Panasonic
ideas for life

Normativa de Seguridad

Nueva Directiva Europea sobre Máquinas 2006/42/EG

J. Cerratos

Panasonic Electric Works España, S.A.

Seguridad en Máquinas

Estándares Europeos para Fabricantes de Componentes y Maquinaria

Directiva Maquinaria
2006/42/EG

Seguridad Funcional

- IEC/EN 61508-1
- EN ISO 13849-1/2
- IEC/EN 62061

Directiva Baja Tensión
2006/95/EG

Seguridad Eléctrica

- EN 50178
- EN 60950-1
- EN 61131-2

Directiva EMC
2004/108/EG

Compatibilidad Electromagnética :
- Radiación
- Inmunidad
- Interferencias

- Serie EN 61000
- Serie EN 550xx
- EN 61131-2

Dependiendo del producto, se pueden aplicar normas adicionales

¿Qué ha cambiado?

- **Gran parte de la maquinaria entra ahora en el ámbito de la presente Directiva.**

- **Los documentos técnicos asociados a la máquina deben indicar qué requisitos de la Directiva cumplen.**

- **Un manual de instalación, así como las instrucciones de montaje deben acompañar al producto en uno de los idiomas oficiales de la UE; este lenguaje debe corresponder al idioma oficial de la empresa que fabrique la máquina. (En cambio, el manual de instrucciones debe de estar en el idioma donde se instale la máquina).**

Los requisitos de seguridad y salud básica han sido actualizados de acuerdo con los avances tecnológicos

Los componentes de seguridad han sido etiquetados con la marca CE en conformidad con la Directiva de Maquinaria.

En escenarios de Automatización Industrial

Puntos Esenciales:

-**Los fabricantes deben prever situaciones anormales (evaluación de riesgos) a la hora de diseñar y construir máquinas.**

- **Hardware y software puede ser utilizado a la hora de cumplir los objetivos de seguridad.**

- Es la primera vez que se incluye a los PLC's en las normativas de seguridad:

→ Soluciones integradas con PLC's son mucho más eficientes para los fabricantes de maquinaria.

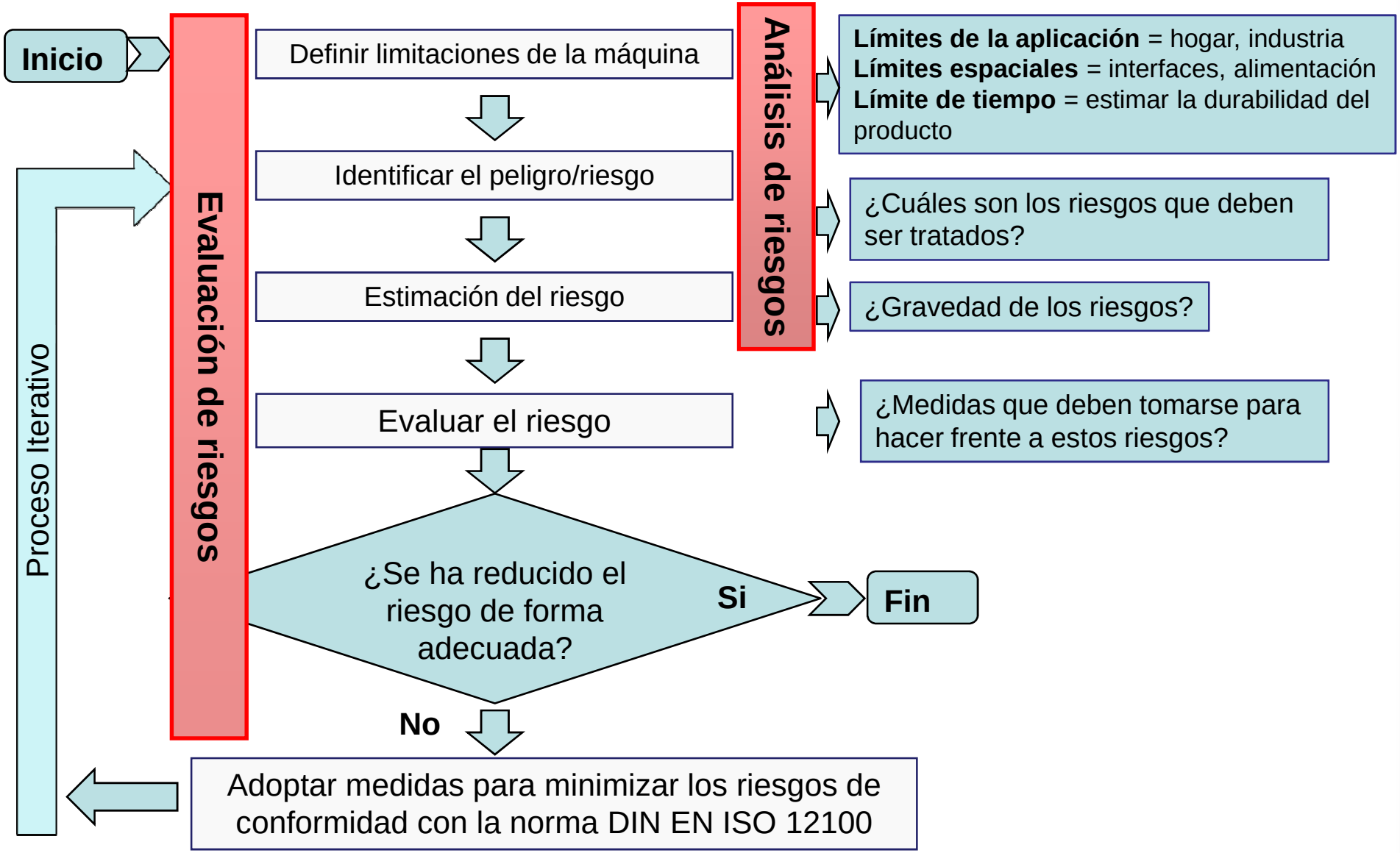
- Un máquina actual o componente de seguridad "peligroso" (aunque esté marcado CE) debe de ser retirado del mercado.

