CRITICAL SYSTEMS

Ian Sommerville, 8° edição – Capítulo 3

Aula de Luiz Eduardo Guarino de Vasconcelos

Objetivos

- Explicar que uma falha pode causar graves consequências humanas ou econômicas
- Explicar as quatro dimensões de confiança no sistema: disponibilidade, confiabilidade, segurança e proteção
- Explicar que para obter confiança, deve-se evitar erros durante o desenvolvimento, detectar e corrigir erros quando em uso e limitar danos causados por falhas operacionais

Tópicos abordados

- Sistema crítico de segurança simples
- Confiança no sistema
- Disponibilidade e confiabilidade
- Segurança (Security)
- Proteção (Safety)

Concepção de Confiança

- A propriedade emergente mais importante de um sistema crítico é a confiança
- A confiança em um sistema está no grau de confiança dos usuários em que o sistema irá operar conforme sua expectativa e que não irá 'falhar' durante o uso normal
- Confiança e utilidade não são a mesma coisa. Um sistema pode não ser muito confiável, mas pode ser útil

Confiança é importante

- Reflete o grau de confiança do usuário no sistema
- Sistemas não confiáveis, inseguros ou desprotegidos são frequentemente rejeitados por seus usuários. Se não confia, não usa. Além disso, podem se recusar a comprar/usar outros produtos da mesma empresa.
- Custos de falha de sistema podem ser muito altos (queda de aeronave, míssil, aeroespacial, etc)
- Sistemas não confiáveis podem causar perda de informação: redundância é cara

Sistemas críticos

- Sistemas críticos de segurança
  - Ferimentos, perda de vida ou danos ao ambiente. Ex.: sistema de fábrica de produtos químicos
- Sistema crítico de missão
  - Não atingir o objetivo. (Controle de aeronaves)
- Sistema crítico de negócios
  - Falha resulta em custos para os negócios. (Sistema de contabilidade de clientes de um banco)

Métodos de desenvolvimento para sistemas críticos

- Uma falha em sistema crítico tem custo alto
- Uso de técnicas onerosas de engenharia de software para sistemas não críticos, podem ser usadas:
  - Métodos formais para redução de testes (testes representam mais de 50% do custo de um sistema crítico)
  - Análise estatística

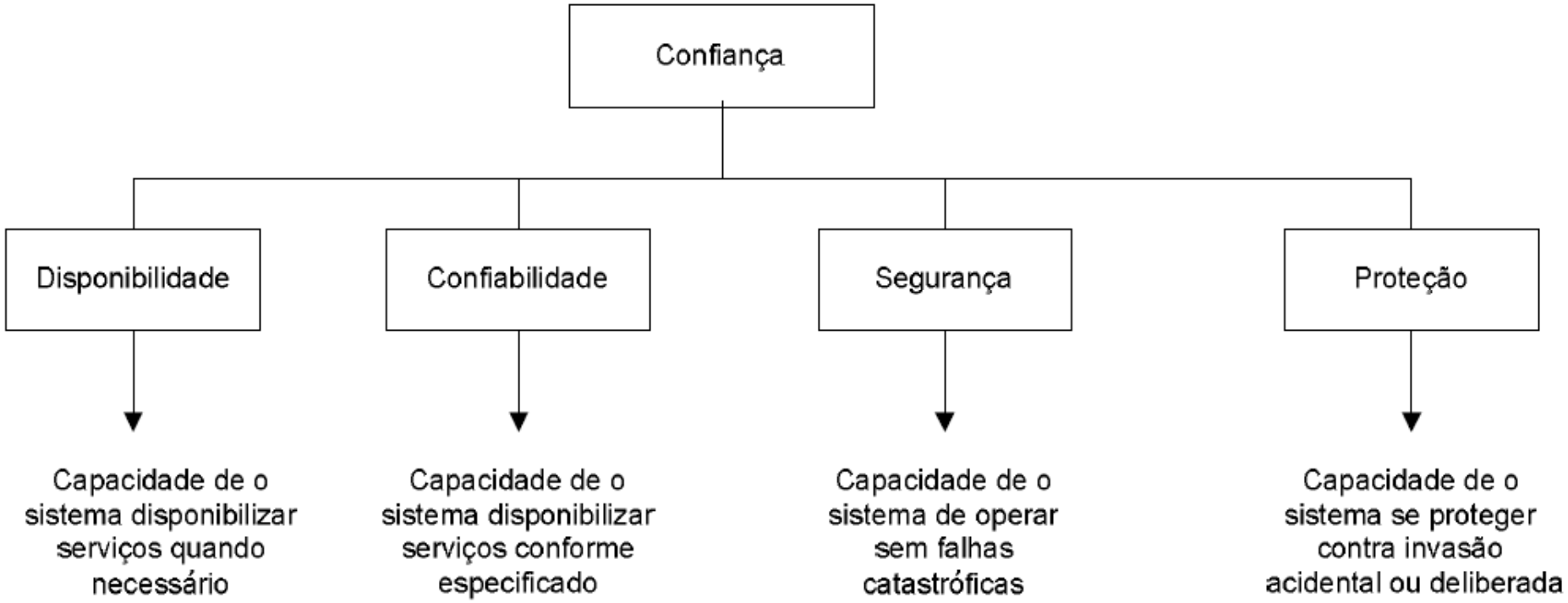
Componentes sujeitos a falhas

- Hardware
  - Erros de fabricação
  - Fim da vida útil (MTBF)
  - Erro de especificação no projeto
- Software
  - Enganos ou erros de implementação ou especificação
- Humanos
  - Má operação do sistema. Como o hardware e o software tornaram-se mais confiáveis, falhas de operação são atualmente a maior causa de falhas de sistema.

Dimensões de confiança

- Software Crítico – Software cujas características possuem riscos inerentes a danos físicos, financeiros e pessoais.
- Disponibilidade A capacidade do sistema disponibilizar serviços quando necessário;
  - Tempo Real intervalo <= a 1 segundo
  - On-line intervalo > que 1 segundo
- Confiabilidade A capacidade do sistema disponibilizar serviços conforme especificado;
- Segurança (safety) A capacidade do sistema operar sem falhas catastróficas;
- Proteção (security) A capacidade do sistema se proteger contra invasão acidental ou deliberada.

Dimensões de confiança



Outras propriedades de confiança

- Facilidade de reparo / Repairability
  - Falhas são inevitáveis, mas interrupções devem ser minimizadas.
- Facilidade de manutenção / Maintainability
  - Sistema deve ser adaptado aos novos requisitos;
- Capacidade de sobrevivência / Survivability
  - Capacidade do sistema funcionar mesmo sob ataque. Garantia de que pode fornecer o mínimo dos serviços acordados. Três estratégias para aprimorar sobrevivência: resistência a ataques; reconhecimento de ataque; recuperação de danos causados por ataques
- Tolerância a falhas / Error tolerance
  - Relacionada a usabilidade. Até o onde o sistema foi projetado para evitar erros de entrada dos usuários. Quando ocorrem erros de usuários, o sistema deve detectá-lo, corrigi-lo ou solicitar nova entrada do usuário

Facilidade de manutenção / Maintainability

- Um atributo de sistema com capacidade de reparação de sistema após uma falha ter sido descoberta ou alterando o sistema para incluir novos recursos
- É muito importante para os sistemas críticos como falhas são muitas vezes introduzidas num sistema por causa de problemas de manutenção
- Manutibilidade é diferente das outras dimensões da confiança porque é um atributo de sistema estático e não dinâmico

Sobrevivência / Survivability

- A capacidade de um sistema de continuar a entregar os seus serviços aos usuários após um ataque acidental ou deliberado
- Este é um atributo cada vez mais importante para sistemas distribuídos cuja segurança pode ser comprometida
- Sobrevivência incorpora a noção de resiliência – a capacidade de um sistema para continuar em funcionamento, apesar dos fracassos de componentes

