TEMA 6. FIABILIDAD

PLANIFICACIÓN DE PROYECTOS Y ANÁLISIS DE RIESGOS

Grado en Ingeniería Informática. Mención Tecnologías de la Información

Dpto. Lenguajes y Ciencias de la Computación

UNIVERSIDAD DE MÁLAGA

TEMA 6. FIABILIDAD

- Generalidades.
- Fiabilidad de sistemas
- Árbol de fallos
- Fiabilibidad del hardware y del software

CREUS SOLE, Fiabilidad y Seguridad.

O'CONNOR, Practical reliability engineering.

Generalidades

1713 Ley de probabilidad de dos eventos independientes. Jacob Bernouilli

1942 Segunda Guerra Mundial. Peemunde base de las bombas volantes V1 y V2: el éxito de las misiones no llegaba al 30%.

- Pieruschka asumió que las componentes técnicas siguen las mismas leyes que las sustancias radiactivas y los seres vivos
- EJEMPLO: si la tasa media de fallos de cada componente es de 10^{-5} fallos/horas y el sistema incluye 100000 componentes la tasa de fallos del sistema es $100000 \cdot 10^{-5} = 1$ fallo/hora. Por lo tanto una misión de 1.5 horas tendrá una probabilidad de éxito $e^{-\lambda t} = e^{-1 \cdot 1.5} = 0.22$
- La probabilidad de éxito de un sistema es el producto de las probabilidades de éxito de sus componentes.
- Los fallos producidos en dispositivos con soluciones sencillas y débiles en apariencia eran menos frecuentes que soluciones complejas diseñadas para corregir los fallos.
- Esto condujo a mejorar la fiabilidad media de las componentes mejorando la fiabilidad del sistema

En la industria militar normas MIL

Vuelos tripulados a la luna.

Industria nuclear, electrónica, microelectrónica

Generalidades

FIABILIDAD (reliability): probabilidad de que un aparato o dispositivo trabaje correctamente un tiempo determinado en las condiciones de servicio que encuentre.

NO ES UNA PREDICCIÓN SINO UNA PROBABILIDAD: el dispositivo puede fallar nada más ponerlo en funcionamiento o más allá de su vida útil

Es necesario especificar exactamente la función que tiene que desempeñar el dispositivo

$R(t)$=Fiabilidad, función de t: $R(0)=1$, $R(\infty)=0$

Generalidades

EJEMPLOS

Fiabilidad de un microprocesador: el servicio postventa indica que de 400 unidades fabricadas se ha averiado una al cabo de 1 año de servicio.

Fiabilidad para un año=399/400=0.9975

Fiabilidad humana: probabilidad anual de errores de un operador en la lectura de instrumentos analógicos es 0.997.

Dos posibles interpretaciones:

1. en 1 año observando a 1000 operarios 3 cometieron fallos,
2. en la toma de 1000 lecturas un operario cometió 3 errores.

Generalidades

$$R(t) = \frac{N_s(t)}{N(0)} = \frac{N(0) - N_f(t)}{N(0)} = 1 - \frac{N_f(t)}{N(0)}$$

R Fiabilidad (reliability)

N_s(t) número de componentes que siguen funcionando en tiempo t

N_f(t) número de componentes que han fallado en tiempo t

$N(0)$ número de componentes al inicio del ensayo

Función de distribución de fallos: probabilidad de fallo: Infiabilidad: (faillure) Mortalidad: F(t)

F(t)=1-R(t)

Generalidades

$$R(t) = \frac{N_s(t)}{N(0)} = \frac{N(0)-N_f(t)}{N(0)} = 1 - \frac{N_f(t)}{N(0)}$$

Función de densidad de la probabilidad de fallo: representa la variación por unidad de tiempo o pendiente de la infiabilidad

$$f(t) = \frac{dF}{dt}(t) = -\frac{dR}{dt}(t) = \frac{1}{N(0)}\frac{dN_f}{dt}(t)$$

Probabilidad instantánea de fallos

$$\frac{dN_f}{dt}(t) = \mathrm{N}(0) f(t)$$

Tasa instantánea de fallos

$$\lambda(t) = \frac{1}{N_s(t)}\frac{dN_f}{dt}(t) = -\frac{N(0)}{N_s(t)}\frac{dR}{dt}(t) = -\frac{1}{R(t)}\frac{dR}{dt}(t)$$

Generalidades

Tasa instantánea de fallos

$$\lambda(t) = -\frac{1}{R(t)}\frac{dR}{dt}(t)$$

Integrando:

$\int_0^t \lambda(t)dt = -\int_0^t \frac{1}{R(t)}\ dR(t) = -LnR(t)+LnR(0) = -LnR(t)$

Fiabilidad: probabilidad de supervivencia:

$$R(t) = e^{-\int_0^t \lambda(t)dt}$$

$$f(t) = \lambda(t)e^{-\int_0^t \lambda(t)dt}$$

La tasa de fallos puede ser creciente o decreciente o tomar valores diferentes según el tiempo transcurrido