→ Alto riesgo para fabricantes de maquinaria.

→ Los fabricantes deben tomar medidas

→ Finales del 2.011 es la fecha tope para adaptar la maquinaria actual a la nueva Directiva

Objetivos de Seguridad relativos al diseño: Evaluación de riesgos (ISO 14121)



Análisis de Riesgos

EN ISO 14121

- Riesgos mecánicos
- Riesgos eléctricos
- Riesgos relacionados con el calor
- Riesgos relacionados con materiales y sustancias
- Riesgos de ruidos
- Peligro de radiación
- Riesgos relacionados con vibración
- Riesgos ergonómicos

- Golpear
- Aplastar
- Recortar
- Cortar
- Perforar

EN ISO 12100

Minimizar los riesgos

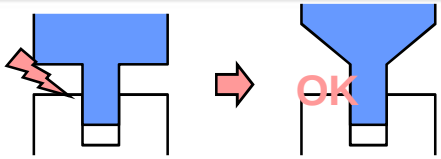
Reducción del riesgo a través de equipos de protección

Reducción del riesgo a través del diseño de seguridad intrínseca

DIN EN ISO 13849
Componente seguro del sistema de control (SRP/CS):
Seguridad funcional

Minimizar los riesgos (ISO 12100)

Localizar, evaluar y finalmente controlar los peligros realizando las protecciones adecuadas



Ejemplo:
Herramienta punzonado

Diseño de seguridad intrínseca → ej.: Modificar la forma del producto

Equipo de protección (SRP/CS) → ej..: Cubiertas de protección
Sensores de seguridad
Sistemas de control de seguridad

Información del usuario → ej.: Manual de usuario

¿Las medidas de seguridad adopatadas dependen de un sistema de control? (SRP/CS)

No → Riesgo residual; ¿Surgen nuevos riesgos?

Si → Diseñar el sistema de control de seguridad de conformidad con la norma DIN EN ISO 13849

Diseñar el sistema de control de seguridad de conformidad con la norma DIN EN ISO 13849 → Riesgo residual; ¿Surgen nuevos riesgos?

SRP/CS (Safety-related parts of the control system)
Componente seguro del sistema de control que actúa sobre señales de entrada seguras y genera señales de salida seguras.

