Problemas de Rendimiento y Seguridad Funcional

Fco Javier Molina Cantero

23 de mayo de 2012

Problema 1. Defina, justifique y relacione entre sí los siguientes conceptos:

a) $R(t)$ - Función de supervivencia, rendimiento y fiabilidad

b) $\lambda(t)$ - Tasa de fallos

c) $A(t)$ - Disponibilidad en un instante t.

d) $f(t)$ - Función de distribución de fallos

e) $MTFF$ - Tiempo medio al primer fallo.

f) $MTBF$ - Tiempo medio entre fallos.

g) A_{AVG} - Disponibilidad media

SOLUCIÓN:

a) $R(t)$ - Función de supervivencia, rendimiento y fiabilidad. Define la probabilidad de que un dispositivo continúe en funcionamiento trascurrido un tiempo t. Para dispositivos no reparables, este concepto coincide con la disponibilidad.

b) $\lambda(t)$ - Tasa de fallos. Es la proporción de dispositivos que se averían por unidad de tiempo. También se conoce como velocidad de fallos.

c) $A(t)$ - Disponibilidad en un instante t. Mide la probabilidad de que el dispositivo esté en funcionamiento en el instante t. Coincide con la supervivencia en dispositivos no reparables. Difiere en los reparables, ya que en éstos existe probabilidad de funcionamiento tras una reparación.

d) $f(t)$ - Función de distribución de fallos. El producto $f(f)dt$ es la probabilidad (infinitesimal, ya que se trata de una función continua) de que el dispositivo falle entre t y $t + dt$.

e) $MTFF$ - Tiempo medio al primer fallo. Mide el valor medio del instante donde se produce el primer fallo.

f) $MTBF$ - Tiempo medio entre fallos. Concepto aplicable a dispositivos reparables. Mide la distancia media ente fallos. Es la suma del $MTTF$ y el tiempo medio que se encuentra fuera de servicio antes de ser reparado.

g) A_{AVG} - Disponibilidad media. Aplicable a dispositivos reparables. Es la proporción de tiempo que el sistema se encuentra operativo entre fallos. Se estima a través de la siguiente expresión:

$$A_{AVG} = \frac{MTTF}{MTTF + MDT}$$

donde MDT es el tiempo medio fuera de servicio (Mean Down Time).

Problema 2. Calcule la relación entre la función de distribución de fallos f(t), la función de supervivencia R(t), y la tasa de fallos.

SOLUCIÓN:

La función de distribución de fallos $f(t)dt$ mide la probabilidad de que el sistema falle entre t y $t+dt$. Por otro lado $F(t) = 1 - R(t)$ mide la probabilidad de que el dispositivo falle antes del instante t. De todo ello se deduce que:

$$f(t)\Delta t = (F(t+\Delta t) - F(t)) = -(R(t+\Delta t) - R(t))$$

en el límite $\Delta t \to 0$

$$f(t) = -\frac{dR}{dt}$$

La relación entre el rendimiento $R(t)$ y la tasa de fallos:

$$\lambda(t) = -\frac{d}{dt}\left(\ln R(t)\right) = -\frac{1}{R(t)}\frac{dR(t)}{dt}$$

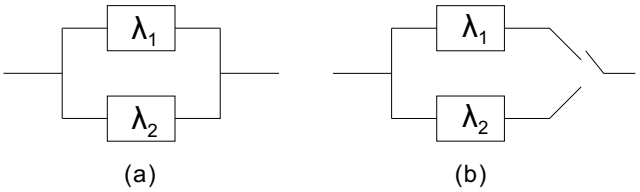
y por tanto,

$$\lambda(t) = \frac{1}{R(t)} f(t)$$

despejando,

$$f(t) = \lambda(t) \cdot R(t)$$

Problema 3. Analice los sistemas redundantes que se muestran en sendas figuras. Justifique en cada caso si se trata de redundancia en caliente o en frío.Comente ventajas e inconvenientes de ambos esquemas.



SOLUCIÓN: El primer esquema (a) corresponde a un sistema con redundancia en caliente, ya que ambos dispositivos están en funcionamiento de forma simultánea.

El segundo corresponde a un esquema con redundancia en frío o mixto. La función es ejecutada por uno sólo de los sistemas. En caso de avería, se conmuta al segundo.

La ventaja de la redundancia en caliente es que ofrece una respuesta en tiempo 0 a fallos de uno de sus elementos. En cambio, el desgaste o envejecimiento temporal afecta por igual a ambos.
En la segunda estructura exsiste un intervalo de tiempo δt sin servicio, pero en cambio, el dispositivo auxiliar se encuentra en día cero (nuevo).

Problema 4. Imagine un sistema compuesto por dos dispositivos EMS simples, cuyas tasas de fallos son respectivamente λ_1 y λ_2. Suponga que se instalan en funcionamiento y «nuevos». Calcule los siguientes datos:

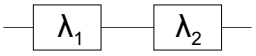
a) Probabilidad de que transcurrido un tiempo t, esté averiado alguno de ellos.

b) Probabilidad de que nos encontremos ambos averiados simultáneamente en un instante t.

c) Probabilidad de que se averíen exactamente en $t = T_0$.

d) Probabilidad de que ambos se averíen entre T_0 y T_1.

e) Suponiendo que la función que soportan ambos dispositivos tiene el diagrama de rendimiento de la figura, calcule cuál es la probabilidad de fallo de la funcionalidad del sistema.



SOLUCIÓN:

a) *Probabilidad de que transcurrido un tiempo t, esté averiado alguno de ellos.*

Si R(t) es la función de supervivencia, entonces, la probabilidad de que en t se encuentre averiado es la de que no haya sobrevivido, es decir, que se averíe en t o antes. Por tanto:

$$F(t) = 1 - R(t)$$

Y la probabilidad de que sobrevivan ambos simultáneamente

$$R(t) = R_1(t) \cdot R_2(t)$$

En consecuencia:

$$F(t) = 1 - R_1(t) \cdot R_2(t)$$

b) *Probabilidad de que nos encontremos ambos averiados simultáneamente en un instante t.*

Teniendo en cuenta que la avería de cada uno de ellos es estadísticamente independiente, entonces la coincidencia de ambas se expresa como:

$$F_{AB}(t) = F_A(t) \cdot F_B(t) = [1 - R_A(t)] \cdot [1 - R_B(t)]$$

c) *Probabilidad de que se averíen exactamente en $t = T_0$.*

Cero. f(t) es una función de distribución continua. La probabilidad en un valor t exacto es un infinitesimal $f(t) \cdot dt$.

d) *Probabilidad de que ambos se averíen entre T_0 y T_1.*

La probabilidad de que un dispositivo se averíe entre T_0 y T_1 sería $F(T_1) - F(T_0)$.
Por tanto, que coincidan entre ambos instantes será:

$$\begin{aligned} F(T_0 - T_1)_{AB} &= [F_A(T_1) - F_A(T_0)] \cdot [F_B(T_1) - F_B(T_0)] \\ &= [R_A(T_0) - R_A(T_1)] \cdot [R_B(T_0) - R_B(T_1)] \end{aligned}$$

e) *Suponiendo que la función que soportan ambos dispositivos tiene el diagrama de rendimiento de la figura, calcule cuál es la probabilidad de fallo de la funcionalidad del sistema.*

Al tratarse de una función de rendimiento serie, es necesario que ambas funcionen simultáneamente para que lo haga el conjunto. Es decir:

$$R_{2oo2}(t) = R_A(t) \cdot R_B(t)$$

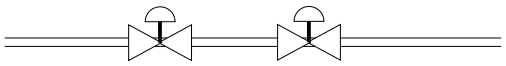
Y en consecuencia, la probabilidad de que se averíe será:

$$F_{2oo2}(t) = 1 - R_A(t) \cdot R_B(t)$$

Problema 5. Las válvulas del circuito de la figura tienen las tasas de fallo a la apertura y al cierre que se muestran en la tabla.

a) Calcule la probabilidad de que falle la función «*Cerrar el flujo*» a lo largo del primer año de uso.

b) Repita el ejercicio si la función que se ejecuta es «*Abrir el flujo*».



λ_A	λ_C
10^{-4}	$1{,}5 \cdot 10^{-4}$

SOLUCIÓN:

a) *Calcule la probabilidad de que falle la función* «Cerrar el flujo» *a lo largo del primer año de uso.*
Para cerrar el flujo con la conexión en serie de las válvulas, bastará con que una de ellas ejecute el cierre. Por tanto, desde el punto de vista del rendimiento, se trata de una estructura redundante *1oo2*.
La probabilidad de fallo antes de t sería:

$$\begin{aligned} F_{1oo2}(t) &= F_c \cdot F_c = \\ &= \left(1 - e^{-\lambda_c \cdot t}\right) \cdot \left(1 - e^{-\lambda_c \cdot t}\right) \\ &= \left(1 - e^{-\lambda_c t}\right)^2 \end{aligned}$$

Teniendo en cuenta que un año son aproximadamente $10^4 horas$

$$\begin{aligned} F_{1oo2}(t) &= \left(1 - e^{-\lambda_c t}\right)^2 \\ &= \left(1 - e^{-1{,}5 \cdot 10^{-4} \cdot 10^4}\right) \\ &= (1 - 0{,}22)^2 = 0{,}6 \\ F_{1oo2} &= 60\,\% \end{aligned}$$

** Si se compara con el de un dispositivo simple $1 - e^{-\lambda_c t} = 1 - 0{,}22 = 0{,}78$ puede obervarse cómo se reduce la probabilidad de fallo.

b) *Repita el ejercicio si la función que se ejecuta es* «Abrir el flujo».
En este caso, para que se abra el conjunto, deben hacerlo simultáneamente ambas válvulas. Por tanto, desde el punto de vista del rendimiento se trata de una estructura 2oo2.
La probabilidad de que el conjunto 2oo2 funciones correctamente antes del instante t es:

$$R_{2oo2}(t) = e^{-\lambda_a \cdot t} \cdot e^{-\lambda_a \cdot t} = e^{-2\lambda_a \cdot t}$$

Y la probabilidad de que falle antes de t:

$$F_{2oo2} = 1 - R_{2oo2}(t) = 1 - e^{-2\lambda_a \cdot t}$$

Como 1 año son $\approx 10^4$ horas.

$$\begin{aligned} F_{2oo2}(t) &= 1 - e^{-2\lambda_a t}|_{t=10^4 h} \\ &= 1 - e^{-2 \cdot 10^{-4} \cdot 10^4} = 0,86 \\ F_{2oo2} &= 86\,\% \end{aligned}$$

** En este caso, el fallo del conjunto es más probable que el de un dispositivo simple, aunque podrá observar que tampoco es el doble.

Problema 6. Calcule la función de rendimiento de una estructura 1oo2. Estime además la tasa de fallos de la misma. Extienda el resultado a 1ooN

SOLUCIÓN: Una estructura 1oo2 fallará cuando fallen simultáneamente los dos dispositivos. Es decir:

$$F_{1oo2}(t) = F_1(t) \cdot F_2(t) =$$

El rendimiento por tanto,

$$\begin{aligned} R_{1oo2}(t) &= 1 - F_{1oo2}(t) = 1 - (1 - e^{-\lambda_1 \cdot t}) \cdot (1 - e^{-\lambda_2 \cdot t}) \\ &= 1 - (1 - e^{-\lambda_1 \cdot t} - e^{-\lambda_2 \cdot t} + e^{-(\lambda_1 + \lambda_2) \cdot t}) \\ &= e^{-\lambda_1 \cdot t} + e^{-\lambda_2 \cdot t} - e^{-(\lambda_1 + \lambda_2) \cdot t} \end{aligned}$$

De la expresión se deduce claramente que el conjunto no tienen la misma evolución temporal de los dispositivos sin redundancia (NooN), es decir, no sigue una exponencial simple $e^{-\lambda \cdot t}$

Para calcular una tasa de fallos equivalente, se recurre a la expresión que la relaciona con el tiempo medio al primer fallo:

$$MTFF = \frac{1}{\lambda}$$

Partiendo de la definición, y de los resultados de teoría:

$$\begin{aligned} MTFF &= \int_0^\infty t \cdot f(t) \cdot dt = \int_0^\infty R(t) \cdot dt \\ &= \int_0^\infty e^{-\lambda_1 \cdot t} \cdot dt + \int_0^\infty e^{-\lambda_2 \cdot t} \cdot dt - \int_0^\infty e^{-(\lambda_1 + \lambda_2) \cdot t} \end{aligned}$$

$$MTTF = \frac{1}{\lambda_{eq}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

Problema 7. Repita el ejercicio para una estructura 2/3.

