

GARANTÍA DE FUNCIONAMIENTO EN EQUIPOS E INSTALACIONES INFORMÁTICAS

Garantía de funcionamiento (Dependability) de un equipo:

Conjunto de propiedades que permiten a sus usuarios depositar una confianza justificada en el servicio proporcionado por el equipo

Servicio que proporciona un equipo:

Queda definido por el comportamiento que observan sus usuarios
Un usuario es otro equipo o una persona

Problemas con el servicio:

Se detecta un **FALLO** en el equipo si el servicio no cumple las especificaciones
El fallo es consecuencia de un **ERROR** en el estado del equipo
La causa hipotética o estimada del error es una **AVERÍA** en el equipo

La garantía de funcionamiento (dependability) es un concepto muy general
Dependiendo de la aplicación se pueden enfatizar diferentes atributos

PROPIEDADES DE LA GARANTÍA DE FUNCIONAMIENTO

El término denominado “Garantía de Funcionamiento” puede englobar a las siguientes propiedades:

- Fiabilidad (reliability):

Propiedad relacionada con la continuidad del servicio que puede ofrecer el equipo

- Mantenibilidad (maintainability, serviceability):

Propiedad relacionada con la rapidez con la que se puede reparar o sustituir un equipo que se ha averiado

- Disponibilidad (availability):

Propiedad relacionada con que el equipo esté disponible para ser utilizado

- Seguridad (safety):

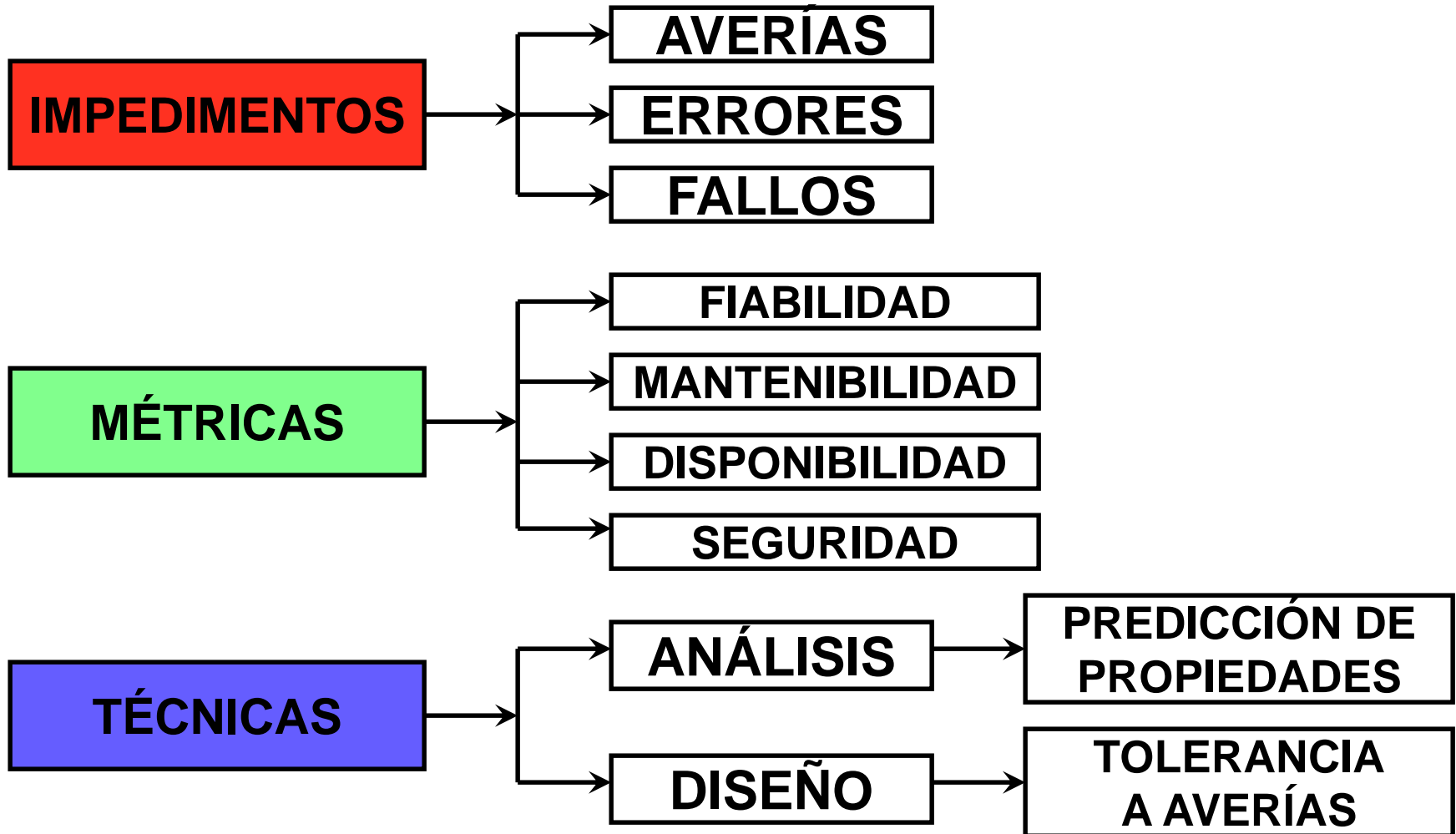
Propiedad relacionada con la prevención de consecuencias catastróficas sobre el entorno

