# UNE EN ISO 13849-1:2008
# Partes de los sistemas de mando relativas a la seguridad

Applus Formación

UNE EN ISO 13849-1:2008

PARTES DE LOS SISTEMAS DE MANDO RELATIVAS A LA SEGURIDAD

Vigente a partir de
29 de Diciembre de 2009

Albert Barella i Civit
APPLUS / LGAI,Technological Center, S.A.
Certificación de Producto



# UNE EN ISO 13849-1:2008
# Partes de los sistemas de mando relativas a la seguridad

Applus Formación

**- La Norma UNE EN ISO 13849-1:2008 es vigente a partir del 29/12/2009, sustituye a la anterior UNE EN ISO 13849-1:2007, la cual a su vez sustituía a la EN 954-1.**

**- La EN 954-1 puede seguirse utilizando hasta el 31-12-2011, que quedará definitivamente anulada.**

**- La norma UNE EN ISO 13849-1:2008 es más exigente que la EN 954-1**

## LOS CRITERIOS DE LA PRESENTE NORMA SE APLICAN A:

- **Las partes de los sistemas de mando relativas a la seguridad (SRP/CS), incluyendo el diseño del soporte lógico, de cualquier tipo de máquina:**
  - Hidráulica
  - Neumática
  - Eléctrica
  - Mecánica
  - Etc..
- **No importa el tipo de energía utilizada ni la tecnología aplicada**

# UNE EN ISO 13849-1:2008
# Partes de los sistemas de mando relativas a la seguridad

Applus Formación

## LA PRESENTE NORMA PROPORCIONA:

- Requisitos de seguridad
- Orientación sobre los principios para el diseño
- Integración de las partes de los sistemas de mando relativas a la seguridad (SRP/CS)
- Diseño del soporte lógico
- Se especifican las características incluyendo el nivel de prestaciones requerido (PL) para desempeñar las funciones de seguridad.
- PL: "nivel de prestaciones", expresa la probabilidad de fallo peligroso en una hora.

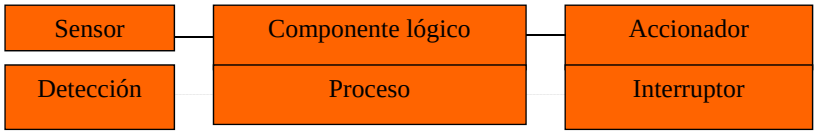


# UNE EN ISO 13849-1:2008
# Partes de los sistemas de mando relativas a la seguridad

Applus Formación

## APLICACIÓN DE LA UNE EN 13849-1:2008

- **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,**
- **LO PRIMERO a realizar es determinar el PLr: Nivel de prestaciones requerido. Es producto de la consideración del gráfico de riesgo.**
  **Dicha consideración es global y siempre referida a la cadena de sensores, al componente lógico y al accionador (detección-proceso-interruptor)**




- **Dicho PLr se obtiene de realizar el correspondiente análisis de riesgos mediante el siguiente gráfico:**

## APLICACIÓN DE LA UNE EN 13849-1:2008

- **PLr: Nivel de prestaciones requerido**

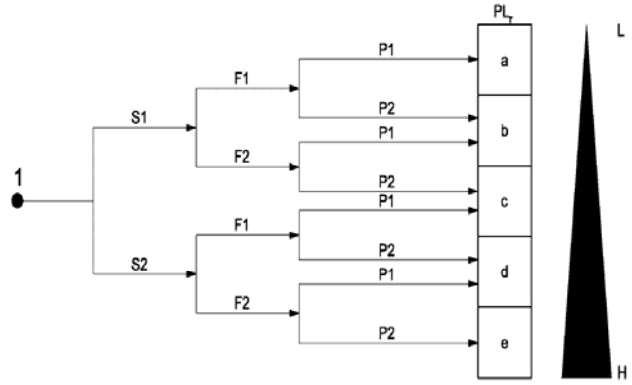



Gráfico del riesgo para determinar el nivel de prestaciones requerido (PLr) para cada función de seguridad

**Parámetros del 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

**1**- Punto de partida para la estimación de la contribución de las funciones de seguridad a la reducción del riesgo
**L**- Contribución a la reducción del riesgo baja
**H**- Contribución a la reducción de riesgo alta



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

## APLICACIÓN DE LA UNE EN 13849-1:2008

- **EN SEGUNDO LUGAR , una vez determinado el PLr debe encontrarse el PL: Nivel de prestaciones alcanzado, del sistema diseñado.**

  **Estimación: Puede realizarse cualitativamente o bien cuantitativamente.**

- **PARA ESTIMAR CUANTITATIVAMENTE 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)**

