad (PL)

El nivel de fiabilidad en sustitución de la categoría de control

El resultado de los análisis del 1 al 4 (es decir, el análisis de la arquitectura designada, el $MTTF_d$ por canal, la DC y el CCF) se introducen en un diagrama de bloques a partir del cual se obtiene el nivel de fiabilidad alcanzado (véase la Figura 8).

Ello significa que un PL “e” requiere una estructura que corresponda a la categoría 4, un valor $MTTF_d$ por canal “alto” y una DC igualmente “alta” (el concepto de DC_{avg} corresponde a la cobertura media de diagnóstico).

Si, en cambio, el objetivo es que la reducción del riesgo alcance un PL “c” o “d”, pueden seleccionarse varias posibilidades de diseño; por ejemplo, para un PL “d”, una estructura conforme a la categoría 2, un $MTTF_d$ “alto” y una DC “media”. A partir de la categoría 2 debe tenerse siempre en cuenta el factor CCF.

Debido a que los límites entre los diferentes PL del diagrama no coinciden exactamente con las categorías, se permite una simplificación (en la norma se incluye una tabla, en lugar de un gráfico). Véase la Figura 9.

Aquí concluye esta breve descripción a grandes rasgos de la prEN ISO 13849-1.

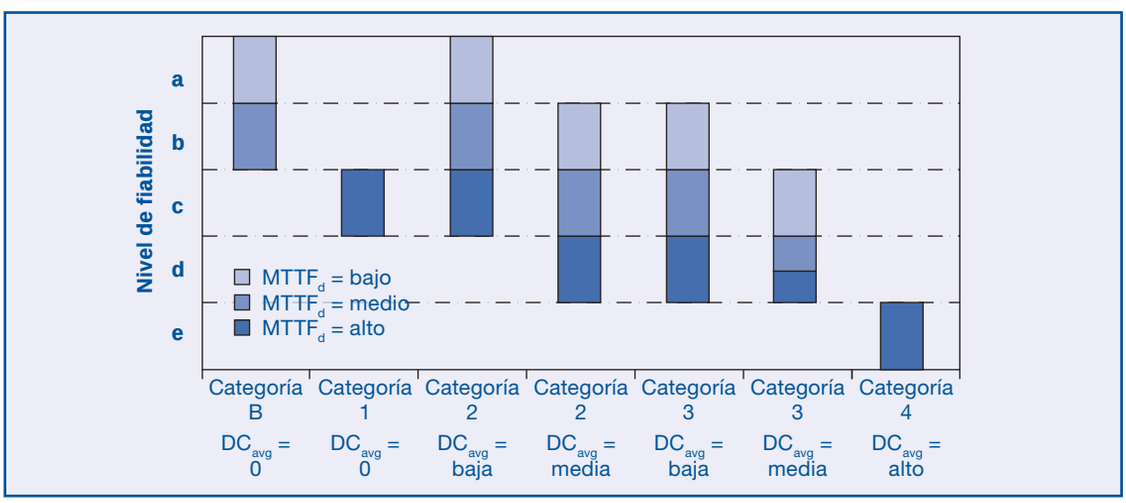
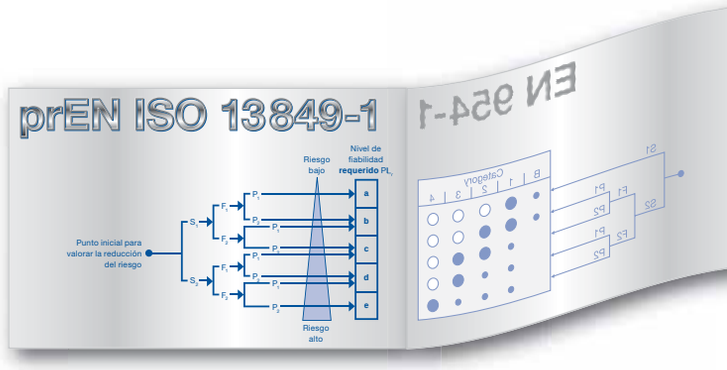


Figura 9: Nivel de fiabilidad (PL): determinación alternativa mediante una tabla



Arquitecturas designadas

Antecedentes
La norma prEN ISO 13849-1 tiene en cuenta las categorías de control ya conocidas a través de las denominadas “arquitecturas designadas”, que pueden describirse como un cálculo avanzado de las estructuras de SRP/CS. Por cálculo avanzado nos referimos a que ya se ha comprobado la contribución de estas estructuras a la reducción del riesgo en el marco de los modelos de Markov, conforme a la norma IEC 61508. Por tanto, el usuario de la norma prEN ISO 13849-1 ya no tiene que preocuparse por esos cálculos matemáticos complejos.

La consideración de la arquitectura designada de una SRP/CS actualiza el enfoque determinista anterior a la EN 954-1. Sin embargo, como ya se ha indicado, en el futuro se referirá sólo a un aspecto de los muchos que conforman el nivel de fiabilidad.

Si le parece que ya ha oído hablar de las arquitecturas designadas, está en lo cierto. Básicamente, se refieren ni más ni menos que a las estructuras de SRP/CS ya conocidas, establecidas y comprobadas de las varias categorías de control que se aplican en la norma EN 954-1. Sin embargo, una excepción es la categoría 2 (como hemos indicado).

Ejecución
La norma prEN ISO 13849-1 reconoce las arquitecturas designadas de la Figura 10.

Aplicación
El establecimiento de arquitecturas designadas supone un avance positivo hacia la simplificación en la prEN ISO 13849-1; sin embargo, quedan algunas cuestiones por resolver (que tampoco se resuelven en la interpretación de la EN 954-1).

Entre ellas está la cuestión de cómo debe ejecutarse la función de dos canales en el nivel del sensor y el accionador en las categorías 3 y 4. Ello significa que las funciones del sensor y el accionador deben estar físicamente presentes dos veces, por ejemplo en forma de dos interruptores en el controlador de posición de un resguardo móvil, y no se especifica qué medidas deben tomarse si uno desea desviarse de las arquitecturas designadas.

Pueden considerarse muchas alternativas:

La opción 1 se basa en la norma C (norma de productos), que ofrece sugerencias de diseño precisas. Por ejemplo, en máquinas de papel e impresoras, basta con un único interruptor de seguridad eléctrico de 2 canales para el control de posición de un resguardo móvil.

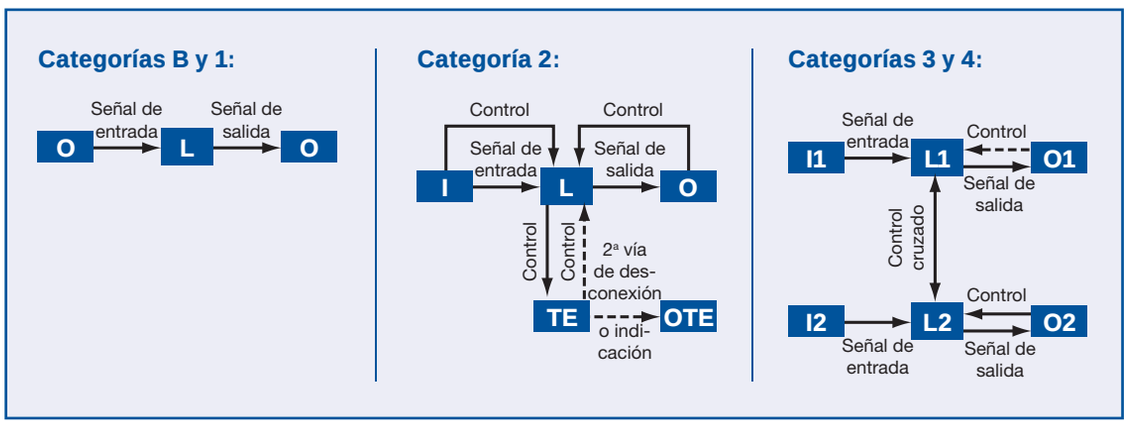


Figura 10: Introducción a las arquitecturas designadas

La opción 2 consiste en utilizar la exclusión de defectos (véase Figura 11). En tal caso, debe realizarse con las mismas precauciones que con la EN 954-1. Se pueden emplear las listas de exclusiones de defectos de los Anexos A al D de la norma EN ISO 13849-2 (anteriormente EN 954-2) o realizar los análisis uno mismo, siguiendo estrictamente la Sección 3.3 de la norma ISO 13849-2.

¿Cuándo puedo realizar una exclusión de defecto?

No siempre es posible evaluar una SRP/CS sin asumir la exclusión de ciertos defectos. Para obtener información detallada sobre exclusión de defectos, véase la norma EN ISO 13849-2.

Las exclusiones de defectos pueden basarse en:

- La improbabilidad técnica de la incidencia de ciertos defectos.
- La experiencia técnica generalmente aceptada, independientemente de la aplicación.
- Las exigencias técnicas relativas a la aplicación y a los riesgos especiales.

Figura 11: Exclusión de defectos

La opción 3 consiste en dejar de lado las simplificaciones de la prEN ISO 13849-1 y realizar los cálculos matemáticos según los modelos de Markov, las redes de Petri o similares (o encargar a alguien que los realice) (véase la Figura 12).

¿Es absolutamente fundamental que utilice arquitecturas designadas, o puedo prescindir de ellas?

4.5.1 ... Existen varios métodos para estimar los aspectos cuantificables del PL de cualquier tipo de sistema, por ejemplo una estructura compleja. Algunos de ellos son los modelos de Markov, las redes de Petri estocásticas generalizadas (GSPN) o los diagramas de bloques de fiabilidad [véase la serie EN 61508 (IEC 61508)].

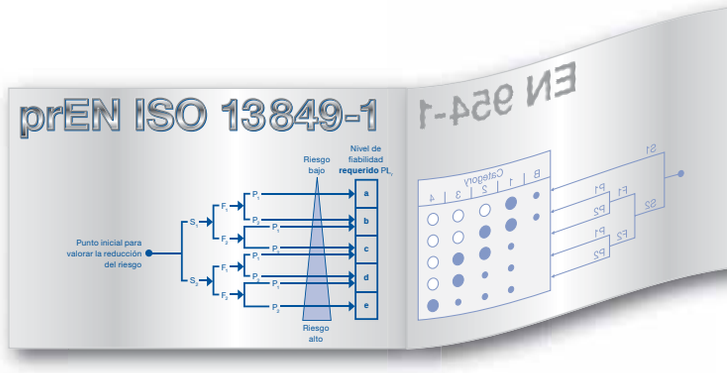
Para facilitar la evaluación de los aspectos cuantificables del PL, la norma proporciona un método simplificado basado en la definición de cinco arquitecturas designadas que cubren criterios de diseño y comportamientos específicos en condiciones de fallo.

Figura 12: "No hay norma sin excepción"

¡ATENCIÓN al utilizar la arquitectura designada para la categoría 2!

Aunque la descripción anterior da por sentado que las llamadas arquitecturas designadas son bien conocidas, existe una excepción fundamental, que es la estructura recomendada para la categoría de control 2.

En este caso se producirá un cambio considerable: mientras que la categoría de control 2 establecía hasta ahora que las estructuras de 1 canal debían ser controladas automáticamente por los mandos de la máquina a intervalos adecuados, en el futuro, con una arquitectura designada, la frecuencia de comprobación deberá ser 100 veces más elevada que la demanda previsible de la función de seguridad, y deberá existir una segunda salida (véase la Figura 13 de la pág. 15).



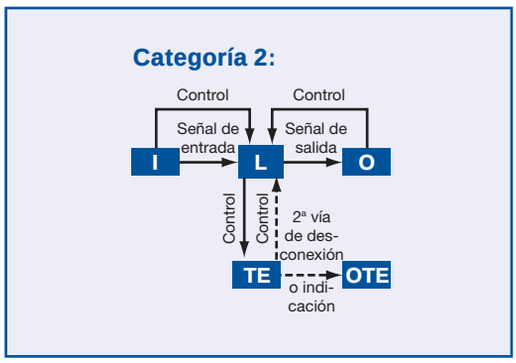


Figura 13: Nuevos requisitos de la categoría de control 2

Básicamente, esta arquitectura designada es como una versión “light” de la categoría de control 3. Cuando al final de este documento intentemos resumir las modificaciones prácticas derivadas de la introducción de la prEN ISO 13849-1, el resumen incluirá la recomendación imperativa de que se comprueben las SRP/CS con categoría de control 2 para ver si cumplen con los requisitos futuros.

Valores de $MTTF_d$

Antecedentes

Lo primero que hay que decir sobre las consideraciones de la prEN ISO 13849-1 sobre el $MTTF_d$, a pesar de que a veces se olvide, es que las SRP/CS siempre conservan un potencial de fallo residual de efecto crítico para la seguridad (el potencial de fallo por coincidencia de fallos peligrosos). De ahí la necesidad de controlar este riesgo residual, es decir, de reducirlo a un nivel aceptable.

Un ejemplo sería un interruptor que no abre o no cierra. Generalmente, en una máquina, un interruptor que no abre conlleva un estado peligroso, en ausencia de redundancia o de una pronta identificación del fallo. Sin embargo, no todos los interruptores son iguales: existen diferencias de diseño, material, etc.

Asimismo, puede decirse que existen diferencias de calidad que pueden afectar a la probabilidad de estos fallos coincidentes.

Así pues, el $MTTF_d$ es un indicador de calidad que se refiere a la fiabilidad de los componentes y dispositivos de seguridad de una SRP/CS.

Por definición, el $MTTF_d$ es una media estadística que representa el tiempo de funcionamiento sin averías previsto por año (= MTTF), si bien en la prEN ISO 13849-1 sólo se tienen en cuenta las averías como un componente peligroso. De ahí el término $MTTD_d$ (“d”, del inglés “dangerous”, significa “peligroso”, y no todos los fallos tienen un efecto crítico sobre la seguridad). Por tanto, el valor $MTTF_d$ siempre es mayor que el MTTF. El valor se expresa en años (= a).

Por consiguiente, el valor $MTTF_d$ es siempre el inverso (el valor recíproco) del valor PFH_d. Un valor $MTTF_d$ de 10 a, por ejemplo, equivale a un valor PFF_d de $1{,}14 \times 10^{-5}$ (1/10 × 8.760), aunque sólo hace referencia a un canal[1].

Al considerar el MTTF o el $MTTF_d$, se asume una distribución exponencial del fallo coincidente, es decir, después de la secuencia del MTTF o $MTTF_d$, el 63% de todas las unidades (peligrosas) ya han fallado, y la probabilidad de supervivencia de las unidades afectadas es de sólo el 37% (véanse las Figuras 14 y 15).

1) Los valores de PFH, calculados según la norma IEC EN 61508, pueden incluirse en cálculos realizados según la prEN ISO 13894-1, siempre que se tengan en cuenta los detalles del SIL. De este modo se obtiene una visión simplificada, especialmente en estructuras de 2 canales, pero existe menos riesgo de que los cálculos den unos resultados demasiado optimistas.

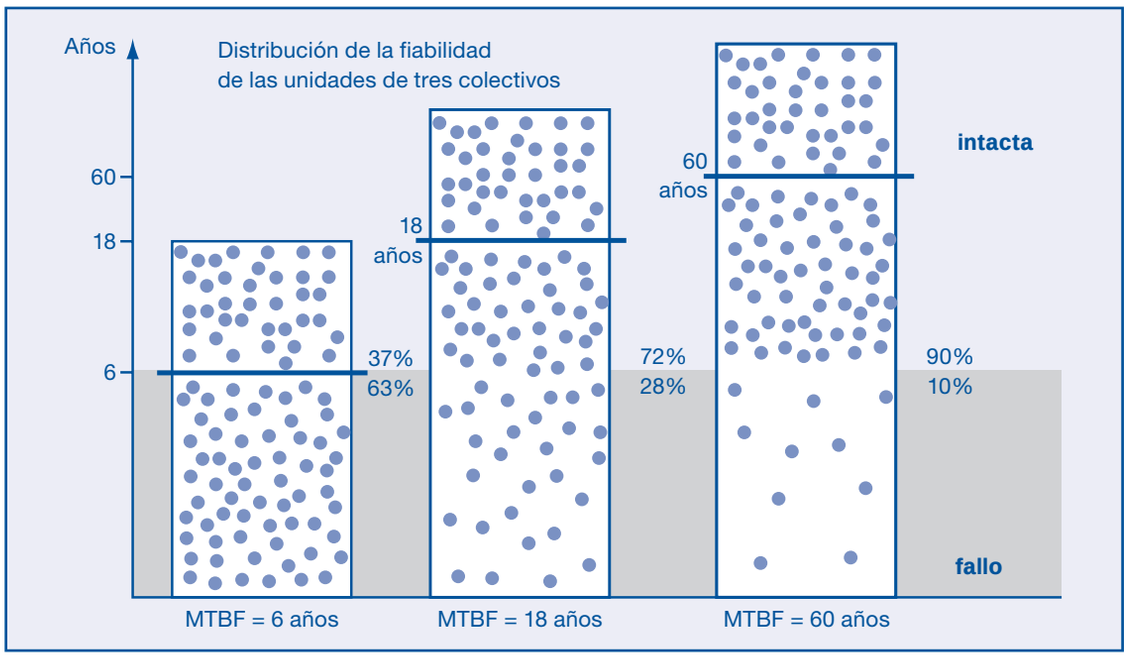


Figura 14: Ilustración de la vida útil media: se representan tres colectivos con diferentes niveles de fiabilidad. Sus unidades (representadas por los puntos) fallan en momentos coincidentes. Las coordenadas verticales indican el momento del fallo. Estos momentos están separados por períodos largos. Por ejemplo, en el caso del primer colectivo, algunas unidades duran 18 años mientras que otras ya han fallado al cabo de un año. El 63% ya han fallado al cabo de 6 años. (Fuente: Introducción a los métodos de análisis de fiabilidad, SIEMENS AG, 1&S IS ICS IT2)

Dicho de otro modo:

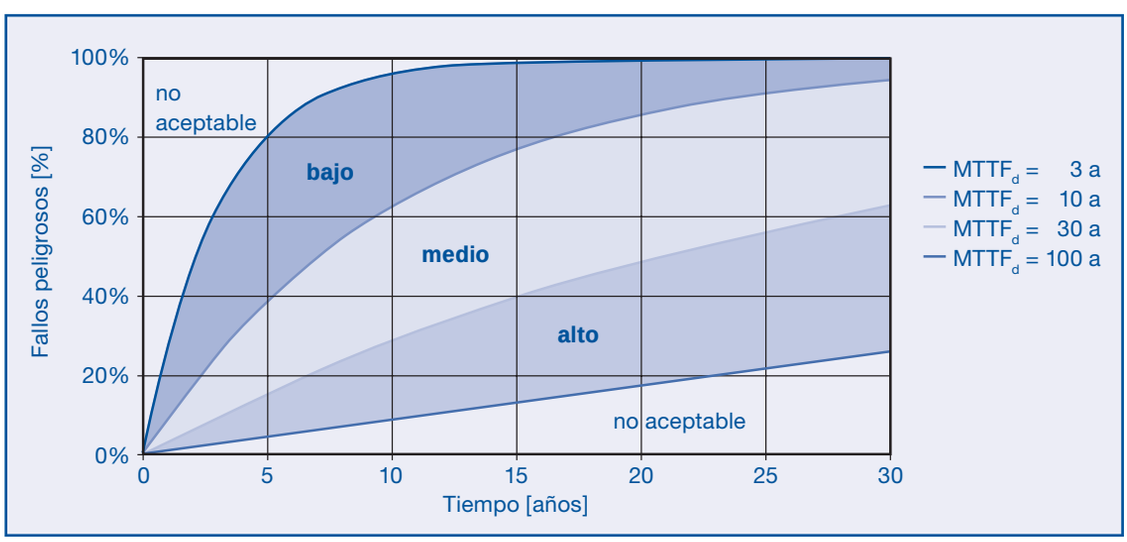
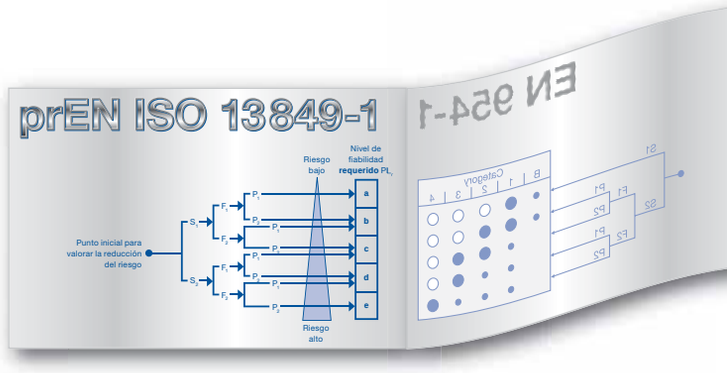


Figura 15: ¿Qué significa exactamente el MTTF$_d$?



ATENCIÓN: Una excepción a esta distribución exponencial asumida, típica de la electrónica, son los componentes afectados por desgaste, que tienen una distribución de vida útil diferente. Este factor se refleja en la norma prEN ISO 13849-1 a través del tamaño intermedio del cálculo del valor B_{10d} (véase más adelante).

Ejecución
En la norma prEN ISO 13894-1, la consideración del $MTTF_d$ y el PHF varía dependiendo de si se usan:

- en un único componente de seguridad
- en un único canal de una SRP/CS
- en una SRP/CS completa.

La diferenciación indicada sólo puede entenderse teniendo en cuenta que una gran parte de los usuarios de componentes de seguridad y otros dispositivos recogidos en la prEN ISO 13894-1 no los fabrican, sino que los adquieren y los integran a una SRP/CS.

En el futuro, estos usuarios de la prEN ISO 13894-1 que adquieran componentes de seguridad listos para su uso, como los del Grupo Schmersal, lo tendrán aún más fácil, ya que se supone que todos los principales fabricantes incluirán los valores correspondientes a la norma prEN ISO 13894-1 en su documentación técnica.

El comprador de componentes de seguridad tiene derecho a exigir a su proveedor que le proporcione estos datos a tiempo, antes de que la prEN ISO 13849-1 entre en vigor. No tiene por qué ser inmediatamente, pero sí al menos pronto (véase el apartado “Entrada en vigor de la norma prEN ISO 13849-1”).

Asimismo, también pueden exigir esta información de los proveedores quienes adquieran otro tipo de componentes y dispositivos que desde el punto de vista de la directiva sobre máquinas CE (MRL) no sean estrictamente componentes de seguridad, sino productos de doble uso, es decir, aplicables simultáneamente a tareas operativas y a funciones de seguridad.

ATENCIÓN: Si se establece una exclusión de defectos para un componente, el valor $MTTF_d$ de la fórmula correspondiente debe considerarse ∞ (véase más adelante).

Aplicación:
$MTTF_d$ para un solo canal
En este caso, en referencia a la fórmula de la Figura 16, el usuario sólo tiene que sumar los valores de $MTTF_d$ individuales de los componentes del SRP/CS mediante el método denominado de recuento de partes. Véase también el ejemplo de cálculo de la página 18.

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

Figura 16: $MTTF_d$ por canal (método de recuento de partes)

La suma se compara con los valores de las tablas siguientes (véase la Figura 17) para indicar la calidad de la seguridad de un canal individual de un SRP/CS.

Descripción de la calidad	Rango de valores de $MTTF_d$
baja	3 años ≤ $MTTF_d$ < 10 años
media	10 años ≤ $MTTF_d$ < 30 años
alta	30 años ≤ $MTTF_d$ ≤ 100 años

¡El $MTTF_d$ es una media estadística y no garantiza la duración de la vida útil!

Figura 17: El $MTTF_d$ es una media estadística del tiempo de funcionamiento sin fallos peligrosos en un solo canal de control

Ejemplo de cálculo

j	Componente	Unidades (n_j)	$MTTF_{d,j}$ [a] peor caso	$1/MTTF_{d,j}$ [1/a] peor caso	$nj/MTTF_{d,j}$ [1/a] en peor caso
1	Transistor biploar de baja potencia	2	1142	0,000876	0,001752
2	Resistencia de película de carbón	5	11416	0,000088	0,000438
3	Condensador convencional, sin alimentación	4	5708	0,000175	0,000701
4	Relé (datos del fabricante)	4	1256	0,000796	0,003185
5	Contactor	1	32	0,031250	0,031250
$\Sigma(n_j/MTTF_{d,j})$					0,037325
$MTTF_d = 1/\Sigma(n_j/MTTF_{d,j})$ [y]		**26,79**			

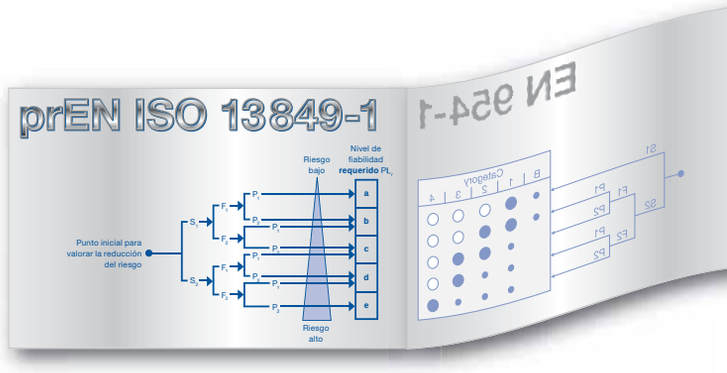
Este ejemplo da un $MTTF_d$ de 16,8 años, un valor “medio” según la figura 17.
En este ejemplo, el contactor tiene una gran influencia. En general se obtienen resultados mucho mejores, es decir, un $MTTF_d$ más alto.

Además, se aplican las siguientes normas:

- Los valores de $MTTF_d$ siempre se aplican a un canal, es decir, no importa si se trata de una estructura (o arquitectura designada) de 1 o 2 canales, a menos que los canales se estructuren de forma distinta. En este caso se aplica una fórmula denominada de simetrización (véase la Figura 18).

- El fabricante o distribuidor de la maquinaria es responsable de calcular o encargar el cálculo del valor $MTTF_d$ de un canal según las condiciones de la directiva CE sobre máquinas.

- ATENCIÓN: Si el cálculo produce varios valores de $MTTF_d$ por canal superiores a 100 años, el exceso se “recorta”, ya que un canal de SRP/CS sólo puede tener un valor $MTTF_d$ de 100 años como máximo (a diferencia de un componente de seguridad, que, considerado individualmente, puede tener un valor muy superior). Con esta restricción de 100 años, los creadores de la norma pretenden evitar que los valores de $MTTF_d$ den una visión demasiado optimista, con el fin de obtener un nivel de fiabilidad superior o permitir el uso de métodos de cálculo para sustituir las estructuras de 1 canal cuando se requieren estructuras de 2 canales.



- **Las arquitecturas designadas asumen el mismo $MTTF_d$ para ambos canales.**
- **Fórmula de simetrización para valores de $MTTF_d$ distintos:**

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

- **Ejemplo: $MTTF_{d\,c1}$ = 3 años, $MTTF_{d\,c3}$ = 100 años, de modo que el $MTTF_d$ = 66 años**

Figura 18: Diferentes $MTTF_d$ por canal –> simetrización

- ATENCIÓN: La unificación de los diferentes dispositivos de seguridad de una SRP/CS debe cumplir las siguientes condiciones:
  - la aplicación debe seguir estrictamente la información contenida en el manual de instrucciones
  - pueden realizarse exclusiones de defectos adicionales, especialmente en lo referente al cableado eléctrico, de acuerdo con la norma ISO 13849-2.
- Cuando se utilice software, hay que cumplir los requisitos adicionales de la prEN ISO 13849-1 (véase la Sección 4.6).
- La denominada fórmula de simetrización es aplicable cuando dos canales de una SRP/CS se hayan estructurados de forma diferente (véase la Figura 18).

Notas

- En el caso de los componentes o dispositivos individuales diseñados para una SRP/CS del sector que cubre la norma IEC EN 61508 (o IEC EN 62061), en general se aplica un valor denominado lambda (λ). El valor equivale al PFH_d de la norma prEN ISO 13849-1.

  Sin embargo, si se desea oscilar entre los ámbitos de la prEN ISO 13849-1 y la IEC EN 61508 (o IEC EN 62061) en componentes y dispositivos de seguridad (véase la página 44), recomendamos el uso del nivel de fiabilidad o SIL.

- Si sólo se dispone de un valor MTTF (es decir, no existe valor $MTTF_d$), éste puede duplicarse (siempre y cuando exista un equilibrio aproximado entre fallos peligrosos e inofensivos) para obtener el valor $MTTF_d$. La norma prEN ISO 13849-1 recomienda que en caso de duda sólo se incluya una parte del valor en el cálculo (se sugiere un 10%) para quedarse corto.
- Si sólo se dispone de un valor MTBF, para simplificar, se puede considerar generalmente como un valor MTTF.

Aplicación: cálculo del $MTTF_d$ para un único dispositivo de seguridad

Este apartado va dirigido a quienes construyen para su propio uso dispositivos de seguridad, sistemas de mando y productos de uso dual. La norma es dividir los equipos de seguridad en sus componentes funcionales y calcular el valor $MTTF_d$ mediante el método de recuento de partes (ya descrito).

En este caso, la norma prEN ISO 13849-1 también ofrece alternativas si no existen valores MTTF ni $MTTF_d$, proporcionando valores típicos en las tablas del anexo C para componentes eléctricos y electrónicos individuales (véase la Figura 19). Otros documentos de referencia son, por ejemplo, la norma SN 29500 o los manuales MIL.

Las tablas C.2 a C.7 indica los valores típicos $MTTF_d$ para componentes eléctricos según la norma SN 29500:

Componente	Ejemplo	MTTF [a] compo-nente	$MTTF_d$ [a] tipico	$MTTF_d$ [a] peor caso	Fallos peli-grosos
Transistor bipolar	TO18, TO92, SOT23	34.247	68.493	6.849	50%
Diodo supresor		15.981	31.963	3.196	50%
Condensador	KS, KP, MKT, MKC …	57.078	114.155	11.416	50%
Resistencia de película de carbón		114.155	228.311	22.831	50%
Optoacoplador con salida bipolar	SFH 610	7.648	14.840	1.484	50%

Figura 19: $MTTF_d$ para componentes electrónicos (ejemplos)

Los componentes y dispositivos afectados por desgaste en una SRP/CS reciben una consideración especial en la norma prEN ISO 13849-1, ya que en estos casos la demanda (concretamente, el modo de demanda) tiene una influencia sustancial sobre el valor $MTTF_d$.

Sólo los componentes y dispositivos de seguridad electrónicos tienen un valor $MTTF_d$ directo, puesto que en estos casos la denominada “curva de bañera” puede considerarse un indicador de los fallos independientes del desgaste. Tanto la parte izquierda (fallos tempranos) como la parte derecha de la curva de bañera se excluyen. La parte izquierda no se considera porque se supone que el fabricante ya ha abordado los fallos tempranos mediante las medidas adecuadas, como por ejemplo el envejecimiento artificial. La parte derecha se excluye porque se asume que se encuentra mucho más allá de la vida útil real.

Valores B_{10d}

Existen magnitudes intermedias para la conversión del valor $MTTF_d$. La primera de ellas es el valor B_{10d}, empleada en los componentes afectados por desgaste, como por ejemplo los dispositivos electromecánicos, fluídicos y mecánicos. Este valor equivale a una especie de índice de capacidad de ciclo funcional, que valora la aceptabilidad de la función de seguridad según el método Weibull.

El valor B_{10d} se convierte teniendo en cuenta las condiciones de la aplicación, es decir, la duración del uso y la demanda media de la función de seguridad del componente correspondiente, en un valor $MTTF_d$ (véase la Figura 20).

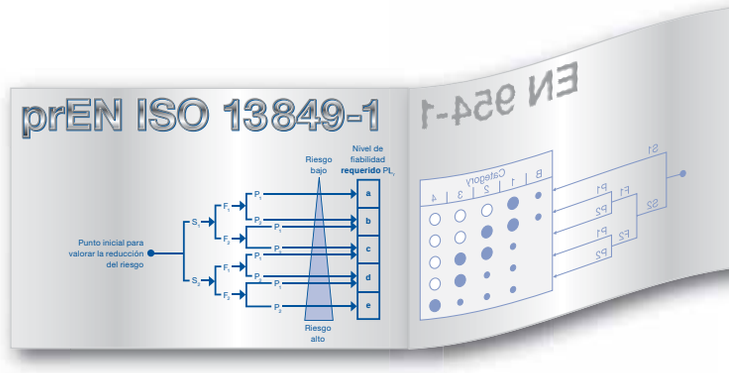
- **El fabricante proporciona el valor B_{10d} para el componente** (valor en ciclos de funcionamiento, en que estadísticamente el 10% de las muestras analizadas son fallos peligrosos).
- **Es necesario determinar la frecuencia media de conmutación de la aplicación, por ejemplo 0,2 Hz => intervalo t_{ciclo} = 5 s.**
- **Conversión de B_{10d} (ciclo de funcionamiento) a $MTTF_d$ (años):**

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3.600 \frac{s}{h}}{t_{ciclo}}$$

d_{op} = número de días de servicio por año
h_{op} = media de horas de servicio por día
n_{op} = media de ciclos de funcionamiento por año
t_{cycle} = demanda media de la función de seguridad en s (por ejemplo, 4 x por hora = 1 x por 15 min = 900 s)

Figura 20: Cálculo del $MTTF_d$ para componentes con desgaste.