- Seguridad o Impenetrabilidad (security):

Propiedad relacionada con la prevención del acceso no autorizado y/o la manipulación de la información contenida en el equipo

GARANTÍA DE FUNCIONAMIENTO

Aspectos de estudio y análisis



IMPEDIMENTOS: AVERÍAS, ERRORES Y FALLOS

FALLO (failure):

Se produce cuando el equipo no se comporta según sus especificaciones
El equipo falla cuando NO puede suministrar el servicio deseado

ERROR:

Es un estado incorrecto del equipo que puede provocar un fallo
Si hay un error puede haber una secuencia de acciones que generen un fallo

AVERÍA (fault):

Es la causa, hipotética o estimada, de un error
Cuando un equipo se comporta mal se supone que es porque está averiado

El concepto de avería está asociado con la noción de defecto
También se define una avería como los defectos que pueden generar errores

RELACIÓN ENTRE AVERÍAS, ERRORES Y FALLOS

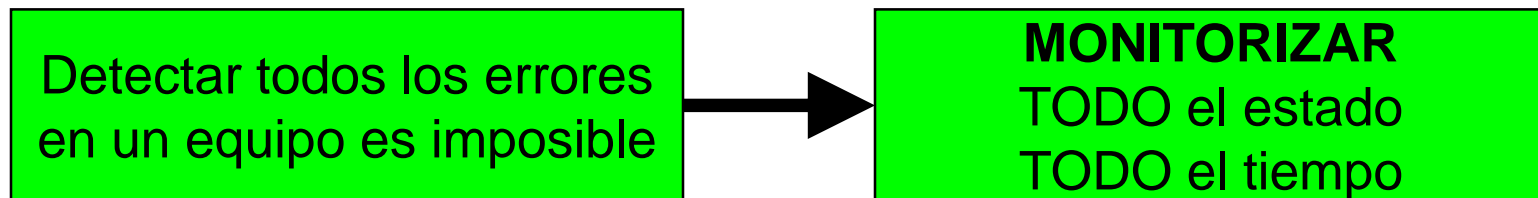
ERROR: Propiedad del estado del equipo que puede observarse y evaluarse

FALLO: No es una propiedad del estado del equipo

La ocurrencia de un fallo se deduce detectando algún error en el estado del equipo
Se detecta el fallo al cruzar el error la interface equipo-usuario afectando al servicio



