Safety@Festo

Valoración y evaluación de funciones de seguridad según EN ISO 13849-1/EN 61508/EN 61511/EN 62061

FESTO

Evaluación de riesgos

Análisis de riesgos > Valoración > Reducción de riesgos

> Medidas constructivas

> Medidas técnicas

> Información para el usuario

Más información → **www.festo.com/safety-guideline**

Subfunciones de seguridad de la tecnología de accionamientos neumáticos

STO Safe torque off (desconexión segura del par)

PUS Prevención de puesta en marcha accidental

SSC Detención y cierre seguros

SDI Sentido seguro del movimiento

SSB Detención y bloqueo seguros

SLS Velocidad segura limitada

SLT Par seguro limitado

Subfunciones de seguridad de la técnica de actuadores eléctricos

STO Safe torque off (desconexión segura del par)

SS1 Parada segura 1

SS2 Parada segura 2

SDI Sentido seguro del movimiento

SSB Detención y bloqueo seguros

SLS Velocidad segura limitada

SLT Par seguro limitado (Safely-limited Torque)

Diagrama de bloques relacionado con la seguridad

Evento de activación → **Entrada** → **Lógica** → **Salida** → **Actuador**

¿Qué es lo que activa el requisito de seguridad?

Por ejemplo:
- Aproximación a un punto de peligro
- Apertura de una puerta de protección
- El proceso supera un valor límite definido

Un dispositivo que detecta la situación de activación:
- Barrera de luz
- Puerta de protección
- Alfombrillas de seguridad
- Parada de emergencia
- Error
- Escáner láser
- Cámara
- Sensor de temperatura
- Sensor de presión
- Sensor de caudal

Un dispositivo que procesa la señal de forma segura:
- Cableado
- Relé de seguridad
- PLC de seguridad
- Unidad de control neumática

Un dispositivo que controla de forma segura el movimiento peligroso
- Energía neumática
- Energía eléctrica
- Energía hidráulica
- Energía potencial (posición)

Seis pasos para la valoración de funciones de seguridad

EN ISO 13849-1 Aplicable a partes relativas a la seguridad de sistemas de control y a todo tipo de máquinas, independientemente de la tecnología y la energía utilizadas: eléctrica, neumática, hidráulica o mecánica.

EN 61508 Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.

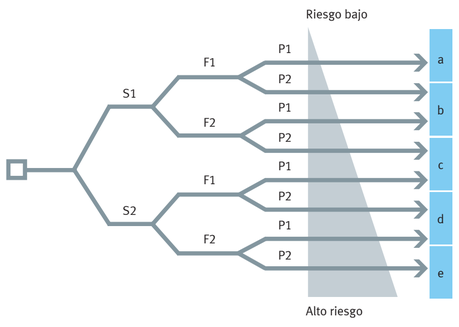
EN 61511 Seguridad funcional de sistemas instrumentados de seguridad para la industria de procesos.

EN 62061 Seguridad de las máquinas. Seguridad funcional de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad.

Valoración de la aplicación ↓

Valoración de la función de seguridad ↑

1 Evaluación de riesgos: determinación del nivel de prestaciones requerido (PL_r)



S Gravedad de la lesión
- S1 Lesión leve (normalmente reversible)
- S2 Lesión grave (normalmente irreversible e incluso mortal)

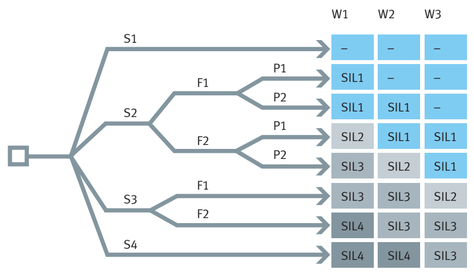
F Frecuencia y/o duración de la exposición al peligro
- F1 Exposición infrecuente a poco frecuente y/o duración breve
- F2 Exposición frecuente a permanente y/o duración larga

