Actos de Engenharia

Aplicações Industriais de Sistemas Electrónicos e de Telecomunicações

9.º ENCONTRO NACIONAL DO COLÉGIO DE ENGENHARIA ELECTROTÉCNICA

19 de Junho de 2009

Pedro Moreira da Silva

Indice

- Actos de Engenharia cada vez mais exigentes aplicáveis a produtos e sistemas:
  - Directivas europeias e marcação CE, declaração de conformidade, normas harmonizadas
  - Requisitos avançados : ex. Norma IRIS
  - RAMS : fiabilidade
  - DRA : design risk assessment
  - SIL : safety integrity level
  - Gestão de requisitos

Directivas Europeias

Garantem que, para cada tipo de produto, produzido por fabricantes Europeus ou não e utilizados no Espaço Europeu (compreendendo os países da União Europeia e alguns outros que aderiram às mesmas regras), se cumprem requisitos mínimos ao estabelecerem o que cada produto, que seja abrangido pelas Directivas, deve obedecer para ser possível, legalmente, colocá-lo no mercado Europeu.

Directivas Europeias

New Approach directives (directives providing for CE marking)		
Text of directive and amendments	**Consolidated version of directive**	**Subject (short title of directive)** **Lists of references of harmonised standards and general information**
2006/95/EC		Low Voltage
87/404/EEC 90/488/EEC 93/68/EEC	87/404/EEC	Simple Pressure Vessels
88/378/EEC 93/68/EEC	88/378/EEC	Safety of toys
89/106/EEC 93/68/EEC	89/106/EEC	Construction products
89/336/EEC 92/31/EC 93/68/EEC 2004/108/EC	89/336/EEC	Electromagnetic compatibility (EMC)
98/37/EC 98/79/EC 2006/42/EC	98/37/EC	Machinery
89/686/EEC 93/68/EEC 93/95/EEC 96/58/EC	89/686/EEC	Personal protective equipment (PPE)
90/384/EEC 93/68/EEC	90/384/EEC	Non-automatic weighing instruments
90/385/EEC 93/42/EEC 93/68/EEC	90/385/EEC	Active implantable medical devices
90/396/EEC 93/68/EEC	90/396/EEC	Appliances burning gaseous fuels
92/42/EEC 93/68/EEC 2004/8/EC 2005/32/EC	92/42/EEC	Efficiency requirements for new hot-water boilers fired with liquid or gaseous fuels
93/15/EEC		Explosives for civil uses
93/42/EEC 98/79/EC 2000/70/EC 2001/104/EC	93/42/EEC	Medical devices
94/9/EC		Equipment explosive atmospheres (ATEX)
94/25/EC 2003/44/EC	94/25/EC	Recreational craft
95/16/EC		Lifts
97/23/EC		Pressure equipment
98/79/EC		In vitro diagnostic medical devices
1999/5/EC		Radio Equipment and Telecommunications Terminal Equipment and the Mutual Recognition of their Conformity
2000/9/EC		Cableway installations designed to carry persons
2004/22/EC		Measuring instruments

Directivas Europeias

Directiva de Baixa Tensão
(2006/95/CE)

No artigo 1º refere-se o “material eléctrico” que está no âmbito da aplicação desta Directiva que, com excepção do referido no Anexo II, é todo aquele que é utilizado para tensão nominal entre 50V e 1000V (corrente alternada) e entre 75V e 1500V (corrente contínua).

Directiva de Baixa Tensão (2006/95/CE)

Protecção contra os riscos resultantes do material eléctrico

Serão previstas medidas de ordem técnica de acordo com o ponto 1, a fim de que:

a) As pessoas e os animais domésticos fiquem protegidos de forma adequada contra os riscos de ferimentos ou de outros acidentes resultantes de contactos directos ou indirectos;

b) Não se produzam temperaturas, descargas ou radiações que possam provocar perigo;

c) As pessoas, os animais domésticos e os bens sejam protegidos de forma adequada contra os riscos de natureza não eléctrica provenientes do material eléctrico que a experiência venha a revelar;

d) O isolamento seja adequado aos condicionamentos previstos.

Protecção contra os riscos que possam ser provocados por influências exteriores sobre o material eléctrico

Serão previstas medidas de ordem técnica de acordo com o ponto 1, a fim de que:

a) O material eléctrico responda às exigências mecânicas previstas, de modo a não pôr em perigo as pessoas, os animais domésticos e os bens;

b) O material eléctrico resista às influências não mecânicas nas condições ambientes previstas, de modo a não pôr em risco as pessoas, os animais domésticos e os bens;

c) O material eléctrico não ponha em risco as pessoas, os animais domésticos e os bens nas condições de sobrecarga previstas.

Directiva de Compatibilidade electromagnética (2004/108/CE)

1. **Requisitos de protecção**

Os equipamentos serão concebidos e fabricados de forma a, tendo em conta a evolução técnica mais recentes, assegurar que:

a) as perturbações electromagnéticas geradas não excedem o nível acima do qual os equipamentos de rádio e de telecomunicações ou outros não possam funcionar da forma prevista;

b) tenham o nível de imunidade às perturbações electromagnéticas que é de esperar na sua utilização prevista e que lhes permita funcionar sem uma degradação inaceitável nessa utilização.

2. **Requisitos específicos para instalações fixas**

Instalação e utilização prevista de componentes:

As instalações fixas serão instaladas segundo as boas práticas de engenharia e no respeito da informação sobre a utilização prevista dos seus componentes, de modo a preencher os requisitos de protecção referidos no ponto 1. Estas boas práticas de engenharia deverão estar documentadas e a pessoa ou pessoas responsáveis e deverão manter a referida documentação à disposição das autoridades nacionais pertinentes, para efeitos de inspecção, enquanto a instalação fixa estiver em funcionamento.

Marcação CE – Directiva 93/68/CEE

A Marcação CE, que os equipamentos abrangidos devem exibir obrigatoriamente, de forma indelével, é a maneira visível para todos os que tenham, de alguma forma, contacto com esses equipamentos de se aperceberem que obedecem a Requisitos no âmbito das Directivas aplicáveis que exijam tal Marcação CE.

Declaração de Conformidade

O Fabricante ou o Representante do Fabricante exterior àUnião Europeia (podendo ser a Entidade que comercializa o produto) é obrigado a fazer a avaliação da Conformidade onde Garante e Declara a Conformidade do Produto (Componente, Equipamento, Sistema, etc.) com os Requisitos previstos nas Directivas Comunitárias aplicáveis.

