SAA0187
Sistemas Aeronáuticos de Acionamento

Análise de falhas em sistemas aeronáuticos
Parte 3

Prof. Dr. Jorge Henrique Bidinotto

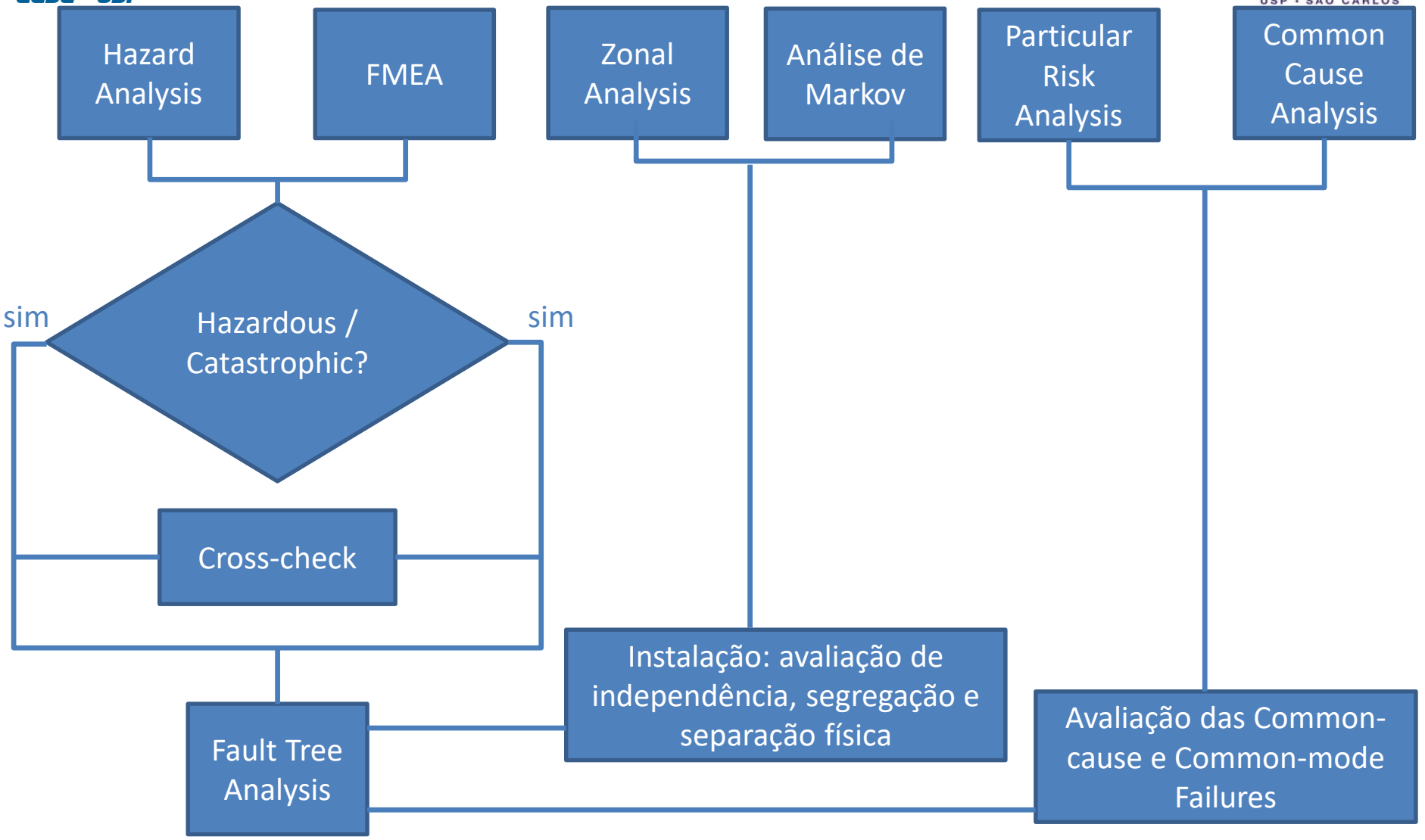
jhbidi@sc.usp.br

Tipos de análise

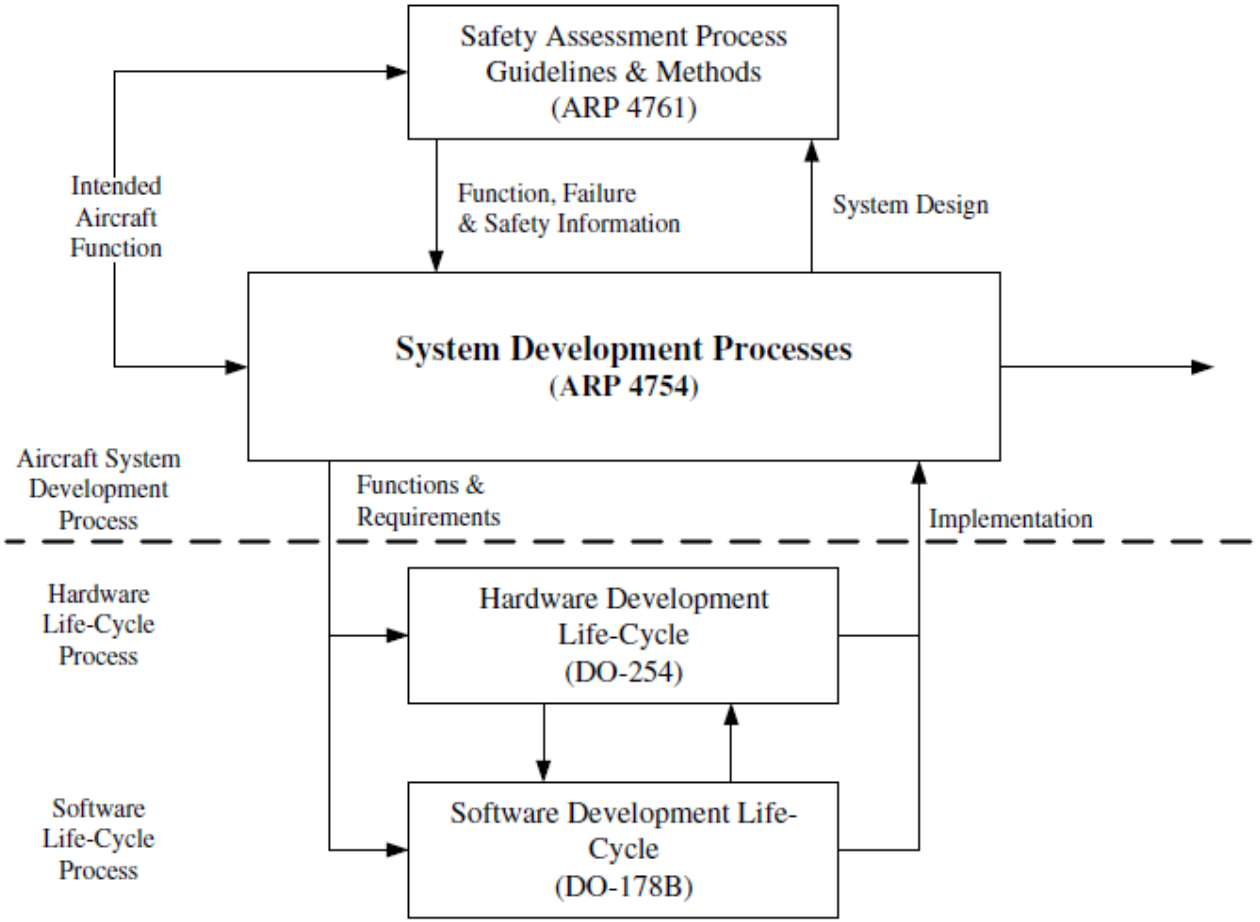
- Functional Hazard Analysis (FHA)
- Fault Tree Analysis (FTA)
- Failure Modes and Effect Analysis (FMEA)
- Análise de Markov
- Análise Zonal
- Particular Risk Analysis (PRA)
- Common-Mode Analysis (CMA)

