INSTITUTO NACIONAL
DE SEGURIDAD E HIGIENE
EN EL TRABAJO

Notas Técnicas de Prevención

946

Máquinas: diseño de las partes de los sistemas de mando relativas a la seguridad

Machinery: Design of safety-related parts of control systems
Machines: Conception des parties des systèmes de commande relatives à la sécurité

Redactores:

Fco. Javier Badiola Aldarondo
Ingeniero Industrial

Ibon Unzueta Estébanez
Ingeniero de Telecomunicaciones

CENTRO NACIONAL DE VERIFICACIÓN DE MAQUINARIA

En la presente Nota Técnica de Prevención se exponen los aspectos más importantes de la norma UNE EN ISO 13849-1:2008, trasposición de la norma armonizada de tipo B EN ISO 13849-1:2008 "Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño", que como tal, ofrece la presunción de conformidad con los requisitos esenciales referentes al sistema de mando de la nueva Directiva Máquinas 2006/42/CE. Dada su gran repercusión en las normas específicas de máquinas (normas de tipo C) y el carácter novedoso de sus contenidos, requiere una explicación detallada para su correcta aplicación, a lo que pretende contribuir esta nota técnica.

1. INTRODUCCIÓN

Las exigencias de productividad, flexibilidad, disponibilidad, etc. que se plantean a las máquinas hoy en día hacen que éstas incorporen soluciones cada vez más complejas y que dependan en mayor medida del sistema de mando. La seguridad no ha sido ajena a esta evolución y el número de funciones de seguridad que se confían al sistema de mando registra un aumento imparable.

En el año 1996 se publicó la norma europea armonizada EN 954-1:1996 "Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño" (después adoptada como norma nacional UNE-EN 954-1:1997 e internacional ISO 13849-1:1999), en apoyo de la Directiva Máquinas 98/37/CE, para orientar a los fabricantes de maquinaria durante el diseño de las partes del sistema de mando que desempeñan funciones de seguridad.

La creciente complejidad de los diseños de los sistemas de mando relativos a la seguridad obligó a revisar dicha norma, cuyos contenidos empezaban a ser insuficientes, y como resultado se publicó la versión EN ISO 13849-1:2006 y su correspondiente norma nacional UNE-EN ISO 13849-1:2007. Posteriormente la norma ha sufrido una serie de ligeras modificaciones para adaptarla a la nueva Directiva Máquinas 2006/42/CE y corregir algunos errores, plasmadas en la versión EN ISO 13849-1:2008 y su corrigendum AC 2009.

La norma EN 954-1:1996 ha coexistido con la versión EN ISO 13849-1:2006 hasta finales de 2011. A partir de 2012, se encuentra en vigor, únicamente, la versión EN ISO 13849-1:2008 (adoptada como norma nacional UNE-EN ISO 13849-1:2008).

La parte 1 de esta norma fue completada con una segunda parte EN ISO 13849-2:2003 "Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 2: Validación" (adoptada como norma nacional UNE-EN ISO 13849-2:2004), actualizada posteriormente como EN ISO 13849-2:2008 (adoptada como norma nacional UNE-EN ISO 13849-2:2008), que se refiere exclusivamente, como su propio nombre indica, a la etapa de validación del proceso de diseño esbozado en la parte 1.

La presente nota técnica explica el proceso de diseño de las partes de los sistemas de mando relativas a la seguridad, expresado de forma abreviada con las siglas SRP/CS, del inglés "Safety-Related Parts of Control Systems", propuesto en la norma UNE-EN ISO 13849-1:2008, haciendo hincapié en los nuevos parámetros utilizados para caracterizar una SRP/CS y en el procedimiento simplificado para estimar los aspectos cuantificables del nivel de prestaciones (PL), del inglés "Performance Level".

2. CAMPO DE APLICACIÓN

La norma UNE-EN ISO 13849-1:2008 proporciona requisitos y orientaciones sobre los principios para el diseño e integración de las SRP/CS que desempeñan funciones de seguridad, incluyendo el diseño del soporte lógico (software). No es pertinente para el resto de funciones encomendadas al sistema de mando.

Esta norma se aplica a las SRP/CS de cualquier tipo de máquina, independientemente de la tecnología y del tipo de energía utilizadas (eléctrica, hidráulica, neumática, mecánica, etc.). No es una norma de producto, por ejemplo, relés, interruptores de posición, electroválvulas, equipos sensibles a la presión, PLCs, etc.). Sin embargo, en el diseño de esos productos, se pueden utilizar los principios generales contenidos en esta norma.
Nota: Para el diseño de productos, es importante remitirse a las normas internacionales específicas, por ejemplo, IEC 60947, ISO 13851, ISO 13856, IEC 61113, etc.

La Comisión Electrotécnica Internacional, en el año 2005, publicó la norma IEC 62061:2005 "Seguridad de las máquinas. Seguridad funcional de sistemas de mando

eléctricos, electrónicos y programables", que establece requisitos para el diseño de sistemas de mando de esas tecnologías. El hecho de reconocer esta norma como norma europea armonizada (EN 62061) en el marco de la Directiva Máquinas, ha creado cierta confusión entre los fabricantes de maquinaria que, cuando diseñan una SRP/CS empleando la tecnología eléctrica, electrónica o electrónica programable, se encuentran ante la disyuntiva de tener que elegir entre dos normas armonizadas de diseño diferentes.

Para ayudar precisamente en esa elección, al menos temporalmente, los organismos de normalización ISO, CEN e IEC acordaron incluir un cuadro con recomendaciones sobre la aplicación de cada norma en el apartado Introducción de ambas normas.

Esas recomendaciones, que fueron escritas durante la elaboración de la norma EN ISO 13849-1:2006, deben considerarse obsoletas y, hoy por hoy, se acepta que no existe ninguna restricción para la aplicación de la norma EN ISO 13849-1:2008, salvo el uso de la norma IEC 61508-3 para el desarrollo del software relativo a la seguridad en determinados casos muy específicos (software empotrado de componentes de tecnología electrónica compleja en el caso de diseño de SRP/CS con PL_r e que no poseen una arquitectura completamente redundante y diversificada).

Esto es lo que viene a confirmar el informe técnico con la referencia ISO TR 23849:2010 e IEC/TR 62061-1:2010 titulado "Guía para la aplicación de las normas ISO 13849-1 e IEC 62061 en el diseño de sistemas de mando relativos a la seguridad en maquinaria", que ofrece pautas adicionales para resolver el conflicto planteado. Está previsto iniciar, próximamente, una modificación de las dos normas (ISO 13849-1 e IEC 62061) a fin de sustituir el cuadro mencionado por una referencia a esa guía.

El enfoque genérico en relación con las tecnologías y el enfoque simplificado en relación con la cuantificación, con el uso de las arquitecturas tipo basadas en el concepto ya extendido de categorías, pueden ser los argumentos decisivos desde el punto de vista del usuario para decantarse por la norma EN ISO 13849-1:2008 como base para la implementación de las funciones de seguridad.

3. CONCEPTOS BÁSICOS

Antes de explicar el proceso de diseño de las SRP/CS, es preciso introducir las definiciones de los términos empleados para especificar las prestaciones de las SRP/CS.

Parte de un sistema de mando relativa a la seguridad (SRP/CS)

Parte de un sistema de mando que responde a señales de entrada y genera señales de salida relativas a la seguridad.

Las partes combinadas de un sistema de mando relativas a la seguridad comienzan en los puntos en los que se generan las señales de entrada relativas a la seguridad (incluyendo, por ejemplo, la leva de accionamiento y la roldana de un interruptor de posición) y terminan a la salida de los elementos de mando de los accionadores (incluyendo, por ejemplo, los contactos principales de un contactor).

