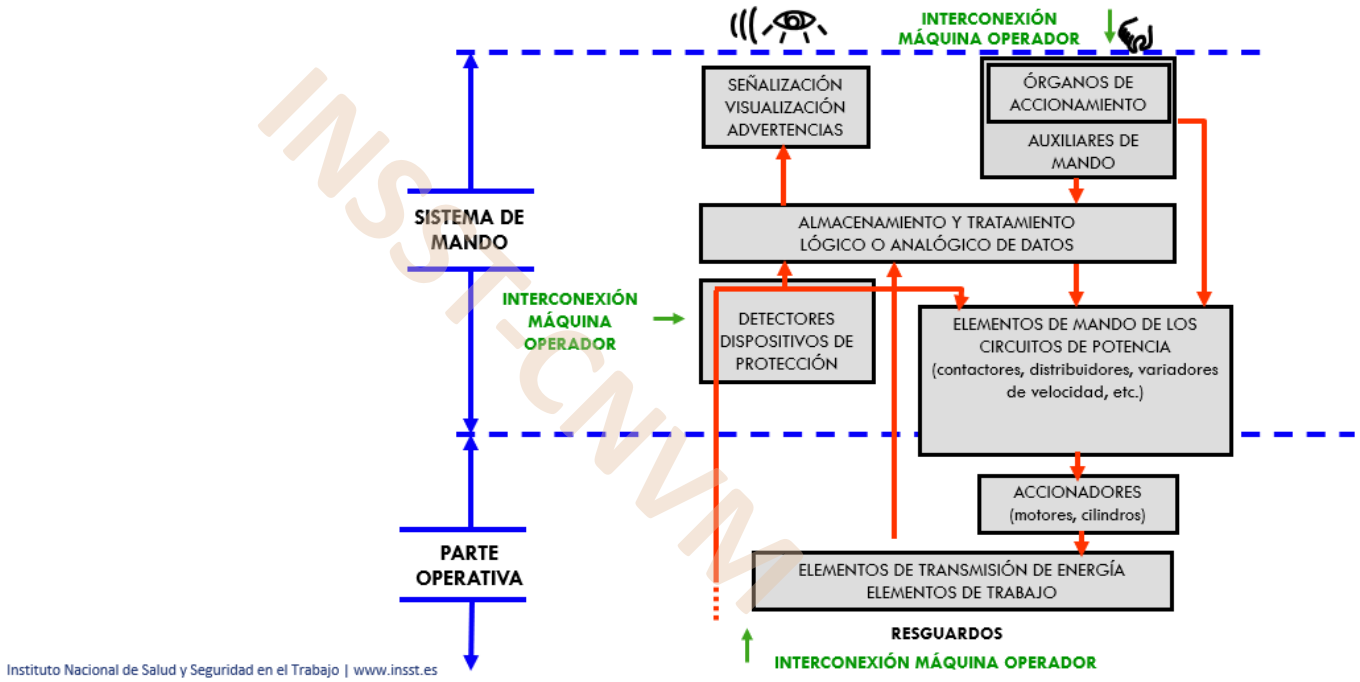
Curso Seguridad en Máquinas
CNVM - 13 y 14 de junio de 2024

PARTES DE LOS SISTEMAS DE MANDO RELATIVAS A LA SEGURIDAD

GOBIERNO DE ESPAÑA · MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL · insst Instituto Nacional de Seguridad y Salud en el Trabajo

Ibon Unzueta Estébanez - CNVM

SISTEMA DE MANDO



PARTE DE UN SISTEMA DE MANDO RELATIVA A LA SEGURIDAD

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

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

NOTA 1 Las partes combinadas de un sistema de mando relativas a la seguridad comienzan en los puntos en los que se generan las señales de entrada relativas a la seguridad (incluyendo, por ejemplo la leva de accionamiento y la roldana de un interruptor de posición) y terminan a la salida de los elementos de mando de los accionadores (incluyendo, por ejemplo, los contactos principales de un contactor).

NOTA 2 Si se utilizan sistemas de control para los diagnósticos, éstos también se consideran SRP/CS.

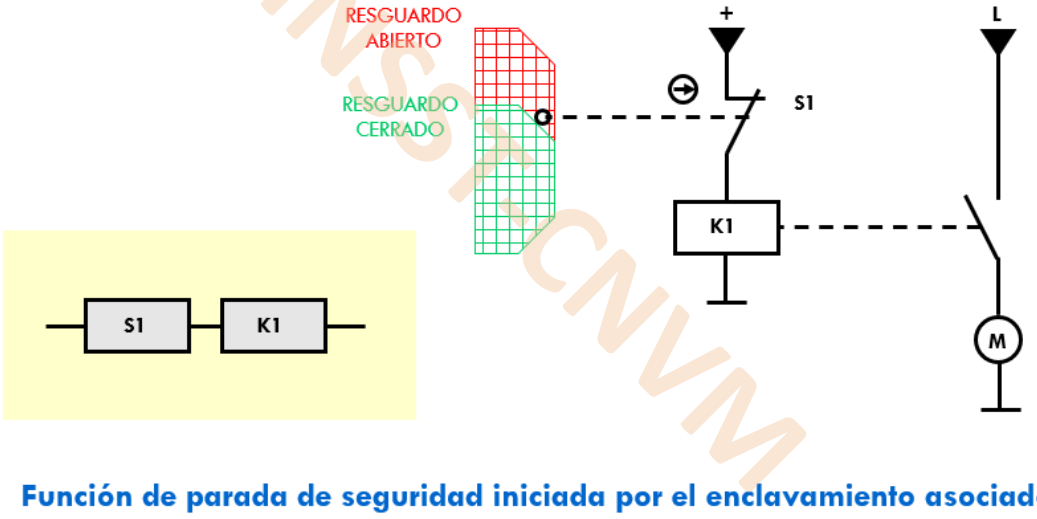
FUNCIÓN DE SEGURIDAD

Función de seguridad

Función de una máquina cuyo fallo podría dar lugar a un aumento inmediato del (de los) riesgo(s).