P Posibilidad de evitar el peligro
- P1 Posible en determinadas condiciones
- P2 Apenas posible

a – e Nivel de prestaciones (PL_r)

Fuente: EN ISO 13849-1

Evaluación de riesgos: determinación del nivel de integridad de la seguridad requerido (SIL_r)



SIL (nivel de integridad de seguridad)
Cuatro niveles discretos (SIL1 a SIL4). Cuanto más alto sea el valor SIL de un circuito de seguridad, mayor será la capacidad de las funciones de seguridad implementadas para evitar un daño o, por lo menos, para reducirlo.

S Alcance del daño
- S1 Lesión leve de una persona
- S2 Lesiones graves de varias personas, incluso la muerte de una persona
- S3 Muerte de varias personas
- S4 Consecuencias catastróficas con numerosos muertos

F Probabilidad de estancia en la zona de peligro
- F1 Poco frecuente a ligeramente frecuente
- F2 Frecuente a permanente

P Protección/prevención de peligros
- P1 Posible en determinadas condiciones
- P2 Apenas posible

W Probabilidad de ocurrencia
- W1 Relativamente alta
- W2 Baja
- W3 Muy baja

2 Determinación de los parámetros de fiabilidad requeridos de PL_r y SIL_r

Determinación de $MTTF_D$ = tiempo medio hasta un fallo (peligroso)

Determinación de PL = nivel de prestaciones	DC < 60 % ninguno	DC < 60 % ninguno	60 % ≤ DC <90 % bajo	90 % ≤ DC <99 % medio	60 % ≤ DC <90 % bajo	90 % ≤ DC <99 % medio	99 % ≤ DC alto
a							
b							
c							
d							
e							
	Cat. B	Cat. 1	Cat. 2		Cat. 3		Cat. 4
	CCF, no relevante		CCF ≥ 65 %				

Valoración	$MTTF_D$
Bajo	3 años ≤ $MTTF_D$ < 10 años
Medio	10 años ≤ $MTTF_D$ < 30 años
Alto	30 años ≤ $MTTF_D$ < 100 años

Fuente: EN ISO 13849-1

Determinación de los parámetros de fiabilidad requeridos de PL_r y SIL_r

Nivel SIL	Modo de alta demanda	Fallo máx. aceptable del sistema de seguridad	Tipo de equipo A – Safe Failure Fraction (SFF) < 60 %	60…90 %	90…99 %	>99 %	Tipo de equipo B – Safe Failure Fraction (SFF) < 60 %	60…90 %	90…99 %	>99 %	Modo de baja demanda	Fallo máximo aceptable del sistema de seguridad
	$10^{-5} \le PFH < 10^{-4}$	Un riesgo de fallo cada 10 000 horas										
1	$3 \cdot 10^{-6} \le PFH < 10^{-5}$	Un riesgo de fallo cada 1250 días	HFT 0				HFT 1	HFT 0			$10^{-2} \le PFH < 10^{-1}$	Una vez cada 10 años
1	$10^{-6} \le PFH < 3 \cdot 10^{-6}$	Un riesgo de fallo cada 115,74 años										
2	$10^{-7} \le PFH < 10^{-6}$	Un riesgo de fallo cada 115,74 años	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \le PFH < 10^{-2}$	Una vez en 100 años
3	$10^{-8} \le PFH < 10^{-7}$	Un riesgo de fallo cada 1157,41 años	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \le PFH < 10^{-3}$	Una vez en 1000 años
4	$10^{-9} \le PFH < 10^{-8}$	Un riesgo de fallo cada 11 157,41 años		HFT 2	HFT 1 HFT 2	HFT 1 HFT 2			HFT 2	HFT 1 HFT 2	$10^{-5} \le PFH < 10^{-4}$	Una vez en 10 000 años

[por hora]

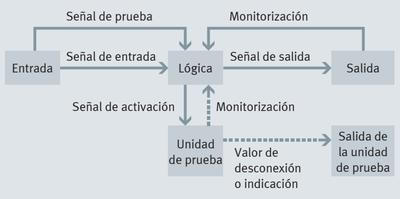
Tipo de equipo A
Equipo para el que se ha determinado de forma suficiente el comportamiento de fallo de todos los componentes utilizados y el comportamiento de error.

