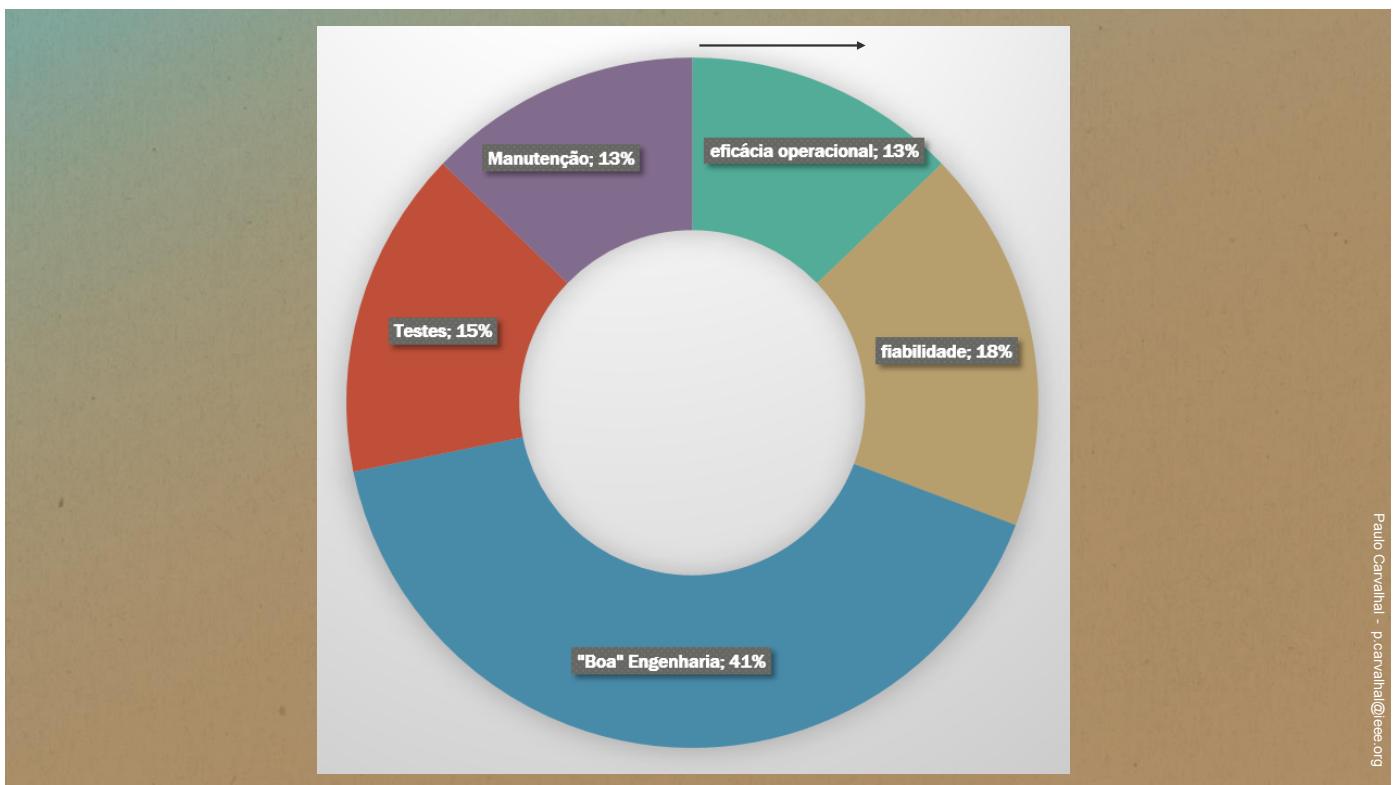


Fiabilidade e boas práticas de Projecto

UMINHO DEI - LPI-I 2014/15



Eficácia Operacional

Eficácia Operacional e conceitos associados

É muito diferente

E

- * montar um “dispositivo” que trabalhe na bancada
- * conceber um “dispositivo” que
 - i) Trabalhe “bem”(ie que cumpra as especificações de desenho)
 - ii) Sem problemas críticos
 - iii) Durante um determinado intervalo de tempo
 - iv) Respeite a normalização aplicável



Eficácia Operacional e conceitos associados



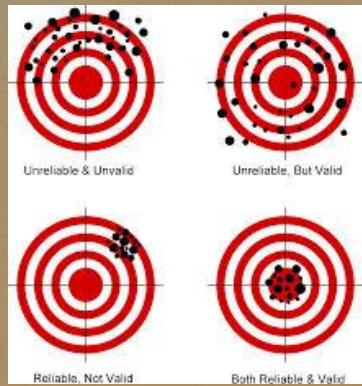
$$\text{Eficácia Operacional} = P_{\text{performance}} \times P_{\text{fiabilidade}} \times P_{\text{disponibilidade}}$$

Probabilidade de o sistema apresentar o desempenho para que foi desenhado, durante o tempo necessário e quando for necessário

Eficácia Operacional

Convém não esquecer que

A eficácia operacional pode ser controlada em todas as fases de desenvolvimento e desenho para garantir sucesso, muito antes da entrega do produto final.



