Electricidade e Electrónica
Xornadas 2016 - Culleredo

Fiabilidad, Seguridad y Automatización: Sistemas Electrónicos de Control Seguros ante Averías (Fail Safe Systems)

Jorge Marcos Acevedo - Dr. Ingeniero Industrial

Departamento de Tecnología Electrónica

Universidad de Vigo

Universidade Vigo

DTE

Contenido

- **Tecnologías RAMS**
  - Fiabilidad
  - Mantenibilidad
  - Dsiponibilidad
  - Seguridad
- **Aplicaciones educativas**
  - Sensores de bajo coste
  - Herramientas multimedia

Tecnologías RAMS

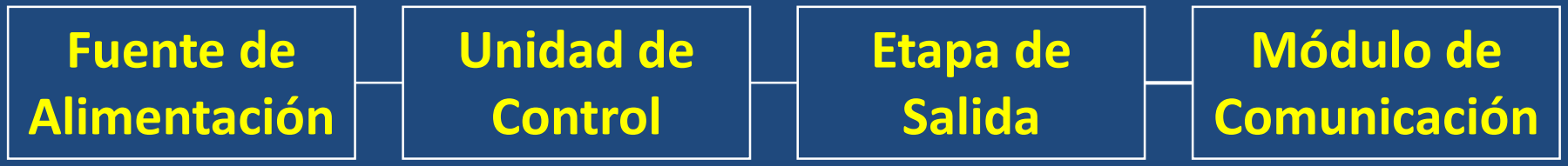
Confiabilidad (Dependability)

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

Fiabilidad

(Reliability)

Fiabilidad: Probabilidad de funcionamiento correcto durante un tiempo "t" y en condiciones de trabajo especificadas



$R_{FA} = 0,8$ $R_{UC} = 0,9$ $R_{ES} = 0,7$ $R_{MC} = 0,6$

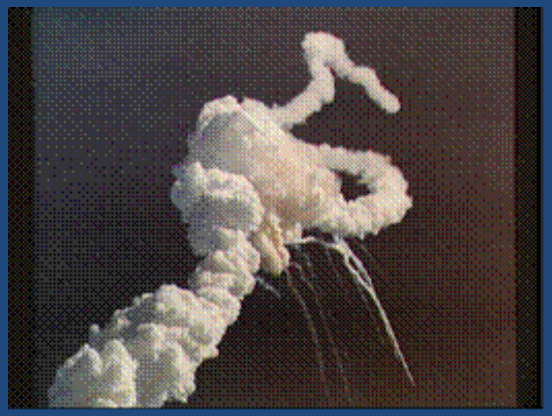
$$\mathbf{R_S = R_{FA} \cdot R_{UC} \cdot R_{ES} \cdot R_{MC} = 0,3\ (30\%)}$$

- La fiabilidad del sistema es el producto de las fiabilidades de los componentes "Ley del producto"
- La cadena se rompe por el eslabón más débil

Evolución histórica de la fiabilidad

Wernher von Braun, Robert Lusser y Eric Pieruschka lograron una fiabilidad de 0,75 con las V2

Situación actual

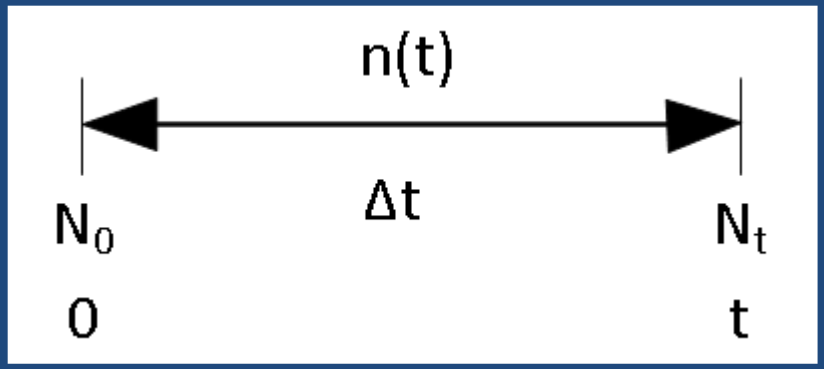


Fallos

- Componentes/sistemas electrónicos:
  - Hardware: Físicos/Diseño
  - Software: Diseño
- Componentes/sistemas eléctricos y mecánicos

Fiabilidad R(t)

- Probabilidad de funcionamiento entre 0 y t



$$R(t) = \frac{N_t}{N_0} = \frac{N_0 - n(t)}{N_0}$$

Infiabilidad F(t)

- Probabilidad de fallo entre 0 y t

$$F(t) = \frac{n(t)}{N_0} = 1 - R(t)$$

Parámetros de la Fiabilidad

- Tasa instantánea 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]

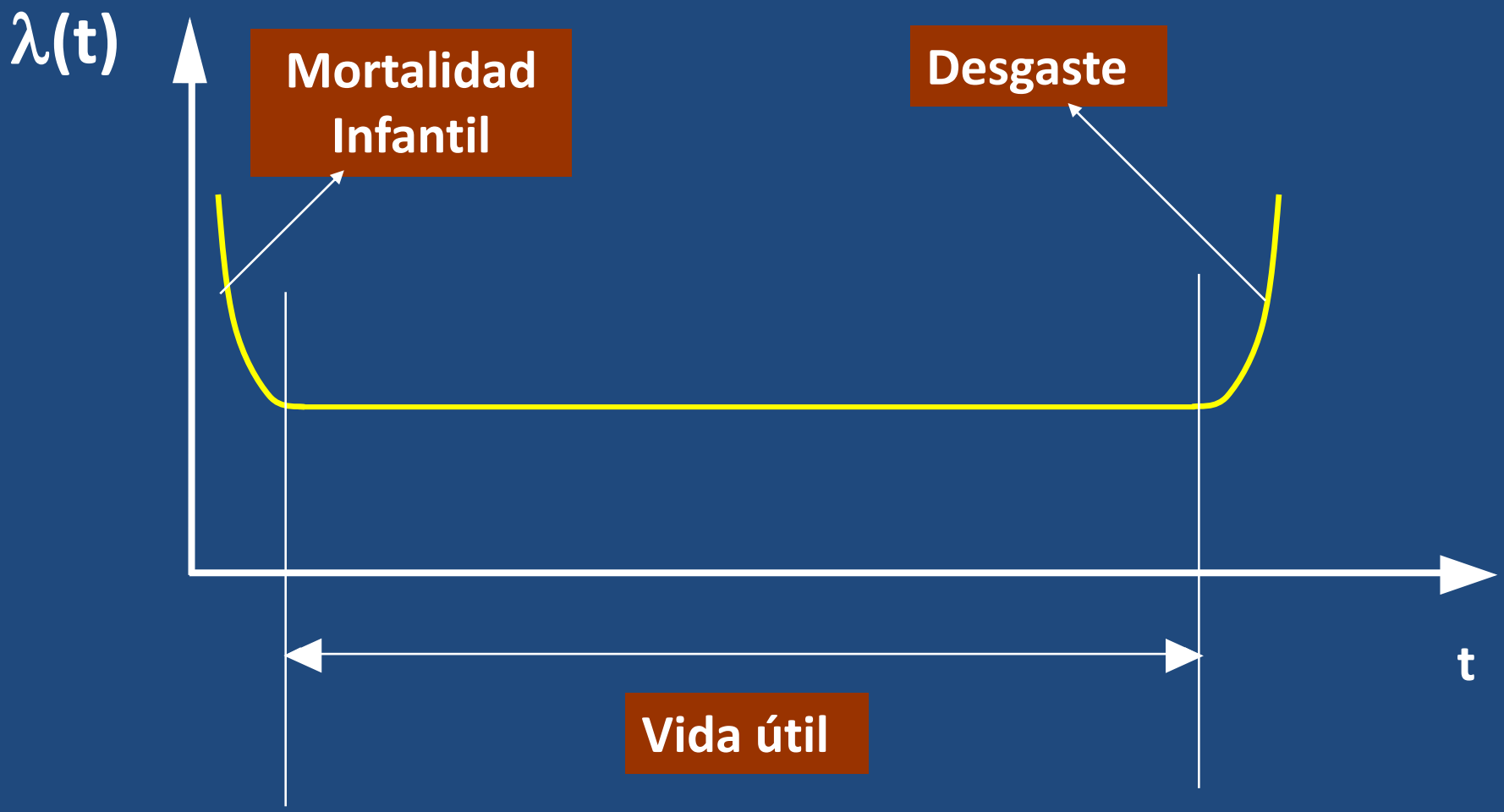
Tasa de Fallos λ(t) [1]

λ(t): Velocidad a la que fallan los componentes

λ(t): Probabilidad de que un componente falle entre “t” y “t+dt” condicionado a que viva en “t”

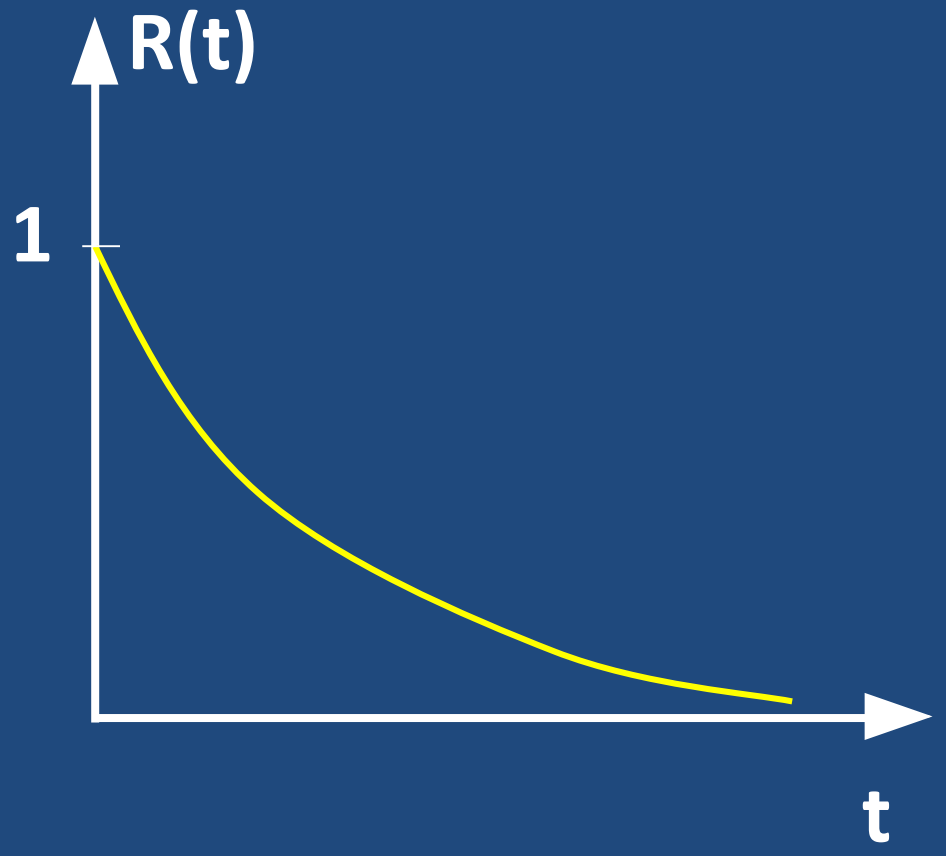
$$R(t) = e^{-\lambda(t)\cdot t}$$

Tasa de Fallos λ(t) [2]



Cálculo de Fiabilidad

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



Tasa de Fallos λ(t) [2]

$$\lambda(t) = \left[\frac{Fallos}{Componente \cdot hora}\right] = \left[\frac{F}{C \cdot h}\right] = [h^{-1}]$$

$$\lambda(t) = \left[\frac{Fallos}{Componente \cdot 10^6\ horas}\right]$$

$$\lambda(t) = \left[\frac{Fallos}{Componente \cdot 10^9\ horas}\right] = [FITs]$$

$$\lambda = a \cdot 10^{-9} \left[\frac{F}{C \cdot h}\right] = a\ [FITs]$$

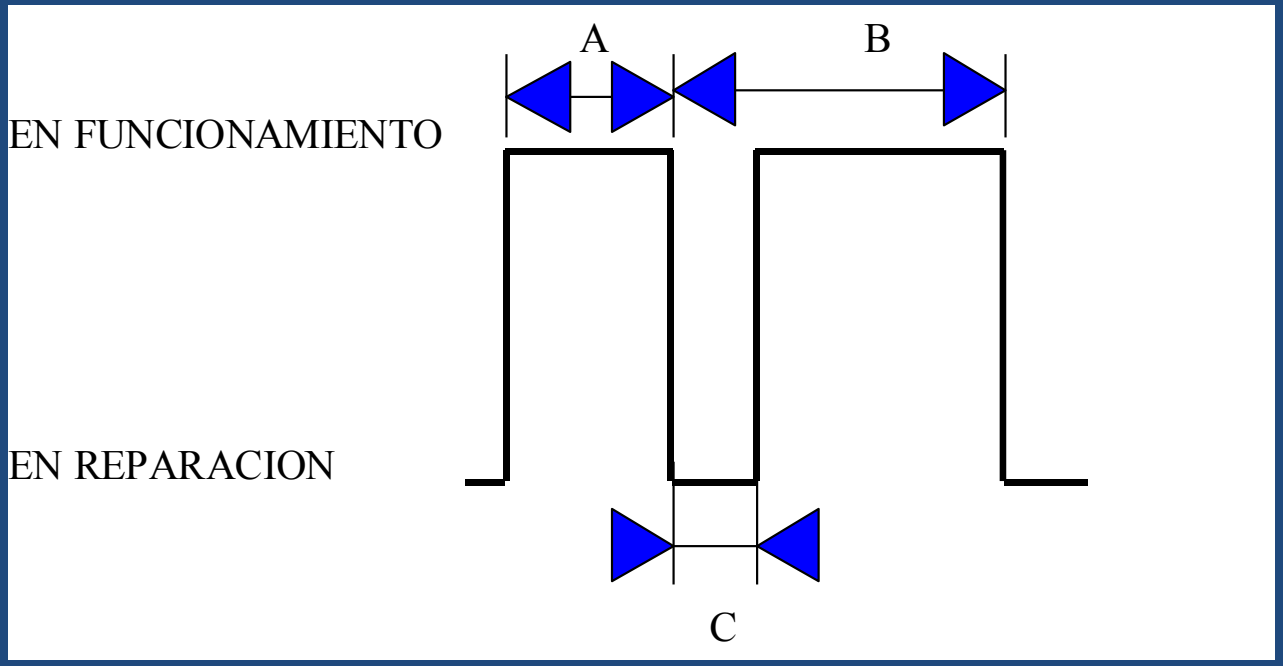
Tasa de Fallos λ(t) [3]

$$\lambda(t) = 5{,}1 \cdot 10^{-4} \left[\frac{F}{C \cdot h}\right] = 510 \left[\frac{F}{C \cdot 10^6 h}\right]$$

$$\lambda(t) = 5{,}1 \cdot 10^{-4} \left[\frac{F}{C \cdot h}\right] = 51 \cdot 10^4 [FITs]$$

Para 10^4 Componentes => 5,1 Fallos por hora

MTBF, MTTF y MTTR (I)



- MTBF: Media tiempos B (Reparables)
- MTTF: Media tiempos A (No reparables)
- MTTR: Media tiempos C

MTBF, MTTF y MTTR (II)

$$MTBF = MTTF + MTTR$$

- **Sistemas reparables**

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

- **Sistemas no reparables**

$$MTBF = MTTF$$

Vida Media "θ" [1]

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

- Sistemas Reparables:

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

- Sistemas no Reparables:

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

Vida Media "θ" [2]

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

- Para componentes electrónicos en el período de vida útil λ = Cte.
- Para $t = \theta \Rightarrow R(t) = e^{-1} = 0{,}37$
- La vida media "θ" es el tiempo al cabo del cual sobreviven el 37% de los componentes y ha fallado el 63% de la población inicial.

Cálculo de Tasas de Fallo de Componentes Electrónicos

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

Cálculo de tasas de fallo según MIL-HDBK-217F

$$\lambda_P = \lambda_b * [\pi_1 * \pi_2 * ..... * \pi_n]$$

λ_P: Tasa de fallos del componente

λ_b: Tasa de fallos base

π : Factores de corrección

Cálculo de tasas de fallo (I)

Resistencia fija de película metálica

$$\lambda_P = \lambda_b * \pi_R * \pi_Q * \pi_E \left[\frac{Fallos}{10^6 Horas} \right]$$

$$\lambda_b = 3{,}25 * 10^{-4} * e^{\left[\frac{T+273}{343} \right]^3} * e^{\left[\frac{S(T+273)}{273} \right]}$$

π_R (Factor de resistencia): Varía entre 1 y 5 según el tipo de resistencia

π_Q (Factor de calidad): Varía entre 0,003 y 15 según la calidad del componente

π_E (Factor ambiental): Varía entre 1 y 490 según el ambiente de trabajo del componente (Terrestre, naval, aerospacial, etc.)

Cálculo de tasas de fallo (II)

Condensador fijo electrolítico de aluminio
$$\lambda_P = \lambda_b * \pi_{CV} * \pi_Q * \pi_E \left[\frac{Fallos}{10^6\ Horas}\right]$$
$$\lambda_b = 0{,}00254\left[\left(\frac{S}{0{,}5}\right)^3 + 1\right] * e^{5{,}09\left[\frac{T+273}{358}\right]^5}$$
π_{CV} (Factor de capacidad): $0{,}34C^{0{,}18}$. C es la capacidad del condensador
π_Q (Factor de calidad): Varía entre 0,003 y 10 según la calidad del componente
π_E (Factor ambiental): Varía entre 1 y 690 según el ambiente de trabajo del componente (Terrestre, naval, aerospacial, etc.)

Cálculo de tasas de fallo (III)

Transistor bipolar de baja frecuencia

$$\lambda_P = \lambda_b * \pi_T * \pi_A * \pi_R * \pi_S * \pi_Q * \pi_E$$

f<200 MHz => λ_b = 0,00074, f>200 MHz => λ_b = 0,18

π_T (Factor de temperatura):
T_J = Temperatura de la unión

$$\pi_T = e^{-2114\left[\frac{1}{T_J+273}-\frac{1}{298}\right]}$$

π_A (Factor de aplicación): Amplificación: π_A= 1,5
Conmutación: π_A= 0,7; f>200 MHz => π_A = 1

π_R (Factor de potencia):

$$\pi_R = (Potencia)^{0,37}$$

π_S (Factor de tensión):

$$\pi_S = 0,045 * e^{3,1*\frac{V_{CE}}{V_{CEO}}}$$

π_Q (Factor de calidad): Varía entre 0,5 y 5, según la calidad del componente

π_E (Factor ambiental): Varía entre 1 y 320 según el ambiente de trabajo del componente (Terrestre, naval, aeroespacial, etc.)

Cálculo de tasas de fallo (IV)

Circuito integrado (Microprocesador)
$\lambda_P = (C_1 * \pi_T + C_2 * \pi_E) * \pi_Q * \pi_L$
C_1: Factor que depende del número de bits y del tipo tecnología, y varía entre 0,06 y 0,56
π_T (Factor de temperatura): Depende de la temperatura y del tipo de tecnología, y varía entre $3,2*10^{-8}$ y 480
C_2: Factor que depende del tipo de encapsulado y del número de terminales, y varía entre 0,00022 y 0,12
π_E (Factor ambiental): Varía entre 0,5 y 220 según el ambiente de trabajo del componente (Terrestre, naval, aerospacial, etc.)
π_Q (Factor de calidad): Varía entre 0,25 y 2, según la calidad del componente
π_L (Factor de aprendizaje) Y: Nº de años que el componente lleva en producción $\pi_L = 0,01 * e^{(5,35-0,35*Y)}$

Cálculo de tasas de fallo según IEC 62380

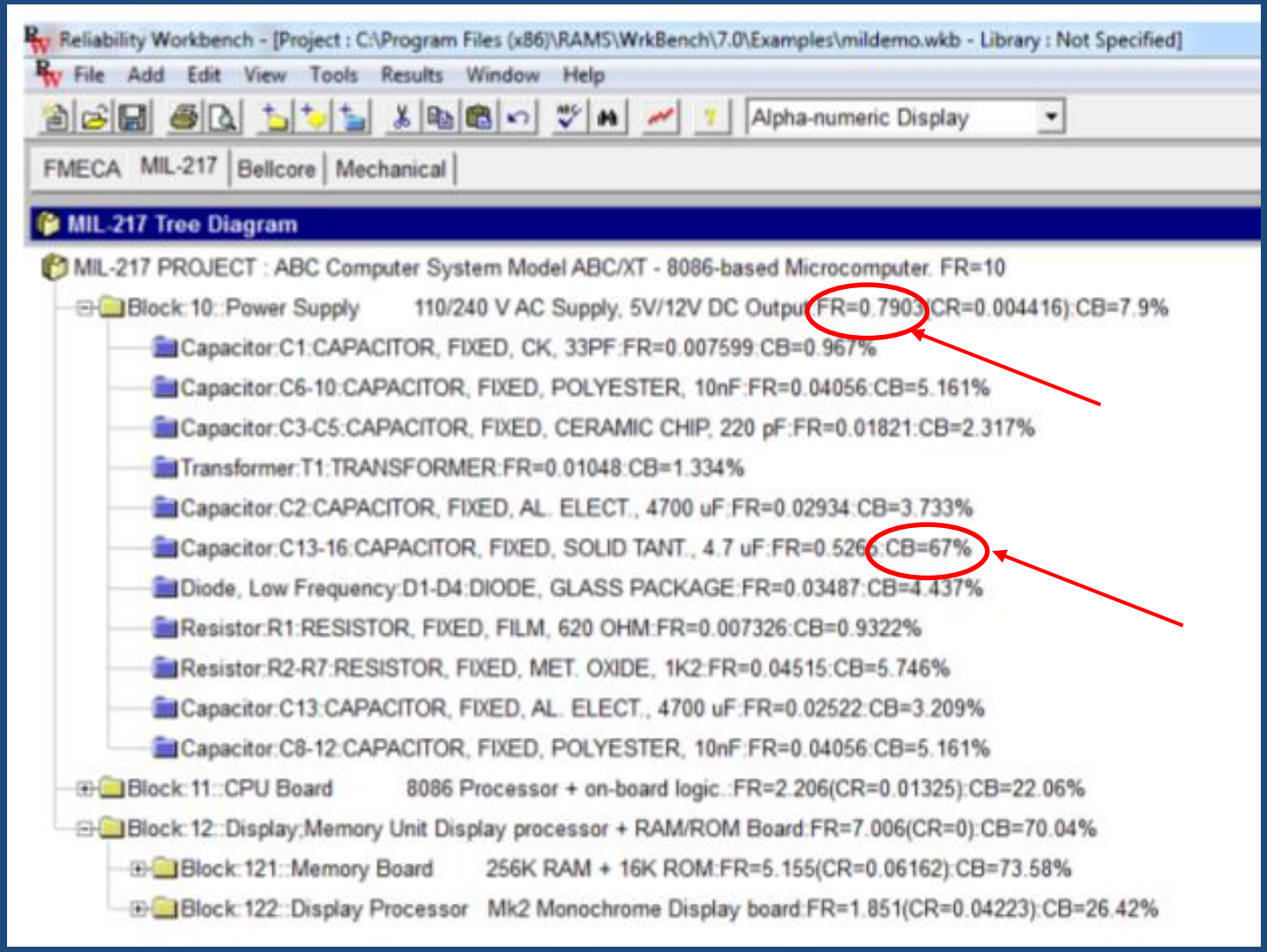
Transistores

$$\lambda = \left\{ \underbrace{\{\pi_S \times \lambda_0\} \times \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\}}_{\lambda_{die}} + \left\{ \underbrace{2.75 \times 10^{-3} \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_B}_{\lambda_{package}} \right\} + \left\{ \underbrace{\pi_I \times \lambda_{EOS}}_{\lambda_{overstress}} \right\} \right\} \times 10^{-9} / h$$