Nota: Dado el carácter abierto de la definición, este término se puede emplear para designar a un(os) componente(s) que puede(n) constituir un canal de un subsistema o un subsistema completo, o bien a un conjunto de componentes que constituyen el sistema.

Nivel de Prestaciones (PL)

Nivel discreto utilizado para especificar la aptitud de las SRP/CS para desempeñar una función de seguridad en condiciones previsibles. La aptitud de las SRP/CS se ha clasificado en cinco niveles que se definen en términos de probabilidad media de fallo peligroso por hora (PFH) y en ciertos requisitos contra los fallos sistemáticos (véase tabla 1).

El nivel de prestaciones depende, por tanto, de la probabilidad de que se produzca un fallo en la SRP/CS y que en esas condiciones (antes de detectar el fallo en la SRP/CS y reaccionar) se solicite o demande la función de seguridad.

PL	Probabilidad media de fallo peligroso por hora (PFH) 1/h
a	$\geq 10^{-5}$ a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
e	$\geq 10^{-8}$ a $< 10^{-7}$
Para alcanzar un determinado PL, además de la PFH, son necesarias las medidas contra los fallos sistemáticos.	

Tabla 1.Niveles de prestaciones (PL)

Nota: La PFH no es un parámetro (intrínseco) que dependa sólo del equipo, sino que depende también del régimen de demandas de la función de seguridad, es decir, de la aplicación, lo que a priori significa que cada SRP/CS puede ofrecer diferentes valores de PFH en función de la aplicación. No obstante, se ha demostrado que para los valores de fiabilidad de los componentes utilizados en las SRP/CS, las frecuencias a las que se realizan las comprobaciones internas, los tiempos de reparación, etc., la frecuencia con la que se demanda una función de seguridad de las SRP/CS en máquinas (como mínimo una vez por año) no influye significativamente en la PFH de una SRP/CS, salvo en casos excepcionales (determinada estructura), como se explicará más adelante.

La PFH es, en realidad, un término de tasa media de fallos peligrosos de la función de seguridad y se puede interpretar como el número medio de demandas no atendidas de la función de seguridad por hora.

En esta norma se considera que el nivel de prestaciones de una SRP/CS depende de una serie de aspectos que, desde el punto de vista de la evaluación, se pueden agrupar en:

a) aspectos cuantificables (la estructura, el tiempo medio hasta un fallo peligroso $MTTF_d$ de los componentes, la cobertura de los diagnósticos DC, la resistencia a fallos de causa común CCF…), y
b) aspectos cualitativos no cuantificables (el comportamiento de la función de seguridad en condiciones de defecto, el software relativo a la seguridad, la gestión del proyecto, la documentación, la revisión del diseño y los ensayos, la resistencia a las condiciones ambientales…)

Los aspectos cuantificables son aquellos utilizados para caracterizar la propensión o resistencia a que se produzca un fallo de la función de seguridad (pérdida o malfuncionamiento) por causa de un defecto o avería aleatorio del soporte físico (hardware), mientras que los aspectos no cuantificables se refieren a los que valoran el comportamiento en condiciones de defecto y la posible presencia de defectos sistemáticos en el hardware y en el software o la comisión de errores durante el servicio y el mantenimiento, que pudieran producir un fallo de la función de seguridad.

Nota: Los mecanismos que causan los fallos o defectos aleatorios de hardware no son del todo conocidos, pero la experiencia muestra que la variable "tiempo hasta el fallo" sigue una determinada distribución de probabilidad. Por ello, podemos estimar la probabilidad de que se produzca un fallo en la SRP/CS que provoca un fallo en el desarrollo de una misión con una duración determinada (infiabilidad) o la probabilidad de que la SRP/CS se encuentre defectuosa en un instante de tiempo (indisponibilidad), pero no podemos indicar el instante en que se producirá el fallo ni cuales han sido las causas que lo han provocado. En el caso de los fallos o defectos sistemáticos el enfoque es justamente el contrario: se considera que se puede establecer la relación causa-efecto pero no es posible calcular una probabilidad de fallo de la SRP/CS para una misión (por ejemplo, se sabe que un error de dimensionamiento de un contactor, que provoca una sobrecarga de los contactos, tarde o temprano acabará soldando los mismos). Los defectos sistemáticos de los componentes pueden provocar fallos en subsistemas inmediatamente, en el momento en que se ejercitan por primera vez éstos, o después de un tiempo de uso o un número de solicitaciones.

El peso relativo de unos y otros aspectos varía de un diseño a otro. La creciente presencia de software relativo a la seguridad en los diseños inclina la balanza al lado de los aspectos cualitativos por lo que en estos casos habrá que reforzar las medidas adoptadas para evitar y controlar los fallos o defectos sistemáticos.

Categoría

Término utilizado originalmente (norma EN 954-1:1996) para designar la aptitud de las SRP/CS para desempeñar una función de seguridad. En la norma EN ISO 13849-1:2008, se ha mantenido el término de categoría por su gran repercusión en el cuerpo normativo existente (normas de tipo B y C) y, básicamente, se utiliza para designar unas arquitecturas con unos criterios de diseño y unos comportamientos en caso de defecto específicos.

4. ESTRATEGIA PARA LA REDUCCIÓN DEL RIESGO

En la evaluación de riesgos realizada al conjunto de la máquina se identifican los peligros presentes en cada tarea o actividad que efectúan los operarios de la máquina y se estiman los riesgos asociados. Si los niveles de riesgo son inaceptables se intenta eliminar el peligro o reducir el nivel de riesgo mediante la aplicación de las medidas preventivas conocidas, respetando el orden jerárquico que establece la Directiva Máquinas, es decir, aplicando primero las medidas de prevención intrínseca, después, las de protección y las suplementarias y, finalmente, facilitando la información para la utilización.

Una de las medidas pertenecientes al grupo de las medidas de prevención intrínseca es la basada en dotar a la máquina de funciones de mando adicionales, que ofrecen ciertas garantías de funcionamiento, y que contribuyen a reducir el nivel de riesgo en determinadas situaciones peligrosas (por ejemplo, una función de selección de los diferentes modos de mando y funcionamiento, una función de parada de los elementos móviles peligrosos en caso de detectarse el acceso a una zona peligrosa, una función de control de momento de vuelco, una función de control de velocidad reducida durante las pruebas de ajuste…). Esas funciones adicionales reciben el nombre de funciones de seguridad del sistema de mando y deben ser diseñadas conforme a la norma UNE-EN ISO 13849-1:2008.

La identificación (definición) de las funciones de seguridad del sistema de mando no siempre resulta sencilla y puede tener repercusión en sus especificaciones.

El riesgo asociado a una situación peligrosa se puede reducir mediante la aplicación de una o varias medidas de prevención, que, además, pueden pertenecer al mismo tipo de medida o a diferentes tipos. También, es posible que un operario se vea expuesto a varios peligros simultáneamente en una situación peligrosa (peligros superpuestos).

Una vez que se han identificado las funciones de seguridad del sistema de mando de la máquina, comienza el proceso de diseño de cada una de las mismas.

5. PROCESO DE DISEÑO DE LAS SRP/CS

El proceso de diseño de las SRP/CS que realizan una función de seguridad del sistema de mando se inicia especificando los requisitos de seguridad que comprenden las características funcionales y el nivel de prestaciones requerido (PL_r) (véase figura 1).