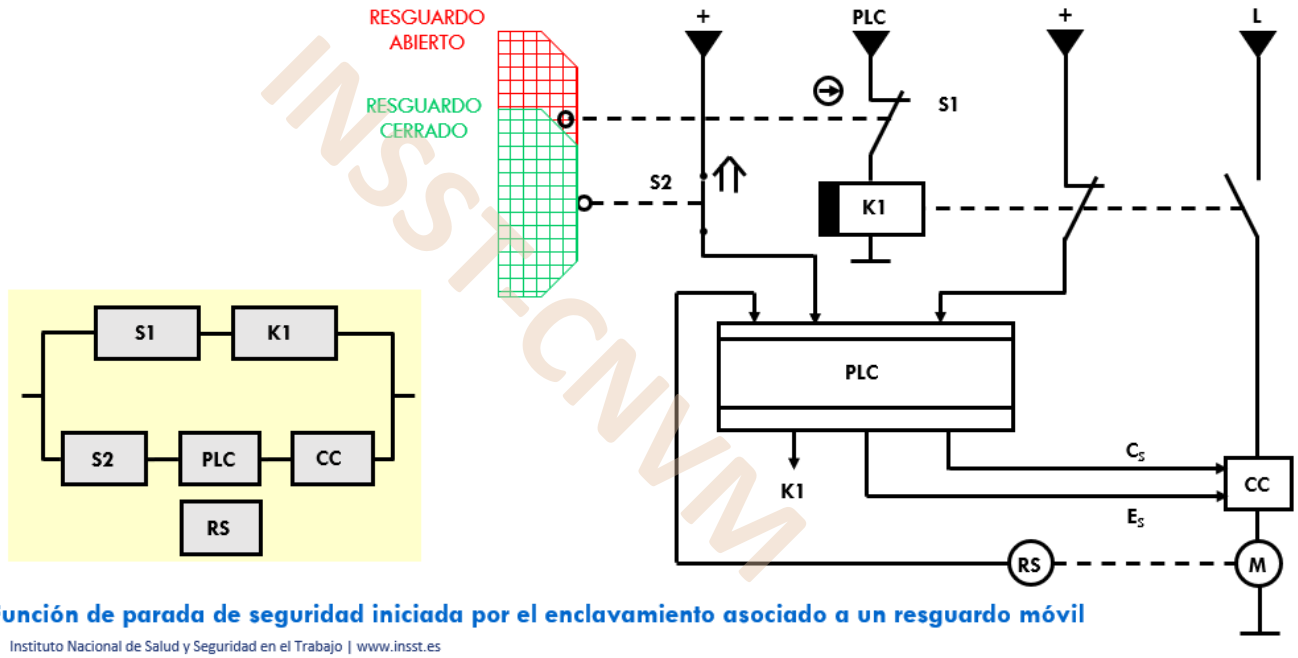
- Función de parada relativa a la seguridad iniciada por un protector
- Función de rearme manual
- Función de puesta en marcha/ nueva puesta en marcha
- Función de inhibición
- Función de mando sensitivo
- Función de validación
- Prevención de una puesta en marcha intempestiva
- Modos de mando y su selección
- Función de parada de emergencia

EJEMPLO 1



Función de parada de seguridad iniciada por el enclavamiento asociado a un resguardo móvil

EJEMPLO 2



Función de parada de seguridad iniciada por el enclavamiento asociado a un resguardo móvil

