Computação Distribuída

Odorico Machado Mendizabal

Universidade Federal de Santa Catarina – UFSC
Departamento de Informática e Estatística – INE

Confiabilidade de Sistemas

Motivação

- Falhas em sistemas simplesmente acontecem
  - Problemas durante o desenvolvimento do sistema
  - Sistemas mais complexos
  - Falhas físicas (HW ou fenômenos ambientais)
  - Falhas ocasionadas por atuação dos usuários

Atualmente: Hardware mais robusto, software mais complexo, sistemas de larga escala, com maiores chances de algum componente falhar

- Os custos de uma falha variam dependendo do quão crítico o sistemas é
  - Insatisfação, Custos financeiros, Risco à vida humana

Exemplo: Ariane – 5

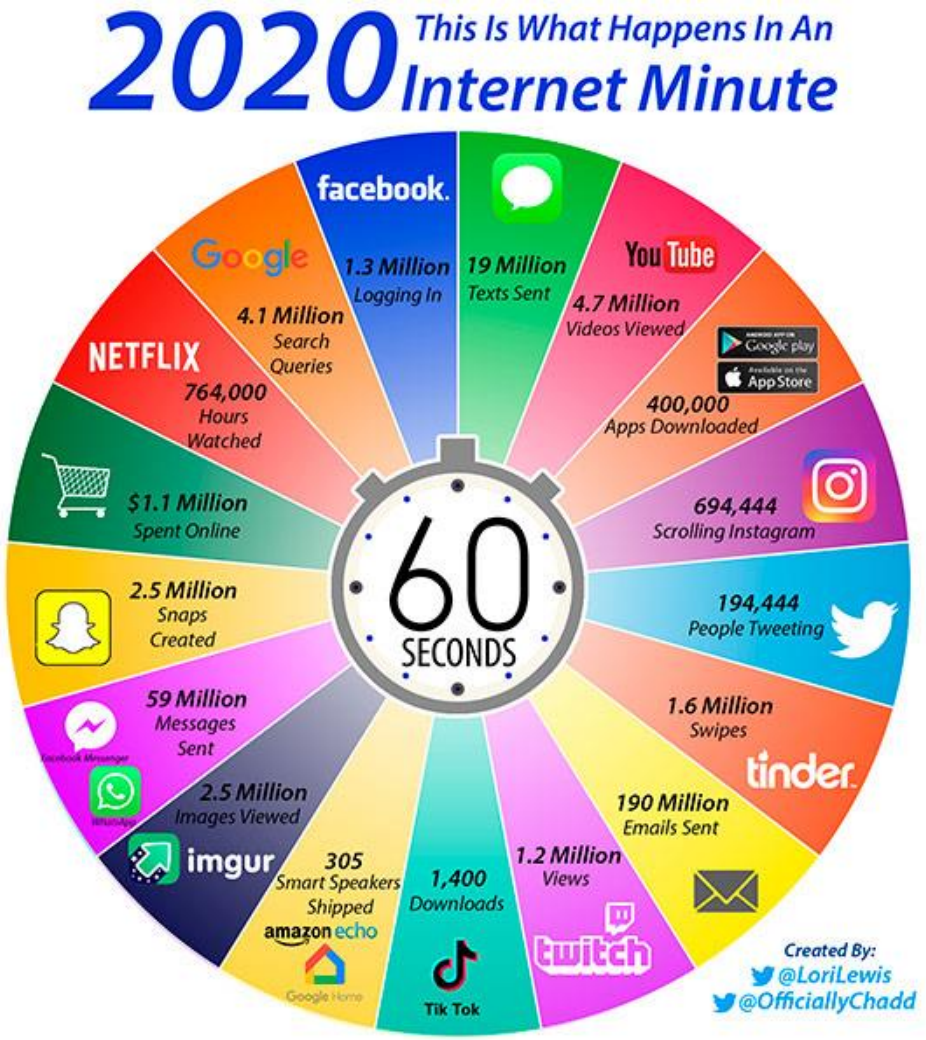
- Ariane 5 e sua carga foram destruídos 37 segundos após levantar voo
- Erro causado por uma falha de software:
  - Conversão de número em ponto flutuante para inteiro de 16 bits
  - Conversão gerou uma exceção que não foi tratada
- Custo do Projeto: US$ 7B
- Custo da Carga: US$ 500M

Exemplo: Sistemas na Internet

Sistemas de larga escala e alta vazão

- Confiabilidade no funcionamento

Falhas e indisponibilidade do serviço podem levar a prejuízo ou danos irreparáveis



Fonte: https://www.allaccess.com/merge/archive/31294/infographic-what-happens-in-an-internet-minute

Conceitos Básicos sobre *Confiança no Funcionamento*

É necessário entender os elementos relacionados à confiança no funcionamento de sistemas

Confiança no Funcionamento (*dependability*)

- **Ameaças**
  - **Falhas**
  - **Erros**
  - **Defeitos**
- **Atributos**
  - **Confiança**
  - **Disponibilidade**
  - **Segurança (*Safety*)**
  - **Manutenibilidade**
  - **...**
- **Medidas Adotadas**
  - **Prevenção de Falhas**
  - **Tolerância a Falhas**
  - **Remoção de Falhas**
  - **Previsão de Falhas**

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004 11

Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avižienis, *Fellow, IEEE*, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, *Senior Mem*

Abstract—This paper gives the main definitions as reliability, availability, safety and integrity.

