INVASSAT

Institut Valencià de
Seguretat i Salut en el Treball

Riesgos asociados a los órganos de mando.

Castellón, 25 de abril de 2.013

CENTRO TERRITORIAL DEL INVASSAT DE CASTELLÓN

ANGEL DÍAZ RUIZ

Técnico de Seguridad y Salud en el Trabajo

GENERALITAT VALENCIANA
CONSELLERIA D'ECONOMIA, INDÚSTRIA, TURISME I OCUPACIÓ



R.D. 1215/1997, por el que se establecen las disposiciones mínimas de seguridad y salud para la utilización por los trabajadores de los equipos de trabajo

ANEXO I

Disposiciones mínimas aplicables a los equipos de trabajo

Apdo. 1 pto 1º párrafo 4º

Los ***sistemas de mando*** deberán ser seguros y elegirse teniendo en cuenta los posibles fallos, perturbaciones y los requerimientos previsibles, en las condiciones de uso previstas.



DEFINICIÓN

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball

Los órganos de accionamiento son todos aquellos elementos sobre los que actúa el operador para comunicar las órdenes a un equipo de trabajo, modificar sus parámetros de funcionamiento y seleccionar sus modos de funcionamiento y de mando o, eventualmente, para recibir informaciones.



Se trata, en general, de pulsadores, palancas, pedales, selectores, volantes y, en el caso de algunos equipos de trabajo (por ejemplo máquinas), de teclados y pantallas interactivas (control numérico).







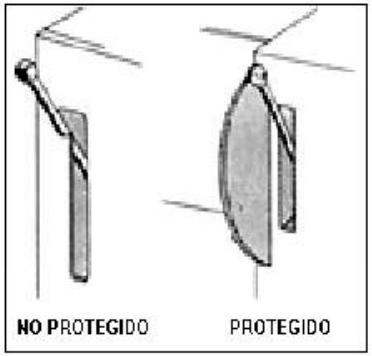


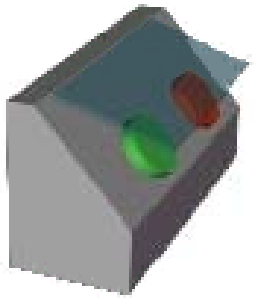


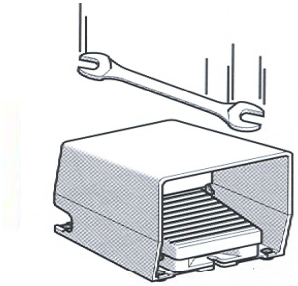
ÓRGANOS DE MANDO

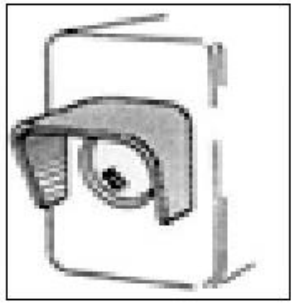
INVASSAT
Institut Valencià de Seguretat i Salut en el Treball

Todos aquellos órganos de mando que tengan alguna incidencia en seguridad deben estar **identificados y posicionados** de manera que se **dificulte un accionamiento erróneo** que pueda propiciar, bien un movimiento peligroso, o bien que una parada de un riesgo no se produzca con la suficiente rapidez.









Pulsadores encastrados

Pedal PROTEGIDO

Protecciones fijas o abatibles





Los colores de los mandos deben ser **normalizados (**Norma EN 60204. *Seguridad de las máquinas. Equipo eléctrico de máquinas)*.





MARCHA: BLANCO (Gris, negro o **verde**)

PARADA: NEGRO (gris, blanco o **rojo**)

PARADA EMERGENCIA: ROJO sobre amarillo

RESET o RESTABLECIMIENTO: AMARILLO

REARME: AZUL (blanco, gris o negro)

Nunca se admite un pulsador **verde** para una función **distinta de la puesta en marcha**, ni un pulsador **rojo** para una función **diferente de la parada o parada de emergencia**.

Si en una máquina se ha elegido un **color para una función** (blanco para la puesta en marcha…), **todos los pulsadores** que tengan esa función deberían tener ese **mismo color**.

SEÑALIZACIÓN

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball



Se utilizarán **pictogramas normalizados**.

Marcha / paro **0/1**

Movimiento a la izquierda.....←

Movimiento a la derecha .....→

Movimiento arriba.....↑

Movimiento abajo.....↓

Velocidades lenta / rápida **tortuga/liebre**



Indicaciones y pictogramas impresos de forma **indeleble**.

ARRANQUE o puesta en tensión/ON	PARADA o puesta fuera de tensión/OFF	Pulsadores que actúan alternativamente como botones ON o OFF y como botones ARRANQUE o PARADA	Pulsadores que actúan como botones ARRANQUE/ON mientras están presionados y como PARADA/OFF cuando están liberados (por ejemplo mando sensitivo)
IEC 60417-5007 (DB:2002-10)	IEC 60417-5008 (DB:2002-10)	IEC 60417-5010 (DB:2002-10)	IEC 60417-5011 (DB:2002-10)

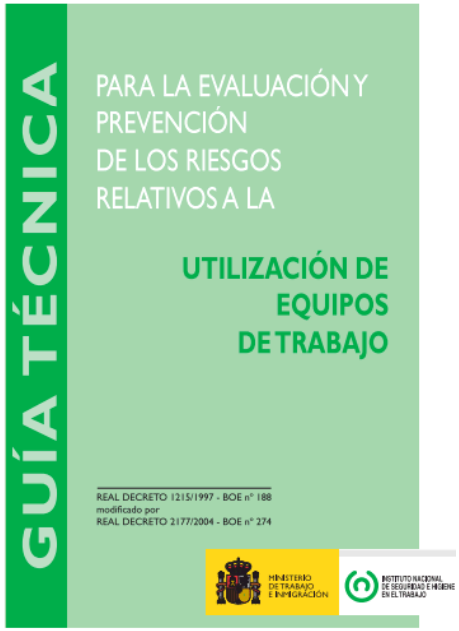
SEÑALIZACIÓN

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball





Se considera que un **sistema de mando cumple** los requisitos establecidos si, en general, todas sus funciones **cumplen los requisitos básicos aplicables** y además, **realiza la(s) función(es) de seguridad requerida(s),** de manera que ofrezcan unas prestaciones de seguridad adecuadas al nivel de riesgo.



Las prestaciones de seguridad se apoyan en el concepto de **categoría**.

De acuerdo con los resultados de la Evaluación de Riesgos.

GUÍA TÉCNICA R.D. 1.215/97

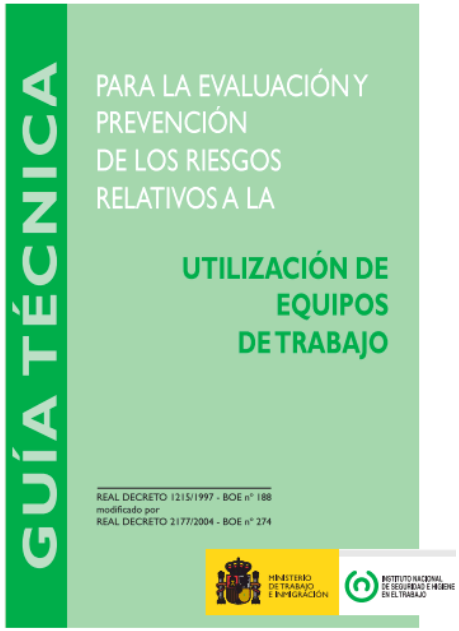
INVASSAT
Institut Valencià de Seguretat i Salut en el Treball

ANEXO I
DISPOSICIONES MÍNIMAS APLICABLES A LOS EQUIPOS DE TRABAJO

OBSERVACIÓN PRELIMINAR

Las disposiciones que se indican a continuación sólo serán de aplicación si el equipo de trabajo da lugar al tipo de riesgo para el que se especifica la medida correspondiente.

En el caso de los equipos de trabajo que ya estén en servicio en la fecha de entrada en vigor de este Real Decreto, la aplicación de las citadas disposiciones no requerirá necesariamente la adopción de las mismas medidas que las aplicadas a equipos nuevos.



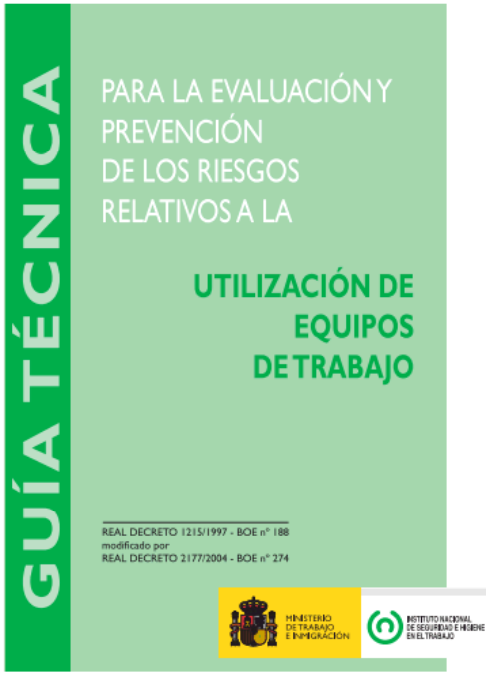
APÉNDICE F
ALCANCE Y SIGNIFICADO DE LAS OBSERVACIONES PRELIMINARES DE LOS ANEXOS I Y II

Las observaciones preliminares del Anexo I y del Anexo II establecen los **criterios fundamentales** que deben guiar la aplicación de las disposiciones mínimas establecidas en dichos anexos.

que se produzca un daño, con unas determinadas **consecuencias**. Por tanto, existe un **riesgo**.

Nota 2:
Si se toma la decisión de que es necesario reducir el riesgo

Los fallos en la alimentación de energía y los fallos en cualquiera de los elementos integrantes de las partes del sistema de mando que realizan funciones de seguridad pueden dar lugar a sucesos peligrosos motivados por:



– Puesta en marcha intempestiva.

– La variación incontrolada de ciertos parámetros del equipo de trabajo.

– La anulación de un dispositivo de protección

– La imposibilidad de parar un equipo

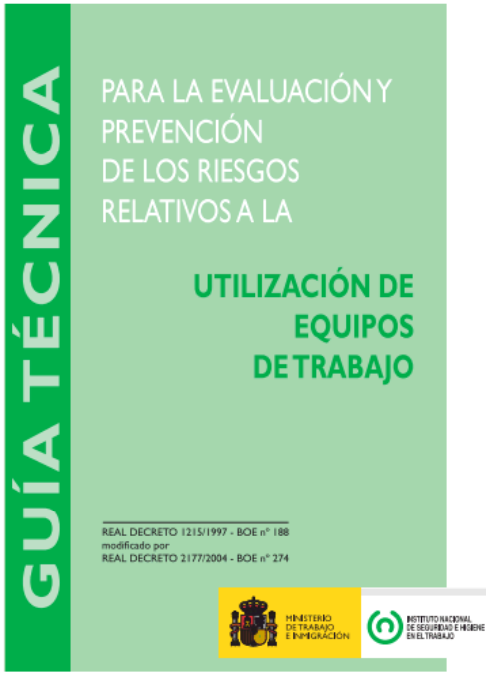
– La caída o proyección de elementos, etc

Se trata de conseguir, en primer lugar, que dichos fallos no se puedan producir;

Si esto no es posible, se tratará de que dichos fallos no provoquen un fallo de una función de seguridad:

a) Haciendo que la parte del sistema de mando correspondiente adopte un estado de seguridad, o

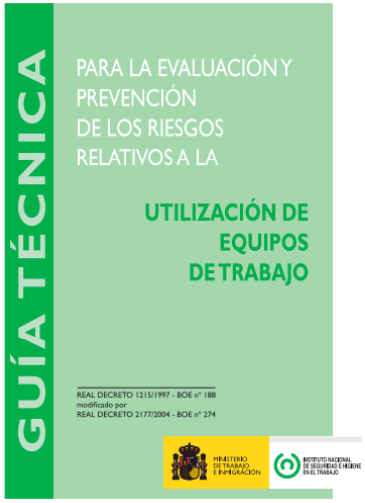
b) Garantizando la respuesta por la acción de otro elemento que ejerce la misma función de seguridad.



La experiencia demuestra que en muchas ocasiones estos objetivos se pueden alcanzar utilizando **técnicas, principios y componentes que han demostrado su eficacia a lo largo del tiempo en aplicaciones de la técnica de la seguridad (de eficacia probada)**

TÉCNICAS DE EFICACIA PROBADA

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball



Técnicas, principios y componentes de eficacia probada

- Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía
- Prevención de los sucesos peligrosos debidos a los fallos a masa
- Prevención de los sucesos peligrosos debidos a puentes entre conductores
- Prevención de los sucesos peligrosos originados por fallos en los sistemas electrónicos
- Enclavamientos de protección entre diferentes operaciones y movimientos contrarios
- Selección de las diversas formas de funcionamiento o de mando de un equipo de trabajo
- Prevención de los peligros generados al sobrepasar ciertos límites
- Acción mecánica positiva

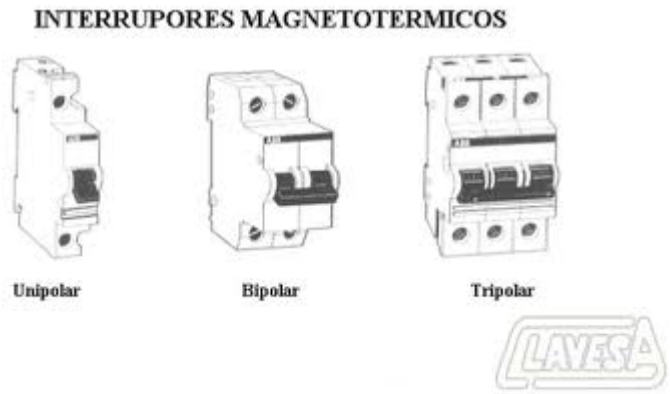
Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía

Las **variaciones de energía** en los circuitos de mando, como pueden ser:

Sobreintensidades,



Interruptores magnetotérmicos



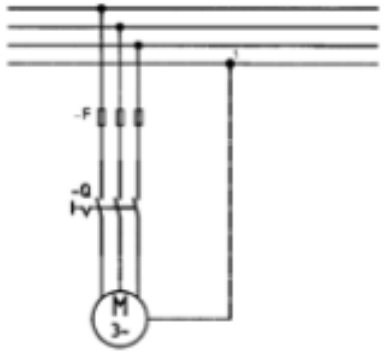
Sobrepresiones o las caídas de presión en los circuitos hidráulicos y/o neumáticos





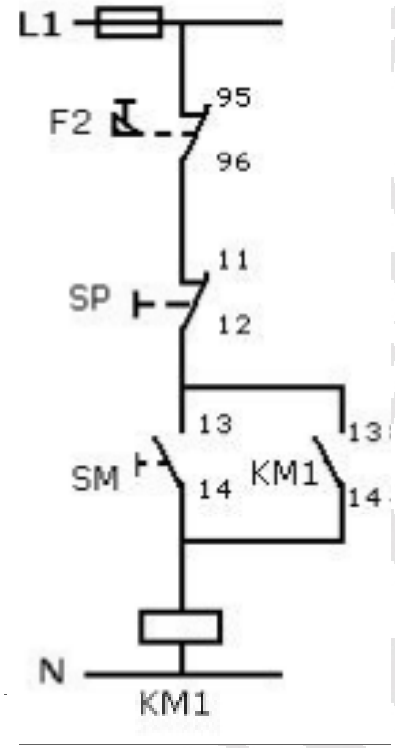
Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía

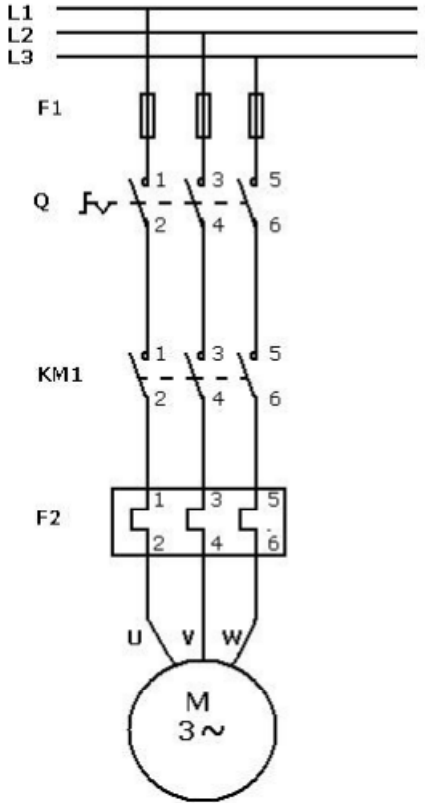
Para evitar que se produzcan sucesos peligrosos, por ejemplo un arranque intempestivo, **al restablecerse la alimentación de energía** de un circuito de mando, después de que aquélla se haya interrumpido o haya variado



a)







Fusibles

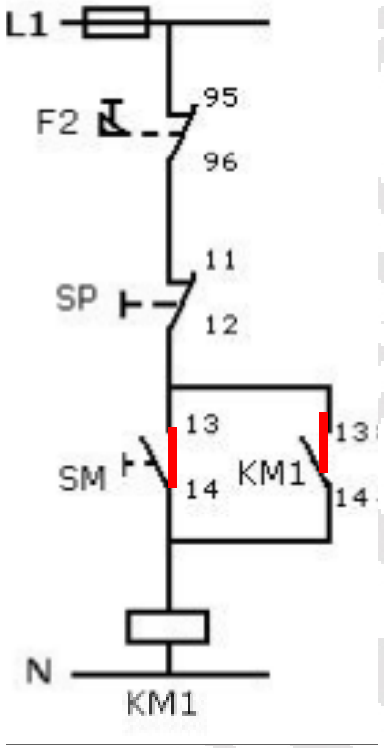
Interruptor

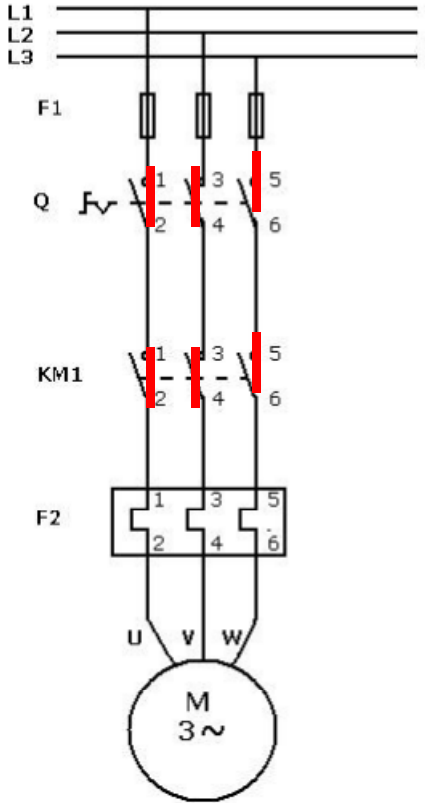
Contactor

Relé térmico

Motor

Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía





Fusibles

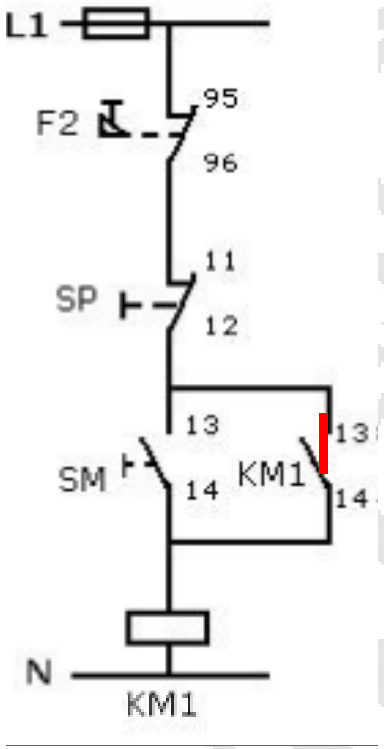
Interruptor

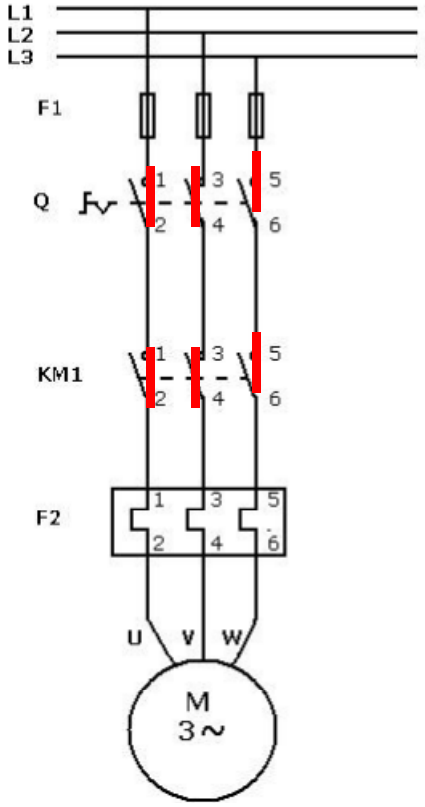
Contactor

Relé térmico

Motor

Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía





Fusibles

Interruptor

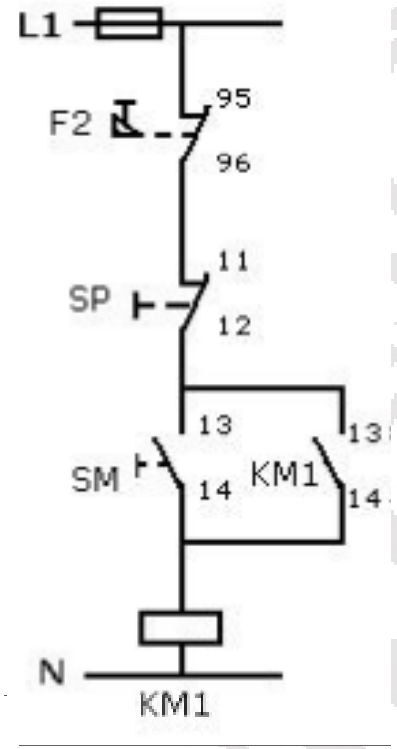
Contactor

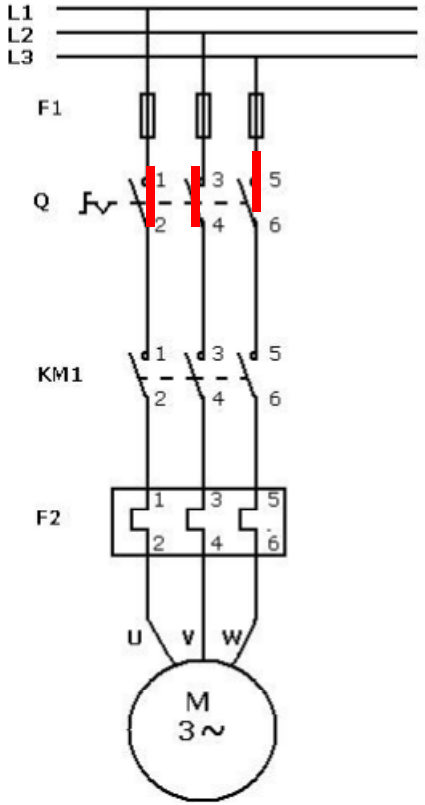
Relé térmico

Motor

Prevención de sucesos peligrosos debidos a los fallos en la alimentación de energía

Para evitar que se produzcan sucesos peligrosos, por ejemplo un arranque intempestivo, **al restablecerse la alimentación de energía** de un circuito de mando, después de que aquélla se haya interrumpido o haya variado





Fusibles

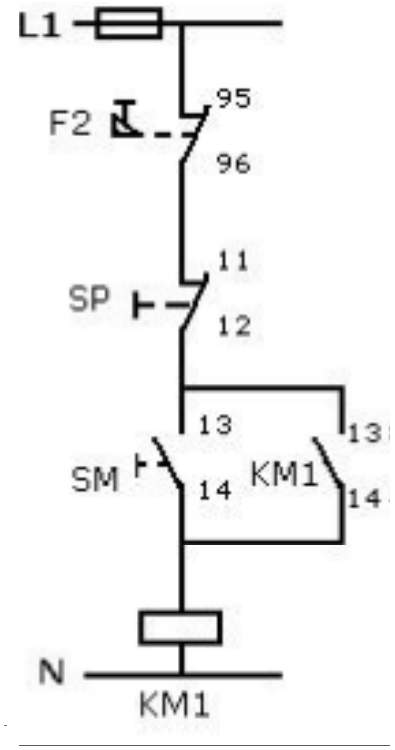
Interruptor

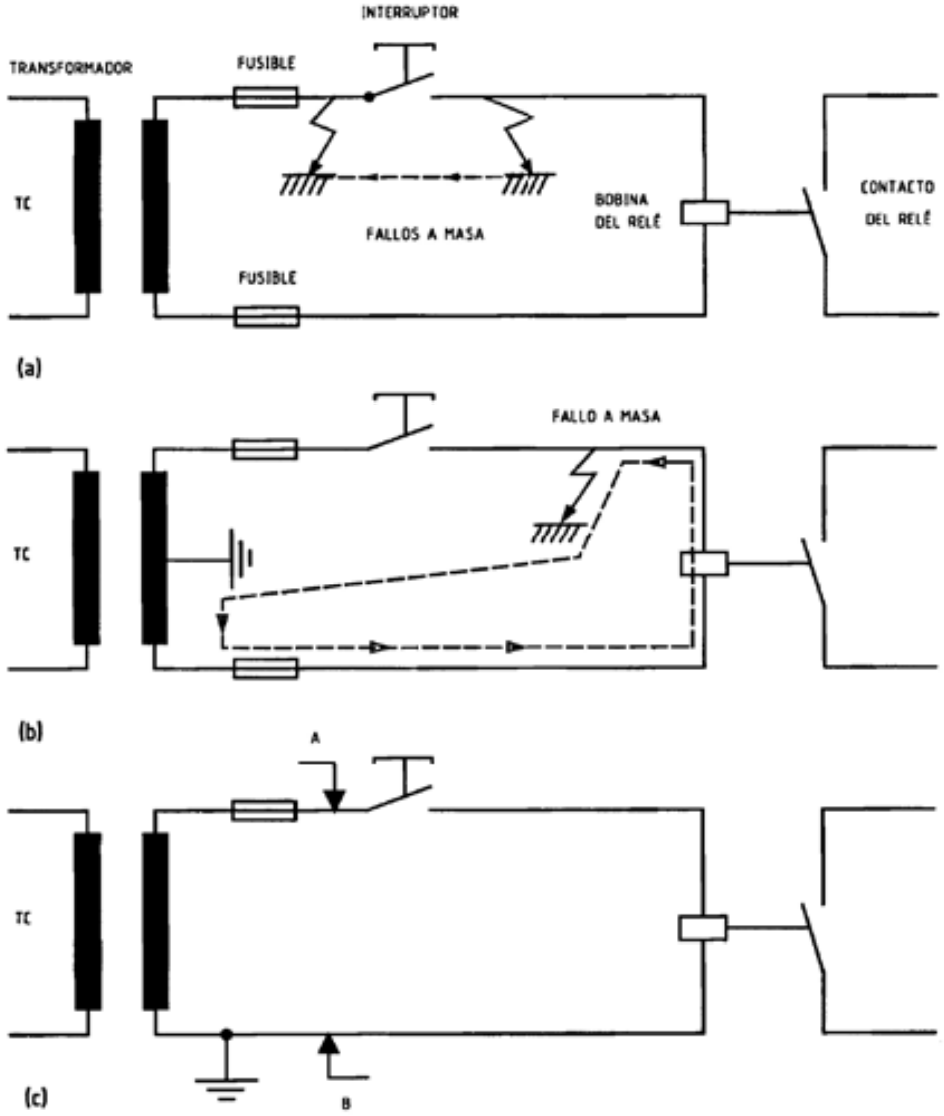
Contactor

Relé térmico

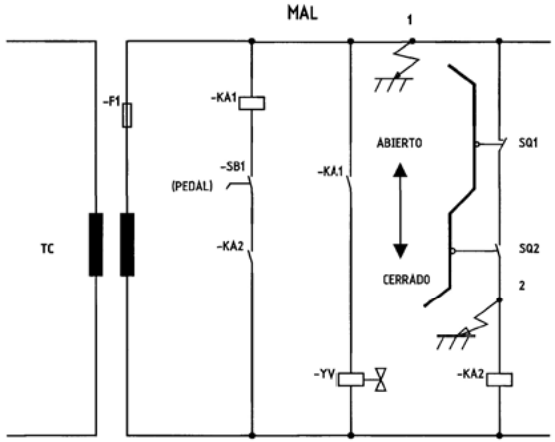
Motor

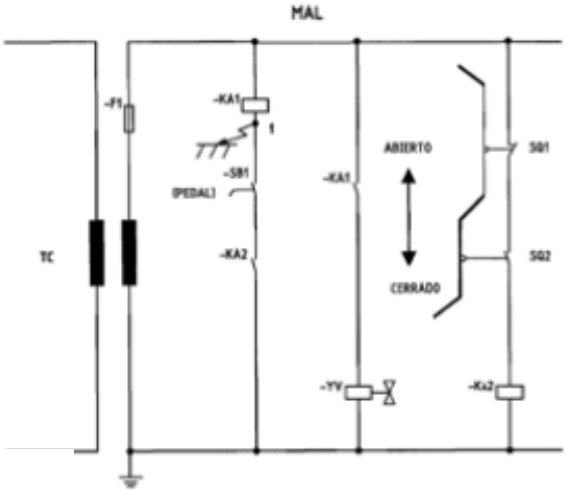
Prevención de los sucesos peligrosos debidos a los fallos a masa

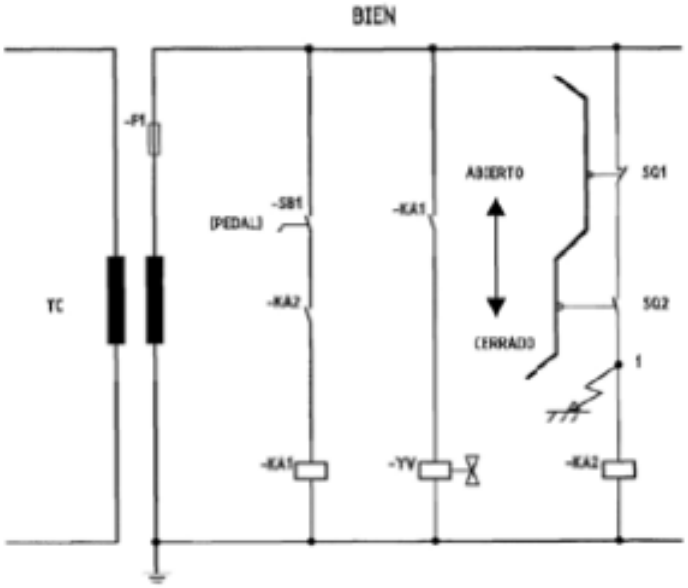




Prevención de los sucesos peligrosos debidos a puentes entre conductores







Prevención de los sucesos peligrosos originados por fallos en los sistemas electrónicos

Cuando se utilizan **sistemas electrónicos programables en funciones relativas a la seguridad**, es preciso tener en cuenta que el hecho de que sean reprogramables permite modificar, o anular incluso, las funciones de seguridad iniciales del equipo de trabajo, en general de una manera más fácil que con la técnica electromecánica.