Si la tasa instantánea de fallos λ es constante se obtiene

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

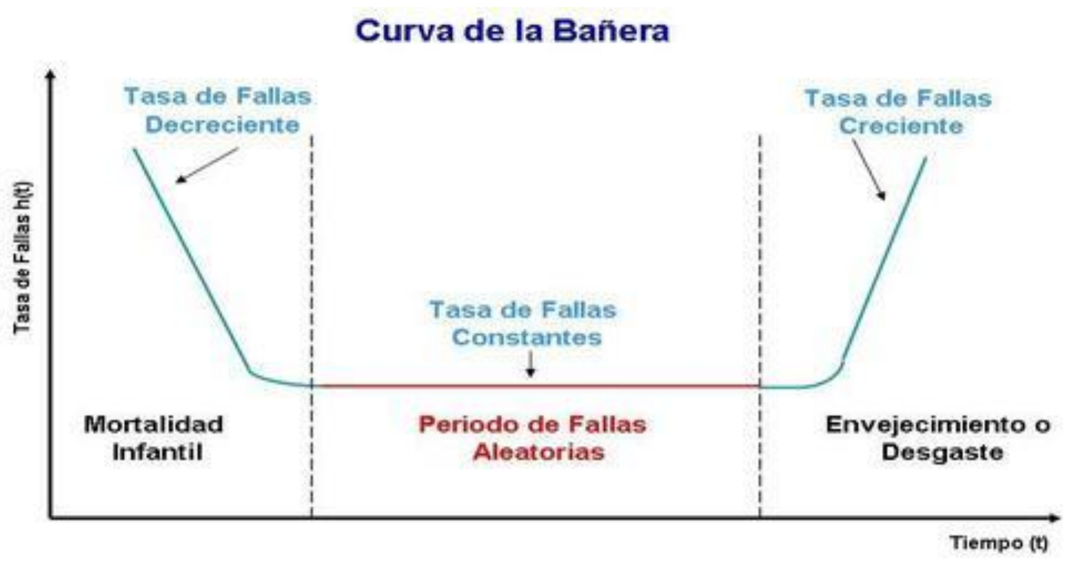
λ es la frecuencia con que se presentan los fallos en las componentes y se suele expresar en fallos/hora .

Su inversa es el tiempo medio entre fallos

Generalidades

Tasa instantánea de fallos: curva de la bañera

- Fallos iniciales o infantiles: corresponde a la existencia de dispositivos defectuosos con una tasa de fallo superior a la normal. Disminuye con el tiempo hasta alcanzar un valor casi constante
- Operación normal o de fallos constantes o aleatorios: vida útil del dispositivo
- Fallos de desgaste o envejecimiento



Generalidades

Vida media: valor matemático esperado del tiempo entre fallos (dispositivo reparable) o el tiempo medio para el primer fallo (dispositivo no reparable)

$$\int_0^\infty tf(t)dt = \int_0^\infty -t\,\frac{dR}{dt}(t)dt = -tR(t)|_0^\infty + \int_0^\infty R(t)dt = \int_0^\infty R(t)dt$$

Si λ es constante $R(t) = e^{-\lambda t}$ y la vida media es $\int_0^\infty R(t)dt$=1/ λ

EJEMPLO

El número de fallos/año de un circuito de alarmas es 0.4. Suponiendo una distribución exponencial con tasa de fallos constantes su vida media es 1/0.4=2.5 años

Generalidades

FUNCIONES DE DISTRIBUCIÓN DE FALLOS

Distribuciones discretas: los valores de las componentes no pueden subdividirse y mezclarse unos con otros, están representados por números enteros

- Binomial
- Poisson

Distribuciones continuas: los valores de las componentes pueden subdividirse y mezclarse unos con otros. Están representados por números reales

- Exponencial
- Normal
- Log-normal
- Weibull

Generalidades

DISTRIBUCIÓN BINOMIAL (O DE BERNOUILLI)

Proporciona la probabilidad de obtener un número especificado de éxitos en un conjunto finito de pruebas independientes con la misma probabilidad de éxito. Cada prueba sólo puede resultar éxito o fracaso

p= probabilidad de fallo
q= probabilidad de no fallo

$$p+q=1$$

Probabilidad de que en una muestra de tamaño n haya k fallos=P[D=k]

$$P[D=k]=\binom{n}{k}p^k q^{n-k}$$

Puede aproximarse por una normal cuando n es grande en cuyo caso $\mu=np$ y $\sigma^2=npq$

Generalidades

DISTRIBUCIÓN BINOMIAL (O DE BERNOUILLI)

EJEMPLO

Probabilidad de obtener en una línea de fabricación de condensadores dos unidades defectuosas al muestrear 5 si en el lote del que se extraen las muestras el 4% de los componentes son defectuosos

p= probabilidad de condensador defectuoso (0.04)
q= probabilidad de condensador sin defecto (0.96)

