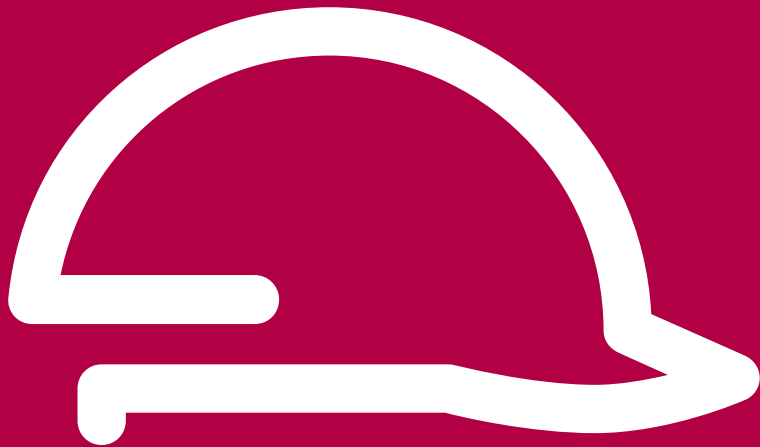


# Soluciones de seguridad Preventa

Software SISTEMA



**Conceptos y parámetros EN ISO 13849**

**Descarga e instalación del Software**

**Estructura y conceptos**

**Creación de un proyecto y carga de librerías**

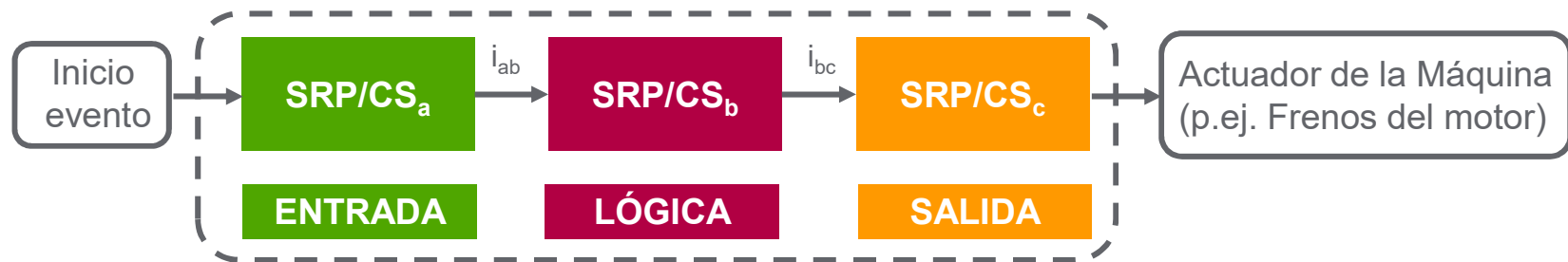
**Creación de una librería propia**

# Conceptos y parámetros EN ISO 13849-1

## 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.

Se componen de entrada, lógica y salida.



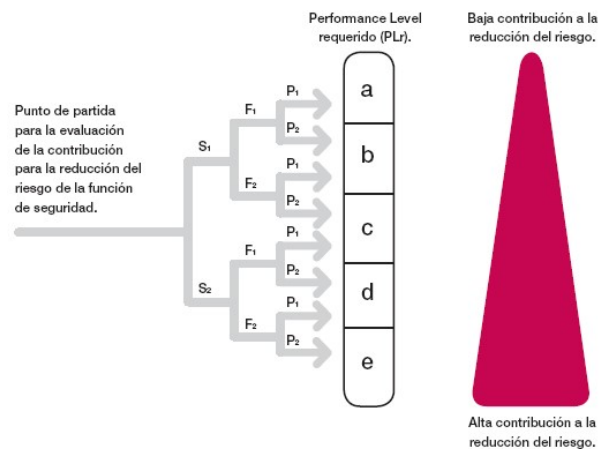
# Conceptos y parámetros EN ISO 13849

## PL (Performance Level): Performance Level):

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

## PL<sub>r</sub> (Performance Level requerido):

Nivel de prestaciones (PL) necesario con el fin de conseguir la reducción de riesgo requerida para cada función de seguridad.



**S** Gravedad de la lesión

**F** Presencia en la zona peligrosa

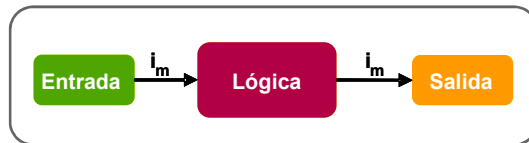
**P** Posibilidad de prevenir el accidente

# Conceptos y parámetros EN ISO 13849

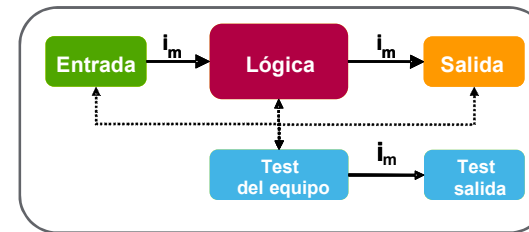
## Categoría

Clasificación de las partes de un sistema de mando relativas a la seguridad en función de su resistencia a defectos y de su comportamiento subsecuente en caso de defecto, y que se obtiene mediante la arquitectura de dichas partes, la detección de defectos y/o su fiabilidad.

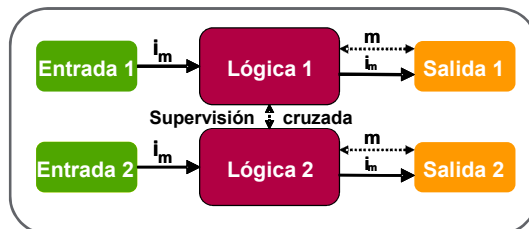
### Categoría B ó 1



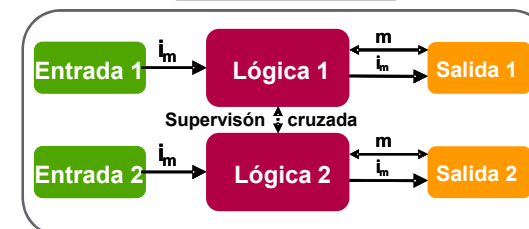
### Categoría 2



### Categoría 3



### Categoría 4



# Conceptos y parámetros EN ISO 13849

## MTTFd (Tiempo medio hasta un fallo peligroso)

Valor probable de la duración media hasta un fallo peligroso.

Valor facilitado por el fabricante del dispositivo.

Tres niveles de MTTFd se definen en esta norma para clasificar los requerimientos los “Performance Level” (PL):

Denotación del tiempo medio al fallo peligroso	Rango de MTTFd
BAJO	$3 \text{ años} \leq \text{MTTFd} < 10 \text{ años}$
MEDIO	$10 \text{ años} \leq \text{MTTFd} < 30 \text{ años}$
ALTO	$30 \text{ años} \leq \text{MTTFd} < 100 \text{ años}$

# Conceptos y parámetros EN ISO 13849

## B10<sub>d</sub>

Es el número medio de ciclos hasta que el 10% de los componentes falla de manera peligrosa.

A partir de B10<sub>d</sub> y del número medio de operaciones por año  $n_{op}$ , el MTTFd para componentes se puede calcular de la siguiente manera:

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}}$$

donde:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{ s/h}}{t_{ciclo}}$$

$h_{op}$  = es el número medio de horas de utilización por día

$d_{op}$  = es el número medio de días de utilización por año

$t_{ciclo}$  = es el tiempo medio entre el comienzo de dos ciclos sucesivos del componente en segundos por ciclo.

# Conceptos y parámetros EN ISO 13849

**PFH<sub>d</sub>**

Probabilidad media de un fallo peligroso por hora

PL	Probabilidad media de un 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, son necesarias otras medidas para obtener el PL.



# Conceptos y parámetros EN ISO 13849

## Cobertura del diagnóstico (DC)

Medida de la efectividad del diagnóstico, que se puede determinar como la relación entre la tasa de fallo de los fallos peligrosos detectados y la tasa de fallo del total de fallos peligrosos.

Valor facilitado por el fabricante del dispositivo.

El diagnóstico de cobertura se define por el ratio entre fallos peligrosos detectados y fallos peligrosos totales.

Denotación del diagnóstico de cobertura	Rango del DC
NINGUNO	$DC < 60\%$
BAJO	$60\% \leq DC < 90\%$
MEDIO	$90\% \leq DC < 99\%$
ALTO	$99\% \leq DC$

# Conceptos y parámetros EN ISO 13849

## Fallo de causa común (CCF)

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

Los fallos coincidentes en dos o más canales de un sistema de canales múltiples pueden conducir al fallo del sistema



# Conceptos y parámetros EN ISO 13849

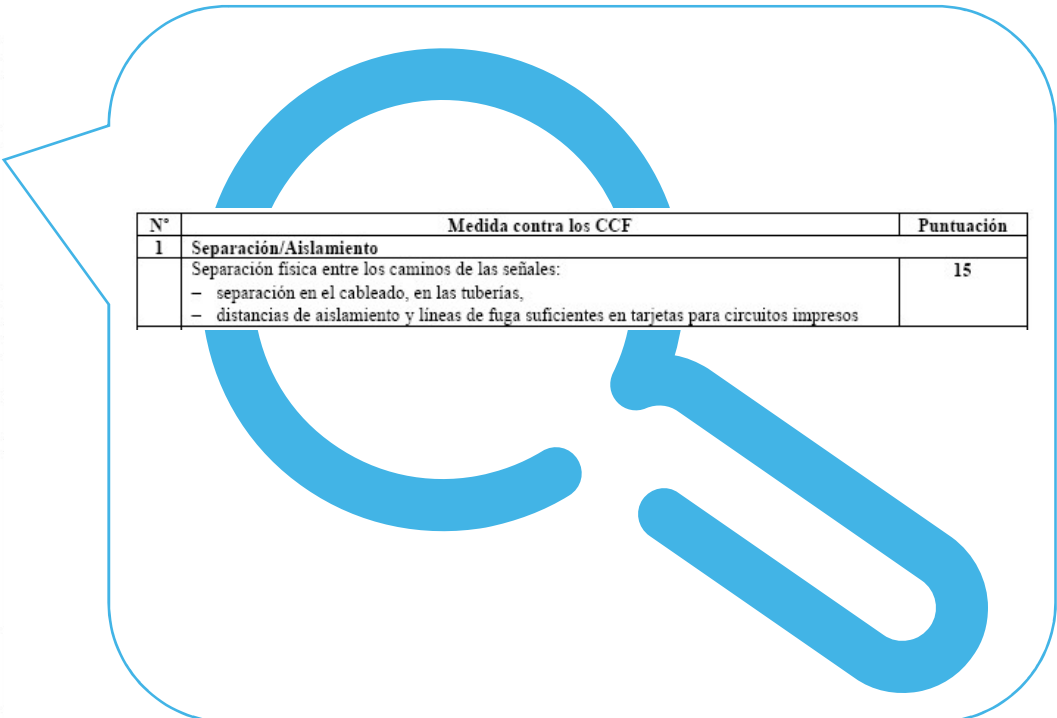
## Fallo de causa común (CCF)

Las medidas contra CCF deben ser chequeadas usando la Tabla F.1 del Anexo F de la EN ISO 13849-1. El resultado de este chequeo ha de ser mayor ó igual a 65 puntos.