Motivação

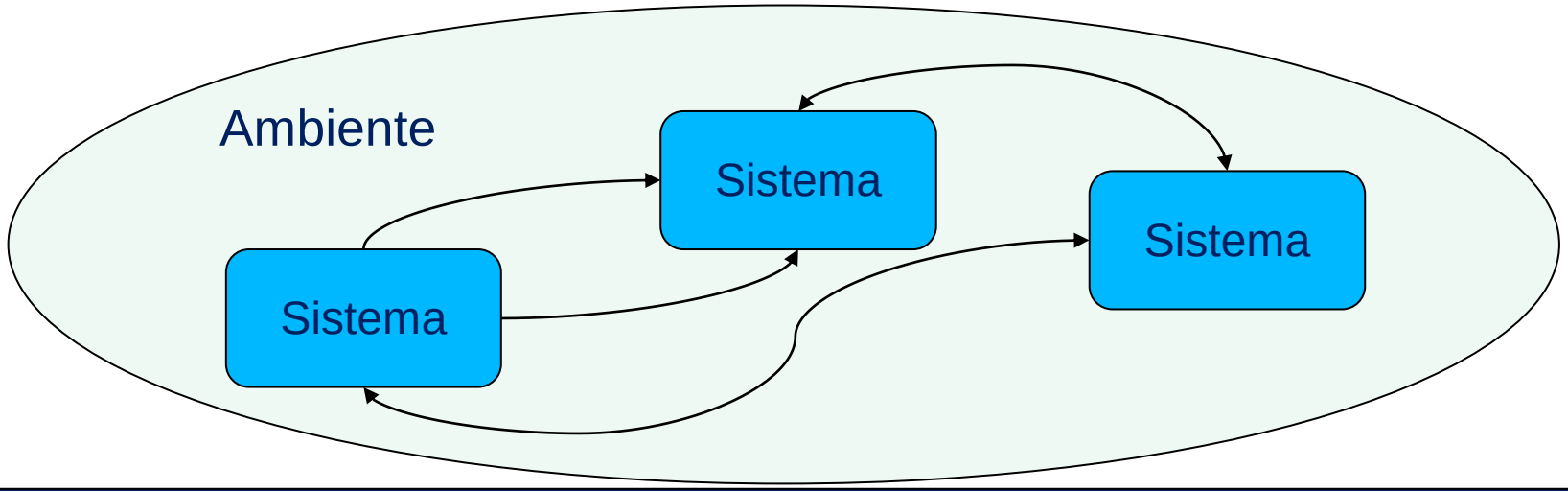
Estamos interessados em entender o que são as falhas, quais atributos de um sistema são afetados por elas e como desenvolver sistemas tolerantes a falhas

- Sistemas Tolerantes a Falhas
  - Na presença de falhas, permitem que o sistema comporte-se de maneira aceitável
  - Em sistemas críticos, serviços tolerantes a falhas são cruciais