Normas Harmonizadas

Norma Harmonizada no contexto da Marcação CE :

deve ser publicada no Jornal Oficial da União Europeia e válida no contexto da **MARCAÇÃO CE** , conferindo, ao Produto que a cumpre, a chamada Presunção de Conformidade com os Requisitos Essenciais da(s) Directiva(s) Comunitária(s) que se aplique(m)

Para os diversos requisitos das Normas há várias maneiras previstas para se demonstrar a conformidade:

- Ensaios
- Medições
- Inspecção

Norma IRIS (International Railway Industry Standard)

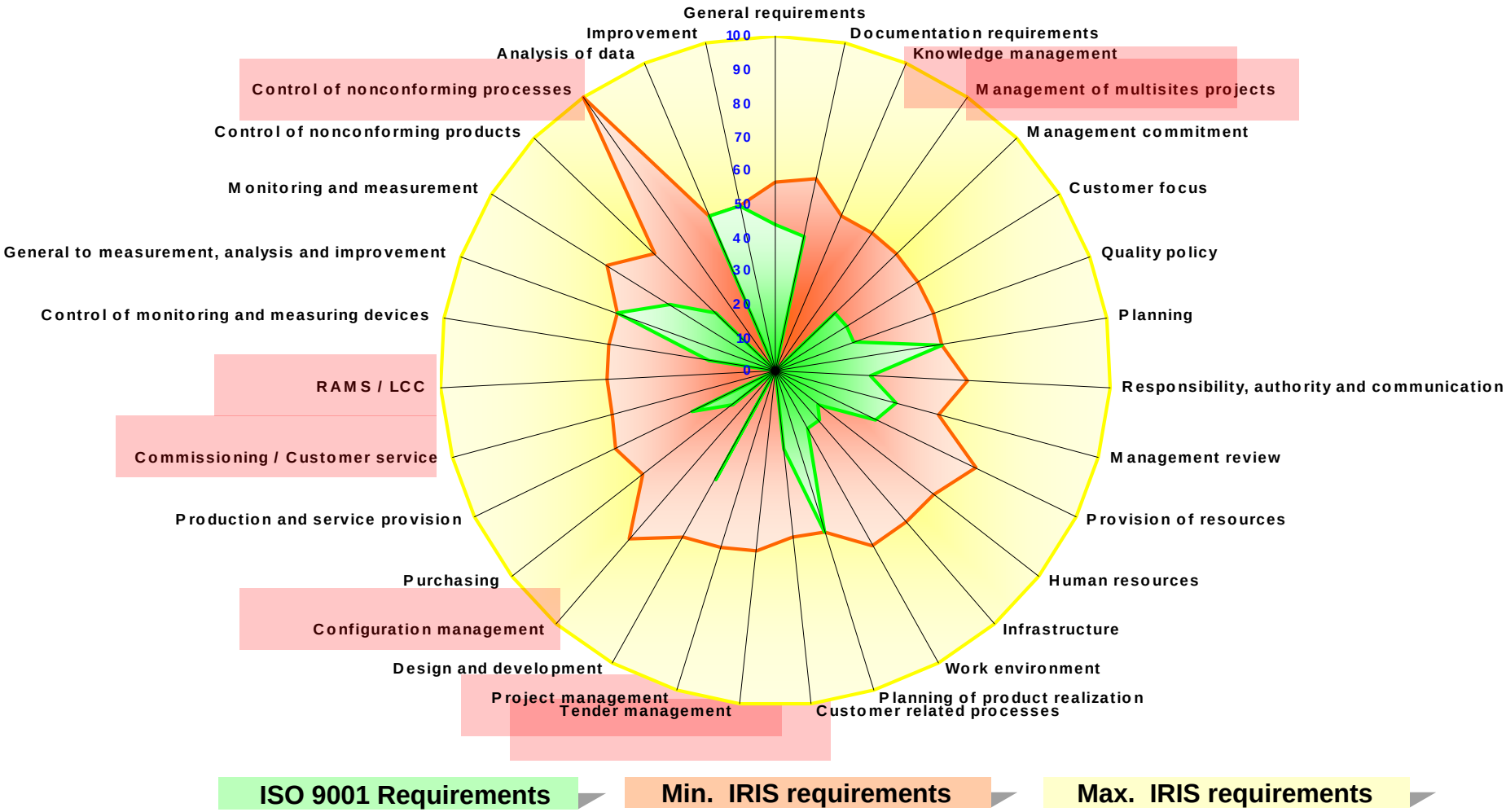
- **A norma IRIS surge como uma necessidade do sector ferroviário em ter uma norma específica para esta actividade, tal como acontece com outras áreas – automóvel, espaço, alimentar**

- **Esta norma apresenta requisitos com enfoque prático ao nível da qualidade do produto, ex:**

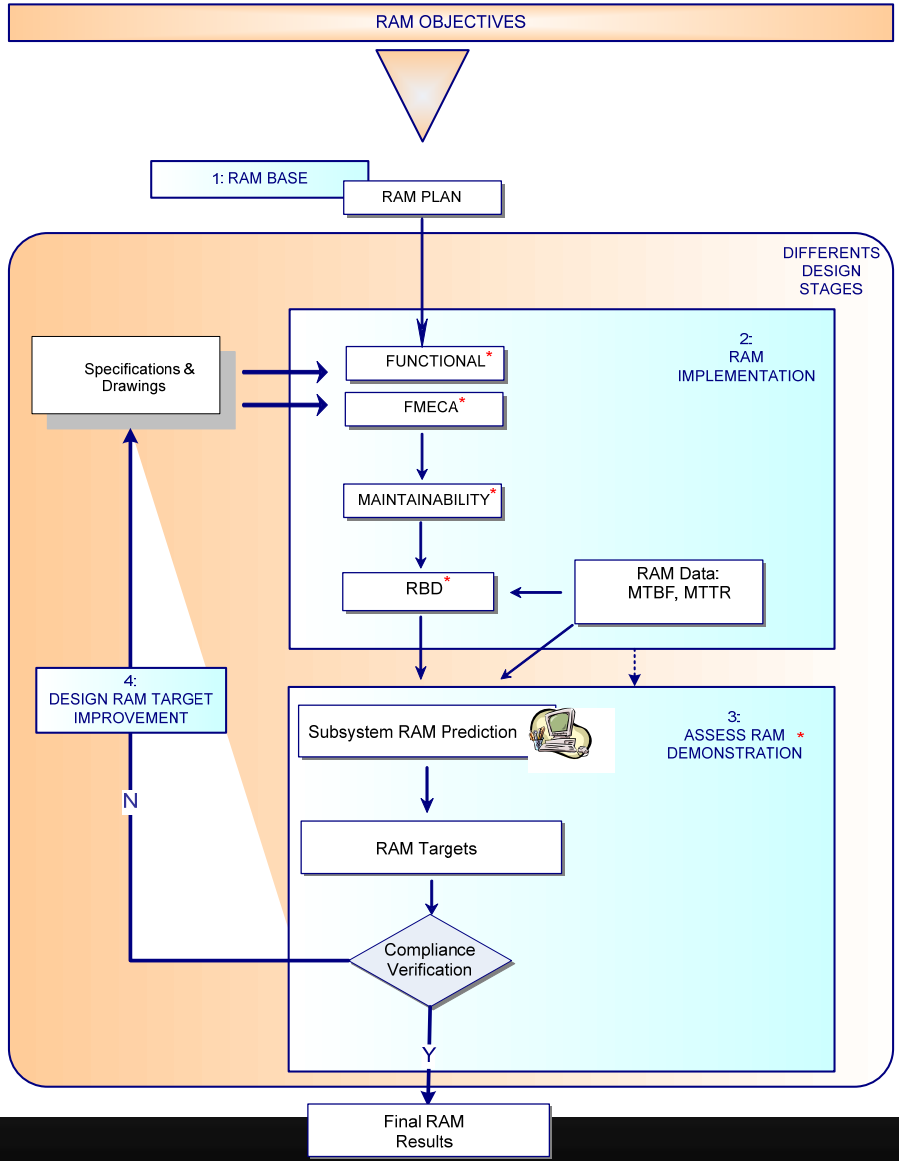
  - Life Cycle Cost (LCC)
  - Reliability, availability, maintainability and safety (RAMS)
  - Gestão de Configurações
  - Gestão de Multi-Projectos
  - First Article Inspection
  - Gestão do Conhecimento

