# Fundamentos de Tolerância a Falhas

*Taxonomia*

*Taisy Silva Weber*

# Falhas: classificação

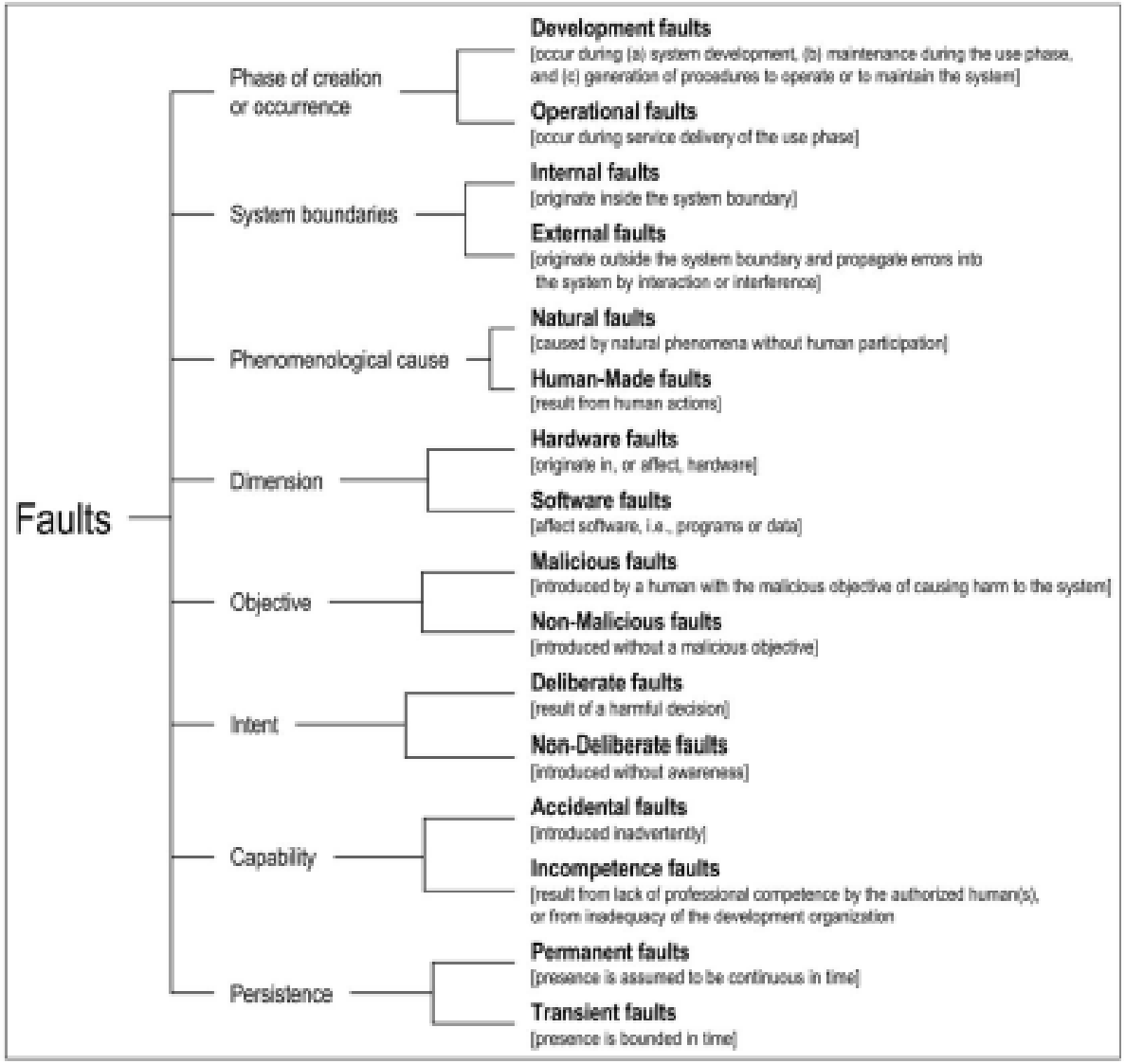
- inúmeras classificações diferentes
  - a classificação muda mesmo entre artigos do mesmo autor
    - exemplo: artigos do Avizienis
- classificação não é lei
    - apenas ajuda a entender os fenômenos e falar a mesma língua
- falhas maliciosas
  - mais importantes agora

