Asociación Española para la Calidad (AEC)

XVIII Congreso de Confiabilidad - AEC

Madrid - 2016

FIABILIDAD, SEGURIDAD Y AUTOMATIZACIÓN: Sistemas electrónicos de control seguros ante averías (Fail Safe Systems)

Jorge Marcos Acevedo

DTE Departamento de Tecnología Electrónica
Universidad de Vigo

Universidade Vigo

Índice

Tecnologías RAMS

Fiabilidad

Sistemas Seguros ante Averías (SIS)

Normativas aplicables

- Sector de Maquinaria:
  - UNE-EN ISO 13849
  - UNE-EN IEC 62061
- Sector de Procesos:
  - UNE-EN-IEC 61508
  - UNE-EN-IEC 61511
- Sector Ferroviario:
  - UNE-EN 50126
  - UNE-EN 50128
  - UNE-EN 50129
- Sector de Automoción:
  - ISO 26262

Tecnologías RAMS

- Fiabilidad (Reliability)
- Disponibilidad (Availability)
- Mantenibilidad (Maintainability)
- Seguridad (Safety)

Fiabilidad R(t)

- Probabilidad de funcionamiento entre 0 y t

$$R(t) = e^{-\lambda(t)\cdot t}$$

Infiabilidad F(t)

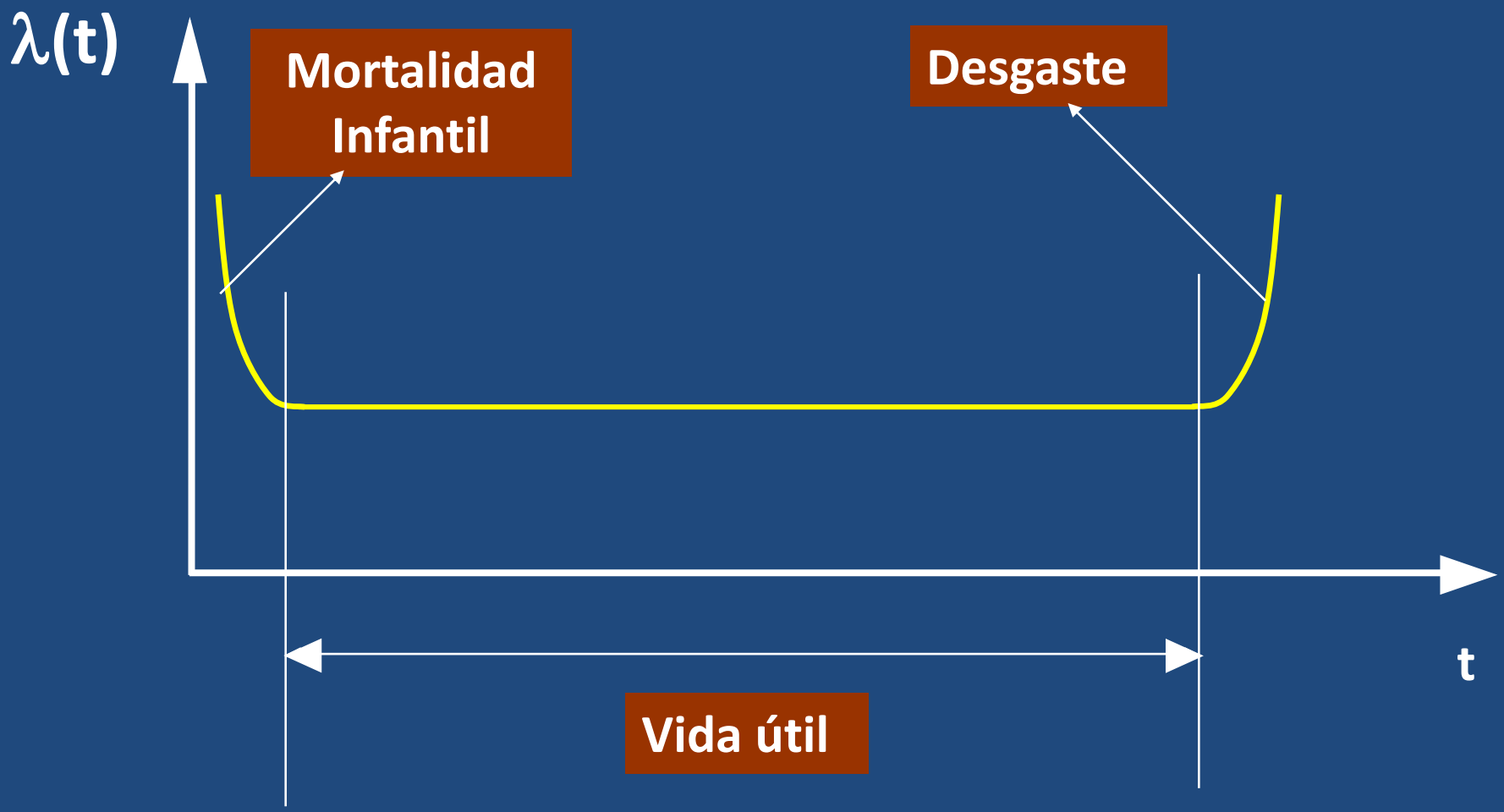
- Probabilidad de fallo entre 0 y t

$$F(t) = 1 - R(t) = 1 - e^{-\lambda(t)\cdot t}$$

Para $\lambda(t)\cdot t < 0{,}1$ =>

$$F(t) = 1 - e^{-\lambda(t)\cdot t} \approx \lambda(t)\cdot t$$

Tasa de Fallos λ(t)

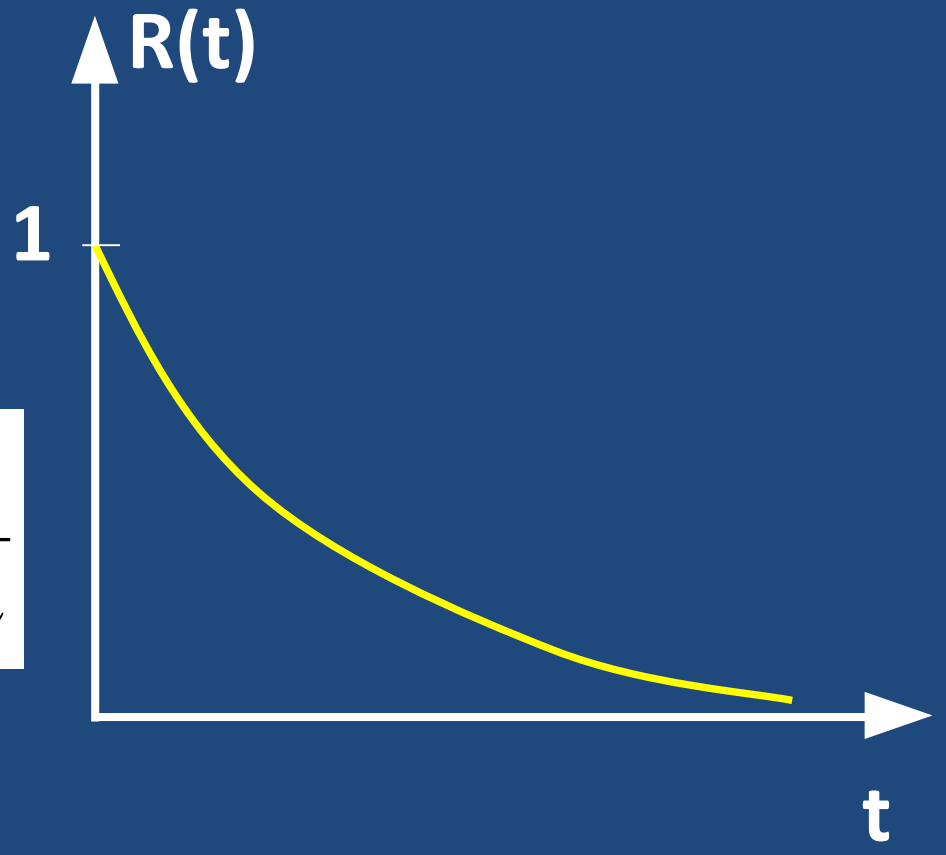


Cálculo de Fiabilidad

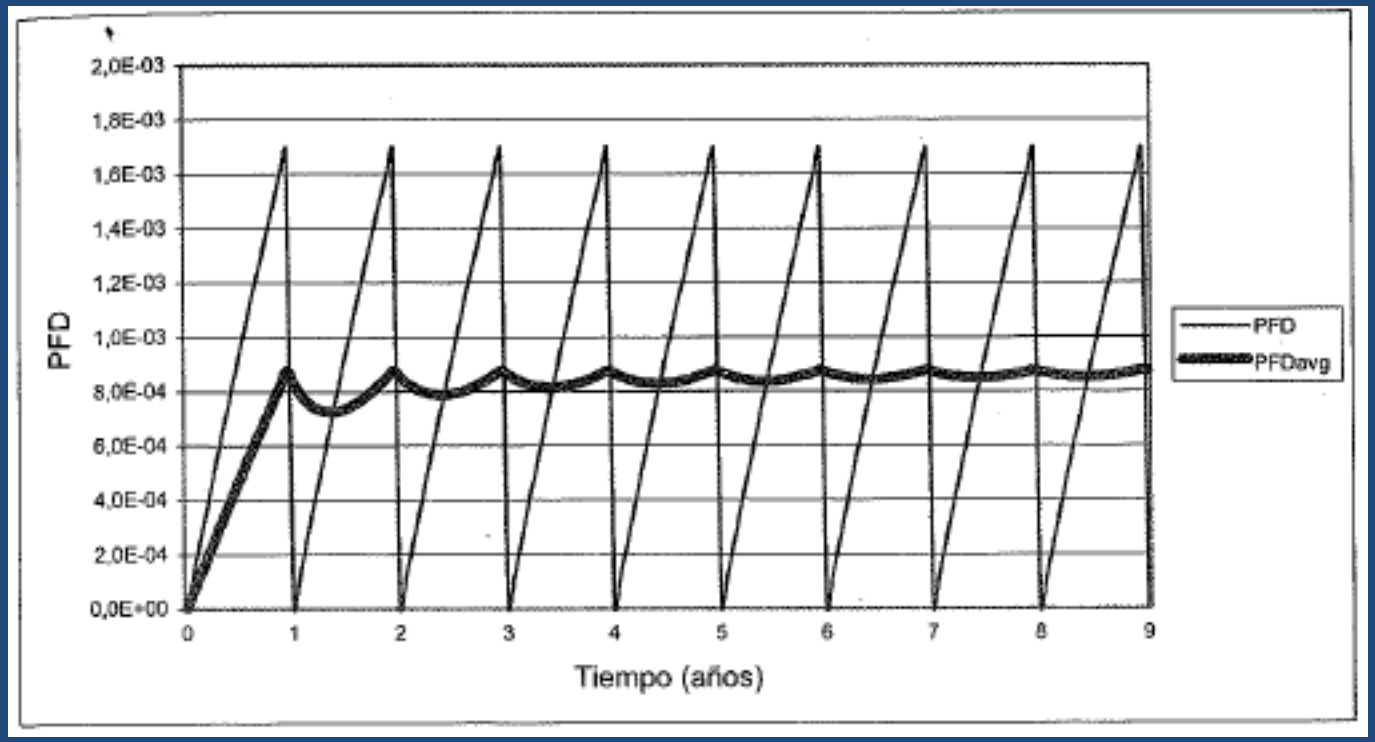
$$R(t) = e^{-\lambda \cdot t}$$

$$F(t) = 1 - e^{-\lambda \cdot t}$$

$$\theta = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t}dt = \frac{1}{\lambda}$$



Definiciones



$$PF = 1 - e^{-\lambda t} \qquad \text{Si } PF < 0{,}1 \Rightarrow PF \approx \lambda t \qquad PF = \lambda[h^{-1}] \cdot t[h]$$

$$PF_{avg} \cdot T = \int PF\, dt = \int \lambda t dt = \frac{\lambda t^2}{2}$$

Parámetros de la Fiabilidad

- Tasa de fallos [λ(t)]
- Vida media [θ]
- Tiempo medio entre fallos (Mean Time Between Failures) [MTBF]
- Tiempo medio hasta el fallo (Mean Time To Failure) [MTTF]
- Tiempo medio de reparación (Mean Time To Repair) [MTTR]

MTBF, MTTF y MTTR

$$MTBF = MTTF + MTTR$$

- **Sistemas reparables**

$$MTTF \gg MTTR \Rightarrow MTBF \cong MTTF$$

- **Sistemas no reparables**

$$MTBF = MTTF$$

Vida Media "θ"

- Sistemas Reparables:

$$\theta = \text{MTBF};\ \lambda = \frac{1}{\text{MTBF}}$$

- Sistemas no Reparables:

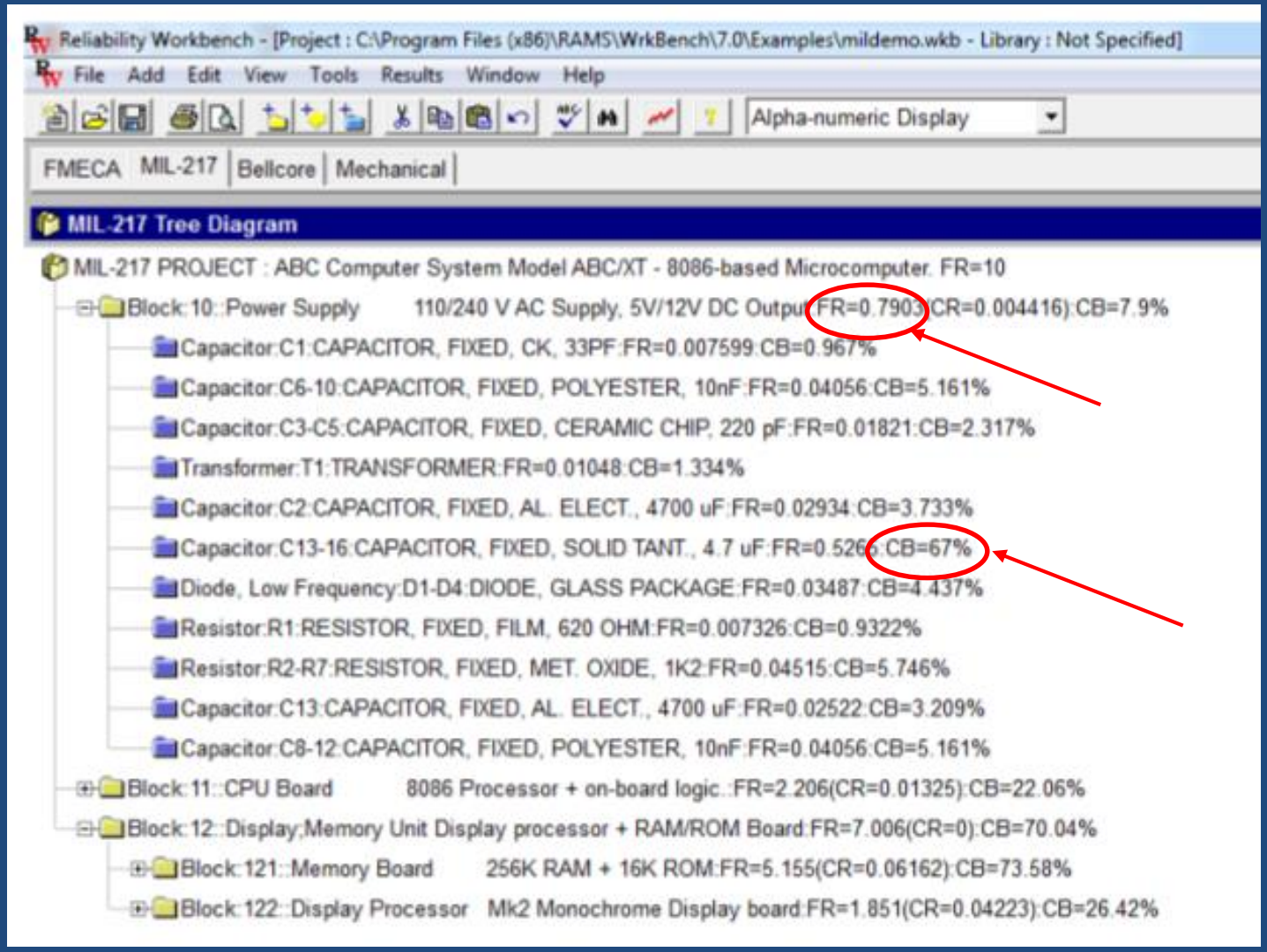
$$\theta = \text{MTTF};\ \lambda = \frac{1}{\text{MTTF}}$$