IRIS Certification

Requisitos norma IRIS *versus* ISO 9001



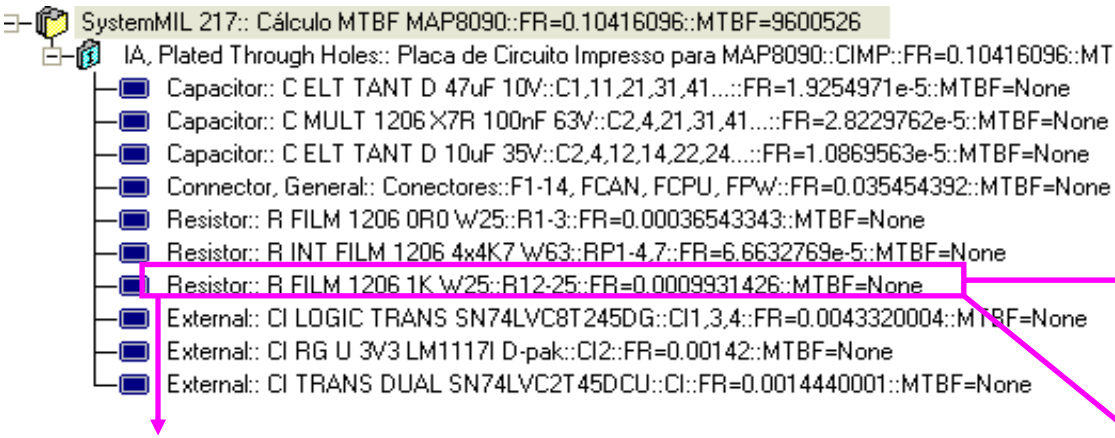
RAMS
Reliability, Availability, Maintainability, Safety

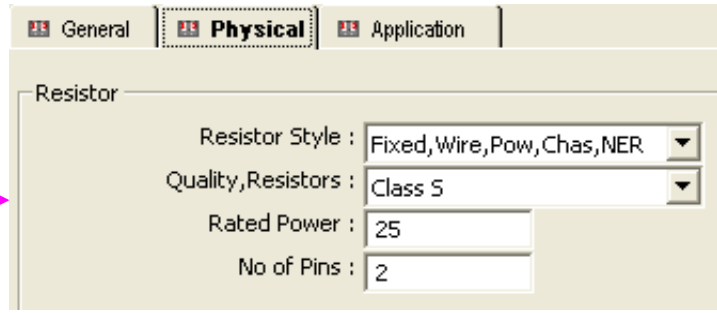


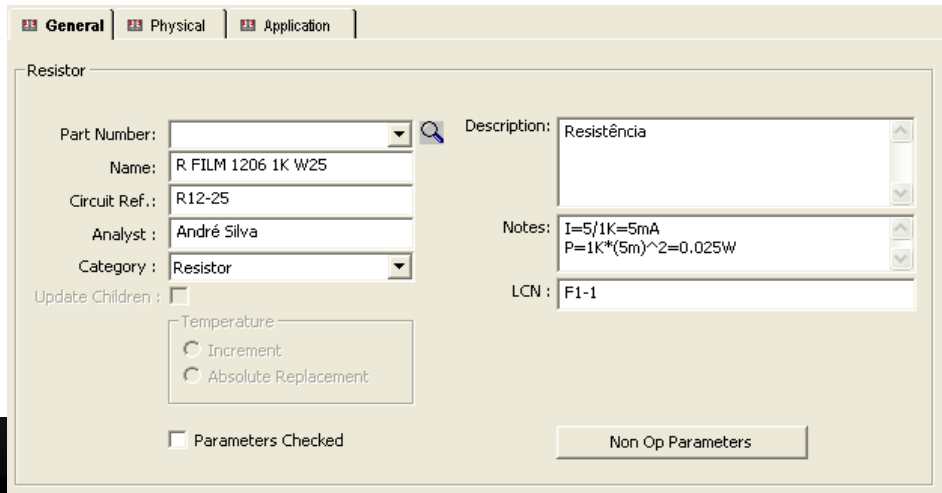
Aplicação a
Projectos
ou
Produtos

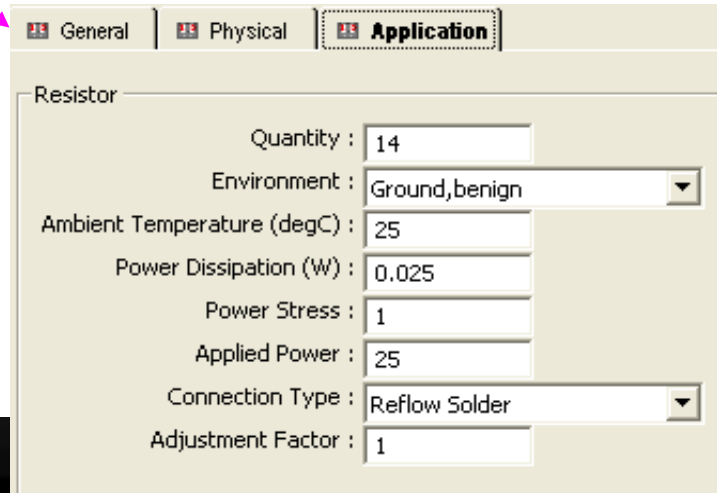
Reliability - Fiabilidade

- ✓ Dados utiiizados nos cálculos provêm de:
- ◆ Datasheets dos respectivos fornecedores/Fabricantes de componentes
- ◆Dados de Campo
- ◆Registos de Manutenção
- ◆Baseada por exemplo na norma MIL-HDBK-217F, *(Reliability Prediction of Electronic Equipment)*









FMECA – Failure Mode Effects Criticality Analysis

(Análise Crítica de Modos de Falhas e seus Efeitos)

- Técnica de Fiabilidade que permite analisar modos de falha, causas, efeitos *(em diferentes níveis)*, severidade, detecção de falha, probabilidade de ocorrência

Failure Modes Effects and Criticality Analysis (FMECA)

Equipment: TDP8
Project/Phase: AEEF - TDP8 / B
Subsystem: TM/TC

Prepared by: Joana Eliseu
Approved by: Costa Pinto

Item	Description	Function	Failure Mode	Effect on subsystem	Effect on Equipment	Effect on System (Spacecraft)	Observable Symptoms	Compensation provisions	Criticality	Recommendations and Remarks
1.1.1.1	CTTB_J2	1553 B RT Address and Parity bits definition	Open Circuit on a pin Short Circuit between adjacent pins Connector Disconnection	Loss of TM/TC	Loss TDP8	No effect	Response Absence to commands on both channels (A and B); Response with error flag asserted; Response to other addresses;	None at TDP8 level and TDP8 switch off by S/C	2S	Each 1553B bus user shall have an unique address that, in case of a single failure, does not become an already existing address of another user. This is assuming 5 bus users maximum.

