



Instituto Federal de Educação, Ciência e Tecnologia da Bahia - IFBA  
Departamento de Ciência da Computação  
Tecnólogo em Análise e Desenvolvimento de Sistemas

# Falhas em sistemas sociotécnicos

André L. R. Madureira <[andre.madureira@ifba.edu.br](mailto:andre.madureira@ifba.edu.br)>  
Doutorando em Ciência da Computação (UFBA)  
Mestre em Ciência da Computação (UFBA)  
Engenheiro da Computação (UFBA)

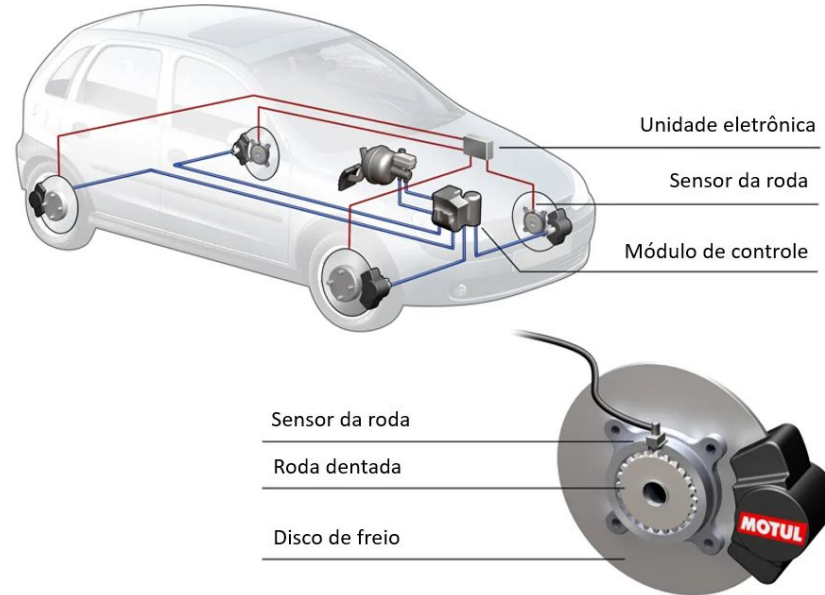
# O que é um sistema sociotécnico?

---

- **Sistema sociotécnico:** hardware + software + elementos não técnicos
  - O hardware sozinho não faz nada
  - De forma parecida, o software sem hardware não executa
  - Pessoas interpretam dados gerados pelo hardware+software
    - Pessoas são o elo criativo, criando conhecimento a partir de dados brutos
  - **Exemplo de elementos não técnicos:** pessoas, processos, regulamentos, documentações

# Complexidade de sistemas sociotécnicos

- Esses sistemas são complexos de entender como um todo
  - Há muitos elementos interagindo simultaneamente



# Complexidade de sistemas sociotécnicos

---

- **Solução:** dividir o sistema em camadas:
  - **Equipamentos:** dispositivos de hardware
  - **Sistema operacional:** interage com o hardware
  - **Comunicações e gerenciamento de dados (*middleware*):** interface que permite interação entre aplicações e o sistema operacional
  - **Aplicação:** funcionalidade específica da aplicação
  - **Processos de negócio:** processos do negócio da organização que usa o sistema
  - **Organizacional:** processos de alto nível estratégico (regras de negócio, políticas e normas)
  - **Social:** leis e os regulamentos da sociedade que governam o funcionamento do sistema

Normalmente, cada camada interage com a camada subjacente (quando isso não ocorre, podemos ter problemas)

# Sistemas sociotécnicos

- É preciso pensar no sistema como um todo (visão holística)
  - Software interage com o hardware, que interage com o mundo físico
  - Se essa interação for incorreta, problemas fatalmente irão ocorrer
  - **Ex:** Therac-25 (falha de software de aparelho de raio-X, que levou a administração de doses fatais de radiação em pacientes)



# Evitando falhas em sistemas sociotécnicos

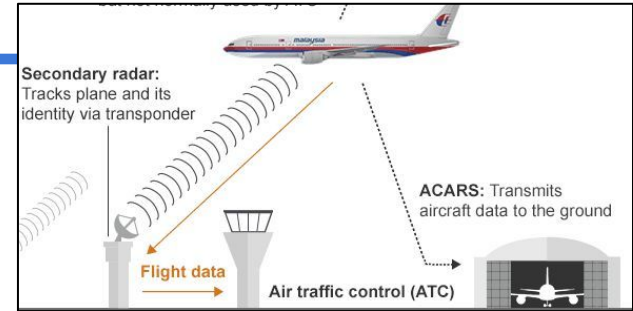
---

- Precisamos analisar a forma como o software interage com seu ambiente imediato para nos assegurarmos que:
  - Falhas do software não devem afetar gravemente o funcionamento de outras camadas do sistema
    - *“Falhas de software não devem ocasionar a falha do sistema”*
  - Devemos entender como defeitos e falhas de outras camadas, que não são software, afetam o funcionamento do programa
    - *“Como as verificações podem ser incorporadas ao software para ajudar a detectar e recuperar essas falhas”*

# Evitando falhas em sistemas sociotécnicos

- **Ex:** radar com fantasmas na imagem

- Colocaram um radar em um local onde há muita interferência eletromagnética
- **Problema:** A interferência dificulta a criação de imagens nítidas
- **Solução:** corrigir o problema em software, retirando os fantasmas no pós-processamento da imagem



O problema é do software, ou do projeto do sistema?

- **Porque?**

- Software é flexível (é mais fácil ajustar no software que mover o radar para outro local)

- **Consequencia:** Software se torna lento demais

# Evitando falhas em sistemas sociotécnicos

---

- Muitas vezes, as “falhas de software” não são consequência de problemas inerentes ao software
  - Elas são resultados da tentativa de mudar o software para acomodar os requisitos de um sistema complexo
  - **Ex:** fantasmas na imagem do radar (interferencias)
  - **Ex:** sistema de bagagem do aeroporto de Denver
    - Esteira tinha um problema e queria que o software resolvesse isso!



# Exercício

Considerando os escopo de falhas em sistemas, marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Um sistema sociotecnico é composto por software, hardware, pessoas, processos e documentações. **V**

II - Para gerenciar a alta complexidade de sistemas sociotecnicos, os mesmos são divididos em camadas. **V**

III - Cada camada de um sistema sociotecnico interage com a camada subjacente. **V**

IV - Um sistema deve ser visto como um todo (visão holística) a fim de evitar interações incorretas e problemas potencialmente fatais. **V**

 ☐ Todas as assertivas são verdadeiras.

☐ Somente II e III.

☐ Somente II e IV.

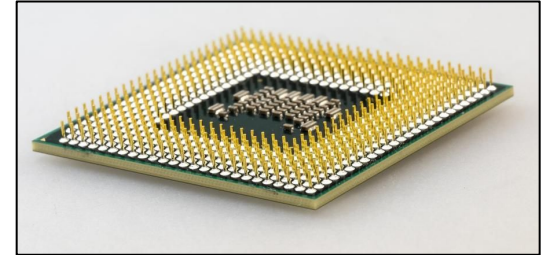
☐ Somente I e IV.

