Análise da Confiabilidade de Sistemas

1. Considerações Gerais

- A análise da confiabilidade de um sistema a partir de seus componentes básicos é um dos mais importantes aspectos da engenharia de confiabilidade
- Um sistema corresponde a um conjunto de itens como subsistemas, componentes, software e operadores (elemento humano), cujo funcionamento adequado e coordenado implicam no próprio funcionamento do sistema
- Na análise da confiabilidade de um sistema, portanto, torna-se necessária a avaliação não só das relações entre componentes mas também das confiabilidades dos mesmos a fim de podermos determinar a confiabilidade do sistema como um todo
- No capítulo anterior nós discutimos a análise de confiabilidade a nível de componente, ou seja, elemento ou item para o qual possuímos informação disponível para estimar a sua confiabilidade
- Neste capítulo apresentaremos procedimentos para a modelagem das relações entre componentes e posterior quantificação da confiabilidade do sistema. Em particular, estaremos aptos a responder as seguintes perguntas:
    - Como as probabilidades de falha de componentes podem ser utilizadas na avaliação do desempenho do sistema?
    - Qual é o impacto da arquitetura do sistema na confiabilidade do mesmo?
    - Quais são os benefícios da utilização de componentes redundantes?
    - Qual é o impacto de falhas de modo comum na confiabilidade do sistema?
- Abordaremos os seguintes métodos para a avaliação da confiabilidade do sistema a partir de seus componentes constituintes:
    - Diagrama de Blocos
    - Árvore de Falhas

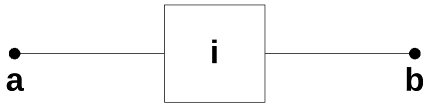
2. Diagrama de Blocos

- *Diagrama de Blocos* são freqüentemente utilizados na prática para modelar o impacto das falhas (ou funcionamento) de componentes no desempenho do sistema
- Sabemos que confiabilidade é definida como sendo a probabilidade de um sistema (ou componente) realizar a sua <u>função</u> por um período de tempo. Assim:

- Um diagrama de blocos reflete a relação funcional entre os componentes do sistema
- Cada bloco corresponde a uma função desempenhada por um componente ou conjunto de componentes para o qual dispomos de dados de confiabilidade

☞ Diagrama de Blocos é uma rede descrevendo a função do sistema. Se um sistema possui mais de uma função, então cada função é considerada individualmente e um diagrama de blocos distinto é estabelecido para cada função do sistema.

- Por exemplo, considere um sistema com *n* componentes distintos:
    - Cada um dos *n* componentes é ilustrado por um bloco como mostrado a seguir:
    - Quando existem uma conexão entre os pontos *a* e *b*, podemos dizer que o componente *i* está *funcionando*, ou seja, que o modo de falha



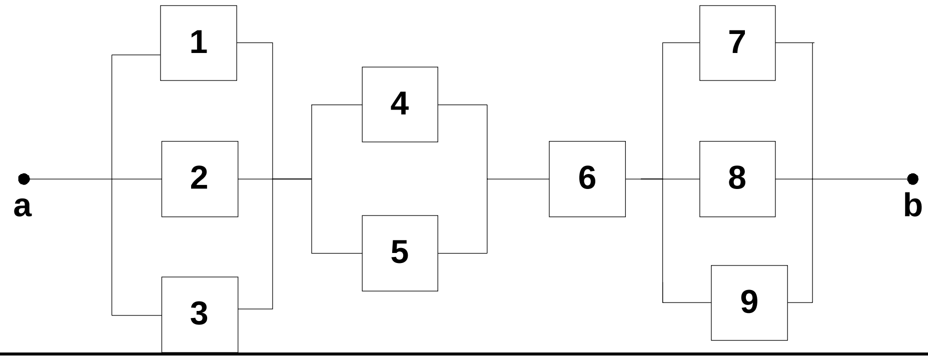
representado não ocorre

- Lembre: modo de falha corresponde a uma das formas que o componente ou sistema pode falhar. Assim, se cada bloco corresponde a uma ou mais funções desempenhadas pelo componente, então a ocorrência do modo de falha implica que o mesmo não está funcionando satisfatoriamente

    - Porém, isto não significa que o componente *i* satisfaz <u>todas</u> as suas funções. Apenas podemos afirmar que uma função ou um conjunto de funções específicas representadas por este bloco são satisfatoriamente desempenhadas, ou seja, o modo de falha ou modos de falha não ocorrem
    - Note que o significado de estar funcionando deve ser especificado em cada caso e depende dos objetivos da análise em questão
- Em resumo:

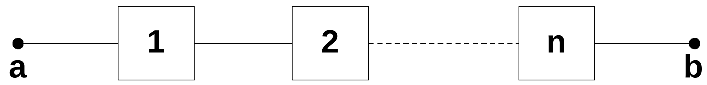
☞ As diversas maneiras através das quais *n* componentes estão interconectados para a realização de uma determinada função do sistema podem ser ilustradas por um diagrama de bloco

    - Veja a próxima figura:



☞ Quando tem-se uma conexão estabelecida entre os pontos *a* e *b*, pode se dizer que a função do sistema representada pelo diagrama de blocos é realizada. Isto significa que um ou mais modos de falha não ocorrem.

- <u>Sistema em Série</u>:
  - Considere um sistema formado por *n* componentes independentes. O modelo em série assume que todos os *n* componentes independentes devem estar funcionando para que o sistema desempenhe a sua função apropriadamente
  - O sistema falha se qualquer um de seus componentes falha
  - Apesar da hipótese de componentes independentes ou da condição de que a falha do primeiro componente acarreta na falha do sistema não podem ser estritamente válidas para muitos sistemas, na prática porém o modelo em série é geralmente uma aproximação tanto razoável como conveniente da situação real
  - O diagrama de blocos para um conjunto de componentes que estão em série é mostrado a seguir:



  - A confiabilidade do sistema, $R_S(t)$, pode ser obtida a partir das confiabilidades de seus componentes:
    - Por exemplo, considere apenas dois componentes em série com confiabilidades $R_1(t), R_2(t)$. Sejam:

E_1 Evento de que o componente 1 não falha

E_2 Evento de que o componente 2 não falha

Como a probabilidade de que um componente opere (não falhe)durante um período de tempo *t* é a sua confiabilidade, então temos que

$$P(E_1) = R_1(t) \quad \text{e} \quad P(E_2) = R_2(t)$$

Agora, para um sistema em série, a confiabilidade para uma missão *t*, $R_S(t)$, é a probabilidade de que todos os componentes simultaneamente operem satisfatoriamente durante a missão *t*:

$$R_S(t) = P(E_1 \cap E_2)$$

assumindo que os componentes são independentes (a falha ou não falha de um deles não altera a confiabilidade do outro), então a confiabilidade do sistema é simplesmente o produto das probabilidades individuais de completar a missão:

$$R_S(t) = P(E_1)P(E_1) = R_1(t)R_2(t)$$

Ou seja, para que o sistema funcione, ambos os componentes devem funcionar.

- Generalizando para *n* componentes independentes em série:

$$R_S(t) = \prod_{i=1}^{n} R_i(t) = R_1(t) \times R_2(t) \times \cdots \times R_n(t)$$

- É importante notar que para um sistema em série tem-se:

$$R_S(t) \leq \min\left\{R_1(t), R_2(t), \ldots, R_n(t)\right\}$$

☞ A confiabilidade de um sistema em série nunca é maior do que a menor confiabilidade de seus componentes constituintes

A desigualdade acima resulta do fato de que $0 \leq R_i(t) \leq 1$ e da multiplicação. Assim, é importante que todos os componentes tenham confiabilidade elevadas particularmente para sistemas contendo um grande número de componentes. Veja a tabela a seguir:

$R_i(t)$	Número de Componentes		
	10	**100**	**1000**
0.900	0.3487	0.266×10^{-4}	0.1747×10^{-45}
0.950	0.5987	0.00592	0.5292×10^{-22}
0.990	0.9044	0.3660	0.432×10^{-4}
0.999	0.9900	0.9048	0.3677

- Componentes com taxa de falha constante:
  - Se cada componente possui uma taxa de falha constante, λ_i, ou seja, o tempo de falha de cada componente é distribuído de acordo com a distribuição Exponencial, então a confiabilidade do sistema é:

$$R_S(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} \exp(-\lambda_i t) = \exp\left(-\sum_{i=1}^{n} \lambda_i t\right)$$

ou seja,

$$R_S(t) = \exp(-\lambda_S t)$$

onde λ_S é a taxa de falha do sistema dada por

$$\lambda_S = \sum_{i=1}^{n} \lambda_i$$

> ☞ Quando todos os componentes em série possuem taxa de falha constante, o sistema também possui taxa de falha constante

  - É importante notar que apesar de todos os componentes terem tempos de falha governados pela distribuição Exponencial, estas distribuições não são necessariamente as mesmas, ou seja, as taxas de falha dos componentes podem (e em geral são) distintas

☞ *Exemplo 1*:

Considere um sistema composto por quatro componentes em série os quais são independentes e possuem a mesma taxa de falha constante λ. Se $R_S(100) = 0.95$, encontre o *MTTF* de cada componente.

- O tempo de falha do sistema também e distribuído exponencialmente, logo

$$R_S(t) = e^{-100\lambda_S} = e^{-100(4)\lambda} = 0.95$$

ou

$$\lambda = \frac{-Ln(0.95)}{400} = 0.000128$$

Portanto,

$$MTTF = \frac{1}{0.000128} = 7812.5 hrs$$

- Em geral, quando todos os componentes em série possuem taxa de falha constante, o *MTTF* do sistema é fornecido por:

$$MTTF_S = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\sum_{i=1}^{n} 1/MTTF_i}$$

- Componentes com tempos de falha dados pela distribuição de Weibull:
  - Se as falhas dos *n* componentes são governadas por distribuições de Weibull, então a confiabilidade do sistema em série é dada por:

$$R_S(t) = \prod_{i=1}^{n} \exp\left[-\left(\frac{t}{\alpha_i}\right)^{\beta_i}\right] = \exp\left[-\sum_{i=1}^{n}\left(\frac{t}{\alpha_i}\right)^{\beta_i}\right]$$

com $\alpha_1, \alpha_2, \ldots, \alpha_n$ e $\beta_1, \beta_2, \ldots, \beta_n$, respectivamente

  - A taxa de falha do sistema é obtida a partir de $h(t) = f(t)/R(t)$, logo

$$h_S(t) = \exp\left[-\sum_{i=1}^{n}\left(\frac{t}{\alpha_i}\right)^{\beta_i}\right]\left[\sum_{i=1}^{n}\frac{\beta_i}{\alpha_i}\left(\frac{t}{\alpha_i}\right)^{\beta_i-1}\right] \Big/ \exp\left[-\sum_{i=1}^{n}\left(\frac{t}{\alpha_i}\right)^{\beta_i}\right]$$

obtendo-se

$$h_S(t) = \sum_{i=1}^{n} \frac{\beta_i}{\alpha_i} \left(\frac{t}{\alpha_i} \right)^{\beta_i - 1}$$

> ☞ O sistema em série não possui tempo de falha do tipo Weibull apesar de todos os seus componentes possuírem falhas governadas por distribuições de Weibull.

☞ *Exemplo 2*:

Um sistema é formado por quatro componentes em série cada um dos quais possuindo tempo de falha distribuído de acordo com Weibull e com parâmetros fornecidos na seguinte tabela:

Componente	**Parâmetro de Escala, α_i**	**Parâmetro de Forma, β_i**
1	100	1.20
2	150	0.87
3	510	1.80
4	720	1.00

Estime a confiabilidade do sistema.

- Temos que:

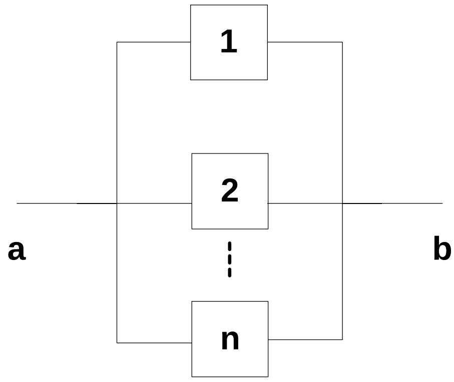
$$R_S(t) = \exp\left\{ - \left[\left(\frac{t}{100} \right)^{1.2} + \left(\frac{t}{150} \right)^{0.87} + \left(\frac{t}{510} \right)^{1.8} + \left(\frac{t}{720} \right)^{1.0} \right] \right\}$$

Por exemplo, para uma missão de 10 horas, a confiabilidade do sistema atinge o seguinte valor:

$$R_S(10) = e^{-0.1726} = 0.8415 \rightarrow 84.15\%$$

- <u>Sistema em Paralelo (Ativo)</u>:
  - Dois ou mais componentes estão em paralelo, ou são redundantes, quando todos os componentes devem falhar para que o sistema falhe

- Se pelo menos um dos componentes funciona, então o sistema continua a funcionar (não falha)
- Ativo significa que todos os componentes estão operando durante o período de missão do sistema
- O diagrama de blocos para um conjunto de componentes que estão em paralelo ativo é mostrado a seguir:
- A confiabilidade do sistema formado por *n* componentes independentes e em paralelo ativo corresponde a 1 menos a probabilidade de que todos os componentes falhem, ou seja, é igual a probabilidade de que pelo menos



um componente funcione:

- Para apenas dois componentes

$$R_S(t) = P(E_1 \cup E_2) = 1 - P(\overline{E_1 \cup E_2}) = 1 - P(\overline{E_1} \cap \overline{E_2})$$

o qual resulta em

$$R_S(t) = 1 - P(\overline{E_1})P(\overline{E_2})$$

Assim, a confiabilidade do sistema é:

$$R_S(t) = 1 - \left[1 - R_1(t)\right]\left[1 - R_2(t)\right]$$

- Generalizando para *n* componentes independentes:

$$R_S(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right]$$

- Note que para um sistema em paralelo ativo

$$R_S(t) \geq \max\left\{R_1(t), R_2(t), \ldots, R_n(t)\right\}$$

uma vez que $\prod_{i=1}^{n}\left[1-R_i(t)\right]$ deve ser menor do que a probabilidade de falha do componente de maior confiabilidade

☞ A confiabilidade de um sistema em paralelo ativo é pelo menos igual a confiabilidade do seu componente mais confiável.

