Aula 2 - Modelos de Falhas

Monday, March 7, 2016 13:51

Revisão da Aula 1

Sistema distribuído: Coleção de processos que colaboram para a execução de uma tarefa e se comunicam através de troca de mensagem.

Modelos Temporais
Sistema síncrono: Quando são conhecidos os limites de tempo para (1) transmitir uma mens sagem e (2) executar uma tarefa.

Sistema assíncrono: Quando tais limites não são conhecidos. Na verdade vai além disso - o t empo é ignorado.

Modelos parcialmente síncronos: diversas alternativas existem, mas nenhuma é "perfeita".

Tarefa da semana passada:
Pensar sobre o seguinte problema:

- Considere dois processos que nunca falham e devem executar uma de duas ações: α c ou β.
- Se comunicam por um canal que perde mensagens eventualmente.

Existe um algoritmo que resolve este problema?
Considere que existem vários algoritimos que resolvem este problema.
Selecione o algoritmo que resolve o problema com o menor número de mensagens.

O canal de comunicação é não-confiável (ele perde mensagens).
Não há como saber se a última mensagem chegou ou não.
Portanto, o algoritmo não precisa da última mensagem para resolver o problema.

-ABSURDO- o____O
Pois iniciamos com a premissa de que se tratava do menor algoritmo que resolve o problem a, mas vimos que há um menor ainda.m

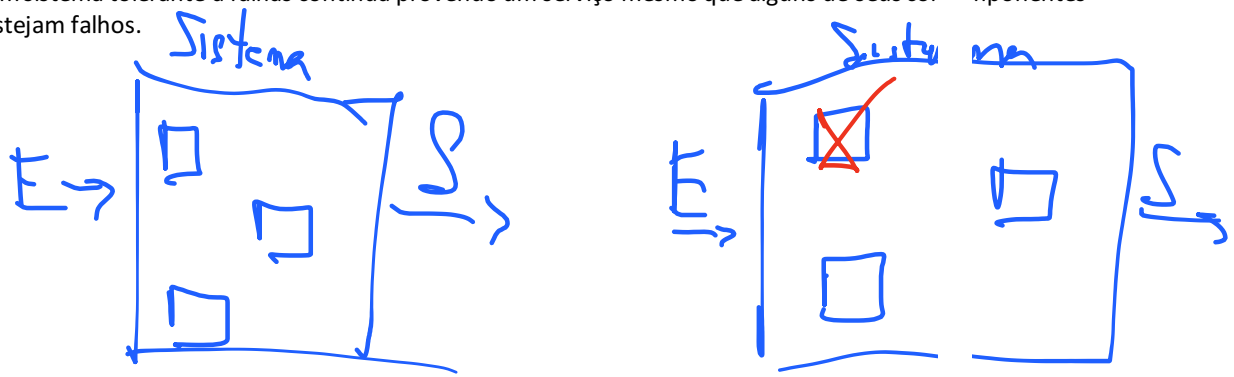
Conclusão: Não há algoritmo que resolve esse problema.

Tolerância a Falhas

É necessário ter sistemas confiáveis.

As redes têm se tornado indistinguíveis das organizações que as possuem.

Um sistema tolerante a falhas continua provendo um serviço mesmo que alguns de seus cor mponentes estejam falhos.



Quantos componentes podem falhar?

Parâmetro *t*: Sistemas *t*-tolerantes a falhas sobrevivem a até *t* componentes falhos.

Em geral: sistemas tolerantes a falhas empregam redundância.
Muitas vezes o sistema é redundante por definição
Por exemplo, sistemas distribuídos.

Propriedades

1. Dependability (confiança no serviço)
   Atributos:
   - Reliability (confiabilidade): Capacidade do sistema de oferecer o serviço sem int errupções.
   - Availability (disponibilidade): Capacidade de oferecer o serviço com interrupçõe es e recuperações.
   - Safety (segurança): Sistemas críticos cujas falhas colocam vidas em risco
   - Security (segurança): Somente pessoas (partes) autenticadas podem comunicar , acessar informações, alterar informações, etc.

O conceito de falha

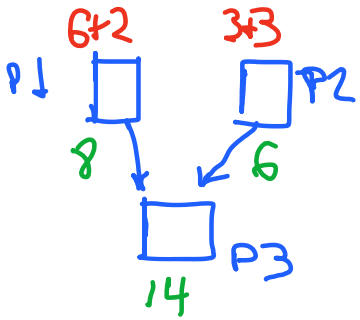
Fault -> Error -> Failure

Falha/Falta/Defeito -> Erro -> Falha/Colapso

Failure: O sistema produz uma saída fora de sua especificação.
Error: Um componente do sistema produz uma saída incorreta.
Fault: Um defeito de um componente, que pode se manifestar ou não.

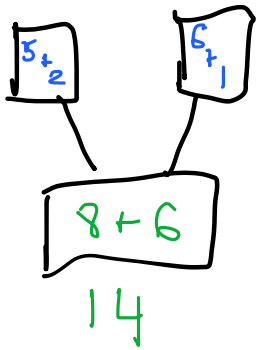
Exemplo

Considere um sistema com 3 processadores. Cada um soma dois inteiros recebidos como entrada e o resultado da soma é a saída.

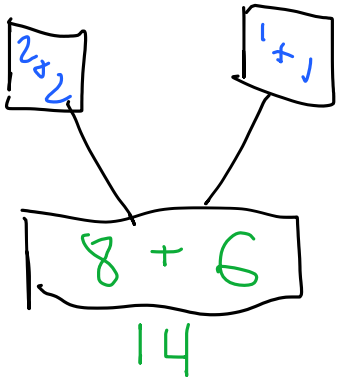


P1 sempre produz 8.
P2 sempre produz 6.

Há **fault**, mas não **error**.



Fault
Error
No **Failure**



Fault
Error
Failure

Uma classificação de falhas:
Crash: Falha por parada total. O componente ou sistema não produz nenhuma saída para nenhuma

entrada.
Omissão: O componente/sistema não responde para todos os elementos do conjunto de entradas em todos os casos. Em outras palavras: às vezes não produz saída.
Timing: Temporização; ou responde cedo demais ou tarde demais. Só faz sentido no contexto de sistemas síncronos.
Bizantina: O componente se comporta de maneira arbitrária.

Hierarquia: