Modelagem para cálculo de confiabilidade

Taisy Silva Weber

Modelagem

- Modelos de confiabilidade
- Modelos combinatórios série e paralelo
  - Aplicação a TMR
- Modelos de Markov
  - Aplicação a TMR
- Modelos para confiabilidade, safety e disponibilidade

Barry Johnson,
cap. 1, livro-texto Pradhan96

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

Cálculo de confiabilidade

- R(t) = um dos principais atributos de dependabilidade
    - quase a totalidade das especificações determina que certos valores para R(t) devem ser alcançados e demonstrados
- estimar R(t) para sistema com mais de um componente
- usual: métodos analíticos
    - métodos analíticos mais comuns:
        - modelos combinatórios
        - modelos de Markov

para aplicar o método, um **modelo** do sistema deve ser criado

Modelos combinatórios

- baseado em técnicas probabilísticas
  - enumerar as diferentes maneiras de um sistema permanecer operacional
  - calcular a probabilidade dos eventos que levam o sistema a permanecer operacional
  - usar a confiabilidade dos componentes individuais
- dois modelos mais comuns na prática:
  - sistema em série
  - sistema em paralelo

não confundir com **circuitos** em série e paralelo

Modelos combinatórios: série

- cada elemento no sistema deve operar corretamente para o sistema operar corretamente
  - usado em sistemas que **não** apresentam **redundância**
- confiabilidade:
  - probabilidade que nenhum elemento apresente falha ou
  - probabilidade que todos os componentes operem corretamente
- sistema em série:

$$\boxed{R_{série}(t) = \Pi\, R_i(t)}$$

Modelos combinatórios: paralelo

- apenas um elemento no sistema precisa operar corretamente para o sistema operar corretamente
  - sistema com redundância
- não confiabilidade Q(t):
  - probabilidade que todos os componentes falhem
- sistema em paralelo

$$Q_{paralelo}(t) = \Pi \, Q_i(t)$$

$$R_{paralelo}(t) = 1 - \Pi \, (1 - R_i(t))$$

assume-se que as falhas que afetam os componentes paralelos são randômicas e independentes

Modelos combinatórios

- sistema em série

todos devem operar corretamente

$$R_{série}(t) = \prod_{i=1}^{n} R_i(t)$$

- sistema em paralelo

$$R_{paralelo}(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

ao menos um deve operar corretamente

sistemas mistos são tratados com uma combinação destas fórmulas

Sistemas M-of-N

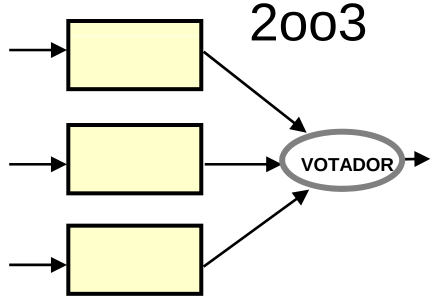
- generalização de um sistema paralelo ideal
    - M de um total de N módulos idênticos devem operar corretamente
        - aparece também como MooN (M-out-of-N)
    - exemplo: TMR: 2-of-3

$$R_{M\text{-}of\text{-}N}(t) = \sum_{i=0}^{N-M} \binom{N}{i} R^{N-i}(t)(1.0 - R(t))^{i}$$

$$\binom{N}{i} = \frac{N!}{(N-i)!\,i!}$$

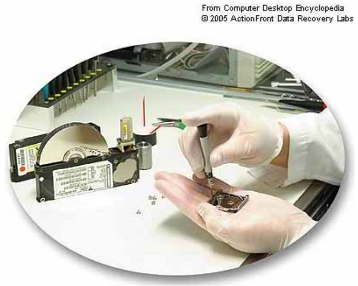
combinação de N elementos i a i

2oo3



Desvantagens

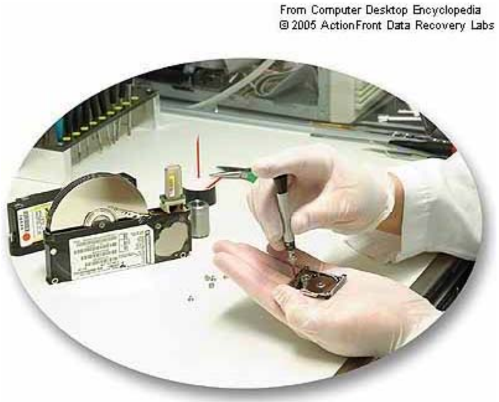
- modelos combinatórios:
  - geram equações grandes e complexas
- outras dificuldades:



