Cálculo de Índices de Confiabilidade em um Sistema Instrumentado de Segurança a partir de Modelos de Markov

Trabalho de Conclusão de Curso

Aluno: Thiago Antonio Melo Euzébio

Orientador: Péricles Rezende Barros, PhD. (UFCG/CEEI/DEE)

Universidade Federal de Campina Grande - UFCG
Centro de Engenharia Elétrica e Informática - CEEI
Departamento de Engenharia Elétrica - DEE

Campina Grande - PB - Brasil

Agosto 2008

Biblioteca Setorial do CDSA. Fevereiro de 2021.

Sumé - PB

Banca Examinadora

Péricles Rezende Barros, PhD
Professor/DEE/UFCG

José Sérgio da Rocha Neto, Doutor
Professor/DEE/UFCG

Apresentação

Este trabalho apresenta o uso de Modelos de Markov para o cálculo de índices de confiabilidade de Sistemas Instrumentados de Segurança.

O trabalho é dividido em cinco capítulos. O primeiro capítulo apresenta uma breve introdução e aborda o contexto no qual o projeto está inserido. O segundo capítulo introduz os principais termos usados em engenharia de confiabilidade, suas definições a partir de normas da ISA e IEC e as mais importantes variáveis probabilísticas necessárias para o projeto de um Sistema Instrumentado de Segurança. No terceiro capítulo é introduzido o modelamento de sistemas através de diagramas de Markov, além de mostrar como usá-lo para obter os índices de confiabilidade desejados. Já no quarto capítulo é feita a modelagem de três arquiteturas reais de sistemas, com estes modelos aplicamos os métodos descritos no capítulo anterior para obter resultados de PFD, PFS e MTTF. O último capítulo aborda as conclusões adquiridas nesse trabalho.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

O fenômeno do crescimento da indústria no século XX, norteada principalmente pela busca do aumento da produtividade através dos avanços tecnológicos utilizados nas plantas de controle de processo cada vez mais sofisticadas, trouxe também como conseqüências novos perigos, resultado dos desafios técnicos e dos novos limites de segurança e risco atingidos. O futuro da segurança no controle do processo encontra-se no gerenciamento integrado da segurança ou gestão de risco integrado, através do cumprimento dos padrões e normas que usam o risco como fator de medida a ser observado.

Tipicamente, em indústrias de processamento há pelo menos dois tipos de sistemas de controle automático: sistemas de controle regulatório e sistemas de segurança. A diferença entre os dois está na função que suas lógicas exercem. O primeiro está dedicado a manter as variáveis do processo controladas com o objetivo de otimizar o desempenho do processo; e o segundo volta-se para os sistemas de segurança, de forma a garantir que estas mesmas variáveis estejam dentro de limites considerados seguros para a operação da unidade.

A operação da maioria dos processos industriais, especialmente nas indústrias químicas e petroquímicas, envolve um grande risco de vazamentos de fluídos químicos, incêndios e explosões.

A instrumentação de segurança (Safety Instrumented Systems - SIS) foi especificamente aplicada para a proteção do pessoal de operação, do equipamento e do meio ambiente através da redução da probabilidade ou da severidade desses acidentes.

Capítulo 2

Sistemas Instrumentados de Segurança

2.1 Introdução

Um sistema instrumentado de segurança (SIS) é um sistema de controle que consiste de sensores, um ou mais controladores (frequentemente chamados de executor da lógica) e elementos finais.

O propósito de um sistema instrumentado de segurança é reduzir para um nível tolerável o risco de um processo se tornar perigoso. O SIS faz isso diminuindo a freqüência de acontecer acidentes indesejáveis. A quantidade de redução de risco que um SIS pode fornecer é representado pelo seu nível de integridade de segurança (*SIL - Safety Integrity Level*), o qual é definido por uma escala de probabilidade de falha em demanda (*PFD - Probability of Failure on Demand*).Um SIS elimina circunstâncias perigosas e, então, toma ações para mover o processo para um estado seguro, prevenindo assim ocorrência de acidentes.

Implementar um Sistema Instrumentado de Segurança e, consequentemente, selecionar um SIL deve envolver leis, regulamentações e padrões nacionais e internacionais. Na década de 90, empresas e grupos industriais desenvolveram normas para projetar, construir e manter um SIS. Em 1996, a ISA (The Instrumentation, Systems, and Automation Society) publicou uma norma para guiar a classificação de Sistemas Instrumentados de Segurança para indústrias de processo dos Estados Unidos, a norma ANSI/ISA-S84.01, que introduziu o conceito de Nível de Integridade de Segurança (Safety Integrity Level - SIL). Subsequentemente, em 1998, o IEC (International Eletrotechnical Commission), com sede em Genebra, começou a elaborar a norma de segurança IEC61508 para auxiliar as empresas que utilizam sistemas instrumentados de segurança a proteger seu pessoal e suas instalações de eventos perigosos. A norma, formalmente intitulada "Segurança Funcional de Sistemas de Segurança Elétricos/Eletrônicos/Eletrônico-

Programáveis", é composta de sete partes que orientam o adequado gerenciamento do ciclo de vida e de todos os componentes do SIS. As três primeiras partes da norma referem-se ao gerenciamento, ao desenvolvimento, à instalação e à operação do hardware e do software do sistema de segurança. As quatro partes restantes tratam especificamente das definições, aplicações e anexos informativos à norma.

2.2 Nível de Integridade de Segurança

Níveis de Integridade de Segurança (*SILs - Safety Integrity Levels*) são categorias baseadas na probabilidade de falha em demanda (PFD) para uma função instrumentada de segurança particular. As categorias de PFD são divididas de um até três, como definido pela norma ANSI/ISA-S84.01-1996, ou de um até quatro como definido pela norma IEC 61508 e 61511. Na tabela 2.1 temos os níveis de PFD associados com os níveis de fator de redução de riscos (RRF - risk reduction factor) e seus respectivos valores de SIL.

Tabela 2.1: Níveis de Integridade de Segurança e correspondentes PFD e RRF

SIL	Escala PFD	Escala RRF
4	$10^{-4} \rightarrow 10^{-5}$	$10.000 \rightarrow 100.000$
3	$10^{-3} \rightarrow 10^{-4}$	$1.000 \rightarrow 10.000$
2	$10^{-2} \rightarrow 10^{-3}$	$100 \rightarrow 1.000$
1	$10^{-1} \rightarrow 10^{-2}$	$10 \rightarrow 100$

O SIL é o parâmetro chave que especifica a quantidade de redução de risco que um equipamento de segurança deve alcançar para uma função em particular. Se um SIL não for selecionado, o equipamento não poderá ser projetado de maneira satisfatória, já que só a ação será especificada sem a integridade necessária. Para se fazer um projeto adequado, dois tipos de informações são necessárias: uma especificação do que o equipamento faz e uma especificação de quão bem o equipamento desempenha essa função. O nível de integridade de segurança quantifica essa segunda especificação, indicando a mínima probabilidade que o equipamento irá desempenhar sua função com sucesso quando requisitado.

Selecionar nível de integridade de segurança significa escolher uma meta a ser alcançada ao longo dos próximos passos em que o ciclo de vida de segurança é baseado. Portanto, a seleção do SIL resulta em um importante guia quando se está selecionando equipamentos ou tomando decisões de manutenção.

2.3 Funções Instrumentadas de Segurança

Segundo a terminologia adotada pela norma IEC 61511, uma função instrumentada de segurança (*SIF - Safety Instrumented Function*) é uma ação que um SIS toma para trazer o processo ou o equipamento sob controle para um estado seguro. Essa função consiste de um conjunto de ações que protege contra um perigo específico. Um sistema instrumentado de segurança (SIS), por outro lado, é uma coleção de sensores, solucionadores da lógica e atuadores que executam uma ou mais funções instrumentadas de segurança que são implementadas por um propósito comum, tal como um grupo de funções protegendo o mesmo processo. Alguns exemplos de SIF são:

- SIF 1: Alta temperatura do reator fecha as duas válvulas de alimentação.
- SIF 2: Alta pressão na coluna ou alta temperatura na coluna fecha a válvula do vaporizador.
- SIF 3: Alta pressão na coluna fecha as duas válvulas de alimentação do reator.

A lógica para todas funções de segurança é desenvolvida em um CLP de segurança. Esse CLP irá então combinar-se com todos equipamentos associados a cada SIF para assim constituir o SIS.

Como é apresentado na figura 2.1, pode-se implementar uma ou mais SIF num SIS. Ainda na figura, podemos ver que uma função de segurança pode conter múltiplas entradas e saídas, por exemplo, a SIF 1 é executada com duas saídas, as duas válvulas de alimentação do reator, e a SIF 2 possui duas entradas, as medidas de pressão e de temperatura elevadas. Um sistema pode conter equipamentos comuns entre as suas múltiplas SIF, no caso da figura as duas SIF usam o mesmo executor da lógica, quando isso ocorre os equipamentos devem ser projetados tal que alcancem a SIL da SIF que possui maior número de requerimentos.

2.4 Taxa de Falha

Em engenharia de confiabilidade, a variável estatística de interesse fundamental é o "tempo para ocorrer uma falha". A medição do tempo para ocorrer uma falha pode ser analisada para se gerar uma outra importante medição, a taxa de falha. Taxa de falha instantânea é uma medida comum de confiabilidade que representa o número de falhas por unidade de tempo de uma quantidade de componentes expostos à falha. Falhas de equipamentos industriais são normalmente especificadas como taxas de falha. Para se quantificar as taxas de falha de equipamentos é preciso ter um histórico de informações de como eventos que causam ou propagam um acidente ocorreram no passado.

$$\lambda = \frac{\texttt{Falhas por Unidade de Tempo}}{\texttt{Quantidade Exposta}} \tag{2.1}$$

