Fundamentos de Tolerância a Falhas

Conceitos básicos

Taisy Silva Weber

Conceitos básicos

- falha, erro e defeito
- dependabilidade
  - confiabilidade, disponibilidade, segurança e outros
- taxonomia

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

conceitos básicos encontrados em livros de SO, redes, arquitetura, além de grande número de artigos (Laprie, Avizienis, Nelson, Cristian, Schneider, Siewiorek, Rennels…)

Falha, erro ou defeito?

- estado errôneo (ou erro)
  - se processamento posterior pode levar a defeito
- falha
  - causa física ou algorítmica do erro

falhas podem ser toleradas, defeitos não

falha → erro → defeito

válido aqui

fault → *error* → *failure*

alguns grupos no Brasil usam:
falta → erro → falha (tolerância a falta)

Falha, erro e defeito

falha é a causa do erro

falha

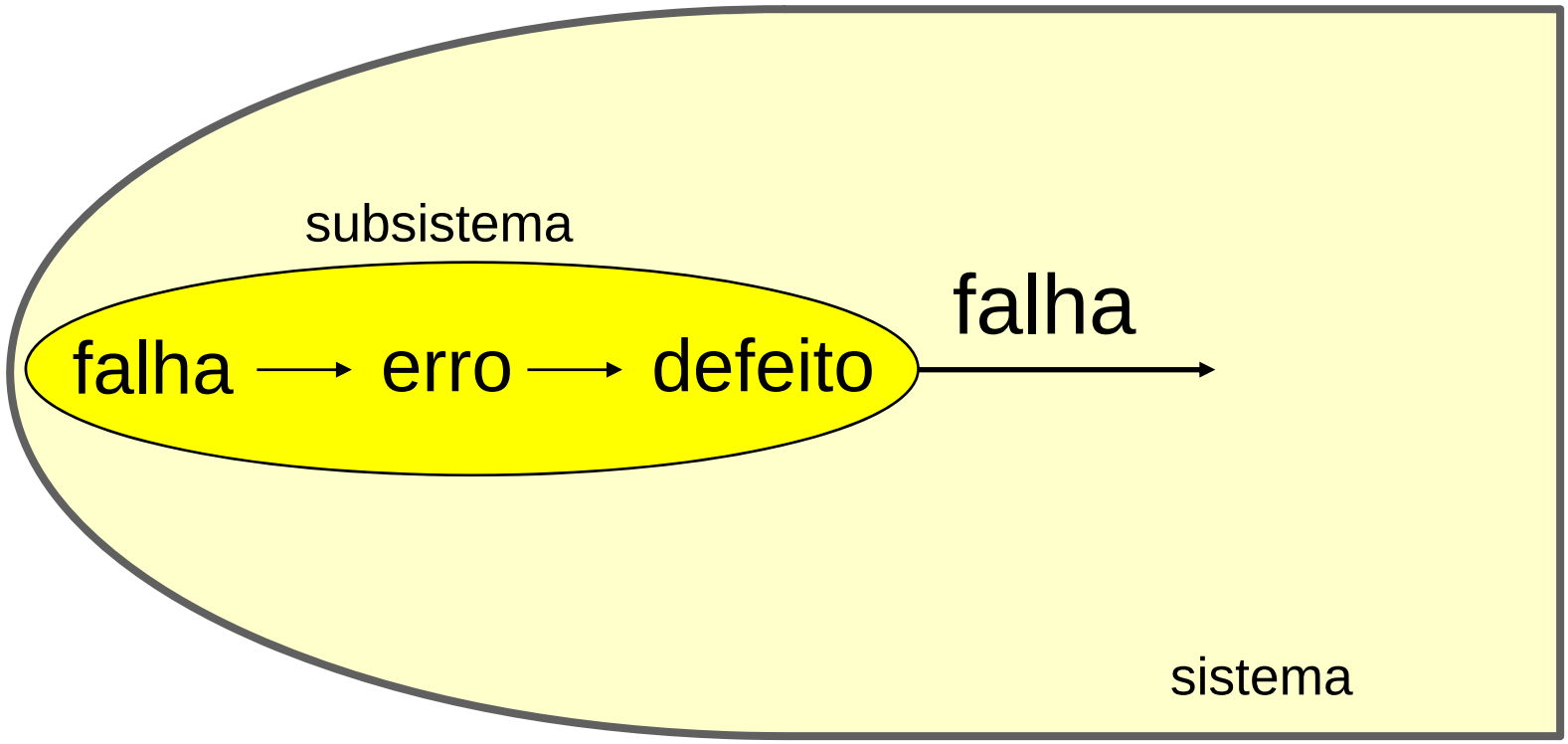
erro

um sistema está em estado errôneo (em **erro**) se processamento posterior pode levar a um defeito

