FTF

Tema 5: Técnicas de Evaluación de la Fiabilidad

1.- Introducción

2.- Funciones para la evaluación de STFs

3.- Técnicas de modelado

- Arboles de fallos
- Modelos combinatorios
- Cadenas de Markov

4.- Modelado con coberturas

5.- Modelos de Markov para la fiabilidad

6.- Modelos de Markov para la Modelo para la seguridad

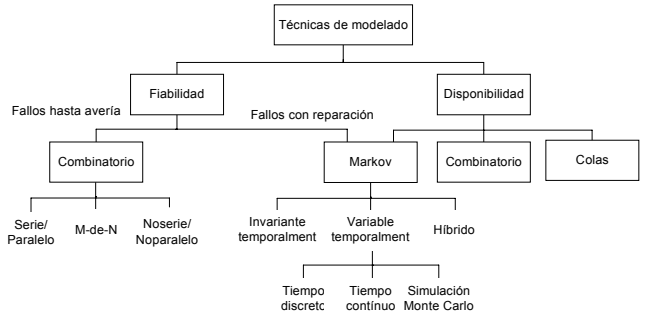
7.- Modelos de Markov para la disponibilidad

8.- Ejemplos

FTF

1 - Introducción

- La evaluación de la garantía de funcionamiento de un STF es necesaria para demostrar el buen funcionamiento de los distintos mecanismos de tolerancia a fallos que éste incluye y consecuentemente poder poner cierta confianza en el servicio que proporciona el sistema.
- Tiene como objetivo el realizar una estimación cuantitativa de las características de garantía de funcionamiento de un sistema
- Permite realizar comparaciones entre diferentes STFs dependiendo de sus especificaciones de funcionamiento
- Para evaluar la fiabilidad se utilizan diferentes técnicas de modelado, dependiendo de las suposiciones de operación del sistema (degradación y reparación)



FTF

- Los criterios de evaluación utilizan dos técnicas básicas
  - Modelado determinista: Calcula el nº máximo de fallos que tolera el sistema
  - Modelado probabilístico: Se basa en las tasas de fallos y de recuperación de los componentes

MODELO	CRITERIO
Determinista	Se sobrevive a al menos k fallos
Probabilístico	*Funciones* Función tasa de fallos $z(t)$ Fiabilidad $R(t)$ Tiempo de misión $MT(r)$ Tasa de reparación μ Disponibilidad $A(t)$ *Parámetros* Tiempo medio al fallo (MTTF) Tiempo medio de reparación (MTTR) Tiempo medio entre fallos (MTBF) Cobertura *Medidas comparativas* Diferencia en la fiabilidad $R_2(t) - R_1(t)$ Ganancia de fiabilidad $R_2(t) / R_1(t)$ Incremento del tiempo de misión $MT_2(r) / MT_1(r)$ Indice de incremento en la fiabilidad log R_{viejo} / log R_{nuevo}

- Se utilizan 4 niveles de modelado:
  - Nivel de sistema, nivel de módulo, nivel de puertas y nivel de componentes
- En los sistemas con degradación hay que estudiar las prestaciones ante los fallos

FTF

2 - Funciones para la evaluación de STFs

- R(t) - Función de fiabilidad: Es la probabilidad de que el sistema funcione correctamente durante un intervalo de tiempo
  - Si considero T como una v.a. que mide el tiempo que transcurre hasta el próximo fallo y F(t) es su función de distribución.

$$F(t) = P[T \le t] = \int_0^t f(t)dt$$

  - La fiabilidad se calcula como:

$$R(t) = 1 - F(t) = P[T > t]$$

Si T sigue una distribución exponencial $f(t) = \lambda e^{-\lambda t}$

$$F(t) = \int_0^t \lambda e^{-\lambda t} = 1 - e^{-\lambda t} \quad \rightarrow \quad R(t) = e^{-\lambda t}$$

  - La fiabilidad (y no-fiabilidad) de un componente en un instante t viene dada por:

$$R(t) = \frac{N_0(t)}{N} = \frac{N_0(t)}{N_0(t) + N_f(t)} \qquad Q(t) = \frac{N_f(t)}{N} = \frac{N_f(t)}{N_0(t) + N_f(t)} = 1 - R(t)$$