- Para um sistema redundante nos quais todos os componentes possuem taxa de falha constante, a confiabilidade do sistema é

$$R_S(t) = 1 - \prod_{i=1}^{n}\left[1 - e^{-\lambda_i t}\right]$$

onde λ_i é a taxa de falha do *i-ésimo* componente

☞ *Exemplo 3*:

Para um sistema formado por dois componentes em paralelo ativo e possuindo taxas de falha constantes λ_1 e λ_2, determine o *MTTF* do sistema

‣ A confiabilidade do sistema é dada por

$$R_S(t) = 1 - \left(1 - e^{-\lambda_1 t}\right)\left(1 - e^{-\lambda_2 t}\right)$$

resultando em

$$R_S(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}$$

‣ O *MTTF* do sistema é então estimado como

$$MTTF = \int_0^\infty R_S(t) = \int_0^\infty \left[e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}\right]dt$$

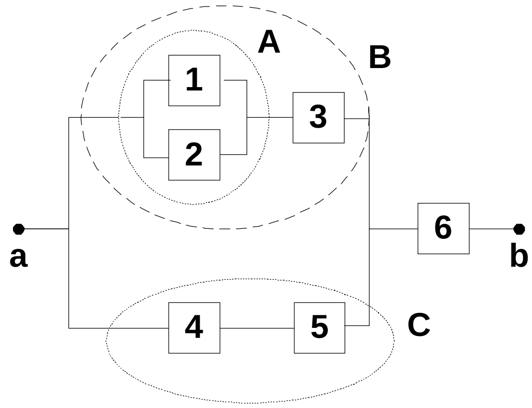
obtendo-se

$$MTTF_S = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

- <u>Sistemas em Série-Paralelo</u>:

- Sistemas complexos tipicamente incluem componentes em paralelo e em série. Veja a figure que segue:

- A confiabilidade de um sistema em série-paralelo é determinada a partir



das confiabilidades dos seus subsistemas a depender se o mesmo está em série o paralelo:
  - Identifique e categorize os subsistemas série ou paralelo
  - Determine a confiabilidade de cada subsistema em série
  - Determine a confiabilidade de cada subsistema em paralelo
  - Utilize cada subsistema em série e/ou paralelo como um novo bloco fazendo parte de um novo sistema em um nível mais elevado de detalhamento
  - Repita os passos anteriores até completar a análise
- Por exemplo, considere o sistema mostrado anteriormente:
  - Inicialmente dividimos o diagrama de blocos em subsistemas em série e paralelo
  - No caso acima, tem-se que o subsistema *A* é formado pelos componentes *1* e *2* em paralelo. Logo, a confiabilidade deste subsistema é

$$R_A(t) = \left[1 - \left(1 - R_1(t)\right)\left(1 - R_2(t)\right)\right]$$

  - Subsistema *B* é formado pelo subsistema *A* em série com o componente *3*, assim

$$R_B(t) = R_A(t) \times R_3(t)$$

- Subsistema *C* é constituído pelos componentes *4* e *5* em série, logo

$$R_C(t) = R_4(t) \times R_5(t)$$

- Como os subsistemas *B* e *C* estão em paralelo e ambos em série com o componente *6*, a confiabilidade do sistema é determinada como:

$$R_S(t) = \left[1 - \left(1 - R_B(t)\right)\left(1 - R_C(t)\right)\right]R_6(t)$$

- Se supormos que $R_1 = R_2 = 0.90$, $R_3 = R_6 = 0.98$, e $R_4 = R_5 = 0.99$, então

$$R_B = \left[1 - (0.10)^2\right](0.98) = 0.9702$$

$$R_C = (0.99)^2 = 0.9801$$

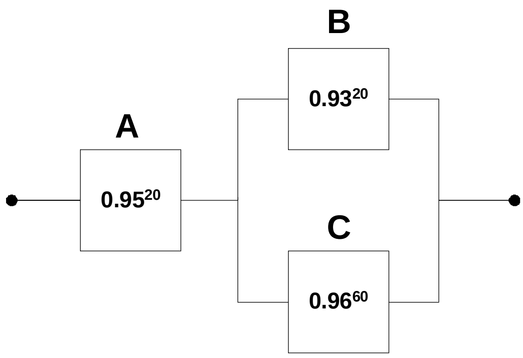
e

$$R_S = \left[1 - (1 - 0.9702)(1 - 0.9801)\right](0.98) = 0.9794 \rightarrow 97.94\%$$

☞ *Exemplo 4*:

Um sistema possui 100 componentes distribuídos em três subsistemas diferentes. Subsistema *A* é composto por 20 componentes em série sendo que cada um deste componentes apresenta uma confiabilidade de 95%. Subsistema *B* tem 20 componentes em série cada um destes com confiabilidade de 93%. Subsistema *C* é formado por 60 componentes em série sendo que cada componentes apresenta uma confiabilidade de 96%. Os subsistemas *B* e *C* estão cada um em série com o subsistema *A*, mas estão em paralelo entre si. Qual é a confiabilidade do sistema?

- Observe na figura que segue a configuração do sistema fornecido:
- Agora calculamos os valores das confiabilidades para os subsistemas:



$$R_A = 0.95^{20} = 0.358$$

$$R_B = 0.93^{20} = 0.234$$

$$R_C = 0.96^{60} = 0.086$$

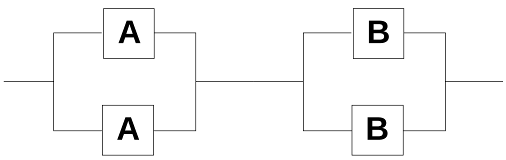
- Subsistema paralelo de *B* e *C*:

$$R_{BC} = 1 - (1 - R_B)(1 - R_C) = 0.30$$

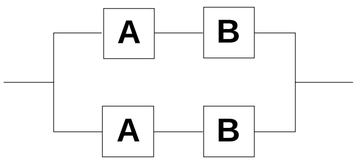
- Confiabilidade do sistema:

$$R_S = R_A R_{BC} = 0.107 \rightarrow 10.7\%$$

- Redundância em Alto Nível versus Redundância em Baixo Nível:
  - Sistemas redundantes podem ser obtidos a partir de duas configurações básicas:
    - Cada componente do sistema pode possuir um ou mais componentes em paralelo a este, o que é conhecido como *Redundância em Baixo Nível*
    - O sistema como um todo pode ser colocado em paralelo com um ou mais sistemas idênticos a este. Esta configuração é conhecido como *Redundância em Alto Nível*
  - Por exemplo, considere um sistema simples composto de dois componentes em série:
    - Redundância em baixo nível é mostrada a seguir



    - Redundância em alto nível é mostrada a seguir:



- Impacto do tipo de redundância na confiabilidade do sistema:
  - Se é considerado que ambos os componentes possuem a mesma confiabilidade, $R_A(t) = R_B(t) = R(t)$, então a confiabilidade do sistema com redundância em baixo nível é dada por:

$$R_b(t) = \left[1 - \left(1 - R(t)\right)^2\right]^2 = \left(2R(t) - R(t)^2\right)^2$$

  - Para o sistema com redundância em alto nível, tem-se

$$R_a(t) = 1 - \left(1 - R(t)^2\right)^2 = 2R(t)^2 - R(t)^4$$

  - Através da comparação das confiabilidades deste dois tipos de sistemas, pode-se dizer que:

> ☞ Um sistema com redundância em baixo nível possui maior confiabilidade do que com redundância em alto nível.

  - Como chegamos a esta conclusão? Observe que

$$\begin{aligned} R_b(t) - R_a(t) &= \left[2R(t) - R(t)^2\right]^2 - \left[2R(t)^2 - R(t)^4\right] \\ &= R(t)^2\left[2 - R(t)\right]^2 - R(t)^2\left[2 - R(t)^2\right] \\ &= 2R(t)^2\left[R(t) - 1\right]^2 \geq 0 \end{aligned}$$

    com igualdade obtida quando $R(t) = 1$. Note que esta equação somente é válida quando os componentes são mutuamente independentes e se as suas respectivas confiabilidades são independentes da configuração na qual os componentes são colocados.
  - Este resultado também pode ser justificado intuitivamente:
    - › O sistema falha tanto com a configuração em baixo nível como na de alto nível se ambos os componentes *A* falham ou ambos os componentes *B* falham
    - › Entretanto, o sistema com configuração de redundância em alto nível também falha se apenas

um componente A falha ou apenas um componente B falha assumindo que estas falhas ocorres em percursos distintos

☞ O sistema em redundância em alto nível possui um maior número de trajetórias que o levam a falhar.