Tipo de equipo B
Equipo para el que no se ha determinado de forma suficiente el comportamiento de al menos uno los componentes utilizados, ni el comportamiento en caso de error.

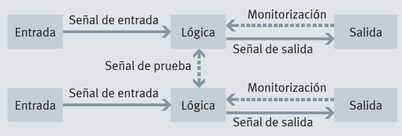
3 Estructura de control: determinación de la categoría

Categoría B/categoría 1

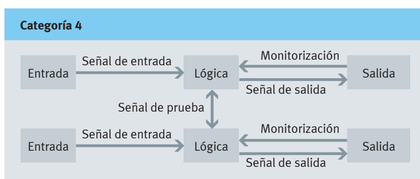
Categoría 2



Categoría 3

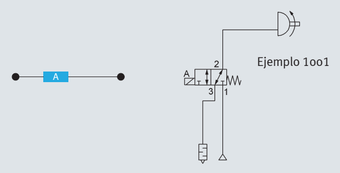


Categoría 4



HFT: determinación de la tolerancia de error del hardware

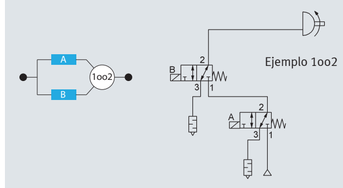
HFT 0



1oo1 (uno de uno)

Un único error puede causar una pérdida de seguridad.

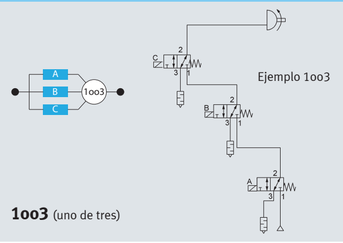
HFT 1



1oo2 (uno de dos)

Deben ocurrir por lo menos 2 errores simultáneos para que se produzca una pérdida de seguridad.

HFT 2



1oo3 (uno de tres)

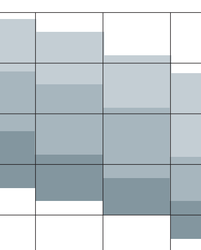
Deben ocurrir por lo menos 3 errores simultáneos para que se produzca una pérdida de seguridad.

HFT (Hardware Failure Tolerance)
Capacidad de seguir ejecutando una función requerida en caso de errores y desviaciones

4 Medidas para el control y la detección de errores

Medidas contra fallos con causa común (CCF)

Medidas	Puntos
Separación/segregación	15
Diversidad	20
Diseño/aplicación	20
Evaluación/análisis	5
Competencia/formación	5
Entorno/influencias	35



Cobertura del diagnóstico (DC)

Componente

- ¿Qué errores pueden producirse?
- ¿Son peligrosos los errores?
- ¿Es posible detectar los errores peligrosos?

$$DC_1 = \frac{\Sigma \text{ (error peligroso detectado)}}{\Sigma \text{ (error peligroso total)}}$$

Sistema completo

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots\ldots + \frac{DC_n}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots\ldots + \frac{1}{MTTF_{DN}}}$$

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_D + \lambda_S}$$

$DC \le SFF \le 1$

para $\lambda_S \to SFF = DC$
para $\lambda_D \to SFF = 1$

Safe Failure Fraction (SFF): determinación de la proporción de errores

Modo de alta demanda

FME(D)A

Tipo de fallo	Detectado	No detectado
Seguro λ_S	Seguro Detectado λ_{SD}	Seguro No detectado λ_{SU}
Peligroso λ_D	Peligroso Detectado λ_{DD}	Peligroso No detectado λ_{DU}

$$SFF = \frac{\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}}{\Sigma\lambda_{total}} \qquad DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}$$