Primárias

Aplicação de cada tipo de análise



Documentação envolvida



Documentação envolvida

DO-178B Overview Design Assurance for Airborne Software (1 December 1992)

- Introduction
- System Aspects relating to Software Development
- Software Life Cycle
- Software Planning Process
- Software Development Process
- Software Verification Process
- Software Configuration Management Process
- Software Quality Assurance Process
- Certification Liaison Process
- Overview of Aircraft and Engine Certification
- Software Life Cycle Data
- Additional Considerations

DO-254 Overview – Design Assurance Guidance for Airborne Electronic Hardware (April 2000)

- Introduction
- System Aspects of Hardware Design Assurance
- Hardware Design Life Cycle
- Planning Process
- Validation and Verification Process
- Configuration Management Process
- Process (Quality) Assurance
- Certification Liaison
- Hardware Design Life Cycle Data
- Additional Considerations

System Development Processes – ARP 4754

- System development
- Certification process and coordination
- Requirements determination and assignment of development assurance level
- Safety assessment process
- Validation of requirements
- Implementation verification
- Configuration management
- Process assurance
- Modified aircraft

Methodologies and Techniques – ARP 4761

- Functional Hazard Assessment (FHA)
- Preliminary System Safety Analysis (PSSA)
- System Safety Analysis (SSA)
- Fault Tree Analysis (FTA)
- Dependency Diagrams
- Markov Analysis (MA)
- Failure Modes and Effects Analysis (FMEA)
- Failures Modes and Effects Summary (FMES)
- Zonal Safety Analysis (ZSA)
- Particular Risks Analysis (PRA)
- Common Mode Analysis (CMA)
- Contiguous safety assessment process example

Functional Hazard Analysis

- Análise do tipo Top-down
  - Parte-se do nível mais alto da falha até se chegar no componente
- Deve ser imaginada todas as possíveis falhas
- Para esse tipo de análise, utiliza-se o chamado “pessimismo moderado”
- Para cada análise é preenchido um formulário como o indicado abaixo
  - Outros formatos podem ser utilizados, desde que tenham as mesmas informações

Functional Hazard Analysis (FHA) Form

Higher Level Function:							
Function	Failure Condition	Flight Phase	Effect of Failure			Hazard Classification	Remarks
			Aircraft	Crew	Occupants		

Functional Hazard Analysis

- Exemplo
  - Perda/dano do sistema de freios

Failure Modes and Effects Analysis (FMEA)

- Mesmo princípio do FHA, porém em análise bottom-up
- A análise parte da falha de cada tipo de componente (parafuso, fusível, etc.) e vê sua consequência no funcionamento do sistema
- Em geral, essas falhas devem ser suprimidas pelo próprio sistema
- Formulário sugerido para o FMEA:

Failure Mode and Effect Analysis (FMEA) Form

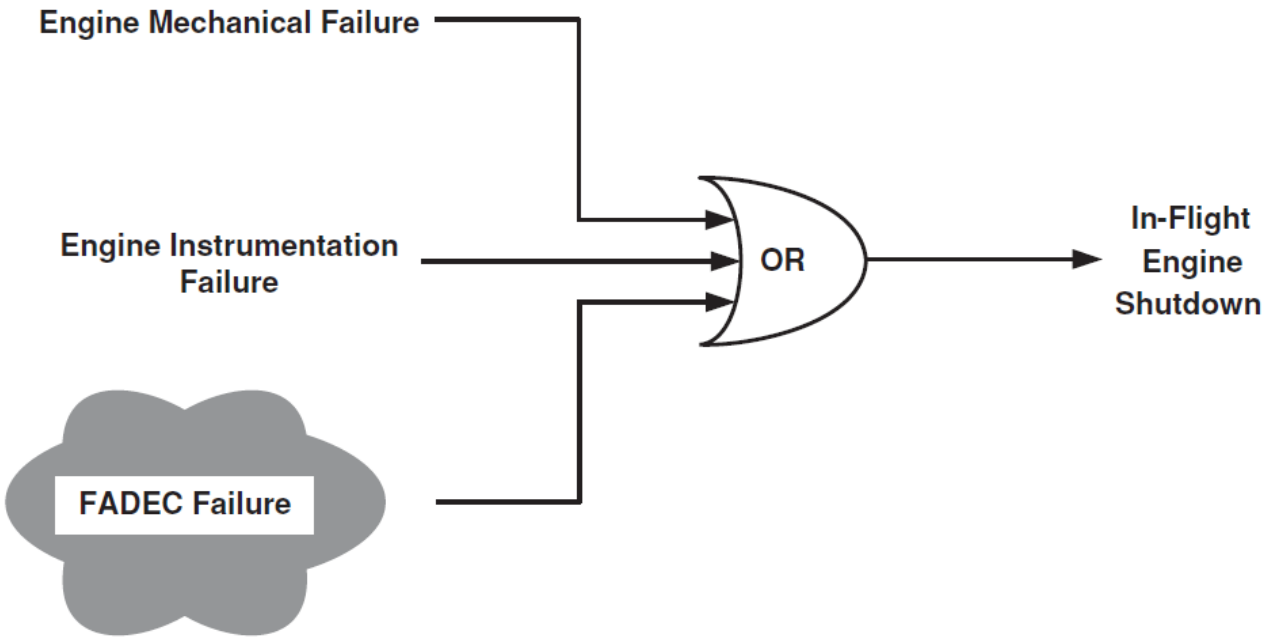
System:	
Component:	
Function:	