Fiabilidade

Fiabilidade – conceitos associados



Fiabilidade – conceitos associados

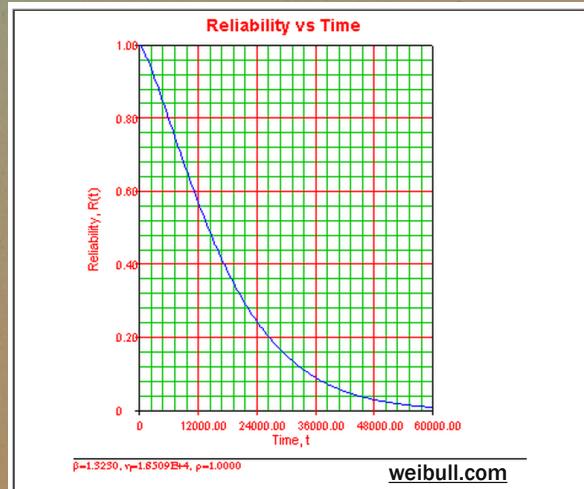
Um sistema ou equipamento diz-se fiável quando:

- Apresenta resultados previsíveis (determinismo)
- Está livre de erros catastróficos
- Capaz de recuperar de erros

Isto num
determinado
Contexto de operação
(ie, ambiente)...

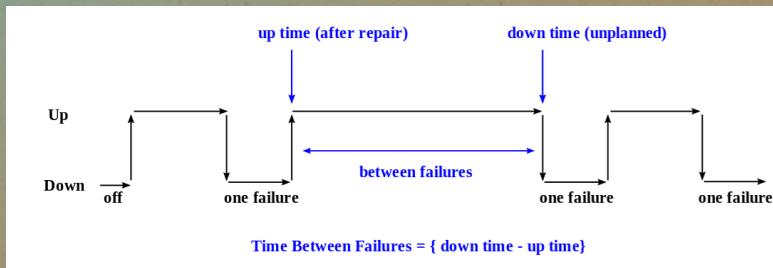
...e durante um
determinado
período de tempo.

Fiabilidade – conceitos associados



Qualquer sistema falhará, se lhe dermos tempo para isso!

Fiabilidade – conceitos associados



$$\text{Mean time between failures} = \text{MTBF} = \frac{\sum (\text{start of downtime} - \text{start of uptime})}{\text{number of failures}}.$$

Que é o mesmo que dizer: $\text{MTBF} = \text{operating hours/number of failures}$

Nota: o conceito de MTBF é aplicável apenas a sistemas ditos *repairable*

Wikipedia (Mean time between failures)

Fiabilidade – conceitos associados

Disponibilidade (Availability) $A = MTBF/(MTBF + MTTR)$

Em que:

MTBF – mean time between failures

MTTR – mean time to repair (muitas vezes é um factor mencionado nos contratos de manutenção)

Exemplo:

Um equipamento tem um MTBF de 8736h e um MTTR de 1 dia (24h)

A sua disponibilidade= $8736 / (8736 + 24) = 0.997$

Por vezes utiliza-se o conceito de failure rate, em vez de MTBF:

Failure rate $\lambda = 1/MTBF$

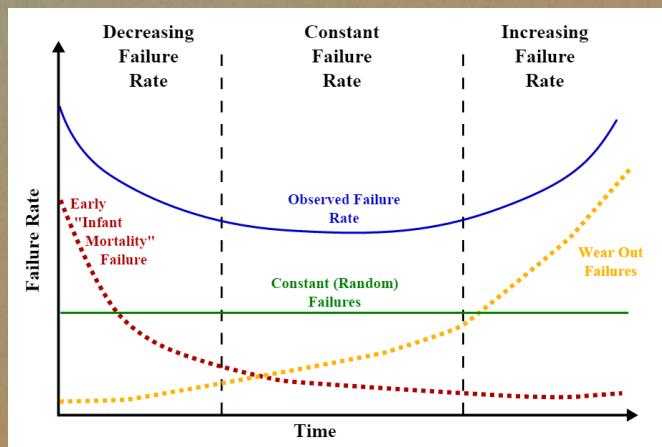
Calculador de MTBF

<http://www.aldservice.com/en/reliability-software/free-mtbf-calculator.html>

Wikipedia (Mean time between failures)

Fiabilidade – conceitos associados

Estes conceitos são apenas válidos durante o “período de vida” do produto



Wikipedia (Bathtub curve)

Fiabilidade – conceitos associados

The slide contains four main sections:

- Falha**: Evento indesejável não previsto no funcionamento normal do sistema. Podem ser internas e externas (provocadas pelo contexto operacional do equipamento).
- Ambiente**: Condições Climatéricas, Transporte, Instalação, Utilizadores, Manutenção.
- Tempo**: Com mais tempo de operação, aumenta a probabilidade de falha. OBS: tempo neste contexto não é necessariamente medido em unidades de tempo!
- Probabilidade**: A teoria das probabilidades é uma ciência fundamental para a análise de fiabilidade, disponibilidade, risco, etc.

Impact			
Trivial	Minor	Moderate	Major
Low	Low	Low	Medium
Medium	Low	Medium	Medium
High	Medium	Medium	Medium
Very High	Medium	Medium	High
Extremely High	Medium	High	High

Boa Engenharia

(ie, desenho robusto, qualidade de projeto, qualidade de produto)



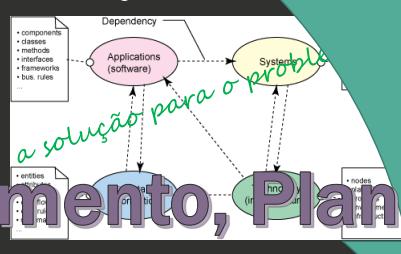
Boa Engenharia

Domínio do Problema



Análise , Levantamento, Planeamento e... introdução de problemas!

