CENTRO UNIVERSITÁRIO
UNI METROCAMP | WYDEN

Sistemas Distribuídos – Tolerância a Falhas

Santiago Azevedo Robles
santiago.robles@unimetrocamp.edu.br

Uma Falha resulta num Defeito

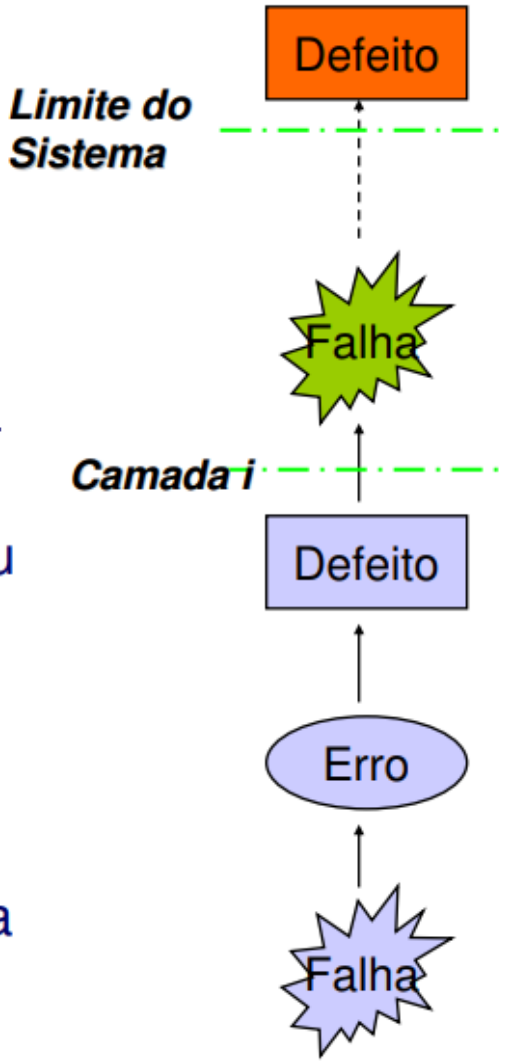
- Estado não especificado do HW ou SW

Um Erro é a manifestação de uma Falha no sistema

- O estado lógico do sistema difere do seu valor esperado

Um defeito é a manifestação do Erro no sistema

- O comportamento real do sistema deriva do seu comportamento esperado



O que é um sistema Tolerante a Falhas ?

- É um sistema que continua provendo corretamente os seus serviços mesmo na presença de falhas de hardware ou de software.
- Defeitos não são visíveis para o usuário, pois o sistema detecta e mascara (ou se recupera) defeitos antes que eles alcancem os limites do sistema.

O que é Tolerância a Falhas ?

- É o conjunto de técnicas utilizadas para detectar, mascarar e tolerar falhas no sistema.
- Redundância (técnica fundamental)
- Alta Disponibilidade

NÃO significa que falhas não vão ocorrer!

Conceitos Básicos

Requisitos para confiabilidade:

- Disponibilidade (availability)
- Confiabilidade (reliability)
- Segurança (safety)
- Capacidade de manutenção (maintainability)

Disponibilidade (availability)

- Indica que um sistema está pronto para uso imediato;
- Refere-se à probabilidade de que sistema está operando corretamente num dado instante e está disponível para executar suas funções;
- Alta disponibilidade indica que sistema muito provavelmente estará funcionando num dado instante;

Confiabilidade (reliability)

- Refere-se à propriedade que um sistema irá operar continuamente sem falha;
- É definida em termos de um intervalo de tempo, ao invés de num dado instante como ocorre com a disponibilidade;
- Sistema confiável é aquele que muito provavelmente irá operar sem interrupção durante um período relativamente longo de tempo;

Segurança (safety)

- Refere-se às consequências da falha de um sistema em operar corretamente;
- Sistemas críticos devem prover alto grau de segurança;

Capacidade de manutenção (maintainability)

- Indica a facilidade para que um sistema que falhou seja reparado;
- Sistema com alta capacidade de manutenção normalmente também apresenta alto grau de disponibilidade, especialmente se falhas podem ser detectadas e reparadas automaticamente;

DISPONIBILIDADE x CONFIABILIDADE

- Sistema que falha por 1 milissegundo a cada hora:
    - Disponibilidade alta, acima de 99.9999 %;
    - Confiabilidade baixa;
- Sistema que nunca cai (crashes) mas é desligado por 2 semanas no ano:
    - Alta confiabilidade;
    - Apenas 96 % de disponibilidade;

TIPOS DE FALHAS

- Transiente:
  - Ocorre uma vez e desaparece;
- Intermitente:
  - Ocorre, para por um período indeterminado, reaparece, e assim por diante;
- Permanente:
  - Continua a existir até que o componente faltoso seja substituído;

Tipo de falha	Descrição
Falha por queda	O servidor pára de funcionar, mas estava funcionando corretamente até parar.
Falha por omissão *Omissão de recebimento* *Omissão de envio*	O servidor não consegue responder a requisições que chegam O servidor não consegue receber mensagens que chegam O servidor não consegue enviar mensagens
Falha de temporização	A resposta do servidor se encontra fora do intervalo de tempo
Falha de resposta *Falha de valor* *Falha de transição de estado*	A resposta do servidor está incorreta O valor da resposta está errado O servidor se desvia do fluxo de controle correto
Falha arbitrária	Um servidor pode produzir respostas arbitrárias em momentos arbitrários

REDUNDÂNCIA

- Redundância de informação:
  - bits extras para recuperação de pacotes (Hamming);
- Redundância de tempo:
  - executar novamente uma ação, se for preciso;
- Redundância física:
  - adicionar equipamentos ou processos extras para possibilitar tolerância a perda ou mal funcionamento de alguns componentes;

RECUPERAÇÃO

Ocorrida uma falha, é necessário não apenas identificá-la, mas recuperar-se da mesma e voltar para um estado correto.

Essencialmente existem 2 maneiras de se recuperar:

- Recuperação retroativa – volta para um estado anterior à falha;
- Recuperação para a frente – tenta levar o sistema para um novo estado correto para que possa continuar a executar.

Faci facid FACIMP FBV fmc Faculdade Martha Falcão ISL UNIFAVIP UNI METROCAMP RUY BARBOSA | AREA1 UniFBV UniFanor