Mathematical formulas for π_t and π_S

π_t	Bipolar GaAs	$\pi_t = e^{4640(\frac{1}{373} - \frac{1}{t_j + 273})}$ (activation energy: 0.4 ev)
	MOS IGBT	$\pi_t = e^{3480(\frac{1}{373} - \frac{1}{t_j + 273})}$ (activation energy: 0.3 ev)
π_S	FET,MOS IGBT	$\pi_{S1} = 0.22e^{1.7S_1}$ $\Pi_{S2} = 0.22e^{3S_2}$
	Bipolar	$\Pi_S = 0.22e^{1.7S}$

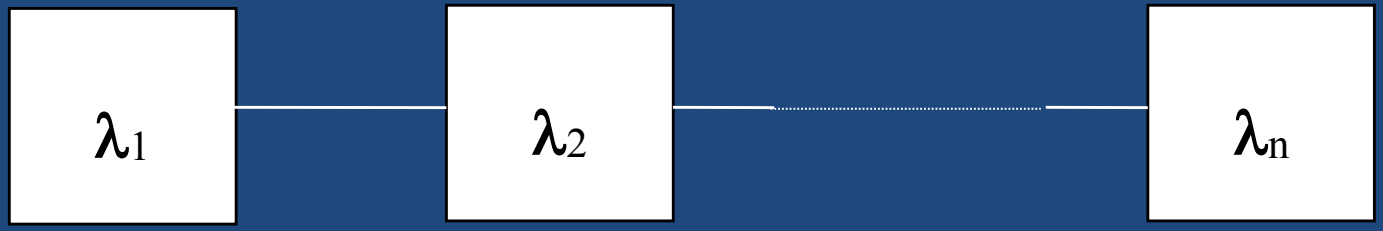
Ejemplo de Cálculo de Tasas de Fallo



Fiabilidad de sistemas

- Sistemas serie
- Sistemas paralelo
  - Redundancia activa
  - Redundancia pasiva

Fiabilidad de Sistemas Serie (I)



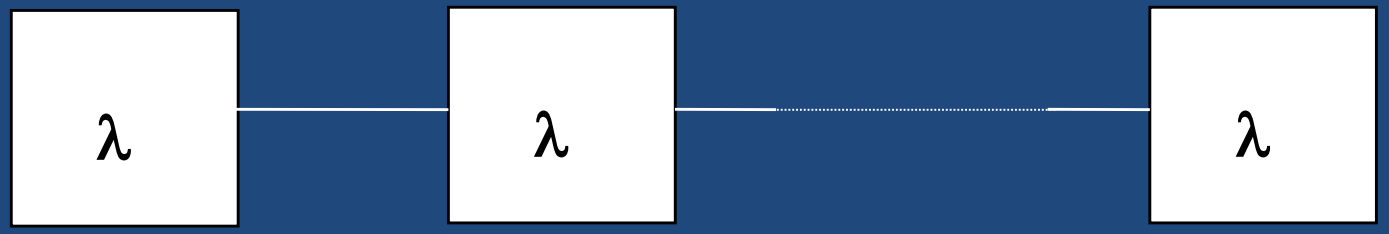
$$R_S(t) = R_1(t) \cdot R_2(t) \cdot \ldots\ldots\ldots \cdot R_n(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \cdot \ldots\ldots \cdot e^{-\lambda_n t} = e^{-\lambda_S t}$$

$$\lambda_S = \lambda_1 + \lambda_2 + \ldots\ldots\ldots + \lambda_n$$

$$\theta_S = \frac{1}{\lambda_S} = \frac{1}{\lambda_1 + \lambda_2 + \ldots\ldots + \lambda_n} =$$

$$= \frac{1}{\frac{1}{\theta_1} + \frac{1}{\theta_2} + \ldots\ldots\ldots + \frac{1}{\theta n}}$$

Fiabilidad de Sistemas Serie (II)



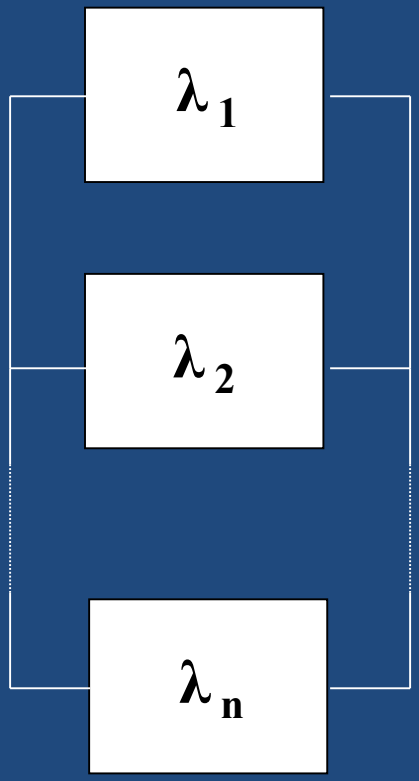
$$R_S(t) = R^n(t) = e^{-\lambda n t} = e^{-\lambda_S t}$$

$$\theta_S = \frac{1}{\lambda_S} = \frac{1}{n\lambda} = \frac{\theta}{n}$$

Fiabilidad de Sistemas Paralelo

Redundancia activa

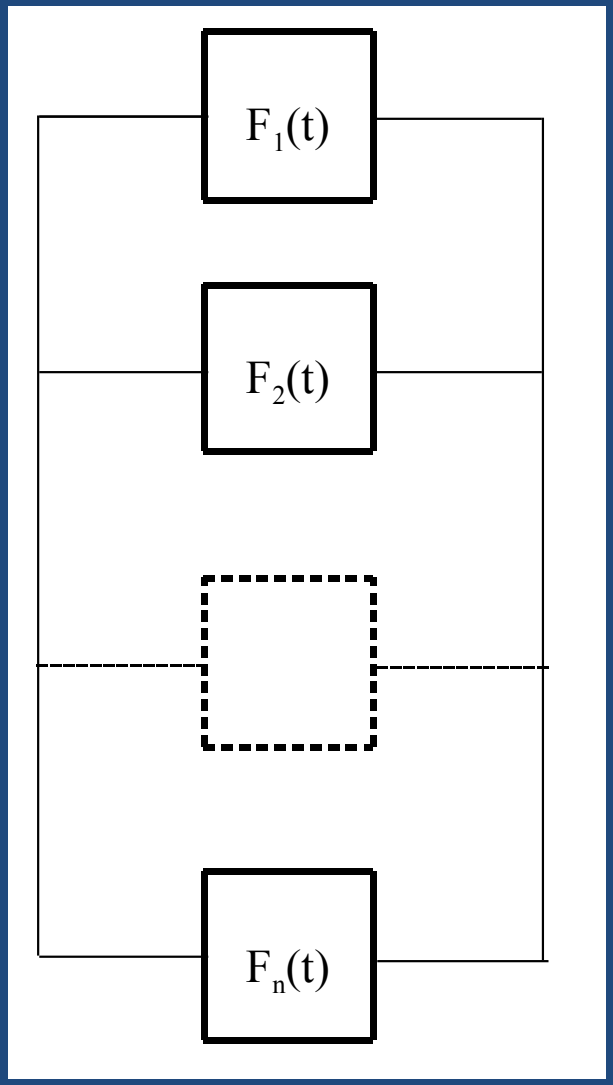
Redundancia activa (I)



$$F_S(t) = F_1(t) \cdot F_2(t) \cdot .... \cdot F_n(t) =$$
$$= \left[1 - R_1(t)\right] \cdot \left[1 - R_2(t)\right] \cdot .... \cdot \left[1 - R_n(t)\right] =$$
$$= \prod_{i=1}^{n} \left[1 - R_i(t)\right]$$

$$R_S(t) = 1 - F_S(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right] =$$
$$= 1 - \prod_{i=1}^{n} \left[1 - e^{-\lambda_i t}\right]$$

Redundancia activa (II)



$$R_S(t) = 1 - \left(1 - e^{-\lambda_1 t}\right)$$

$$\left(1 - e^{-\lambda_2 t}\right) \cdots\cdots \left(1 - e^{-\lambda_n t}\right)$$

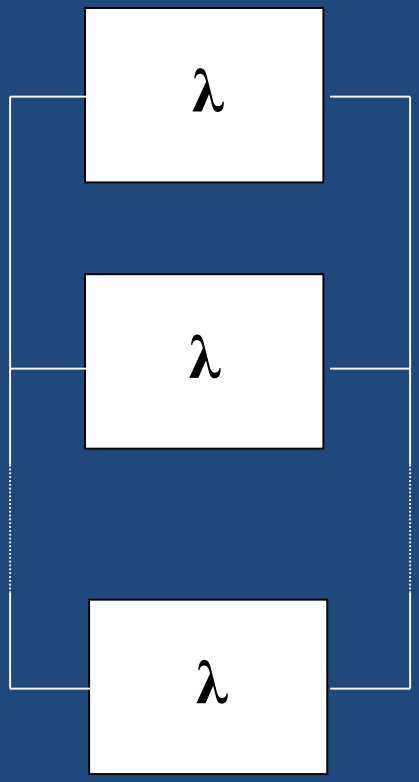
Para n = 3

$$R_S(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} + e^{-\lambda_3 t} - e^{-(\lambda_1+\lambda_2)t} - e^{-(\lambda_1+\lambda_3)t} - e^{-(\lambda_2+\lambda_3)t} + e^{-(\lambda_1+\lambda_2+\lambda_3)t}$$

$$\theta_S = \int_0^\infty R(t)dt = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \frac{1}{\lambda_1+\lambda_2} -$$

$$- \frac{1}{\lambda_1+\lambda_3} - \frac{1}{\lambda_2+\lambda_3} + \frac{1}{\lambda_1+\lambda_2+\lambda_3}$$

Redundancia activa (III)

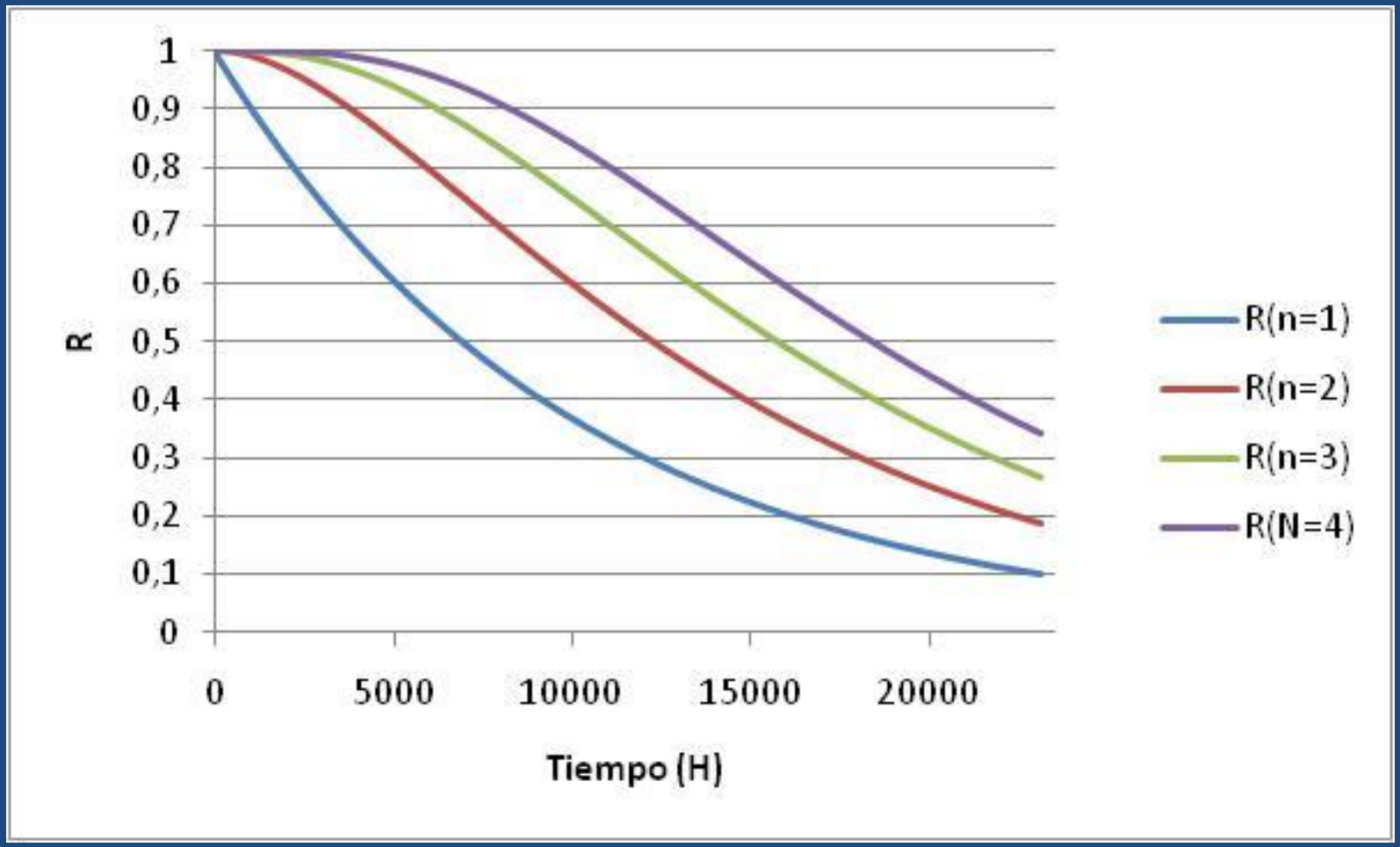


$$F_S(t) = F^n(t)$$

$$R_S(t) = 1 - \left[1 - R(t)\right]^n = 1 - \left[1 - e^{-\lambda t}\right]^n$$

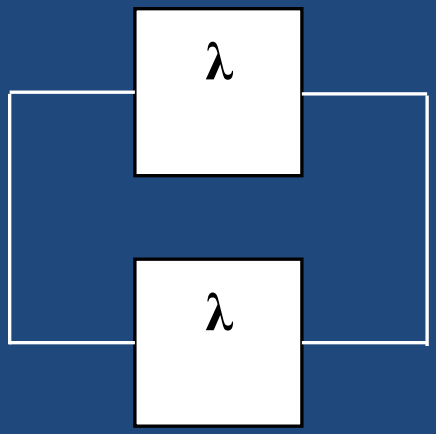
$$\theta_S = \int_0^\infty R(t)dt = \frac{1}{\lambda}\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots\ldots\ldots\ldots + \frac{1}{n}\right)$$

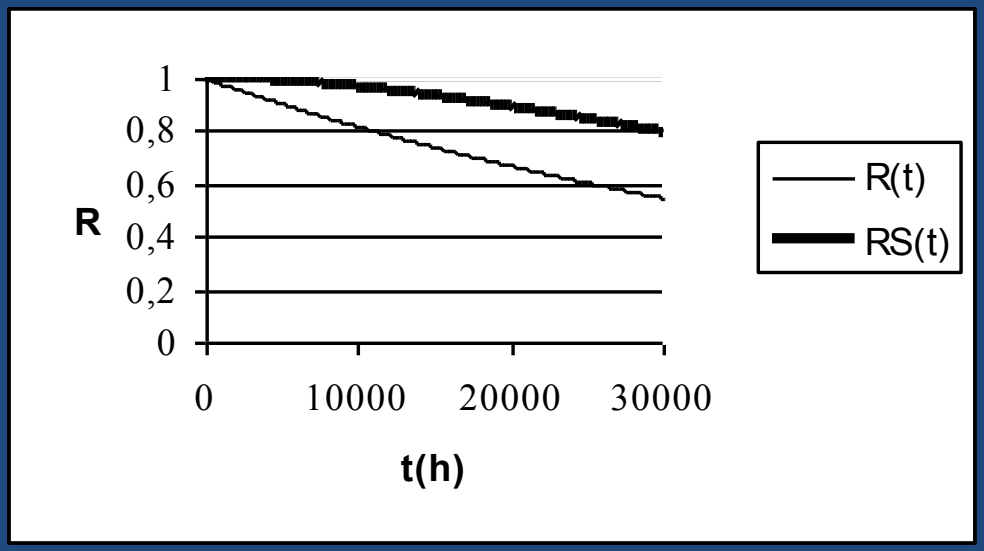
Redundancia activa (IV)



Redundancia activa (V)

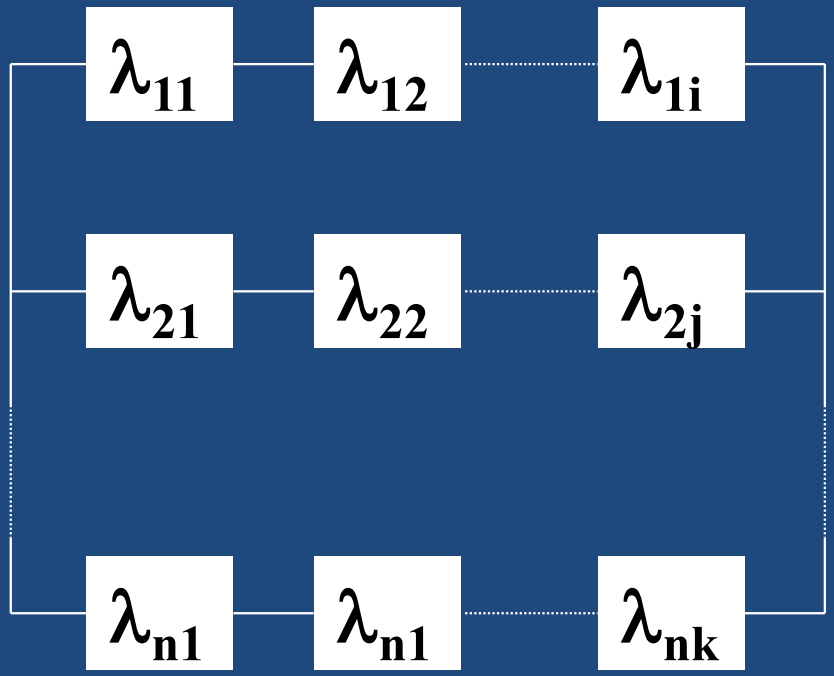
$$R_S(t) = 1 - [1 - R(t)]^2 = 2R(t) - R^2(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$





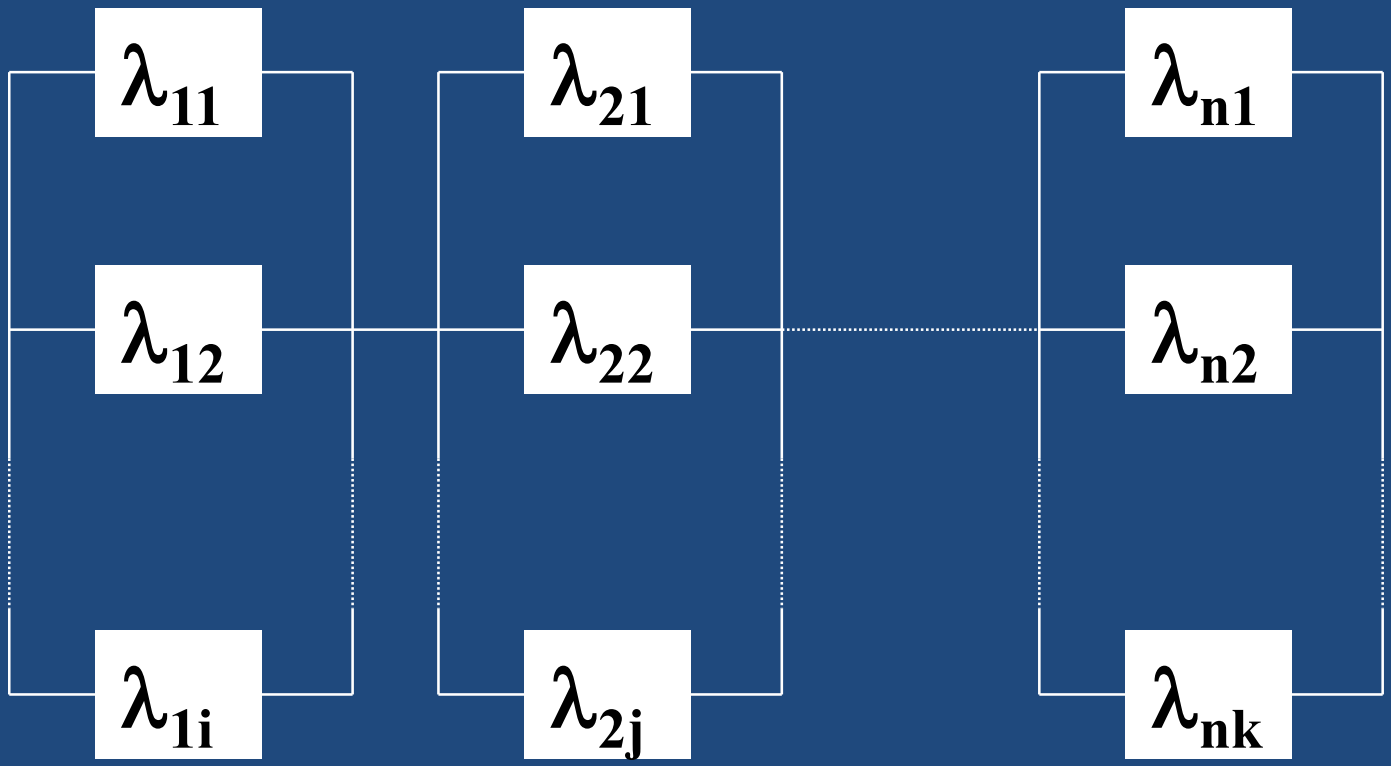
$$\theta_S = \int_0^\infty (2e^{-\lambda t} - e^{-2\lambda t})dt = \frac{3}{2\lambda} = 1{,}5 * \theta$$