defeito

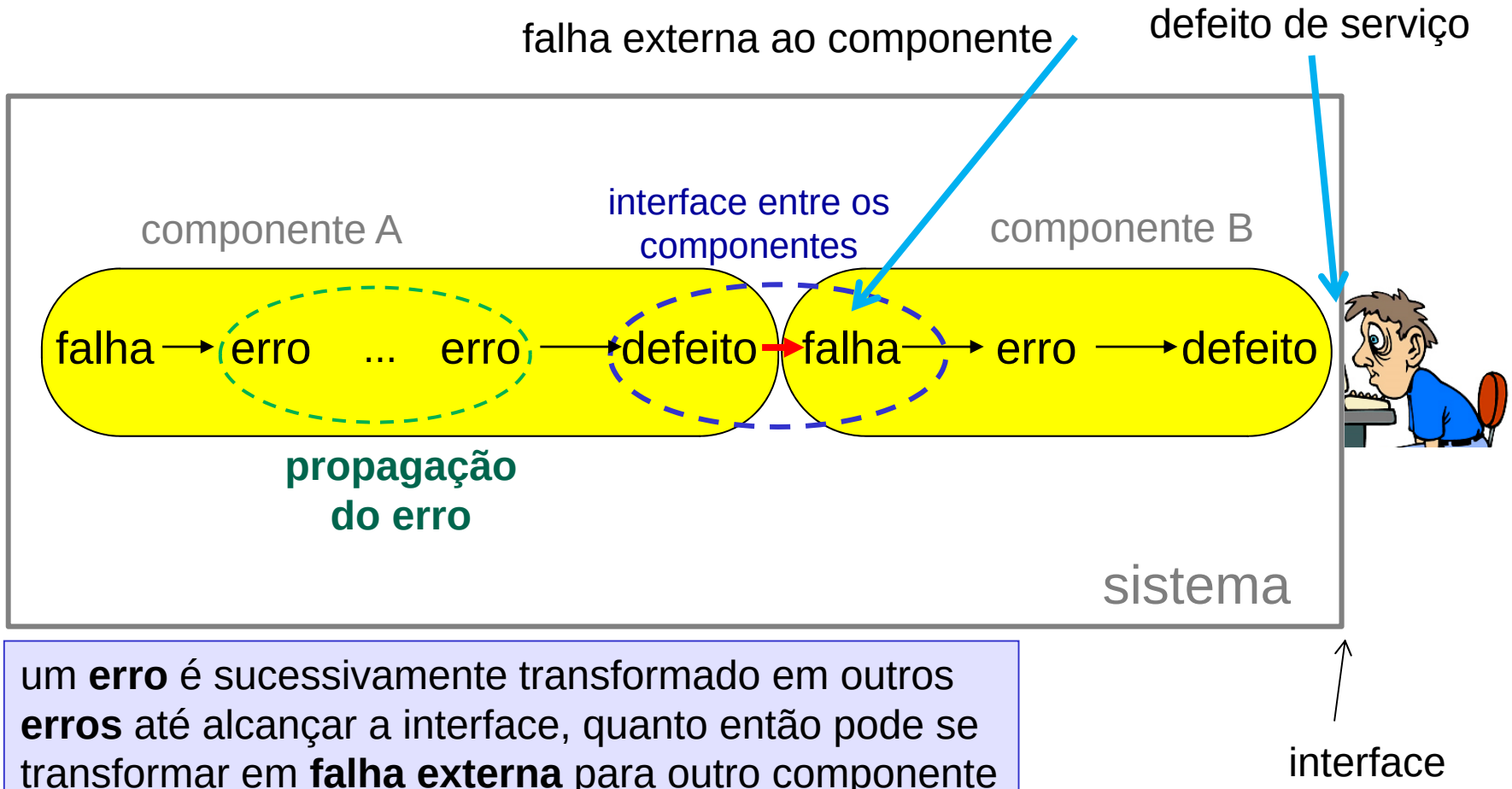
um **defeito** ocorre quando um sistema não fornece o serviço esperado