Componentes mecánicos	$MTTF_d$ = 150 años
Componentes hidráulicos	$MTTF_d$ = 150 años
Componentes neumáticos	B_{10d} = 20.000.000
Relés/contactores (con carga pequeña)	B_{10d} = 20.000.000
Relés/contactores (con carga máxima)	B_{10d} = 400.000
Contactor principal (carga pequeña)	B_{10d} = 20.000.000
Contactor principal (carga máxima)	B_{10d} = 2.000.000
Dispositivo de parada de emergencia	B_{10d} = 10.000
Dispositivo de mando (pulsador)	B_{10d} = 100.000

Factor de 50

Figura 21: Valores B_{10d} (extracto) según la norma

Además (véase figura 21), la norma prEN ISO 13849-1 ofrece recomendaciones para decidir qué valores B_{10d} pueden adoptarse para dispositivos típicos afectados por desgaste, en el caso de que el fabricante no dé ninguna indicación.

Estos valores se diferencian según si el dispositivo correspondiente trabaja a plena carga o a carga baja (por ejemplo, en el caso de los contactores y relés). El término “a plena carga” no sólo se usa en su sentido eléctrico, sino que también se refiere a las condiciones ambientales especialmente desfavorables, y en general a toda condición de funcionamiento no óptima.

La magnitud de la carga pequeña se define en la norma como un 20%, aunque se permite la representación (no lineal) de valores intermedios. Por ejemplo, a 20,0 millones de ciclos de funcionamiento al 20%: 2,5 millones de ciclos de funcionamiento al 40%, 2,5 millones de ciclos de funcionamiento al 60% y 1,0 millón de ciclos de funcionamiento al 80%.

t_{ciclo} =	24 h	1 h	1 min	1 s
Componentes neumáticos	547.945	22.831	380	6,3
Relés/contactores (con carga pequeña)	547.945	22.831	380	6,3
Relés/contactores (con carga máxima)	10.960	457	7,6	0,1
Contactor principal (carga pequeña)	547.945	22.831	380	6,3
Contactor principal (carga máxima)	54.794	2.283	38	0,6
Dispositivo de parada de emergencia	274	11	0,2	0,003
Dispositivo de mando (pulsador)	2.739	114	1,9	0,032

$MTTF_d$ > 100 años

Figura 22: Valores $MTTF_d$ convertidos para componentes neumáticos y electromecánicos dependiendo del modo de demanda (t_{ciclo})

Existe una excepción para los componentes mecánicos e hidráulicos que se desvían del bucle de cálculo. En este caso, los creadores de la norma han determinado unos valores $MTTF_d$ de 150 años independientemente del modo de demanda sobre la base de pruebas empíricas 1.

La Figura 22 muestra un ejemplo de conversión de valores B_{10d} a valores $MTTF_d$ en varios modos de demanda (1 x por 24 horas, 1 x por hora, etc.) (se asume un funcionamiento las 24 horas, los 365 días del año).

Valores T_{10d}
ATENCIÓN: El denominado valor T_{10d} que se deriva de la consideración del valor B_{10d}, también está incluido en la norma prEN ISO 13849-1, y corresponde al 10% del valor $MTTF_d$ calculado. De ahí viene la recomendación de que los dispositivos relativos a la seguridad se sustituyan cuando alcancen el valor T_{10d} como medida de precaución.

Buenas prácticas de ingeniería
Al calcular los valores $MTTF_d$, la norma prEN ISO 13849-1 prefiere el uso de las especificaciones del fabricante, y sólo como alternativa recurrir a los métodos simplificados mencionados, es decir, el uso de tablas que permitan obtener los valores $MTTF_d$ que falten, cuando sea necesario.

Sin embargo, al mismo tiempo se estipulan ciertas condiciones generales, especialmente en cuanto al uso de tablas que, como se indica en la Figura 24, también deben tenerse en cuenta.

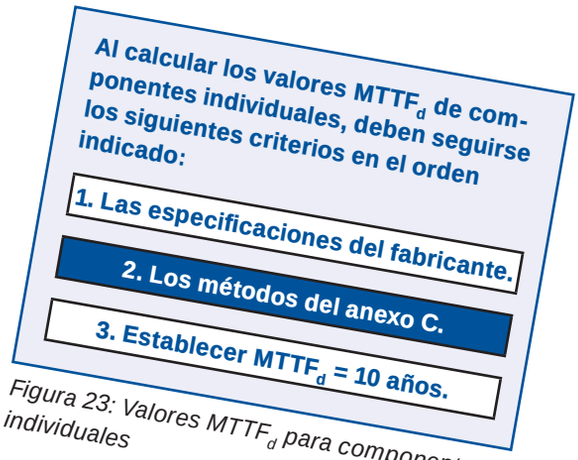


Figura 23: Valores $MTTF_d$ para componentes individuales

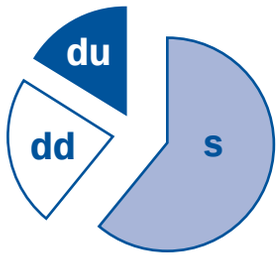
- **Tener en cuenta para el diseño los principios de seguridad básicos y probados (EN ISO 13849-2).**
- **Tener en cuenta las especificaciones del fabricante sobre aplicaciones adecuadas y condiciones de funcionamiento permitidas.**
- **Tener en cuenta los principios de seguridad básicos y probados en la instalación y operación de componentes.**

➥ **Teniendo en cuenta estas condiciones, se aplican los modos de fallo estipulados en la norma.**

➥ **El fabricante, instalador y operador están obligados a cumplir las condiciones.**

Figura 24: Buenas prácticas de ingeniería

1) Informe BIA 6/04, Análisis de los procesos de envejecimiento de las válvulas hidráulicas, www.hvbg.de/bgia. Código web: 1006447



$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Modo de fallo en fallos peligrosos detectados
Modo de fallo en todos los fallos peligrosos

Figura 25: Cobertura de diagnóstico DC

Cobertura de diagnóstico

Antecedentes
Si bien los requisitos de la norma prEN ISO 13849-1 en cuanto a los cálculos del $MTTF_d$ resultan, a pesar de todo, relativamente fáciles de comprender (una vez superado el obstáculo mental de la consideración probabilista, y completada la búsqueda meticulosa de los valores), la denominada cobertura de diagnóstico (DC) requiere un esfuerzo superior.

Este valor indica la proporción entre los fallos peligrosos detectados y la activación del modo de fallo en todos los fallos peligrosos, así como la cuantificación de la eficacia de las medidas para descubrir fallos en una SRP/CS.

Se asume que (a) pueden ocurrir fallos (véase $MTTF_d$) y (b) que los mecanismos para su detección (y la prevención de otros posteriores) no son todos igual de efectivos, por lo que existe una proporción de fallos no detectados.

Se trata de algo obvio, sobre todo porque no todos los fallos de una SRP/CS pueden detectarse inmediatamente, sino que en ocasiones no se hacen evidentes hasta la siguiente demanda de la función de seguridad. Por ejemplo, al abrir un resguardo móvil podemos darnos cuenta de que existe un cruce en un contacto de seguridad electromecánico o un contacto soldado.

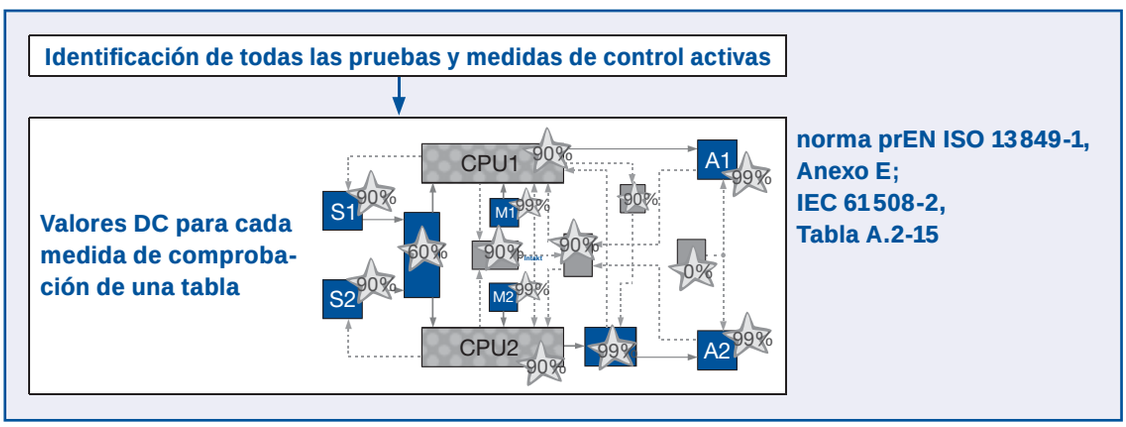


Figura 26: Determinación de la DC media para la totalidad del sistema, parte 1

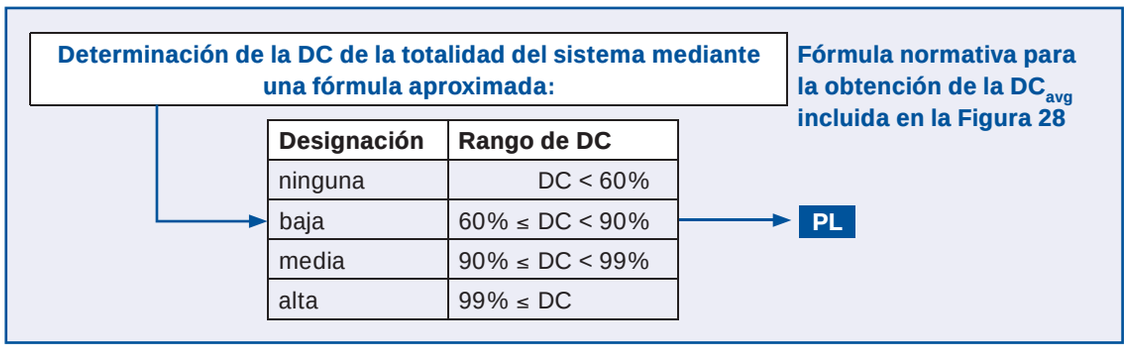


Figura 27: Determinación de la DC media para la totalidad del sistema, parte 2

La cuestión del reconocimiento de fallos es de especial importancia desde el punto de vista de la seguridad, sobre todo para evitar la denominada acumulación de defectos acumulados, es decir, una situación en que a un defecto no detectado en una SRP/CS se le añade otro (el denominado segundo defecto) que puede dejar inservible la función de seguridad.

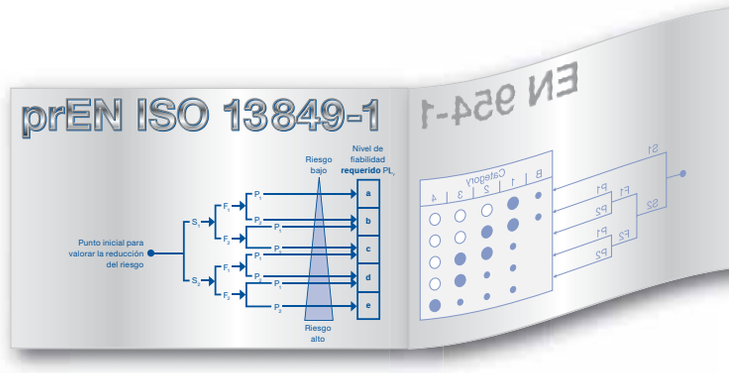
A partir de análisis empíricos vemos que un sistema redundante simple con detección de defectos tiene una mejor seguridad que un sistema redundante múltiple sin detección de defectos, lo que ilustra claramente la gran importancia de la calidad de esta detección, que mejora no sólo la seguridad sino la rentabilidad.

Ejecución
Para simplificarlo, la norma prEN ISO 13849-1 divide la calidad de la detección de defectos (la denominada cobertura de diagnóstico) en pasos (véase la Figura 27).

En el anexo E, la norma prEN ISO 13849-1 ofrece una simplificación aún mayor (véase la página 25).

	Medida	DC
Relé/ contactor	Prueba de plausibilidad, por ejemplo aplicación de contactos NA y NC de accionamiento positivo	99%
Accionador	Control de salidas a través de 2 canales sin pruebas dinámicas	0–99% dependiendo de los cambios de señal en la aplicación
Sensor	Control de ciertas propiedades (tiempo de reacción, ámbito de señales analógicas, por ejemplo resistencias eléctricas, capacidad)	60%
Proceso lógico	Software de autocomprobación	60–90%

Figura 29. Ejemplos de cobertura



- **En el PL sólo se incluye un valor medio DC_{avg}, que debe ponderarse en todas las pruebas**
- **El factor de ponderación es el $MTTF_d$ de las partes *comprobadas*:**

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

- **Las partes no comprobadas se introducen como DC = 0. Todas las partes que no pueden demostrar una exclusión de defecto entran en la suma (exclusión de defecto => $MTTF_d = \infty$).**

Figura 28: Cobertura de diagnóstico media, DC_{avg}

Aplicación
Se calcula el valor medio DC_{avg}, que refleja la calidad de la detección de defectos de todas las partes de cada canal.

Los valores $MTTF_d$ de los componentes y dispositivos relativos a la seguridad que forman un canal de SRP/CS influyen sobre el resultado, ya que una combinación de un “mal” $MTTF_d$ y una “mala” DC individual hacen bajar el valor DC_{avg}, y viceversa.

Este enfoque inductivo para el cálculo del valor DC_{avg} de detección de defectos tiene su justificación, pero no ayuda precisamente a simplificar las cosas, aunque el anexo E de la norma prEN ISO 13849-1 contenga una tabla de referencia exhaustiva.

El anexo E presenta una multitud de medidas comprobadas para la detección de defectos con los correspondientes valores DC expresados en porcentajes, pero en algunos casos la evaluación de una medida de la tabla se indica como “0 ... 99%, dependiendo de ...”, lo que deja un enorme margen de maniobra, algo que la norma prEN ISO 13849-1 pretende evitar y que requiere un análisis más profundo, como el realizado en la norma IEC EN 61508.

Gestión de fallos por causa común (CCF)

Antecedentes
Además de las arquitecturas designadas, el cálculo del $MTTF_d$ y el análisis de la DC, el nivel de fiabilidad de una SRP/CS viene dado por un cuarto parámetro, el denominado gestión de fallos por causa común (CCF).

El parámetro se aplica sólo en estructuras de 2 canales a partir de la categoría 2, puesto que está destinado a prevenir fallos en una SRP/CS con una causa y un efecto comun.

Estos fallos pueden producir la activación de un modo de fallo crítico en ambos canales al mismo tiempo, por ejemplo como consecuencia de un relámpago (sobretensión), afectando las salidas de semiconductores redundantes y produciendo como resultado la incapacidad de ambos canales de abrirse o cerrarse.

Las medidas de protección frente a CCF son necesarias en estructuras de múltiples canales (cat. 2, 3, 4) que, según el anexo D de la norma IEC 61508-6 correspondan a un factor β de 2% o menos.

Figura 30: Fallos por causas comunes (CFF)

Ejecución
En la norma prEN ISO 13849-1, la forma más fácil de analizar los métodos de prevención de los fallos CCF es la aplicación de una tabla en que aparece cada método evaluado según un sistema de puntos.

Dada la motivación de los análisis de CCF, las medidas como una clara separación de las vías de señal o el uso de criterios de compatibilidad electromagnética (EMC) más rigurosos, ganan muchos puntos (al igual que las medidas de protección ante sobretensiones o sobrepresiones, así como medidas de filtrado en la tecnología fluídica).

La norma prEN ISO 13849-1 establece en este sentido una puntuación máxima de 100 puntos y una mínima de 65.

