Tolerância a Falhas: medidas

Taisy Silva Weber

Medidas

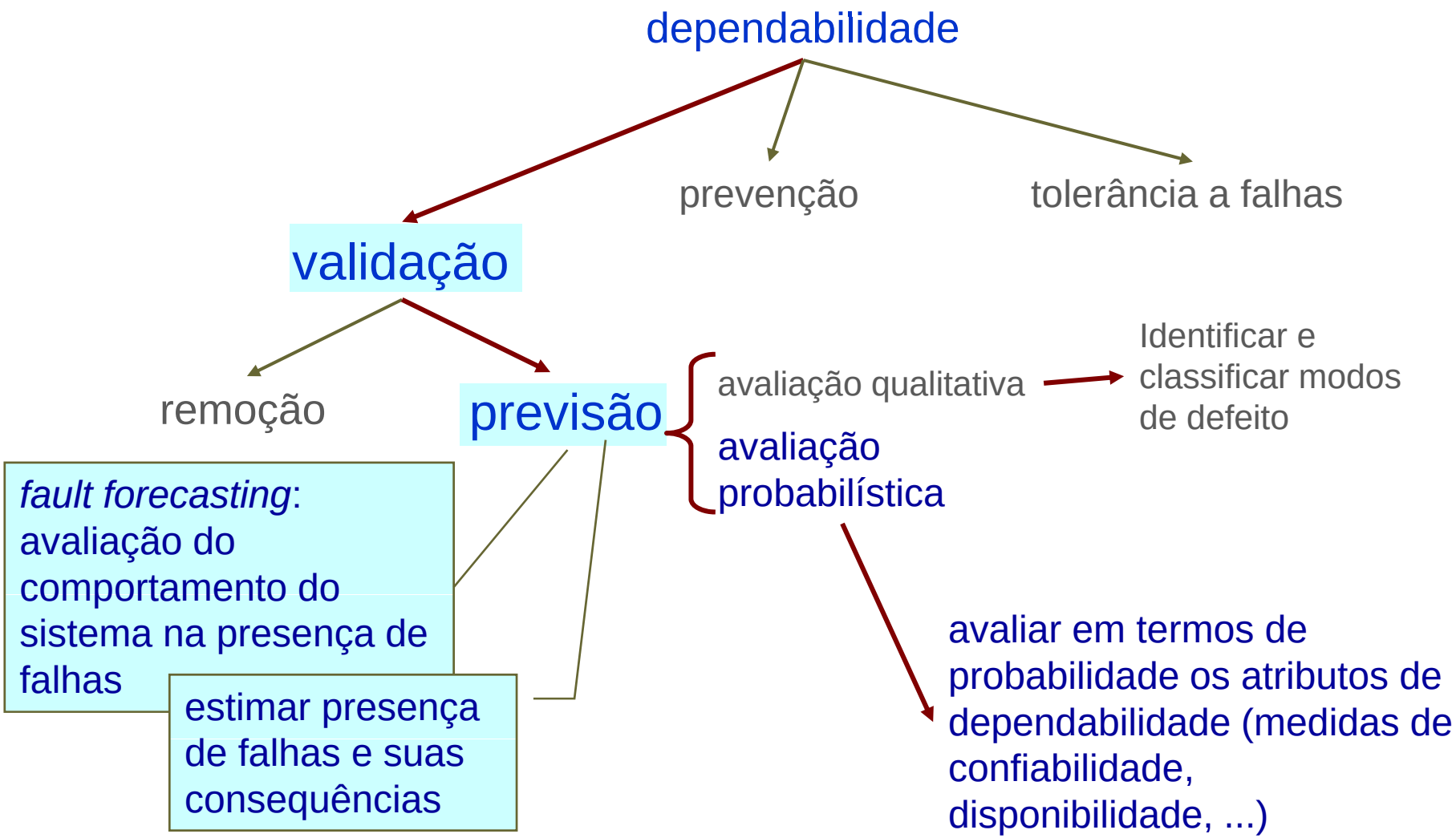
- taxa de defeitos
- curva da banheira
- tempos médios *(mean times)*
  - MTTF, MTBF, MTTR
  - exemplos de cálculo de tempos médios
- confiabilidade
- disponibilidade
- cobertura

Barry W. Johnson. **Design and Analysis of Fault-Tolerant Digital Systems**. Addison-Wesley, 1989 (**cap 4**)

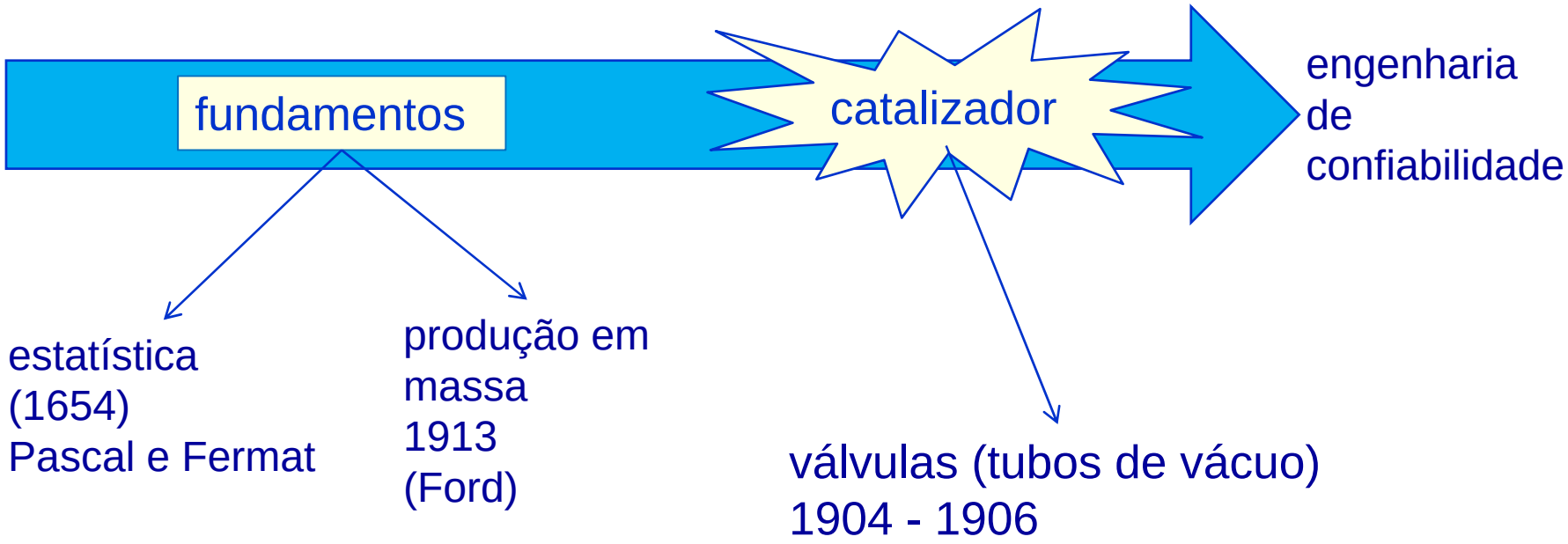
Johnson, B.W. "**Fault Tolerance**"
The Electrical Engineering Handbook
Ed. Richard C. Dorf
Boca Raton: CRC Press LLC, 2000

Barry Johnson,
cap. 1, livro-texto Pradhan96

Meios: previsão



Reliability engineering



J.H. Saleh, K. Marais. Highlights from the early (and pre-) history of reliability engineering. Reliability Engineering and System Safety 91 (2006) 249–256

Reliability engineering

- Walter Shewhart
  - década de 20 – métodos estatísticos para o controle de qualidade na produção
    - métodos não foram bem recebidos
- segunda guerra
  - acelerou a adoção de técnicas estatísticas de controle de qualidade
- Edward Deming
  - década de 50
    - não teve muito sucesso nos USA
    - se mudou para o Japão e teve enorme sucesso

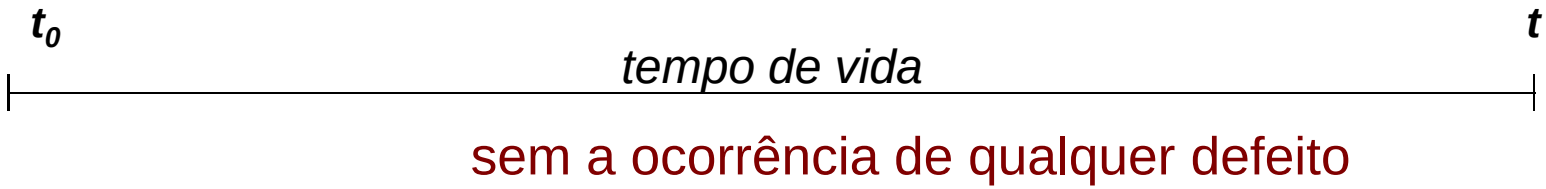
Reliability engineering

- data oficial de nascimento: 4 junho de 1954
  - relatório AGREE
    - Advisory Group on Reliability of Electronic Equipment (AGREE),
  - 1952
    - department of defense
    - industria eletrônica americana
- previsão de falhas (ou de defeitos de componentes)
    - falhas permanentes (randômicas)
    - medidas para software - problema ainda em aberto

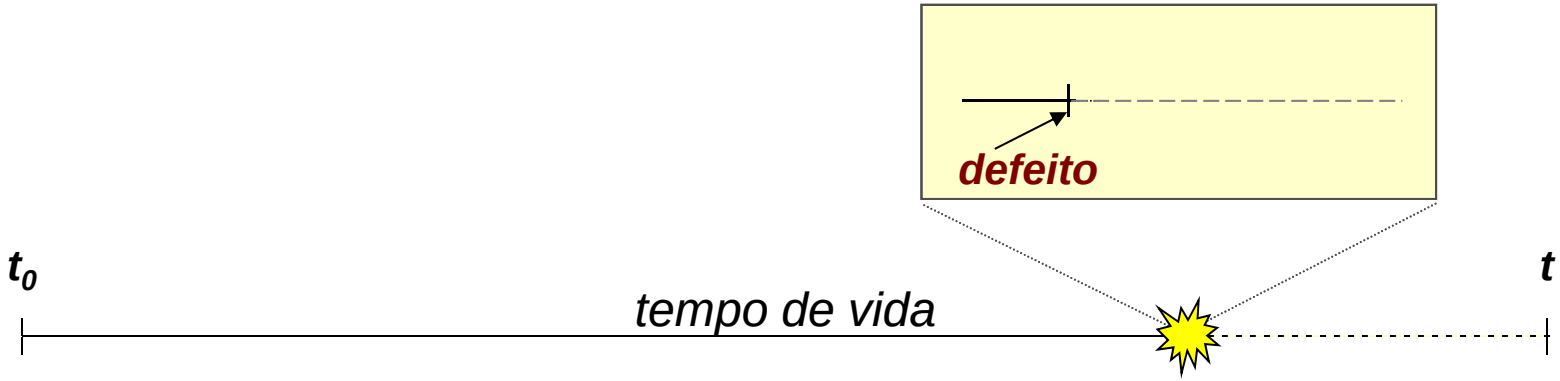
problemas com válvulas
(em uso até o final dos 60s)

Comportamento ideal *x* real

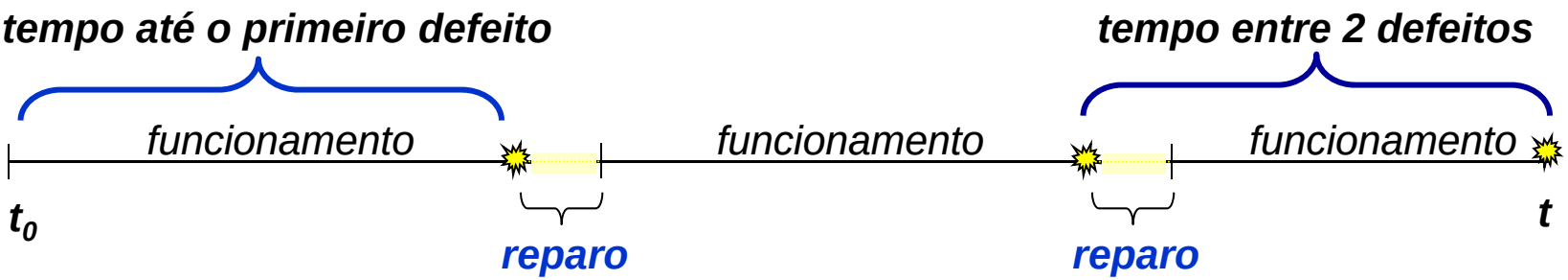
- ideal



- real



O que medir?