Defeito de subsistema



todo defeito é consequência de um erro, nas nem todo erro provoca um defeito

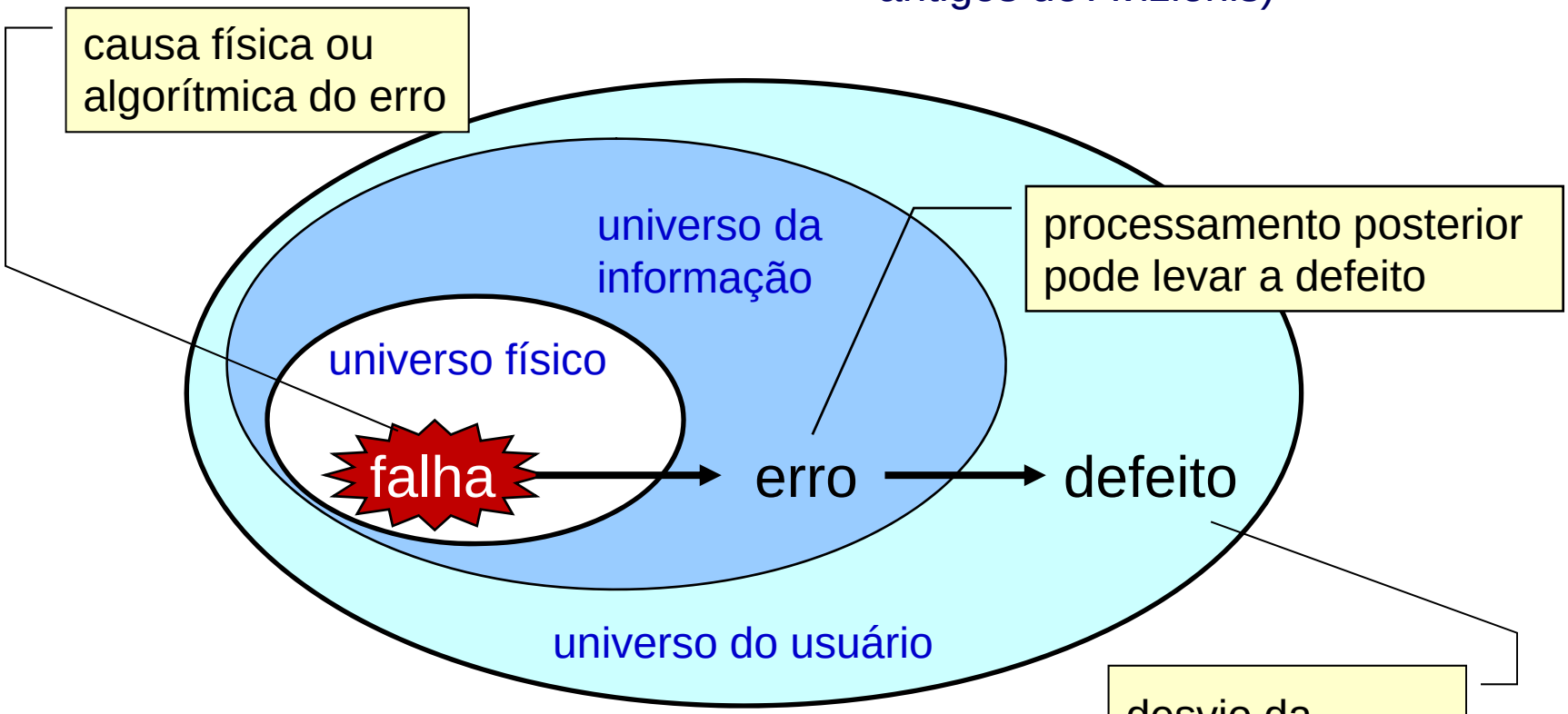
Propagação de erro



um **erro** é sucessivamente transformado em outros **erros** até alcançar a interface, quanto então pode se transformar em **falha externa** para outro componente ou em **defeito de serviço**