Modo de baja demanda

FME(D)A

Tipo de fallo	Detectado	No detectado
Seguro λ_S	Seguro Detectado λ_{SD}	Seguro No detectado λ_{SU}
Peligroso λ_D	Peligroso Detectado λ_{DD}	Peligroso No detectado λ_{DU}

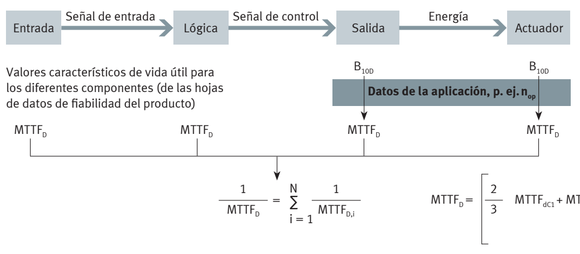
$$SFF = \frac{\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}}{\Sigma\lambda_{total}} \qquad DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_D}$$

λ **(tasas de fallo)**
λ_S: tasa total de fallos seguros
λ_D: tasa total de fallos peligrosos
λ_{SD}: tasa total de fallos seguros detectados
λ_{SU}: tasa total de fallos seguros no detectados
λ_{DD}: tasa total de fallos peligrosos detectados
λ_{DU}: tasa total de fallos peligrosos no detectados

FME(D)A
(Failure Modes, Effects and Diagnostics Analysis)
Método de análisis para la determinación cuantitativa de tipos y tasas de fallos

SFF
(Safe Failure Fraction)
Proporción de errores seguros en el número total de errores

5 $MTTF_D$: determinación del tiempo medio hasta un fallo



Valores característicos de vida útil para los diferentes componentes (de las hojas de datos de fiabilidad del producto)

$$MTTF_D = \frac{B_{10D}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\ s/h}{t_{ciclo}}$$

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D,i}}$$

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

$MTTF_D$ (Mean Time to Failure)
Tiempo medio hasta un fallo peligroso

MTTR (Mean Time to Restoration)
Tiempo medio de reparación

$MTBF = MTTF + MTTR$

para MTTF ›› MTTR es válido MTBF = MTTF

Fórmula para calcular el valor $MTTF_D$ para un elemento mecánico en un canal

Cantidad media de activaciones anuales n_{op} del elemento mecánico

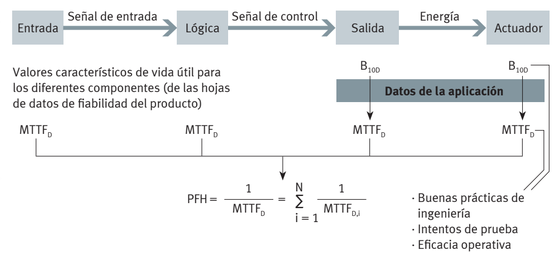
$PFH = \frac{1}{MTTF_D}$

Cálculo de $MTTF_D$ total con varios canales paralelos

Valoración $MTTF_D$
Bajo: 3 años ≤ $MTTF_D$ < 10 años
Medio: 10 años ≤ $MTTF_D$ < 30 años
Alto: 30 años ≤ $MTTF_D$ < 100 años
(Fuente: EN ISO 13849-1)

PFH/PFD: determinación de la probabilidad de fallo

Modo de alta demanda



Valores característicos de vida útil para los diferentes componentes (de las hojas de datos de fiabilidad del producto)

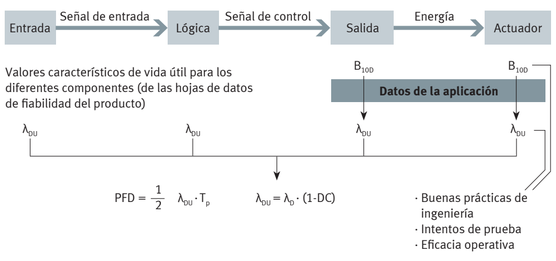
$$PFH = \frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{D,i}}$$