Cálculo de Tasas de Fallo de Componentes Electrónicos

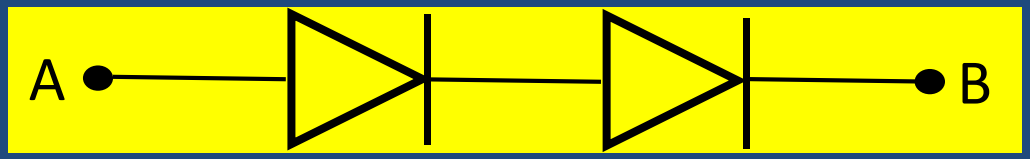
PREDICCIÓN DE FIABILIDAD

- MIL HDBK-217F
- Bellcore
- Fides
- IEC TR 62380
- SN 29500 (Siemens)
- HDBK 217 Plus

Ejemplo de Cálculo de Tasas de Fallo



Análisis Modal de Fallos Efectos y Criticades (AMFEC)



Fallo peligroso: Cortocircuito entre A y B

λ: Tasa de fallos del diodo

Modos de fallo de un diodo (IEC TR 62380)	%
Cortocircuito	80
Circuito abierto	20

$$\lambda_D = \lambda \cdot 0{,}8 \qquad \lambda_S = \lambda \cdot 0{,}2$$

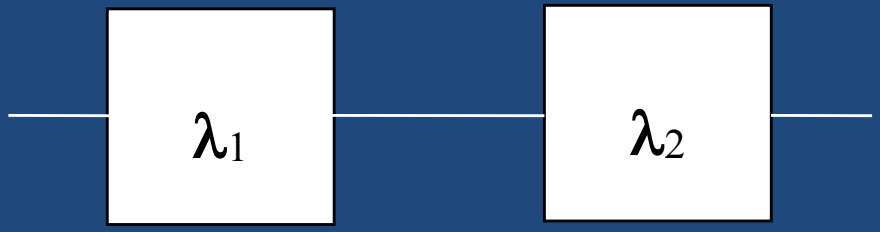
Tasas de fallo de componentes/sistemas

λ: Tasa de fallos del componente
λ_S: Tasa de fallos segura (Safety)
λ_D: Tasa de fallos peligrosa (Dangeorus)
λ_{SD}: Tasa de fallos segura y detectable
λ_{SU}: Tasa de fallos segura y no detectable
λ_{DD}: Tasa de fallos peligrosa y detectable
λ_{DU}: Tasa de fallos peligrosa y no detectable

$$\lambda = \lambda_S + \lambda_D = (\lambda_{SD} + \lambda_{SU}) + (\lambda_{DD} + \lambda_{DU})$$

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \qquad SFF = \frac{\lambda_{SU} + \lambda_{SD} + \lambda_{DD}}{\lambda_{SU} + \lambda_{SD} + \lambda_{DD} + \lambda_{DU}}$$

Sistemas Serie



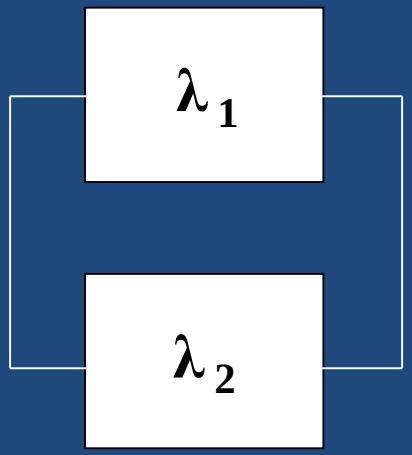
$$R_S(t) = R_1(t) \cdot R_2(t) = e^{-\lambda_S t}$$

$$\lambda_S = \lambda_1 + \lambda_2$$

$$\theta_S = MTTF_S = \frac{1}{\lambda_S} = \frac{1}{\lambda_1 + \lambda_2} = \frac{1}{\frac{1}{MTTF_1} + \frac{1}{MTTF_2}}$$

$$\frac{1}{MTTF_S} = \frac{1}{MTTF_1} + \frac{1}{MTTF_2}$$

Sistema paralelo



$$R_S(t) = 1 - F_S(t) = 1 - F_1 \cdot F_2 = \\ = R_1 + R_2 - R_1 R_2$$

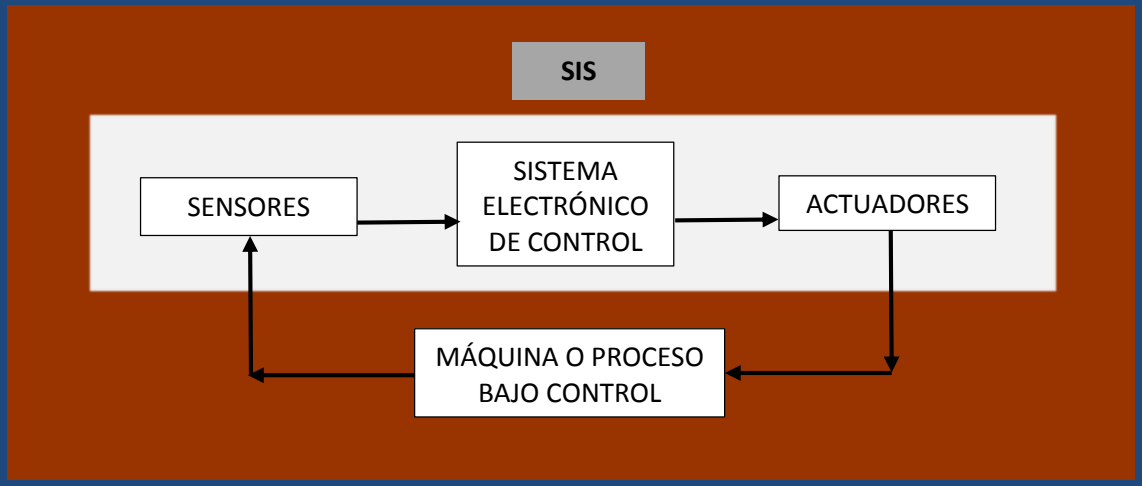
$$\theta_S = MTTF_S = \frac{1}{\lambda_S} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} =$$

$$= MTTF_1 + MTTF_2 - \frac{MTTF_1 \cdot MTTF_2}{MTTF_1 + MTTF_2}$$

Seguridad

- **Seguridad (Safety)**: Capacidad de un sistema para que, ante la presencia de un fallo en la instalación que controla o en el propio sistema de control, se alcance el estado seguro, que garantice la seguridad de las instalaciones, las personas y el medio ambiente.
- **Sistemas Seguros ante Averías (Fail-Safe Systems)**

Sistema seguro ante averías

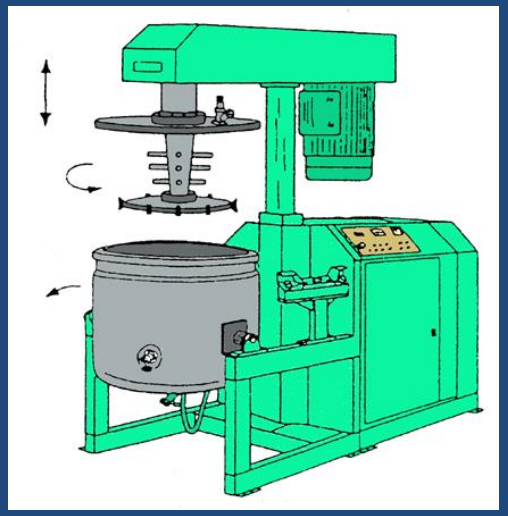


- **SIS** (Safety Instrumented System): Sistema Instrumentado de Seguridad
- **Fail-Safe System**: Sistema seguro ante averías
- **Sistema E/E/PE**: Sistema Eléctrico-Electrónico-Electrónico programable, relacionado con la seguridad

Aplicaciones (I)

- Maquinaria
- Químicas y petroquímicas
- Industria de alimentación
- Transporte de combustibles
- Transporte de personas
- Electromedicina
- Minería

Aplicaciones (II)



Directivas y normas

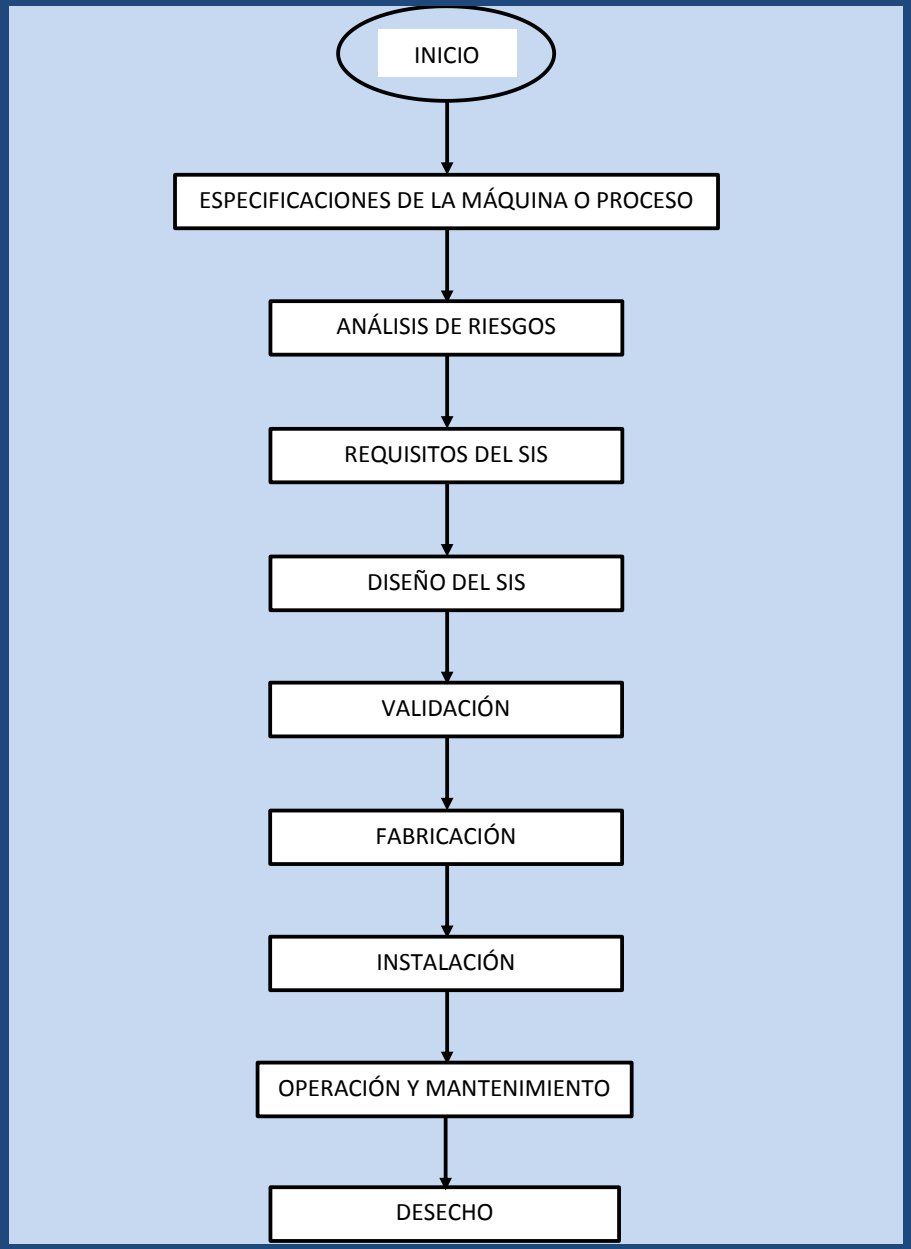
- Directivas Europeas
- Normas técnicas: Organismos de normalización europeos (ETSI, CEN, CENELEC, etc.) e internacionales (ISO, IEC, ANSI, ISA, etc.).
- La aplicación de las normativas armonizadas europeas presupone el cumplimiento con las directivas correspondientes.

Procedimiento General

- **Análisis de Riesgos.**
  - **UNE-EN ISO 12100 (2012)**

$$R = G \cdot P$$

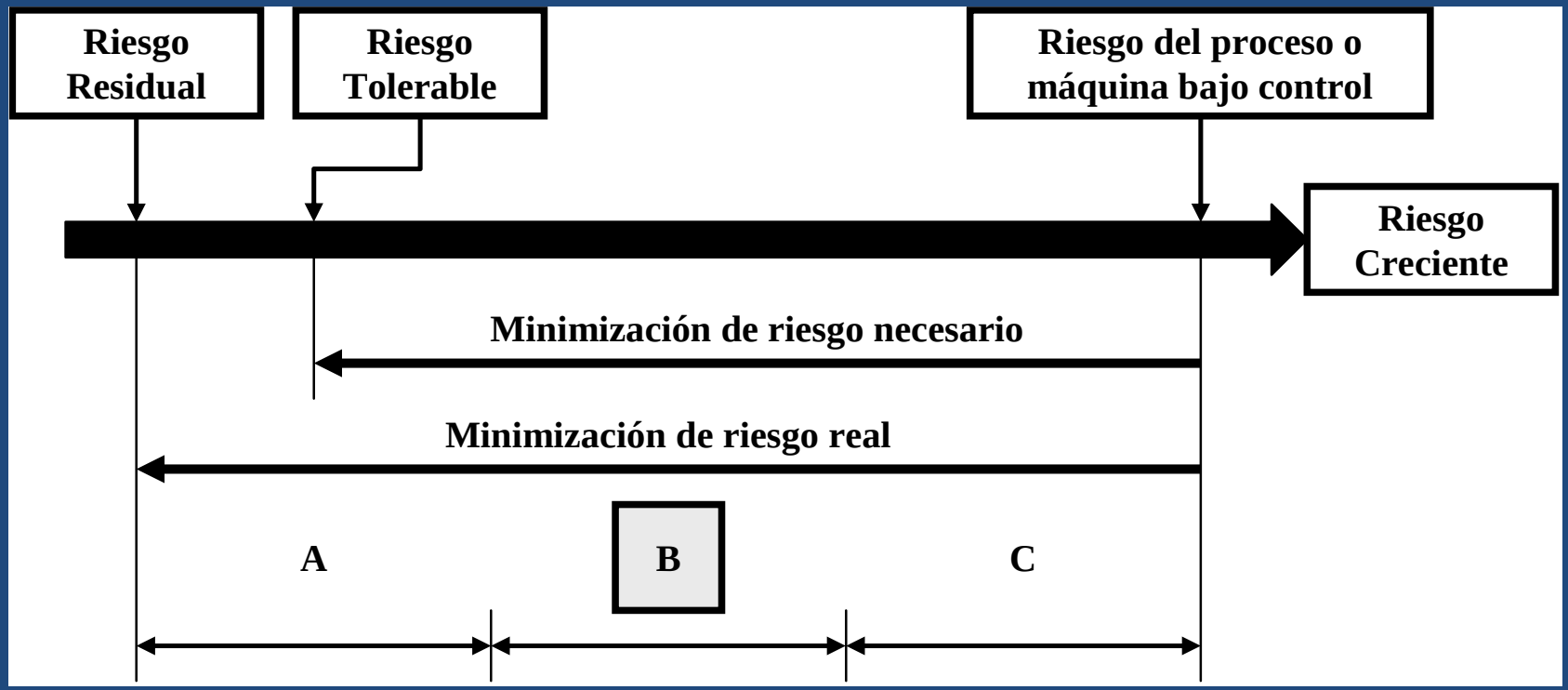
- **Nivel de seguridad exigido**
- **Implementación**
- **Verificación**
- **Certificación:** Organismos internacionales (Exida, TÜV Nord, TÜV Rheinland y TÜV Süd)
- **Operación y mantenimiento**