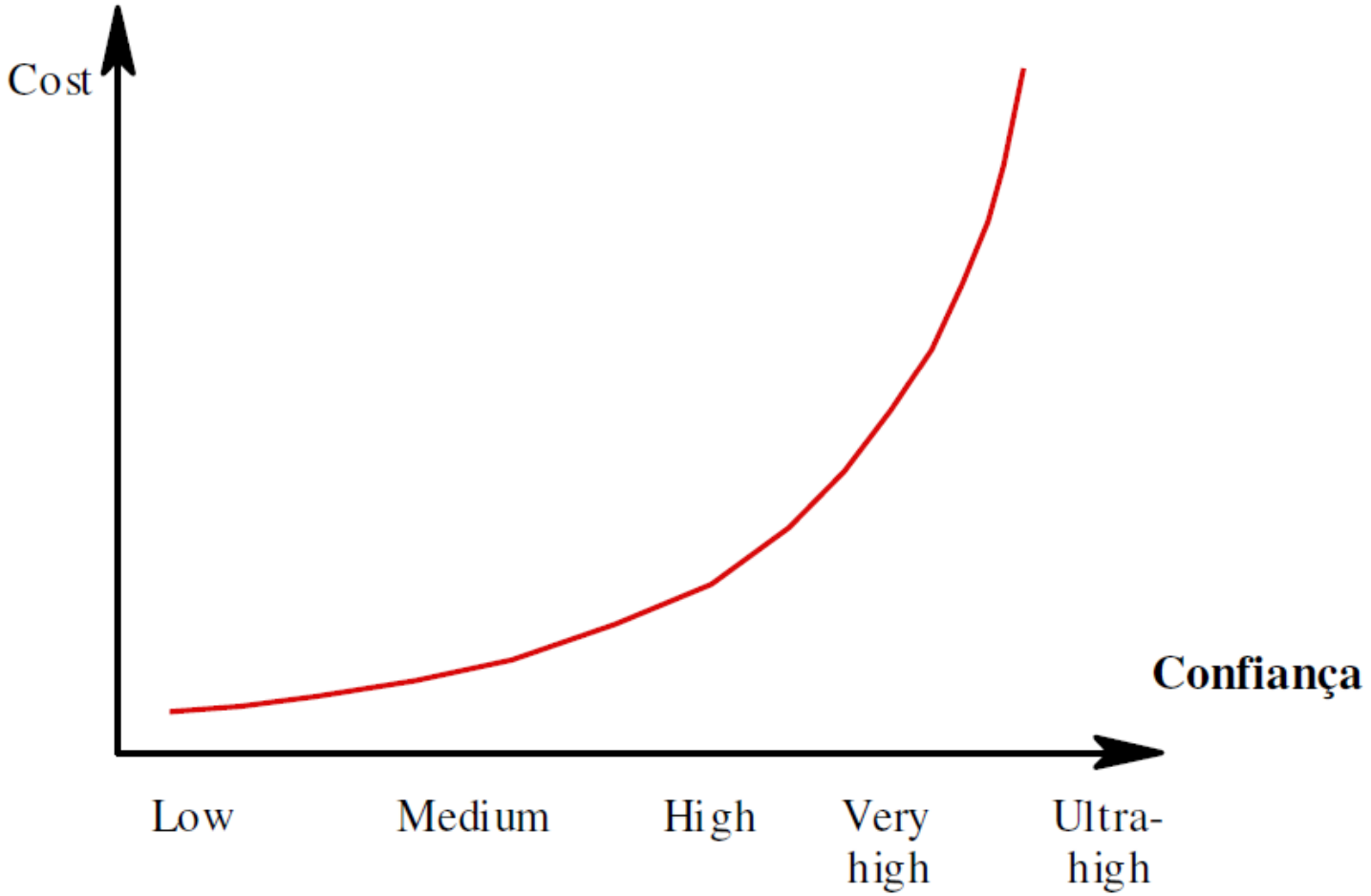
Confiança vs Desempenho

- Os sistemas que não são confiáveis, não apresentam segurança ou são inseguros não são utilizados
- Os custos da falha de um sistema podem ser enormes
- É difícil readequar a confiança
- Freqüentemente, é possível compensar a falta de desempenho do sistema
- Sistemas não confiáveis podem causar a perda de informações