Combinación Paralelo - Serie



$$R_S(t) = 1 - \left[\left(1 - \prod_{i=1}^{i} R_{1i} \right) \left(1 - \prod_{j=1}^{j} R_{2j} \right) ..... \left(1 - \prod_{k=1}^{k} R_{nk} \right) \right]$$

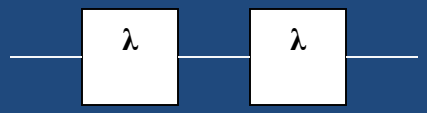
Combinación Serie - Paralelo



$$R_S(t) = \left[1 - \prod_{1=1}^{i}\left(1 - R_{1i}\right)\right]\left[1 - \prod_{j=1}^{j}\left(1 - R_{2j}\right)\right].....\left[1 - \prod_{k=1}^{k}\left(1 - R_{nk}\right)\right]$$

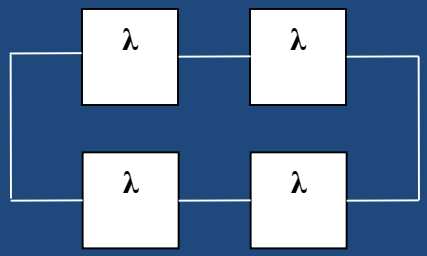
Comparación de Redundancias (I)

a)



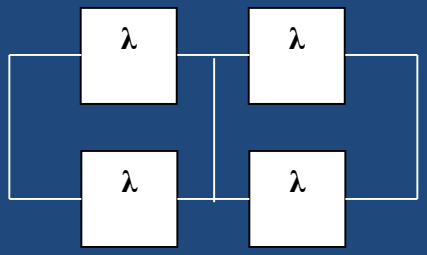
$$R_a(t) = R^2(t) = e^{-2\lambda t}$$

b)



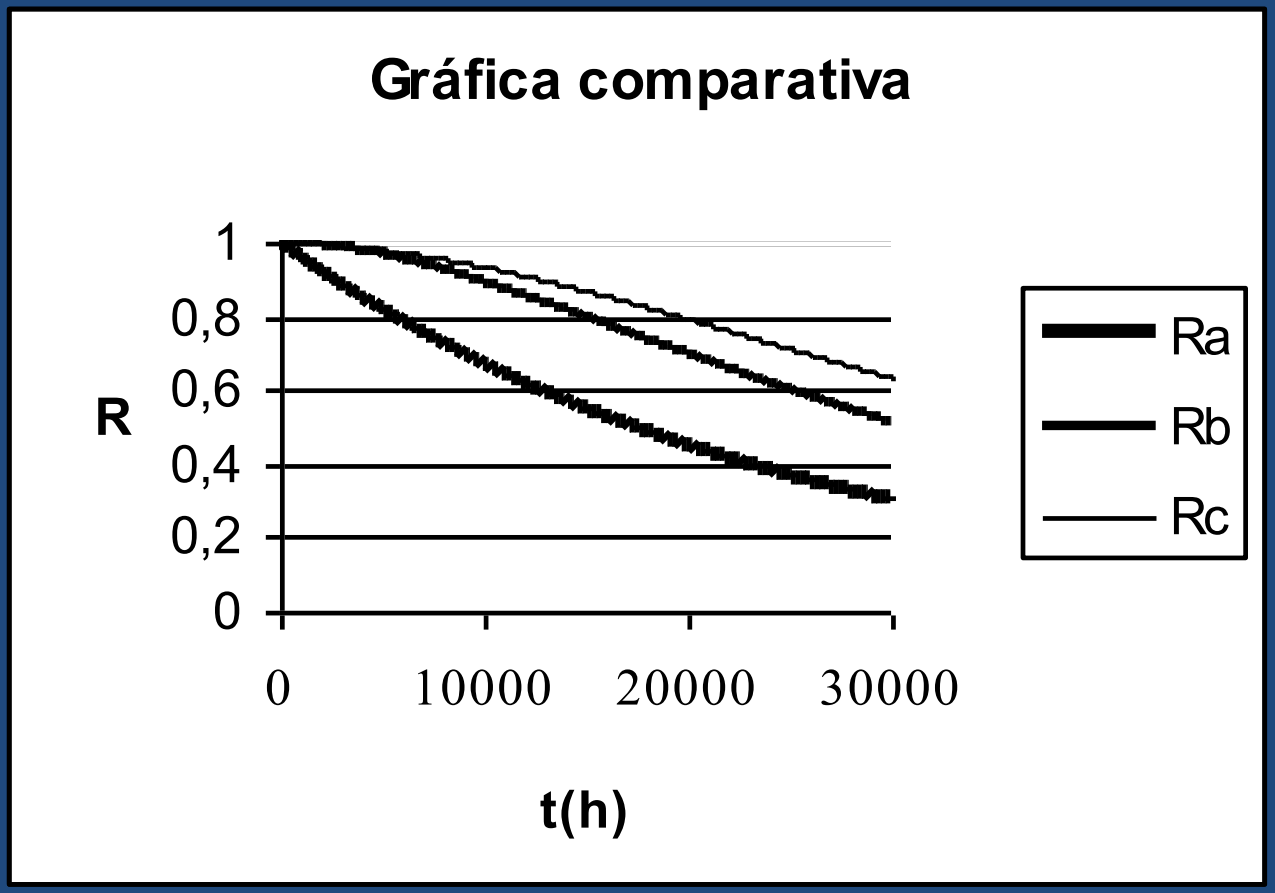
$$R_b(t) = 2R^2(t) - R^4(t) = 2e^{-2\lambda t} - e^{-4\lambda t}$$

c)

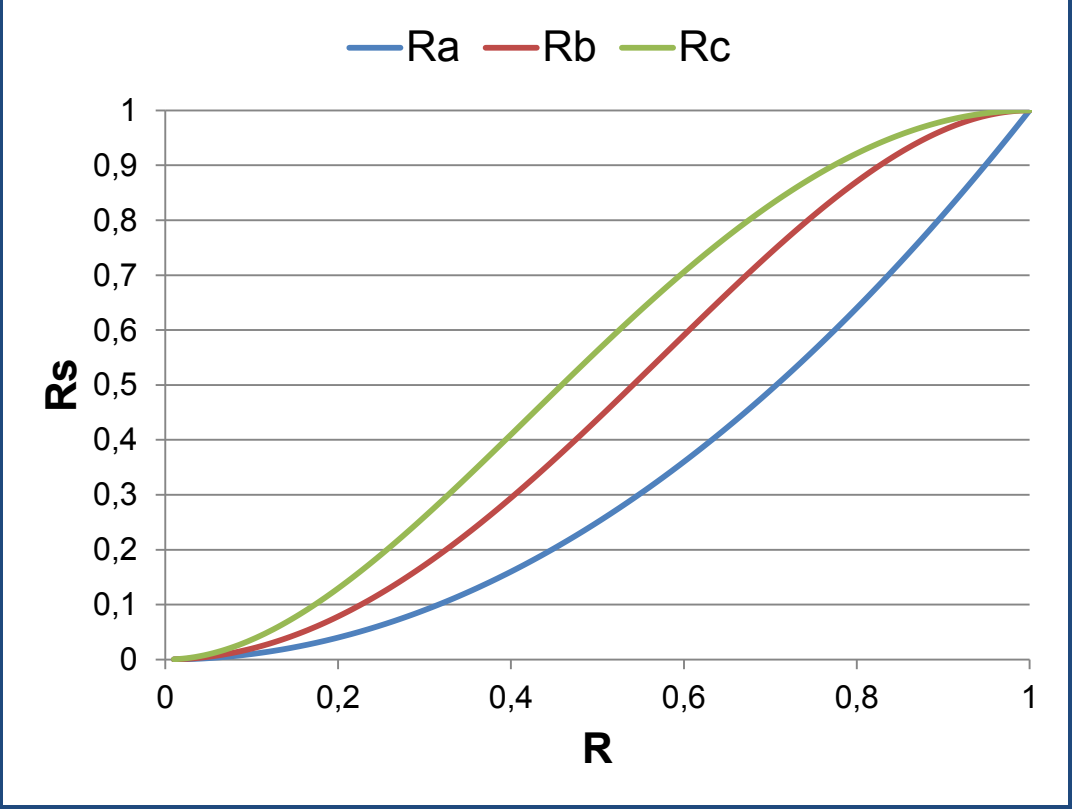


$$R_c(t) = R^4(t) - 4R^3(t) + 4R^2(t) =$$
$$= e^{-4\lambda t} - 4e^{-3\lambda t} + 4e^{-2\lambda t}$$

Comparación de Redundancias (II)

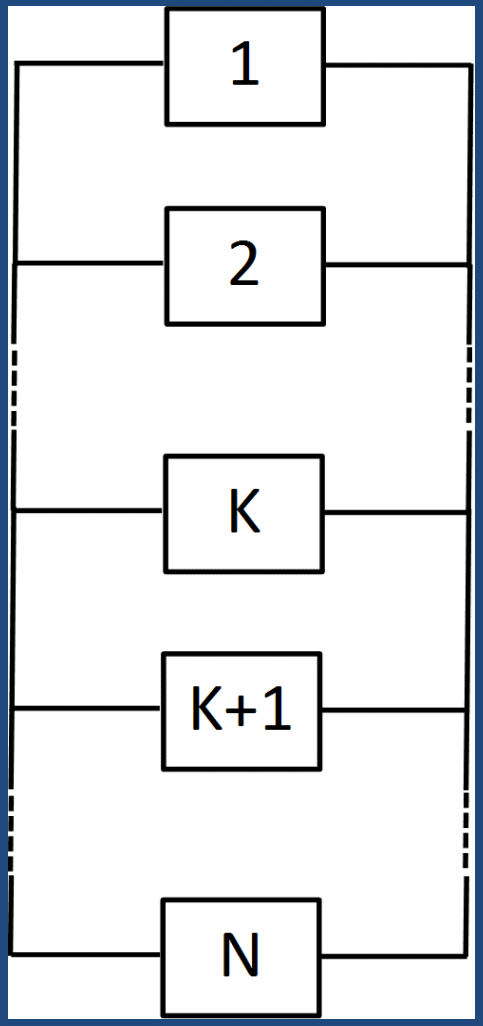


Comparación de Redundancias (III)



$R_a < R_b < R_c$ Para cualquier valor de R

Sistemas K out of N (KooN)

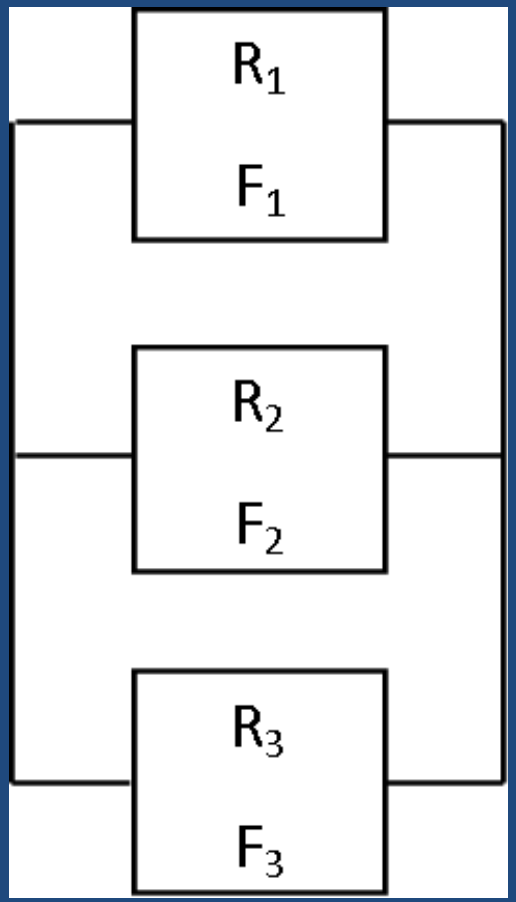


$$R_S(t) = P(X \geq K) =$$

$$\sum_{X=K}^{N} \binom{N}{X} R^X (1-R)^{N-X}$$

$$\binom{N}{X} = \frac{N!}{X!\,(N-X)!}$$

Sistemas K out of N (2oo3)



$$R_S(t) = R_1R_2R_3 + R_1R_2F_3 + R_1F_2R_3 +$$
$$+F_1R_2R_3 = R_1R_2R_3 + R_1R_2(1-R_3) +$$
$$+R_1(1-R_2)R_3 + (1-R_1)R_2R_3 =$$
$$= R_1R_2 + R_1R_3 + R_2R_3 - 2R_1R_2R_3$$

Si todos los bloques son iguales:

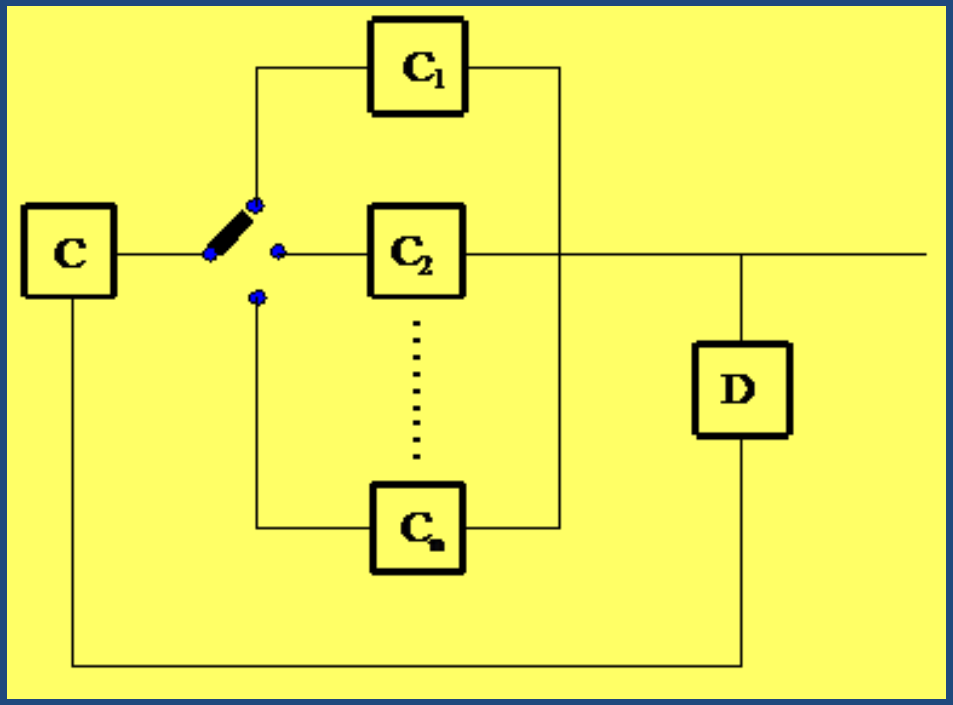
$$R_S(t) = 3R^2 - 2R^3$$

$$R_S(t) = P(X \geq 2) = \sum_{X=2}^{3} \binom{3}{X} R^X(1-R)^{3-X} =$$
$$= 3R^2 - 2R^3$$

Fiabilidad de Sistemas Paralelo

Redundancia pasiva

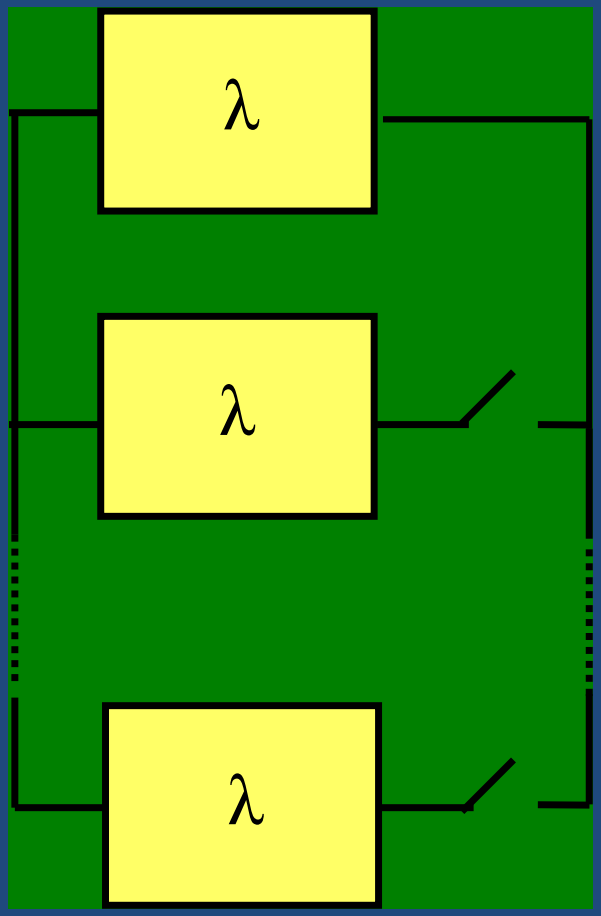
Redundancia pasiva (I)



- Funciona un elemento y los redundantes están en reserva (stand-by).
- Si el conmutador y el detector son ideales, y los elementos en espera tienen una tasa de fallos nula entonces la probabilidad de encontrar “k” fallos en un tiempo “t”, sigue la distribución de Poisson:

$$P(K) = \frac{(\lambda t)^K}{K!} e^{-\lambda t}$$

Redundancia pasiva (II)



- N bloques en paralelo iguales.
- Conmutador y detector ideales.
- Tasa de fallos en reposo nula.

$$R_S(t) = P(K \leq N-1) =$$

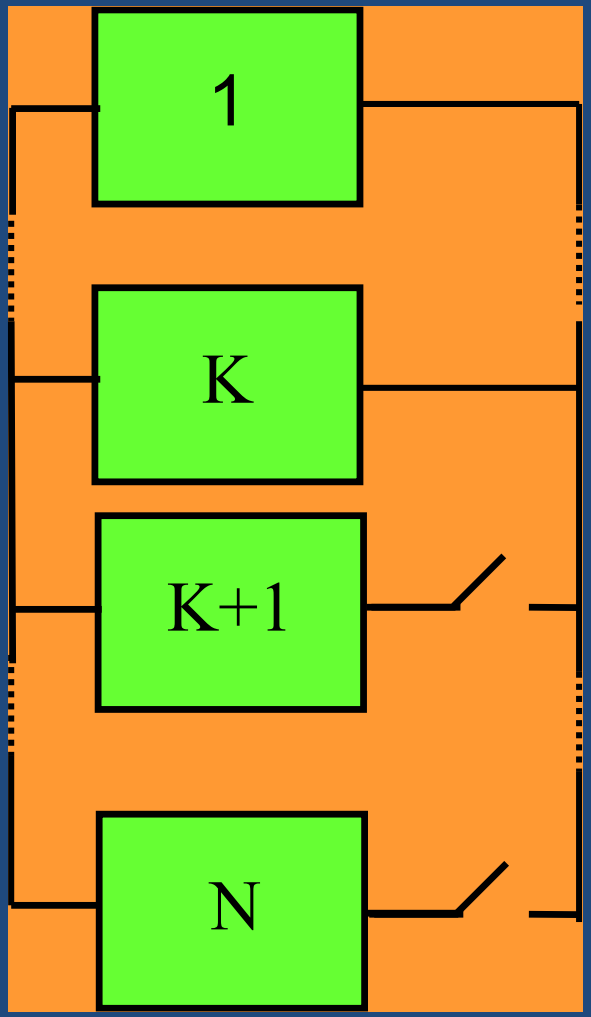
$$= \sum_{K=0}^{N-1} \frac{(\lambda t)^K}{K!} e^{-\lambda t} =$$

$$= e^{-\lambda t} \sum_{X=1}^{N} \frac{(\lambda t)^{X-1}}{(X-1)!}$$

$$\theta_S = \int_0^\infty R_S(t) = \int_0^\infty e^{-\lambda t} \sum_{X=1}^{N} \frac{(\lambda t)^{X-1}}{(X-1)!} dt =$$

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

Redundancia pasiva (III)