Tabla F.1 – Proceso de puntuación de las medidas contra los CCF

Nº	Medida contra los CCF	Puntuación
1	<b>Separación/Aislamiento</b>	
	Separación física entre los caminos de las señales: <ul style="list-style-type: none"><li>– separación en el cableado, en las tuberías,</li><li>– distancias de aislamiento y líneas de fuga suficientes en tarjetas para circuitos impresos</li></ul>	15
2	<b>Diversidad</b>	
	Utilizar diferentes tecnologías/principios de diseño o principios físicos, por ejemplo: <ul style="list-style-type: none"><li>– primer canal electrónico programable y segundo canal cableado,</li><li>– tipo de iniciación,</li><li>– presión y temperatura</li></ul> Medida de la distancia y de la presión, por ejemplo: <ul style="list-style-type: none"><li>– digital y analógica</li></ul> Componentes de diferentes fabricantes	20
3	<b>Diseño/aplicación/experiencia</b>	
3.1	Protección contra sobretensión, sobrepresión, sobreintensidad, etc.	15
3.2	Utilización de componentes de eficacia probada	5
4	<b>Evaluación/Análisis</b>	
	¿En el diseño se tienen en cuenta los resultados de un análisis de los modos de fallo y sus efectos para evitar los fallos de causa común?	5
5	<b>Competencia/formación</b>	
	¿Han sido formados los diseñadores y el personal de mantenimiento para entender las causas y consecuencias de los fallos de causa común?	5
6	<b>Medio ambiente</b>	
6.1	Prevención de la contaminación y de las perturbaciones electromagnéticas (CEM) contra los CCF, de conformidad con las normas pertinentes	25
	Sistemas fluidicos: 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?	
	Para sistemas combinados fluidicos y eléctricos, se deberían considerar ambos aspectos	
6.2	Otras influencias	10
	¿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 (por ejemplo, tal como se especifica en las normas pertinentes)?	
	<b>Total</b>	[máx. alcanzable 100]
<b>Puntuación total</b>		<b>Medidas para evitar los CCF <sup>a</sup></b>
65 o mejor		Cumple los requisitos
Menos de 65		Proceso fallido ⇒ seleccionar medidas adicionales

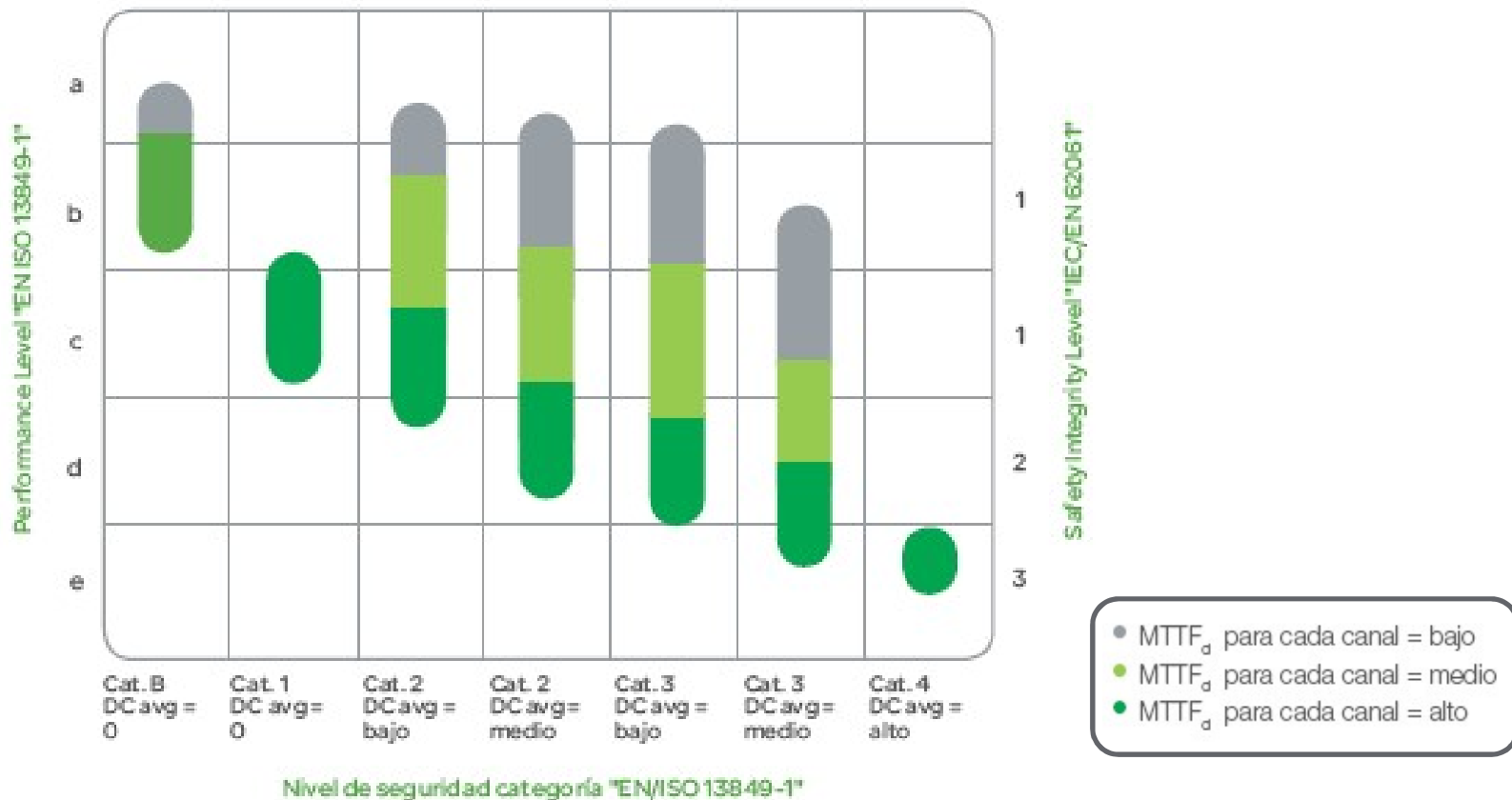
<sup>a</sup> Cuando no son pertinentes las medidas técnicas, los puntos detallados en la columna de la derecha se pueden considerar como un cálculo completo.



Nº	Medida contra los CCF	Puntuación
1	<b>Separación/Aislamiento</b>	
	Separación física entre los caminos de las señales: <ul style="list-style-type: none"><li>– separación en el cableado, en las tuberías,</li><li>– distancias de aislamiento y líneas de fuga suficientes en tarjetas para circuitos impresos</li></ul>	15

# Conceptos y parámetros EN ISO 13849

## Relación entre categoría, $MTTF_d$ , DC y PL



# Conceptos y parámetros EN ISO 13849

## Relación entre PL, PFH<sub>d</sub> y SIL

Siguiendo la tabla K.1 del Anexo K de la EN ISO13849-1, podemos obtener la Probabilidad de Fallo peligroso por Hora (PFH<sub>d</sub>) que nos puede dar el nivel de Safety Integrity Level (SIL) alcanzado:

Probabilidad media de un fallo peligroso por hora (PFH <sub>d</sub> )	Performance Level (PL)	Safety Integrity Level (PL)
$\geq 10^{-5}$ a $< 10^{-4}$	a	no SIL
$\geq 3 \times 10^{-6}$ a $< 10^{-5}$	b	1
$\geq 10^{-6}$ a $< 3 \times 10^{-6}$	c	1
$\geq 10^{-7}$ a $< 10^{-6}$	d	2
$\geq 10^{-8}$ a $< 10^{-7}$	e	3

**Conceptos y parámetros EN ISO 13849**

**Descarga e instalación del Software**

**Estructura y conceptos**

**Creación de un proyecto y carga de librerías**

**Creación de una librería propia**

# Descarga e instalación

<http://www.schneiderelectric.es/sites/spain/es/solutions/oem/seguridad-maquinas/machine-safety.page>



Se encuentra aquí: Inicio > Soluciones > Maquinaria > Soluciones generales de control de maquinaria > Seguridad de máquina

## Seguridad en máquinas

### Seguridad en máquinas

- Manual de seguridad en máquinas
- Seleccione la solución más adecuada a su función de seguridad
- Evalúe la seguridad de su maquinaria
- Oferta de productos de seguridad de Preventa



Nuevas máquinas: la Directiva de Maquinas

Saber más

Le ayudamos a alcanzar de una forma sencilla el nivel de seguridad requerido según normativa en su máquina

Saber más

No espere más para implementar de una forma sencilla las nuevas normas funcionales, nosotros le guiamos en cada paso del proceso

Manual de seguridad en máquinas



Consulte el Manual de seguridad en máquinas



Seleccione la solución más adecuada a su función de seguridad

9 Soluciones para funciones de seguridad de Schneider Electric, aprobadas por el TÜV para alcanzar el nivel de seguridad requerido



Evalúe la seguridad de su maquinaria

Una herramienta de software que le asistirá en la sencilla aplicación del estándar de control EN ISO 13849-1 (Acceso web IFA - inglés)

La importancia de la seguridad en el ciclo de vida de una máquina.