Etapa 1 Especificación de los requisitos de seguridad

La especificación de las características funcionales de una función de seguridad debe contener suficientes detalles para que se pueda abordar el diseño propiamente dicho de la(s) SRP/CS, incluyendo en la medida que sea pertinente:

- una descripción de la función de seguridad,
- las condiciones de la máquina en las que la función se encuentra activa (por ejemplo, en qué modos de funcionamiento y en qué fases del ciclo de trabajo de la máquina),
- el comportamiento de la máquina cuando se dispara la función de seguridad,
- las condiciones a tener en cuenta para el restablecimiento de la función de seguridad una vez disparada,
- el tiempo de respuesta de la función de seguridad (SRP/CS) y otras características temporales,
- la frecuencia de demanda de la función,
- …

El capitulo 5 de la norma ofrece una lista y detalles de funciones de seguridad típicas implementadas en los sistemas de mando de las máquinas.

Para determinar el nivel de prestaciones requerido (PL_r) para una función de seguridad, la norma UNE-EN ISO 13849-1:2008 ofrece un gráfico del riesgo (véase figura 2) que relaciona los parámetros del riesgo con los niveles de prestaciones.

Si en una situación peligrosa, para reducir el nivel de riesgo, se utilizan más de una medida preventiva, al aplicar el gráfico del riesgo sucesivamente para cada medida

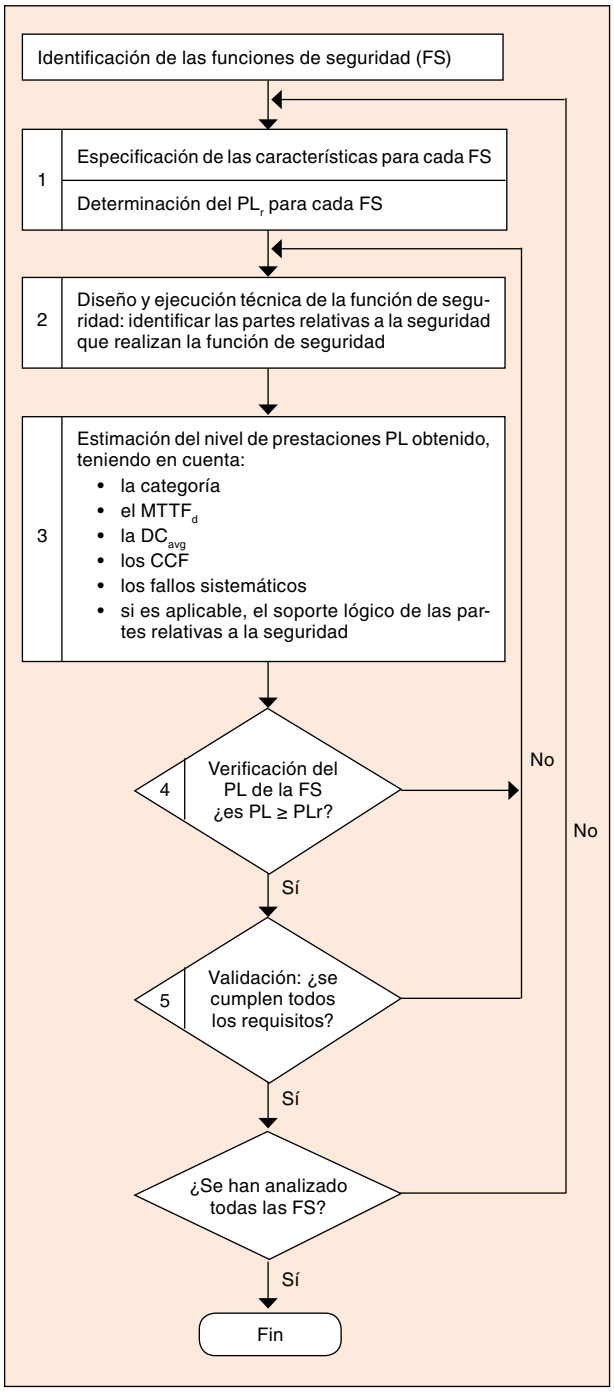


Figura 1. Proceso iterativo para el diseño de las SRP/CS

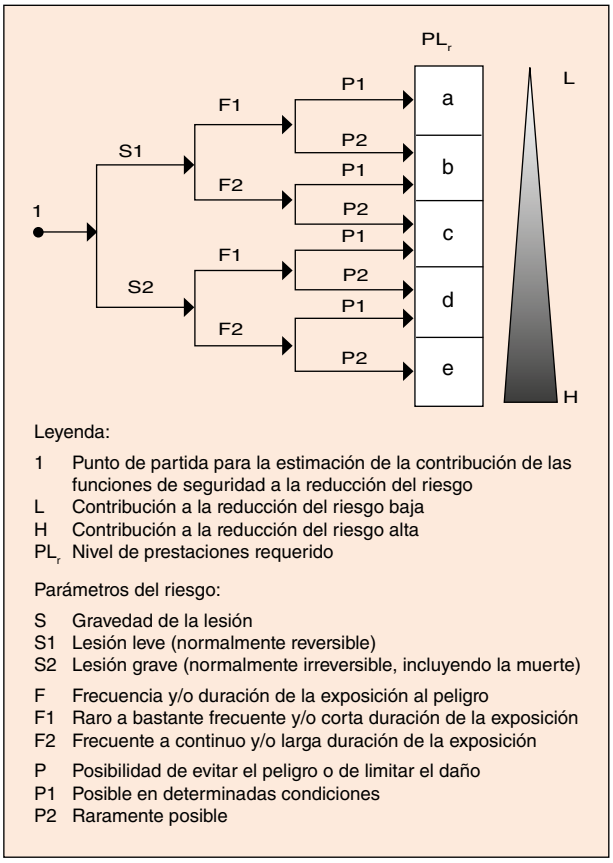


Figura 2. Gráfico del riesgo para determinar el nivel de prestaciones requerido (PL_r) para cada función de seguridad

preventiva se debe tener en cuenta la(s) aportación(es) realizada(s) por la(s) medida(s) preventiva(s) aplicada(s) previamente.

Se trata de un gráfico simplificado en el que no se considera la probabilidad de que ocurra el suceso peligroso desencadenante del accidente, lo que proporciona estimaciones más exigentes de los PLs.

Etapa 2 Diseño y ejecución

Una vez que se han especificado los requisitos para una función de seguridad se inicia el diseño propiamente dicho de las SRP/CS.

El nivel de prestaciones requerido PL_r para la función de seguridad impone ciertas exigencias al diseño de los circuitos (la arquitectura, los diagnósticos, la fiabilidad de los componentes, las medidas para evitar y controlar los fallos sistemáticos…).

El diseño comienza con la descomposición de la función de seguridad en bloques funcionales (generalmente tres: entrada, lógica o tratamiento y salida) seguido de un planteamiento de los circuitos (componentes o subsistemas) que van a implementar dichos bloques y, por último, una agrupación de los circuitos en SRP/CS.

Nota: Según el espíritu de la norma a los componentes comerciales simples no se les debería asignar una categoría (componentes que no poseen una estructura redundante o algún autocontrol, como por ejemplo un detector de posición, un contactor o una válvula hidráulica). No obstante, cuando un componente simple se aplica en un diseño y constituye por sí solo una SRP/CS, a esa SRP/CS se le asigna una categoría.

Según el procedimiento simplificado de estimación de la PFH, una función de seguridad puede ser realizada por una única SRP/CS sólo si la estructura de su implementación se puede aproximar a una de las arquitecturas tipo (véase el apartado Especificaciones de las Categorías).