falha → erro → defeito

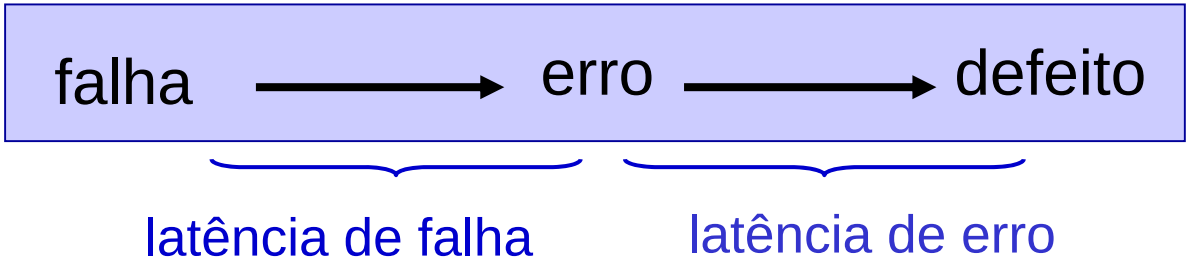
modelo de 3 universos (trabalhos antigos de Avizienis)



falhas podem ser toleradas, defeitos não

Latência

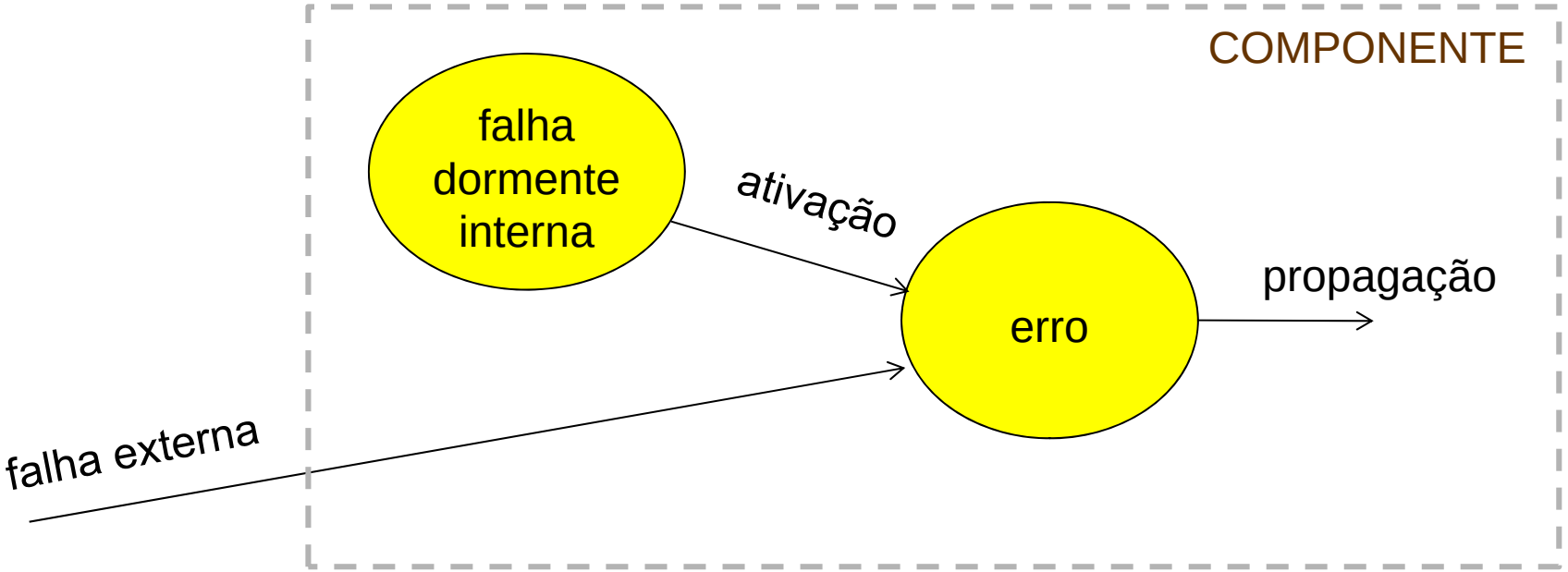
- latência de falha
  - período de tempo desde a ocorrência da falha até a manifestação do erro devido aquela falha
- latência de erro
  - período de tempo desde a ocorrência do erro até a manifestação do defeito devido aquele erro