Saber más

Implementación del concepto "Seguridad funcional"

### Información adicional

Solicite información sobre productos y servicios



Contacte con su centro de atención al cliente ahora

### Descargas clave

- La guía esencial: Guía de elección soluciones de seguridad preventiva (castellano)
- Manual de seguridad en máquinas - descúbrelo
- Funciones certificadas de seguridad Preventa (castellano PDF 0.5 Mb)
- Biblioteca para el software Sistema de soluciones Preventa de Schneider Electric (Inglés - SLB 0.5 Mb)
- Descarga de la herramienta SISTEMA (acceso web IFA - inglés)



Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

## SISTEMA

Safety Integrity Software Tool for the Evaluation of Machine Applications

Version: 1.1.2

Standard: ISO 13849-1:2006, ISO 13849-2:2003

<http://www.dguv.de/webcode.jsp?q=d34183>

### Software SISTEMA



Download Version: 1.1.5

Version history

SISTEMA Cookbooks

Example circuits with corresponding SISTEMA project files (zip file)

Collection of SISTEMA libraries

All versions

### File Download

Do you want to open this file?



Name: se-preventa-en-2010\_01\SLB  
Type: SISTEMA - Library files, 1,57 MB  
From: www.schneider-electric.com

Open

Save

Cancel

☒ Always ask before opening this type of file



While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

Descarga de la librería SE

Link a la web de la BGIA

**Conceptos y parámetros EN ISO 13849**

**Descarga e instalación del Software**

**Estructura y conceptos**

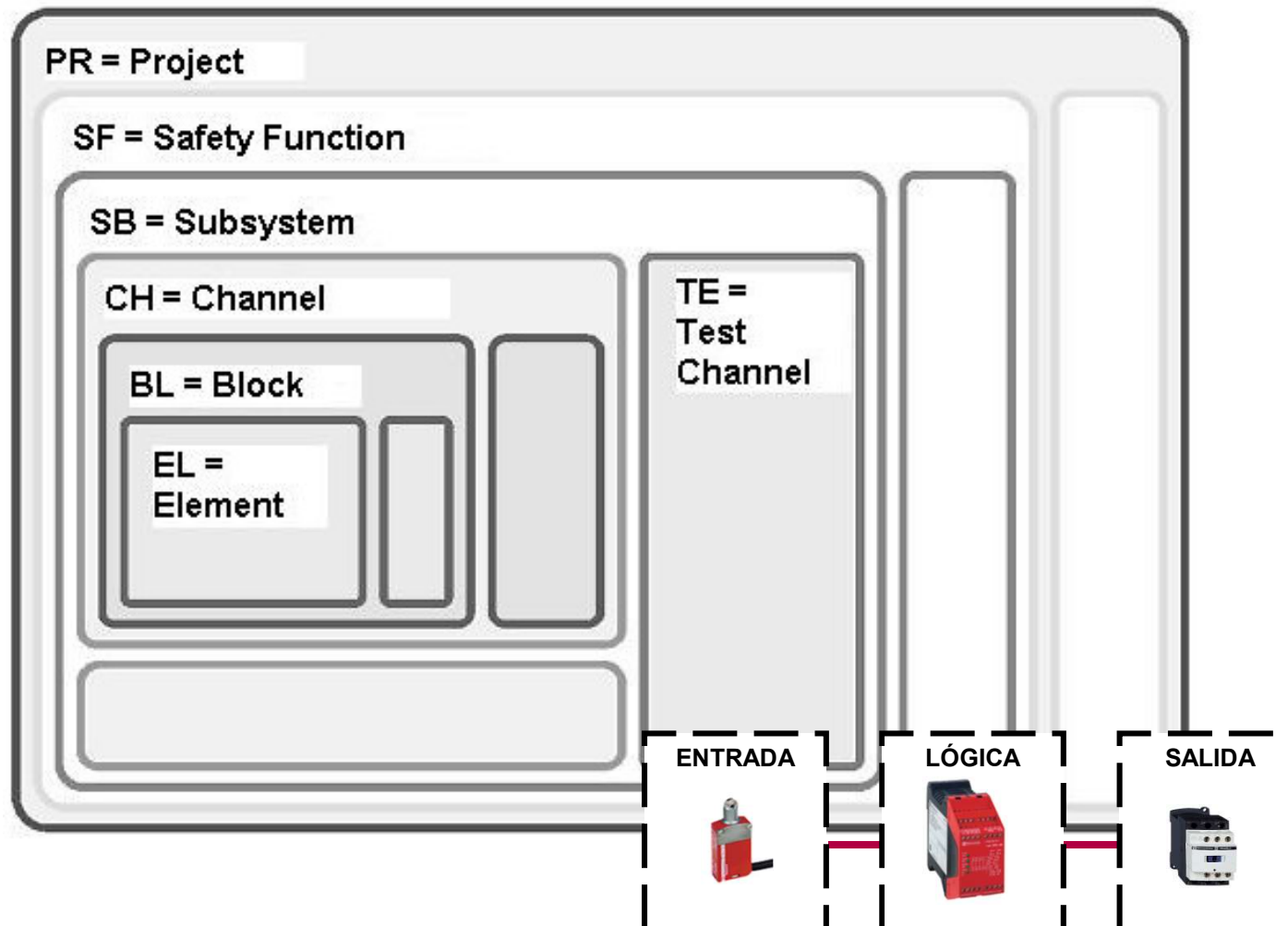
**Creación de un proyecto y carga de librerías**

**Creación de una librería propia**



# Estructura y conceptos

## Capas en que se compone el Software



# Estructura y conceptos

## Niveles de jerarquía en Sistema

**PR Project:** Sumario de funciones de seguridad, por ejemplo una máquina ó una parte de ésta.

**Ejemplo:** Área de trabajo de una prensa.



**SF Safety Function:** Respuesta segura a una situación peligrosa (lo que se define como SRP/CS).

**Ejemplo:** Parada segura cuando una puerta de seguridad se abre.



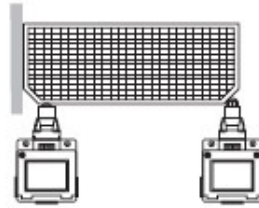
# Estructura y conceptos

## Niveles de jerarquía en Sistema

**SB Subsystem:** Puede ser de dos tipos:

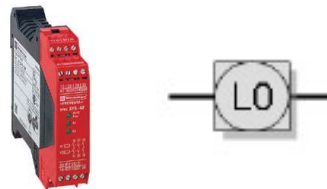
a) Grupo de bloques dentro de una estructura rígida (categoría)

**Ejemplo:** Finales de carrera en modo combinado



b) Componente de seguridad con la declaración por parte del fabricante del PL, PFH<sub>d</sub>, y categoría (sistema encapsulado)

**Ejemplo:** Módulo de seguridad XPSAF

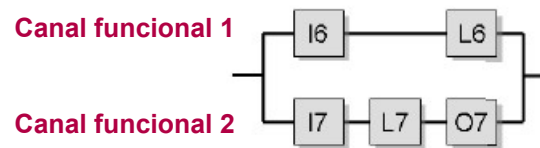


# Estructura y conceptos

## Niveles de jerarquía en Sistema

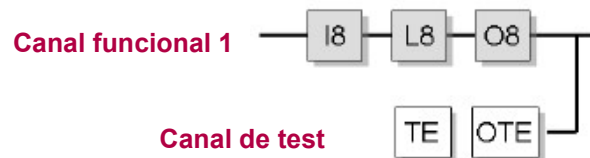
**CH Channel:** Conexión de bloques en serie; Sistema crea uno ó dos canales funcionales, dependiendo de la categoría seleccionada.

**Ejemplo:**



**Test channel:** Conexión de bloques en serie para la función de test; Sistema únicamente crea un canal de test para categoría 2.

**Ejemplo:**

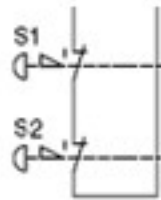


# Estructura y conceptos

## Niveles de jerarquía en Sistema

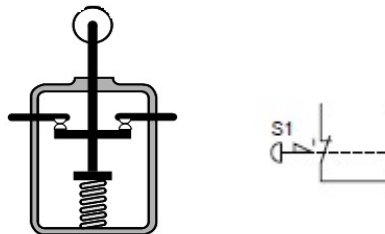
**BL Block:** Componente en la función ó en el canal de test.

**Ejemplo:** Dos contactos de dos setas puestas en serie



**EL Element:** Un bloque contiene uno ó más elementos. El valor  $B_{10d}$  puede ser únicamente introducido por elementos.

**Ejemplo:** Contactos de contactores, interruptores de posición... todo componente con el valor  $B_{10d}$  proporcionado por el fabricante.



**Conceptos y parámetros EN ISO 13849**

**Descarga e instalación del Software**

**Estructura y conceptos**

**Creación de un proyecto y carga de librerías**

**Creación de una librería propia**

# Creación de un nuevo proyecto

The screenshot shows the 'Project' dialog box in SIMATIC Manager. The 'Project name' field is highlighted with a red callout bubble. The 'Project file name' field is empty. The 'Last change' field shows '14/06/2010'. The 'Checksum' field shows 'dbccf110fa8b33b929b6447b0cf8c1f0'. The 'Author' field shows 'SESA28875'. The 'Dangerous point/machine' field is empty. The 'Home folder for standards' field shows '..\Standards'. The 'Home folder for documents' field shows '..\Documents'. The 'Documentation' field is empty. The 'Document' field is empty. The 'Open' button is visible at the bottom right.