☐ Somente I e III.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

# Afinal, o que é um sistema sociotécnico?

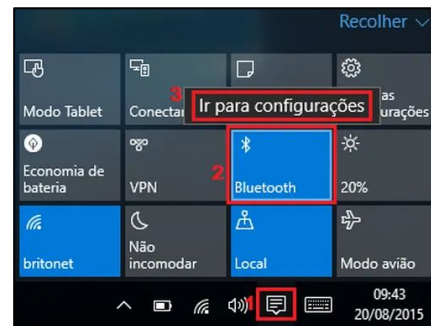
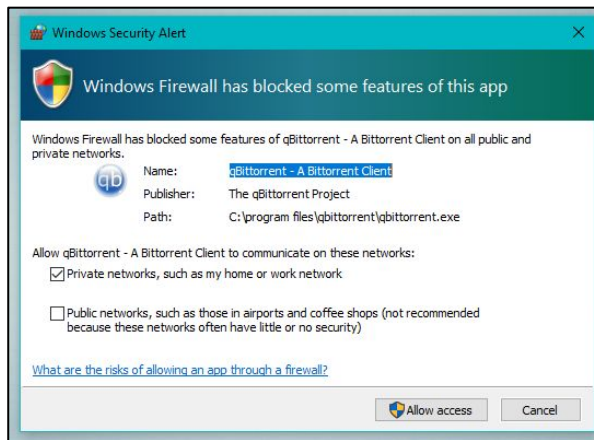
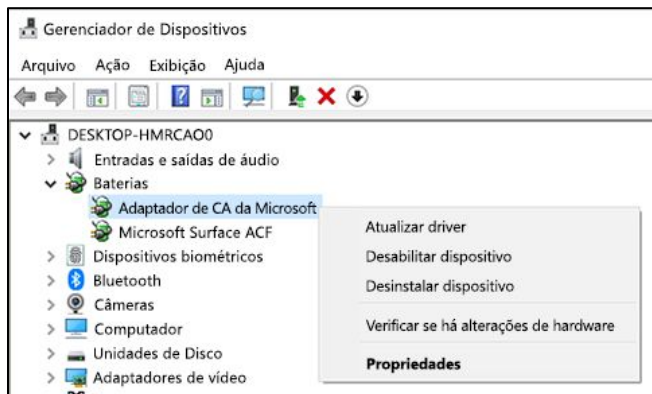
- **Sistema:** *“é uma coleção intencional de componentes inter-relacionados, de diferentes tipos, que funcionam em conjunto para atingir um objetivo”* (SOMMERVILLE, 2003)
  - O bom funcionamento de cada componente do sistema depende do funcionamento de outros componentes



- **Engenharia de sistemas:** processo de projeto de sistemas completos, não apenas o software desses sistemas

# Sistemas e subsistemas

- Um sistema pode ser composto por vários sub-sistemas integrados
  - **Ex:** Windows (stack de rede TCP/IP + drivers de hardware + firewall + anti-virus + navegador de internet + ... )



# Características de Sistemas Sociotécnicos

---

- Sistemas sociotécnicos possuem características importantes para proteção e confiança do sistema:
  - Possuem **propriedades emergentes**
  - São **sistemas não determinísticos**
  - Há **independência entre os objetivos organizacionais e o sistema**




# Propriedades emergentes

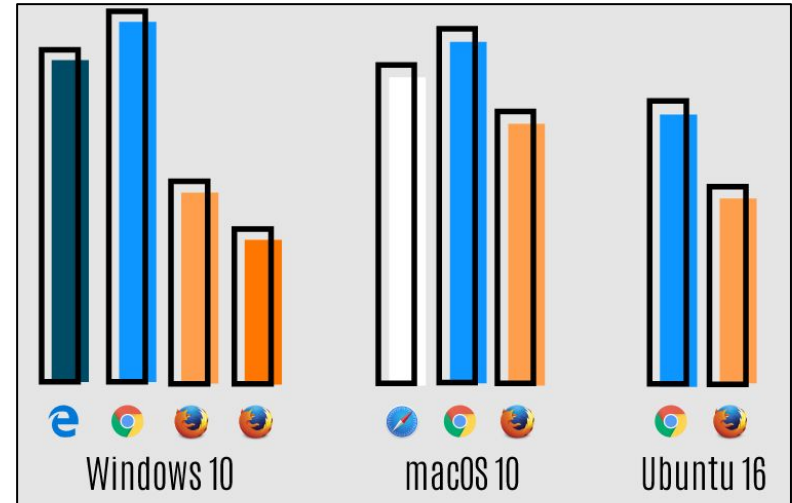
---

- São propriedades do sistema como um todo, e não associadas apenas a partes individuais do sistema
  - Dependem tanto dos componentes do sistema quanto dos relacionamentos entre eles
  - Só podem ser avaliadas uma vez que o **sistema tenha sido montado**
    - Essas propriedades só surgem quando os componentes do sistema são **integrados**
  - **Ex:** Proteção, confiança, desempenho

# Exemplo de Propriedades emergentes

- **O uso de memória** de navegadores de internet é uma propriedade de um sistema emergente
  - O uso de memória depende não somente do navegador, mas também do sistema operacional

			
	Google Chrome	Microsoft Edge	Mozilla Firefox
10 tabs	952MB	873MB	956MB
20 tabs	1.8GB	1.4GB	1.6GB
60 tabs	3.7GB	2.9GB	3.9GB