- com que frequência ocorrem defeitos?
- qual o tempo entre um defeito e outro?
- qual o tempo até o primeiro defeito?
- qual o tempo gasto para reparar cada defeito?
- quais as chances do sistema funcionar sem defeitos durante um determinado período de tempo?
- quais as chances do sistema estar funcionando em um determinado instante?

Taxa de defeitos

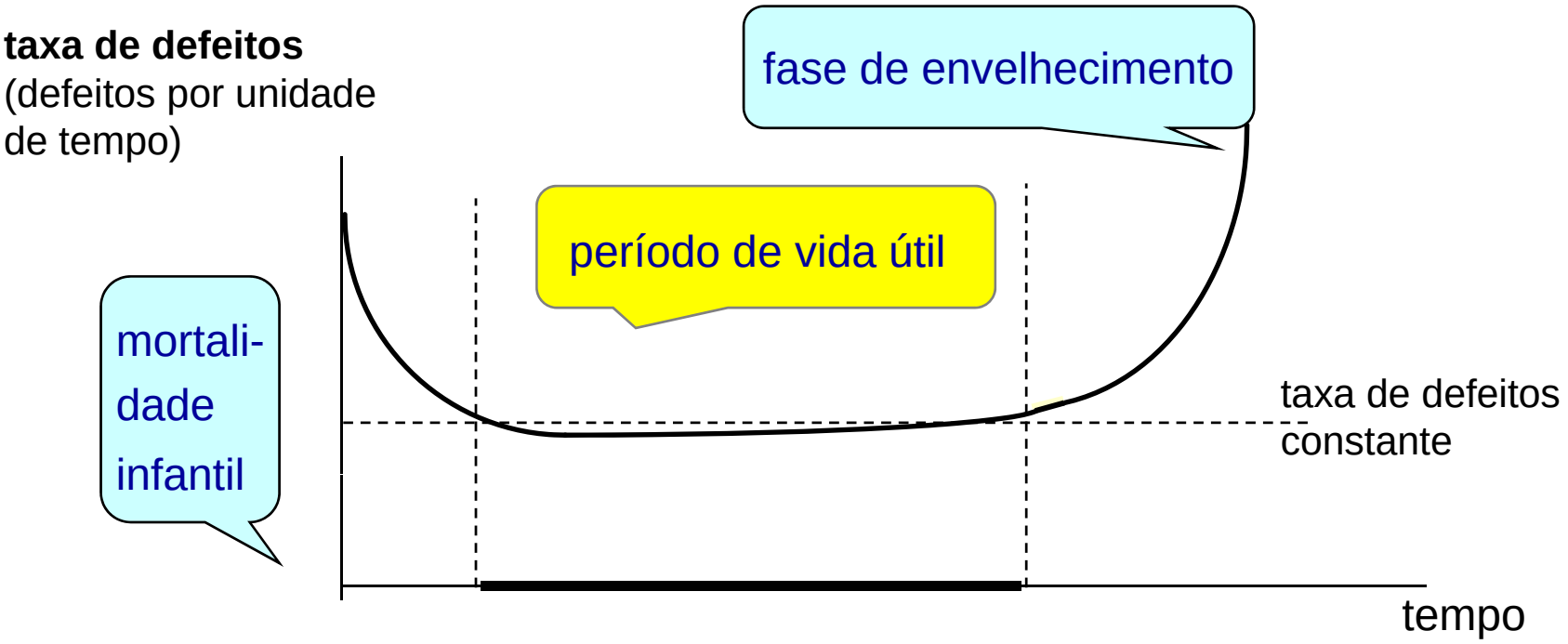
- com que frequência ocorrem defeitos?
  - taxa de defeitos
    - geralmente assumido valor constante
    - na verdade não é constante
    - boa aproximação: curva da banheira
  - unidade: defeitos por unidade de tempo
  - função:
    - z(t) - hazard function, hazard rate ou taxa de defeitos (failure rate)

número esperado de defeitos em um dado período de tempo (*failure rate)*

Exemplo: um computador apresenta defeito a cada 2000 horas, qual a taxa de defeito?

Curva da banheira

fases de mortalidade infantil e envelhecimento muito pequenas comparadas ao período de vida útil



válido para hardware (componentes eletrônicos)

Mortalidade infantil

- alta taxa de defeitos que diminui rapidamente no tempo
  - componentes fracos e mal fabricados

mortalidade infantil é uma fase de curto período de duração

- burn-in: remoção de componentes fracos
  - operação acelerada de componentes antes de colocá-los no produto final
  - só entram em operação componentes que sobreviveram à mortalidade infantil

Envelhecimento

- taxa de defeitos aumenta rapidamente com o tempo
  - devido ao desgaste físico do componente
  - conhecendo o início da fase de envelhecimento é possível substituir o componente
    - sistema volta a operar na fase de vida útil

envelhecimento é também uma fase de curto período de duração

ideal é evitá-la

Tempo de vida útil

- λ – taxa de defeitos **constante**
  - unidade: defeitos por hora

    λ corresponde a taxa de defeitos no tempo de vida útil
    - essa fase apresenta um serviço mais previsível em relação a falhas
- relação exponencial entre confiabilidade e tempo
  - usa λ – taxa de defeitos constante
  - válido para hardware
    - será visto mais adiante

$$R(t) = e^{-\lambda t}$$

Curva da banheira em software

- software comporta-se diferente do hardware
  - erros (bugs) são constantemente removidos
    - taxa de defeitos continua caindo com o tempo
    - confiabilidade aumenta com o tempo ?

considerar alterações, adaptações ou mudança de plataforma (sisop e hardware)