Diseño del sistema de control relativo a la seguridad (SRP/CS):

1. Determinación del nivel de cumplimiento (PL) requerido (PL_r)

(PL – Perfomance level) → Nivel de cumplimiento que especifica la capacidad de los componentes seguros de un sistema de control de ejecutar una función segura en condiciones previsibles

2. Elegir categoría

3. Determinar los componentes utilizados

4. Evaluación / considerar el nivel de coincidencia de diagnóstico

(DC – Diagnostic coverage) → Reducción de la probabilidad de fallos peligrosos de hardware que resulta de las pruebas de diganóstico automatizadas

5. Evaluación / considerar las solidez del sistema de control (CCF)

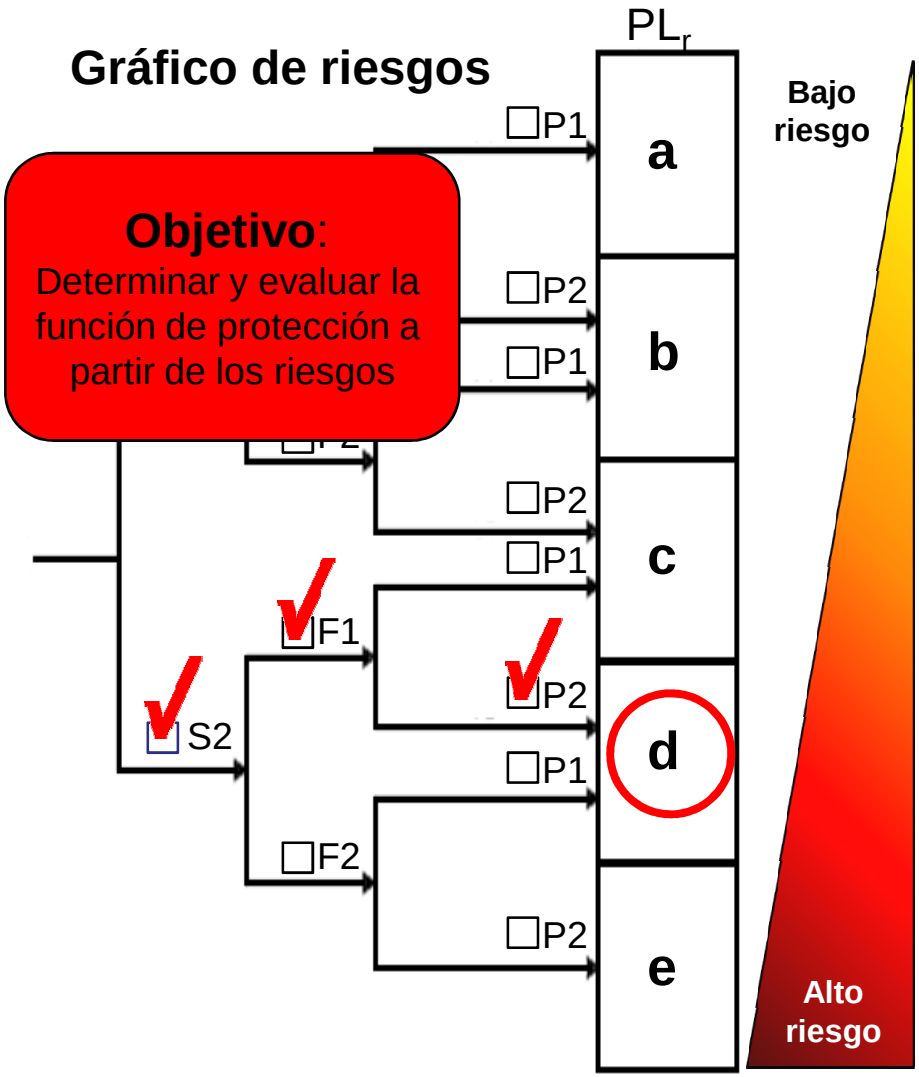
(CCF – Common Cause Faliure) → Fallo a consecuencia de una causa común (ej. Cortocircuito)

6. Verificación $PL \geq Pl_r$

7. Validación: ¿Se cumplen todos los requisitos?

Determinación del PL_r (*Required* Machine Performance Level)

Gráfico de riesgos



Objetivo:
Determinar y evaluar la función de protección a partir de los riesgos

Importancia de lesiones (S)

S1: Lesión de menor impo
general, reversible)
S2: Lesión grave (irrevers

Resultado:
Determinar el nivel de seguridad integral necesario

Frecuencia y/o tiempo de e

F1: Muy poca o poca frecuencia y/o corta exposición

F2: Mayor frecuencia hasta permanente y/o larga exposición

Posibilidad de evitar el peligro o minimización de daños (P)

