

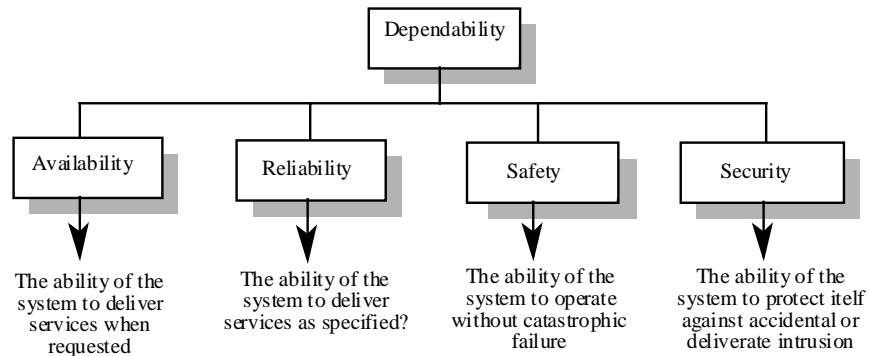
Confiança (Dependability)

- Disponibilidade
- Fiabilidade
- Segurança
 - Safety
 - Security

O conceito de confiança

- Para sistemas críticos, é a característica mais importante
- Reflete o grau de confiança no sistema, que o sistema não vai falhar numa utilização normal
- Um sistema não precisa ser fiável para ser útil

Confiança: Dimensões



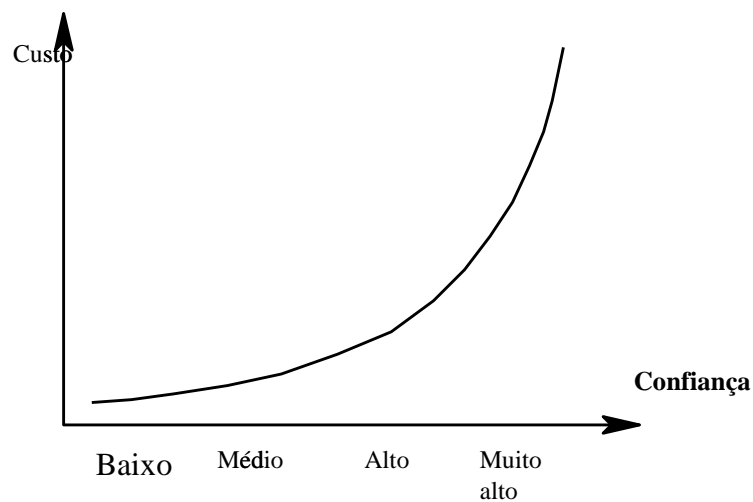
Manutenibilidade

- É um atributo do sistema que se preocupa com a facilidade de reparação depois que uma falha ocorreu ou novas características são adicionadas ao sistema
- É fundamental p/ sistemas críticos pois falhas são frequentemente introduzidas por causa de problemas de manutenção
- É um atributo estático e não dinâmico

Sobrevivência (*Survivability*)

- É a habilidade de um sistema continuar a oferecer seus serviços aos utilizadores apesar de um acidente (deliberado ou não) ou de falhas de componentes
- É um atributo especialmente importante para sistemas distribuídos cuja segurança pode estar comprometida

Confiança x custos



Confiança: custos

- Os custos tendem a aumentar exponencialmente com o aumento dos níveis de *confiança*
- Razões para isto:
 - A utilização de hardware e técnicas de desenvolvimento mais caras
 - Aumento do nº de testes e da validação do sistema necessários para convencer o cliente que os níveis de *confiança* foram conseguidos

Confiança vs performance

- Podem ser inversamente proporcionais
- Sistemas com pouca confiança podem ser rejeitados pelos utilizadores
- Os custos de falhas dum sistema podem ser altos
- É difícil “calibrar” os sistemas para aumentar a confiança
- Pode ser possível compensar uma performance pobre
- Sistemas não fiáveis causam perda de informação valiosa