SOLUCIÓN: Una estructura en votación tipo 2oo3, requiere que funcionen 2 o 3 dispositivos para que el conjunto también lo haga. Por tanto,

$$\begin{aligned} R_{2oo3}(t) = {} & R_1(t) \cdot R_2(t) \cdot [1 - R_3(t)] + \\ & R_1(t) \cdot [1 - R_2(t)] \cdot R_3(t) + \\ & [1 - R_1(t)] \cdot R_2(t) \cdot R_3(t) + \\ & R_1(t) \cdot R_2(t) \cdot R_3(t) \end{aligned}$$

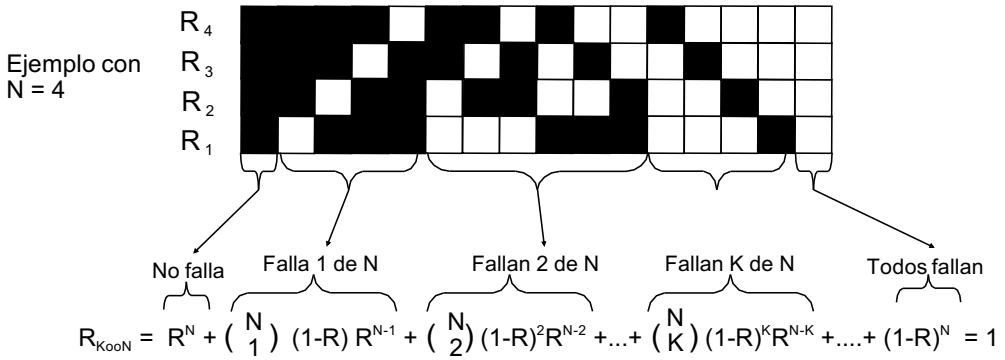
$$\begin{aligned} R_{2oo3}(t) &= R_1(t) \cdot R_2(t) + R_1(t) \cdot R_3(t) + R_2(t) \cdot R_3(t) - 2 \cdot R_1(t) \cdot R_2(t) \cdot R_3(t) \\ &= e^{-(\lambda_1+\lambda_2)t} + e^{-(\lambda_1+\lambda_3)t} + e^{-(\lambda_2+\lambda_3)t} - 2e^{(\lambda_1+\lambda_2+\lambda_3)t} \end{aligned}$$

La tasa de fallos equivalente se obtendría integrando la función de rendimiento

$$\begin{aligned} MTTF = \frac{1}{\lambda_{EQ}} &= \int_0^\infty R(t) \cdot dt \\ &= \frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \frac{1}{\lambda_1 + \lambda_3} - \frac{2}{\lambda_1 + \lambda_2 + \lambda_3} \end{aligned}$$

Problema 8. Para una estructura de votación NooM, calcule la probabilidad de supervivencia, la probabilidad de fallo, y el tiempo medio al primer fallo.Suponga que todos los dispositivos son iguales.

SOLUCIÓN: Para que funcione una estructura redundante R_{NooM} deben funcionar como mínimo N de los M elementos. Si suponemos que todos los elementos son iguales.
En la figura, se muestran todas las combinaciones para N=4.



Que funcionen al menos K incluyen los casos de que funcionen todos, todos menos 1, etc. Por tanto:

$$\begin{aligned} R_{KooN}(t) &= R^M(t) + \binom{N}{1} R^{N-1}\dot{(}1-R) + \binom{N}{2} R^{N-2}\dot{(}1-R)^2 + \ldots + \\ &+ \binom{N}{K-1} R^{N-K+1}\dot{(}1-R)^{K-1} + \binom{N}{K} R^{N-K}\dot{(}1-R)^K \\ &= \sum_{i=0}^{K} \binom{N}{i} \cdot R^{N-i} \cdot (1-R)^i \end{aligned}$$

Problema 9. Estudie las tablas de restricciones de arquitectura de las normas IEC-61508 e IEC-61511 y conteste a las cuestiones que se plantean:

a) En general, ¿para qué dispositivos es más restrictiva la norma IEC 61508?. Encuentre una justificación.

b) Para diferentes niveles de calidad, compare las restricciones de impuestas a los dispositivos programables de la norma IEC 61511 con los de la norma IEC 61508.

c) Responda razonadamente si los dispositivos no programables de la norma IEC 61511 corresponden con los simples de la IEC 61508.

d) Compare razonadamente las restricciones sobre dispositivos no programables de la IEC 61511 y los correspondientes en la IEC 61508. Incluya en el estudio los casos de reducción o incremento del HFT contemplado en la primera.

Tabla 1. IEC 61508. Dispositivos tipo A (simples).

	Tolerancia a Fallos Hardware		
SFF	**0**	**1**	**2**
SFF < 60%	SIL1	SIL2	SIL3
60% < SFF < 90%	SIL2	SIL3	SIL4
90% < SFF < 99%	SIL3	SIL4	SIL4
99% > SFF	SIL3	SIL4	SIL4

Tabla 2. IEC 61508. Dispositivos tipo B (complejos)

SFF	**Tolerancia a Fallos Hardware**		
	0	**1**	**2**
SFF < 60%	---	SIL1	SIL2
60% < SFF < 90%	SIL1	SIL2	SIL3
90% < SFF < 99%	SIL2	SIL3	SIL4
99% > SFF	SIL3	SIL4	SIL4

Tabla 3. IEC 61511. Sensores, actuadores y dispositivos lógicos no programables (non-PE LS)

SIL	**1**	**2**	**3**	**4**
HFT	0	1	2	---

Tabla 4. IEC 61511. Dispositivos lógicos programables (PE-LS)

SIL	**HFT Mínimo**		
	SFF < 60%	SFF de 60% a 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	No aplicable		

SOLUCIÓN:

a) *En general, ¿para qué dispositivos es más restrictiva la norma IEC 61508?. Encuentre una justificación.*

Si se comparan por diferentes niveles de calidad se observa que los dispositivos simples (tipo A) alcanzan un nivel mayor de integridad (SILx+1) que los complejos (SILx), salvo cuando $SFF > 99\,\%$ donde coinciden.
Este resultado se justifica en que por definición, los modos de fallo de los dispositivos simples pueden ser determinados completamente por el fabricante. En este sentido, se consideran más fiables.

b) *Para diferentes niveles de calidad, compare las restricciones de impuestas a los dispositivos programables de la norma IEC 61511 con los de la norma IEC 61508.*
Mientras que la norma IEC 61508 habla de dispositivos simples y complejos, la IEC diferencia entre dispositivos lógicos programables (PE LS) por un lado, y lógicos no programables (non-PE LS), sensores y actuadores, por otro. Desde el punto de vista de la IEC 61508, los dispositivos lógicos programables son de tipo complejo. Por tanto, se deben comparar sendas tablas.

Para facilitar esta comparativa vamos a transformar la tabla de la norma IEC 61511 para que represente el máximo SIL alcanzable, del mismo modo como lo hace la IEC 61508.

SIL	HFT mínimo		
	SFF < 60%	SFF de 60% a 90%	SFF >= 90%
SIL1	1	0	0
SIL2	2	1	0
SIL3	3	2	1
SIL4	No aplicable		

SFF	HFT			
	0	1	2	3
SFF < 60%	---	SIL1	SIL2	SIL3
60% <=SFF < 90%	SIL1	SIL2	SIL3	SIL3
SFF >= 90%	SIL2	SIL3	SIL3	SIL3

La comparación entre ambas tablas queda ahora como sigue:

IEC 61508. Restricciones para dispositivos complejos

SFF	HFT		
	0	1	2
SFF < 60%	---	SIL1	SIL2
60% <= SFF < 90%	SIL1	SIL2	SIL3
90% <= SFF < 99%	SIL2	SIL3	SIL4
99% < SFF	SIL3	SIL4	SIL4

IEC 61511. Restricciones para dispositivos lógicos programables

SFF	HFT			
	0	1	2	3
SFF < 60%	---	SIL1	SIL2	SIL3
60% <=SFF < 90%	SIL1	SIL2	SIL3	SIL3
SFF >= 90%	SIL2	SIL3	SIL3	SIL3

1.- El estándar IEC 61508 permite alcanzar hasta SIL4, el IEC 61511 no.

2.- EL 61511 no trata de forma especial los dispositivos con $SFF > 99\,\%$ (alta calidad). Para éstos, la norma es más restrictiva que la IEC 61508.

3.- Para dispositivos con $SFF < 90\,\%$ y tolerancias a fallos $HFT = 0, 1, 2$, ambas tablas coinciden.

4.- IEC 61511 permite construir estructuras con redundancia cuádruple (HFT=3) facilitando que dispositivos de menor calidad puedan alcanzar niveles SIL superiores a los que le permite la IEC 61508 (p.e con $SFF < 60\,\%$ y HFT $= 3$).

c) *Responda razonadamente si los dispositivos no programables de la norma IEC 61511 corresponden con los simples de la IEC 61508.*
No todos los sensores y actuadores pueden ser considerados dispositivos simples o de tipo A. Los transmisores de señal, por ejemplo, se consideran complejos. También los dispositivos lógicos no programables (non-PE LS) son complejos según la IEC 61508.

d) *Compare razonadamente las restricciones sobre dispositivos no programables de la IEC 61511 y los correspondientes en la IEC 61508. Incluya en el estudio los casos de reducción o incremento del HFT contemplado en la primera.*
Igual que en los apartados anteriores, vamos a transformar la tabla de restricciones hardware para estos dispositivos, añadiendo los casos $SFF < 50\,\%$ y «proven-in-use».

IEC 61511. Sensores, actuadores y disp. lógicos no programables.

	HFT			
SIL	SIL1	SIL2	SIL3	SIL4
HFT	0	1	2	---

SFF	HFT			
	0	1	2	3
SFF < 50%	---	SIL1	SIL2	SIL3
50% <=SFF	SIL1	SIL2	SIL3	SIL3
50% <=SFF "Proven –in-use"	SIL2	SIL3	SIL3	SIL3

* 50% <=SFF indica un modo dominante de fallos seguros

Basándonos en el análisis del apartado anterior, compararemos por un lado los sensores y actuadores que puedan considerarse simples, y por otro los complejos (transmisores de señal, dispositivos lógicos programables o no, etc). SIL4 está excluido

de la norma IEC 61511, por tanto no lo tendremos en cuenta en los razonamientos. Tampoco tiene en cuenta si se trata de dispositivos extremadamente seguros ($SFF > 99\,\%$)

IEC 61508. Restricciones para dispositivos simples

SFF	HFT		
	0	1	2
SFF < 60%	SIL1	SIL2	SIL3
60% <= SFF < 90%	SIL2	SIL3	SIL4
90% <= SFF < 99%	SIL3	SIL4	SIL4
99% < SFF	SIL3	SIL4	SIL4

IEC 61508. Restricciones para dispositivos complejos

SFF	HFT		
	0	1	2
SFF < 60%	---	SIL1	SIL2
60% <= SFF < 90%	SIL1	SIL2	SIL3
90% <= SFF < 99%	SIL2	SIL3	SIL4
99% < SFF	SIL3	SIL4	SIL4

IEC 61511. Sensores, actuadores y disp. lógicos no programables.

SFF	HFT			
	0	1	2	3
SFF < 50%	---	SIL1	SIL2	SIL3
50% <=SFF	SIL1	SIL2	SIL3	SIL3
50% <=SFF "Proven –in-use"	SIL2	SIL3	SIL3	SIL3

Caso 1) Sensores y actuadores (IEC 61511) simples según IEC 61508.
En general, IEC 61511 es más restrictiva. Tan sólo los dispositivos seguros que cumplan las condiciones «proven-in-use» tienen las mismas restricciones que los seguros de la IEC 61508 ($SFF >= 60\,\%$).
Para dispositivos no seguros ($SFF <= 50\,\%$) IEC 61511 obliga a utilizar un nivel más de redundancia que la IEC 61508.
Los dispositivos seguros ($SFF > 50\,\%$) que no cumplen las condiciones «proven-in-use» se les exhige las mismas restricciones que a los inseguros de la IEC-61508 ($SFF < 60\,\%$).
Tan sólo el caso de dispositivos «proven-in-use» simples y con $50\,\% < SFF < 60\,\%$ la IEC 61511 es menos restrictiva.