FTF

- Z(t) - Función Tasa de fallos (*Hazard function*)
  - Si diferenciamos el número de componentes que han fallado en un instante t con respecto al tiempo, obtenemos la tasa de fallos instantánea de esos componentes. Dividiendo este valor por el número de componentes que aún están operativos en ese instante, obtenemos la función tasa de fallos o función de riesgo del componente.

$$z(t) = \frac{1}{N_0(t)} \frac{dN_f(t)}{dt} = \frac{1}{N_0(t)} \left(-N \frac{dR(t)}{dt} \right) = -\frac{\frac{dR(t)}{dt}}{R(t)} = \frac{\frac{dQ(t)}{dt}}{1 - Q(t)}$$

En fallos por unidad de tiempo

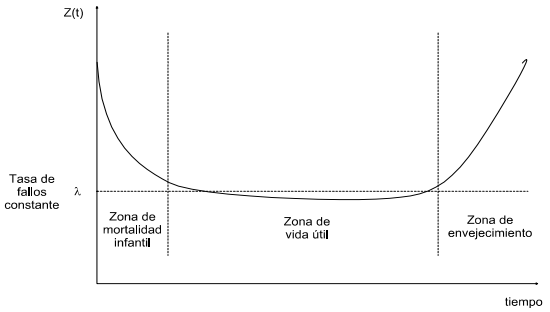
  - La tasa de fallos instantánea se calcula también como la P de que un superviviente en t, falle en un instante t + Δt, cuando $\Delta t \to 0$

$$P(t < X < t + \Delta t \,/\, X > t) = \frac{P(t < X < t + \Delta t)}{P(X > t)} = \frac{F(t + \Delta t) - F(t)}{R(t)}$$

$$Z(t) = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{R(t)} = \frac{\frac{dF(t)}{dt}}{R(t)} = \frac{f(t)}{R(t)}$$

FTF

Distribución de la tasa de fallos



La función tasa de fallos depende claramente del tiempo, sin embargo la experiencia muestra que para los componentes electrónicos existe un periodo de tiempo en donde es practicamente constante

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

Si integramos la ec. diferencial $R(t) = e^{-\lambda t}$

A la relación entre la fiabilidad y el tiempo de se denomina *Ley de fallos exponencial*: Para un valor constante de la función tasa de fallos, la fiabilidad varía exponencialmente con el tiempo
En el sw, la tasa de detección de fallos no es constante por lo que se utilizan funciones que se basan en la D. de Weibull

FTF

Cálculo de la tasa de fallos

- Es fácil de medir si conocemos la historia de la vida del componente
  - Se calcula teniendo en cuenta el tiempo entre los fallos
- Se puede estimar mediante el estándar MIL-HDBK-217
  - El modelo calcula la tasa de fallos usando los datos experimentales de componentes reales.
  - La tasa de fallos constante de un circuito integrado viene dada por la expresión:

$$\lambda = \pi_L \pi_Q (C_1 \pi_T + C_2 \pi_E) \pi_P \qquad \text{fallos por millón de horas}$$

- L (factor de aprendizaje): Representa la madurez del proceso de fabricación (de 1 a 10)
- Q (factor de calidad): Mide el nº de tests recibidos antes de ser vendido (de 1 a 300)
- T (factor de temperatura): Su valor es una función de la tecnología de fabricación

$$\pi_T = 0.1 e^{-8121\left(\frac{1}{T_J+273}-\frac{1}{298}\right)} \qquad \pi_T = 0.1 e^{-4794\left(\frac{1}{T_J+273}-\frac{1}{298}\right)}$$

- E (factor ambiental): Depende de lo ruidoso que sea el entorno (de 0'2 a 10)
- P (factor de terminales): Depende del número de terminales (de 1'0 a 1'2)
- Los factores de complejidad son función del nº de puertas para los circuitos lógicos, del nº de transistores para los circuitos lineales y del nº de bits para las memorias.