Cuando se trata de una función de seguridad compleja es posible que los elementos que realizan dicha función en su conjunto no se puedan aproximar a ninguna de las arquitecturas tipo. En tal caso, la cadena de elementos se divide en secciones de modo que éstas se asemejen a las arquitecturas tipo. Estas secciones constituyen las SRP/CS que realizan la función de seguridad (véase figura 3). En este caso, el PL de referencia para cada SRP/CS será igual al PL_r de la función de seguridad.

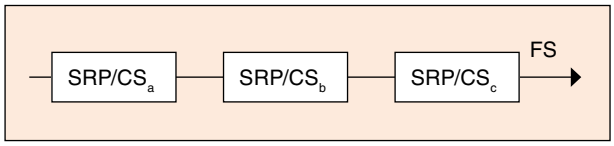


Figura 3. Representación de la implementación de una función de seguridad mediante varias SRP/CS.

Nota: En ocasiones, la descomposición de una función de seguridad en varias SRP/CS viene obligada por el uso de subsistemas comerciales (por ejemplo, un PLC de seguridad), de los cuales sólo se dispone de datos de conjunto (PL) y no de datos detallados (la categoría, el $MTTF_d$ de cada canal, la DC_{avg} y las medidas contra CCF).

Se puede dar el caso también de que varias funciones de seguridad compartan una o más SRP/CS (por ejemplo, una unidad lógica o el elemento de mando del accionador). Entonces, si las funciones de seguridad poseen el mismo PL_r, ese PL_r debe ser el PL de referencia para la SRP/CS compartida, y si las funciones de seguridad poseen PL_r diferentes, el PL de referencia para la SRP/CS compartida debe ser igual al PL_r más alto, a menos que se pueda demostrar que la implementación de las diferentes funciones es suficientemente independiente.

También es posible que una SRP/CS implemente funciones de seguridad y funciones de mando no relativas a la seguridad.

Cuando se ha esbozado el diseño arquitectónico corresponde diseñar el resto de las medidas estructurales como son los diagnósticos (comprobaciones de verosimilitud de señales de entrada, un control temporal de la secuencia del software, etc.) y las medidas contra los fallos de causa común (separación física de las señales críticas, utilización de tecnologías diferentes en canales redundantes, etc.).

A continuación, se dimensionan y eligen los componentes que forman parte de la SRP/CS, teniendo en cuenta los requisitos de fiabilidad, las solicitaciones de funcionamiento (por ejemplo, en unidades de tecnología eléctrica, los tipos de carga, las tensiones, las intensidades y las frecuencias de corte) y las influencias externas.

Durante el diseño del hardware, también se deben considerar los fallos sistemáticos y adoptar las medidas apropiadas.

En el diseño, siempre se deben aplicar los principios fundamentales de seguridad y, dependiendo del PL_r, además, los principios y componentes de eficacia probada (véase la norma UNE-EN ISO 13849-2:2008).

Si alguna de las SRP/CS que realiza la función de seguridad es programable, en el desarrollo de su programa de aplicación relativo a la seguridad se deben aplicar medidas para evitar fallos debido a causas sistemáticas (por ejemplo, errores de diseño del programa, errores de codificación, etc.). Finalmente, se combinan todos los componentes del hardware y el software, y se procede a la integración de ambos soportes para formar la SRP/CS.

Una SRP/CS diseñada de acuerdo con las arquitecturas tipo disfruta de la ventaja de disponer de unas pautas para el diseño y de poder aplicar el procedimiento simplificado para la estimación de la PFH que se describe a continuación. Si por contra, la SRP/CS no respeta las arquitecturas tipo, el diseñador debe proporcionar un cálculo detallado para demostrar que se ha alcanzado el nivel de prestaciones requerido PL_r.

Si la función de seguridad se implementa mediante varias SRP/CS, el diseño finaliza con la combinación de las mismas.

Etapa 3 Estimación del PL obtenido

Cuando se ha completado el diseño de cada SRP/CS, se deben estimar las prestaciones de seguridad conseguidas.

El procedimiento de evaluación de las prestaciones de seguridad de una SRP/CS que ofrece la norma consiste en estimar la probabilidad media de fallo peligroso por hora (PFH) y comprobar la adecuada aplicación de las medidas recomendadas contra los fallos sistemáticos.

Estimación de los aspectos cuantificables

La probabilidad media de fallo peligroso por hora (PFH) debido a un defecto aleatorio del hardware depende principalmente de:

- la arquitectura o estructura de la SRP/CS,
- la fiabilidad de los componentes (tiempo medio hasta un fallo peligroso $MTTF_d$),
- la efectividad de los mecanismos de detección de defectos (cobertura del diagnóstico DC) y
- la resistencia a los fallos de causa común CCF.

Existen otros factores que pueden tener cierta influencia en la probabilidad de fallo peligroso de una SRP/CS, como son la tasa de solicitación o demanda, la tasa de verificación o comprobación, las revisiones o pruebas periódicas y la tasa de restauración, pero se ha demostrado que éstos no son significativos, excepto en el caso de una arquitectura particular, como se verá más adelante.

Nota: La norma no contempla la revisión o prueba periódica de la SRP/CS (que en las normas IEC se designa "proof test") por considerar que la Directiva Máquinas prioriza la aplicación de medidas preventivas adoptadas por el diseñador a las medidas preventivas adoptadas por el usuario y que, en muchas aplicaciones de maquinaria, unos intervalos de revisión o prueba periódica ajustados no son realistas ni practicables.

Se parte de la hipótesis de que el fallo aleatorio de todos los componentes hardware sigue una distribución exponencial (véase la NTP 316) y se propone un método de conversión para aquellos componentes que se ajustan más a una distribución de Weibull (véase la NTP 331).

Para facilitar la estimación de la probabilidad media de fallo peligroso por hora (PFH) de una SRP/CS, la norma proporciona un procedimiento simplificado que ofrece una representación gráfica para la estimación directa de la gama de PFH (PL) y otra tabulada que proporciona valores numéricos concretos de PFH. Este procedimiento se basa en caracterizar la arquitectura del diseño (categoría) y en estimar una serie de parámetros (el tiempo medio hasta un fallo peligroso $MTTF_d$ de un canal, la cobertura del diagnóstico media DC_{avg} y las medidas contra los fallos de causa común).

En realidad, el procedimiento se refiere a un conjunto de arquitecturas tipo, definidas implícitamente en las especificaciones de las categorías de la antigua norma EN 954-1:1996, a las que ahora se añaden requisitos de fiabilidad. De este modo se asegura la continuidad del concepto de categoría, necesario por su gran repercusión como ya se ha señalado.

Especificaciones de las Categorías

Las categorías, se puede decir, representan un conjunto de diseños tipo para las SRP/CS con unas características (arquitectura tipo, fiabilidad del conjunto de los componentes que constituyen un canal, calidad de las pruebas y comprobaciones internas y, en caso de diseños con algún grado de redundancia, la inmunidad de las partes

a los fallos de causa común) que pueden variar dentro de unos márgenes, y un comportamiento ante defectos determinado.

Las arquitecturas tipo reflejan la mayoría de las estructuras que se encuentran en el ámbito de las máquinas. Son representaciones lógicas de las estructuras de las SRP/CS y, por ello, pueden no concordar exactamente con los esquemas de circuito (estructuras físicas) de las SRP/CS.

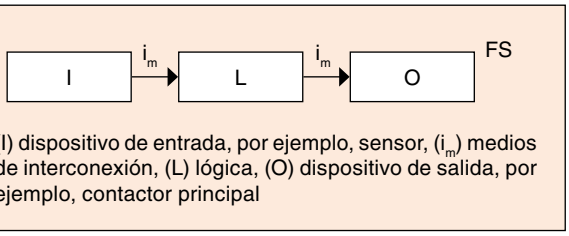
Categoría B

Una SRP/CS de categoría B debe, como mínimo, ser diseñada de acuerdo con las normas pertinentes y utilizar los principios fundamentales de seguridad para la aplicación específica (véase UNE-EN ISO 13849-2:2008), de manera que resista los esfuerzos de funcionamiento esperados, las influencias del material procesado y otras influencias externas relevantes.