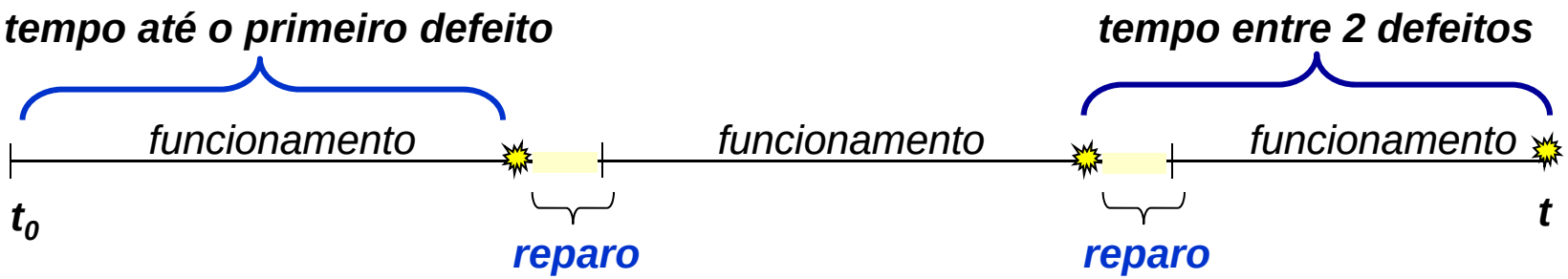
  - fase de envelhecimento de software ?
    - obsolescência dos programas
    - alterações nas plataformas
    - *aging*

Exemplos de taxa de defeitos

categoria	**módulo**	**taxa de defeitos**
CPU	processador	$19{,}0 \times 10^{-6}$ /hrs
	memória	$13{,}0 \times 10^{-6}$ /hrs
saída	relé	$9{,}2 \times 10^{-6}$ /hrs
	triac	$33{,}8 \times 10^{-6}$ /hrs
entrada	conversor A/D	$10{,}4 \times 10^{-6}$ /hrs
comunicações	controlador de barramento	$19{,}8 \times 10^{-6}$ /hrs
outros	fonte	$33{,}0 \times 10^{-6}$ /hrs
	rack	$2{,}6 \times 10^{-6}$ /hrs

fator de incerteza = 10

Tempos médios



- com que frequência ocorrem defeitos?
- qual o tempo entre um defeito e outro?
- qual o tempo até o primeiro defeito?
- qual o tempo gasto para reparar cada defeito?
- quais as chances do sistema funcionar sem defeitos durante um determinado período de tempo?
- quais as chances do sistema estar funcionando em um determinado instante?

taxa de defeitos

Medidas

- MTTF
  - tempo esperado até a primeira ocorrência de defeito

mean time to failure

- MTTR
  - tempo médio para reparo do sistema

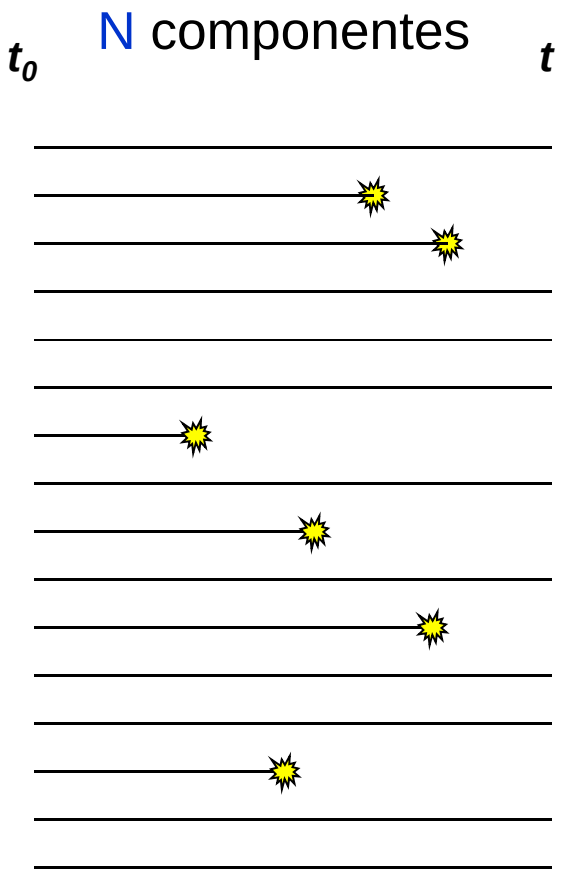
mean time to repair

- MTBF
  - tempo médio entre defeitos do sistema

mean time between failures

MTTF - mean time to failure

- tempo esperado de operação do sistema antes da ocorrência do primeiro defeito
  - considera-se N sistemas idênticos colocados em operação a partir do tempo t=0
  - mede-se o tempo de operação ti de cada um até apresentar defeito
  - MTTF é o tempo médio de operação



MTTF - mean time to failure

- tempo esperado de operação do sistema antes da ocorrência do primeiro defeito

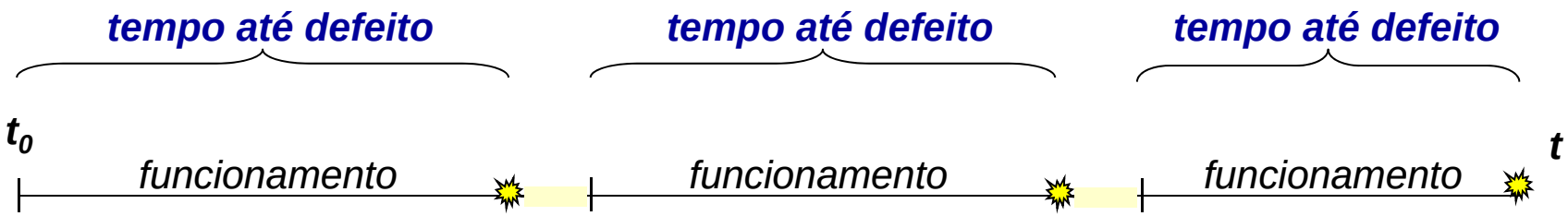
$$MTTF = \sum_{i=1}^{N} \frac{t_i}{N}$$

quanto maior a quantidade de amostras **N**, mais próximo do valor real será o **MTTF** estimado

considerando **R(t) = e $^{-\lambda t}$**

MTTF = $1/\lambda$

MTTF



$$MTTF = \sum_{i=1}^{N} \frac{t_i}{N}$$

para **um** único sistema o procedimento é semelhante:

t_i passa a ser Δt_i , o intervalo de tempo em operação entre os defeitos, e *N* o número de defeitos

MTTR - mean time to repair

- tempo médio de reparo do sistema
  - difícil de estimar
    - geralmente usa-se **injeção de falhas**
    - injeta-se uma falha de cada vez e mede-se o tempo
  - nova constante μ
    - taxa de reparos