  - incorporar reparos no modelo
  - incorporar fator de cobertura
    - cobertura da detecção ou diagnóstico de falhas
      - falhas detectadas podem ser tratadas
      - se a falha for tratada (ou o erro corrigido) o sistema pode ser recuperado ou ir para um estado seguro

Modelos de Markov

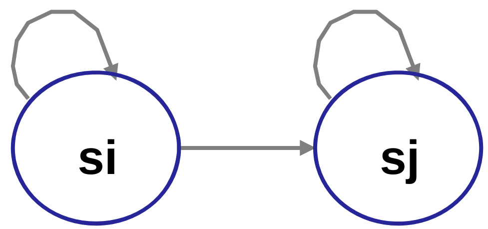
- modelam sistemas complexos
  - incorporam a **cobertura** imperfeita de falhas
  - incorporam probabilidade de estados **seguros**
  - consideram reparo
    - podem ser colocados links entre os estados conhecendo a taxa de reparo dos componentes



- elementos básicos do modelo
  - diagramas de transição de estados
  - estados e transições

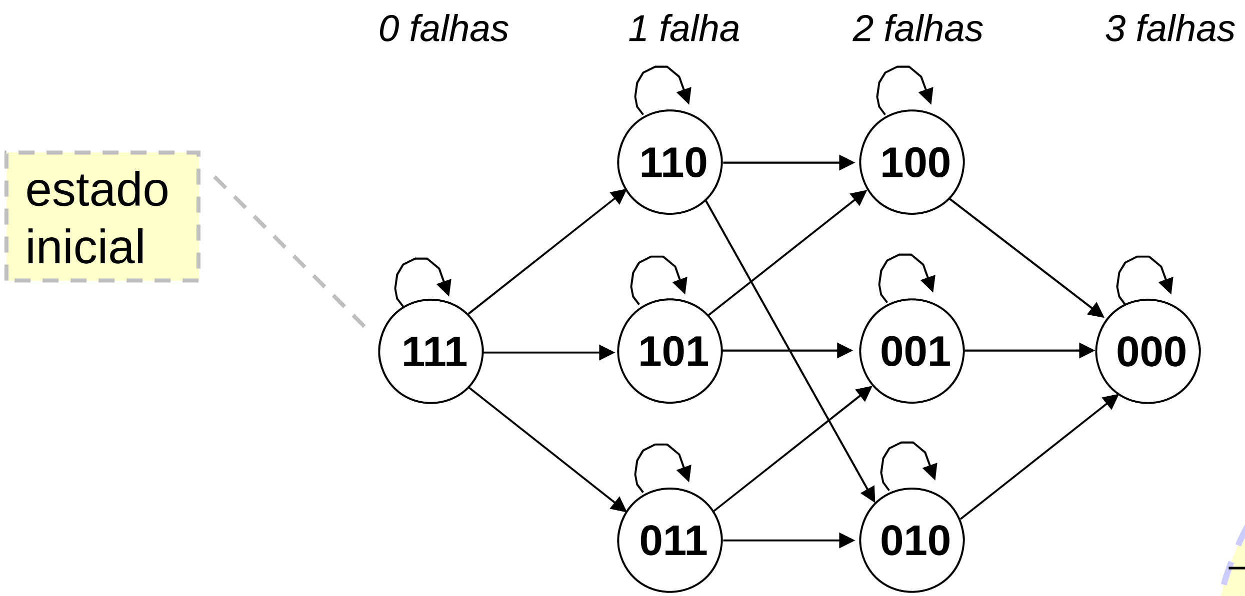
Markov: transição de estados

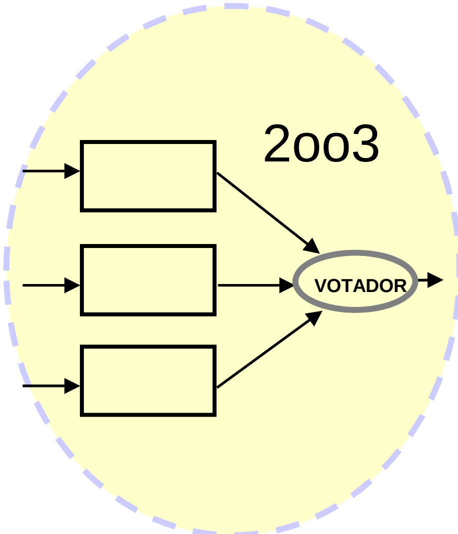
- estados = combinações de componentes operacionais e falhos



- transições = probabilidades para cada mudança de estado
    - probabilidade de **ocorrência de uma falha**
    - probabilidade de **cobrir uma falha**
    - probabilidade de **reparo**
  - probabilidade de uma transição de si a sj é independente do método de chegada em si

exemplo: TMR

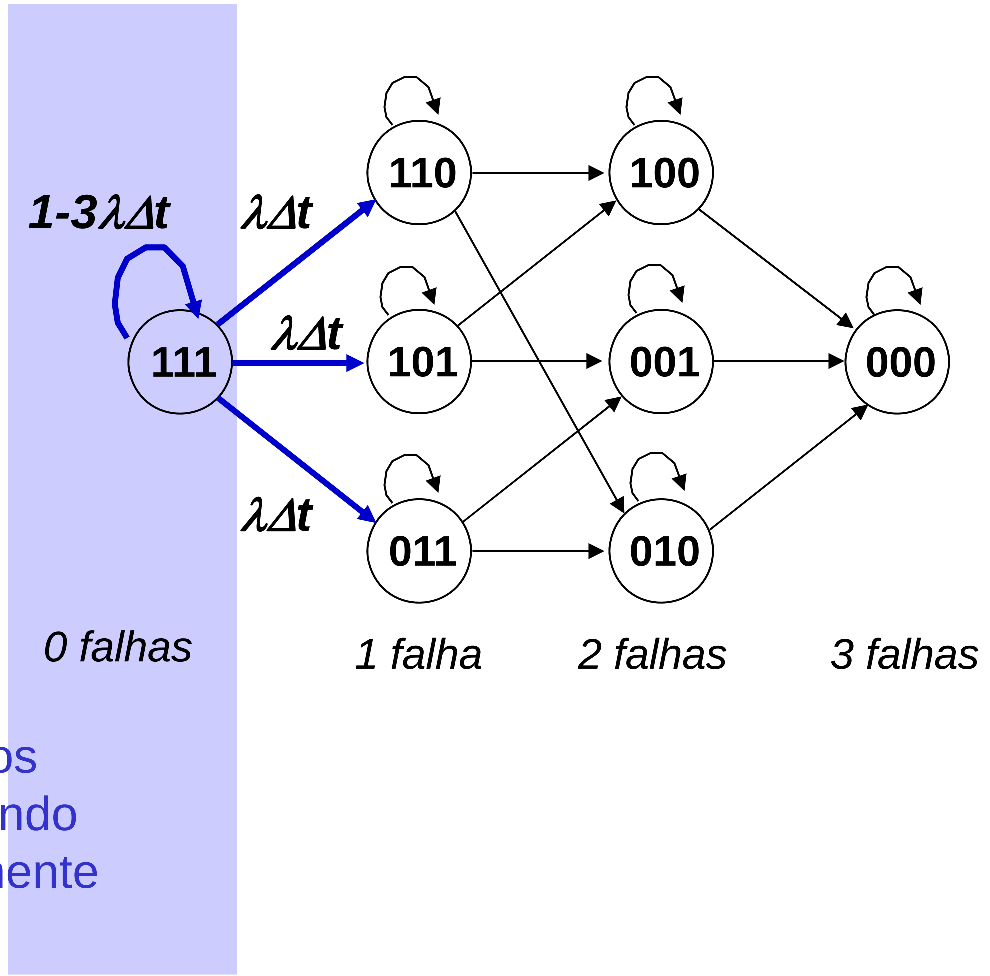




considerando que cada módulo no TMR obedece a lei de falhas exponencial, a probabilidade de um módulo falhar no intervalo **t + Δt** estando operacional em t é, simplificando:

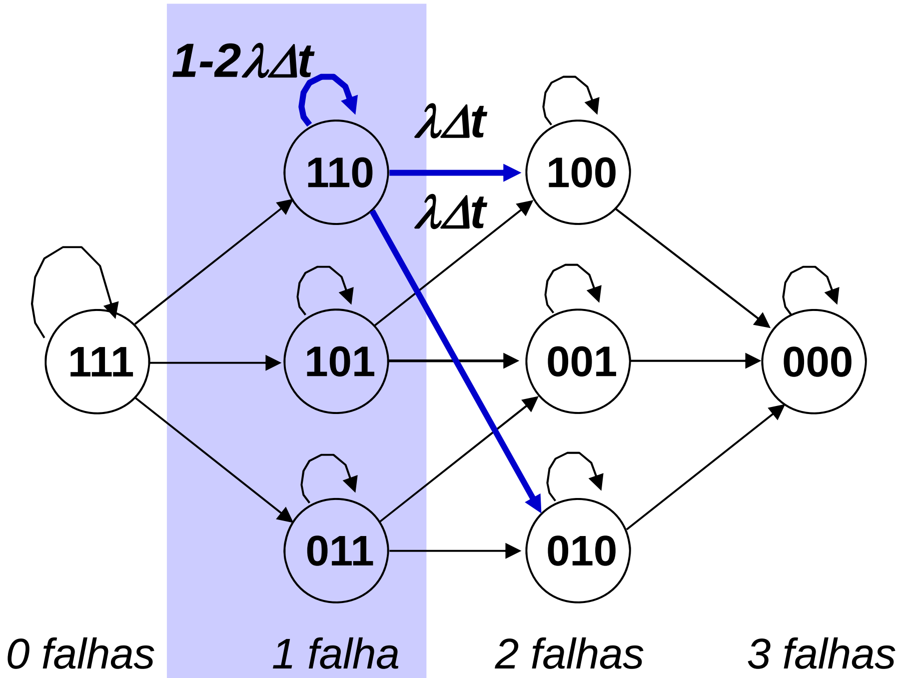
$$\lambda \Delta t$$

exemplo: TMR



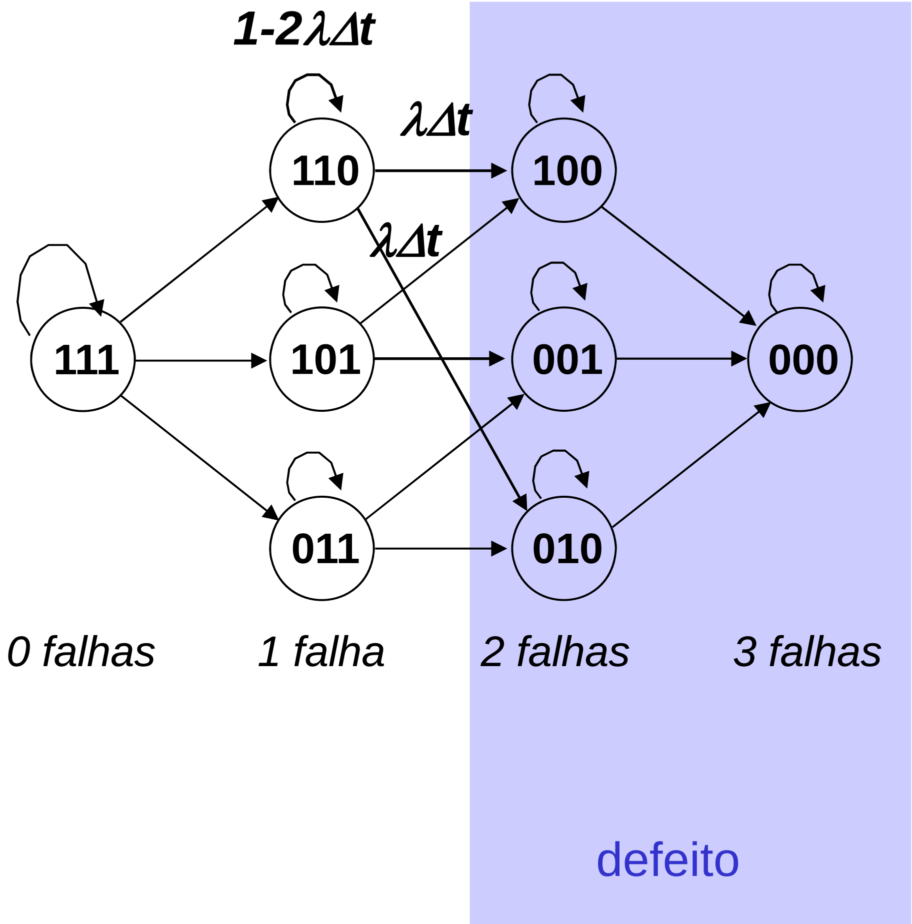
3 módulos
funcionando
corretamente

exemplo: TMR



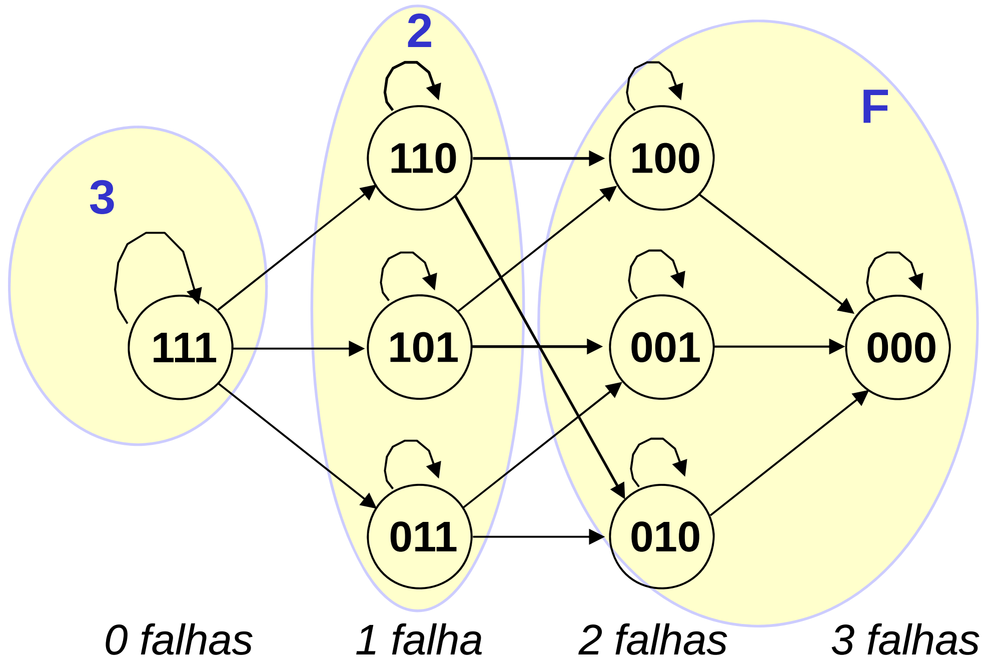
2 módulos
funcionando
corretamente

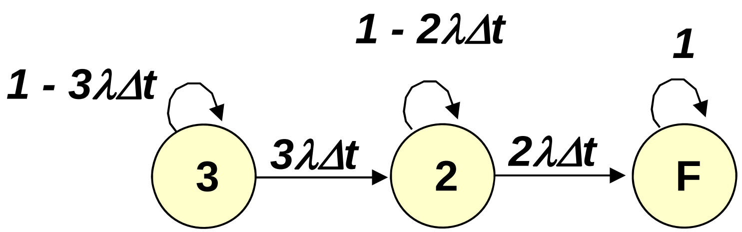
exemplo: TMR



quando em defeito, qualquer transição permanece em defeito

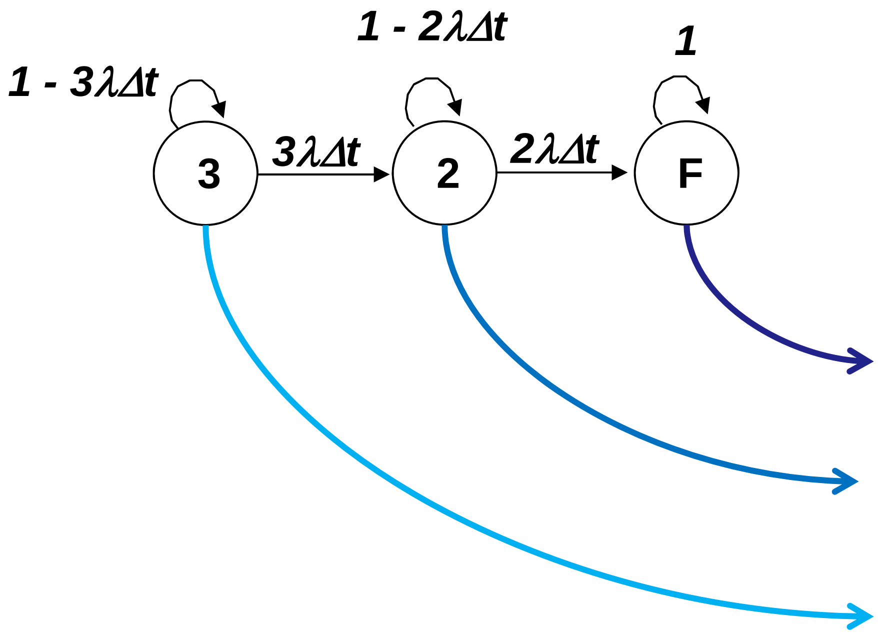
Markov reduzido