P/N	Part Type	Failure Mode	Flight Phase	Failure effect on component output	Failure effect on next level	Detection method	Comments

Análise de Markov

- Analisa o “caminho” das múltiplas falhas que devem acontecer em componentes até que haja a falha no sistema

- Exemplo: falha em motor do tipo Engine In-flight Shut Down (IFSD)

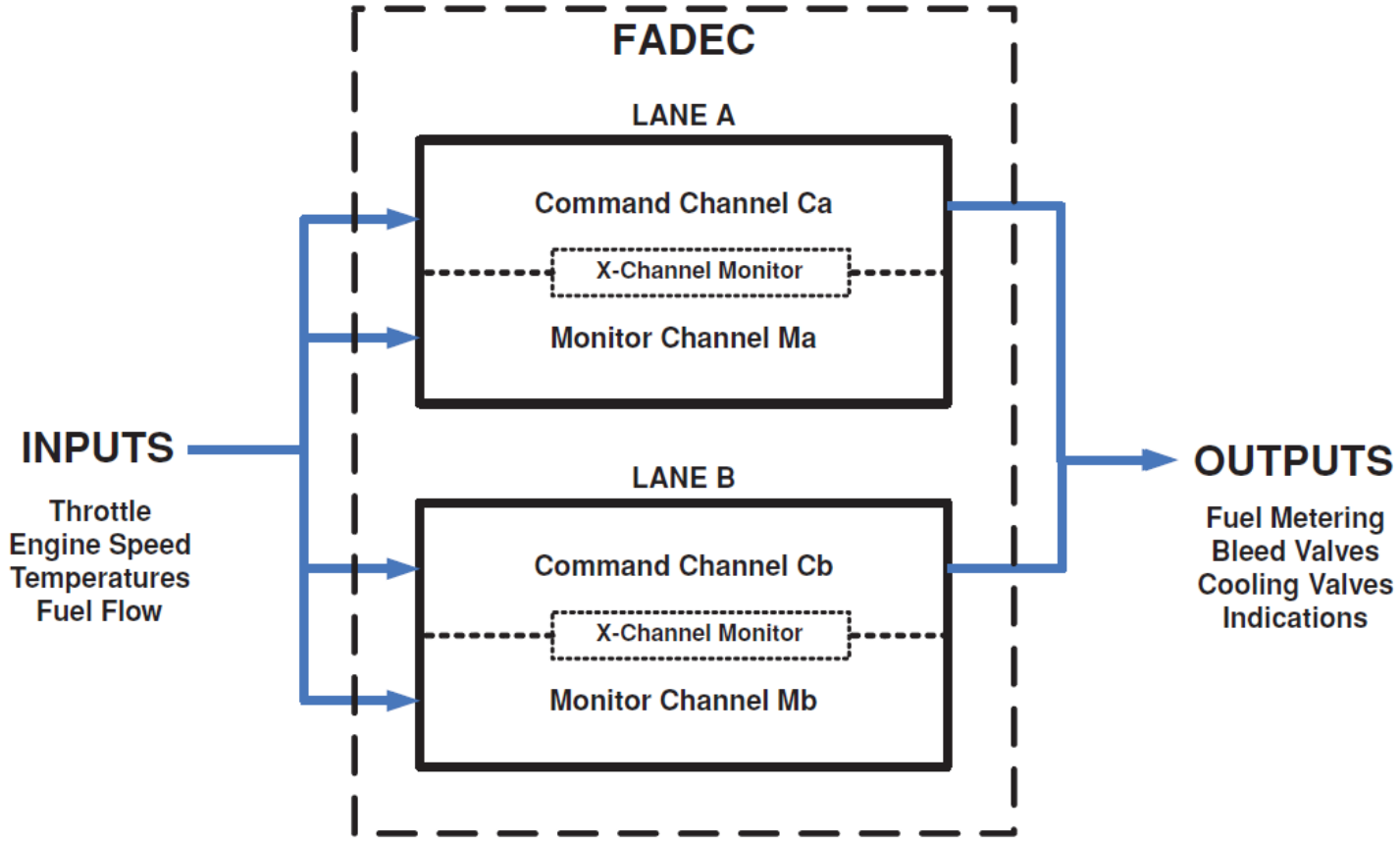


Análise de Markov

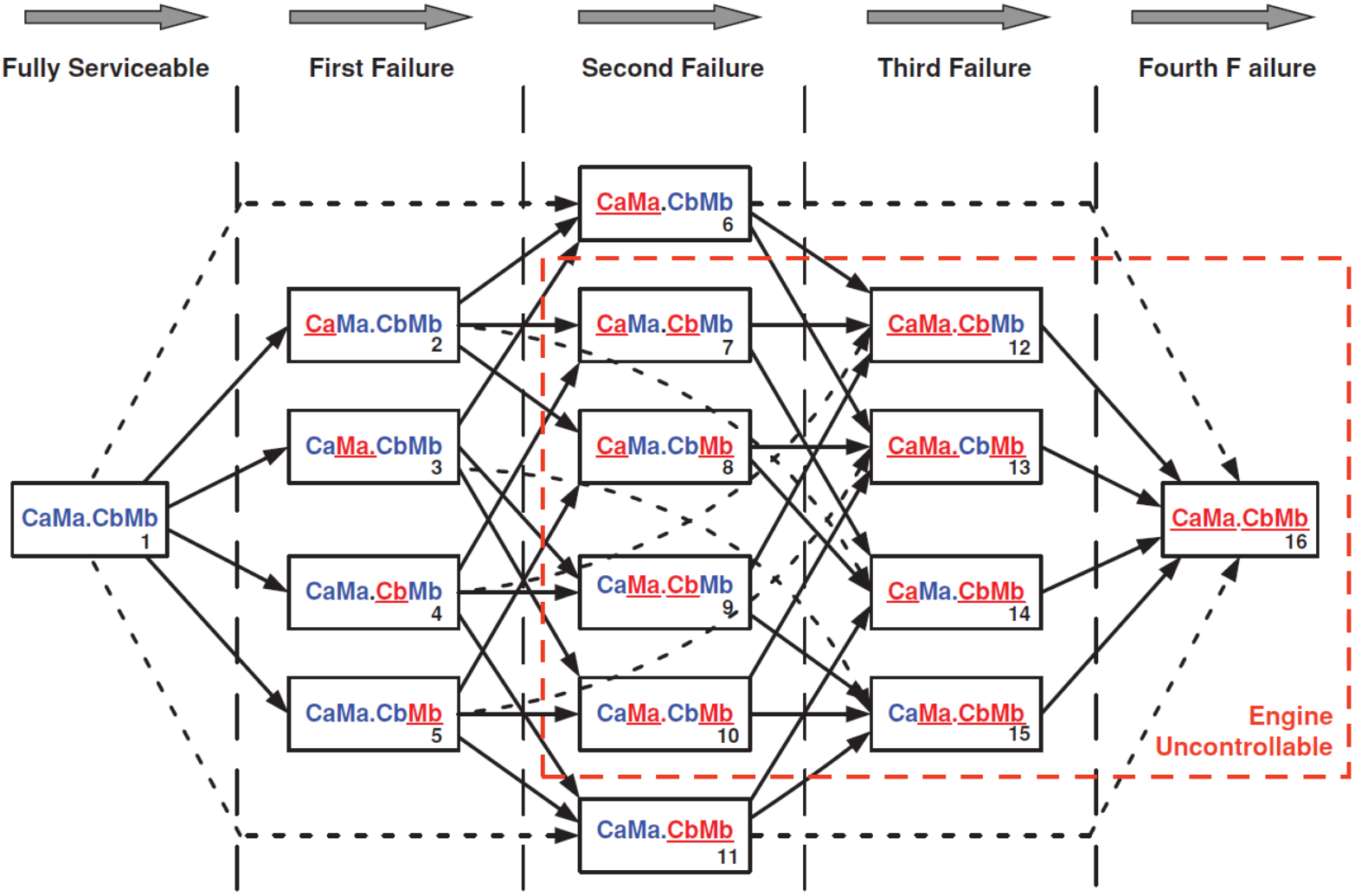
- Arquitetura do sistema:

  - O FADEC (Full Authority Digital Engine Control) é construído em dois canais independentes (Lane A / Lane B) e cada um deles possui Comando-monitor (COM:MON)

Análise de Markov



Análise de Markov

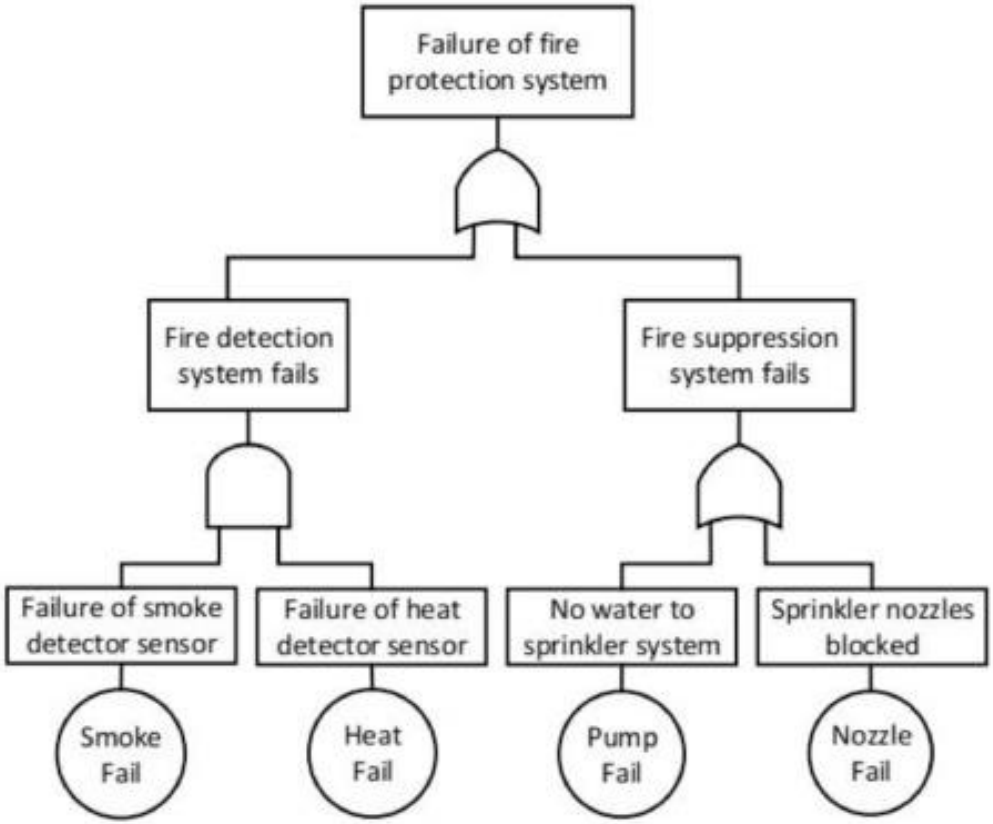


Fault Tree Analysis (FTA)