Domínio Solução



Feature	equivalent set	Total
Rifle accessory Sales	15.00%	
Rifle cannot fire more than one shot at a time by a single trigger pull	2.50%	
The report of the firearm cannot be muffled	2.50%	
Robust to sand, dirt, and other debris	3.00%	
Rare occurrence of jamming	21.00%	
Highly durable	6.50%	
High accuracy at long distances	37.00%	
Ability to penetrate body armor	7.00%	
Minimal report (i.e. quiet discharge)	2.00%	
Availability of low-cost ammunition	3.50%	
Total:	100.00%	

ou requisitos do sistema

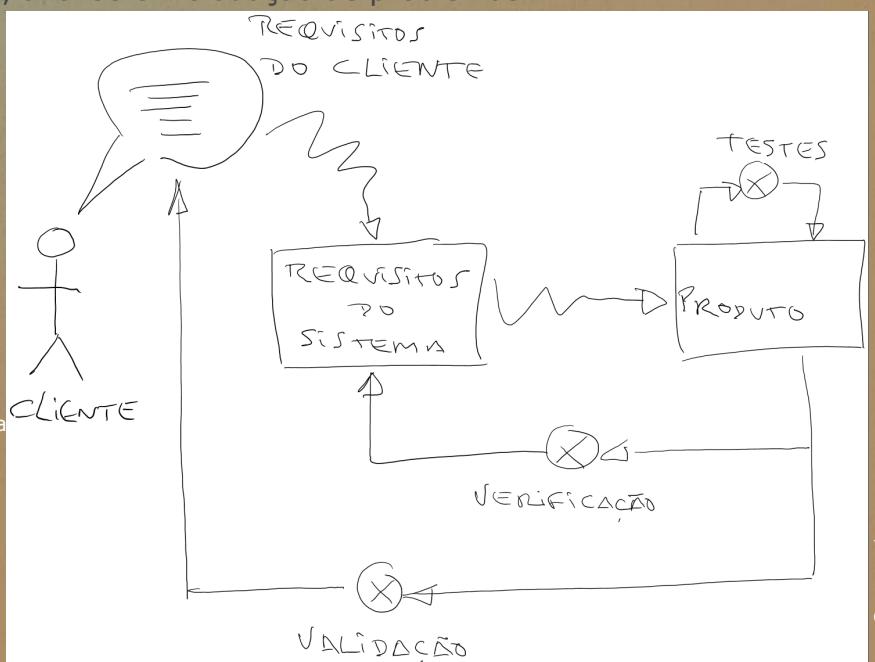
Boa Engenharia – levantamento, análise e introdução de problemas!

Alguns requisitos do cliente são “deitados fora”
Alguns requisitos do sistema “caem do céu”

E assim

Alguns requisitos do cliente são diferentes
de alguns requisitos do sistema

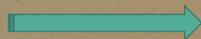
Resultados da validação são diferentes dos
Resultados da verificação



Boa Engenharia – requisitos do sistema e certificação

Os requisitos do sistema englobam:

- Objectivos
- Funcionalidades
- Specs
- Processo de verificação
- Certificação/adesão a normas



- Imposição de mercado
/Regime legal para acesso a um mercado



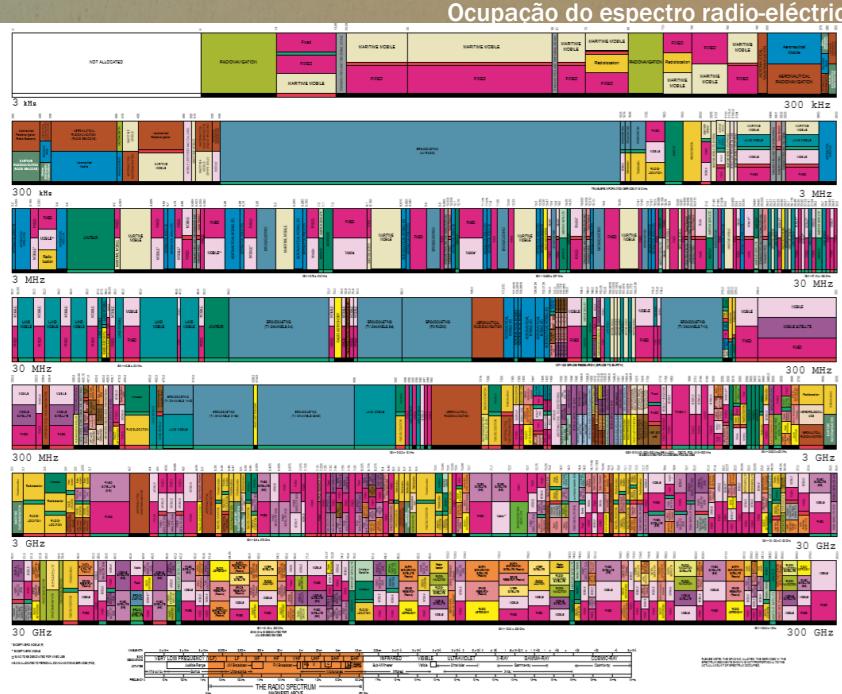
Exemplos:

comunicações rádio
sistemas que interagem com crianças
ambiental
produtos perigosos
segurança
industriais (inúmeros ramos de actividade)