X: Nº de bloques que pueden fallar

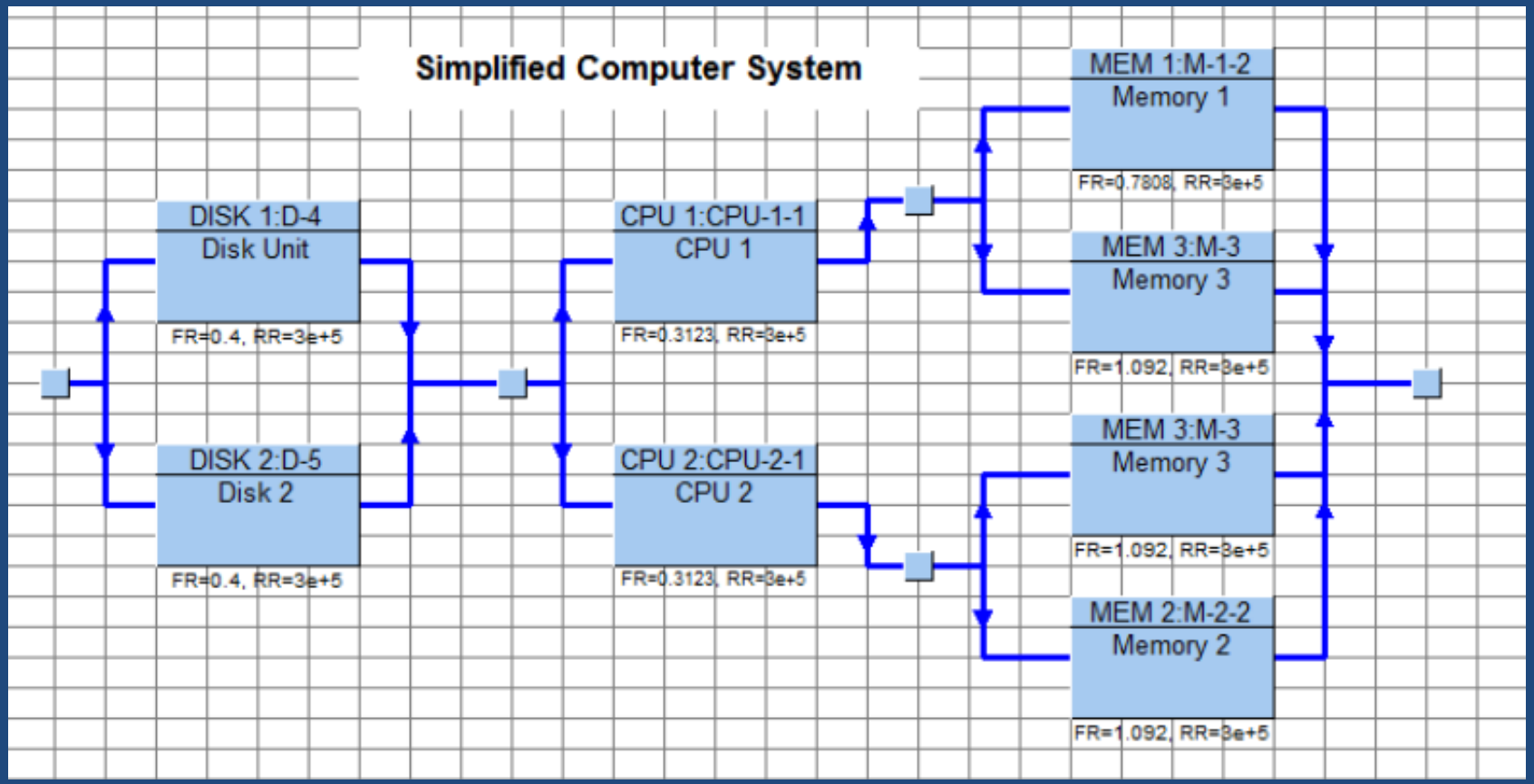
$$R_S(t) = P(X \leq N - K) =$$

$$= e^{-K\lambda t} \sum_{X=0}^{N-K} \frac{(K\lambda t)^X}{X!}$$

$$\theta_S = \int_0^\infty R_S(t) = \int_0^\infty e^{-K\lambda t} \sum_{X=0}^{N-K} \frac{(K\lambda t)^X}{X!} dt$$

$$\theta_S = \frac{N - K + 1}{K\lambda}$$

Diagrama de bloques



Mantenibilidad

(Maintainability)

Mantenibilidad M(t) (I)

Probabilidad de que un sistema con fallo sea reparado en un tiempo determinado

- **Mantenimiento Correctivo**
- **Mantenimiento Preventivo**
- **Mantenimiento Predictivo**

Mantenibilidad M(t) (II)

$$M(t) = 1 - e^{-\mu t}$$

Tasa de reparación:

$$\mu = \frac{1}{MTTR}$$

$$MDT = MTTR + DT$$

MTBM: Tiempo medio entre acciones de mantenimiento (Preventivo o correctivo)

Disponibilidad

(Availability)

Disponibilidad A(t) (I)

Probabilidad de que un componente, circuito o sistema funcione correctamente en un instante determinado y en condiciones de trabajo especificadas

$$A(t) = R(t) + M(t) \bullet F(t)$$

$$A(t) = e^{-\lambda t} + (1 - e^{-\mu t}) \bullet (1 - e^{-\lambda t})$$

Tipos de Disponibilidad

$$A = \frac{TiempoOperativo}{TiempoOperativo + TiempoNoOperativo}$$

Disponibilidad Intrínseca

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Disponibilidad Operacional

$$A_O = \frac{MTBM}{MTBM + MDT}$$

Seguridad

(Safety)

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 de seguridad (Fail-Safe Systems)**

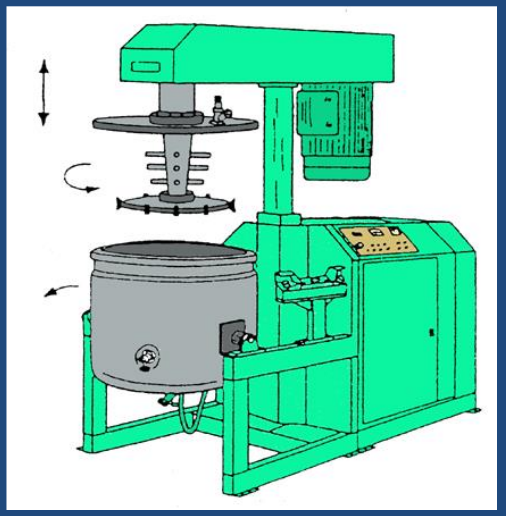
Seguridad

Seguridad (Security): La Seguridad (Security) se refiere a la protección de un dispositivo, equipo, sistema o instalación frente a "ataques/sucesos/hechos provocados" (sabotajes). La acción desencadenante del daño potencial se produce de afuera (el exterior al equipo) hacia dentro (interior del equipo).

Aplicaciones (I)

- 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 (I)

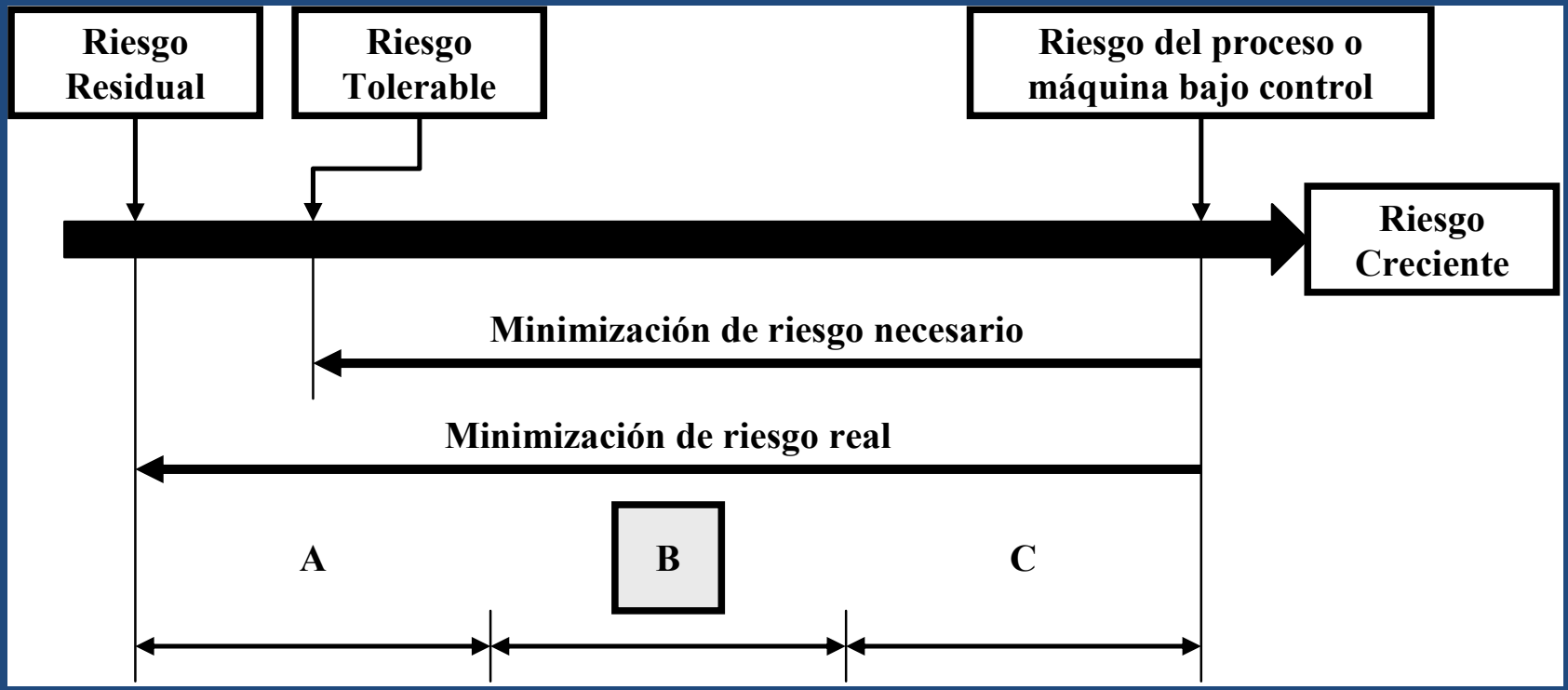
- **Análisis de Riesgos**.
  - **UNE-EN ISO 12100 (2012)**
  - **UNE-EN ISO 14121-1 (2008)**

$$R = G \cdot P$$

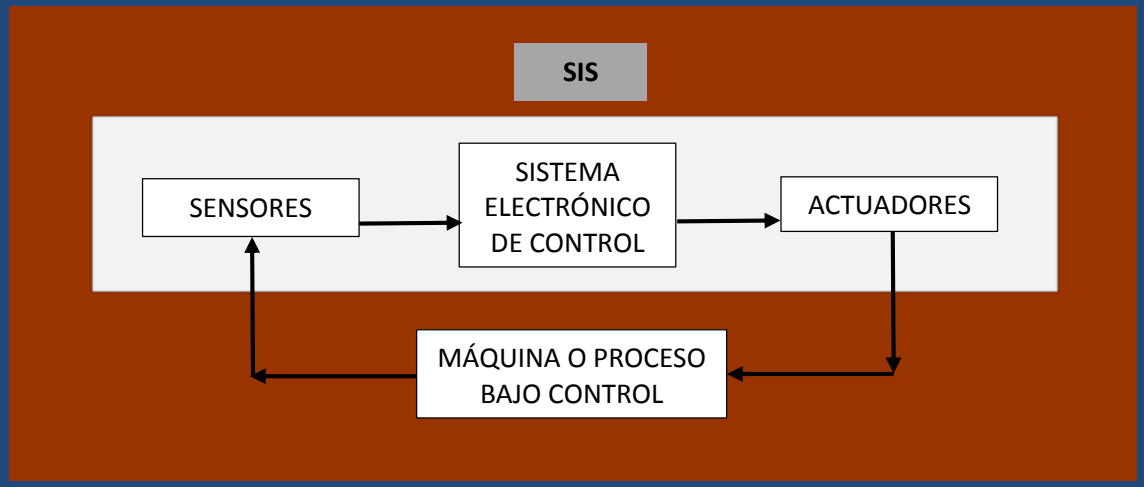
- **Nivel de seguridad exigido**
- **Implementación**
- **Verificación**
- **Certificación:** Organismos internacionales (Exida, TÜV Nord, TÜV Rheinland y TÜV Süd)
- **Operación y mantenimiento**

Procedimiento General (II)

RIESGO bajo el punto de vista del peligro observado = **GRAVEDAD** del posible daño según el peligro observado x **PROBABILIDAD DE QUE OCURRA DICHO DAÑO**
1) Duración y frecuencia de la exposición al peligro
2) Posibilidad de evitar o limitar los daños



Sistema de seguridad



- **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

Normativas de seguridad

- Maquinaria
- Procesos
- Ferroviario
- Automoción

Normativas Maquinaria (I)

- **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.

Normativas Maquinaria (II)

- **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 $< 10^{-7}$

Normativas Maquinaria (III)

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

  SIL (Safety Integrity Level). Nivel de seguridad integral

SIL	Probabilidad media de fallo bajo demanda (PFD_{avg})
SIL 3	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-6}$ to $< 10^{-5}$

Normativas Maquinaria (IV)

- 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

Normativas Maquinaria (V)

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

	Tecnología utilizada	ISO 13849	IEC 62061
A	No eléctrico (Hidráulico, etc.)	X	No contemplado
B	Electrómecánico (Relés, etc.) y electrónica no compleja	Hasta PL = e	Hasta SIL 3
C	Electrónica compleja (Programable, etc.)	Hasta PL = d	Hasta SIL 3
D	A combinado con B	Hasta PL = e	*)
E	C combinado con B	Hasta PL = d	Hasta SIL 3

*) Para partes usadas con tecnología no eléctrica conforme a ISO 13849

Normativas Procesos (I)

- **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.

Normativas Procesos (II)

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

  SIL (Safety Integrity Level). Nivel de seguridad integral

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

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	$< 10^{-6}$

MIL-STD-882D

Descripción	Categ.	Efectos
Catastrófico	I	Muerte, Incapacidad Total Daños > 1M$ Daño ambiental irreversible
Crítico	II	Incapacidad parcial, Enfermedad o lesión 200K$<Daños<1M$ Daño ambiental reversible
Marginal	III	Enfermedad o lesión, 10K$<Daños<200k$ Daño ambiental leve
Insignificante	IV	Enfermedad o lesión muy leve 2K$<Daños<10K$ Daño ambiental mínimo

Niveles de Seguridad

Sector de Maquinaria

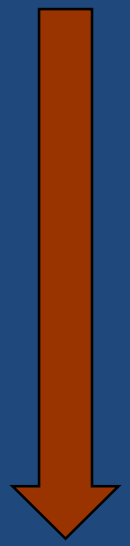
UNE-EN ISO 13849

Obtención del nivel de seguridad (I)

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

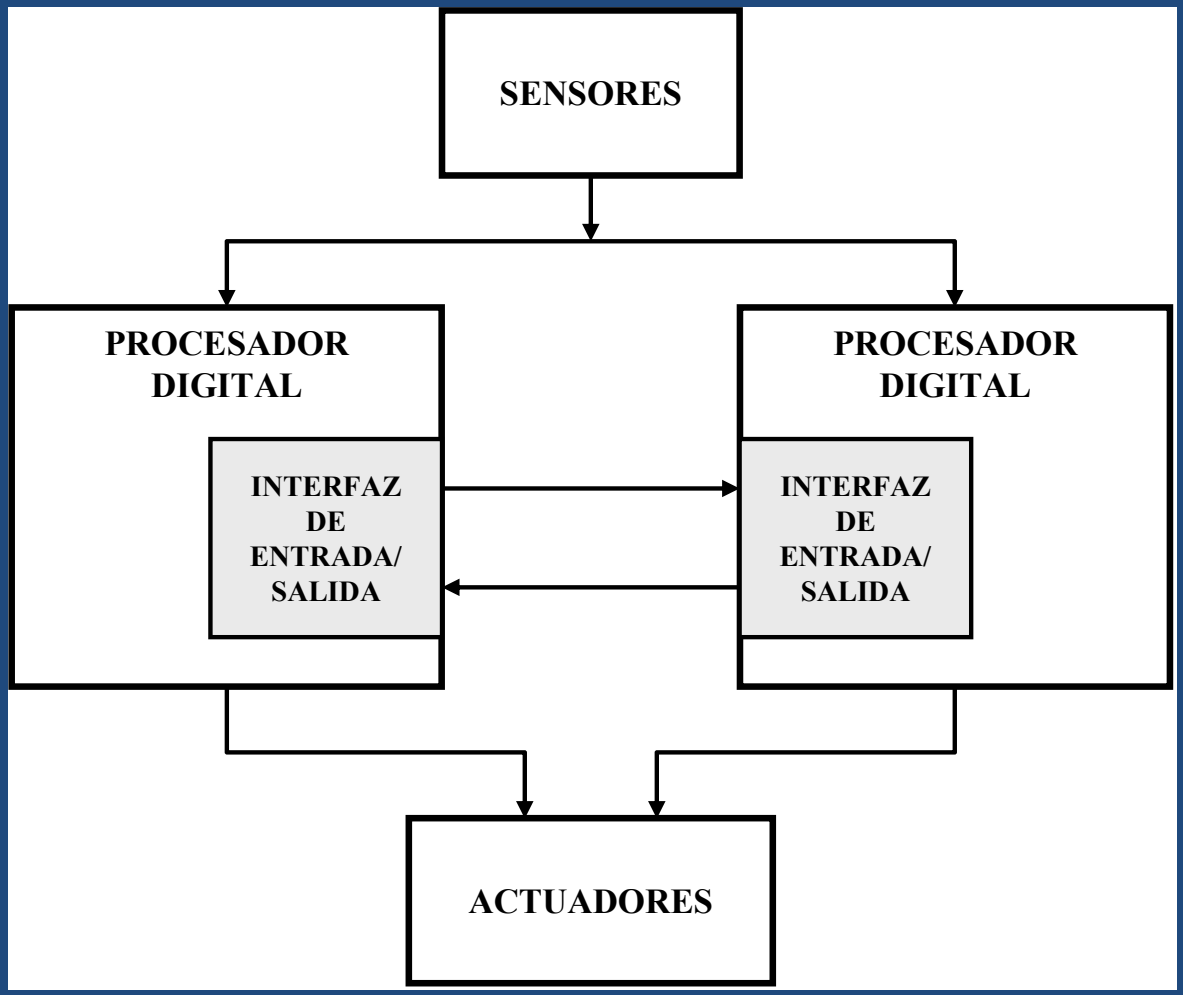
Obtención del nivel de seguridad (II)

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

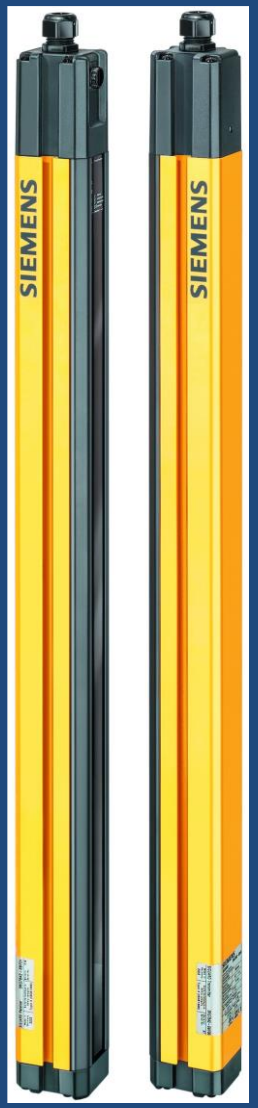


Riesgo Creciente

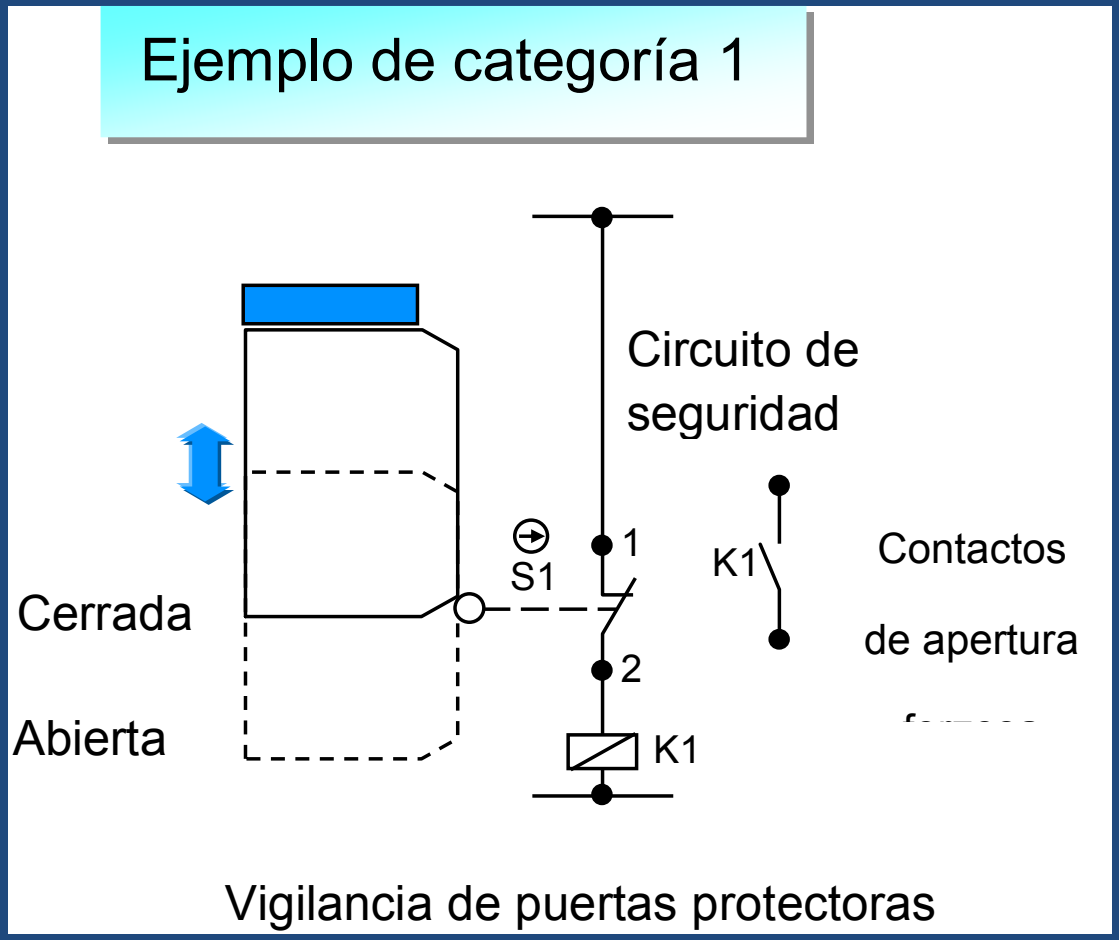
Sistemas de paro de emergencia (I)



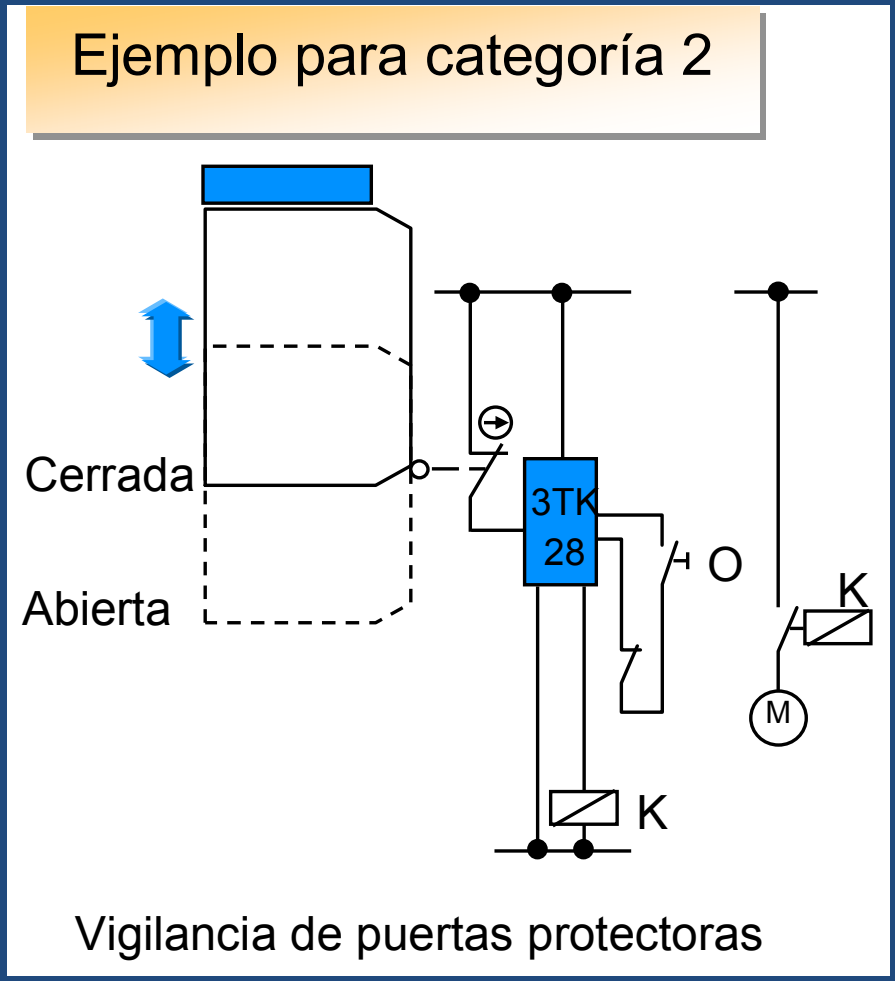
Sistemas de paro de emergencia (II)