Caso 2) Sensores y actuadores complejos, dispositivos lógicos programables y no programables.
En general, la IEC 61511 es algo menos restrictiva que la IEC 61508. Excepto por los límites de la SFF, las

restricciones entre ambas tablas coinciden para los inseguros y seguros sin certificado «proven-in-use». En cambio, los dispositivos «proven-in-use» de la IEC 61511 tienen las mismas restricciones que los complejos muy seguros de la norma IEC 61508 ($90\,\% < SFF < 99\,\%$. Es decir, en la primera se permite el uso de dispositivos de menor calidad para alcanzar los mismos niveles de integridad que la segunda.

Problema 10. En la siguiente tabla se muestran los datos de rendimiento de un detector de presión, con el que se van a diseñar medidas de seguridad SIS.

$$\text{MTTF} = 150 \text{ años, SFF} = 90\,\%$$
$$\text{DCF} = 0$$

Tenga en cuenta en el razonamiento las tablas de restricción HFT de las normas IEC 61511 e IEC 61508.

a) Analice cuáles son las probabilidades medias de fallo peligroso en demanda de este dispositivo para ciclos de inspección de 1 año, 5 años y 10 años.

b) Verifique si con estos ciclos de inspección se mantiene en nivel SIL de la especificación inicial.

c) Estudie el promedio de fallos peligrosos, el nivel SIL alcanzable y los periodos máximos de inspección para una estructura redundante 1oo2 del dispositivo anterior.

SOLUCIÓN:

a) *Analice cuáles son las probabilidades medias de fallo peligroso en demanda de este dispositivo para ciclos de inspección de 1 año, 5 años y 10 años.*
Del tiempo medio entre fallos puede deducirse la tasa de fallos

$$MTTF = \frac{1}{\lambda}$$

Los peligrosos se obtienen a partir de la fracción de fallos seguros y el factor de cobertura por diagnósticos

$$\lambda_D = (1 - SFF) \cdot (1 - DCF) \cdot \lambda$$

Y el promedio de fallos en un ciclo de inspección TI para un dispositivo no redundante:

$$\overline{PDF} = \frac{\lambda_D \cdot TI}{2}$$

Por tanto,

$$\overline{PDF} = \frac{\lambda_D \cdot TI}{2} = (1 - SFF) \cdot (1 - DCF)\lambda\frac{TI}{2} \quad = \frac{(1 - SFF)}{MTFF}\frac{TI}{2}$$

Resolviendo los datos para TI = 1 año, 5 años y 10 años

$$\overline{PDF}_{1a} = \frac{0,1}{150 \cdot 10^4}\frac{10^4}{2} = 3,33 \cdot 10^{-4}$$
$$\overline{PDF}_{5a} = \frac{0,1}{150 \cdot 10^4}\frac{10^4}{2} = 1,66 \cdot 10^{-3}$$
$$\overline{PDF}_{10a} = \frac{0,1}{150 \cdot 10^4}\frac{10^4}{2} = 3,33 \cdot 10^{-3}$$

b) *Verifique si con estos ciclos de inspección se mantiene en nivel SIL de la especificación inicial.*
Para ciclos a 1 año, se cumple tanto con el límite SIL3 legal como el técnico (35 % del rango). De igual forma, a 2 y 10 años se verifican los límites legal y técnico de SIL2.

c) *Estudie el promedio de fallos peligrosos, el nivel SIL alcanzable y los periodos máximos de inspección para una estructura redundante 1oo2 del dispositivo anterior.*
En una estructura «1oo2», la probabilidad de que falle el sensor es la de que fallen ambos simultáneamente. Empleando las ecuaciones simplificadas sería:

$$PDF_{1oo2}(t) = PDF(t) \cdot PDF(t) = (\lambda t) \cdot (\lambda t) = \lambda^2 \cdot t^2 =$$
$$\overline{PDF}_{1oo2} = \frac{1}{TI}\int_0^{TI} PDF_{1oo2}(t) \cdot dt = \frac{1}{TI}\int_0^{TI} \lambda_D^2 t^2 dt$$
$$= \frac{\lambda_D^2 \cdot TI^2}{3}$$

Utilizando la tasa de fallos peligrosos:

$$\lambda_D = (1 - SFF) \cdot (1 - DCF) \cdot \lambda = (1 - 0,9) \cdot \frac{1}{150 \cdot 10^4} = 6,6 \cdot 10^{-8}$$
$$\overline{PDF}_{1oo2} = \frac{(6,6 \cdot 10^{-8})^2 \cdot 10^8}{3} = 14,2 \cdot 10^{-7}$$

Bajo el punto de vista de la tasa de fallos, la estructura supera muy por encima los requisitos incluso de SIL4. Sin

embargo, también existen limitaciones a la estructura. En el caso del IEC-61508, se diferencia entre dispositivos simples y complejos. En este caso, se trata presumiblemente de un dispositivo simple, ya que no se especifica la existencia de un factor de cobertura de diagnósticos (los autodiagnósticos se ejecutan mediante estructuras internas complejas). Examinando la tabla IEC 61508, con un HFT=1 (estructura 1oo2), y $SFF = 90\,\%$, con un $HFT = 1$ se lograría hasta SIL4.
Empleando la tabla IEC-61511 con HFT=1, y al tener un modo dominante seguro ($SFF > 50\,\%$) puede alcanzarse SIL2. Sin embargo, si se considera que se cumple la cláusula de «probado en uso», entonces sería posible llegar hasta SIL3 con una tolerancia a fallos hardware $HFT = 1$.

Problema 11. Analice las siguientes arquitecturas redundantes. Calcule para cada una de ellas el HFT, el promedio de fallos en demanda PFD_{AVG}, y el promedio de fallos espúreos (falsas alarmas).

a) 1oo2. La función de seguridad se ejecuta por la demanda de uno de los elementos.

b) 2oo2. La función de seguridad se ejecuta por la demanda simultánea de los dos elementos.

c) 2oo3. La función de seguridad se ejecuta por la demanda de dos de tres elementos.

d) Compare y justifique los resultados obtenidos.

SOLUCIÓN:

a) *1oo2. La función de seguridad se ejecuta por la demanda de uno de los elementos.*

$\overline{PFD}_{1oo2}$
Para que falle la estructura, deben hacerlo simultáneamente ambos dispositivos, por tanto:

$$PFD_{1oo2}(t) = PFD(t) \cdot PFD(t) = (\lambda_D \cdot t)^2$$

Integrando sobre un periodo de inspección:

$$\overline{PFD}_{1oo2} = \frac{1}{TI} \int_0^{TI} (\lambda_D \cdot t)^2 \cdot dt = \frac{\lambda_D^2 \cdot TI^2}{3}$$

$\overline{PFS}_{1oo2}$
Para que se produzca una falsa alarma, basta con que uno de los dispositivos, o ambos, fallen indicando la alarma. Es decir:

$$PFS_{1oo2}(t) = PFS(t) \cdot (1 - PFS(t)) + (1 - PFS(t)) \cdot PFS(t) + \\ + PFS(t) \cdot PFS(t) = \\ = 2PFS(t) \cdot (1 - PFS(t)) + PFS(t)^2 = \\ = 2PFS(t) - PFS(t)^2 = 2 \cdot \lambda_S \cdot t - \lambda_S^2 \cdot t^2$$

Integrando sobre un periodo de inspección:

$$\overline{PFS}_{1oo2}(t) = \frac{1}{TI} \int_0^{TI} PFS_{1oo2}(t) = \frac{1}{TI} \int_0^{TI} 2\lambda_S t - \frac{1}{TI} \int_0^{TI} (\lambda_S t)^2$$

$$= \lambda_S TI - \frac{\lambda_S^2 TI^2}{3} = \approx \lambda_S TI$$

b) *2oo2. La función de seguridad se ejecuta por la demanda simultánea de los dos elementos.*

$\overline{PFD}_{2oo2}$
Para que falle la estructura, basta con que falle uno de ellos, o bien ambos simultáneamente.

$$PFD_{2oo2}(t) = PFD(t) \cdot (1 - PFD(t)) + (1 - PFD(t)) \cdot PFD(t) + \\ + PFD(t) \cdot PFD(t) = \\ = 2PFD(t) \cdot (1 - PFD(t)) + PFD(t)^2 = \\ = 2\lambda_D t(1 - \lambda_D \cdot t) + \lambda_D^2 \cdot t^2 = 2 \cdot \lambda_D \cdot t - \lambda_D^2 \cdot t^2 \\ \approx 2 \cdot \lambda_D \cdot t$$

Integrando sobre un periodo de inspección:

$$\overline{PFD}_{2oo2}(t) = \frac{1}{TI} \int_0^{TI} PFD_{1oo2}(t) \approx \int_0^{TI} 2\lambda_D t dt = \lambda_D TI$$

$\overline{PFS}_{2oo2}$
Para que se produzca una falsa alarma, tienen que fallar simultáneamente los dos dispositivos de forma segura. Es decir:

$$PFS_{2oo2}(t) = PFD(t) \cdot PFD(t) = (\lambda_S \cdot t)^2$$

Integrando sobre un periodo de inspección:

$$\overline{PFS}_{2oo2}(t) = \frac{1}{TI}\int_0^{TI} PFS_{2oo2}(t) =$$
$$= \frac{1}{TI}\int_0^{TI} 2\lambda_S^2 t^2 \qquad\qquad = \frac{\lambda_S^2 TI^2}{3}$$

c) *2oo3. La función de seguridad se ejecuta por la demanda de dos de tres elementos.*

$\overline{PFD}_{2oo3}$
Para que falle la estructura, deben hacerlo 2 o 3 elementos de forma simultánea. Es decir:

$$\begin{aligned} PFD_{2oo3}(t) = 3 \cdot PFD(t) \cdot PFD(t) \cdot (1 - PFD(t)) + \\ + PFD(t) \cdot PFD(t) \cdot PFD(t) = \\ 3 \cdot [PFD(t)]^2 - 2 \cdot [PFD(t)]^3 \end{aligned}$$

Integrando sobre un periodo de inspección:

$$\begin{aligned} \overline{PFD}_{2oo3}(t) = \frac{1}{TI}\int_0^{TI} PFD_{2oo3}(t) = \frac{1}{TI}\int_0^{TI} 3\lambda_D^2 t^2 dt - \\ = -\frac{1}{TI}\int_0^{TI} 2\lambda_D^3 t^3 dt = \lambda_D^2 \cdot TI^2 - \frac{1}{2}\lambda_D^3 \cdot TI^3 \\ \approx \lambda_D^2 \cdot TI^2 \end{aligned}$$

$\overline{PFS}_{2oo3}$
Para que se produzca una falsa alarma, tienen que fallar simultáneamente dos o tres dispositivos de forma segura. Es decir:

$$\begin{aligned} PFS_{2oo3}(t) = 3 \cdot PFS(t) \cdot PFS(t) \cdot (1 - PFS(t)) + \\ + PFS(t) \cdot PFS(t) \cdot PFS(t) = \\ 3 \cdot [PFS(t)]^2 - 2 \cdot [PFS(t)]^3 \end{aligned}$$

Integrando sobre un periodo de inspección:

$$\begin{aligned}\overline{PFS}_{2oo3}(t) &= \frac{1}{TI}\int_0^{TI} PFS_{2oo3}(t) = \frac{1}{TI}\int_0^{TI} 3\lambda_S^2 t^2 dt - \\ &= -\frac{1}{TI}\int_0^{TI} 2\lambda_S^3 t^3 dt = \lambda_S^2 \cdot TI^2 - \frac{1}{2}\lambda_S^3 \cdot TI^3 \\ &\approx \lambda_S^2 \cdot TI^2\end{aligned}$$

d) *Compare y justifique los resultados obtenidos.*
En la siguiente tabla se resumen los resultados

Estructura	$\overline{PFD}$	$\overline{PFS}$
$1oo2$	$\frac{\lambda_D^2 \cdot TI^2}{3}$	$\lambda_S \cdot TI$
$2oo2$	$\lambda_D \cdot TI$	$\frac{\lambda_S^2 \cdot TI^2}{3}$
$2oo3$	$\lambda_D^2 \cdot TI^2$	$\lambda_S^2 \cdot TI^2$

Conclusiones:

- La estructura $1oo2$ es la más segura (menor promedio de fallos peligrosos), pero también la que posee unamayor probabilidad de falsas alarmas.
- La estructura $2oo2$ es la menos segura, aunque tiene el mejor promedio de falsas alarmas.
- La estructura $2oo3$ es la que ofrece un mejor compromiso entre fallos peligrosos y seguros.

Problema 12. Justifique razonadamente qué estructuras redundantes del problema anterior son o no adecuadas para ejecutar una función de ESD manual *(Emergency ShutDown)* empleando setas de emergencia.

