

SAA0187

Sistemas Aeronáuticos de Acionamento

Análise de falhas em sistemas aeronáuticos
parte 2

Prof. Dr. Jorge Henrique Bidinotto

jhbidi@sc.usp.br

§25.1309 Equipment, systems, and installations.

(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that—

(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and

(2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.

(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.

(d) Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider—

(1) Possible modes of failure, including malfunctions and damage from external sources.

(2) The probability of multiple failures and undetected failures.

(3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and

(4) The crew warning cues, corrective action required, and the capability of detecting faults.

(e) In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft.

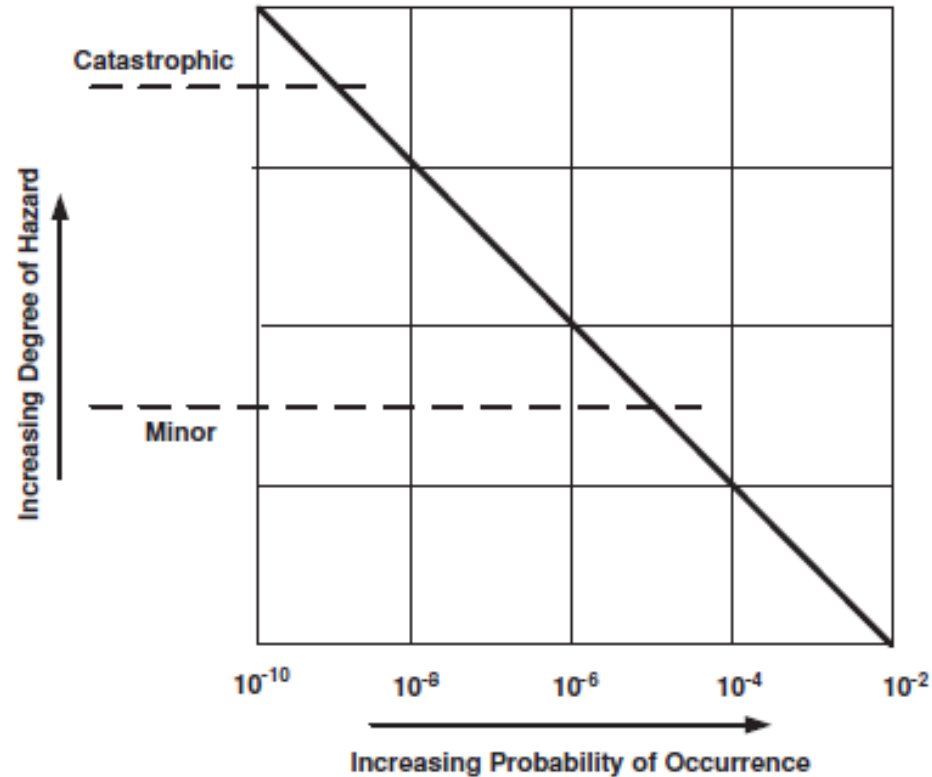
(f) EWIS must be assessed in accordance with the requirements of §25.1709.

- Década de 1970
- Surge o requisito FAR 25.1309

- Classificação segundo órgãos certificadores

Tipo	Efeito sobre a aeronave	Efeito sobre a tripulação	Efeito sobre os ocupantes
No safety effect	-	-	-
Minor (classe I)	Pequeno prejuízo na capacidade	Leve aumento da carga de trabalho	Efeitos físicos, mas sem ferimentos
Major (Classe II)	Pequena limitação	Redução da habilidade	Ferimentos leves
Hazardous (Classe III)	Grande limitação	Aumento da carga de trabalho a ponto de a tripulação não ser capaz de efetuar suas tarefas eficazmente	Ferimentos graves e/ou morte de pequena parcela dos ocupantes
Catastrophic (Classe IV)	Perda total		Morte de parcela considerável dos ocupantes

- Classificação segundo órgãos certificadores



- Classificação segundo órgãos certificadores

EFFECT ON AIRCRAFT AND OCCUPANTS	Normal	Nuisance	Operating limitations; emergency procedures	Significant reduction in safety margins; difficult for crew to cope with adverse conditions; passenger injuries	Large reduction in safety margins; crew extended because of workload or environmental conditions; serious injury or death of small number of occupants	Multiple deaths; usually with loss of aircraft	EFFECT ON AIRCRAFT AND OCCUPANTS
FAR 25 PROBABILITY	←-----→			←-----→		←-----→	FAR 25 PROBABILITY
JAR 25/CS PROBABILITY	←-----→		←-----→	←-----→	←-----→	←-----→	JAR 25/CS PROBABILITY
FAILURE RATE (per flight hour)		10^{-3}	10^{-5}	10^{-7}	10^{-9}		
CATEGORY OF EFFECT	←-----→		←-----→	←-----→	←-----→	←-----→	CATEGORY OF EFFECT
		MINOR		MAJOR	HAZARDOUS	CATASTROPHIC	

- **Aspectos quantitativos**

- Para se quantificar o índice aceitável de acidentes, criaram-se métricas correspondentes

- Criou-se a “entidade” 10^{-9}

- Sua origem:

- 1. Eventos catastróficos poderiam surgir a cada 1 milhão de horas de voo (10^{-6})
- 2. Falhas em sistemas eram consideradas 1/10 das causas desses eventos em aeronaves
- 3. Considerou-se que as aeronaves possuíam 10 sistemas
- 4. Cada sistema era suscetível a 10 falhas diferentes