Custos de confiança

- Custos de confiança tendem a aumentar exponencialmente como os níveis de confiança são necessários
- Existem duas razões:
  - O uso de técnicas mais caras desenvolvimento e de hardware que são necessários para atingir os níveis mais elevados de confiabilidade
  - O aumento dos testes e validações de sistema que são necessários para verificar que os níveis de confiabilidade exigidos foram atingidos

Curva de custo/confiança



Disponibilidade e Confiabilidade

- Confiabilidade
  - É a probabilidade de operação livre de falhas durante um tempo especificado, em um dado ambiente, para um propósito específico
- Disponibilidade
  - É a probabilidade de um sistema, em determinado instante, ser operacional e capaz de fornecer os serviços requeridos
- Estes atributos podem ser expressados quantitativamente

Disponibilidade e Confiabilidade

- Sistema A: Falha uma vez por ano, porém a cada falha o sistema demora 3 dias para reiniciar

- Sistema B: Falha 1 vez por mês e cada falha demora 10 minutos para reiniciar o sistema.

Conclusão:

A é mais CONFIÁVEL que B.

B tem mais DISPONIBILIDADE que A.

Disponibilidade e Confiabilidade

- Saber se um sistema é confiável ou não, é uma questão relativa, ou seja, depende do contexto em que está sendo aplicado.
  - Exemplo do carro a 100 Km/h (Convencional e de corrida)
  - Exemplo de limpador em chuva forte (Seatle – clima úmido, pode usar; Las Vegas – clima seco – pode nem usar)

Terminologia da confiabilidade

Termo	Definição
Falha de sistema	Um evento que ocorre em algum momento, quando o sistema não fornece um serviço conforme esperado por seus usuários.
Erro de sistema	Um estado errôneo de sistema que pode levá-lo a um comportamento inesperado pelos seus usuários.
Defeito de sistema	Uma característica do sistema de software que pode levar a um erro de sistema. Por exemplo, a falha em iniciar uma variável pode levar a um valor errado quando esta for usada.
Erro humano ou engano	Comportamento humano que resulta na introdução de defeitos em um sistema.

Falhas e fracassos

- Fracassos são geralmente um resultado de erros de sistema que são derivados de falhas no sistema
- No entanto, falhas não necessariamente resultam em erros no sistema
- Erros não conduzem necessariamente para falhas de sistema