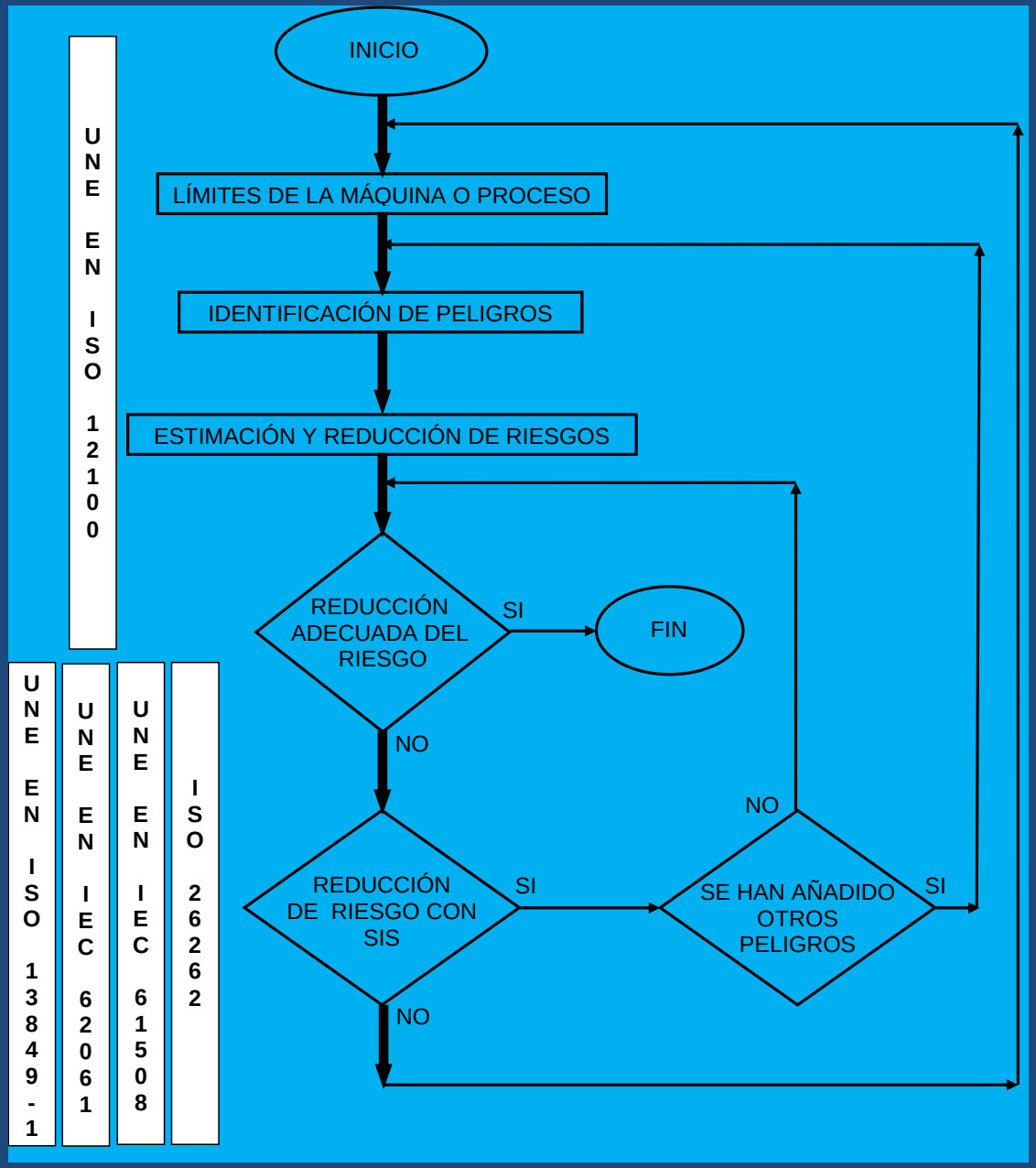
Herramientas de análisis

- PHA (Preliminary Hazard Analisys) o HAZID (Hazard Identification): Análisis preliminar con escasa información de histórico de fallos, causas y consecuencias.
- HAZOP (Hazard and Operability Study): Es una estructura analítica dentro de un grupo (brainstorming) que analiza de forma sistemática todas las posibles desviaciones del proceso e identifica sus causas y consecuencias.
- FMECA (Failure Mode, Effects and Criticity Analisys), AMFEC: UNE-EN 60812:2008 Técnicas de análisis de la fiabilidad de sistemas. Procedimiento de análisis de los modos de fallo y de sus efectos (AMFE).
- FTA (Fault Tree Analisys): UNE-EN 61025:2011 Análisis por árbol de fallos (AAF).

Reducción del riesgo



Diseño de un SIS



Normativas de seguridad

- Maquinaria
- Procesos
- Ferroviario
- Automoción

Normativas Maquinaria

- **UNE-EN ISO 13849**: Seguridad de las máquinas. Partes de los sistemas de mando relativas a la seguridad. Parte 1 (2008): Principios generales para el diseño. Parte 2 (2013): Validación.
- **UNE-EN IEC 62061 (2005)**: Seguridad de las máquinas. Seguridad funcional de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad.

Obtención del nivel de seguridad (I)

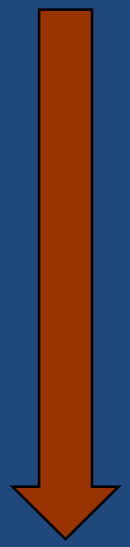
- **Norma UNE-EN ISO 13849**

S Gravedad del daño	S_1	Daño leve (normalmente reversible)
	S_2	Daño grave (normalmente irreversible, incluyendo la muerte)
F Frecuencia y/o tiempo de exposición	F_1	Rara vez hasta a menudo y/o tiempo de exposición corto
	F_2	Frecuente a continuo y/o tiempo de exposición largo
P Posibilidad de evitar el peligro	P_1	Posible en ciertas condiciones
	P_2	Difícilmente posible

Obtención del nivel de seguridad (II)

- Norma UNE-EN ISO 13849

S	F	P	PL
S_1	F_1	P_1	a
		P_2	b
	F_2	P_1	
		P_2	c
S_2	F_1	P_1	
		P_2	d
	F_2	P_1	
		P_2	e



Riesgo Creciente

Niveles de Seguridad (UNE-EN ISO 13849)

PL (Performance Level) Nivel de prestaciones

PL	Probabilidad media de fallo peligroso por h (PFH_d)
a	$\geq 10^{-5}$ a $< 10^{-4}$
b	$\geq 3\times10^{-6}$ a $< 10^{-5}$
c	$\geq 10^{-6}$ a $< 3\times10^{-6}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
e	$\geq 10^{-8}$ a $< 10^{-7}$

$$\lambda_d = \frac{1}{MTTF_d}$$

$$PFH_d = \lambda_d[h^{-1}] \cdot t[h]$$

Componentes no eléctricos

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600[\frac{s}{h}]}{t_{ciclo}} \qquad T_{10d} = \frac{\beta_{10d}}{n_{op}} \qquad F(T_{10d}) = 1 - e^{-\lambda_d \cdot T_{10d}} = 0{,}1(10\%)$$

$$\lambda_d \approx \frac{0{,}1}{T_{10d}} \qquad MTTF_d = \frac{1}{\lambda_d} = \frac{T_{10d}}{0{,}1} = \frac{\beta_{10d}}{n_{op} \cdot 0{,}1}$$

- $\mathbf{n_{op}}$ = nº medio de ciclos por año
- $\mathbf{d_{op}}$ = nº medio de días de utilización por año
- $\mathbf{h_{op}}$ = nº medio de horas de utilización por día
- $\mathbf{t_{ciclo}}$ = nº medio de segundos por ciclo
- $\mathbf{T_{10d}}$ = Tiempo medio hasta que fallan el 10% de los componentes
- $\mathbf{\beta_{10d}}$ = nº medio de ciclos hasta que fallan el 10% de los componentes

Componentes electrónicos

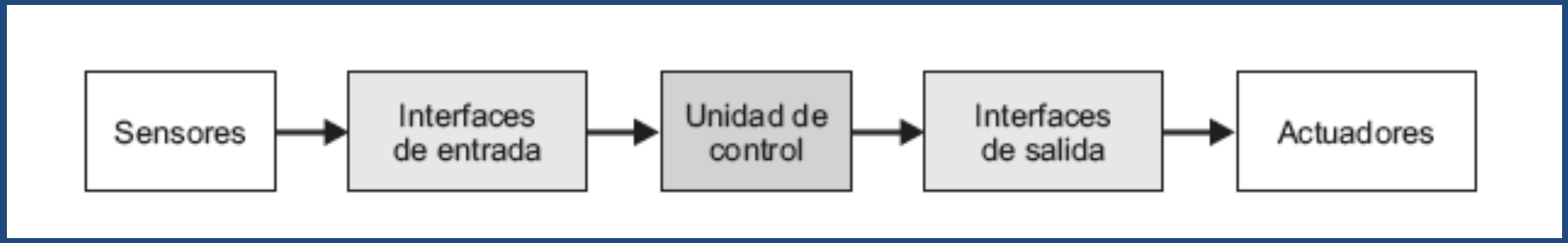
- Se puede obtener el $MTTF_d$ de la propia norma que da datos para componentes genéricos funcionando a 40ºC y carga nominal, obtenidos de la norma SN 29500.
- Da también el **$MTTF_d$ más favorable** que es el 10% del valor anterior ($MTTF_d$).

Componente	MTTF [Años]	Fallos peligrosos	$MTTF_d$ [Años]	Caso más favorable (10%)
	X	50%	2X	2X/10

- Como mejor solución se sugiere un AMFE del componente.

Categorías de SIS (I)

Categorías: B, 1, 2, 3 y 4



Categoría B:

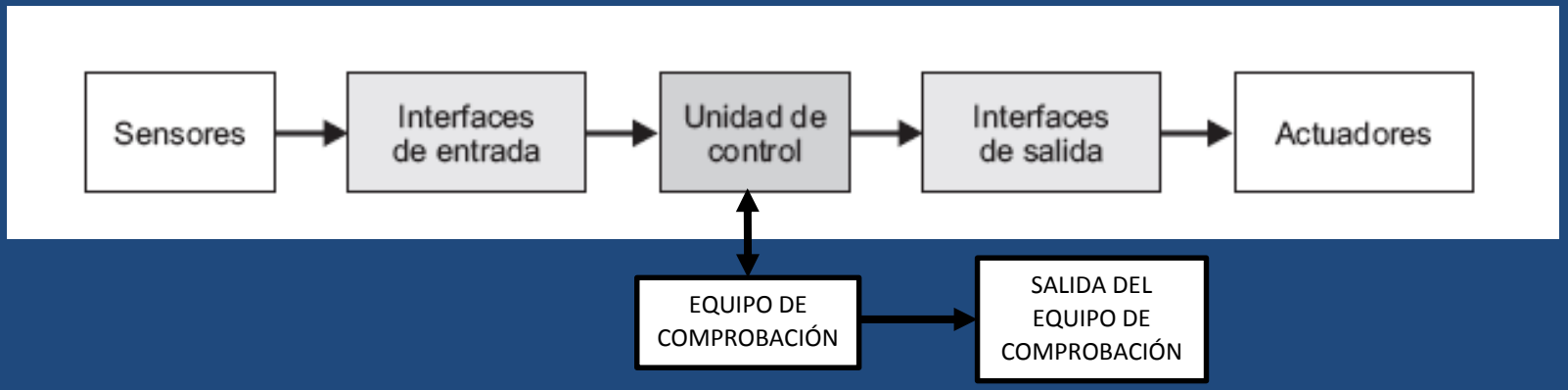
Diseño según los principios básicos de seguridad, DC_{avg} = 0, $PL_{Máx.}$ = b

Categoría 1:

Requisitos de B, componentes que han dado buenos resultados en aplicaciones similares, demuestra ser adecuado y fiable para aplicaciones de seguridad, DC_{avg} = 0, $PL_{Máx.}$ = c

Categorías de SIS (II)

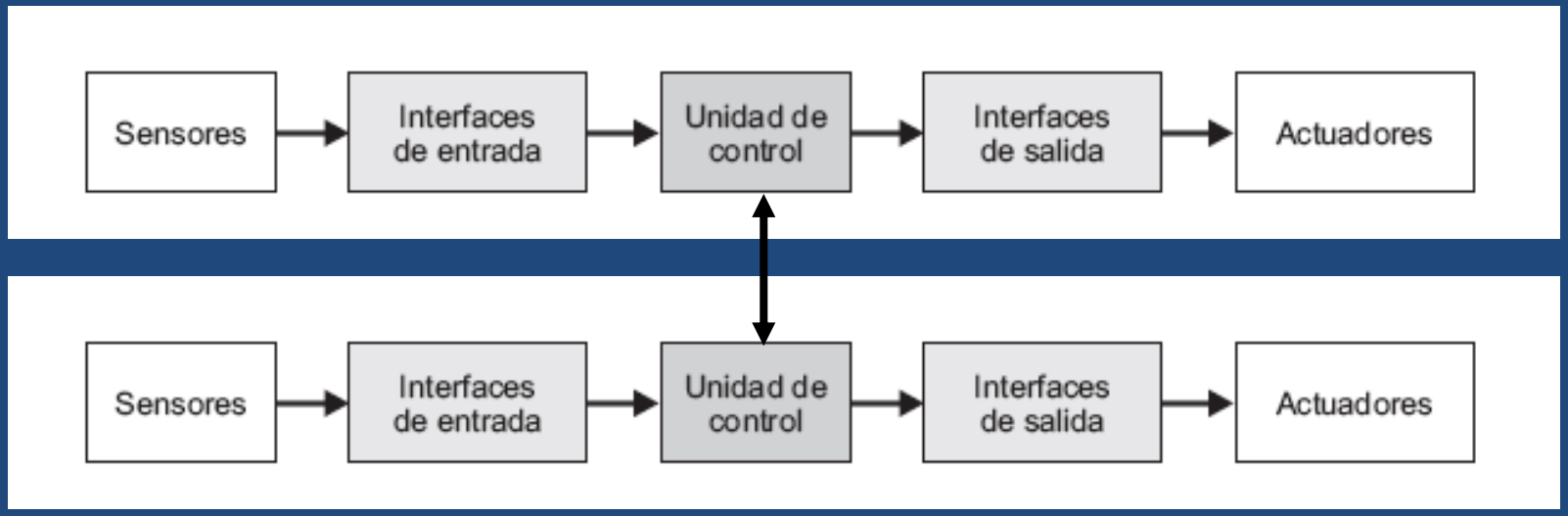
Categoría 2:



- Requisitos de 1, las funciones de seguridad se deben comprobar periódicamente, de forma manual o automática
- DC_{avg} = Baja, $PL_{Máx.}$ = d
- En el cálculo del $MTTF_d$ y de DC_{avg} no entran los bloques de comprobación

Categorías de SIS (III)

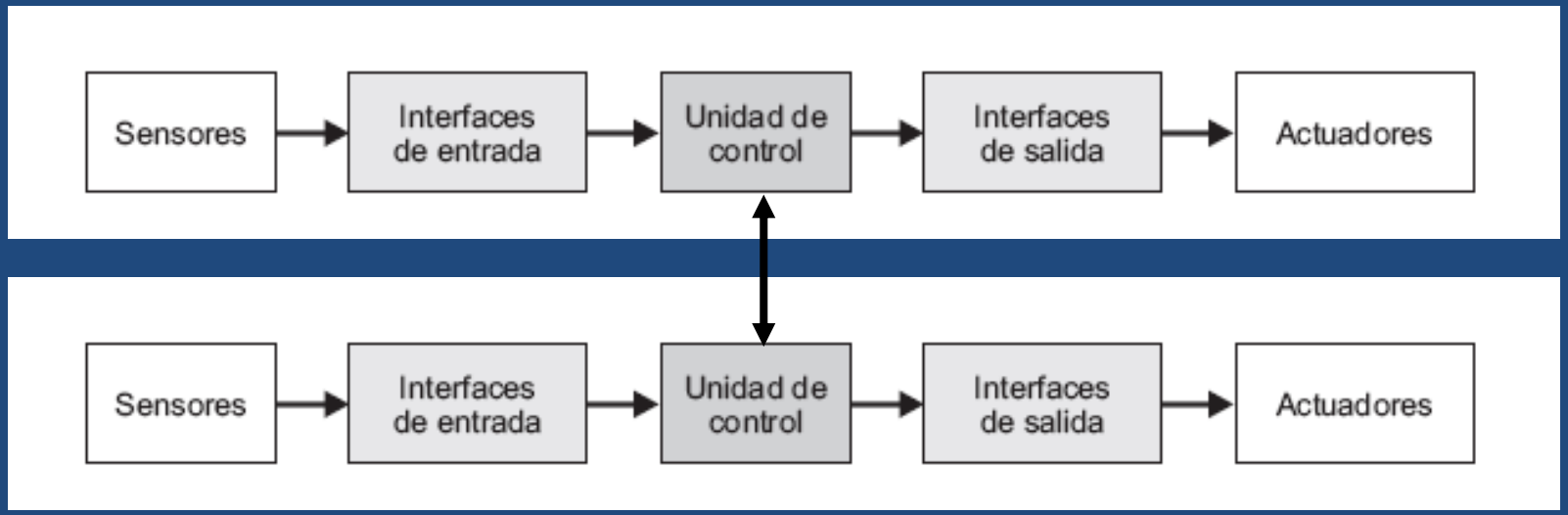
Categoría 3:



- Requisitos de B y eficacia probada, un solo defecto no lleva a la pérdida de la función de seguridad (FS), algunos defectos se detectan pero no todos, la acumulación de defectos no detectados pueden producir la pérdida de la función de seguridad.
- Dc_{avg} = Baja,

Categorías de SIS (IV)

Categoría 4:



- Requisitos de B y de eficacia probada, un solo defecto no lleva a la pérdida de la función de seguridad (FS), los defectos se detectan a tiempo para no perder la FS. La acumulación de defectos no detectados no pueden producir la pérdida de la función de seguridad.
- Dc_{avg} = Alta, El $MTTF_d$ de cada canal redundantes debe ser alto.

Evaluación del nivel PL (I)

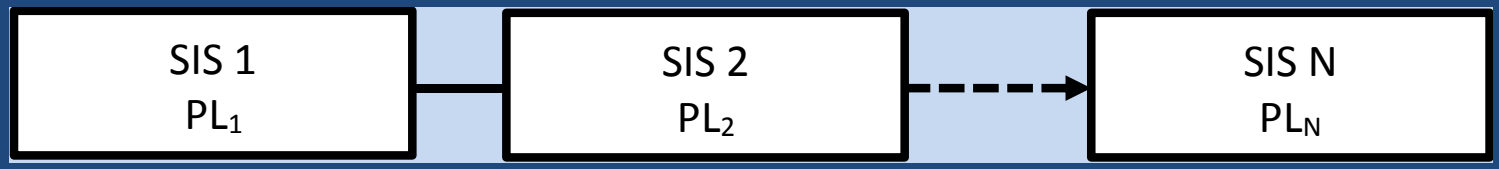
$MTTF_d$	
Índice para cada canal	**Rango**
Bajo	3 años ≤ $MTTF_d$ < 10 años
Medio	10 años ≤ $MTTF_d$ < 30 años
Alto	30 años ≤ $MTTF_d$ ≤ 100 años

DC	
Índice	**Rango**
Nula	DC < 60%
Baja	60% ≤ DC < 90%
Media	90% ≤ DC < 99%
Alta	99% ≤ DC

Evaluación del nivel PL (II)

Categoría	B	1	2	2	3	3	4
DC_{avg}	Nula	Nula	Baja	Media	Baja	Media	Alta
$MTTF_d$							
Bajo	a	No cubierto	a	b	b	C	No cubierto
Medio	B	No cubierto	b	c	c	d	No cubierto
Alto	No cubierto	c	c	d	d	d	e

Método Simplificado (I)

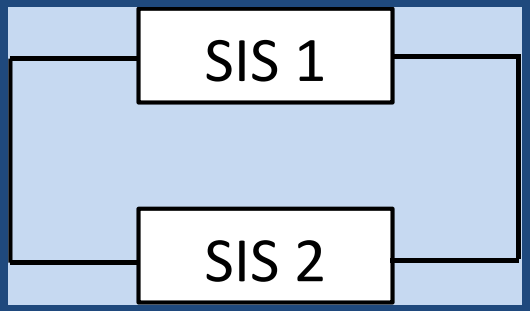


PL_i más bajo = PL_{Low} ; Identificar N_{Low} con $PL_i = PL_{Low}$

PL_{low}	N_{low}	PL
a	>3	No autorizado
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} = \sum_{j=1}^{N} \frac{n_j}{MTTF_{dj}}$$

Método Simplificado (II)



$$MTTF_d = \frac{2}{3}\left[MTTF_{d1} + MTTF_{d2} - \frac{1}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}}}\right]$$

El sistema es equivalente a uno formado por dos bloques iguales con el $MTTF_d$ calculado

Obtención del nivel de seguridad (I)

➢ Norma UNE-EN-IEC 62061

Fr		Pr		Av	
≤ 1h	5	Frecuentemente	5		
> 1h - 1Día	5	Probable	4		
> 1Día - 2Semanas	4	Posible	3	Imposible	5
> 2Semanas – 1Año	3	Poco Frecuente	2	Posible	3
> 1Año	2	Despreciable	1	Probable	1

Consecuencias	Se	Cl = Fr + Pr + Av				
		3-4	5-7	8-10	11-13	14-15
Muerte, pérdida de ojos, brazos	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanente, pérdida de dedos	3			SIL 1	SIL 2	SIL 3
Reversible, tratamiento médico	2				SIL 1	SIL 2
Reversible, primeros auxilios	1					SIL 1

Obtención del nivel de seguridad (II)

- **Niveles de Seguridad (UNE-EN-IEC 62061):**

  SIL (Safety Integrity Level). Nivel de seguridad integral

SIL	Probabilidad de Fallo Peligroso por Hora (PFH_D)
SIL 3	≥ 10^{-8} to < 10^{-7}
SIL 2	≥ 10^{-7} to < 10^{-6}
SIL 1	≥ 10^{-6} to < 10^{-5}

$$PFH_D = \lambda_D[h^{-1}] \cdot t[h]$$

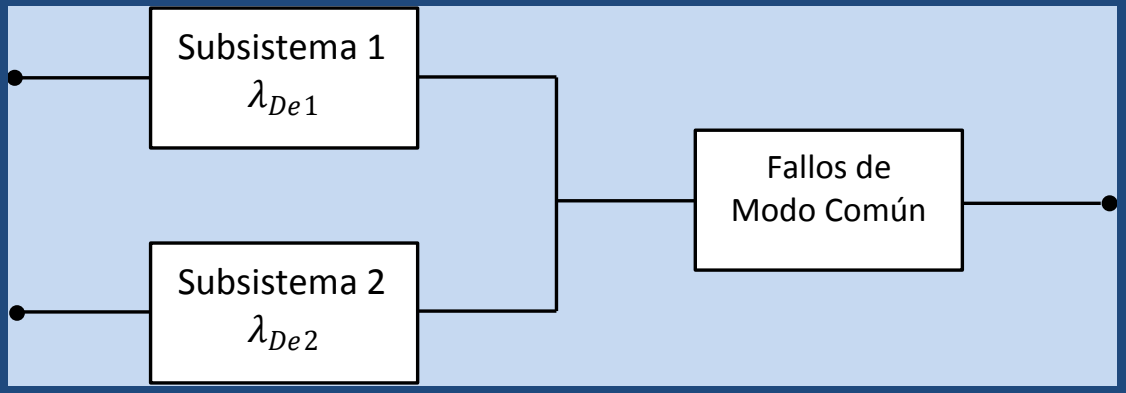
Arquitecturas Hardware (I)

Arquitectura A

$$\lambda_{DssA} = \lambda_{De1} + \cdots + \lambda_{Den}$$

$$PFH_{DssA} = \lambda_{DssA} \cdot 1h$$

Arquitectura B

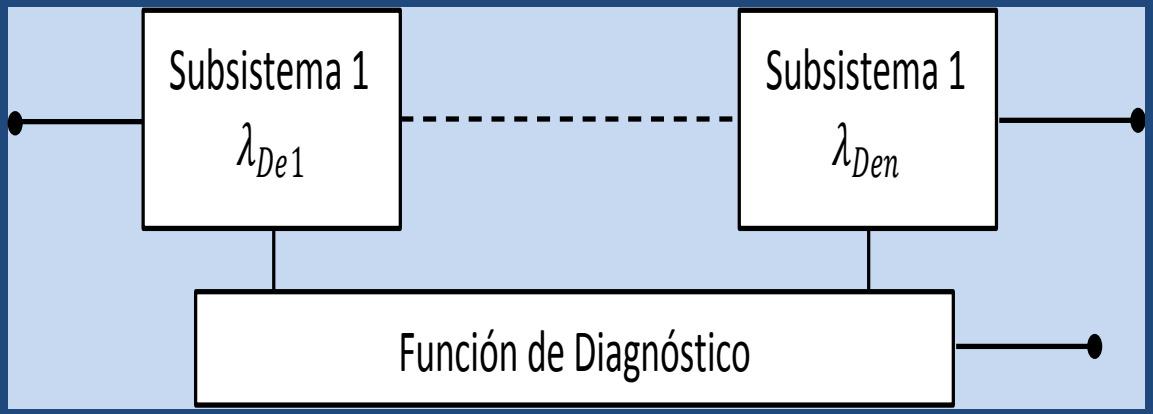


$$\lambda_{DssB} = (1-\beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \frac{\lambda_{De1} + \lambda_{De2}}{2}$$

$$PFH_{DssB} = \lambda_{DssB} \cdot 1h$$

Arquitecturas Hardware (II)

Arquitectura C

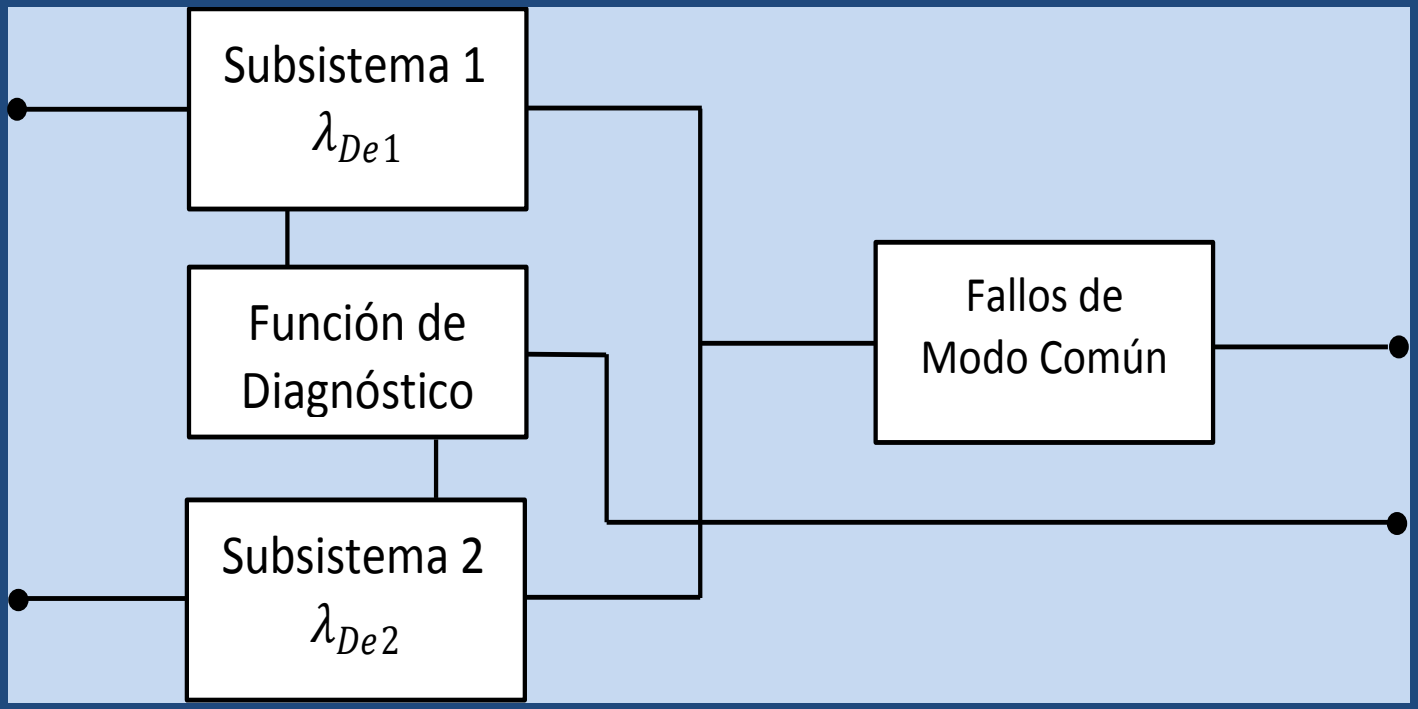


$$\lambda_{DssC} = \lambda_{De1}(1 - DC_1) + \cdots + \lambda_{Den}(1 - DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \cdot 1h$$

Arquitecturas Hardware (III)

Arquitectura D



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

$$\lambda_{DU} = \lambda_D \cdot (1 - DC)$$

Arquitecturas Hardware (IV)

Arquitectura D

Elemento distintos

$$\lambda_{DssD} = (1-\beta)^2 \left\{ [\lambda_{De1} \cdot \lambda_{De2} (DC_1 + DC_2)] \frac{T_2}{2} + [\lambda_{De1} \cdot \lambda_{De2} (2 - DC_1 - DC_2)] \frac{T_1}{2} \right\}$$

$$PFH_{DssD} = \lambda_{DssD} \cdot 1h$$

Elemento iguales

$$\lambda_{DssD} = (1-\beta)^2 \left\{ [\lambda_{De}^2 \cdot 2 \cdot DC] \frac{T_2}{2} + [\lambda_{De}^2 \cdot (1 - DC)] T_1 \right\} + \beta \cdot \lambda_{dE}$$

$$PFH_{DssD} = \lambda_{DssD} \cdot 1h$$

Evaluación del nivel SIL (I)

