FTF

Tema 1: Introducción: Conceptos básicos y definiciones

1.- Necesidad de los sistemas tolerantes a fallos

2.- Definición de garantía de funcionamiento

3.- Arbol de la garantía de funcionamiento

4.- Definición de fallo, error y avería

4.1 Clasificación de los fallos

5.- Técnicas para aumentar la fiabilidad de un sistema

6.- Medios para validar la garantía de funcionamiento

8.- Aplicaciones de la computación tolerante a fallos

FTF

1. Necesidad de los sistemas tolerantes a fallos

- Históricamente los sistema fiables se limitaban a aplicaciones
  - Militares
  - Industriales (Tiempo Real)
  - Espaciales y Aeronáuticas
  - Telemáticas (Comunicaciones)

  puesto que los fallos producían un grave impacto económico y la pérdida de vidas humanas
- Actualmente se aplican estas técnicas a los ordenadores de propósito general debido a que
  - Se instalan en ambientes industriales mucho más ruidosos: temperatura, humedad, interferencias electromagnéticas
  - Los utilizan operarios no especializados haciendo que el sistema deba de tolerar el mal uso
  - Se incrementa el costo de reparación (baja el hw y sube la mano de obra)
  - Los sistemas son más complejos, habiendo muchos más componentes que pueden fallar

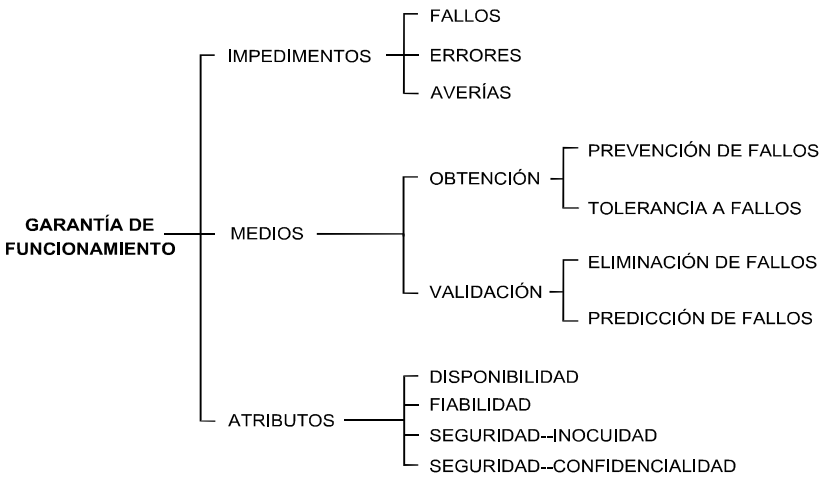
2. Definición de garantía de funcionamiento

FTF

- Un *Sistema Tolerante a Fallos* es aquel que posee la capacidad interna para preservar la ejecución correcta de las tareas a pesar de la ocurrencia de fallos hw o sw. En ellos, se enmascara la presencia de los fallos usando *redundancia* (en cualquier nivel).
- **OBJETIVO de la Tolerancia a Fallos**
  - Evitar la avería del sistema, incluso en presencia de fallos
- *Garantía de Funcionamiento* (Dependability) de un sistema informático es la propiedad que permite a sus usuarios depositar una confianza justificada en el servicio que les proporciona.
- Dependiendo de la aplicación, la garantía de funcionamiento pondrá énfasis en un subconjunto de estas características:
  - El sistema funciona sin interrupciones (*reliability*)
  - El sistema no provoca averías catastróficas (*safety*)
  - El sistema está disponible el máximo tiempo posible (*availability*)
  - El sistema es fácilmente reparable (*maintainability*)
  - El sistema impide el acceso no autorizado (*confidentiality*)
  - El sistema impide la alteración inadecuada de la información (*integrity*)

3. Árbol de la garantía de funcionamiento

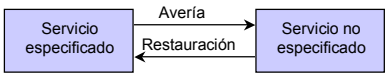
FTF



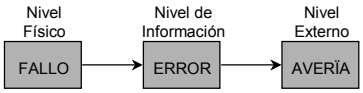
FTF

4. Definición de fallo, error y avería

- La vida de un sistema informático supone un cambio continuo entre dos estados:
  - Estado de funcionamiento correcto
  - Estado en el que el sistema está averiado

