

# *Sistemas Distribuídos e Tolerância a Falhas*

## *Mestrado em Engenharia Informática*

*1<sup>a</sup> ano / 2<sup>a</sup> semestre*

### *Bibliografia:*

- *Basic Concepts and Taxonomy of Dependable and Secure Computing*, **A. Avizienis, J.C. Laprie B. Randell and C. Landwehr**, *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, January-March 2004.

**[Tanenbaum2007]** “Distributed Systems Principles and Paradigms”, Andrew S. Tanenbaum and Maarten Van Steen, Pearson International Edition, 2007. (Cap. 6,7 e 8).

**[Verissimo2001]** “Distributed Systems for System Architects”, Paulo Veríssimo and Luís Rodrigues, Kluwer Academic Publishers, 2001.

**[Jalote1998]** “Fault Tolerance in Distributed Systems”, Pankaj Jalote, Prentice-Hall, 1998.

## Confiança no funcionamento

*“Dependability”*

*Dependabilidade / Confiabilidade*

“Dependability – the measure in which reliance can justifiably be placed on the service delivered by a system”

### Confiabilidade

Indica a qualidade do serviço fornecido por um dado sistema e a confiança que justificadamente pode ser depositada nesse serviço

Dizemos que um sistema é confiável se existe uma elevada probabilidade de o seu comportamento estar de acordo com a especificação.

- *Algumas causas de avarias:*
  - *problemas de especificação,*
  - *problemas de implementação,*
  - *componentes defeituosos,*
  - *fadiga dos componentes,*
  - *distúrbios externos: radiação, interferência electromagnética, variações ambientais, problemas de operação ...*

Causas mais comuns de avarias [Laprie98]:

Sistemas Tradicionais

Redes cliente-servidor

Não tolerantes a falhas

Tolerantes a falhas

(não tolerantes a falhas)

MTTF !: 6 a 12 semanas

Indisponibilidade após  
avaria: 1 a 4 horas

Avarias:

hardware 50%

software 25%

Comunicação  
/ambiente 15%

operação 10%

MTTF: 21 anos

(Tandem)

Avarias:

software 65%

operação 10%

hardware 8%

ambiente 7%

Disponibilidade média: 98%

Avarias:

projecto 60%

operação 24%

físicas 16%

[Laprie98], *Dependability of Computer Systems: from Concepts to Limits*, IFIP International Workshop on Dependable Computing and its Applications, Johannesburg, January 1998, pp. 108 - 126

Algumas Definições:

**Sistema:** Entidade que interage ou interfere com outras entidades, i. é, com outros sistemas.

**Serviço:** Comportamento do sistema tal como é observado pelos seus utilizadores

**Utilizador:** Outro sistema (humano ou não) que interage com o primeiro. Faz uso do serviço fornecido pelo sistema

**Especificação:** Descrição do serviço ou função que se espera que o sistema desempenhe.

**Estado do Sistema:** Condição em que o sistema se encontra relativamente a certas circunstâncias (e.g., relativamente à ocorrência de falhas, às operações internas)

## Entraves à Confiabilidade:

Definições de “fault”, “error”, “failure”:

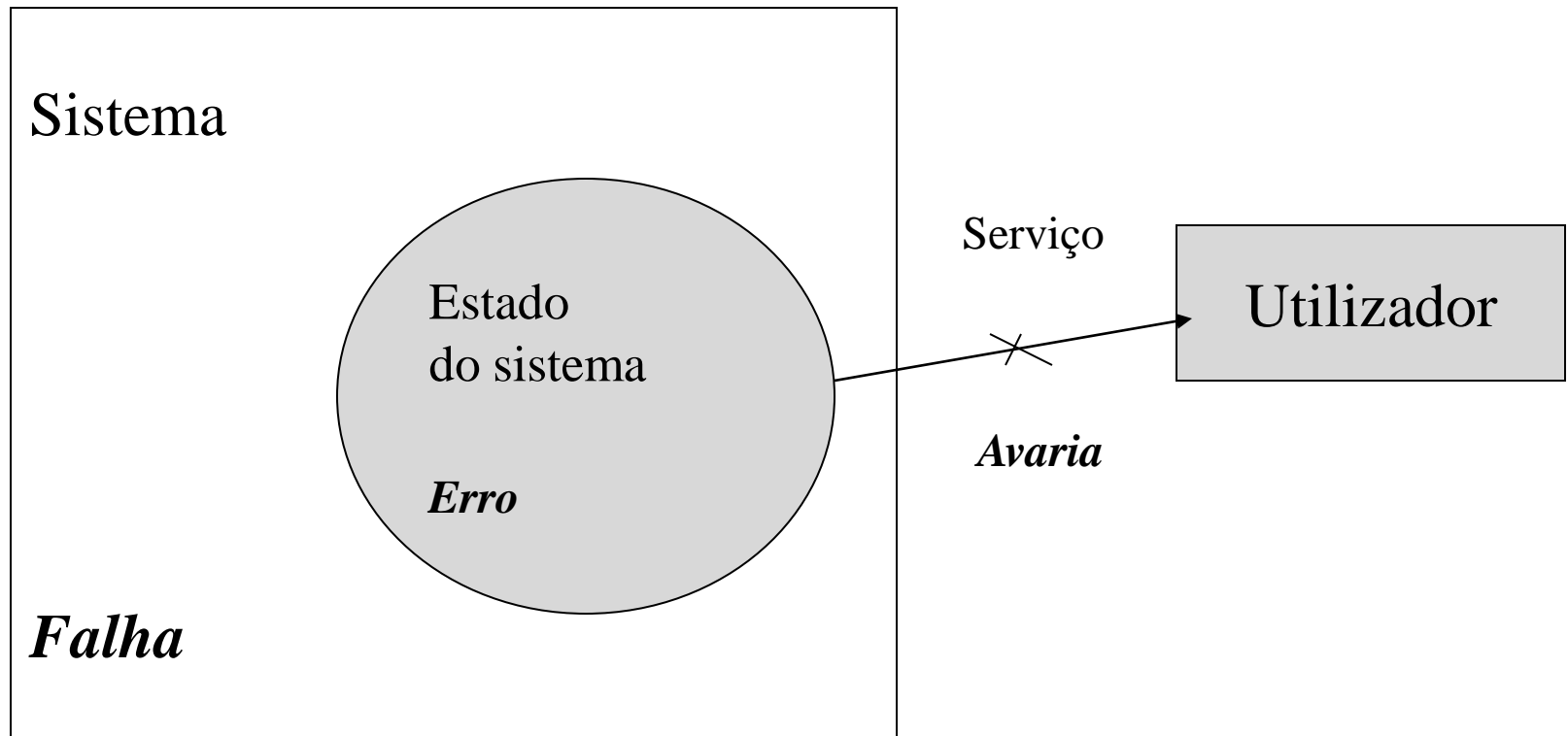
Termos em português:

falha, erro, avaria (grupo de Coimbra) - adoptado neste curso

*(falta/defeito, erro, falha - grupo de Lisboa)*

Falha (“fault”) – uma falha é uma alteração do funcionamento de um componente (hardware ou software) do sistema

Uma falha pode ocorrer de forma acidental ou intencional.



## Falha (“fault”)

Podemos classificar as falhas em três grandes grupos:

Falhas de Projecto (hardware ou software):

uma falha pode ocorrer em qualquer etapa do desenvolvimento de um sistema:  
especificação, desenho, implementação.