Además, pueden tener una serie de fallos en ciertos casos aún no muy bien conocidos. Finalmente pueden ser muy influenciados por otros fenómenos a los que los componentes electromecánicos son insensibles como, por ejemplo: campos magnéticos, descargas electrostáticas, calor, puntas de tensión en la red, microcortes de tensión, etc.

Prevención de los sucesos peligrosos originados por fallos en los sistemas electrónicos

Elevador vertical

Presillas de sujeción



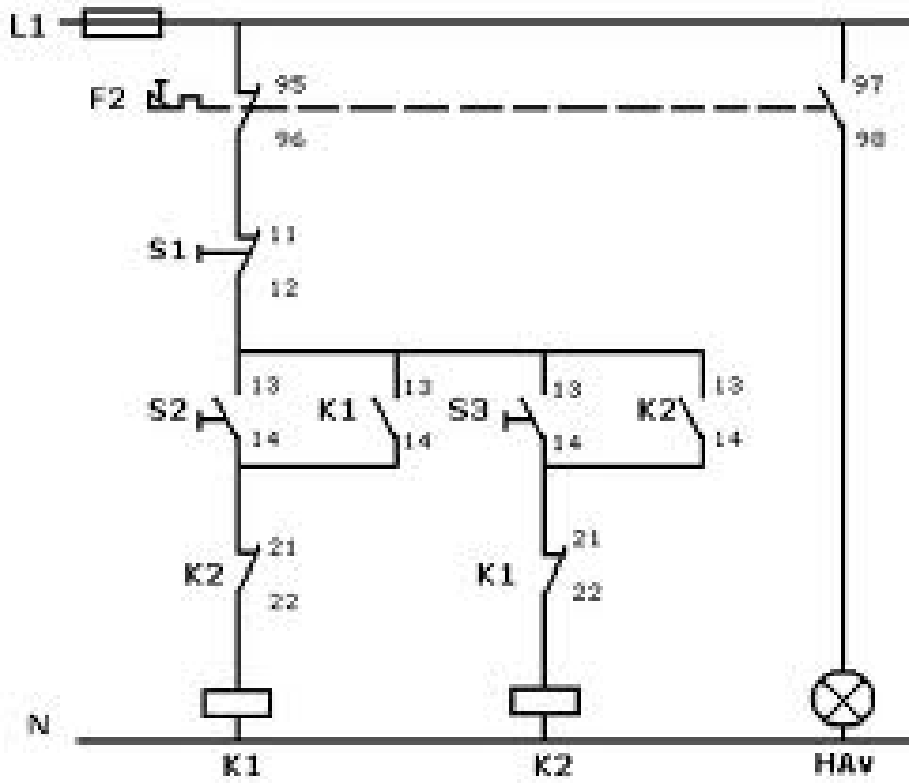
Transportador horizontal

Zona a desmontar

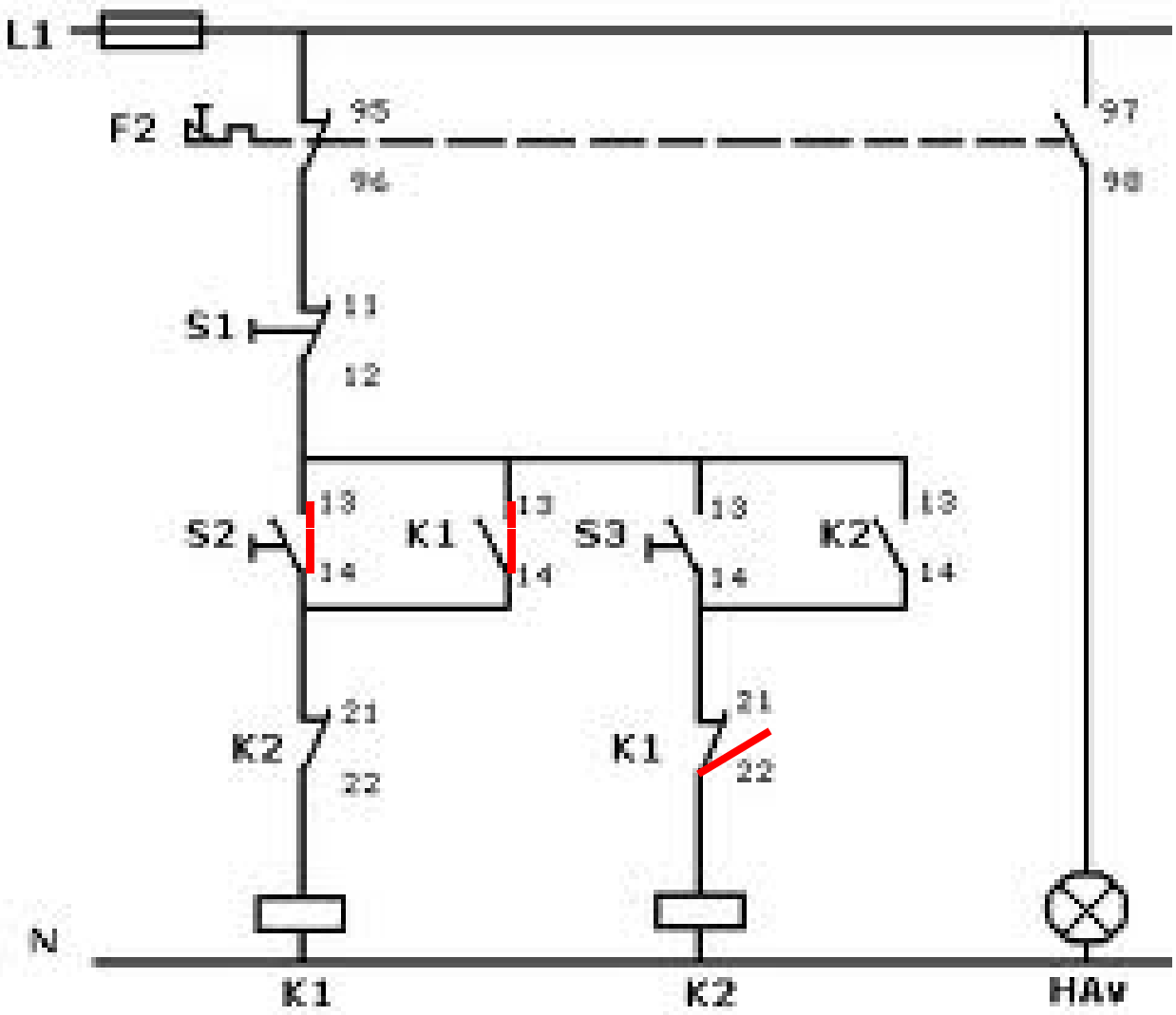


Enclavamientos de protección entre diferentes operaciones y movimientos contrarios

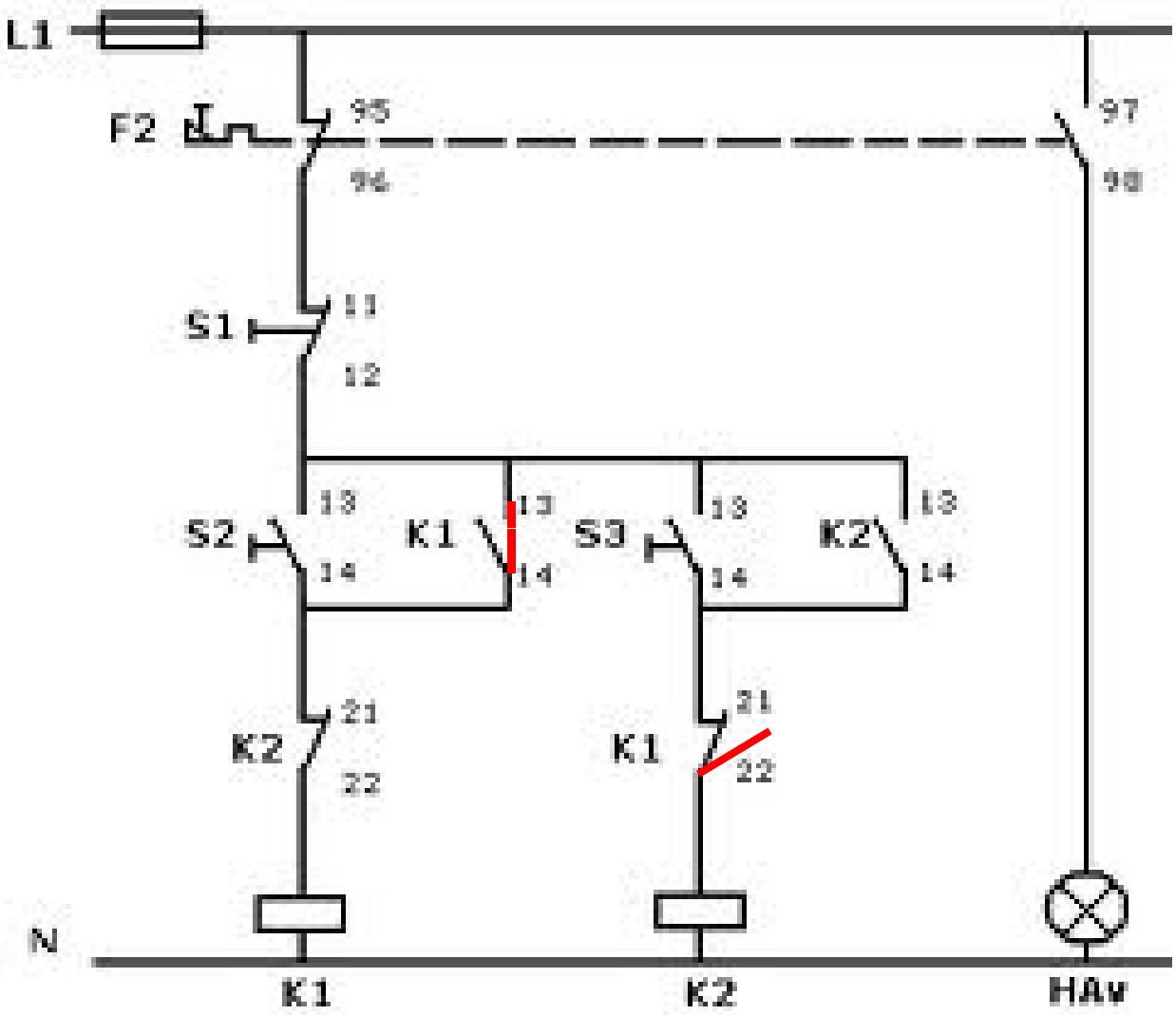
Cuando la **ejecución errónea de una secuencia** de ciertos elementos o de ciertas funciones del equipo de trabajo pueda dar lugar a sucesos peligrosos se deben prever los enclavamientos precisos para garantizar que dichos elementos o funciones se realizan de manera coordinada.



Enclavamientos de protección entre diferentes operaciones y movimientos contrarios



Enclavamientos de protección entre diferentes operaciones y movimientos contrarios



Selección de las diversas formas de funcionamiento o de mando de un equipo de trabajo

Cuando un equipo de trabajo puede **funcionar según diversas formas de mando o de funcionamiento y el cambio a una u otra forma de mando o de funcionamiento puede dar lugar a peligros o a situaciones peligrosas de diferente nivel de riesgo**, es preciso dotarlo de un **dispositivo que permita seleccionar las diferentes formas de mando o de funcionamiento y que se pueda bloquear en cada posición mediante una llave**.

Dicho dispositivo se puede sustituir por otros medios de eficacia similar (por ejemplo, códigos de acceso).



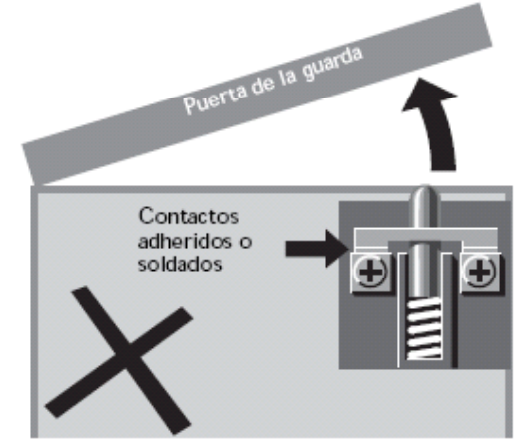
Prevención de los peligros generados al sobrepasar ciertos límites

En ciertos equipos de trabajo sobrepasar ciertos límites establecidos puede originar peligros para las personas.

Son ejemplos de estos límites:

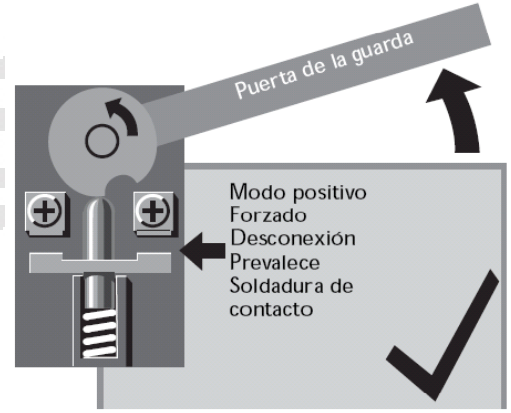
– el límite de presión en un recipiente sometido a presión;
– el límite de temperatura en un reactor;
– el límite de velocidad en una rectificadora o en un esmeril fijo;
– el límite de recorrido o de final de ciclo en una máquina (parada en punto muerto superior de una prensa excéntrica en funcionamiento golpe a golpe, cuando se alimenta o se extrae manualmente la pieza).