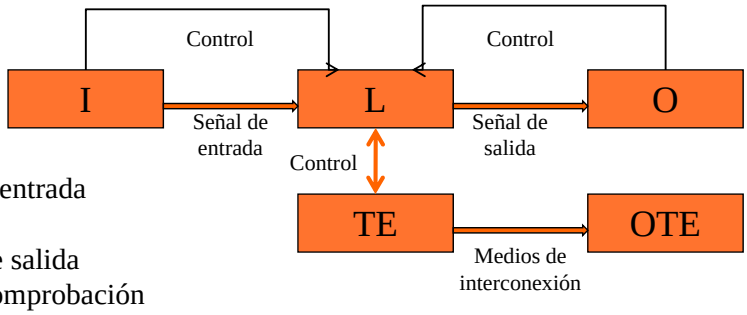
  **4 - CCF: El "Fallo de causa común" (fallo de varios elementos, que resultan de un solo suceso y que no son consecuencia unos de otros)**

## 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**



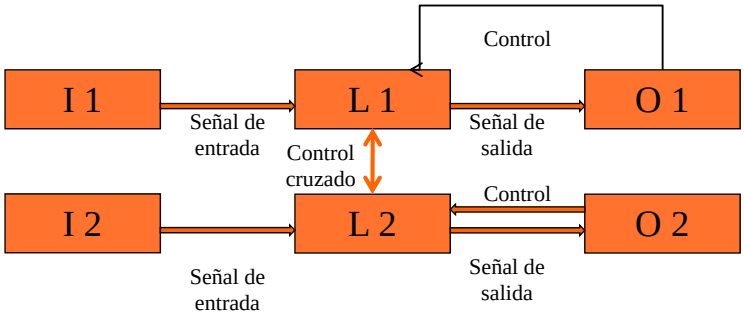

**I**: Dispositivo de entrada
**L**: Lógica
**O**: Dispositivo de salida
**TE**: Equipo de comprobación
**OTE**: Salida de TE



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

APLICACIÓN DE LA UNE EN 13849-1:2008

- **Categoría 3 y 4**




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

www.applusformacion.com

## APLICACIÓN DE LA UNE EN 13849-1:2008

### 2 - MTTFd: Tiempo medio hasta un fallo peligroso (Depende de los Componentes)

- Es un indicador de calidad que se refiere a la fiabilidad de los componentes y dispositivos de seguridad de una SRP/CS. Los datos los debe dar el fabricante.
- Es una media estadística que representa el tiempo de funcionamiento sin averías previsto por año (MTTF).
- Se asume una distribución exponencial del fallo coincidente.

- **MTTFd para un solo canal**
- Método de recuento de partes: hay que sumar los valores de MTTFd individuales de los componentes del SRP/CS.

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

| $MTTF_d$ | |
|---|---|
| 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 $\leq MTTF_d \leq$ 100 años |

**Casos particulares:**

- $MTTF_d$ para varios canales: Ver fórmula D.2 en anexo D de EN 13849-1: 2008.
- $MTTF_d$ para componentes con desgaste. Ver fórmula C.1 del anexo C de EN 13849-1: 2008



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

Applus Formación

APLICACIÓN DE LA UNE EN 13849-1:2008

### 3 - DC: Cobertura del diagnóstico (Depende de la capacidad de detectar fallos en el circuito y por tanto tiene que ver con la arquitectura del circuito)

- Indica la proporción entre los fallos peligrosos detectados y la activación del modo de fallo en todos los fallos peligrosos.
- Indica la cuantificación de la eficacia de las medidas para descubrir fallos en una SRP/CS.
- Se asume que pueden ocurrir fallos y que los mecanismos para su detección no son todos igual de efectivos, de manera que existe una proporción de fallos no detectados.

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

**Determinación de la DC media para la totalidad del sistema**

- La metodología considera las categorías como arquitecturas con una $D_{avg}$ (cobertura de diagnóstico media) definida.
- Ver tabla E.1 del anexo E de la norma 13849-1:2008

## APLICACIÓN DE LA UNE EN 13849-1:20

- **DCavg: Cobertura del diagnóstico media**
  - **La metodología considera las categorías como arquitecturas con una $D_{avg}$ (cobertura de diagnóstico media) definida.**
  - **Refleja la calidad de la detección de defectos de todas las partes de cada canal**

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

- **En el PL sólo se incluye un valor medio $DC_{avg}$ que debe ponderarse en todas las pruebas**
- **El factor de ponderación es el $MTTF_d$ de las partes comprobadas**
- **Las partes no comprobadas se introducen como DC=0**
- **Las partes que no pueden demostrar una exclusión de defectos entran la suma (exclusión de defecto-> $MTTF_d=\infty$)**