modelo de Markov reduzido para TMR

Confiabilidade a partir de Markov



seja $p_3(t)$, $p_2(t)$ e $p_F(t)$ a probabilidade de estar no estado 3, 2, F no tempo t

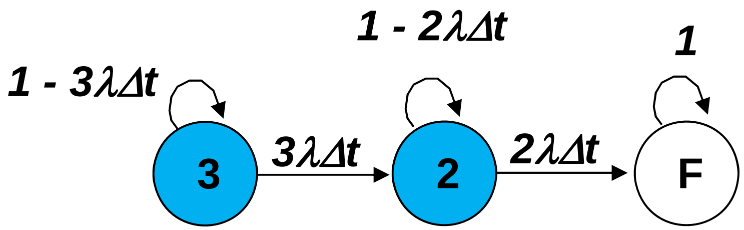
$$p_F(t + \Delta t) = \mathbf{2\lambda\Delta t}\, p_2(t) + p_F(t)$$

$$p_2(t + \Delta t) = \mathbf{3\lambda\Delta t}\, p_3(t) + (\mathbf{1 - 2\lambda\Delta t})\, p_2(t)$$

$$p_3(t + \Delta t) = (\mathbf{1 - 3\lambda\Delta t})\, p_3(t)$$

probabilidade de permanecer no estado somada a probabilidade de chegar ao estado

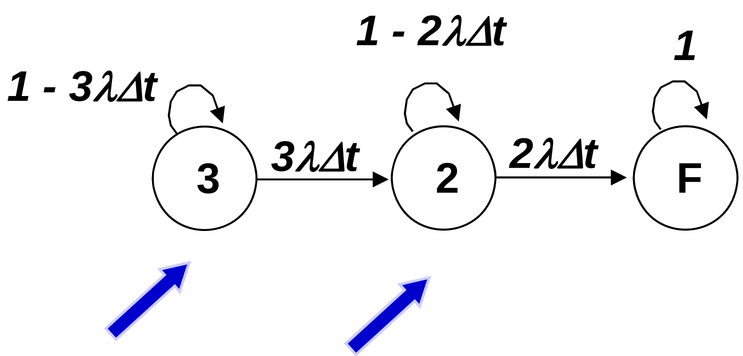
Confiabilidade a partir de Markov



confiabilidade é a probabilidade de estar no estado **3** ou **2**

ou a probabilidade de **não** estar no estado **F**

Confiabilidade do TMR



Considerando que no limite **delta t** se aproxima de zero, podemos construir uma série de equações diferenciais.