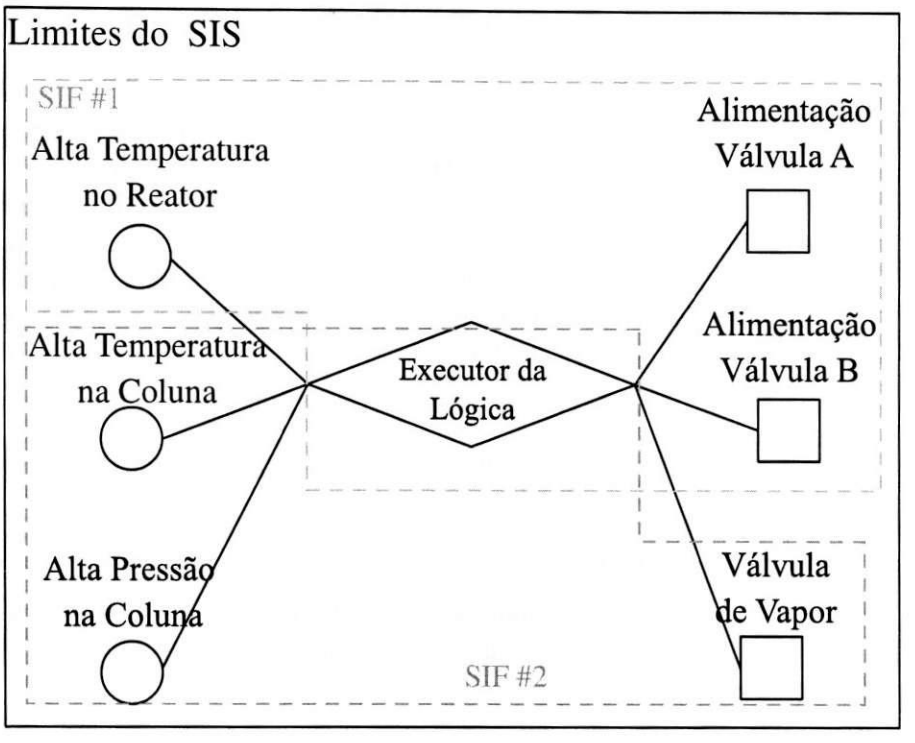

Figura 2.1: SIS contendo duas Funções Instrumentadas de Segurança

A taxa de falha é comumente representada pela letra minúscula grega lambda (λ), cuja unidade é a inversa do tempo. No projeto de dispositivos eletrônicos é comum usar unidade de "falhas por bilhão (10^9) de horas", esta unidade é conhecida como FIT (*Failure unIT*). Por exemplo, um circuito integrado particular passará por sete falhas durante um bilhão de horas de operação, logo possui uma taxa de falha de 7 FITs.

2.5 PFD e PFS

Existe a probabilidade de que um sistema instrumentado de segurança falhe com suas saídas não energizadas, isto é chamado de probabilidade de falha segura (PFS). Existe também a probabilidade de que o sistema falhe com suas saídas energizadas, nesse caso temos uma probabilidade de falha em demanda (PFD).

2.5.1 Modos de Falha

Modos de falha devem ser considerados em sistemas projetados para aplicações de proteção de segurança. Dois modos de falha são importantes: seguro e em demanda. A norma ISA S84.01 define estado seguro como o estado em que o equipamento sob

controle ou processo alcançará após operação adequada do SIS. Na maioria das aplicações mais críticas, projetistas optam por uma condição não energizada como sendo o estado seguro, assim um sistema projetado para aplicações de proteção de segurança deve desenergizar suas saídas para alcançar tal estado.

Quando um sistema normalmente energizado está operando com sucesso, figura 2.2 ,o circuito de entrada lê o sensor, desempenha as funções de cálculo e gera a saída. As chaves de entrada são normalmente energizadas para indicar uma condição segura, e os circuitos de saída fornecem energia para uma carga (válvulas, por exemplo). A chave do sensor abre, desenergiza, para indicar uma condição de perigo potencial. Se o executor da lógica, tipicamente um CLP de segurança, for programado para reconhecer a entrada desenergizada vinda do sensor como um perigo potencial, deverá desenergizar suas saídas, essa ação é projetada para abrandar o perigo.

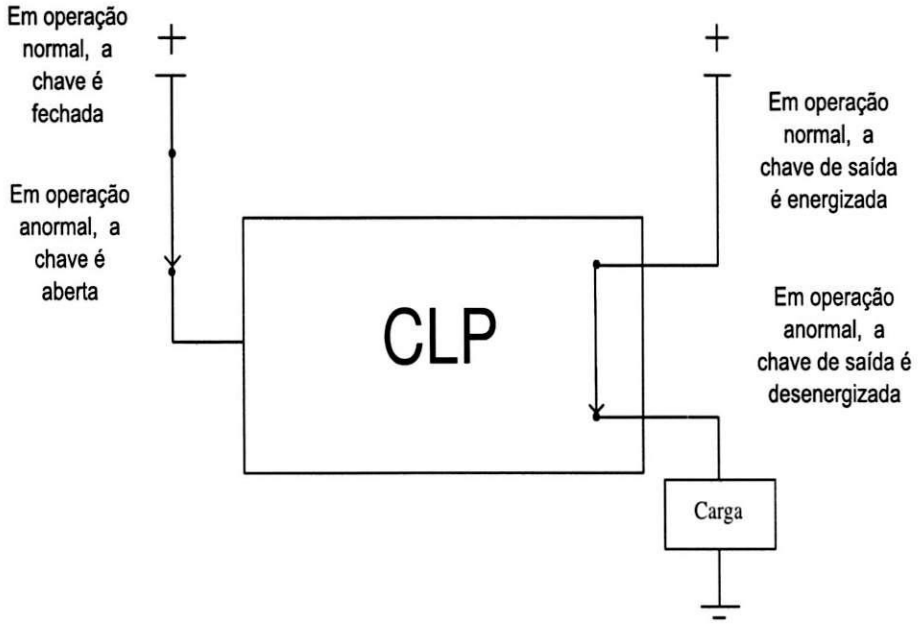

Figura 2.2: Sistema Normalmente Energizado - Operação com sucesso

Uma falha segura em tal sistema acontece quando a saída se desenergiza mesmo quando não há uma condição de perigo potencial. Isto pode acontecer de diversas formas, os circuitos de entrada podem falhar de tal maneira que o executor da lógica leia do sensor uma situação de perigo que não exista, o próprio executor da lógica pode falhar em suas funções e enviar para saída o comando de desenergizar a carga, ou mesmo os circuitos de saída podem falhar em circuito-aberto.