SOLUCIÓN: Una parada de emergencia manual (ESD) es una función que ejecutan los operadores de planta o se ordena desde el sistema de supervisión (SCADA). El objetivo debe ser el detener la función de proceso o la celda de producción en cuanto algún operador pulse la seta. Por ello, de las tres funciones que se plantean, 1*oo*2, 2*oo*2 y 2*oo*3, tan sólo la primera tiene sentido.

Estrictamente hablando, una parada manual no es parte de una medida SIL ya que el sensor es esencialmente un operador humano, no se trata de un sistema electrónico automático.

Problema 13. Calcule de nuevo la probabilidad de fallo peligroso para las estructuras del ejercicio 12 teniendo en cuenta que los dispositivos redundantes son distintos, es decir, no replicantes, y por tanto, poseen diferentes datos de rendimiento.

Comparando los resultados con los del problema 12, calcule la tasa de fallos equivalente para cada estructura. Esto es, la que debería tener un dispositivo para que, utilizado de forma replicante, se obtenga la misma tasa de fallos.

SOLUCIÓN:

a) *1oo2. La función de seguridad se ejecuta por la demanda de uno de los elementos.*

$\overline{PFD}_{1oo2}$
Para que falle la estructura, deben hacerlo simultáneamente ambos dispositivos, por tanto:

$$PFD_{1oo2}(t) = PFD_1(t) \cdot PFD_2(t) = \lambda_{D1}\lambda_{D2} \cdot t^2$$

Integrando sobre un periodo de inspección:

$$\overline{PFD}_{1oo2} = \frac{1}{TI}\int_0^{TI} \lambda_{D1}\lambda_{D2}t^2 dt = \frac{\lambda_{D1}\lambda_{D1}TI^2}{3}$$

Comparando con la expresión para un dispositivo simple en estructura «1oo2», la tasa de fallos equivalente sería:

$$\begin{aligned} \overline{PFD}_{1oo2} &= \frac{\lambda_D^2 \cdot TI^2}{3} = \frac{\lambda_{D1}\lambda_{D2}TI^2}{3} \\ &\Rightarrow \lambda_D^2 = \lambda_{D1}\lambda_{D2} \\ &\Rightarrow \lambda_D = \sqrt{\lambda_{D1}\lambda_{D2}} \end{aligned}$$

b) *2oo2. La función de seguridad se ejecuta por la demanda simultánea de los dos elementos.*

$\overline{PFD}_{2oo2}$
Para que falle la estructura, basta con que falle uno de ellos, o bien ambos simultáneamente.

$$\begin{aligned}PFD_{2oo2}(t) &= PFD_1(t)\cdot(1-PFD_2(t)) + (1-PFD_1(t))\cdot PFD_2(t) + \\ &+ PFD_1(t)\cdot PFD(t)_2 = \\ &= PFD_1(t) + PFD_2(t) - PFD_1(t)\cdot PFD_2(t) = \\ &= \lambda_{D1}t + \lambda_{D2}t - \lambda_{D1}\lambda_{D2}t^2 \\ &\approx (\lambda_{D1}+\lambda_{D2})t\end{aligned}$$

Integrando sobre un periodo de inspección:

$$\overline{PFD}_{2oo2}(t) = \frac{1}{TI}\int_0^{TI}(\lambda_{D1}+\lambda_{D2})t = (\lambda_{D1}+\lambda_{D2})\frac{TI}{2}$$

Comparando de nuevo con la tasa de fallos empleando dispositivos idéntivos en una estructura «2oo2»:

$$\begin{aligned}\overline{PFD}_{2oo2} &= \lambda_D\cdot TI = (\lambda_{D1}+\lambda_{D2})\frac{TI}{2} \\ \Rightarrow \lambda_D &= \frac{\lambda_{D1}+\lambda_{D2}}{2}\end{aligned}$$

c) *2oo3. La función de seguridad se ejecuta por la demanda de dos de tres elementos.*

$\overline{PFD}_{2oo3}$
Para que falle la estructura, deben hacerlo 2 o 3 elementos de forma simultánea. Es decir:

$$\begin{aligned}PFD_{2oo3}(t) &= PFD_1(t)\cdot PFD_2(t)\cdot(1-PFD_3(t)) + \\ &+ PFD_1(t)\cdot(1-PFD_2(t))\cdot PFD_3(t) + \\ &+ (1-PFD_1(t))\cdot PFD_2(t)\cdot PFD_3(t) + \\ &+ PFD_1(t)\cdot PFD_2(t)\cdot PFD_3(t) = \\ &= PFD_1(t)\cdot PFD_2(t) + PFD_1(t)\cdot PFD_3(t) + \\ &+ PFD_2(t)\cdot PFD_3(t) - 2\cdot PFD_1(t)\cdot PFD_2(t)\cdot PFD_3(t) = \\ &= (\lambda_{D1}\lambda_{D2}+\lambda_{D1}\lambda_{D3}+\lambda_{D2}\lambda_{D3})\cdot t^2 - 2\lambda_{D1}\lambda_{D2}\lambda_{D2}\cdot t^3 \\ &\approx (\lambda_{D1}\lambda_{D2}+\lambda_{D1}\lambda_{D3}+\lambda_{D2}\lambda_{D3})\cdot t^2\end{aligned}$$

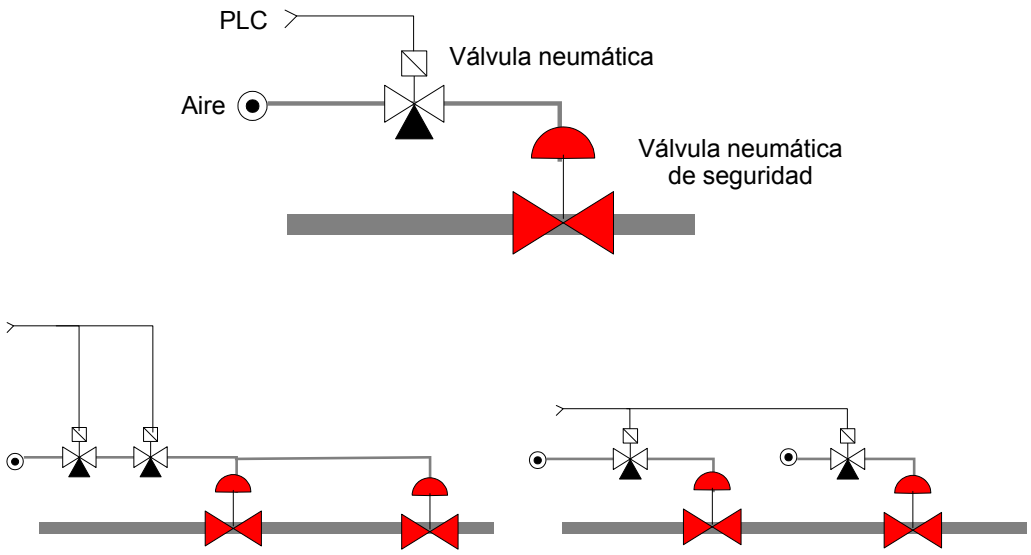
Integrando sobre un periodo de inspección:

$$\begin{aligned}\overline{PFD}_{2oo3}(t) &= \frac{1}{TI}\int_0^{TI} PFD_{2oo3}(t) = \\ &= \frac{1}{TI}\int_0^{TI} (\lambda_{D1}\lambda_{D2} + \lambda_{D1}\lambda_{D3} + \lambda_{D2}\lambda_{D3}) \cdot t^2 \\ &= (\lambda_{D1}\lambda_{D2} + \lambda_{D1}\lambda_{D3} + \lambda_{D2}\lambda_{D3})\frac{TI^2}{3}\end{aligned}$$

Comparando de nuevo los resultados empleando dispositivos iguales y diversos:

$$\begin{aligned}\frac{\lambda_D^2 \cdot TI^2}{3} &= (\lambda_{D1}\lambda_{D2} + \lambda_{D1}\lambda_{D3} + \lambda_{D2}\lambda_{D3})\frac{TI^2}{3} \\ \Rightarrow \lambda_D^2 &= \frac{\lambda_{D1}\lambda_{D2} + \lambda_{D1}\lambda_{D3} + \lambda_{D2}\lambda_{D3}}{3} \\ \Rightarrow \lambda_D &= \sqrt{\frac{\lambda_{D1}\lambda_{D2} + \lambda_{D1}\lambda_{D3} + \lambda_{D2}\lambda_{D3}}{3}}\end{aligned}$$

Problema 14. Las figuras muestran tres circuitos actuadores de seguridad diferentes. El objetivo es cerrar la tubería principal por donde circula gas. En este tipo de aplicaciones, la normativa obliga a emplear válvulas de seguridad de tipo neumático. Además, la norma IEC 61511 recomienda que la función de seguridad se ejecute cuando el actuador está de-energizado, en este caso sin presión. Por ello, tanto las válvulas de seguridad como las electroválvulas son de tipo NC.



a) Calcule para las tres estructuras los siguientes datos:

   1. HFT.
   2. Promedio de fallos peligrosos en demanda para un periodo de inspección TI.
   3. Tasa de fallos peligrosos equivalente λ_D.
   4. Tasa de fallos peligrosos del conjunto (si tiene sentido)

b) Modifique el cálculo del PFD promedio si las válvulas poseen un factor de fallo en modo común no nulo: β_{EV} y β_{VS}

SOLUCIÓN:

a) *Calcule para las tres estructuras los siguientes datos: HFT, promedio de fallos en demanda para un ciclo de inspección TI, tasa de fallos peligrosos equivalente y*

b) *Tasa de fallos peligrosos del conjunto (si tiene sentido).*

1. **Estructura A**. No es redundante, un fallo peligroso en cualquiera de los elementos produce una pérdida de seguridad.
   HFT = 0
   Se trata de una estructura «2oo2» con dispositivos distintos.

$$PFD_{2oo2}(t) \approx PFD_1(t) + PFD_2(t) = \lambda_{DEV}t + \lambda_{DVS}t = \\ = (\lambda_{DEV} + \lambda_{DVS})\, t$$

   Promediando para un ciclo TI

$$\overline{PFD}_{2oo2}(TI) = (\lambda_{DEV} + \lambda_{DVS})\, \frac{TI}{2}$$

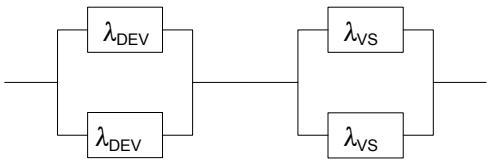
   La tasa equivalente la obtenemos sustituyendo cada uno de los dispositivos originales del sistema por réplicas de un mismo elemendo. Es decir:

$$\overline{PFD}^{EQ}_{2oo2}(TI) = 2\lambda^{EQ}_D \frac{TI}{2} = (\lambda_{DEV} + \lambda_{DVS})\, \frac{TI}{2}$$
$$\lambda^{EQ}_D = \frac{\lambda_{DEV} + \lambda_{DVS}}{2}$$

   Para el cálculo de la tasa de fallos del conjunto, el sistema se sustituye por un único dispositivo simple. Esto sólo es posible si dicho conjunto se comporta de forma análoga a un dispositivo simple. En este caso es cierto ya que se trata de una estructura no redundante (HFT=0). Comparando su tasa de fallos con la de uno simple:

$$PFD_{2oo2}(t) \approx (\lambda_{DEV} + \lambda_{DVS})\, t$$
$$PFD_{1oo1}(t) = \lambda_D \cdot t$$
$$\Rightarrow \lambda_D = \lambda_{DEV} + \lambda_{DVS}$$

2. **Estructura B**. Es redundante, su diagrama de rendimiento es el de la figura.



HFT = 1
La probabilidad de fallo sería:

$$PFD(t) \approx PFD^{EV}_{1oo2}(t) + PFD^{VS}_{1oo2}(t) = \\ = \lambda^2_{DEV} \cdot t^2 + \lambda^2_{DVS} \cdot t^2$$

Y el promedio a lo largo de TI

$$\overline{PFD} = \left(\lambda^2_{DEV} + \lambda^2_{DVS}\right) \frac{TI^2}{3}$$

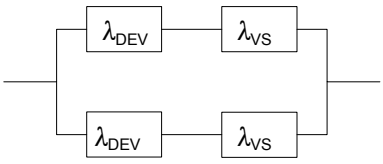
La tasa equivalente empleando dispositivos idénticos en toda la estructura:

$$\overline{PFD}^{EQ} = 2\lambda^2_{DEQ} \frac{TI^2}{3} = \left(\lambda^2_{DEV} + \lambda^2_{DVS}\right) \frac{TI^2}{3}$$

$$\lambda_{DEQ} = \sqrt{\frac{\lambda^2_{DEV} + \lambda^2_{DVS}}{2}}$$

La tasa de fallos del conjunto no tiene sentido, ya que como se demuestra en su $PFD(t)$ no se comporta como un dispositivo simple, donde $PFD(t) = \lambda_D \cdot t$

3. **Estructura C**. Es efectivamente una estructura redundante con el diagrama de rendimiento de la figura.