NORMA EN ISO 13849-1

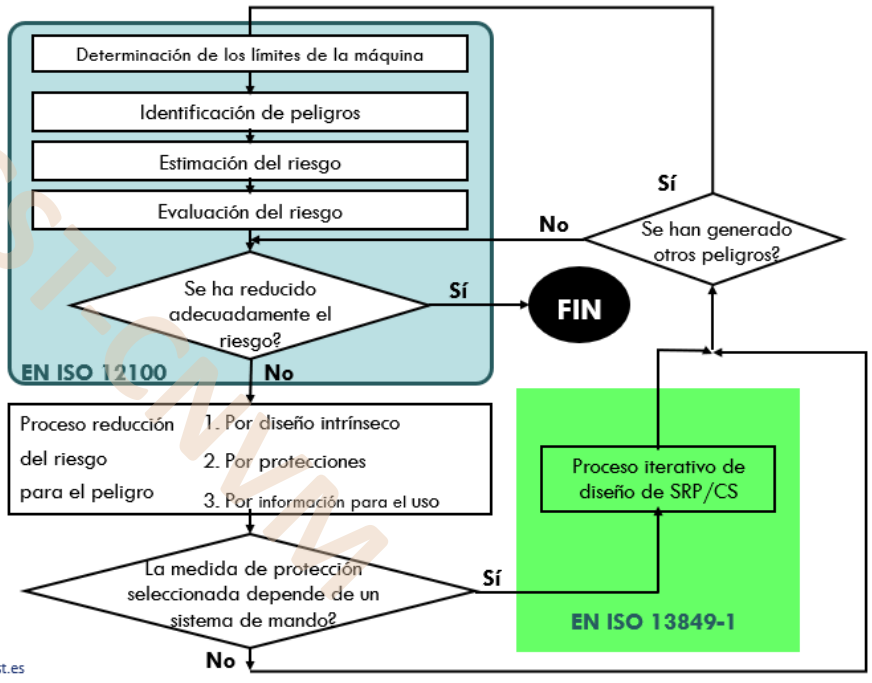
UNE
Normalización Española

Norma Española
UNE-EN ISO 13849-1
Marzo 2024

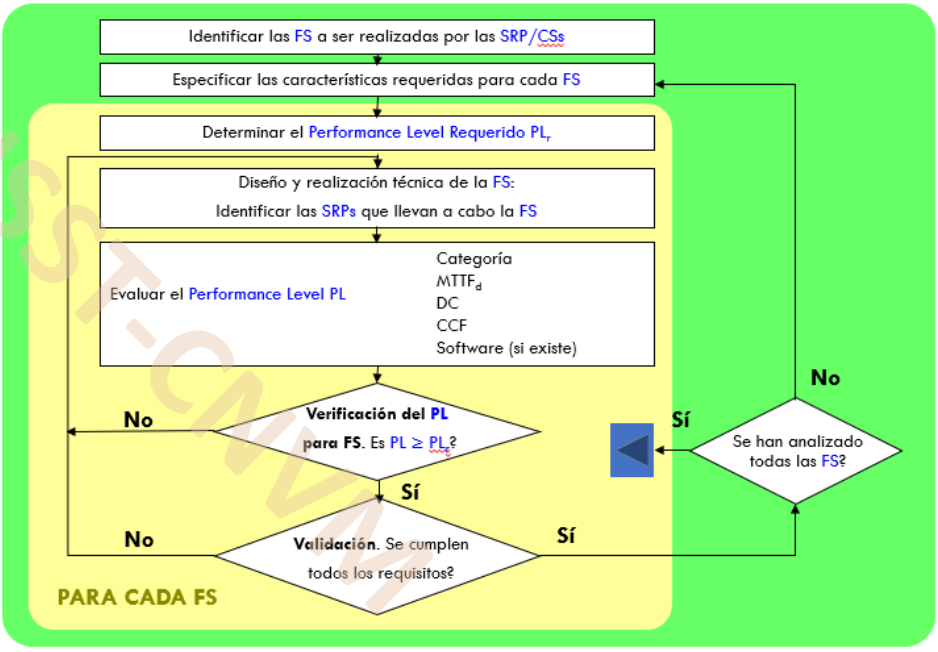
Seguridad de las máquinas
Partes de los sistemas de mando relativas a la seguridad
Parte 1: Principios generales para el diseño
(ISO 13849-1:2023)

Esta norma ha sido elaborada por el comité técnico CTN-UNE 81 *Seguridad y salud en el trabajo*, cuya secretaría desempeña INSST.