Falha ativa

- falha
  - ativa
  - inativa ou dormente

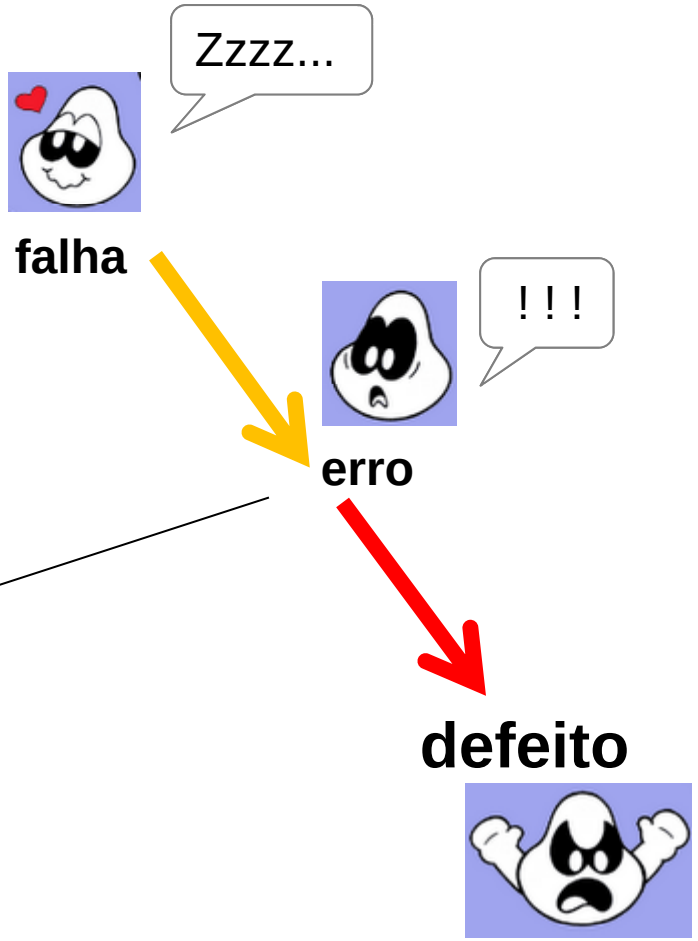
quando produz um erro



Dormentes e latentes

falhas presentes mas não ativadas são **dormentes**

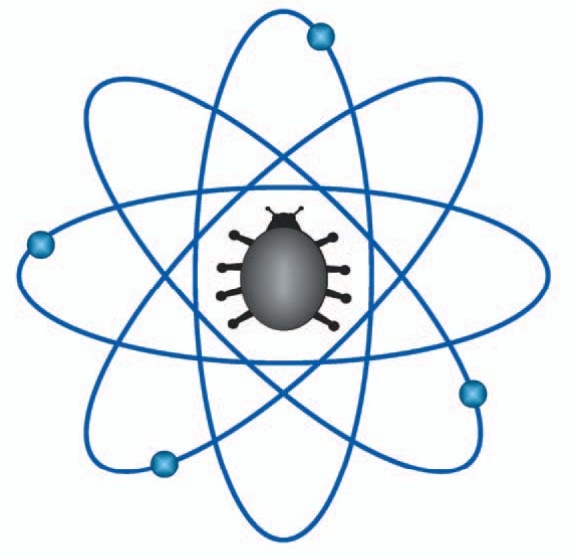
erros presentes mas não detectados são **latentes**



Reprodutibilidade da falha

- falhas sólidas (*hard*)
  - ativação reproduzível
- falhas evasivas (*soft*)
  - ativação não reproduzível
    ou reproduzível muito dificilmente

falhas residuais
geralmente soft



Fighting Bugs: Remove, Retry, Replicate, and Rejuvenate, Grottke e Trivedi, IEEE Computer, fev. 2007.

Dependabilidade

- *dependability*
  - habilidade de fornecer um serviço em que se pode depositar confiança
  - habilidade do sistema de evitar defeitos que sejam mais frequentes ou mais severos do que aceitável
- outras definições:
  - qualidade do serviço fornecido por um dado sistema
  - confiança justificável no serviço fornecido

Atributos de dependabilidade

- confiabilidade (*reliability*):
  - continuidade do serviço correto
- disponibilidade (*availability*):
  - prontidão para serviço correto

mais conhecidas

- segurança (*safety*):
  - ausência de consequências catastróficas para o usuário ou ambiente
- integridade (*integrity*):
  - ausência de alterações impróprias no sistema
- *maintainability*:
  - facilidade de executar modificações e reparos

Confiabilidade

reliability

- capacidade de atender à especificação
  - dentro de condições definidas
  - durante certo período de funcionamento
  - condicionado a estar operacional no início do período
- probabilidade que um sistema funcione corretamente durante um intervalo de tempo