P1: Posible en ciertas condiciones

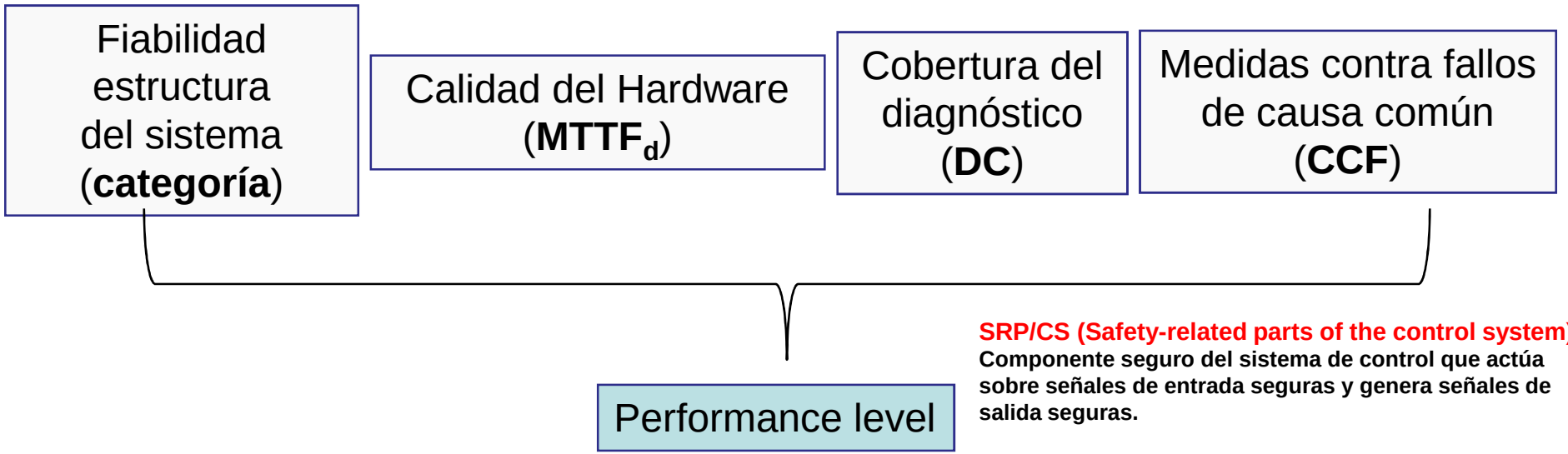
P2: Apenas posible

→ **La máquina debe cumplir el PL_d requerido**

Conseguir el PL (Performance Level – Nivel de cumplimiento)

El nivel de cumplimiento (para diseño SRP/CS) **es una medida de diferentes factores que determina la seguridad y fiabilidad del sistema**

El PL se mide principalmente en 4 cantidades auxiliares:



SRP/CS (Safety-related parts of the control system)
Componente seguro del sistema de control que actúa sobre señales de entrada seguras y genera señales de salida seguras.

MTTFd (Mean Time To Failure dangerous)
Tiempo medio hasta que se produce un fallo o fallo peligroso.

Categoría B y Categoría 1

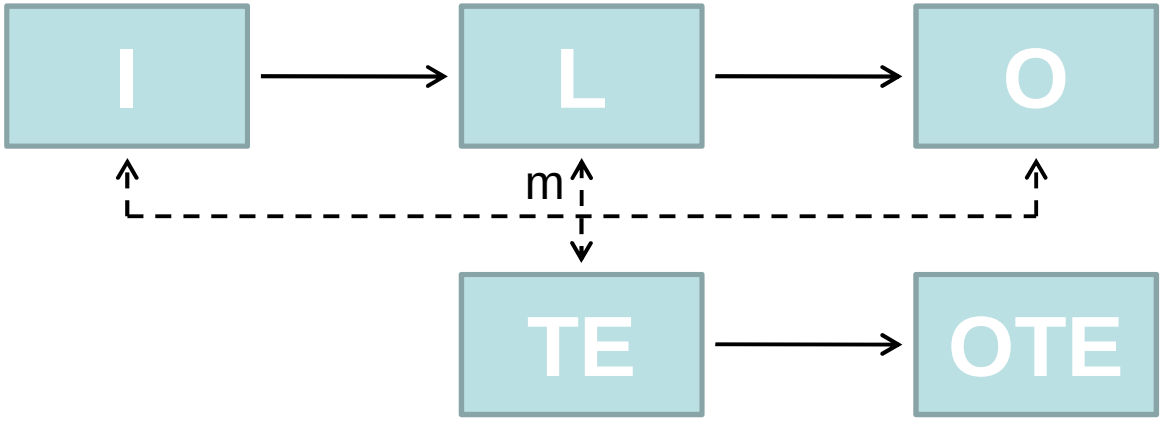
I = Dispositivo de entrada (ej. Sensor)
L = Lógica
O = Dispositivo de salida (ej. Contactor de potencia)