- Buenas prácticas de ingeniería
- Intentos de prueba
- Eficacia operativa

PFH (Probability of failure per hour)
Probabilidad de fallo por hora de una función de seguridad

MTBF (Mean Time between Failure)
Tiempo medio entre dos fallos consecutivos

Modo de baja demanda



Valores característicos de vida útil para los diferentes componentes (de las hojas de datos de fiabilidad del producto)

$$PFD = \frac{1}{2}\ \lambda_{DU} \cdot T_p \qquad \lambda_{DU} = \lambda_D \cdot (1\text{-}DC)$$

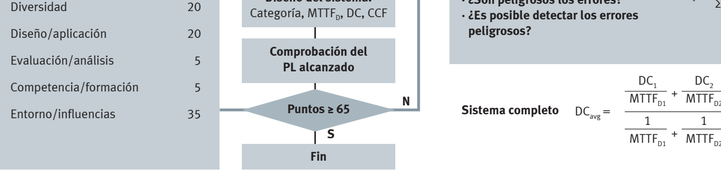
- Buenas prácticas de ingeniería
- Intentos de prueba
- Eficacia operativa

PFD (Probability of Failure on Demand)
Probabilidad de fallo de una función de seguridad

T_p (Proof test interval)
Intervalo de comprobación

6 Sistema completo, objetivo: PL ≥ PL_r

Ejemplo de diseño de un circuito de seguridad



Entrada	Lógica	Salida	Actuador
$B10_D$		$B10_D$	
		$MTTF_D$	
$MTTF_D$		$MTTF_D$ por canal	
Cat.		Cat.	
DC		DC	
CCF		CCF	
PL	PL	PL	

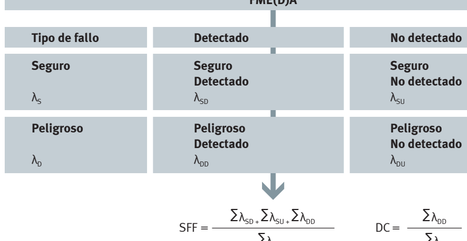
Se determina en función de la aplicación

Información ofrecida por el fabricante (la información para determinar el valor $B10_D$ debe ser proporcionada por el fabricante)

PL ≥ PL_r

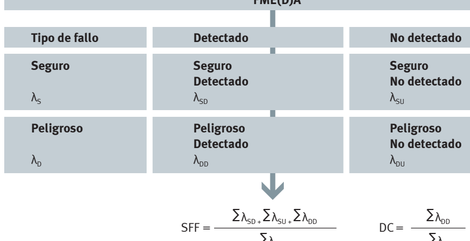
Objetivo: SIL ≥ SIL_r

Distribución habitual de la PFH entre los subsistemas de una función de seguridad en sistemas de un canal



Sensor ≥ 35 %		Lógica ≥ 15 %		Actuador ≥ 50 %	
PFH	λ_{SD}	PFH	λ_{SD}	PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
$SIL_{requerido}$ (SIL_r)					
PFH_{total}					

Distribución habitual de la PFD entre los subsistemas de una función de seguridad en sistemas de un canal



Sensor ≥ 35 %		Lógica ≥ 15 %		Actuador ≥ 50 %	
PFD	λ_{SD}	PFD	λ_{SD}	PFD	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
$SIL_{requerido}$ (SIL_r)					
PFD_{total}					

SIL ≥ SIL_r

Al convertir el PL al SIL o viceversa deben tenerse en cuenta los requisitos adicionales de las normas utilizadas (EN ISO 13849-1, EN 61508, EN 61511, EN 62061).

www.festo.com