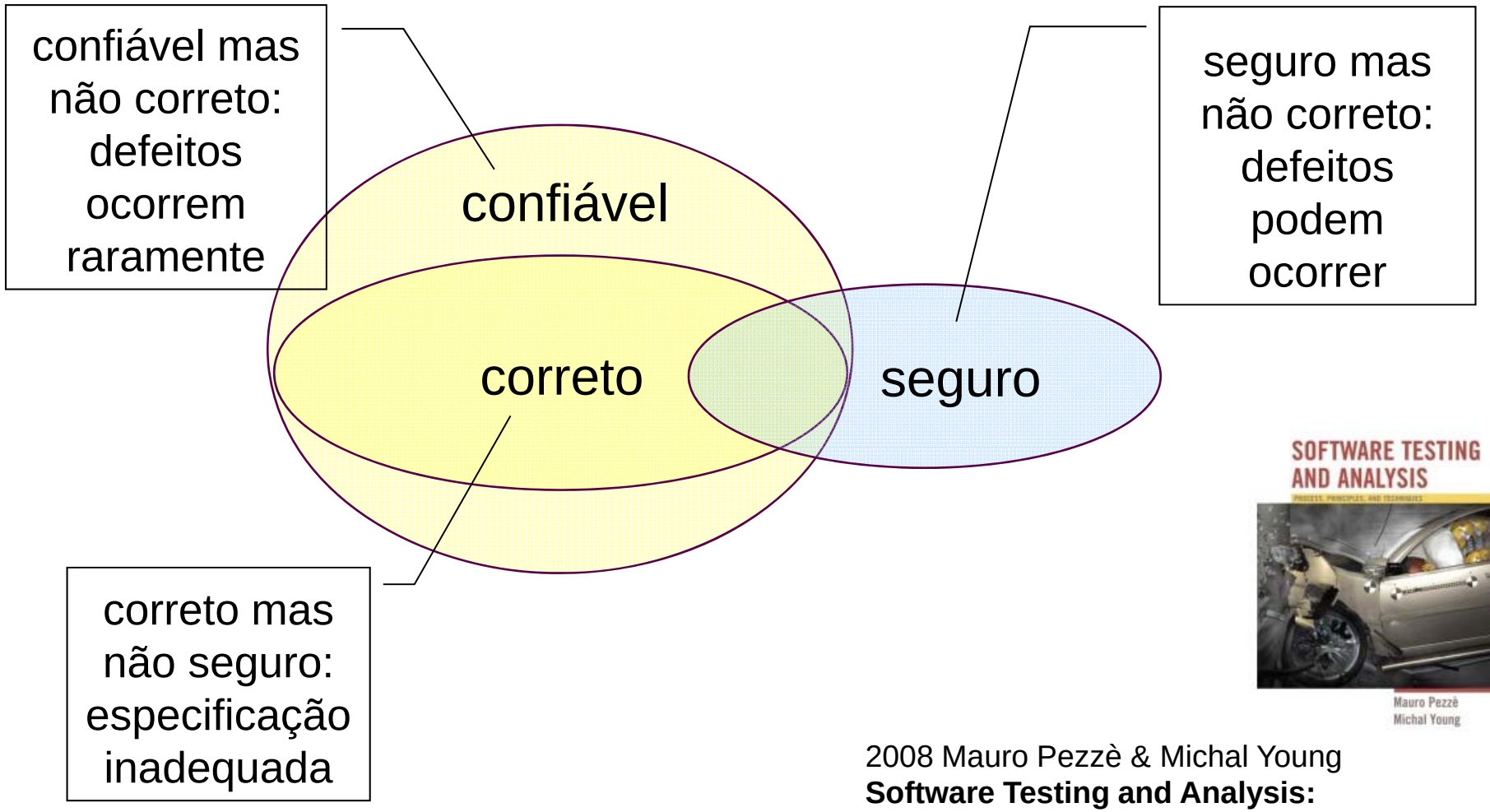
Confiabilidade: exemplo

- sistemas em que mesmo curtos períodos de operação incorreta são inaceitáveis
- aviação
  - tempo de missão: 10 a 12 horas

Confiabilidade e correção

- confiabilidade é uma aproximação estatística da correção
  - correção funcional é sempre absoluta (um sistema é correto ou não)
  - confiabilidade de 100% = correção
- semelhança: ambas definidas em relação a uma especificação
- diferença:
  - confiabilidade é relacionada ao perfil de utilização
    - um sistema pode ser mais ou menos confiável dependendo de como é usado