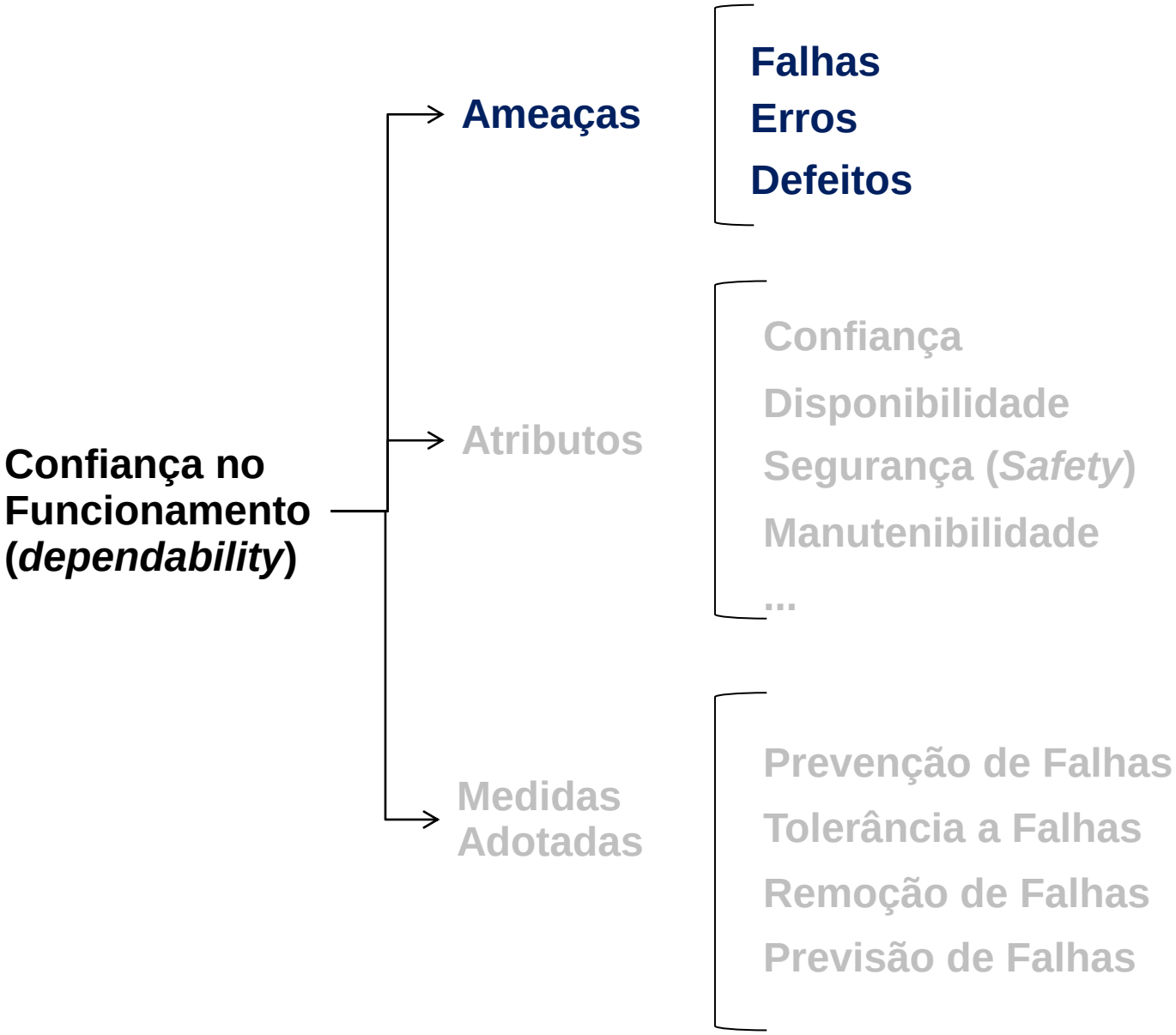
Conceitos Básicos – Sistemas

Sistemas

- Entidade que implementa uma determinada função e interage com outras entidades
  - Outros sistemas (dispositivo de HW, Software, Humano, atuadores ou sensores – mundo físico, etc.)
- A composição de sistemas que interagem entre si estabelece um ambiente
- Limite do Sistema
  - Fronteira entre um sistema e o ambiente



Conceitos Básicos – Ameaças



Conceitos Básicos – Falha, Erro, Defeito

- Falha (*fault*)
  - Causa raiz do efeito anômalo que poderá ser observado (mas talvez não chegue a ser observado)

- Erro (*error*)
  - Erro é um estado errôneo, cujo próximo estado pode revelar um defeito

- Defeito (*failure*)
  - É o desvio do comportamento esperado

Falha ⟶ Erro ⟶ Defeito

Alguns autores adotam outra nomenclatura:

Falta ⟶ Erro ⟶ Falha

Confiança no Funcionamento: Proposta para uma Terminologia em Português. Veríssimo, P.; Lemos R. INESC Technical Report (RT/48-89)

Conceitos Básicos – Falha, Erro, Defeito – Exemplo

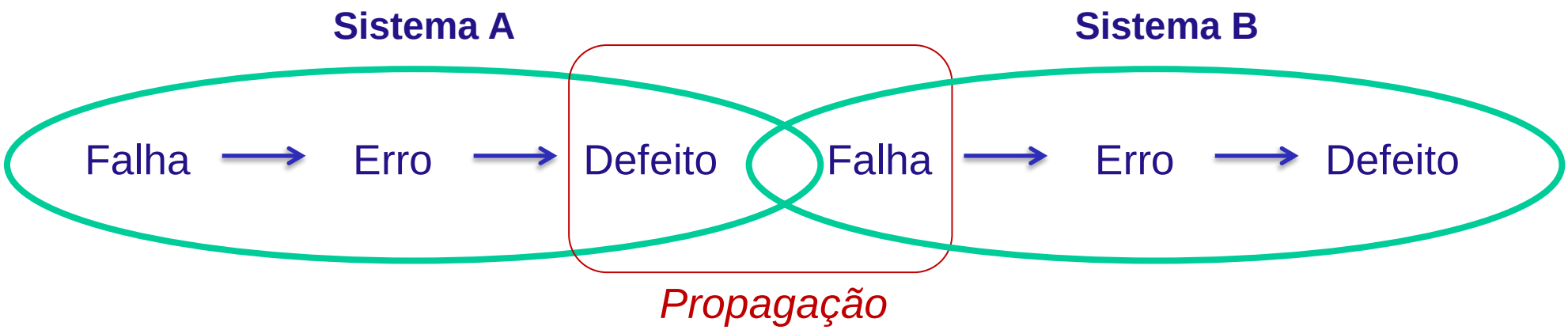
- Falha
  - Bit 3 de uma célula de memória está avariado (*stuck at 0*). Ele sempre marca 0, independente do que for escrito nesta posição

- Erro
  - Um valor do programa é armazenado na célula comprometida
    - Se o valor armazenado no bit for 0, não ocorrerá um defeito
    - Se o valor for 1, mas o dado nunca for acessado, também não será percebido o defeito
    - Se o valor for 1 e o dado for acessado, ocorrerá um defeito

- Defeito
  - É o desvio do comportamento esperado, por exemplo, uma instrução inválida, pois não foi possível decodificar a instrução com valor 1 no bit 3