Exemplos

FMECA - 1. Operators Workstations

Level code (1)	N. (2)	Item Description (3)	Item failure mode/s (4)	Item failure cause/s (5)	Detection methods (6)	Effect in Reliability Analysis: Local Effect (7)	Effect on high level (8)	Effect on top level (9)	Severity level (10)	Frequency or Probability Occurrence (11)	Failure rate (h^{-1}) (12)	Preventive Measures (13)	Comments (14)
1.1; 1.2 & 1.3	1	Workstations 1; 2 e 3 – HP dc7800	One or two Workstations failure	Intrinsic cause	HMI not available	Doesn't work	CCS operation limited to one or two operator	CCS operation limited to one or two operator	III	99,5%		Maintenance preventive	----
	2		Failure of three Workstation	Intrinsic cause		Doesn't work	CCS operates in degraded mode	CCS operates in degraded mode	II	0,5%			
1.4; 1.5 & 1.6	1	Audio Splitter 1; 2 & 3	One or two Audio Splitter failure	Intrinsic cause	Audio not available	Doesn't work	CCS operation (audio functions) limited to one or two operator	CCS operation (audio functions) limited to one or two operator	IV	99,5%		No	----
	2		Failure of three Audio Splitter	Intrinsic cause		Doesn't work	CCS operates in degraded mode for functions that requires audio	CCS operates in degraded mode for functions that requires audio	III	0,5%			

Maintainability

- medida pelo índice MTTR (*Mean Time To Repair*)
- Usual efectuar-se: Manutenção preventiva e Correctiva

Manutenção Preventiva

PREVENTIVE MAINTENANCE - 3. CCTV System – Irish Police - Brennanstown Stop - LRU

Level code (1)	Item description (2)	Maintenance type (3)	Task description (4)	Operation Time (h) (5)	Number of Men (6)	Personnel Category (7)	Interval / (Periodicity) Months (8)	Special Tools (9)	Comments (10)
3.3.1	Encoder – Bosch VJT-X40S	N/A							
3.3.2	Encoder – Bosch VJT-X20S	N/A							
3.3.3 & 3.3.4	E/O Video Converter	N/A							
3.3.7 & 3.3.8 3.3.5 & 3.3.6	Autodome 300 VG4-313-ECS2M	Visual Inspection	Inspect all connecting cables for deterioration or other damage. Verify if all mounting hardware is secure	1/6	1	T	6	---	---
		Cleanness	Wipe housing with a clean damp cloth.	1/2	1	T	6	Clean dump cloth	---
		Functional Verifications	Test the camera movements	1/6	1	T	6	---	---
3.3.1 3.3.2 3.3.3 & 3.3.4	Autodome 300 VG4-313-ECS2MF	Visual Inspection	Inspect all connecting cables for deterioration or other damage. Verify if all mounting hardware is secure.	1/6	1	T	6	---	---
		Cleanness	Wipe housing with a clean damp cloth.	1/2	1	T	6	Clean dump cloth	---
			ments	1/6	1	T	6	---	---
		N/A							

CORRECTIVE MAINTENANCE

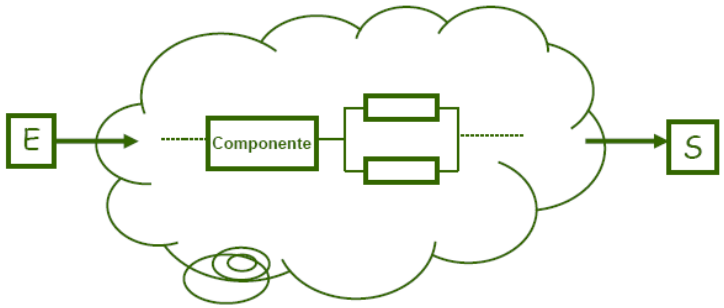
3. CCTV System Irish Police – Brennanstown Stop - LRU

Level code (1)	Item description (2)	Item Failure Mode (3)	Task description (4)	Replaceable (Y/N) (5)	Repairable (Y/N) (6)	MTTR (7)	Number of Men (8)	Personnel Category (9)	Special Tools (10)	Comments (11)
3.3.7 & 3.3.8	Autodome 300 VG4-313-ECS2M	Hardware malfunction	Replace Camera	Y	N	60	1	T	---	---
		Rotation system malfunction or camera movements	Replace Camera	Y	N	60	1	T	---	---
3.3.5 & 3.3.6	Autodome 300 VG4-313-ECS2MF	Hardware malfunction	Replace Camera	Y	N	60	1	T	---	---
		E/O converter built-in malfunction	Replace Camera	Y	N	60	1	T	---	---
		Rotation system malfunction or camera movements	Replace Camera	Y	N	60	1	T	---	---

Exemplos

Manutenção Correctiva

Availability



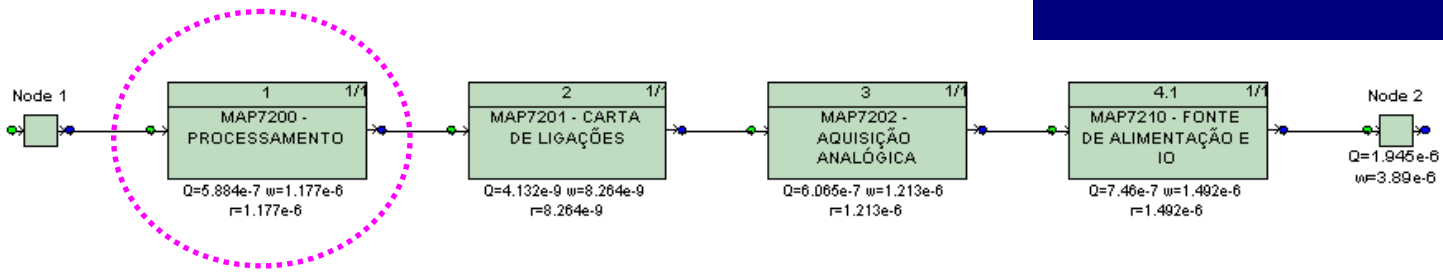
RBD

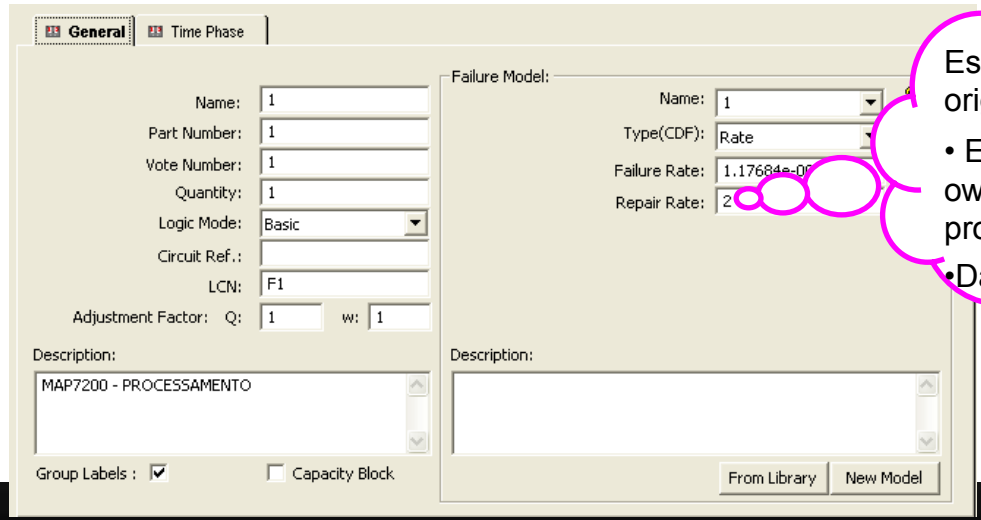
Reliability Block Diagram

- Modelização de sistemas/produtos

✓ Informação inserida nos (blocos):
→ Failure Rate; Repair Time; Quantidade, redundância

✓ Informação extraída (sistema/produto):
→ MTBF; MTTR; TDT; N. Exp. Failures, Unavailability





Este dado tem origem:

- Experiência owners dos projectos
- Dados manutenção

Spare Parts

Usando a distribuição de Poisson, com base nos custos, quantidade e Failure Rate, o tempo em que o sistema estará sem suporte, indisponibilidade durante o tempo de contrato.

- Output do programa : Qt. Peças reserva e Custos

Base Spare Results

	Name	Description	Qty	Cost	F/Rate (fpmh)	Bkup Stock	Repl Stock	Total Stock	Actual SOR(%)
1	1.1	HP Proliant ML370 Server	5	3500	3.898e-6	1	1	2	0.0
2	1.2	Industrial PC (FEP)	3	1300	1e-5	1	1	2	0.0
3	1.3	Switch HP Procurve 2600	2	575	2.433e-6	1	1	2	0.0
4	1.4								

Site Spare Results

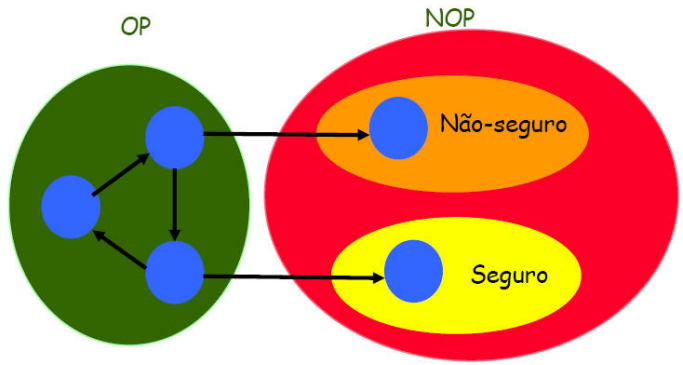
	Name	Description	Qty	Cost	F/Rate (fpmh)	Exp No Of Fails	No. Of Spares	Actual SOR(%)
1	1.1	HP Proliant ML370 Server	5	3500	3.898e-6	1.6830941e-7	0.0	1.7881393e-5
2	1.2	Industrial PC (FEP)	3	1300	1e-5	2.5907039e-7	0.0	2.3841858e-5
3	1.3	Switch HP Procurve 2600	2	575	2.433e-6	4.2021217e-8	0.0	5.9604645e-6
4	1.4	Circuit Breaker	9	15	4.651e-9	7.7721118e-8	0.0	5.9604645e-6