Confiança: economia

- Por causa dos altos custos para obtenção da *confiança*, pode ser mais vantajoso aceitar sistemas não fiáveis e pagar pro custos das falhas
- Entretanto, isto depende de factores políticos e sociais
- Uma má reputação dos produtos pode ocasionar a perda de negócios futuros
- Depende do tipo de sistema, para *business systems* in níveis modestos de *confiança* podem ser adequados

Disponibilidade e fiabilidade

- **Fiabilidade**
 - É a probabilidade de uma operação do sistema livre de falhas num determinado período em um dado ambiente para um dado propósito
- **Disponibilidade**
 - É a probabilidade que um sistema estará operacional e poderá realizar os serviços requisitados
- Ambos os atributos podem ser expressos qualitativamente

Disponibilidade e fiabilidade

- Às vezes é possível subordinar a disponibilidade do sistema à sua fiabilidade
- Entretanto é possível ter sistemas com baixa fiabilidade que devam estar disponíveis. Provado que as falhas do sistema sejam reparadas rapidamente e não danifiquem os dados, baixa fiabilidade pode não ser um problema
- Disponibilidade leva em conta tempo de reparo

Terminologia de fiabilidade

Termo	Descrição
Falha do sistema	Um evento que ocorre quando o sistema não satisfaz um serviço, como esperado pelos utilizadores
Erro do sistema	Comportamento não correcto do sistema, que não está de acordo com a especificação
Falta do sistema	Um estado incorrecto do sistema, i.e., um estado do sistema inesperado pelos engenheiros
Erro humano	Comportamento humano que resulta na introdução de faltas no sistema

Faltas e falhas

- Falhas decorrem de erros do sistema que são derivados de faltas no sistema
- Entretanto, faltas não resultam em erros, necessariamente
 - O sistema com falta pode estar em estado transiente e depois corrigido antes que o erro aconteça
- Erros não levam a falhas do sistema necessariamente
 - O erro pode ser corrigido por procedimentos de detecção e recuperação de erros
 - A proteção à falha pode ser conseguida através de recursos de proteção especiais

Percepções de fiabilidade

- A definição formal de fiabilidade nem sempre reflecte a percepção do utilizador
 - As considerações sobre o ambiente do sistema podem estar incorretas
 - A utilização de um sistema em ambiente industrial é diferente do que em um ambiente universitário
 - As consequências das falhas afectam a percepção da fiabilidade
 - Falhas com consequências graves têm mais peso que falhas que são apenas inconvenientes

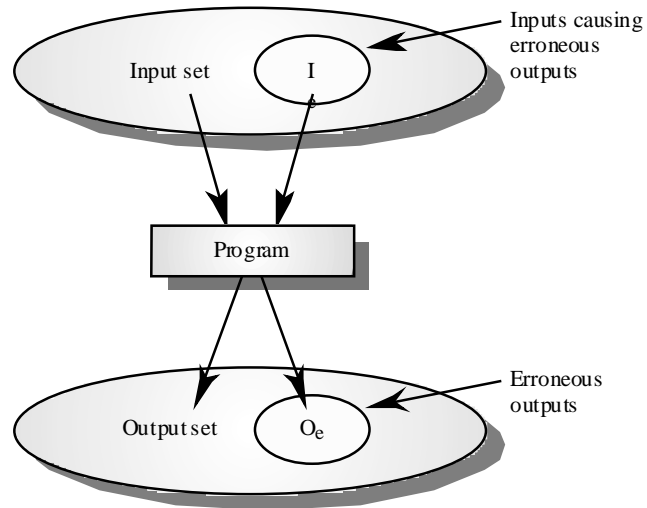
A conquista da fiabilidade

- Evitar falta
 - Técnicas de desenvolvimento são usadas para minimizar a possibilidade de erros antes que eles resultem na introdução de faltas no sistema
- Detecção e remoção de faltas
 - Técnicas de verificação e validação que aumentam a probabilidade de detecção e correção de erros antes da execução do sistema devem ser usadas
- Tolerância a faltas (falhas)
 - Técnicas *run-time* são usadas para certificar que as faltas do sistema não resultam em erros e/ou os erros não levam a falhas