Se trata de un valor equivalente al 2% del denominado factor β, al que se refiere la norma IEC EN 61508

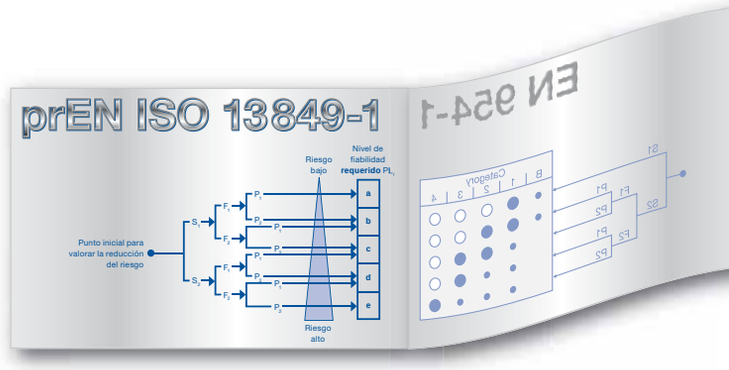
CCF: Fallos de varias partes por causas comunes

Lista de medidas con sistema de puntuación (valor máximo: 100 puntos)

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

Objetivo: 65 puntos como mínimo

Figura 31: Medidas de prevención de fallos por causa común (CCF)



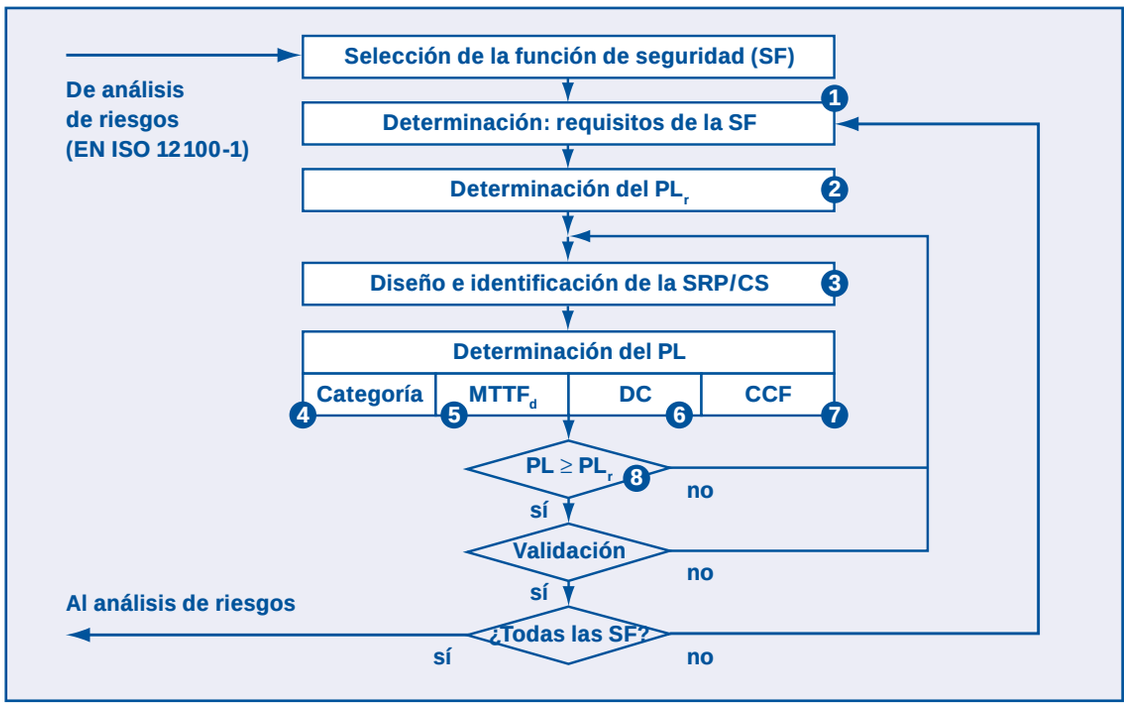


Figura 32: Proceso iterativo de diseño y desarrollo según la norma prEN 13849-1

Ejemplo

En primer lugar, el proceso iterativo de diseño y desarrollo de la norma prEN 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

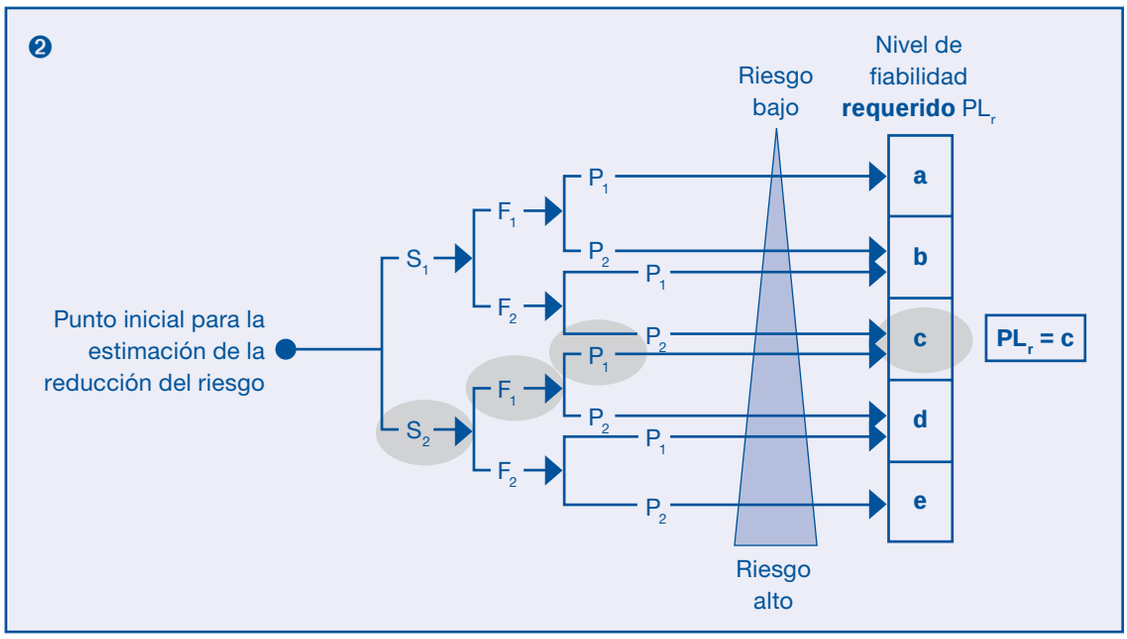


Figura 34: Determinación del PL_r

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

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

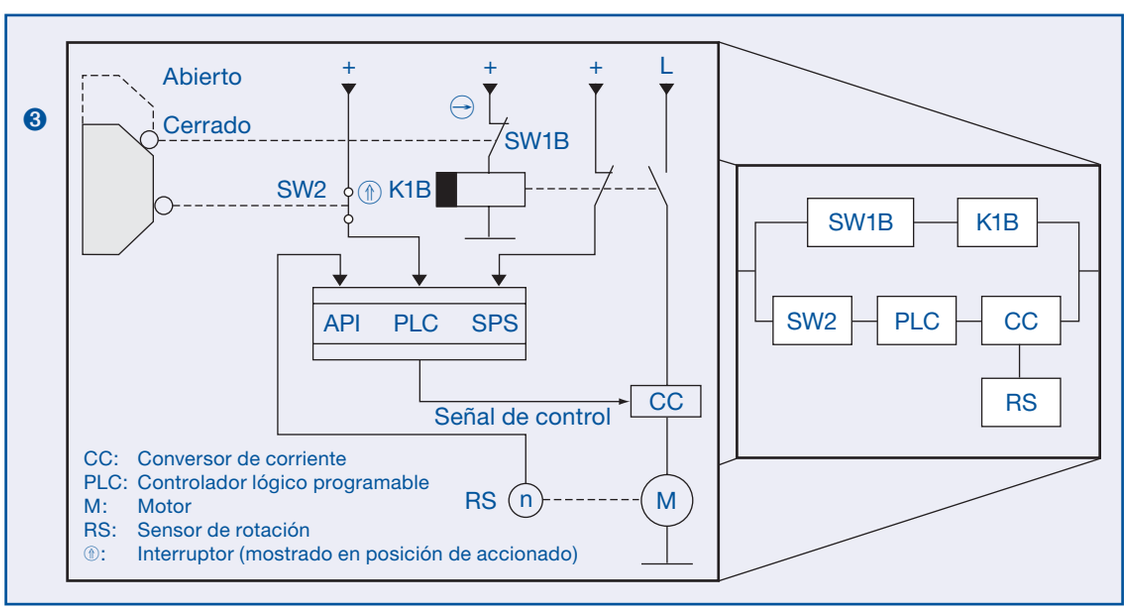
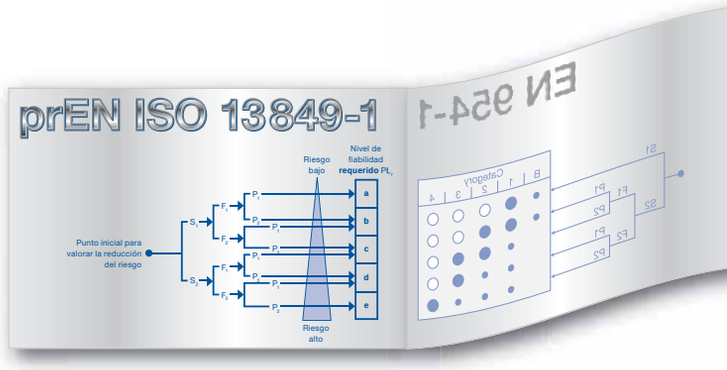


Figura 35: Diseño e identificación de una SRP/CS



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 prEN 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.

❽

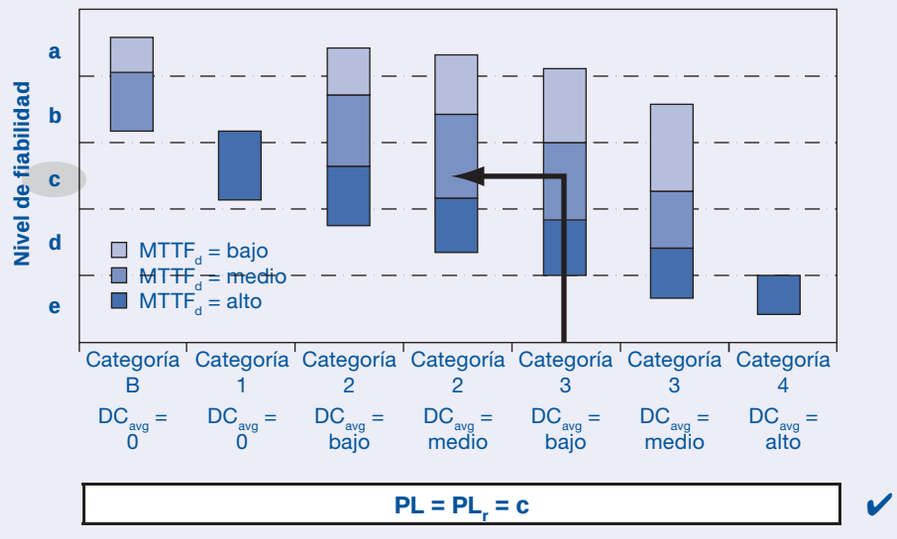
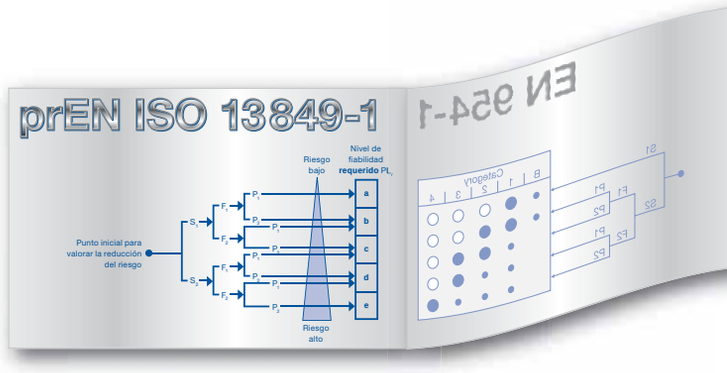
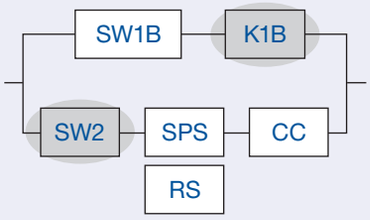


Figura 41: Determinación de si se ha conseguido que PL ≥ PL_r



¿Se ha fijado en un detalle?

Diagrama de bloques de seguridad:



$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3.600 \frac{s}{h}}{t_{cycle}}$$

n_{op} = media de ciclos de funcionamiento por año

Figura 42: Los componentes electromecánicos sí tienen un valor B_{10d}

El valor B_{10d} requeriría un nuevo cálculo del $MTTF_d$ para el K_{1B} y el SW2, como se indica a continuación, asumiendo que el resguardo funciona 240 días por año a razón de 16 horas diarias, con un modo de demanda medio de 20 s:

Presupuesto: 240 días / 16 horas / acceso cada 20 s

$$n_{op} = \frac{240 \cdot 16 \cdot 3.600}{20} = 691.200 \ \frac{\text{ciclos de conmutación}}{\text{año}}$$

$$MTTF_d = \frac{20.000.000}{0{,}1 \cdot 691.200} = 289 \text{ años}$$

El tiempo de funcionamiento máximo, según la norma, es el siguiente:
$T_{10d} = B_{10d}/n_{op} = 28{,}9$ años

Figura 43: Cálculo del $MTTF_d$ para el K_{1B} y el SW2

En este ejemplo, el presupuesto F1 del gráfico de riesgo ya no sería aplicable (véase la referencia anterior a la frecuencia de la exposición a los peligros y/o duración de la exposición). Debería asumirse el F2, y con él el nivel de fiabilidad requerido “d”. Sin embargo, gracias a la corrección del valor $MTTF_d$, que pasa a ser “bueno”, ello no supone un problema.

Comentario

El bucle de corrección necesario en el ejemplo anterior sugiere que el establecimiento de normas es también un proceso iterativo, ya que el ejemplo se deriva de la norma, pero fue creado cuando no se había incorporado la consideración del valor B_{10d}. Sin embargo, la consideración de este valor es una parte fundamental de la norma de cara a los usuarios. Sin ella, la prEN ISO 13849-1 tendría problemas para justificar la aplicación práctica de sus requisitos específicos.

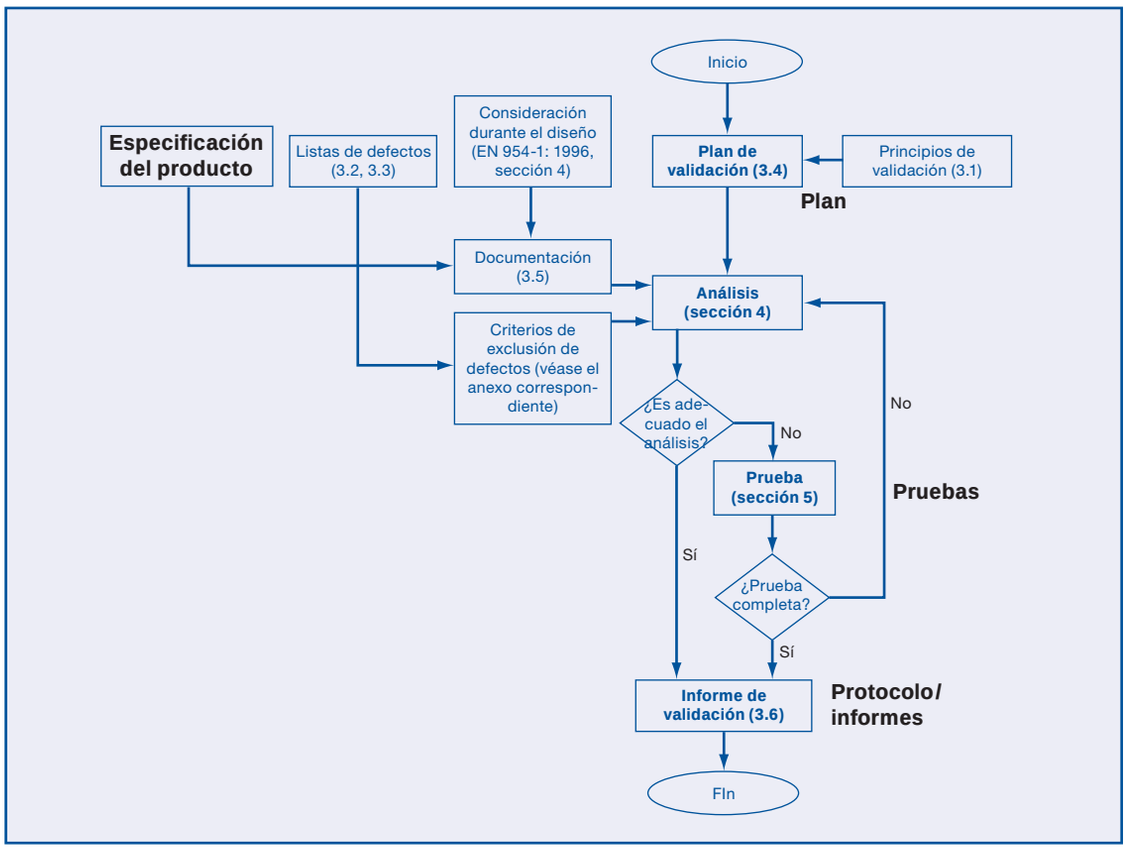


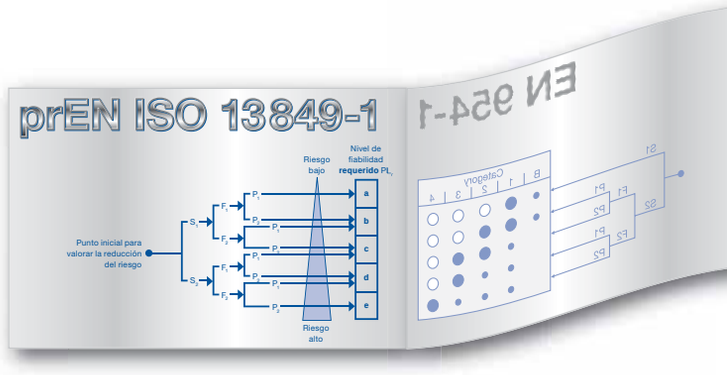
Figura 44: Plan de validación según la norma prEN ISO 13849-2

Validación[1]

El siguiente paso es la validación según la norma prEN ISO 13849-2, que no examinaremos en detalle aquí, puesto que las consideraciones que deben seguirse ya son observadas en la actualidad.

La norma prEN ISO 13849-2 contiene material originalmente previsto para la EN 954-2, que, una vez aprobado, pasó directamente al nivel ISO. Sin embargo, se espera que tarde o temprano se someta a una revisión para adaptar las versiones de 1988/1999 y las referencias a la EN 954-1 a la situación actual, es decir, a la norma prEN ISO 13849-1.

1) No examinaremos en detalle las medidas de prevención de fallos sistemáticos porque ya forman parte de los requisitos globales de las SRP/CS. En el anexo G de la norma prEN ISO 13849-1 puede encontrarse una descripción detallada de las mismas.



De todos modos, teniendo en cuenta que la mayoría de los accidentes de máquinas no pueden achacarse a fallos coincidentes, sino a errores en las especificaciones y a posteriores ajustes y modificaciones, el tema de la validación es de suma importancia en la seguridad de la maquinas.

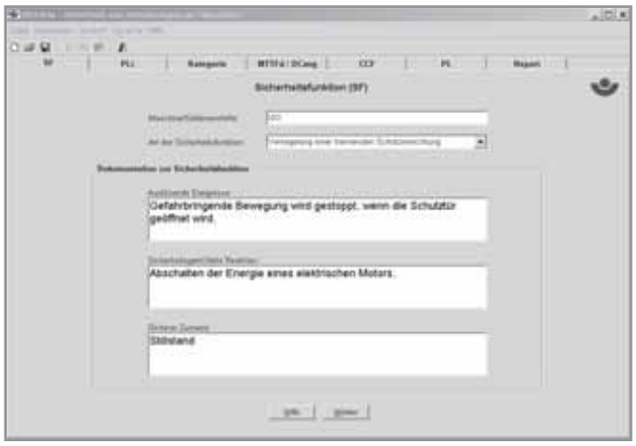
Los anexos informativos de la norma prEN ISO 13849-2 tienen un papel fundamental en relación con la prEN ISO 13849-1. Se dividen en los sectores de la mecánica (A), neumática (B), hidráulica (C) y eléctrica (D), y contienen las siguientes listas:

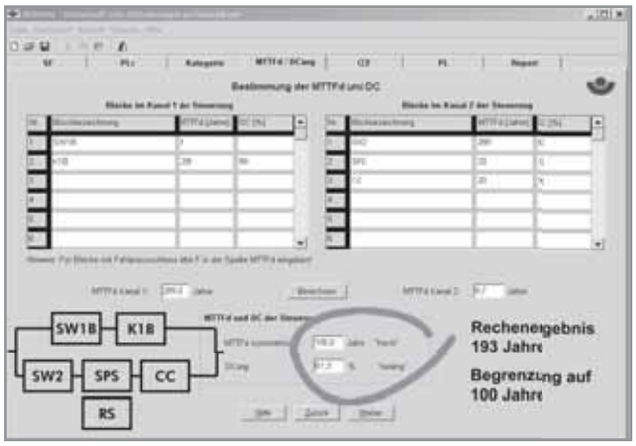
- Principios de seguridad fundamentales (importantes para la categoría de control B y el PL “a” de la EN 954-1).
- Principios de seguridad probados (importantes para la categoría de control 1 y siguientes y los PL del “b” al “e”).
- Componentes relativos a la seguridad probados (importantes para la categoría de control 1 y el PL “b” de la EN 954-1).
- Listas de defectos aplicables y exclusiones permisibles (importantes para las categorías de control 2, 3 y 4 y los PL del “c” al “e” de la EN 954-1).

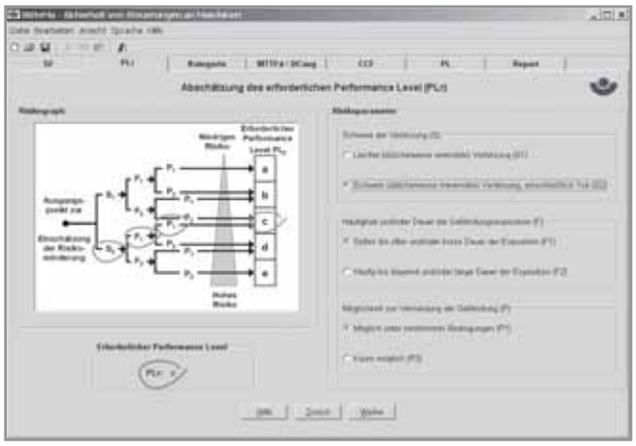
SiSteMa

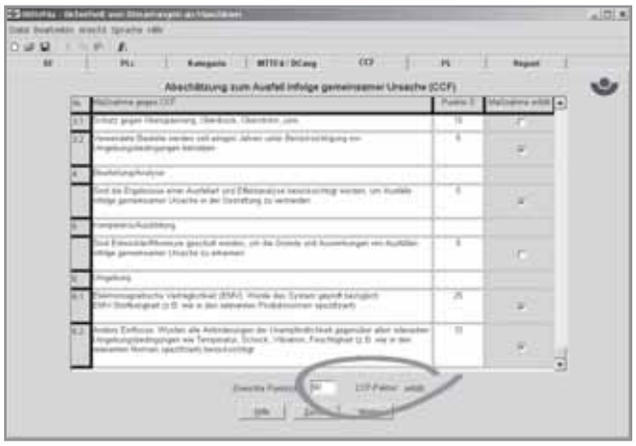
Llegados a este punto se plantea una pregunta obvia: ¿No podrían simplificarse enormemente estos procedimientos con el uso de software? La respuesta es que, sin duda, sólo es cuestión de tiempo.

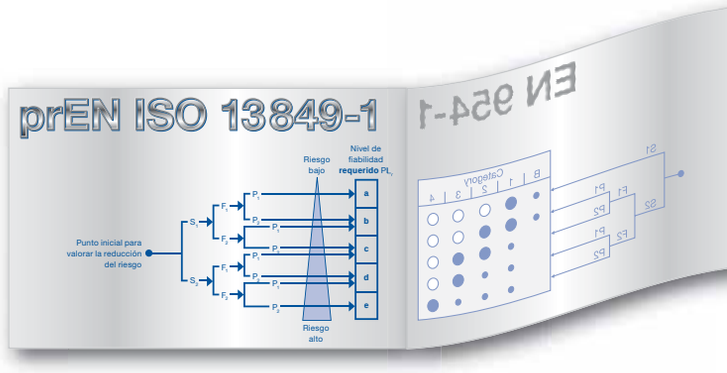
El BGIA, por ejemplo, trabaja en una aplicación llamada SiSteMa (para la seguridad de mandos de máquinas) que estará disponible como software gratuito próximamente.

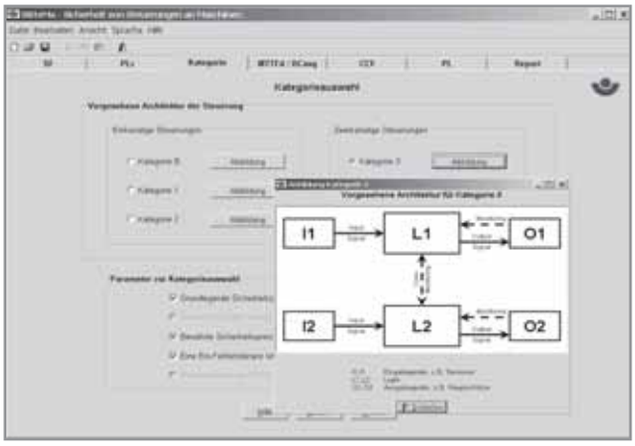


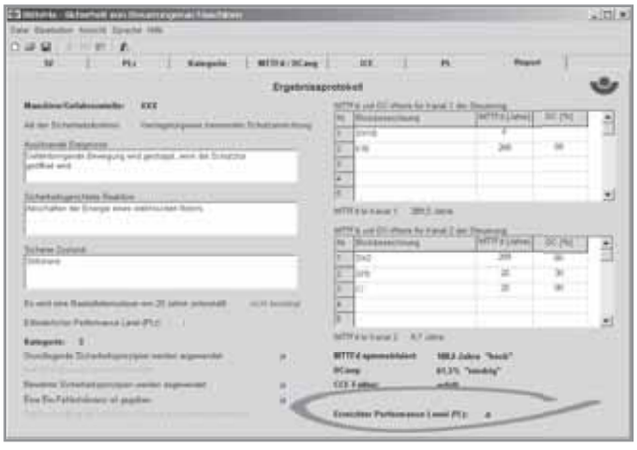












Referencia del PLC:
www.hvbg.de/d/bia/pra/drehscheibe.html

Aunque SiSteMa aún no está disponible (se prevé que lo esté a principios de 2007), la entidad de seguros profesionales alemana BGIA ya ofrece asistencia relativa a la norma prEN ISO 13849-1, en forma de un disco denominado PLC que simplifica la determinación del nivel de PL, y que se ha desarrollado con el apoyo de la Zentralverband Elektrotechkik und Elektroindustrie (ZVEI) – Fachverband Automation (la asociación alemana de electrotecnología, industria eléctrica y profesionales de la automoción), así como la Verband Deutscher Maschinen- und Anlagenbau VDMA (la asociación alemana de ingeniería mecánica y fabricantes de bienes de equipo).

Los métodos de la norma prEN ISO 13849-1 quedan expresados de una forma comprensible mediante dos discos que giran el uno contra el otro. El nivel de fiabilidad se determina simplemente girando un disco hasta que aparece en la ventana inferior el nivel $MTTF_d$ (tiempo medio hasta fallo peligroso) deseado.

A continuación, sólo hay que seleccionar la categoría y la cobertura de diagnóstico (DC) deseadas en la ventana superior, y leer el valor que aparece en la ventana contigua. El tiempo medio hasta fallo peligroso del sistema de mando de seguridad se obtiene multiplicando este valor por un factor que aparece en la leyenda (orden de magnitud). El código de color facilita la selección del factor y a su vez indica qué PL se ha alcanzado.

La norma prEN ISO 13849-1 en SRP/CS simples

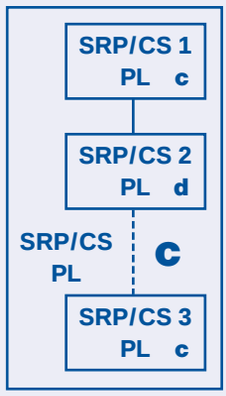
Antecedentes
Una vez conozcamos los niveles de fiabilidad de los dispositivos relativos a la seguridad, podemos discernir en la complejidad manejable con que la norma prEN ISO 13849-1 trata a las SRP/CS, a partir de su concepto singular de simplificación.

Al mismo tiempo, este concepto contempla que la conexión de múltiples componentes y dispositivos de seguridad pueden afectar al PL global de un sistema de mando completo (formado por varias SRP/CS conectadas en serie), que puede ser inferior al de los componentes individuales que integran la cadena. Esta filosofía nos lleva a una conclusión evidente: en este caso, las diferentes probabilidades residuales de fallo se suman, por lo que el PL global puede perfectamente verse reducido en un grado.

Diseño
Esta filosofía a favor de la simplificación vuelve a hacerse evidente en la tabla de la figura 45 (conocida también como tabla de combinación), que presenta a la izquierda el número de PL individuales de un sistema de mando. Los PL más bajos se suman y se presenta a la derecha el PL global.

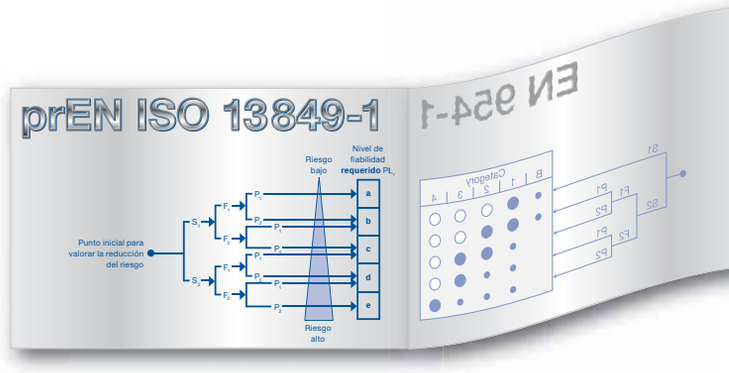
Por lo general (al tratar con estructuras más simples), más de tres PL individuales idénticos, o más de cuatro, en estructuras de 2 canales, hacen descender en un grado el PL global. Es decir, 3 x 1 PL “c” producen un PL global “b”, y 4 x 1 PL “e” producen un PL global “d”.

El ejemplo siguiente (véase la Figura 45) indica que los dos PL individuales más bajos se suman (2 x PL “c”), mientras que el PL más alto, “d”, no se incluye en el cálculo (el PL “d” se considera un orden de magnitud mejor que el PL “c” para establecer el valor PFH). Por tanto, 2 x PL “c” representan un PL “c”. Sin embargo, un PL “c” en lugar del PL “d”, sólo se llegaría a un PL global “b”.



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

Figura 45: Combinación lineal de múltiples SRP/CS



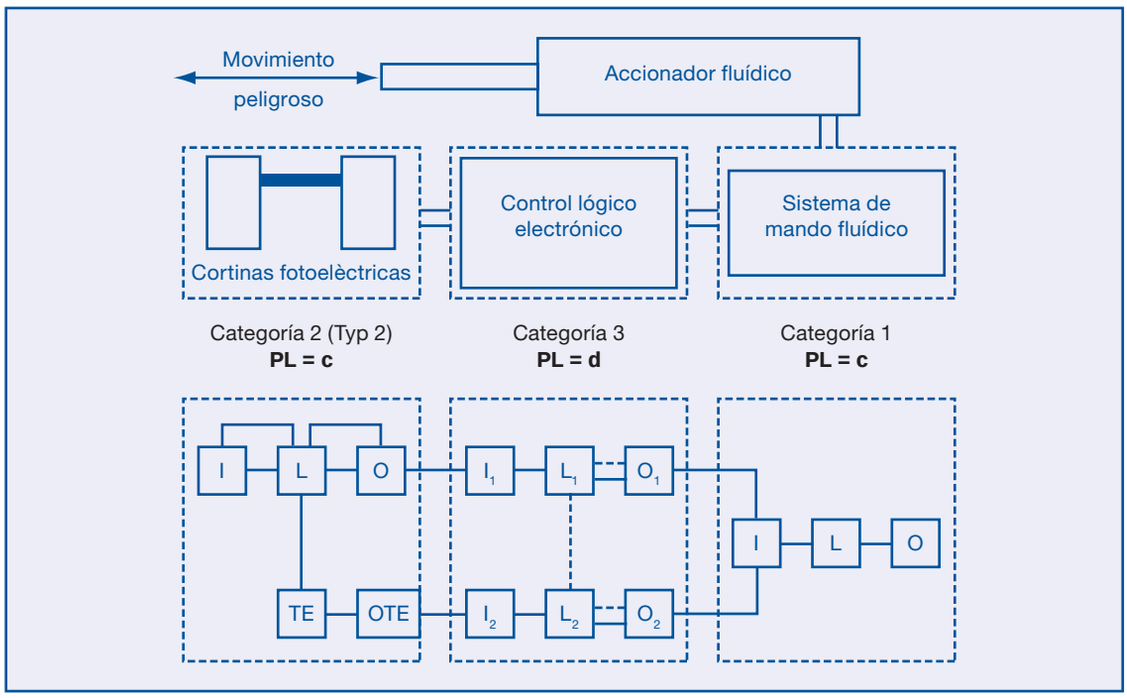


Figura 46: Combinación de SRP/CS (ejemplo)

Aplicación

La aplicación de la tabla superior tiene sin duda su atractivo, ya que su examen, derivado del análisis de riesgos precedente para determinar la función de seguridad adecuada, produce el PL_r deseado. Además, hay que tener en cuenta que pueden incluirse exclusiones de defectos en la evaluación, aunque no se computen aquí.

Sin embargo, si se obtiene un PL global que no coincide con el PL_r, es necesario un análisis más detallado. La no consecución del valor deseado no es definitiva, sino que se debe principalmente a la generalización del análisis.

En este caso, la norma prEN ISO 13849-1 también ofrece ayuda (véase el apartado siguiente sobre conexión en serie).

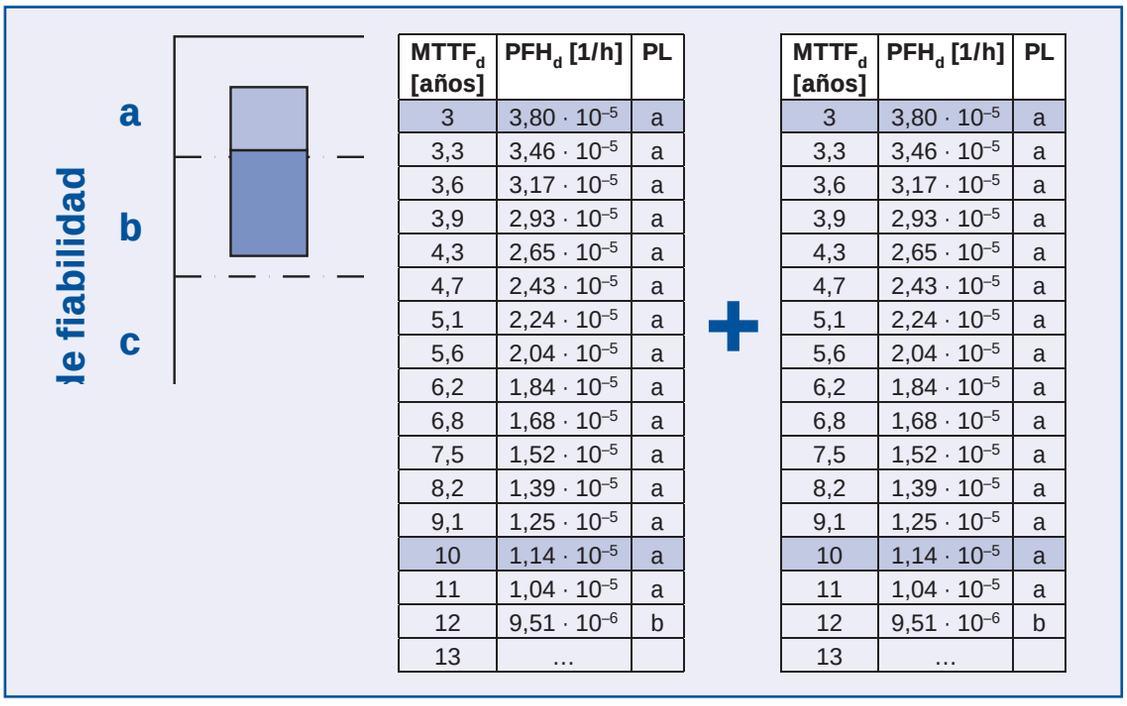
La norma prEN ISO 13849-1 en conexiones en serie

Antecedentes
En la filosofía de la norma prEN ISO 13849-1, una conexión en serie debe considerarse como la suma de las probabilidades residuales de fallo.

En la actualidad, la norma EN 954-1 ya contempla esta situación, lo que se ve reflejado por ejemplo en la documentación de las entidades aseguradoras de riesgos laborales y también en la nuestra: la conexión en serie de dispositivos de conmutación de seguridad electromecánicos, cada uno de ellos de la categoría 4, recibe una clasificación global sólo de la categoría 3. Pero no todos los fabricantes informan de ello, y también existen muchas interpretaciones erróneas por parte de los clientes.

Diseño
La tabla de la figura 47 puede servir para comprender mejor la calificación de la seguridad de una conexión en serie compleja según la norma prEN ISO 13849-1 (en el apartado “suma de las probabilidades residuales de fallo”).

La tabla del anexo K de la norma prEN ISO 13849-1 es una representación detallada del diagrama de bloques central (véase la Figura 8) para determinar los PL alcanzados. Es posible determinar con mayor exactitud el PFH_d si se conoce un $MTTF_d$ por canal más preciso. Los valores de las SRP/CS individuales deben sumarse, comparándose el resultado con el PFH global máximo permitido para ese PL concreto (véase la Figura 4). La regla es que, a mejor valor de PFH_d, menor es el riesgo de colapso.

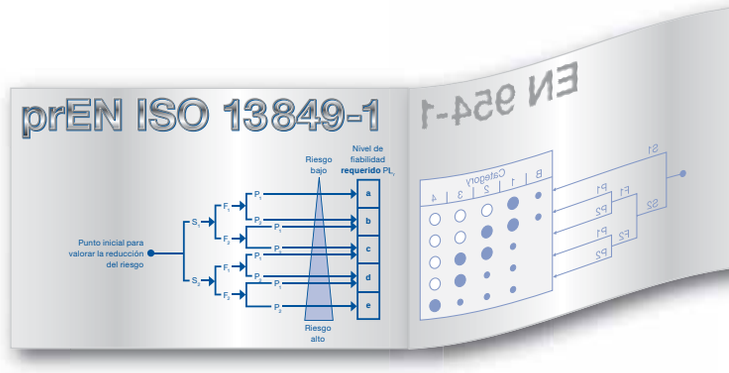


$MTTF_d$ [años]	PFH_d [1/h]	PL
3	$3{,}80 \cdot 10^{-5}$	a
3,3	$3{,}46 \cdot 10^{-5}$	a
3,6	$3{,}17 \cdot 10^{-5}$	a
3,9	$2{,}93 \cdot 10^{-5}$	a
4,3	$2{,}65 \cdot 10^{-5}$	a
4,7	$2{,}43 \cdot 10^{-5}$	a
5,1	$2{,}24 \cdot 10^{-5}$	a
5,6	$2{,}04 \cdot 10^{-5}$	a
6,2	$1{,}84 \cdot 10^{-5}$	a
6,8	$1{,}68 \cdot 10^{-5}$	a
7,5	$1{,}52 \cdot 10^{-5}$	a
8,2	$1{,}39 \cdot 10^{-5}$	a
9,1	$1{,}25 \cdot 10^{-5}$	a
10	$1{,}14 \cdot 10^{-5}$	a
11	$1{,}04 \cdot 10^{-5}$	a
12	$9{,}51 \cdot 10^{-6}$	b
13	...	

+

$MTTF_d$ [años]	PFH_d [1/h]	PL
3	$3{,}80 \cdot 10^{-5}$	a
3,3	$3{,}46 \cdot 10^{-5}$	a
3,6	$3{,}17 \cdot 10^{-5}$	a
3,9	$2{,}93 \cdot 10^{-5}$	a
4,3	$2{,}65 \cdot 10^{-5}$	a
4,7	$2{,}43 \cdot 10^{-5}$	a
5,1	$2{,}24 \cdot 10^{-5}$	a
5,6	$2{,}04 \cdot 10^{-5}$	a
6,2	$1{,}84 \cdot 10^{-5}$	a
6,8	$1{,}68 \cdot 10^{-5}$	a
7,5	$1{,}52 \cdot 10^{-5}$	a
8,2	$1{,}39 \cdot 10^{-5}$	a
9,1	$1{,}25 \cdot 10^{-5}$	a
10	$1{,}14 \cdot 10^{-5}$	a
11	$1{,}04 \cdot 10^{-5}$	a
12	$9{,}51 \cdot 10^{-6}$	b
13	...	

Figura 47: Suma alternativa del PFH_d con conexiones en serie complejas



Conexión en serie sin pérdida de categoría de control

- Existen componentes electrónicos instalados que controlan la función de conmutación (autocontrol)
- Detección de todos los fallos en la conexión en serie (hasta 31 dispositivos)
- Conexión en serie de interruptores (CSS 180 **y/o** AZM 200) **sin** pérdida de categoría de control

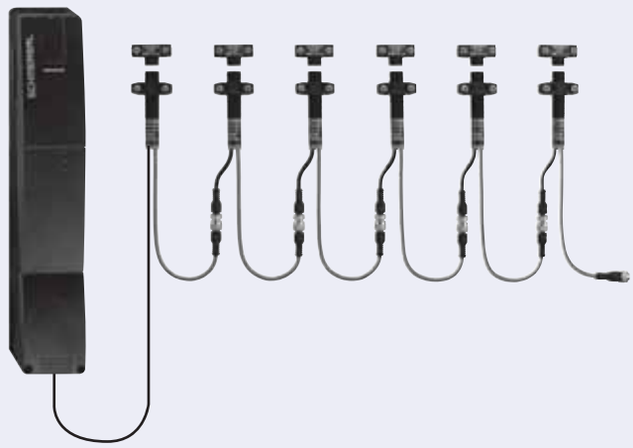


Figura 48: Dispositivos de enclavamiento sin contacto con y sin mecanismo de enganche

Conexiones en serie complejas...
¡con un PL “e”!
El problema de la reducción del PL de las SRP/CS en las conexiones en serie complejas es especialmente causado por los componentes de seguridad electromecánicos.

Las tecnologías de conmutación con funciones de seguridad basadas en microprocesador ofrecen nuevas posibilidades a este respecto, ya que permiten una comprobación dinámica del dispositivo, de modo que la categoría de control y el nivel de fiabilidad se mantienen incluso cuando se conectan varios componentes de seguridad en serie.

El catálogo de productos de Schmersal cuenta con los sensores de seguridad CSS 180, entre otros, así como los enclavamientos sin contacto de la serie AZM 200, que pueden combinarse y unirse a una conexión en serie.

Encontrará más información en www.schmersal.com

Sensores y enclavamientos electrónicos de seguridad

Los sensores y enclavamientos electrónicos de seguridad sirven para el control de resguardos móviles. Cuando el resguardo se abre, la máquina se detiene, de modo que se evita totalmente el movimiento peligroso. La ventaja principal de estos dispositivos es la detección sin contacto de la posición del resguardo, con lo que desparece el desgaste y la posibilidad de desajustes entre sensores y accionadores.

La norma prEN ISO 13849-1 y el software

Antecedentes
Mientras que la actual norma EN 954-1 no aborda la tecnología basada en microprocesador con función de seguridad (sistemas PES), y por tanto tampoco contempla el software, la norma prEN ISO 13849-1 sí la tiene en cuenta, y en gran detalle. De todos modos, sus requisitos no sustituyen totalmente a los de la norma IEC 61508 (por ejemplo, en aplicaciones con un PL "e"), este aspecto sólo interesa a los fabricantes de sistemas PES por lo que no lo trataremos aquí.

La filosofía básica de la norma prEN ISO 13849-1 se muestra en la Figura 49.

- Para todos los PL y SRESW + SRASW
- básicamente, medidas para **evitar fallos y favorecer una programación defensiva**
- tener en cuenta que se introducirán fallos durante la especificación y el diseño del software
- requisitos basados en el criterio de seguridad fundamental de la IEC 61508-3
- ... sin embargo, sin llegar a un elevado nivel científico
- principalmente sin relación con la IEC 61508
- comprensibles, prácticos y fáciles de seguir

Figura 49: Filosofía básica de los requisitos sobre SW de la norma prEN ISO 13849-1

Diseño
Los requisitos en cuanto a software de la norma se dividen en requisitos generales, requisitos referentes al software de seguridad integrado y requisitos referentes a las aplicaciones informáticas de seguridad, y existen asimismo divisiones según el lenguaje usado (LVL[1] o FVL[2]) y el PL (véanse figuras 50 y 51).

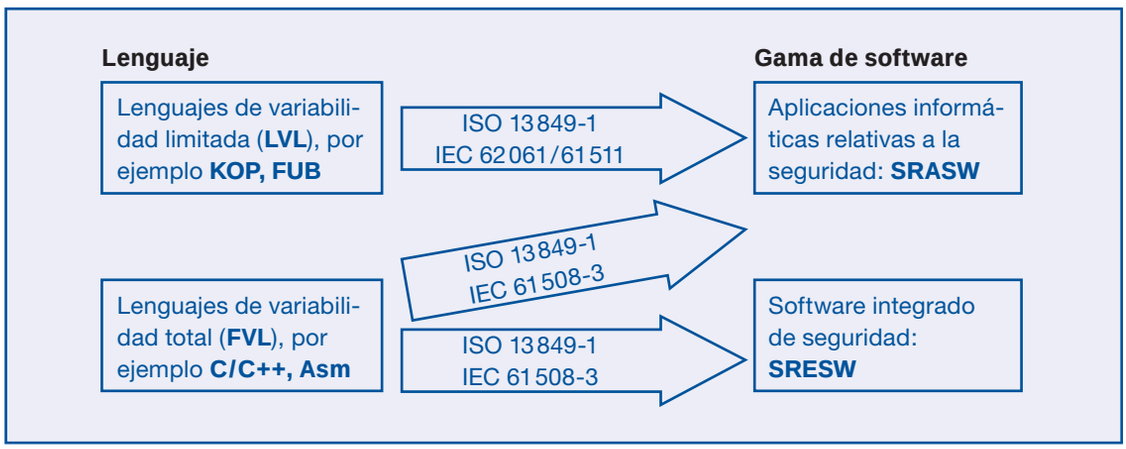
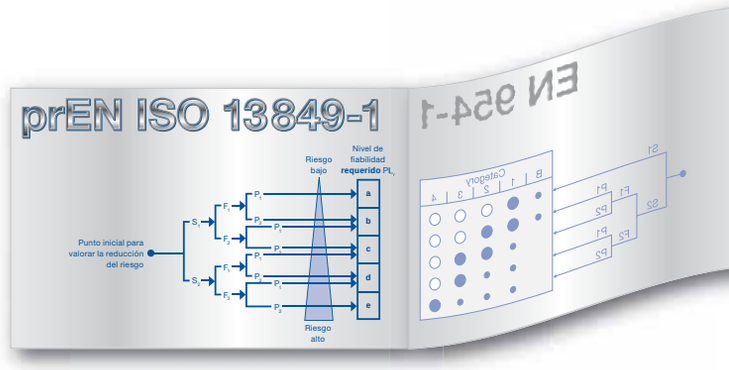


Figura 50: Diagrama del software de seguridad

1) LVL (lenguaje de variabilidad limitada) – lenguaje con una posibilidad de programación limitada, que permite implementar y combinar funciones preestablecidas y bibliotecas para cumplir los requisitos de seguridad.

2) FVL (lenguaje de variabilidad total) – lenguaje con una posibilidad de programación ilimitada, que permite implementar una amplia variedad de funciones y aplicaciones.



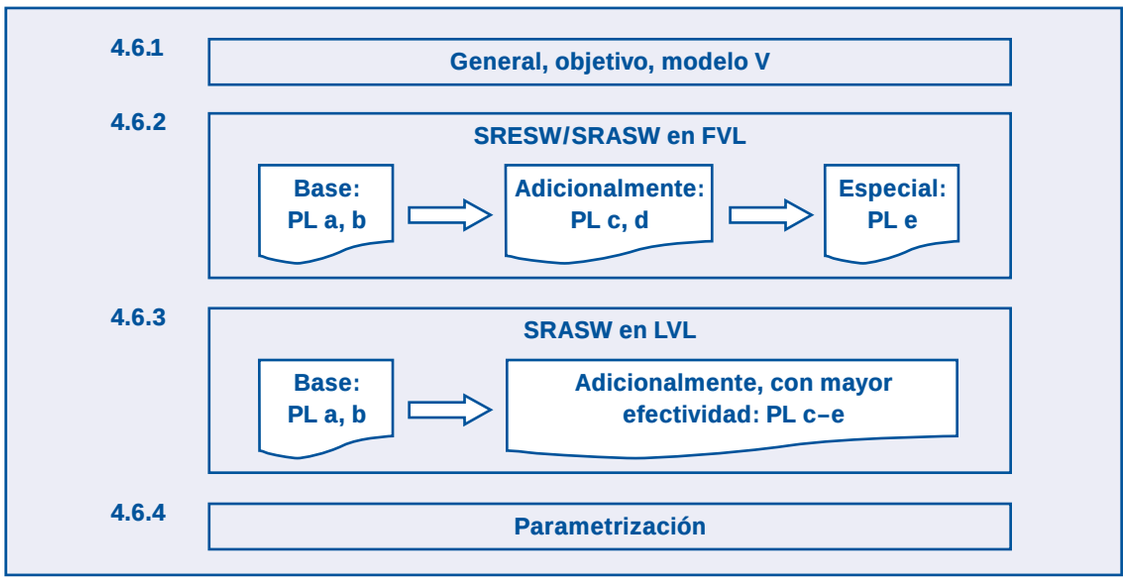


Figura 51: Estructura de los requisitos del SW de acuerdo con el apartado 4.6 de la norma prEN ISO 13849-1

Aplicación

No entraremos en detalle en el software de seguridad integrado, ya que sólo afecta a los usuarios de la norma prEN ISO 13849-1 en casos excepcionales. En cambio, cada vez es más habitual el uso de aplicaciones informáticas en las SRP/CS, ya sea para gestionar las propias unidades SRP/CS, sistemas de bus o controles de seguridad.