      μ = número de reparos por hora

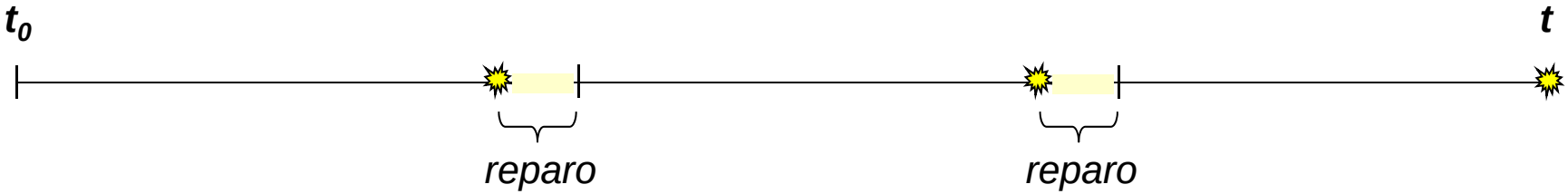
$$MTTR = \frac{1}{\mu}$$

em sistemas de **alta disponibilidade**, é importante diminuir o **tempo de reparo** para aumentar a disponibilidade do sistema

MTTR

R_i tempo de reparo da falha *i*

n número de falhas



$$MTTR = \sum_{i=1}^{n} R_i/n \quad \text{ou} \quad MTTR = 1/\mu$$ sendo μ = taxa de reparo

quanto maior o número de amostras, melhor

MTTR: Exemplo

grandemente simplificado

tempo de reparo do 1º defeito (R_1) = 0,5 h
tempo de reparo do 2º defeito (R_2) = 1 h

MTTR = (R_1+ R_2) / nº reparos
MTTR = 1,5 / 2

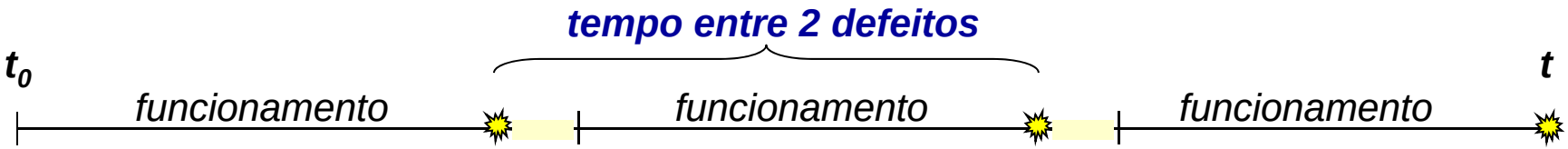
MTTR = 0,75 h

Mean Time Between Failure

- MTBF = MTTF + MTTR
  - diferença numérica pequena em relação a MTTF
    - os tempos de operação são geralmente muito maiores que os tempos de reparo
    - na prática valores numéricos muito aproximados (não faz diferença usar um ou outro)
  - considera-se:
    - reparo coloca sistema em condições ideais de operação

e se o MTBF for maior que o tempo até obsolescência?

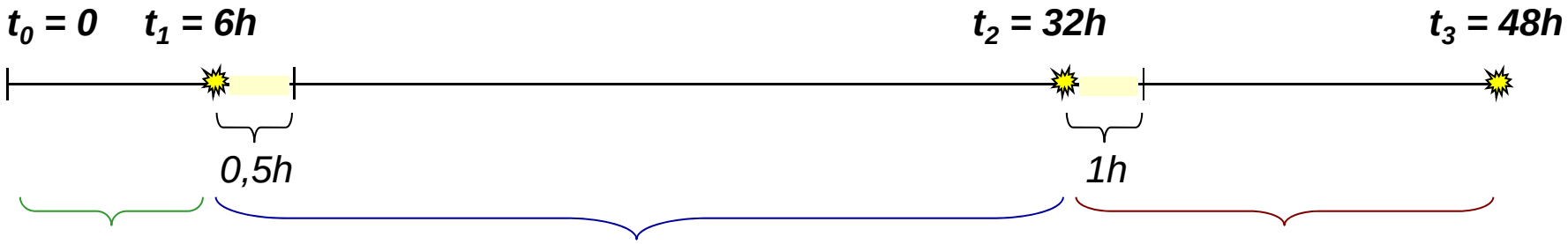
MTBF



$$MTBF = \sum_{i=1}^{n} \Delta d_i / n \quad \text{ou} \quad MTBF = MTTF + MTTR$$

MTBF: Exemplo

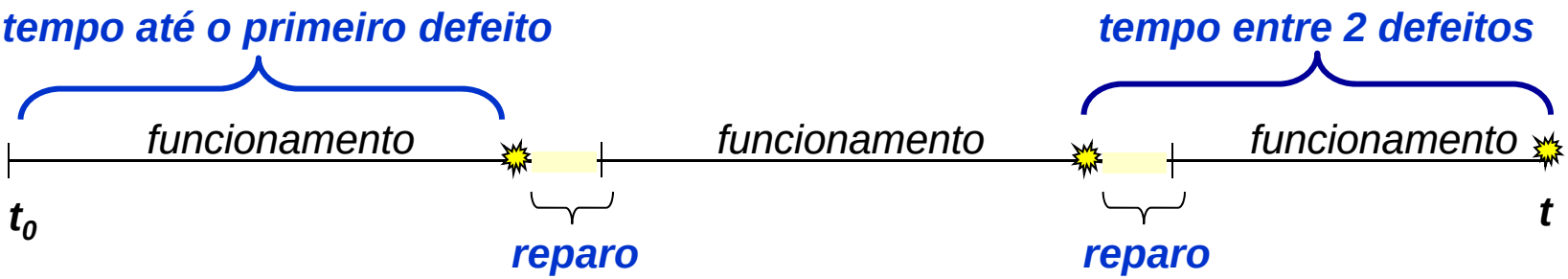
grandemente simplificado



tempo entre o início e o 1º defeito (Δd_1) = 6 h
tempo entre 1º e 2º defeitos (Δd_2) = 26 h
tempo entre 2º e 3º defeitos (Δd_3) = 16h