Visión de la Evaluación de Riesgos Reducción de Riesgos



Visión de la Evaluación de Riesgos
Reducción de Riesgos

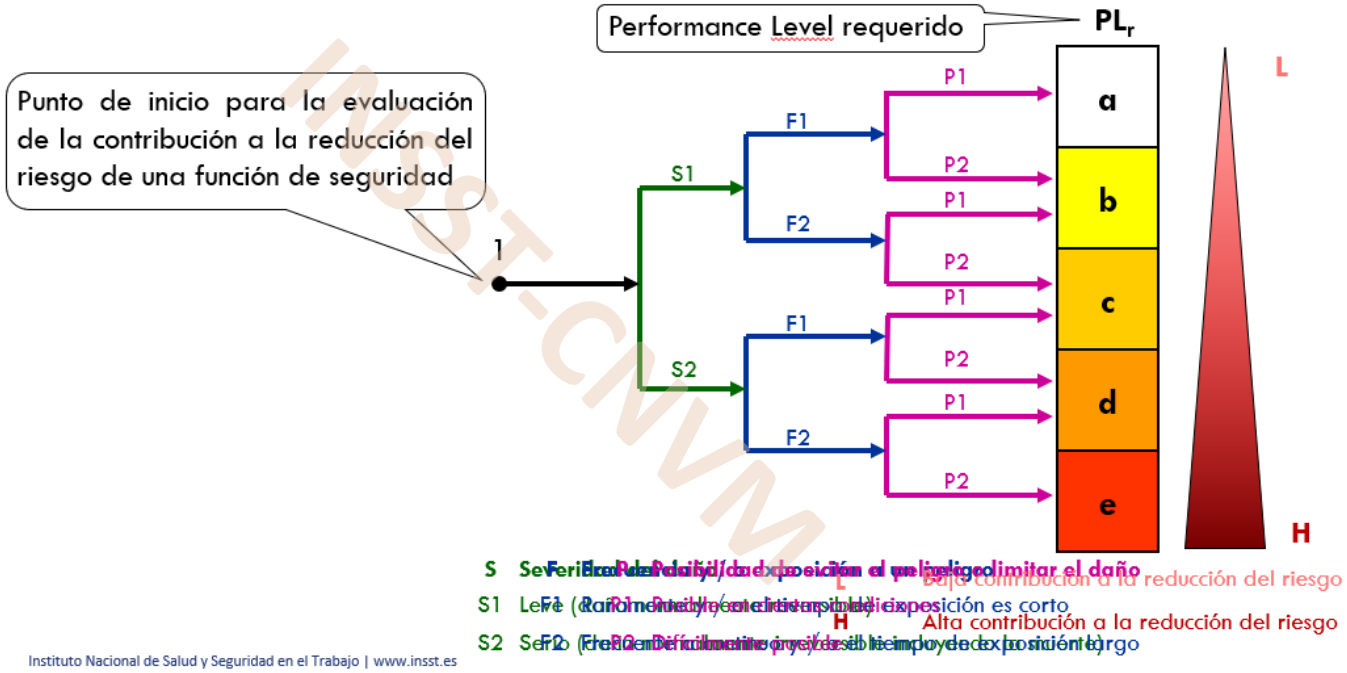


Nivel de Prestaciones
Performance Level - PL

Nivel discreto para especificar la capacidad de las partes de los sistemas de mando relativas a la seguridad para desempeñar una función de seguridad en condiciones previsibles.

Performance level (PL)	Probabilidad media de fallo peligroso por hora 1/h
a	$\geq 10^{-5}$ a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
e	$\geq 10^{-8}$ a $< 10^{-7}$
Nota: Además de la probabilidad media de fallo peligroso por hora también son necesarias otras medidas para lograr el PL	

Gráfico del riesgo para determinar el PL requerido para cada función de seguridad



PROCESO DE DISEÑO
EVALUACIÓN DEL NIVEL DE PRESTACIONES

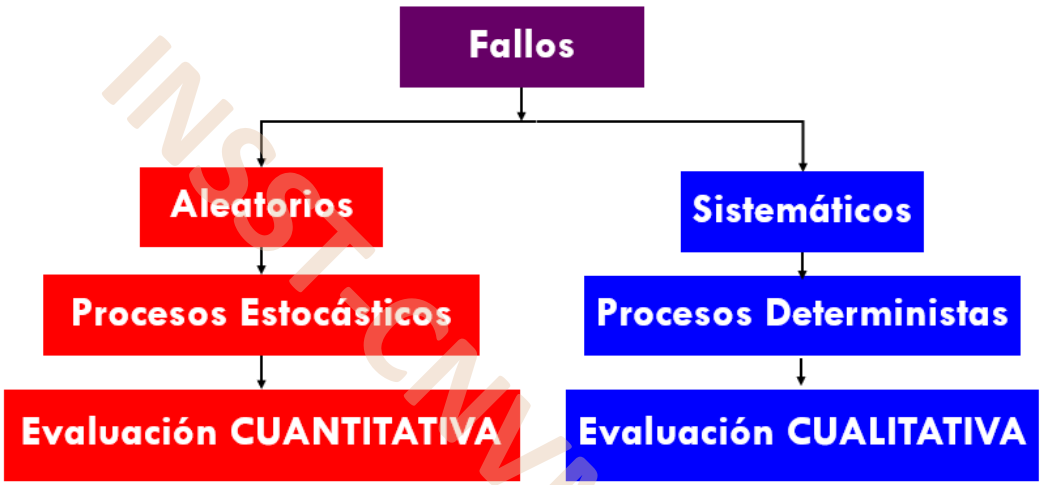
a) Aspectos cuantificables

- Estructura (categoría)
- $MTTF_d$ de los componentes (fallos aleatorios)
- La cobertura de diagnóstico (DC), frecuencia de los diagnósticos
- Fallos de causa común (CCF), a través del factor β
- Frecuencia de solicitación de la función de seguridad
- Duración de la misión

b) Aspectos no cuantificables

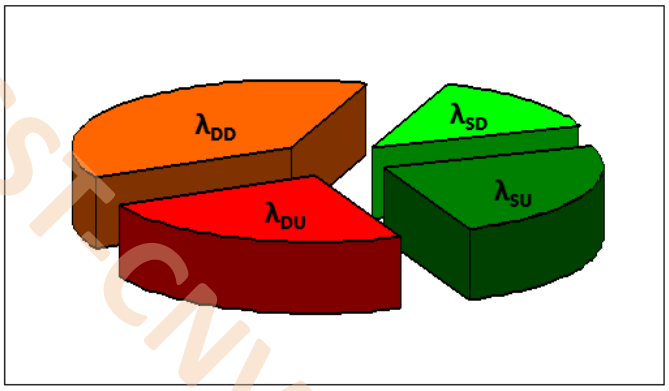
- El comportamiento de la función de seguridad en condiciones de defecto
- El soporte lógico de seguridad
- La aptitud para desempeñar la función de seguridad en las condiciones ambientales previstas
- Los fallos sistemáticos