HFT	ARQUITECTURAS POSIBLES
0	1oo1
1	1oo2 ó 2oo3
2	1oo3 ó 2oo4

SFF	HFT		
	0	1	2
<60%	No Permitido	SIL 1	SIL 2
60%≥ ÷ <90%	SIL 1	SIL 2	SIL 3
90%≥ ÷ <99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3

Evaluación del nivel SIL (I)

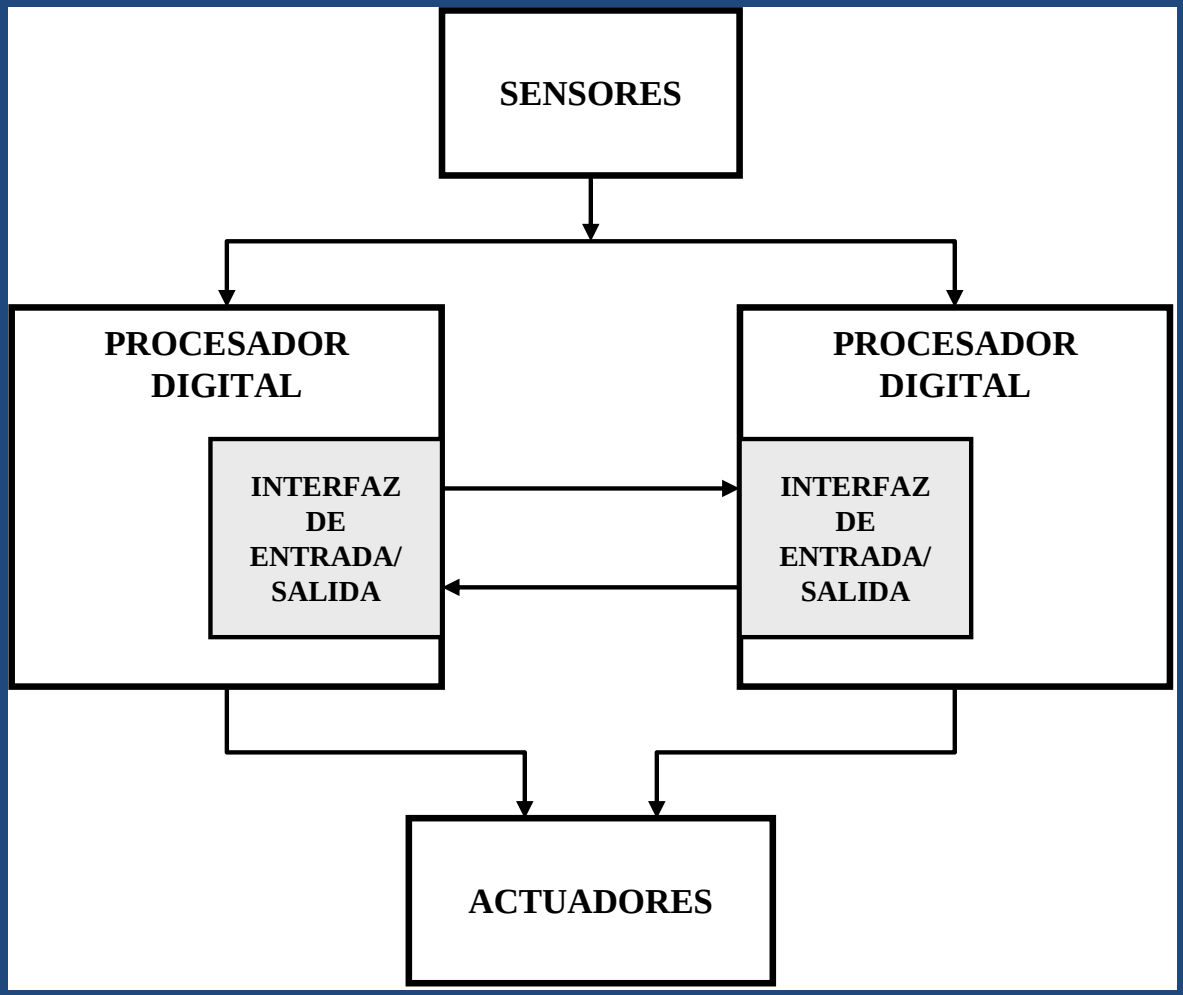
Categoría	HFT	SFF	SIL Máx.
1	0	< 60%	1
2	0	60% ≥ ÷ < 90%	1
3	1	< 60%	1
	1	60% ≥ ÷ < 90%	2
4	>1	60% ≥ ÷ < 90%	3
	1	≥ 90%	3

Categoría	HFT	DC	PFH_D
1	0	0%	Anexo D
2	0	60% > ÷ ≤ 90%	$\geq 10^{-6}$
3	1	60% > ÷ ≤ 90%	$\geq 2 \cdot 10^{-7}$
4	>1	60% > ÷ ≤ 90%	$\geq 3 \cdot 10^{-8}$
	1	> 90%	$\geq 3 \cdot 10^{-8}$

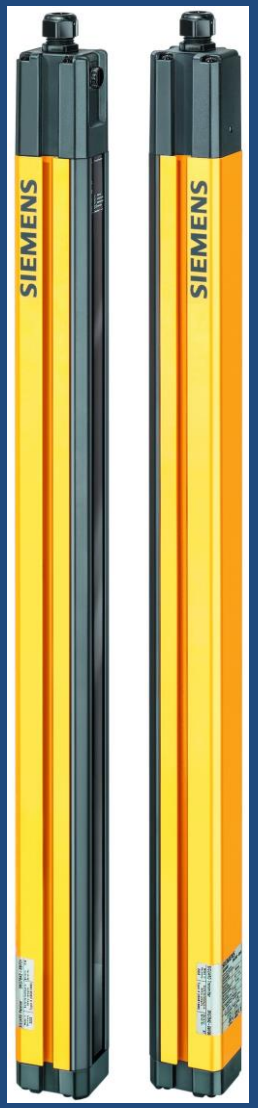
Comparativa
UNE-EN-IEC 62061 / UNE-EN ISO 13849

SIL	Probabilidad media de fallo peligroso por h (PFH_D)	PL
--	$\geq 10^{-5}$ a $< 10^{-4}$	a
1	$\geq 3\times10^{-6}$ a $< 10^{-5}$	b
1	$\geq 10^{-6}$ a $< 3\times10^{-6}$	c
2	$\geq 10^{-7}$ a $< 10^{-6}$	d
3	$\geq 10^{-8}$ a $< 10^{-7}$	e

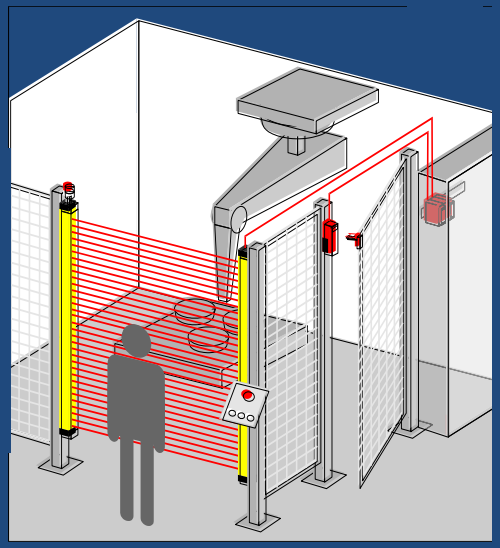
Sistemas de paro de emergencia (I)

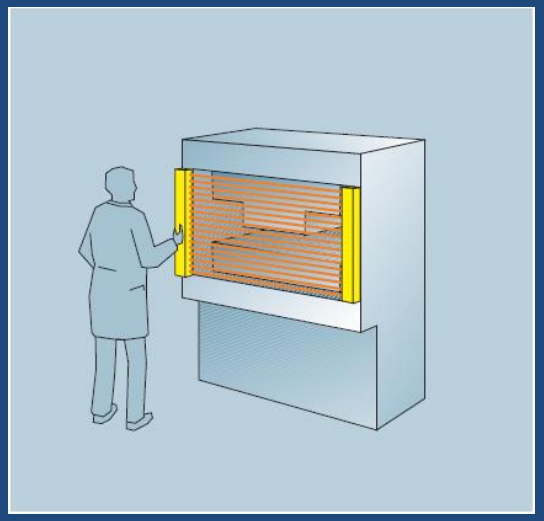


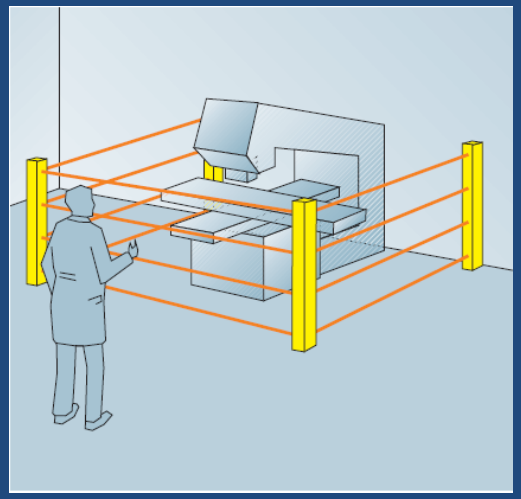
Sistemas de paro de emergencia (II)



Ejemplos



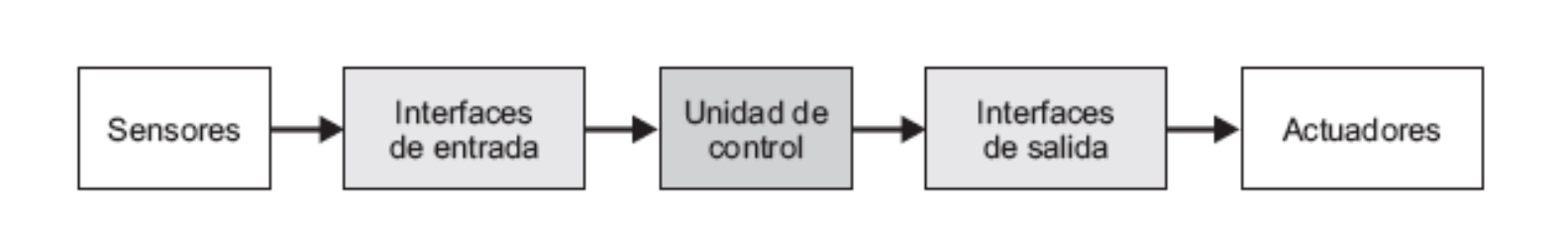




Normativas Procesos

- **UNE-EN-IEC 61508 (2011)**: Seguridad funcional de los sistemas eléctricos-electrónicos-electrónicos programables, relacionados con la seguridad.
- **UNE-EN-IEC 61511 (2006)**: Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias de procesos.

SIS



MODOS DE OPERACIÓN DE UN SIS	
CONTINUO	La función de seguridad es parte del modo normal de operación
ALTA DEMANDA	La función de seguridad se lleva a cabo solo bajo demanda y se ejecuta más de una vez al año
BAJA DEMANDA	La función de seguridad se lleva a cabo solo bajo demanda y se ejecuta menos de una vez al año

Normativas Procesos (I)

- **Niveles de Seguridad (UNE-EN-IEC 61508):**

  SIL (Safety Integrity Level). Nivel de seguridad integral

SIL	PFD_{avg} (Baja demanda)	PFH $[h^{-1}]$ (Alta demanda)	Disponibilidad	< RRF ≤
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	$\geq 10^{-9}$ a $< 10^{-8}$	>99,99%	10^4 a 10^5
SIL 3	$\geq 10^{-4}$ a $< 10^{-3}$	$\geq 10^{-8}$ a $< 10^{-7}$	99,90-99,99%	10^3 a 10^4
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	$\geq 10^{-7}$ a $< 10^{-6}$	99,00-99,90%	10^2 a 10^3
SIL 1	$\geq 10^{-2}$ a $< 10^{-1}$	$\geq 10^{-6}$ a $< 10^{-5}$	90,00-99,00%	10 a 10^2

Normativas Procesos (II)

SIL	PFD_{avg} (Baja demanda)	Disponibilidad	< RRF ≤
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	>99,99%	10^4 a 10^5
SIL 3	$\geq 10^{-4}$ a $< 10^{-3}$	99,90-99,99%	10^3 a 10^4
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	99,00-99,90%	10^2 a 10^3
SIL 1	$\geq 10^{-2}$ a $< 10^{-1}$	90,00-99,00%	10 a 10^2

$$Disponibilidad = 1 - PFD_{avg}$$

$$RRF = \frac{1}{PFD_{avg}}$$

Normativas Procesos (III)

SIL	> PFD_{avg} ≥ (Baja demanda)	< RRF ≤
SIL 4	0,0001 a 0,00001	10000 a 100000
SIL 3	0,001 a 0,0001	1000 a 10000
SIL 2	0,01 a 0,001	100 a 1000
SIL 1	0,1 a 0,01	10 a 100

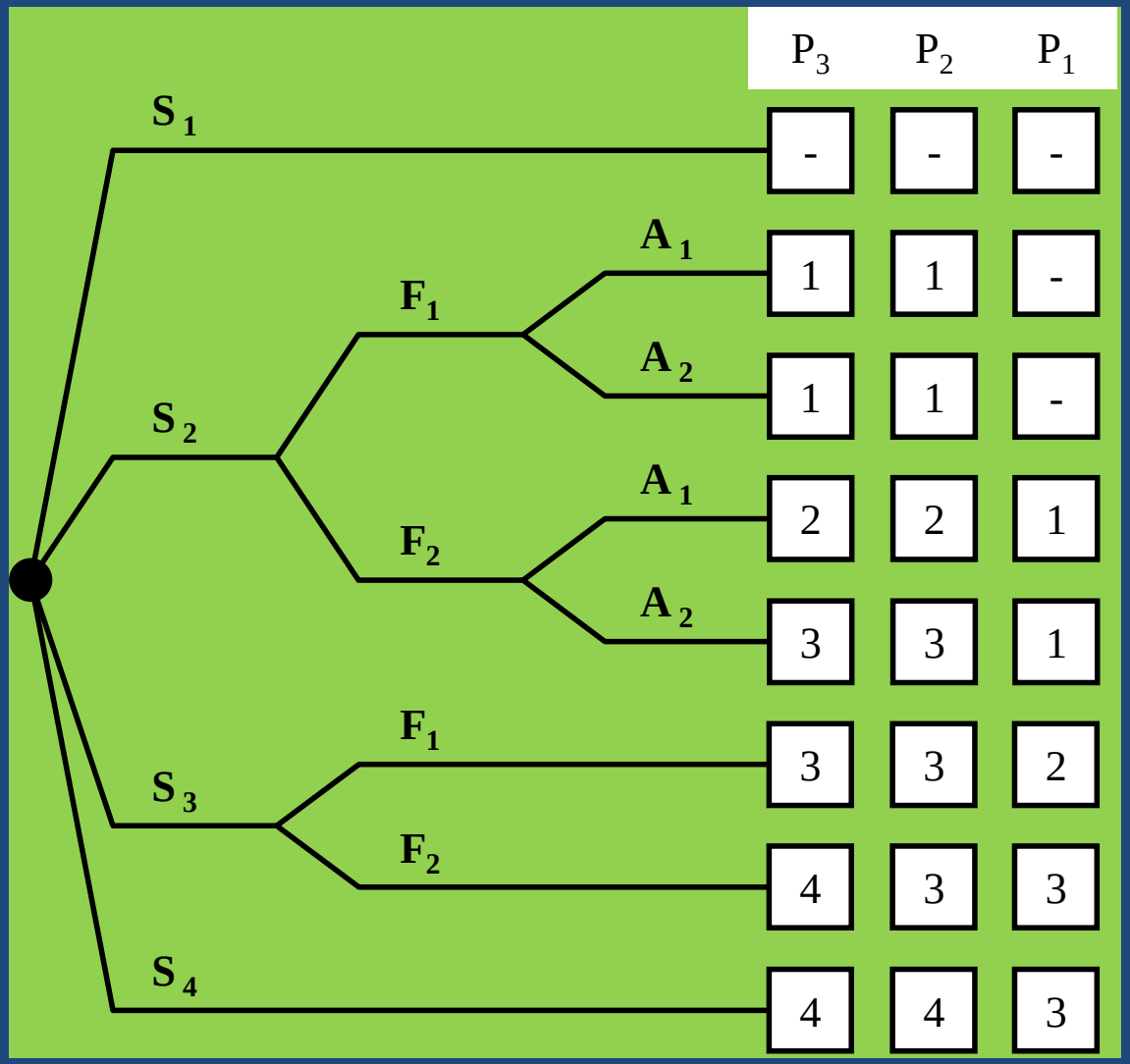
$$Disponibilidad = 1 - PFD_{avg}$$

$$RRF = \frac{1}{PFD_{avg}}$$

Determinación del Nivel SIL (I)