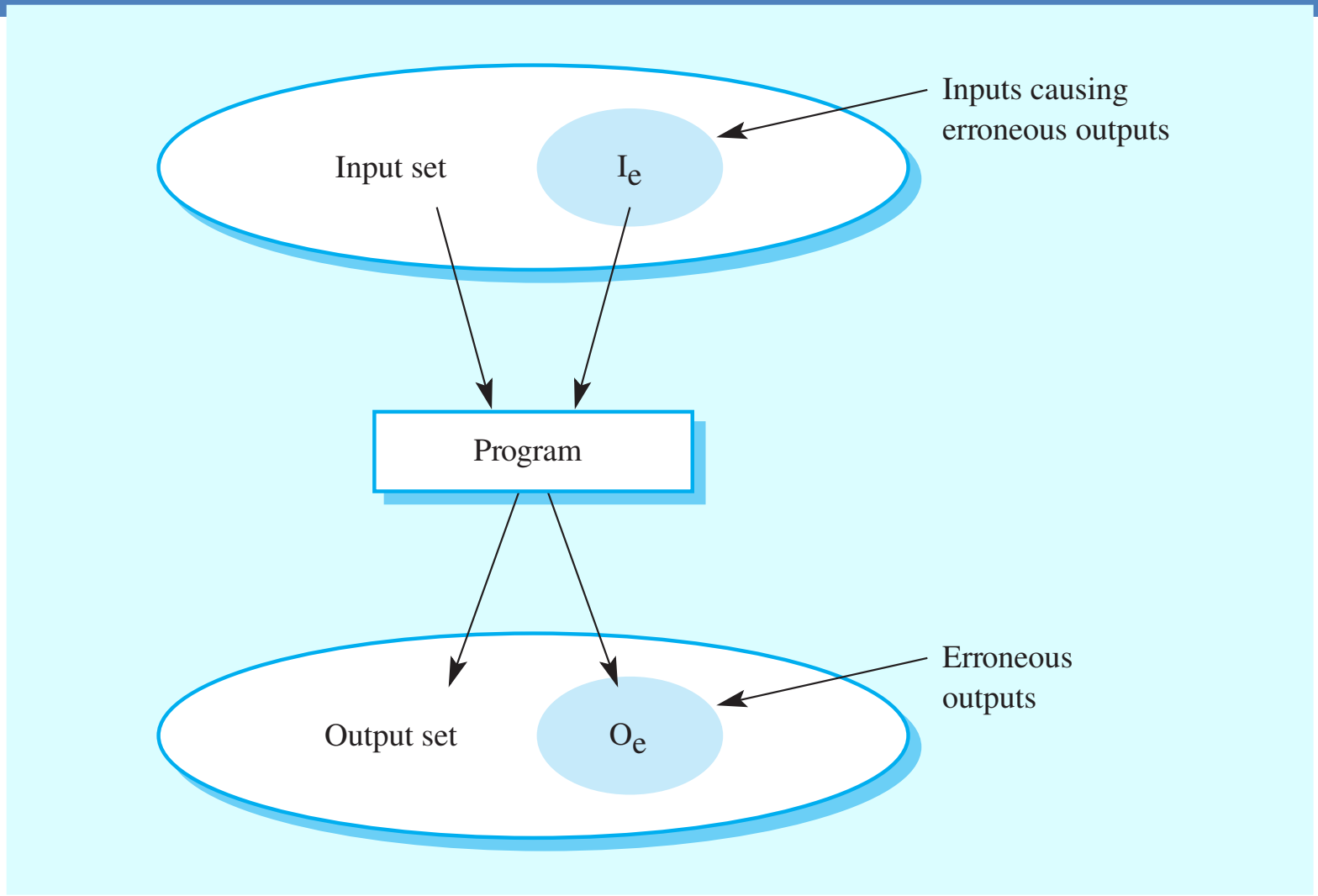
Assegurar a confiabilidade

- Evitar defeitos
  - São utilizadas técnicas de desenvolvimento que minimizam a possibilidade de erros e/ou os captam antes que eles resultem na introdução de defeitos no sistema
- Detecção e exclusão de defeitos
  - Uso de técnicas de verificação e validação, que aumentam as chances de que defeitos sejam detectados e removidos antes que o
- sistema seja utilizado
- Tolerância a defeitos
  - Uso de técnicas que asseguram que os defeitos em um sistema não resultem em erros do sistema ou que assegurem que os erros do sistema não resultem em falhas