Estas SRP/CS no poseen cobertura del diagnostico (DC_{avg} nula) y el $MTTF_d$ del canal puede ser bajo o medio. Al tratarse de sistemas de canal simple, no tiene sentido considerar los fallos de causa común CCF.

Los componentes de la SRP/CS se encuentran organizados en serie, de manera que el fallo de uno cualquiera de ellos provoca el fallo de la SRP/CS. En esta arquitectura tipo no se realiza ningún diagnóstico sobre los componentes/unidades de la SRP/CS.

La arquitectura tipo de las SRP/CS es la que se muestra en la figura 4.



(I) dispositivo de entrada, por ejemplo, sensor, (i_m) medios de interconexión, (L) lógica, (O) dispositivo de salida, por ejemplo, contactor principal

Figura 4. Arquitectura tipo para las categorías B y 1

El PL máximo que se puede conseguir con la categoría B es PL b (véase la figura 7).

Categoría 1

Una SRP/CS de categoría 1 debe ser diseñada conforme a los requisitos de la categoría B y, además, aplicando componentes y principios de seguridad de eficacia probada (véase UNE-EN ISO 13849-2:2008).

Estas SRP/CS no poseen cobertura del diagnostico (DC_{avg} nula) y el $MTTF_d$ de cada canal debe ser alto.

La arquitectura tipo de las SRP/CS de categoría 1 es la misma que las de categoría B (véase la figura 4).

El PL máximo que se puede conseguir con la categoría 1 es PL c (véase la figura 7).

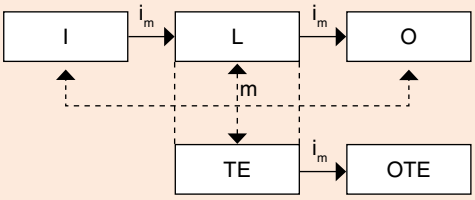
Nota: Este nivel máximo de PL alcanzable con la categoría 1 se debe a la limitación del valor máximo de $MTTF_d$ de un canal.

Tanto en una SRP/CS de categoría B como en una de categoría 1, un defecto puede conducir a la pérdida de la función de seguridad, pero en la categoría 1 dicha pérdida es menos probable.

Categoría 2

Una SRP/CS de categoría 2 debe ser diseñada conforme a los requisitos de la categoría B y aplicando los principios de seguridad de eficacia probada (véase UNE-EN ISO 13849-2:2008). Además, debe ser diseñada de manera que su función se compruebe a intervalos de tiempo adecuados.

La arquitectura tipo de las SRP/CS es la que se muestra en la figura 5.



(I) dispositivo de entrada, por ejemplo, sensor, (i_m) medios de interconexión, (L) lógica, (O) dispositivo de salida, por ejemplo, contactor principal, (m) comprobación, (TE) equipo de comprobación, (OTE) salida del TE

Figura 5. Arquitectura tipo para la categoría 2

La cobertura del diagnostico media DC_{avg} de la SRP/CS puede ser baja o media y el $MTTF_d$ de cada canal de bajo a alto. Dada la arquitectura tipo que posee, se deben aplicar medidas contra fallos de causa común CCF.

Los componentes principales de la SRP/CS se encuentran organizados en serie (I+L+O). Adicionalmente, en esta arquitectura existe un circuito de comprobación (TE+OTE) que realiza diagnósticos sobre todos o ciertos componentes del canal "principal".

El PL máximo que se puede conseguir con la categoría 2 es PL d (véase la figura 7).

En una SRP/CS de categoría 2, un defecto entre dos comprobaciones sucesivas puede conducir a la pérdida de la función de seguridad, pero dicha condición de inseguridad se detecta en la siguiente comprobación.

Categoría 3

Una SRP/CS de categoría 3 debe ser diseñada conforme a los requisitos de la categoría B y aplicando los principios de seguridad de eficacia probada (véase UNE-EN ISO 13849-2:2008). Además, debe ser diseñada de manera que un solo defecto en cualquiera de sus componentes no conduzca a la pérdida de la función de seguridad. Siempre que sea razonablemente factible, el defecto debe ser detectado en o antes de la siguiente solicitación de la función de seguridad.

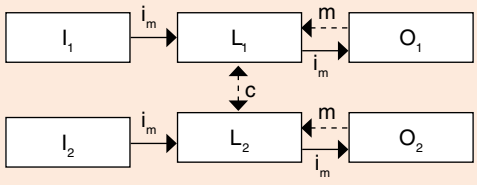
La cobertura del diagnóstico media DC_{avg} de la SRP/CS puede ser baja o media y el $MTTF_d$ de cada canal de bajo a alto. Dada la arquitectura tipo que posee, se deben aplicar medidas contra fallos de causa común CCF.

La arquitectura tipo de la SRP/CS es la que se muestra en la figura 6.

La función de seguridad es ejecutada por dos canales separados y los componentes de cada canal se encuentran organizados en serie (I+L+O). Las SRP/CS incorporan ciertas pruebas y comprobaciones internas para detectar al menos los defectos más probables.

El PL máximo que se puede conseguir con la categoría 3 es PL e (véase la figura 7).

En una SRP/CS de categoría 3, la función de seguridad está garantizada ante un solo defecto. Parte de estos defectos son detectados por los circuitos de prueba y comprobación en o antes de la solicitación de la función.



(I) dispositivo de entrada, por ejemplo, sensor, (i_m) medios de interconexión, (L) lógica, (O) dispositivo de salida, por ejemplo, contactor principal, (c) comprobación cruzada, (m) comprobación

Figura 6. Arquitectura tipo para las categorías 3 y 4

Una acumulación de defectos no detectados puede conducir a la pérdida de la función de seguridad.

Categoría 4

Una SRP/CS de categoría 4 debe ser diseñada conforme a los requisitos de la categoría B y aplicando los principios de seguridad de eficacia probada (véase UNE-EN ISO 13849-2:2008). Además, debe ser diseñada de manera que un solo defecto en cualquiera de sus componentes no conduzca a la pérdida de la función de seguridad. El defecto debe ser detectado en o antes de la siguiente solicitación de la función de seguridad; en caso de que no fuera posible detectarlo, una acumulación de defectos no detectados no debe conducir a la pérdida de la función de seguridad.

La cobertura del diagnóstico media DC_{avg} de la SRP/CS debe ser alta y el $MTTF_d$ de cada canal también alto. Dada la arquitectura tipo que posee, se deben aplicar medidas contra fallos de causa común CCF.

La arquitectura tipo de las SRP/CS de categoría 4 es prácticamente igual a la de las partes de categoría 3, exceptuando la cantidad y calidad de las comprobaciones.

El PL que se consigue con la categoría 4 es PL e (véase la figura 7).