- Realizado para sistemas que apresentem classificação “Hazardous” ou “Catastrophic”
  - Análise top-down até o nível de componente
- Busca-se a probabilidade das diversas falhas e suas causas
- Pode afetar a arquitetura do sistema
  - Pela FTA pode se descobrir a necessidade de se incluir uma nova redundância, ou BIT, entre outras soluções

Fault Tree Analysis (FTA)

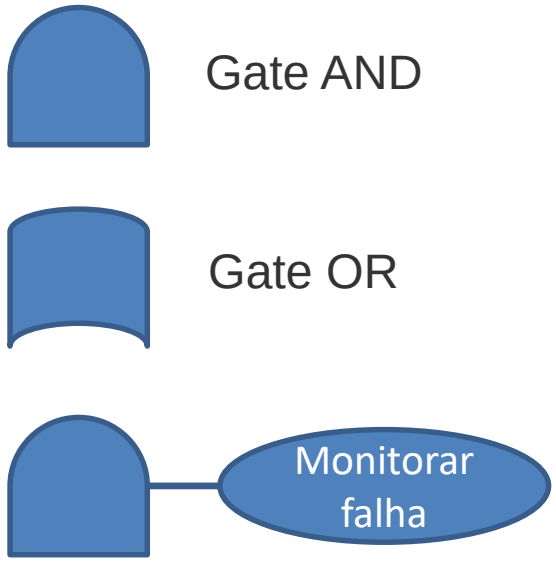
✓ Exemplo



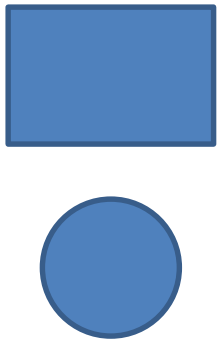
Fault Tree Analysis (FTA)