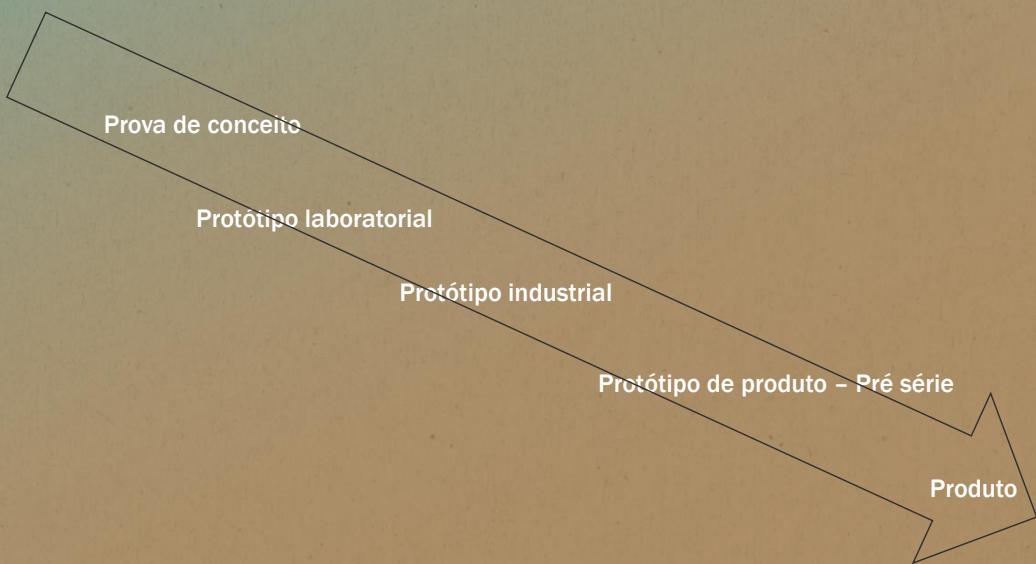
Boa Engenharia certificação

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



Boa Engenharia O Processo



Boa Engenharia O processo de desenvolvimento - Modelo funcional do sistema

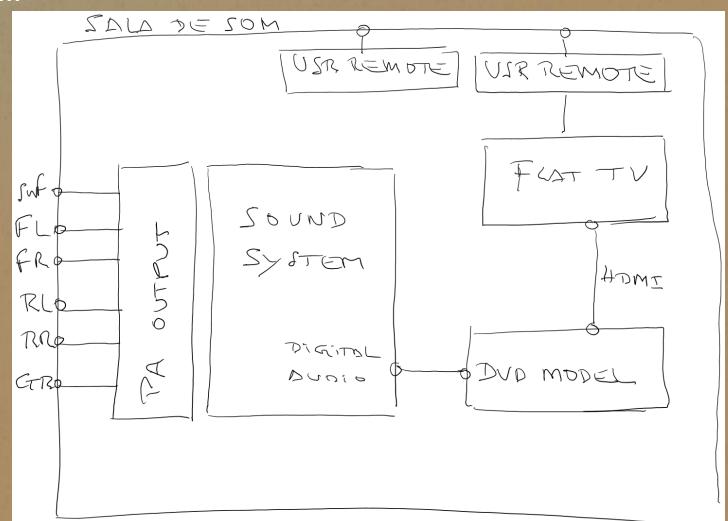
Sistema a desenvolver: DVD inserido numa sala de som

Descrição da globalidade do sistema
Integração do sistema a desenvolver no todo
Definição das fronteiras e interfaces

Condições de compatibilidade com o meio

Descrição dos factores externos relevantes
handling
storage
manutenção
radiação
vibração
emi/rfi

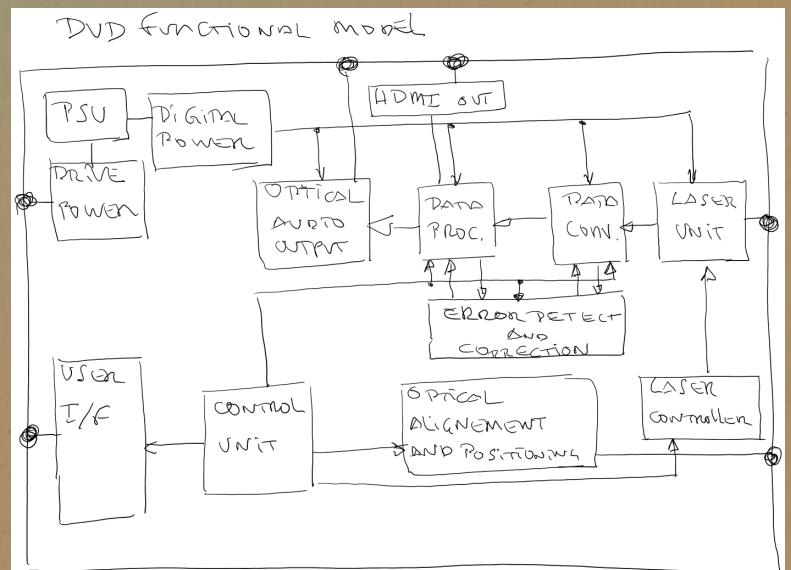
...
(só depende do sistema)



Boa Engenharia Modelo Funcional - "Vista" relevante do sistema

Com este modelo é possível identificar

O tipo de componentes necessários
As quantidades dos mesmos
Os períodos típicos de
funcionamento sem avarias

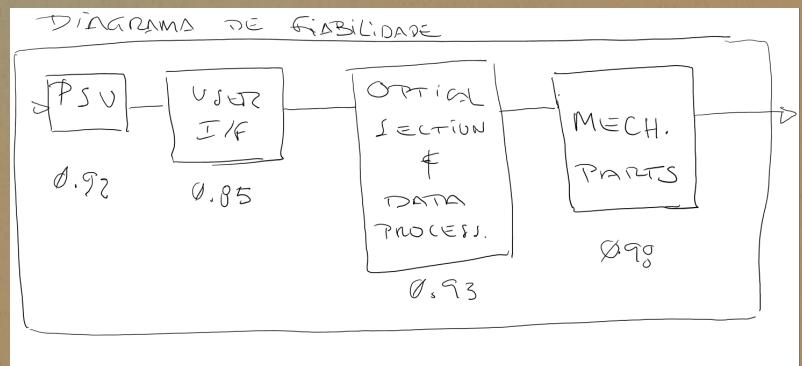


Boa Engenharia

Diagrama de fiabilidade- "Vista" relevante do sistema

Se
a probabilidade de sucesso de operação
num determinado intervalo de tempo
for conhecida para cada um dos blocos funcionais,
(e se essas probabilidades forem independentes entre si),
a probabilidade operação com sucesso do conjunto
nesse intervalo de tempo,
calcula-se através
do produto das probabilidades de cada bloco.