Probabilidad de que en una muestra de tamaño 5 haya 2 defectuosos

$$P[D=2]=\binom{5}{2}0.04^2 0.96^3$$

Generalidades

DISTRIBUCIÓN DE POISSON

Caso particular de la binomial cuando n es muy grande ($n>100$) y p muy pequeño ($p<0.05$)

Proporciona la probabilidad de obtener un número especificado de éxitos en un conjunto finito de pruebas independientes todas con la misma probabilidad de éxito. Cada prueba sólo puede resultar éxito o fracaso

Probabilidad de que en una muestra de tamaño n haya k defectuosos=P[D=k]

$$P[D = k] = \frac{(np)^k}{k!} e^{-np}$$

Puede aproximarse por una normal cuando n es grande en cuyo caso $\mu=np$ y $\sigma^2=npq$

Generalidades

DISTRIBUCIÓN DE POISSON

EJEMPLO

Probabilidad de fallo de un circuito en una alarma electrónica es 0.003.
Calcular la probabilidad de que fallen 3 alarmas en una serie de 3000

p= probabilidad de condensador defectuoso (0.003)
q= probabilidad de condensador sin defecto (0.997)

Probabilidad de que en una muestra de tamaño 3000 haya 3 defectuosos

$$P[D=3]=\frac{(3000\cdot 0.003)^3}{3!}e^{-3000\cdot 0.003}=\frac{9^3}{6}e^{-9}=0.015$$

Generalidades

DISTRIBUCIÓN CONTINUA

EJEMPLO

Un medidor de nivel de sólidos de sondeo electromagnético que trabaja en un ambiente de polvo adherente tiene una vida media de 2000 horas tras las cuales el cable que sostiene el peso puede quedar trabado en la polea por el polvo adherido y dejar de funcionar.

Tasa de fallos: 1/2000=0.0005 fallos/hora

Fiabilidad durante 10 horas: R(10),

$R(10) = e^{-0.0005\cdot 10}$=0.995

Fiabilidad al cabo de 2000 horas: R(2000),

$R(2000) = e^{-0.0005\cdot 2000}$=0.36

Tiempo medio entre fallos:

2000 horas

Fiabilidad de sistemas

SISTEMAS EN SERIE
Están en operación sólo si todas sus componentes operan

Su fiabilidad es el producto de las fiabilidades de sus componentes

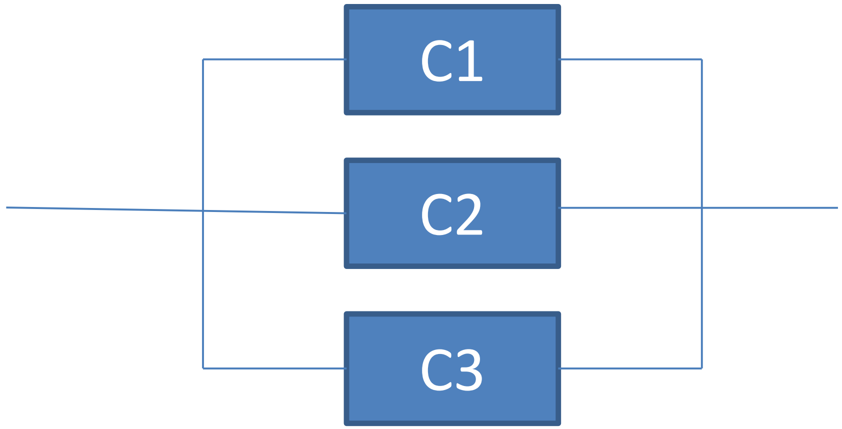
La fiabilidad del sistema es menor que la de cualquiera de sus componentes

EJEMPLO
Dos válvulas de solenoides en serie en un circuito con tasas de fallo individuales 0.05 fallos/año. La tasa de fallo conjunta es 0.05+0.05=0.1 y la fiabilidad del conjunto en un año es
$e^{-0.1}$=0.9048

Fiabilidad de sistemas

SISTEMAS EN PARALELO

El sistema falla sólo si todas sus componentes fallan



Su no fiabilidad es el producto de las no fiabilidades de sus componentes

La fiabilidad del sistema es mayor que la de cualquiera de sus componentes.