confiabilidade é a probabilidade de estar no estado **3** ou **2** ou não estar no estado **F**

Derivando as equações, a solução é:

$$p_3(t) = e^{-3\lambda t}$$

$$p_2(t) = 3e^{-2\lambda t} - 3e^{-3\lambda t}$$

$$p_F(t) = 1 - 3e^{-2\lambda t} + 2e^{-3\lambda t}$$

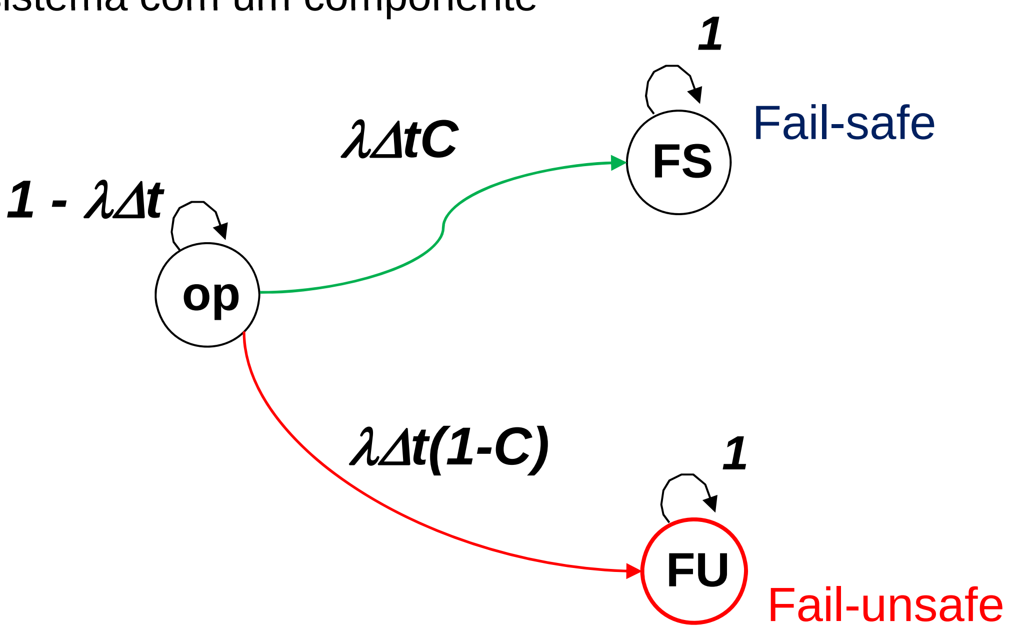
Modelagem de safety

- importante a cobertura de falhas da estratégia de safety
  - Cobertura perfeita: C = 1.0
  - Cobertura imperfeita: 0 <= C <= 1.0
- cobertura de falhas
  - probabilidade condicional que dada uma falha o sistema se recupere
  - probabilidade que dada uma falha o sistema a trate corretamente

por exemplo, indo para o estado seguro

2 transições

sistema com um componente



Cada estado operacional apresenta duas transições: uma para um estado seguro e outra para um estado inseguro.

A segurança do sistema é a probabilidade de estar em op ou FS.

