Tolerância a falhas

Eduardo Ferreira dos Santos

Ciência da Computação
Centro Universitário de Brasília – UniCEUB

Junho, 2017

Sumário

Desafios

- Desafios para sistemas de computação confiáveis e disponíveis [Weber, 2002]:
  - Como evitar, detectar e contornar bugs no projeto de hardware e software?
  - Como gerenciar a altíssima complexidade dos sistemas atuais de computação?
  - Como aproveitar novas tecnologias mais rápidas baratas e eficientes, mas ainda não totalmente provadas e testadas?
  -
- No que tange aos sistemas embarcados:
  - Como garantir confiabilidade e segurança nesses dispositivos?
  - Como garantir o baixo consumo de potência?
  - É preciso levar em consideração detalhes como peso e volume.

Falha, erro e defeito

- O objetivo do sistema de computação é atender a especificação;
- Defeito: desvio de especificação.
- Não se deve tolerar os defeitos, e sim evitar que eles aconteçam;
- O sistema está em erro (estado errôneo) se o processamento posterior levar a um defeito [Weber, 2002];
- Falha: causa física ou algorítmica do erro. São inevitáveis.

Defeito, erro e falha

- Uma falha necessariamente não leva a um erro;
- Um erro não necessariamente conduz a um defeito.

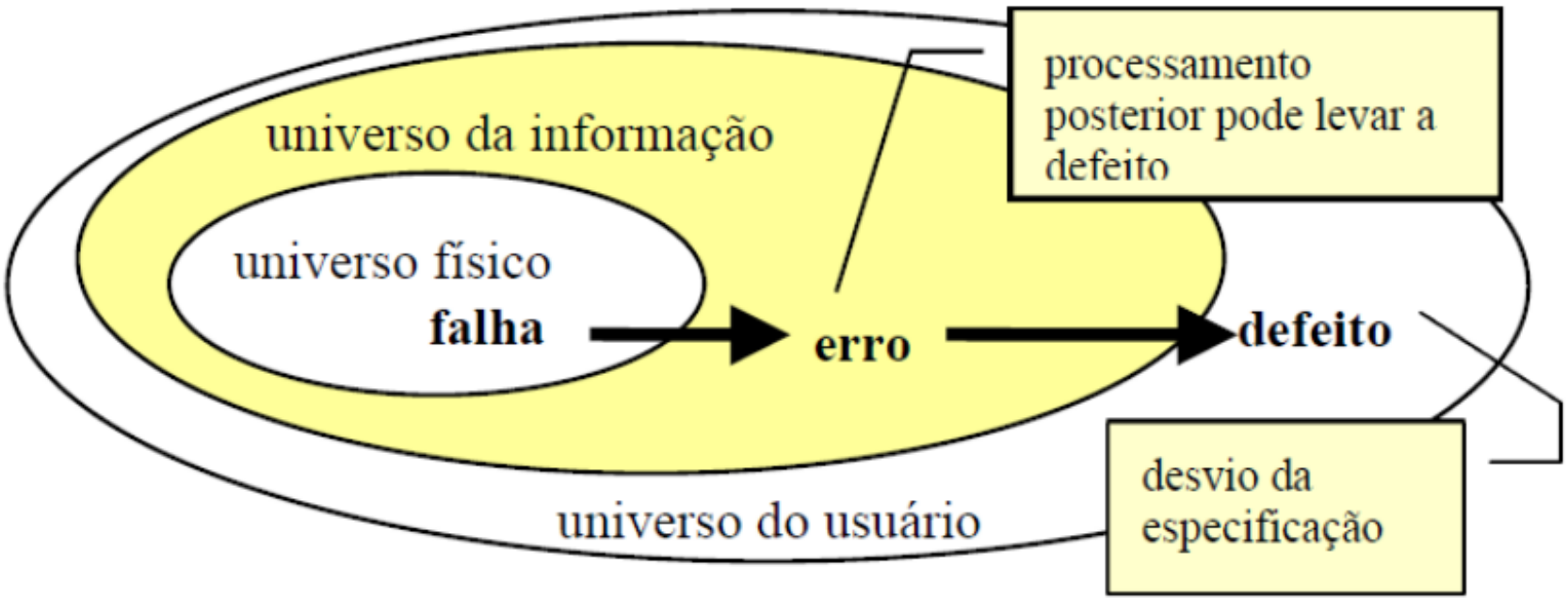

Figura 1.1: Universo de defeito, erro e falha [Weber, 2002]

Falhas [Weber, 2002]

Físicas	Relacionadas a componentes;
Humanas	Compreendem falhas de projeto;
Natureza	Hardware, software, projeto;
Persistência	Permanente ou temporária;
Extensão	Local ou global.