– Na prática, a configuração de redundância em baixo nível é geralmente preferível com relação a configuração de redundância em alto nível devido a possuir maior nível de confiabilidade e menores custos de substituição (manutenção)

☞ *Exemplo 5*:
Um equipamento de rádio transmissão consiste de três sistemas principais: fonte de potência, um receptor, e um amplificador, com confiabilidades de 0.8, 0.9, e 0.85, respectivamente. Calcule as confiabilidades deste sistema para ambas as configurações de redundância em alto nível e baixo nível considerando subsistemas de dois componentes em paralelo.

- Para redundância em alto nível:

$$R_a = 1 - [1 - 0.8 \times 0.9 \times 0.85]^2 = 0.849$$

- Para redundância em baixo nível:

$$R_b = \left[1 - (1 - 0.8)^2\right]\left[1 - (1 - 0.9)^2\right]\left[1 - (1 - 0.85)^2\right] = 0.929$$

- <u>Sistemas em Redundância *k-N*</u>:
  - Redundância *k-N* (lê-se k de N) é um generalização de N componentes em paralelo quando existe a condição de que k componentes do total de N componentes idênticos e independentes devem funcionar para que o sistema também funcionar
  - Note que:
    - Devemos ter $k \leq N$
    - Quando $k = 1$ tem-se o caso de redundância completa, ou seja, é apenas necessário que qualquer componente opere satisfatoriamente para o sistema funcionar

- Quando $k = N$, tem-se que os N componentes estão em série, ou seja, todos devem funcionar para o sistema funcionar

- Confiabilidade de um sistema *k*-*N*:
  - Pode ser obtida a partir da distribuição de probabilidade Binomial
  - Se cada componente é considerado como sendo um evento independente com probabilidade constante de sucesso R (a sua confiabilidade), então

$$P(x) = \binom{N}{x} R^x (1 - R)^{N-x}$$

    é a probabilidade de que exatamente x componentes estejam operando
  - Observe que esta conclusão é válida pois

$$\binom{N}{x} = \frac{N!}{x!(N-x)!}$$

    corresponde ao número de maneiras que x sucessos (não falhas) podem ocorrer a partir de N componentes, enquanto que

$$R^x (1 - R)^{N-x}$$

    é a probabilidade de x sucessos e N - x falhas para um único arranjo de sucessos e falhas
  - Portanto

$$R_S = \sum_{x=k}^{N} P(x)$$

    é a probabilidade de k ou mais sucessos a partir de N componentes

---

☞ *Exemplo 6*:

Um certo tipo de foguete utilizado no transporte de satélites para a orbita terrestre requer que três de suas quatro turbinas operem satisfatoriamente para que o foguete atinja a orbita da Terra. Se cada turbina possui uma confiabilidade de 0.97, estime a probabilidade de sucesso do foguete alcançar a orbita.

- Nós queremos a confiabilidade da missão, ou seja, a probabilidade de sucesso:

$$R_S = \sum_{x=3}^{4} \binom{4}{x} 0.97^x (1 - 0.97)^{4-x}$$

logo,

$$R_S = 4(0.97)^3(0.03) + 0.97^4 = 0.9948 \rightarrow 99.48\%$$

- O caso de falhas exponenciais:
  - Se a distribuição do tempo de falha é Exponencial com taxa de falha λ, sabemos que a confiabilidade (probabilidade de sucesso) de cada componente do sistema é

$$R(t) = e^{-\lambda t}$$

  - Então, a confiabilidade do sistema *k-N* é dada por:

$$R_S(t) = \sum_{x=k}^{N} \binom{N}{x} e^{-\lambda x t} \left[1 - e^{-\lambda t}\right]^{N-x}$$

  - Pode-se mostrar que o *MTTF* do sistema *k-N* neste caso é

$$MTTF = \int_0^{\infty} R_S(t) dt = \frac{1}{\lambda} \sum_{x=k}^{N} \frac{1}{x}$$

  - Note que se $k = 1$, então o *MTTF* obtido a partir da expressão anterior corresponde ao tempo médio de falha para um sistema composto de *N* componentes idênticos em paralelo e com taxa de falha constante

---

☞ *Exemplo 7*:

No exemplo anterior, considere que é requerido que as turbinas operem em potência máxima por um período de 8 minutos. Se a taxa de falha constante de cada turbina é $\lambda = 3.8 \times 10^{-3} / \min$, determine o *MTTF* do foguete.

- A confiabilidade de cada turbina para uma missão de 8 minutos é

$$R(8) = e^{-0.0038(8)} = 0.97$$

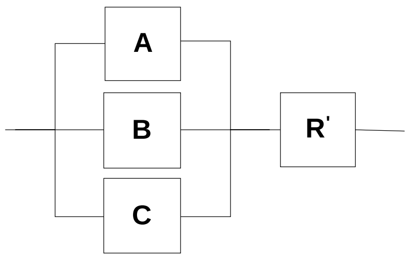
- O *MTTF* de cada turbina é

$$MTTF = \frac{1}{0.0038} = 262.65\,\text{min}$$

- Logo, o *MTTF* do sistema é calculado como

$$MTTF_S = 262.65\left(\frac{1}{3} + \frac{1}{4}\right) = 153.21\,\text{min}$$

- <u>Falhas de Causa Comum (“Common-Cause Failures”)</u>:
  - Até agora trabalhamos com a hipótese de que todos os N componentes do sistema falham de forma independente
  - Esta hipótese, entretanto, pode ser muitas vezes violada em sistemas. Por exemplo:
    - Diversos componentes que obtém energia elétrica a partir do mesmo gerador
    - Condições ambientais como calor excessivo ou vibração podem afetar diversos componentes da mesma forma
    - Erros operacionais ou de manutenção, falhas de projeto, uso de materiais de baixa qualidade na fabricação podem também contribuir para a ocorrência de falhas de causa comum
  - O modo de falha de causa comum pode ser considerado em série com os componentes que são afetados por este tipo de falha
  - A figura que segue mostra um modo de falha de causa comum associado a três componentes em paralelo:



  - A confiabilidade do sistema é dada por

$$R_S(t) = \left[1 - \left(1 - R_A(t)\right)\left(1 - R_B(t)\right)\left(1 - R_C(t)\right)\right]R'(t)$$

- É importante notar que:
  - Para podermos representar o modo de falha de causa comum via diagrama de blocos é necessário que sejamos capazes de identificar e separar as falhas independentes das falhas de causa comum
  - Para que o sistema redundante tenha impacto positivo na confiabilidade do sistema, ou seja, para que seja eficiente, a falha de causa comum deve possuir baixa probabilidade de ocorrência (deve ter elevada confiabilidade)

3. Árvore de Falhas

- Árvore de falhas é um método gráfico de análise de sistemas alternativo a diagrama de blocos
- Árvore de falhas difere com relação ao diagrama de blocos nos seguintes aspectos
  - É um processo de análise dedutivo estruturado em termos de eventos ao invés de componentes (por exemplo, equipamentos)
  - A análise é realizada em termos de falhas ao invés de confiabilidade (sucesso na operação de equipamentos)
  - Uma das vantagens de focalizar a análise em termos de falhas é que falhas são em geral mais fáceis de definir e identificar do que não-falhas, além do fato de que normalmente existe um número bem mais reduzido de formas que um sistema pode falhar do que maneiras do mesmo funcionar (não falhar)
- Assim, pode-se dizer que:

> ☞ *Árvore de Falhas* é um processo dedutivo através do qual um evento indesejável chamado de *evento topo* é postulado e as possíveis formas deste evento ocorrer são sistematicamente deduzidas