Falhas Físicas: defeitos de produção, deterioração dos componentes, interferência

Falhas de interacção homem – máquina: inputs errados, ataques ou intrusões



## Falha (“fault”)

As Falhas de hardware são geralmente classificadas em relação à sua duração:

- Falhas permanentes (“permanent faults”) - resultam de um defeito físico irreversível, permanecem indefinidamente até serem reparadas.
- Falhas intermitentes (“intermittent faults”) - falhas temporárias que ocorrem repetidamente.
- Falhas transitórias (“transient faults”) – falhas temporárias que ocorrem ocasionalmente num muito curto espaço de tempo.
  - são as mais frequentes e mais difíceis de detectar
  - podem ser causadas por oscilações na corrente eléctrica, interferências electromagnéticas ou radiação

## Falha (“fault”)

*A crescente complexidade do hardware e software aumenta a probabilidade de falhas na sua concepção e implementação, assim como a susceptibilidade do hardware a factores externos.*

Uma falha pode não produzir qualquer efeito, permanecendo inactiva, ou pode dar origem a uma alteração do estado do sistema, tornando-se uma falha activa

O intervalo de tempo entre a ocorrência da falha e a sua activação denomina-se por latência de falha

Erro (“error”) – um erro é a manifestação de uma falha

Um erro provoca a corrupção de elementos de dados (afecta o estado do sistema)

Quando, como resultado de um erro, o sistema executa erradamente uma das suas funções, i.é, o sistema avaria, o erro tornou-se efectivo

Se um erro causa ou não a avaria do sistema depende de:

- . Composição do sistema (por exemplo, existe redundância que mascare a ocorrência do erro)
- . Actividade do sistema (por exemplo, o estado que contém o erro pode não ser suficientemente duradoiro para causar uma avaria)
- . Definição de avaria, do ponto de vista do utilizador ...

O intervalo de tempo entre a ocorrência do erro e o aparecimento da avaria correspondente denomina-se por latência do erro

Avaria (“failure”) – uma avaria é qualquer alteração do comportamento do sistema em relação ao esperado (i.é, em relação à sua especificação)



As avarias de um sistema podem ser caracterizadas de acordo com 4 pontos de vista,

(Modos de Avaria)

- . Domínio
- . Percepção pelos utilizadores
- . Consistência
- . Consequências sobre o meio envolvente

## Modos de Avaria:

### . Domínio

- Avarias de conteúdo ou de valor.

Os resultados produzidos são diferentes dos esperados para a funcionalidade do sistema.

- Avarias temporais.

Os resultados são produzidos fora do tempo esperado (demasiado cedo ou demasiado tarde)

## Modos de avaria:

### . Percepção do utilizador

A avaria pode ser detectada e assinalada ao utilizador ou não.

- Avaria sinalizável
- Avaria não sinalizável

### . Consistência

- Avaria consistente

a avaria é percebida de igual forma por todos os utilizadores

- Avaria inconsistente

diferentes utilizadores recebem diferentes resultados (avaría Byzantina)

## Modos de avaria:

### . Consequências sobre o meio envolvente

- Avarias benignas
- Avarias catastróficas

A severidade de uma avaria representa uma medida das respectivas consequências sobre o meio envolvente.

Um sistema cuja avaria, tem severidade máxima denomina-se sistema crítico.



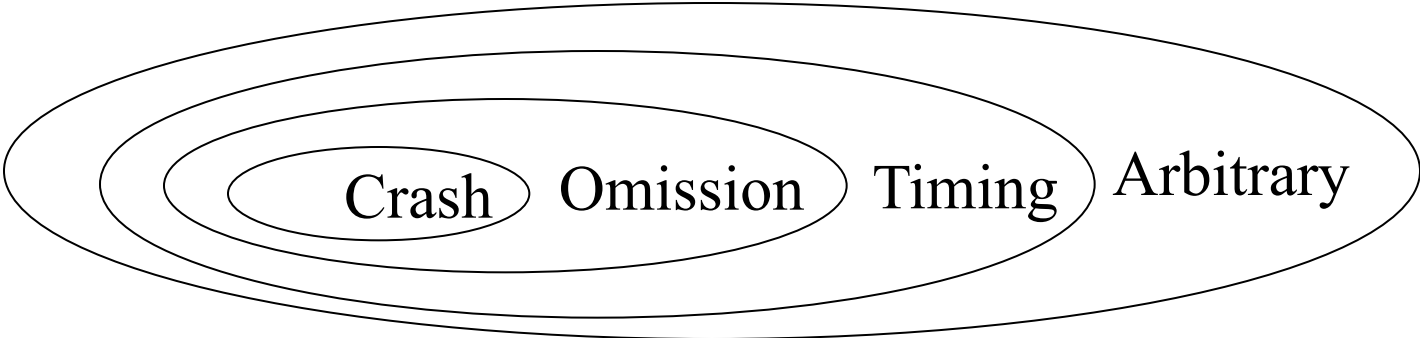
## Modelos de Avarias:

“Crash failures” - o componente deixa de funcionar

“Omission failures” - o componente não responde a alguns dos inputs (ex. perda de uma mensagem)

“Timing failures” - o tempo de resposta não corresponde ao esperado (o componente responde demasiado cedo ou demasiado tarde)

“Arbitrary failures” – o componente comporta-se de uma forma completamente arbitrária, não responde, responde no tempo indevido, responde com valores errados, ...



Entraves {  
Falha (*fault*)  
Erro (*error*)  
Avaria (*failure*)

Confiança

no funcionamento

Atributos

{  
Fiabilidade (*Reliability*)  
Disponibilidade (*Availability*)  
Segurança contra falhas acidentais (*Safety*)\*  
Confidencialidade (*Confidentiality*)  
Integridade (*Integrity*)  
Facilidade de Manutenção (*Maintainability*)

Segurança contra falhas intencionais (security): *Disponibilidade, Confidencialidade, Integridade*

Atributos da Confiança no Funcionamento:

Fiabilidade (*Reliability*)

Probabilidade de o sistema funcionar de acordo com as especificações, dentro de certas condições, durante um certo período de tempo.

Disponibilidade (*Availability*)

Probabilidade de o sistema estar operacional num dado instante de tempo.

*Um sistema pode ser de alta fiabilidade e ter baixa disponibilidade*

## Atributos da Confiança no Funcionamento:

### Fiabilidade versus Disponibilidade

#### **Sistemas baseados na Fiabilidade – Indústria da Aviação**

- pretende-se uma alta probabilidade de sucesso para um dado tempo de missão
- adequado quando as reparações são caras ou difíceis

#### **Sistemas baseados na Disponibilidade – Indústria Automóvel**

- grande percentagem de tempo em que o sistema cumpre as especificações
- adequado quando o funcionamento contínuo é importante

## Atributos da Confiança no Funcionamento:

### Segurança contra falhas acidentais (*Safety*)

- probabilidade de o sistema ou estar operacional executando as suas funções correctamente, ou parar as suas funções de forma a não provocar dano a outros sistemas ou pessoas que dele dependam.

### Confidencialidade (*Confidentiality*)

- inexistência de acessos não autorizados à informação

### Integridade (*Integrity*)

- inexistência de alterações incorrectas do estado do sistema

Atributos da Confiança no Funcionamento:

Facilidade de Manutenção (*Maintainability*)

- probabilidade de um sistema com avarias ser reparado continuando a funcionar

Medidas mais comuns para avaliar a confiabilidade de um sistema:

Taxa de Avarias – número de avarias esperado num dado intervalo de tempo

MTTF – (Mean Time To Failure) – tempo esperado até à primeira avaria

MTTR – (Mean Time To Repair) – tempo médio para reparação do sistema

MTBF – (Mean Time Between Failures) – tempo médio entre avarias do sistema

dificuldades práticas ...

Confiança

no funcionamento

Meios para obter

Prevenção de falhas (*fault prevention*)

Supressão de falhas (*fault removal*)

Tolerância a falhas (*fault tolerance*)

Previsão de falhas (*fault forecasting*)



Meios para obter sistemas confiáveis:

Prevenção de falhas – como evitar a ocorrência ou introdução de falhas  
*técnicas de controlo de qualidade no desenho e produção de hardware e software*

Supressão de falhas – como reduzir o número ou a gravidade das falhas  
*testes de verificação*

Tolerância a falhas – como produzir o serviço correcto na presença de falhas

Previsão de falhas – como estimar o número de falhas presente, a incidência futura e as prováveis consequências das falhas

*-> construção de um modelo das falhas passíveis de ocorrer*