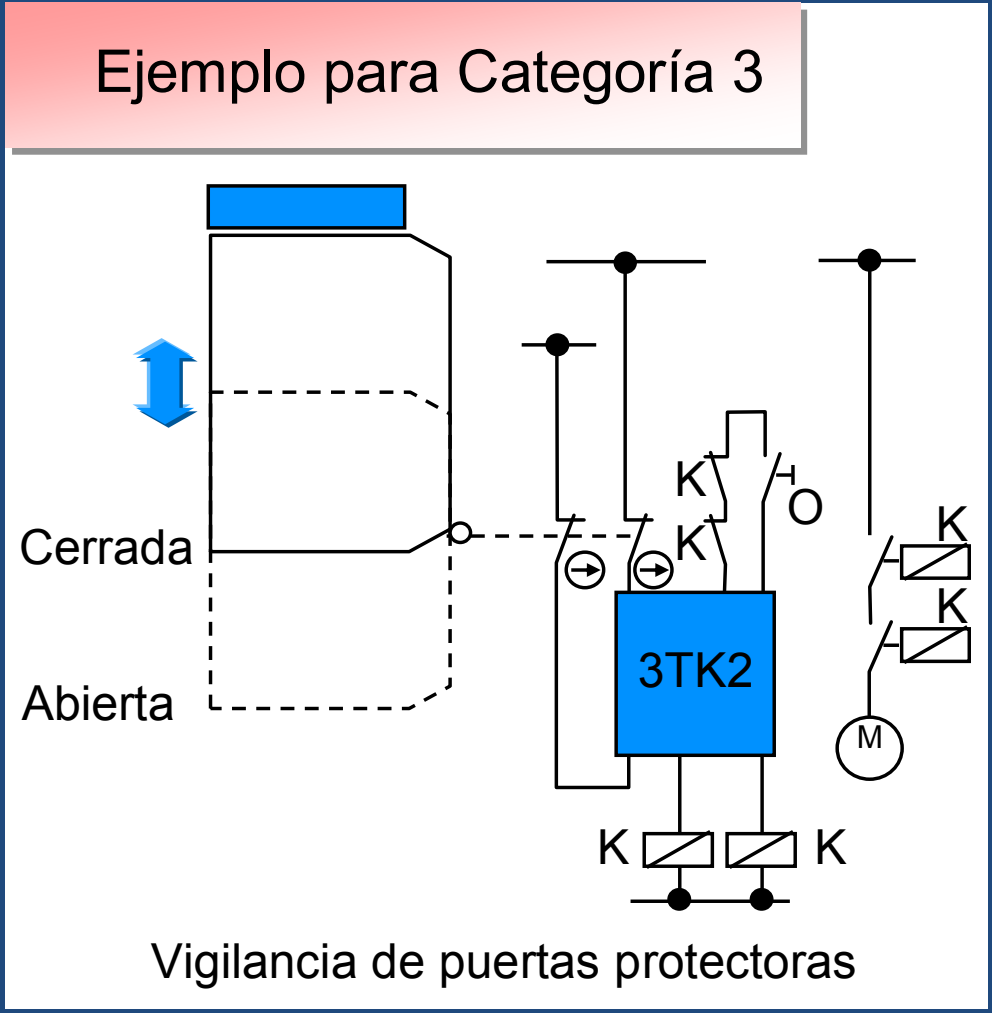
Ejemplo (I)


Ejemplo de categoría 1
Circuito de seguridad
S1
1
2
K1
K1
Contactos
de apertura
Cerrada
Abierta
Vigilancia de puertas protectoras

Ejemplo (II)

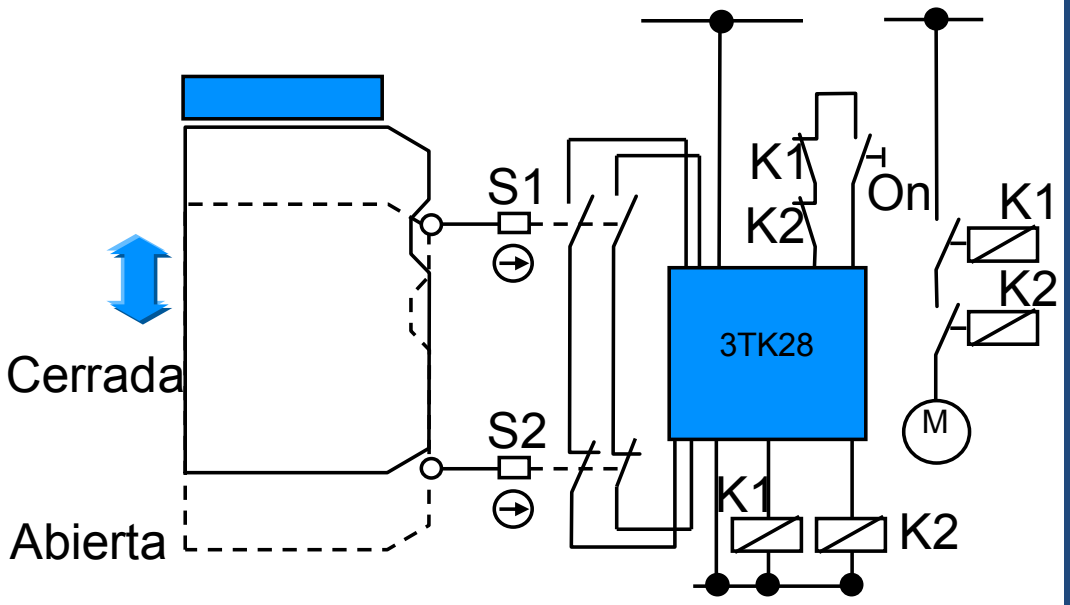

Ejemplo para categoría 2
Cerrada
Abierta
3TK
28
O
K
M
K
Vigilancia de puertas protectoras

Ejemplo (III)


Ejemplo para Categoría 3
Cerrada
Abierta
K
K
O
3TK2
K
K
M
K
K
Vigilancia de puertas protectoras

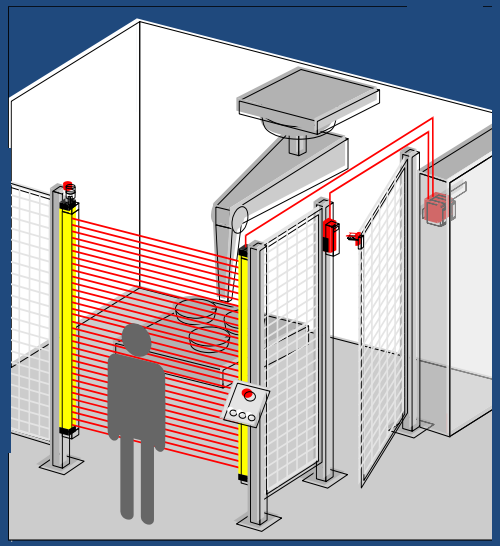
Ejemplo (IV)

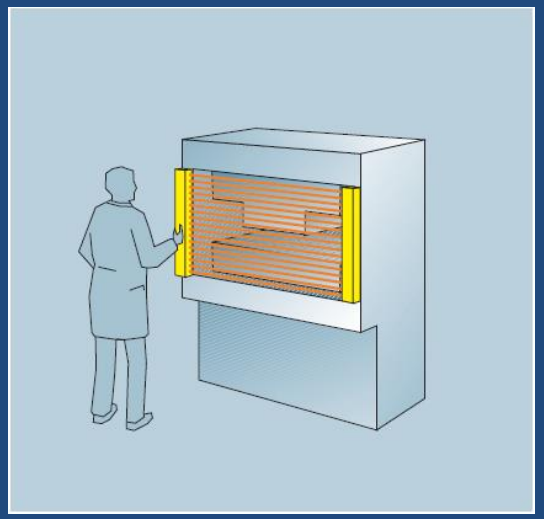
Ejemplo para Categoría 4

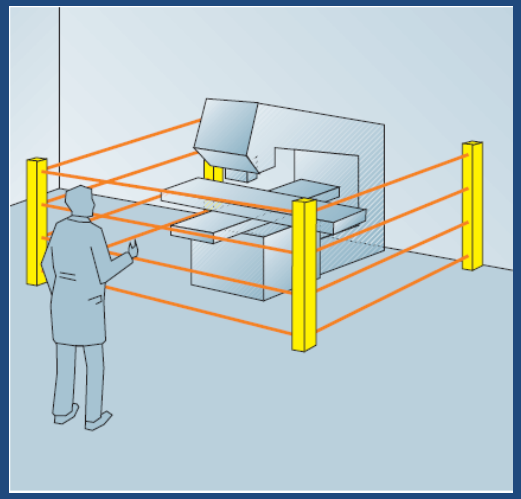


Vigilancia de puertas protectoras

Ejemplo (V)







Niveles de Seguridad

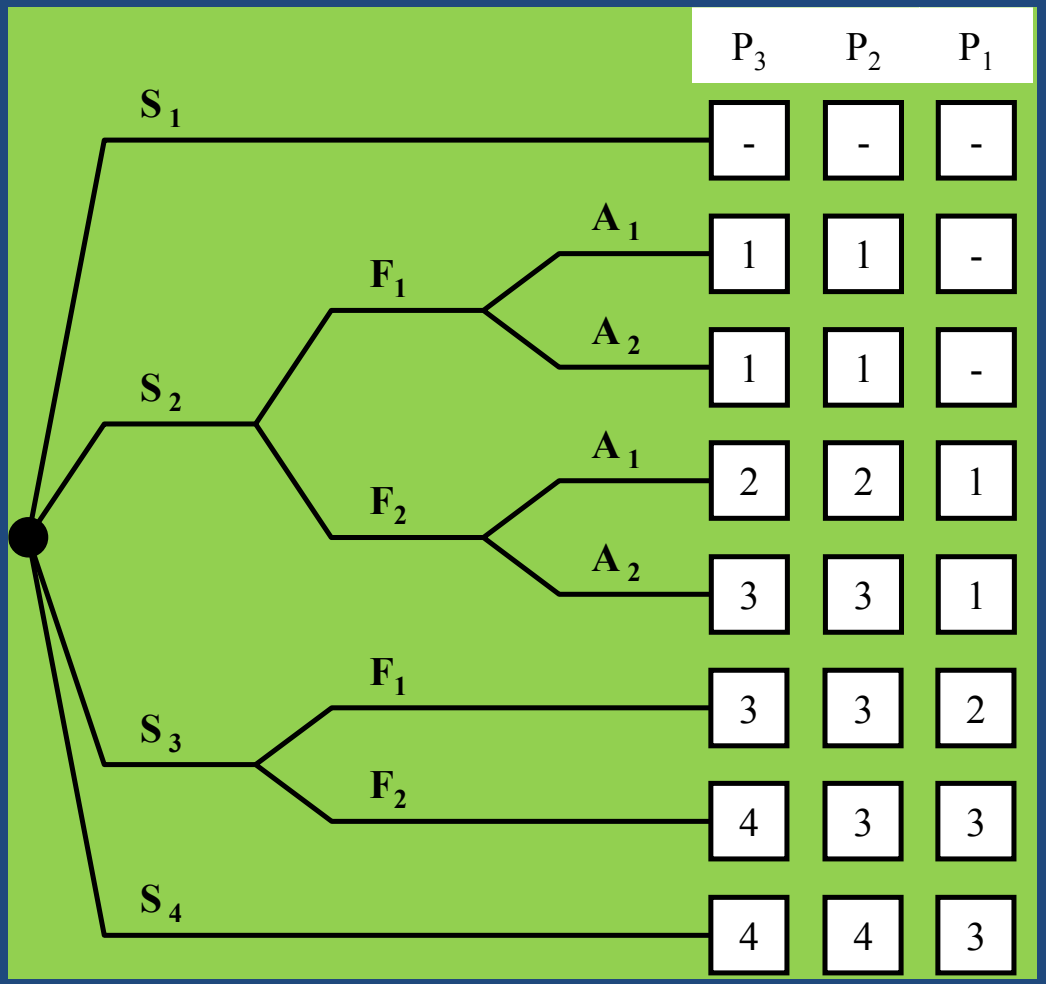
Procesos Industriales

UNE-EN-IEC 61508

Obtención del nivel de seguridad (I)

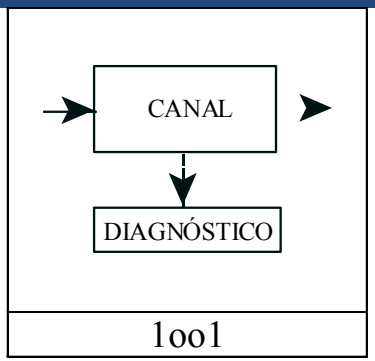
S (Severidad de lesiones/daños)	
S_1	Lesiones pequeñas, daños medioambientales menores
S_2	Lesiones serias irreversibles de muchas personas o una muerte daños medioambientales temporales serios
S_3	Muerte de muchas personas daños medioambientales serios de larga duración.
S_4	Resultados catastróficos, 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
A_2	No posible
P (Probabilidad de que ocurra)	
P_1	Muy baja
P_2	Baja
P_3	Relativamente alta

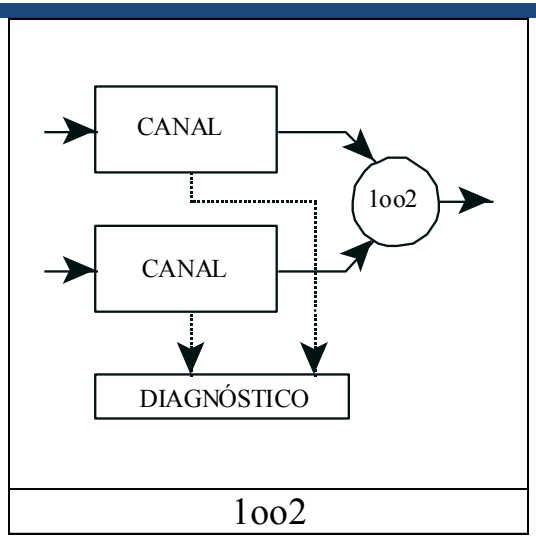
Obtención del nivel de seguridad (II)



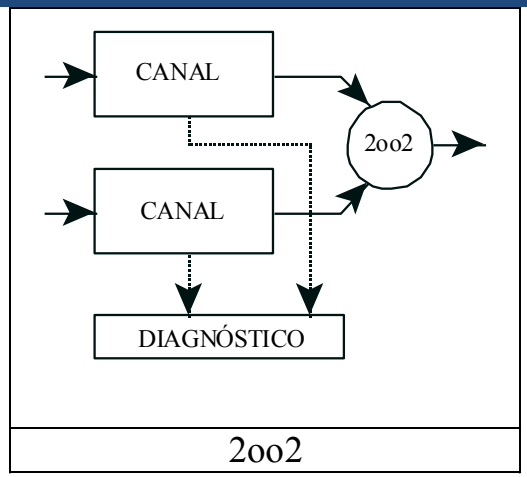
NIVEL SIL:
1 - 4

Estructuras (I)

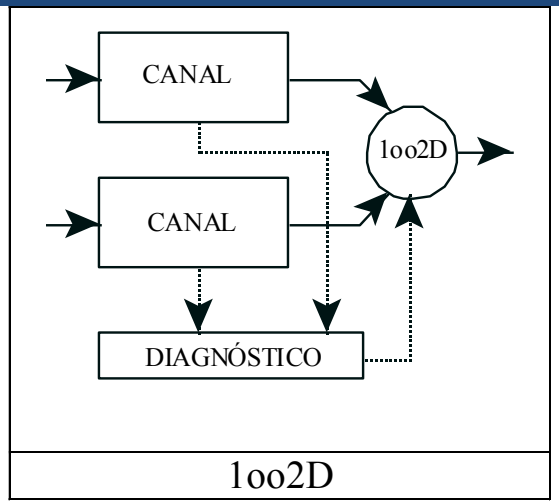




Estructuras (II)