Causas de falhas

- Problemas de implementação;
- Problemas de especificação;
- Componentes defeituosos;
- Distúrbios externos: radiação, interferência eletromagnética, temperatura, humidade, etc.

Causas de falhas (cont.)

- Interação humana maliciosa [Chagas, 2016]:
  - Tratadas por técnicas de segurança não por técnicas de tolerância a falhas;
  - Software tolerante a falhas deve ser seguro a instruções e ações maliciosas;
- Sistemas críticos:
  - Construídos para suportar falhas físicas;
  - Problemas mais graves: falhas de software e de projeto;
  - Potencial de comprometer a confiabilidade e disponibilidade do sistema.

Defeito, erro e falha

Sistemas tradicionais				**Redes cliente-servidor** (não tolerantes a falhas)	
Não tolerantes a falhas		**Tolerantes a falhas**			
MTTF: 6 a 12 semanas Indisponibilidade após defeito: 1 a 4 horas		MTTF: 21 anos (Tandem)		Disponibilidade média: 98%	
Defeitos:		**Defeitos:**		**Defeitos:**	
hardware	50%	software	65%	projeto	60%
software	25%	operações	10%	operações	24%
comunicação/ambiente	15%	hardware	8%	físicos	16%
operações	10%	ambiente	7%		

Figura 1.2: Principais causas dos defeitos [Weber, 2002]

Definições

- O objetivo de um sistema tolerante a falhas é alcançar a dependabilidade [Chagas, 2016].

  O termo dependabilidade (...) indica a qualidade do serviço fornecido por um dado sistema e a confiança depositada no serviço fornecido. [Weber, 2002]

Atributos

Atributo	**Significado**
Dependabilidade *(dependability)*	qualidade do serviço fornecido por um dado sistema
Confiabilidade *(reliability)*	capacidade de atender a especificação, dentro de condições definidas, durante certo período de funcionamento e condicionado a estar operacional no início do período
Disponibilidade (*availability*)	probabilidade do sistema estar operacional num instante de tempo determinado; alternância de períodos de funcionamento e reparo
Segurança *(safety)*	probabilidade do sistema ou estar operacional e executar sua função corretamente ou descontinuar suas funções de forma a não provocar dano a outros sistema ou pessoas que dele dependam
Segurança (*security*)	proteção contra falhas maliciosas, visando privacidade, autenticidade, integridade e irrepudiabilidade dos dados

Figura 2.1: Principais atributos da dependabilidade [Weber, 2002]

Confiabilidade [Weber, 2002]

- Definição: capacidade de atender a especificação dentro de condições definidas;
- Algumas condições são essenciais para a confiabilidade:

  Especificação Sem a especificação não é possível determinar se o sistema está operando conforme o esperado

  Condições definidas As condições de funcionamento devem ser bem definidas;

  Período de funcionamento Conceito de tempo de missão;

  Estado operacional É necessário garantir o estado operacional no início da operação. Se o sistema já inicia com defeito, não é possível falar em confiabilidade.
- Confiabilidade é a medida mais importante em sistemas críticos.

Disponibilidade

- Definição: disponibilidade é a probabilidade do sistema estar operacional num instante de tempo determinado.
- A disponibilidade não deve ser confundida com a confiabilidade:
  - Mesmo o sistema tendo grandes intervalos inoperantes pode possuir alta disponibilidade. Ex.: manutenção programada.
  - Os períodos de indisponibilidade não podem alterar a qualidade do serviço.