Categoría	Requisitos (resúmen)	Comportamiento del sistema	$MTTF_d$	DC_{avg}	CCF
B	Las partes del sistema de mando relativas a seguridad deben ser diseñadas, construidas, seleccionadas, montadas de acuerdo con las normas pertinentes de manera que puedan resistir las solicitudes de funcionamiento previstas. **Los principios fundamentales de seguridad deben ser aplicados.**	La aparición de un fallo puede conducir a la pérdida de la función de seguridad.	Medio o bajo	Nada	No relevante
1	Se deben aplicar los requisitos de la categoría B, además de **utilizar componentes** y principios de eficacia probada en seguridad.	La aparición de un fallo puede conducir a la pérdida de la función de seguridad. La probabilidad de que pueda producirse una avería es menor que en la categoría B.	Alto	Nada	No relevante

Principio de seguridad de estas categorías:

- Determinante: selección y aplicación de componentes adecuados

Categoría 2



TE = Equipo de chequeo
OTE = Salida de TE
m = Supervisión (comprobación)

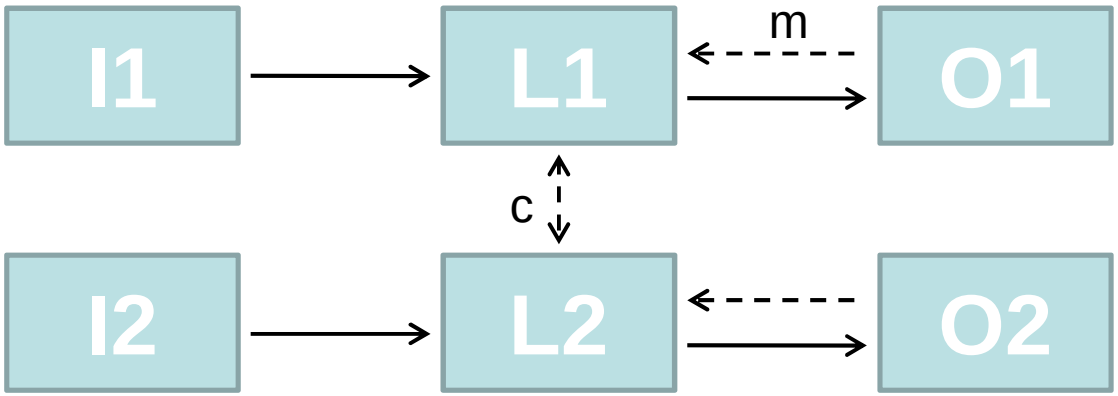
Línea discontínua = detección de fallos factible.

Categoría	Requisitos (resúmen)	Comportamiento del sistema	$MTTF_d$	DC_{avg}	CCF
2	Se deben aplicar los requisitos de la categoría B. Además las **funciones de seguridad se deben comprobar a intervalos mediante el sistema de control de la máquina.** El inicio de esta comprobación debe ser **automático**, a diferencia de lo indicado en su antecesora EN 954-1, donde se permitía el inicio manual.	La aparición de un defecto puede conducir a la pérdida de la función de seguridad en el intervalo entre 2 testeos El test detectará cualquier fallo.	Bajo a Alto	Bajo a medio	Debe ser comprobado

Principio de seguridad de esta categoría:

- Determinante: Arquitectura del sistema
  → Equipo de chequeo; supervisión (comprobación)

Categoría 3



c = Supervisión cruzada (validación)
m = Supervisión (comprobación)