HFT = 1
La probabilidad de fallo sería:

$$PFD(t) = \left[PFD^{EV}(t) + PFD^{VS}(t)\right]^2 \\ \approx \left[\lambda_{DEV} \cdot t + \lambda_{DVS} \cdot t\right]^2 \\ = \left(\lambda_{DEV} + \lambda_{DVS}\right)^2 \cdot t^2$$

Y el promedio a lo largo de TI

$$\overline{PFD} = (\lambda_{DEV} + \lambda_{DVS})^2 \frac{TI^2}{3}$$

La tasa equivalente empleando dispositivos idénticos en toda la estructura:

$$\overline{PFD}^{EQ} = 4\lambda_{DEQ}^2 \frac{TI^2}{3} = (\lambda_{DEV} + \lambda_{DVS})^2 \frac{TI^2}{3}$$
$$\lambda_{DEQ} = \frac{\lambda_{DEV} + \lambda_{DVS}}{2}$$

En este caso, tampoco tiene sentido la tasa de fallos del conjunto.

c) *Modifique el cálculo del PFD promedio si las válvulas poseen un factor de fallo en modo común no nulo: β_{EV} y β_{VS}*
El factor de fallo en modo común sólo tiene sentido aplicarlo a estructuras redundantes debido a que las transforma en no redundantes para un cierto porcentaje de los fallos peligrosos $\beta\lambda_D$.

Estructura B. Partiendo de la ecuación de probabilidad de fallo aleatorio:

$$PFD(t) \approx \lambda_{DEV}^2 \cdot t^2 + \lambda_{DVS}^2 \cdot t^2$$

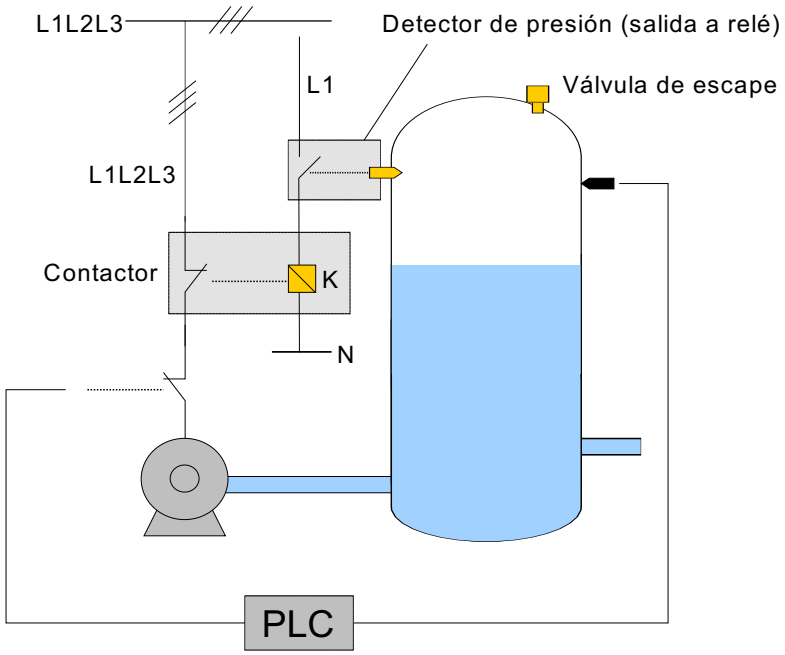
Comparando la ecuación con la del modelo β, cada término cuadrático representa la probabilidad de fallo independiente (en este caso, en lugar de λ_D habrá que emplear $(1-\beta)\lambda_D$. Además hay que añadir un término $\beta\lambda_D t$ que representa el fallo común, fallos cuya causa provoca la avería simultánea de ambas válvulas. Por tanto, la ecuación quedaría:

$$PFD(t) \approx (1-\beta_{EV})^2\lambda_{DEV}^2 t^2 + \beta_{EV}\lambda_{DEV} t + (1-\beta_{VS})^2\lambda_{DVS}^2 t^2 + \beta_{VS}\lambda_{VS} t$$

Promediando para un ciclo de inspección:

$$\overline{PFD}(TI) \approx (1-\beta_{EV})^2\lambda_{DEV}^2 \frac{TI^2}{3} + \beta_{EV}\lambda_{DEV}\frac{TI}{2} + \\ + (1-\beta_{VS})^2\lambda_{DVS}^2 \frac{TI^2}{3} + \beta_{VS}\lambda_{DVS}\frac{TI}{2}$$

Problema 15. En un sistema de impulsión de agua a alta presión, se ha diseñado una medida SIS, paralela al PLC de control, que detiene el bombeo hacia el calderín de en caso de que se detecte una sobrepresión en el mismo. La medida implementada consta de de un detector de presión con salida a relé con el que se abre un contactor que detiene el bombeo.



			«Proven-in-use»
Detector	$\lambda_{HIGH} = 120FIT$	$\lambda_{LOW} = 68FIT$	Sí
Contactor	$\lambda_{CLOSE} = 1{,}38 \cdot 10^{-6}$	$\lambda_{OPEN} = 1{,}62 \cdot 10^{-6}$	No

a) Analice el nivel máximo SIL alcanzable para periodos de inspección de 1 año.

b) Empleando estructuras redundantes, verifique si se alcanzarían niveles SIL2 o SIL3.

SOLUCIÓN:

a) *Analice el nivel máximo SIL alcanzable para periodos de inspección de 1 año.*
Desde el punto de vista de la estructura, sensores, LS y Actuadores poseen HFT = 0. El nivel SIL alcanzable depende de este dato y de la fracción de fallos seguros SFF.

Para calcular la fracción de fallos seguros, debe tenerse en cuenta el diseño concreto de la medida SIS. Para el detector de presión instalado, el fallo seguro será aquel en el que excite al contactor, es decir, (λ_{HIGH}). Por tanto:

$$SFF_{DETECTOR} = \frac{\lambda_S}{\lambda_S + \lambda_D} = \frac{\lambda_{HIGH}}{\lambda_{LOW} + \lambda_{HIGH}} = 0,71$$

Aplicando la tabla de dispositivos simples del IEC-61511, para $SFF > 60\,\%$ y HFT=0 el máximo nivel SIL permitido es SIL1. Sin embargo, al cumplir las condiciones «proven-in-use», entonces $HFT = 1 - 1 = 0$, lo que permite a diseño actual alcanzar SIL2.
Utilizando la tabla IEC 61508 para dispositivos simples, el resultado también sería SIL2.
La etapa actuadora está formada por un contactor, cuyo fallo seguro corresponde a aquel en el que se encuentra permanentemente abierto.

$$SFF_{CONTACTOR} = \frac{\lambda_S}{\lambda_S + \lambda_D} = \frac{\lambda_{OPEN}}{\lambda_{OPEN} + \lambda_{CLOSE}} = 0,54$$

Empleando de nuevo la tabla HFT de dispositivos simples, y teniendo en cuenta que se trata de un dispositivo con un modo dominante seguro ($SFF > 50\,\%$), y sin las condiciones «proven-in-use», sólo sería admisible una integridad SIL1 [1] .
Con la IEC 61508, el dispositivo no es esencialmente seguro ($SFF < 60\,\%$), y sólo es admitido para SIL1.

[1] Es importante señalar en este punto, que en la práctica es difícil que un dispositivo con una SFF tan baja pueda cumplir las cláusulas «proven-in-use». Sin embargo, salvo que se indique lo contrario, se supondrá cierta esta condición.

En una interconexión serie, el máximo nivel de integridad del conjunto es el menor de los de sus subsistemas. En este caso SIL1. Ahora debe probarse que el rendimiento también cumple con ese nivel de integridad:

$$\begin{aligned}\overline{PFD}_{SIS} &= \overline{PFD}_{SENS} + \overline{PFD}_{LS} + \overline{PFD}_{ACT} = \\ &= \lambda^D_{SENS}\frac{TI}{2} + 0 + \lambda^D_{ACT}\frac{TI}{2} \\ &= 68 \cdot 10^{-9}\frac{10^4}{2} + 1{,}38 \cdot 10^{-6}\frac{10^4}{2} \\ &= 0{,}72 \cdot 10^{-2} < 10^{-1}\end{aligned}$$

Si tenemos en cuenta que

$$\begin{aligned}\lambda^D_{SENS} &= \lambda_{LOW} \\ \lambda^D_{ACT} &= \lambda_{CLOSE}\end{aligned}$$

Entonces:

$$\begin{aligned}\overline{PFD}_{SIS} &= 68 \cdot 10^{-9}\frac{10^4}{2} + 1{,}38 \cdot 10^{-6}\frac{10^4}{2} \\ &= 0{,}72 \cdot 10^{-2} < 10^{-1}\end{aligned}$$

Por tanto, se cumple SIL1.

b) *Empleando estructuras redundantes, verifique si se alcanzarían niveles SIL2 o SIL3.*
La restricción de arquitectura permite emplear el detector seleccionado sin redundancia en SIL2 (ver apartado anterior). En cambio, con la calidad del actuador elegido (SFF), tanto tanto IEC 61511 como 61508, exigen $HFT = 1$. Empleando, por ejemplo una estructura «1oo2», el promedio de fallos para ciclos de inspección de un año sería:

$$\begin{aligned}\overline{PFD}_{SIS} &= \overline{PFD}_{SENS} + \overline{PFD}_{LS} + \overline{PFD}_{ACT} = \\ &= \lambda^D_{SENS}\frac{TI}{2} + 0 + \frac{(\lambda^D_{ACT}TI)^2}{3} \\ &= \frac{68 \cdot 10^{-9} \cdot 10^4}{2} + \frac{(1{,}381 \cdot 10^{-6}10^4)^2}{3} \\ &= 3{,}4 \cdot 10^{-4} + 0{,}63 \cdot 10^{-4} = 0{,}44 \cdot 10^{-3} < 10^{-2}\end{aligned}$$

Como vemos, cumple perfectamente SIL2. Y la medida habría que rediseñarla tal y como se indica en la siguiente figura:

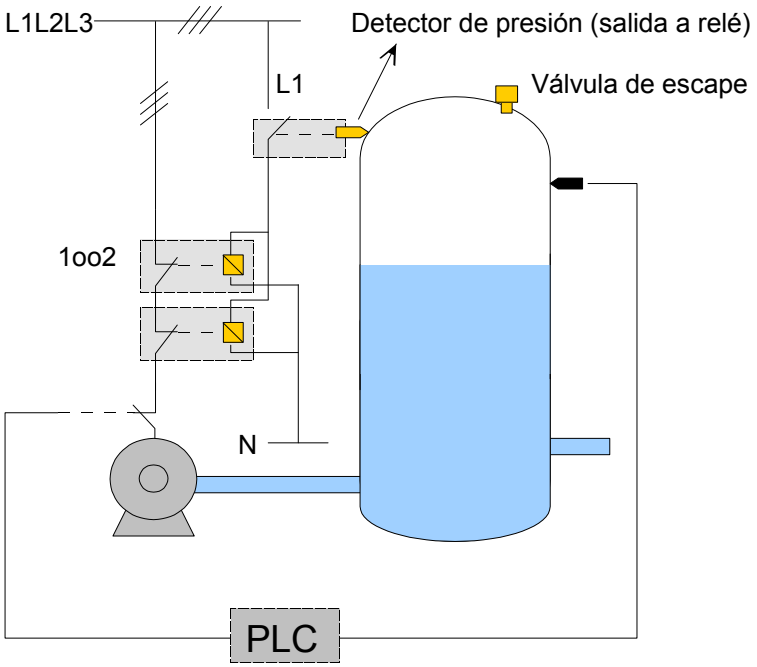


Figura 1: Arquitectura compatible con SIL2

Para un nivel SIL3, deben modificarse tanto la estructura del detector como la del actuador. Las restricciones impuestas por IEC 61508 para dispositivos simples y un SIL3 son de $HFT = 1$ para el sensor ($SFF = 71\,\%$) y de $HFT = 2$ para el relé ($SFF = 54\,\%$). El mismo resultado se obtiene de la tabla definida en IEC 61511 (si se tiene en cuenta la cláusula «proven-in-use» del sensor. La figura 2 muestra solución.