S (Severidad de lesiones/daños)	
S_1	Lesiones pequeñas, daños medioambientales menores (Daños mínimos)
S_2	Lesiones serias irreversibles de muchas personas o una muerte daños medioambientales temporales serios
S_3	Muerte de varias personas daños medioambientales serios de larga duración.
S_4	Resultados catastróficos, muchos muertos
F (Frecuencia y/o tiempo de exposición al peligro)	
F_1	Rara vez a bastante frecuente
F_2	Frecuente a continuo
A (Posibilidad de evitar el peligro)	
A_1	Posible (Posible en determinadas circunstancias)
A_2	No posible (Casi imposible)
P (Probabilidad de que ocurra)	
P_1	Muy baja (Poco probable)
P_2	Baja (Probable)
P_3	Relativamente alta (Muy probable)

Determinación del Nivel SIL (II)



NIVEL SIL:
1 - 4

Fallos de causa común

β: Porcentaje de fallos debido a causa común. Debe existir más de un componente.
(1-β): Porcentaje de fallos debido a causa normal.

$$\lambda_C = \beta \cdot \lambda \qquad \lambda_N = (1-\beta) \cdot \lambda$$

$$\lambda_{SDC} = \beta \cdot \lambda_{SD} \qquad \lambda_{SDN} = (1-\beta) \cdot \lambda_{SD}$$
$$\lambda_{SUC} = \beta \cdot \lambda_{SU} \qquad \lambda_{SUN} = (1-\beta) \cdot \lambda_{SU}$$
$$\lambda_{DDC} = \beta \cdot \lambda_{DD} \qquad \lambda_{DDN} = (1-\beta) \cdot \lambda_{DD}$$
$$\lambda_{DUC} = \beta \cdot \lambda_{DU} \qquad \lambda_{DUN} = (1-\beta) \cdot \lambda_{DU}$$

Elección del tipo de Arquitectura (III)

Método 61508

- **Elementos tipo A**: Elementos sin diagnóstico y con modos de fallo muy definidos (Interruptores, válvulas de seguridad, etc.). Fallos no detectados.
- **Elementos tipo B**: Elementos con diagnóstico (Inteligentes) tipo PLCs, Transmisores, etc.

HFT	ARQUITECTURAS POSIBLES
0	1oo1
1	1oo2 ó 2oo3
2	1oo3 ó 2oo4

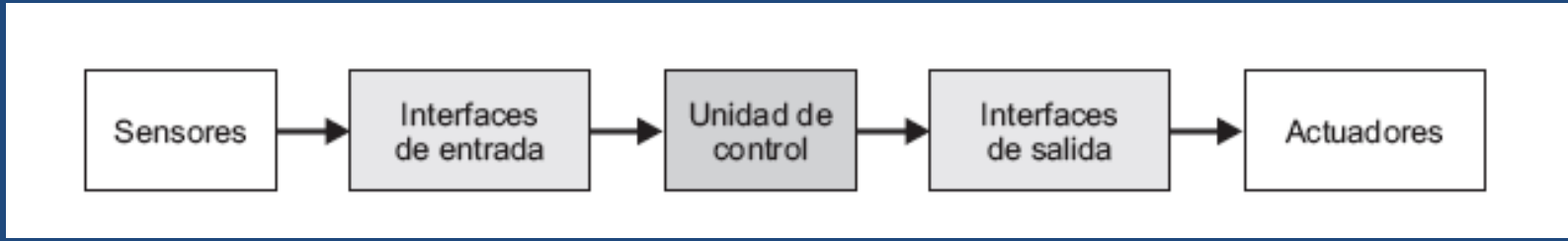
Elección del tipo de Arquitectura (IV)

SFF	HFT (Tipo A)		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60%≤ - <90%	SIL 2	SIL 3	SIL 4
90%≤ - <99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

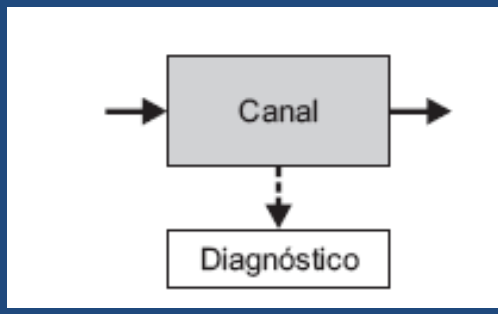
SFF	HFT (Tipo B)		
	0	1	2
<60%	NO	SIL 1	SIL 2
60%≤ - <90%	SIL 1	SIL 2	SIL 3
90%≤ - <99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

SIL	PFD_{avg} (Baja demanda)	PFH $[h^{-1}]$ (Alta demanda)
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	$\geq 10^{-9}$ a $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ a $< 10^{-3}$	$\geq 10^{-8}$ a $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	$\geq 10^{-7}$ a $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ a $< 10^{-1}$	$\geq 10^{-6}$ a $< 10^{-5}$

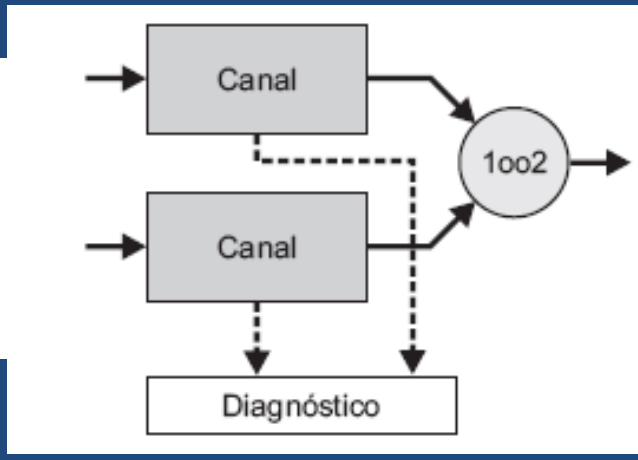
Estructuras (I)



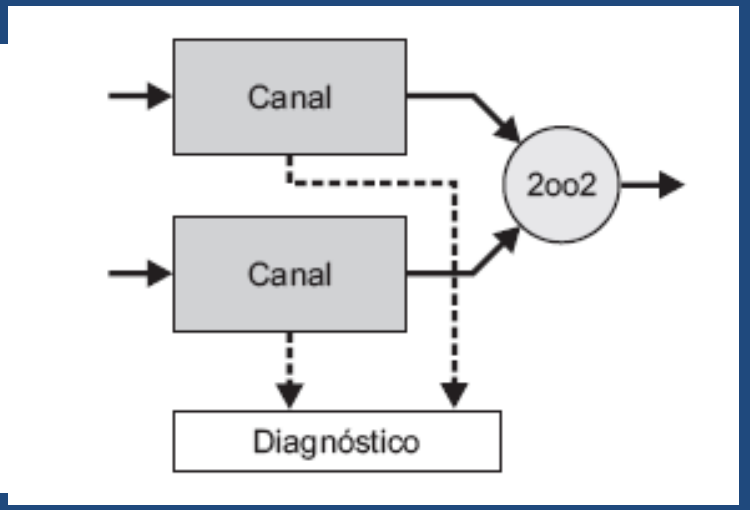
1oo1



1oo2

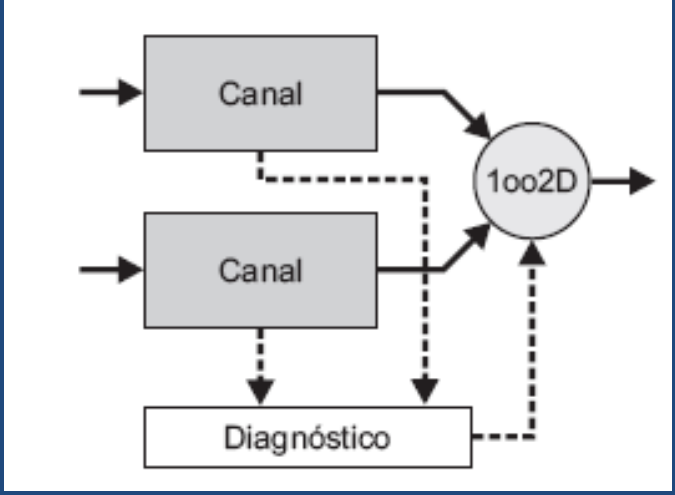


2oo2

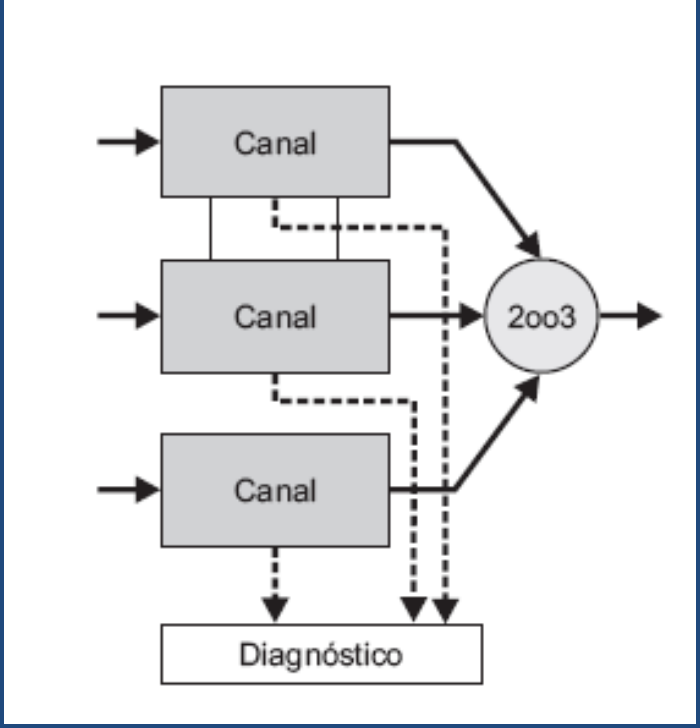


Estructuras (II)

