

# Fundamentos de Tolerancia de Falhas

---

## Definições

**Tolerância de falhas:** é a capacidade de um sistema de continuar operando mesmo que uma ou mais falhas ocorram. A tolerância de falhas é uma propriedade desejável em qualquer sistema crítico, pois falhas são inevitáveis.

- **Dependabilidade:** capacidade de um sistema de entregar um serviço que pode ser justificado como confiável.
- **Confiabilidade:** capacidade de um sistema de entregar um serviço que pode ser justificado como confiável.
- **Disponibilidade:** capacidade de um sistema de estar disponível para uso.
- **Segurança:** capacidade de um sistema ou de estar operacional e executar sua função corretamente ou de descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam
- **Mantenabilidade:** capacidade de um sistema de ser facilmente mantido e modificado.
- **Testabilidade** capacidade de um sistema de ser testado.
- **Performability** capacidade de um sistema de manter um nível de desempenho aceitável mesmo em caso de falhas.
- **MTBF (Mean Time Between Failures):** é a média de tempo entre falhas.

## Falha → Erro → Defeito:

- **Erro:** é um estado anormal ou uma condição incorreta no software que pode levar a uma falha.
- **Falha:** ocorre quando o sistema não executa uma ação conforme esperado. Isso pode resultar em um mau funcionamento perceptível pelo usuário ou em uma interrupção total do serviço. (falhas podem ser toleradas, defeitos não)
- **Defeito:** é a causa de um erro.



## Latência:

- **Latência de falha:** período de tempo desde a ocorrência da falha até a manifestação do erro devido aquela falha.
- **Latência de erro:** período de tempo desde a ocorrência do erro até a manifestação do defeito devido aquele erro



## Falhas:

*confiabilidade sempre foi um problema de engenharia, assim falhas físicas, que afetam diretamente o hardware, tradicionalmente vem recebendo atenção especial*

- **Falhas Físicas:**

- **Falhas permanentes:** ocorrem devido a danos físicos, como queima de componentes eletrônicos, falhas de disco rígido ou falhas de memória.
  - **Falhas temporárias:**
    - **Intermitentes:** ocorrem de forma intermitente, como falhas de contato em conectores ou falhas de solda.
    - **transitórias:** ocorrem devido a condições temporárias, como interferência eletromagnética ou flutuações de tensão.
  - **Falhas Humanas:**
    - **Falha de projeto:** ocorre devido a erros de projeto, como a falta de verificação de limites de entrada ou a falta de validação de dados.
    - **interação**
      - **intencionais:** ocorrem devido a ações deliberadas, como a exclusão de arquivos ou a modificação de configurações.
      - **não intencionais:** ocorrem devido a erros humanos, como a inserção de dados incorretos ou a execução de comandos errados.
- 

## Dependabilidade vs Desempenho

Quanto maior a ênfase na confiabilidade e na capacidade de tolerância a falhas de um sistema, maior pode ser o impacto no desempenho. Isso ocorre porque a implementação de mecanismos para garantir alta confiabilidade, disponibilidade e segurança muitas vezes envolve a introdução de redundância, verificações adicionais, mecanismos de recuperação de falhas e outros recursos que podem consumir recursos computacionais e, conseqüentemente, afetar o desempenho do sistema.

---

## Causas de Falhas

*falhas são inevitáveis*

- **Problema de especificação:** ocorre quando os requisitos do sistema não são claramente definidos ou são mal interpretados.
  - **problemas de implementação:** ocorrem quando o código-fonte do sistema contém erros ou bugs.
  - **componentes defeituosos:**
    - **imperfeições de manufatura:** ocorrem devido a defeitos de fabricação em componentes eletrônicos.
    - **fadiga** ocorre devido ao desgaste de componentes mecânicos.
  - **distúrbios externos:** radiação, interferência eletromagnética, variações ambientais (temperatura, pressão, umidade), problemas de operação
- 

## Descritores de Falhas

- **Natureza:** falhas podem ser classificadas de acordo com sua natureza, falha de hardware, falhas de software, falhas de comunicação, falhas de rede, etc.
- **Duração:** falhas podem ser classificadas de acordo com sua duração, falhas permanentes ou falhas temporárias.