CLASIFICACIÓN DE LOS FALLOS
SEGÚN NORMAS EN, ISO, CEI



CLASIFICACIÓN DE LOS FALLOS SEGÚN NORMAS EN, ISO, CEI

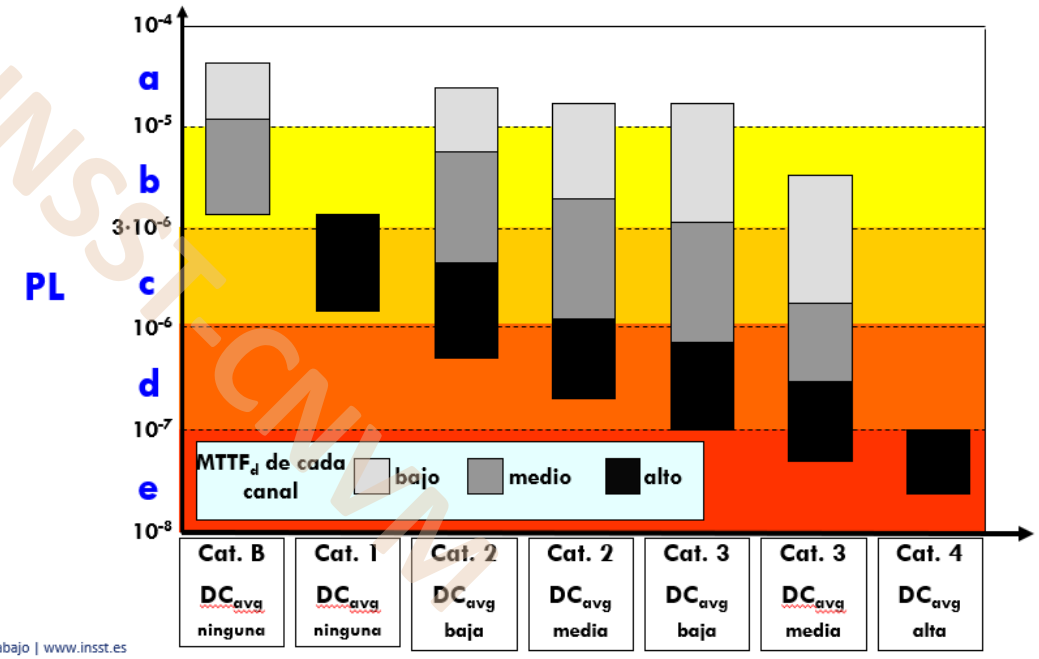
λ = Tasa de Fallos = λ_D (fallos peligrosos) + λ_S (fallos seguros)



λ_D Fallos peligrosos
- λ_{DD} Fallos peligrosos detectados
- λ_{DU} Fallos peligrosos no detectados

λ_S Fallos seguros
- λ_{SD} Fallos seguros detectados
- λ_{SU} Fallos seguros no detectados

Relación entre categorías, DC_{avg}, $MTTF_d$ de cada canal y PL



Método simplificado

a) Definir la **CATEGORIA** de la combinación de SRP/CS, en base a la arquitectura adoptada

b) Estimar el **$MTTF_d$** de cada canal

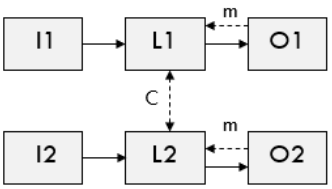
c) Estimar la **DC_{media}** del conjunto de la combinación de SRP/CS

d) Adoptar las medidas suficientes contra los **CCF** (fallos de causa común)

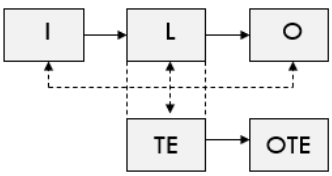
Clasificación de las partes de los sistemas de mando relativas a la seguridad con respecto a su resistencia a fallos y el consiguiente comportamiento en condición de fallo, y que es lograda por una disposición estructural de las partes, por la detección de fallos y/o por su fiabilidad.

Categorías B y 1

Categorías 3 y 4



Categoría 2



Dos salidas independientes

$$\text{Tasa de solicit.} \leq \frac{1}{100} \cdot \text{Tasa de verific.}$$

$$MTTF_{d,TE} > \frac{MTTF_{d,L}}{2}$$

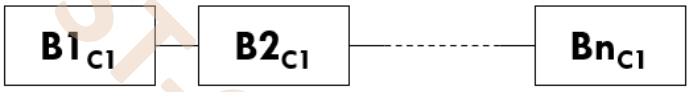
MTTF$_d$ de un componente

Valor probable (esperado) de la duración media hasta un fallo peligroso del componente.

El MTTF$_d$ se calcula a partir del MTTF cuando conocemos cual es el porcentaje de fallos peligrosos en el conjunto de los modos de fallo de un componente.

Denotación de MTTF$_d$ de cada canal	Rango de MTTF$_d$ de cada canal
Bajo	3 años ≤ MTTF$_d$ < 10 años
Medio	10 años ≤ MTTF$_d$ < 30 años
Alto	30 años ≤ MTTF$_d$ ≤ 100 años

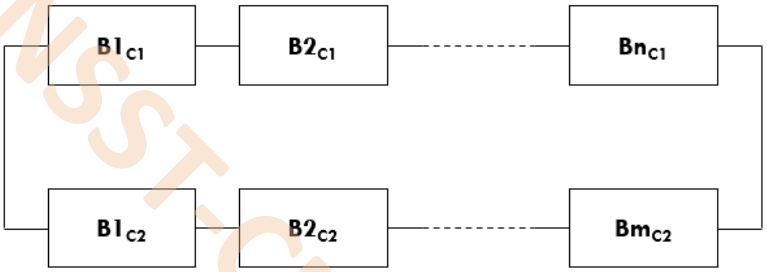
MTTF$_d$ de un canal. Categoría B, 1 y 2



$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,B1_{C1}}} + \frac{1}{MTTF_{D,B2_{C1}}} + \ldots\ldots + \frac{1}{MTTF_{D,Bn_{C1}}}$$