Avizienis, Laprie, Randell, Landwehr. **Basic Concepts and Taxonomy of Dependable and Secure Computing**. IEEE Trans. on dep. and secure comp. 2004

# Classes elementares de falhas

- fase:
  - desenvolvimento
  - ou operacional
- limites:
  - interna
  - externa
- causa:
  - natural
  - humana
- dimensão:
  - falha de hardware
  - falha de software
- objetivo:
  - maliciosa
  - não maliciosa
- intenção:
  - deliberada
  - não deliberada
- capacidade:
  - acidental
  - devida a incompetência
- persistência:
  - permanente
  - temporária

# Classes de falhas

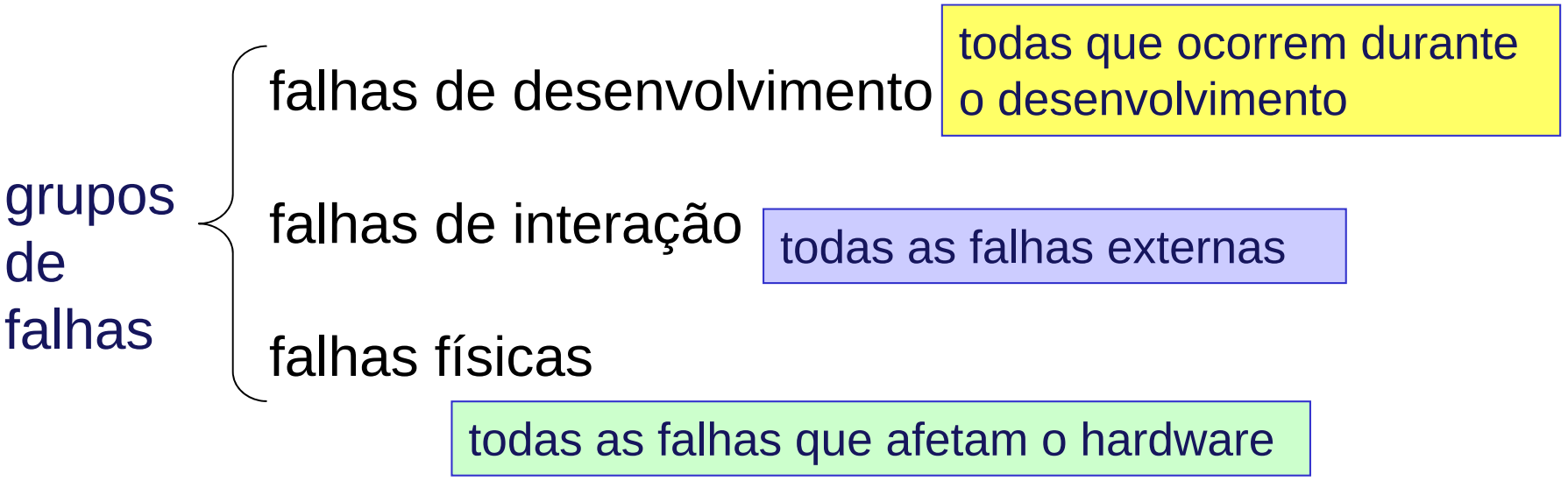



Avizienis, Laprie, Randell, Landwehr. **Basic Concepts and Taxonomy of Dependable and Secure Computing**. 2004