(Teorema da Multiplicação)



Há regras para eventos mutuamente exclusivos, condicionais etc
Ver wikipédia "Probability"

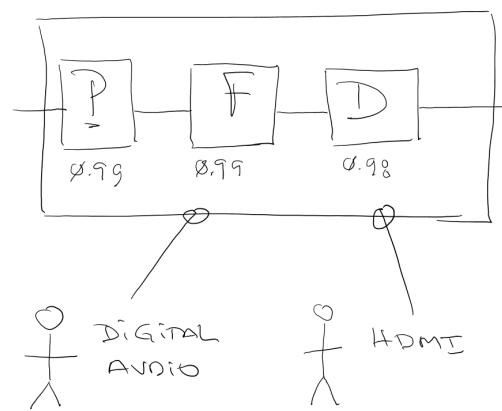
Boa Engenharia Modelo de Eficácia do Sistema

$$\text{Eficácia} = P_p \cdot P_f \cdot P_d = 0.99 \cdot 0.99 \cdot 0.98 = 0.96$$

Com esta perspectiva do sistema
podemos definir os

Requisitos Operacionais

DVD (modelo de eficácia)



Boa Engenharia – boas práticas

Checklist para um “desenho sólido”

Fault Tolerance – o sistema mantém-se funcional mesmo na presença de uma falha (H/W ou S/W)

Introdução de **Técnicas de Recovery**

É introduzido no desenho um conjunto de “pontos de controlo” que permitem aferir se algo está a correr mal. Em caso afirmativo (e em alguns casos, no contrário!!), o sistema é inicializado com um *soft-reboot* ou um *hard-reboot* em função dos casos. (Esta é uma técnica muito utilizada em software)

Introdução de **Redundância** (analisado em detalhe mais à frente)

Boa Engenharia – boas práticas

Checklist para um “desenho sólido”

Integrar funcionalidade de **BIT (Built In Test)**

Neste desenho o próprio sistema deteta situações anormais, executando testes ou identificando condições elétricas improváveis, desencadeando alarmes ou ações específicas.

Controlo de **falsas Interrupções** (ocorrem por interferência)

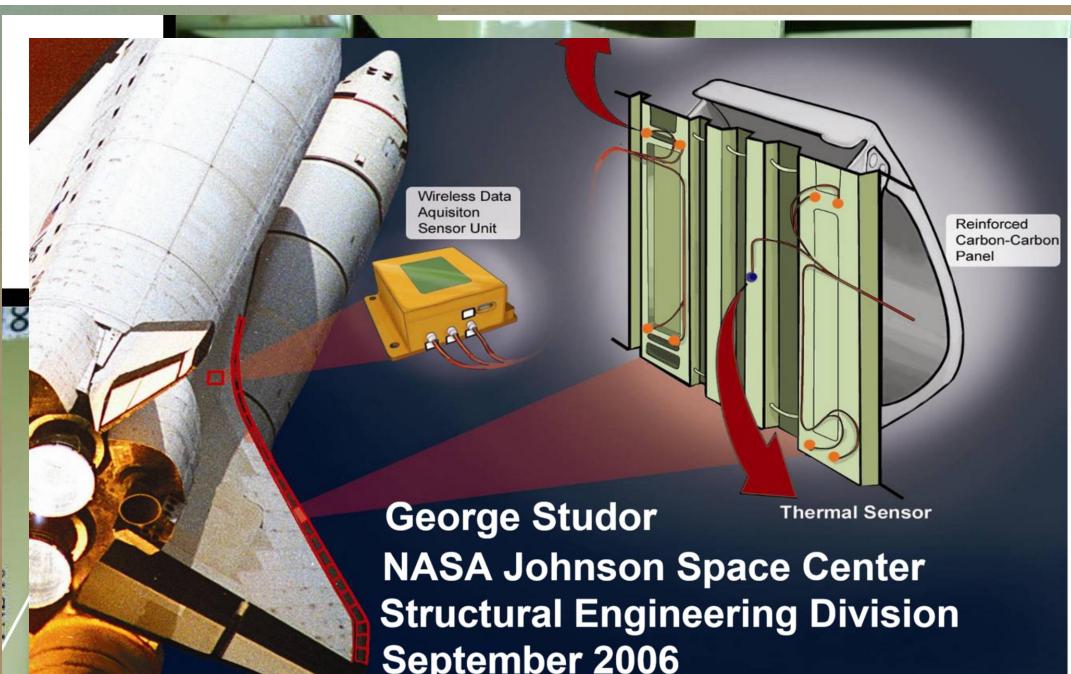
Recorre-se a flags adicionais para saber se a interrupção foi causada pelo sistema ou por fenómenos aleatórios fora do controlo do sistema.