- Aspectos quantitativos
- Na prática:
- Considere que uma aeronave voa 10h/dia; 300 dias/ano
 - 3000 horas/ano
- Considere que a vida de uma aeronave é de 20 anos
 - 60.000 horas em sua vida
- Uma frota de 200 aeronaves deve acumular 12.000.000 de horas
 - Ou seja: $1,2 \times 10^7$ horas
- Hoje em dia os sistemas já trabalham com a meta de probabilidade de falhas catastróficas em 10^{-12}

- **Definições**
- **Falha** – quando um item é incapaz de desempenhar sua função dentro dos limites especificados
- **Mau-funcionamento (malfunction)** – quando o item opera fora dos seus limites pré-estabelecidos
- **Fault** – Mudança de estado que, se não houver ação corretiva, pode levar a um mau-funcionamento
- **Evento** – ocorrência com origem fora da aeronave, não causado por um componente interno (ex.: impacto com pássaros, turbulência, etc.)
- **Erro** – Ocorrência causada por uma ação ou decisão incorreta da tripulação, manutenção, etc.

- **Classificação das falhas**
- **Falhas simples ou ativas (single active failures)** – produzem efeitos imediatos e perceptíveis (ex.: queima de lâmpada)
- **Falhas passivas ou dormentes (passive, hidden ou dormant failures)** – falhas que não produzem efeito perceptível e imediato, mas ficarão evidentes quando ocorrer uma segunda falha (ex.: falha de sensores ou alarmes)
- **Falhas de modo comum ou de causa comum (commom-mode/commom-cause failures)** – Falhas que invalidam redundâncias, provocando falhas simultâneas e que teoricamente seriam independentes (ex.: estouro de pneu que ejeta pedaços em superfícies aerodinâmicas)

- **Classificação das falhas**
- **Falhas em cascata (cascade failures)** – uma variação das falhas simples, onde não há contenção e se propaga, gerando novas falhas
- **Falhas ambientais (environmental failures)** – causadas pela sensibilidade de certos equipamentos a fatores ambientais, como vibração, umidade, temperatura, etc.
- **Falhas de performance** – o item desempenha sua função, mas fora dos limites especificados
- **Runaways** – Quando não há proporcionalidade entre o comando e a resposta (ex.: comando de profundor respondendo mais que o solicitado)
- **Hardover** – disparo inadvertido de algum comando

- **Conceitos importantes:**
 - Confiabilidade
 - Disponibilidade
 - Integridade
 - Redundância
 - Dissimilaridade
 - Segregação
- } Independência

- **Medidas de Confiabilidade**
- MTBF – Mean Time Between Failure:
- (Tempo Médio Entre Falhas)
- Em algumas literaturas, chamado de Tm
- Deve ser medido em grande amostragem de aeronaves, em grande espaço se tempo
- Pode variar para diferentes regiões, temperaturas, tipos de operação, etc.
- Exemplo: um determinado componente falhou 10 vezes em 10.000 horas, logo:

$$MTBF = \frac{10.000}{10} = 1.000 \text{ horas}$$

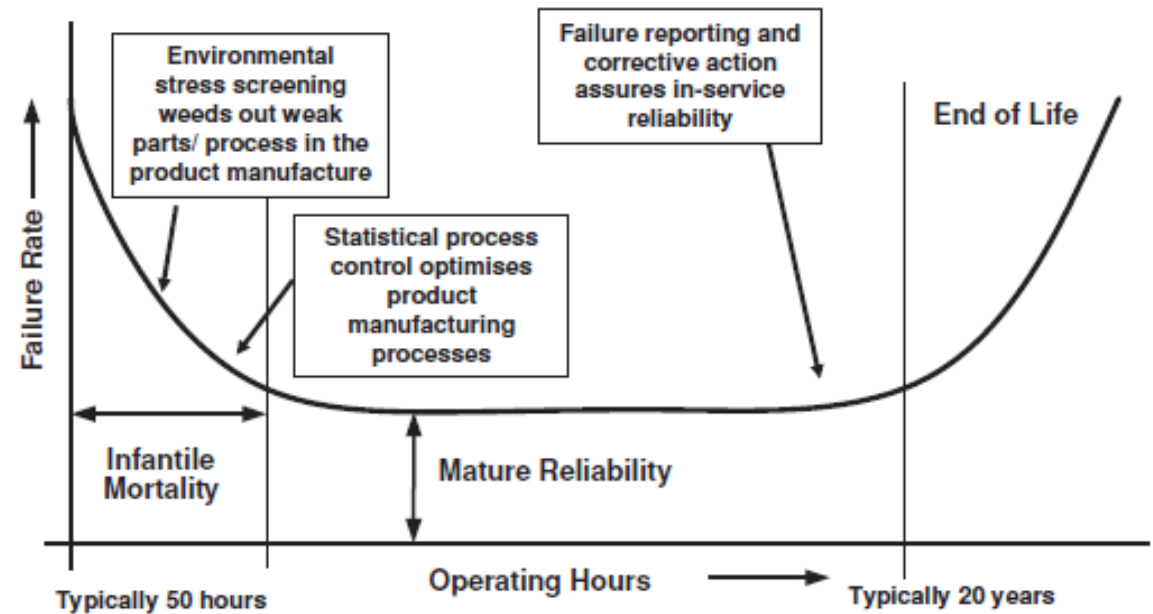
- **Medidas de Confiabilidade**

- Failure Rate (λ):