Crear un nuevo proyecto

Nombre del proyecto

Project

Documentation Safety functions

There are warnings with yellow status listed for this project (or it's subordinate basic elements). Please consider these hints.

Project name: Formación Schneider Electric

Project file name:

Last change: 14/06/2010

Checksum: dbccf110fa8b33b929b6447b0cf8c1f0

Author: SESA28875

Dangerous point/machine:

Home folder for standards: ..\Standards

Home folder for documents: ..\Documents

Documentation:

Document:

Open

# Creación de una función de seguridad

**Crear una función de seguridad nueva SF**

**Descripción de la función**

Name	Type	PLr	PL
<unknown safety function>		d	e

**Vigilancia de puerta**

PLr	PL	PFH [1/h]
d	e	0

**Name of safety function:** Vigilancia de puerta

**Type of safety function:** Safety-related stop function initiated by safeguard

**Triggering event:** Obertura de la puerta

**Reaction:** Parada del movimiento peligroso

**Safe state:** Movimiento peligroso parado

**Documentation:**

**Document:**

Open



# Performance Level requerido (PLr)

El Performance Level requerido (PLr) debe ser especificado para cada función de seguridad. El Performance Level (PL) alcanzado por el sistema de control debe ser validado mediante una verificación para ver si es mayor ó igual que el PLr.

The screenshot displays the 'Safety function' configuration interface. On the left, a project tree shows 'PR Formación Schneider Electric' and 'SF Vigilancia de puerta'. The main area is titled 'Safety function' and includes tabs for 'Documentation', 'PLr', 'PL', and 'Subsystems'. The 'PLr' tab is active, showing a risk graph and three selection criteria: 'Severity of injury (S)', 'Frequency and/or exposure times to hazard (F)', and 'Possibility of avoiding hazard or limiting harm (P)'. The risk graph shows a path from S2 to F2 to P1, highlighted in red. The selection criteria are as follows:

- Severity of injury (S)**
  - ☐ S1 Slight (normally reversible injury)
  - ☒ S2 Serious (normally irreversible injury or death)
- Frequency and/or exposure times to hazard (F)**
  - ☐ F1 Seldom to less often and/or exposure time is short
  - ☒ F2 Frequent to continuous and/or exposure time is long
- Possibility of avoiding hazard or limiting harm (P)**
  - ☒ P1 Possible under specific conditions
  - ☐ P2 Scarcely possible

Below the risk graph, a table shows the required (PLr) and achieved (PL) performance levels for the 'Vigilancia de puerta' function:

PLr	PL
d	e
PFH [1/h]	0

# Añadir un subsistema a partir de la Librería

**Hacer Click en el botón derecho**

**Cargar y Cerrar**

**Libraries**

- Schneider Electric PREVENTA...
- SISTEMA default library

**SB Subsystems**

- ASISSLC
- ASISLLS
- ASISE
- ASISLE
- Emergency Stop, 2 contacts
- Coded Magnetic Switch XCSDMC/P/R, several sensors in series at a monitoring device.
- Coded Magnetic Switch XCSDMC/P/R, single sensor at a monitoring device.
- Coded Magnetic System XCSDM3
- Coded Magnetic System XCSDM4

**Set Changes**

**Load Selection**

**Load & Close**

**Close**

**Coded Magnetic Switch XCSDMC/P/R, single sensor at a monitoring device.**

PL	e
PFH [1/h]	2,47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

**Projects**

- Formación Schneider Electric
- Vigilancia de puerta
- Coded Magnetic Switch XCSDMC/P/R
- Channel 1
- Reed contact
- Reed Contact
- Channel 2
- Reed contact
- Reed Contact

# Performance Level del subsistema

El Performance Level (PL) del subsistema puede ser determinado de acuerdo a su uso (arquitectura, datos de fiabilidad y número de operaciones por año).

También es posible introducir directamente los valores PL y PFHd cuando éstos son valores conocidos por el fabricante

**Subsystem** IFA

Documentation | **PL** | Category | MTTFd | DCavg | CCF | Blocks

☐ Enter PL/PFH directly (manufacturer ensures compliance with the requirements of the Category)

☒ Determine PL/PFH from Category, MTTFd and DCavg

Performance Level (PL):

PFH [1/h]:

# Categoría del subsistema

**Subsystem** IFA

Documentation | PL | **Category** | MTTFd | DCavg | CCF | Blocks

Category of subsystem:

Category	Requirements	When a single fault occurs	Mainly characterized by structure
4	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that 1. a single fault in any of these parts does not lead to a loss of the safety function, and 2. the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure
3	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that 1. a single fault in any of these parts does not lead to a loss of the safety function, and 2. whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure

Click & mover

Requirements for the category:

- ☒ Basic safety principles are being used.
- ☒ Well-tried safety principles are being used.
- ☒ A single fault tolerance is given.
- ☒ MTTFd is Low or Medium or High.
- ☒ DCavg is Low or Medium.
- ☒ The achieved score of the CCF-rating is at least 65.

Seleccionar la arquitectura del subsistema

# MTTFd del subsistema

El valor para el tiempo medio al fallo peligroso (MTTFd) puede ser calculado a partir de los datos de fiabilidad de los elementos del subsistema.

The screenshot shows the 'Subsystem' configuration window in the SISTEMA IFA software. The 'MTTFd' tab is selected. There are two radio buttons: 'Determine MTTFd value from blocks' (selected) and 'Enter MTTFd value directly'. Below the radio buttons, there are input fields for 'MTTFd (after symmetrization):' with the value '100' and 'a', and 'MTTFd level:' with the value 'High'. There is also a section for 'Mission time' with input fields for 'Mission time:' (value '20') and 'Shortest mission time:' (value '20'), both followed by 'a'. A note at the bottom states: 'SISTEMA always assumes 20 years for the purpose of calculation.'

También es posible introducir directamente el valor del MTTFd cuando éste es conocido por el fabricante

El Mission time para los elementos del subsistema se asume que es de 20 años por SISTEMA, pero este valor puede ser modificado por el usuario

# MTTFd cálculo de los elementos

Desde Subsistema, a nivel de elemento, podemos acceder al cálculo del número de operaciones

The screenshot shows the SISMA software interface. At the top, there are two tabs: 'Subsystem' and 'Block'. The 'Subsystem' tab is active, showing a list of elements under 'Channel 1'. A red arrow points from the 'Reed contact' element in the 'Subsystem' tab to the 'Block' tab. The 'Block' tab is active, showing a list of elements under 'MTTFd'. A red arrow points from the 'Reed contact' element in the 'Block' tab to the 'Element' tab. The 'Element' tab is active, showing the 'MTTFd' calculation screen. A red arrow points from the 'Calculate nop' button to a red callout box that says 'Click'. The 'Calculate nop' button is located next to the 'nop' input field, which contains the value '211200 Cycles/a'. The 'Calculate nop' button is also labeled 'Click' in a red callout box. Below the 'Calculate nop' button, there is a 'Mission time' section with a formula for calculating the number of operations ( $n_{op}$ ). The formula is 
$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}}$$
 The inputs for the formula are: 

- $d_{op}$ : 220 Days
- $h_{op}$ : 16 Hours
- $t_{cycle}$ : 60 Seconds

 The 'Mission time' section also includes a 'Cancel' button and an 'Ok' button. A red callout box points to the 'Mission time' section with the text: 'Introducir los valores para calcular el número de operaciones (nop)'. The 'Element' tab also shows the 'MTTFd' value of 2367,42 a and the 'MTTFd level' set to 'High'. The 'Block' tab shows the 'Name' of the element as 'Reed Contact' and the 'EL' status as 'Green'.

Click

Introducir los valores para calcular el número de operaciones (nop)



# DC del subsistema

La Cobertura del Diagnóstico (DC) puede ser introducida manualmente de acuerdo a las características de los componentes

**Subsystem** IFA

Documentation | PL | Category | MTTFd | **DCavg** | CCF | Blocks

☐ Determine DCavg value from blocks  
☒ Enter DCavg value directly

Diagnostic coverage (DCavg): 99 % DCavg level: High

Documentation/reasoning: The coded magnetic switch is used with a monitoring device; no sensors are connected in series in order to detect each first fault. DC=99%

Para un subsistema constituido por un módulo de seguridad con diagnóstico de los dos canales redundantes, puede alcanzarse un valor del 99%

# CCF del subsistema

Los fallos de causa común (CCF) son evaluados según la concepción del componente

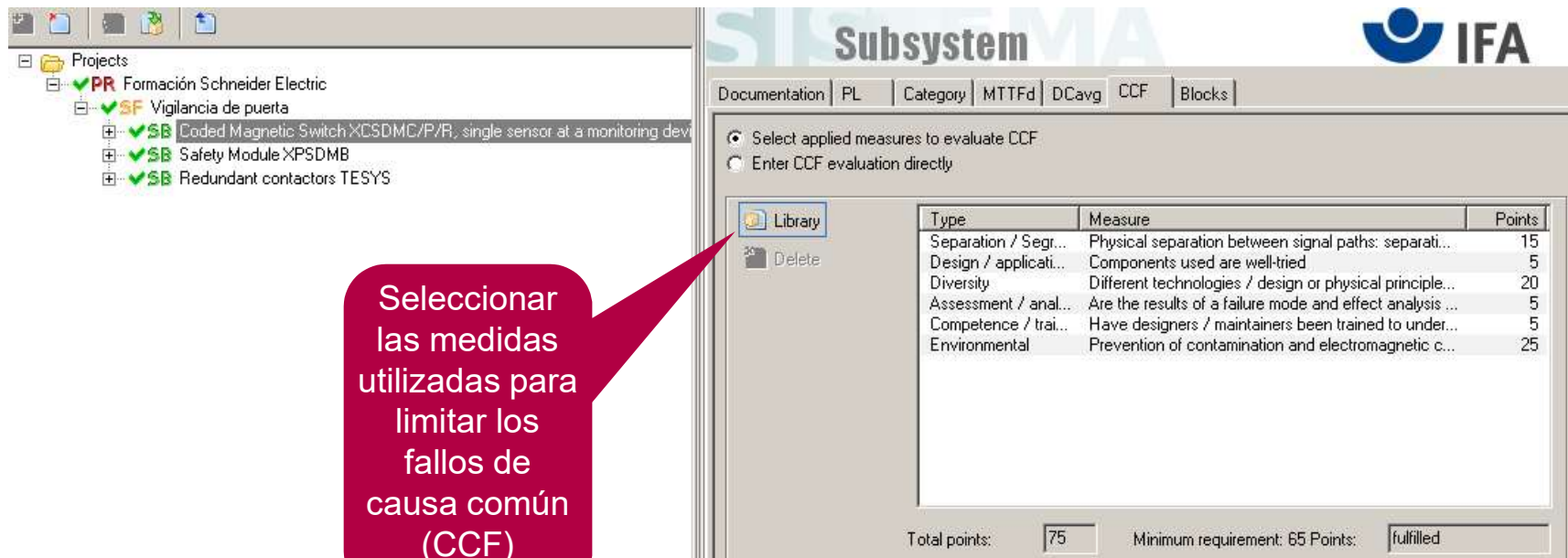


**Subsystem** IFA

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☐ Select applied measures to evaluate CCF  
☒ Enter CCF evaluation directly