- **Extensão:** falhas podem ser classificadas de acordo com sua extensão, falhas local a um módulo ou falhas globais.
  - **Valor:** falhas podem ser classificadas de acordo com seu valor, determinado ou indeterminado no tempo.
- 

## Confiabilidade

- **Confiabilidade:** é a probabilidade de um sistema de entregar um serviço que pode ser justificado como confiável. A confiabilidade é uma medida da probabilidade de que um sistema funcione corretamente por um determinado período de tempo.
  - dentro de condições definidas
  - durante certo período de funcionamento
  - condicionado a estar operacional no início do período



- **Mais usada como medida em:**
    - sistemas em que mesmo curtos períodos de operação incorreta são inaceitáveis
    - sistemas em que reparo é impossível
- 

## Disponibilidade

*disponibilidade e confiabilidade são os atributos mais conhecidos e usados, muitas vezes aparecem como sinônimos de dependabilidade*

- **Disponibilidade:** é a probabilidade de um sistema de estar disponível para uso. A disponibilidade é uma medida da probabilidade de que um sistema esteja operacional em um determinado momento.
  - **alternância de períodos de funcionamento e reparo**
    - um sistema pode ser altamente disponível mesmo apresentando períodos de inoperabilidade
- 

## Segurança

- **Segurança:** é a capacidade de um sistema de estar operacional e executar sua função corretamente ou de descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam.
    - medida da capacidade fail-safe do sistema
    - não está relacionado diretamente a security
- 

## Performabilidade

- **Performabilidade:** Está relacionado a queda de desempenho provocada por falhas
  - sistema continua a operar, mas com queda de desempenho (graceful degradation: degradação suave ou degradação gradual)



## Mantenabilidade

- **Mantenabilidade:** é a capacidade de um sistema de ser facilmente mantido e modificado.
  - **Quantitativamente:** probabilidade que um sistema com defeitos seja restaurado a um estado operacional dentro de um período  $t$
  - **Restauração**
    - *localização do problema*
    - *reparo físico*
    - *colocação em operação*

## Testabilidade

- **Testabilidade:** capacidade de testar certos atributos internos ao sistema
- **facilidade de realizar certos testes**
- **relacionada a manutenibilidade**
  - a testabilidade aumenta a manutenibilidade
- **testes:**
  - Manuais
  - Automáticos

## Aplicações de Tolerância a Falhas

- **Longa Vida:** sistemas que devem operar por longos períodos de tempo sem interrupção
- **Manutenção Adiada:** sistemas que não podem ser interrompidos para manutenção (manutenção é ou impossível ou extremamente cara)
- **Computação Crítica:** sistemas que devem operar corretamente em situações críticas, como sistemas de controle de tráfego aéreo, sistemas de controle de usinas nucleares, etc.
- **Alta Disponibilidade:** sistemas que devem estar disponíveis para uso a maior parte do tempo, como sistemas de telecomunicações, sistemas de comércio eletrônico, etc.

## Técnicas para alcançar dependabilidade

*a dependabilidade de um sistema depende de decisões de projeto desse sistema*

- para alcançar dependabilidade (ou seja para alcançar os atributos de dependabilidade) é necessário o emprego de técnicas de projeto adequadas
- nem todas as técnicas estão relacionadas a TF
  - por exemplo: bons componentes podem levar a uma boa confiabilidade dos sistema



## Técnicas de Tolerância a Falhas

- **prevenção e remoção de falhas não são suficientes:**
    - quando o sistema exige alta confiabilidade,
    - ou alta disponibilidade
  - **técnicas de TF exigem:**
    - componentes adicionais
    - algoritmos especiais
  - **Mascaramento**
    - falhas são mascaradas e não chegam a provocar defeito
  - **detecção, localização e recuperação**
    - ou erros (ou falhas) devem ser inicialmente detectados
    - o sistema entra em um estado de tratamento de exceção até poder voltar a operação normal
- 