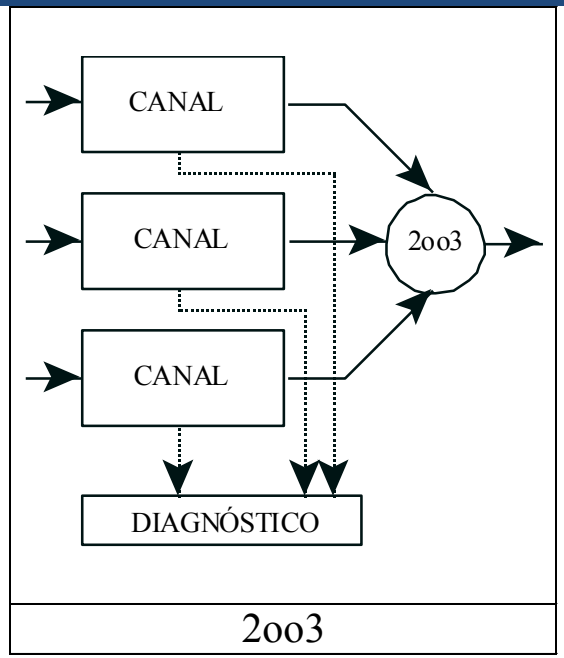


2oo2

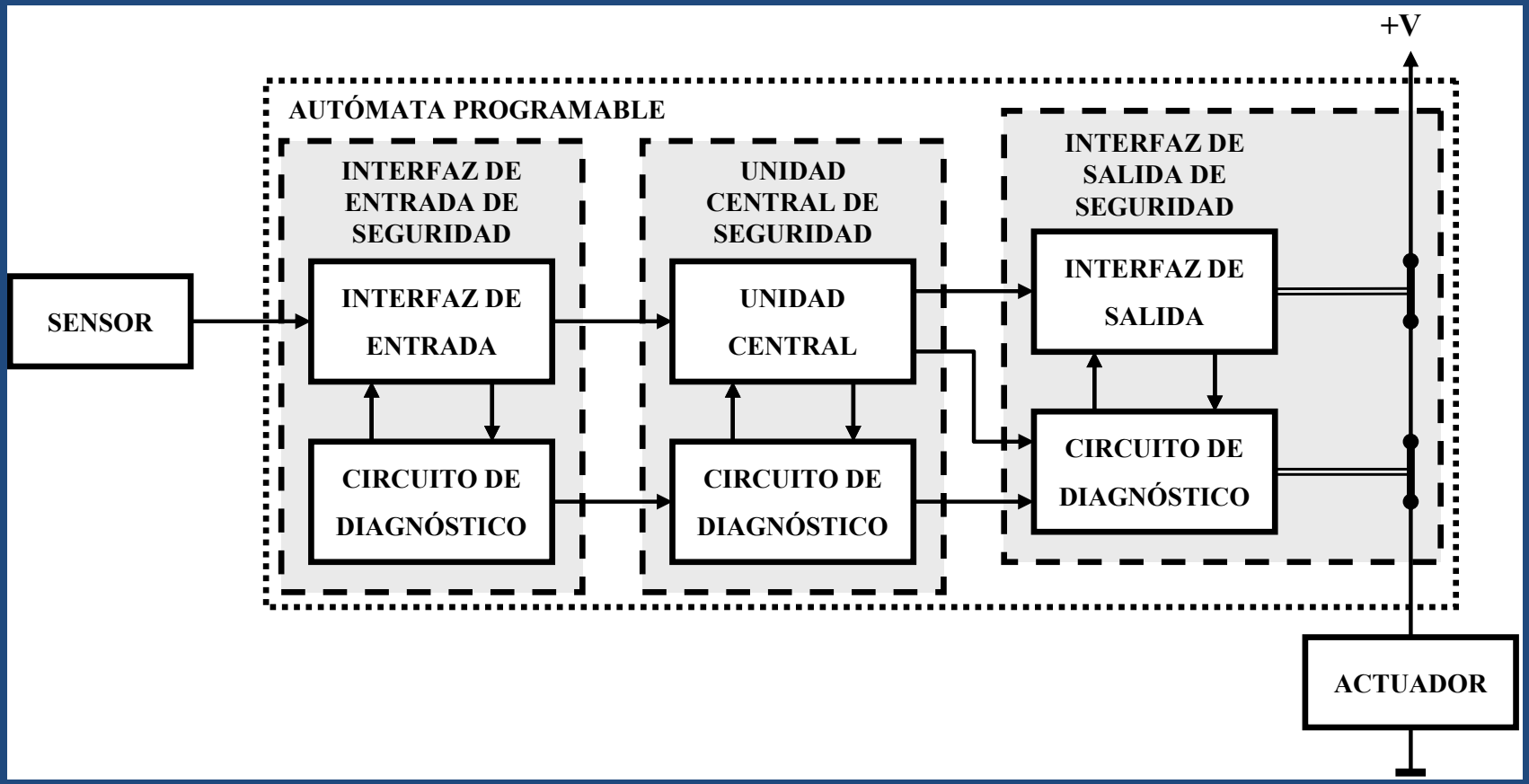


1oo2D

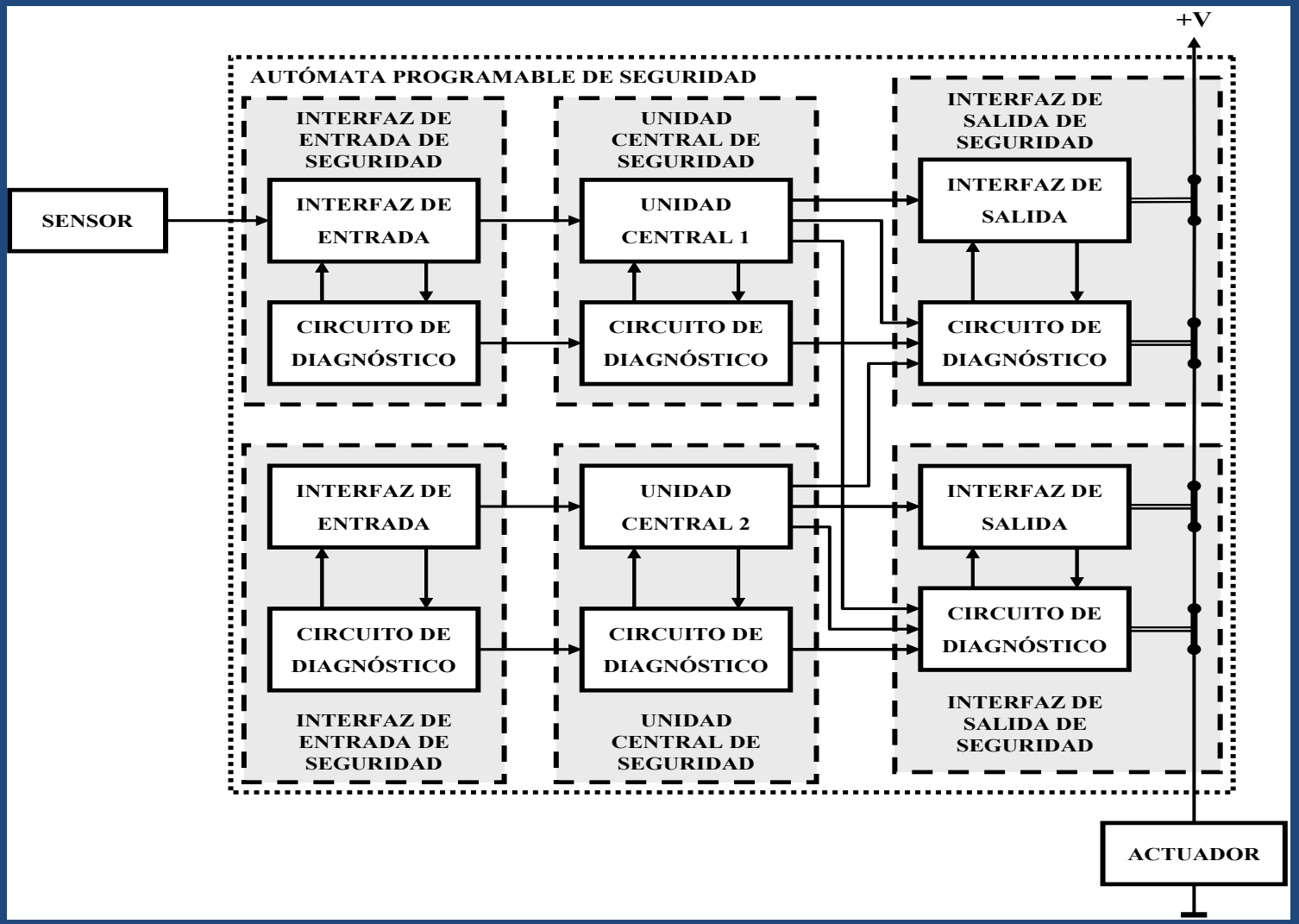
Estructuras (III)



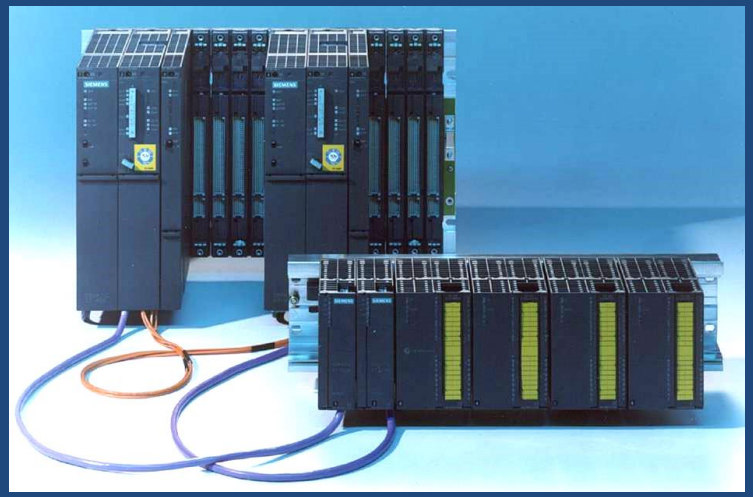
Estructura 1oo1D



Estructura 1oo2D

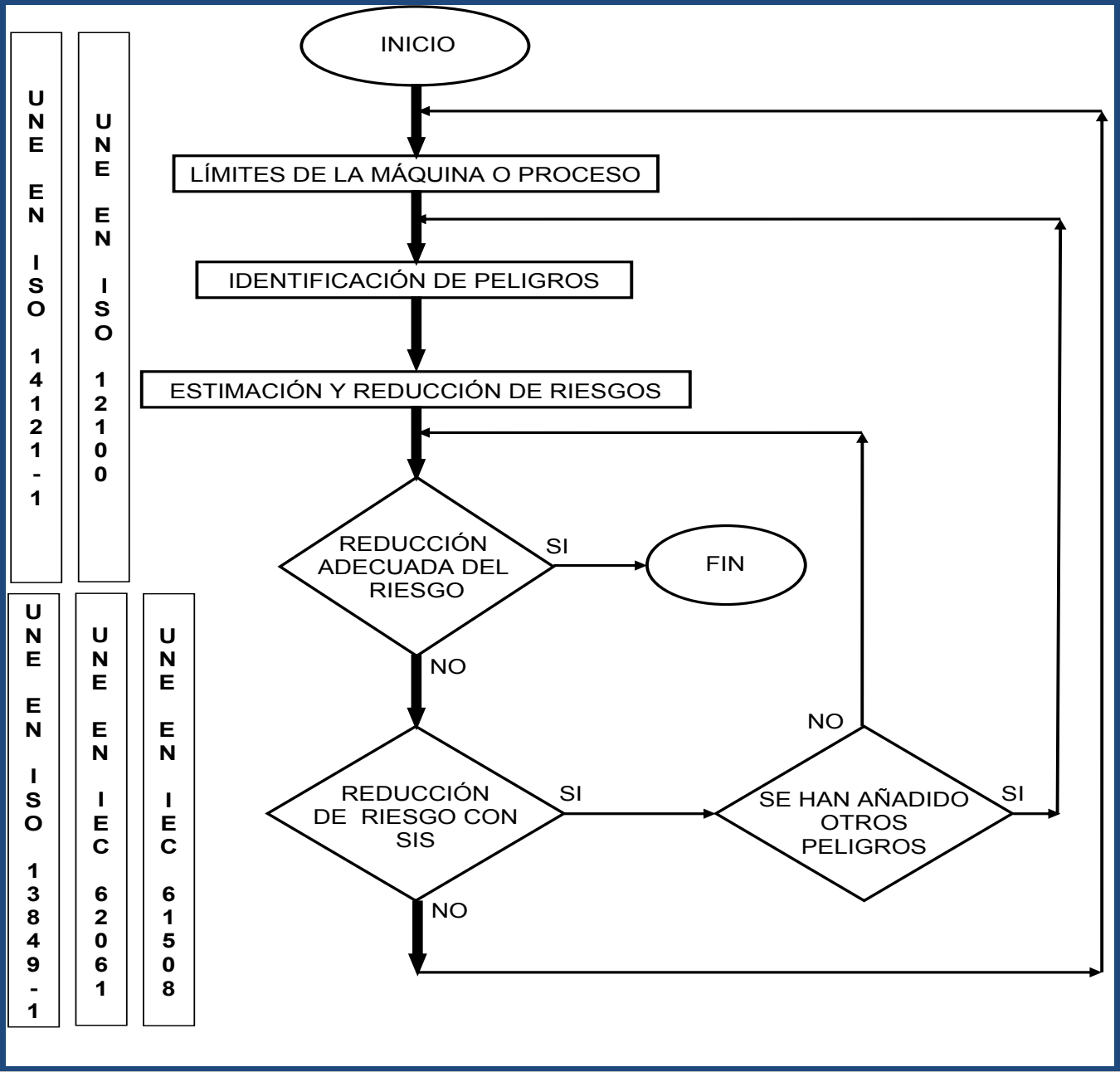


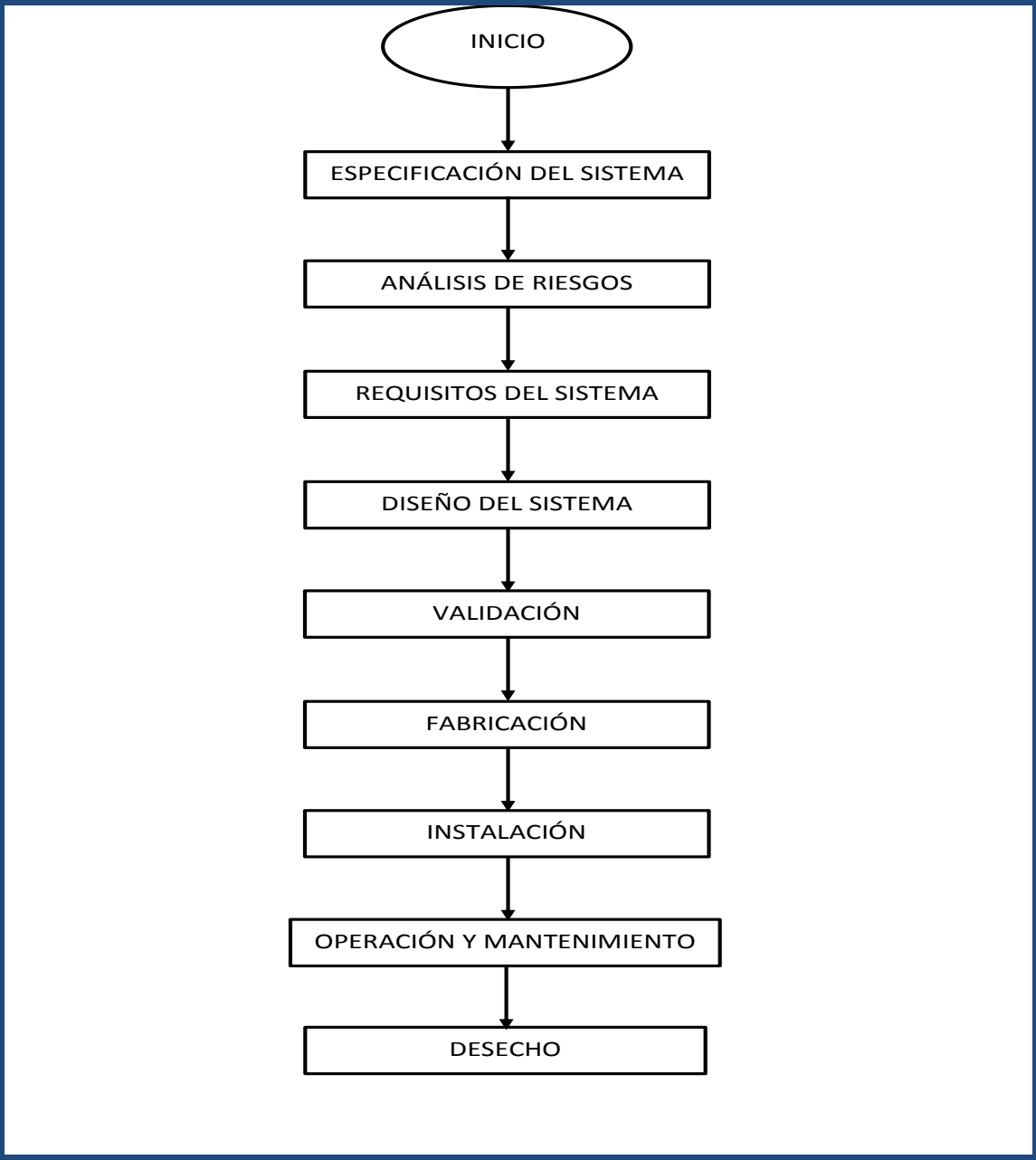
Autómatas Programables de Seguridad



Autómatas Programables de Seguridad

Diseño de un SIS


UNE EN ISO 14121-1
UNE EN ISO 12100
UNE EN ISO 13849-1
UNE EN IEC 62061
UNE EN IEC 61508
INICIO
LÍMITES DE LA MÁQUINA O PROCESO
IDENTIFICACIÓN DE PELIGROS
ESTIMACIÓN Y REDUCCIÓN DE RIESGOS
REDUCCIÓN ADECUADA DEL RIESGO
SI
FIN
NO
REDUCCIÓN DE RIESGO CON SIS
SI
NO
SE HAN AÑADIDO OTROS PELIGROS
SI
NO


INICIO
ESPECIFICACIÓN DEL SISTEMA
ANÁLISIS DE RIESGOS
REQUISITOS DEL SISTEMA
DISEÑO DEL SISTEMA
VALIDACIÓN
FABRICACIÓN
INSTALACIÓN
OPERACIÓN Y MANTENIMIENTO
DESECHO

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

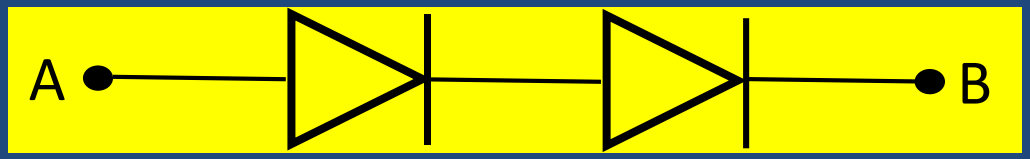
λ_{DD}: Tasa de fallos peligrosa y detectable

λ_{DU}: Tasa de fallos peligrosa y no detectable

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

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

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

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

Seguridad con Autómatas Programables (I)

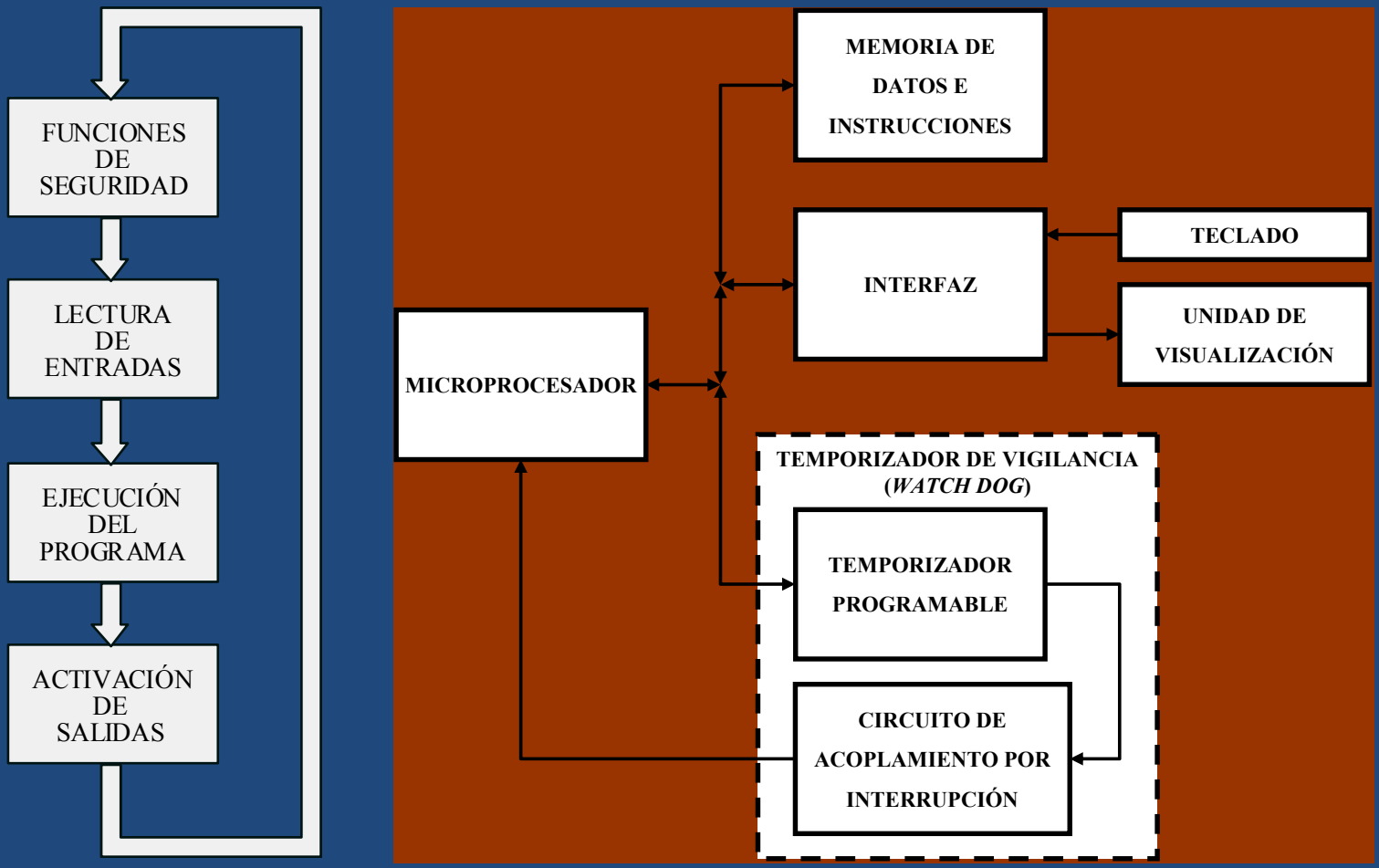
- Seguridad en la CPU
- Seguridad en las entradas
- Seguridad en las salidas

Seguridad con Autómatas Programables (II)

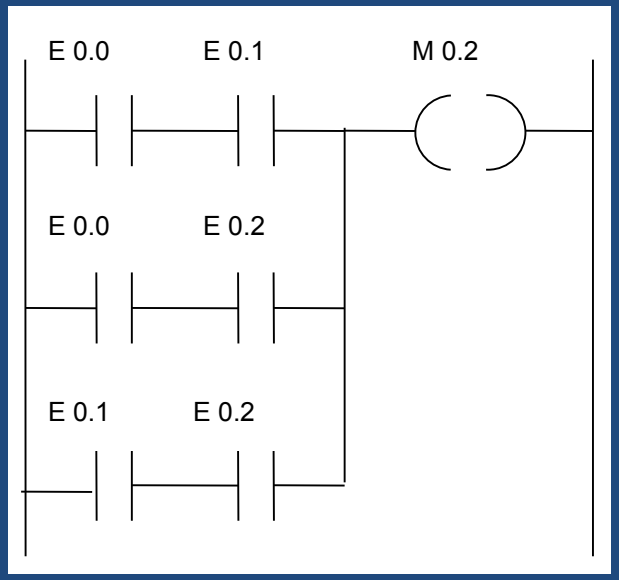
FALLOS AUTÓMATA

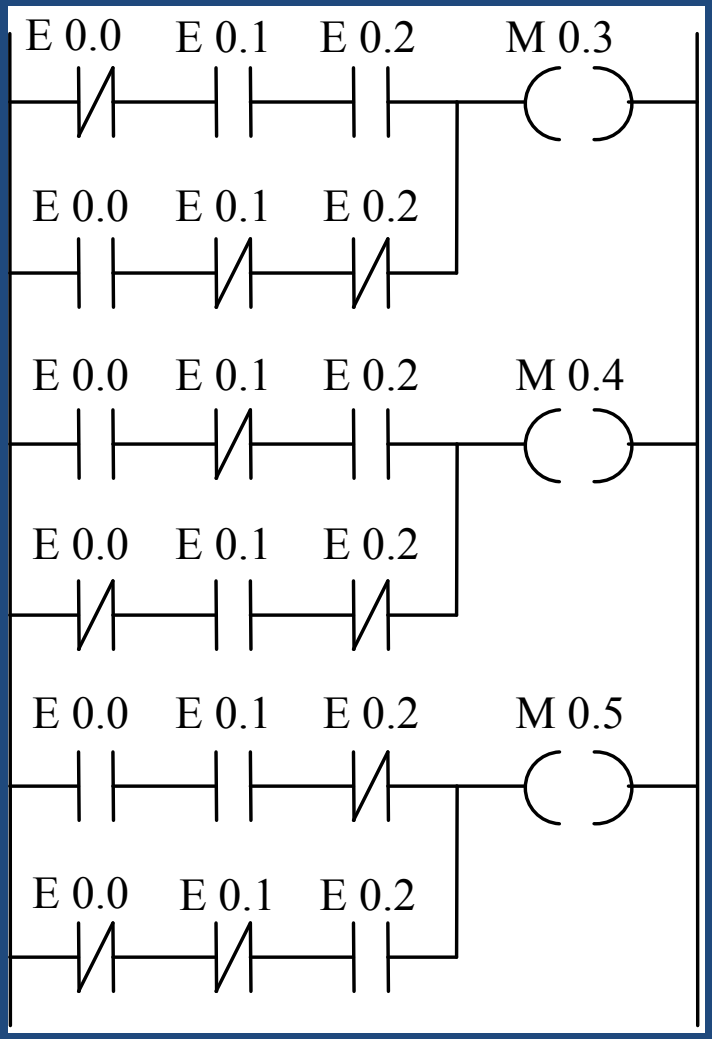
- CPU + FUENTE DE ALIMENTACIÓN: 10%
  - CPU: 10%
  - FUENTE DE ALIMENTACIÓN: 90%
- ENTRAS/SALIDAS: 90%