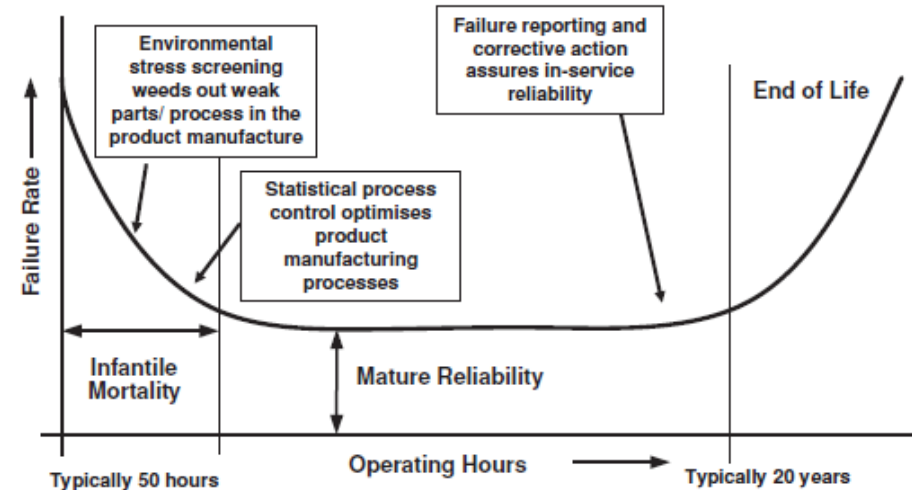
- Inverso do MTBF

$$\lambda = \frac{1}{MTBF}$$

- Varia ao longo da vida operacional de um item



- **Medidas de Confiabilidade**
- Failure Rate (λ):
- A “curva da banheira” é medida com o item em bancada, sendo estressado ao extremo de seu funcionamento
- Itens sujeitos a sobrecarga em algum momento de sua vida, tendem a reduzir a curva, diminuindo a fase de maturidade



- **Medidas de Confiabilidade**

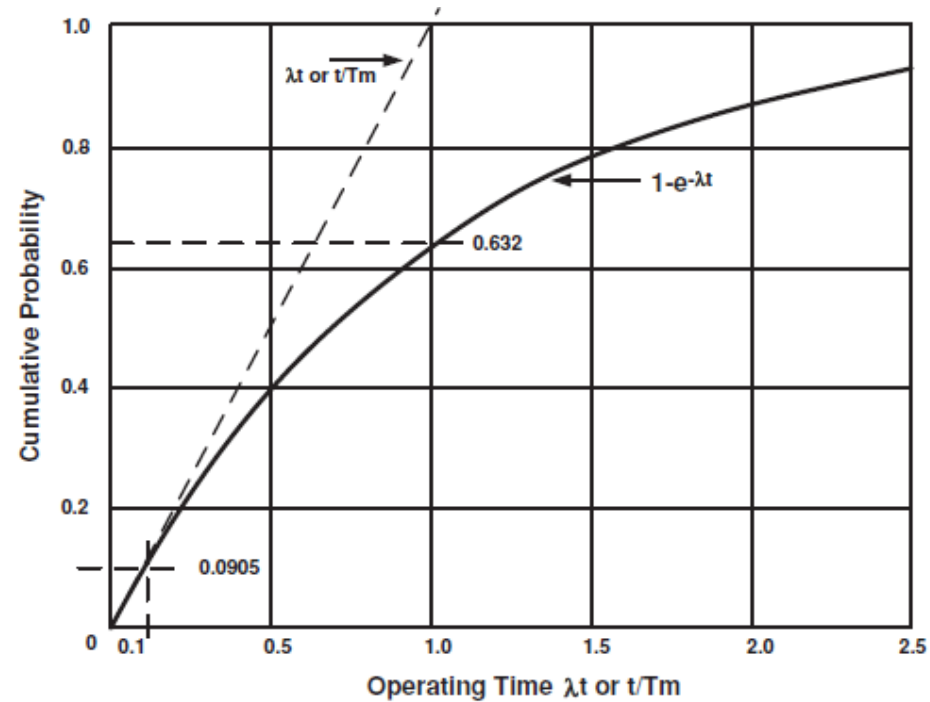
- Probabilidade de falha:

- A probabilidade de um item falhar depende do seu tempo de exposição t , e é dada por

$$P = 1 - e^{-\lambda t}$$

- Para λt pequenos:

$$P = \lambda t$$



- **Medidas de Disponibilidade**
- Estatística em Probabilidade de falha:
- evento1 **E** evento2 : produto
- evento1 **OU** evento2 : soma
- Exemplo: a probabilidade de se obter COROA em dois lançamentos de moeda

Evento	Moeda 1	Moeda 2	Probabilidade
1	CARA	CARA	$0,5 \times 0,5 = 0,25$
2	CARA	COROA	$0,5 \times 0,5 = 0,25$
3	COROA	CARA	$0,5 \times 0,5 = 0,25$
4	COROA	COROA	$0,5 \times 0,5 = 0,25$

**Em 6 lançamentos:
Ocorrência de evento 1 OU 2 OU 3**

$$0,25 + 0,25 + 0,25 = 0,75 = 75\%$$

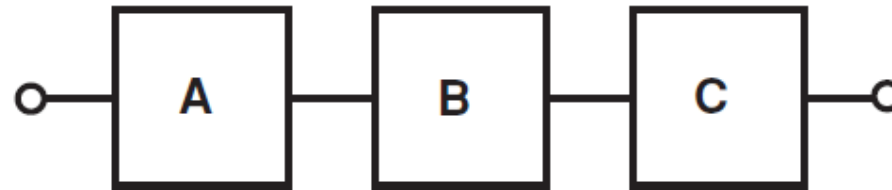
**Em 6 lançamentos:
Ocorrência de evento 1 E 2 E 3**

$$0,25 \times 0,25 \times 0,25 = 0,015 = 1,5\%$$

- **Medidas de Disponibilidade**
- Estatística em Probabilidade de falha:
- Aplicação para o caso aeronáutico (duas LRUs em operação)