En estos casos se deben tomar las medidas preventivas apropiadas para garantizar que no se sobrepasan esos límites; estas medidas deben ser adecuadas al nivel de riesgo que presenta la situación peligrosa considerada



5

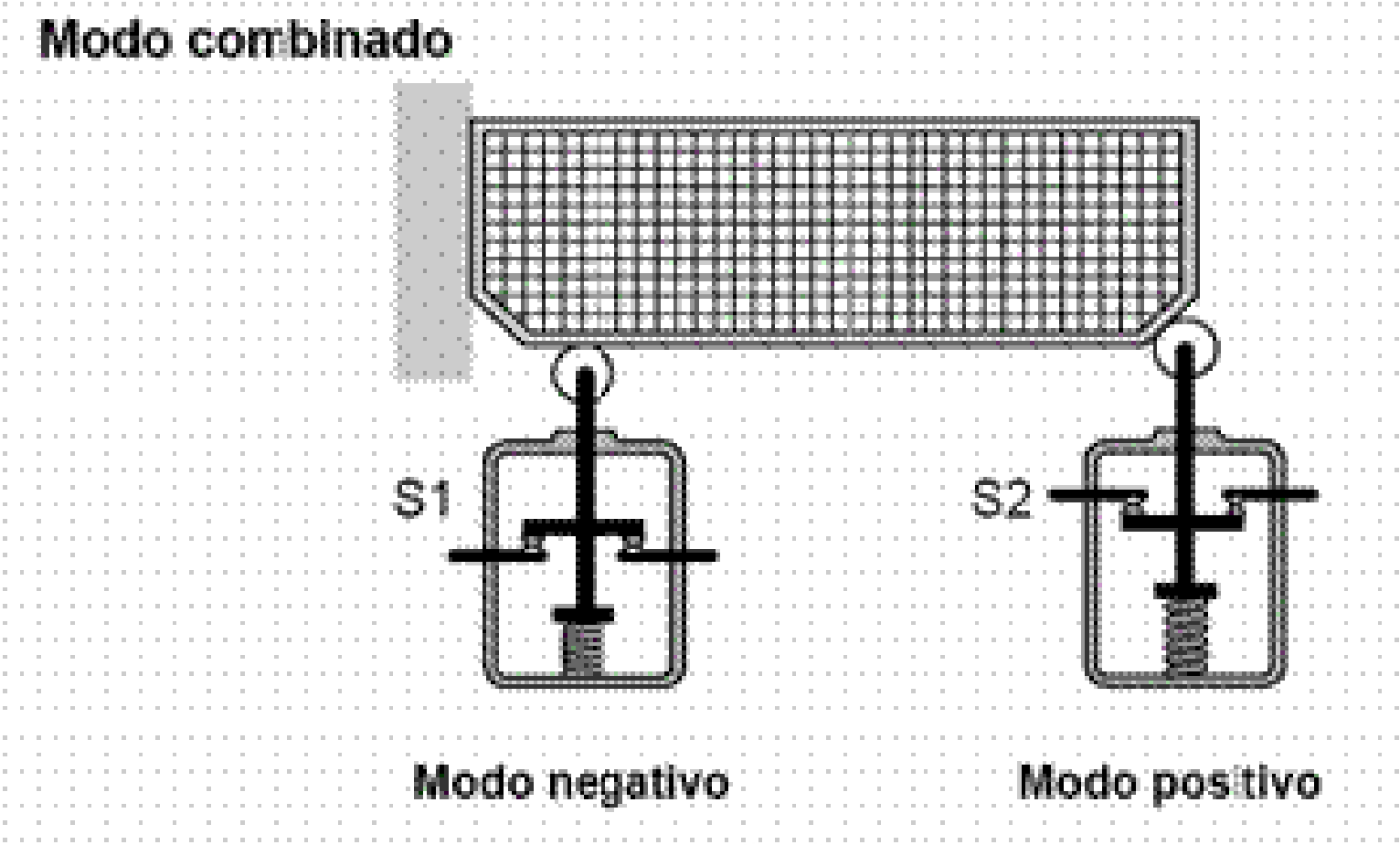
Sistema operativo en modo negativo (o no positivo) típico.



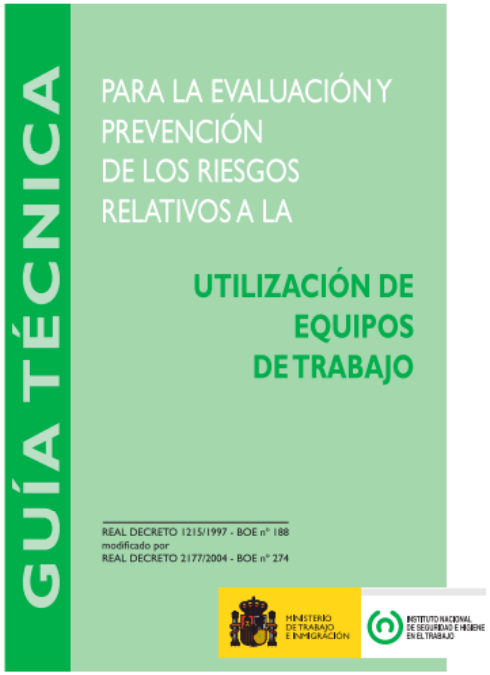
6

Sistema operativo en modo positivo típico.

Acción combinada

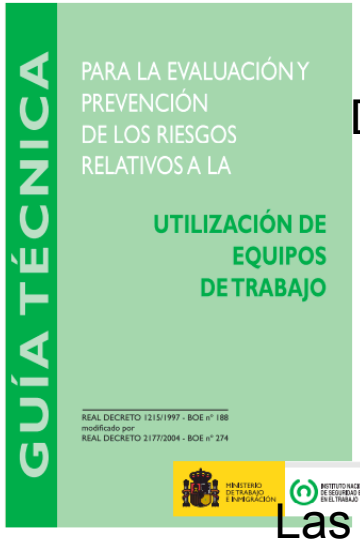


A efectos de los criterios desarrollados en el Apéndice H de la Guía Técnica, conviene indicar que hasta el **31/12/2011** se mantiene la presunción de conformidad de la norma EN 954–1, que establece las categorías de las partes de los sistemas de mando relativas a la seguridad, con los requisitos esenciales de seguridad y salud pertinentes de la Directiva de Máquinas.



A partir de dicha fecha solamente estará en vigor la norma **EN 13849–1**.





ANEXO I
DISPOSICIONES MÍNIMAS APLICABLES A LOS EQUIPOS DE TRABAJO

OBSERVACIÓN PRELIMINAR

Las disposiciones que se indican a continuación sólo serán de aplicación si el equipo de trabajo da lugar al tipo de riesgo para el que se especifica la medida correspondiente.

En el caso de los equipos de trabajo que ya estén en servicio en la fecha de entrada en vigor de este Real Decreto, la aplicación de las citadas disposiciones no requerirá necesariamente la adopción de las mismas medidas que las aplicadas a equipos nuevos.



La primera etapa consiste en evaluar el riesgo de la máquina en la zona protegida por la función de seguridad que se esté analizando.

PL: "*nivel de prestaciones*", expresa la probabilidad de fallo peligroso en una hora.

En la evaluación de riesgos se determina el nivel de prestaciones requerido, **PLr** , por la función de seguridad a estudio.

Atención: se debe tener en cuenta que dicha norma debe aplicarse a todas y cada una de las funciones de seguridad de que disponga la máquina. Ejemplo:

- **Parada de emergencia**
- **Enclavamiento con resguardos móviles**
- **Etc,**

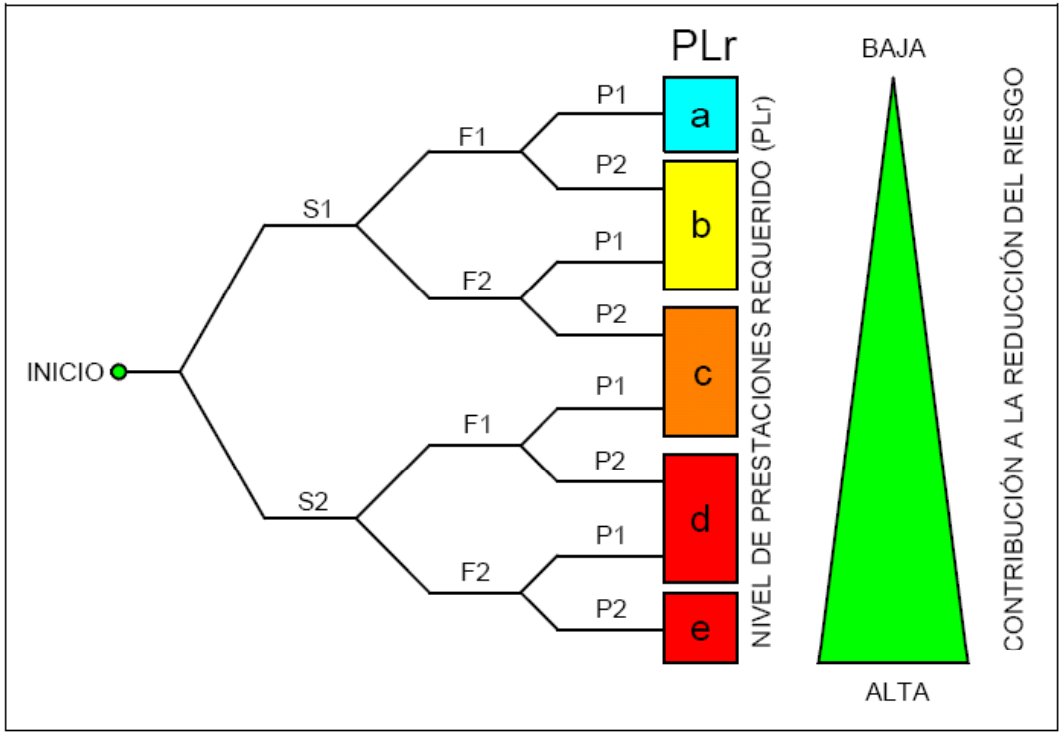


Figura 1: *Gráfico del riesgo para determinar el nivel de prestaciones requerido (PLr) para cada función de seguridad. (Figura A.1 de UNE EN 13849-1).*

Parámetros de riesgo	
S1	Lesión leve (normalmente reversible).
S2	Lesión grave (normalmente irreversible, incluyendo la muerte).
F1	Raro a bastante frecuente y/o corta duración de la exposición.
F2	Frecuente a continuo y/o larga duración de la exposición.
P1	Posible de evitar en determinadas condiciones.
P2	Raramente posible de evitar.

Tabla 1: *Parámetros del riesgo.*

Una vez determinado el **PLr** debe encontrarse el

PL: Nivel de prestaciones alcanzado del sistema diseñado.

PARA ESTIMAR EL **PL** SE NECESITA CONOCER LOS SIGUIENTES PARÁMETROS:

1 – La "***Categoría***" de control (se obtiene a partir de su arquitectura, la detección de defectos y / o su fiabilidad)

2 - El valor **MTTFd**: ***Tiempo medio hasta un fallo peligroso*** (valor probable de la duración media hasta un fallo peligroso)

3 - **DC**: La "***Cobertura del diagnóstico***" (medida de la efectividad del diagnostico: relación entre tasa de fallo de los fallos peligrosos detectados y la tasa de fallo del total de fallos peligrosos)

4 - **CCF**: El "***Fallo de causa común***" (fallo de varios elementos, que común resultan de un solo suceso y que no son consecuencia unos de otros)

CATEGORÍAS

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball

La categoría designada hace referencia al **nivel de fiabilidad** de la parte del circuito de mando relacionada con la función de seguridad.

La **fiabilidad** se refiere a la **capacidad de detección de los fallos que puede presentar la función de seguridad**, fallos que podrían ocasionar la inoperatividad o pérdida de la misma cuando sea demandada.

La categoría depende del diseño y construcción del circuito que desarrolla la función de seguridad.

La norma UNE-EN ISO 13849-1 contempla 5 posibilidades de categoría designada que de menos a más fiabilidad o capacidad de detección de fallos son: B, 1, 2, 3 y 4.

La categoría B es la categoría más básica y designa una probabilidad de fallo mayor, mientras que la categoría 4 indica que la probabilidad de fallo es muy baja.

Las categorías B y 1 se basan en la prevención de fallos mientras que las categorías 2 a 4 se basan además en la detección de los mismos.

Cualquier sistema que desarrolla una función de seguridad en una máquina puede ser dividido en componentes básicos o "subsistemas".

Cada subsistema tiene su propia función discreta. La mayoría de los sistemas pueden ser divididos en tres funciones básicas: entrada, lógica y salida (algunos sistemas simples de categoría B y 1 pueden no tener función lógica).

Los grupos de componentes que implementan estas funciones son los subsistemas.

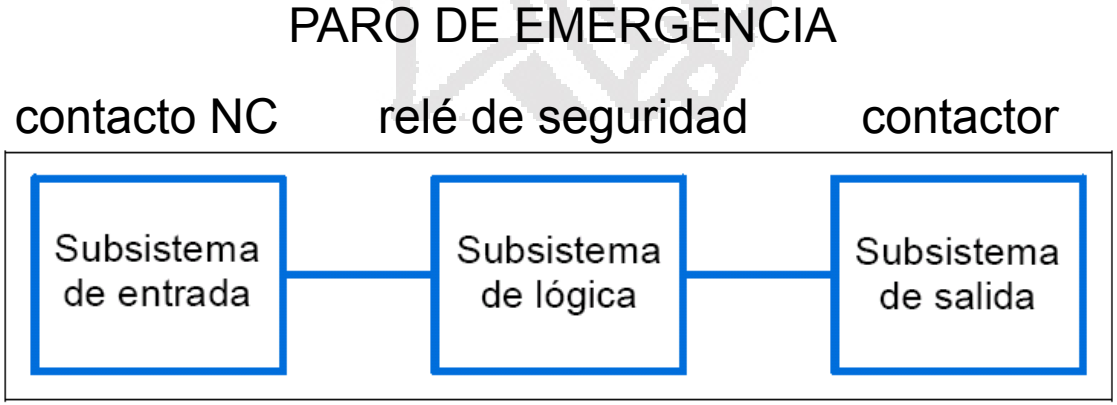


Figura 2: *Componentes básicos de un sistema que desarrolla una función de seguridad.*

Categoría B.

La categoría B requiere la aplicación de los principios de seguridad básicos.

La norma UNE-EN ISO 13849-2 indica los principios de seguridad básicos para sistemas eléctricos, neumáticos, hidráulicos y mecánicos. Los principios eléctricos se resumen de la siguiente manera:

- Correcta selección, combinación, configuración, montaje e instalación de los componentes (es decir, según las instrucciones del fabricante).
- Compatibilidad de componentes con tensiones e intensidades.
- Resistencia a las condiciones ambientales.
- Supresión de transitorios.
- Reducción del tiempo de respuesta.
- Protección contra arranques inesperados.
- Instalación segura de dispositivos de entrada (por ejemplo, instalación de dispositivos de enclavamiento).
- Protección del circuito de control.
- Correcta conexión equipotencial de protección.

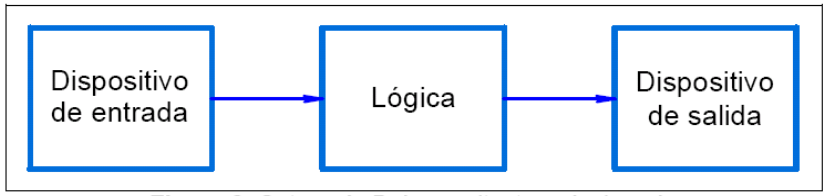


***Figura 3**: Categoría B de arquitectura designada.*

El sistema o subsistema puede fallar en el caso de un fallo único.