Seguridad en la CPU



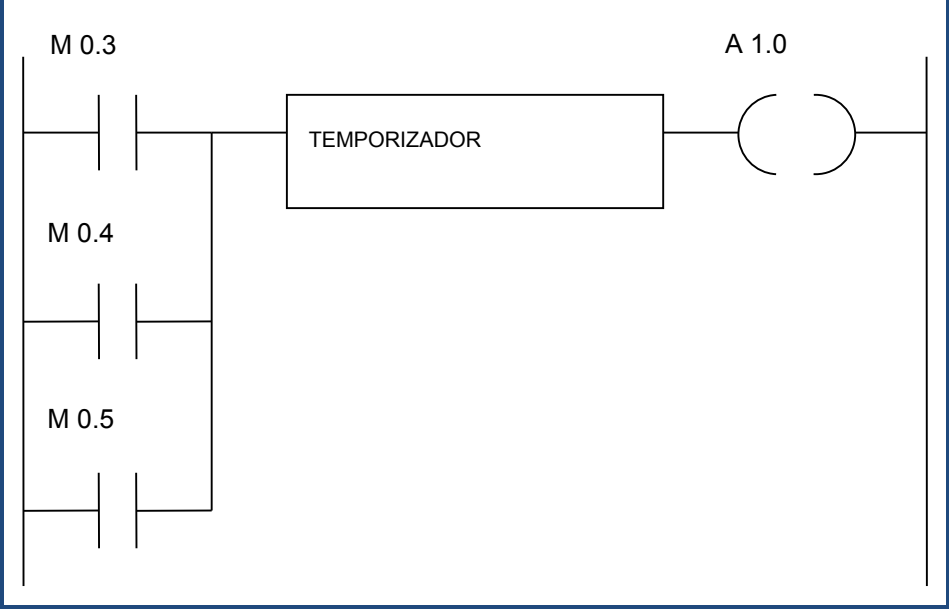
Seguridad en las entradas (I)





Seguridad en las entradas (II)

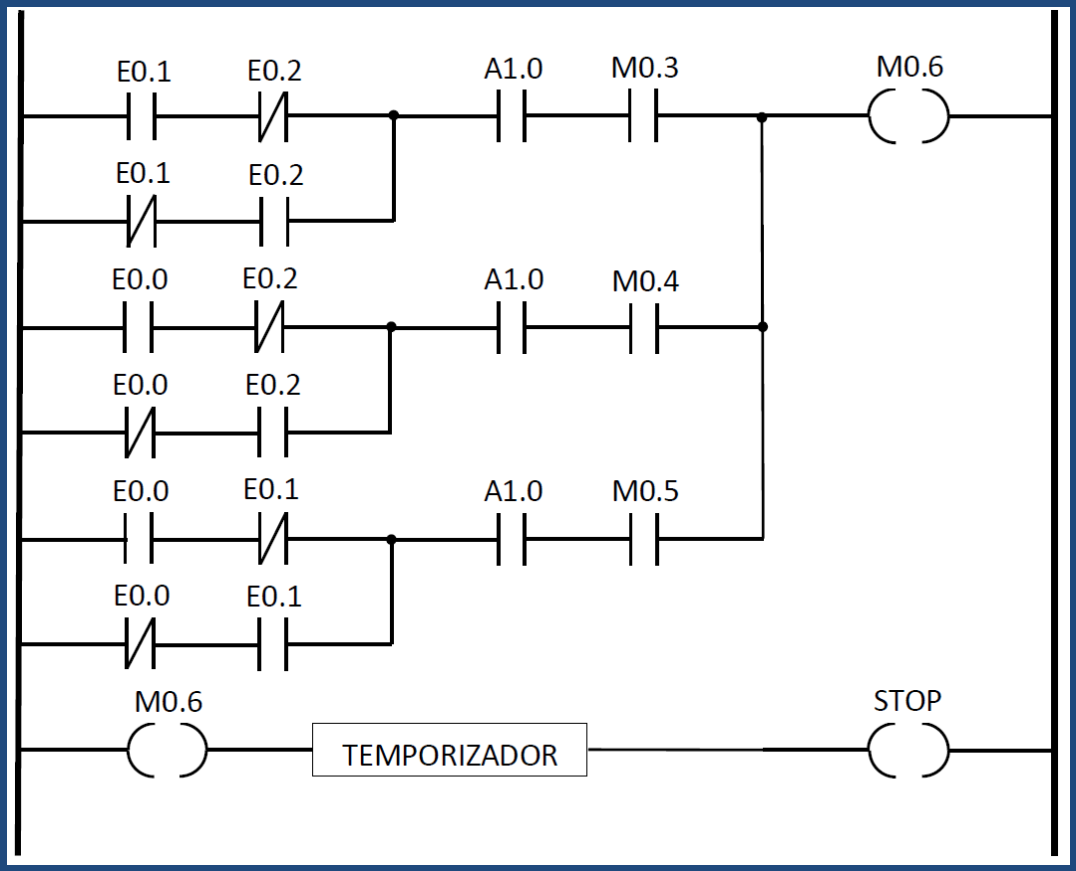
SEÑALIZACIÓN DE AVERÍA



Seguridad en las entradas (III)

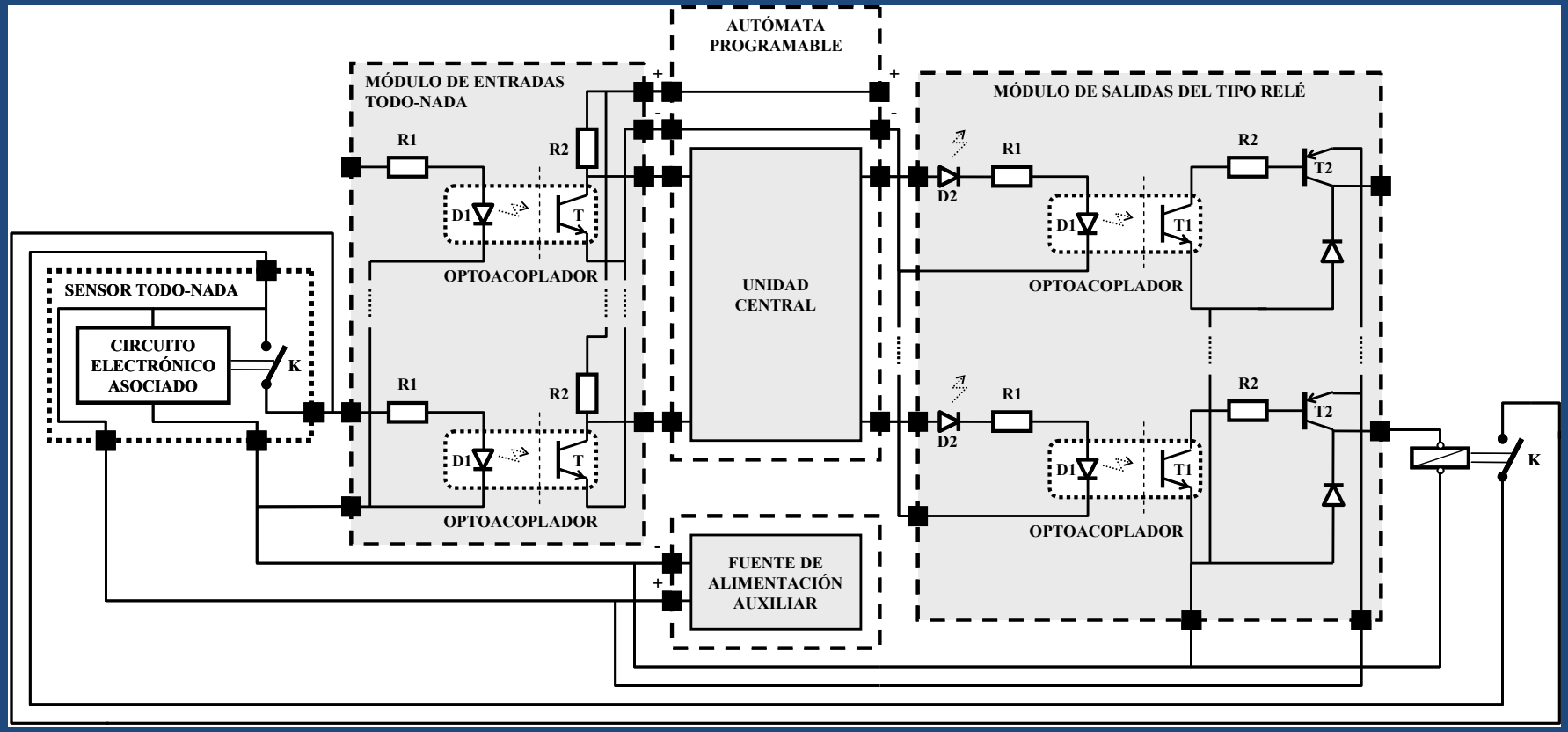
SISTEMA 2oo3

FALLO DE DOS ENTRADAS => STOP



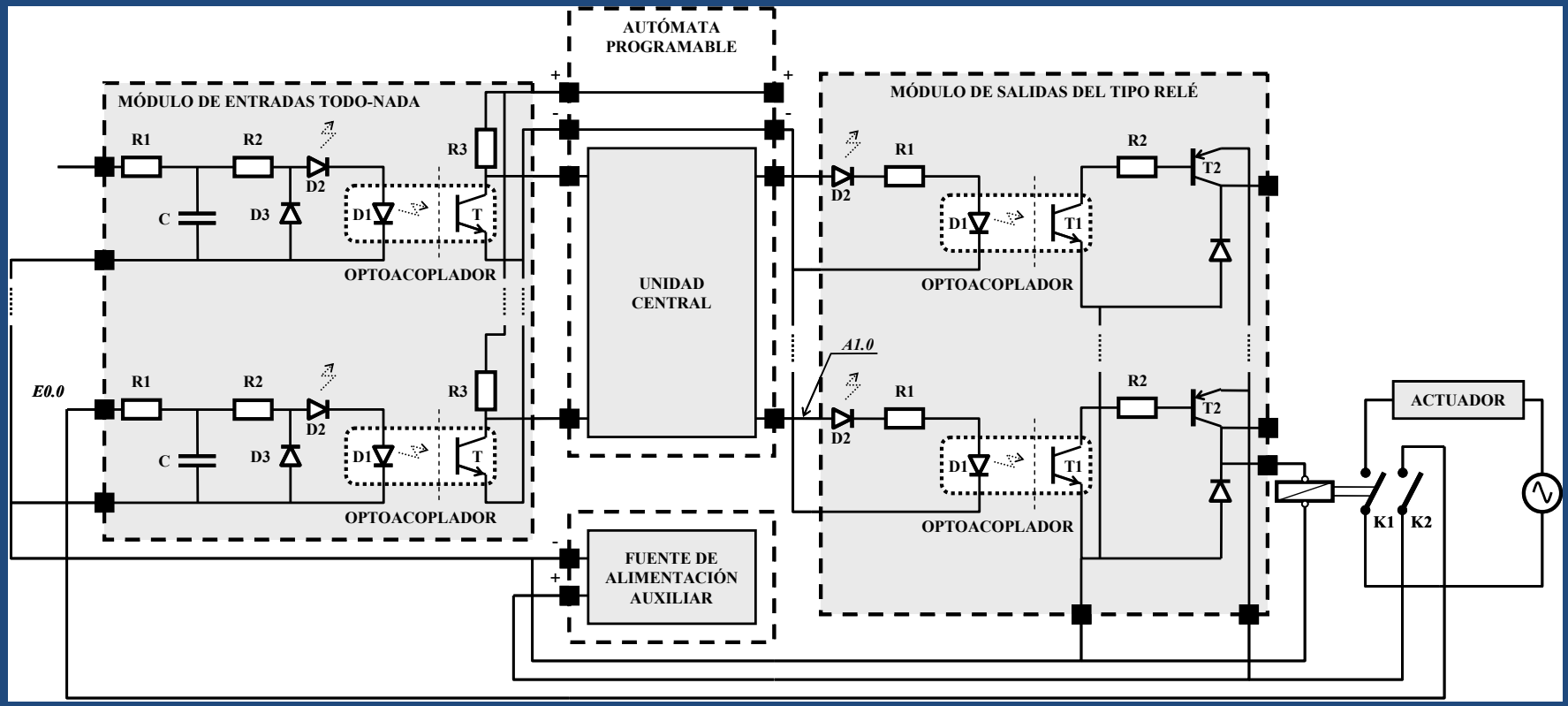
Seguridad en las entradas (IV)

COMPROBACIÓN DE ENTRADAS



Seguridad en las salidas

COMPROBACIÓN DE SALIDAS CRÍTICAS



APLICACIONES EDUCATIVAS

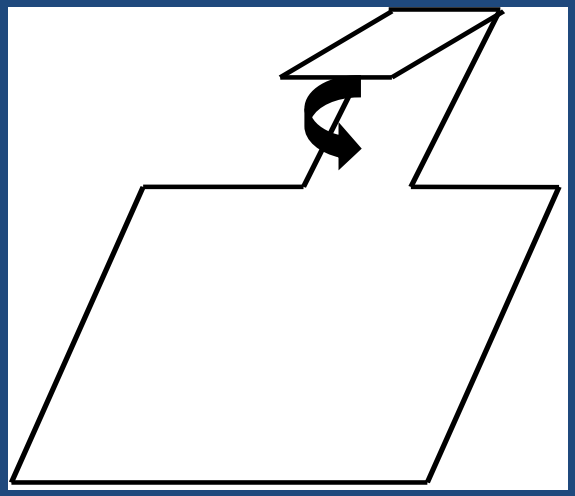
Sensores educativos de bajo coste

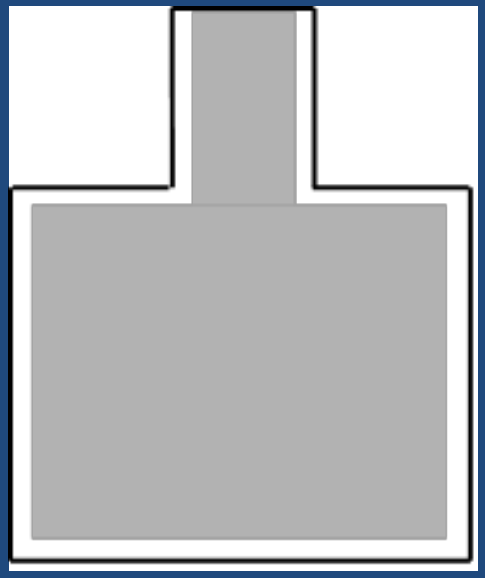
- **Sensores de nivel**
  - Sensores capacitivos planos
  - Sensores capacitivos cilíndricos
- **Sensores de proximidad**
  - Sensores capacitivos abiertos

Aplicaciones multimedia

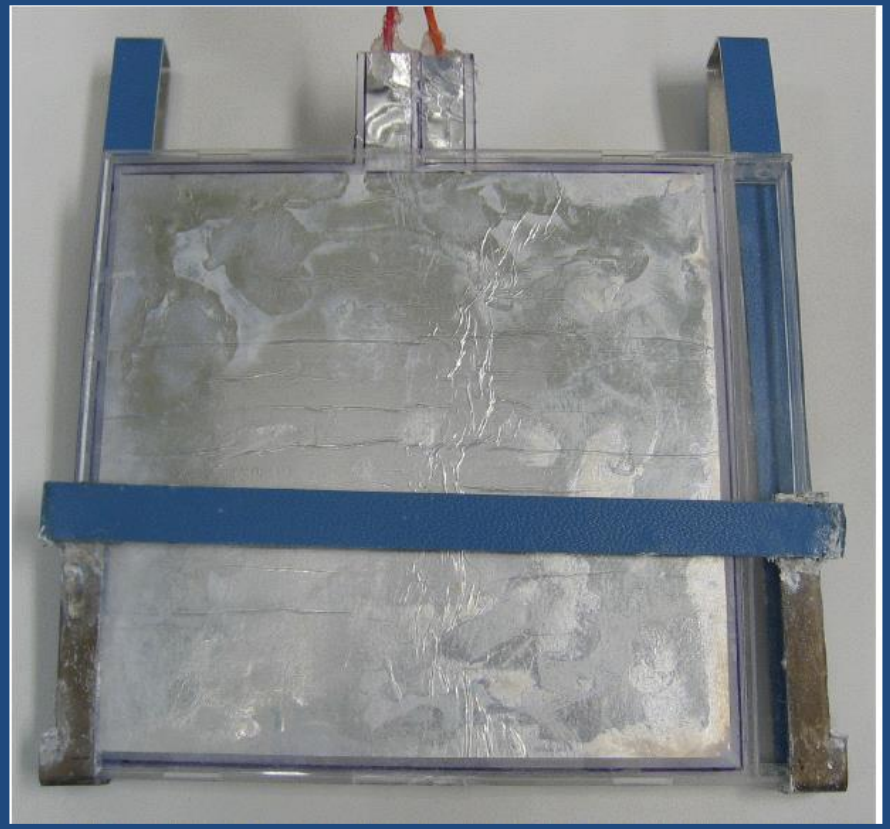
Sensores capacitivos planos (I)

Placas formadas por papel de aluminio (*albal)* plastificado y ubicadas en la caja de un CD



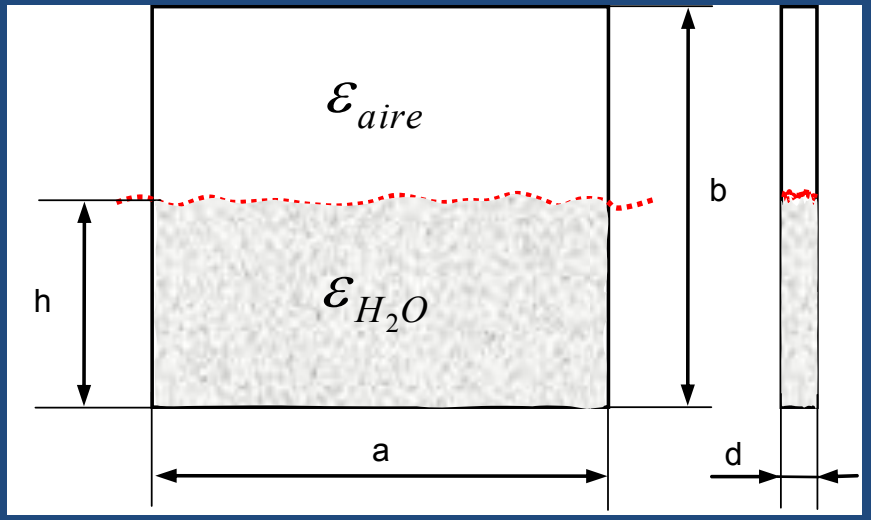


Sensores capacitivos planos (II)



Sensores capacitivos planos (III)

Medida de nivel

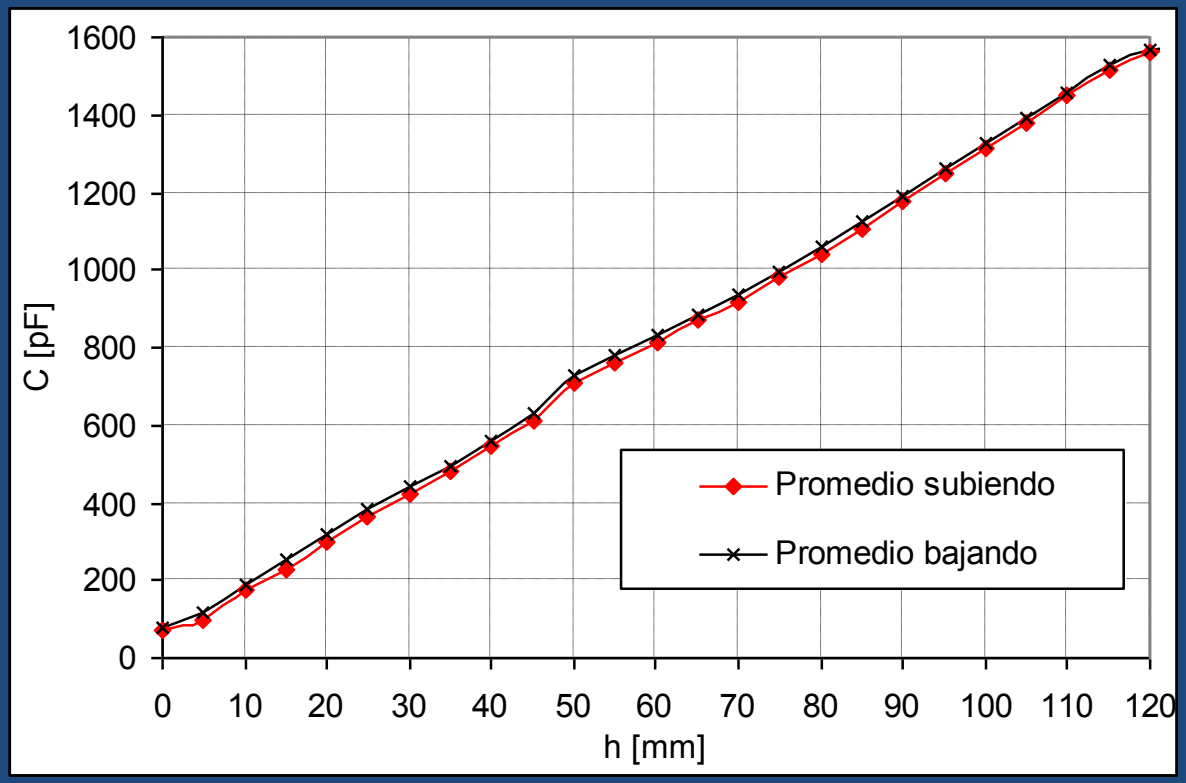


$$C_{Total} \cong C_{aire} + C_{líquido} = \varepsilon_{líquido} \cdot \frac{a \cdot h}{d} + \varepsilon_{aire} \frac{a \cdot (b-h)}{d} =$$

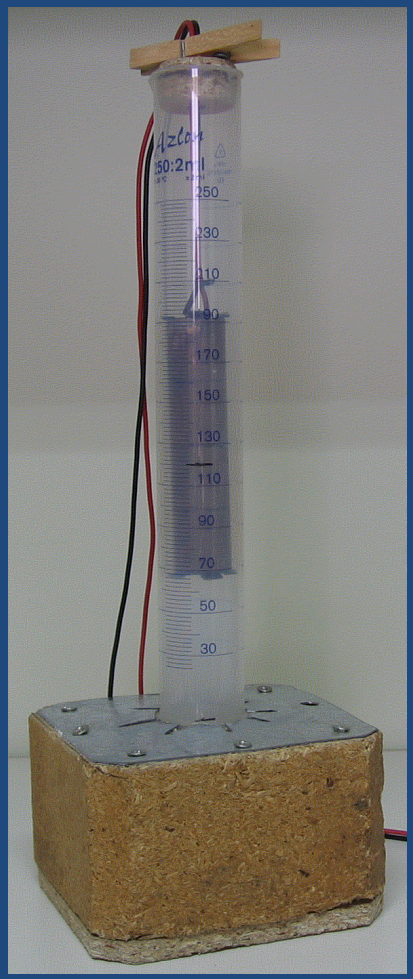
$$\frac{a}{d} \cdot \left[h \cdot (\varepsilon_{líquido} - \varepsilon_{aire}) + \varepsilon_{aire} \cdot b \right]$$

$$h[mm] = 0.0791 \cdot C[pF] - 4.383$$

Sensores capacitivos planos (IV)

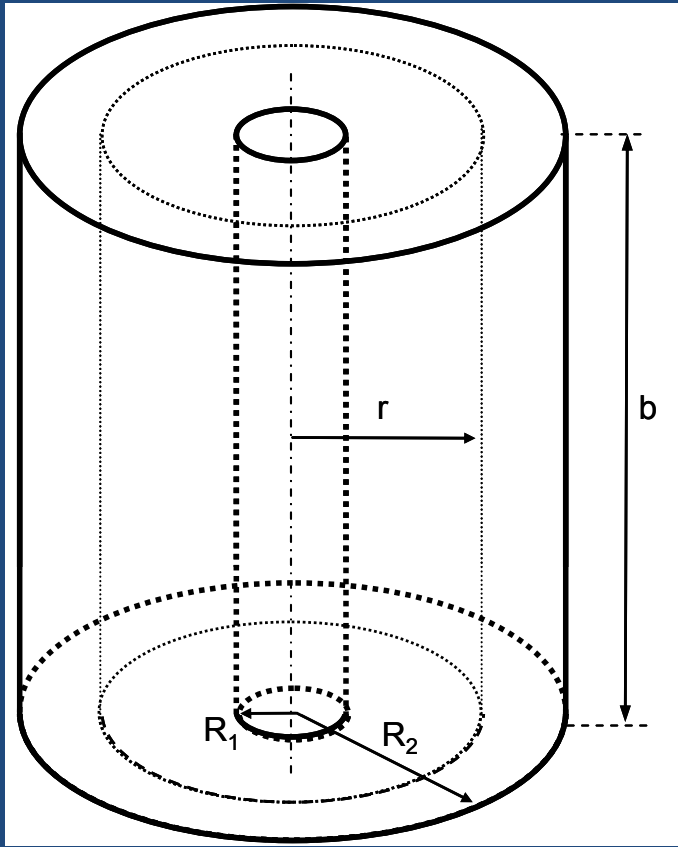


Sensores capacitivos cilíndricos (I)



- Construidos con dos tubos de cobre coaxiales.
  - Tubo exterior => L = 120 mm., D = 27 mm.
  - Tubo exterior => L = 120 mm., D = 17 mm.
- Longitud de la probeta ≈ 240 mm.
- Se utilizan para la medida de nivel de aceite.
- El sensor está suspendido por los propios cables.