LRU A	LRU B	Probability
Operational	Operational	$\lambda = (1 - \lambda_A) \times (1 - \lambda_B)$
Operational	Failed	$\lambda = (1 - \lambda_A) \times \lambda_B$
Failed	Operational	$\lambda = \lambda_A \times (1 - \lambda_B)$
Failed	Failed	$\lambda = \lambda_A \times \lambda_B$

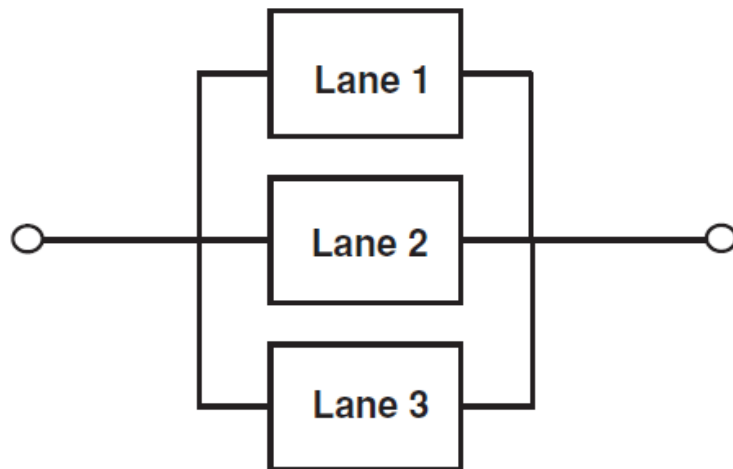
- **Medidas de Disponibilidade**
- Estatística em Probabilidade de falha:
- Três sistemas operando em série



- Probabilidade de falha do sistema (OU):

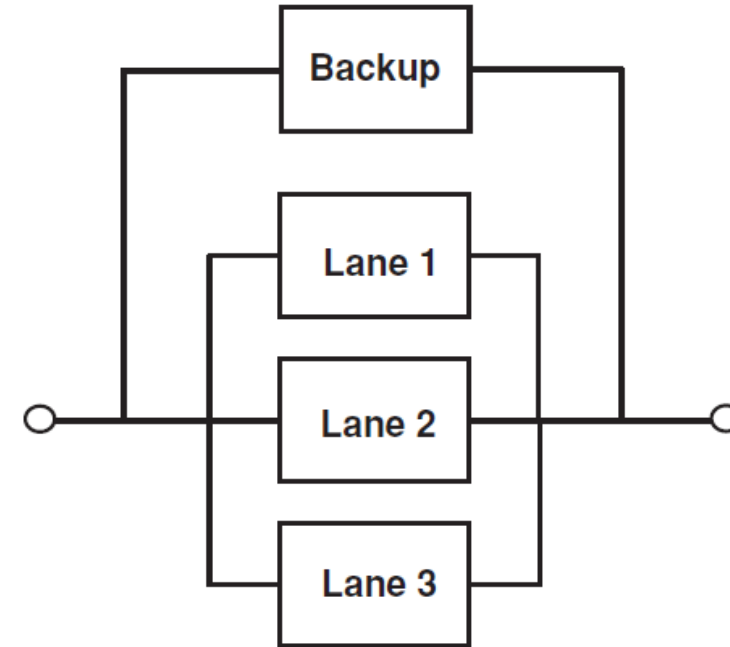
If $\lambda_A = 3.0 \times 10^{-4}/\text{hr}$ (MTBF = 3333 hrs)
 $\lambda_B = 5.0 \times 10^{-4}/\text{hr}$ (MTBF = 2000 hrs)
 $\lambda_C = 2.0 \times 10^{-4}/\text{hr}$ (MTBF = 5000 hrs)
 Then $\lambda = (3.0 + 5.0 + 2.0) \times 10^{-4}/\text{hr} = 1 \times 10^{-3}/\text{hr}$

- Medidas de Disponibilidade
- Estatística em Probabilidade de falha:
- Arquitetura triplex



If $\lambda_1 = \lambda_2 = \lambda_3 = 1.0 \times 10^{-3}/\text{hr}$;
 Then $\lambda = (1.0 \times 10^{-3})^3 = 10^{-9}/\text{hr}$
 $= (5.0 \times 10^{-3})^3 = 1.25 \times 10^{-7}$ for a 5-hour flight

- Medidas de Disponibilidade
- Estatística em Probabilidade de falha:
- Arquitetura tríplex com backup

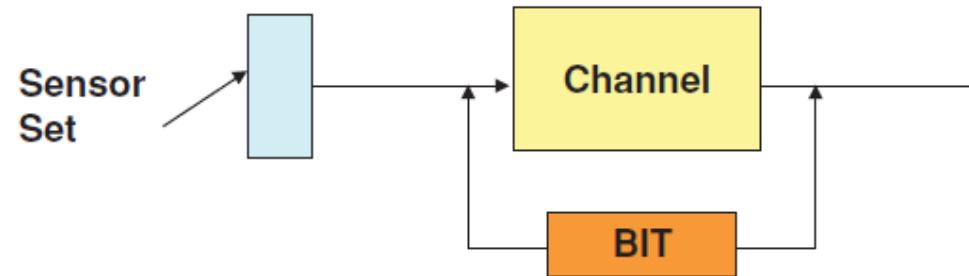


If $\lambda_1 = \lambda_2 = \lambda_3 = 1.0 \times 10^{-3}/\text{hr}$; and $\lambda_B = 1.0 \times 10^{-2}/\text{hr}$
 then $\lambda = (5.0 \times 10^{-3})^3 \times (1.0 \times 10^{-2}) = 1.25 \times 10^{-9}$ for a 5-hour flight with 1-hour emergency

- **Medidas de Disponibilidade**
- Estatística em Probabilidade de falha:
- Em geral...
 - **Minor** – a simplex architecture will probably meet the safety objectives.
 - **Major** – a duplex architecture is likely to meet the safety objectives.
 - **Hazardous** – a triplex architecture is almost certainly required.
 - **Catastrophic** – a quadruplex or triplex plus backup architecture will be necessary.