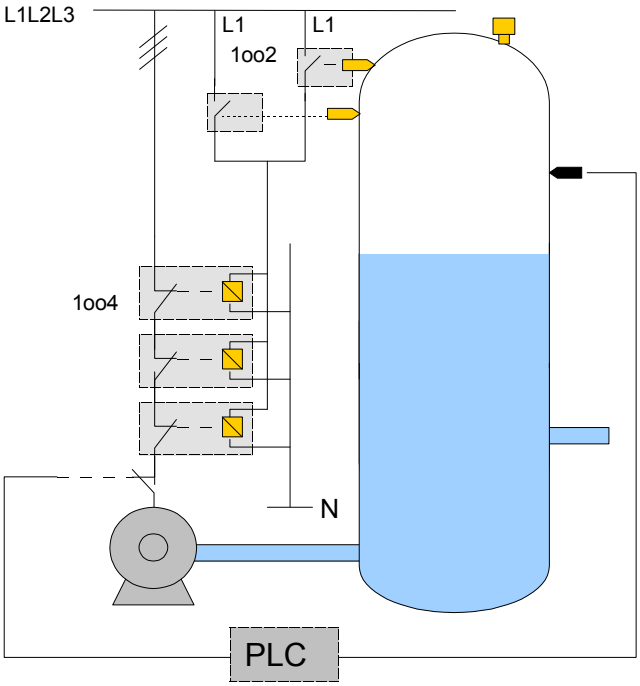
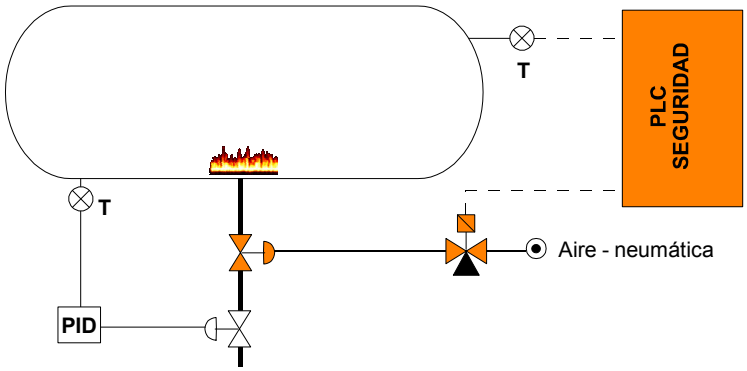


Figura 2: Arquitectura compatible con SIL3

El rendimiento cumple sobradamente el nivel SIL3 ($< 10^{-3}$ como se demuestra en el siguiente cálculo:

$$\begin{aligned}\overline{PFD}_{SIS} &= \overline{PFD}_{SENS} + \overline{PFD}_{LS} + \overline{PFD}_{ACT} = \\ &= \frac{(\lambda^D_{SENS} TI)^2}{3} + 0 + \frac{(\lambda^D_{ACT} TI)^3}{4} \\ &= \frac{(68 \cdot 10^{-9} 10^4)^2}{3} + \frac{(1{,}381 \cdot 10^{-6} 10^4)^3}{4} \\ &= 0{,}15 \cdot 10^{-6} + 0{,}65 \cdot 10^{-6} = 0{,}80 \cdot 10^{-6} < 10^{-3}\end{aligned}$$

Problema 16. En la figura se muestra el control de temperatura y las medidas de seguridad de una caldera de gas. Siguiendo normativas específicas, para evitar riesgos de explosión se utilizan válvulas de seguridad neumáticas.



a) Indique qué normativa de las que se relacionan debe aplicarse en los casos que se indican. Normativas: IEC 61508, IEC 61021, IEC 61513, IEC-954 o ninguna.

   1. Diseño y fabricación del controlador
   2. Diseño y fabricación de la válvula neumática de seguridad
   3. Diseño e implementación de las medidas de seguridad

b) Justifique si el bucle de control PID puede considerarse o no como parte del sistema de seguridad a efectos de análisis de riesgos.

c) Describa la función de seguridad que debe ejecutarse y las acciones que requiere de cada uno de sus elementos. Justifique especialmente si deben emplearse dispositivos normalmente energizados o no *(energized/de-energized to trip)*;

d) Con los valores de rendimiento de la tabla que se adjunta, determine el nivel SIL que alcanza esta medida para ciclos de inspección de un año.

e) Justifique si es posible emplear los ciclos de inspección recomendados por los fabricantes y las consecuencias que tendría.

f) Encuentre el tiempo medio entre fallos peligrosos del sistema.

g) Encuentre el valor PFD a un año del conjunto empleando una estructura redundante en la válvula de seguridad y en la de control neumático. Suponga un factor de fallo común $\beta_{VS} = 0{,}2$ para la primera y de $\beta_{EV} = 0{,}3$ para la segunda.

Sensor Temp.	Electroválvula	Válvula de seguridad	PLC
$\overline{PDF} = 1{,}2 \cdot 10^{-3}$ (TI = 2 años) SFF = 80 % Tipo A	$\overline{PDF}_{EV} = 1{,}2 \cdot 10^{-3}$ (TI = 1 año) SFF = 65 %	$\overline{PDF}_{VS} = 1{,}2 \cdot 10^{-3}$ (TI = 1 año) SFF = 70 %	$\overline{PDF}_{LS} = 1{,}2 \cdot 10^{-3}$ (TI = 3 años) SFF = 90 %

SOLUCIÓN:

a) *Indique qué normativa de las que se relacionan debe aplicarse en los casos que se indican. Normativas: IEC 61508, IEC 62061, IEC 61511 o ninguna.*

1. *Diseño y fabricación del controlador.*
   La norma dirigida a fabricantes de dispositivos de seguridad funcional eléctricos, electrónicos y programables es la IEC-61508.

2. *Diseño y fabricación de la válvula neumática de seguridad.*
   Ninguna de las anteriores, sin bien es cierto que en la actualidad los fabricantes comienzan a aplicar los métodos de la IEC-61508.

3. *Diseño e implementación de las medidas de seguridad.*
   Para maquinaria IEC-62061 y para procesos IEC-61511.

b) *Justifique si el bucle de control PID puede considerarse o no como parte del sistema de seguridad a efectos de análisis de riesgos.*

Respecto al peligro sobretemperatura, sí. El bucle regula la temperatura aumentando la potencia de ignición si baja, y reduciéndola si dicha temperatura sube.

c) Describa la función de seguridad que debe ejecutarse y las acciones que requiere de cada uno de sus elementos. Justifique

especialmente si deben emplearse dispositivos normalmente energizados o no *(energized/de-energized to trip)*;

La medida de seguridad consiste en el corte del suministro de gas al quemador si se detecta una temperatura excesiva en la caldera. Un sensor mide la temperatura, el controlador compara con el valor límite prefijado, y ordena el cierre del gas en caso necesario. El sistema actuador electroneumático debe diseñarse para que no se pierda la seguridad con el fallo de las instalaciones auxiliares (aire o suministro eléctrico). Por tanto, el estado de-energizado debe corresponder al cierre del gas. Para ello, se necesita una electroválvula NC y una válvula neumática de seguridad NC. Para que circule el gas, el controlador debe activar la electroválvula que a su vez presurizará la válvula de seguridad para que se abra. El corte o ciere del gas cierre se consigue en cualquiera de las siguientes circunstancias:

- Al desactivar la electroválvula
- Con una parada o desconexión del controlador
- Cuando falla la instalación de aire a presión

d) *Con los valores de rendimiento de la tabla que se adjunta, determine el nivel SIL que alcanza esta medida para ciclos de inspección de un año.*

Sensor Temp.	Electroválvula	Válvula de seguridad	PLC
$\overline{PDF} = 1{,}2 \cdot 10^{-3}$ (TI = 2 años) SFF = 80 % Tipo A	$\overline{PDF}_{EV} = 1{,}2 \cdot 10^{-3}$ (TI = 1 año) SFF = 65 %	$\overline{PDF}_{VS} = 1{,}2 \cdot 10^{-3}$ (TI = 1 año) SFF = 70 %	$\overline{PDF}_{LS} = 1{,}2 \cdot 10^{-3}$ (TI = 3 años) SFF = 90 %

El **ANÁLISIS DE LA ARQUITECTURA** es el primer paso para la comprobación y el diseño de la media.

SENSOR) Aplicando la IEC 61508, para SFF = 80 % el nivel alcanzable sin redundancia es SIL2. Siguiendo la norma IEC 61511, sólo llega a SIL1 salvo que se cumpla la cláusulas «proven-in-use» en cuyo caso sí se alcanza SIL2. Conclusión:

SIL2.
CONTROLADOR) Desde el punto de vista de la IEC 61508 un PLC es un dispositivo complejo. Según la tabla y para una fracción de fallos del 90 % se puede alcanzar SIL2 sin redundancia. Según la tabla de dispositivos PE-LS de la IEC 61511, el nivel máximo sin redundancia sería también SIL2.

ACTUADOR) El mismo razonamiento que en los casos anteriores podría aplicarse a la etapa de actuadores. Sin embargo, en ella no hay un dispositivo simple, definido con un único SFF, sino dos dispositivos con diferentes SFF conectados en una estructura «2002». En general, podemos encontrarnos en alguna de las siguientes situaciones:

a) Si no se conoce el valor SFF de un dispositivo, o no podemos calcularlo con los datos del problema, se supondrá que se trata de un elemento fundamentalmente inseguro, es decir $SFF < 50$.

b) Algunas estructuras se ofrecen con la tasa de fallos y/o el SFF del conjunto. En este caso, ambos dispositivos se tratarán como uno simple.

c) Con carácter general, si se trata de dispositivos independientes, como es nuestro caso, se aplican las reglas empíricas de fusión sobre sistemas heterogéneos. En primer lugar se estudian los límites SIL por separado. Los actuadores del problema presentan, desde el punto de vista del rendimiento, una estructura serie. Por tanto, el máximo SIL alcanzable es el menor de los calculados individualmente.

Utilizando la norma 61508 para dispositivos simples, tanto la electroválvula como la válvula de corte se encuentran en el rango $SFF \in [60, 90)$ y podrían usarse hasta un SIL2. Con la norma 61511, se lograría SIL1. Sólo es posible SIL2 si se demuestra la cláusula "proven-in-use"[2]. Tomando el resultado más favorable (el primero), tendríamos un SIL2 para el conjunto.

La medida completa alcanzaría SIL2.

[2]Aunque en este caso es más restrictivo el estándar de procesos, si se posee una certificación SIL2 con 61508 de un organismo independiente del fabricante, ésta también se considera como válida a efectos de la cláusula "proven-in-use"

ANÁLISIS DEL RENDIMIENTO. Además de la arquitectura, debe comprobarse que el promedio de fallos aleatorios en demanda se ajusta al nivel SIL.Para el cálculo del promedio de fallos, partimos de la ecuación:

$$\overline{PFD}_{SIS} = \overline{PFD}_{Sens} + \overline{PFD}_{LS} + \overline{PFD}_{Act}$$

En todos los casos, al no tener redundancia

$$\overline{PFD} = \lambda_D \frac{TI}{2}$$

En el sensor nos ofrecen el PFD para TI=2años, por tanto:

$$\overline{PFD}_{Sens}(TI = 1a) = \frac{\overline{PFD}_{Sens}(TI = 2a)}{2} = 6 \cdot 10^{-4}$$

Para el disp. lógico igual:

$$\overline{PFD}_{LS}(TI = 1a) = \frac{\overline{PFD}_{Sens}(TI = 3a)}{3} = 4 \cdot 10^{-4}$$

Pero para los actuadores, la probabilidad de fallo peligroso del conjunto sería:

$$\begin{aligned} PFD(t) &= 1 - (1 - PFD_{EV}(t)) \cdot (1 - PFD_{VS}(t)) = \\ &= PFD_{EV}(t) + PFD_{VS}(t) - PFD_{EV}(t) \cdot PFD_{VS}(t) \\ &\approx PFD_{EV}(t) + PFD_{VS}(t) \end{aligned}$$

Y en promedio:

$$\begin{aligned} PFD(t) &\approx PFD_{EV}(t) + PFD_{VS}(t) \\ &= 2 \cdot 10^{-3} + 3 \cdot 10^{-4} = 2{,}3 \cdot 10^{-3} \end{aligned}$$

$\overline{PFD}_{SIS} = 6 \cdot 10^{-4} + 4 \cdot 10^{-4} + 6 \cdot 10^{-4} + 6 \cdot 10^{-4} = 3{,}4 \cdot 10{-}3$

Por fallos aleatorios podría alcanzar hasta SIL2.

CONCLUSIÓN. Tanto por rendimiento como por arquitectura, es posible alcanzar SIL2.

e) *Justifique si es posible emplear los ciclos de inspección recomendados por los fabricantes y las consecuencias que tendría.*
El promedio de fallo medio en un ciclo de inspección, y la clasificación SIL, se aplica a la medida completa. De no hacerlo así, si por ejemplo un elemento se inspecciona cada año, y otro cada 2, habría que calcular el PFD para el primer año y otro PFD para el segundo. En el primero los dispositivos están a día cero, mientras que en el segundo hay uno a día cero y otro que no. Al final, el peor caso consiste en sumar todos los valores sean o no anuales.

En la realidad, los ciclos de inspección deben ser iguales para todos los elementos, ya que el coste de personal y desplazamiento es el mismo. Tan sólo incrementaría un poco las horas dedicadas a la inspección.

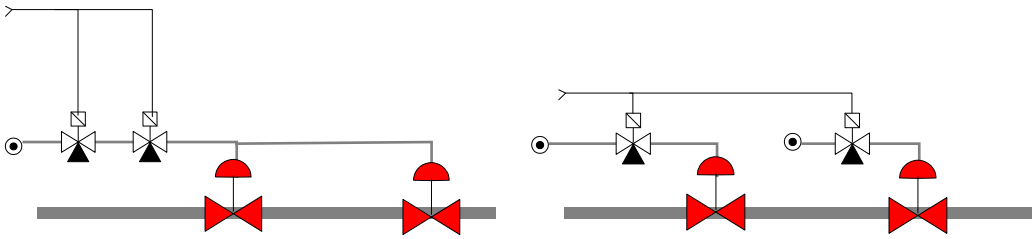
f) Encuentre el tiempo medio entre fallos peligrosos del sistema.
De la fórmula del tiempo medio al primer fallo, puede deducirse la del tiempo medio al primer fallo peligroso:

$$MTTF = \frac{1}{\lambda_D}$$

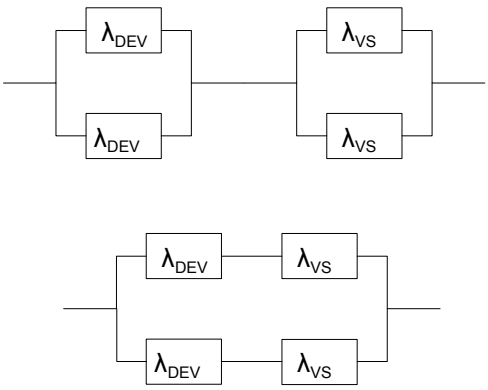
Como todas las fases de la medida SIS son NO REDUNDANTES, cabe describir el conjunto como un dispositivo simple. es decir:

$$\begin{aligned} PFD_{SIS}(t) &= \lambda_{SENS}\frac{TI}{2} + \lambda_{PLC}\frac{TI}{2} + \lambda_{ACT}\frac{TI}{2} \\ &= \lambda_{SIS}\frac{TI}{2} \\ \Rightarrow \lambda_{SIS} &= \frac{2}{TI}PFD_{SIS} \\ \Rightarrow MTTF_{SIS} &= \frac{TI}{2}\frac{1}{PFD_{SIS}} \end{aligned}$$

g) *Encuentre el valor PFD a un año del conjunto empleando una estructura redundante en la válvula de seguridad y en la de control neumático. Suponga un factor de fallo común $\beta = 0{,}2$ para la primera y de $\beta = 0{,}3$ para la segunda.*
Los fallos peligrosos de la estructura corresponden a la situación en que una de las válvulas quede abierta. Teniendo esto en cuenta, se proponen las siguientes como estructuras redundates:



De ambas, la primera es la que mejor comportamiento presenta ante fallos peligrosos es la primera, ya que cualquiera de las válvulas de seguridad puede ser cerrada con que cierre una única electroválvula. En cambio, en la segunda propuesta, la avería en uno de los elementos, invalida el funcionamiento del otro. Desde el punto de vista del rendimiento la función de ambas sería:



La probabilidad de fallo peligroso en demanda para primera estructura:

$$\begin{aligned} PFD(t) &= PFD^{EV}_{1oo2}(t) \cdot \left[1 - PFD^{VS}_{1oo2}(t)\right] + \left[1 - PFD^{EV}_{1OO2}(t)\right] \cdot PFD^{VS}_{1oo2}(t) + \\ &+ PFD^{EV}_{1oo2}(t) \cdot PFD^{VS}_{1oo2}(t) \\ &\approx PFD^{EV}_{1oo2}(t) + PFD^{EV}_{1OO2}(t) \\ &= \lambda^2_{DEV} t^2 + \lambda^2_{DVS} t^2 \end{aligned}$$

Si tenemos en cuenta el modelos β, para dispositivos redundantes, en la ecuación anterior debe sustituirse λ_D por la proporción

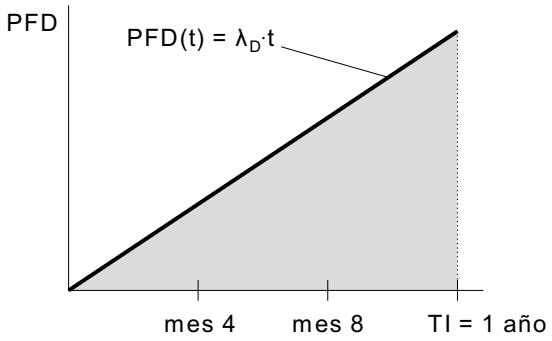
de fallos aleatorios sin causa común: $(1-\beta)\lambda_D$ y añadir un término que describe el fallo simultáneo por causa común: $\beta\lambda_D$. La ecuación quedaría entonces:

$$PFD(t) = (1-\beta_{EV})^2\lambda_{DEV}^2 t^2 + \beta_{EV}\lambda_{EV}t + \\ + (1-\beta_{VS})^2\lambda_{VS}^2 t^2 + \beta_{VS}\lambda_{VS}t$$

Integrando para un ciclo de inspección, se obtiene:

$$\overline{PFD}(TI) = \frac{1}{TI}\int_0^{TI} PFD(t)dt = \\ = \frac{(1-\beta_{EV})^2\lambda_{DEV}^2 TI^2}{3} + \beta_{EV}\lambda_{EV}\frac{TI}{2} \quad + \frac{(1-\beta_{VS})^2\lambda_{DVS}^2 TI^2}{3} + \beta_{VS}\lambda_{VS}\frac{TI}{2}$$

Problema 17. Un fallo muy habitual en las válvulas es la obstrucción causada por sedimentos. Este fallo es especialmente grave en las válvulas de seguridad que pueden permanecer inactivas durante años. Para reducir estos fenómenos se utiliza una técnica de cierre parcial que deja una apertura de un 10-20 %(Partial Stroking). Esta maniobra se ejecuta periódicamente y, además de determinar si hay o no un atasco, permite mover los sedimientos y reducir su acumulación.



A) La figura representa la gráfica de evolución de PFD(t) para una válvula convencional (sin cierre parcial) durante un periodo de inspección de un año. Para ésta válvula calcule el promedio de fallos peligrosos en demanda $\overline{PFD}(TI)$ para un periodo de inspección TI. Indique además qué significado geométrico tiene la expresión resultante.

B) Suponiendo que el cierre parcial detecta todos los fallos peligrosos de una válvula de seguridad, dibuje sobre la figura anterior la curva PFD(t) para un periodo de un año si el cierre parcial se ejecuta cada 4 meses. Aplicando el resultado del apartado anterior, calcule el $\overline{PFD}(TI = 1a)$

C) Si el cierre parcial sólo detecta un porcentaje P de los fallos peligrosos de una válvula de seguridad, dibuje sobre la figura anterior la curva PFD(t) para un periodo de un año suponiendo que el cierre parcial se ejecuta cada 4 meses.

D) Teniendo en cuenta los resultados del apartado A, calcule la tasa de fallos peligrosos equivalente de una válvula con cierre parcial, es decir la que debería tener un dispositivo sin cierre parcial para lograr el mismo promedio de fallos peligrosos.

E) La técnica de cierre parcial puede considerarse como un método de autodiagnóstico del dispositivo. Bajo esa perspectiva, cuál sería la DCF de la misma.

F) ¿Puede considerarse una válvula con cierre parcial como un actuador simple, no inteligente?. ¿Pueden, por tanto, aplicarse tablas simplificadas en la estimación SIL?.

SOLUCIÓN:

A) *La figura representa la gráfica de evolución de PFD(t) para una válvula convencional (sin cierre parcial) durante un periodo de inspección de un año. Para ésta válvula calcule el promedio de fallos peligrosos en demanda $\overline{PFD}(TI)$ para un periodo de inspección TI. Indique además qué significado geométrico tiene la expresión resultante.*

Partiendo de la ecuación del promedio de fallos en un ciclo TI:

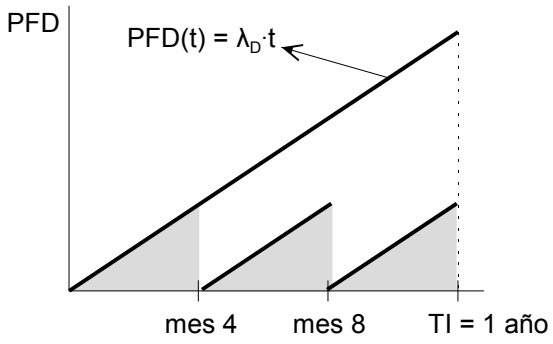
$$\overline{PFD}(TI) = \frac{1}{TI}\int_0^{TI} PFD(t)dt = \lambda_D \frac{TI}{2}$$

Geométricamente la ecuación representa la ratio entre el área bajo la curva $PFD(t)$ y el periodo de inspección TI. Para el caso particular de un dispositivo simple el valor $\lambda_D TI$ es la máxima probabilidad alcanzable en el ciclo. $\overline{PFD}(TI)$ representa la mitad de este valor.

B) *Suponiendo que el cierre parcial detecta todos los fallos peligrosos de una válvula de seguridad, dibuje sobre la figura anterior la curva PFD(t) para un periodo de un año si el cierre parcial se ejecuta cada 4 meses. Aplicando el resultado del apartado anterior, calcule el $\overline{PFD}(TI = 1a)$*

La evolución de la probabilidad de fallos con los datos del problema sería de la figura B:

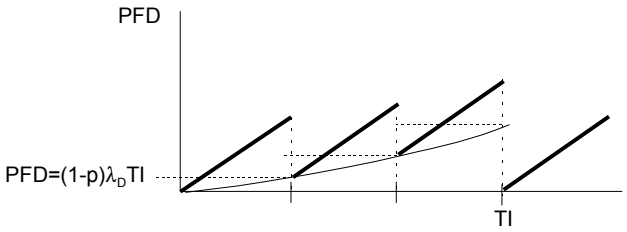
Teniendo en cuenta la interpretación del apartado anterior, el promedio de fallos lo calculamos a partir del área bajo la curva. Con 3 cierres parciales por ciclo de inspección, el resultado sería:



$$A_T = 3\lambda_D \frac{TI/3 \cdot TI/3}{2} = \lambda_D \frac{TI^2}{6}$$
$$\overline{PFD}(TI) = \frac{A_T}{TI} = \frac{1}{3}\lambda_D \frac{TI}{2}$$

C) *Suponiendo que el cierre parcial detecta un porcentaje P de los fallos peligrosos de una válvula de seguridad, dibuje sobre la figura anterior la curva PFD(t) para un periodo de un año si el cierre parcial se ejecuta cada 4 meses.*

Como dejan de detectarse $(1 - P)$ del la tasa de fallos en cada maniobra de cierre parcial, la curva que representa la probabilidad de fallo seria la siguiente:



El promedio de fallos a $TI = 1a$ se calculará sumando el

área bajo la curva anterior y dividiento por TI:

$$\begin{aligned}
A_T =& \lambda_D \frac{TI/3 \cdot TI/3}{2} \\
&+\lambda_D \frac{TI/3 \cdot TI/3}{2} + (1-P)\lambda_D TI/3 \cdot TI/3 + \\
&+\lambda_D \frac{TI/3 \cdot TI/3}{2} + (1-P)(\lambda_D TI/3 + (1-P)\lambda_D TI/3)\frac{TI}{3} \\
=& \lambda_D \frac{TI^2}{2}\frac{1}{9}[1+1+2(1-P)+1+2(1-P)+2(1-P)^2] \\
=& \lambda_D \frac{TI^2}{2}\frac{1}{9}[3+4(1-P)+2(1-P)^2] \\
\overline{PFD}(TI) =& \frac{A_T}{TI} = \lambda_D \frac{TI}{2}\frac{1}{9}[9-8P+4P^2] = \\
\approx& \lambda_D \frac{TI}{2}\left(1-\frac{8}{9}P\right)
\end{aligned}$$

D) *Teniendo en cuenta los resultados del apartado A, calcule la equivalente de una válvula con cierre parcial, es decir la que debería tener un dispositivo sin cierre parcial para lograr el mismo promedio de fallos peligrosos.*

Comparando la expresión anterior con la de un dispositivo simple:

$$\lambda_D^{eq}\frac{TI}{2} = \lambda_D \frac{TI^2}{2}\left(1-\frac{8}{9}P\right)$$
$$\lambda_D^{eq} = \left(1-\frac{8}{9}P\right)\lambda_D$$

E) *La técnica de cierre parcial puede considerarse como un método de autodiagnóstico del dispositivo. Bajo esa perspectiva, cuál sería la DCF de la misma.*

Comparando la expresión anterior con la de un dispositivo simple CON DCF

$$(1-DCF)\lambda_D\frac{TI}{2} = \lambda_D \frac{TI^2}{2}\left(1-\frac{8}{9}P\right)$$
$$(1-DCF) = 1-\frac{8}{9}P$$
$$DFC = \frac{8}{9}P$$

** El factor de cobertura de diagnósticos es prácticamente igual al porcentaje de eficiencia del cierre parcial, resultado completamente lógico.