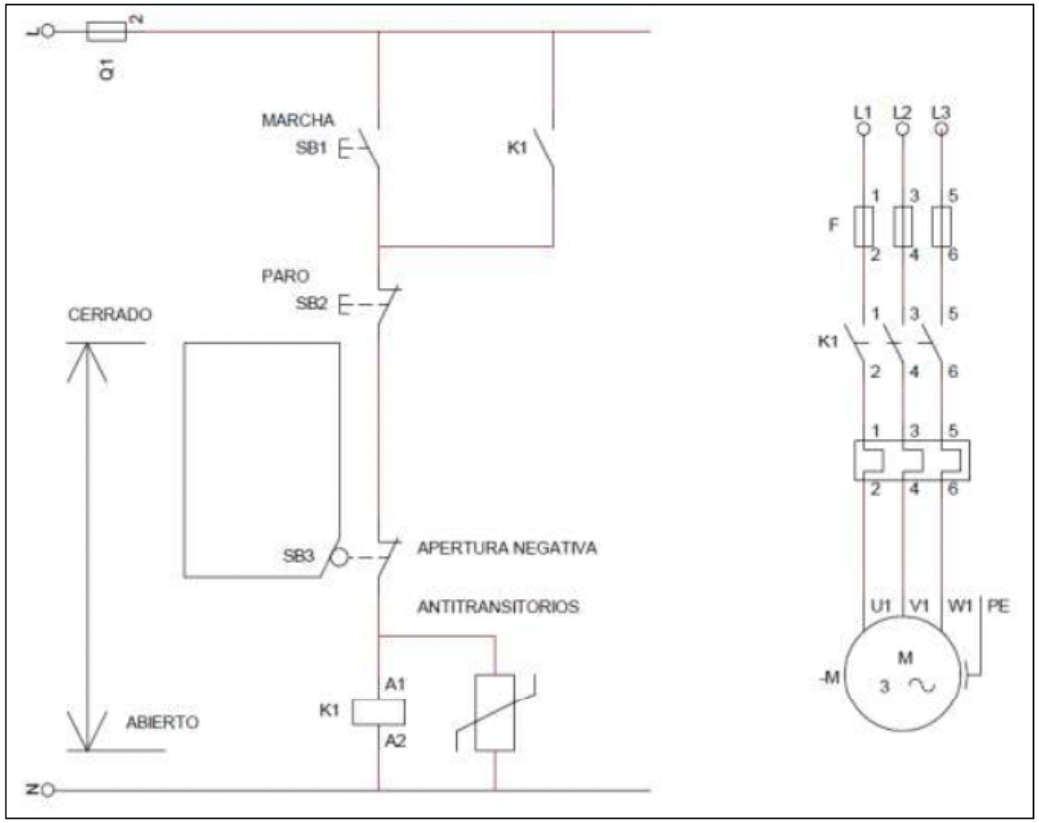


***Figura 4**: Esquema de categoría B para el enclavamiento de un resguardo.*

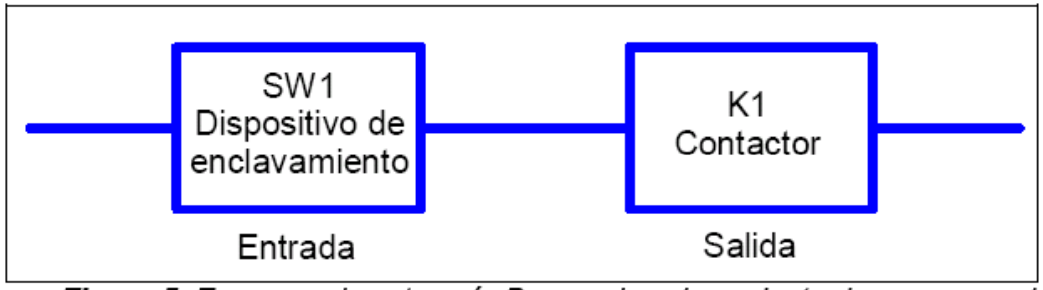


***Figura 5**: Esquema de categoría B para el enclavamiento de un resguardo.*

Categoría 1.

La categoría 1 requiere que el sistema que desarrolla una función de seguridad cumpla con los requisitos de la categoría B, y además, requiere la utilización de componentes de seguridad de eficacia probada.

La categoría 1 de arquitectura designada tiene la misma estructura que la categoría B e igualmente puede fallar en el caso de un fallo único.

Sin embargo, debido a que también debe utilizar *principios de seguridad y componentes de eficacia probada*, la probabilidad de fallo es menor que para la categoría B.

En la norma UNE-EN ISO 13849-2 se encuentra una lista no exhaustiva de componentes de eficacia probada para los sistemas mecánicos, hidráulicos, neumáticos y eléctricos. En la tabla siguiente se describen los componentes eléctricos. También se mencionan las normas según las cuales los componentes deben haber sido ensayados.

COMPONENTE DE EFICACIA PROBADA	NORMAS
Interruptor con accionamiento de modo positivo (acción de abertura directa).	IEC 60947-5-1
Dispositivo de parada de emergencia ISO 13850, IEC 60947.	ISO 13850, IEC 60947-5-5
Fusible.	IEC 60269-1
Interruptor automático.	IEC 60947-2
Contactores.	IEC 60947-4-1, IEC 60947-5-1
Contactos unidos mecánicamente.	IEC 60947-5-1
Contactor auxiliar (por ejemplo: contactor, relé de control, relés guiados mecánicamente).	EN 50205, IEC 60204-1, IEC 60947-5-1
Transformador.	IEC 60742
Cable.	IEC 60204-1
Dispositivos de enclavamiento.	ISO 14119
Termostato.	IEC 60947-5-1
Presostato.	Requisitos de sistemas neumáticos o hidráulicos más IEC 60947-5-1
Dispositivo o equipo de maniobra y protección (SCP).	IEC 60947-6-2
Controlador lógico programable.	IEC 61508, IEC 62061

Tabla 2: *Componentes de eficacia probada (véase EN ISO 13849-2)*

El diagrama de bloques de la categoría 1 tiene igual representación que en el caso de la categoría B.

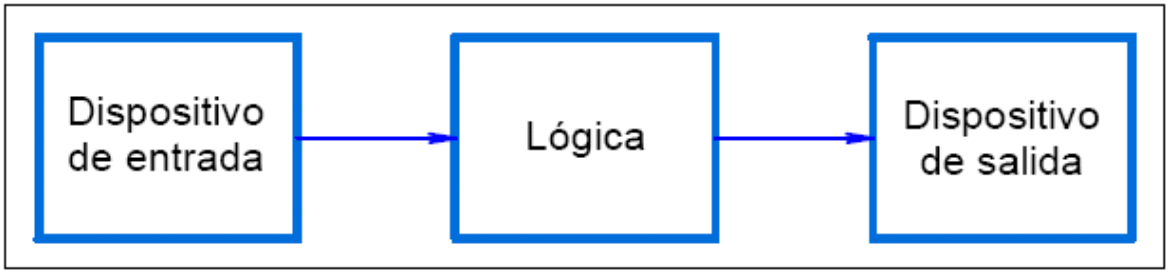


***Figura 6**: Categoría 1 de arquitectura designada.*

Esquema del mismo ejemplo utilizado en el caso de la categoría B pero adaptado a categoría 1. La diferencia fundamental se encuentra en el dispositivo de enclavamiento que debe ser de apertura positiva.

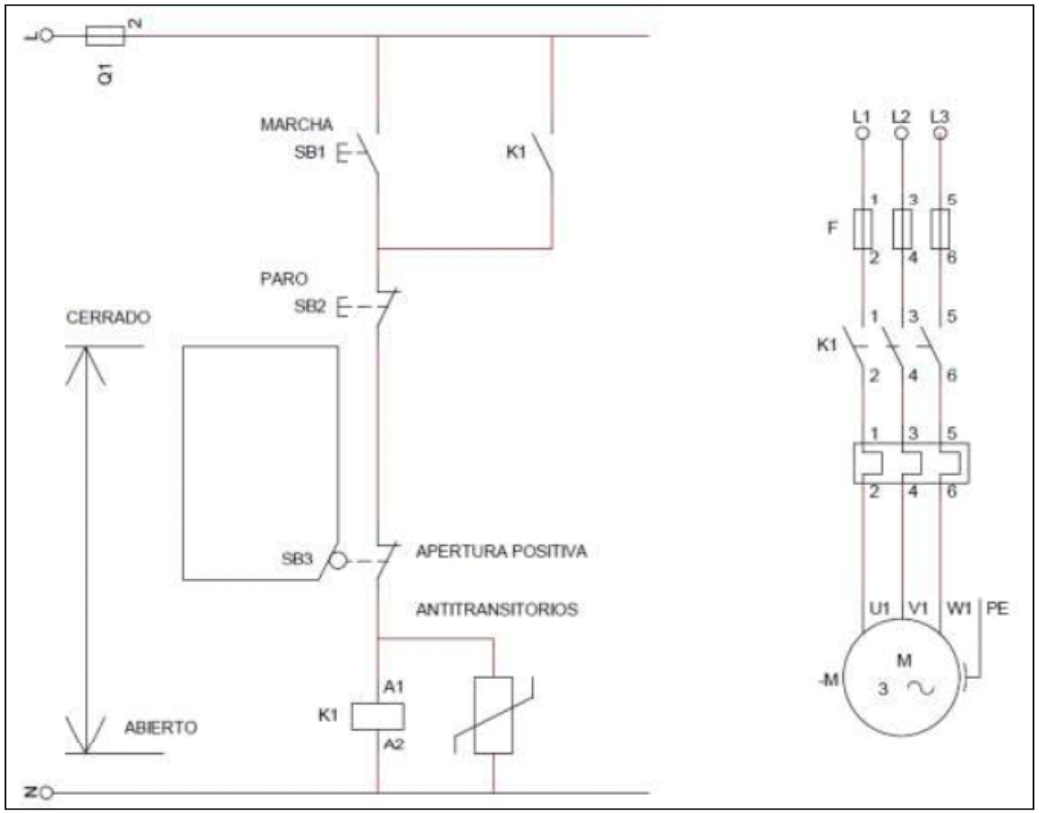


***Figura 7**: Esquema de categoría 1 para el enclavamiento de un resguardo.*

Con los componentes debidamente probados, la probabilidad de que se pierda la función de seguridad es menor en la categoría 1 que en la categoría B.

El uso de componentes de eficacia probada está diseñado para evitar la pérdida de la función de seguridad.

Utilizando técnicas y componentes de eficacia probada.

Categoría 2.

La **categoría 2** debe usar principios de seguridad básicos y principios de eficacia probada.

Además debe existir una monitorización de diagnóstico mediante una prueba funcional del sistema o del subsistema.

La prueba debe realizarse durante la puesta en marcha y luego periódicamente con una frecuencia que sea igual o mayor a **cien pruebas** para cada demanda de la función de seguridad.

Por ejemplo, si se prevé que la apertura de un resguardo se va a necesitar con una frecuencia de una vez por hora, el diagnóstico de la función debe realizarse al menos 100 veces por hora.

El sistema o subsistema, al igual que en las categorías B y 1, puede fallar si ocurre un fallo único entre las pruebas funcionales pero esto es normalmente menos probable que para la categoría 1.

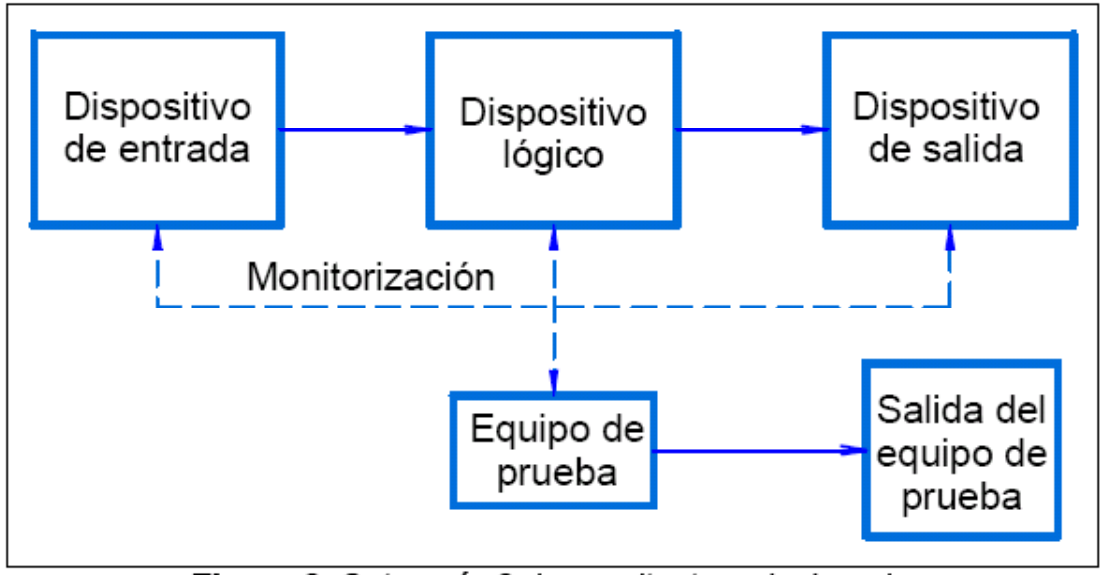


***Figura 8**: Categoría 2 de arquitectura designada.*

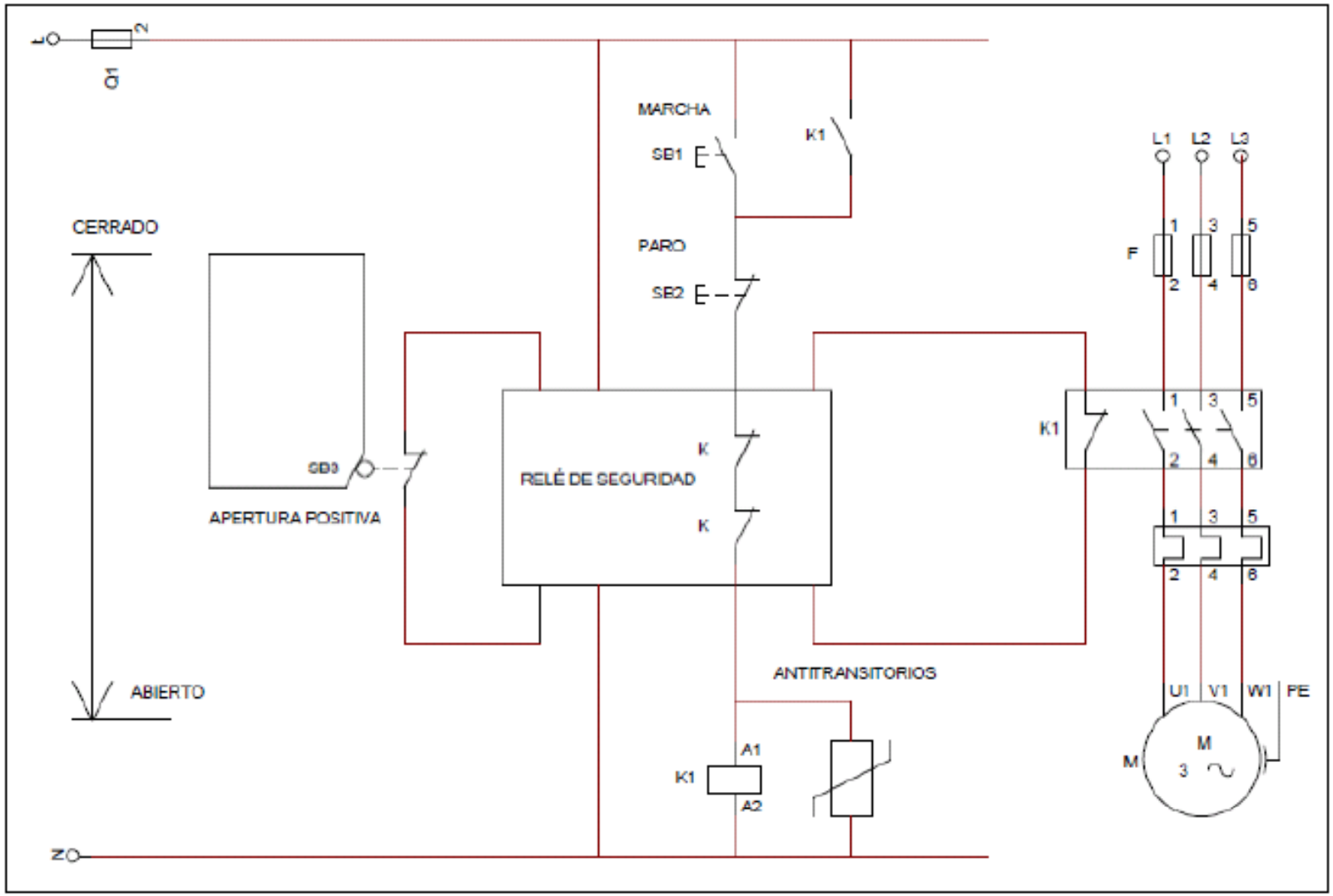


***Figura 9**: Esquema de categoría 2 para el enclavamiento de un resguardo.*

Categoría 3.