Tiempo medio hasta un fallo peligroso de un canal de la SRP/CS ($MTTF_{dCH}$)

El tiempo medio hasta un fallo peligroso de un componente ($MTTF_{dC}$) es el valor probable del tiempo medio hasta un fallo peligroso. Si la variable tiempo hasta el fallo del componente sigue una distribución exponencial (véase NTP 316), el parámetro $MTTF_{dC}$ es igual a la inversa de la tasa de fallos peligrosos (λ_{dC}).

$$MTTF_{dC} = \frac{1}{\lambda_{dC}}$$

Los fallos de un componente o de un sistema, en una primera subdivisión, se agrupan en fallos seguros (expresados con la sigla s, del inglés “safe”) y fallos peligrosos (expresados con la sigla d, del inglés “dangerous”), y así, la tasa de fallos de un componente resulta $\lambda_C = \lambda_{sC} + \lambda_{dC}$.
Nota: En esta nota técnica, con el fin de evitar confusiones, la tasa de fallos y el tiempo medio hasta un fallo de un componente se designan con el subíndice C y la tasa de fallos y el tiempo medio hasta un fallo de un canal con el subíndice CH.

Si no se facilita directamente la tasa de fallos peligrosos de un componente (λ_{dC}), ésta se puede obtener a partir de la tasa de fallos del componente (λ_C) y de la proporción de fallos peligrosos del componente (λ_{dC}/λ_C), resultando $\lambda_{dC} = \lambda_C.(\lambda_{dC}/\lambda_C)$; o asumiendo que los fallos se reparten por igual en fallos seguros y fallos peligrosos de manera que $\lambda_{dC} = \lambda_C.0{,}5$; o bien se puede realizar un análisis tipo FMEA, para lo cual se necesitan conocer los distintos modos de fallos de cada componente y sus proporciones relativas.

En general, la hipótesis del 50 % proporciona estimaciones conservadoras de la λ_{dC}, mientras que una estimación detallada resulta laboriosa y, por ello, sólo se justifica para componentes que ofrecen tasas de fallos peligrosos altas en una primera aproximación.

El procedimiento jerárquico para buscar los datos para la estimación del $MTTF_{dC}$, debe ser:

a) utilizar los datos del fabricante,
b) utilizar los métodos del anexo C de la norma, o
c) tomar 10 años.

Nota: Los valores de $MTTF_{dC}$ de los componentes se dan para unas condiciones de referencia, por ejemplo, un margen de temperatura. Si en una aplicación determinada se sospecha que un componente estará sometido a unas condiciones o esfuerzos diferentes a las de referencia, se debe convertir el $MTTF_{dC}$ de referencia a un $MTTF_{dC}$ real.

A falta de datos del fabricante, en el anexo C de la norma se ofrece la posibilidad de asumir ciertos valores de MTTFdC y B10dC para componentes mecánicos, hidráulicos, neumáticos y electromecánicos, considerados típicos, siempre y cuando se cumplan una serie de criterios. A este modo de proceder se le denomina método de las buenas prácticas de la ingeniería.

En las tablas C2 a C7, del mismo anexo C, se ofrecen datos típicos de $MTTF_{dC}$ para componentes eléctricos.

En el anexo C se asume que la condición segura de la aplicación se alcanza con una anulación de la energía, de modo que los valores de $MTTF_{dC}$ y B_{10dC} representan fallos del tipo: imposibilidad de cierre de una válvula, imposibilidad de apertura de los contactos NA de un contactor, imposibilidad de corte de un transistor, imposibilidad de cambio a estado bajo de una salida digital de un PLC, etc. Por ello, el diseñador, antes de utilizar los datos del anexo C, debe asegurarse de que la función que trata de diseñar es una función de desconexión.

Para resolver el problema que plantean los componentes cuyos fallos, en lugar de una distribución exponencial, siguen la distribución de Weibull, que se caracterizan con el parámetro B_{10d}, la norma ofrece un método para convertir ese dato en un valor de $MTTF_{dC}$, a partir del régimen de funcionamiento al que se somete el componente en una aplicación determinada.

Nota: El parámetro B_{10} representa el número medio de ciclos realizados hasta que el 10 % de los componentes falla. Del mismo modo, el B_{10d} representa el número medio de ciclos realizados hasta que el 10 % de los componentes falla peligrosamente. Disponiendo del dato de B_{10}, se puede asumir que la proporción de fallos peligrosos es del 50 %, al igual que para la estimación de la $MTTF_{dC}$, de manera que $B_{10d} = 2 \cdot B_{10}$.

En este método se limita la vida útil o tiempo de servicio (tiempo en que la tasa de fallos de un componente que sigue una distribución exponencial permanece constante) de un componente a T_{10d} (tiempo medio hasta que el 10% de los componentes falla peligrosamente), que se estima:

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

siendo n_{op} el número medio de operaciones que el componente realiza en un año.

Suponiendo que para $t = T_{10d}$ la función de distribución exponencial equivalente debe dar una probabilidad de fallo del 10 %, se obtiene que:

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

Si la vida útil de un componente (T_{10d}) que forma parte de la SRP/CS es inferior a la duración de la misión (T_M) de la aplicación, habrá que prever una sustitución del componente a tiempo.

Para estimar el $MTTF_{dCH}$ de un canal, por separado, la norma propone el método de recuento de partes. Este método se basa en la hipótesis de que un fallo peligroso de un componente en un canal conduce a un fallo peligroso de todo el canal.

Una vez se tienen los $MTTF_{dC}$ de los n componentes individuales que forman el canal, el $MTTF_d$ del canal completo se obtiene mediante la fórmula:

$$\frac{1}{MTTF_{dCH}} = \sum_{i=1}^{n} \frac{1}{MTTF_{dCi}}$$

En las arquitecturas tipo los dos canales de un sistema redundante son iguales y, por tanto, el valor de $MTTF_{dCH}$ de los canales es idéntico. Si una SRP/CS posee una arquitectura redundante formada por dos canales diferentes, existen dos posibilidades:

a) asumir el valor de $MTTF_{dCH}$ de canal más bajo, como hipótesis más desfavorable, o
b) aplicar la fórmula de simetrización que figura en el anexo D de la norma.

En el procedimiento simplificado de estimación de la PFH (PL), el valor del $MTTF_{dCH}$ de cada canal se ha clasificado en tres niveles (véase tabla 2) y se debe tener en cuenta para cada canal individualmente (por ejemplo, el canal en un sistema monocanal o cada uno de los canales en un sistema redundante).

Según esta clasificación, el valor máximo de $MTTF_{dCH}$ para un canal es cien años. No obstante, se pueden utilizar valores de $MTTF_{dC}$ más elevados para los componentes individuales que forman parte del canal.

Esta restricción se establece porque se entiende que las SRP/CS para situaciones de riesgo elevado no deben depender exclusivamente de la fiabilidad de los componentes. En esos casos, se deben aplicar medidas adicionales tales como la redundancia y las comprobaciones internas.

Las gamas de $MTTF_{dCH}$ establecidas están basadas en las tasas de fallo encontradas en campo en el estado actual de la técnica.

$MTTF_{dCH}$	
Índice para cada canal	**Gama para cada canal**
Bajo	3 años ≤ $MTTF_{dCH}$ < 10 años
Medio	10 años ≤ $MTTF_{dCH}$ < 30 años
Alto	30 años ≤ $MTTF_{dCH}$ ≤ 100 años

Tabla 2. Tiempo medio hasta un fallo peligroso de cada canal ($MTTF_{dCH}$)

Cobertura del diagnóstico media (DC_{avg})

La cobertura del diagnóstico (DC) mide la efectividad de una prueba o comprobación sobre una unidad o parte de una unidad (un componente, un subsistema, una memoria de un subsistema programable, etc.) y se puede determinar como la relación entre la suma de las tasas de fallos peligrosos detectados y la suma de las tasas de fallos peligrosos potenciales de la unidad:

$$DC(\%) = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}} \cdot 100 = \frac{\sum \lambda_{dd}}{\sum \lambda_{d}} \cdot 100$$

donde λ_{dd} es la tasa de fallos peligrosos detectados, λ_{du} es la tasa de fallos peligrosos no detectados y $\lambda_d = \lambda_{dd} + \lambda_{du}$ es la tasa de fallos peligrosos totales.