La norma prEN ISO 13849-1 recomienda que se adopte el denominado modelo V como base para las aplicaciones informáticas (y también para el software integrado), dada su fuerte implantación en el sector del software, aunque en este caso sea en una forma simplificada.

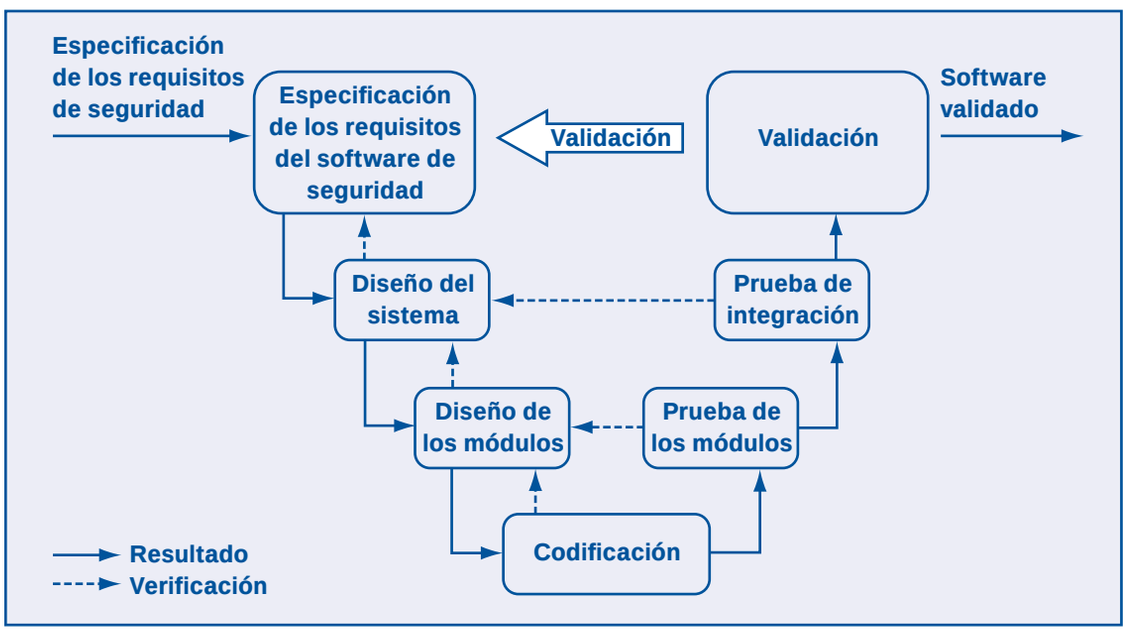
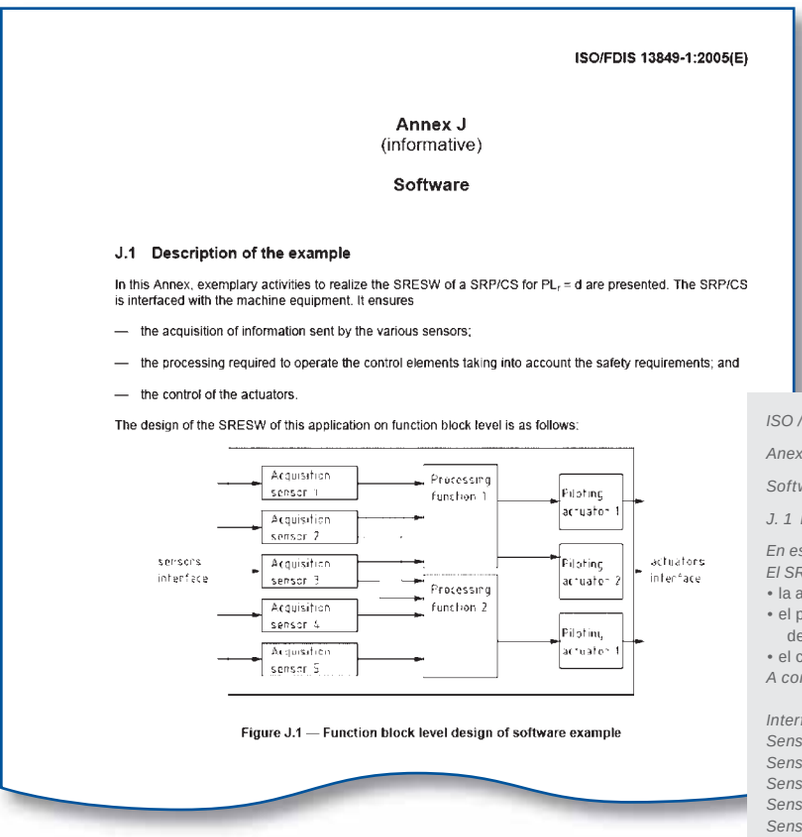


Figura 52: Modelo V simplificado para SRESW y SRASW en la norma prEN ISO 13849-1

Si, en cambio, el software consiste simplemente en una serie de parámetros, como en los escáneres láser de seguridad, por ejemplo, pueden emplearse simplificaciones aún mayores, ya que en principio el proveedor ya ha realizado los ajustes previos.

El anexo J de la norma prEN ISO 13849-1 contiene más requisitos referidos al software (véase la Figura 53).



ISO/FDIS 13849-1:2005(E)

Annex J
(informative)

Software

J.1 Description of the example

In this Annex, exemplary activities to realize the SRESW of a SRP/CS for PL_r = d are presented. The SRP/CS is interfaced with the machine equipment. It ensures

— the acquisition of information sent by the various sensors;

— the processing required to operate the control elements taking into account the safety requirements; and

— the control of the actuators.

The design of the SRESW of this application on function block level is as follows:

Figure J.1 — Function block level design of software example

Figura 53: Anexo J de la norma prEN ISO 13849-1

Requisitos del software de asignación de parámetros

Requisitos más importantes de la parametrización

- herramienta especial del fabricante
- protección ante accesos no autorizados (por ejemplo, contraseña)
- controles de plausibilidad de los parámetros
- integridad de los datos garantizada durante la parametrización
- transferencia de datos garantizada (con varias opciones de presentación)

Figura 54: Requisitos del software de asignación de parámetros

ISO / FDIS 13849-1: 2005(E)

Anexo J (Informativo)

Software

J. 1 Descripción del ejemplo

En este anexo se presentan ejemplos para que el SRESW de una SRP/CS alcance un PL_r = d. El SRP/CS se conecta mediante un interfaz a la SRP/CS. Permite:
- *la adquisición de información enviada por varios sensores;*
- *el proceso requerido para operar los elementos de control, teniendo en cuenta los requisitos de seguridad;*
- *el control de los accionadores*

A continuación se presenta el diagrama por bloques de función del SRESW de esta aplicación

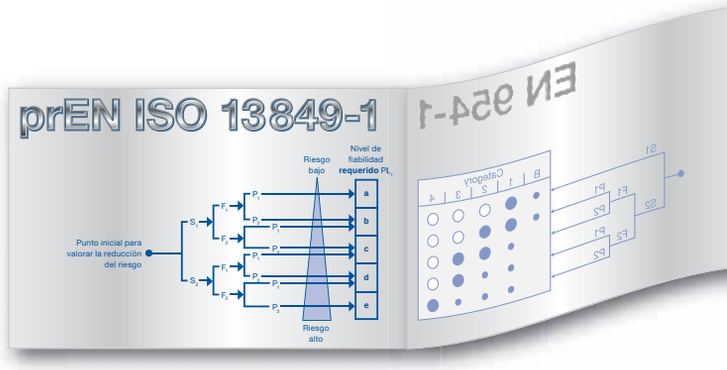
Interfaz de sensores
Sensor de adquisición 1
Sensor de adquisición 2
Sensor de adquisición 3
Sensor de adquisición 4
Sensor de adquisición 5

Función de proceso 1
Función de proceso 2

Accionador 1
Accionador 2
Accionador 3

interfaz de accionadores

Figura J.1 – Ejemplo de diagrama de bloques de funciones del software.



La norma prEN ISO 13849-1 en comparación con la EN 62061

Antecedentes

Como hemos indicado al principio, la norma IEC EN 62061 compite con la prEN ISO 13849-1 para suceder a la EN 954-1, aunque el término “competir” sea un poco exagerado en este contexto. De todos modos, ya no puede hablarse de “convivencia”, como se había apuntado anteriormente.

A diferencia de la IEC 61508, podemos suponer que tanto la IEC EN 62061 como la EN ISO 13849-1 se armonizarán bajo la directiva sobre máquinas CE, por lo que ambas tendrán la ventaja de ese supuesto impacto adicional

La IEC EN 62061 deriva de la IEC EN 61508 y es la versión específica del sector de la ingeniería mecánica. Además de ésta existe también la IEC EN 61511[1] para la industria de procesos (sectores químico y de ingeniería de procesos).

Originalmente, la IEC EN 61508 se creó exclusivamente para rellenar una vacío de la norma EN 954-1, concretamente la ausencia de requisitos específicos para las SRP/CS complejas, especialmente en relación con los sistemas electrónicos programables, es decir, sistemas basados en microprocesador con función de seguridad (PES). Sin embargo, el comité responsable de la IERC 61508 ha extendido su ámbito de aplicación a lo largo de su desarrollo para incorporar a los sistemas eléctricos y electrónicos (E/E/PES)

En consecuencia, la IEC EN 61508 se ha convertido en una norma fundamental y exhaustiva para casi todos los tipos de problemas relativos a la seguridad, y por tanto ha incrementado su complejidad (con más de 350 páginas divididas en 8 secciones) y ha generado normas específicas para ciertos sectores, entre otras la IEC 62061[2], destinada a la ingeniería mecánica.

En este apartado abordamos los requisitos típicos para este sector, dejando de lado los aplicables a otros ámbitos y diseños.

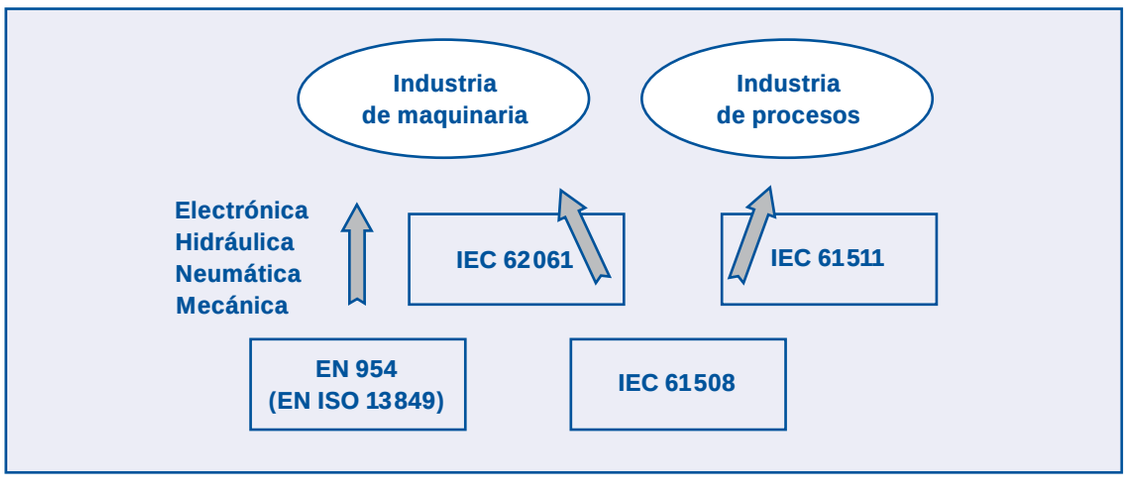


Figura 55: Situación de las normas en competencia

1) IEC EN 61511-1 (VDE 0810-1: 2005-05): seguridad funcional – sistemas de seguridad para la industria de procesos – parte 1: introducción, terminología, requisitos del sistema, software y hardware

2) IEC EN 62061-1 (VDE 0113-59): seguridad de máquinas – seguridad funcional de sistemas de mando de seguridad eléctricos, electrónicos y electrónicos programables

4 Niveles de seguridad de integridad y 2 modos de operación

Nivel de seguridad de integridad	Demanda menor Probabilidad media de un fallo peligroso PFD	Demanda superior o demanda continuada Probabilidad media de un fallo peligroso por hora PFH
4	≥ 10^{-5} to < 10^{-4} y	≥ 10^{-9} to < 10^{-8} y
3	≥ 10^{-4} to < 10^{-3} y	≥ 10^{-8} to < 10^{-7} y
2	≥ 10^{-3} to < 10^{-2} y	≥ 10^{-7} to < 10^{-6} y
1	≥ 10^{-2} to < 10^{-1} y	≥ 10^{-6} to < 10^{-5} y

¿Concierne al área de las máquinas?

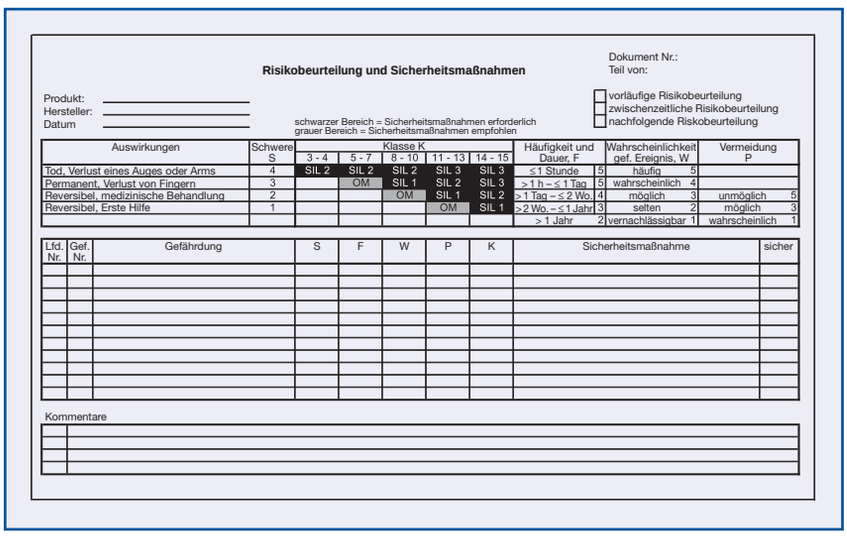
Figura 56: Niveles de seguridad: IEC 61508 (aplicación universal) y IEC 62061 (aplicaciones de ingeniería mecánica)

Respecto a la ingeniería mecánica, nos limitaremos a los requisitos de seguridad del denominado modo de demanda superior o de demanda continuada (expresado por el valor PFH) (no incluimos el modo de demanda menor, que representa una demanda de menos de una función de seguridad por año). Asimismo, excluimos el nivel de integridad de seguridad 4 (parámetro de riesgo: muerte de varias personas como mínimo, efectos catastróficos).

Aplicación

En este apartado no abordaremos en detalle la norma IEC EN 62061. De todos modos, hay voces críticas que afirman que la norma es más difícil de seguir que la prEN ISO 13849-1, sobre todo en lo relativo a cuestiones de seguridad más “claras” y que con más frecuencia afectan la construcción de máquinas y sistemas de mando. En cambio, para aspectos más complejos, la IEC 61508 resulta imprescindible. Otra diferencia es la incorporación de la mecánica, la neumática y la hidráulica en la prEN ISO 13849-1, que la IEC EN 62061 no cubre debido a su origen.

Figura 57: Ejemplo de solicitud para el proceso de determinación del SIL



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil von:

Produkt:
Hersteller:
Datum

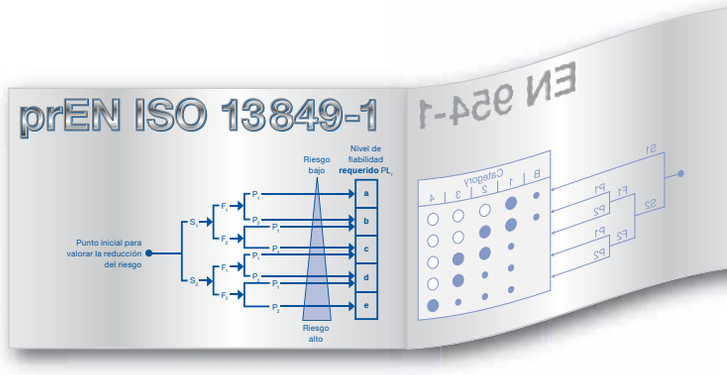
schwarzer Bereich = Sicherheitsmaßnahmen erforderlich
grauer Bereich = Sicherheitsmaßnahmen empfohlen

☐ vorläufige Risikobeurteilung
☐ zwischenzeitliche Risikobeurteilung
☐ nachfolgende Risikobeurteilung

Auswirkungen	Schwere S	Klasse K 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Häufigkeit und Dauer, F		Wahrscheinlichkeit gef. Ereignis, W		Vermeidung P	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 Stunde	5	häufig	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ 1 Tag	5	wahrscheinlich	4		
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3
							> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Lfd. Nr.	Gef. Nr.	Gefährdung	S	F	W	P	K	Sicherheitsmaßnahme	sicher

Kommentare



Compatibilidad prevista entre la prEN ISO 13849-1 y la IEC 62061 (IEC EN 61508)
A pesar de todo, los responsables de ambas normas se han esforzado para que sean compatibles entre sí, coordinando los requisitos de nivel de integridad de seguridad y nivel de fiabilidad. Así, por ejemplo, el SIL 1 corresponde a los PL “b” o “c”, etc. (véase la Figura 58).