$MTTF_d$ de cada canal

$MTTF_d$ de un canal. Categoría 3 y 4

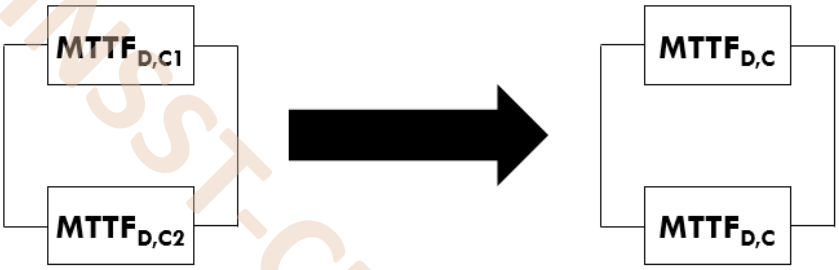


$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,B1_{C1}}} + \frac{1}{MTTF_{D,B2_{C1}}} + ... + \frac{1}{MTTF_{D,Bn_{C1}}}$$

$$\frac{1}{MTTF_{D,C2}} = \frac{1}{MTTF_{D,B1_{C2}}} + \frac{1}{MTTF_{D,B2_{C2}}} + ... + \frac{1}{MTTF_{D,Bm_{C2}}}$$

$MTTF_d$ de cada canal

$MTTF_d$ de un canal. Categoría 3 y 4



Fórmula de Simetrización

$$MTTF_{D,C} = \frac{2}{3}\left[MTTF_{D,C1} + MTTF_{D,C2} - \frac{1}{\frac{1}{MTTF_{D,C1}} + \frac{1}{MTTF_{D,C2}}}\right]$$

Cobertura de diagnóstico (DC)

Cobertura de diagnóstico (DC)

Medida para la efectividad de los diagnósticos, puede ser determinada como una relación entre la tasa de fallos de los fallos peligrosos detectados y la tasa de fallos peligrosos totales. La DC varía entre 0 y 1.

$$DC = \frac{\lambda_{DD}}{\lambda_D}$$

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d_1}} + \frac{DC_2}{MTTF_{d_2}} + ... + \frac{DC_n}{MTTF_{d_n}}}{\frac{1}{MTTF_{d_1}} + \frac{1}{MTTF_{d_2}} + ... + \frac{1}{MTTF_{dn}}}$$

Denotación de DC	Rango de DC
Ninguna	DC < 60 %
Baja	60 % ≤ DC < 90 %
Media	90 % ≤ DC < 99 %
Alta	99 % ≤ DC

$$DC_{avg} = \frac{\sum_{i=1}^{n} \lambda_{DD_i}}{\sum_{i=1}^{n} \lambda_{D_i}}$$

Estimación de Fallos de Causa Común (CCF)

Fallo de causa común (CCF)

Fallo de varios elementos, que resultan de un suceso y que no son consecuencia unos de otros.

Los fallos de causa común se representan mediante el factor Beta. Este factor varía entre 0 y 1.

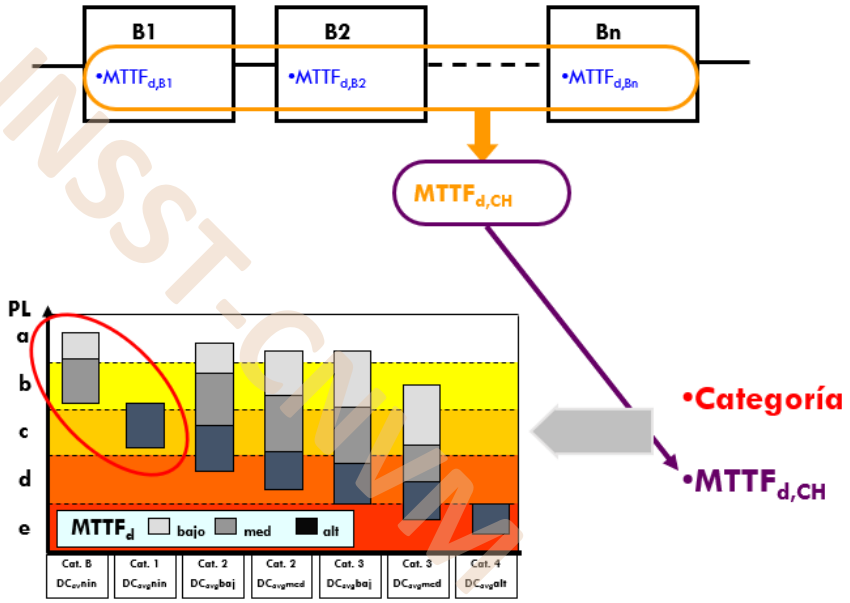
$$\beta = \frac{\lambda_C}{\lambda} \quad \Rightarrow \quad \lambda_C = \beta \cdot \lambda \quad \text{y} \quad \lambda_N = (1 - \beta) \cdot \lambda$$

En el método simplificado se considera que si se implementan suficientes medidas del Anexo F en el conjunto del sistema, el factor β es igual o inferior a 2%.