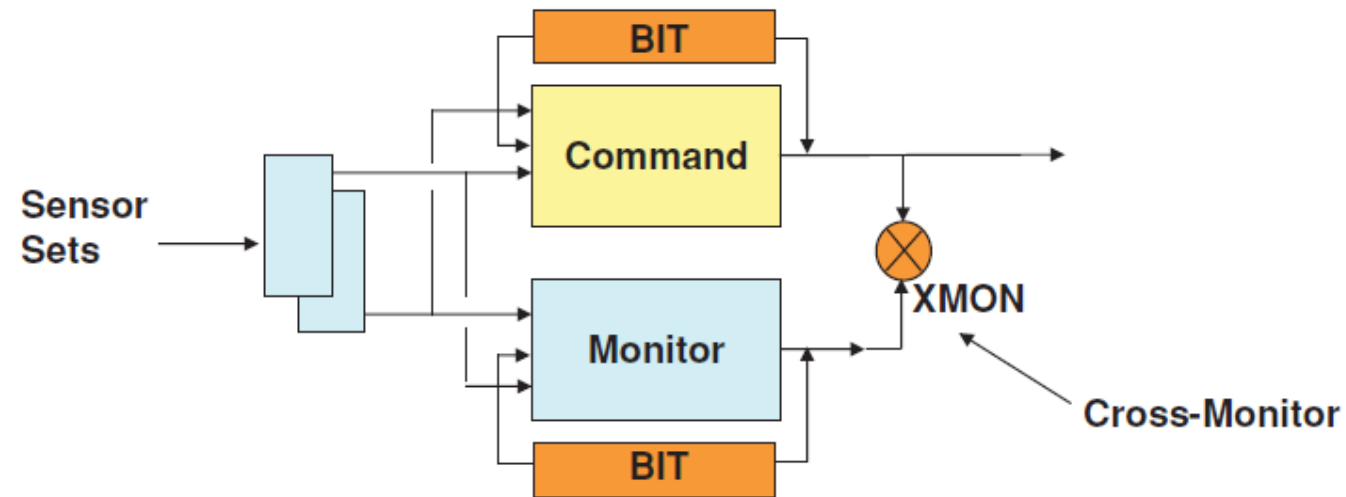
- **Integridade**
- Definição: ter o sistema disponível e trabalhando corretamente
- Pode afetar a análise de risco de diferentes formas, conforme o tipo de perda de integridade.
Exemplo:
 - Perda de informações primárias (altitude, velocidade, atitude e proa) é considerado “hazardous”
 - Informações primárias erradas é considerado “catastrophic”
- Existem duas formas principais de se garantir integridade em sistemas aeronáuticos
 - Built-in-Test (BIT)
 - Cross-Monitoring (XMON)

- **Integridade**
- Built-in-Test (BIT):
- Pode ser dos seguintes tipos:
 - Power-up ou Statup BIT
 - Interruptive BIT
 - Continuous BIT

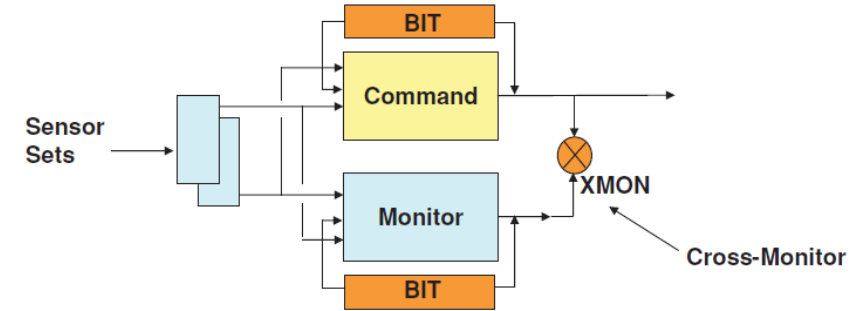


- Em termos de probabilidade de falha
 - **Probabilidade de perda da função (disponibilidade): λ_c**
 - Probabilidade de perda não-anunciada da função (integridade): $\lambda_c \times \lambda_B$

- **Integridade**
- Cross-Monitoring (XMON):
- Sistemas de canais independentes monitoram o funcionamento do comando e a confiabilidade de seu sinal
- Ambos sinais são computados no XMON