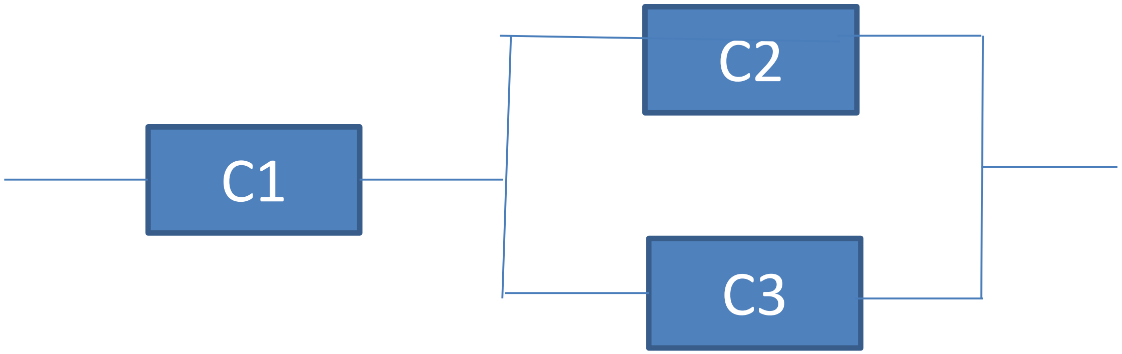
Puede conseguirse una alta fiabilidad del sistema con componentes de fiabilidad moderada

EJEMPLO

Dos válvulas de solenoides en paralelo con tasas de fallo individuales 0.05 fallos/año. La no fiabilidad conjunta en un año es $(1-e^{-0.05})\cdot(1-e^{-0.05})=0.00238$ y la fiabilidad del conjunto en un año es $1-0.00238=0.99762$

Fiabilidad de sistemas

COMBINACIONES SERIE-PARALELO
Cuando existen estructuras combinadas pueden subdividirse secuencialmente en serie y paralelo para llegar a la expresión final de la fiabilidad resultante



C1, C2, C3 con distribuciones exponenciales con tasas de fallo individuales 0.05, 0,1 y 0.2 respectivamente

Fiabilidades individuales en 1 año

$R1=e^{-0.05}=0.9512$, $R2=e^{-0.1}=0.9048$, $R3=e^{-0.2}=0.8187$.

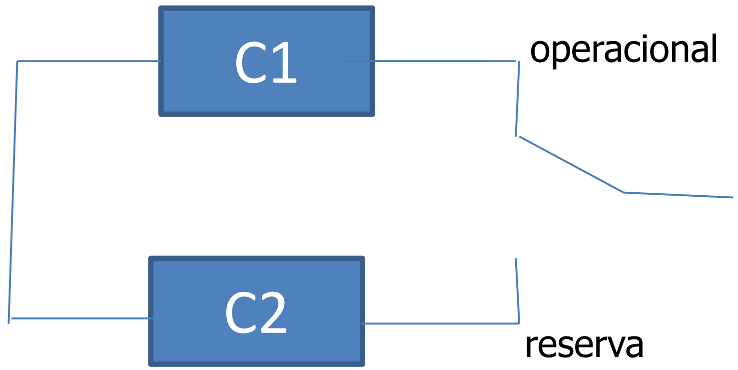
Fiabilidad conjunta en un año

$R=R1\cdot(1-(1-R2)(1-R3))=0.9348$

Fiabilidad de sistemas

SISTEMAS EN RESERVA

Las componentes en reserva permanecen desactivadas y en paralelo con las componentes en operación entrando en servicio cuando el sistema falla.

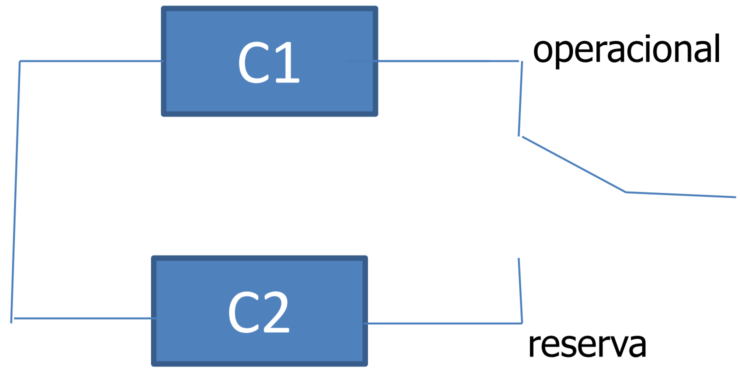


La fiabilidad de un sistema en reserva formado por dos componentes, el operacional y el de reserva es la probabilidad de que la unidad operacional funcione en tiempo t o que si ha fallado en tiempo t1 y las unidades de captación y conmutación del fallo funcionen con éxito y que la unidad de reserva no falle:

$$\mathrm{R(t)} = R_1(\mathrm{t}) + \int_0^t f1(\tau) R_2(t-\tau)\, d\tau$$

Fiabilidad de sistemas

SISTEMAS EN RESERVA



Suponiendo λ_1 tasa de fallos del sistema operacional y λ_2 la tasa de fallos del sistema de reserva:

$R1(t)=e^{-\lambda_1 t}$

$R2(t-t1)=e^{-\lambda_2 (t-t1)}$

$$f1(t1) = \lambda_1 e^{-\lambda_1 t_1}$$

$$R(t) = \begin{cases} e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_2 (t-\tau)} d\tau = e^{-\lambda_1 t} + \lambda_1 \frac{e^{-\lambda_2 t}}{\lambda_1 - \lambda_2} \left(1 - e^{-(\lambda_1 - \lambda_2)t}\right) \; si \; \lambda_1 \neq \lambda_2 \\ e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_1 (t-\tau)} d\tau = e^{-\lambda_1 t} + \lambda_1 t e^{-\lambda_1 t} \quad si \quad \lambda_1 = \lambda_2 \end{cases}$$

Fiabilidad de sistemas

SISTEMAS EN RESERVA. EJEMPLO

El circuito de agua de alimentación de una caldera de vapor dispone de dos bombas centrífugas en paralelo de las cuales una está en marcha y la otra en reserva (tasa de fallos: 0.1 fallos/año)

Si se supone que la conmutación de una a otra es instantánea y sin fallos la fiabilidad del sistema en dos años se calcula como
R(2)=$e^{-0.1\cdot 2}(1+0.1\cdot 2)$=0.9824

Si se supone que la conmutación de una a otra puede fallar y su fiabilidad es de 0.002, la fiabilidad del sistema en dos años se calcula como
R(2)=$e^{-0.1\cdot 2}(1+0.002\cdot 0.1\cdot 2)$=0.8190

Fiabilidad de sistemas

PROCESOS ESTOCÁSTICOS

- Un proceso estocástico de tiempo discreto es una descripción de la relación entre las variables aleatorias X_0,X_1,...que representan alguna característica de un sistema en puntos discretos en el tiempo.
  - Ejemplo: ruina del jugador: inicialmente tengo 2€, en los tiempos 1,2,... participo en un juego en el que apuesto 1€ que gano con probabilidad p y pierdo con probabilidad 1-p. Dejo de jugar cuando mi capital es 4€ o he perdido todo mi capital. Si X_i es la cantidad de dinero que tengo en el tiempo i, X_0,X_1,... es un proceso estocástico.
- Un proceso estocástico de tiempo continuo es un proceso estocástico en el que el estado del tiempo se puede examinar en cualquier tiempo.
  - Ejemplo: número de personas en un supermercado a los t minutos de abrir

Fiabilidad de sistemas

CADENAS DE MARKOV

- Cadena de Markov: proceso estocástico de tiempo discreto que para t=0,1,2,... y todos los estados verifica

  $P(X_{t+1}=i_{t+1} \mid X_t=i_t, X_{t-1}=i_{t-1}, \ldots, X_1=i_1, X_0=i_0)=P(X_{t+1}=i_{t+1} \mid X_t=i_t)$

- Hipótesis de estabilidad: $P(X_{t+1}=j \mid X_t=i)=p_{ij}$ (no depende de t)
- Probabilidades de transición: p_{ij}
- Matriz de probabilidades de transición:

$$P=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1s} \\ p_{21} & p_{22} & \cdots & p_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ p_{s1} & p_{s2} & \cdots & p_{ss} \end{bmatrix}$$

- Se debe verificar: $\sum_{j=1}^{s} p_{ij} = 1$
- Distribución inicial de probabilidad de una cadena de Markov: $q=[q_1,\ldots,q_s]$ donde $q_i=P(X_0=i)$

Fiabilidad de sistemas

PROBABILIDADES DESPUÉS DE N PASOS

- Si una cadena de Markov estacionaria está en el estado i en el tiempo m, ¿cuál es la probabilidad de que n períodos después la cadena esté en el estado j?

  $P(X_{m+n}=j|X_m=i)=P(X_n=j|X_0=i)=P_{ij}(n)$

- $P_{ij}(n)$ es la probabilidad en la etapa n de una transición del estado i al estado j

  $P_{ij}(1)=p_{ij},\quad P_{ij}(2)=\sum_{k=1}^{s} p_{ik}\,p_{kj}\quad P_{ij}(n)=$ elemento ij-ésimo de P^n

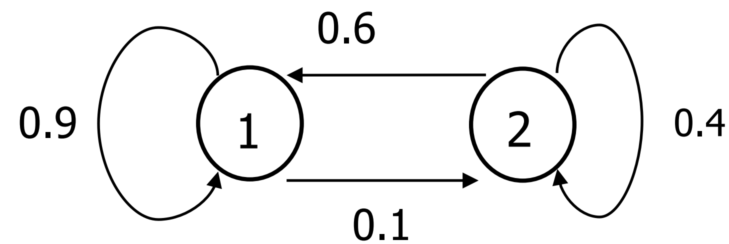
- Probabilidad de estar en el estado j en el tiempo n = $\sum_{i=1}^{s} q_i P_{ij}(n)$

Fiabilidad de sistemas

EJEMPLO

- Sea un componente único reparable con sólo dos estados: 1 disponible, 2 fallo.
- La probabilidad de mantenerse disponible al cabo de un mes es 0.9 y de estando en fallo pasar a disponible es 0.6
- Matriz de probabilidades de transición:

$$P = \begin{bmatrix} 0.9 & 0.1 \\ 0.4 & 0.6 \end{bmatrix}$$



- ¿Probabilidad de disponibilidad al cabo de dos meses? ¿De tres meses?