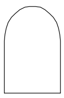
  - O evento topo é assim o foco da análise e em geral corresponde a um evento catastrófico (por exemplo, ruptura de tanque) ou uma falha significativa
  - O processo de construção de uma árvore de falha é dedutivo pois consiste na sistemática decomposição das falhas começando do evento topo e caminhando em direção das causas (eventos básicos)
  - A análise qualitativa consiste em identificar as diversas combinações de eventos que acarretam na ocorrência do evento topo
  - Esta etapa qualitativa pode ser seguida por uma análise quantitativa com o intuito de estimar a probabilidade de ocorrência do evento topo
  - Por exemplo, um evento topo pode corresponder a "falha do circuito de controle em enviar sinal". O processo dedutivo de construção da árvore de falha é realizado a fim de se identificar e incluir todas as falhas (na medida do possível como veremos adiante) dos componentes do sistema que contribuem para a ocorrência do evento topo
  - É possível incluir não só modos de falha individuais de componentes mas também erros humanos, falhas de softwares, e as interações destes elementos durante a operação do sistema

  - A árvore de falha em si é uma representação gráfica das várias combinações de falhas que acarretam na ocorrência do evento topo
- É importante notar que na prática uma árvore de falha não necessariamente contém todos os modos falha possíveis dos componentes do sistema:
  - Somente aqueles modos de falha que efetivamente contribuem e são relevantes a ocorrência do evento topo são incluídos na construção da árvore de falha
    - Por exemplo, se a perda de energia de um circuito causa este em abrir um contato, que por conseqüência envia um sinal para um outro sistema entrar em operação, então uma árvore de falha com evento topo "circuito de controle falha em gerar sinal" não incluiria um evento "falha do gerador" apesar do componente gerador de energia ser parte integral do circuito de controle. Isto se deve ao fato de que o evento topo não ocorre quando o gerador falha
  - Os eventos fazendo parte de uma árvore de falhas muitas vezes não são exaustivos, ou seja, não correspondem a totalidade dos eventos que contribuem para a ocorrência do evento topo
    - Somente aquele eventos considerados importantes devem ser incluídos
    - Deve-se notar, porém, que a inclusão ou não de um evento relevante não é arbitrária:
      - Esta escolha é influenciada pelo processo de construção da árvore de falha
      - Como o sistema é projetado
      - Como o sistema é operado
      - Histórico operacional do sistema
      - Dados de falha disponíveis
      - A experiência do analista
    - Logo:

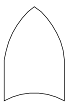
> ☞ Em cada nível da árvore de falha, os eventos considerados representam as causas *imediatas*, *necessárias*, e *suficientes* para a ocorrência do evento (eventos) em um nível imediatamente superior a estes, incluindo o evento topo

- Etapas na análise de sistemas via árvore de falha:
  - Defina o sistema, as suas fronteiras, e o evento topo
  - Construa a árvore de falha a qual simbolicamente representa o sistema e os seus eventos relevantes a ocorrência do evento topo
  - Realize uma análise qualitativa (avaliação lógica) do as combinações de eventos que acarretam na ocorrência do evento topo
  - Realize uma análise quantitativa (avaliação probabilística) que consiste em associar probabilidades de falha a os eventos básicos e estimando a probabilidade do evento topo
- A figura que segue mostra os símbolos utilizados na construção de árvores de falha:

Portões Lógicos:

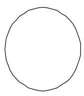


AND:portão lógico no qual um evento de saída (resultante) somente ocorre se todos os eventos de entrada tem ocorrido. Em álgebra Booleana, a saída deste portão corresponde a operação de interseção dos eventos de entrada

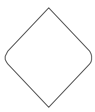


OR:um portão lógico no qual um evento de saída ocorre se pelo menos um dos eventos de entrada tem ocorrido. Em álgebra Booleana, a saída deste portão corresponde a operação de união dos eventos de entrada

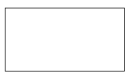
Eventos:



Evento Básico: evento que não requer mais detalhamento (desenvolvimento)

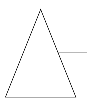


Evento Incompleto: é um evento que não é desenvolvido pois ou não há informação suficiente (dados) ou porque o mesmo é considerado pouco relevante (consequencias mínimas) por parte do analista

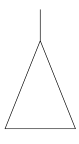


Evento Intermediário: evento que resulta da combinação lógica de outros eventos e geralmente corresponde à saída de um portão lógico

Transferências: usados para conectar porções de uma mesma árvore



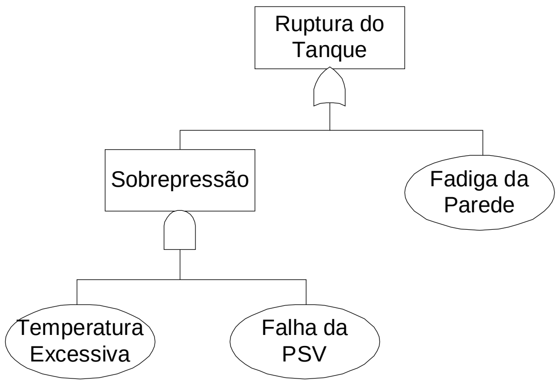
Transferência Para: indica que a árvore é desenvolvida posteriormente (em outra página) na ocorrência do portão de "transferência para"



Transferência De: indica que esta porção da árvore deve ser conectada à porção indicada pelo portão de "transferência de"

☞ *Exemplo 8*:

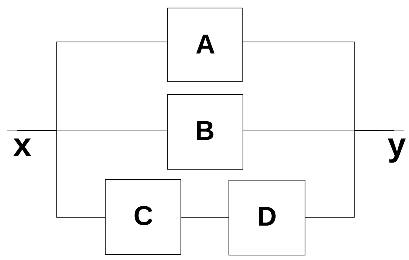
Na figura que segue, o portão OR indica que a "ruptura do tanque" ocorre ou por "sobrepressão" ou por "fadiga da parede do tanque" (falha inerente ao tanque). A falha devido a fadiga é considerada como evento básico. Por outro lado, o evento "sobrepressão" é considerado como intermediário e posteriormente desenvolvido através do uso de um portão AND. Assim, se o evento "temperatura excessiva" e "falha da PSV" ocorrerem, então a ruptura do tanque ocorrerá.



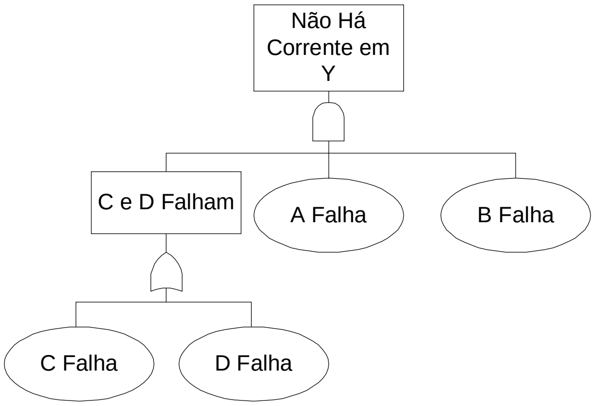
- <u>Construindo uma Árvore de Falha</u>:
  - O desenvolvimento de uma árvore de falha é um procedimento dedutivo, ou seja, é a sistemática decomposição das falhas começando do evento topo e prosseguindo em direção às suas causas
  - Para melhor entender o conceito de árvore de falha, veja o exemplo que segue

☞ *Exemplo 9*:

Considere um circuito elétrico representado pelo se diagrama de blocos a seguir



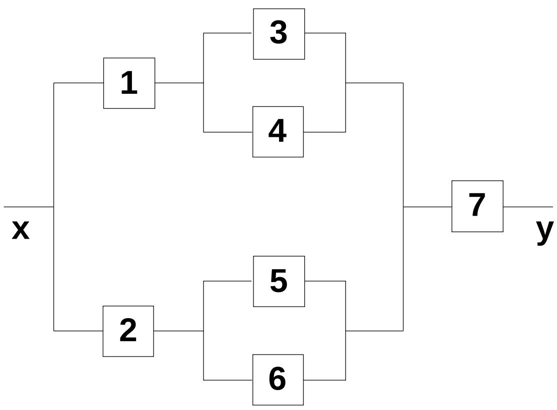
- A função deste sistema é fornecer corrente elétrica no ponto *y*.
- Logo o evento topo pode ser "Não Há Corrente em Y"
- Claramente, o evento topo resulta da ausência simultânea de corrente a partir dos três ramos deste sistema em paralelo:
  - Falha do componente *A*
  - Falha do componente *B*
  - Falha do componente *C* ou falha do componente *D*
- A árvore de falha resultante para este evento topo é mostrada a seguir:



- Resolva agora o próximo caso

Exemplo 10 (Resolver):

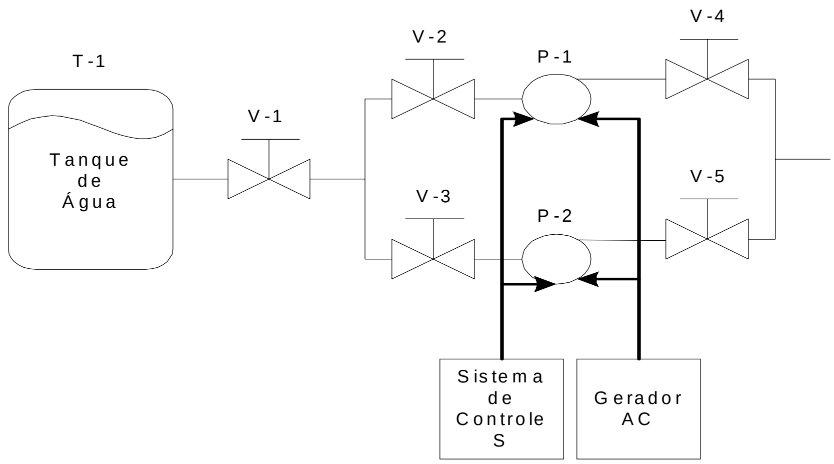
Considere o circuito elétrico representado pelo seu diagrama de blocos mostrado a seguir:



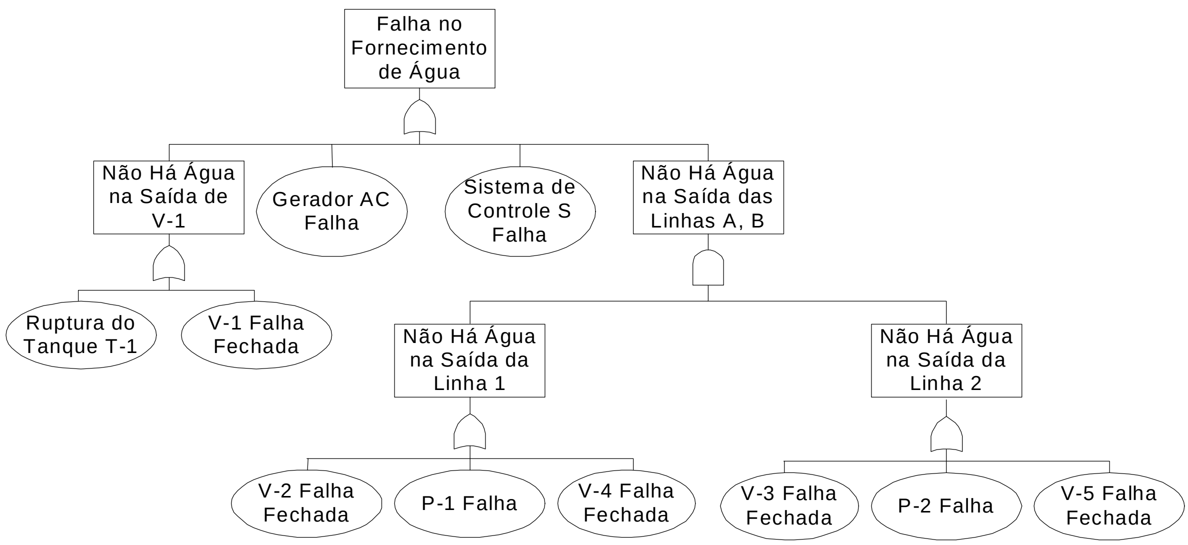
A função deste sistema é fornecer corrente no ponto *y*. Construa a árvore de falha para o evento topo "Ausência de Corrente em Y"

Exemplo 11:

Considere o sistema de bombeamento mostrado a seguir. Vazão suficiente de água é bombeada do tanque *T-1* quando apenas uma da duas bombas *P-1* ou *P-2* opera adequadamente. Todas as válvulas de *V-1* até *V-5* estão normalmente abertas. O sistema de controle *S* automaticamente aciona ambas as bombas *P-1* e *P-2* quando há a necessidade de água. Se uma das bombas falha na partida ou durante operação, o sistema ainda realiza a sua função satisfatoriamente se apenas uma das bombas operar. Ambas as bombas e o sistema de controle utilizam a mesma fonte de energia originada pelo gerador *AC*. Assuma que sempre há suficiente água no tanque *T-1*, não há falhas humanas, e não há falhas relevantes nas tubulações. Desenvolva uma árvore de fala para este sistema.



- Para o evento topo "Falha no Fornecimento de Água", a árvore de falha é mostrada na figura que segue:



- Note que nós consideramos apenas um modo de falha para ambas as bombas.

- <u>Análise Qualitativa de uma Árvore de Falha</u>:
  - A avaliação lógica ou qualitativa de uma árvore de falha consiste na determinação de todas as combinações de eventos que levam a ocorrência do evento topo, ou seja, na identificação dos *conjuntos de cortes mínimos*

> ☞ *Corte* corresponde a um conjunto de eventos que levam a ocorrência do evento topo.
> ☞ *Corte Mínimo* é um corte o qual não possui eventos desnecessários, ou seja, todos os eventos deste corte devem ocorrer para causar a ocorrência do evento topo.

  - É importante notar que cortes e cortes mínimos são definidos no contexto de falha do sistema:
    - O complemento lógico de um corte é uma conjunto de eventos chamado de caminho
    - O complemento lógico de um corte mínimo é um caminho mínimo

> ☞ *Caminho* é um conjunto de eventos cuja ocorrência implica o funcionamento do sistema.
> ☞ *Caminho Mínimo* é o caminho que não possui eventos desnecessários, ou seja, possui o mínimo de eventos necessários para garantir o funcionamento do sistema.

    - Logo, caminhos e caminhos mínimos são definidos dentro do domínio de sucesso (funcionamento) do sistema
  - A avaliação qualitativa de uma árvore de falha envolve a determinação dos seus cortes mínimos
  - Os cortes mínimos podem ser obtidos através de simples manipulação Booleana dos eventos representados na árvore de falha com o objetivo de expressar o evento topo em termos de eventos básicos não redundantes, ou seja, em termos de seus cortes mínimos
    - Note que redundância existe quando um mesmo evento ocorre mais de uma vez na árvore de falha ou quando este evento é um subconjunto de um outro evento

- Antes de continuar, a tabela a seguir apresenta as regras de manipulação algébrica Booleana as quais utilizaremos na determinação dos cortes mínimos de árvores de falha

Propriedade	**Exemplo**
Comutativa	$X \cap Y = Y \cap X$ $X \cup Y = Y \cup X$
Associativa	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$ $X \cup (Y \cup Z) = (X \cup Y) \cup Z$
Distributiva	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
Idempotência	$X \cap X = X$ $X \cup X = X$
Absorção	$X \cap (X \cup Y) = X$ $X \cup (X \cap Y) = X$
Complemento	$X \cap \overline{X} = \varnothing$ $X \cup \overline{X} = \Omega$ $\overline{\overline{X}} = X$
Teorema de Morgan	$\overline{(X \cap Y)} = \overline{X} \cup \overline{Y}$ $\overline{(X \cup Y)} = \overline{X} \cap \overline{Y}$