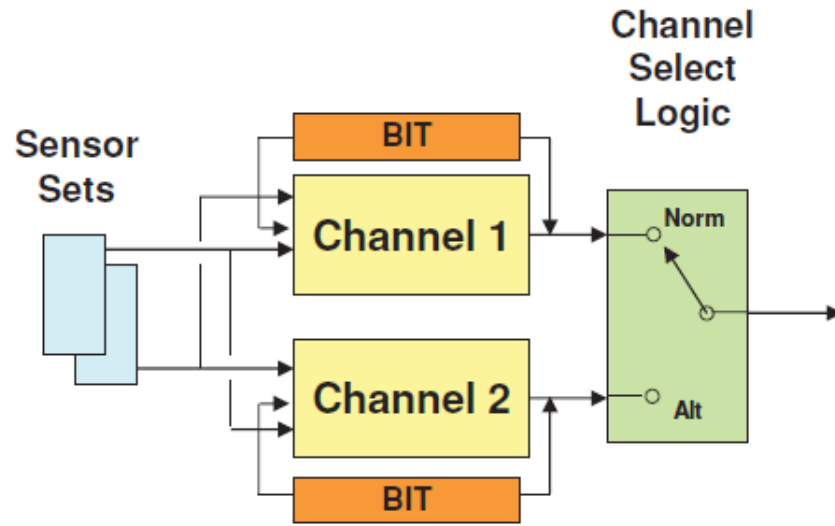


- Integridade
- Cross-Monitoring (XMON):
- Início do conceito de dissimilaridade
- Em termos de probabilidade de falha
 - Probabilidade de perda do canal de comando: λ_C
 - Probabilidade de falha do BIT: λ_B
 - Probabilidade de falha do XMON: λ_{XMON}
 - Probabilidade de falha do canal de monitoramento: λ_M
 - Probabilidade de um alarme falso: $\lambda_C + \lambda_M + \lambda_{XMON}$
 - Probabilidade falha não-anunciada do canal de comando: $\{\lambda_C(1 - \lambda_B) + \lambda_M(1 - \lambda_B)\} \times \lambda_{XMON}$

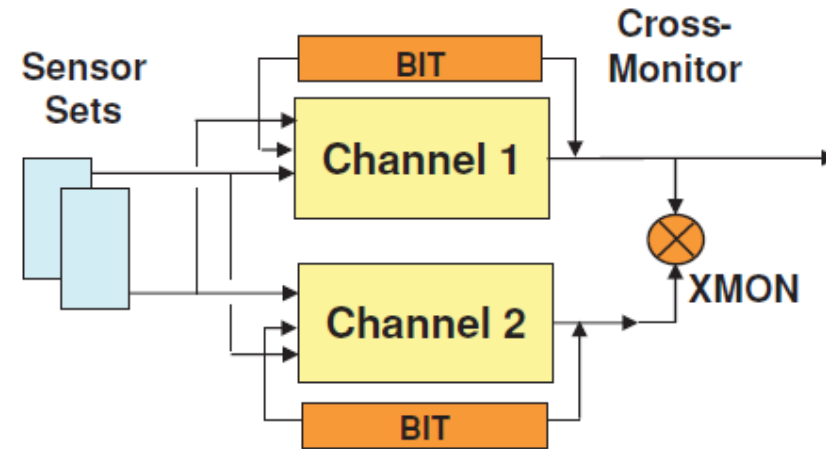


- **Redundância**
- Tipos de arquitetura:
 - Simplex
 - Redundância Duplex
 - Redundância Dual
 - Redundância Triplex
 - Redundância Quadruplex