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

Applus Formación

## APLICACIÓN DE LA UNE EN 13849-1:2008

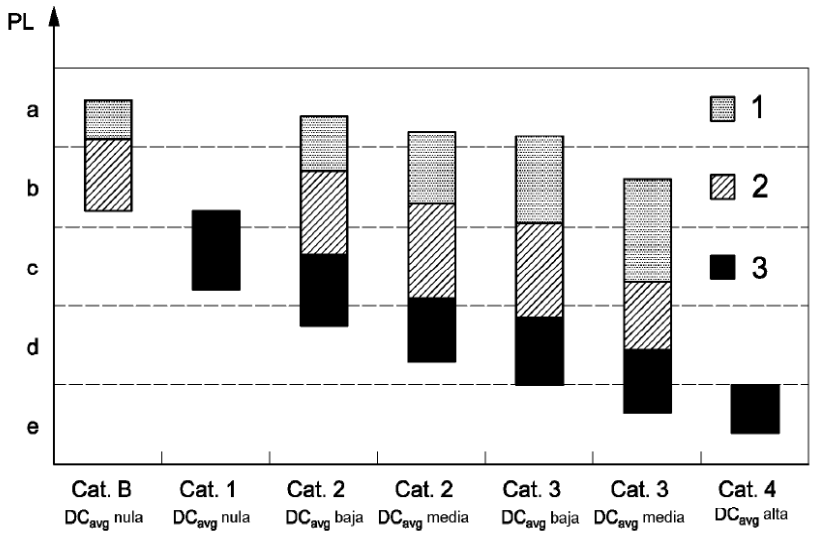
**4 - CCF: Gestión de fallos de causa común (Depende del diseño eléctrico/electro-nico y de criterios de instalación) :**

- Parámetro aplicable en estructuras de 2 canales a partir de la categoría 2
- Está destinado a prevenir fallos en una SRP/CS con una causa y un efecto común
- Las medidas de protección frente a CCF son necesarias de estructuras de múltiples canales.
- Se detalla una lista de medidas de protección con un sistema de puntuación de valor máximo 100 puntos.
- *El objetivo son **65 puntos** como mínimo*

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

## APLICACIÓN DE LA UNE EN 13849-1:2008

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




Leyenda

PL nivel de prestaciones

1 $MTTF_d$ de cada canal = bajo

2 $MTTF_d$ de cada canal = medio

3 $MTTF_d$ de cada canal = alto



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

Applus Formación

## 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)**

## APLICACIÓN DE LA UNE EN 13849-1:2008

- **Procedimiento simplificado para valorar el PL obtenido por la SRP/CS**

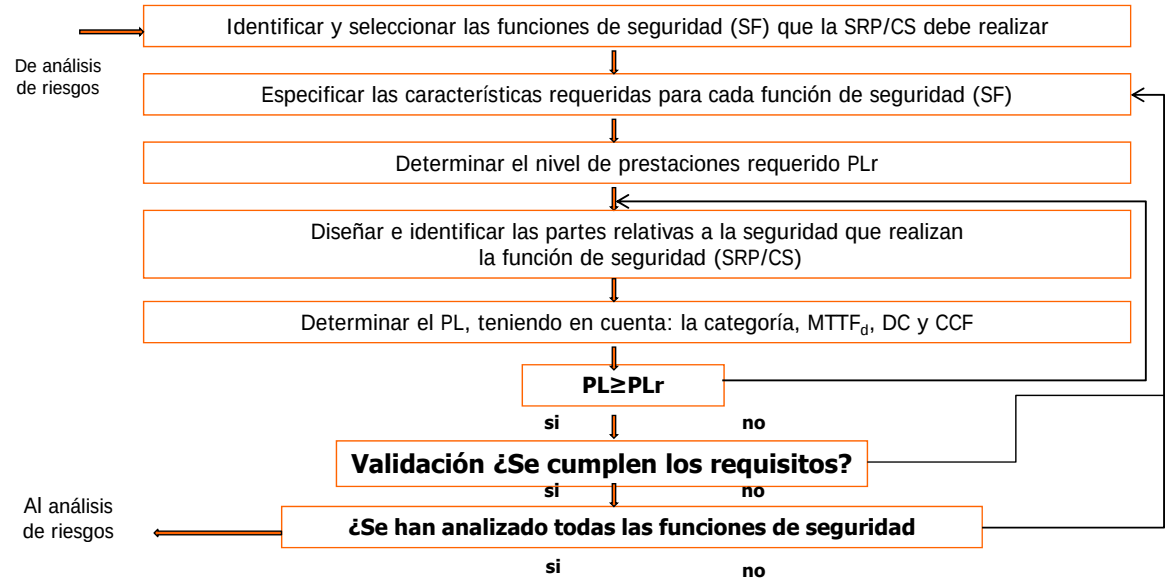
| Categoría | | B | 1 | 2 | 2 | 3 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|
| $DC_{avg}$ | | nula | nula | baja | media | baja | media | alta |
| $MTTF_d$ de cada canal | | | | | | | | |
| | Bajo | a | No cubierto | a | b | b | c | No cubierto |
| | Medio | b | No cubierto | b | c | c | d | No cubierto |
| | Alto | No cubierto | c | c | d | d | d | e |