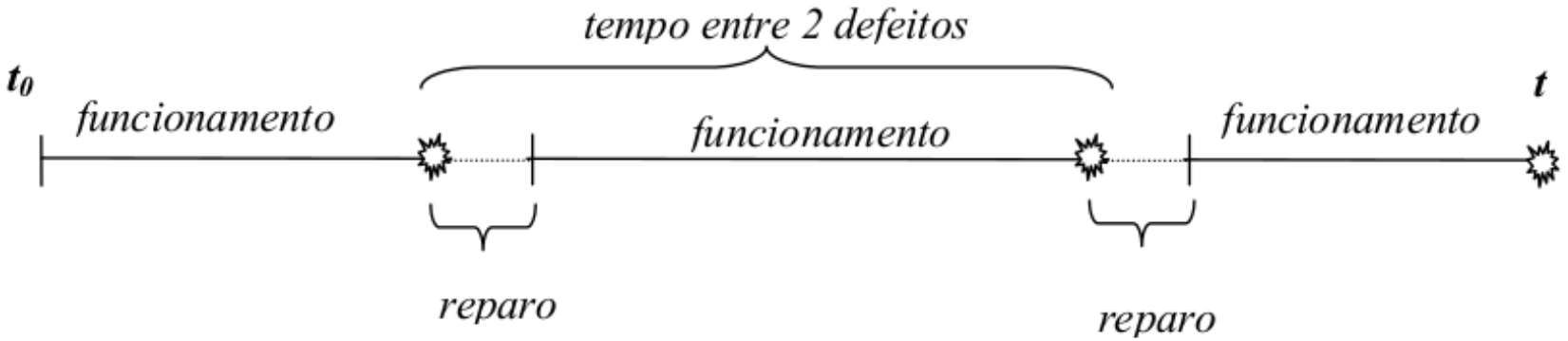

Figura 2.2: Alternância de períodos de funcionamento e reparo [Weber, 2002]

Segurança

- Definição: segurança de funcionamento (safety) é a probabilidade do sistema operacional executar sua função corretamente, ou descontinuar suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam [Weber, 2002];
- Definição II: Segurança é a medida da capacidade do sistema de se comportar de forma livre de falhas (fail-safe) [Weber, 2002];
- Ou a saída é correta ou o sistema é levado a um estado seguro;
- Proteção: o sistema deve garantir a autenticidade, privacidade, integridade e irrepudiabilidade dos dados (security).

Técnicas I

Figura 2.3: Métodos e técnicas para alcançar a dependabilidade [Chagas, 2016]

Técnicas II

Figura 2.4: Métodos e técnicas para alcançar a dependabilidade [Chagas, 2016]