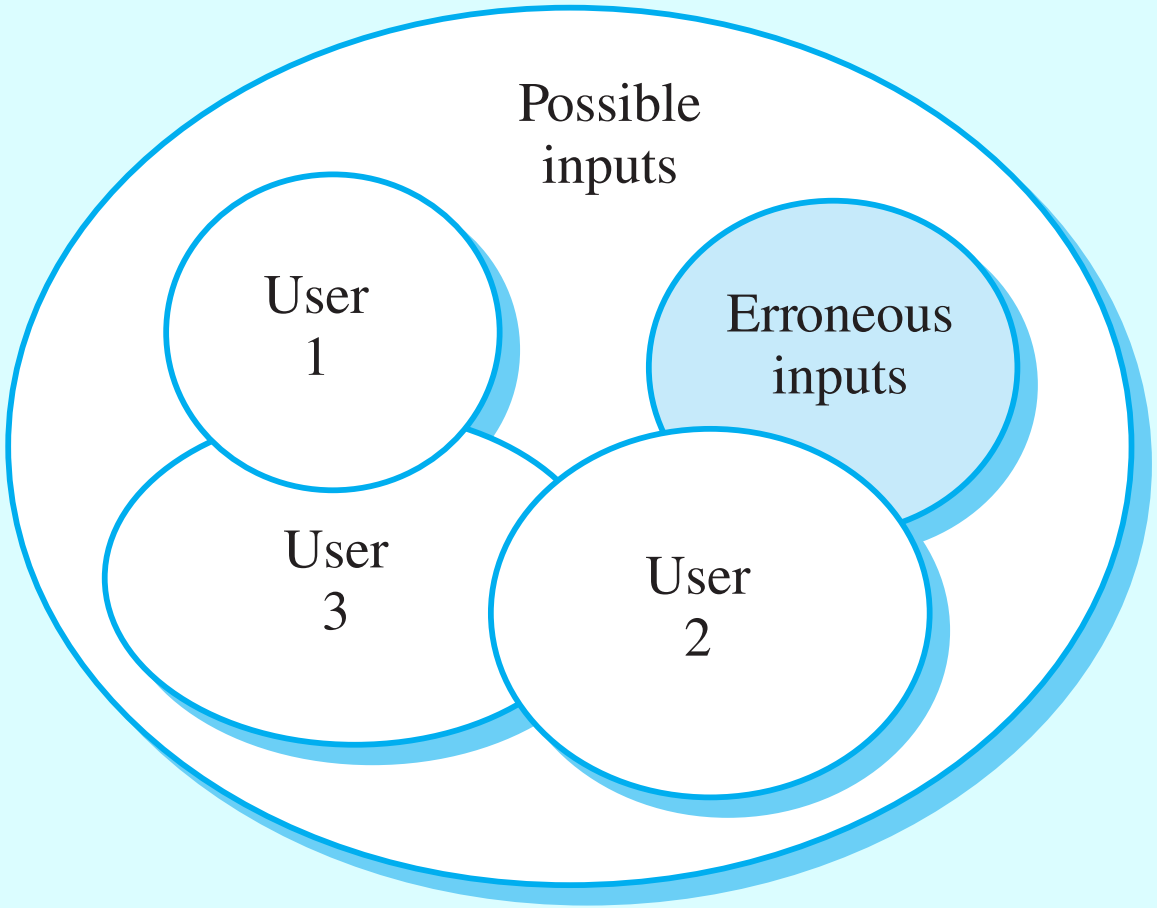
Modelando confiabilidade

- Pode-se modelar um sistema com o mapeamento de entrada/saída onde algumas entradas podem resultar em saídas errôneas
- A confiabilidade do software é a probabilidade de que, em uma execução em particular, a entrada seja membro do conjunto de entradas que provoquem um saída errônea
- Cada usuário de um sistema utiliza-o de diferentes maneiras

Mapeamento de Entrada e Saída



Percepção de confiabilidade



Melhoria da confiabilidade

- Removendo X% de falhas de um sistema não quer dizer que melhorou a confianbilidade em X%. Um estudo da IBM mostrou que removendo 60% de defeitos de um produto o resultado foi de 3% na melhoria da confiança
- Defeitos em programas podem estar em áreas do código que são raramente executadas e podem nunca ser encontrado pelo usuário. Removendo estes defeitos a percepção de confiança não será alterada

Segurança (safety)