Boa Engenharia

Boa "sinalização"
/documentação

Boa organização do
layout

Facilita
montagem
inspeção
ensaios
manutenção



Boa Engenharia – boas práticas “desenho sólido”

Protecção contra transitórios

Recurso a circuitos de *wave-shaping (clipping)* com diodos, *buffering*, outras técnicas que permitam **minimizar a interação entre dispositivos** do circuito, para garantir que em caso de interferência ou transitórios tensão numa linha não ultrapassem os limites.

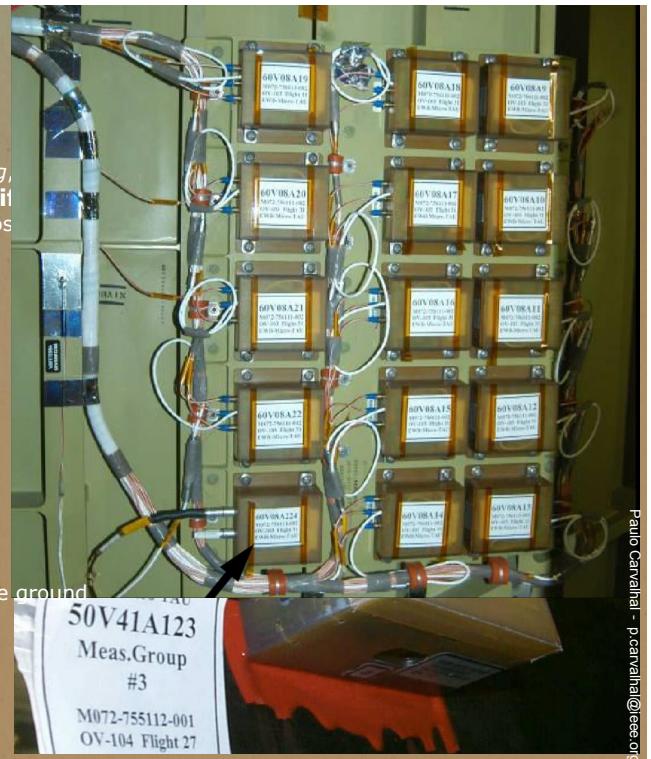
Protecção contra EMI/RFI

Colocar circuitos em caixas metálicas ligadas à terra, com todos os cabos isolados e tb ligados à terra

Recorrer sempre que possível em ligações longas, ou ligações a zonas de potência, a dispositivos opto-isolados

Protecção contra *GROUND LOOPS*

Normalmente quando num sistema eléctrico há várias ligações (ie em diferentes pontos "distantes") à terra, tem-se um problema de ground Loop: flui uma corrente entre diferentes pontos de ground (ie quedas ao longo do trajecto) que trazem ruído ou danos potenciais aos Circuitos.



Boa Engenharia – boas práticas

Checklist para um “desenho sólido”

Component “derating”

Permite deixar a operação dos componentes “folgada” e suportar situações momentâneas de stress, causadas por exemplo por interferência, ou por fenómenos mais violentos como trovoadas por exemplo.

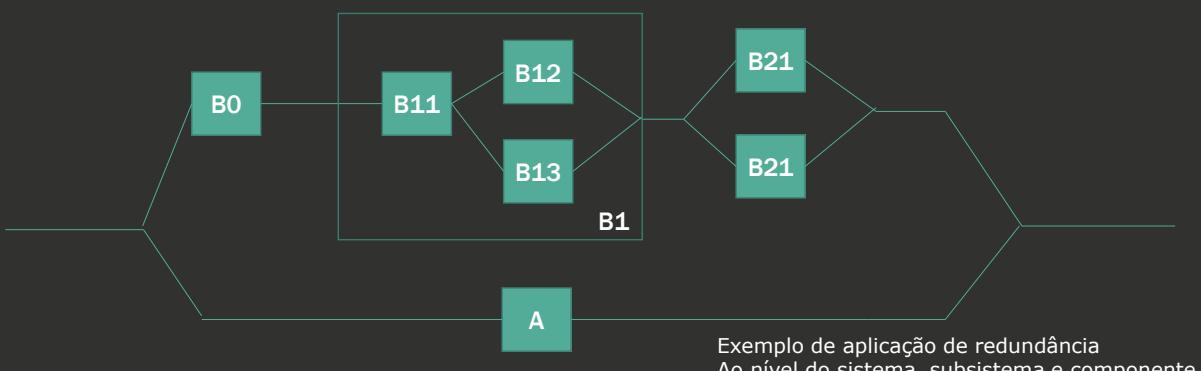
Introdução de Redundância

A ideia de sist. Redundantes vem de 1952 por John Von Newman com a introdução do chamado MAJORITY ORGAN, Um sistema de votação electrónica. Na altura não teve grande aceitação (triplicar um sistema digital na altura era uma ideia demasiado radical)!!

A partir da década de 60 no entanto, com o programa Apollo começaram a surgir os primeiros sistemas utilizáveis

A redundância introduz-se para diminuir a probabilidade de falha (aumentar a fiabilidade), acrescentando alternativas funcionais em áreas críticas do sistema.