La causa probable del error es la presencia de una avería en el equipo



RELACIÓN ENTRE AVERÍAS, ERRORES Y FALLOS

Ejemplo: Celda de memoria averiada

Siempre devuelve el valor lógico 0, independientemente de lo que se escriba

La avería sólo se manifiesta si se almacena un 1 y luego se lee la celda

Mientras no se use o se escriba un 0, la avería no genera un error

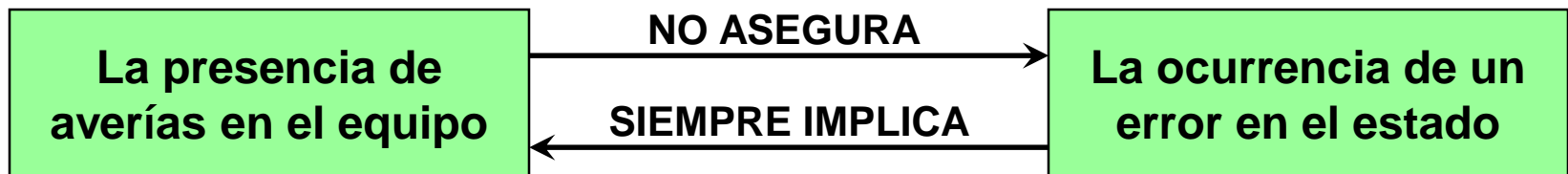
Ejemplo: Un código incorrecto en un programa

Es una avería que permanece inactiva ...

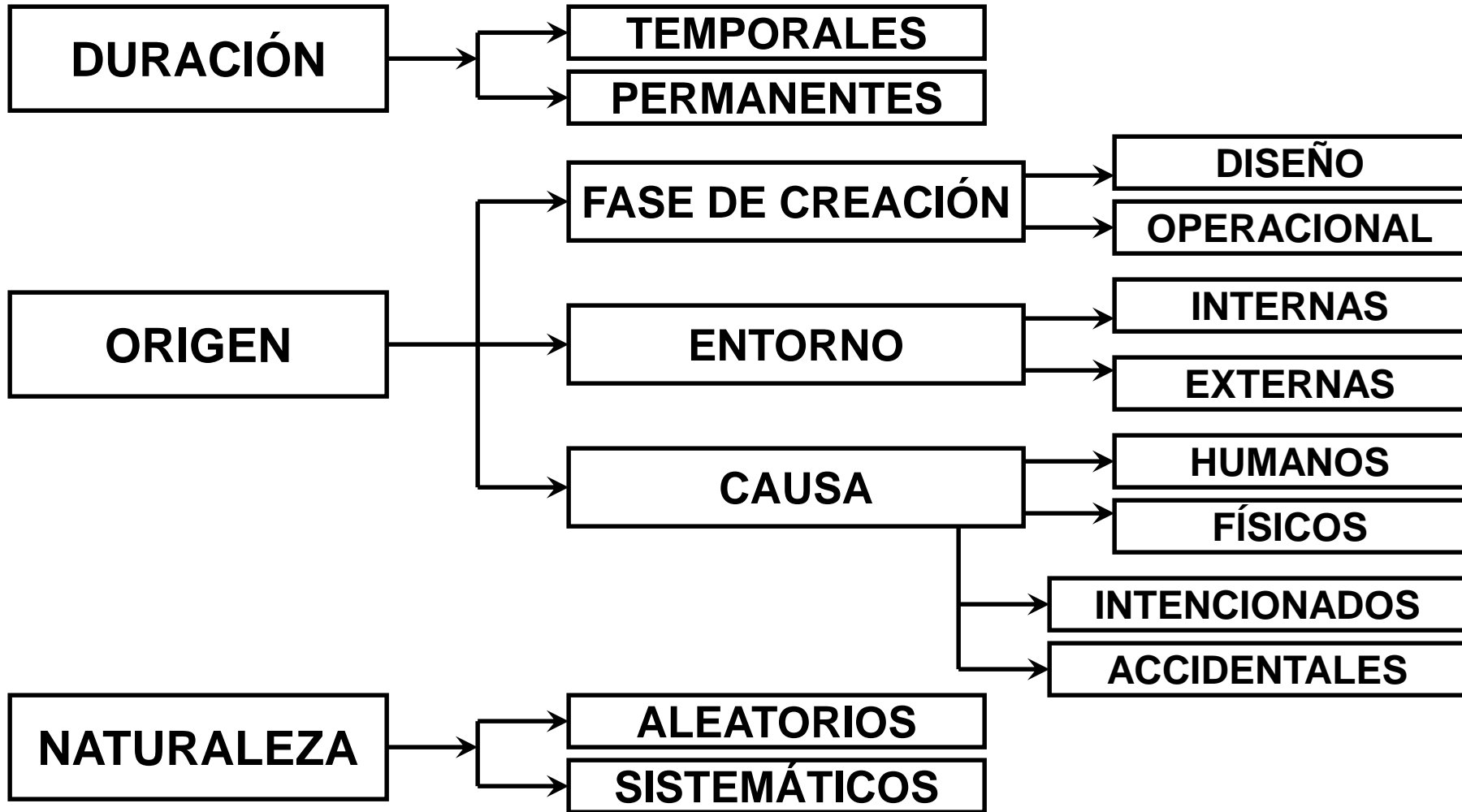
Al ejecutarse el código se generarán errores