FTF

- MTTF - Tiempo medio hasta la avería: Es el tiempo medio en que trabajará un sistema antes de que se estropee por primera vez
  - Si tenemos N sistemas idénticos que empiezan a funcionar en el instante t = 0 y medimos el tiempo que tarda cada uno en averiarse, la media de estas medidas constituye el MTTF.
  - Si T es una v.a. que mide el tiempo que tarda un componente en averiarse

$$E[T] = MTTF = \int_0^\infty t f(t)dt = \int_0^\infty t \frac{dQ(t)}{dt} dt = -\int_0^\infty t \frac{dR(t)}{dt} dt = \int_0^\infty R(t)dt$$

D. Exponencial: MTTF = 1 / λ R(MTTF) = e^{-1} = 0'3678

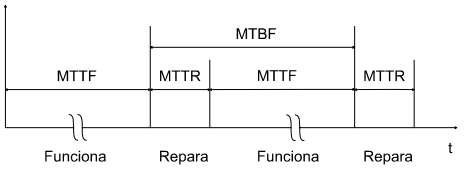
- MTTR - Tiempo medio de reparación: Indica el tiempo medio que se necesita para reparar un sistema
  - Su valor se calcula experimentalmente inyectando fallos y calculando el t de reparación
  - Se expresa mediante una tasa de reparación μ que es el nº medio de reparaciones por u. t.

$$MTTR = \frac{1}{\mu} \qquad \text{En horas}$$

  - La reparación requiere: desmontar, diagnosis, cambiar componente, comprobar, montar
    - La diagnosis gasta el 80 % del tiempo ---- Uso de circuitos BIST

FTF

- MTBF - Tiempo medio entre fallos: Es el tiempo medio que transcurre entre dos averías consecutivas de un sistema
  - Para calcularlo se tiene que tener en cuenta el tiempo necesario para reparar el sistema y volverlo a poner en funcionamiento
  - Se aplica únicamente a sistemas reparables
    - Si consideramos que al reparar un sistema, este queda como nuevo (en las mismas condiciones que cuando se puso en funcionamiento por primera vez), existe una relación entre MTTF, MTTR y MTBF:



- A(t) - Disponibilidad: Define la probabilidad de que el sistema esté funcionando en un tiempo determinado
  - Se aplica a sistemas reparables
  - A veces importa más la P de que el sistema este funcionando que la P de fallo
  - Intuitivamente, A(t) = tiempo total del sistema operativo / tiempo desde la instalación

FTF

–En el estado estable (tiempo infinito) la disponibilidad depende
- •Tiempo medio entre fallos
- •Tiempo de reparación del sistema

Si un sistema experimenta *N* fallos a lo largo de su vida, estará N*MTTF horas operativo y N*MTTR horas en reparación. La disponibilidad media será

$$A_{SS} = \frac{N * MTTF}{N * MTTF + N * MTTR} = \frac{MTTF}{MTTF + MTTR}$$

Para tasas de fallos y de reparación constante $A_{SS} = \frac{\mu}{\lambda + \mu}$

- MT(r) - Función del Tiempo de Misión:
  - Calcula el tiempo a partir del cual la fiabilidad de un sistema se reduce por debajo de un cierto nivel r. Se aplica en sistemas con necesidades de un tiempo de vida mínimo
    - Imposibilidad de reparación / Reparación cara / Con mantenimiento periódico

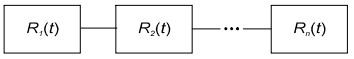
$$R[MT(r)] = r \qquad MT[R(t)] = t$$

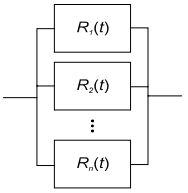
  - Para un sistema con una tasa de fallos constante

$$MT(r) = \frac{-\ln r}{\lambda}$$

3 - Técnicas de modelado

- **Modelos combinatorios**
  - Se utilizan en sistemas sencillos sin reparación para modelar la fiabilidad
  - Cada parte del sistema se representa con un bloque en estado operativo o de fallo
  - Se utilizan dos modelos: Modelo serie y modelo paralelo
  - Se mezclan para calcular la fiabilidad de un conjunto