→ $p_{op}(t) = e^{-\lambda t}$

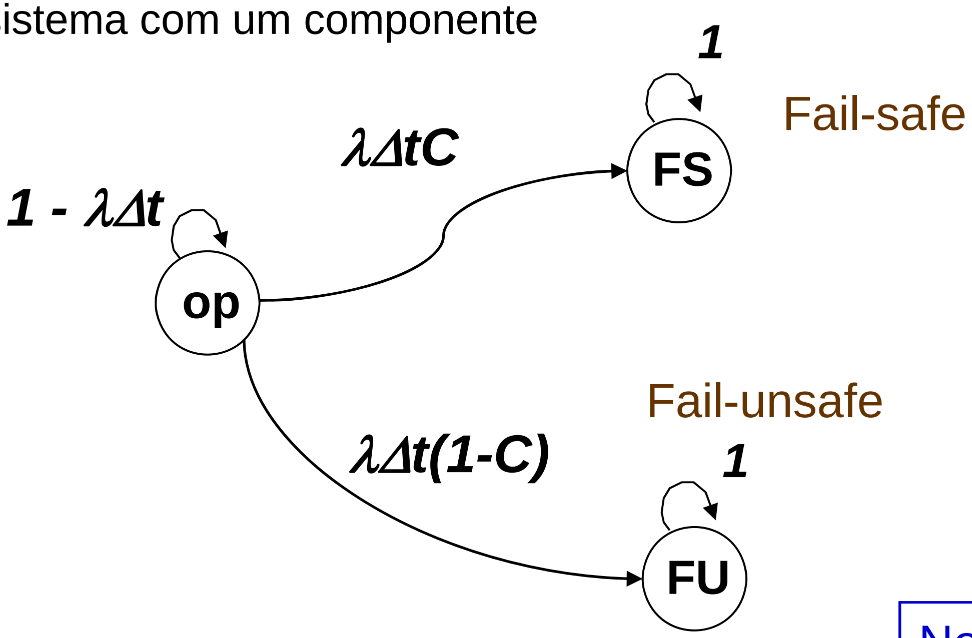
$p_{FU}(t) = (1-C) - (1-C)e^{-\lambda t}$

→ $p_{FS}(t) = C - Ce^{-\lambda t}$

$$\boxed{S(t) = C + (1- C)e^{-\lambda t}}$$

Safety e cobertura

sistema com um componente



No tempo t = 0, safety é 1.
No tempo infinito, safety igual a C.

$$S(t) = C + (1- C)e^{-\lambda t}$$

$$S(\infty) = C$$

A situação estável de um sistema seguro (*safety*) depende diretamente de sua cobertura de falhas

Modelagem de disponibilidade

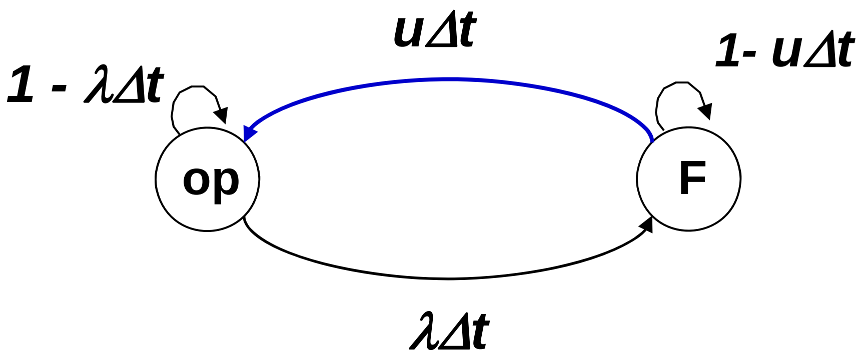
- noção de reparo
    - a capacidade de retornar de um estado menos operacional ou com defeito para um estado mais operacional ou totalmente operacional
- TAXA DE REPARO: número de reparos que se espera ocorrer num dado período de tempo

MTTF = $1/\lambda$
MTTR = $\frac{1}{\mu}$

para sistemas simplex

Markov com reparo

o reparo leva o sistema de F (com defeito) para op (operacional)



o reparo permite uma cadeia de Markov cíclica

Conclusão

- métodos analíticos
  - permitem obter medidas sobre um sistema antes de sua implementação
  - não dispensam medidas experimentais posteriores (sobre um protótipo)
  - exigem
    - domínio de probabilidade e estatística
    - ou o uso de programas apropriados que permitam modelar e estimar atributos de dependabilidade de um sistema

Bibliografia para modelagem

- 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
  - Stiffler, J.J. Reliability Estimation, cap 6. *Fault-Tolerant System Design*. Prentice Hall, New Jersey, 1996
  - 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