- Veja o próximo exemplo

Exemplo 12:

Simplifique a seguinte expressão:

$$\left[\overline{(A \cap B) \cup (A \cap \overline{B}) \cup (\overline{A} \cap \overline{B})}\right]$$

- Simplificando, obtemos:

Simplificação	**Propriedade Utilizada**
$\overline{\left[(A\cap B)\cup(A\cap \overline{B})\cup(\overline{A}\cap \overline{B})\right]}$	de Morgan
$\overline{(A\cap B)}\cap\overline{(A\cap \overline{B})}\cap\overline{(\overline{A}\cap \overline{B})}$	de Morgan
$(\overline{A}\cup \overline{B})\cap(\overline{A}\cup \overline{\overline{B}})\cap(\overline{\overline{A}}\cup \overline{\overline{B}})$	Complemento
$(\overline{A}\cup \overline{B})\cap(\overline{A}\cup B)\cap(A\cup B)$	Distributiva
$\left[\overline{A}\cap(\overline{A}\cup B)\right]\cup\left[\overline{B}\cap(\overline{A}\cup B)\right]\cap(A\cup B)$	Distributiva
$\left[\overline{A}\cup(B\cap \overline{A})\right]\cup\left[(\overline{B}\cap \overline{A})\cup(\overline{B}\cap B)\right]\cup(A\cup B)$	Absorção
$\left[\overline{A}\cup(B\cap \overline{A})\right]\cap(A\cup B)$	Distributiva
$\overline{A}\cap(A\cup B)$	Absorção
$\overline{A}\cap B$	

- O procedimento para a determinação dos cortes mínimos de uma árvore de falha que utilizaremos é denominado de *Método da Substituição Sucessiva*:
  - Encontra-se a expressão Booleana de cada portão da árvore de falha de tal forma que somente eventos básicos são envolvidos
  - Para tanto, diversas manipulações Booleanas (veja tabela acima) são empregadas para reduzir as expressões de eventos a sua forma mais compacta
  - O processo de substituição inicia-se a partir do portão representando o evento topo e prossegue em direção à base da árvore de falha, ou seja, de cima para baixo
  - Ao final deste processo de substituição, a expressão final corresponderá aos cortes mínimos da árvore de falha. Cada corte

mínimo corresponde a um ou mais eventos cuja realização simultânea implica na ocorrência do evento topo (falha do sistema)

- Para melhor entender este processo, considere o próximo exemplo

---

Exemplo 13:

Considere a árvore de falha do exemplo 9. Encontre os cortes mínimos e os caminhos mínimos.

- Vamos chamar de G_1 o portão representando o *AND* do evento topo e G_2 o portão *OR* representando o evento "C e D Falham"
- Assim, começando do topo tem-se:

$$T = A \cdot B \cdot G_1$$

onde T corresponde ao evento topo. Por sua vez,

$$G_1 = C + D$$

Substituindo na expressão anterior do evento topo,

$$T = A \cdot B \cdot (C + D)$$

expandindo e simplificando, encontramos os cortes mínimos como:

$$T = A \cdot B \cdot C + A \cdot B \cdot D$$

- Os caminhos mínimos podem ser obtidos como complemento dos cortes mínimos:

$$\overline{T} = \overline{ABC + ABD} = \overline{ABC} \cdot \overline{ABD} = \left(\overline{A} + \overline{B} + \overline{C}\right)\left(\overline{A} + \overline{B} + \overline{D}\right)$$

$$\overline{T} = \left(\overline{A} + \overline{A}\overline{B} + \overline{A}\overline{D} + \overline{A}\overline{B} + \overline{B} + \overline{B}\overline{D} + \overline{A}\overline{C} + \overline{B}\overline{C} + \overline{C}\overline{D}\right)$$

$$\overline{T} = \overline{A} + \overline{B} + \overline{C}\overline{D}$$

- <u>Árvore de Sucesso</u>:
  - Vimos no exemplo anterior que mesmo para um sistema bastante simples, a obtenção dos caminhos mínimos a partir da inversão (complemento lógico) dos cortes mínimos requer um trabalho considerável!
  - Em situações práticas, muitas vezes uma árvore de sucesso se constitui em um método alternativo para a determinação dos caminhos mínimos de um sistema a partir de uma árvore de falha

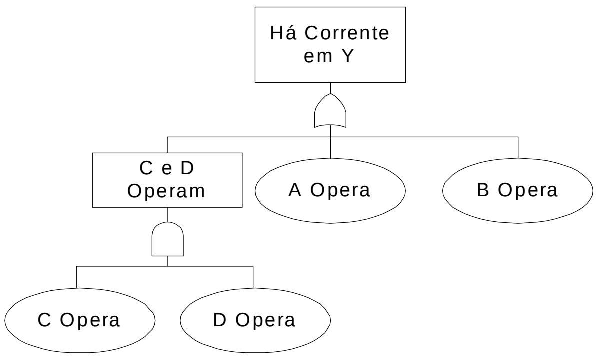
- *Árvore de Sucesso* é um método que é conceitualmente o mesmo que árvore de falha:
  - Define-se um evento topo que corresponde a um *evento desejável*
  - Os eventos intermediários e básicos são assim especificados de forma a garantir a ocorrência (desejável) do evento topo

> ☞ *Árvore de Sucesso* representa as diversas combinações de eventos desejáveis (sucessos) que garantem a ocorrência do evento topo.

- Uma árvore de sucesso é o complemento lógico de uma árvore de falha:
  - Se o complemento lógico do evento topo de uma árvore de falha é utilizado como o evento topo de uma árvore de sucesso, então a estrutura lógica (Booleana) representada pela árvore de sucesso é o complemento lógico da árvore de falha

> ☞ A partir de uma árvore de sucesso cujo evento topo é o complemento do evento topo de uma árvore de falha, obtemos os caminhos mínimos do sistema.

  - Assim, para construir uma árvore de sucesso a partir de uma árvore de falha nós simplesmente utilizamos os complementos de todos os eventos intermediários e básicos da árvore de falha, assim como invertemos todos os portões lógicos da árvore de falha: $AND \rightarrow OR$ e $OR \rightarrow$ AND
  - Por exemplo, invertendo a árvore de falha do exemplo 9, obtemos



– Sendo

$$\overline{A} \equiv A \ funciona$$

$$\overline{B} \equiv B \ funciona$$

$$\overline{C} \equiv C \ funciona$$

$$\overline{D} \equiv D \ funciona$$

Obtemos os seguintes caminhos mínimos:

$$\overline{T} = \overline{A} + \overline{B} + \overline{C}\,\overline{D}$$

onde $\overline{T}$ corresponde ao complemento do evento topo da árvore de falha, ou seja, “Há Corrente em Y”

- Tente agora resolver os seguintes casos

Exemplo 14 (Resolver):

Considere a árvore de falha do exemplo 10.

(a) Encontre os cortes mínimos

(b) Determine os caminhos mínimos utilizando árvore de sucesso

---

Exemplo 15 (Resolver):

Considere a árvore de falha do exemplo 11.