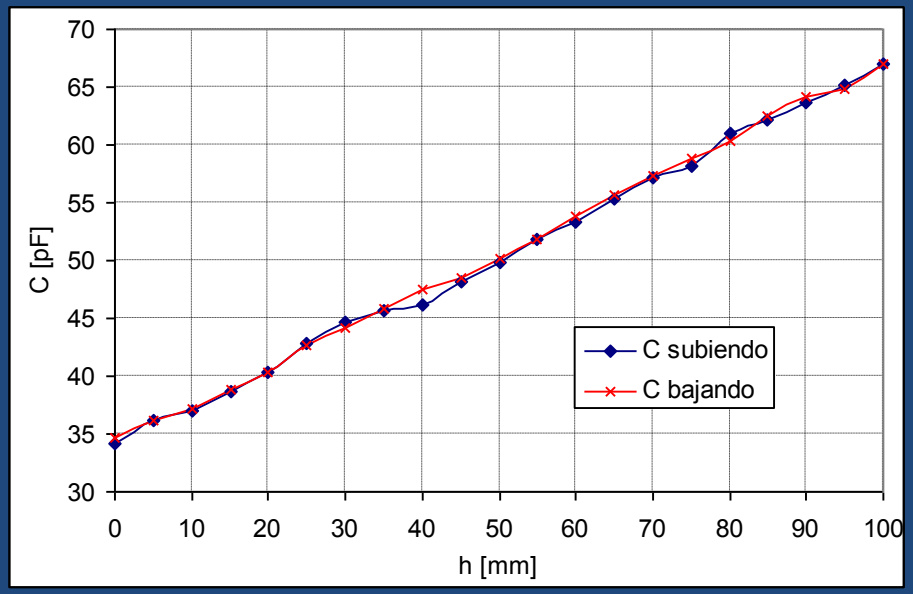
Sensores capacitivos cilíndricos (II)

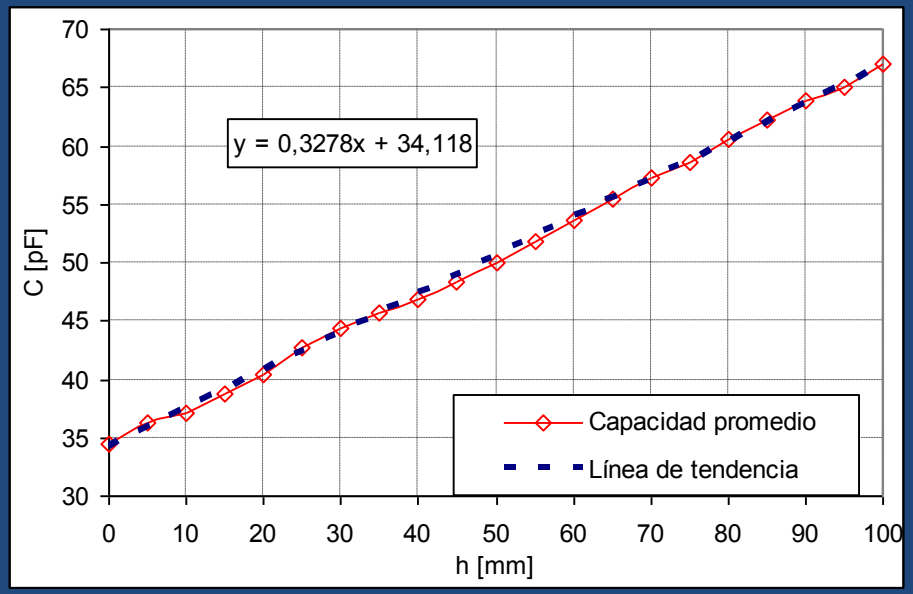


$$C \cong \frac{2 \cdot \pi}{\ln \frac{R_2}{R_1}} \cdot \left[h \cdot \left(\varepsilon_{liquido} - \varepsilon_{aire} \right) + b \cdot \varepsilon_{aire} \right]$$

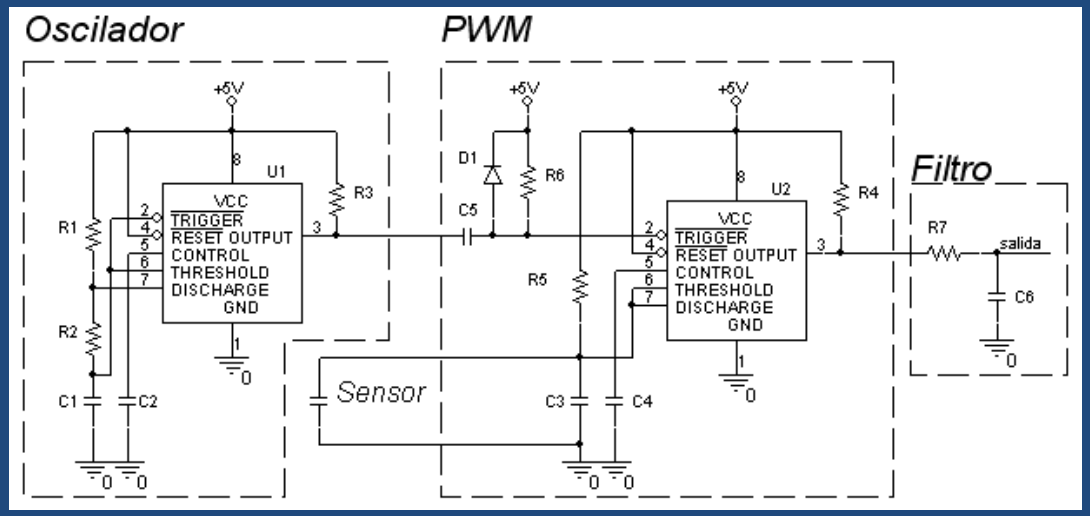
$$h[mm] = 3{,}0506 \cdot C[pF] - 104{,}081$$

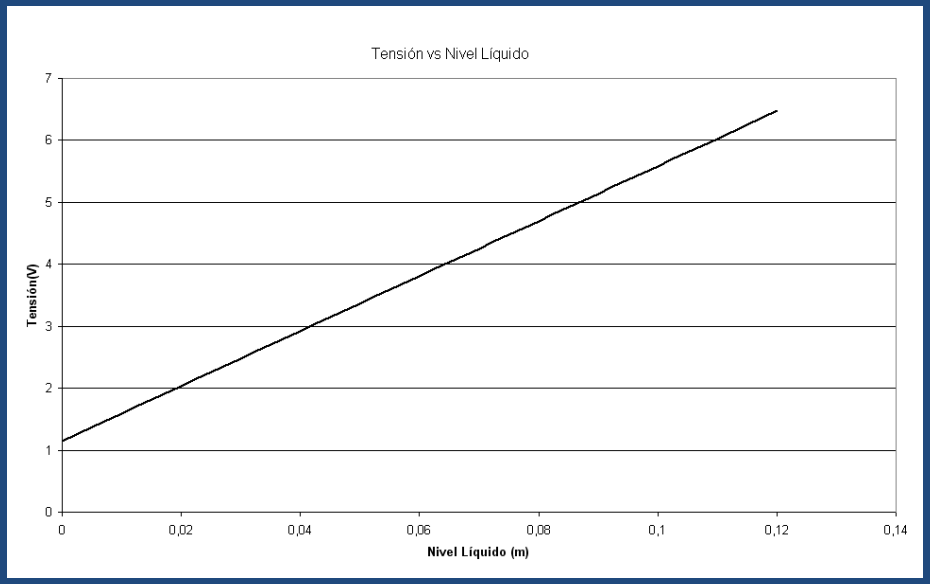
Sensores capacitivos cilíndricos (III)





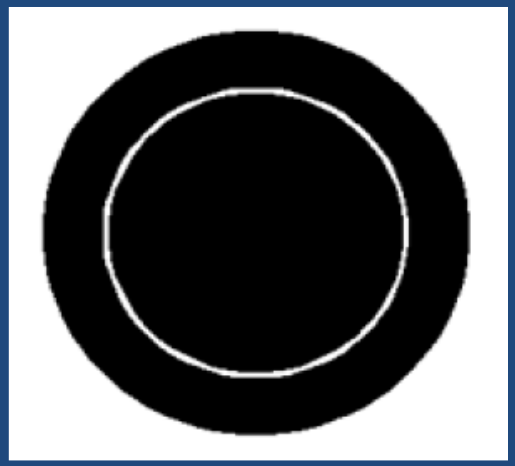
Circuito de acondicionamiento

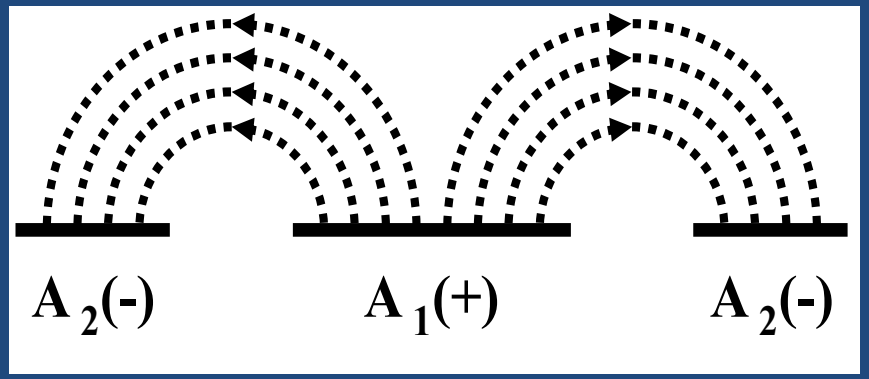


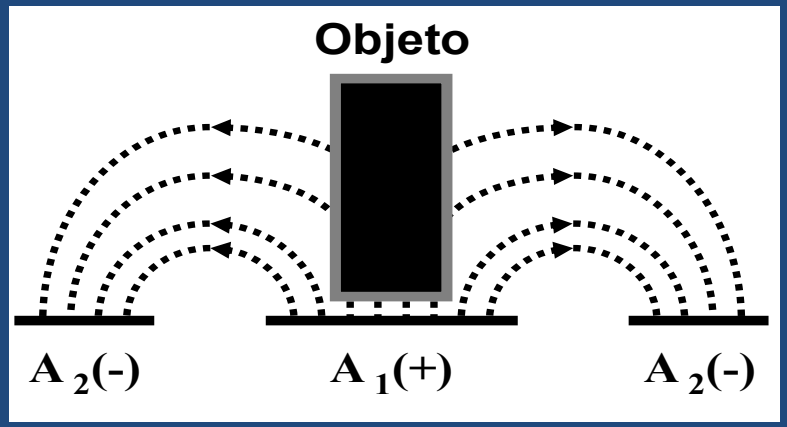


Sensores capacitivos abiertos (I)

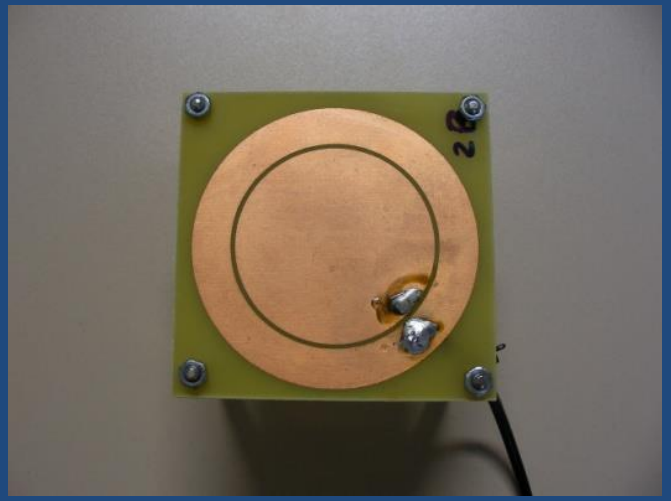
Aplicación: Sensor de proximidad





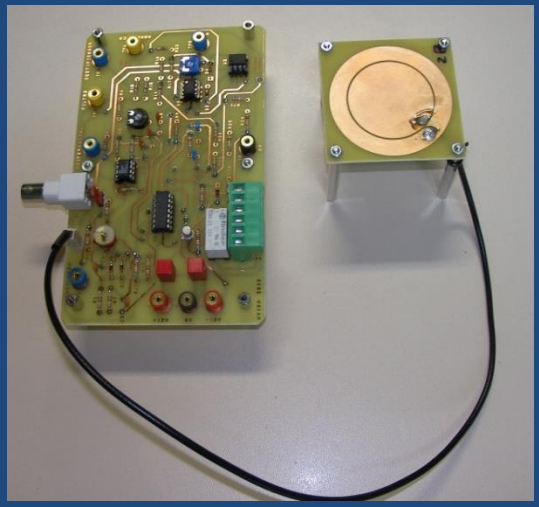


Sensores capacitivos abiertos (II)



	r mm	R mm	d mm	A mm²	Tipo	C [pF]		
						Aire	Madera	Fe
1	10.8	16	1	366	A	6	7	8
					B	15	16	17
2	20	29	1	1256	A	13	14	16
					B	43	48	51
3	29.9	43	1	2808	A	19	20	22
					B	95	96	97

Sensores capacitivos abiertos (III)



Pieza	Grosor	Distancia		
		Se activa	Se desactiva	Media
Metal	1 mm	0.9 mm	1.7 mm	1.3 mm
	6 mm	6.7 mm	11.2 mm	8.95 mm
Madera	3 mm	0.1 mm	0.2 mm	0.15 mm
	6 mm	1.4 mm	1.7 mm	1.55 mm

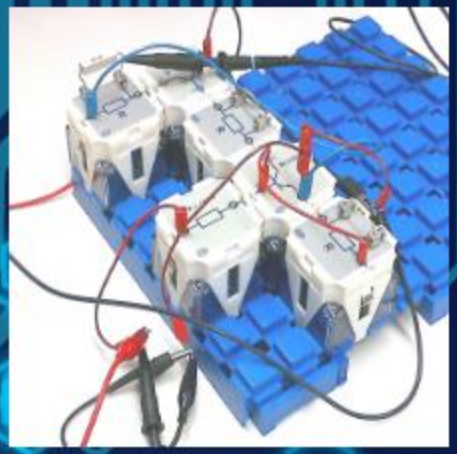
Aplicaciones multimedia

http://aprenderelectronica.webs.uvigo.es/

Web interactiva para el aprendizaje de la Electrónica

Web gratuita y de uso educativo para el aprendizaje y formación en temas relacionados con la **Electrónica**.

Con unos sencillos datos de registro podrás acceder a los contenidos interactivos realizados durante los últimos años por el **Departamento de Tecnoloxía Electrónica de la Universidade de Vigo**.



Iniciar sesión

Usuario acevedo

Password ••••••

Olvide mi contraseña

Enviar

Deseo registrarme

- Convertidores electrónicos de potencia
- Sensores
- Baterías
- Electromagnetismo
- Herramientas
- SAD Sistema de Adquisición de datos

Atrás

¿Qué es Aprender Electrónica?

La enseñanza de las distintas partes de la electrónica resulta una tarea complicada, especialmente con documentación presentada de forma estática. Pero mediante la utilización de herramientas interactivas en las que se muestra a los usuarios, mediante presentaciones dinámicas los conceptos más complicados, se facilita en gran medida esta labor, por lo que el uso de estas aplicaciones autoformativas favorece al alumno y al profesor. El objetivo de estas herramientas no es sustituir a los libros clásicos, sino complementar estos mediante la exposición dinámica de algunos conceptos. Incluso muchas de estas animaciones son aplicaciones interactivas en las que el usuario puede cambiar algunos parámetros y comprobar su efecto.

En nuestro Departamento y a lo largo de los últimos años se han desarrollado un buen número de aplicaciones para la enseñanza de diversos temas relacionados con la formación en electrónica. Estas herramientas están desarrolladas para su utilización vía internet, por lo que el usuario puede hacer uso de ellas en cualquier momento y desde cualquier lugar con conexión a la red. La utilización de estas aplicaciones a lo largo de los últimos años nos han animado a seguir en esta línea, lo que ha dado lugar a que en la actualidad existan un buen número de herramientas sobre distintos temas, aunque mayormente relacionadas con la formación en sensores y en electrónica de potencia.

Sin embargo el número de aplicaciones desarrolladas, así como la variedad de las mismas han aconsejado el desarrollo de una página web específica que incluya todas las herramientas, de forma que se facilite su utilización a cualquier usuario.

Las aplicaciones interactivas desarrolladas se puede agrupar en 5 apartados principales. Con los desplegables de la barra lateral se puede accede a los contenidos:

Convertidores electrónicos de potencia	Sensores Electrónicos
Baterías	Electromagnetismo

Sensores

spositivos muy utilizados en la industria y creemos que la educación y formación en este l para el desarrollo de la actividad profesional de nuestros alumnos. En el aprendizaje de os que es necesario mostrar al estudiante la constitución física, el principio de caciones, la interpretación de las características técnicas de los sensores que aparece en fabricantes, algunos fabricantes, etc.

Sensores de Proximidad

En la aplicación desarrollada se tratan los sensores:

- Capacitivos.
- Inductivos.
- Optoelectrónicos.
- Ultrasónicos.
- Magnéticos.
- Microrruptores.
- Sensores para aplicaciones de seguridad.

Sensores de Caudal

La aplicación presenta los distintos principiosutilizados en este tipo de medidas, así como características y modos de operación de diversos tipos de sensores de caudal. Se incluyen procedimientos de cálculo, aplicaciones y características técnicas dadas por los fabricantes. En la aplicación se tratan los sensores de presión diferencial (placa de orificio, tobera de caudal, tubo Venturi, tubo Pitot y tubo Annubar), los de área variable (rotámetros), caudalímetros de velocidad, térmicos y electromagnéticos físicos.

Sensores de Temperatura

Esta aplicación permite la formación en sensores de temperatura y en la misma se tratan los termopares, las termorresistencias, los termistores y los pirómetros de radiación. Se analizan cuatro tipos de sensores: pirométricos, termorresistencias, termopares y termistores. Además se muestran las características técnicas de otros sensores, sin llegar a profundizar en su estudio. Estos sensores son el bolómetro, el bimetálico y algunos de semiconductores AD590,LM135 yTMP275).

SENSORES DE PROXIMIDAD

Bibliografía

- A. Kumar Verma, S. Ajit, D. Rao Ka. *Reliability and Safety Engineering*. Springer, 2016.
- B. R. Mehta Y. J. Reddy. *Industrial Process Automation Systems Design and Implementation*. Elsevier, 2015.
- J. W. Vincoli. *Basic Guide to System Safety*. Wiley, 2014.
- B. R. Mehta, Y. J. Reddy. *Industrial Process*. Butterworth-Heinemann, 2014.
- D. J. Smith. *Reliability, Maintainability and Risk*. Butterworth Heinemann, 2011.
- A. Creus Solé. *Fiabilidad y seguridad: Su aplicación en procesos industriales*. Marcombo, S.A., 2005.
- E. Nikolaidis, D. M. Ghiocel, S. Singhal. *Engineering Design Reliability Handbook*. CRC Press, 2005.
- D. Kececioglu. *Reliability Engineering Handbook*. DEStech, 2002.
- T.I. Bajenescu, M.I. Bâzu. *Reliability of Electronic Components*. Springer-Verlag, 1999.
- P. Kales, *Reliability*. Prentice-Hall, 1998.
- MIL-HDBK-338B. *Electronic Reliability Design*. Department of Defense. USA, 1998,
- MIL-HDBK-217F, Notice 2. *Reliability Prediction of Electronic Equipment Handbook*. Department of Defense. USA, 1995.

Software

- http://www.reliasoft.es/
- https://www.relexsolutions.com/
- http://www.isograph.com/
- http://www.itemsoft.com/

Webs interesantes

- The Intrernational System Safety Society (http://www.system-safety.org/)
- Society of Reliability Engineers (http://www.sre.org/)
- ASQ Reliability Division (http://asqrd.org/)
- RAC: Reliability Analysis Center (https://global.ihs.com/standards.cfm?publisher=RAC)

MUCHAS GRACIAS POR SU ATENCIÓN

Jorge Marcos Acevedo
Dpto. de Tecnología Electrónica
Universidade de Vigo
acevedo@uvigo.es