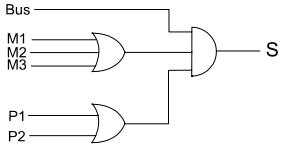


$$R_{serie}(t) = R_1(t)R_2(t)\cdots R_N(t) = \prod_{i=1}^{N} R_i(t)$$

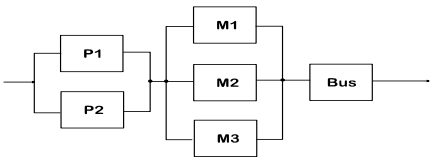
$$R_{serie}(t) = e^{-\lambda_1 t}e^{-\lambda_2 t}\cdots e^{-\lambda_N t} = e^{-\sum_{i=1}^{N}\lambda_i t}$$

$$R_{paraleo}(t) = 1 - Q_{paralelo}(t) = 1 - \prod_{i=1}^{N} Q_i(t) = 1 - \prod_{i=1}^{N}(1 - R_i(t))$$

- **Arboles de fallos**
  - Es un método gráfico que se aplica a los casos más simples
  - El sistema se representa como un árbol de puertas AND y OR
  - La salida del árbol tiene una función lógica que representa la fiabilidad del conjunto
  - Para un sistema con 2 procesadores y 3 módulos de memoria conectados por un bus



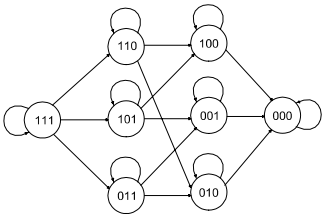
  - El sistema funciona si al menos funcionan un Procesador, una Memoria y el bus
  - El diagrama de bloques para el cálculo combinatorio es:



$$R_c(t) = \left[R_{P1}(t) \parallel R_{P2}(t)\right] \bullet \left[R_{M1}(t) \parallel R_{M2}(t) \parallel R_{M3}(t)\right] \bullet \left[R_{Bus}(t)\right]$$

FTF

- **Modelos de Markov**
  - Desventajas de los modelos combinacionales:
    - No es fácil modelar sistemas complejos de forma combinacional.
    - La inclusión de la cobertura en estos modelos es bastante difícil.
    - No contemplan el proceso de reparación y de reconfiguración de los sistemas.
    - No se ve el estado en el que se encuentra el sistema
  - Se basan en los Procesos de Markov (Cadenas de Markov si el nº de estados es finito)
    - Son procesos estocásticos (la v.a. es el tiempo)
    - Tienen ausencia de memoria (El tiempo en un estado no influye sobre la distribución de probabilidad, ni del estado actual ni del próximo estado).
    - Las Cadenas de Markov pueden ser discretas (t. discreto) o continuas (t. continuo)
  - En los modelos se utilizan dos conceptos:
    - Estado del sistema (combinación de módulos con fallo o sin fallo)
    - Transiciones entre estados (se basan en P o tasas de transición de un estado a otro)



Estados sin fallo = {(111),(110),(101),(011)}
Estados con fallo ={(001),(010),(100),(000)}

FTF

- Si consideramos un modelo de Markov discreto en el tiempo
  - Cada transición entre estados lleva asociada una probabilidad de transición
  - Estas probabilidades se recogen en una matriz de transiciones ***A*** cuyos elementos p_{ij} son las probabilidades de transición desde el estado *i* al *j*.
  - El modelo se resuelve mediante un conjunto de ecuaciones lineales que se basan en la matriz de probabilidades de transición. Estas ecuaciones se definen como:

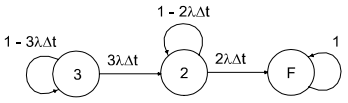
$$\vec{P}(k+1) = \mathrm{A}\vec{P}(k)$$

A^n es la matriz de probabilidades de transición del paso n

  - Para calcular las probabilidades de transición, se supondrá que cada módulo sigue la ley de fallos exponencial (tasa constante de fallos λ). Su tasa de fallos instantánea (probabilidad de que haya fallado en un instante $t + \Delta t$ dado que funcionaba en t) será:

$$P(t < T < t + \Delta t \mid T > t) = \frac{F(t+\Delta t) - F(t)}{1 - F(t)} = 1 - \frac{R(t+\Delta t)}{R(t)} = 1 - \frac{e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} = 1 - e^{-\lambda \Delta t} \approx \lambda \Delta t$$