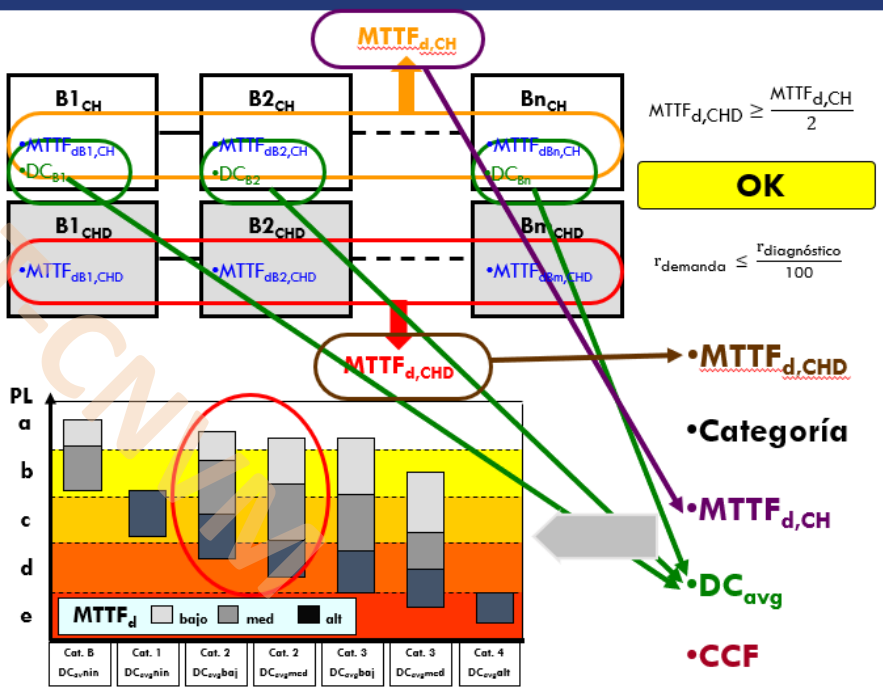
Fallos de Causa Común (CCF)

Nº	Medida contra CCF	Puntos
1	Separación / Segregación	15
2	Diversidad	20
3	Diseño / Aplicación / Experiencia	20
4	Evaluación / Análisis	5
5	Competencia / Formación	5
6	Entorno	35
	Máximo Total	100

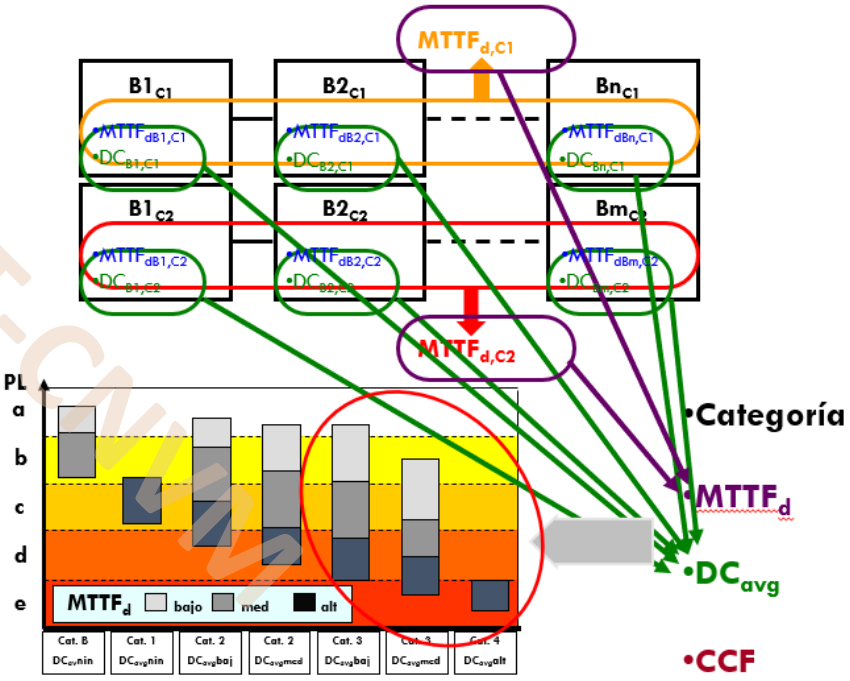
TOTAL < 65 puntos ▶ requisitos adicionales



MÉTODO SIMPLIFICADO: CATEGORÍA 2



MÉTODO SIMPLIFICADO: CATEGORÍAS 3 y 4



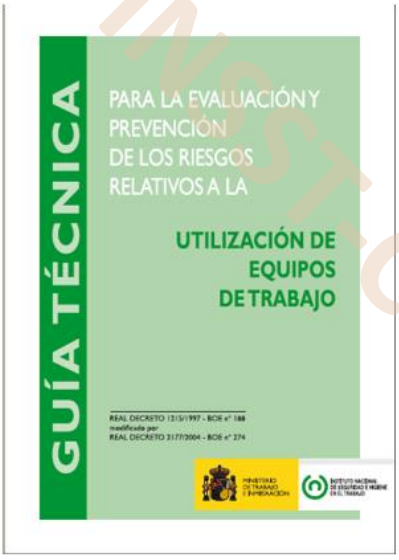
MÉTODO SIMPLIFICADO

Categoría

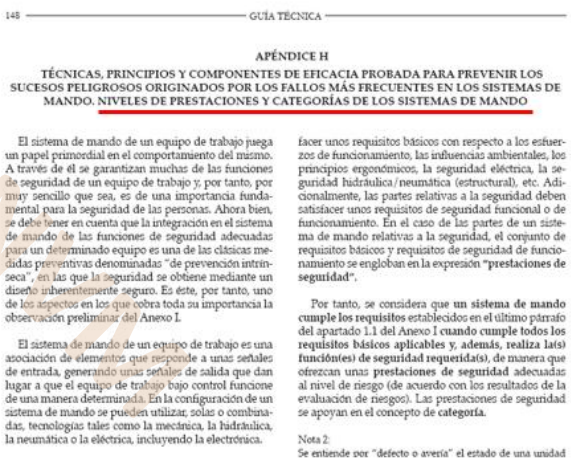
$MTTF_{dB1,C1}$	Cálculo o valoración del $MTTF_d$ para componentes individuales
$MTTF_{d,C1}$	Método simplificado para estimar el $MTTF_d$ para cada canal
$MTTF_d$	$MTTF_d$ para diferentes canales, simetrización
$DC_{B1,C2}$	Estimaciones para la cobertura del diagnóstico (DC)
DC_{avg}	Estimación de la DC media (DC_{avg})
CCF	Estimaciones para los fallos de causa común (CCF)