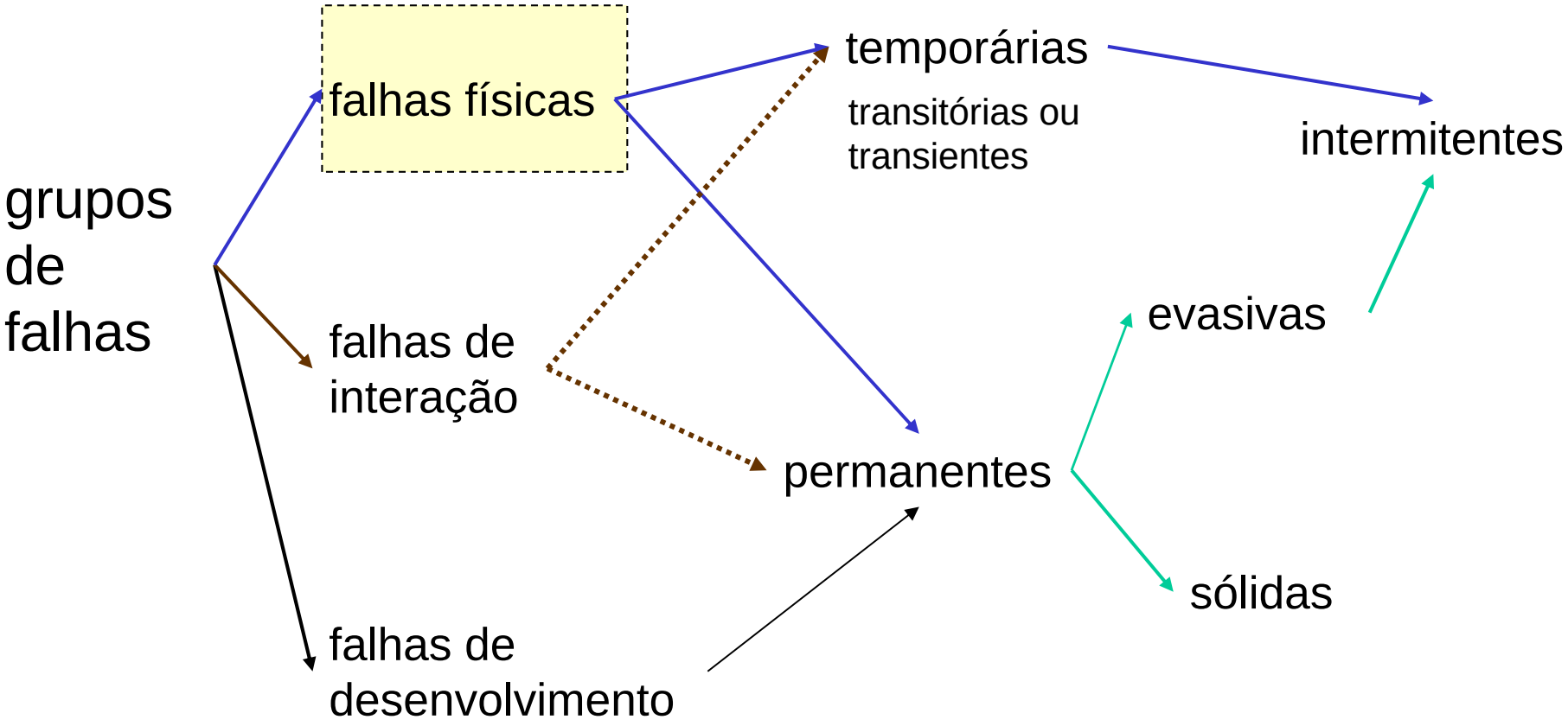
FIGURA 4

# Classes elementares de falhas

- 8 classes
  - podem ser combinadas entre si
  - nem todas as combinações fazem sentido
- as classes combinadas levam a 3 grupos parcialmente sobrepostos



# Falhas: grupos




falhas físicas, que afetam diretamente o hardware, foram mais estudadas

# Classes elementares de falhas

- fase:
  - desenvolvimento
  - ou operacional
- limites:
  - interna
  - externa
- causa:
  - natural
  - humana
- dimensão:
  - falha de hardware
  - falha de software
- objetivo:
  - maliciosa
  - não maliciosa
- intenção:
  - deliberada
  - não deliberada
- capacidade:
  - acidental
  - devida a incompetência
- persistência:
  - permanente
  - temporária

# Falhas naturais classe: causa

- naturais

  falhas causadas por fenômenos naturais sem participação humana

  - durante desenvolvimento
    - problemas de produção (*production defects*)
  - durante operação
    - interna: processos naturais de envelhecimento e deterioração física
    - externa: processos naturais originados fora dos limites do sistema que causam interferência física
      - radiação
      - transientes de potência
      - ruídos nas linhas de sinais, ...

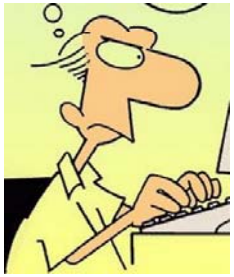
# Falhas humanas classe: causa

- fase:
  - desenvolvimento
  - ou operacional
- limites:
  - interna
  - externa
- causa:
  - natural
  - **humana**
- dimensão:
  - de hardware
  - de software

- objetivo:
  - maliciosa
  - não maliciosa
- intenção:
  - deliberada
  - não deliberada
- capacidade:
  - acidental
  - devida a incompe-tência
- persistência:
  - permanente
  - temporária