- A segurança de um sistema é um atributo que reflete a capacidade do sistema de operar, normal e anormalmente, sem ameaçar as pessoas ou o ambiente
- É cada vez mais importante a considerar como software de segurança cada vez mais incorporam os dispositivos software baseado em sistemas de controle
- Requisitos de segurança são necessidades exclusivas, ou seja, eles excluem situações indesejáveis em vez de especificar o que é exigido pelos serviços de sistema

Softwares críticos de segurança

- Software crítico de segurança primária
  - É um software que é embutido como um controlador em um sistema, a disfunção desse software pode causar um disfunção de hardware, o que resulta em ferimentos em pessoas ou em dano ambiental. Ex.: sistema de aeronave.
- Software crítico de segurança secundária
  - É um software que pode indiretamente resultar em ferimentos. Ex.: Banco de dados com detalhes de medicamentos. Se tiver erros neste sistema, a administração incorreta pode resultar em danos ao paciente

Segurança e confiabilidade

- Segurança e confiabilidade estão relacionadas, mas são distintas
  - Em geral, segurança e confiabilidade são necessárias, mas não são condições suficientes para a segurança de um sistema
- Confiabilidade está relacionada com a conformidade de uma especificação e prestação de serviço
- Segurança está relacionada com a garantia de que o sistema não pode causar danos independentemente de serem ou não conforme a especificação
- Confiabilidade = Qualidade no tempo!
- Segurança (safety) = Qualidade no uso!

Sistemas confiáveis inseguros

- Especificação incompleta, por não descrever o comportamento exigido do sistema em algumas situações críticas. Dificuldades com requisitos constituem a causa principal dos erros de software relacionados com segurança, ainda mais se chegarem a integração.
- Disfunções de hardware podem fazer com que o sistema se comporte de maneira imprevisível e apresentar o software com um ambiente não previsto.
- O operador do sistema pode gerar entradas que não são individualmente incorreta, mas que podem levar a uma disfunção do sistema. Ex. mecânico aciona botão para levantar trem de pouso mas avião está no chão.

Terminologia de segurança

Termo	Definição
Acidente (ou desgraça)	Evento ou seqüência de eventos não planejados que resulta em morte ou ferimento de humanos, danos à propriedade ou ao ambiente. Uma máquina controlada por computador que fere seu operador é um exemplo de um acidente.
Perigo	Condição com potencial para causar ou contribuir para um acidente. A falha de um sensor que detecta um obstáculo em frente de uma máquina é um exemplo de perigo.
Dano	Medida de perda resultante de um acidente. Um dano pode variar desde a morte de várias pessoas como resultado de um acidente até ferimentos de pouca importância ou danos à propriedade.
Severidade do perigo	Avaliação do pior dano possível que poderia resultar de determinado perigo. A severidade do perigo pode variar de catastrófica, na qual várias pessoas são mortas, até somente danos de pouca importância.
Probabilidade de perigos	Probabilidade de ocorrência de eventos que criam um risco. Valores de probabilidade tendem a ser arbitrários, mas variam de provável (digamos, chance de 1/100 de ocorrência de um risco) a implausível (não existem situações concebíveis nas quais o perigo possa ocorrer)
Risco	É a medida da probabilidade de que o sistema causará um acidente. O risco é avaliado considerando-se a probabilidade do perigo, a severidade do perigo e a probabilidade de que o perigo resultará em um acidente.