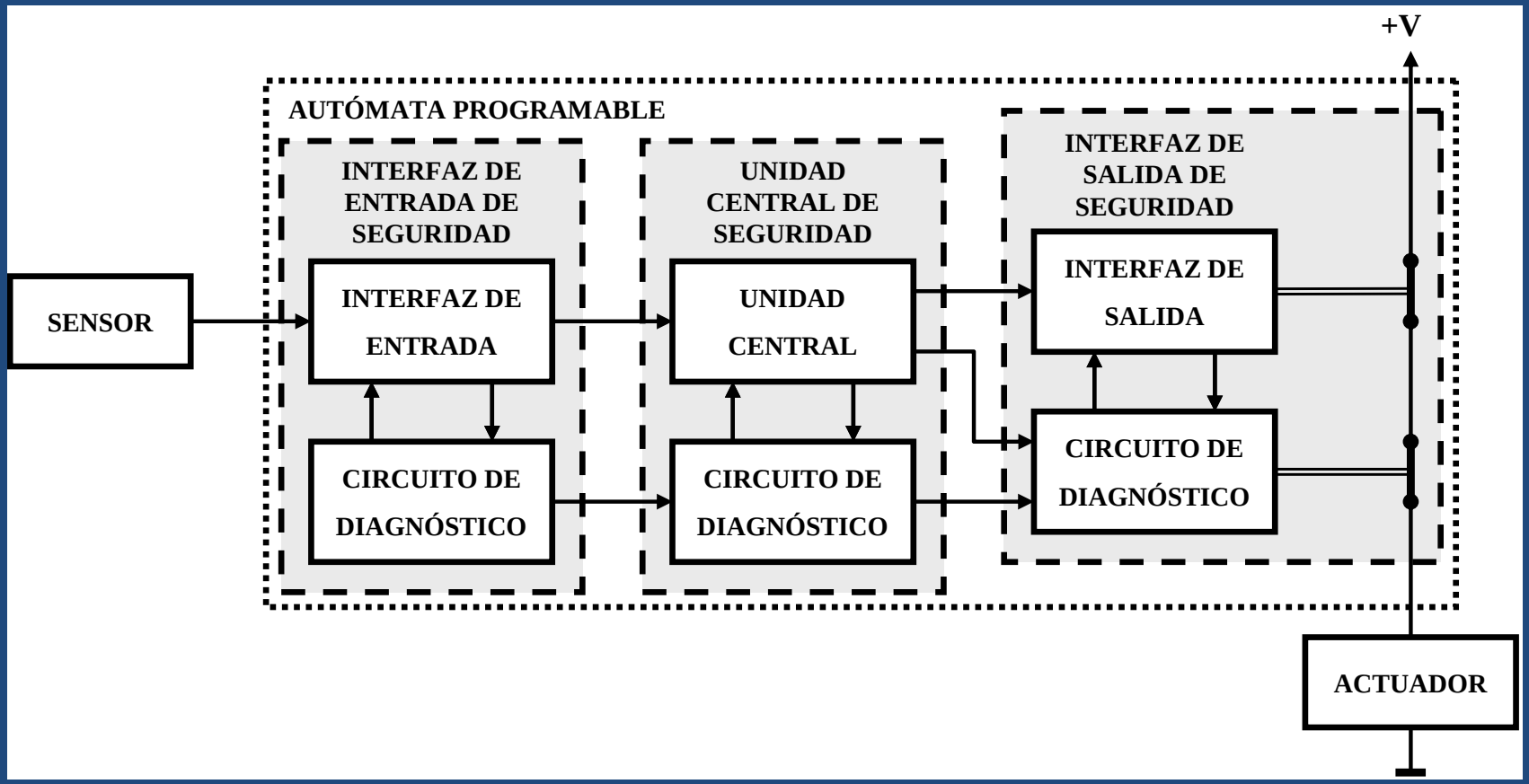
1oo2D



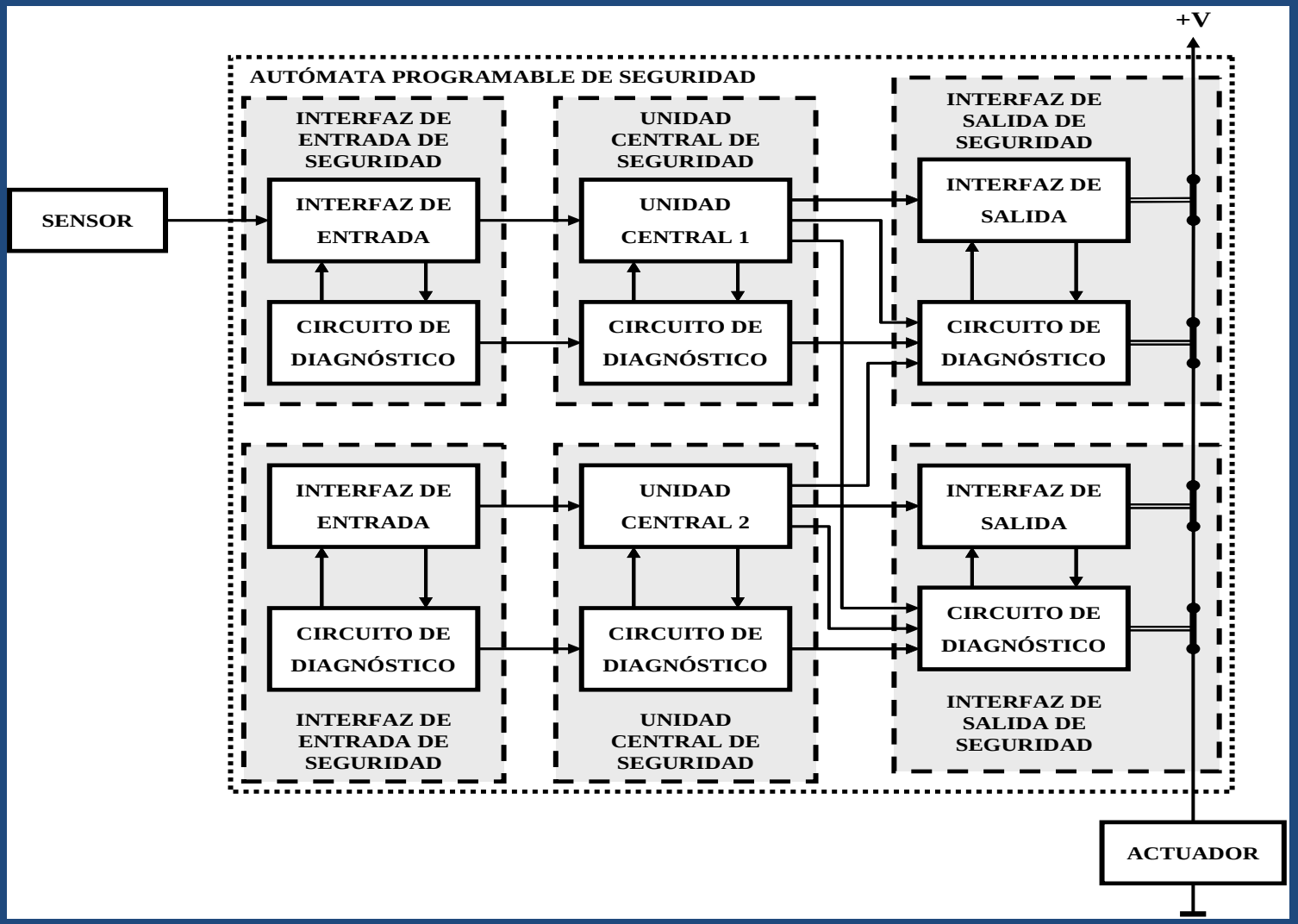
2oo3



Estructura 1oo1D



Estructura 1oo2D



SIS 1oo1 (I)

TI: Tiempo entre dos pruebas de inspección
RT: Tiempo de reparación
LT: Tiempo de vida de la SIF

$$PFD = \lambda_{DU} \cdot TI + \lambda_{DD} \cdot RT \qquad PFD_{avg} = \lambda_{DU} \cdot \frac{TI}{2} + \lambda_{DD} \cdot RT$$

$$PFD_{avg} = \frac{Frecuencia\ Tolerable\ de\ Accidentes}{Frecuencia\ de\ Accidentes\ sin\ Protecciones}$$

$$RRF = \frac{1}{PFD_{avg}} = \frac{Frecuencia\ de\ Accidentes\ sin\ Protecciones}{Frecuencia\ Tolerable\ de\ Accidentes}$$

$$Disponibilidad\ de\ la\ Seguridad = 1 - PFD_{avg}$$

SIS 1oo1 (II)

C_{PT} = Eficiencia de las pruebas periódicas

Si C_{PT} = 1 => Eficiencia de las pruebas periódicas = 99-100%

$$PFD_{avg} = C_{PT} \cdot \lambda_{DU} \cdot \frac{TI}{2} + (1 - C_{PT}) \cdot \lambda_{DU} \cdot \frac{LT}{2} + \lambda_{DD} \cdot RT$$

Como TI >> RT: $$PFD_{avg} = C_{PT} \cdot \lambda_{DU} \cdot \frac{TI}{2} + (1 - C_{PT}) \cdot \lambda_{DU} \cdot \frac{LT}{2}$$

Tasa de fallos seguros (espurios): $\lambda_S = \lambda_{SD} + \lambda_{SU} = STR$

Tiempo medio entre fallos seguros : $$MTTFs = \frac{1}{STR}$$

SIS 1oo1 (III)

$$\lambda_{TOTAL} = \lambda_{SENSOR} + \lambda_{PLC} + \lambda_{ACTUADOR}$$

$$\lambda_{S\,TOTAL} = \lambda_{S\,SENSOR} + \lambda_{S\,PLC} + \lambda_{S\,ACTUADOR}$$

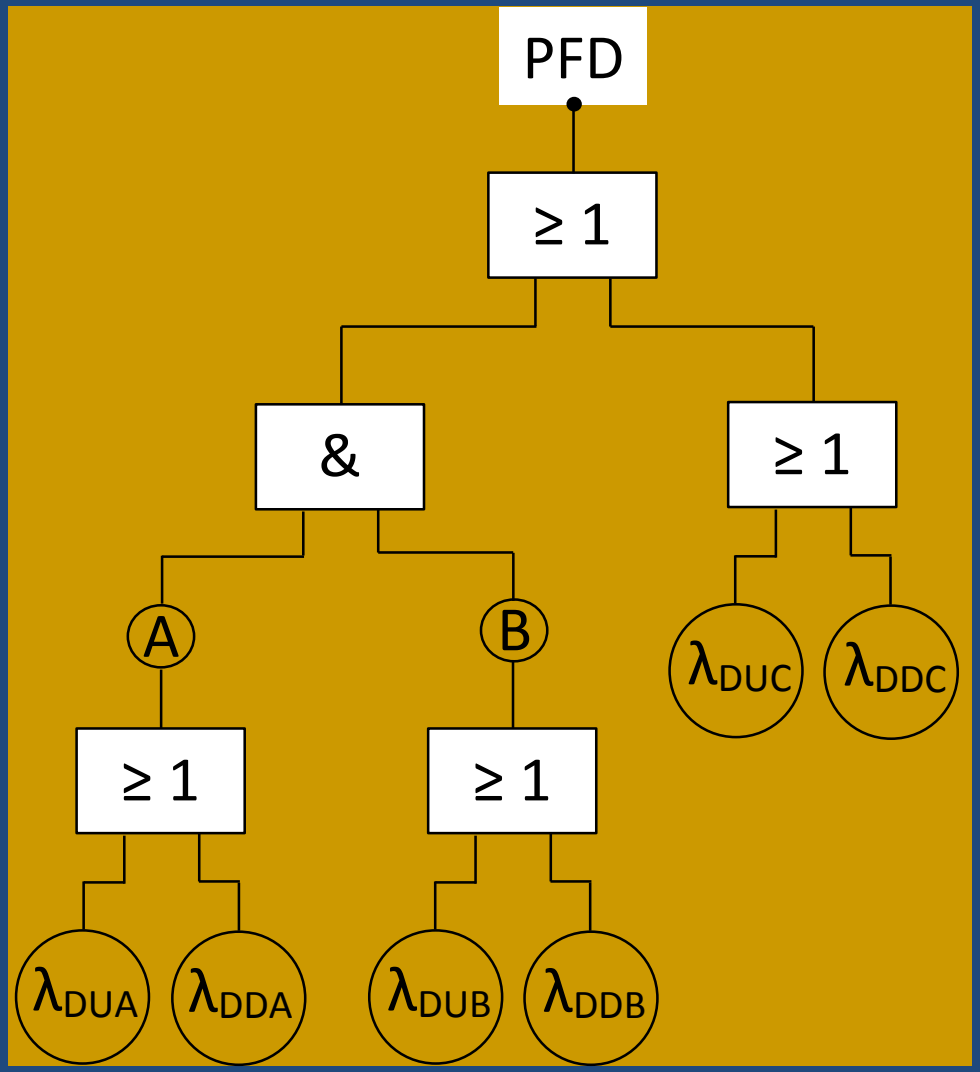
$$\lambda_{D\,TOTAL} = \lambda_{D\,SENSOR} + \lambda_{D\,PLC} + \lambda_{D\,ACTUADOR}$$

$$MTFF_S = \frac{1}{\lambda_{S\,TOTAL}} \qquad MTFF_D = \frac{1}{\lambda_{D\,TOTAL}}$$

$$MTTF_{TOT} = \frac{1}{\frac{1}{MTTF_S} + \frac{1}{MTTF_D}}$$

$$PFS = (\lambda_{SU} + \lambda_{SD})\, T_{re-arranque}$$

SIS 1oo2 (I)



SIS 1oo2 (II)

$$PFD = PFD_A \cdot PFD_B + PFD_C$$

$$PFD_A = \lambda_{DUA} \cdot TI + \lambda_{DDA} \cdot RT$$

$$PFD_B = \lambda_{DUB} \cdot TI + \lambda_{DDB} \cdot RT$$

$$PFD_C = \lambda_{DUC} \cdot TI + \lambda_{DDC} \cdot RT$$

$$\lambda_{DUC} = \beta \cdot \lambda_{DU} \qquad \lambda_{DDC} = \beta \cdot \lambda_{DD}$$

C: De causa común

$$PFD_{avg} = \frac{\lambda_{DUA}\,\lambda_{DUB}\,TI^2}{3} + \frac{\lambda_{DUA}\,TI\,\lambda_{DDB}\,RT}{2} + \frac{\lambda_{DUB}\,TI\,\lambda_{DDA}\,RT}{2} + \\ + \lambda_{DDA}\,\lambda_{DDB}\,RT^2 + \frac{\lambda_{DUC}\,TI}{2} + \lambda_{DDC}\,RT$$

Si A ≡ B => $$PFD_{avg} = \frac{\lambda_{DU}^2\,TI^2}{3} + \lambda_{DU}\,TI\,\lambda_{DD}\,RT + \lambda_{DD}^2\,RT^2 + \frac{\lambda_{DUC}\,TI}{2} + \lambda_{DDC}\,RT$$

Si RT << TI => $$PFD_{avg} = \frac{\lambda_{DU}^2\,TI^2}{3}$$

$$STR = \lambda_{SUA} + \lambda_{SDA} + \lambda_{SUB} + \lambda_{SDB} + \lambda_{SUC} + \lambda_{SDC}$$

SIS 1oo2 (III)

1oo2

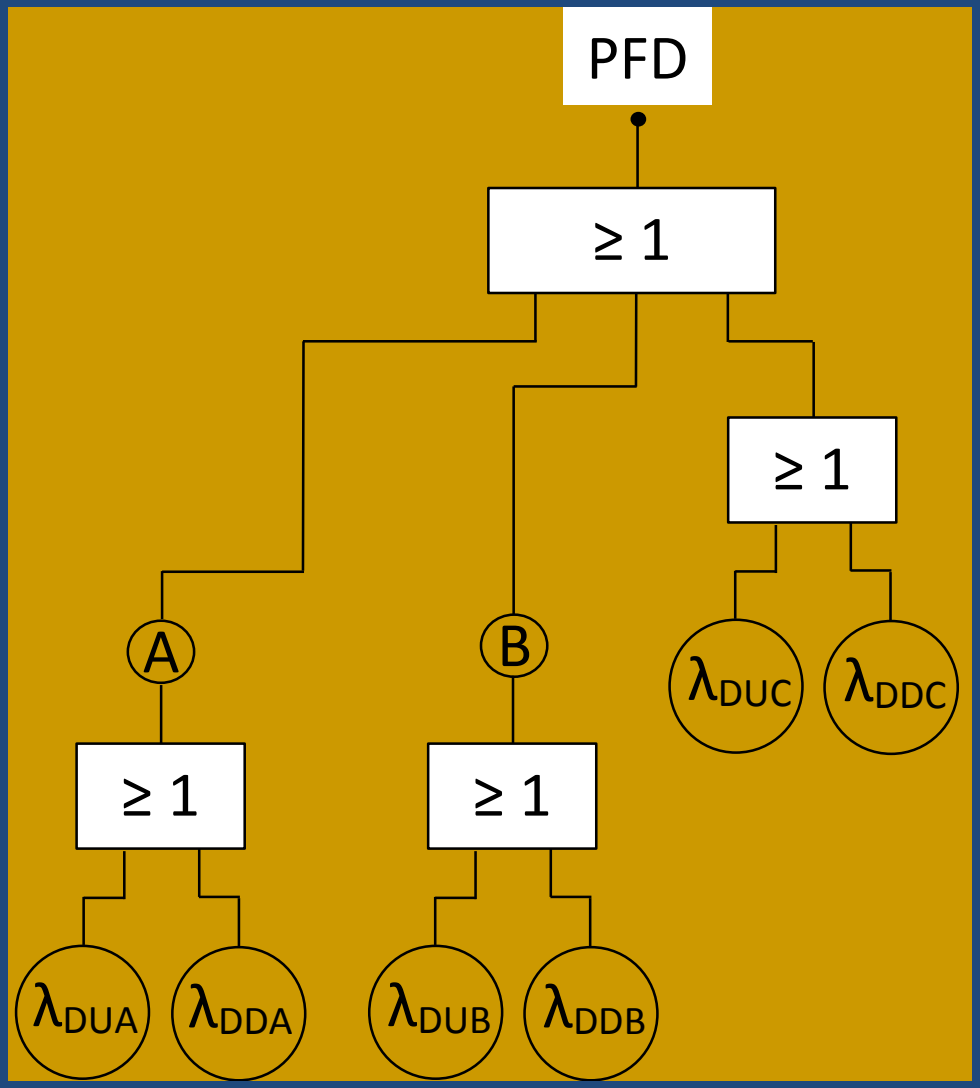
Si existe β (Componentes iguales)

$$PFD_{avg} = \frac{[(1-\beta)(\lambda_{DU}\,TI)]^2}{3} + \frac{\beta\lambda_{DU}\,TI}{2}$$

Para componentes iguales y sin fallos de causa común:

$$STR = 2 \cdot (\lambda_{SU} + \lambda_{SD}) = 2\,\lambda_S$$

SIS 2oo2 (I)



SIS 2oo2 (II)

$$PFD = PFD_A + PFD_B + PFD_C$$

$$PFD_A = \lambda_{DUA} \cdot TI + \lambda_{DDA} \cdot RT$$
$$PFD_B = \lambda_{DUB} \cdot TI + \lambda_{DDB} \cdot RT$$
$$PFD_C = \lambda_{DUC} \cdot TI + \lambda_{DDC} \cdot RT$$

$$\lambda_{DUC} = \beta \cdot \lambda_{DU}$$
$$\lambda_{DDC} = \beta \cdot \lambda_{DD}$$

$$PFD_{avg} = \frac{\lambda_{DUA}\, TI}{2} + \lambda_{DDA} \cdot RT + \frac{\lambda_{DUB}\, TI}{2} + \lambda_{DDB} \cdot RT + \frac{\lambda_{DUC}\, TI}{2} + \lambda_{DDC} \cdot RT$$