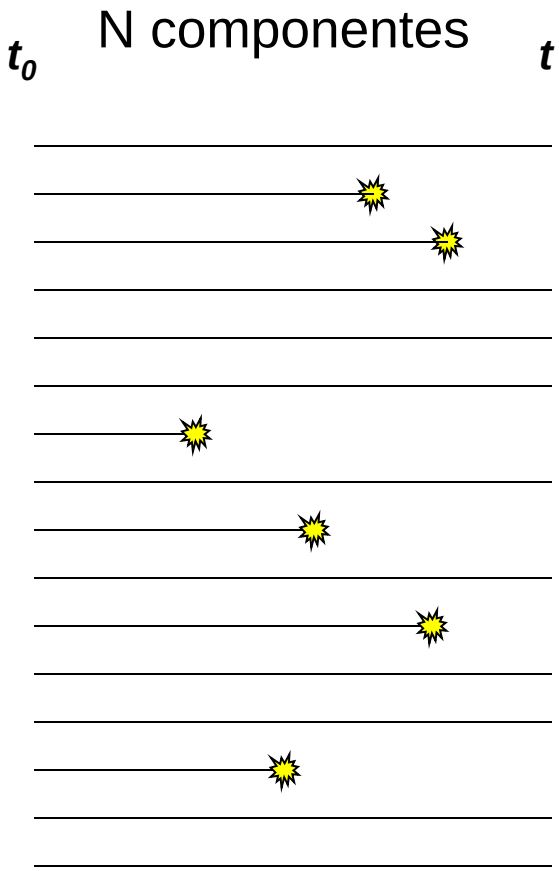
MTBF = ($\Delta d_1 + \Delta d_2 + \Delta d_3$)/nº defeitos
MTBF = 48 / 3
MTBF = 16 h

Demais medidas



- com que frequência ocorrem defeitos? taxa de defeitos
- qual o tempo entre um defeito e outro? MTBF
- qual o tempo até o primeiro defeito? MTTF
- qual o tempo gasto para reparar cada defeito? MTTR
- quais as chances do sistema funcionar sem defeitos durante um determinado período de tempo?
- quais as chances do sistema estar funcionando em um determinado instante?

Confiabilidade e taxa de defeitos



N componentes idênticos, operacionais em t_0

$N_f(t)$ número de componentes com defeito em t

$N_o(t)$ núm. de componentes operacionais em t

$$R(t) = N_o(t) / N = N_o(t) / (N_o(t) + N_f(t))$$

confiabilidade: a probabilidade que um componente tenha sobrevivido no intervalo

Q(t) é a não confiabilidade

$$Q(t) = N_f(t) / N = N_f(t) / (N_o(t) + N_f(t))$$

$$R(t) = 1{,}0 - Q(t) = 1 - N_f(t) / N$$

Confiabilidade e taxa de defeitos

$R(t) = 1,0 - Q(t) = 1 - N_f(t) / N$

fazendo a diferencial da confiabilidade em relação ao tempo

$dR(t)/dt = (- 1/N)\ dN_f(t) / dt$

$dN_f(t) / dt$ é a taxa instantânea em que componentes estão falhando.

$dN_f(t) / dt = (- N)\ dR(t) / dt$

Dividindo esta taxa por $No(t)$

Confiabilidade e taxa de defeitos

$dN_f(t)/dt = (-N)\, dR(t)/dt$ dividindo por $N_o(t)$

$z(t) = dN_f(t)/dt \,.\, 1/N_o(t) = (-N/N_o(t)) \,.\, dR(t)/dt$

$R(t) = N_o(t)/N$

$z(t) = -1/R(t) \,.\, dR(t)/dt$

z(t) - hazard function ou taxa de defeitos

$dR(t)/dt = -R(t) \,.\, z(t)$

solução geral dessa equação é $R(t) = e^{-\int z(t)dt}$

considerando z(t) constante então: $R(t) = e^{-\lambda t}$

Confiabilidade

probabilidade de que um sistema funcione corretamente durante um intervalo de tempo $[t_0,t]$

- para um taxa de defeitos constante λ a confiabilidade R(t) varia exponencialmente em função do tempo
  - sistema na fase de vida útil: taxa de defeitos constante λ

- $R(t) = e^{-\lambda t}$ *exponential failure law*
  - é a mais usada relação entre confiabilidade e tempo
  - válida principalmente para componentes eletrônicos

Distribuição de Weibull

Weibull W. A statistical distribution function of wide applicability. J Appl Mech 1951;18:293–7.

- se taxa de defeitos varia com o tempo
  - z(t) distribuição de Weibull
    - importante para modelagem de software onde a confiabilidade pode inclusive aumentar com o tempo
  - $z(t) = \alpha\lambda(\lambda t)^{\alpha-1}$ para $\alpha>0$ e $\lambda>0$

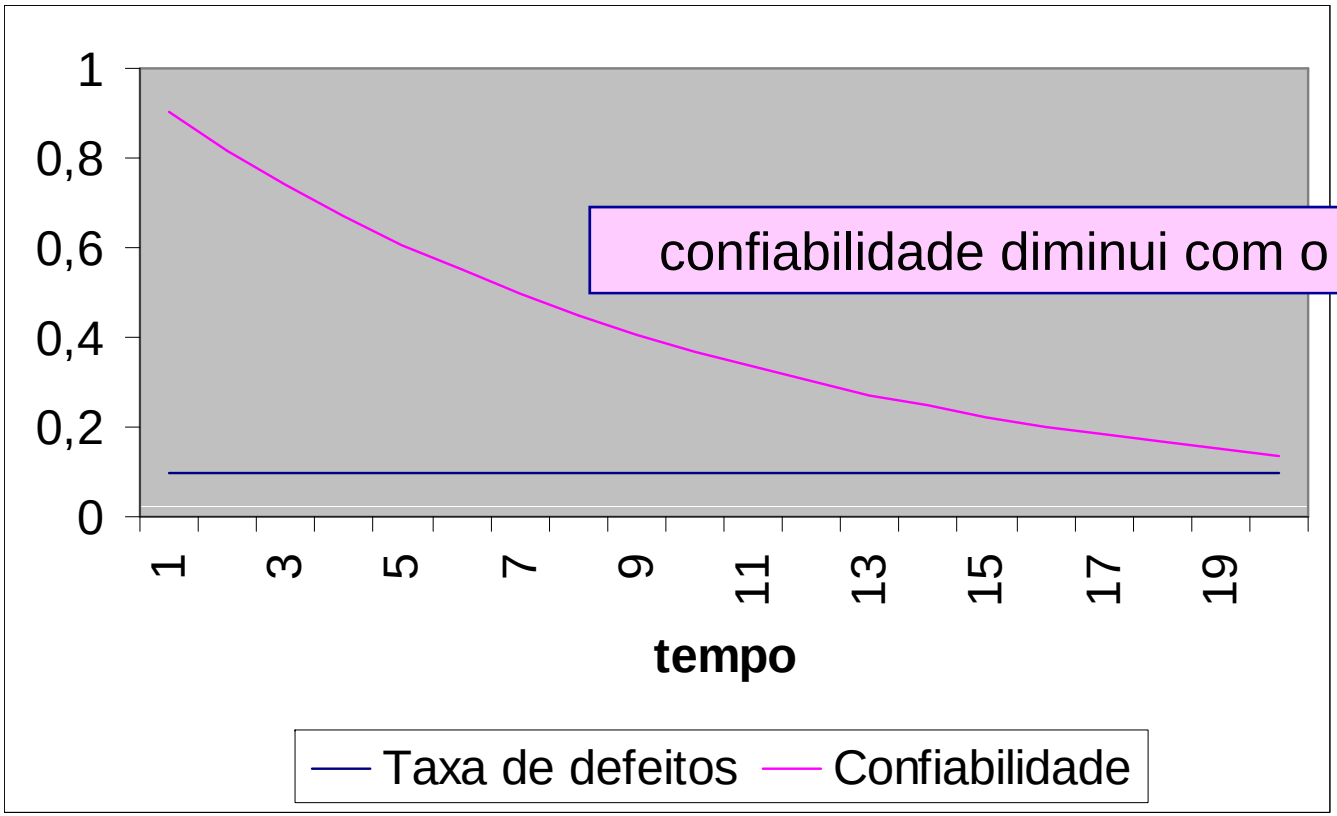
α e λ são constantes que controlam a variação de z(t) no tempo