Falhas perigosas são definidas como sendo aquelas que evitam que o SIS atue numa

condição de potencial perigo chamada de "demanda". Um CLP de segurança é especialmente projetado para evitar que este modo de falha aconteça.

Capítulo 3

Modelos de Markov

3.1 Sistemas Reparáveis

Os sistemas reparáveis são comuns em ambientes industriais por oferecerem vantagens em disponibilidade e segurança, porém eles devem ser instalados em locais de fácil acesso para a substituição de seus módulos e manutenção. Algumas configurações de sistemas são bastante tolerantes a falhas de módulos reparáveis, podendo funcionar sem parar com uma probabilidade pequena de falha ao longo de anos.

O modelamento de Markov de sistemas de segurança preenche alguns objetivos que outros métodos não possuem, como, por exemplo, modelar um sistema reparável para uma grande variedade de taxas de falha e tempo de reparo, além de levar em conta tempos de reparo realísticos e diversas configurações de sistemas. Outro diferencial é que o modelamento de Markov pode ser aplicado a sistemas totalmente reparáveis e também a sistemas parcialmente reparáveis.

A técnica de modelamento através de diagramas de Markov usa apenas dois símbolos que estão na figura 3.1.

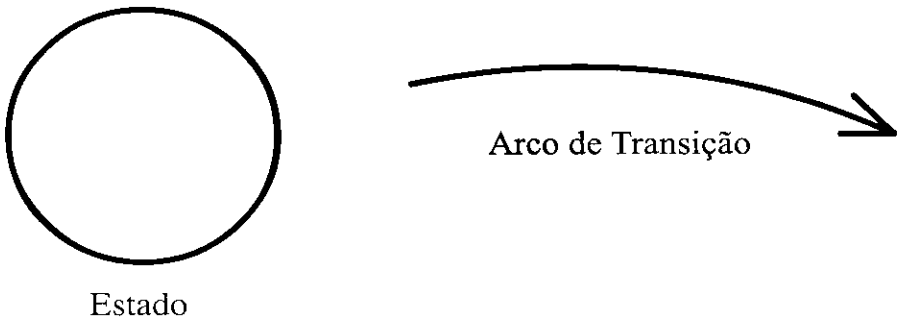

Figura 3.1: Símbolos do modelo de Markov

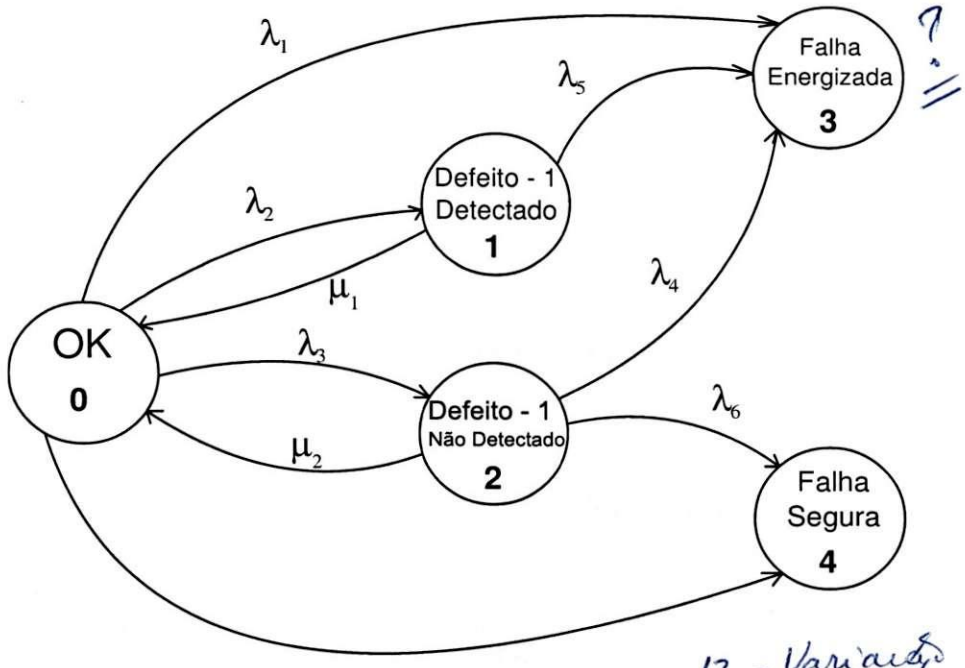

Figura 3.2: Modelo de Markov

O modelo de Markov na figura 3.2 demonstra como esses símbolos são usados. Os estados (círculos) representam combinações de componentes em operação com sucesso e componentes com falha. Possíveis falhas e reparos de componentes são representados com arcos de transição, setas que partem de um estado para outro, sendo possível um grande número de combinações de sucesso e de falha de operação de componentes.

Um modelo de Markov pode mostrar em um único desenho a operação inteira de sistema de controle tolerante a faltas. Nele há o estado em que todo o sistema opera com sucesso, os estados em que o sistema falha como todo e ainda há aqueles estados em que o sistema opera com sucesso, mas degradado, isto é, existindo falta de um ou mais componente que o deixa vulnerável a uma falha completa.

Um grande número de diferentes índices de confiabilidade e segurança podem ser gerados a partir de um modelo de Markov. Além disso pode ser calculada a probabilidade de operação em sucesso contínuo durante um intervalo de tempo; a probabilidade de sucesso de um sistema em um tempo t, conhecido como disponibilidade; índices de sucesso do sistema, como MTTF.

Para sistemas totalmente reparáveis, a disponibilidade é obtida tanto como função do tempo, quanto em estado estacionário. Confiabilidade do sistema como função do tempo é obtida ignorando os arcos de reparo dos estados de falha para estados de

sucesso.

Uma série completa de índices de segurança pode ainda ser calculada a partir do modelo de Markov. Sabendo que com as técnicas usadas as probabilidades de estado são função do tempo, a probabilidade de falha em demanda (PFD) pode ser obtida adicionando probabilidades dos estados, em que o sistema não poderá responder a uma requisição (estados onde há falha perigosa). O valor da PFD é fornecido como uma função do tempo como parte da solução do processo. De forma geral, o modelamento por Markov é a técnica mais flexível para evolução do sistema de controle.

3.2 Resolvendo Modelos de Markov

Um processo de Markov é definido como aquele em que a variável futura é determinada pela variável presente, mas é independente das variáveis precedentes. Esta definição foi feita pelo matemático russo Andrei Andreyevich Markov (1856-1922), o qual enfatizou seqüências onde a variável toma valores discretos, chamadas então de *cadeias de Markov*. Esses métodos aplicam-se bem aos precessos falha/reparo porque as combinações de falhas formam sistemas de estados discretos. Além disso, processos falha/reparo têm o movimento entre estados unicamente em função do estado presente e da falha atual.

A técnica de construção do modelo de Markov envolve definição de todos estados mutuamente exclusivos sucesso/falha em um sistema, esses são representados por círculos com tarjas descritivas. O sistema pode fazer a transição de um estado para outro sempre que uma falha ou reparo ocorre. Transições entre estados são representados por setas (arcos de transição) e são nominados com a taxa de falha ou taxa de reparo como apropriado. Este método é usado para descrever a característica do sistema com o tempo, o qual é modelado em incrementos discretos, por exemplo, uma vez por hora.

Um modelo de Markov para um único componente não reparável com um modo de falha pode ser visto na figura 3.3, em que dois estados são apresentados. No estado 0, o componente está operando com sucesso. No estado 1, o componente falhou e permanece em falha. Uma transição que representa falha do componente, a qual indica movimento do estado 0 para o estado 1, essa seta acompanha a letra minúscula grega lambda (λ) que representa a taxa de falha instantânea do componente.

Um único componente reparável com um modo de falha tem um modelo de Markov como o da figura 3.4. Os dois estados são os mesmos dos dois descritos anteriormente para um compenente não reperável, porém nesse novo caso existem dois arcos de transição, o arco superior representa uma falha - movimento do estado 0 para o estado 1. O arco inferior representa um reparo - movimento do estado de falha 1 para o estado

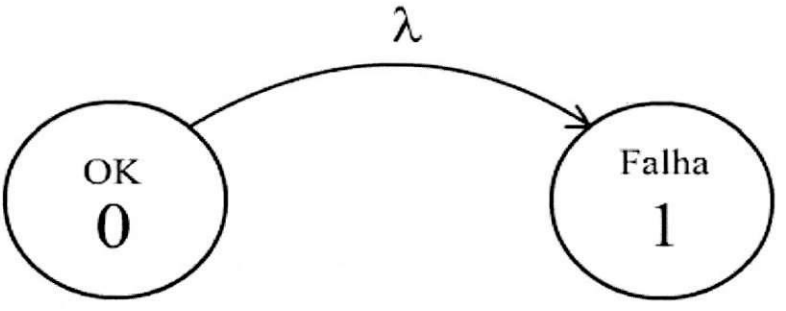

Figura 3.3: Modelo de Markov para um único componente não reparável

de sucesso 0. A taxa de reparo é representada pela letra minúscula grega mu (μ).

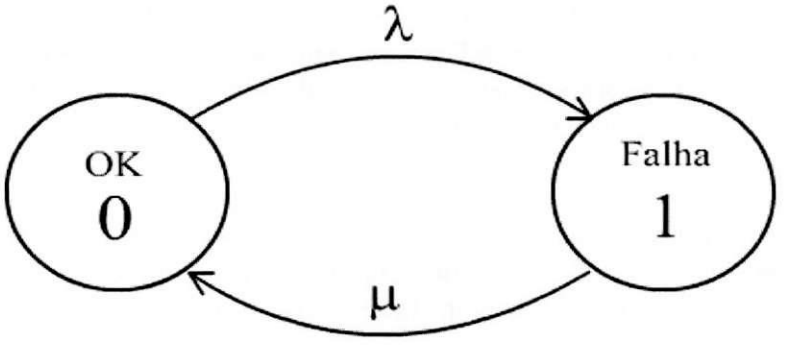

Figura 3.4: Modelo de Markov para um único componente reparável

Modelos de Markov podem representar sistemas não reparáveis, parcialmente reparáveis, ou completamente reparáveis. Múltiplos modos de falha podem ser modelados usando quantos estados de falha forem necessários. Falhas detectadas por diagnósticos on-line podem ser distinguidas daquelas indetectáveis, separando os estados. Falhas de modo comum também podem ser acrescidas ao modelo. Na figura 3.2 temos um modelo de Markov para um sistema de controle dual. Ele é parcialmente reparável em dois estados de falha. Falhas que são detectadas por diagnósticos computadorizados (estado 1) são diferenciadas daquelas que não são (estado 2). Os modelos podem crescer o quanto for necessário para que se encaixem ao nível de precisão desejado. Assim, temos que os modelos de Markov podem representar sistemas não reparáveis, parcialmente reparáveis ou completamente reparáveis.