Conceitos Básicos – Falha, Erro, Defeito

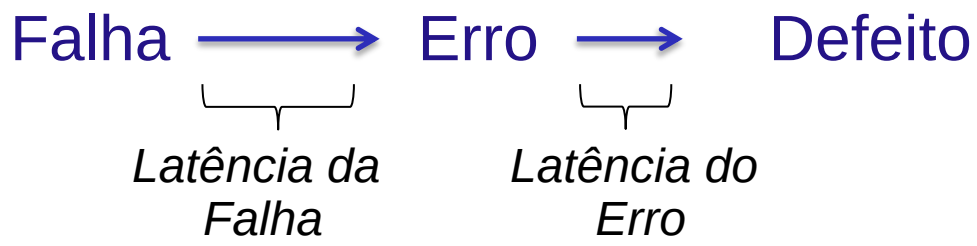
- Propagação de defeitos
  - Em um ambiente, o defeito em um sistema pode ocasionar a falha de outro



Conceitos Básicos – Falha, Erro, Defeito

- Latência da Falha: tempo em que uma falha permanece dormente, até que ela se manifeste (causando um erro)

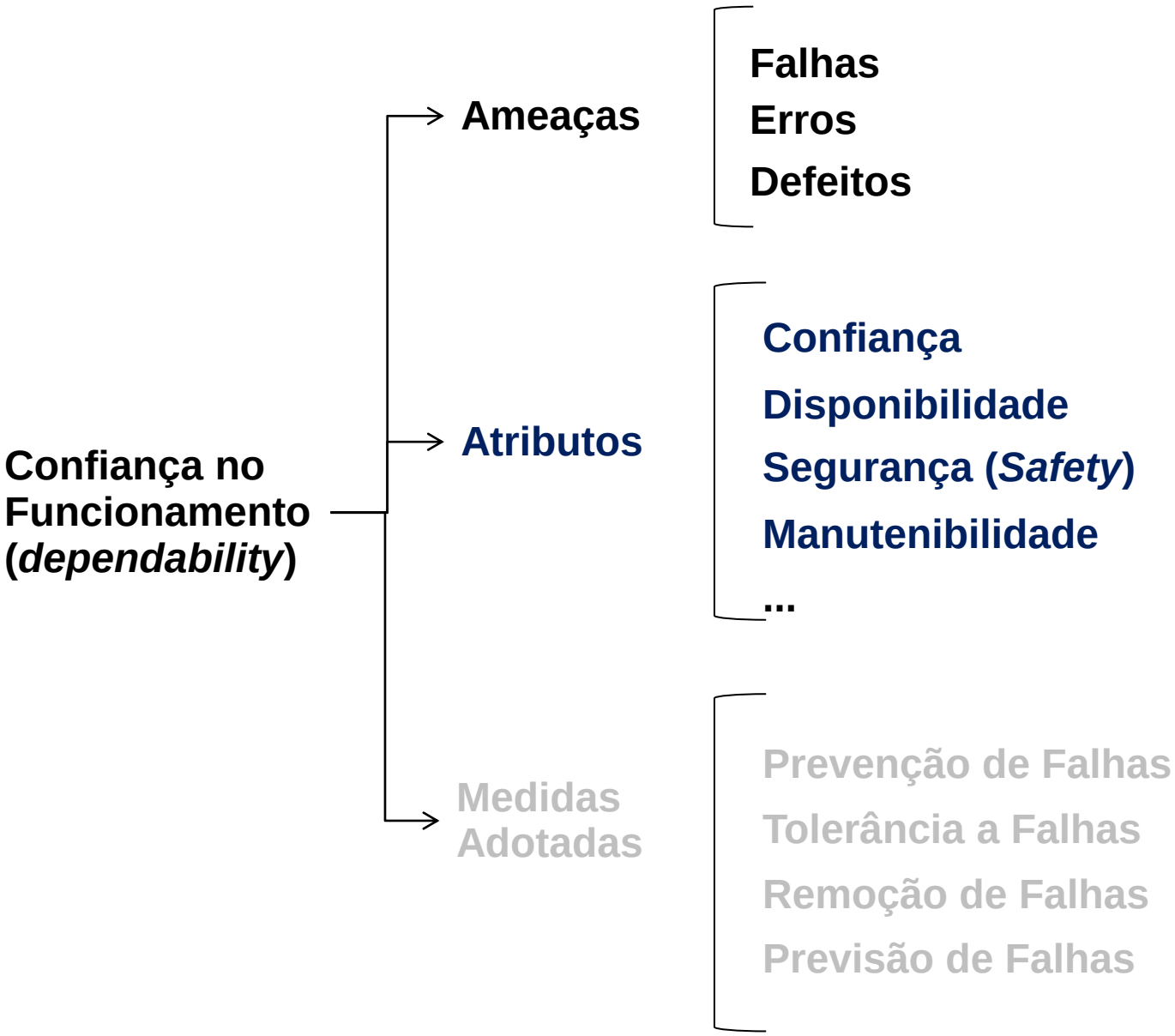
- Latência do Erro: tempo em que um erro permanece dormente, até que ele se manifeste (causando um defeito)



Além disso, as falhas podem ser:

- Transientes
- Intermitentes
- Permanentes

Conceitos Básicos – Atributos



Conceitos Básicos – Atributos e Medidas

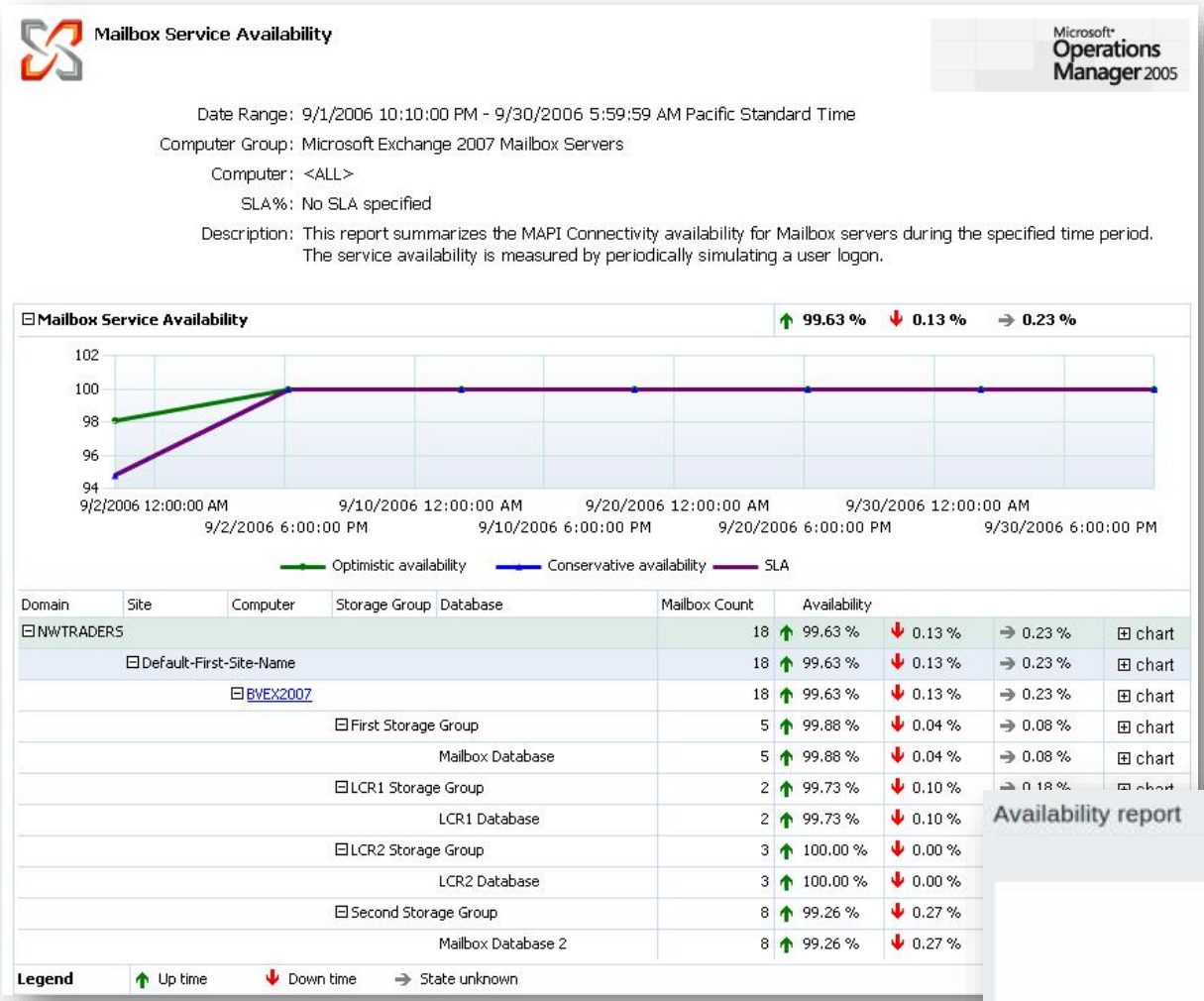
- Disponibilidade (*Availability*)
  - Sistema estar pronto para o uso imediato
    - % de tempo de funcionamento

- Confiabilidade (*Reliability*)
  - Capacidade de manter o sistema em funcionamento correto
    - Tempo de funcionamento ininterrupto

- Segurança “contra falhas acidentais” (*Safety*)
  - Ausência de efeitos catastróficos sobre o ambiente ou o desvio do comportamento correto

- Capacidade de Manutenção
  - Facilidade com que um sistema que falhou pode ser consertado

Exemplo de Disponibilidade – Relatórios de Disponibilidade



Mailbox Service Availability

Microsoft Operations Manager 2005

Date Range: 9/1/2006 10:10:00 PM - 9/30/2006 5:59:59 AM Pacific Standard Time
Computer Group: Microsoft Exchange 2007 Mailbox Servers
Computer: <ALL>
SLA%: No SLA specified
Description: This report summarizes the MAPI Connectivity availability for Mailbox servers during the specified time period. The service availability is measured by periodically simulating a user logon.