Confiabilidade, correção e safety



2008 Mauro Pezzè & Michal Young
Software Testing and Analysis: Process, Principles, and Techniques

Disponibilidade

availability

- alternância de períodos de funcionamento e reparo
  - um sistema pode ser altamente disponível mesmo apresentando períodos sem operabilidade

desde que esses períodos sejam curtos

Disponibilidade vs confiabilidade

Taisy Weber

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

não são sinônimos: um sistema pode ser altamente confiável e ter baixa disponibilidade

Segurança funcional

safety

- ausência de consequências catastróficas

atributo usual na área de controle de processos industriais, transporte, aviônica e instrumentação médica

necessita do conhecimento e especificação dos danos a serem evitados

Outros atributos

- *maintainability*
  - facilidade de realizar a manutenção do sistema

probabilidade que um sistema com defeitos seja restaurado dentro de um dado período de tempo

- testabilidade
  - facilidade de realizar testes

relacionada a facilidade de manutenção

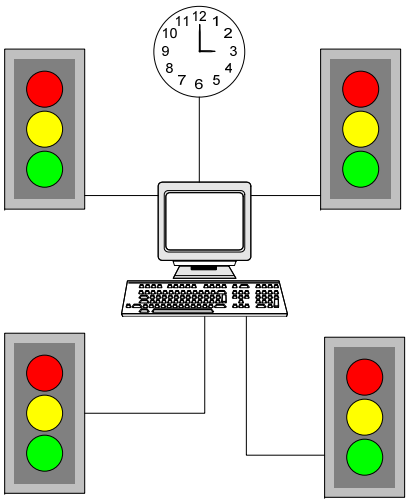
Outros atributos

- *performability*
  - queda de desempenho provocada por falhas
- robustez
  - modo como o sistema apresenta defeito se usado fora das condições normais

sistema continua a operar, mas com queda de desempenho

um sistema é robusto quando em condições inesperadas apresenta defeito, mas sem provocar danos consideráveis

Exemplo de atributos



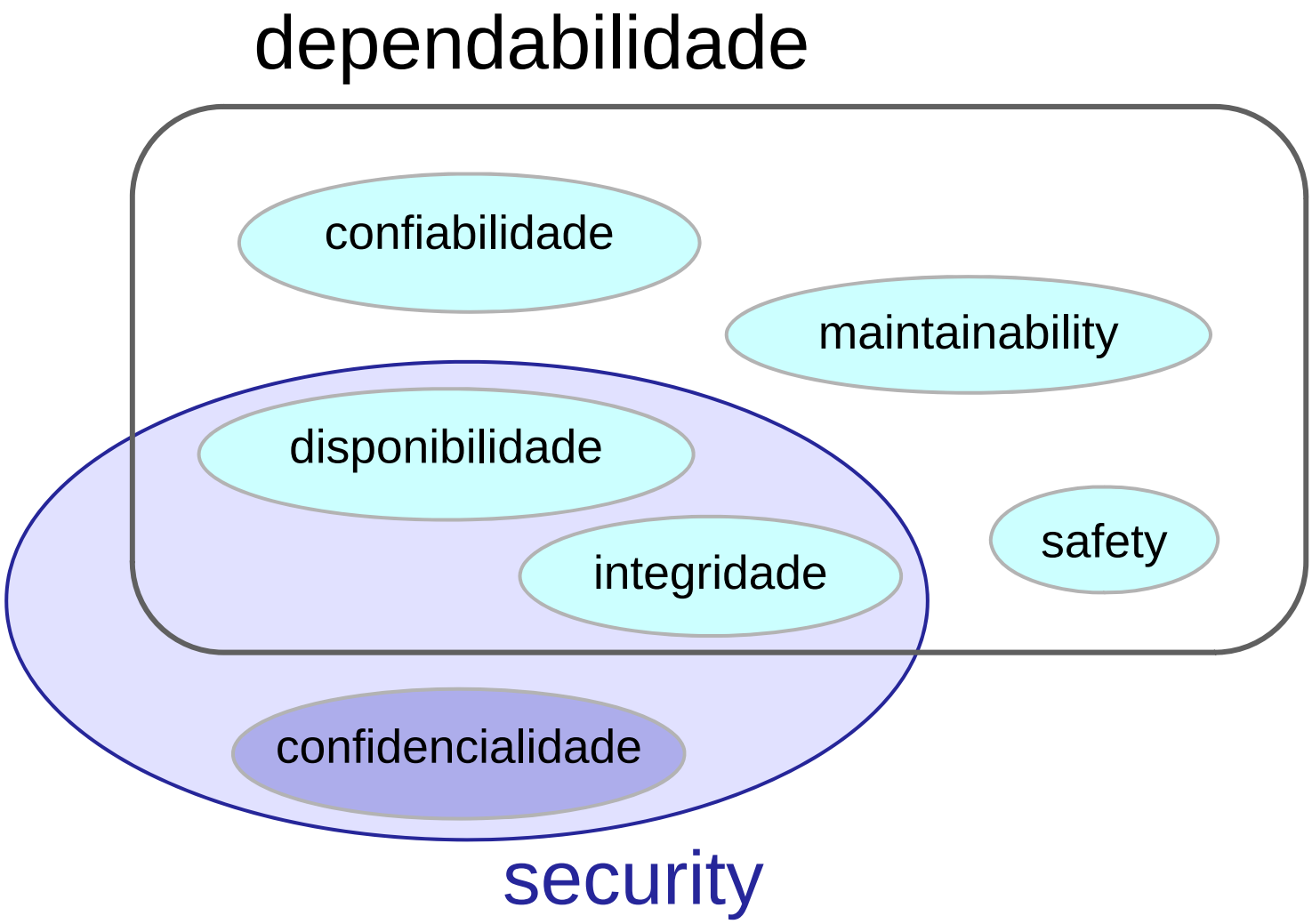
- correção, confiabilidade
  - permitir tráfego de acordo com especificação e escalonamento
- robustez
  - degradação de função se possível:
    - amarelo piscando é melhor que todos desligados
    - desligados é melhor que todos verdes
- segurança
  - nunca todos verdes