  - La Cadena de Markov del sistema TMR se puede reducir agrupando estados equivalentes y sumando sus tasas de transición, quedando como:



$R(t) = 1 - p_F(t) = p_2(t) + p_3(t)$

FTF

– Cálculo de la Matriz de transición:
  - La P de estar en un estado *s* en un tiempo *t* depende
    – De la p de estar en un estado en donde exista una transición a *s*
    – De la p de que se produzca esa transición

$$\begin{bmatrix} p_3(t+\Delta t) \\ p_2(t+\Delta t) \\ p_F(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-3\lambda\Delta t & 0 & 0 \\ 3\lambda\Delta t & 1-2\lambda\Delta t & 0 \\ 0 & 2\lambda\Delta t & 1 \end{bmatrix} \begin{bmatrix} p_3(t) \\ p_2(t) \\ p_F(t) \end{bmatrix} \qquad \vec{P}(t+\Delta t) = \mathrm{A}\vec{P}(t)$$

Vector de probabilidad en t + Δt — Matriz de transición — Vector de probabilidad en t

$$\boxed{\vec{P}(n\Delta t) = \mathrm{A}^n \vec{P}(0)}$$

Solución a la Cadena de Markov en tiempo discreto

- Cadenas de Markov contínuas
  – En este modelo, las transiciones pueden tener lugar en cualquier instante de tiempo. Se consideran las ecuaciones anteriores como un conjunto de ecuaciones diferenciales utilizando límites cuando $(\Delta t \to 0)$

Ecuaciones de Chapman-Kolmogorov

$$\frac{dp_3(t)}{dt} = 3\lambda p_3(t)$$
$$\frac{dp_2(t)}{dt} = 3\lambda p_3(t) - 2\lambda p_2(t)$$
$$\frac{dp_F(t)}{dt} = 2\lambda p_2(t)$$

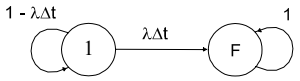
$$p_3(t) = e^{-3\lambda t}$$
$$p_2(t) = 3e^{-2\lambda t} - 3e^{-3\lambda t}$$
$$p_F(t) = 1 - 3e^{-2\lambda t} + 2e^{-3\lambda t}$$

Función de fiabilidad

$$\boxed{R(t) = 1 - p_F(t) = \\ = 3e^{-2\lambda t} - 2e^{-3\lambda t}}$$

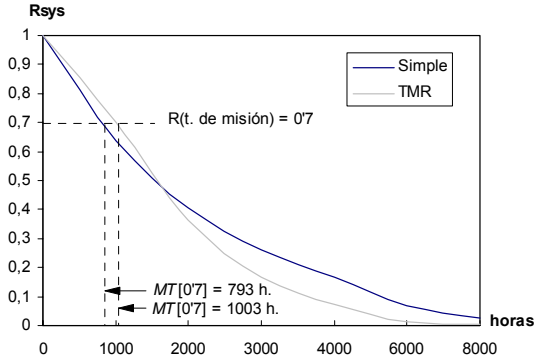
FTF

– Comparación con un sistema sencillo



$$p_1(t) = e^{-\lambda t}$$
$$p_F(t) = 1 - e^{-\lambda t}$$

$$\boxed{R(t) = 1 - p_F(t) = e^{-\lambda t}}$$



$$MTTF_{simple} = \frac{1}{\lambda}$$

$$MTTF_{TMR} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda}$$

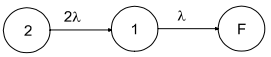
$$\boxed{MTTF_{simple} > MTTF_{TMR}}$$

FTF

4 - Modelado con coberturas

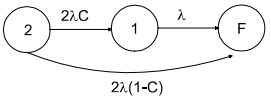
- La cobertura de fallos es la capacidad del sistema en:
  - DETECCIÓN
  - LOCALIZACIÓN
  - AISLAMIENTO
  - RECUPERACIÓN

  de fallos cuando el sistema entra en una situación no válida
- Los métodos de evaluación pueden ser:
  - Experimentales: Inyección de fallos
  - Teóricos: Generación de test
- Variación de la fiabilidad en función de la cobertura (Sistema dual)



$R(t) = p_2(t) + p_1(t) = 1 - p_F(t)$

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



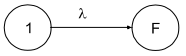
$R(t) = 2Ce^{-\lambda t} - (2C-1)e^{-2\lambda t}$

FTF

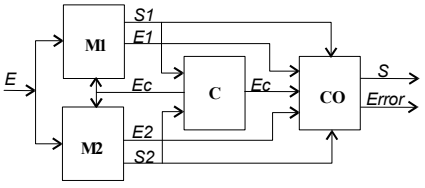
5 - Modelos de Markov para la fiabilidad

- No distinguen entre los fallos seguros de los no seguros
- No tienen en cuenta la reparación
- $R(\infty) = 0$

Sistema sencillo



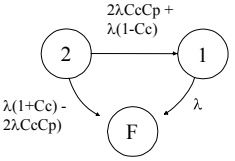
$R(t) = e^{-\lambda t}$



2 : 2 Módulos bien
1 : Falla 1 módulo (Fallo cubierto)
F : Fallo de 2 módulos o no detectado

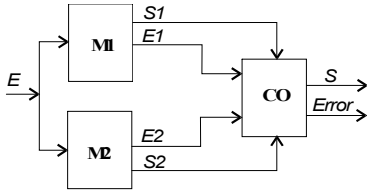
Sistema dual (diagnosis off-line)

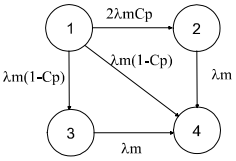
C_p = Cobertura de la autodetección de fallos
C_c = Cobertura del comparador
λ = Tasa de fallos del módulo



FTF

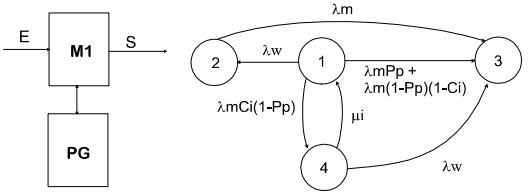
- Sistema dúplex





1 : 2 Modulos ok
2 : Falla repuesto (F. Cubierto)
ó falla el ppal y entra R
3 : Falla el repuesto
(No cubierto)
4 : Falla todo

- Sistema con procesador de guardia



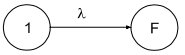
1 : Funciona todo
2 : Falla el P. G.
3 : Fallo total
4 : Fallo temporal cubierto

P_p = P (fallo permanente)
C_i = Cobertura fallos transitorios
λ_m = Tasa de fallos del módulo
λ_w = Tasa de fallos del P.G.

FTF

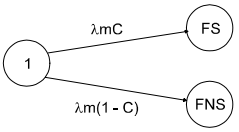
6 - Modelos de Markov para la seguridad

- Tenemos estados de fallo seguros y no seguros
- $S(\infty) \neq 0$ si existe la detección de fallos
- Sistema sencillo sin detección de fallos



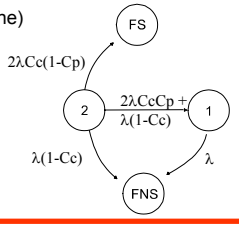
$$S(t) = R(t) = p_1(t)$$

- Sistema sencillo con detección de fallos



$$R(t) = p_1(t)$$
$$S(t) = p_1(t) + p_{FS}(t)$$

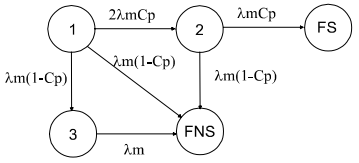
- Sistema dual
(Diagnosis off-line)



$$R(t) = p_1(t) + p_2(t)$$
$$S(t) = p_1(t) + p_2(t) + p_{FS}(t)$$

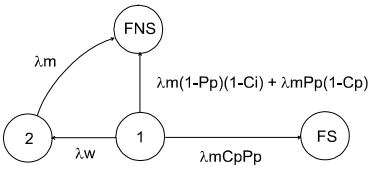
FTF

- Sistema dúplex



$$R(t) = p_1(t) + p_2(t) + p_3(t)$$
$$S(t) = p_1(t) + p_2(t) + p_3(t) + p_{FS}(t)$$