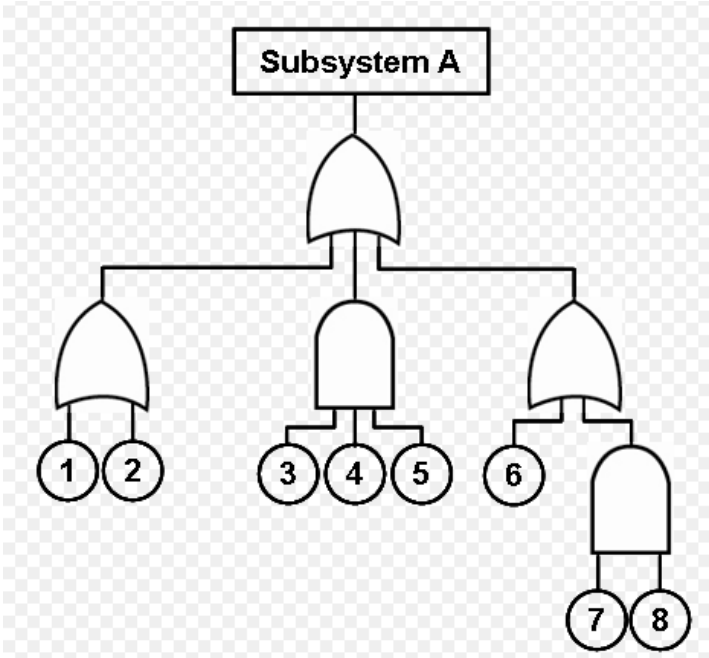
Safety

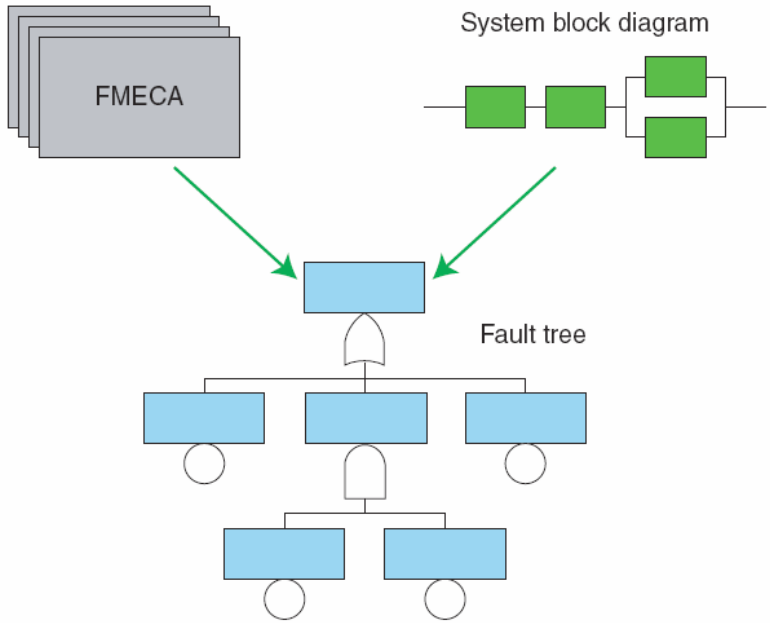
FTA

Fault Tree Analysis

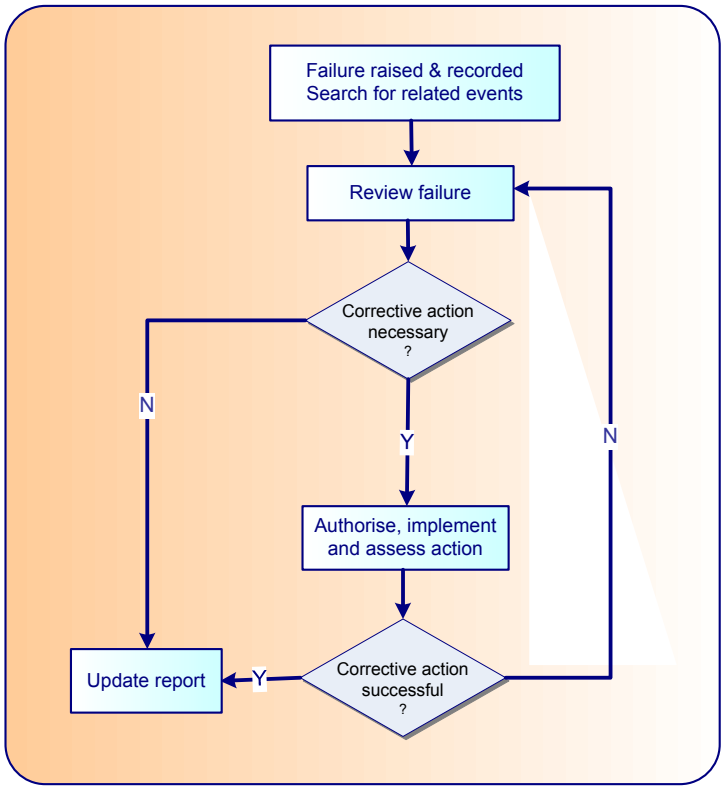
Árvores de Falha são usadas na fiabilidade e avaliações de risco de segurança para representar graficamente as interacções lógicas e probabilidades de ocorrência de falhas de componentes, e outros eventos no sistema



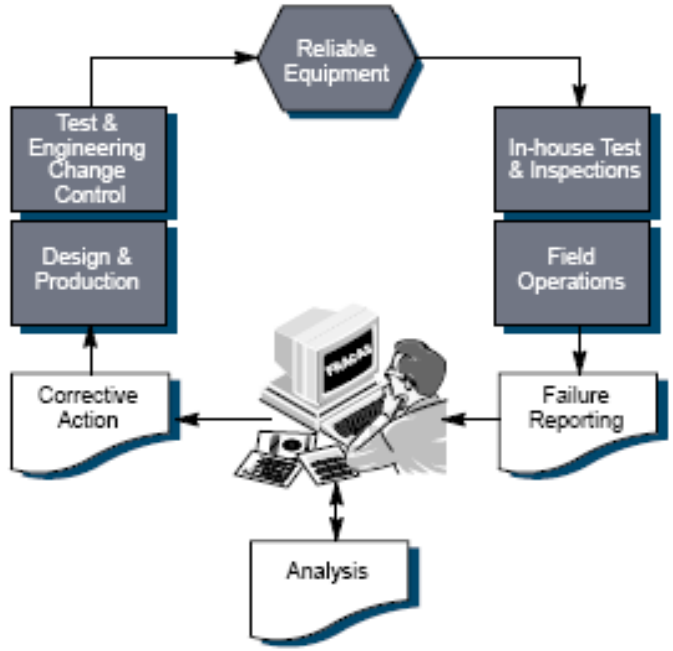




FRACAS – Failure Reporting and Corrective Action System



DRACAS – Data Reporting and Corrective Action System



Registo detalhado do processo, permite recolher, quantificar e controlar uma larga gama de reports de incidentes, tais como:

- Dados de teste
- Dados de Campo
- Dados de reparação

Os outputs do FRACAS/DRACAS podem ser utilizados como inputs do FMECA

Avaliação de Riscos na Concepção
(Design Risk Assessment)

- metodologia usada para avaliação de riscos na fase da concepção e desenvolvimento de uma solução / equipamento / sistema

- principal objectivo é a segurança das pessoas e bens tendo em consideração as fases de montagem, operação, manutenção até ao fim do ciclo de vida do equipamento.

- envolvimento das equipas de projecto na identificação das soluções mais adequadas, logo na fase inicial de um projecto

- requisito contratual de grandes projectos, em alguns países (ex. Irlanda) é requisito legal

- "obriga" a pensar nas várias vertentes da segurança

Avaliação de Riscos na Concepção
(Design Risk Assessment)

- critérios usados para avaliação de riscos

Likelihood	
Probability of Occurrence	Probability Index
So unlikely that probability is close to zero	A
Unlikely to occur, though conceivable	B
Likely to occur sometime	C
Occurrence not surprising. May occur more than once	D
Occurrence inevitable. May occur many times	E

Severity	
Potential Maximum Consequence (Hazard Severity)	Hazard Severity Index
Minor injury/illness resulting in lost time of 3 days or less	1
Injury/illness causing lost time more than 3 days	2
Major illness/injury to one or more persons not causing permanent disability	3
Single fatality or single/multiple permanent disability	4
Multiple fatality	5

Risk Level					
Hazard Severity Index	Probability Index				
	A	B	C	D	E
1	L	L	M	H	H
2	L	M	H	H	H
3	L	M	H	S	S
4	M	H	S	S	S
5	M	H	S	S	S

Risk Level Action		
Risk Level	Description	Action by Designer
L	Low	Check that risks cannot be further reduced by simple design changes
M	Medium	
H	High	Amend design to reduce risk, or seek alternative option. Only accept option if justifiable on other grounds.
S	Severe	

Quando o risco é avaliado como “alto” ou “severo” devem ser implementadas alterações no projecto

Avaliação de Riscos na Concepção
(Design Risk Assessment)
- exemplo -

Scope of Design	**Fire and Intruder Detection Systems**	Designer **Claúdio Martins**

(1) Haz Ref	(2) Activity/Process/ Material/Element	(3) Hazard	(4) Stage of Work	(5) Initial Risk Level[1]			(6) Risk Control Measures: Design action taken, record of decision process including option considered, design constraints and justification for options/actions not having been taken	(7) Residual Risk Level			(8) Is there a 'significant[2] residual risk to be passed on? (Y/N)	(9) If answer to (8) is Yes, information flow: D/P/F[3]
				Probability	Severity	Risk Level		Probability	Severity	Risk Level		
1	Installation of smoke detector system and sounder & verification	Electric Shock due to connecting to system. Working adjacent to electrical & control cabinets. Damage to cabinets. Disruption to system	Construction	D	4	S	Competent & qualified personnel to carry out works. Works as to Design BS & Method Statement controls. Full compliance with client controls, Procedures & Permit Systems. Signing and isolating of High Voltage area.	A	1	L	N	P
2	Installation of smoke detector system and sounder	Falling from Heights	Construction	D	3	S	Competent & qualified personnel to carry out works. All equipment to be used to BS, checked prior to use and in the case of scaffolding - signed and certified.In the case of ladders works only to short duration. Full conformance to method statement for such works. Strict compliance to client controls and permit systems.	B	2	M	N	P
3	Maintentance of smoke detector and sounder	Falling from Heights / electrocution	Maintenance	D	4	S	Competent & qualified personnel to carry out works. All equipment to be used to BS, checked prior to use and in the case of scaffolding - signed and certified.In the case of ladders works only to short duration. Strict compliance to client controls and permit systems.	B	2	M	Y	F