security & safety

- safety: segurança funcional
  - ausência de consequências catastróficas para o usuário ou ambiente
- security: segurança computacional
  - confidencialidade, integridade, autenticidade
  - autenticidade
    - disponibilidade apenas para ações autorizadas
  - integridade é um atributo comum a dependabilidade e *security*

desejável que um sistema seja seguro nas duas acepções do termo

security & safety



Termos relacionados

- Dependability
  - habilidade do sistema de evitar defeitos que sejam mais frequentes ou mais severos do que aceitável
- High Confidence
  - consequências do comportamento do sistema são perfeitamente compreendidas e previsíveis
- Survivability
  - capacidade do sistema de cumprir sua missão no tempo adequado
- Trustworthiness
  - garantia que o sistema vai funcionar como esperado

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

Trustworthiness

- fidedignidade (?)
- atributos de software
  - correção
  - segurança funcional (safety)
  - qualidade de serviço
    - disponibilidade
    - confiabilidade
    - desempenho
  - segurança computacional (security)
  - privacidade

no documento Grandes Desafios da Computação, SBC 2007, fidedignidade aparece como tradução de *dependability*

Wilhelm Hasselbring, Ralf Reussner
Toward Trustworthy Software Systems
Computer, april 2006

Falhas são inevitáveis

- problemas de especificação
- problemas de projeto e implementação
- componentes defeituosos
    - imperfeições de manufatura
    - fadiga e/ou envelhecimento
- distúrbios externos
    - radiação,
    - interferência eletromagnética,
    - variações ambientais (temperatura, pressão, umidade),
    - problemas de operação

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, jan 2004, pp 11-33
  - Grottke e Trivedi, ***Fighting Bugs: Remove, Retry, Replicate, and Rejuvenate***, IEEE Computer, fev. 2007.
  - Wilhelm Hasselbring, Ralf Reussner. ***Toward Trustworthy Software Systems***. Computer, april 2006

Bibliografia

- livros
  - Koren, Israel, e C. Mani Krishna. 2007. **Fault-Tolerant Systems**. Morgan Kaufmann
  - Birman, K. **Reliable distributed systems**. Springer, New York, 2005.
  - Pezzè, Mauro, e Michal Young. 2008. **Software Testing and Analysis: Process, Principles, and Techniques**. Wiley.
- capítulo de livro
  - Johnson, Barry. An introduction to the design na analysis of the fault-tolerant systems, cap 1**. Fault-Tolerant System Design**. Prentice Hall, 1996