# Falhas humanas

fenômenos naturais sem participação humana



área de security

natural

humana

causa

objetivo

não-maliciosa

maliciosa

intenção

não intencional

intencional

intencional

capacidade

acidental

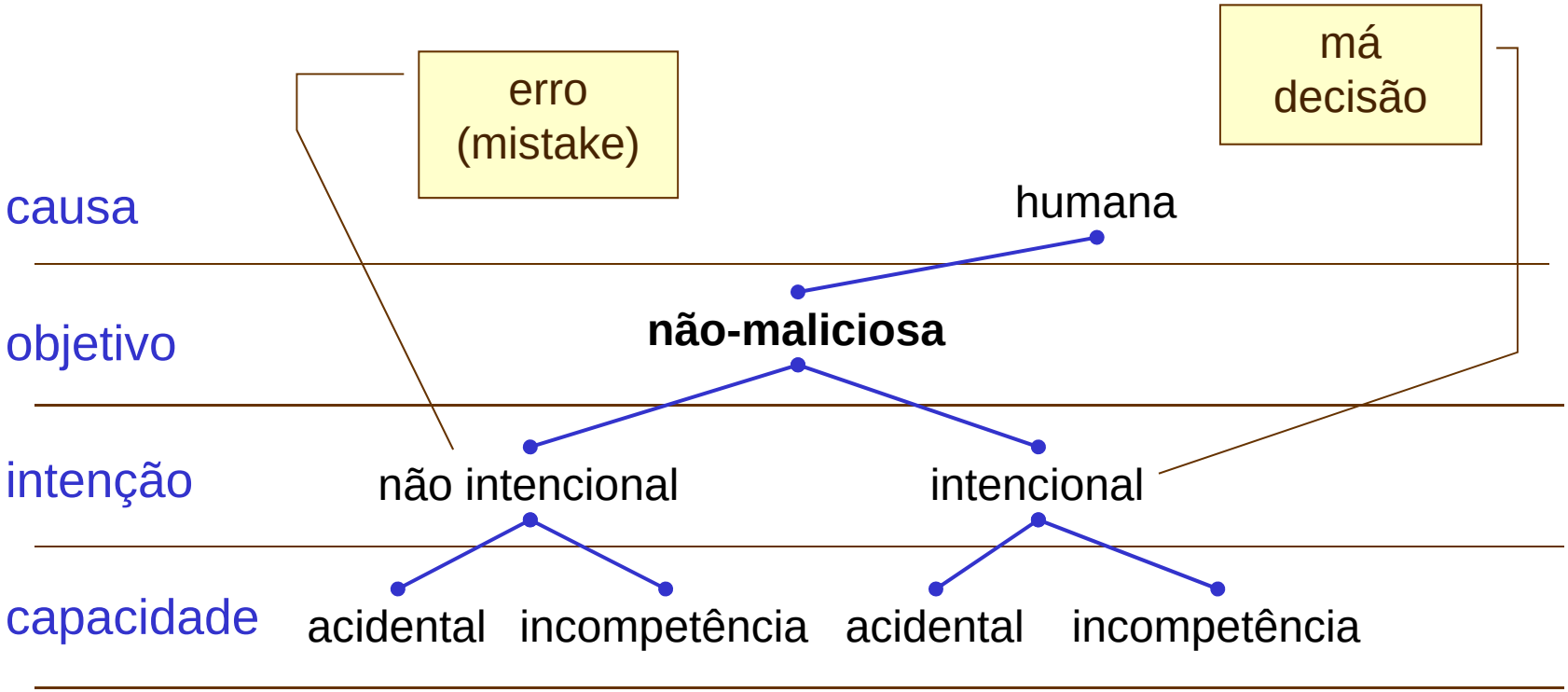
incompetência

acidental

incompetência

# Falhas humanas não-maliciosas

podem ocorrer na **fase** de desenvolvimento ou
na **fase** de operação do sistema