F) *¿Puede considerarse una válvula con cierre parcial como un actuador simple, no inteligente?. ¿Pueden, por tanto, aplicarse tablas simplificadas en la estimación SIL?.*

La maniobra de cierre parcial requiere inteligencia cuya ejecución se efectuará sobre un controlador específico o mediante un PLC. En cualquier caso, habría que tratarlo como un dispositivo complejo.

Problema 18. Los elementos de una medida SIS son revisados una vez al año. Estas inspecciones permiten prevenir un 80 % de fallos.

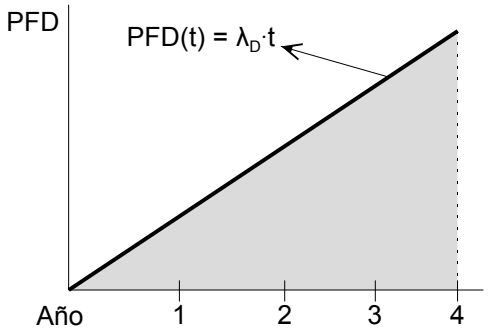
a) Dibuje gráficamente cómo evoluciona la probabilidad de fallos peligrosos en demanda durante un intervalo de 4 años desde el instante del «primer día».

b) Para evitar que la medida salga de la categoría SIL a la que ha sido diseñada para inspecciones anuales. Calcule cuál es la necesaria reducción del periodo de inspección.

c) Si los fallos no detectados por inspección fueran siempre del mismo tipo, sería aplicable todo el razonamiento anterior?.

SOLUCIÓN:

a) *Dibuje gráficamente cómo evoluciona la probabilidad de fallos peligrosos en demanda durante un intervalo de 4 años desde el instante del «primer día».*



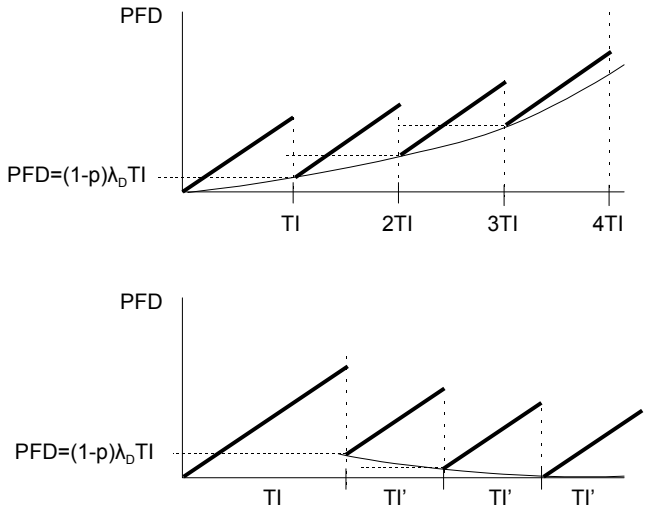
b) *Para evitar que la medida salga de la categoría SIL a la que ha sido diseñada para inspecciones anuales. Calcule cuál es la necesaria reducción del periodo de inspección.*

A largo plazo, la tendencia de la curva de fallos es a subir exponencialmente. Si se reduden los periodos de inspección,

es posible frenar este crecimiento, e incluso hacer que decaiga, también exponencialmente. La ecuación que describe la evolución del los fallos es:

$$PFD(t) = \lambda_D t + PFD(t=0) \Rightarrow \overline{PFD}(\widehat{TI}) = \lambda_D \frac{\widehat{TI}}{2} + PFD(t=0)$$

Una primera aproximación sería emplear el periodo de inspección original TI para el primer año, y reducir a partir del segundo de modo como se ilustra en la figura.



$$\begin{aligned}(1-p)PFD(TI') &< (1-p)\lambda_D TI \\ \Rightarrow PFD(TI') &< \lambda_D TI \\ \Rightarrow \lambda_D TI' + (1-p)\lambda_D TI &< \lambda_D TI \\ \Rightarrow TI' + (1-p)TI &< TI \\ TI' &< p \cdot TI\end{aligned}$$

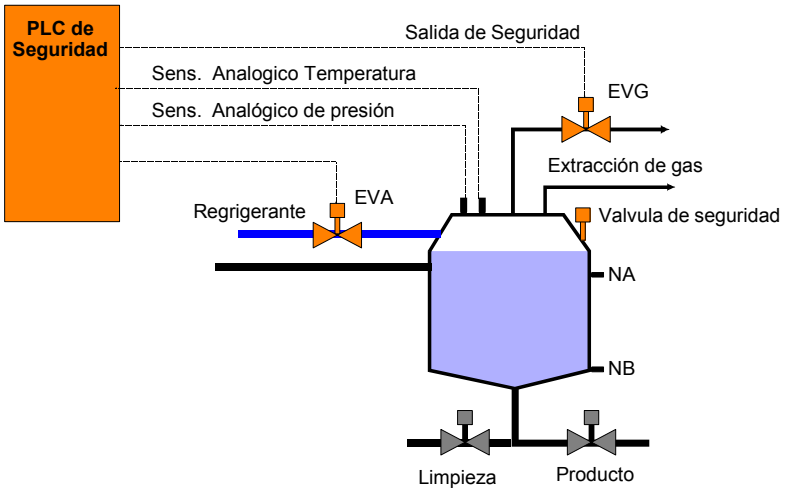
c) *Si los fallos no detectados por inspección fueran siempre del mismo tipo, sería aplicable todo el razonamiento anterior?.*

No, serían acumulativos, la probabilidad de error crecería indefinidamente.

Problema 19. En la figura se muestra un reactor químico donde la mezcla produce un gas tóxico inflamable que debe ser eliminado si se produce una elevada concentración, o si la temperatura sube por encima de cierto valor de seguridad. Para evitar ambas situaciones se han diseñado dos medidas complementarias que se implementan según la figura:

M1) Si la presión sobrepasa cierto valor, indica que existe una elevada acumulación de gases que no ha sido extraída por el sistema de control. Automáticamente se abrirá una segunda electroválvula de seguridad.

M2) Si la temperatura supera cierto umbral, fijado por debajo del valor de ignición, el sistema inyectará líquido refrigerante al depósito de mezcla abriendo una electroválvula de seguridad a tal efecto.



Sens. Presión.	Sens. Temp	PLC	EVG	EVA
$\lambda_D = 2{,}5 \cdot 10^{-7}$	$\lambda_D = 1{,}2 \cdot 10^{-7}$	$PFD = 3 \cdot 10^{-4}$	$\lambda_D = 4{,}2 \cdot 10^{-6}$	$\lambda_D = 3{,}6 \cdot 10^{-6}$
SFF = 70 %	SFF = 90 %	1 año	SFF = 80 %	SFF = 70 %
Salida 4-20mA	Salida 4-20mA)	SFF = 95 %	Entrada	$\beta = 0{,}01$
Tipo A	Tipo A	$HFT = 1$	0-24V	Entrada
				0-24V

a) Con los datos de rendimiento que se muestran en la tabla anterior, verifique el nivel SIL a DOS AÑOS de la medida 1.

b) Suponiendo que el control de temperatura (medida 2) requiere SIL3 con inspecciones anuales, diseñe los cambios necesarios para lograrlo.

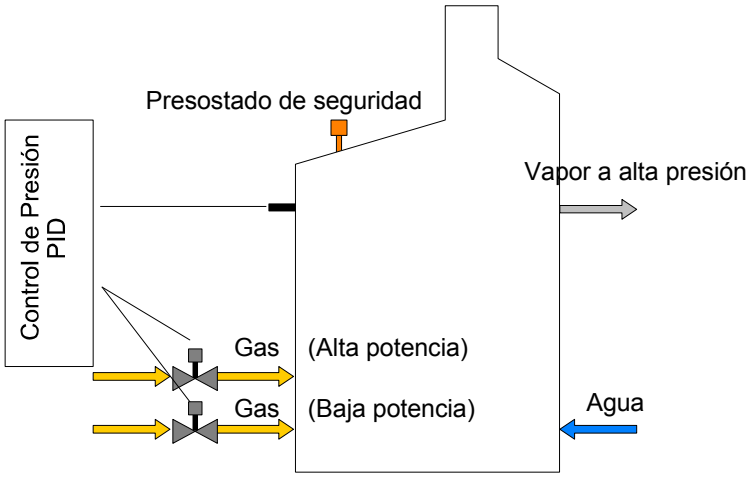
c) Diseñe la conexión de los elementos de seguridad en la instalación diseñada en el apartado anterior.

d) Desarrolle en LADDER dos unidades de programa para el control de sendas medidas de seguridad

---

SOLUCIÓN: xxx

Problema 20. La figura representa un generador de vapor pirotubular de alta presión. Un quemador de gas calienta el flujo de agua de la entrada hasta producir vapor a alta presión y temperatura. Para controlar la potencia de la llama, el generador emplea DOS TIPOS DE GAS de alto y bajo poder calorífico.



A) Describa verbalmente cuál es (¿qué debe hacer?) una función de seguridad contra la sobrepresión. Indique cómo actúan sensores, disp. lógico y válvulas.

B) B) Utilizando los límites técnicos recomendados del 35 %, 15 % y 50 % para el promedio de fallos de la etapas de sensores, LS y actuadores respectivamente, diseñe una medida SIS para el control de la PRESIÓN de vapor con una integridad SIL2 para ciclos de inspección de 1 año. Tenga en cuenta las siguientes restricciones de diseño:

- Se desea la menor redundancia posible
- Los sensores a emplear son dispositivos complejos
- Las válvulas de seguridad pueden ser tipo eléctrico

Para cada etapa de la medida SIS responda a las siguientes cuestiones:

- HFT, estructura y diagrama de rendimiento.
- Calidad mínima necesaria del componente
- Tiempo medio (mínimo) al primer fallo de los dispositivos

Electroválvula	Válvula de seguridad
$\lambda = 400\ FIT$ $SFF = 61\,\%$	$\lambda_D = 1{,}2 \cdot 10^{-6}$ $SFF = 80\,\%$ $\beta = 0{,}05$

C) Rediseñe la etapa de actuadores teniendo en cuenta que según la normativa, las válvulas de seguridad deben ser de tipo neumático. Utilice los datos de rendimiento de la tabla.

D) Las paradas de producción en un alto horno tienen un coste económico muy elevado. Por ello, una condición habitual de diseño de las medidas SIS es que posea una baja tasa de falsas alarmas producidas por los sensores. Modifique el diseño de la etapa de sensores para reducir dicha tasa **sin que aumenten los fallos peligrosos**. Para la nueva estructura, indique su diagrama de rendimiento, y calcule el PDS o promedio de falsas alarmas que se generan a lo largo de un año. Compare los resultados con el diseño original

---

SOLUCIÓN: xxx