✓ Componentes de uma árvore

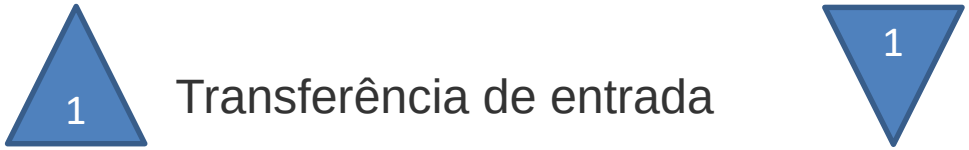
Símbolos Lógicos



Representação de eventos

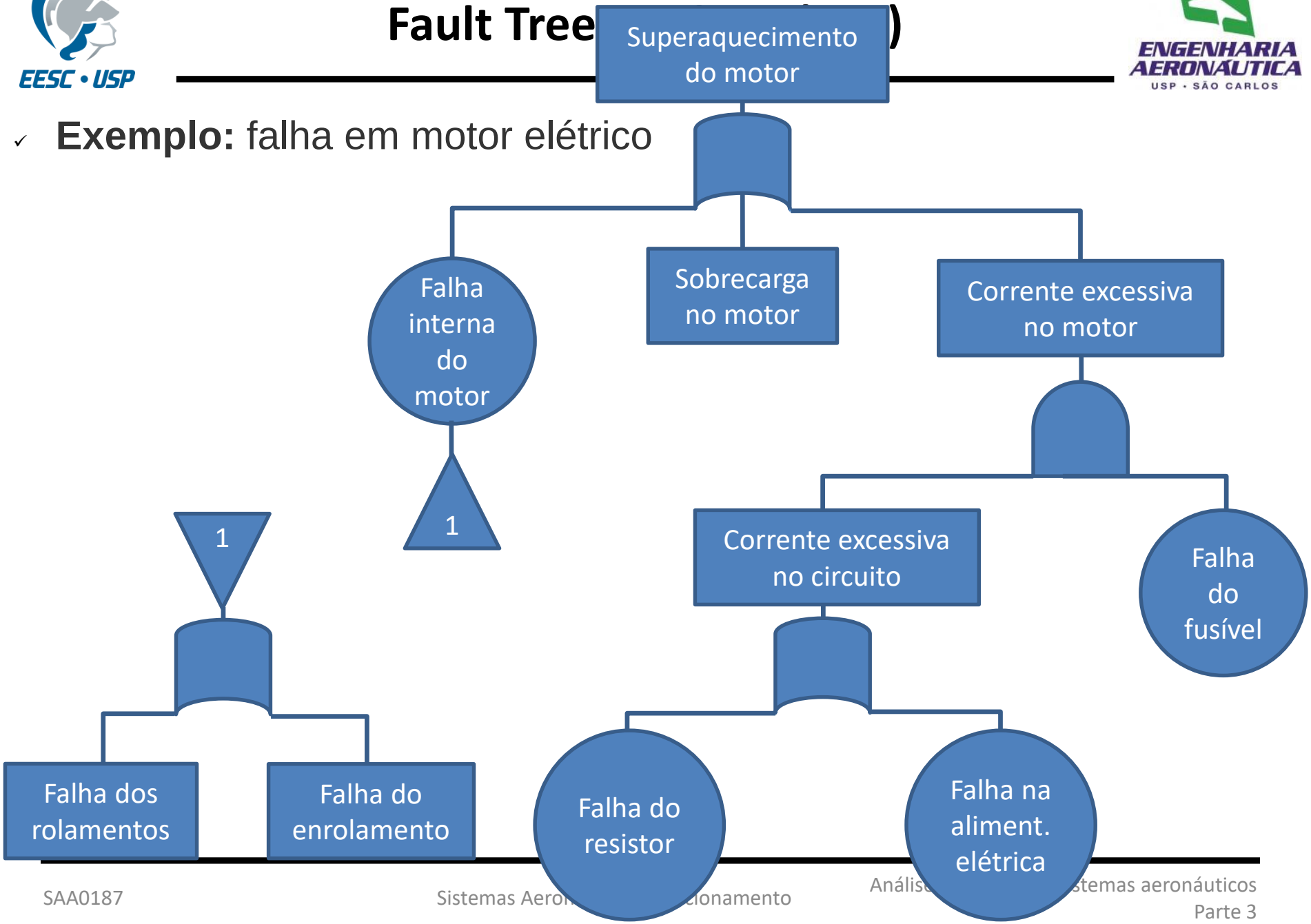


Transferência de eventos



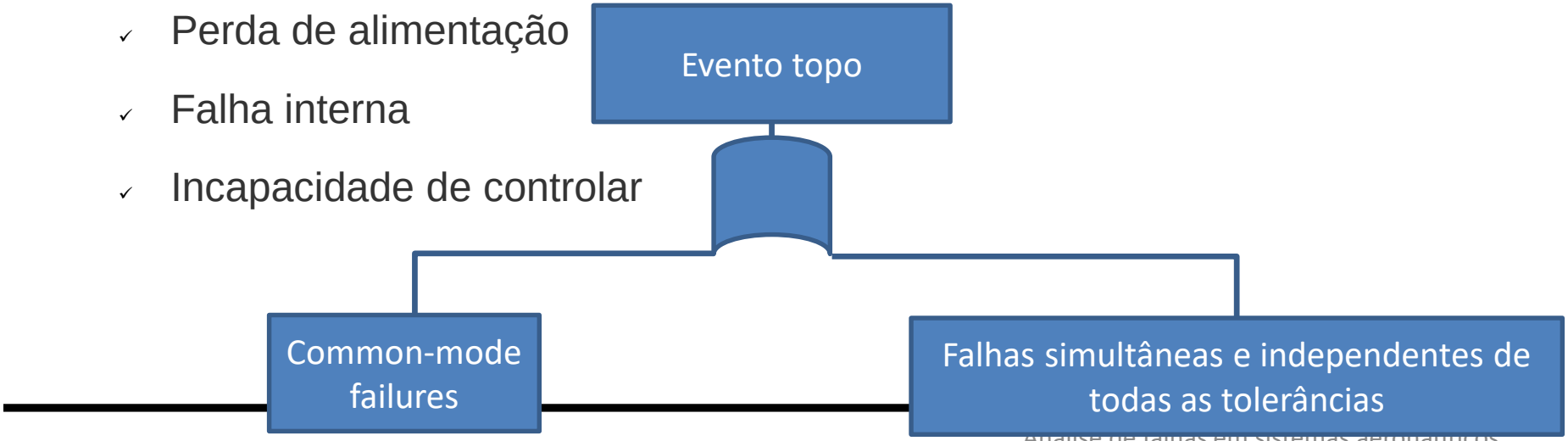
Fault Tree

- **Exemplo:** falha em motor elétrico



Fault Tree Analysis (FTA)

- **Montagem de uma árvore**
- Em geral coloca-se em um dos lados da primeira ramificação as falhas common-mode, e do lado oposto as falhas simultâneas e independentes
- Isso faz com que, no lado das common-modes, fiquem as falhas devido a fatores externos à aeronave