Total points:  Minimum requirement: 65 Points:



**Subsystem** IFA

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☒ Select applied measures to evaluate CCF  
☐ Enter CCF evaluation directly

**Library**

Type	Measure	Points
Separation / Segr...	Physical separation between signal paths: separati...	15
Design / applicati...	Components used are well-tried	5
Diversity	Different technologies / design or physical principle...	20
Assessment / anal...	Are the results of a failure mode and effect analysis ...	5
Competence / trai...	Have designers / maintainers been trained to under...	5
Environmental	Prevention of contamination and electromagnetic c...	25

Total points:  Minimum requirement: 65 Points:

**Projects**

- PR Formación Schneider Electric
  - SF Vigilancia de puerta
    - SB Coded Magnetic Switch XCSDMC/P/R, single sensor at a monitoring dev...
    - SB Safety Module XPSDMB
    - SB Redundant contactors TESYS

Seleccionar las medidas utilizadas para limitar los fallos de causa común (CCF)



# Evaluación del Performance Level del subsistema

El resultado del cálculo de la función de seguridad se muestra automáticamente por el resultado del Performance Level (PL) y el valor de la Probabilidad de Fallo Peligroso por hora (PFHd) a partir de la combinación de subsistemas

The screenshot displays the IFA Subsystem software interface. On the left, a project tree shows the hierarchy: 'Formación Schneider Electric' > 'Vigilancia de puerta' > 'Coded Magnetic Switch XCSDMC/P/R, single sensor at a monitoring device' > 'Channel 1' and 'Channel 2'. The main window shows the 'Vigilancia de puerta' function details. A table lists the following data:

Parameter	Value
PLr	d
PL	e
PFH [1/h]	2,47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

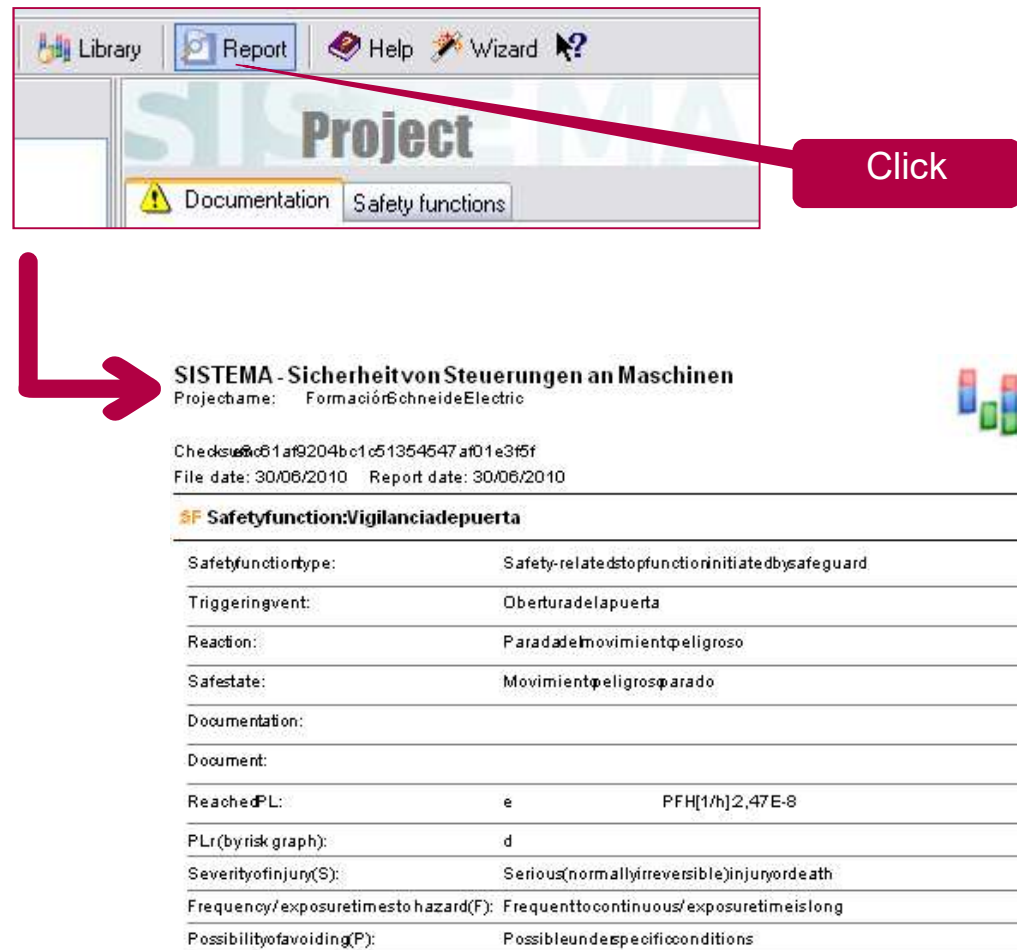
On the right, the 'Documentation' tab is active, showing the 'Enter CCF evaluation directly' option selected. The 'Total points' field is set to 65, and the 'Minimum requirement: 65 Points' field is marked as 'fulfilled'.

Three red callout boxes provide additional context:

- PL requerido para la función de seguridad** (Required PL for the safety function) points to the 'PLr' value 'd'.
- PL alcanzado por la función de seguridad** (Achieved PL for the safety function) points to the 'PL' value 'e'.
- Probabilidad de Fallo Peligroso por hora (PFHd) para la función de seguridad** (Dangerous Failure Rate per hour (PFHd) for the safety function) points to the 'PFH [1/h]' value '2,47E-8'.

# Impresión del informe de Seguridad

Este informe debe incluirse en el expediente técnico de la máquina (anexo VII de la Directiva de Máquinas)



The screenshot shows the SIMATIC Manager software interface. The 'Report' menu is highlighted, and a red arrow points to it with the text 'Click'. Below the interface, a red arrow points to the generated report. The report is titled 'SISTEMA - Sicherheit von Steuerungen an Maschinen' and includes the following information:

Projectname: FormaciónSchneiderElectric

Checksum: 61af9204bc1c51354647af01e3f5f

File date: 30/06/2010 Report date: 30/06/2010

**SF Safetyfunction:Vigilanciadepuerta**

Safetyfunctiontype:	Safety-relatedstopfunctioninitiatedbysafeguard
Triggeringevent:	Oberturadelapuerta
Reaction:	Paradadelmovimientopeligroso
Safestate:	Movimientopeligrosoparado
Documentation:	
Document:	
ReachedPL:	e PFH[1/h]2,47E-8
PLr(byrisk graph):	d
Severityofinjury(S):	Serious(normallyirreversible)injuryordeath
Frequency/exposuretime to hazard(F):	Frequenttocontinuous/exposuretimeislong
Possibilityofavoiding(P):	Possibleundespecificconditions

**Conceptos y parámetros EN ISO 13849**

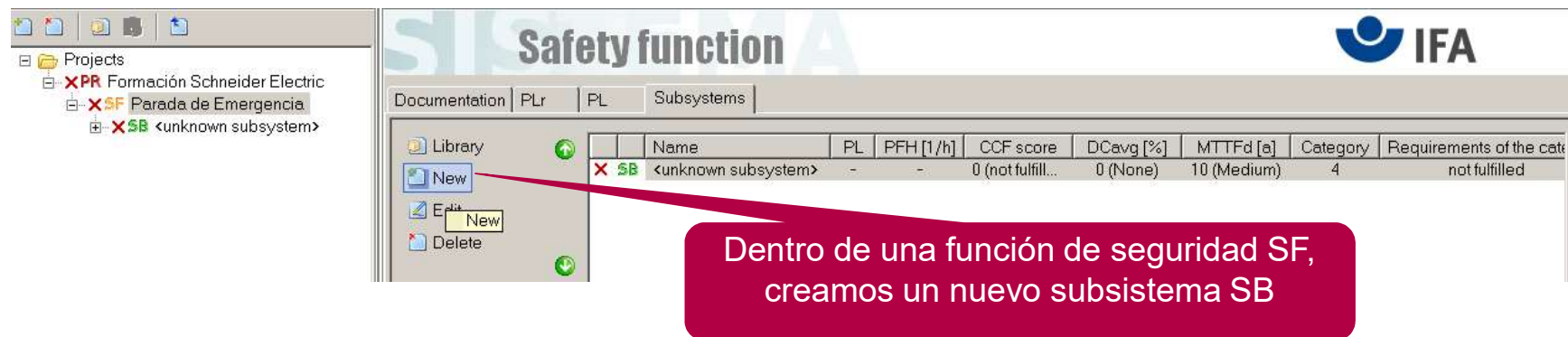
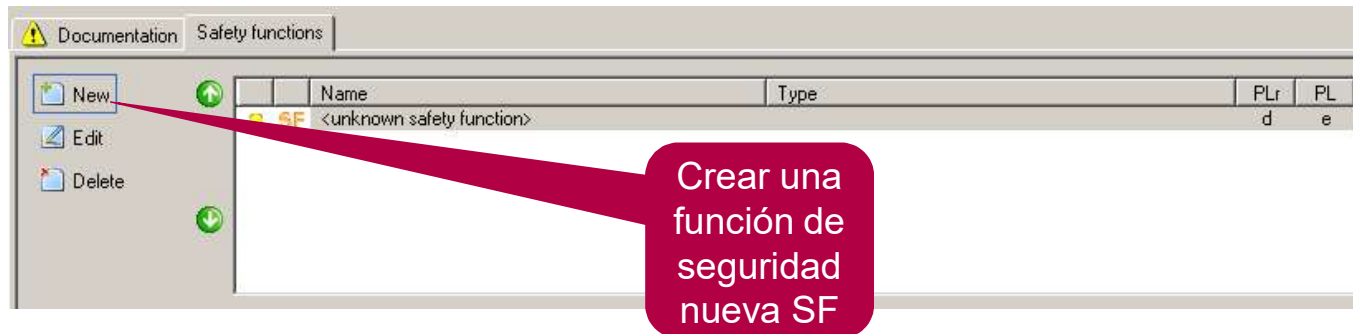
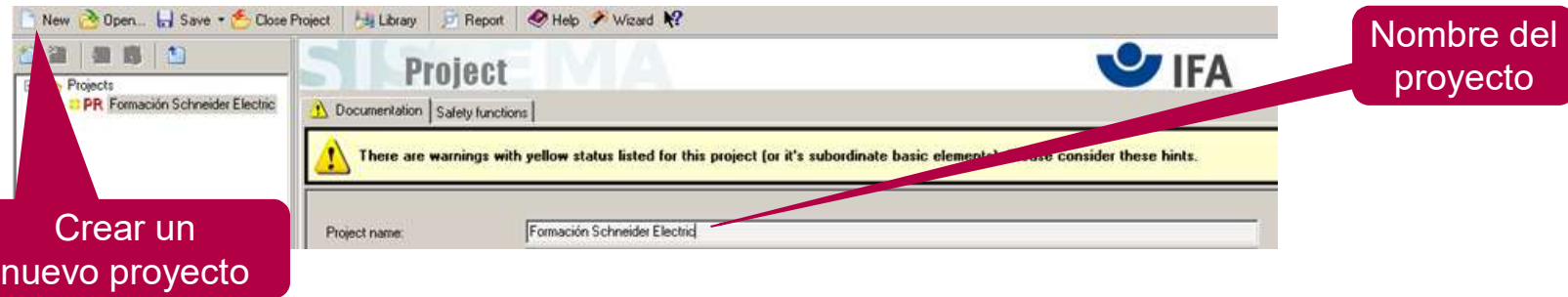
**Descarga e instalación del Software**

**Estructura y conceptos**

**Creación de un proyecto y carga de librerías**

**Creación de una librería propia**

# Creación de un subsistema propio



# Creación de un subsistema propio

The screenshot shows the 'Subsystem' configuration window. On the left, a project tree lists 'PR Formación Schneider Electric', 'SF Parada de Emergencia', and 'SB SETA DE EMERGENCIA'. The main window has tabs for 'Documentation', 'PL', 'Category', 'MTTFd', 'DCavg', 'CCF', and 'Blocks'. The 'Name of Subsystem' field is filled with 'SETA DE EMERGENCIA'.

Asignamos nombre del subsistema

This screenshot shows the 'PL' tab of the 'Subsystem' configuration. Two radio buttons are present: 'Enter PL/PFH directly (manufacturer ensures compliance with the requirements of the Category)' (selected) and 'Determine PL/PFH from Category, MTTFd and DCavg'. Below, the 'Performance Level (PL)' dropdown is set to 'a', and the 'PFH [1/h]' field contains '3,16E-5'. A 'Fault exclusion' checkbox is also visible.

Si el PL del subsistema es conocido ó su PFH, podemos introducirlo directamente

This screenshot shows the 'PL' tab with the 'Performance Level (PL)' dropdown set to 'e' and the 'PFH [1/h]' field set to '0'. The 'Fault exclusion' checkbox is checked.

Si la función se presuponen que realmente nunca se va a utilizar (por caso una seta de emergencia en una zona en la que el peligro es inexistente y el acceso a la misma no es posible) podemos forzar la opción Fault exclusion PFH =0

# Creación de un subsistema propio

The screenshot shows the 'Subsystem' configuration window in the Schneider Electric software. The 'Documentation' tab is active, and the 'Category' sub-tab is selected. The 'Performance Level (PL)' and 'PFH [1/h]' fields are empty. The 'Determine PL/PFH from Category, MTTFd and DCavg' radio button is selected. The 'Category of subsystem' table is displayed, showing a category with a description, a safety function description, and a structure diagram. Below the table, the 'Requirements for the category' section is visible, with several checkboxes selected, indicating that the subsystem meets the requirements for the category.

**Subsystem**

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☐ Enter PL/PFH directly (manufacturer ensures compliance with the requirements of the Category)  
☒ Determine PL/PFH from Category, MTTFd and DCavg

Performance Level (PL):  PFH [1/h]:

**Subsystem** IFA

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

Category of subsystem

<b>4</b> Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that 1. a single fault in any of these parts does not lead to a loss of the safety function, and 2. the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	
--	---	-----------------------------------	--

Requirements for the category

- ☐ Basic safety principles are being used.
- ☐ Well-tried safety principles are being used.
- ☐ A single fault tolerance is given.
- ☐ Accumulation of faults does not lead to a loss
- ☐ MTTFd is High.
- ☐ DCavg is High.
- ☐ The achieved score of the CCF-rating is at least 65.

Requirements for the category

- ☒ Basic safety principles are being used.
- ☒ Well-tried safety principles are being used.
- ☒ A single fault tolerance is given.
- ☒ Accumulation of faults does not lead to a loss of the safety function.
- ☐ MTTFd is High.
- ☐ DCavg is High.
- ☐ The achieved score of the CCF-rating is at least 65.

Si no es conocido el PL ni el PFH, lo calcularemos a partir de los siguientes parámetros

Indicamos la categoría en que estará estructurado el subsistema

Se marcan los requerimientos necesarios para la categoría que se cumplen

# Creación de un subsistema propio

**Subsystem**

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☐ Determine MTTFd value from blocks  
☒ Enter MTTFd value directly

MTTFd:  a MTTFd level:

☐ Fault exclusion

Mission time

Mission time:  a Shortest mission time:  a

SISTEMA always assumes 20 years for the purpose of calculation.

Si el  $MTTF_d$  del subsistema es conocido, podemos introducirlo directamente

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☒ Determine MTTFd value from blocks  
☐ Enter MTTFd value directly

MTTFd (after symmetrization):  a MTTFd level:

Mission time

Mission time:  a Shortest mission time:  a

SISTEMA always assumes 20 years for the purpose of calculation.

Si no se conocido se calculará a partir de los bloques



# Creación de un subsistema propio

The screenshot shows the 'Subsystem' configuration window. The 'DCavg' tab is active. Two radio buttons are present: 'Determine DCavg value from blocks' (unselected) and 'Enter DCavg value directly' (selected). Below the radio buttons, there is a text input field for 'Diagnostic coverage (DCavg):' containing the value '0', followed by a '%' symbol. To the right, there is a 'DCavg level:' label and a dropdown menu currently set to 'None'. A 'Documentation/reasoning' text area is visible at the bottom left.

Si el  $DC_{avgd}$  del subsistema es conocido, podemos introducirlo directamente

This screenshot shows the same 'Subsystem' configuration window, but with the 'Determine DCavg value from blocks' radio button selected. The 'Enter DCavg value directly' option is now unselected. The 'Diagnostic coverage (DCavg):' field still shows '0' and the 'DCavg level:' dropdown remains at 'None'.

Si no se conocido se calculará a partir de los bloques



# Creación de un subsistema propio

**Subsystem**

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☐ Select applied measures to evaluate CCF  
☒ Enter CCF evaluation directly

Total points:  Minimum requirement: 65 Points:

Si el valor del test para CCF es conocido, podemos introducirlo directamente

Documentation | PL | Category | MTTFd | DCavg | CCF | Blocks

☒ Select applied measures to evaluate CCF  
☐ Enter CCF evaluation directly

Library Delete

**Library of CCF Measures**

Library: SISTEMA default library

No.	Measure against CCF
1	Physical separation between signal paths: separation in wiring / piping, sufficient clearances and creep age distances on printed-circuit boards.
2	Different technologies / design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature. Measuring of distance and pressure, digital and analog. Components of different manufacturers
3.1	Protection against over-voltage, over-pressure, over-current, etc.
3.2	Components used are well-tried
4	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.
5	Have designers / maintainers been trained to understand the causes and consequences of common cause failures?
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against in accordance with appropriate standards. Fluidic systems: filtration of the

Total points:  Minimum requirement: 65 Points:

Si no es conocido, podemos calcularlo.  
Hacemos click en library y vamos seleccionando los puntos

Type	Measure	Points
Separation / Segregation	Physical separation between signal paths: separation in wiring / piping, suffi...	15
Diversity	Different technologies / design or physical principles are used, for example...	20
Design / application / experi...	Protection against over-voltage, over-pressure, over-current, etc.	15
Design / application / experi...	Components used are well-tried	5
Competence / training	Have designers / maintainers been trained to understand the causes and c...	5
Environmental	Prevention of contamination and electromagnetic compatibility (EMC) again...	25

Total points:  Minimum requirement: 65 Points:

# Creación de un subsistema propio

The screenshot shows the IFA Subsystem software interface. At the top, there is a header with the 'Subsystem' title and the IFA logo. Below the header is a navigation bar with tabs: Documentation, PL, Category, MTTFd, DCavg, CCF, and Blocks. The 'Blocks' tab is selected, and a red arrow points to it from a callout box.