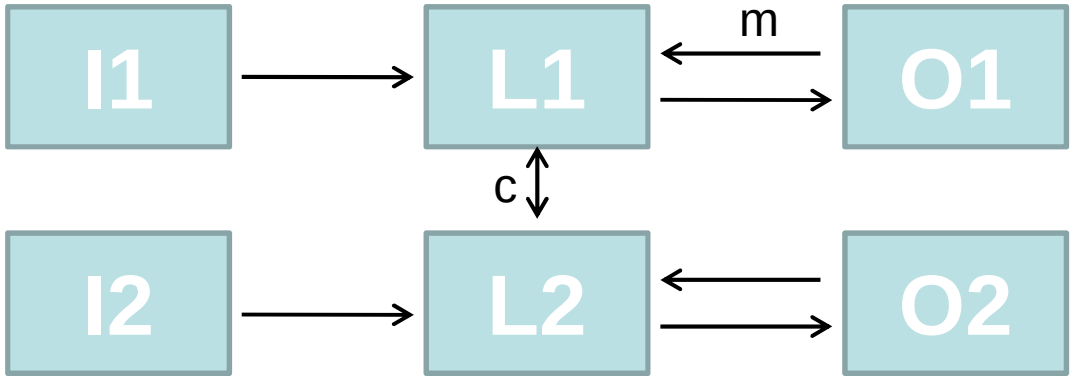
Línea discontínua = detección de fallos factible.

Categoría	Requisitos (resúmen)	Comportamiento del sistema	$MTTF_d$	DC_{avg}	CCF
3	Se deben aplicar los requisitos de la categoría B, además se deben aplicar los principios de eficacia probada en seguridad. Las partes del sistema de mando relativas a seguridad se deben diseñar de forma que: **1. un solo defecto en cualquiera de esta partes no conduzca a la pérdida de seguridad,** y **2. si la detección es factible, se debe detectar este defecto en el momento de producirse o antes de la siguiente función de seguridad**	Cuando se produce un sólo defecto, la función de seguridad se desempeña siempre. Se detectan algunos defectos, pero no todos. Una acumulación de defectos no detectados puede conducir a la pérdida de la función de seguridad.	Bajo a Alto	Bajo a medio	Debe ser comprobado

Principio de seguridad de esta categoría:

- Determinante: Arquitectura
  → Canal dual / redundancia

Categoría 4



c = Supervisión cruzada (validación)
m = Supervisión (comprobación)

Línea discontínua = detección de fallos factible.

Categoría	Requisitos (resúmen)	Comportamiento del sistema	$MTTF_d$	DC_{avg}	CCF
4	Se deben aplicar los requisitos de la categoría B, además se deben aplicar los principios de eficacia probada en seguridad. Las partes del sistema de mando relativas a seguridad se deben diseñar de forma que: **1. un solo defecto en cualquiera de esta partes no conduzca a la pérdida de seguridad,** y **2. dicho defecto debe ser detectado en el momento de producirse o antes de la siguiente solicitud de la función de seguridad. Si la detección no es posible, la acumulación de defectos no debe conducir a la pérdida de seguridad.**	Cuando se produce un sólo defecto, la función de seguridad se desempeña siempre. Si la acumulación de defectos es detectada, la función se seguridad será menos probable que falle(cobertura de diagnóstico alta).	Alto	Alto	Debe ser comprobado

Principio de seguridad de esta categoría:

- Determinante: Arquitectura

→ Canal dual / redundancia

$MTTF_d$ – Calidad del componente

Definición:

El valor del $MTTF_d$ representa el **tiempo medio hasta fallo peligroso** de cada canal

Se trata de un valor estadístico; no representa garantía en durabilidad del producto.

El valor $MTTF_d$ se divide en 3 categorías:

$MTTF_d$ categoría para cada canal	$MTTF_d$ rango para cada canal
Bajo	3 a 10 años
Medio	10 a 30 años
Alto	30 a 100 años

El valor PFH_D es casi equivalente: especifica la probabilidad de un fallo peligroso por hora – ej. La inversa de $MTTF_d$

NOTE: El valor máximo por canal es de 100 años para que la seguridad de las partes del sistema de mando relativas a seguridad no dependa sólo de la fiabilidad de los componentes, sino además de otros aspectos como la arquitectura

Este valor viene especificado por el fabricante del componente

DC – Nivel de coincidencia de diagnóstico

Definición:

Reducción de la probabilidad de fallos peligrosos de hardware que resulta de las pruebas de diagnóstico automatizadas.

$$DC = \frac{\text{Fallos peligrosos detectados}}{\text{Número total de fallos peligrosos}}$$