- Algumas das falhas geralmente presentes:
  - Perda de alimentação
  - Falha interna
  - Incapacidade de controlar

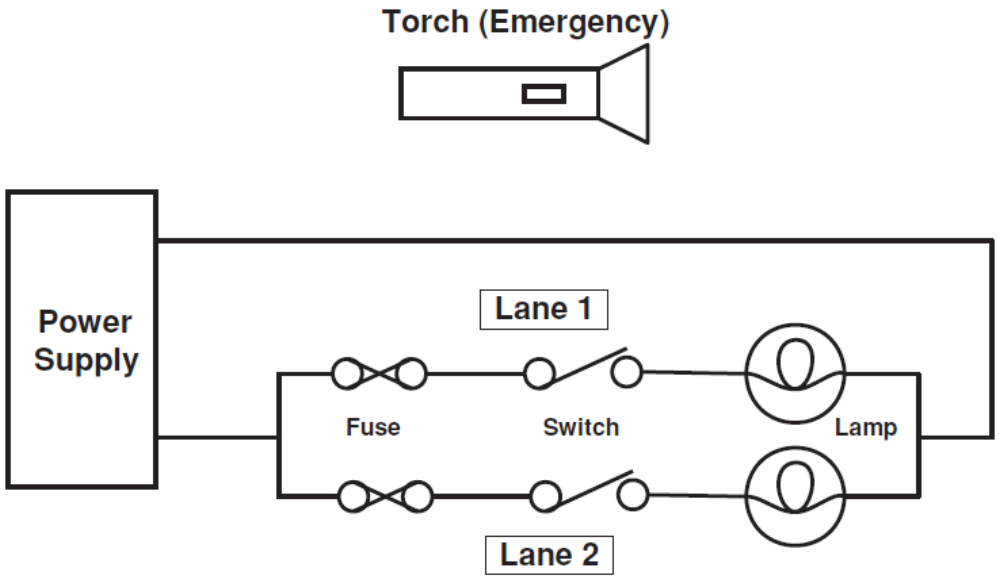


Fault Tree Analysis (FTA)

- **Exemplos**
- Analisar caso de perda simultâneas de dois motores (página 255, Serra, P.)
- Construir o seguinte exemplo:
  - Em uma casa com três televisores, avaliar a possibilidade de você não conseguir assistir à final da Copa América

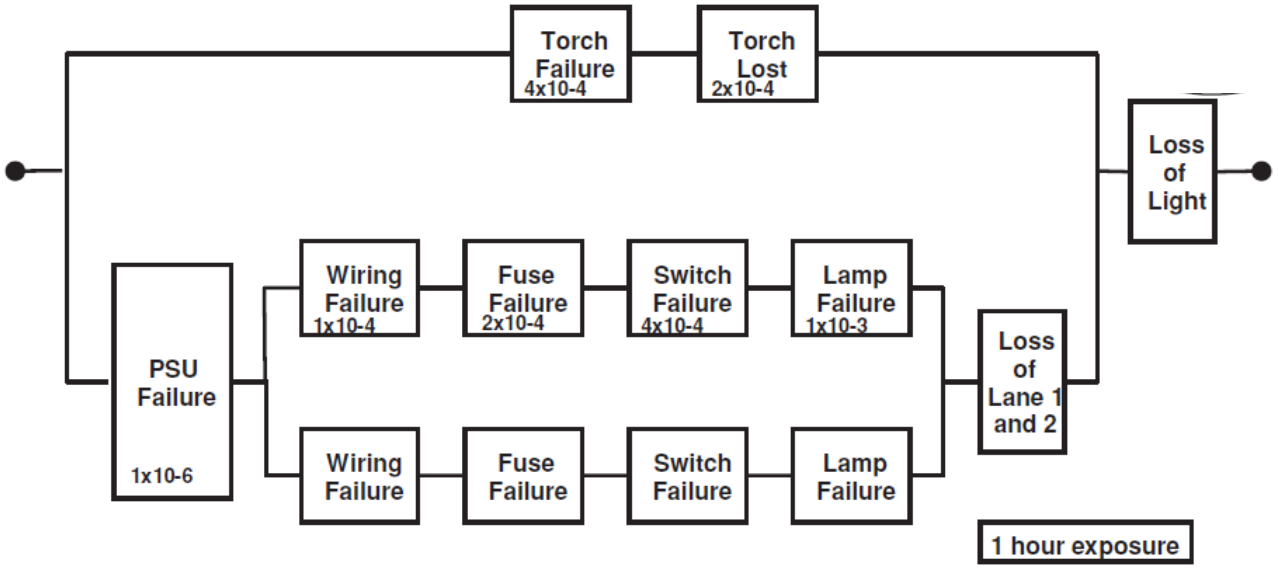
Fault Tree Analysis (FTA)