DIRECCIONES DE INTERÉS

http://www.insht.es/InshtWeb/Contenidos/Normativa/GuiasTecnicas/Ficheros/equipo1.pdf



Consultar Apéndice H



148 GUÍA TÉCNICA

APÉNDICE H

TÉCNICAS, PRINCIPIOS Y COMPONENTES DE EFICACIA PROBADA PARA PREVENIR LOS SUCESOS PELIGROSOS ORIGINADOS POR LOS FALLOS MÁS FRECUENTES EN LOS SISTEMAS DE MANDO. NIVELES DE PRESTACIONES Y CATEGORÍAS DE LOS SISTEMAS DE MANDO

El sistema de mando de un equipo de trabajo juega un papel primordial en el comportamiento del mismo. A través de él se garantizan muchas de las funciones de seguridad de un equipo de trabajo y, por tanto, por muy sencillo que sea, es de una importancia fundamental para la seguridad de las personas. Ahora bien, se debe tener en cuenta que la integración en el sistema de mando de las funciones de seguridad adecuadas para un determinado equipo es una de las clásicas medidas preventivas denominadas "de prevención intrínseca", en las que la seguridad se obtiene mediante un diseño inherentemente seguro. Es éste, por tanto, uno de los aspectos en los que cobra toda su importancia la observación preliminar del Anexo I.

El sistema de mando de un equipo de trabajo es una asociación de elementos que responde a unas señales de entrada, generando unas señales de salida que dan lugar a que el equipo de trabajo bajo control funcione de una manera determinada. En la configuración de un sistema de mando se pueden utilizar, solas o combinadas, tecnologías tales como la mecánica, la hidráulica, la neumática o la eléctrica, incluyendo la electrónica.

facer unos requisitos básicos con respecto a los esfuerzos de funcionamiento, las influencias ambientales, los principios ergonómicos, la seguridad eléctrica, la seguridad hidráulica/neumática (estructural), etc. Adicionalmente, las partes relativas a la seguridad deben satisfacer unos requisitos de seguridad funcional o de funcionamiento. En el caso de las partes de un sistema de mando relativas a la seguridad, el conjunto de requisitos básicos y requisitos de seguridad de funcionamiento se engloban en la expresión **"prestaciones de seguridad"**.

Por tanto, se considera que **un sistema de mando cumple los requisitos** establecidos en el último párrafo del apartado 1.1 del Anexo I **cuando cumple todos 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 (de acuerdo con los resultados de la evaluación de riesgos). Las prestaciones de seguridad se apoyan en el concepto de **categoría**.

Nota 2:
Se entiende por "defecto o avería" el estado de una unidad

DIRECCIONES DE INTERÉS

http://www.insht.es/InshtWeb/Contenidos/Documentacion/NTP/NTP/Ficheros/926a937/ntp-946%20w.pdf

INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO

NTP Notas Técnicas de Prevención 946

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

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

CENTRO NACIONAL DE VERIFICACIÓN DE MAQUINARIA

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

DIRECCIONES DE INTERÉS

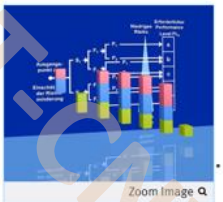
http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/sicherheit-von-maschinensteuerungen/index.jsp

News | Research | Technical information | GESTIS | Practical solutions | Testing/Certification | Publications | Events | Networks | About us

Home › Practical solutions › Practical solutions: Machine safety › Safety of machine controls to EN ISO 13849

- Elektromagnetic Fields
- Indoor workplaces
- Practical Solutions: Ergonomics
- Practical solutions: Hazardous substances
- Practical solutions: Noise
- Practical solutions: Machine safety
  - Defeating Protective Devices
  - Electro-sensitive protective equipment
  - Power drive systems with integrated safety functions
  - Logic units to ensure safety functions
  - Performance Level Calculator

Safety of machine controls to EN ISO 13849



Zoom Image

Risk graph and bar chart for determining the required and attained Performance Level
Source: IFA

On complex machines in particular, the operator's safety is dependent upon the reliability of the control system. EN ISO 13849-1 serves as a basis for evaluation of the safety of complex machine controls. For application of this standard, the IFA provides the following resources for download:

- IFA Report 2/2017e, "Functional safety of machine controls – Application of EN ISO 13849"
- IFA Report 4/2018e "Safe drive controls with frequency converters"
- Amendment of EN ISO 13849-1, A survey of the essential improvements in 2015
- The SISTEMA software assistant
- The SISTEMA Cookbooks
- A PLC disk, with which the Performance Level of control systems can be determined

IFA Reports 2/2017e and 4/2018e

Further information and downloads

- IFA Report 2/2017e and
- IFA Report 4/2018e
- Fourth edition of EN ISO 13849-1. Most important new features in 2023 at a glance (accessible)
- Software Assistent SISTEMA
- SISTEMA Cookbooks
- PLC disc

Further reading

- DGUV Test Information 06: Can PL c be achieved with a standard PLC?
- Apfeld, R.; Schaefer, M.: Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present (PDF, 285 kB, non-accessible) , 23-25 November 2010, Nuremberg - lecture
- Hauke, M.: Functional safety of