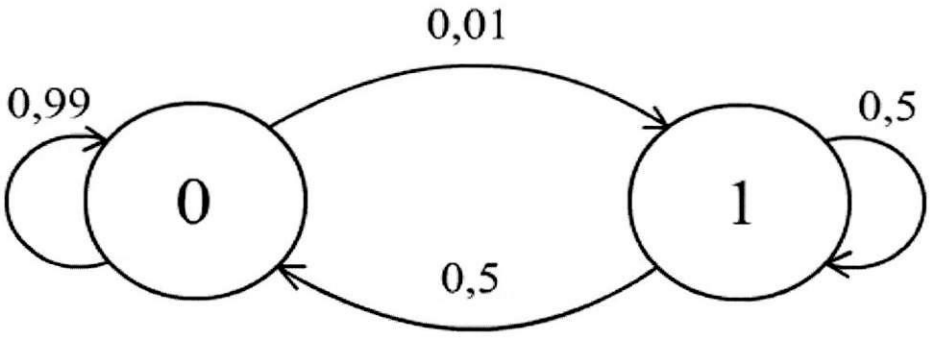

Figura 3.5: Exemplo de Modelo de Markov

3.3 Matriz de Transição

O modelo pode ser representado em uma forma matricial contendo as taxas de probabilidade de transição entre os estados. Uma matriz n x n é feita contendo essas taxas de probabilidades, em que n é igual ao número de estados. Essa matriz é conhecida como matriz estocástica de probabilidade de transição, ou ainda matriz de transição. A matriz de transição do modelo de Markov apresentado na figura 3.5 é escrita como:

$$P = \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \tag{3.1}$$

Cada linha e cada coluna representa um dos estados. O número em uma determinada linha e coluna exibe a probabilidade de movimento de um estado inicial, representado pela linha para um estado final representado pela coluna. Por exemplo, na matriz P, o número na linha 0 e coluna 1 $(0,01)$ representa a probabilidade de movimento do estado 0 para o estado 1 durante o próximo intervalo de tempo. O número na linha 0, coluna 0 $(0,99)$ representa a probabilidade de se mover do estado 0 para o próprio estado 0, isto é, probabilidade de permanecer no estado 0 no próximo intervalo de tempo. As demais entradas têm interpretação similar. Uma matriz de transição contém toda informação necessária sobre um modelo de Markov. Essa matriz é usada como ponto de partida para métodos de cálculo mais completos.

3.4 Probabilidades em Estado Estacionário

Como foi dito na seção anterior, uma matriz de transição **P** trata-se de uma matriz que apresenta as probabilidades de movimento de um estado para outro em um intervalo de tempo (passo). Esta matriz pode ser multiplicada por ela mesma para se obter probabilidades de transição para múltiplos intervalos de tempo.

Como **P** é quadrada, o resultado será uma outra matriz n X n que fornece as probabilidades de movimento entre estados dois passos no futuro.

$$P^2 = \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \cdot \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \tag{3.2}$$

$$P^2 = \begin{bmatrix} 0,9851 & 0,0149 \\ 0,745 & 0,255 \end{bmatrix} \tag{3.3}$$

Se esta última matriz for multiplicada por **P** novamente, uma matriz com probabilidades de transição após três passos é obtida.

$$P^3 = \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \cdot \begin{bmatrix} 0,9851 & 0,0149 \\ 0,745 & 0,255 \end{bmatrix} \tag{3.4}$$

$$P^3 = \begin{bmatrix} 0,9827 & 0,0173 \\ 0,8650 & 0,1350 \end{bmatrix} \tag{3.5}$$

Este processo pode ser prolongado o quanto for desejado para se obter a matriz de probabilidades de transição no enésimo passo. Por exemplo:

$$P^4 = P \cdot P^3 = \begin{bmatrix} 0,9815 & 0,0185 \\ 0,9239 & 0,0761 \end{bmatrix} \tag{3.6}$$

$$P^5 = P \cdot P^4 = \begin{bmatrix} 0,9809 & 0,0191 \\ 0,9527 & 0,0473 \end{bmatrix} \tag{3.7}$$

$$P^6 = P \cdot P^5 = \begin{bmatrix} 0,9807 & 0,0193 \\ 0,9668 & 0,0332 \end{bmatrix} \tag{3.8}$$

Após esses passos é possível perceber que as mudanças entre as probabilidades referentes ao mesmo movimento (mesma posição da matriz) vai diminuindo, assim, em algum passo teremos $P^{n+1} = P^n$, como vemos abaixo para o exemplo.

$$P^{18} = P \cdot P^{17} \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \cdot \begin{bmatrix} 0,98039 & 0,01961 \\ 0,98039 & 0,01961 \end{bmatrix} \tag{3.9}$$

$$P^{18} = \begin{bmatrix} 0,98039 & 0,01961 \\ 0,98039 & 0,01961 \end{bmatrix} \tag{3.10}$$

Nesse ponto, nomeamos a matriz de P^L, que é conhecida como matriz de probabilidade de estado limite. Observe ainda que a primeira e a segunda linha possuem mesmos números. A probabilidade de se mover para o estado 0 em n passos é a mesma independentemente do estado inicial.