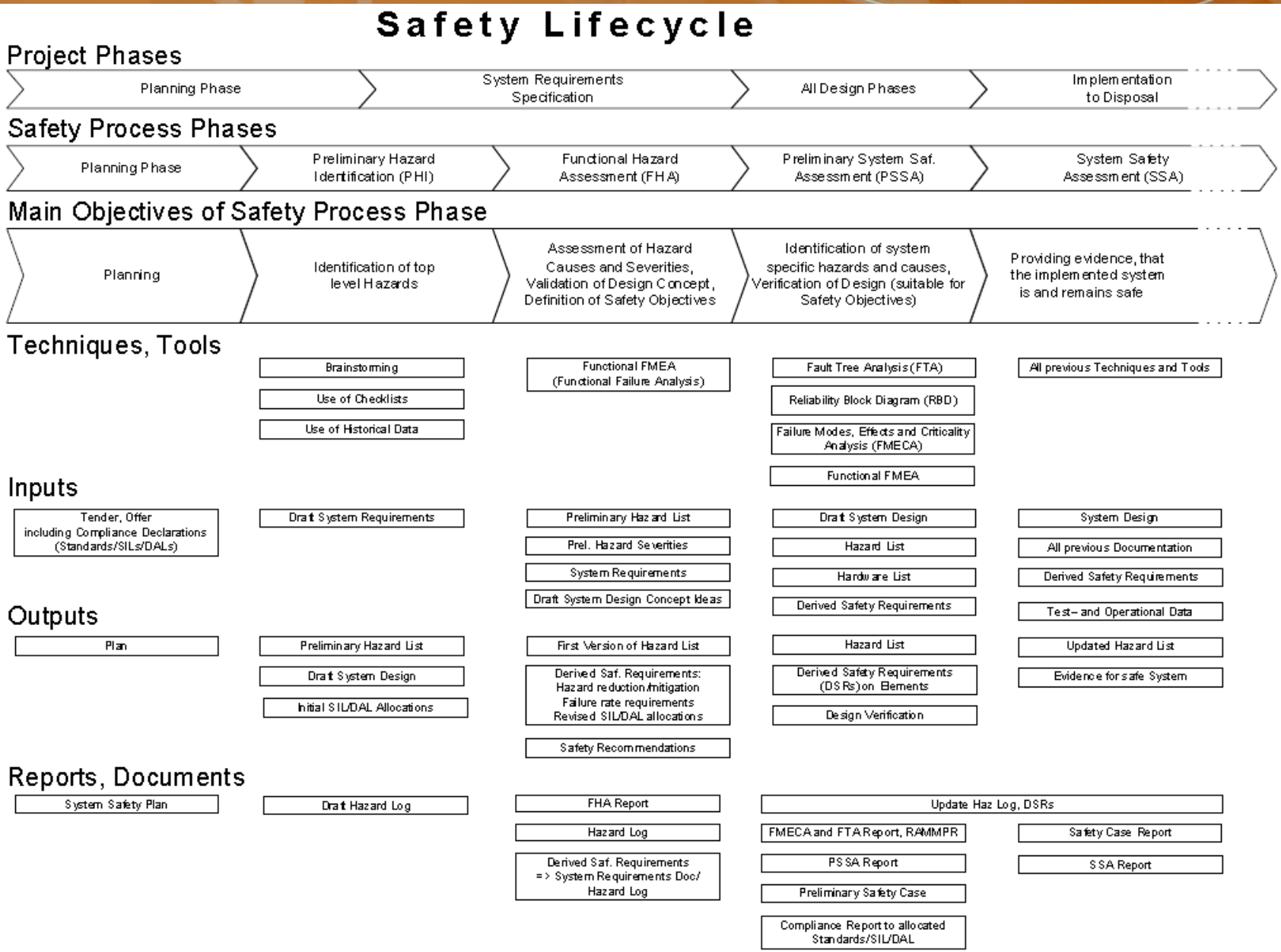
Safety Integrity Levels

- **Engenharia dos Sistemas Electrónicos**
  - Caracterização e desafios dos sistemas:
    - Omnipresentes na actividade humana (ambientes diversificados e exigentes)
    - Desempenho de missões/funções críticas
      - Falha dos sistemas acarretam consequências catastróficas:
        - » Perda de vidas humanas (industria médica, nuclear, química, aviónica, ferroviária, militar, automovel, etc.)
        - » Perdas materiais elevadas (serviços bancários, telecomunicações, industria e serviços em geral)
    - Complexidade crescente em número de componentes
    - Multiplicidade de interfaces
    - Resposta em tempo real
    - Determinismo na resposta

Safety Integrity Levels

- **Engenharia dos Sistemas Electrónicos**
  - Respostas da Engenharia:
    - Controlo da segurança em todo o ciclo de vida dos sistemas - CEI 61508
      - Concepção inicial
      - Análise de perigos & Avaliação de riscos
      - Estabelecimento dos requisitos de segurança
      - Especificação
      - Desenho
      - Implementação
      - Operação
      - Manutenção
      - Abate

Safety Integrity Levels



Safety Integrity Levels

- **Engenharia dos Sistemas Electrónicos**
  - Respostas da Engenharia:
    - Avaliação e redução de riscos
      - Standardização de Metodologias de Análise de Riscos
        - » CEI 61882 – HAZOP
    - Estabelecimento de níveis de integridade de segurança “Safety Integrity Levels” – SIL baseados no calculo de probabilidades – CEI 61508

Probabilidade de falha perigosa por hora

(sistemas solicitados em permanência)