- **Exemplo numérico**
- Possibilidade de falha na iluminação
  - Sistema com redundância dupla e backup (lanterna)



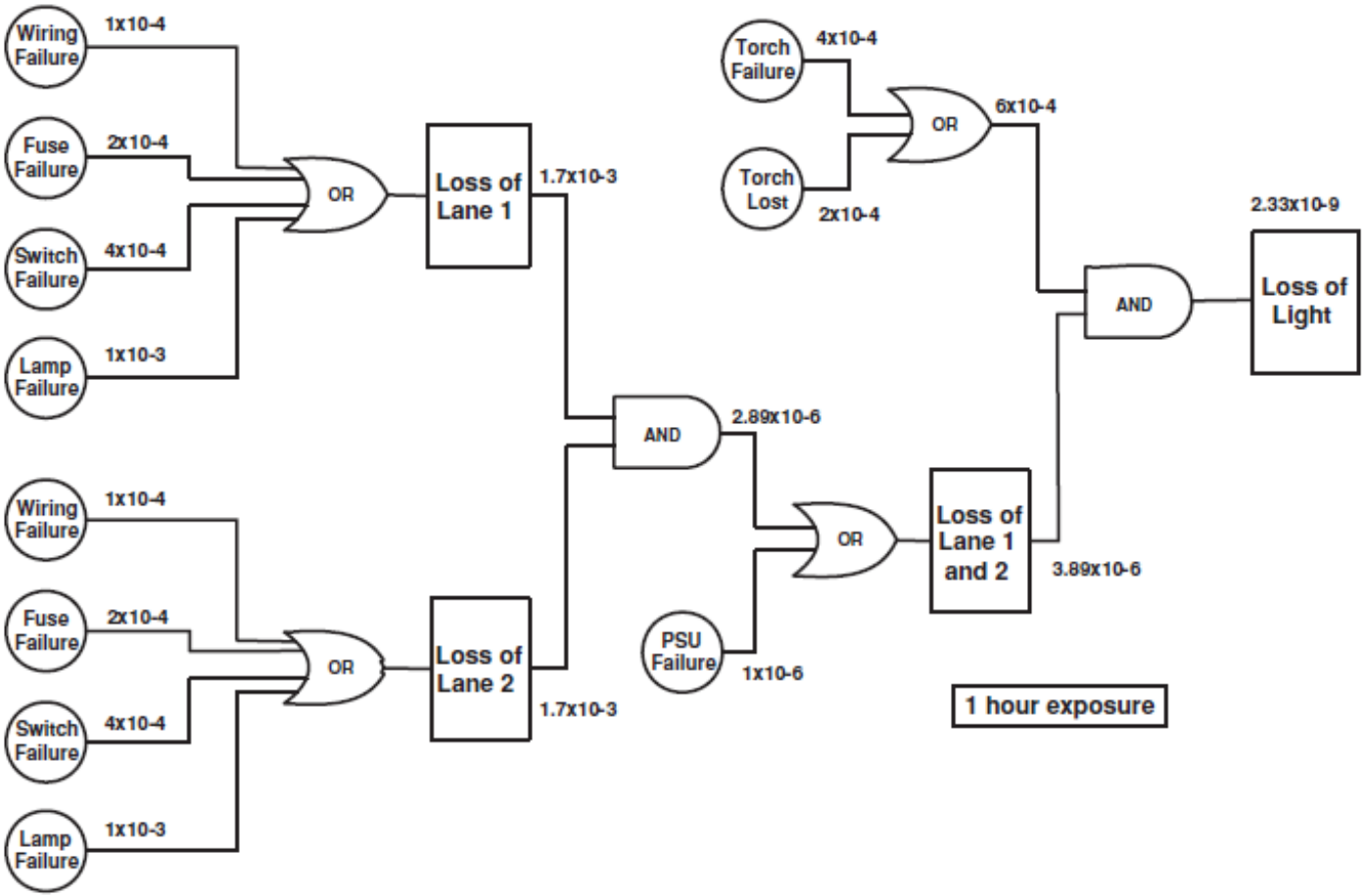
Fault Tree Analysis (FTA)

- **Exemplo numérico**
- Possibilidade de falha na iluminação
  - Sistema com redundância dupla e backup (lanterna)



Fault Tree Analysis (FTA)

✓ Exemplo numérico



Fault Tree Analysis (FTA)

