Introdução A Engenharia de Confiabilidade e Análise de Risco

1. Porque Estudar Confiabilidade?

- Equipamentos falham
- Sistemas e componentes não são perfeitos
- O que seria um sistema perfeito?
  - Sistema perfeito é aquele que sempre se mantém operacional e atinge os objetivos sem a ocorrência de falha durante a sua vida útil
- Na prática isto não acontece!
- Sistema perfeito é inviável:
  - Economicamente
  - Tecnologicamente

> ☞ O Nosso Conhecimento É Limitado!

- Exemplos de falhas em equipamentos do dia a dia:
  - Máquina de lavar:
    - Causa: falha devido ao desgaste "normal" de componentes
  - Tostador elétrico pegou fogo:
    - Causa: projeto ineficiente da tomada do mesmo dada a quantidade de corrente passando na tomada
  - Controle remoto parou de funcionar:
    - Causa: falha "aleatória" de um componente eletrônico do controle remoto
- Exemplos de falhas mais significantes: maior impacto econômico e social
  - Em 1946 a totalidade da frota do Lockheed Constellation foi retida após acidente com uma das aeronaves matando quatro dos cinco tripulantes
    - Causa: falha no projeto dos condutores elétricos que levaram a fuselagem pegar fogo
  - Em 1979 a turbina esquerda de um DC-10 partiu-se, descolou-se da fuselagem durante a decolagem matando 271 pessoas (tripulação e passageiros)
    - Causa: procedimentos de manutenção inadequados, os quais introduziam estresses excessivos nos pinos de sustentação

quando da remoção da turbina

- Acidente na usina nuclear Three Mile Island nos EUA em 1979 que resultou na destruição parcial do reator nuclear liberando radioatividade
  - Causas: Falha mecânica e erro humano.
    - Quando o sistema backup de resfriamento estava em manutenção, ar cortou o fluxo de água de resfriamento para o reator
    - Luzes dos alarmes estavam encobertas por tags de manutenção
    - A PSV falhou fechada
    - Operadores estavam lendo instrumentos que não operavam adequadamente ou estavam tomando decisões errôneas baseando-se nos instrumentos operacionais
- Explosão da nave espacial Challenger em 1986
  - Causas:
    - Falha dos anéis de borracha (chamados "o-rings") usados para vedar as quatro estações dos foguetes booster (externos)
    - Lançamento efetuado em temperatura ambiental abaixo de zero. Nunca feito antes!

- A partir desses exemplos, pode-se concluir que o impacto de falhas em produtos ou equipamentos variam desde meras inconveniências até lesões em pessoas, grandes percas econômicas, e morte.
- Em geral, as causas dessas falhas incluem:
  - Projeto inadequado
  - Erro humano
  - Procedimentos de construção ou produção faltosos
  - Manutenção inadequada
  - Procedimentos de teste e inspeção inapropriados
  - Inexistência de proteções (barreiras ou salva-guardas) contra estresses ambientais excessivos
- Assim, a importância e o interesse crescentes em confiabilidade tem sido motivado por diversos fatores como por exemplo:
  - Aumento da complexidade e sofisticação dos sistemas
  - Conscientização do consumidor, e posterior exigência, com relação a importância da qualidade do produto

- Surgimento de leis e regulamentações estabelecendo responsabilidade do fabricante com relação ao seu produto
- Pressões econômicas resultantes de altos custos das falhas, reparos e programas de garantia

- Uma pesquisa conduzida pelo instituto Gallup em 1985 encomendada pela American Society for Quality Control (ASQC) entrevistou mais de 1000 pessoas perguntando quais seriam os atributos mais importantes para estes na escolha de um produto:
  - Os valores médios dos 10 atributos mais importantes estão listados a seguir em uma escala de 1 (menos importante) até 10 (mais importante)

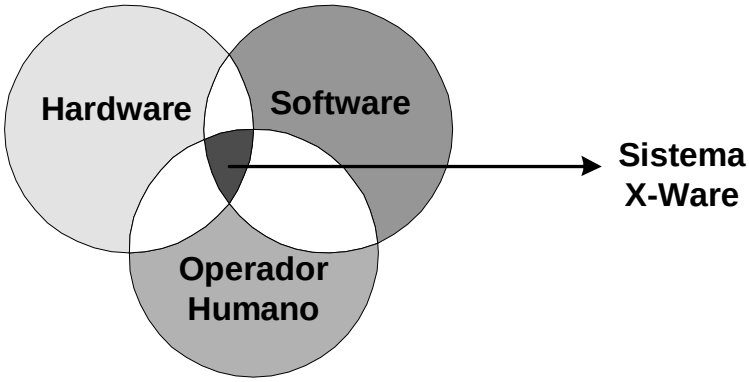
Atributo	Valor Médio
Desempenho	9.5
Longo tempo de duração (Confiabilidade)	**9.0**
Serviço	8.9
Facilidade de reparo (Manutenibilidade)	**8.8**
Garantia	8.4
Facilidade de uso	8.3
Aparência	7.7
Marca	6.3
Embalagem	5.8
Último modelo	5.4
Fonte: Quality Progress, vol. 18, pp. 12-17, 1985	

  - Confiabilidade e manutenibilidade estão classificados entre os mais importantes atributos de um produto segundo os consumidores.

2. Os Domínios da Confiabilidade

- Sistemas tem aumentado em complexidade levando ao surgimento de sistemas onde não há apenas o hardware, mas também software e operadores humanos
- Logo, muitas falhas de equipamentos não são apenas falhas de hardware
- Falhas podem surgir de problemas de software ou erros humanos assim como a partir de falhas no hardware
- Tem-se, então, os chamados *Sistemas X-Ware*:

- Sistemas constituídos de elementos interativos de hardware, software, e operadores humanos (veja a seguinte figura)
- Exemplos:



  - Equipamentos médicos
  - Cockpit de aviões
  - Automóveis
  - Salas de controle em processo petroquímicos
- Falhas podem surgir devido a um desses elementos isoladamente ou a partir da combinação/interação de harware, software e operadores humanos
- As falhas em sistemas x-ware são geralmente dinâmicas, ou seja, um evento iniciador resulta em uma seqüência de eventos levando a falha do sistema como um todo
- Falhas do sistema x-ware podem também ocorrer mesmo quando cada um dos elementos de hardare, software, e operador humano estão funcionando dentro das condições especificadas para cada um destes. Porém, a falha do sistema x-ware resulta da interação simultânea destes três elementos. Cada elemento não está falho, porém o sistema x-ware falha resultante da interação de seus elementos (software, hardware, operador humano).

- Assim, a confiabilidade atua não só em hardware, mas também tem-se a confiabilidade humana e confiabilidade de software
- Confiabilidade humana:
  - Inicialmente, provia-se apenas diretrizes com relação a:
    - Tamanho e tipo de letras em instrumentos
    - Escolha de cores para alarmes
    - Escolha da forma e textura dos “knobs” de controle, etc

- Recentemente, tem-se intensa atividade de pesquisa sobre taxas de erros humanos baseados em fatores físicos e ambientais

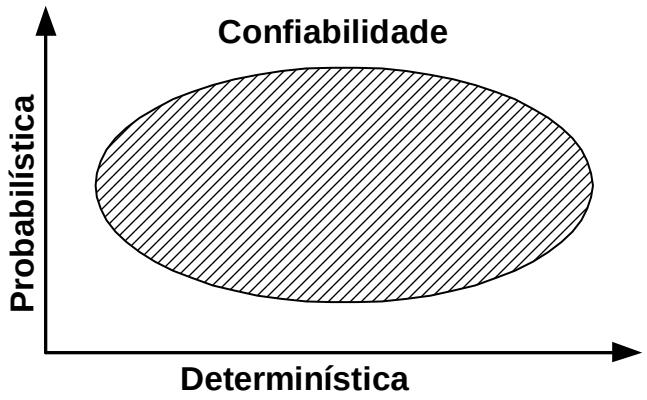
- Confiabilidade de software
  - Tem-se usado técnicas de confiabilidade de hardware
  - Porém, falhas em software são intrinsecamente distintas das falhas em hardware. Por exemplo, uma vez detectadas, as falhas em softwares são erradicadas e as mesmas não voltam a ocorrer
  - Assim, intensa atividade de pesquisa ocorre no desenvolvimento de novas metodologias para a análise da confiabilidade em softwares

3. Dimensões da Confiabilidade

- Em princípio, tendo-se o conhecimento total dos processos químicos, físicos e até biológicos através dos quais falhas se desenvolvem, poderia-se descrever exatamente o que iria acontecer com um sistema e predizer exatamente quando o mesmo iria falhar
- Esta é a dimensão (visão) determinística da confiabilidade:
  - Poderíamos seguir este procedimento "ideal" de tal forma que com um conhecimento total do sistema podemos *garantir* que um dado equipamento irá operar sem falhas por pelo menos um período mínimo de tempo (ou número de ciclos)
- Na prática, porém:
  - Nós não temos um entendimento perfeito de ciência e engenharia
  - Mais importante, nós não temos os recursos ($) para realizar uma análise completa do sistema até o seu nível mais elementar (nível atômico)

☞ Simplesmente As Incertezas São Muito Grandes!

- Logo temos que ser capazes de operar com um conhecimento menos que perfeito:
  - Trabalhamos com uma *garantia menos que perfeita* que um equipamento será capaz operar sem falhas.
- Esta é a dimensão (visão) probabilística da confiabilidade:
  - Por exemplo, nós podemos assegurar que é 99% provável que o nosso equipamento irá operar sem falhas por um certo tempo (ou número de ciclos).



4. Definição de Confiabilidade (*Reliability*)

- Intuitivamente,
  - Um produto confiável é aquele em que o consumidor pode contar para realizar o que ele/ela esperam do mesmo por um período de tempo
- Formalmente:

> *Confiabilidade é a probabilidade que um sistema (componente, produto, etc) irá realizar uma determinada função por um dado período de tempo sob condições operacionais específicas*

- Na prática, a definição de confiabilidade deve ser feita sem abigüidades:
  - Falhas devem ser definidas relativamente à função realizada pelo sistema
  - Unidade de tempo deve ser identificada
    - Tempo corrido (calendário)
    - Tempo de operação
    - Ciclos (exemplo, pousos de um avião, giros de um motor elétrico, etc)
  - Pode-se usar outras unidades além da grandeza tempo, como por exemplo:
    - Em termos de quilômetros percorridos
    - Em termos de unidades ou bateladas produzidas
  - As condições operacionais devem ser especificadas:
    - Condições de operação:
      - Uso (temperatura, corrente, pressão, etc)
      - Manutenção

- Transporte, etc
- Condições ambientais:
  - Temperatura
  - Umidade
  - Vibração
  - Altitude, etc

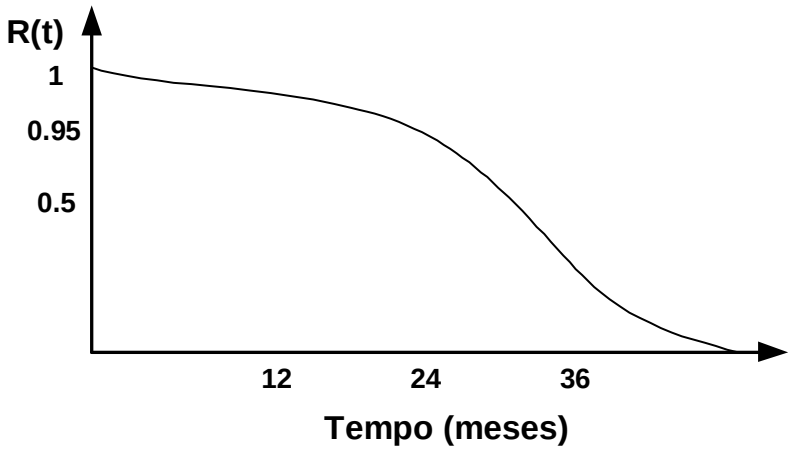
- Exemplo 1: Considere um modelo de bateria para carro cujo fabricante mantém registro das unidades devolvidas. Quando um consumidor retorna uma bateria (mesmo funcionando) durante a garantia, considera-se uma falha, pois a mesma não atendeu as expectativas do consumidor!

Tempo em Serviço (meses)	**Baterias Retornadas**	**# Acumulado de Falhas**	**Probabilidade de Falha (p)**	**Confiabilidade (R)**
0	1	1	1/1000=0.001	1-0.001=0.999
1	0	1	0.001	0.999
2	1	2	2/1000=0.002	1-0.002=0.998
3	0	2	0.002	0.998
4	1	3	3/1000=0.003	0.997
5	1	4	4/1000=0.004	0.996
6	2	6	0.006	0.994
7	1	7	0.007	0.993
8	2	9	0.009	0.991
9	2	11	0.011	0.989
10	3	14	0.014	0.986
Total = 1000 Baterias				

- Ao final dos 10 meses de uso, 14 baterias falharam de um total de 1000
- Logo, temos uma indicação da probabilidade de falha neste período: p = 0.014
- Então, sendo confiabilidade as não-falhas, a confiabilidade deste modelo

de bateria é 0.986 pra um período de 10 meses

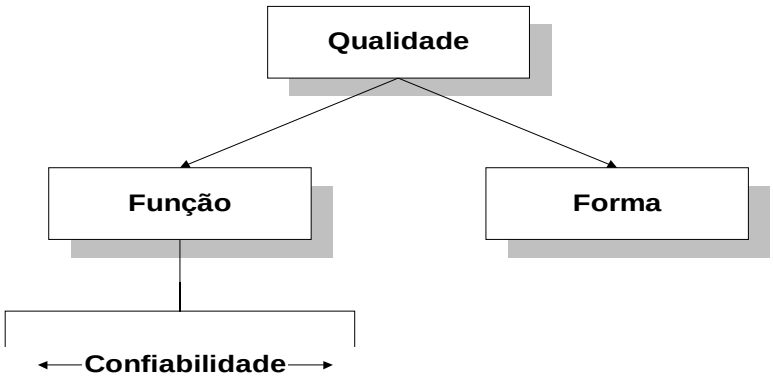
- Pode-se dizer que é 98.6% provável que uma nova bateria ainda estará funcionando após 10 meses de operação
- Assuma que o seguinte gráfico tenha sido obtido para 36 meses:



  - A confiabilidade, R, decresce para 95% em 24 meses
  - A confiabilidade atinge 50% em 32 meses
  - Quanto maior o tempo *t*, menor será a confiabilidade
  - A função de confiabilidade, R(t), é uma função monotônica decrescente
  - Do ponto de vista do fabricante, qual a melhor garantia?? 24 meses.

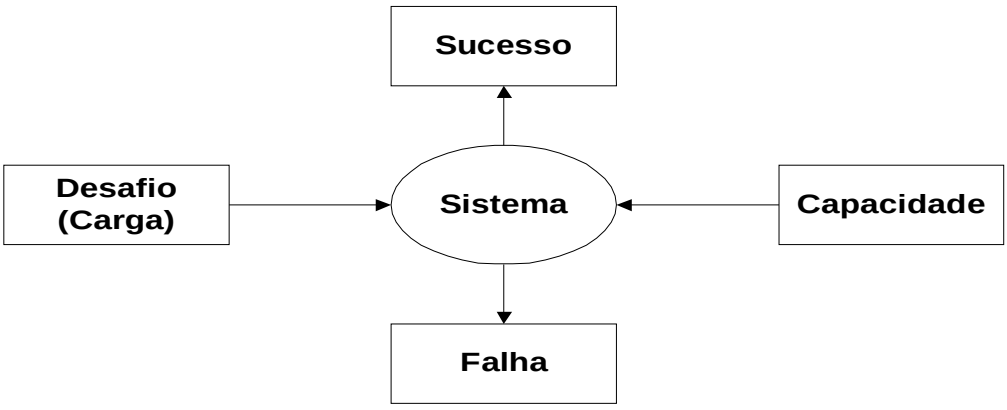
5. Qualidade e Confiabilidade

- Qualidade pode ser considerada como o grau em que um produto atende as expectativas/exigências do consumidor
- Confiabilidade, por sua vez, preocupa-se com a duração do uso de um produto a partir do momento em que o mesmo entra em operação
- Assim, se qualidade pode ser caracterizada por um conjunto de atributos de forma e função, a confiabilidade pode ser considerada como um atributo da qualidade:
  - Confiabilidade está relacionada com a função desempenhada pelo produto
- Assim, pode-se dizer:
  - Produtos de baixa qualidade provavelmente terão baixa confiabilidade
  - Produtos de alta qualidade provavelmente terão elevada confiabilidade



6. O Que é Falha do Sistema

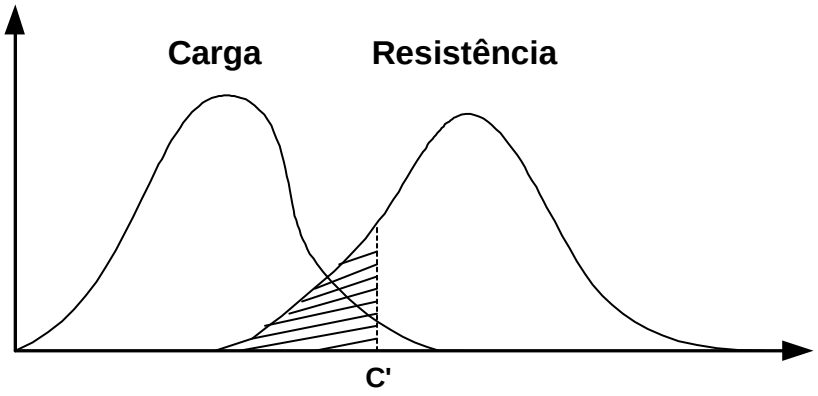
- Como dito anteriormente ao definir confiabilidade, nós precisamos especificar o significado de "falha"
- O que é uma falha?
- *Falha* é a incapacidade do sistema de realizar a sua função
- Durante a vida útil de um sistema, o mesmo é submetido a diversos desafios (aplicam-se cargas)
- Se o sistema não possui a capacidade de realizar a sua função dado este desafio, então o mesmo falha. Veja o seguinte diagrama.



- Exemplos:
  - Uma bomba de água de incêndio falha quando a mesma é incapaz de fornecera vazão de água requerida durante a operação
  - Um carro "zero" falha quando o seu consumo de combustível é maior do que o "anunciado" pelo fabricante e/ou esperado pelo consumidor
  - Um sensor de CO falha quando o mesmo torna-se descalibrado

7. Modelos de Falha

- *Stress-Strength* (Carga-Resistência)
  - Este modelo é baseado no conceito que um sistema está sujeito a cargas durante a sua vida útil
  - O mesmo falha se a resistência é menor do que a carga aplicada (força mecânica, campo elétrico, etc). Veja a figura que segue.



  - A curva à esquerda representa a variabilidade nas possíveis cargas aplicadas ao sistema
  - Considerando-se uma população de sistemas do mesmo tipo (válvulas do mesmo modelo de um mesmo fabricante), a curva à direita pode ser interpretada como a variabilidade na resistência destes sistemas uma vez que unidades deste mesmo sistema apresentam diversos valores de resistência. Quanto mais estreita esta curva, menor a variabilidade, logo mais alta é a qualidade do sistema em questão
  - Ao se aplicar uma certa carga *C'*, todos aqueles sistemas que tiverem uma resistência menor do que a carga aplicada (área tracejada à esquerda de *C'*) irão falhar
  - Note que este modelo de falha assume que a resistência é independente do tempo. Logo
    - Não há efeitos de corrosão ou fadiga, por exemplo, os quais acarretam em degradação da resistência do sistema com o tempo
    - O sistema não deteriora!
- *Damage-Endurance* (Dano-Resistência)
  - Modelo de falha semelhante ao anterior, porém considera-se que o dano resultante/induzido pela carga aplicada acumula irreversivelmente
  - O sistema deteriora com o tempo

- Assim, incluem-se efeitos de corrosão, fadiga
- Falha ocorre quando o dano excede a resistência do sistema
- Exemplo: bondinho do Pão de Açúcar (Rio de Janeiro, 21/10/2000)
  - Cabo de tração do bondinho rompe
  - 100 pessoa ficaram presas em dois bondinhos durante 1 hora
  - Causas prováveis:
    - Corrosão interna do cabo de tração, de dentro para fora
    - A corrosão pode ter acontecido pela infiltração de água na estrutura do cabo

- *Challenge-Response* (Desafio-Resposta)
  - Falha do sistema passa desapercebida até que o mesmo é necessário
  - Somente quando o sistema é desafiado (chamado para operar), a falha se torna evidente. O mesmo falha em responder apropriadamente
  - Exemplos:
    - Sistemas stand-by
    - Defeitos em softwares
- *Tolerance-Requirements* (Tolerância-Especificações)
  - Quando um sistema está operando mas não satisfatoriamente
  - O fator de tolerância é uma variável contínua que indica o grau de degradação na qualidade do desempenho do sistema
  - Especificações determinam o desempenho desejado do sistema e indicam o ponto de transição de aceitável para inaceitável
  - Exemplos:
    - Perda de contraste em uma máquina copiadora
    - Perda de pressão em um compressor
    - Perda de tensão na cordas de uma raquete de tênis

8. Definição de Manutenibilidade (*Maintainability*)

- Quando um equipamento é passível de manutenção (corretiva após falha, ou preventiva), a facilidade com a qual o mesmo sofre manutenção, reparo, e retornado à operação é medida através de sua manutenibilidade
- Formalmente:

> *Manutenibilidade é a probabilidade que um sistema falho seja retornado para operação dentro de um período de tempo quando manutenção é realizada de acordo com procedimentos estabelecidos*

- Manutenibilidade é uma medida do *downtime* do equipamento, i.e., do tempo que o mesmo se encontra fora de serviço
- Em geral, manutenibilidade:
  - Medida em tempo de relógio (tempo corrido)
  - Equivale ao tempo em que os reparos estão sendo efetuados: tempo de reparo
  - Porém, outros "atrasos" podem ser incluídos:
    - Tempo administrativo
    - Tempo de chegada de peças, etc

9. Definição de Disponibilidade (*Availability*)

- Equipamentos reparáveis (que sofrem manutenção) nem sempre estão "prontos" quando são requisitados
- Assim:

> *Disponibilidade é a probabilidade que um sistema está operacional (realizando a sua função) em um dado instante quando utilizado sob condições específicas*

- Como veremos depois, a disponibilidade pode ser matematicamente definida de diversas formas dependendo de como são medidos o tempo operacional e o tempo fora de serviço do sistema
  - Por exemplo, a disponibilidade (média) de um sistema pode ser interpretada como a porcentagem do tempo que o mesmo está operacional

$$A = \frac{Tempo\,Operaional}{Tempo\,Operacional + Tempo\,Fora\,de\,Servico}$$

- Assim, a disponibilidade leva em conta tanto o tempo operacional do sistema (quando o mesmo se encontra em um estado não falho - confiabilidade) e o tempo fora de serviço (o downtime do sistema - manutenibilidade)

10. Definição de Risco

- Qualitativamente, risco é o potencial de perdas (material, humano, meio ambiente) resultante da exposição a um perigo
- Quantitativamente, a análise de risco envolve a estimativa da probabilidade de perdas
- Pode-se dizer que:

Análise de Risco consiste em responder as seguintes perguntas:

- *O que pode acontecer de errado ?*
- *Qual a probabilidade disto vir a acontecer ?*
- *Se acontecer, quais são as conseqüências ?*
- *Qual é a nossa "confiança" nessas respostas ? Ou seja, quais são as incertezas ?*

- Logo, risco pode ser expresso quantitativamente como:

$$R =< S, P, C >$$

onde

S é o cenário (evento) indesejado

P é a probabilidade de que o evento *S* vir a ocorrer

C são as conseqüências resultantes da ocorrência do evento *S*