Nota: Las siglas dd, du y d provienen del inglés y significan respectivamente: "dangerous detected", "dangerous undetected" y "dangerous".

Los sistemas relativos a la seguridad pueden utilizar varias medidas de prueba y comprobación para la detección de defectos (por ejemplo, una unidad de tratamiento puede usar dos señales antivalentes procedentes de una unidad de entrada redundante -dos sensores- y realizar una comprobación de verosimilitud para detectar cualquier defecto en uno de los sensores o en una de las líneas de interconexión o incluso cualquier puente entre líneas; una unidad de tratamiento electrónica puede incorporar una comprobación periódica de los contenidos de la memoria de programa para detectar alteraciones en las instrucciones programadas; una unidad de tratamiento que manda una válvula hidráulica puede utilizar una realimentación del estado de la válvula para comprobar si la válvula actúa tal y como se le ordena …).

Para obtener la cobertura del diagnóstico media de una SRP/CS, en primer lugar, se estiman las coberturas del diagnóstico de las pruebas individuales, a continuación se determinan las coberturas del diagnóstico de cada uno de los bloques o unidades que componen la SRP/CS, y por último, se aplica la fórmula de la DC_{avg}.

Nota: Una prueba generalmente actúa sobre el conjunto del bloque o unidad y se puede asignar el valor de la cobertura de la prueba al bloque. Si se aplican varias pruebas sobre un mismo bloque, la cobertura del bloque será al menos tan buena como la mejor cobertura individual. Y si las pruebas se complementan, se podría asignar una cobertura mejor al bloque. Sin embargo, es posible que las pruebas actúen sobre partes específicas de un bloque o unidad (por ejemplo, sobre la memoria de programa de un sistema electrónico programable). En estos casos, la cobertura del bloque será al menos la cobertura parcial más pobre. Siempre se puede calcular una cobertura media para el bloque si se dispone de las tasas de fallo parciales, del mismo modo que se calcula para el conjunto de la SRP/CS.

La DC media (DC_{avg}) para el conjunto de unidades que componen una SRP/CS, se estima mediante la siguiente fórmula:

$$DC_{avg}(\%) = \frac{\sum_{i=1}^{n} \frac{DC_i}{MTTF_{di}}}{\sum_{i=1}^{n} \frac{1}{MTTF_{di}}} \cdot 100$$

donde DC_i y $MTTF_{di}$ representan la cobertura del diagnóstico y el tiempo medio hasta el fallo peligroso de cada bloque o unidad respectivamente.

En esta fórmula se deben incluir todos los bloques o unidades de la SRP/CS, se comprueben o no, excepto aquellos a los que se les ha aplicado la exclusión de defectos ($MTTF_d = \infty$) y aquellos cuya función es exclusivamente de prueba o comprobación de bloques que intervienen en la función de seguridad.

Para la estimación de la DC de cada bloque o unidad se puede utilizar el análisis de los modos de fallo y sus efectos (FMEA, véase la norma UNE-EN 60812) u otros métodos similares. Si no se dispone de suficiente información para aplicar un método de análisis pormenorizado se puede aplicar el enfoque simplificado del anexo E de la norma.

En el procedimiento simplificado de estimación de la PFH (PL) se utiliza una DC media (DC_{avg}) para el conjunto de las unidades que integran una SRP/CS, que se clasifica en cuatro niveles (vease la Tabla 3).

DC_{avg}	
Indice	**Gama**
Nula	DC < 60 %
Baja	60 % ≤ DC < 90 %
Media	90 % ≤ DC < 99 %
Alta	99 % ≤ DC

Tabla 3. Cobertura del diagnóstico (DC_{avg})

Medidas contra fallos de causa común (CCF)

El último parámetro relevante para la cuantificación de la probabilidad de fallo (PFH) concierne a los fallos de causa común.

El fallo de causa común se define como el fallo de varios elementos, que resultan de un solo suceso y que no son consecuencia unos de otros (por ejemplo, el fallo de los dos canales de una SRP/CS redundante por causa de unas condiciones ambientales severas o sobrecargas que no fueron tratadas adecuadamente durante el diseño).

La susceptibilidad de un sistema a los fallos de causa común es difícil de estimar cuantitativamente. La norma, en su anexo F, ofrece un sistema de puntuación que consiste en obtener un mínimo de puntos (65 puntos de 100) mediante la aplicación de una serie de medidas de diseño que poseen unos valores asociados en función de la contribución de la medida a la reducción de los fallos de causa común (separación física entre los caminos de las señales de los diferentes canales - 15 puntos, utilización de diferentes tecnologías/principios de diseño o principios físicos en los canales - 20 puntos, etc.).

Estimación simplificada de la PFH (PL) de una SRP/CS

El procedimiento simplificado es el resultado de la aplicación de las técnicas de Markov a los diseños tipo o categorías.

Nota: En los cálculos realizados se han asumido las siguientes hipótesis:

- *Duración de la misión: 20 años*
- *Tiempo medio de reparación: 8 horas*
- *Tasa de fallo constante durante la misión*
- *Para la categoría 2, tasa de solicitación ≤ 1/100 de la tasa de verificación*
- *Para la categoría 2, $MTTF_{dTE}$ mayor que la mitad de $MTTF_{dL}$*

La representación gráfica (véase figura 7) permite una rápida estimación de la gama de PFH (PL) de una SRP/CS a partir de la determinación de los cuatro parámetros en el diseño realizado: la categoría, el $MTTF_d$ de cada canal, la DC_{avg} y, en caso de las categorías 2, 3 y 4, el grado de fortaleza del diseño frente a los CCF.

La operativa es muy sencilla: una vez comprobada la suficiencia de las medidas contra los CCF, se determina

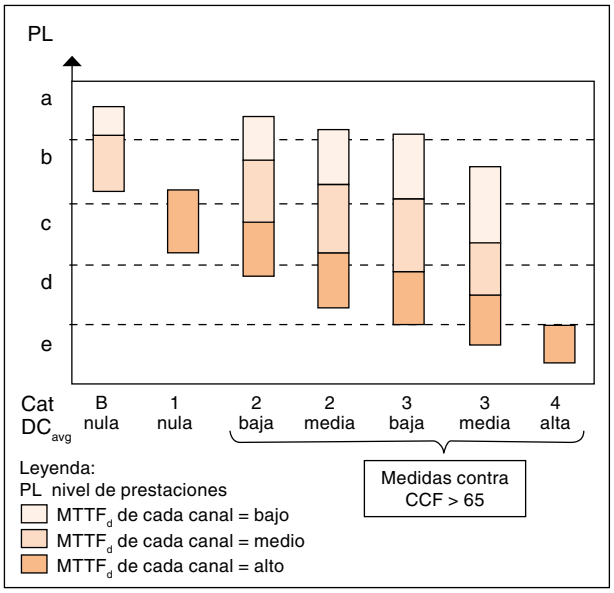


Figura 7. Relación entre las categorías, la DC_{avg}, el $MTTF_d$ de cada canal y la PFH (PL)

la barra correspondiente en el eje horizontal a partir de la categoría y el índice de DC_{avg} obtenido y, sobre dicha barra, se lleva el índice del $MTTF_d$ de cada canal obtenido, lo cual determina la gama de PFH (PL) en el eje vertical.

En el caso de una SRP/CS de categoría 2, además, habrá que comprobar que se cumplen las dos hipótesis asumidas específicamente para esta categoría en el procedimiento simplificado.