- **$R(t) = e^{-(\lambda t)^{\alpha}}$**
  - para $\alpha=1$ z(t) = constante = λ
  - para $\alpha>1$ z(t) = aumenta com o tempo
  - para $\alpha<1$ z(t) = diminui com o tempo

Confiabilidade

- para: α=1 λ=0,1

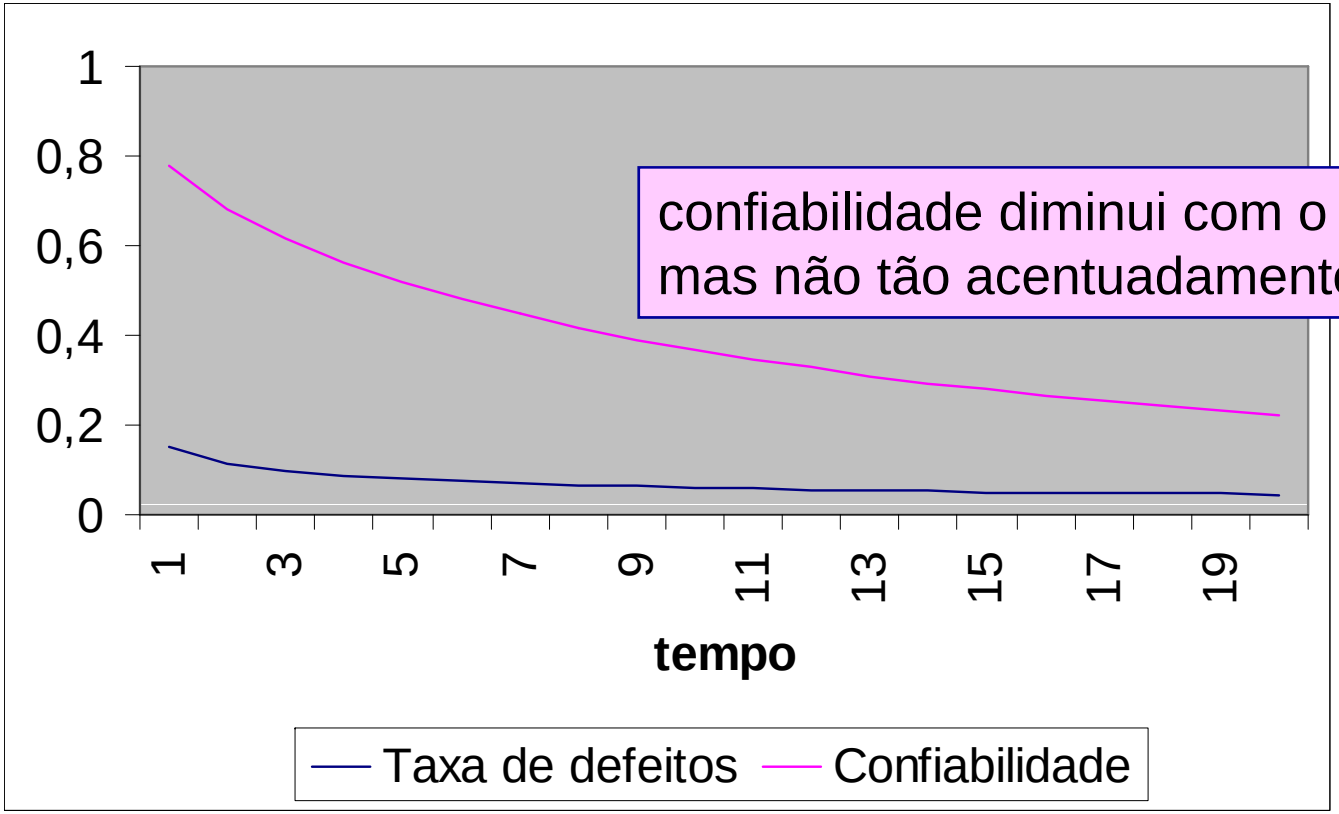
taxa de defeitos constante



Confiabilidade

- para: α=0,6 λ=0,1

taxa de defeitos
diminui com o tempo

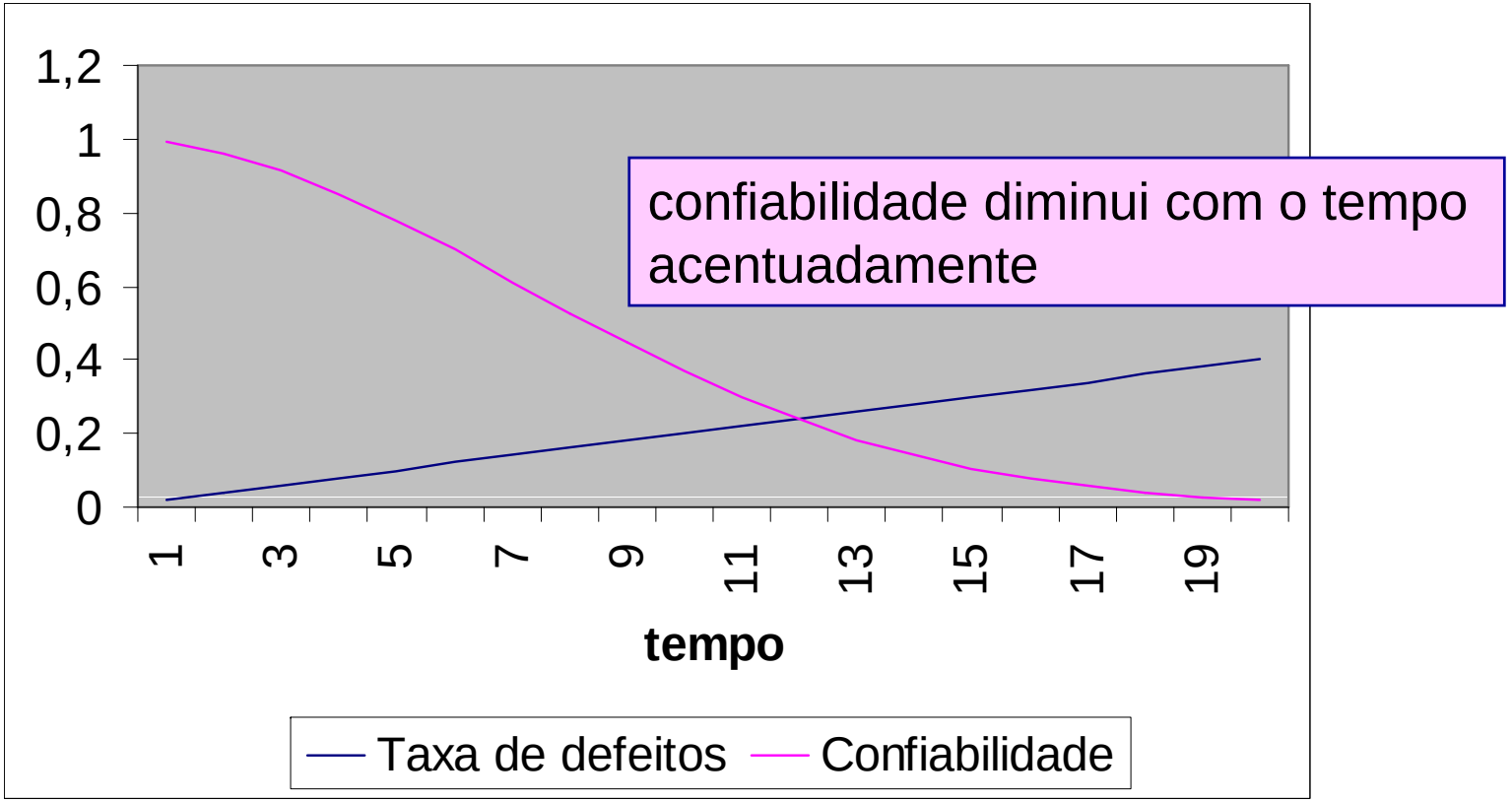


confiabilidade diminui com o tempo
mas não tão acentuadamente

Confiabilidade

- para: α=2 λ=0,1

taxa de defeitos aumenta linearmente com o tempo



Disponibilidade

- probabilidade do sistema estar operacional no instante **t** (disponível para o trabalho útil)
  - alternância entre funcionamento e reparo

    A(t) = R(t) quando reparo tende a zero

  - lembrar que MTBF = MTTF + MTTR
    - intuitivamente

$$A(t) = t_{op} / (t_{op} + t_{reparo})$$

A(t):availability

t_{op} tempo de operação normal

t_{reparo} tempo de reparo

Disponibilidade

- MTBF = MTTF + MTTR
- $A(t) = t_{op} / (t_{op} + t_{reparo})$
- genericamente

$$A(t) = MTTF / (MTTF + MTTR)$$

nessa relação, o significado de alta disponibilidade fica mais claro

diminuindo o tempo médio de reparo, aumenta a disponibilidade

Cobertura

fault coverage

- cobertura de falhas

significado intuitivo

  - habilidade do sistema de realizar detecção, confinamento, localização, recuperação ...
  - habilidade do sistema de tolerar falhas
    - geralmente se refere a habilidade de realizar recuperação de falhas
- significado matemático:
  - probabilidade condicional que dada uma falha o sistema se recupere

extremamente difícil de calcular

Cobertura