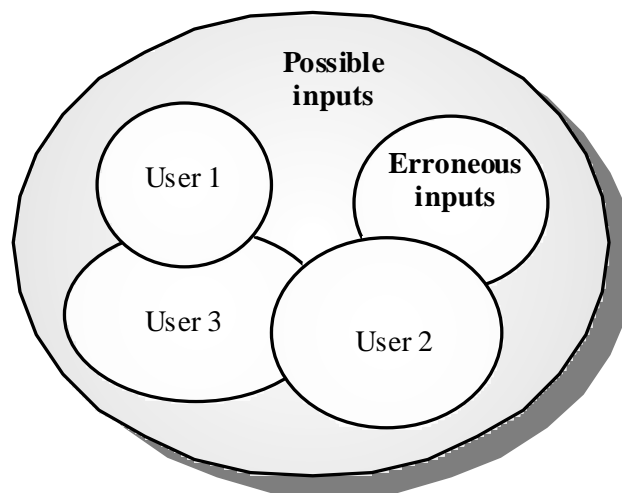
Modelagem da fiabilidade

- Pode-se modelar um sistema como um mapeamento input-output onde algumas entradas resultam em saídas erradas
- A fiabilidade dum sistema é a probabilidade que uma determinada entrada tem em fazer parte do conjunto de entradas que causam saídas erradas
- Pessoas diferentes utilizam o sistema de forma diferente, portanto a probabilidade não é um atributo estático do sistema, mas depende do ambiente

Mapeamento Input/output



Percepção da fiabilidade



Melhoramento da fiabilidade

- Remover X% das faltas em um sistema necessariamente melhorar a fiabilidade em X%. Um estudo realizado pela IBM mostrou que removendo 60% dos defeitos de um produto resultam em 3% de aumento da fiabilidade
- Defeitos de programa podem ocorrer em partes do código que são raramente executadas. Removendo-os não afecta a percepção da fiabilidade
- Um programa com faltas conhecidas pode ainda ser visto como fiável pelos utilizadores

Segurança (safety)

- Segurança (safety) é uma propriedade de um sistema que reflecte a habilidade do sistema para operar normal ou anormalmente sem o perigo de causar danos ou morte às pessoas e sem prejudicar o ambiente do sistema
- É crucial considerá-la, pois cada vez mais há sistemas de controlo baseados em software
- Requisitos de segurança (safety) são requisitos de exclusão, i.e., eles excluem situações não desejáveis em vez de especificar os serviços do sistema

Criticalidade da segurança (*Safety criticality*)

- Sistemas críticos primários
 - Sistemas de software embebidos cujas falhas podem causar falha no hardware associado e prejudicar as pessoas directamente
- Sistemas críticos secundários
 - Sistemas cujas falhas resultam em faltas em outros sistemas que podem prejudicar pessoas
- O foco aqui é o sistema crítico primário

Segurança (safety) e fiabilidade

- Segurança (safety) e fiabilidade estão relacionados, mas são distintos
 - Em geral, fiabilidade e disponibilidade são necessários, mas não são condições suficientes para segurança (safety)
- Fiabilidade: tem em consideração a especificação
- Segurança (safety): preocupa-se em certificar-se de que o sistema não causa danos, não importando se ele está ou não de acordo com a especificação

Sistemas fiáveis e não seguros

- Erros de especificação
 - Se a especificação do sistema está errada, então o sistema pode comportar-se como especificado, mas pode causar um acidente
- Falhas de hardware podem gerar entradas falsas (difícil de antecipar)
- Comandos sensíveis ao contexto: execução do comando certo na hora errada (resultado de erro do operador)