The interface is divided into three main sections, each representing a channel:

- Channel 1:** Contains a 'Library' section with 'New', 'Edit', and 'Delete' buttons. To the right is a table with columns 'Name', 'DC [%]', and 'MTTFd [a]'. The table contains one row: 'BL <unknown block>' with '0 (None)' for DC and '10 (Medium)' for MTTFd.
- Channel 2:** Similar to Channel 1, with a 'Library' section and a table containing one row: 'BL <unknown block>' with '0 (None)' for DC and '10 (Medium)' for MTTFd.
- Test channel:** Similar to the other channels, but the table contains one row: 'BL <unknown block>' with 'not relevant' for both DC and MTTFd.

A red callout box with white text points to the 'Blocks' tab, stating: 'En la pestaña de Blocks podemos acceder a los canales creados y a los bloques que los compondrán'.

# Creación de un subsistema propio

**Block**

Documentation | **MTTFd** | DC | Elements

Name of block: Bloque seta de emergencia

Documentation:

Entramos en el bloque del canal 1 de la seta

**Block**

Documentation | **MTTFd** | DC | Elements

☐ Determine MTTFd value from elements

☒ Enter MTTFd value directly

MTTFd: 10 a MTTFd level: Medium

Rate of dangerous failure: 11415.52 FIT ☒ Fault exclusion

Donde podemos asignarle un valor  $MTTF_d$  directamente ó determinarlo a partir de los elementos

# Creación de un subsistema propio

**Block**

Documentation | MTTFd | DC | Elements

☒ Determine DC value from elements  
☐ Enter DC value directly  
☐ Select applied measures to evaluate DC

Diagnostic coverage (DC):  % DC level:

Para calcular el  $DC_{avg}$  puedo introducirlo directamente, calcularlo a partir de los elementos ó seleccionarlo según las medidas de evaluación

☐ Determine DC value from elements  
☐ Enter DC value directly  
☒ Select applied measures to evaluate DC

Type of measure:

Description of measure:

Library: SISTEMA default library

Description	DC	dependant on
Cyclic test stimulus by dynamic change of the input signals	90	-
Plausibility check, e.g. use of normally open and normally closed mechanical linked contacts	99	-
Cross monitoring of inputs without dynamic test	0 - 99	depending on how often a signal change is by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90	-
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99	-
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 - 99	depending on the application
Direct monitoring (e.g. electrical position	99	-

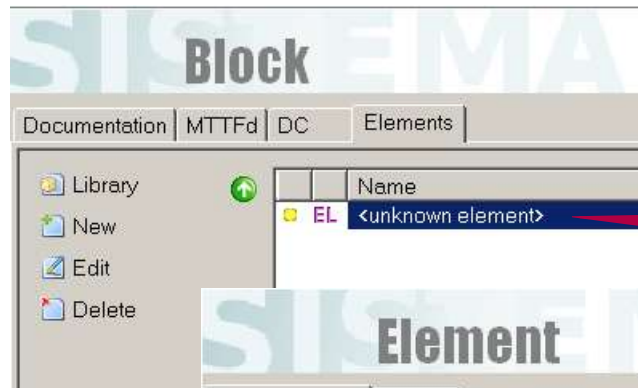
DC range: from  % to  %

Diagnostic coverage (DC):  %

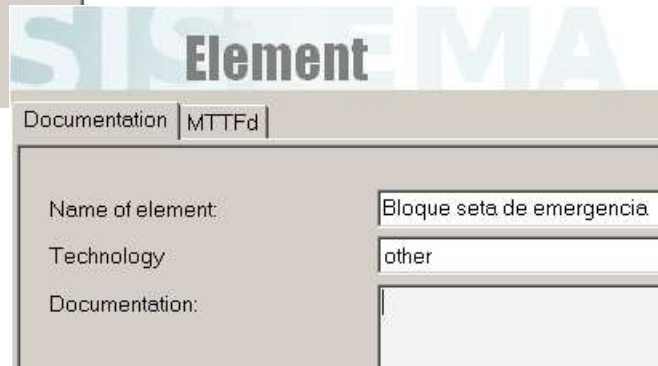
This measure alone is not sufficient for the required performance levels:

☐ a  
☐ b  
☐ c  
☐ d  
☐ e

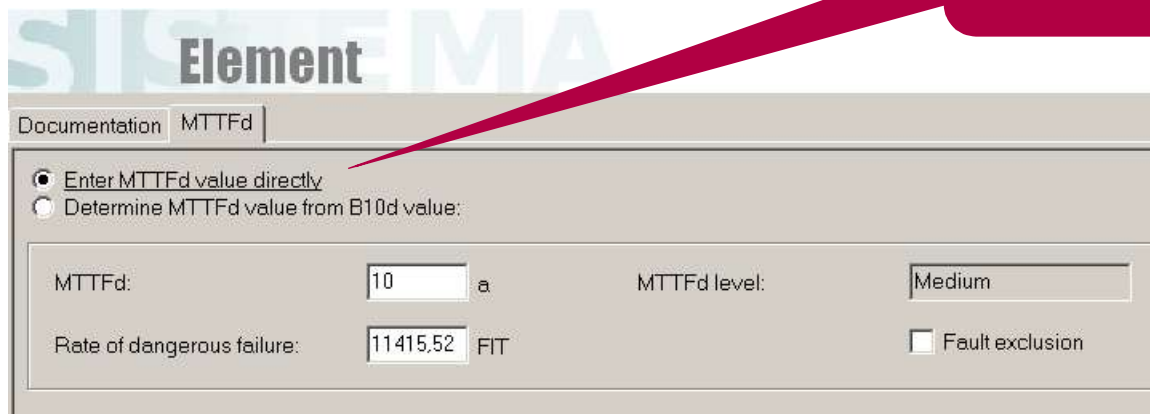
# Creación de un subsistema propio



Si se ha decidido hacer los cálculos de  $MTTF_d$  y de  $DC_{avg}$  a partir de los elementos, entrar en este último subnivel



En este último subnivel se puede introducir directamente el valor  $MTTF_d$  ó determinarlo a partir de  $B10_d$



# Creación de un subsistema propio

**Element**

Documentation | MTTFd

☐ Enter MTTFd value directly  
☒ Determine MTTFd value from B10d value:

B10d:  Cycles      nop:  Cycles/a

T10d:  a     

MTTFd:  a      MTTFd level:

Typical components value

Mission time:  a

**Nop**

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}}$$

d\_op:  Days  
h\_op:  Hours  
t\_cycle:  Seconds

**Nop**

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}}$$

d\_op:  Days  
h\_op:  Hours  
t\_cycle:  Seconds

nop:  Cycles/a

Introducimos el valor de B10<sub>d</sub> y el número de operaciones de este dispositivo

# Creación de un subsistema propio

**Block**

Documentation | MTTFd | DC | Elements

☒ Determine MTTFd value from elements  
☐ Enter MTTFd value directly

MTTFd: 8522.73 a MTTFd level: -

Mission time

Mission time: 20 a Minimum mission time: 20 a

Si vuelvo al Bloque, puedo comprobar como automáticamente se me ha calculado el  $MTTF_d$  para el canal

# Creación de un subsistema propio

**Element**

Documentation | MTTFd | DC

☐ Enter DC value directly  
☒ Select applied measures to evaluate DC

Type of measure:

Description of measure:

DC range: from  % to  % depending on:

Diagnostic coverage (DC):  %

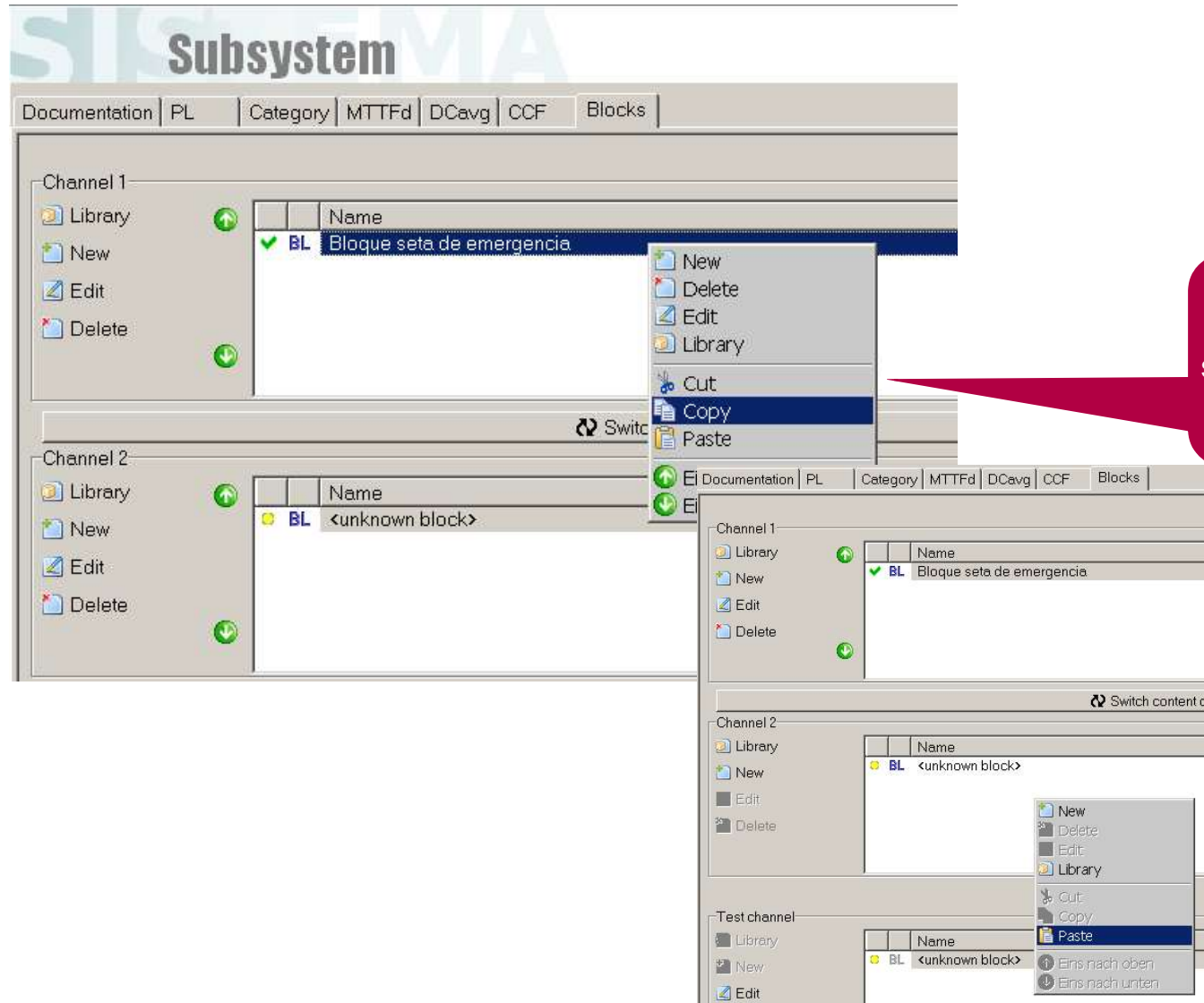
This measure alone is not sufficient for the required performance levels:

☐ a  
☐ b  
☐ c  
☐ d  
☐ e

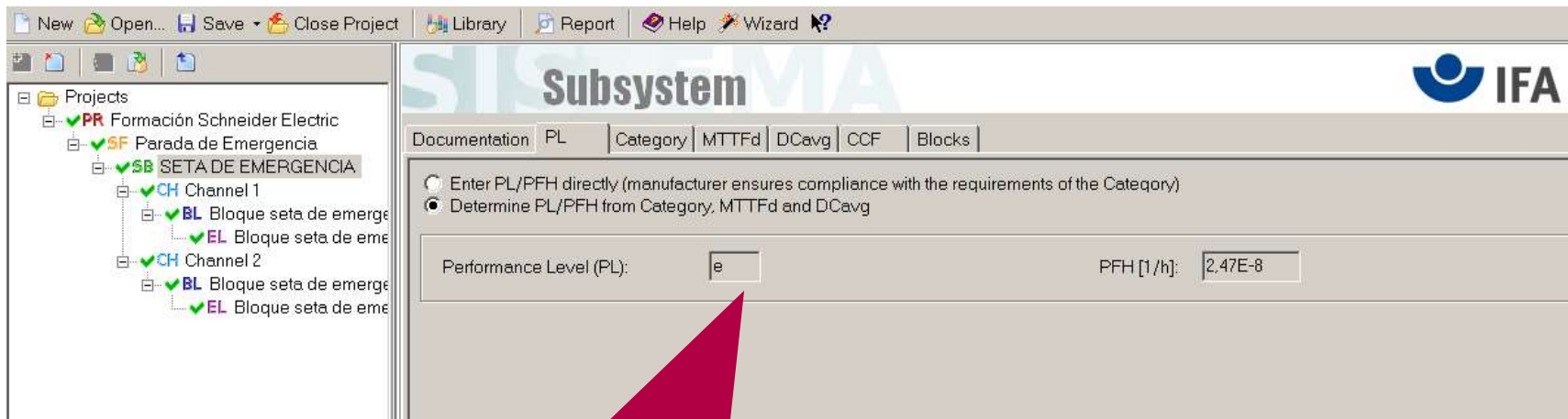
Volviendo nuevamente a elemento se puede rellenar los Dcavg en caso de querer calcularlo el total a partir de éstos. Automáticamente se me calculará para todo el subsistema



# Creación de un subsistema propio



# Creación de un subsistema propio



Si volvemos a la pestaña PL del subsistema SB veremos que el software ha calculado el PL para éste

# Creación de una librería de subsistemas propia

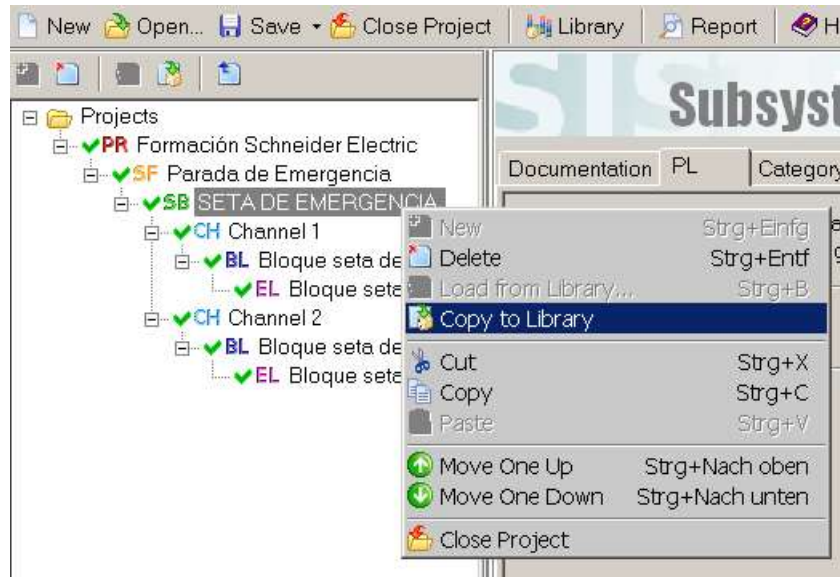
Para incorporar el subsistema a una librería seguimos los siguientes pasos:

The image shows a sequence of three screenshots from the Schneider Electric software interface, illustrating the steps to create a new library. Red callout boxes with white text provide instructions for each step.

- Step 1:** The first screenshot shows the main menu bar with options: New, Open..., Save, Close Project, **Library**, Report, Help, Wizard, and a question mark. A red callout box points to the 'Library' menu with the text: "Abrimos las librerías".
- Step 2:** The second screenshot shows the 'Library' menu open, with options: Create New Library, Add local Library..., Add Network Library..., and Close Library. A red callout box points to 'Create New Library' with the text: "Seleccionamos crear librería".
- Step 3:** The third screenshot shows the 'Save library' dialog box. The 'Guardar en:' (Save in) field is set to 'Escritorio' (Desktop). The file list shows 'Mis documentos', 'Mi PC', 'Mis sitios de red', 'BackupCF', 'Formulario\_archivos', 'Acceso directo a Dani', 'Acceso directo a SEGURIDAD', and 'DANI.SLB'. The 'Nombre:' (Name) field contains 'Librería Auxiliar' and the 'Tipo:' (Type) field contains 'SISTEMALibrary (\*.slb)'. A red callout box points to the 'Nombre:' field with the text: "Indicamos el nombre de la librería y donde queremos ubicarla".

Below the 'Save library' dialog box, there is a 'Set Changes' button. A red callout box points to this button with the text: "Salvamos cambios".

# Creación de una librería de subsistemas propia

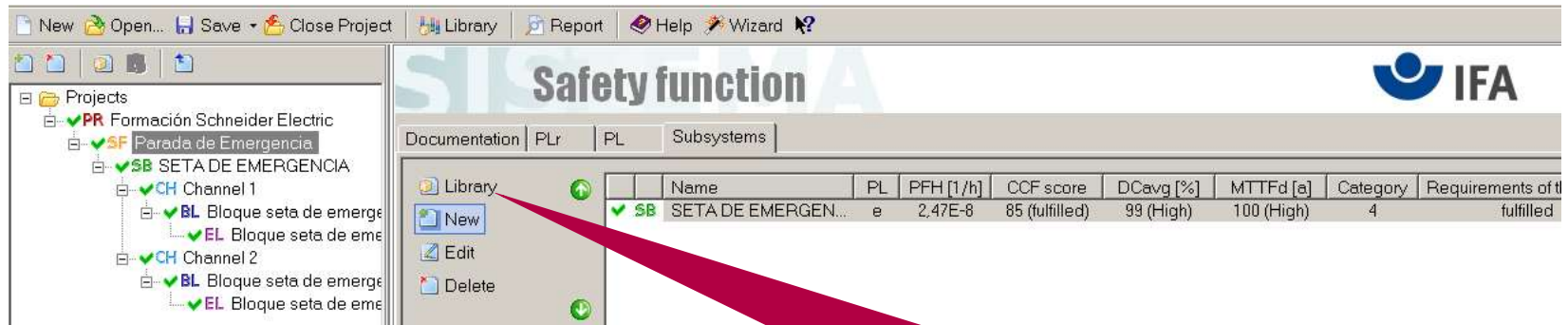


Volvemos al subsistema y con el botón derecho seleccionamos copiar a la librería.

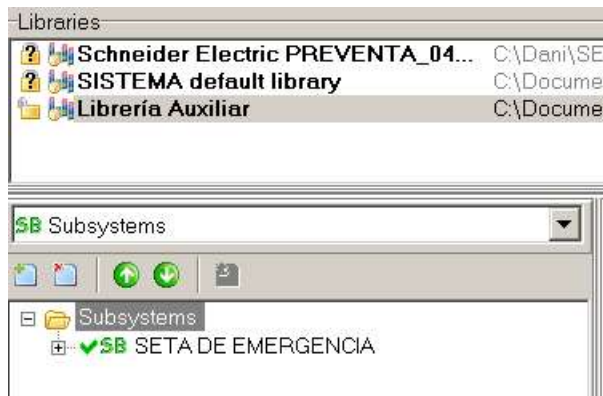


Volviendo a la librería seleccionamos salvar cambios.

# Creación de una librería de subsistemas propia



Si volvemos a la Safety Function y seleccionamos las librerías, comprobamos que podemos seleccionar el subsistema creado anteriormente





**Gracias por su atención**

*Make the most of your energy*

[www.schneiderelectric.es](http://www.schneiderelectric.es)