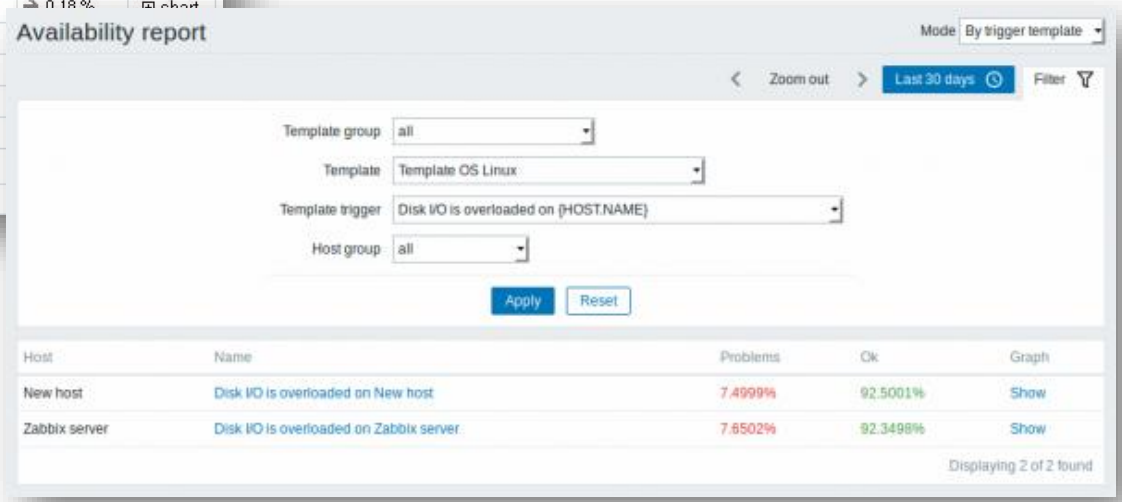
Mailbox Service Availability — 99.63 % — 0.13 % — 0.23 %

102
100
98
96
94
9/2/2006 12:00:00 AM
9/2/2006 6:00:00 PM
9/10/2006 12:00:00 AM
9/10/2006 6:00:00 PM
9/20/2006 12:00:00 AM
9/20/2006 6:00:00 PM
9/30/2006 12:00:00 AM
9/30/2006 6:00:00 PM

Optimistic availability — Conservative availability — SLA

Domain	Site	Computer	Storage Group	Database	Mailbox Count	Availability			
NWTRADERS					18	99.63 %	0.13 %	0.23 %	chart
	Default-First-Site-Name				18	99.63 %	0.13 %	0.23 %	chart
		BVEX2007			18	99.63 %	0.13 %	0.23 %	chart
			First Storage Group		5	99.88 %	0.04 %	0.08 %	chart
				Mailbox Database	5	99.88 %	0.04 %	0.08 %	chart
			LCR1 Storage Group		2	99.73 %	0.10 %		
				LCR1 Database	2	99.73 %	0.10 %		
			LCR2 Storage Group		3	100.00 %	0.00 %		
				LCR2 Database	3	100.00 %	0.00 %		
			Second Storage Group		8	99.26 %	0.27 %		
				Mailbox Database 2	8	99.26 %	0.27 %		

Legend: Up time — Down time — State unknown



Availability report

Mode: By trigger template
Zoom out — Last 30 days — Filter

Template group: all
Template: Template OS Linux
Template trigger: Disk I/O is overloaded on {HOST.NAME}
Host group: all

Apply — Reset

Host	Name	Problems	Ok	Graph
New host	Disk I/O is overloaded on New host	7.4999%	92.5001%	Show
Zabbix server	Disk I/O is overloaded on Zabbix server	7.6502%	92.3498%	Show

Displaying 2 of 2 found

Microsoft Operations Manager

Zabbix

…

Conceitos Básicos – Atributos e Medidas

- Disponibilidade vs. Confiabilidade

Sistema A:
- Fica inoperante 1 segundo a cada hora

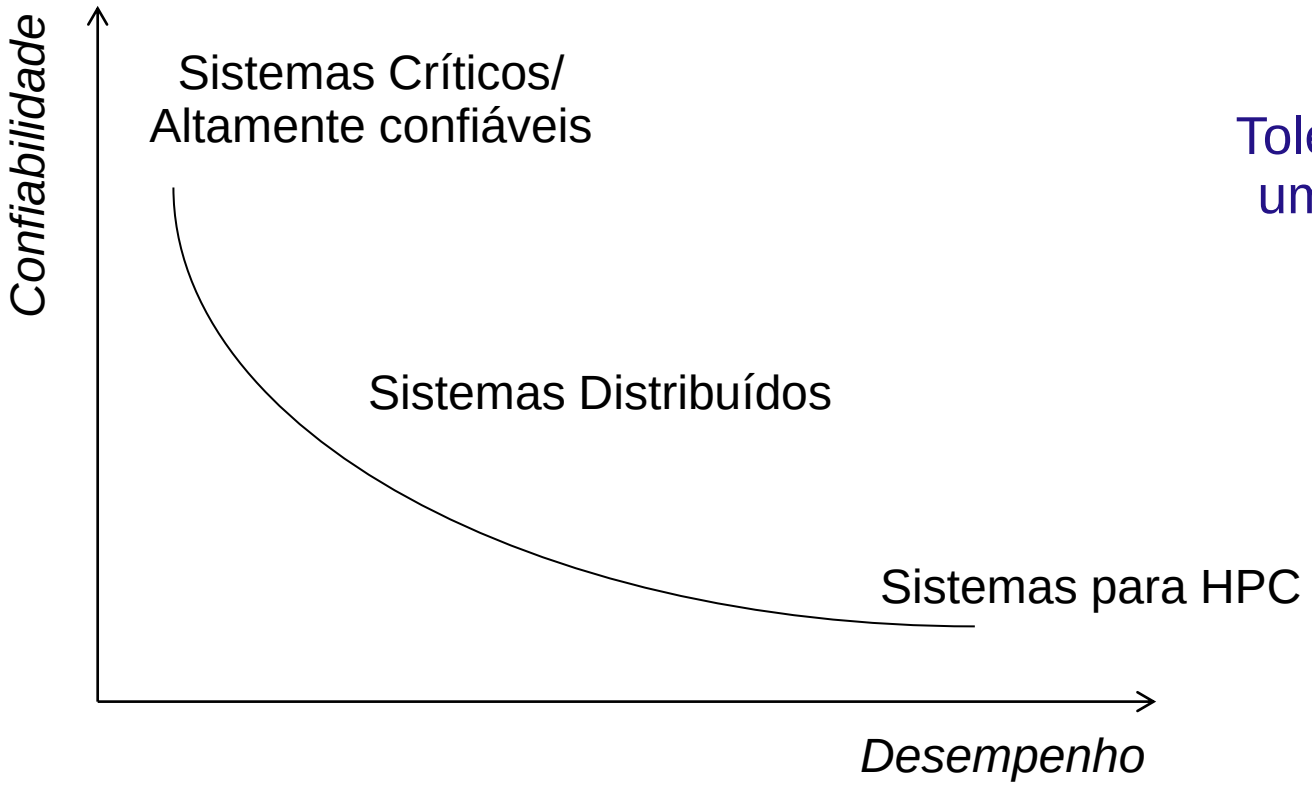
Disponibilidade (mês): Alta (99.9999%)
Confiabilidade (mês): Baixa