Segurança (safety): terminologia

Termo	Definição
Acidente (ou desastre)	Um evento não planeado ou uma sequência de eventos que resultam em perda humana, dano à propriedade or ao ambiente. Uma máquina controlada por computador que fere um operador é um exemplo de acidente.
Perigo	Uma condição com o potencial de causar ou contribuir para um acidente. Uma falha de um sensor que detecta um obstáculo em frente a uma máquina é um exemplo de perigo.
Dano	Uma medida de perda resultante de um desastre. O dano pode ir de várias pessoas mortas a como resultado de um acidente ou ferimentos superficiais.
Severidade do perigo	Uma avaliação do pior dano possível que pode resultar de um perigo. A severidade do perigo pode ser de catastrófico a menor.
Probabilidade do perigo	A probabilidade dos eventos ocorrerem, criando assim o perigo. Os valores vão de provável a não plausível.
Risco	É uma média da probabilidade do sistema causar um acidente. O risco é avaliado considerando a probabilidade de perigo, a severidade do perigo e a probabilidade que um perigo resultará em um acidente.

Segurança (safety): conquista

- Evitação do perigo
 - O sistema é desenhado com o objectivo que algumas classes de perigo não ocorram
- Remoção e detecção do perigo
 - O sistema é desenhado p/ que os perigos sejam detectados e removidos antes que resultem em acidente
- Limitação do dano
 - O sistema inclui características de protecção que minimizam o dano que pode resultar de um acidente

Acidentes normais

- Acidentes em sistemas complexos raramente têm uma causa simples porque estes sistemas são desenhados p/ se recuperarem prontamente para uma falha em um determinado ponto
- Quase todos os acidentes são resultantes de uma combinação de disfuncionamentos
- Antecipar todas as combinações de problemas é impossível

Segurança (security)

- É a propriedade de um sistema que reflecte a habilidade do sistema para se proteger de ataques externos deliberados ou acidentais
- Está a tornar-se cada vez mais importante em virtude da ligação dos sistemas à web
- É um pré-requisito essencial a disponibilidade, fiabilidade e segurança (safety)
- Se um sistema está ligado à rede e é inseguro, então as afirmações sobre sua fiabilidade e segurança (safety) não são fiáveis

Segurança (security): terminologia

Termo	Definição
Exposição	Perda ou dano possíveis em sistema de computador
Vulnerabilidade	Um fraqueza em um sistema baseado em computador que pode ser explorada para causar perda ou dano
Ataque	Exploração da vulnerabilidade de um sistema
Ameaças	Circunstâncias que tem o potencial de causar perda ou dano
Controlo	Uma medida e proteção que reduz a vulnerabilidade do sistema

Danos causados

- **Negação de serviço**
 - O sistema é forçado a entrar em um estado onde serviços normais estão indisponíveis ou onde a provisão do serviço está significativamente degradada
- **Corrupção de programas ou dados**
 - Os programas ou dados do sistema pode ser modificados sem autorização
- **Divulgação de informação confidencial**
 - Informação que é gerida pelo sistema pode ser exposta a pessoas que não estão autorizadas a ler ou usar esta informação

Segurança (security): garantia

- **Evitação da vulnerabilidade**
 - O sistema é desenhado pra que vulnerabilidades não ocorram
- **Eliminação e detecção de ataque**
 - O sistema é desenhado para que ataques sejam detectados e neutralizados (e.g., uso de anti-virus)
- **Limitação de exposição**
 - O sistema é desenhado para que consequências de um ataque bem sucedido sejam minimizadas(e.g. uso de backup)

Pontos chave

- **Confiança:** reflecte a confiança do utilizador no sistema
- **Disponibilidade:** é a probabilidade do sistema estar disponível quando os serviços forem requisitados
- **Fiabilidade:** é a probabilidade dos serviços do sistema serem realizados como especificado
- **Fiabilidade e disponibilidade** são geralmente vistos como necessários , mas não suficientes para segurança (*safety* e *security*)

Pontos chave

- **Fiabilidade:** está relacionada com a probabilidade de um erro ocorrer durante a operação do sistema
- **Segurança (safety):** é um atributo do sistema que reflecte a habilidade do sistema de operar sem ameaçar as pessoas ou o ambiente
- **Segurança (security):** é um atributo do sistema que reflecte a habilidade do sistema para proteger-se de ataques externos