que se manifestarán como fallos de funcionamiento del equipo

Relación entre averías y errores



CLASIFICACIÓN DE LAS AVERÍAS



APLICABILIDAD DEL ANÁLISIS ESTADÍSTICO EN FUNCION DE LA NATURALEZA DE LAS AVERÍAS

Las averías pueden tener una naturaleza { Aleatoria
Sistemática

Los fallos causados por averías de naturaleza ALEATORIA

- NO es posible predecir el instante justo en el que pueden ocurrir
- Observando un número elevado de dispositivos se puede estimar la probabilidad de tener un fallo dentro de un cierto período de tiempo

APLICABLE el análisis estadístico

Los fallos causados por averías de naturaleza SISTEMÁTICA

Se puede predecir, hasta cierto punto, cuándo pueden ocurrir
Ej: Un dispositivo sobre-estresado puede fallar bajo ciertas condiciones

YA Identificadas: Se pueden analizar sus efectos y eliminarlas

NO Identificadas: Sus efectos son impredecibles

NO ES APLICABLE el análisis estadístico

ENFOQUES PARA EL TRATAMIENTO DE AVERÍAS SISTEMÁTICAS

Enfoque 1:

Estas averías son predecibles (típicas en el software)


Ej: Ocurre un fallo cada vez que se ejecuta un código “averiado”

NO SE PUEDEN USAR ANÁLISIS ESTADÍSTICOS

Enfoque 2:


Debido a la complejidad del software/sistemas actuales estas averías

- Pueden tomar un número casi ilimitado de formas
- Pueden estar distribuidas pseudo-aleatoriamente en el software/sistema

Entonces: Los efectos de las averías  Puede considerarse que tienen una naturaleza pseudo-aleatoria y ...
NO se pueden predecir

SE PUEDEN USAR ANÁLISIS ESTADÍSTICOS
(mientras no sean identificadas)

CONCLUSIÓN

Análisis y modelado de fallos { Aleatorios
Sistemáticos  Usar técnicas estadísticas
(No identificados)

FIABILIDAD: Definición y expresión

DEFINICIÓN de la fiabilidad de un componente o sistema: Es su capacidad para funcionar correctamente a lo largo de un período de tiempo especificado

EXPRESIÓN de la fiabilidad $R(t)$ de un sistema S :

$$R(t) = \text{Pr}(S \text{ sea completamente operativo en } [0,t])$$

Definiendo ...