Sistema B:
-Nunca cai, mas é desligado por 2 horas diárias durante todo o mês de agosto

Disponibilidade (mês): Baixa (96%)
Confiabilidade (mês): Alta

Conceitos Básicos – Atributos e Medidas

- Desempenho vs. Confiabilidade

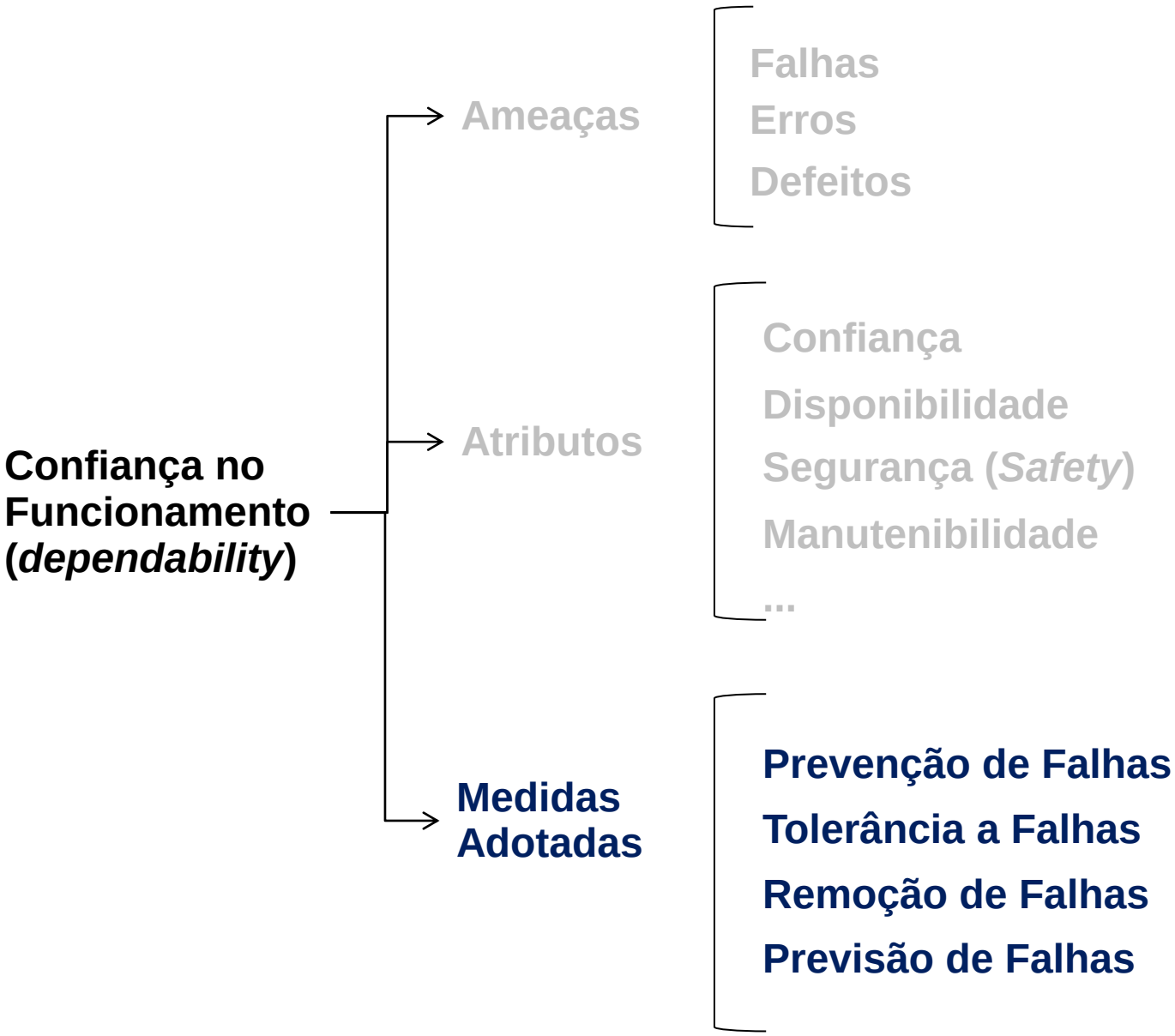


Tolerância a falhas adiciona um custo no desempenho geral do sistema

Conceitos Básicos – Atributos e Medidas

- Segurança: *Safety* vs. *Security*
  - *Safety:* Segurança contra falhas acidentais
    - O sistema garante propriedades relacionadas ao funcionamento correto do sistema
    - Comportamentos indesejados não ocorrem
  - *Security:* Segurança contra falhas intencionais
    - Relacionado as propriedades de integridade e confidencialidade