EL valor DC se divide en 4 categorías:

Categoría DC	Rango DC
Ninguna	< 60%
Baja	60% al < 90%
Media	90% al < 99%
Alta	99% y más

Para una estimación simplificada es suficiente con las tablas dadas en el Anexo E.1. de la EN 13849-1

CCF: Fallo a consecuencia de una causa común

Definición:

Fallo de varias unidades por una sóla incidencia, sin que se trate de fallos provocados recíprocamente entre las unidades

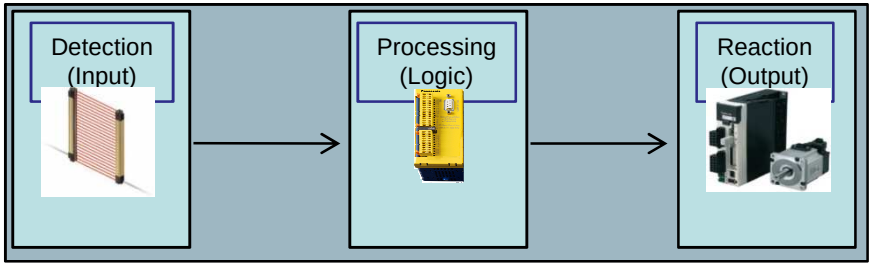
Las medidas para reducir el valor CCF se requiere en las Categorías 2, 3, y 4.

Para estimar el CCF se establece un método simplificado basado en un sistema de puntuación: Tabla F1 del Anexo F según Norma EN ISO 13849-1

⇨ ¡Se debe sumar un mínimo de 65 puntos!

EJEMPLO: Debido a un sobrecalentamiento, se produce un mal funcionamiento de dos sensores de forma independiente.

Cálculo del PL para una Función de Seguridad: 2 Métodos



Función de Seguridad

Método 1:

❖ Método de **Bloqueo**:

- Se requiere un cálculo exacto
- Se considera la totalidad del SRP/CS (Safety Relay Parts of Control System)
- Más apropiados para SRP/CS complejos interconexionados

Método 2:

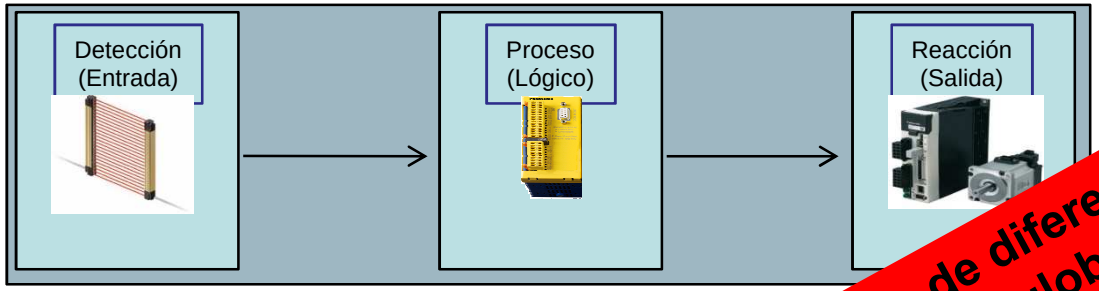
❖ Método de **Subsistema**

- Formulario simple para determinar el PL mediante tablas de combinación
- Si se conoce el valor PFH_D del subsistema, el PL se puede estimar de forma rápida.

El PFH_D viene especificado por el fabricante del componente

Total PL (Performance Level) - Método 1: Cálculo Bloqueo

Impacto del PFH_D en el PL (Performance Level – Nivel de Fiabilidad) total



Caso #1

PLe
$PFH_D = 2.2 \times 10^{-9}$

PLe
$PFH_D = 8.7 \times$

$PFH_D = 2.1 \times 10^{-9}$

$PFH_{D\ total} = 2.2 \times 10^{-9} + 8.7 \times 1$ $= 13 \times 10^{-9} = 1.3 \times 10^{-8}$ ➡ = PLe

Caso #2

PLe
P

PLe
$PFH_D = 6.78 \times 10^{-8}$

PLe
$PFH_D = 2.2 \times 10^{-8}$

P $.2 \times 10^{-8} + 6.78 \times 10^{-8} + 2.2 \times 10^{-8} = 11.18 \times 10^{-8} = 1.12 \times 10^{-7}$ ➡ = PLd