SIL	A	B
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

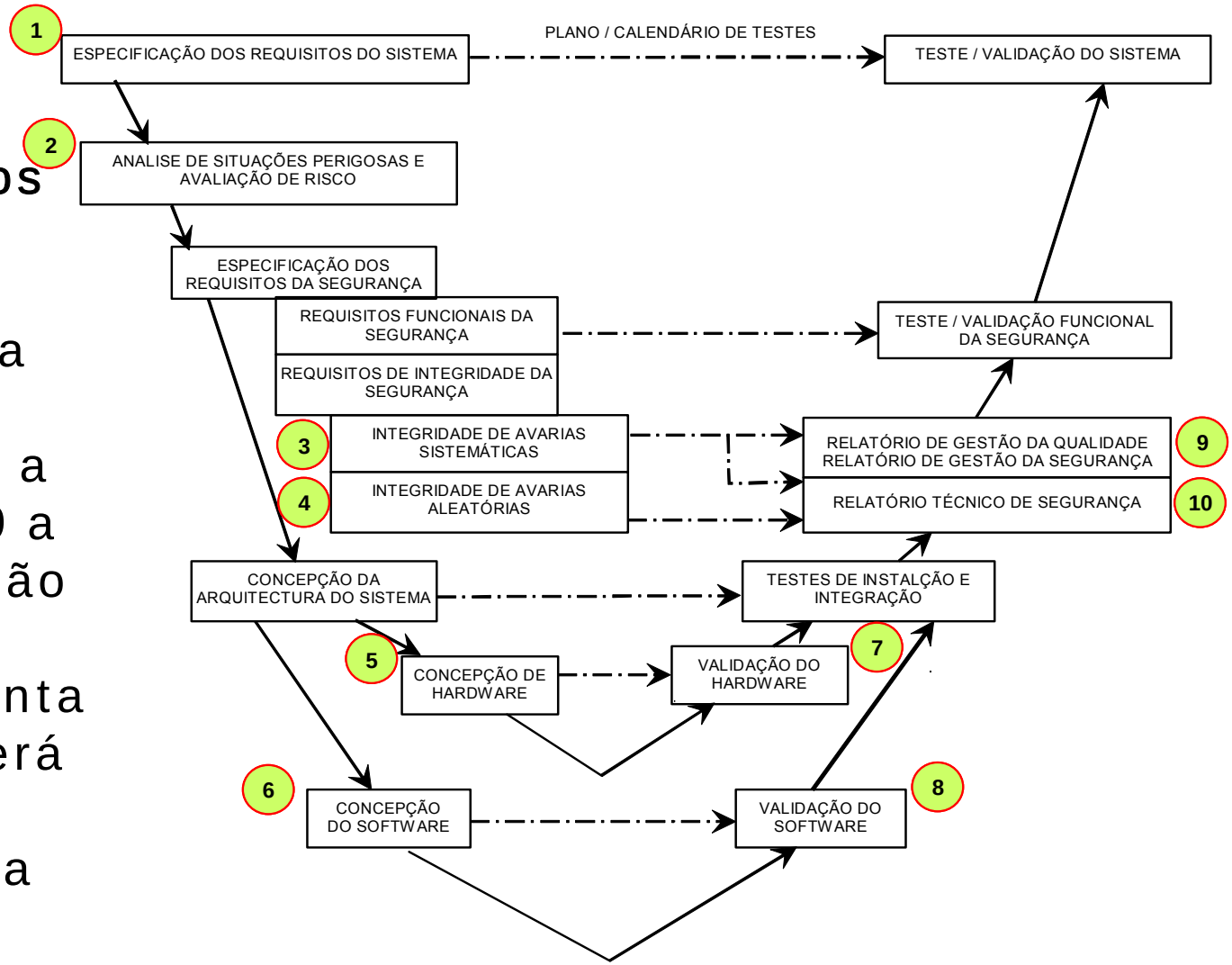
Probabilidade média de falha quando solicitado

Gestão de requisitos

Engenharia dos Sistemas Electrónicos

Respostas da Engenharia:

Segundo a EN50129 a Concepção e Implementação deverá ser composta pelas tarefas do diagrama



Safety Integrity Levels

- **Engenharia dos Sistemas Electrónicos**
  - Respostas da Engenharia:
    - Garantia de integridade das falhas aleatórias
      - Utilização de Metodologias de Análise de Falhas
        - » FMECA (Failure Mode Effect Critical Analysis)
        - » FTA (Fault Tree Analysis)
        - » ETA (Event Tree Analysis)
        - » RBD (Reliability Block Diagram Model)
        - » Markov Chains Model
    - Garantia de integridade das falhas sistemáticas
      - Sistema de Gestão da Qualidade
        - » Utilização de métodos formais e de simulação na Especificação, Verificação e Validação dos sistemas
      - Sistema de Gestão da Segurança
        - » Equipas de Concepção & Implementação independentes das Equipas de Verificação & Validação
        - » Avaliação Independente

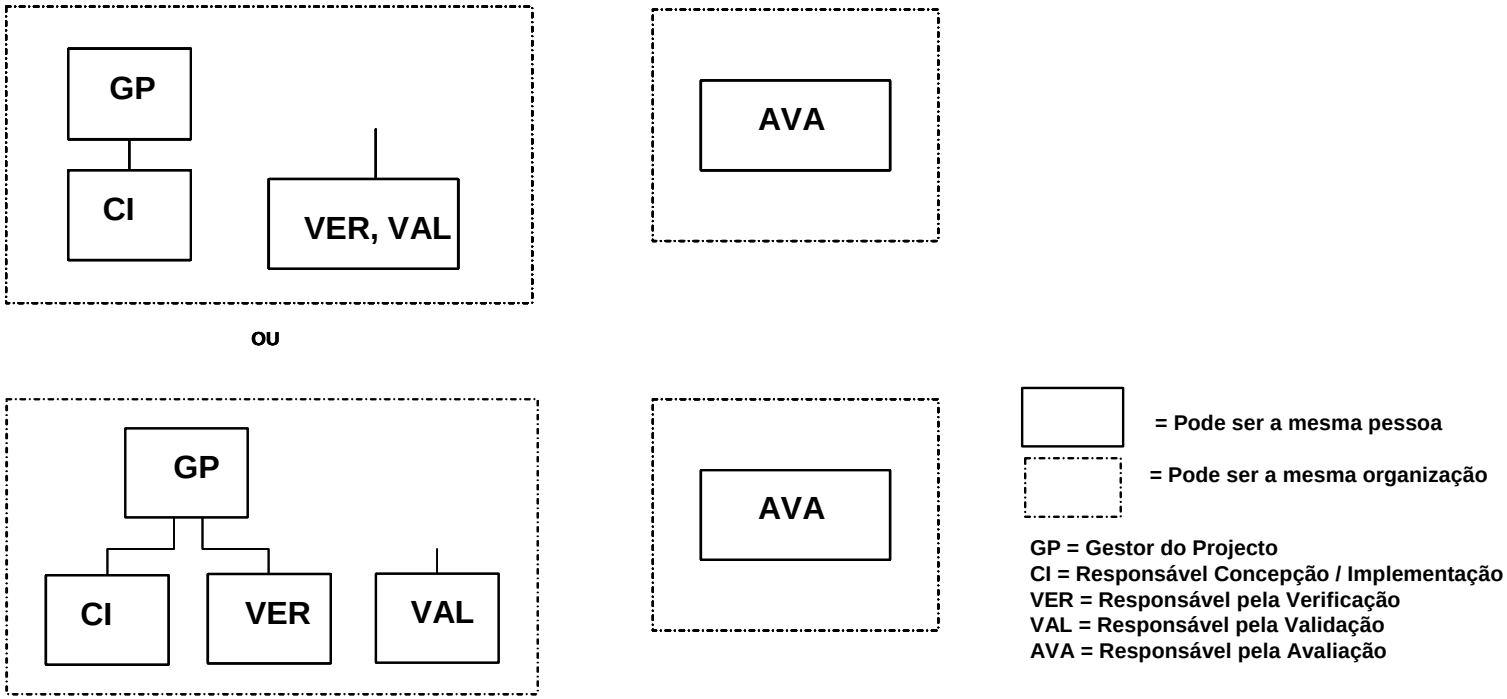
3

4

Safety Integrity Levels

- **Engenharia dos Sistemas Electrónicos**
  - Respostas da Engenharia:
    - » A gestão da segurança segundo a EN50129 e EN50128 para níveis de integridade SIL 3&4 obriga para as tarefas 7 e 8 à separação da entidade responsável pela Concepção & Implementação da entidade responsável pela Verificação e/ou Validação e uma entidade independente das duas na Avaliação

SIL 3 & SIL4



Obrigado pela atenção