Boa Engenharia – Exemplo de sistemas redundantes



Exemplo de aplicação de redundância
Ao nível do sistema, subsistema e componente

MAS:

A redundância implica

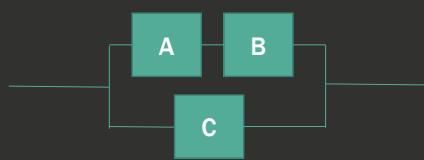
Maior complexidade
Mais peso e espaço
Maior consumo eléctrico

A redundância ao nível do componente é mais "leve"
no que diz respeito a complexidade, peso, espaço e consumo
Mas é mais difícil de implementar e testar

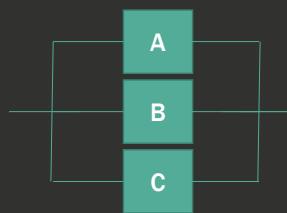
Boa Engenharia – Exemplo de sistemas redundantes



Nenhum dos componentes pode falhar



A e B não podem falhar se C falhar.
Se C não falhar, é indiferente o estado de A e B



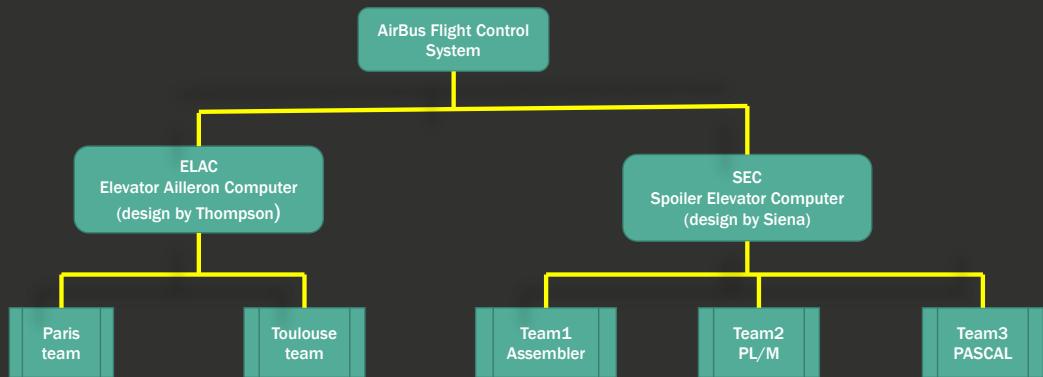
Duas quaisquer componentes podem falhar



C não pode falhar, mas A ou B podem

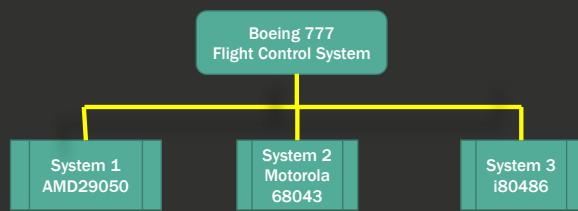
Dentro de determinados limites
é possível controlar e prever quais
as condições que maximizam a
Fiabilidade do sistema, em função da
forma como se introduz redundância.

Boa Engenharia – Exemplo de sistemas redundantes



Diz-se que este sistema tem uma fiabilidade de 1 falha em $10.000.000.000.000$ de operações...

Boa Engenharia – Exemplo de sistemas redundantes



Testes

Testes

Nunca esquecer!

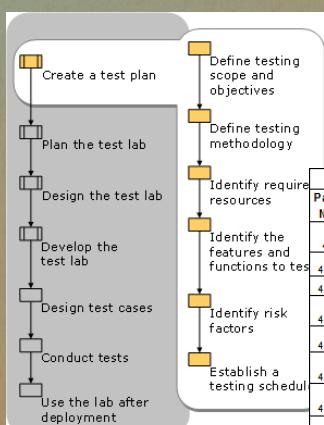


Os erros mais difíceis de detetar
são aqueles que têm
menor probabilidade
de ocorrência

Testes

Um plano de testes deve ser sempre integrado no ciclo de desenvolvimento

A natureza, metodologia, procedimentos, instrumentos de teste, técnicas, equipa técnica, etc dependem em larga escala do tipo de sistema a ser testado.



Test #	Engineering Spec	Verification Method	Fail Criteria
1	Net weight	Analysis	2 people cannot transport
2	System volume	Analysis	
3	Maximum Rotor Diameter	Test	> 1.25m
4	Wire Length between Modules	Test	> 9 m
5	Modularity for Future Systems	Analysis	
6	Power: rated, peak	Test	< 400 W
7	Voltage: rated, peak	Test	< 12 V
8	Dimensions: % of System volume	Test	
		Test	> 24 hours
		Test	< 6 hours
		Test	< 75 Ah
		Analysis	< 15 %
		Analysis	< 50 %
		Test	< 0.91m
		Test	> -2°C or < 35°C
		Demonstration	< 100%
		Test	> 30 minutes
		Analysis	Not all parts are compliant
		Demonstration	Does not charge 8 LVE batteries
		Test	< 25 m/s

Paulo Carvalhal - pcarvalhal@ieee.org

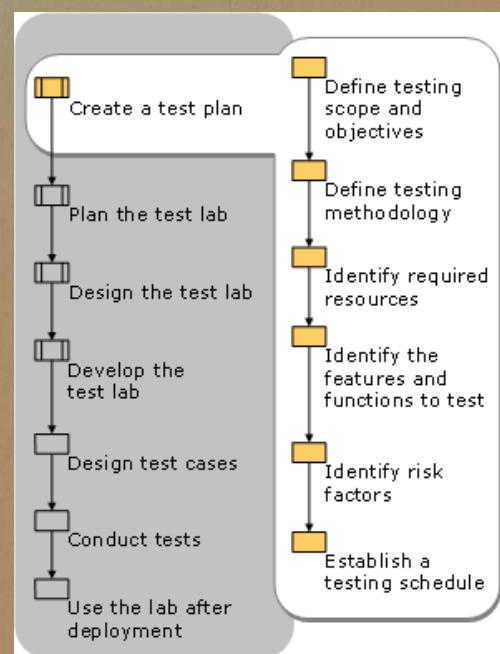
Testes

Um plano de testes deve incluir (entre outros aspectos)

Definição do que se quer testar
Objectivos/requisitos do teste
Projecto dos testes
Implementação dos testes
Análise dos resultados

E muito importante

Registo dos testes para efeitos de histórico e análise posterior



Testes

Stress

Aumentam a probabilidade de falha, forçando maiores taxas de utilização do objecto de teste
Em função do sistema, pode-se tratar de stress

- térmico
- ciclos de humidade
- eléctrico
- lógico
- mecânico
- químico
- ...