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

Applus Formación

- **Proceso iterativo para el diseño de las partes del sistema de mando relativas a la seguridad (SRP/CS):**



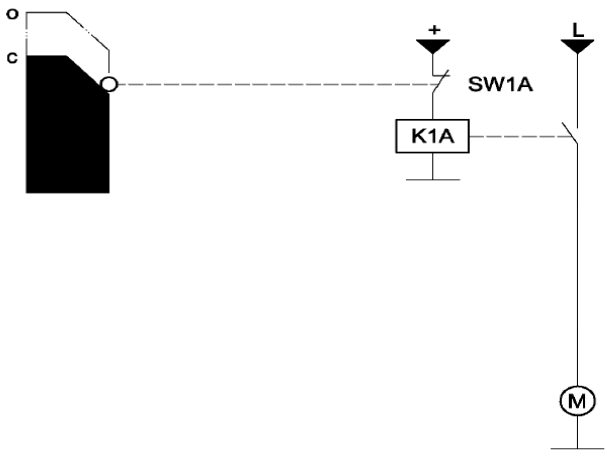
## EJEMPLO DE APLICACIÓN QUE ILUSTRA LAS PRESTACIONES DE LA FUNCIÓN DE SEGURIDAD DEL ENCLAVAMIENTO DE UN RESGUARDO

- **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"**



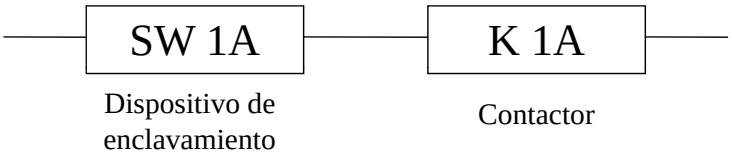
UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

- **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 del ejemplo anterior**




- **Cálculo del $MTTF_d$.**

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

- **Se supone que los datos facilitados por el fabricante son: $MTTF_{d,K1A}$ =80 años y $MTTF_{d,SW1A}$=50 años**

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

**$MTTF_d$= 30,70 años o "alto" para el canal.**



UNE EN ISO 13849-1:2008
Partes de los sistemas de mando relativas a la seguridad

- **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 |

- **Categoría**

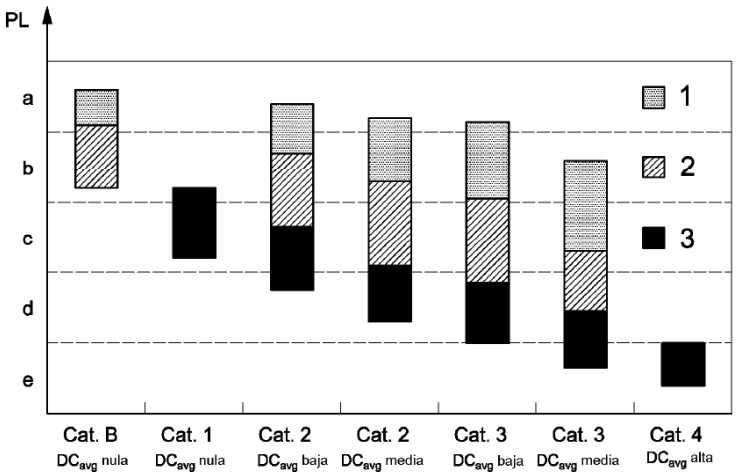
**La categoría preferente para este circuito es la categoría 1.**

## UNE EN ISO 13849-1:2008
## Partes de los sistemas de mando relativas a la seguridad

Applus Formación

- Con los datos obtenidos de:
  - Categoría 1
  - DC= nulo
  - MTTFd= alto

y según el gráfico, de la derecha




**El nivel de prestaciones obtenidos es PL= c**



## UNE EN ISO 13849-1:2008
## Partes de los sistemas de mando relativas a la seguridad

Applus Formación

**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**