Assegurar a segurança

- Evitar o perigo
  - O sistema é projetado de modo que os perigos sejam evitados.
- Detectar e eliminar o perigo
  - O sistema é projetado de modo que os perigos sejam detectados e eliminados antes que resultem em acidentes
- Limitar o prejuízo
  - O sistema pode incluir características de proteção que minimizem os danos que podem resultar de um acidente

Acidentes normais

- Acidentes em sistemas complexos raramente têm uma única causa, uma vez que estes sistemas são projetados para serem resistentes a um único ponto de falha
  - Projetar sistemas de tal forma que um único ponto de falha não cause um acidente constitui um princípio fundamental de seguro de projeto de Sistemas
- Quase todos os acidentes são um resultado de combinações de várias coisas que acontecem de errado ao mesmo tempo
- Os sistema controlados por software podem fornecer intertravamentos de segurança sofisticados e aceitar estratégias de controle que reduzem o tempo

Proteção (security)

- A proteção de um sistema é uma avaliação do ponto em que o sistema protege a si mesmo de ataques externos, que podem ser acidentais ou deliberados
- A proteção é importante para todos os sistemas críticos, onde os ataques externos podem provocar danos ao sistema
- A proteção é um pré-requisito essencial para disponibilidade, confiabilidade e segurança

Proteção fundamental

- Se um sistema foi comprometido de alguma maneira, então os argumentos para confiabilidade e segurança não podem ser sustentados
- O software de sistema pode ser corrompido e se comportar de maneira imprevisível
- Se um sistema não responde a entradas inesperadas ou se seus limites não são verificados, então os atacantes podem explorar essas fraquezas, a fim de obter acesso ao sistema

Terminologia de proteção

Termo	Definição
Exposição	Possível perda ou dano no sistema computacional. Pode ser perda ou danos nos dados ou pode ser perda de tempo ou esforço, se a recuperação é necessária após uma brecha na proteção.
Vulnerabilidade	Uma fraqueza no sistema baseado em computador que pode ser explorada para causar perda ou dano.
Ataque	Uma exploração da vulnerabilidade do sistema. Geralmente parte de fora do sistema e é uma tentativa deliberada para causar algum dano.
Ameaças	Circunstâncias que têm potencial para causar perda ou dano. Você pode pensar nelas como uma vulnerabilidade do sistema que está sujeita a um ataque.
Controle	Uma medida de proteção que reduz uma vulnerabilidade do sistema. Criptografia pode ser um exemplo de controle que reduz a vulnerabilidade de um sistema fraco de controle de acesso

Danos por falta de proteção

- Interrupção de serviço (Denial of Service)
  - O sistema pode ser forçado a um estado em que seus serviços normais se tornem indisponíveis
- Corrupção de programas ou dados
  - Os componentes de software de sistemas podem ser alterados sem autorização
- Revelação de informações confidenciais
  - Informações gerenciadas pelo sistema podem ser expostas a pessoas não autorizadas

Assegurar a proteção

- Evitar a vulnerabilidade
  - O sistema é projetado de modo que vulnerabilidades não ocorram. Por exemplo, se não existir uma conexão de rede externa então um ataque externo é impossível
- Detectar e neutralizar ataques
  - O sistema é projetado para detectar vulnerabilidades e removê-las antes que resultem em uma exposição. Por exemplo, um verificador de vírus que analisa arquivos recebidos a fim de remover os possíveis vírus
- Limitar a exposição
  - O sistema é projetado para que as conseqüências de um ataque bem sucedido sejam minimizadas. Por exemplo, uma política de backup que permita que informações danificadas sejam restauradas.

Pontos-chave

- A confiança em um sistema reflete o grau de confiança do usuário no sistema
- A disponibilidade de um sistema é a probabilidade de que ele será capaz de prestar serviços quando for necessário
- A confiabilidade é a probabilidade de que os serviços do sistema sejam prestados conforme especificado
- A confiabilidade e a disponibilidade são geralmente as mais importantes, mas não são condições suficientes para assegurar
- segurança (safety) ou proteção (security)

Pontos-chave

- A confiabilidade está relacionada à probabilidade de um erro ocorrer durante o uso operacional. Um sistema com erros conhecidos pode ser confiável
- A segurança (safety) de um sistema é um atributo, que reflete a capacidade de o sistema operar sem ameaçar as pessoas ou a ambiente
- A proteção (security) de um sistema é um atributo, que reflete a capacidade do sistema se proteger em caso de ataques externos