# Defeitos

- de serviço
- de desenvolvimento
- de dependabilidade e segurança

# Defeitos de serviço

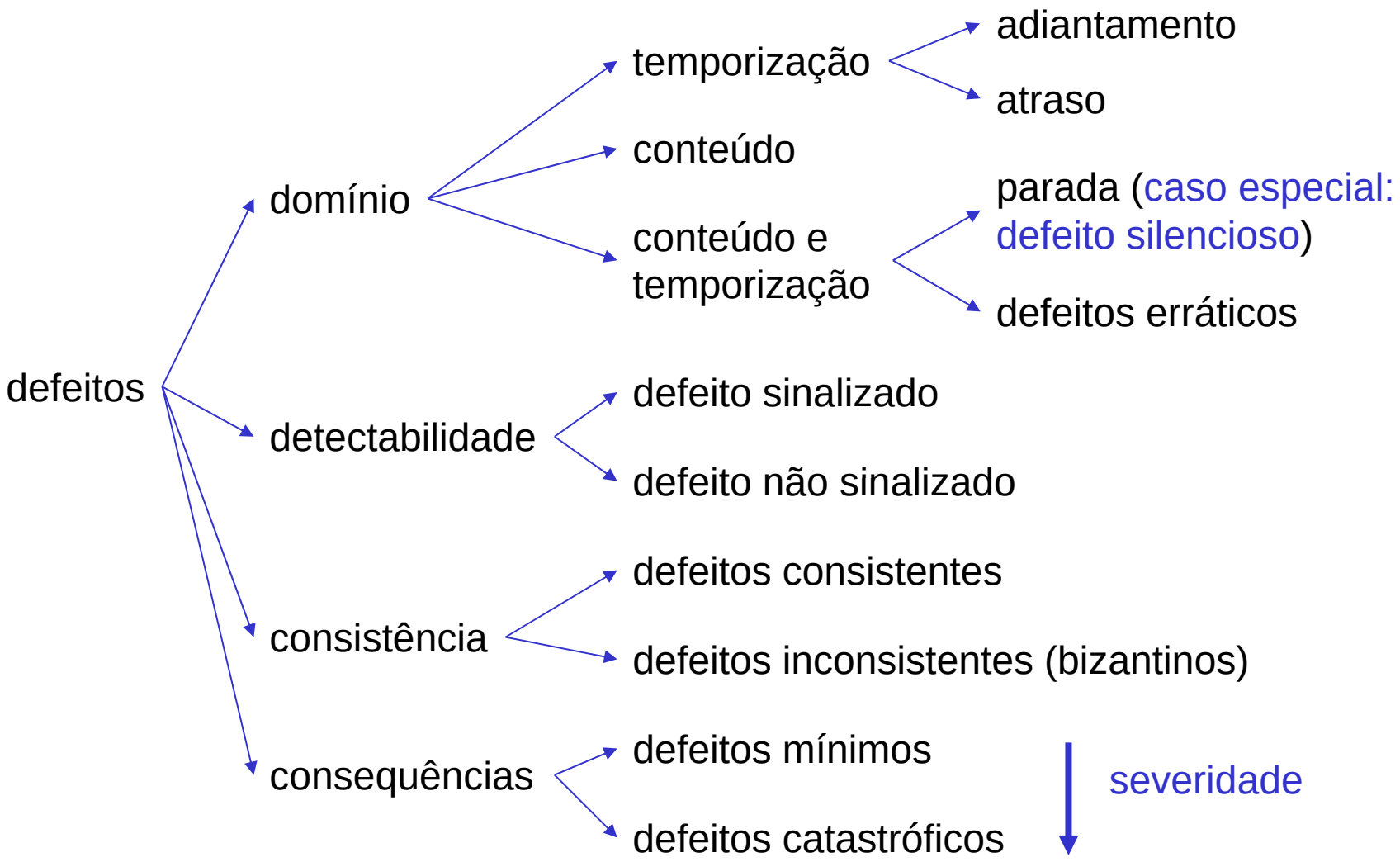
de serviço
de desenvolvimento
de dependabilidade e segurança

- quando o serviço oferecido se desvia de sua função

não quando se desvia da descrição da função, ou seja, da sua especificação

- cuidado:
  - a especificação do sistema identifica se um sistema é correto ou não
  - **mas** a especificação pode conter falhas

# Defeitos de serviço: pontos de vista



# Sistemas com controle de defeito

- sistemas projetados e controlados para apresentar defeito apenas nos modos de defeitos descritos na sua especificação de dependabilidade
- fail-halt ou fail-stop
  - defeitos de parada apenas
- fail-passive
  - serviço travado (congelado)
- fail-silent
  - defeito silencioso
- fail-safe
  - severidade mínima

# Defeitos de desenvolvimento

de serviço
de desenvolvimento
de dependabilidade e segurança

- tipos
  - defeitos completos de desenvolvimento
  - defeitos parciais
  - defeitos que só se manifestam na fase operacional
- origem
  - falhas de desenvolvimento
    - introduzidas por desenvolvedores ou
    - ferramentas de desenvolvimento ou
    - métodos de produção
- aspectos
  - orçamento
  - prazos