Um produto falha quando o nível de stress a que é sujeito excede a sua robustez

Força bruta (muito comuns na indústria de software)

Funcionais (do sistema, de sub-sistemas e de associação de sub-sistemas)

Testes

Há muitos domínios da Engenharia em que os procedimentos de teste são apoiados/substituídos por simuladores

Há situações em que o teste não é exequível em condições iguais às condições reais.

Há situações em que o teste é destrutivo e o custo financeiro do teste se torna muito elevado
(esta é uma situação muito comum nos sistemas ditos non-repairable)



Testes

Há muitos domínios da Engenharia em que se constroem equipamentos específicos para realizar um tipo de teste.

Nestes casos o teste é feito em condições o mais próximo possível do ambiente real relevante.

Os custos destas situações são normalmente muito elevados. Apenas se justificando por razões de Segurança e integridade de seres humanos

- Ascent Impactors: Foam, ice, ablator, and metal
- Hypervelocity
- Additional foam and ice shots to Panel 9 for validation of RCC damage me



Columbia Accident Investigation **Catastrophic Impact Damage Test on RCC Panel 8**

Teste de impacto mecânico (vibração e deformação ou destruição de 3 elementos do bordo de ataque de uma asa do vai-vém Columbia

Manutenção

Manutenção

O conceito de **manutenção** impõe-se neste contexto, no sentido de garantir uma gestão eficaz da vida útil dos equipamentos, assegurando os níveis desejados de

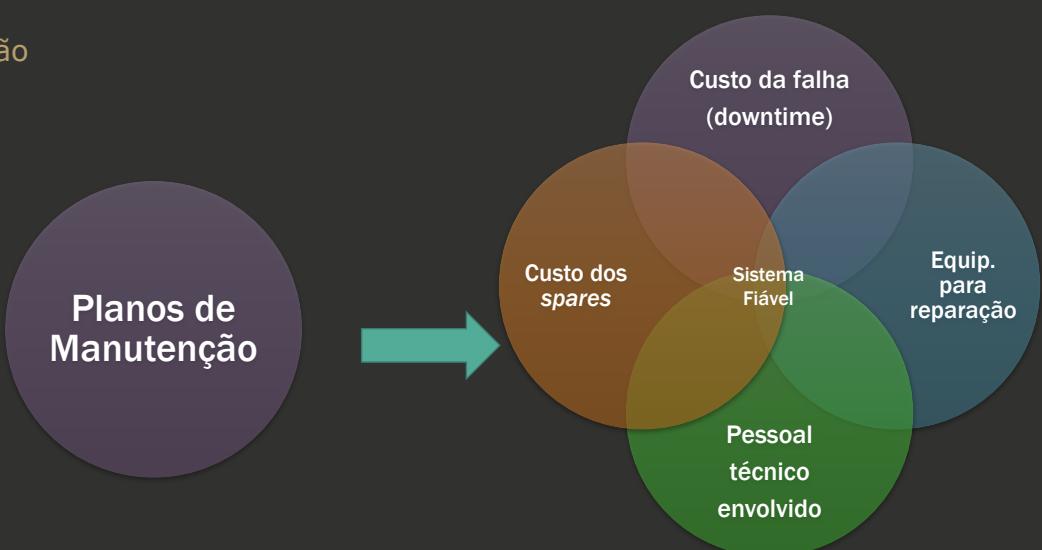
Fiabilidade
Disponibilidade
Performance

De forma a conseguir **tempos de operação sem ocorrência de falhas** consistentes com as especificações dos equipamentos

E ainda acrescentava:

- Melhoria da competitividade do produto
- Manutenção da certificação
- Conformidade com regulamentação aplicável

Manutenção



Construir um plano de manutenção fiável pressupõe o **conhecimento dos mecanismos de falha envolvidos**. Isso implica técnicos com

- Experiência
- Competências de largo espectro

Manutenção

Planos de Manutenção

Lista de tarefas de manutenção

Frequência das mesmas (relacionado com MTBF)

Equipas e meios necessários

Estado do equipamento na altura da manutenção (modo de op., OFF, standby, Running,etc)

Tipo de tarefa (preventiva, curativa, correctiva, emergência)

Tempo estimado de reparação

E muito importante:

os **registos de manutenção**, que fornecem o histórico de avarias, custos, horas de laboração, horas de downtime, etc

Manutenção

A actividade de Engenharia de Manutenção de equipamentos e sistemas implica normalmente conhecimentos nas seguintes áreas (entre outras):

Estatística
Gestão de projectos (para sistemas de grandes dimensões)
Logística (para sistemas de grandes dimensões)
Tecnologias específicas do sistema a controlar
Física dos processos

Referências

Fiabilidade e controlo de qualidade
Manuel Cabral Morais
IST 2007 Secção de estatística e aplicações

Computers take flight
A history of NASA pioneering digital fly-by-wire project
James E. Tomayko
Library of Congress cataloging-in-publication data
NASA SP-2000-4224

Handbook of reliability engineering
Published by the direction of the chief of the Bureau of Naval Weapons
1964
NAVWEPS 00-65-502

On Robust Engineering
George Novacek
Circuit Cellar 25th anniversary issue
2013