(a) Encontre os cortes mínimos

(b) Determine os caminhos mínimos utilizando árvore de sucesso

---

- Atenção com o número de eventos básicos em um corte mínimo:
  - Ao se determinar os cortes mínimos de uma árvore de falha, deve-se dar maior importância aqueles cortes mínimos possuindo um ou dois eventos básicos pois estes são mais prováveis de ocorrerem do que cortes mínimos compostos de múltiplos eventos básicos
  - Por exemplo, se um evento básico possui probabilidade de ocorrência na ordem de 10^{-2}, então podemos esperar que um corte mínimo composto por dois eventos básicos tenha probabilidade de ocorrência na ordem de 10^{-4}, enquanto que um corte mínimo triplo (três eventos básicos) teria probabilidade na ordem de 10^{-6}

- A partir desta informação, pode-se traçar como um provável objetivo a eliminação ou minimização da probabilidade de falha de cortes mínimos formados por apenas um evento básico
- Em geral, a ordenação de cortes mínimos por tamanho fornece uma idéia qualitativa da importância dos diversos cortes mínimos encontrados
- Da mesma forma, eventos básicos aparecendo em mais de um corte mínimo deverão ser analisados atenciosamente e serão candidatos a posterior eliminação (deste modo de falha se possível) ou minimização de sua probabilidade de ocorrência
- Se uma análise quantitativa é realizada, então aqueles cortes mínimos com probabilidades de ocorrência mais elevadas devem receber especial atenção

- <u>Análise Quantitativa de uma Árvore de Falha</u>:
  - Sabemos que cada corte mínimo é uma combinação de eventos básicos que devem obrigatoriamente ocorrer para causar o evento topo
  - Se $C_1, C_2, \ldots, C_n$ são os *n* cortes mínimos, então o evento topo *T* pode ser expresso em termos de seus corte mínimos como

    $$T = C_1 + C_2 + \cdots + C_n$$

    onde cada corte mínimo C_i pode ser formado por um ou mais eventos básicos $E_1, E_2, \ldots, E_k$
  - A probabilidade de que o evento topo *T* ocorra durante um período de tempo *t* é

    $$P(T) = P(C_1 + C_2 + \cdots + C_n)$$

    onde C_i representa o evento de que os elementos (equipamentos, operadores, software) representados neste corte mínimo falhem antes da missão *t*
    - O sinal + corresponde a operação lógica de união ($\cup$), enquanto que $\bullet$ é a operação lógica de interseção ($\cap$)
    - Note que *T* indica o evento topo e não a variável aleatória tempo!
    - Todos os cortes mínimos são assim avaliados para um tempo de missão *t*
    - A um evento básico pode ser associado um simples valor de probabilidade de falha sob demanda (exemplo, bomba falha na partida), ou probabilidade de falha durante o período *t* de operação do sistema
  - Se os cortes mínimos são mutuamente exclusivos (não ocorrem simultaneamente), então

    $$P(T) = P(C_1) + P(C_2) + \cdots + P(C_n) \qquad (1)$$

  - Na prática, porém, os cortes mínimos não são mutuamente exclusivos. Neste caso, a probabilidade de interseção (ocorrência simultânea) de dois ou mais cortes mínimos deve ser estimada
    - Por exemplo, considere que temos os seguintes cortes mínimos:

      $$C_1 = A \cdot B$$
      $$C_2 = A \cdot C$$

Então,

$$P(T) = P(A \cdot B + A \cdot C)$$

resultando em

$$P(T) = P(A \cdot B) + P(A \cdot C) - P(A \cdot B \cdot A \cdot C)$$

Se os eventos básicos são independentes, então

$$P(C_1) = P(A)P(B)$$
$$P(C_2) = P(A)P(C)$$

e

$$P(T) = P(A)P(B) + P(A)P(C) - P(A)P(B)P(C)$$

> ☞ Para se obter a probabilidade do evento topo é suficiente estimar as probabilidades de falha dos eventos básicos.

- Em geral, se os eventos básicos que compõem um determinado corte mínimo são mutuamente independentes, então

$$P(C_i) = P(E_1 \cdot E_2 \cdots E_{ik}) = P(E_1)P(E_2)\cdots P(E_{ik})$$

onde *ik* é o número de eventos básicos no corte mínimo C_i

- A Eq. (1) pode ser uma boa aproximação mesmo quando os cortes mínimos não são mutuamente exclusivos mas as probabilidades de ocorrência dos eventos básicos são pequenas (em geral, quando todos os eventos básicos possuem probabilidades de ocorrência menores do que 0.1)
    - Isto é verdadeiro porque os produtos cruzados, como $P(A)P(B)P(C)$ consistem (assumindo eventos básicos independentes) de produtos entre probabilidades de eventos básicos
    - Por exemplo, se a probabilidade de um evento básico é da ordem de 10^{-6}, então a probabilidade de interseção de dois ou mais eventos será da ordem de 10^{-12} ou menor
    - Esta aproximação para a probabilidade do evento topo é conhecida como *Aproximação do Evento Raro*:

$$P(T) \approx P(C_1) + P(C_2) + \cdots + P(C_n)$$

a qual fornece uma estimativa conservadora (pessimística) da probabilidade de falha do sistema

- Como um exemplo, vamos considerar que

$$P(A) = P(B) = P(C) = 0.001$$

logo,

$$P(A)P(B) = P(A)P(C) = 1\times 10^{-6}$$

e

$$P(A)P(B)P(C) = 1\times 10^{-9}$$

Então, pelo método exato a probabilidade do evento topo é

$$P(T) = 1.999\times 10^{-6}$$

Utilizando a aproximação do evento raro, tem-se

$$P(T) \approx 2.0\times 10^{-6}$$

Obviamente, quanto menores forem as probabilidades dos eventos básicos, melhor será a aproximação.

- Confiabilidade do sistema:
  - É obtida diretamente a partir da probabilidade de falha do mesmo, ou seja, do evento topo.
  - Assim, a confiabilidade do sistema para uma missão com duração t é dada por:

$$R_S(t) = 1 - P(C_1 + C_2 + \cdots + C_n)$$

  - Se as probabilidades dos eventos básicos são reduzidas, então podemos utilizar a aproximação do evento raro. Neste caso, a confiabilidade do sistema é obtida aproximadamente como

$$R_S(t) \approx 1 - \left[P(C_1) + P(C_2) + \cdots + P(C_n)\right]$$

Exemplo 16:

Considere a árvore de falha do exemplo 9. Encontre a probabilidade de ocorrência do evento topo se as probabilidades dos eventos *A*, *B*, e *C* são iguais a 0.1.

- Os cortes mínimos encontrados no exemplo 13 foram:

$$C_1 = A\cdot B\cdot C$$
$$C_2 = A\cdot B\cdot D$$

- Utilizando a aproximação do evento raro, tem-se

$$P(T) \approx P(A)P(B)P(C) + P(A)P(B)P(D)$$

logo,

$$P(T) \approx 0.1 \times 0.1 \times 0.1 + 0.1 \times 0.1 \times 0.1 = 0.003$$

- Note, porém, que os cortes mínimos C_1 e C_2 não são mutuamente exclusivos.
- Assumindo que todos os eventos básicos são independentes, a probabilidade exata do evento topo é

$$P(T) = P(A)P(B)P(C) + P(A)P(B)P(D) - P(A)P(B)P(C)P(D)$$

resultando em

$$P(T) = 0.0028$$

- Tente agora resolver os próximos casos

Exemplo 17 (Resolver):

Considere a árvore de falha do exemplo 10. Utilizando os cortes mínimos encontrados no exemplo 14, determine a probabilidade de ocorrência do evento topo. Considere as seguintes probabilidades de falha:

$$P(1) = P(2) = P(3) = 0.1$$
$$P(4) = P(5) = P(6) = 0.01$$
$$P(7) = 0.001$$

Exemplo 18 (Resolver):

Considere a árvore de falha do exemplo 11. Utilizando os cortes mínimos encontrados no exemplo 15, determine a probabilidade de ocorrência do evento topo. Assuma que:

- Todas as válvulas possuem a mesma probabilidade de falhar fechada igual a 0.02
- As bombas possuem probabilidade de falhar igual a 0.01
- A probabilidade de ruptura do tanque é 0.0001
- As probabilidades de falha do sistema de controle e do gerador são iguais a 0.001