Entretanto, o estado inicial afeta nos passos iniciais as probabilidades dependentes do tempo. As probabilidades de estado inicial são representadas por uma matriz linha (1 x n), **S**. Esta matriz linha é uma lista de números que indica a probabilidade de que um sistema estará em cada um dos estados possíveis. S^0 é a lista de probabilidades iniciais (intervalo de tempo 0). Por exemplo, se um sistema sempre começa em um estado particular, S^0 conterá um único 1 e demais células serão 0. Isto é,

$$S^0 = \begin{bmatrix} 1 & 0 \end{bmatrix} \tag{3.11}$$

A matriz S^n para qualquer outro intervalo de tempo particular é obtida multiplicando S^{n-1} vezes P ou S^0 vezes P^{n-1}.

$$S^1 = S^0 \cdot P = \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \tag{3.12}$$

$$S^1 = \begin{bmatrix} 0,99 & 0,01 \end{bmatrix} \tag{3.13}$$

Assim como na matriz de transição P, esse processo pode continuar até se obter o enésimo passo.

$$S^2 = S^1 \cdot P = \begin{bmatrix} 0,9851 & 0,0149 \end{bmatrix} \tag{3.14}$$

$$S^3 = S^2 \cdot P = \begin{bmatrix} 0,9827 & 0,0173 \end{bmatrix} \tag{3.15}$$

$$S^4 = S^3 \cdot P = \begin{bmatrix} 0,9815 & 0,0185 \end{bmatrix} \tag{3.16}$$

$$S^5 = S^4 \cdot P = \begin{bmatrix} 0,9809 & 0,0191 \end{bmatrix} \tag{3.17}$$

$$S^6 = S^5 \cdot P = \begin{bmatrix} 0,9807 & 0,0193 \end{bmatrix} \tag{3.18}$$

Assim como aconteceu anteriormente, os números mudam menos a cada novo intervalo de tempo. Até que não existe mais variação significativa.

$$S^{18} = S^{17} \cdot P = \begin{bmatrix} 0,98039 & 0,01961 \end{bmatrix} \cdot \begin{bmatrix} 0,99 & 0,01 \\ 0,5 & 0,5 \end{bmatrix} \tag{3.19}$$

$$S^{18} = \begin{bmatrix} 0,98039 & 0,01961 \end{bmatrix} \tag{3.20}$$

Ao final de n passos, temos em cada coluna do vetor-linha S a probabilidade de se estar em cada estado do diagrama. Caso quiséssemos o valor da probabilidade de falha em demanda de um sistema após um ano, bastaria apenas somarmos os valores dos estados que indicam falha em demanda do sistema obtidos na matriz S após 8760 iterações (número de horas em um ano).

3.5 Tempo Médio de Falha - MTTF

Uma única medida de sucesso é requisitada para sistemas modelados com estados absorvedores. O tempo médio de falha, *MTTF - mean time to failure*, é comumente usado para isso. Em termos de um modelo de Markov em tempo discreto, o tempo para occorer uma falha é representado por uma média do número de incrementos de tempo entre o *startup* da planta e a sua falha ao longo de diversos inícios independentes.

Um método de se achar o MTTF seria o de simular diversos modelos de Markov de um sistema e contar o tempo entre o início e a ocorrência de uma falha. Poderíamos então calcular uma média dos resultados obtidos em todas essas simulações, essa média representaria o MTTF do sistema modelado.

Entretanto, não há necessidade de se realizar diversas simulações e obter a média dos resultados para se ter o MTTF. O MTTF a partir de um modelo de Markov pode ser calculado a partir da matriz de transição. O primeiro passo é o de criar uma matriz truncada que contenha apenas os estados transientes da matriz. Isso é feito eliminando as linhas e colunas dos estados absorvedores. Usando o sistema de controle representado no modelo de Markov da figura 3.6, temos a seguinte matriz truncada, a qual denominamos de Q.

$$Q = \begin{bmatrix} 0,996 & 0,002 & 0,002 \\ 0,1 & 0,899 & 0 \\ 0,1 & 0 & 0,899 \end{bmatrix} \tag{3.21}$$

A matriz Q é subtraída da matriz identidade, I.

$$I - Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0,996 & 0,002 & 0,002 \\ 0,1 & 0,899 & 0 \\ 0,1 & 0 & 0,899 \end{bmatrix} \tag{3.22}$$

$$I - Q = \begin{bmatrix} 0,004 & -0,002 & -0,002 \\ -0,1 & 0,101 & 0 \\ -0,1 & 0 & 0,101 \end{bmatrix} \tag{3.23}$$