X = Var aleatoria que representa el tiempo hasta el fallo del sistema

f = Función de densidad de probabilidad de X

F = Función de distribución acumulada de X

$$R(t) = \text{Pr}(X > t) = 1 - F(t)$$

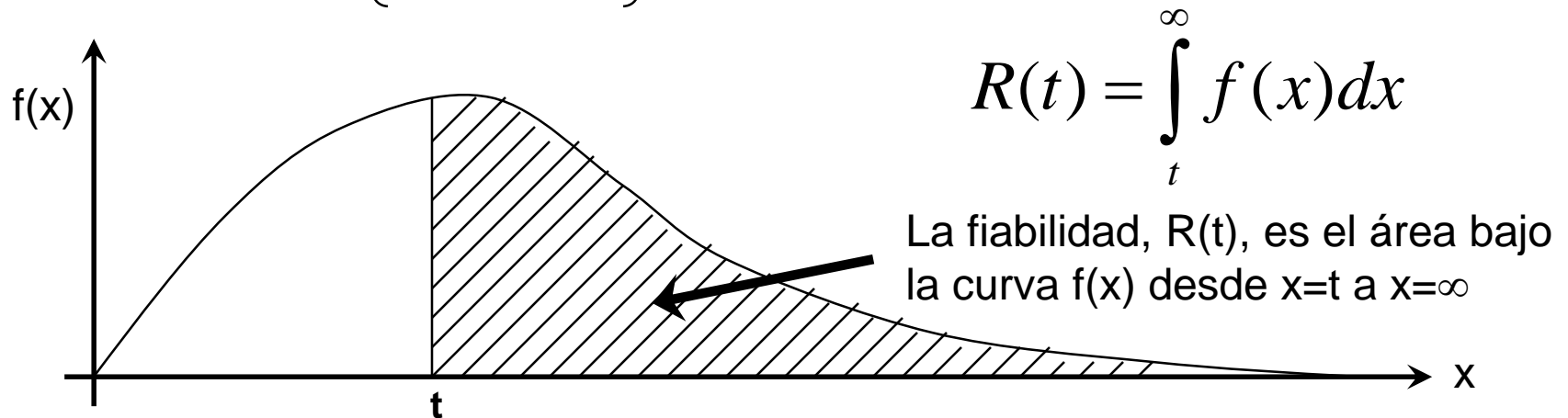
$$R(t) = \int_t^{\infty} f(x) dx$$

FIABILIDAD: Interpretación gráfica

SUPOSICIONES COMUNES:

- 1 El sistema está trabajando correctamente en $t=0$; $R(0)=1$ y $F(0)=0$
Si se consideran sistemas que pueden estar defectuosos en $t=0$
 $F(0) = \Pr(X=0) = p > 0$; $F(t)$ es una distribución mixta con masa p en el origen
- 2 Un sistema no puede trabajar indefinidamente sin fallos; $R(\infty)=0$ y $F(\infty)=1$

$R(t)$ es una función $\left\{ \begin{array}{l} \text{decreciente} \\ \text{continua y} \\ \text{monótona} \end{array} \right\}$ con valores entre 0 y 1 en el intervalo $[0, \infty)$



FIABILIDAD: Medición de fiabilidad e infiabilidad

Considerar un conjunto de N componentes idénticos
Si se ponen todos a funcionar en el mismo instante, $t=0$

- En un instante posterior, t , el número de componentes funcionando es $n(t)$

La fiabilidad del componente es: $R(t) = \frac{n(t)}{N}$ (RELIABILITY)

Probabilidad de que un componente funcione durante un período de tiempo

- En un instante posterior, t , el número de componentes que han fallado es $n_f(t)$

La infiabilidad del componente es: $Q(t) = \frac{n_f(t)}{N}$ (UNRELIABILITY)

Probabilidad de que un componente NO funcione durante un período de tiempo

$$\text{Se verifica: } Q(t) = 1 - R(t)$$

FIABILIDAD: Tasa de fallos

DEFINICIÓN de tasa de fallos (failure rate)