## Classificação

- **4 Fases:**
  - **Detecção:** identificação de falhas
  - **Confinamento e avaliação:** limitação dos efeitos das falhas
  - **Recuperação:** restauração do sistema
  - **Tratamento da Falha:** correção da falha
- **outra classificação:**
  - detecção, diagnóstico, confinamento, mascaramento, compensação

## Detecção de Falhas

- **duplicação e comparação:**
- **testes de limites de tempo:**
  - time-out, cão de guarda (watchdog timers)
- **testes reversos**
- **codificação:**
- **teste de razoabilidade**
  - limites ou compatibilidades
- **testes estruturais**
  - consistência
- **diagnóstico**

### Duplicação e comparação

 Duplicação e comparação

Duplicação e comparação: software



## Confinamento e avaliação de danos

*confinamento e avaliação tratamento dependem de decisões de projeto do sistema*

*facilitam detecção e recuperação, mas não são obrigatórias*

- **latência de falha**
  - pode provocar espalhamento de dados inválidos
- **confinamento**
  - estabelece limites para a propagação do dano

## Mecanismos de confinamento e avaliação

- **confinamento**
  - restrições ao fluxo de informações
    - evitar fluxos acidentais
    - estabelecer interfaces de verificação para detecção de erros
- **avaliação dos danos:**
  - estática: projeto inicial e hardware
  - dinâmica: execução e software

## Exemplos:

- **ações atômicas**
  - operações primitivas auto encapsuladas
  - sem efeitos secundários
- **isolamento de processos**
  - tudo que não é permitido é proibido
- **hierarquia de processos**
  - clareza conceitual
- **controle de recursos**

## Recuperação de erros

- **troca do estado atual incorreto para um estado livre de falhas**
  - pode ser um estado anterior, livre de falhas, do sistema
  - pode ser um novo estado
  - em último caso, pode ser o estado inicial
- **ocorre após detecção**



## Avanço

*mais usadas em sistemas de tempo real, onde o retorno para um estado anterior (no tempo) seja inviável*

- **forward error recovery**
  - condução a novo estado consistente
    - ainda não ocorrido desde a última manifestação de erro
  - eficiente, mas específica a cada sistema
    - danos devem ser previstos acuradamente

## **Retorno**

- **backward error recovery**
  - condução a estado anterior consistente
  - alto custo mas de aplicação genérica
- **exemplo de técnica de recuperação por retorno**
  - pontos de verificação (checkpoints)
    - mais simples
    - salvamento de todo o estado do sistema periodicamente

## **Recuperação**

- **simples em um único processo**
- **complexa em processamento distribuído**
  - **usualmente retroativa (de retorno)**
  - **pode provocar efeito dominó**
    - retorno ao início do processamento
    - problema com mensagens órfãs e perdas
  - **solução**
    - restrições a comunicação entre processos

## **Tratamento da Falha**

- **localizar a origem do erro (falha)**
  - localizar a falha de forma precisa
  - reparar a falha
  - recuperar o restante do sistema

*lembrar diferenças entre falhas permanentes e temporárias*

- **hipótese de falha**
  - uma única falha de cada vez

## **Localização da falha**

- **duas fases:**
  - **localização grosseira (módulo ou subsistema)**
    - deve ser rápida
  - **diagnóstico**
    - reparos de menor custo
- **diagnóstico para localização da falha**

- manual
- automático (componentes livres de falha são responsáveis pela execução do teste)

## **Reparo da falha**

- **remoção do componente defeituoso**
  - manual ou automática
- **automática**
  - **degradação suave:**
    - reconfiguração para operação com menor número de componentes
  - **auto-reparo:**
    - substituição imediata por componente disponível no sistema

## **Auto-reparo**

- **substituição automática**
  - sistemas com longo período de missão sem possibilidade de reparo manual
- **aplicação de redundância de componentes**
  - redundância dinâmica
  - redundância híbrida
  - redundância auto-eliminadora