La categoría 3 de arquitectura designada debe usar principios de seguridad básicos, al igual que todas las categorías anteriores y principios de eficacia probada, al igual que las categorías 1 y 2.

Además existe el requisito de que no debe perderse la función de seguridad en el caso de un fallo único en el sistema/subsistema.

Esto significa que el sistema/subsistema debe tener tolerancia a fallos simples con respecto a su función de seguridad.

La forma más habitual de cumplir este requisito es utilizar una arquitectura de doble canal.

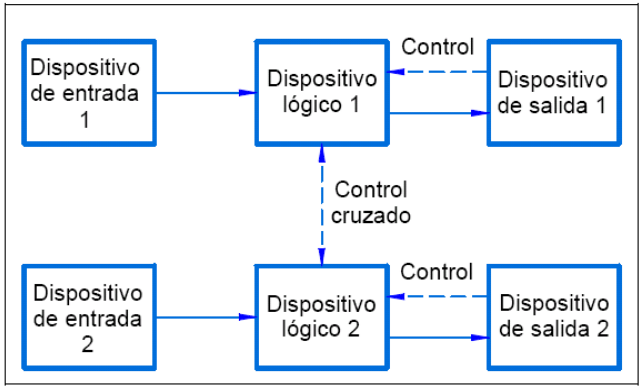


***Figura 10**: Categoría 3 de arquitectura designada.*

Además se debe detectar un fallo único, donde sea posible.

Este aspecto es el mismo que el requisito original para la categoría 3 de la norma precedente UNE-EN 954-1.

En ese contexto el significado de la frase "donde sea posible" resultó ser de alguna manera confuso.

Significaba que la categoría 3 podía cubrir desde un sistema con redundancia pero sin detección de fallo a un sistema redundante donde todos los fallos simples son detectados.

Este aspecto se contempla en la norma UNE-EN ISO 13849-1 mediante el requisito de calcular la calidad de la cobertura de diagnóstico (DC), que necesita alcanzar un valor de al menos un 60% para la arquitectura pueda ser de categoría 3.

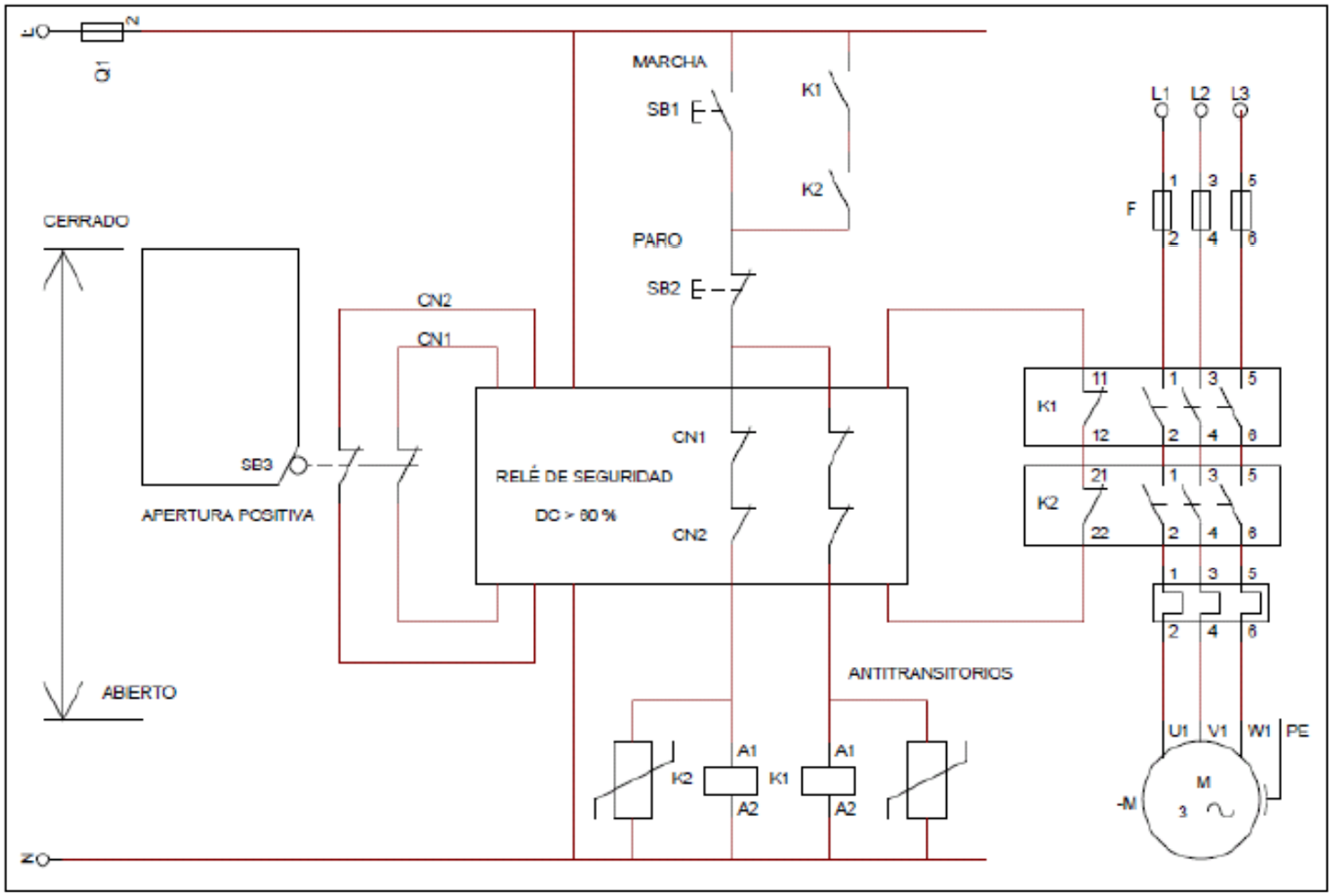


***Figura 11**: Esquema de categoría 3 para el enclavamiento de un resguardo.*

Categoría 4.

La categoría 4 de arquitectura designada debe usar principios de seguridad básicos de igual forma que las categorías anteriores, además de los principios de eficacia probada, de igual manera que las categorías 1, 2 y 3.

Los requisitos para la categoría 4 son similares a los de la categoría 3, pero exige mayor monitorización, es decir, mayor cobertura de diagnóstico, debiéndose alcanzar un índice DC mayor o igual al 99 %.

La categoría 4 exige una cobertura de diagnóstico alta para todas las partes del sistema de mando relativas a seguridad (DCavg = alta).

Esta mayor cobertura de diagnóstico es una de las diferencias básicas entre la categoría 3 y 4.

El MTTFd debe ser alto, por lo que la inmunidad a fallos de los componentes en categoría 4 también es habitualmente mayor que en 3.

Se necesita incorporar medidas contra los fallos de causa común (CCF).

Diagrama de bloques de la categoría 4.

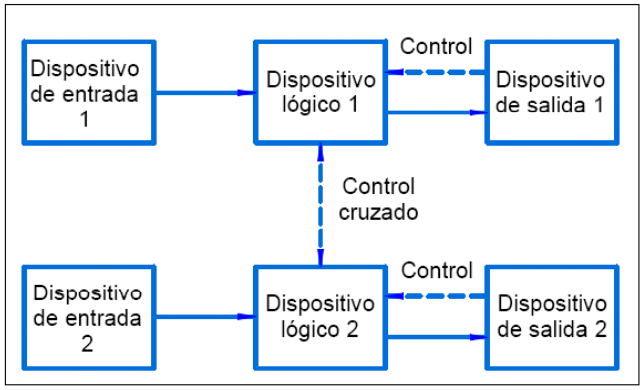


***Figura 13**: Diagrama de bloques de la categoría 4 de arquitectura designada.*

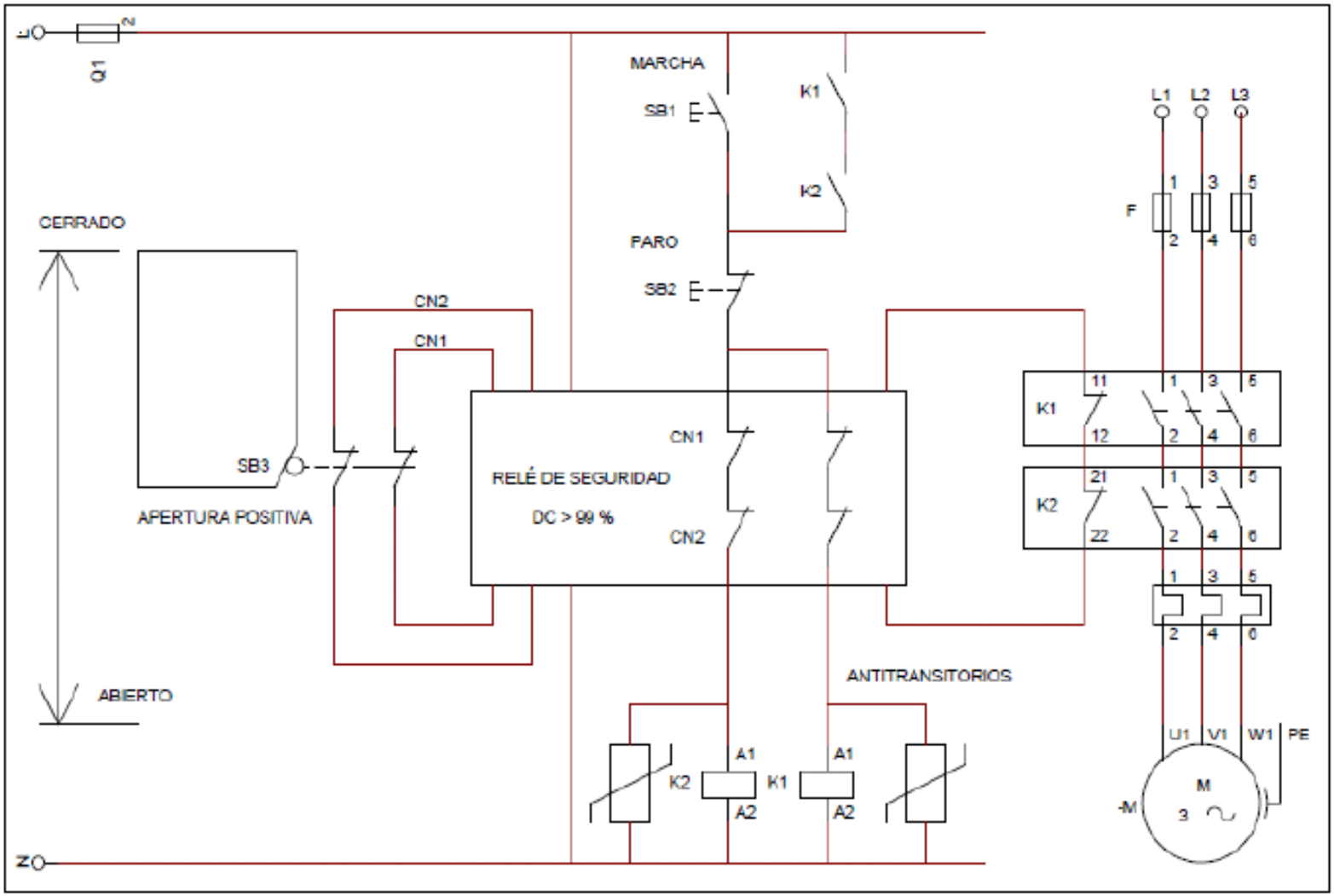


***Figura 14**: Esquema de categoría 4 para el enclavamiento de un resguardo.*

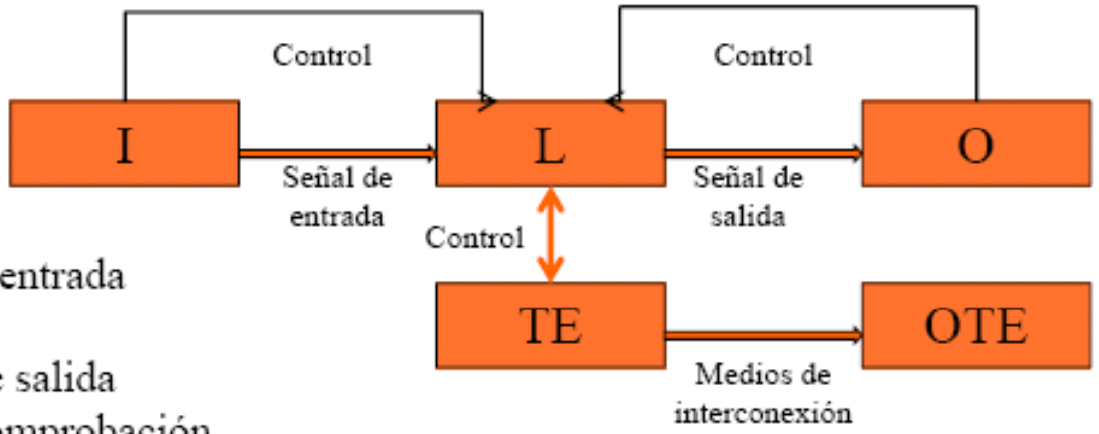
APLICACIÓN DE LA UNE EN 13849-1:2008

1 - Categoría de control: Arquitectura designada (Depende del diseño del circuito)