- Sistema con procesador de guardia

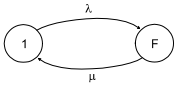


$$R(t) = p_1(t) + p_2(t)$$
$$S(t) = p_1(t) + p_2(t) + p_{FS}(t)$$

FTF

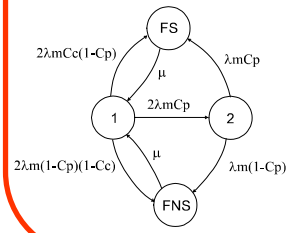
7 - Modelos de Markov para la disponibilidad

- Se añaden tasas de reparación a los modelos de fiabilidad (o seguridad)
- $A(\infty) \neq 0$
- Sistema sencillo

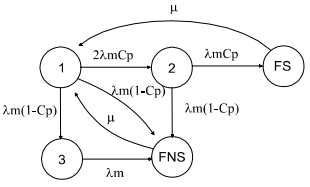


$$p_O(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$
$$p_F(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

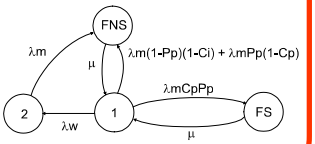
Dual
(Diagnosis on-line)



Dúplex

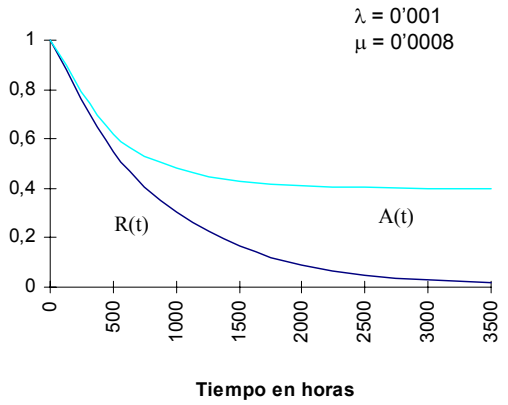


Con P. de Guardia



FTF

- Comparación de un sistema sencillo con y sin reparación



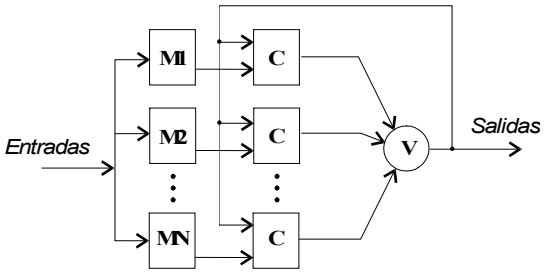
$$A_{SS} = \frac{\mu}{\lambda + \mu}$$

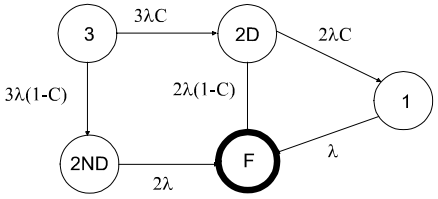
FTF

8 - Ejemplos

Sistema con voto adaptativo

λ = Tasa de fallos
C = Cobertura

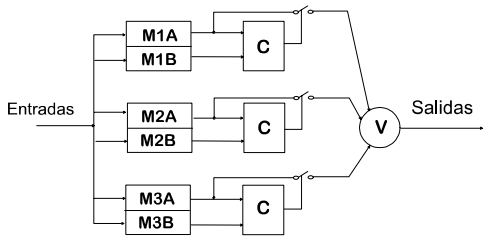




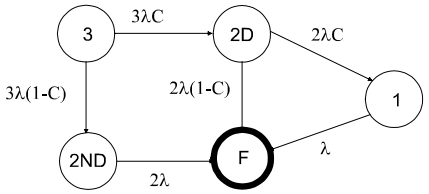
$$R(t) = 1 - p_F(t)$$

FTF

Triple - Dúplex



λ‘ = Tasa de fallos
C = Cobertura del comparador



λ = 2λ‘
C >>> C del caso anterior