Asimismo, ambas normas ofrecen recomendaciones parecidas en cuanto a qué norma hay que aplicar en cada caso. De todos modos, hay motivos para la crítica, ya que los creadores de la norma prEN ISO 13849-1 se han desviado de este compromiso al introducir modificaciones posteriores, si bien siguen incluyendo la tabla de aplicación (véase la Figura 59).

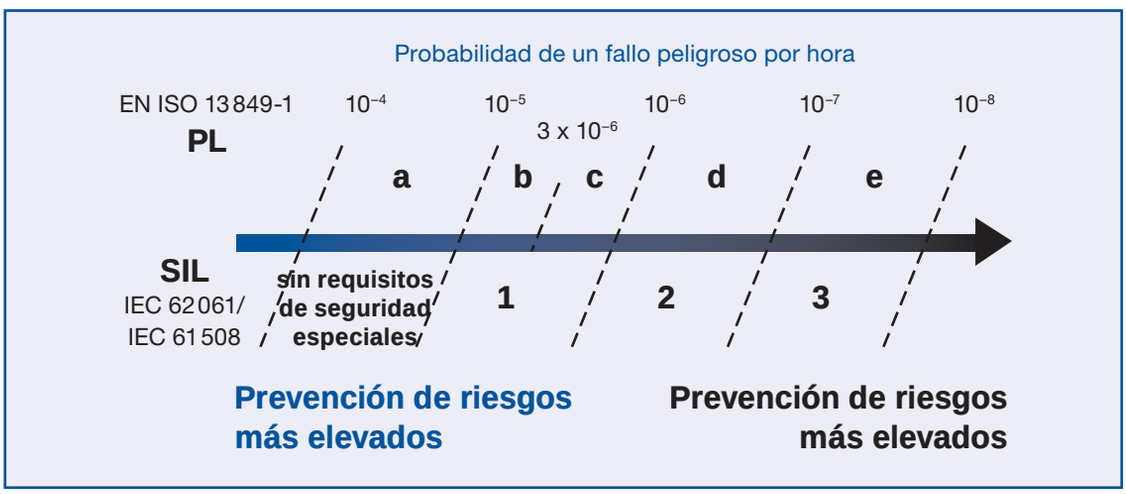


Figura 58: Relación entre SIL y PL

	Tecnología	ISO 13849-1 (en revisión)	IEC 62061
A	No eléctrica, por ejemplo hidráulica	X	Descartada
B	Electromecánica, por ejemplo relés	Arquitecturas designadas[1] y hasta PL = e	Todas las arquitecturas y hasta SIL 3
C	Electrónica compleja, por ejemplo programable	Arquitecturas designadas[1] y hasta PL = d	Todas las arquitecturas y hasta SIL 3
D	A combinada con B	Arquitecturas designadas[1] y hasta PL = e	X (EN ISO 13849-1 para A)
E	C combinada con B	Arquitecturas designadas[1] y hasta PL = d	Todas las arquitecturas y hasta SIL 3
F	C combinada con A, o C combinada con A y B	X[2]	X[3]

“x” significa que el punto está cubierto por la norma indicada sobre la columna.
1) Las arquitecturas designadas se definen en el anexo B de la EN ISO 13849-1 (rev.) para ofrecer una cuantificación simplificada del nivel de fiabilidad.
2) Para la electrónica compleja: uso de las arquitecturas designadas según la EN ISO 13849-1 (rev.) hasta PL = d o todas las arquitecturas según la IEC 62061.
3) Para tecnología no eléctrica: uso según la EN ISO 13849-1 (rev.) como sistema parcial.

Figura 59: Aplicación recomendada de la IEC 62061 y la ISO 13849-1 (en revisión)

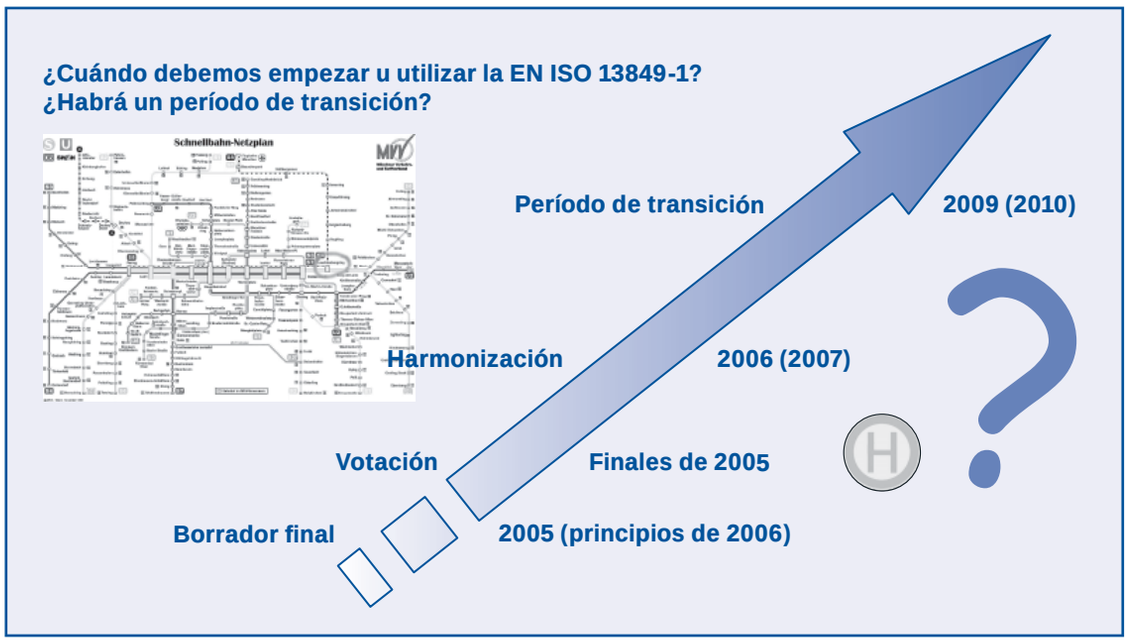


Figura 60: Calendario original (segunda mitad de 2005). En Diciembre 2006 se ha publicado la normativa definitiva.

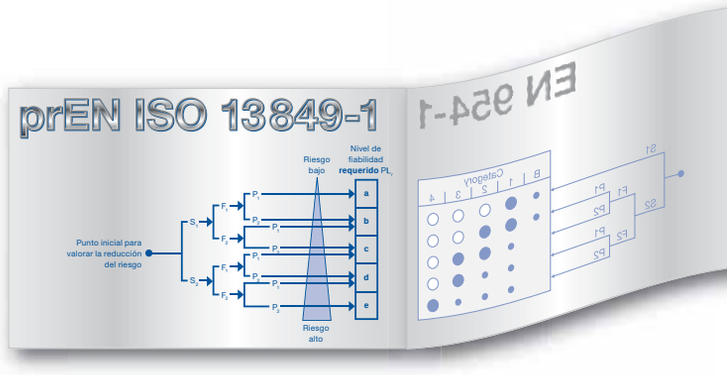
Entrada en vigor de la norma prEN ISO 13849-1

Calendario actual
Mientras que la IEC EN 62061 ya está formalmente en vigor, la prEN ISO 13849 se encuentra todavía en la fase final de votación (FDIS) y corre el riesgo de tener que pasar por otra modificación. Por ello en estos momentos (junio de 2004) sólo existe un borrador disponible en alemán, mientras que la 62061 ya está disponible en su versión definitiva como IEC EN 62061 en la editorial Beuth (www.beuth.de).

De todos modos, si se mantiene el calendario previsto, la EN ISO 13849-1 entrará en vigor en 2006, y tras un período de transición de 3 años sustituirá totalmente la EN 954-1.

Comparación con el estado del borrador a junio de 2004
En comparación con el estado del borrador a junio de 2004, la prEN ISO 13849-1 presenta ciertas enmiendas importantes en la versión definitiva, entre otras en lo referente al ámbito de aplicación (véase apartado correspondiente) y los gráficos de riesgos. Asimismo, aunque con limitaciones, la norma contempla los sistemas PES.

En cuanto a los gráficos de riesgos, actualmente la relación entre riesgos y nivel de fiabilidad queda ambigua. Ya no hay “entradas dobles” (por ejemplo, PL x o PL y). Además, el parámetro de riesgo F1 (frecuencia y/o duración de la exposición al peligro) se clarifica, de modo que “raramente” significa > 1 x por hora.



PREGUNTAS FRECUENTES

¿Cuáles son las diferencias fundamentales entre el borrador actual y el publicado de la norma prEN ISO 13849-1?

- alineación del gráfico de riesgos
- valores concretos de fiabilidad de la seguridad (PFH_d)
- valores concretos de $MTTF_d$ y B_{10d} para hidráulica, neumática y electromecánica
- requisitos para el software
- modificación del ámbito de aplicación
  - no se limita a las arquitecturas designadas
  - sólo se refiere a la IEC 61508 para el software integrado de PL_e

Figura 61: Preguntas seleccionadas

Otra diferencia es la modificación de la interpretación de la categoría de control 4, en la que la consideración de acumulación de defectos debe limitarse en general a dos.

¿Cuántos defectos tengo que combinar en la categoría 4?

1. Los defectos individuales no producen la pérdida de la función de seguridad.
2. Estos defectos iniciales ... no se contemplan. Si no es posible detectarlos, su acumulación no debe producir una pérdida de la función de seguridad.

Nota: En la práctica, la consideración de la combinación de dos defectos puede ser adecuada.

Novedad: Ya no depende de la tecnología de aplicación ni de las tasas de fallo de los componentes

Figura 62: Preguntas seleccionadas

La norma prEN ISO 13849-1 y las normas C
Teniendo en cuenta que en la actualidad existen unos centenares de normas C (de producto), por ejemplo para máquinas-herramienta y centros de mecanizado, se plantea un problema de compatibilidad, puesto que todas las normas C actuales sólo expresan el requisito de una categoría de control.

Por tanto, en los próximos años, los responsables de las normas C deberán hacer algo al respecto. Para adaptarse a la norma prEN ISO 13849-1, tendrán dos opciones.

Pueden limitarse a requerir exclusivamente un nivel de fiabilidad para sus máquinas, con el fin de ofrecer a sus “clientes” una mayor flexibilidad de diseño, sobre todo en el nivel de fiabilidad “medio”.

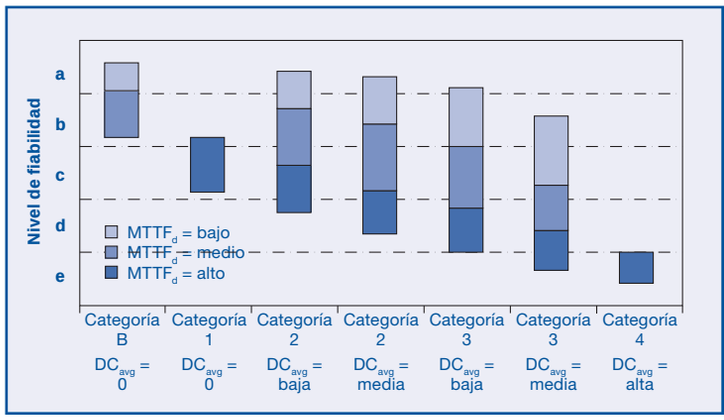


Figura 63: Diversidad de posibilidades de aplicación

Otra opción es determinar una categoría de control, además del nivel de fiabilidad, para tener una mayor influencia sobre la estructura.

Mi norma C exige una categoría de control de la máquina. ¿En el futuro podrá emplearse un nivel de fiabilidad?

- En principio, en el futuro bastará con la declaración de un nivel de fiabilidad. De todos modos, la norma prEN ISO 13849-1 prevé la siguiente especificación para cada SRP/CS en el apartado de información al usuario.

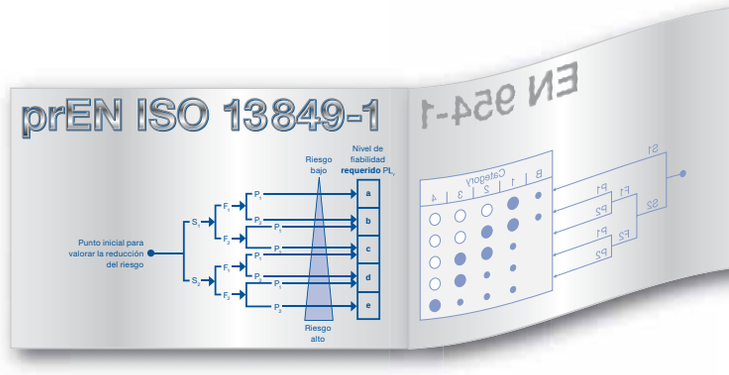
  EN ISO 13849-1:200x
  Categoría X PL Y

Figura 64: Preguntas seleccionadas

De momento, la siguiente tabla debería ser suficiente (¡cuidado al emplear la categoría de control 2 con la arquitectura designada que se especifica! Véase apartado correspondiente).

	B	**1**	**2**	**3**	**4**
Diseño conforme a normas correspondientes para soportar influencias previstas	X	X	X	X	X
Principios de seguridad probados		X	X	X	X
Componentes probados		X			
Tiempo medio hasta fallo peligroso – $MTTF_d$	bajo – medio	alto	bajo – medio	bajo – medio	alto
Detección de defectos (pruebas)			X	X	X
Seguridad en defecto único				X	X
Consideración de acumulación de defectos					X
Cobertura de diagnóstico – DC_{avg}			bajo – medio	bajo – medio	alto
Medidas de prevención de CCF			X	X	X
Caracterizado principalmente por	Selección del componente		Estructura		

Figura 65: Categorías de control y requisitos adicionales



Conclusiones

Sin duda, la norma prEN ISO 13849-1 deja muchas cuestiones pendientes. Por tanto, le seguiremos informando a través de nuestros boletines de próximas aclaraciones en cuanto aparezcan.

En resumen, los efectos de la norma prEN ISO 13849-1 pueden dividirse en dos grupos.

El primero es el de aquellos usuarios que sólo deban revisar la cuantificación ($MTTF_d$, DC, CCF). En este caso, podemos suponer que una máquina con SRP/CS cumplirá la nueva normativa si sus elementos de seguridad se han concebido y ejecutado con la suficiente calidad. No serán necesarias modificaciones sustanciales.

En cambio, quizás deban realizarse modificaciones en las conexiones en serie complejas (para evitar el riesgo de colapso por una acumulación de riesgos residuales), así como en arquitecturas designadas de la categoría 2.

Nota

Glosario

¡Abrirlo por favor!

Una nueva visión en la seguridad de las máquinas: **prEN ISO 13849-1 – Partes de los sistemas de mando relativas a la seguridad**

Glosario

Arquitectura designada:
Estructura predeterminada de una SRP/CS.

B_{10d}:
Número de operaciones de conmutación en que el 10% de la muestra falla.

CCF:
Fallo por causa común.

DC:
Cobertura de diagnóstico.

DC_{avg}:
Cobertura media de diagnóstico.

MTBF:
Tiempo medio entre fallos.

$MTTF_d$:
Tiempo medio hasta fallo peligroso.

PFH:
Probabilidad de fallo por hora.

PFH_d:
Probabilidad de fallo peligroso por hora.

PL:
Nivel de fiabilidad.

PL_r:
Nivel de fiabilidad requerido.

SIL:
Nivel de integridad de seguridad.

SRP/CS:
Partes relacionadas con la seguridad de los sistemas de control de las máquinas

K.A. Schmersal GmbH
Industrial safety switching systems

Möddinghofe 30
D-42279 Wuppertal
Postfach 24 02 63
D-42232 Wuppertal

Teléfono +49 (0)2 02 64 74-0
Fax +49 (0)2 02 64 74-100

E-Mail info@schmersal.com
Internet www.schmersal.com

Schmersal Ibérica, S.L.
Pol. Ind. La Masia
Camí de les Cabòries, Nave 4
08798 Sant Cugat Sesgarrigues
Teléfono +34 93 897 09 06
Fax +34 93 396 97 50
E-Mail info-es@schmersal.com
Internet www.schmersal.es

Schmersal Ibérica, S.L.
Apartado 30
2626-909 Póvoa de Sta. Iria
Teléfono +351 21 959 38 35
Fax +351 21 121 05 75
E-Mail info-pt@schmersal.com
Internet www.schmersal.pt

02/07 W