Es la frecuencia con la que se avería un componente o sistema $\left(\frac{\text{fallos}}{\text{tiempo}} \right)$

EJEMPLO

Un dispositivo falla, en promedio, una vez cada 1000 horas de funcionamiento
Su tasa de fallos es $1/1000 = 0,001$ fallos/hora

EXPRESIÓN

Se parte de dos probabilidades:

- Probabilidad **incondicional** de que ocurra un fallo en el intervalo $[t, t+\Delta t]$

$$\Pr(t < X < t + \Delta t) = f(t) \cdot \Delta t$$

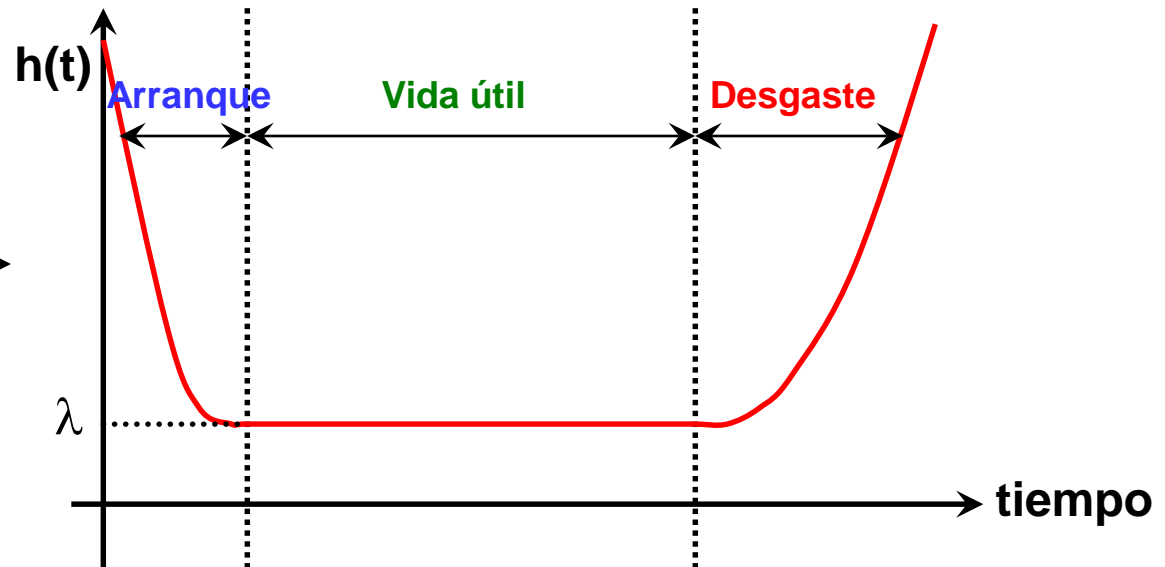
- Probabilidad **condicional** de que ocurra un fallo en el intervalo $[t, t+\Delta t]$ cuando el sistema ha trabajado correctamente hasta el instante t

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

FIABILIDAD: Curva de mortalidad

La curva de mortalidad es la representación de la tasa de fallos como una función del tiempo (edad o envejecimiento del sistema)

La evidencia empírica indica que en los elementos mecánicos siempre tiene esta forma →



- **Fase de Arranque:** Los fallos suelen provenir de defectos inherentes. Generalmente están relacionados con diseño/fabricación/ensamblado incorrectos.
- **Fase de Vida Útil:** Los fallos son aleatorios. Generalmente debidos a condiciones del entorno.
- **Fase de Desgaste:** Los fallos son debidos a la edad excesiva (envejecimiento) del sistema. La tasa de fallos se incrementa continuamente.

FIABILIDAD: Relación con la tasa de fallos

SI (la función de densidad de tiempo hasta el fallo es exponencial)

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

ENTONCES

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

En este caso la tasa de fallos toma el siguiente valor:

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

Observar que durante la fase de vida útil del sistema en la que la tasa de fallos, λ , se supone constante ...