# Defeitos de desenvolvimento: causas

- complexidade do sistema subestimada
  - especificações incompletas ou com falhas
  - número excessivo de mudanças na especificação
  - projeto inadequado com respeito a funcionalidade ou desempenho
  - muitas falhas de desenvolvimento
  - capacidade inadequada de remoção de falhas
  - dependabilidade ou segurança computacional insuficiente
  - falha na estimativa dos custos de desenvolvimento

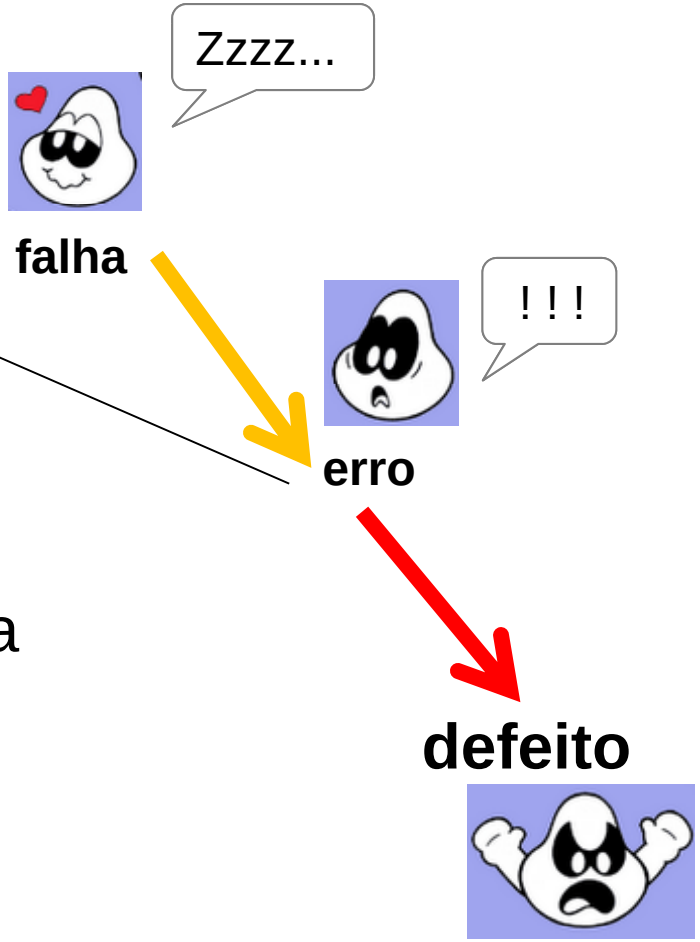
# Defeitos de dependabilidade

de serviço
de desenvolvimento
de dependabilidade e segurança

- a especificação de dependabilidade deve conter:
  - os objetivos de cada um dos atributos: disponibilidade, confiabilidade, segurança funcional, integridade, facilidade de manter, ...
  - identificação das classes de falhas
  - ambiente de uso (operação)
  - essa especificação também pode conter falhas
- defeito de dependabilidade
  - quando o sistema sofre defeitos de serviço mais frequentes ou severos do que o aceitável

# Erros

erros presentes mas não detectados são **latentes**




um erro é detectado se sua presença é indicada por uma mensagem de erro ou sinal de erro

# Erros

- classificação considerando:

**defeitos** de serviço que originam

a **falha** que originou o erro e seu espalhamento

- erro **simples**: falha afetou um único componente
- erros **múltiplos** relacionados: falha afetou mais de um componente

**número de bits** afetados (na área de códigos de detecção e correção de erros)

- erro simples, erro duplo, erro triplo, rajada, etc ..

# Bibliografia


- artigos
  - Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr. *Basic Concepts and Taxonomy of Dependable and Secure Computing*. IEEE trans. on dependable and secure computing, V. 1, n. 1, jan 2004, pp 11-33
  - VINCENZO DE FLORIO and CHRIS BLONDIA. *A Survey of Linguistic Structures for Application-Level Fault Tolerance.* ACM Computing Surveys, Vol. 40, No. 2, April 2008.
- capítulo de livro
  - Johnson, Barry. An introduction to the design na analysis of the fault-tolerante systems, cap 1. **Fault-Tolerant System Design**. Prentice Hall, New Jersey, 1996