Si A ≡ B y RT <<< TI => $PFD_{avg} = \lambda_{DU} \cdot TI$

SIS 2oo2 (III)

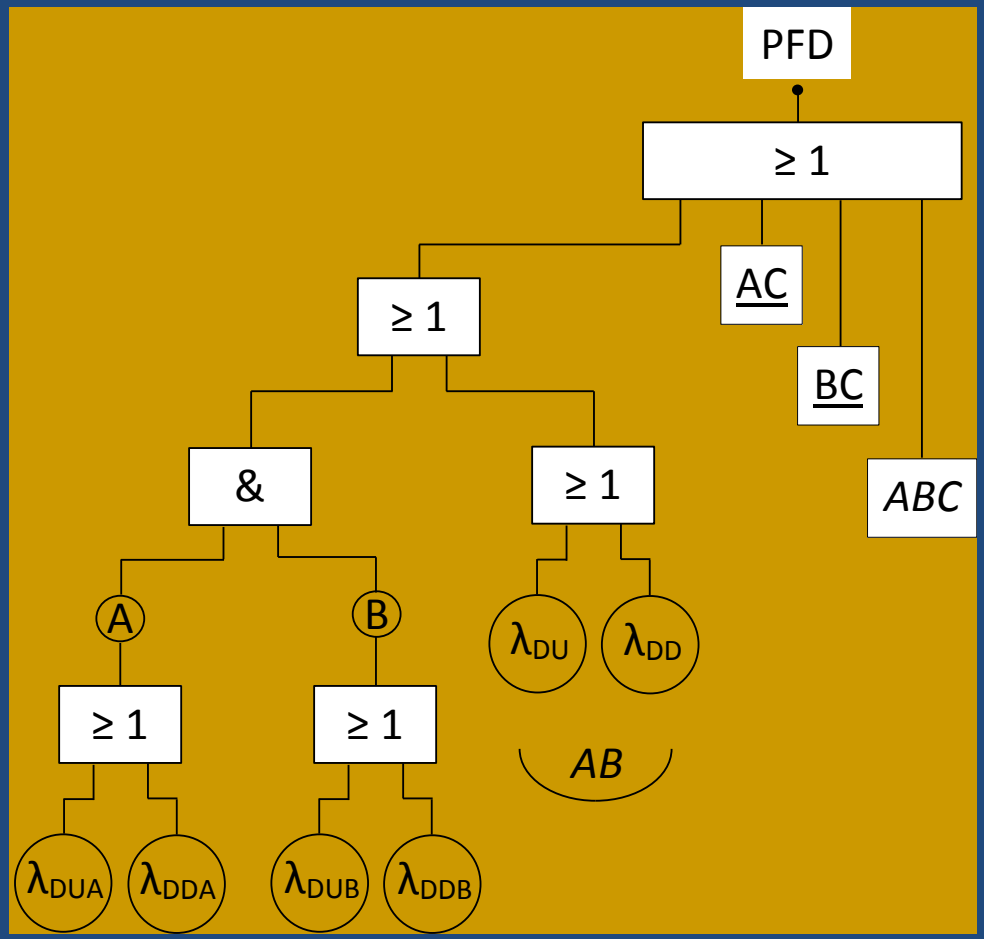
Si existe β (Componentes iguales):

$$PFD_{avg} = (1-\beta)(\lambda_{DU}\,TI) + \frac{\beta\lambda_{DU}\,TI}{2}$$

Para componentes iguales y sin fallos de causa común:

$$STR = \frac{(2\lambda_S)^2}{3\lambda_S + \frac{2}{TI}}$$

SIS 2oo3 (I)



$$PFD = PFD_A \cdot PFD_B + PFD_{AB} + + PFD_A \cdot PFD_C + PFD_{AC} + PFD_B \cdot PFD_C + PFD_{BC} + PFD_{ABC}$$

Si A ≡ B ≡ C =>

$$PFD_{avg} = (\lambda_{DU} \cdot TI)^2$$

SIS 2oo3 (II)

$$PFD_{avg} = \frac{[(\lambda_{DUA}\,\lambda_{DUB}) + (\lambda_{DUA}\,\lambda_{DUC}) + (\lambda_{DUB}\,\lambda_{DUC})] \cdot TI^2}{3}$$

Si existe β (Componentes iguales):

$$PFD_{avg} = [(1-\beta)(\lambda_{DU}\,TI)]^2 + \frac{\beta\lambda_{DU}\,TI}{2}$$

Si los tres elementos son iguales y sin fallos de causa común:

$$PFD_{avg} = (\lambda_{DU} \cdot TI)^2$$

$$STR = \frac{(6\lambda_S)^2}{5\lambda_S + \frac{2}{TI}}$$

Comparativa de arquitecturas

SIS	PFD_{avg} - Distintos	PFD_{avg}
1oo1	$\frac{\lambda_{DU} \cdot TI}{2}$	$\frac{\lambda_{DU} \cdot TI}{2}$
1oo2	$\frac{\lambda_{DU_1} \cdot \lambda_{DU_2} \cdot TI^2}{3}$	$\frac{\lambda_{DU}^2 \cdot TI^2}{3}$
1oo3	$\frac{\lambda_{DU_1} \cdot \lambda_{DU_2} \cdot \lambda_{DU_3} \cdot TI^3}{4}$	$\frac{\lambda_{DU}^3 \cdot TI^3}{4}$
2oo2	$(\lambda_{DU_1} + \lambda_{DU_2}) \cdot \frac{TI}{2}$	$\lambda_{DU} \cdot TI$
2oo3	$(\lambda_{DU_1} \cdot \lambda_{DU_2} + \lambda_{DU_1} \cdot \lambda_{DU_3} + \lambda_{DU_2} \cdot \lambda_{DU_3}) \cdot \frac{TI^2}{3}$	$\lambda_{DU}^2 \cdot TI^2$
2oo4	$(\lambda_{DU_1} \cdot \lambda_{DU_2} \cdot \lambda_{DU_3}) + (\lambda_{DU_1} \cdot \lambda_{DU_2} \cdot \lambda_{DU_4}) + (\lambda_{DU_1} \cdot \lambda_{DU_3} \cdot \lambda_{DU_4}) + (\lambda_{DU_2} \cdot \lambda_{DU_3} \cdot \lambda_{DU_4}) \cdot \frac{TI^3}{4}$	$\lambda_{DU}^3 \cdot TI^3$

Ejemplos

The FMEDA with analysis of the safety critical and dangerous faults provides under the assumption of an annual functional test cycle following parameters:

SIL (Safety integrity level)	:	2	
HFT (Hardware fault-tolerance)	:	0[1] (single use)	
		FMR23x	FMR24x
SFF (Safe failure fraction)	:	>74%	> 75%
PFDavg (fail to danger) [2]	:	$0{,}42 \times 10^{-2}$	$0{,}39 \times 10^{-2}$
MTBFges (mean time between total faults)	:	30,5 Jahre	31,3 Jahre
λ_{du} (failure rate dangerous undetected faults)	:	957 FIT	886 FIT
λ_{dd} (failure rate dangerous detected faults)	:	973 FIT	957 FIT
λ_{su} (failure rate safe undetected faults)	:	1700 FIT	1690 FIT
λ_{sd} (failure rate safe detected faults)	:	105 FIT	105 FIT

[1] according to clause 11.4 of IEC 61511-1(FDIS)
[2] The PFDavg values are also within the range for SIL2 according to ISA S84.01.

The assessment of the proven-in-use demonstration covers the device and its software including the modification process.

Autómatas Programables de Seguridad

Normativas Ferroviarias (I)

- **UNE-EN 50126 (2005)**: Aplicaciones Ferroviarias. Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS).
- **UNE-EN 50128 (2012)**: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Software para sistemas de control y protección del ferrocarril.
- **UNE-EN 50129 (2005)**: Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos relacionados con la seguridad para la señalización.

Normativas Ferroviarias (II)

- **Niveles de Seguridad (UNE-EN 50129):**

SIL (Safety Integrity Level) Nivel de seguridad integral o Nivel integral de seguridad.

SIL	Índice de peligros tolerable por hora y por función (THR)
4	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-6} \leq THR < 10^{-5}$

Normativas Automoción (I)

- **ISO 26262 (2011)**: Road vehicles. Functional safety. Part 1: Vocabulary. Part 2: Management of functional safety. Part 3: Concept phase. Part 4: Product development at the system level. Part 5: Product development at the hardware level. Part 6: Product development at the software level. Part 7: Production and operation. Part 8: Supporting processes. Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses.

Normativas Automoción (II)

- **Niveles de Seguridad (ISO 26262):**
  ASIL (Automotive Safety Integrity Level) Nivel de seguridad integral o Nivel integral de seguridad en aplicaciones de automoción.

ASIL	Valores objetivo de tasas de fallo del hardware
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

Automoción ISO 26262 (I)

Severity

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure

E0	E1	E2	E3	E4
Incredible	Very low probability	Low probability	Medium Probability	High Probability

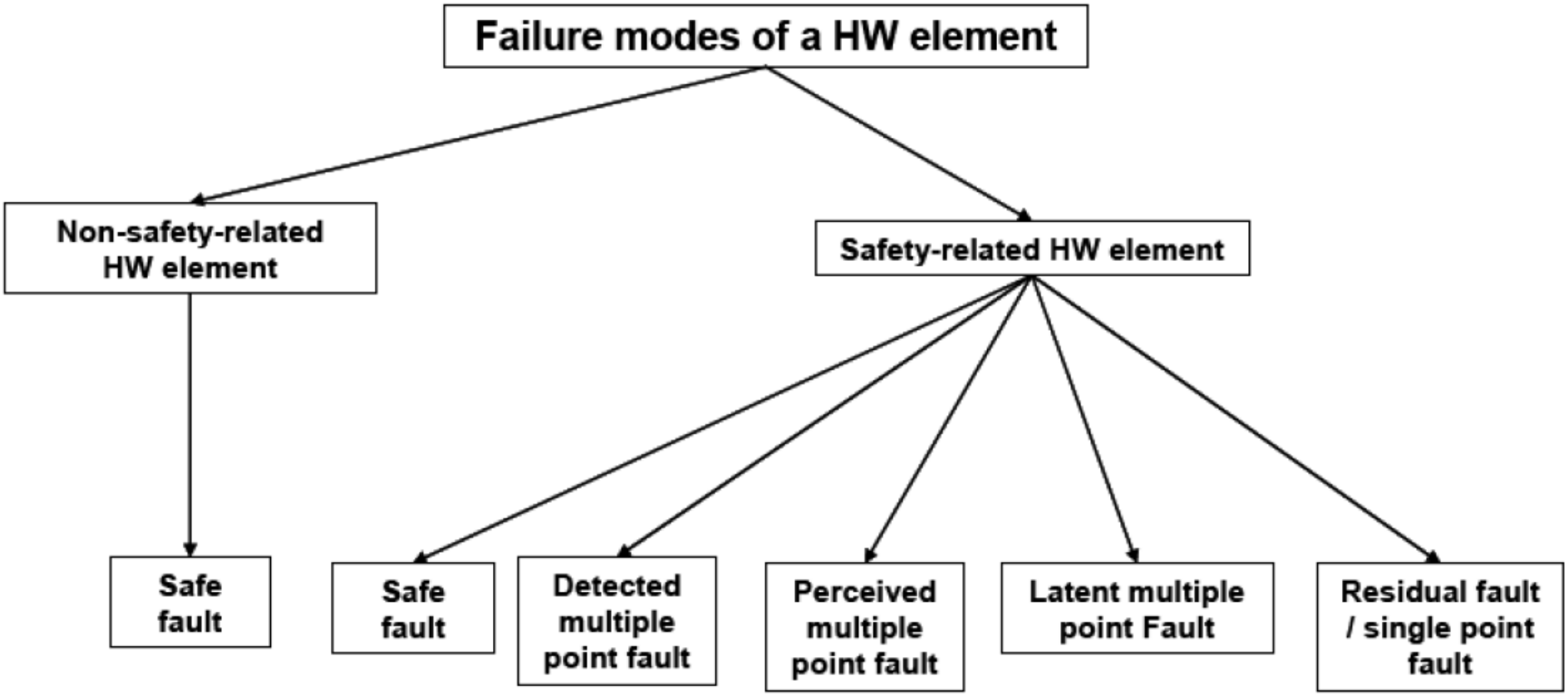
Controllability

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Automoción ISO 26262 (II)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Tipos de Fallos



Definiciones (I)

- **B:** Probabilidad de que el modo fallo cause el efecto final considerado.
- **SPF** (Single Point Fault): Fallo simple que no está cubierto por un mecanismo de seguridad y que lleva al fallo de seguridad del sistema.
- **SM** (Safety Mechanism): Mecanismo de seguridad que detecta el fallo y actúa para llevar el sistema al estado seguro.
- **RF** (Residual Fault): Fallo residual, que representa la parte del fallo que no está cubierto por un mecanismo de seguridad da lugar a un MPF y que lleva al fallo del sistema.
- **MPF** (Múltiple Point Fault): Fallo individual que en combinación con otros fallos independientes que lleva a la pérdida de la función de seguridad. Puede ser detectado, percibido o latente.
- **S** (Safe): Fallo seguro

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_{S}$$

Definiciones (II)

- **Detected Fault**: Fallo detectado por el correspondiente mecanismo de seguridad.
- **Perceived Fault**: Fallo percibido por el conductor.
- **Latent Fault**: Es un fallo múltiple no detectado por un mecanismo de seguridad ni percibido por el conductor.
- **Safety Mechanism**: Solución técnica que detecta el fallo y lleva el sistema al estado seguro.
- **D**: Cobertura del diagnóstico
- λ_{SD} (λ Safe Detectable): $\lambda_{SD} = \lambda \cdot D$
- λ_{SU} (λ Safe Undetectable): $\lambda_{SU} = \lambda \cdot (1 - D)$
- λ_{DMPF} (λ Detectable Multiple Point Fault): $\lambda_{DMPF} = \lambda \cdot D$
- λ_{LMPF} (λ Latent Multiple Point Fault): $\lambda_{LMPF} = \lambda \cdot (1 - D)$

$$\lambda_{MPF} = \lambda_{MPF,DP} + \lambda_{MPF,L}$$

Métricas

$$\mathrm{DC}_{\text{Latent Failures}} = \frac{\lambda_{\mathrm{DMPF}}}{\lambda_{\mathrm{DMPF}} + \lambda_{\mathrm{LMPF}}}$$

$$\mathrm{SPFM} = 1 - \frac{\sum(\lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}})}{\sum \lambda}$$

Esta métrica mide el % de los SPF y RF respecto del total. Cuanto más alto sea el SPFM menor λ de los SPF y RF

$$\mathrm{LFM} = 1 - \frac{\sum \lambda_{\mathrm{LMPF}}}{\sum(\lambda - \lambda_{\mathrm{SPF}} - \lambda_{\mathrm{RF}})}$$

Esta métrica mide el % de los LMPF respecto del total. Cuanto más alto sea el LFM menor λ de los LMPF

Procedimiento

1) Estimación λ_{SPF} y λ_{LMF}
2) Estimación de la cobertura del diagnóstico de los mecanismos de seguridad
3) Calcular las métricas
4) Comprobar si el sistema cumple
5) Si el sistema no cumple se deber rediseñar y cambiar componentes y mecanismos de seguridad

	ASIL B	ASIL C	ASIL D
SPFM	> 90%	> 97%	> 99%
LFM	> 60%	> 80%	> 90%

MUCHAS GRACIAS POR SU ATENCIÓN

Jorge Marcos Acevedo
Dpto. de Tecnología Electrónica
Universidad de Vigo

e-mail: acevedo@uvigo.es