Árbol de fallos

1961-62 Bell Telephone Laboratories. H.A. Watson

A partir de 1970 se generaliza su uso mediante el ordenador

Un árbol de fallos es la representación o desarrollo gráfico deductivo desde el evento principal o suceso final no deseado o peligroso, TOP EVENT, pasando por todas las combinaciones de eventos intermedios hasta llegar a sus causas o eventos básicos que representan el límite de resolución del árbol

Evento: adopción de la variable de uno de los dos estados posibles: seguridad o fallo

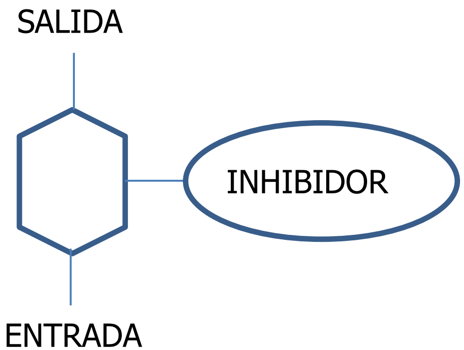
En los sistemas complejos es conveniente seguir también el camino directo o hacia adelante para identificar los diferentes eventos peligrosos o Top Event que permitan realizar un análisis completo del sistema

Árbol de fallos

SÍMBOLOS LÓGICOS

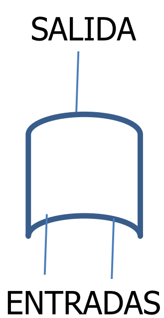
EVENTO BÁSICO: fallo de inicialización a otros eventos de fallo que no pueden descomponerse y que es la partida del árbol

EVENTO INTERMEDIO: resulta de las interacciones con otros elementos

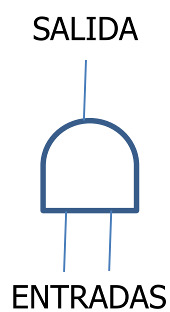


EVENTO DE CONDICIONAMIENTO

Inhibidor: el evento de salida ocurre si se presenta el de entrada y se satisface la condición de inhibición



PUERTA O: el fallo de salida se produce si ocurre cualquiera de los fallos de entrada

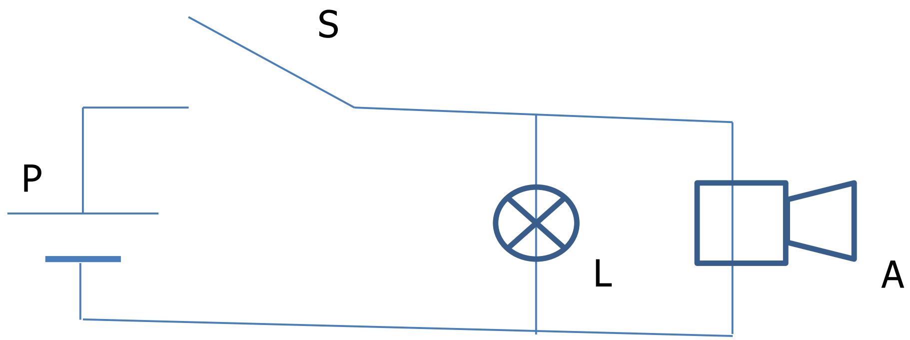


PUERTA Y: el fallo de salida se produce si ocurren simultáneamente todos los de entrada

Árbol de fallos

EJEMPLO

Circuito de alarma formado por una pila, un interruptor y una lámpara y una bocina en serie



Fallo principal: TOP EVENT: fallo del encendido de la lámpara y la bocina

Se supone la integridad de los hilos conductores y conectores (no fallan)

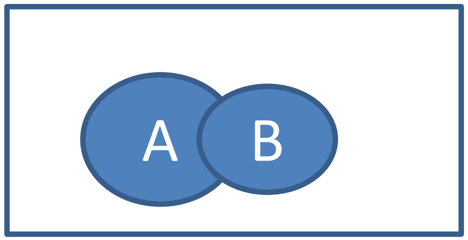
Condiciones iniciales de funcionamiento: P, S, L y A funcionan

Eventos básicos:

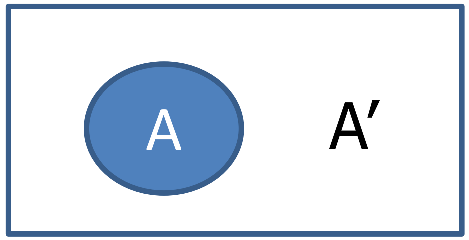
- E1: pila gastada
- E2: fallo en S
- E3: fallo en L
- E4: fallo en A