- geralmente assumido valor constante
- determinação:
  - listar falhas possíveis e falhas que o sistema pode tolerar e calcular o percentual
- usada no modelo de Markov
- muito usada também em experimentos de injeção de falhas

falhas simuladas são injetadas no sistema e se observa a reação do mecanismo de TF

relação entre falhas injetadas e falhas percebidas pelo mecanismo de TF

Problemas com medidas

- defeitos são eventos aleatórios
  - podem demorar muito para ocorrer, não ocorrer ou ocorrer em um momento não apropriado
- custo de avaliação experimental é alto
  - necessária uma grande quantidade de amostras
  - necessário tempo grande de avaliação
- é importante avaliar durante o projeto do sistema
- injeção de falhas

Bibliografia para medidas

- 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
  - Johnson, B.W. “Fault Tolerance” *The Electrical Engineering Handbook.* Ed. Richard C. Dorf. Boca Raton: CRC Press LLC, 2000
- livro
  - Dunn, Willian R. Practical design of safety critical computer systems. Reliability Press. 2002. (cap 4 e 5).
  - Barry W. Johnson. Design and Analysis of Fault-Tolerant Digital Systems. Addison-Wesley, 1989

http://dream.eng.uci.edu/eecs224/johnson_pt1.pdf
http://dream.eng.uci.edu/eecs224/johnson_pt2.pdf
http://dream.eng.uci.edu/eecs224/johnson_pt3.pdf

Bibliografia para medidas

- normas
  - MIL-HDBK-217F-2, *Reliability Prediction of Electronic Equipment*, Department of Defense.
- artigos
  - J.H. Saleh, K. Marais. Highlights from the early (and pre-) history of reliability engineering. Reliability Engineering and System Safety 91 (2006) 249–256