Si se requiere una estimación del valor numérico concreto de PFH, se puede utilizar la representación tabulada del anexo K de la norma.

Estimación de los aspectos cualitativos

El conjunto de medidas que se aplican contra los fallos sistemáticos se clasifican en:

- medidas tendentes a evitar fallos sistemáticos (impedir que se introduzcan) causados por errores cometidos en el sistema (hardware, software o documentación) durante cualquier fase del ciclo de vida de la SRP/CS y
- medidas dirigidas a controlar fallos sistemáticos (tolerar) durante el funcionamiento causados por errores que han podido filtrarse en el diseño después de aplicar las medidas anteriores. Además, se incluyen medidas para controlar los errores que pueden producirse durante la utilización del sistema (funcionamiento y mantenimiento).

Las medidas para evitar fallos sistemáticos son principalmente medidas de carácter procedimental y de organización, mientras que las medidas para el control son medidas técnicas que se incorporan en el sistema.

En el anexo G de la norma se han listado las medidas que deben aplicarse, sobre todo, durante el diseño, contra los fallos o defectos sistemáticos, las cuales se

completan con los principios de seguridad básicos y de eficacia probada (véase UNE-EN ISO 13849-2:2008).

Las medidas se clasifican en aquellas a utilizar con independencia del PL_r, siempre que sea pertinente, y aquellas a aplicar en función del PL_r y la complejidad de la SRP/CS.

El software relativo a la seguridad constituye una parte importante en las SRP/CS programables y, por esa razón, merece un tratamiento específico en la norma.

Se viene observando que el número de fallos del sistema provocados por errores de software está aumentando, en contraste con los defectos de origen físico, dada la cada vez mayor complejidad y tamaño de los programas.

La norma establece requisitos en función del tipo de software a desarrollar y el tipo de lenguaje de programación que se vaya a utilizar.

Entre los tipos de software, la norma distingue el software empotrado relativo a la seguridad (SRESW), es decir, el software inalterable (firmware) de los sistemas, que es desarrollado por técnicos que diseñan componentes de seguridad (por ejemplo, el software de una barrera inmaterial o el sistema operativo de un PLC de seguridad), y el software de aplicación relativo a la seguridad (SRASW) que es desarrollado por técnicos que diseñan aplicaciones como son las máquinas, utilizando componentes programables en el sistema de mando.

En cuanto al lenguaje de programación, se diferencia entre el uso de un lenguaje de variabilidad limitada (LVL), como es el lenguaje de diagrama de escalera de los PLCs, y un lenguaje de variabilidad total (FVL), como es el lenguaje ensamblador o el C.

El software SRASW, generalmente, se programa utilizando un lenguaje LVL y se deben cumplir los requisitos definidos en la norma para el software SRASW.

Por último, para el diseño del software de seguridad, la norma propone una variante simplificada del conocido modelo V (figura 8).

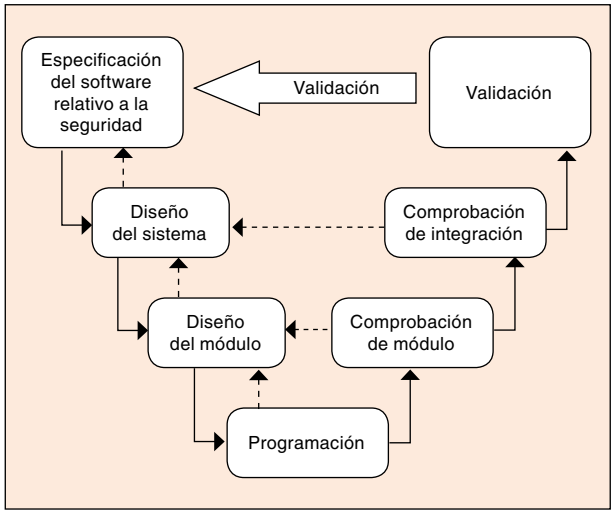


Figura 8. Modelo en V simplificado del ciclo de vida del software de seguridad

Etapa 4 Verificación del PL de la FS

En esta etapa se comprueba que el PL obtenido para cada SRP/CS que realiza la función de seguridad, tras estimar su probabilidad media de fallo aleatorio peligroso por hora (PFH) y comprobar la adecuación de las medidas contra los fallos sistemáticos, es mayor o igual que el PL_r especificado para dicha función de seguridad. En caso negativo, se debe rediseñar la SRP/CS correspondiente y proceder a una re-evaluación del PL.

Si la función de seguridad se implementa mediante varias SRP/CS, se debe calcular el PL global de la combinación de SRP/CS antes de llevar a cabo la verificación ($PL_{global} \geq PL_r$).

Combinación de SRP/CS para obtener un PL global

Con la introducción del concepto de PL, siempre es posible determinar un PL global para una combinación de SRP/CS, sean cuales sean las categorías y los PL individuales, resolviendo así el problema que planteaba la norma EN 954-1:1996 de la dificultad de asignar una categoría global a una combinación de SRP/CS con categorías diferentes.

La norma ofrece un método aproximado para combinaciones en serie de SRP/CS.

El método consiste en identificar el PL más bajo (PL_{low}) de la cadena, definir el número de las SRP/CS con dicho PL (N_{low}) y, con estos datos, entrar en la tabla (ver tabla 4) para determinar el PL_{global}.

Si se ha realizado una estimación más precisa de las prestaciones de seguridad de las SRP/CS y se dispone de los valores de probabilidad media de fallo peligroso por hora (PFH) de cada parte, la probabilidad media de fallo peligroso por hora de la combinación se puede calcular sumando todas las probabilidades de fallo individuales. Entrando en la tabla 11 de la norma con ese valor de probabilidad (PFH) se obtiene el PL_{global}.

PL_{low}	N_{low}	PL_{global}
a	> 3	Ningún PL, no autorizado
	≤ 3	a
b	> 2	
	≤ 2	b
c	> 2	
	≤ 2	c
d	> 3	
	≤ 3	d
e	> 3	
	≤ 3	e

Tabla 4. Cálculo del PL para SRP/CS alineadas en serie

En cuanto a los aspectos cualitativos (medidas no cuantificables) de la combinación de SRP/CS, al cumplirse que los PL individuales son al menos tan altos como el PL_{global}, se considera que las medidas adoptadas contra los fallos sistemáticos son adecuadas para la combinación. No obstante, se debe asegurar que los medios de interconexión de las SRP/CS (conductores, buses de comunicación de datos, etc.) se han considerado como parte de las SRP/CS y que las interfases de las mismas son compatibles.

Etapa 5 Validación

La última etapa del proceso de diseño consiste en demostrar que la implementación de la función de seguridad (la SRP/CS o la combinación de SRP/CS) responde a los requisitos de seguridad especificados, para lo cual se debe revisar el diseño y practicar las pruebas necesarias. La segunda parte de esta norma trata detalladamente este asunto (véase UNE-EN ISO 13849-2:2008).

BIBLIOGRAFÍA CONSULTADA

NORMA EN ISO 13849-1:2008
Seguridad de las máquinas. Partes de los sistemas de mandos relativas a la seguridad. Parte 1: Principios generales para el diseño

HAUKE M., SCHAEFER M., APFELD R. Y OTROS
Functional safety of machine controls – Application of EN ISO 13849 –
BGIA Report 2/2008e

TAMBORERO J.M.
Fiabilidad de componentes: la distribución exponencial
NTP 316 – Notas técnicas de prevención. Barcelona, INSHT, 1993

TAMBORERO J.M.
Fiabilidad: la distribución de Weibull
NTP 331 – Notas técnicas de prevención. Barcelona, INSHT, 1994

 NIPO: 272-13-015-4