- Redundância
- Arquitetura Duplex

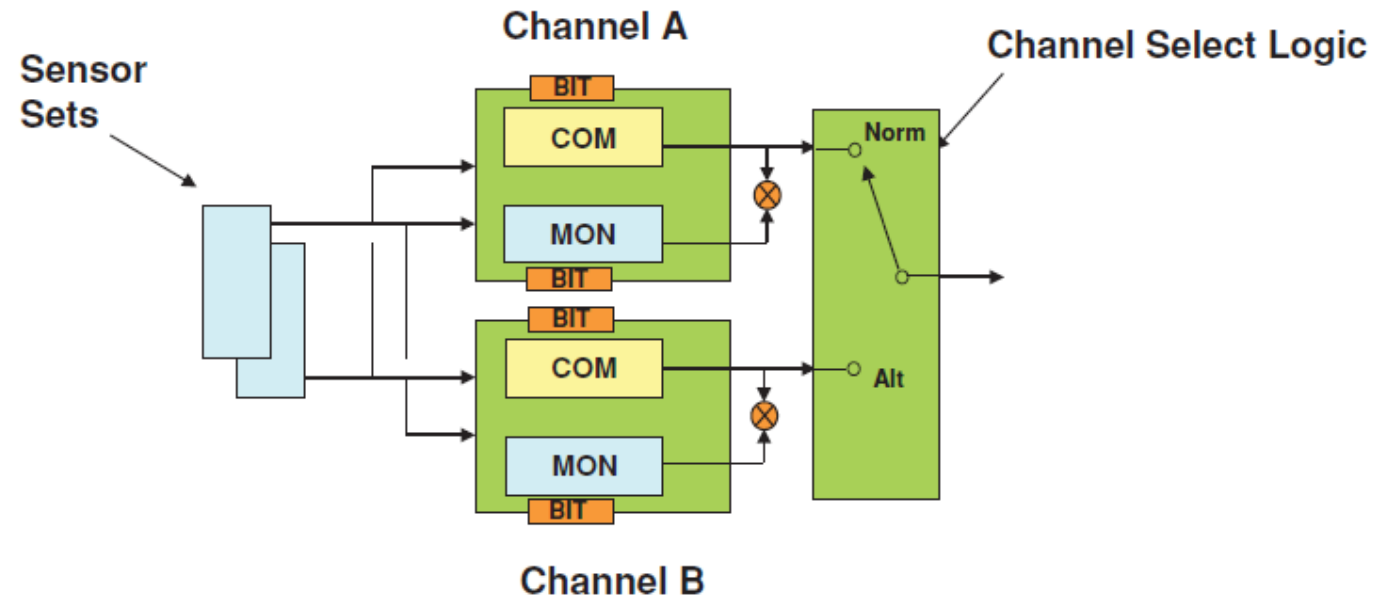


(a) High availability

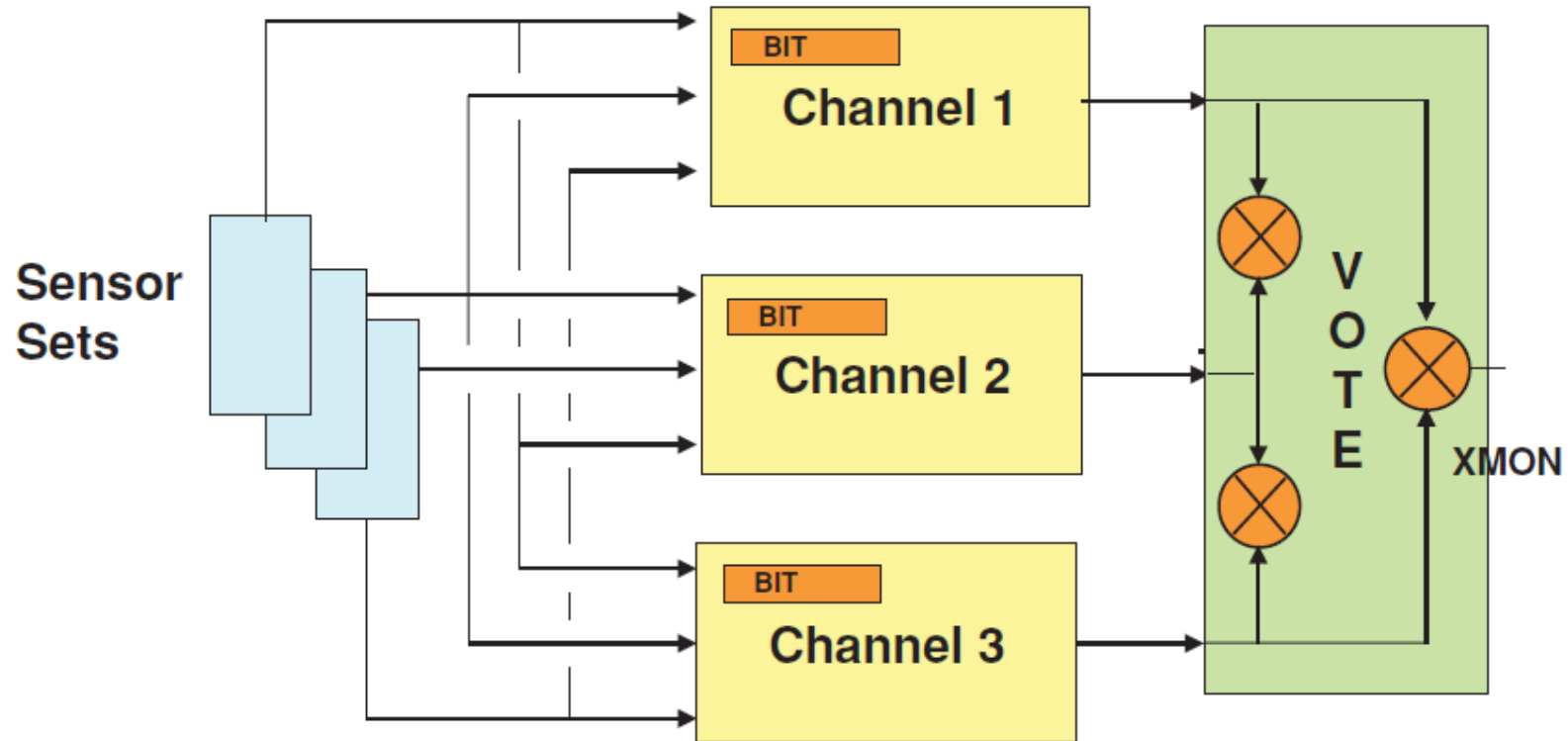


(b) High integrity

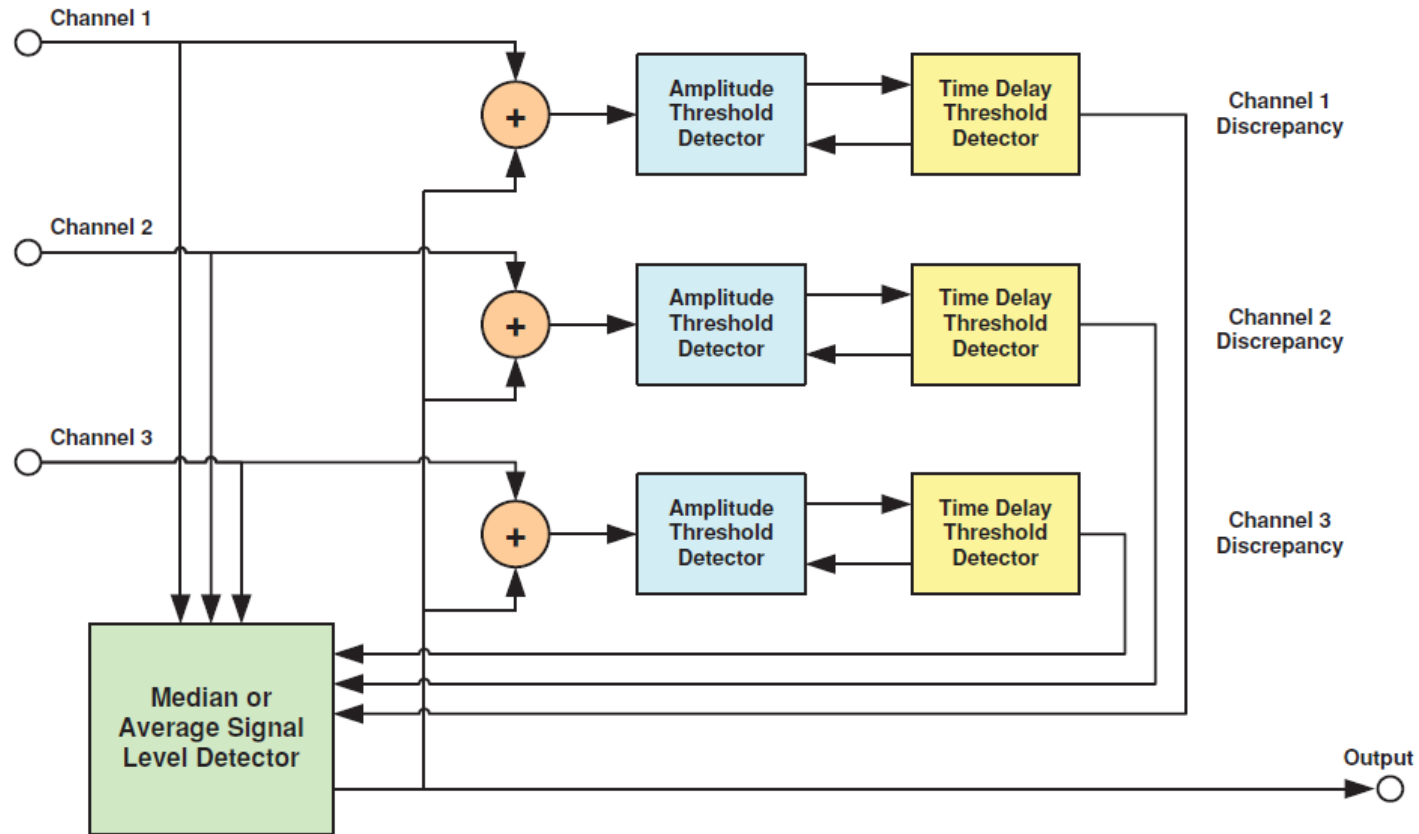
- Redundância
- Arquitetura Dual Command:Monitor