Conceitos Básicos – Atributos



Conceitos Básicos – Medidas Adotadas

- Prevenção de Falhas
  - Prevenir que falhas acontecem
    - Teste de software, revisão de projeto, métodos de desenvolvimento que favorecem a testabilidade, etc.

- Tolerância a Falhas
  - Evitar a ocorrência de defeitos nos serviços mesmo na presença de falhas

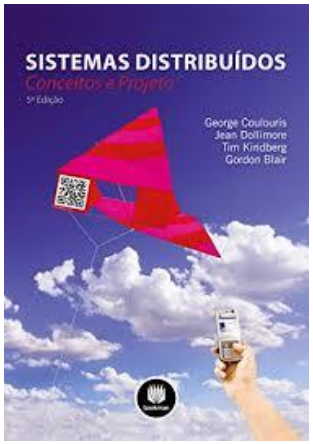
- Remoção de Falhas
  - Reduzir o número de falhas
    - Reconfiguração do sistema, substituição de componentes, etc.

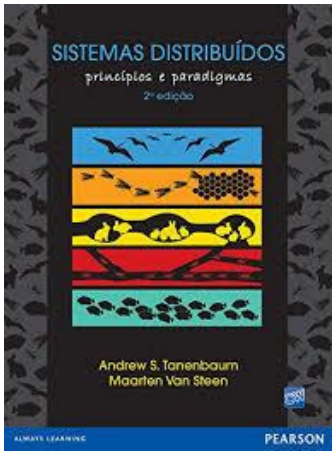
- Previsão de Falhas
  - Estimar a incidência de falhas futuras e as prováveis consequências das falhas

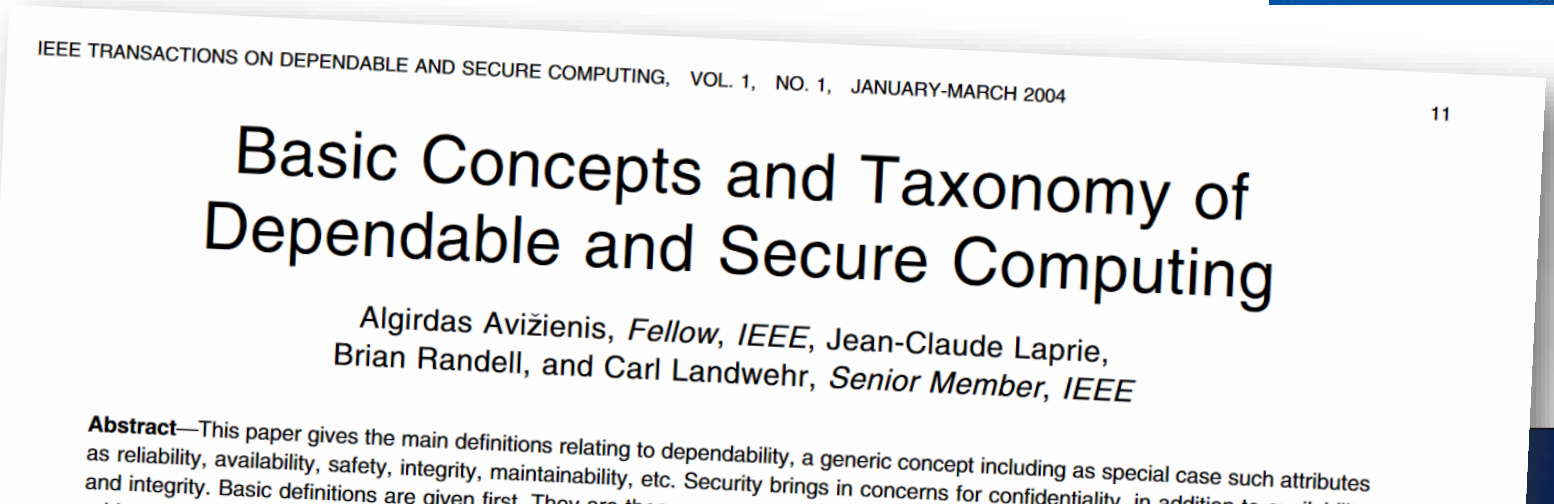
Referências

Parte destes slides são baseadas em material de aula dos livros:

- *Coulouris, George; Dollimore, Jean; Kindberg, Tim; Blair, Gordon. Sistemas Distribuídos: Conceitos e Projetos. Bookman; 5ª edição. 2013.*
- *Tanenbaum, Andrew S.; Van Steen, Maarten. Sistemas Distribuídos: Princípios e Paradigmas. 2007. Pearson Universidades; 2ª edição.*






IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004 11

Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avižienis, *Fellow, IEEE*, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, *Senior Member, IEEE*

Abstract—This paper gives the main definitions relating to dependability, a generic concept including as special case such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to