Técnicas III

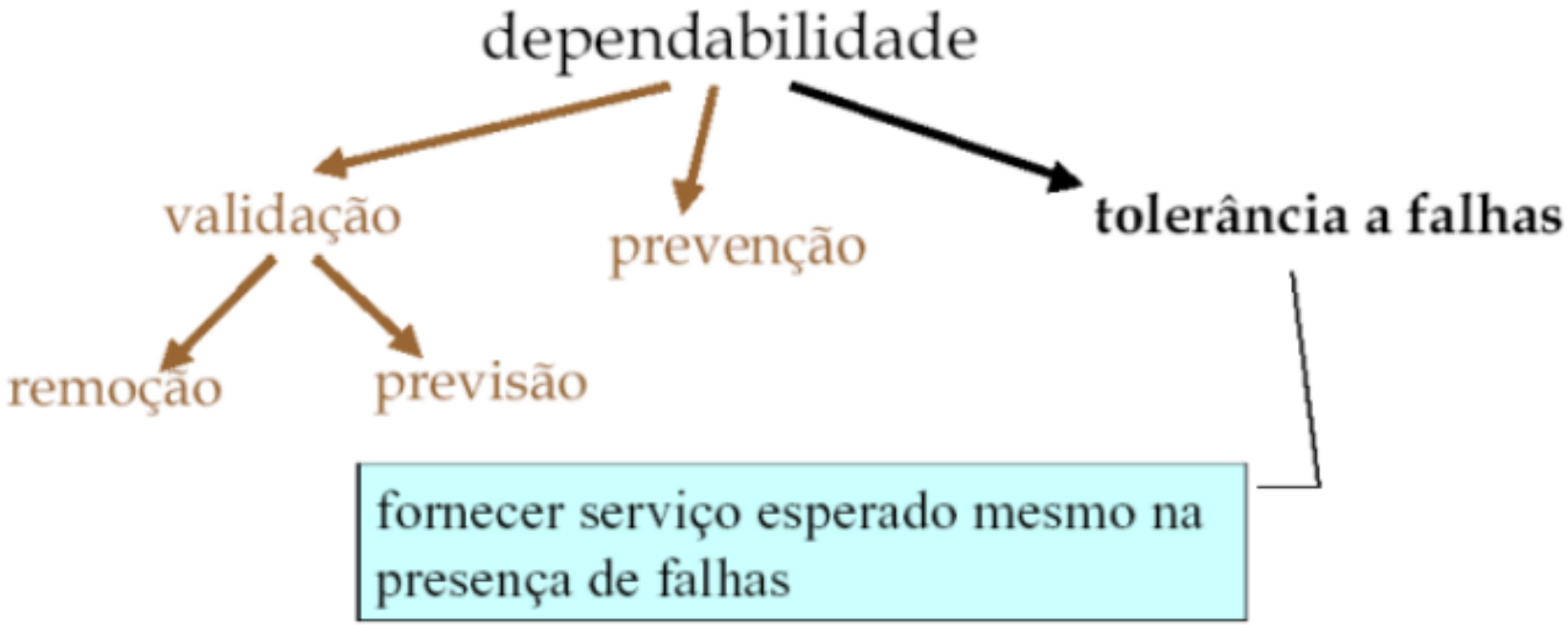

Figura 2.5: Métodos e técnicas para alcançar a dependabilidade [Chagas, 2016]

Outros atributos

Performability Comprometimento do desempenho. Medida da queda de desempenho provocada por falhas.

Manutenibilidade Facilidade de realizar a manutenção do sistema.

- O sistema com defeito deve ser restaurado dentro de um período determinado;
- Restauração: localização do problema, reparo físico e colocação em operação.

Testabilidade Capacidade de testar atributos internos e externos. Maior testabilidade provê maior manutenibilidade.

Tempo de funcionamento

Medida	**Significado**
Taxa de defeitos - *failure rate, hazard function, hazard rate*	número esperado de defeitos em um dado período de tempo; é assumido um valor constante durante o tempo de vida útil do componente.
MTTF - *mean time to failure*	tempo esperado até a primeira ocorrência de defeito
MTTR - *mean time to repair*	tempo médio para reparo do sistema
MTBF - *mean time between failure*	tempo médio entre as defeitos do sistema

Figura 2.6: Medidas relacionadas a tempo médio de funcionamento [Weber, 2002]

Introdução

- Prevenção e remoção de falhas não são suficientes quando o sistema exige alta confiabilidade ou alta disponibilidade;
- O sistema deve continuar funcionando mesmo na ocorrência de falhas;
- Foco das técnicas de tolerância falhas: redundância;
- Componentes frágeis e técnicas inadequadas.

Técnicas

- As técnicas de tolerância a falhas podem ser organizadas em duas classes disjuntas [Weber, 2002]:

  Mascaramento As falhas não são apresentadas como erros, pois são mascaradas na origem;

  Detecção, localização e reconfiguração O sistema reage de forma automatizada quando uma falha acontece.

- As técnicas de detecção, localização e reconfiguração são as preferidas em sistemas de tempo real críticos.

Aplicação

Fases	**Mecanismos**
detecção de erros	duplicação e comparação testes de limites de tempo cão de guarda (*watchdog timers*) testes reversos codificação: paridade, códigos de detecção de erros, Hamming teste de razoabilidade, de limites e de compatibilidades testes estruturais e de consistência diagnóstico
confinamento e avaliação	ações atômicas operações primitivas auto encapsuladas isolamento de processos regras do tipo tudo que não é permitido é proibido hierarquia de processos controle de recursos
recuperação de erros	técnicas de recuperação por retorno (*backward error recovery)* técnicas de recuperação por avanço (*forward error recovery)*
tratamento da falha	diagnóstico reparo

Figura 3.1: Quatro fases de aplicação [Weber, 2002]

Case Multicanal


Chagas, F. (2016).
Notas de aula do Prof. Fernando Chagas.


Weber, T. S. (2002).
Um roteiro para exploração dos conceitos básicos de tolerância a falhas.

OBRIGADO!!!
PERGUNTAS???