- La fiabilidad del sistema “cae” exponencialmente con el tiempo t
- La probabilidad de que un sistema trabaje correctamente durante un período de tiempo t , “decrece” exponencialmente con la duración del período

FIABILIDAD: Tasa de fallos variante en el tiempo

- **FALLOS DEL HARDWARE (aleatorios)**

Generalmente se deben a causas aleatorias

El uso de una tasa de fallos CONSTANTE es apropiado

- **FALLOS DEL SOFTWARE (sistemáticos)**

Generalmente son de diseño

Pueden ser localizados y eliminados durante la vida útil del sistema

El número de fallos tiende a disminuir con el tiempo

El uso de una tasa de fallos CONSTANTE **NO** es apropiado

Los fallos de tipo sistemático se pueden modelizar con una distribución Weibull ...

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} \quad \left\{ \begin{array}{l} \beta = \text{Parámetro de forma} \\ \eta = \text{Vida característica} \end{array} \right.$$

Para ciertos valores de β , la fiabilidad ...

Se incrementa con el tiempo

Se aproxima a la unidad cuando $t \rightarrow \infty$

FIABILIDAD: Métrica MTTF

Tiempo medio hasta el fallo

MTTF (Mean Time To Failure) = $E[X]$

Media de la variable aleatoria X , que representa el tiempo hasta el fallo del sistema

Si X está exponencialmente distribuida ...

$$\left. \begin{aligned} f(t) &= \lambda e^{-\lambda t} \\ F(t) &= 1 - e^{-\lambda t} \end{aligned} \right\} R(t) = 1 - F(t) = e^{-\lambda t}$$

Entonces la métrica MTTF se calcula así:

$$MTTF = E[X] = \int_0^{\infty} t \cdot f(t) dt = \int_0^{\infty} R(t) dt = \frac{1}{\lambda}$$

$$\text{Tiempo medio hasta el fallo} = \frac{1}{\text{Tasa constante de fallos del sistema}}$$

REPARABILIDAD o MANTENIBILIDAD

DEFINICIÓN de Mantenibilidad, $M(t)$

Es una medida de la rapidez de reparación de un sistema que se ha averiado

Cuantitativamente, es la probabilidad de que un sistema averiado vuelva a estar operativo en un periodo de tiempo dado

MÉTRICA de Reparabilidad: Tiempo medio de reparación

MTTR = Mean Time To Repair

Es el tiempo medio empleado para reparar un sistema

Incluye el tiempo empleado en →

{ Detectar el fallo
Localizar la avería
Efectuar la reparación
Reconfigurar el sistema

Puede ser estimado en la fase de diseño o ...

Debe ser medido experimentalmente con el sistema funcionando

TASA DE REPARABILIDAD

Es el número de reparaciones que pueden realizarse en un período de tiempo, generalmente reparaciones / hora

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

COMBINACIÓN DE FIABILIDAD+REPARABILIDAD

Se supone que una vez que el sistema ha fallado y se ha reparado está en las mismas condiciones que el sistema original

MÉTRICA: Tiempo medio entre fallos
MTBF = Mean Time Between Failures

$$\text{MTBF} = \text{MTTF} + \text{MTTR}$$

SIMPLIFICACIÓN

En la mayoría de los sistemas ...