# Classificação de Propriedades emergentes

---

- **Propriedades emergentes funcionais:** finalidade do sistema só surge após seus componentes serem integrados
  - **Ex:** bicicleta tem a propriedade funcional de meio de transporte
- **Propriedades emergentes não funcionais:** se relacionam com o comportamento do sistema em seu ambiente operacional
  - **Ex:** segurança, privacidade, desempenho
  - A falha em alcançar um nível mínimo definido nessas propriedades faz com que o sistema se torne inútil
    - **Ex:** *“Ninguém deseja ter um smartphone inseguro ou lento”*

# Exemplos de Propriedades emergentes

---

Propriedade	Descrição
Volume	O volume de um sistema (o espaço total ocupado) varia conforme os conjuntos de componentes estão dispostos e conectados.
Confiabilidade	A confiabilidade de sistema depende da confiabilidade de componentes, mas interações inesperadas podem causar novos tipos de falhas e, portanto, afetar a confiabilidade do sistema.
Proteção	A proteção do sistema (sua capacidade de resistir ao ataque) é uma propriedade complexa que não pode ser facilmente mensurada. Os ataques podem ser criados de forma imprevista pelos projetistas de sistemas e, assim, derrotar as proteções internas.
Reparabilidade	Essa propriedade reflete quão fácil é corrigir um problema com o sistema uma vez que este tenha sido descoberto. Depende da capacidade de diagnosticar o problema e do acesso a componentes que estejam com defeito, bem como de se modificar ou substituir tais componentes.
Usabilidade	Essa propriedade reflete quão fácil é usar o sistema. Depende dos componentes técnicos de sistema, seus operadores e seu ambiente operacional.



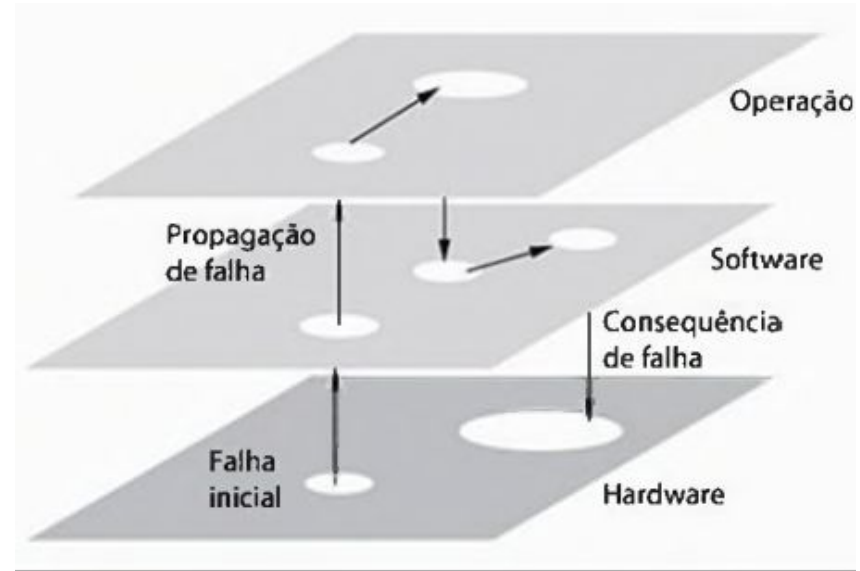
# Confiabilidade

As falhas podem ser propagadas entre níveis diferentes (hardware, software, operador)

- Podemos analisar a confiabilidade sob três níveis (perspectivas):
  - **Confiabilidade de hardware:** probabilidade de falha de hardware
    - **Ex:** memória RAM com defeito
  - **Confiabilidade de software:** probabilidade de falha de software
    - **Ex:** calculadora calculando operações matemáticas erradas
  - **Confiabilidade de operador:** probabilidade de falha humana
    - **Ex:** entrada incorreta em um sistema
    - *“Qual é a probabilidade de o software não detectar esse erro e o propagar?”*