Árbol de fallos

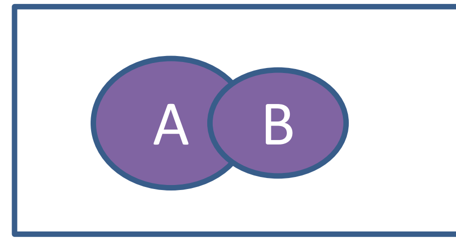
ALBEGRA LÓGICA O DE BOOLE



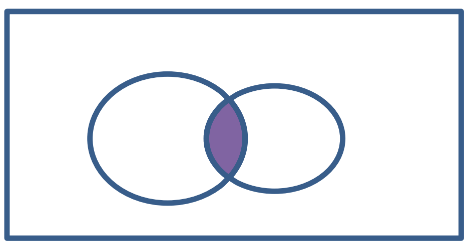
A y B



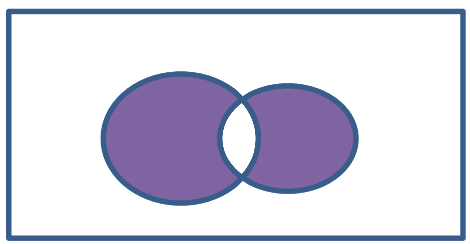
Complementario de A



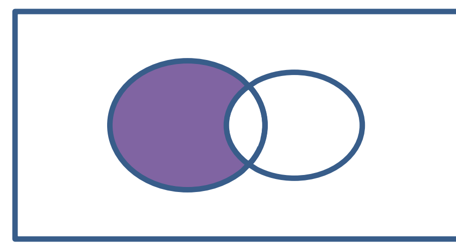
Unión: A+B



Intercesión: A·B



Diferencia simétrica: A∩B



Diferencia: A-B

Árbol de fallos

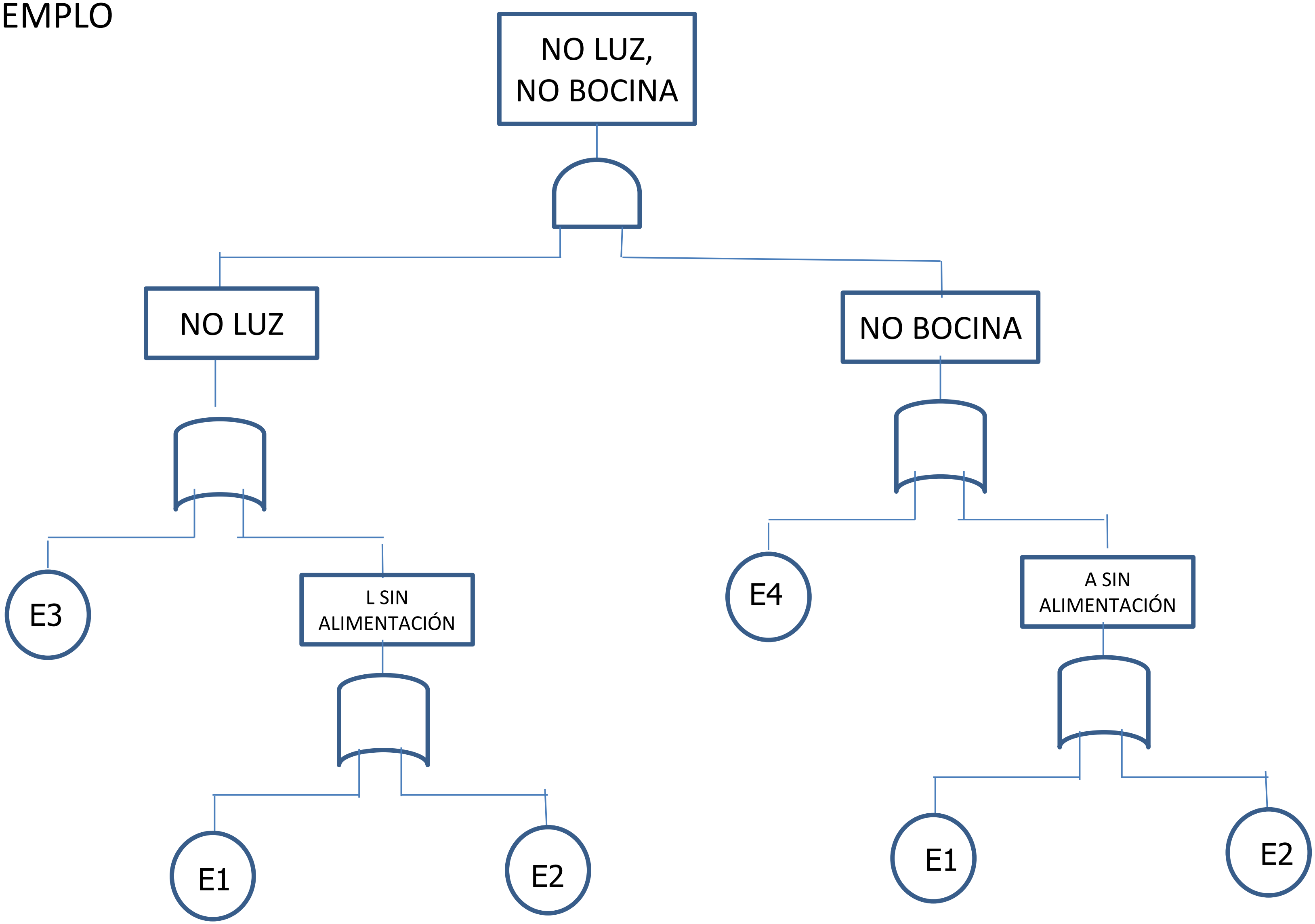
ALBEGRA LÓGICA O DE BOOLE

LEYES:

- Conmutatividad: A+B=B+A, A·B=B·A
- Asociatividad: (A+B)+C=(A+B)+C=A+B+C, (A·B)·C=(A·B)·C=A·B·C
- Distributividad: (A+B)·C=A·C+B·C; A+(B·C)=(A+B)·(A+C)
- Absorción: A+A=A, A·A=A
- Leyes de Morgan: (A+B)’=A’·B’, (A·B)’=A’+B’

Árbol de fallos

EJEMPLO



Árbol de fallos

Método de la matriz: se basa en convertir cada puerta en eventos básicos empezando por el Top Event y siguendo por la matriz hasta que todas las puertas están resueltas

Puertas O: la primera entrada sustituye al identificador de la puerta y todas las demás entradas se insertan en las siguientes filas disponibles una entrada por fila. Si existen otras entradas en la fila donde aparece la puerta éstas deben repartirse en todas las filas que contengan entradas de la puerta

Puertas Y: la primera entrada sustituye al identificador de la puerta y todas las demás entradas se insertan en las siguientes columnas disponibles una entrada por columna en la misma fila

$$\begin{array}{c} A \\ \\ \\ \end{array} \qquad\qquad \begin{array}{cc} B & C \\ & \\ & \\ \end{array} \qquad\qquad \begin{array}{cc} E3 & E4 \\ D & E \\ & \\ \end{array} \qquad\qquad \begin{array}{cc} E3 & E4 \\ E1 & E1 \\ E2 & E2 \end{array}$$

Top=E3·E4+E1·E1+E2·E2

Si se conocen las probabilidades de cada evento puede calcularse la probabilidad del evento principal.

A=Top

B=E3+(E1+E2)

C=E4+(E1+E2)

Fiabilidad del hardware

FALLOS QUE PUEDE EXPERIMENTAR EL HARDWARE

- Fallos en el diseño, en la fabricación , en el uso y en el mantenimiento
- Calentamiento exagerado de las componentes con aviso evidente de fallo
- Fallos por tiempo de operación o por tiempo almacenado sin uso