- **Categoría B y 1**



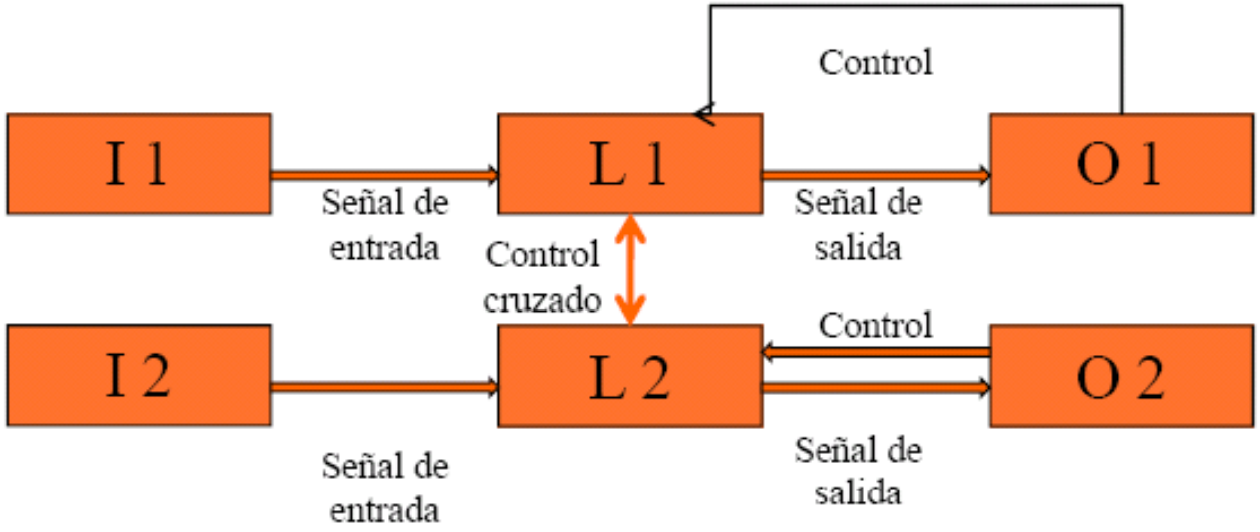
- **Categoría 2**



I: Dispositivo de entrada
L: Lógica
O: Dispositivo de salida
TE: Equipo de comprobación
OTE: Salida de TE

APLICACIÓN DE LA UNE EN 13849-1:2008

- **Categoría 3 y 4**



I: Dispositivo de entrada
L: Lógica
O: Dispositivo de salida

TIEMPO MEDIO HASTA QUE SE PRODUZCA UN FALLO PELIGROSO (MTTFd).

El tiempo medio hasta que se produce un fallo peligroso, MTTFd, está relacionado con la fiabilidad de los componentes individuales en el circuito de seguridad.

Por ejemplo, el órgano de accionamiento de parada de emergencia se usa para detener una máquina en condiciones de trabajo normales y accionado cinco veces al año puede utilizarse durante 30 años antes de que falle peligrosamente atendiendo a consideraciones estadísticas.

Los valores MTTFd de los componentes individuales se basan en los datos proporcionados por los fabricantes.

TIEMPO MEDIO HASTA QUE SE PRODUZCA UN FALLO PELIGROSO (MTTFd).

El valor del MTTFd **para sistemas de un solo canal** se calcula de acuerdo a la siguiente fórmula:

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

El inverso del MTTFd es igual a la suma de los valores inversos de los MTTFd de los componentes individuales de la parte del sistema de mando.

TIEMPO MEDIO HASTA QUE SE PRODUZCA UN FALLO PELIGROSO (MTTFd).

Calificación para cada canal en función del resultado que se obtenga para MTTFd:

MTTFd	
Índice para cada canal	**Gama para cada canal**
Bajo	3 años $\leq$ $MTTF_d$ $<$ 10 años
Medio	10 años $\leq$ $MTTF_d$ $<$ 30 años
Alto	30 años $\leq$ $MTTF_d$ $<$ 100 años

Tabla 2: *Calificación del MTTFd para cada canal en función del resultado numérico.*

TIEMPO MEDIO HASTA QUE SE PRODUZCA UN FALLO PELIGROSO (MTTFd).

El cálculo del MTTFd para varios canales y para componentes con desgaste requiere otro tratamiento.

En el caso de tener una *redundancia con los dos canales diferentes*, utilizando la siguiente ecuación, se lograría encontrar el *MTTFd* que tendría cada canal (fórmula D.2 en anexo D de UNE-EN 13849-1: 2008):

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

TIEMPO MEDIO HASTA QUE SE PRODUZCA UN FALLO PELIGROSO (MTTFd).

La norma UNE-EN ISO 13849-1 limita el valor MTTFd utilizable de un canal individual de un subsistema a un **máximo de 100 años**, aunque los valores reales calculados pueden ser mucho más altos.

El índice logrado del MTTFd promedio se combina con la categoría de arquitecturas designada y la cobertura de diagnóstico (DC) para proporcionar una clasificación de PL (nivel de prestaciones alcanzado).

ÍNDICE DE LA COBERTURA DEL DIAGNÓSTICO (DCavg).

Ya se ha mencionado el término "*cobertura de diagnóstico*" al presentar las categorías 2, 3 y 4 de la arquitectura designada.

Dichas categorías requieren algún tipo de **prueba de diagnóstico** para verificar si la función de seguridad sigue estando operativa.

El término "*cobertura de diagnóstico*" (normalmente abreviado como **DC**) se utiliza para caracterizar la eficacia de esta prueba.

Es importante darse cuenta de que la cobertura de diagnóstico no está basada sólo en el número de componentes que pueden fallar de manera peligrosa.

Tiene en cuenta la tasa total de fallos peligrosos.

ÍNDICE DE LA COBERTURA DEL DIAGNÓSTICO (DCavg).

El símbolo λ . se usa para "*tasa de fallo*". La cobertura de diagnóstico expresa la relación de las tasas de ocurrencia de los dos siguientes tipos de fallos peligrosos:

- Fallo peligroso detectado (λ_{dd}) es decir, aquellos fallos que podrían causar, o podrían llegar a causar, pérdida de la función de seguridad, pero que son detectados. Después de la detección, una función de reacción al fallo ocasiona que el dispositivo o sistema pase al estado de seguridad.

- Fallo peligroso (λ_d) es decir, todos aquellos fallos que pudieran potencialmente causar, o llegar a causar, pérdida de la función de seguridad. Esto incluye tanto los fallos que son detectados como aquellos que no lo son. Desde luego que los fallos verdaderamente peligrosos son los fallos peligrosos no detectados (denominados λdu).

ÍNDICE DE LA COBERTURA DEL DIAGNÓSTICO (DCavg).

La cobertura de diagnóstico se expresa mediante el resultado de la siguiente fórmula expresada en %:

$$DC = \frac{\lambda dd}{\lambda d}$$

De acuerdo con esta definición el promedio del diagnóstico de cobertura *DCavg* puede estimarse con la siguiente fórmula, que se extrae del anexo E de la norma EN ISO 13849-1:

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

ÍNDICE DE LA COBERTURA DEL DIAGNÓSTICO (DCavg).

Dependiendo del control, la cobertura de diagnóstico se encuentra entre menos de 60 por ciento (cuando no se realiza ningún tipo de diagnóstico) y más del 99 por ciento (nivel de diagnóstico alto).

Para la estimación del nivel de cobertura de diagnóstico la norma EN ISO 13849-1 incluye en uno de sus anexos una tabla a modo de guía simplificada:

DC	
Índice	**Gama**
Nula	$DC < 60\,\%$
Baja	$60\,\% \leq DC < 90\,\%$
Media	$90\,\% \leq DC < 99\,\%$
Alta	$99\,\% \leq DC$

Tabla 3: *Determinación de la DC media para la totalidad del sistema.*

GESTIÓN DE FALLOS POR CAUSA COMÚN (CCF).

En la mayoría de los sistemas o de los subsistemas de doble canal (tolerantes a fallo único), el principio de diagnóstico está basado en la premisa de que no habrá fallos peligrosos en ambos canales al mismo tiempo.

El término “al mismo tiempo” puede expresarse con más exactitud como “dentro del intervalo de prueba de diagnóstico”.

Si el intervalo de prueba del diagnóstico es razonablemente corto (por ejemplo, menor de ocho horas) es razonable asumir que dos fallos no relacionados e independientes tienen baja probabilidad de ocurrir dentro de ese tiempo.

Sin embargo, la norma indica que se debe pensar detenidamente acerca de si las posibilidades de fallo son realmente independientes y no relacionadas.

Por ejemplo, si un fallo en un componente puede ocasionar de manera previsible fallos de otros componentes, entonces la totalidad resultante de fallos se considera un fallo único.

GESTIÓN DE FALLOS POR CAUSA COMÚN (CCF).

Además, es posible que un suceso que ocasione el fallo de un componente pueda también causar el fallo de otros componentes.

Esto se denomina "*fallos por causa común*", normalmente abreviado como **CCF**.

El grado de predisposición de fallos por causa común se describe como el factor beta (β).

La norma ofrece una lista de medidas eficaces para evitar los fallos por causa común (tabla F.1 del Anexo F de la UNE-EN ISO 13849-1):

	Tipo de medida	Puntuación
1.	**Separación/Aislamiento de la vía de señal:**	
	Separación física entre los caminos de las señales: – *Separación en el cableado, en las tuberías.* – *Distancias de aislamiento y líneas de fuga en tarjetas para circuitos impresos.*	15 puntos
2.	**Diversidad**	
	Utilizar diferentes tecnologías/principios de diseño o principios físicos: – *Primer canal electrónico programable y segundo canal cableado.* – *Tipo de iniciación.* – *Presión y temperatura.* Medida de la distancia y de la presión, por ejemplo: – *Digital y analógica.* Componentes de diferentes fabricantes.	20 puntos
3.	**Diseño/aplicación/experiencia.**	
3.1	Protección ante sobretensión, sobreintensidad, sobrepresión, etc.	15 puntos
3.2	Utilización de componentes de eficacia probada.	5 puntos
4.	**Evaluación/Análisis.**	
	¿En el diseño se tienen en cuenta los resultados de un FMEA (análisis de modos de fallo y sus efectos) para evitar los CCF?	5 puntos
5.	**Competencia/formación del diseñador.**	
	¿Han sido formados los diseñadores y el personal de mantenimiento para entender las causas y consecuencias de los fallos de causa común?	5 puntos
6.	**Medio ambiente.**	
6.1	Prevención de la contaminación y de las perturbaciones electromagnéticas (EMC) contra los CCF, de conformidad con las normas pertinentes. *Sistemas fluídicos: filtración del medio a presión, prevención de la absorción de impurezas, drenaje del aire comprimido, por ejemplo, de conformidad con los requisitos del fabricante del componente en lo que se refiere a la pureza del medio a presión.* *Sistemas eléctricos: ¿se ha comprobado la inmunidad electromagnética del sistema, por ejemplo, tal como se especifica en las normas pertinentes contra los CCF?*	25 puntos
6.2	*¿Se han tenido en cuenta los requisitos relativos a la inmunidad contra todas las influencias ambientales pertinentes, tales como la temperatura, los choques, las vibraciones, la humedad (como se especifica en las normas pertinentes)*	10 puntos

Tabla 5: Medidas orientativas para reducir fallos y puntuación que representan.

Se deben implementar suficientes medidas tendentes a evitar fallos por causa común hasta alcanzar un **mínimo de 65 puntos.**

6. NIVEL DE PRESTACIONES ALCANZADO (PL).

Una vez definida la categoría de la función de seguridad se debe evaluar el PL que permite alcanzar dicha función.

Para evaluar el PL se requieren los siguientes datos del sistema (o subsistema).

1 – La "***Categoría***" de control (se obtiene a partir de su arquitectura, la detección de defectos y / o su fiabilidad)

2 - El valor **MTTFd**: ***Tiempo medio hasta un fallo peligroso*** (valor probable de la duración media hasta un fallo peligroso)

3 - **DC**: La "***Cobertura del diagnóstico***" (medida de la efectividad del diagnostico: relación entre tasa de fallo de los fallos peligrosos detectados y la tasa de fallo del total de fallos peligrosos)

4 - **CCF**: El "***Fallo de causa común***" (fallo de varios elementos, que común resultan de un solo suceso y que no son consecuencia unos de otros)

La evaluación del PL se puede realizar gráficamente a partir de una combinación de estos factores.

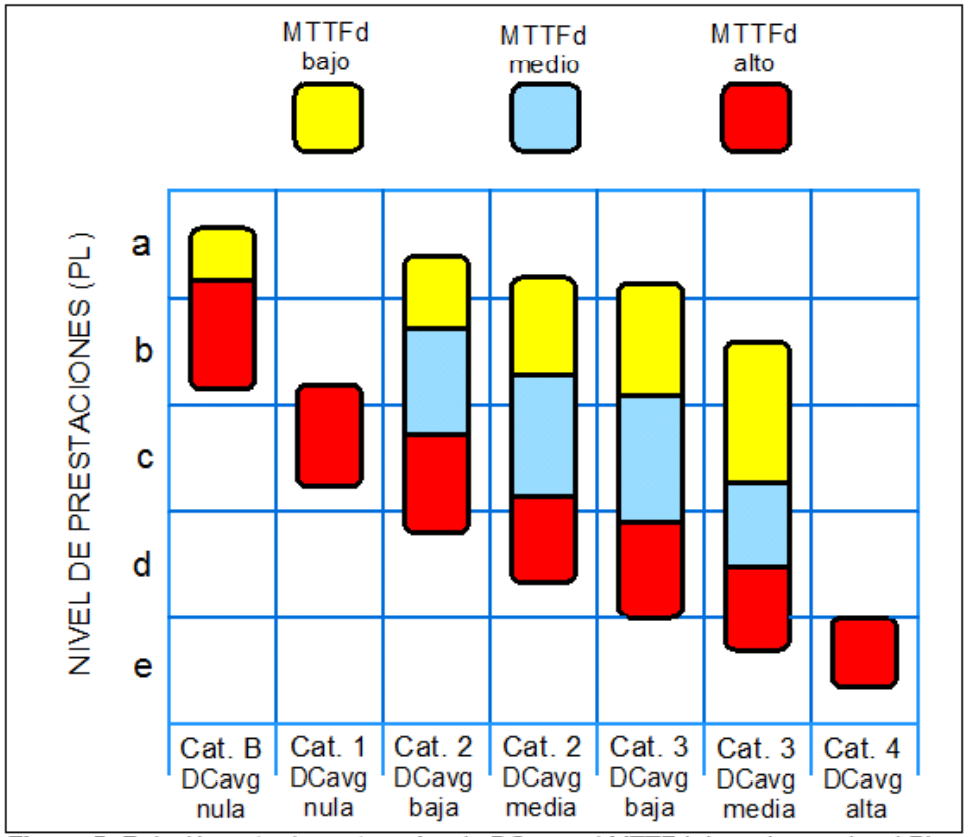


Figura 5: *Relación entre las categorías, la DCavg, el MTTFd de cada canal y el PL*