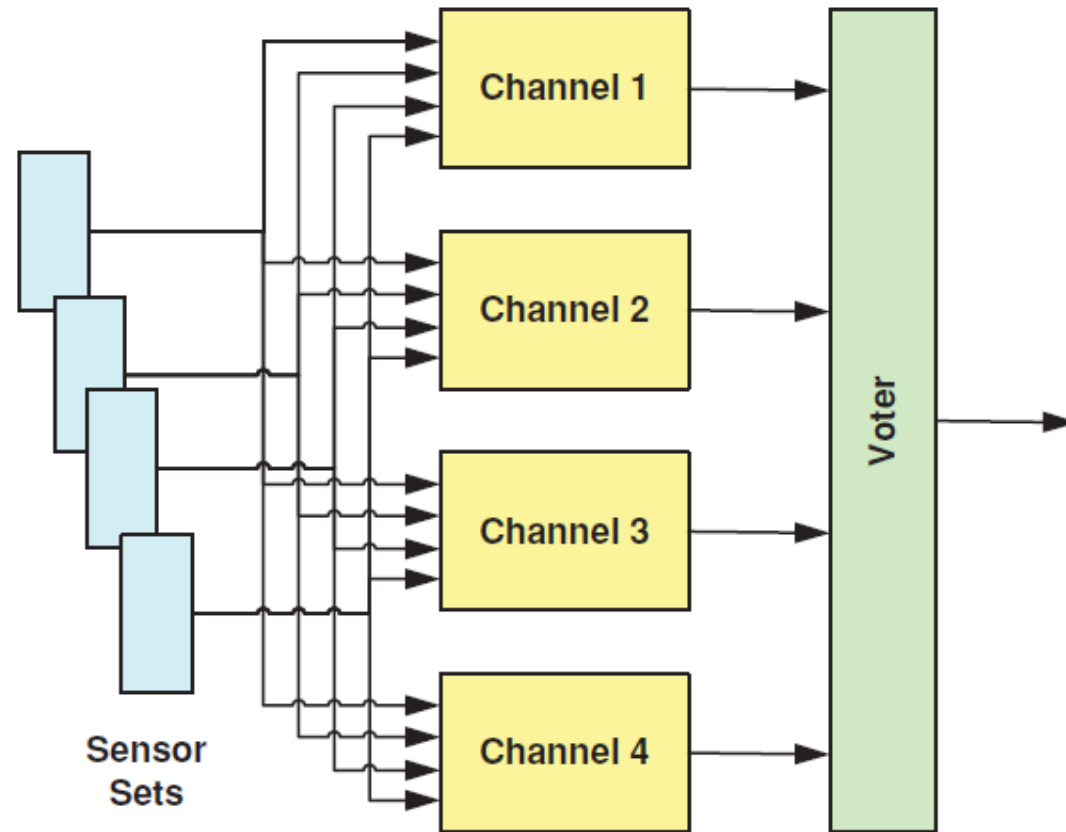
- Redundância
- Arquitetura Triplex



- Redundância
- Arquitetura Triplex



- Redundância
- Arquitetura Quadruplex



- Redundância
- Comparativo

Architecture	Reliability (1st Failure)	Availability (Total Loss)	Integrity (Undetected Malfunction)
Simplex	5000	Minor	Major
Duplex	2500	Major	Hazardous
Dual Com:Mon	1250	Hazardous	Catastrophic
Triplex	1667	Catastrophic	Catastrophic
Quadruplex	1250	Catastrophic	Catastrophic

- **Dissimilaridade**
- Uso de componentes não-similares para uma mesma função
 - Outro fabricante
 - Outro lote
 - Etc.
- Uso de softwares desenvolvidos por times diferentes para uma mesma função

- Segregação
- Separação física e via software de envio de informações