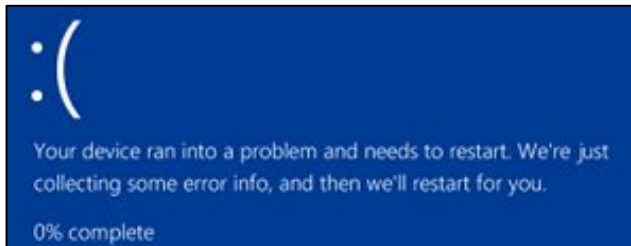
# Propagação de falhas

A falha surgiu no hardware, mas afetou o software. Este por sua vez interferiu com o trabalho do operador, o induzindo ao erro também



# Sistemas não determinísticos

- Sistemas sociotécnicos são não determinísticos
  - Quando apresentados a uma entrada específica, o sistema nem sempre produz a mesma saída
    - *“Comportamento do sistema depende de pessoas, e seres humanos nem sempre reagem da mesma maneira”*
  - Além disso, existem defeitos e falhas de sistema transitórios



# Sistemas não determinísticos

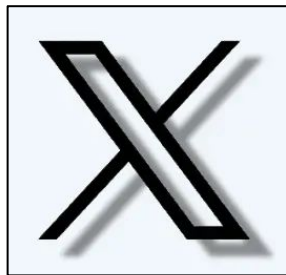
- **Ex:** um chefe pede que um atendente de loja de roupas insira algumas camisetas novas no sistema
  - O atendente pode estar chateado naquele determinado dia e inserir a quantidade de roupas errada no sistema (sem intenção ou propositalmente)



# Independência entre objetivos organizacionais e sistema sociotécnico

---

- O sistema apoia os objetivos organizacionais, mas eles podem mudar a qualquer momento, por várias razões diferentes
  - **Ex:** um novo gerente pode mudar os objetivos organizacionais, fazendo um sistema “bem-sucedido” parecer “fracassado”
- O sistema precisa se adaptar aos objetivos organizacionais o tempo inteiro



Elon Musk achou que havia algo de errado com o Twitter

Então ele mudou a proposta (objetivos) do sistema.

# Exercício

Considerando os escopo de falhas em sistemas, marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Sistemas sociotécnicos possuem propriedades emergentes, que surgem somente quando os componentes do sistema são integrados. **V**

II - Propriedades emergentes podem ser classificadas como funcionais ou não-funcionais. A falha em alcançar uma propriedade emergente não-funcional torna o sistema inútil. **V**

III - A confiabilidade é uma propriedade não-funcional, pois ela depende do comportamento dos componentes do sistema. **V**

IV - A usabilidade é uma propriedade não-funcional. Ela reflete a facilidade no uso do sistema. **V**

 ☒ Todas as assertivas são verdadeiras.

☐ Somente II, III e IV.

☐ Somente II e IV.

☐ Somente III e IV.

☐ Nenhuma das alternativas anteriores.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

# Engenharia de sistemas

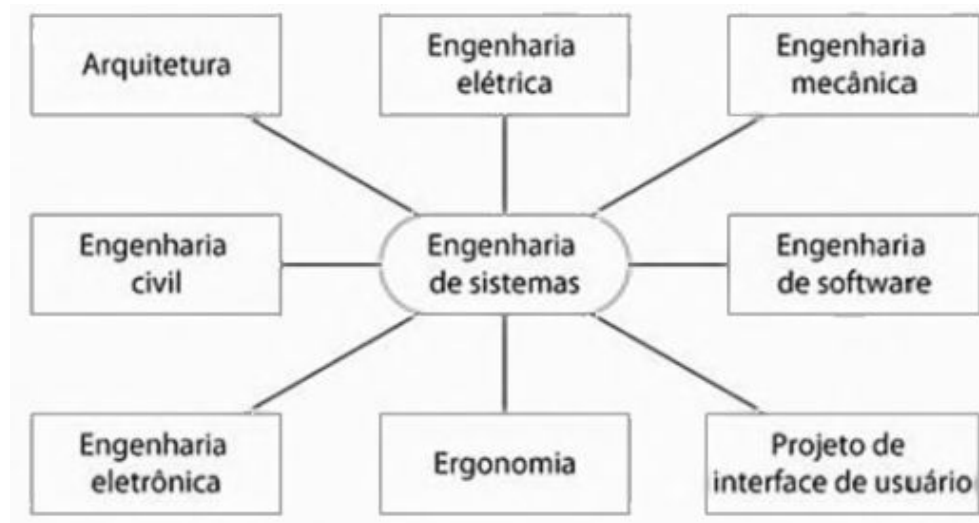
---

- Engloba as atividades envolvidas na aquisição, especificação, projeto, implementação, validação, implantação, operação e manutenção dos sistemas sociotécnicos
  - Preocupação com o bom funcionamento do software + hardware + interações com os usuários + ambiente de operação do sistema
  - *“Que serviços o sistema oferece?”*
  - *“Quais as restrições do sistema? (desempenho, segurança, etc)”*
  - *“De que maneiras o sistema será usado?”*

# Engenharia de sistemas

---

- Envolve uma ampla gama de profissionais trabalhando em conjunto





# Estágios da Engenharia de sistemas

---

- **Obtenção ou aquisição:** define os objetivos e requisitos de alto nível do sistema ; compra dos componentes do sistema
- **Desenvolvimento:** o sistema é desenvolvido (projeto, implementação, e testes) e cursos de treinamento para usuários são projetados
- **Operação:** o sistema é colocado em uso (implantado) e os usuários são treinados

A qualquer momento erros podem ocorrer, comprometendo a proteção e a confiança do sistema

Por isso, os estágios não são independentes.  
Podemos precisar retornar a um estágio ou outro, a qualquer momento.

# Aquisição do sistema

---

- Ênfase na **tomada de decisões** com relação ao sistema, como por exemplo:
  - Orçamentos
  - Fornecedores de componentes
  - Tipo de sistema requerido
  - Requisitos de alto nível de sistema
  - Cronograma de desenvolvimento sistema

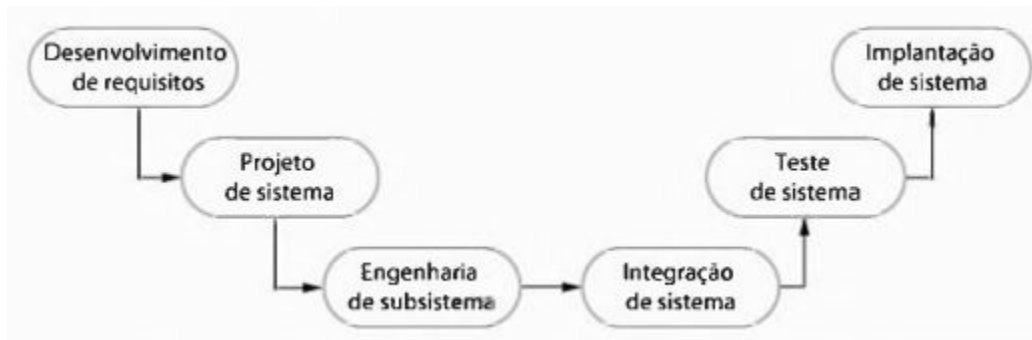
# Exemplo de processo de Aquisição de sistema



# Desenvolvimento de sistemas

---

- Envolve:
  - Desenvolver ou adquirir todos os componentes do sistema
  - Integrar esses componentes para criar um sistema final
- Os requisitos são a ponte entre os processos de aquisição e de desenvolvimento



# Operação de sistemas

---

- São os processos envolvidos no uso do sistema para seus fins definidos
  - **Ex:** *“que atividades precisam ser realizadas por um operador de controle de tráfego aérea para permitir a decolagem de um avião?”*
    - *Definir a altura, rota, velocidade, ...*
- Processos operacionais são definidos e documentados durante o processo de desenvolvimento do sistema

# Operação de sistemas

---

- Esta etapa permite detectar erros que passaram “batido” pelas demais etapas do desenvolvimento de sistemas, tais como:
  - Erros na especificação
  - Funcionalidade faltando no sistema
  - Funcionalidade com defeito ou inadequada
- Processos de operação devem ser flexíveis e adaptáveis
  - **Porque?**

# Flexibilidade de Processos de Operação

---

- Processos de operação devem ser flexíveis e adaptáveis
  - Não devem exigir que determinadas operações sejam realizadas, nem deve determinar a ordem de execução delas
- **Os operadores podem recuperar o controle de uma falha no sistema,** mesmo que isso viole os processos de operação do sistema
  - As pessoas têm a capacidade única de responder eficazmente a situações inesperadas, mesmo sem ter experienciado elas antes
    - **Ex:** Se o sistema de vendas da loja travar, o operador pode realizar a venda usando um recibo escrito a mão

# Erros humanos

---

- Sempre que pessoas estão envolvidas em um processo, há a possibilidade de erro humano. Podemos enxergar esses erros como:
  - **Responsabilidade do indivíduo:** falta de cuidado individual ou do comportamento imprudente do operador
    - **Solução:** sanções disciplinares, procedimentos mais rigorosos, reciclagem (demissão)
  - **Responsabilidade do sistema:** erros como consequência de decisões de projeto de sistema ou fatores organizacionais
    - **Solução:** os sistemas devem incluir **barreiras e salvaguardas** para evitar erros humanos



# Exemplo de barreiras e salvaguardas em sistemas

- **Ex:** exigir que dois operadores autorizem o lançamento de um foguete, girando duas chaves simultaneamente



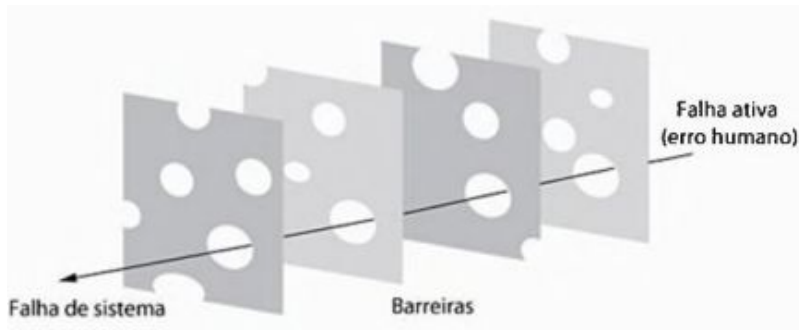
Toda defesa do sistema (barreira, salvaguarda, etc) possui limitações (**condições latentes**).

**Ex:** operadores podem ser rendidos por um terrorista e forçados a realizar o lançamento

# Condições latentes

Devemos reduzir ao máximo a quantidade de condições latentes (*“buracos”*) do sistema

- Levam à falha do sistema quando as defesas construídas não interceptam uma falha ativa de um operador de sistema
- Erro humano é um gatilho, mas não é o único motivo da falha ter ocorrido
  - *“Cada defesa do sistema é uma camada (‘fatias de um queijo suíço’)”*
  - *“Quando os buracos de cada camada se alinham, a falha acontece”*



A posição dos “buracos” de cada camada mudam conforme o estado do sistema

**Ex:** iniciando uma venda, cliente fazendo o pagamento, emissão de recibo, ...

# Exercício

Considerando os escopo de falhas em sistemas, marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os estágios da engenharia de sistemas **são independentes** uns dos outros. **F**

II - Os requisitos do sistema são **definidos no estágio de desenvolvimento** do sistema. **F**

III - Os processos operacionais são **definidos no estágio de operação** dos sistemas. **F**

IV - A aquisição de sistema é o estágio da engenharia de sistemas responsável por avaliar se existe **um sistemas customizado** que pode ser adaptado para atender aos requisitos de negócio da organização. **F**

☐ Somente III.

☐ Somente III e IV.

☐ Somente I, III e IV.

☐ Somente II e III.

☒ Nenhuma das alternativas anteriores.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

I - Os estágios da engenharia de sistemas **NÃO** são independentes uns dos outros, pois podemos precisar retornar a um estágio ou outro, a qualquer momento, para corrigir erros que venham a surgir.

II - Os requisitos do sistema são definidos no estágio de AQUISIÇÃO do sistema.

III - Os processos operacionais são definidos no estágio de DESENVOLVIMENTO do sistema.

IV - A aquisição de sistema é o estágio da engenharia de sistemas responsável por avaliar se existe um sistemas DE PRATELEIRA que pode ser adaptado para atender aos requisitos de negócio da organização.

# Referencial Bibliográfico

---

- SOMMERVILLE, Ian. **Engenharia de Software**. 6. ed. São Paulo: Addison-Wesley, 2003.
- PRESSMAN, Roger S. **Engenharia de Software**. São Paulo: Makron Books, 1995.
- JUNIOR, H. E. **Engenharia de Software na Prática**. Novatec, 2010.

# Obrigado!

- Perguntas?