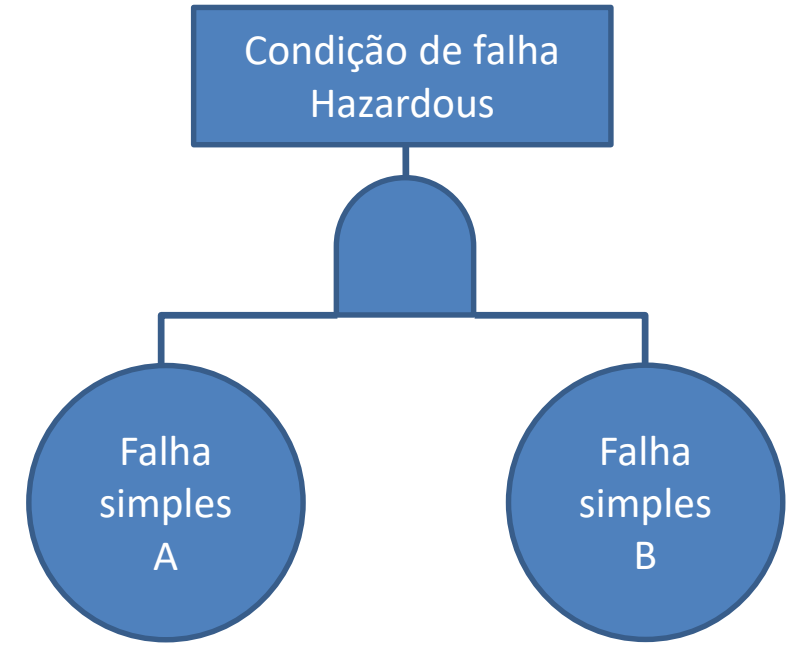
- **Manuais de confiabilidade de componentes**

- Fornecem, entre outras informações, uma estimativa de confiabilidade dos vários tipos de componente

  - MIL HDBK 978B – NASA Parts Application Handbook
  - RAC – Failure Mode and Mechanism Distribution
  - Rome Laboratory – Reliability Engineer's Tool Kit

Fault Tree Analysis (FTA)

- **Tempo de exposição**
- Considere o sistema



$\lambda_A = 1 \times 10^{-3}$ $\lambda_B = 1 \times 10^{-4}$

Para 2 horas de voo:

$$P = 2 \times (\lambda_A \times \lambda_B)$$

Deve-se aplicar o tempo de exposição apenas no final da análise

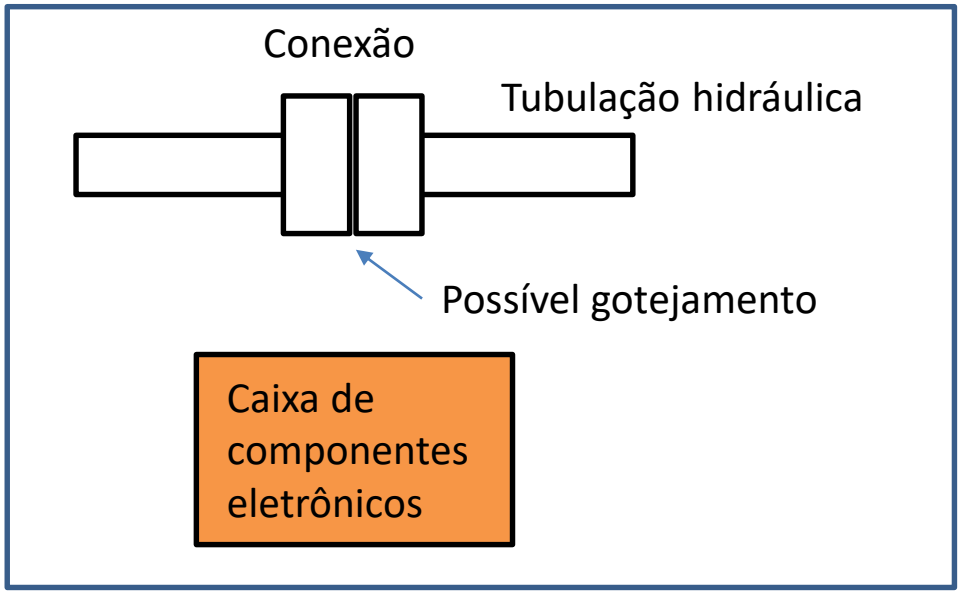
Em geral, a análise é feita por fases do voo, que possuem durações definidas e nem todos os equipamentos participam de todas as fases

Zonal Analysis (ZA)

- Análise baseada em localização física de componentes
- Realizada para operação de voo e para atividades de manutenção
- Busca informações sobre acessos, problemas em potencial, independência das árvores e falha, fatores ambientais, estre outros
- Antigamente era realizada em mockups de madeira em tamanho real. Hoje em dia pode ser feito em softwares de CAD

Zonal Analysis (ZA)

- Exemplos de problemas que podem ser encontrados via ZA:



Trabalho em campo (parte externa da aeronave) que não pode ser realizado com luvas, e deveria ser feito em pista, em possíveis condições de baixa temperatura

Falta de iluminação e/ou de espaço em determinadas regiões da aeronave, onde são realizadas atividades de manutenção

Particular Risk Analysis (PRA)

- Analisa situações de emergência e como elas podem acabar com a independência de funções redundantes
- Casos analisados:
- Incêndios
- Rotor non-containment
- Chamas em maçarico, devido a vazamento de fluidos
- Vazamento de ar quente
- Tubulações que desconectadas podem “chicotear” áreas adjacentes
- Explosão de vasos de pressão
- Estouro de pneus
- Soltura e ejeção de fragmentos de roda
- Desconexão, falha ou afrouxamento de terminais de atuadores

Particular Risk Analysis (PRA)

- Casos analisados:
- Eixos que podem se desconectar, “chicoteando” áreas adjacentes
- Vazamento de fluidos inflamáveis
- Vazamento de fluidos que possam congelar e obstruir drenos
- Desprendimento de pedaços de gelo e seu impacto com outras regiões da aeronave
- Granizo, gelo, lama, e detritos que possam ser atirados pelo pneu da aeronave
- Impacto com pássaros
- Raio
- Interferências eletromagnéticas
- FOD – danos causados por objetos estranhos, como ferramentas deixadas na aeronave

Particular Risk Analysis (PRA)

- Casos analisados:
- Descompressão súbita
- Pouso com trem recolhido
- Rotação excessiva na decolagem
- Atmosfera contaminada (cinzas vulcânicas, tempestade de areia, etc.)

Common-mode Analysis (CMA)

- Tem aspecto semelhante à PRA, pois busca situações onde a redundância perde sua validade
- A diferença é que, enquanto a PRA tem foco em situações de emergência, a CMA busca erros ou desvios de projeto
- Hardwares e Softwares em geral são muito afetados com esse tipo de análise
- A segregação é um forte aliado das CMAs

FIM