APLICACIÓN DE LA UNE EN 13849-1:2008

PASOS PARA DERMINAR EL NIVEL DE FIABILIDAD DE UN SISTEMA DE MANDO (PL)

1 – Definir la Función de Seguridad (FS) a estudiar: Parada emergencia, Enclavamiento, Etc

2 – Evaluar el riesgo a proteger por la función definida y a partir del Gráfico de Reducción del Riesgo y definir el Nivel de Prestaciones requerido (PLr) entre a/b/c/d /e

DETERMINACIÓN DEL PL DEL SISTEMA DISEÑADO

3 – Designar una "Categoría" para el sistema, que en función del PL r deberá ser de "Un canal" (Categorías B y 1), "Un canal con supervisión y salida activa" (Categoría 2) o "Dos canales redundantes con control cruzado" (Categorías 3 y 4)

4 – Determinación (para cada canal) del MTTFd (suma de valores componentes). Posibilidades:

- Baja: 3 años ≤ MTTFd < 10 años
- Media: 10 años ≤ MTTFd < 30 años
- Alta: 30 años ≤ MTTFd < 100 años

5 – Determinación de la Cobertura de Diagnostico (DC): Coeficiente por "Fallos no detectados"

- Ninguna= DC<60%
- Baja= 60% ≤ DC < 90%
- Media= 90% ≤ DC < 99%
- Alta= 99% ≤ DC

6 – Gestión de "Fallos por causa común" (CCF): Aplicable a partir de estructuras de Categoria 2

- Implementar medidas para prevención de fallos que sumen un mínimo de 65 puntos

7 – Con los datos obtenidos verificar si PL ≥ PLr en el Gráfico de Nivel de Fiabilidad a/b/c/d /e

8 – Si PL < PLr deberá rediseñarse el sistema (cambio de Categoria, componenentes o diseño)

EJEMPLO DE APLICACIÓN QUE ILUSTRA LAS PRESTACIONES DE LA FUNCIÓN DE SEGURIDAD DEL ENCLAVAMIENTO DE UN RESGUARDO

- **Para dicho ejemplo, la función de seguridad del enclavamiento de un resguardo se puede seleccionar como sigue: El movimiento peligroso se detiene cuando el resguardo se abre (desactivación de energía al motor)**
- **Parámetros de riesgo (de acuerdo con método del gráfico del riesgo):**
  - **Gravedad de la lesión: S2, grave;**
  - **Frecuencia y/o duración de la exposición al peligro, F: F1 (raro a bastante frecuente y/o corta duración de exposición).**
  - **Posibilidad de evitar el peligro o de limitar el daño, P: P1 (posible)**
- **- Con estos datos el nivel de prestaciones requerido PLr es de "c"**
- **- Dicho nivel se puede conseguir con sistemas de uno o dos canales**
- **- Vamos a ver si con un solo canal muy fiable se puede obtener un PL de "c"**

EJEMPLO DE APLICACIÓN QUE ILUSTRA LAS PRESTACIONES DE LA FUNCIÓN DE SEGURIDAD DEL ENCLAVAMIENTO DE UN RESGUARDO

Para dicho ejemplo, la función de seguridad del enclavamiento de un resguardo se puede seleccionar como sigue: El movimiento peligroso se detiene cuando el resguardo se abre (desactivación de energía al motor)

Parámetros de riesgo (de acuerdo con método del gráfico del riesgo):

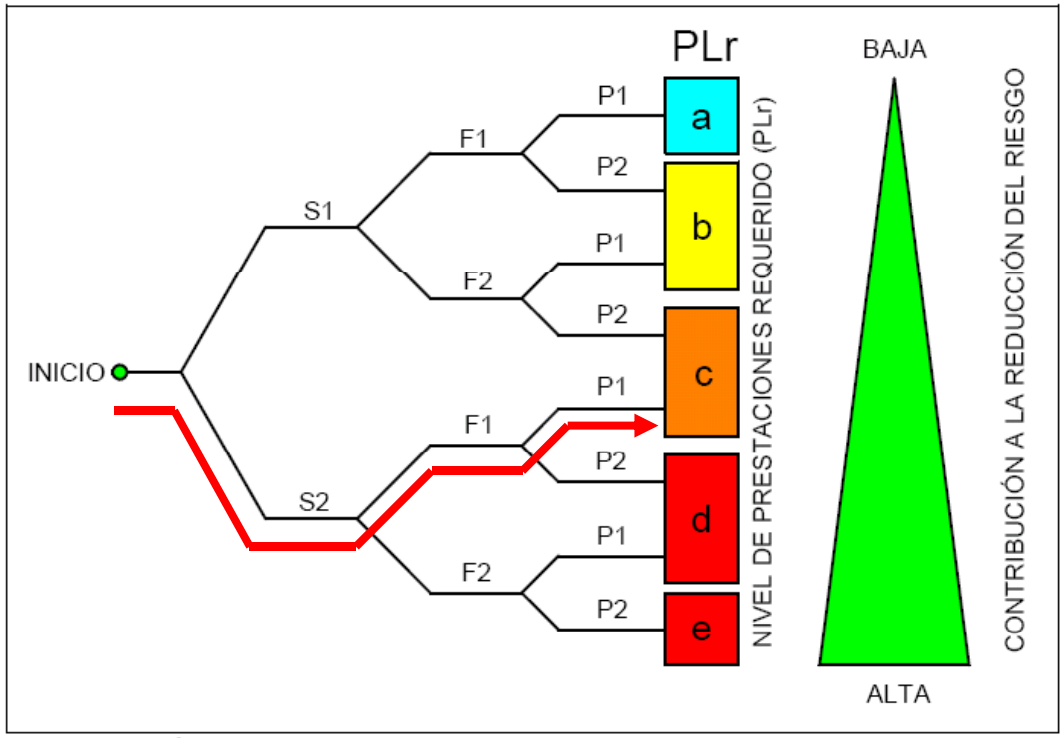


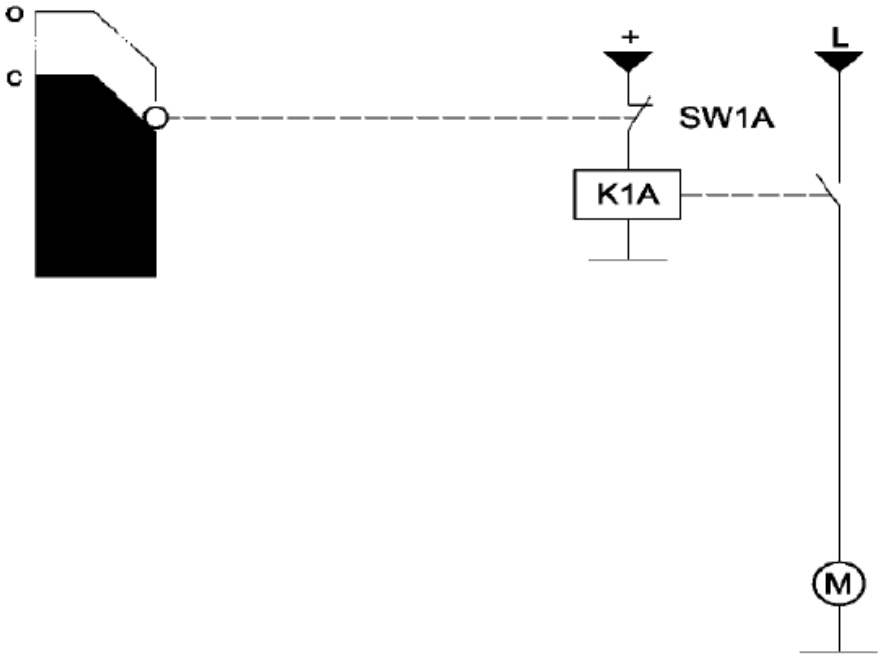
Figura 1: *Gráfico del riesgo para determinar el nivel de prestaciones requerido (PLr) para cada función de seguridad. (Figura A.1 de UNE EN 13849-1).*

Parámetros de riesgo	
S1	Lesión leve (normalmente reversible).
S2	Lesión grave (normalmente irreversible, incluyendo la muerte).
F1	Raro a bastante frecuente y/o corta duración de la exposición.
F2	Frecuente a continuo y/o larga duración de la exposición.
P1	Posible de evitar en determinadas condiciones.
P2	Raramente posible de evitar.

Tabla 1: *Parámetros del riesgo.*

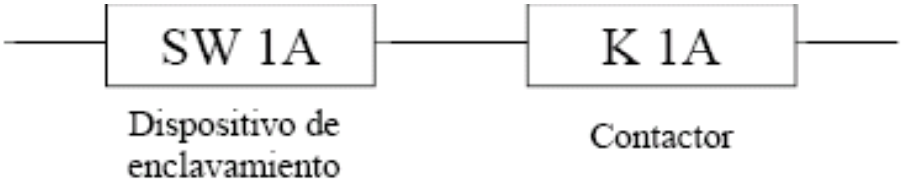
Ejemplo de aplicación:

Interruptor de puerta provisto de contactos normalmente cerrados, conectado a un contactor capaz de desconectar la alimentación de energía del motor.



O: Abierto
C: Cerrado
M: Motor
K1A: Contactor
SW1A: Interruptor

Diagrama de bloques relativo a la seguridad



Cálculo del MTTFd

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

Se supone que los datos facilitados por el fabricante son:
MTTFd,K1A =80 años, y
MTTFd,SW1A=50 años

$1/MTTF_d = 1/MTTF_{SW1A} + 1/MTTF_{K1A} = 1/50\text{años} + 1/80\text{años} = 0{,}0325\text{años}$

MTTFd= 30,77 años o "alto" para el canal.

MTTFd	
Índice para cada canal	**Gama para cada canal**
Bajo	3 años ≤ $MTTF_d$ < 10 años
Medio	10 años ≤ $MTTF_d$ < 30 años
Alto	30 años ≤ $MTTF_d$ < 100 años

Tabla 2: *Calificación del MTTFd para cada canal en función del resultado numérico.*

Cálculo de la DC

Dado que no se realiza ninguna comprobación la DC es 0 o "nula", según la siguiente Tabla:

DC	
Índice	**Gama**
Nula	DC < 60 %
Baja	60 % ≤ DC < 90 %
Media	90 % ≤ DC < 99 %
Alta	99 % ≤ DC

Tabla 3: *Determinación de la DC media para la totalidad del sistema.*

Categoría

La categoría preferente para este circuito es la categoría 1.

Con los datos obtenidos de:

Categoría 1

DC= DC nulo

$MMTF_d$= alto

y según el gráfico, de la derecha

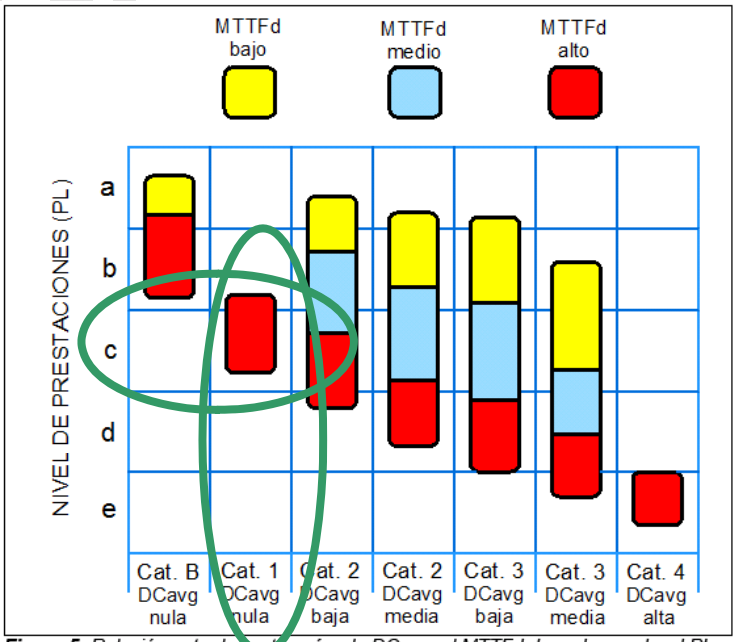


Figura 5: *Relación entre las categorías, la DCavg, el MTTFd de cada canal y el PL*

El nivel de prestaciones obtenidos es PL= c

Nivel de prestaciones obtenidos PL es de c

Nivel de prestaciones requerido PLr es de c

¿ PL≥PLr ? → SI

↓

¿Se cumplen los requisitos? → SI

↓

¿se han analizado todas las funciones de seguridad? → SI

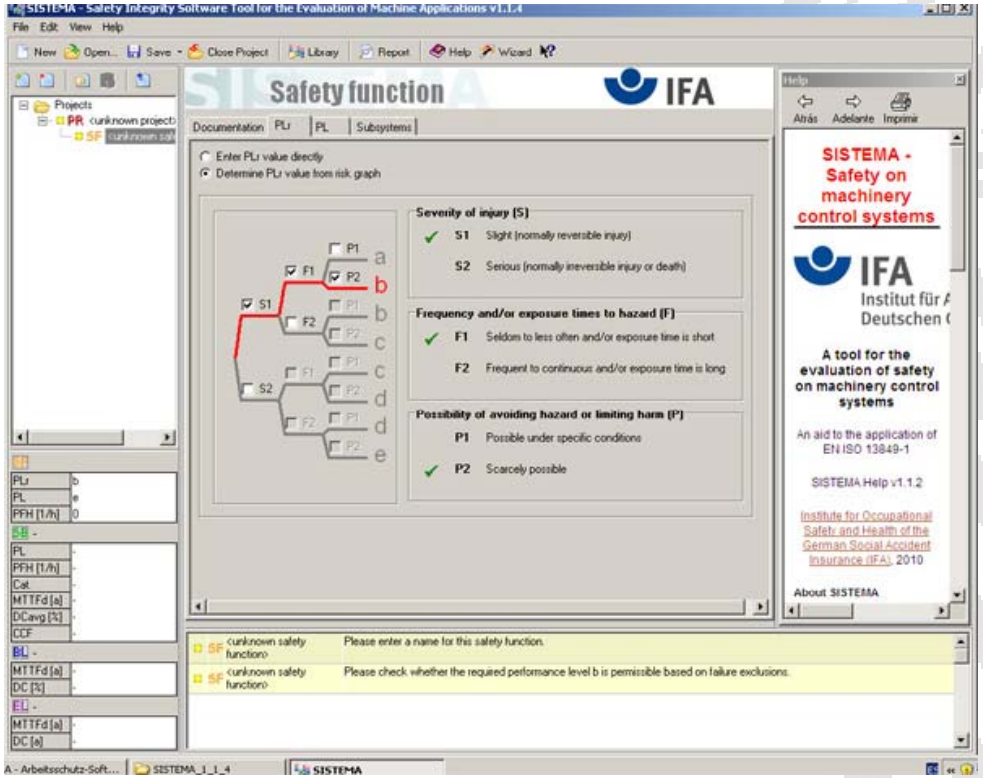
↓

OK

SOFTWARE SISTEMA

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball

http://www.dguv.de/ifa/de/pra/softwa/sistema/index.jsp





DESPEDIDA

INVASSAT
Institut Valencià de Seguretat i Salut en el Treball



¡ Muchas gracias por su atención !