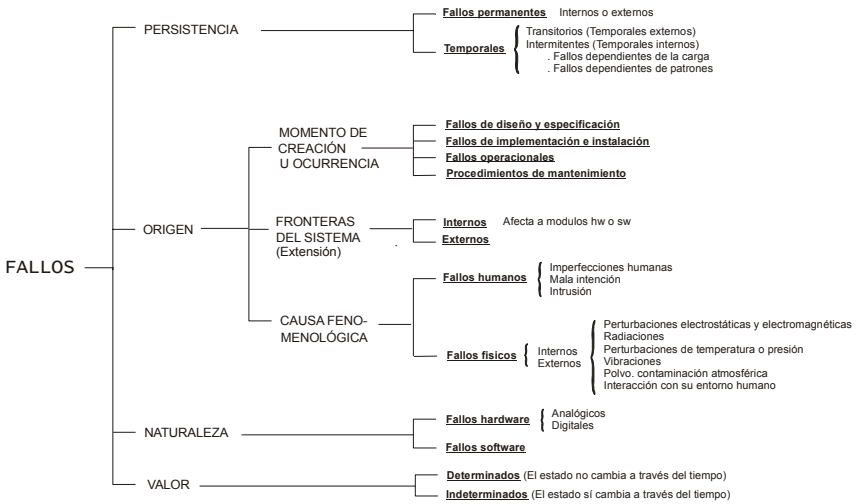


- La garantía de funcionamiento de un sistema disminuye debido a la existencia de:
  - Un **fallo** es un defecto o imperfección física en el hw o sw del sistema
  - Un **error** es un estado interno incorrecto del sistema. Es consecuencia de un fallo y puede dar lugar a una avería
  - Una **avería** ocurre cuando el servicio entregado por el sistema no es el especificado. El usuario aprecia que el sistema no funciona bien. Las averías se deben a errores
- Se considera la relación entre fallos, errores y averías como:



FTF

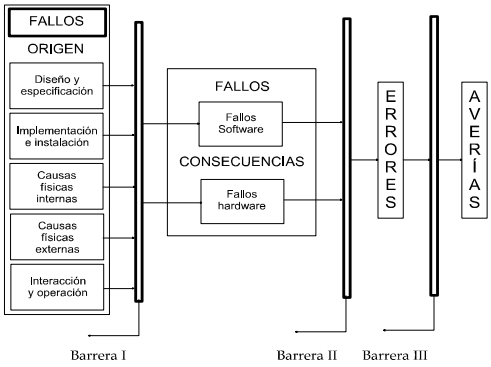
4.1 Clasificación de los fallos



FTF

5. Técnicas para aumentar la fiabilidad de un sistema

- Son los métodos que se combinan para realizar un STF



Prevención de fallos Enmascaramiento Tolerancia a fallos

FTF

5. Técnicas para aumentar la fiabilidad de un sistema (II)

- Prevención de fallos (Fault avoidance)
  - El objetivo es reducir la posibilidad de fallo del sistema, y para ello:
    - Elección de componentes de alta fiabilidad
    - Diseño e implementación extremadamente cuidadoso
    - Protección contra los agentes externos provocadores de fallos
    - Comprobaciones y control de calidad
- Tolerancia a fallos (Fault tolerance)
  - El objetivo es que el sistema funcione a pesar de los fallos
  - La TaF se logra mediante
    - el tratamiento del fallo (prevenir la activación del error)
      - Utilizan la redundancia para suministrar la información necesaria para evitar los efectos de los fallos
      - Para los fallos de diseño --> Diversificación funcional
    - Reconfiguración (eliminación del error antes de que se produzca la avería)
      - Detección, estimación de daños, recuperación del error y tratamiento del fallo y continuación

FTF

6. Medios para validar la garantía de funcionamiento

- *Son los medios para obtener una confianza justificada en que el sistema posee la capacidad de proporcionar el servicio especificado*
- Eliminación de fallos (*Fault Removal*)
  - Consiste en reducir la presencia (número, seriedad) y el alcance de los fallos
  - Se lleva a cabo mediante: verificación, diagnosis y corrección
  - Es un mantenimiento que se hace del sistema
- Predicción de fallos (*Fault Forecasting*)
  - Consiste en la obtención a priori de la garantía de funcionamiento del sistema. Para ello se realiza una evaluación del comportamiento del sistema ante la ocurrencia del fallo
  - Se lleva a cabo mediante:
    - Evaluación de modelos teóricos
      - Modelos de Markov
      - Modelos basados en Redes de Petri Estocásticas
      - Problema: Cálculo de coberturas
    - Inyección de fallos experimental
      - Lógica: Simulación de fallos estructural o comportamental
      - Física: Inyección física de fallos

FTF

7. Aplicaciones de la computación tolerante a fallos

- Sistemas de larga vida
  - Los requerimientos típicos son el 95 % de probabilidad de estar operativo en 10 años
  - Permiten tiempos de reparación elevados
  - Permiten reconfiguración manual por medio del operador
  - Ejemplos: Satélites
- Sistemas para aplicaciones críticas
  - Los requerimientos son del 99’99999 % de probabilidad de no fallar en 3 horas
  - El funcionamiento es crítico para las vidas humanas, medio ambiente o protección de equipos (aviones, sistemas militares y controladores industriales)
  - Lanzadera espacial
- Sistemas de alta disponibilidad
  - Los usuarios deben de tener una probabilidad alta de recibir servicio cuando lo requieren
  - Se utilizan en los sistemas bancarios y de tiempo compartido
  - Ejemplo: Sistema transaccional Tandem Non Stop
- Sistemas de difícil mantenimiento
  - Se utilizan cuando las operaciones de mantenimiento son muy caras o imposibles
  - Tratan de retrasar el mayor tiempo posible el mantenimiento mediante la reconfiguración
  - Ejemplos: Estaciones de procesado remoto o algunas aplicaciones espaciales