- Factores ambientales: polvo, corrosión…

La fiabilidad del hardware puede predecirse a partir del conocimiento del diseño y los factores de uso de sus componentes

Los fallos de hardware siguen la típica curva de la bañera:

- Fallos infantiles: durante su desarrollo y fabricación se detectan y corrigen los errores hasta que se mantiene uniforme el funcionamiento del equipo y se entrega al usuario
- Fallos aleatorios durante la vida útil
- Fallos de desgaste aumentando al final de la vida útil del equipo

Fiabilidad del hardware

TÉCNICAS PARA AUMENTAR LA FIABILIDAD DEL HARDWARE

PREVENCIÓN DE FALLOS: Utilizando componentes fiables, interconexiones seguras…

TOLERANCIA A LOS FALLOS: Se acepta que se puedan producir fallos pero se aporta redundancia al equipo para contrarrestar los fallos y que siga funcionando

SEGURIDAD ANTE LOS FALLOS: ante un fallo el equipo pasa a posición de seguridad para evitar daños

Fiabilidad del software

El concepto de fiabilidad del software no es adecuado desde el punto de vista del fabricante: la fiabilidad es una probabilidad y el software es un programa: si contiene errores la probabilidad de fallo es 1 bajo ciertas circunstancias y 0 si dichas circunstancias no se presentan.

El concepto tasa de fallos tampoco es adecuado: si el programa es correcto funciona sin fallos

El usuario no siempre distingue fallos de hardware y software. Los fallos de software se producen cuando el programa no realiza lo que espera de él.

Fiabilidad del software

La fiabilidad del software es una medida de la aproximación con que los requerimientos del usuario son satisfechos por el programa.

Durante el período de pruebas la fiabilidad del software varía con el tiempo porque se corrigen los errores que se descubren.

Tras el lanzamiento comercial la fiabilidad permanece constante a no ser que se realicen nuevas versiones.

Los errores pueden deberse a una mala especificación de los requisitos funcionales, incorrecta selección de los métodos de resolución, uso indebido de la estructura de datos, errores al enlazar los módulos…