El tiempo necesario para
reparar el sistema

<<

El tiempo que el sistema funciona
ininterrumpidamente hasta el fallo

ENTONCES

$$\text{MTBF} \approx \text{MTTF}$$

DISPONIBILIDAD Instantánea

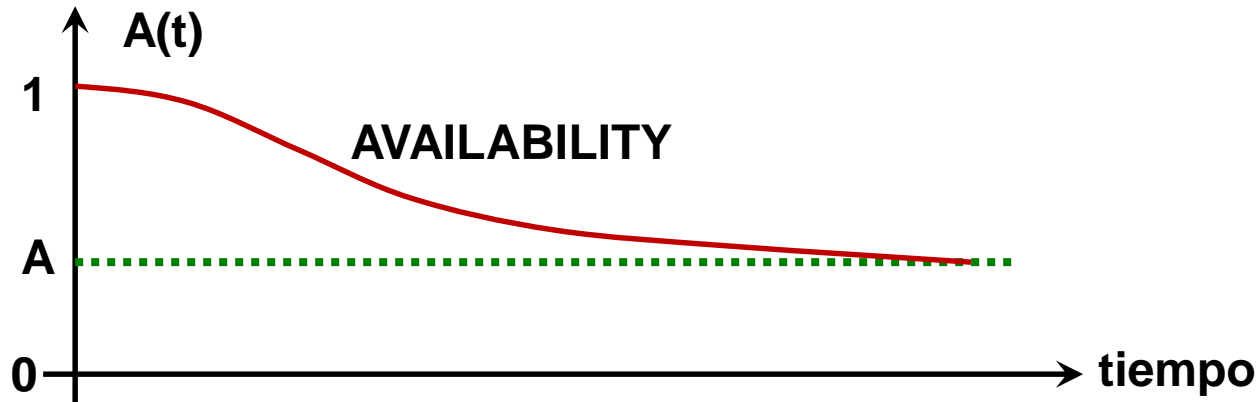
Definición y expresión

Disponibilidad instantánea, $A(t)$

Es la probabilidad de que el sistema esté funcionando en el instante t independientemente del número de veces que el sistema haya fallado y sido reparado en el intervalo $(0,t)$

Si el sistema NO es reparable $\longrightarrow A(t) = R(t)$
Disponibilidad = Fiabilidad

REPRESENTACIÓN GRÁFICA DE $A(t)$



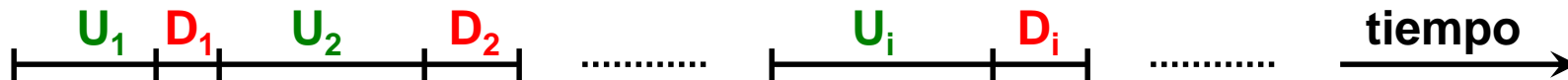
$A(t)=1$ en $t=0$; Luego decrece hasta el valor A = Disponibilidad estacionaria

DISPONIBILIDAD Estacionaria

Disponibilidad estacionaria, A

Es el valor límite de la disponibilidad instantánea $A(t)$ cuando $t \rightarrow \infty$

Escenario de cálculo de A



$\left\{ \begin{array}{l} U_i = i\text{-ésimo período de funcionamiento del sistema (UP)} \\ D_i = i\text{-ésimo período de reparación / sustitución (DOWN)} \end{array} \right.$

Si (U_i y D_i son variables aleatorias IID)

La secuencia $X = U_i + D_i$ es un proceso estocástico de renovación

Proceso bien estudiado y que permite el cálculo de A

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} = \frac{\text{Tiempo que el sistema está operativo}}{\text{Tiempo total}}$$

DISPONIBILIDAD

Caso de usar distribuciones exponenciales

Distribuciones exponenciales de los tiempos de fallo / Reparación

$$\left\{ \begin{array}{ll} \text{Fallo} & w(t) = \lambda \cdot e^{-\lambda t} \\ \text{Reparación} & g(t) = \mu \cdot e^{-\mu t} \end{array} \right.$$

$$\left\{ \begin{array}{ll} \text{Disponibilidad instantánea} & A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \\ \text{Disponibilidad estacionaria} & A = \lim_{t \rightarrow \infty} A(t) = \frac{\mu}{\lambda + \mu} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \end{array} \right.$$

SI $\mu \rightarrow 0$ ENTONCES $A(t) \rightarrow R(t)$

Se confirma que un sistema sin mantenimiento \rightarrow Disponibilidad = Fiabilidad

¡Un buen sistema tiene una disponibilidad muy próxima a la unidad!