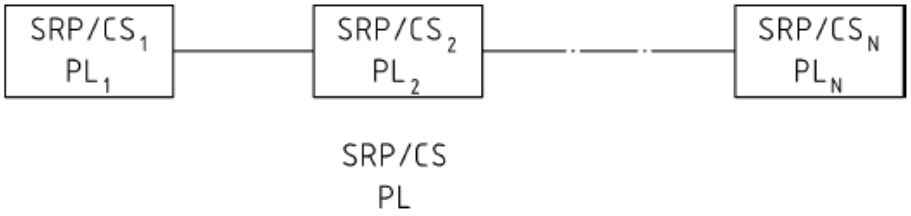
Este ejemplo demuestra que la suma de varios PLe de diferentes componentes de seguridad no asegura que el sistema global sea PLe

PLe = > 10^{-8} to < 10^{-7} (SIL3)

Determinar el PL en aplicación serie - Método 2: Búsqueda en tabla

Método de **Subsistema**

Este procedimiento se utiliza para determinar el PL de un conjunto de SRP/CS que ejecutan las funciones de seguridad



Pasos:

1. Determinar el PL más bajo; este es PL_{low}
2. Determinar el número $N_{low} \leq N$ del SRP/CS, con $Pl_i = PL_{low}$
3. Buscar PL en la tabla

PLe + PLe + PLe → PLe

Pl_{low}	N_{low}		PL
a	> 3	→	Imposible
	≤ 3	→	**a**
b	> 2	→	**a**
	≤ 2	→	**b**
c	> 2	→	**b**
	≤ 2	→	**c**
d	> 3	→	**c**
	≤ 3	→	**d**
e	> 3	→	**d**
	≤ 3	→	**e**

Determinación del Nivel de Seguridad Integral (SIL) según la norma IEC/EN 62061

Los factores de riesgo (Se, Fr, Pr y Av) constituyen los valores base en las dos normas. Dichos factores de riesgo se evalúan de diferentes maneras. Según EN 62061, se determina el nivel de seguridad integral requerido (**SIL**), según EN ISO 13849-1 el Perfomance Level (PL).

Riesgo,
Según el peligro localizado

=

Gravedad de la lesión **Se**

y

Frecuencia y duración	**Fr**
Probabilidad	**Pr**
Posibilidad de evitar el peligro	**Av**

Ejemplo - Paso 1 "Parada segura del husillo en el momento de abrir la cubierta de seguridad"

Frecuencia y/o duración (exposición al peligro) **(Fr)**		Probabilidad de la situación peligrosa **(Pr)**		Posibilidad de evitar el peligro **(Av)**	
≤ 1 hora	5	Frecuentemente	5		
> 1 hora a ≤ 1 día	5	Probable	4		
> 1 día a ≤ 2 semanas	4	Posible	3	Imposible	5
> 2 semanas a ≤ 1 año	3	Poco frecuente	2	Posible	3
> 1 año	2	Despreciable	1	Probable	1

Para obtener la clase (Cl), hay que sumar los valores, Fr, Pr y Av

Cl = 5 + 4 + 3 = 12

Definir el SIL requerido

Ejemplo - Paso 2

Objetivo:
Determinar y evaluar la función de protección a partir de los riesgos

Resultado:
Determinar el nivel de seguridad integral necesario

	Gravedad de la lesión **(Se)**	Clase (Cl) = F				
		3 to 4	5 to 7	8 to		15
, brazos	4	SIL 2	SIL 2	SIL		3
Permanente, pérdida de dedos de la mano	3			SIL 1	SIL 2	SIL 3
Reversible, tratamiento médico	2				SIL 1	SIL 2
Reversible, primeros auxilios	1					SIL 1

Punto de intersección: SIL 2

Procedimiento:

1. **Determinar la gravedad de la lesión (Se)**
2. **Encontrar el punto de intersección entre Se y Cl**

Comparación entre PL y SIL

Los niveles SIL y PL se pueden comparar el uno con el otro a partir del PFH_D (Probabilidad de Fallos Peligrosos)

Nivel de Fiabilidad ISO 13849 PL	Probabilidad de fallos peligrosos por hora (1/h) PFH_D	Nivel de Seguridad Integral IEC 62061 SIL
a	$\geq 10^{-5}$ to $< 10^{-4}$	-
b	$\geq 3*10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3*10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

Thank you!

Panasonic your partner in automation