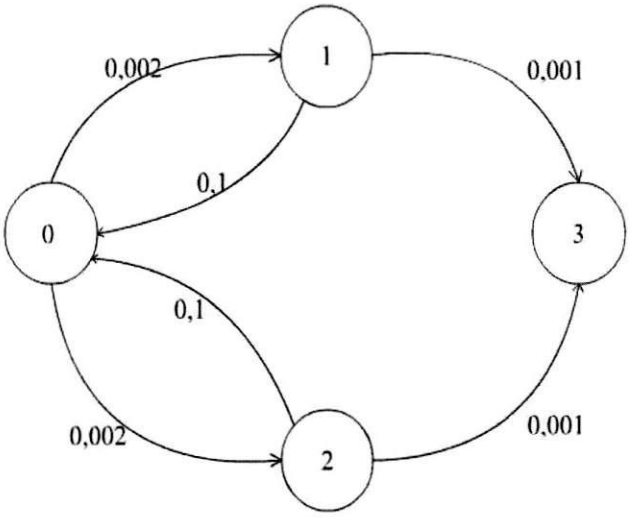

Figura 3.6: Sistema de controle modelado por Markov

Outra matriz, chamada de matriz N, é obtida invertendo a matriz $(I - Q)$.

$$N = [I - Q]^{-1} = \begin{bmatrix} 25250 & 500 & 500 \\ 25000 & 504,95 & 495,05 \\ 25000 & 495,05 & 504,95 \end{bmatrix} \tag{3.24}$$

A matriz N fornece o número esperado de incrementos de tempo que o sistema permanece em cada estado de sucesso (estados de transição) como uma função do estado de partida. No exemplo anterior, a primeira linha da matriz N contém o número de incrementos de tempo que o sitema permanece por cada estado de transição se iniciarmos do estado 0. Na linha do meio temos o número de incrementos de tempo caso o ponto de partida seja o estado 1. Na linha inferior temos o número de incrementos de tempo se iniciarmos do estado 2. Se um sistema sempre parte do estado 0, podemos somar os números da linha superior da matriz N para obter o número total de incrementos de tempo em todos os estados de sucesso do sistema. Quando este valor é multiplicado pelo incremento de tempo, obtemos o MTTF quando o sistema inicia do estado 0. No exemplo, esse número é igual a 26.250 horas, já que usamos um incremento de tempo de 1 hora. Se o sistema fosse iniciado no estado 2 ou 3, esperaríamos que o sistema falhasse após 26.000 horas em média.

* { MTTF ≠ MTBF

Capítulo 4

Arquiteturas do Sistema

4.1 Introdução

As arquiteturas de controle 1oo1 (*one out of one*), 2oo2 (*two out of two*), 2oo3 (*two out of tree*), etc. são configurações específicas de elementos de software ou hardware que compõe um sistema. A nomenclatura dessas arquiteturas são dadas de forma que o primeiro número designa quantos elementos são necessários para sinalizar uma condição de parada do sistema, e o segundo número designa o total de elementos que compõe o sistema.

Existem diversas formas de se planejar componentes de controle ao se construir um sistema. Algumas arquiteturas são projetadas para maximizar a probabilidade de uma operação ser bem sucedida. Já outras arquiteturas são projetadas para minimizar a probabilidade de falha com saídas energizadas.

4.2 1oo1: Sistema de Canal Único

O controlador com única unidade de microprocessamento e única entrada/saída representa um sistema mínimo, figura 4.1 . Não há tolerância a falta nesse sistema, também não há modo de proteção a falha. Os circuitos eletrônicos podem falhar de forma segura (saídas não energizadas, circuito aberto) ou perigosamente (saídas congeladas ou energizadas, curto circuito). Nesse caso quatro categorias de falha são inclusas: DD, *dangerous detected*, perigosa detectada; DU, *dangerous undetected*, perigosa não detectada; SD, *safe detected*, segura detectada; SU, *safe undetected*, segura não detectada.

4.2.1 Modelo de Markov para 1oo1

A arquiterura 1oo1 pode ser modelada usando um modelo de Markov, figura 4.2. No modelo de Markov para esta configuração, estado 0 representa a condição em que não existem falhas. A partir deste estado o controlador pode alcançar outros três estados.

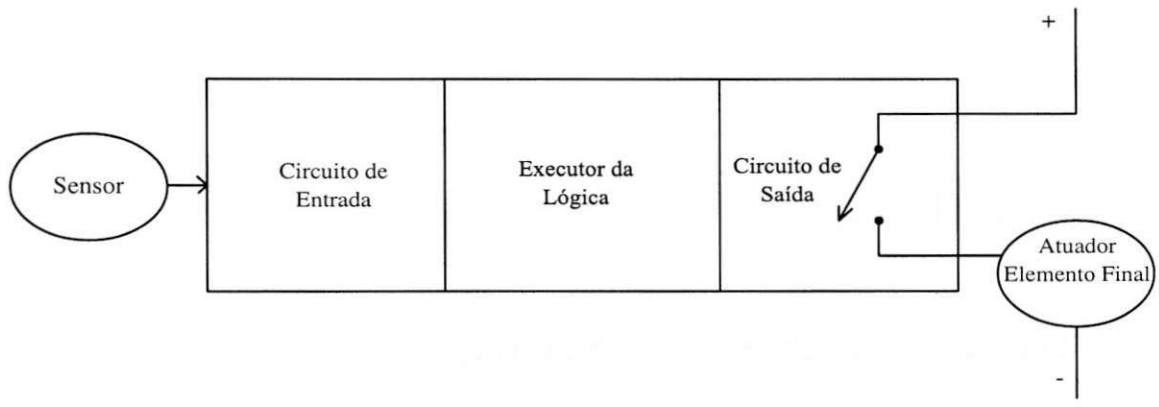

Figura 4.1: Arquitetura 1oo1

Estado 1 representa a condição de falha segura. Nesse estado o controlador falha com suas saídas não energizadas. Estado 2 representa a condição de falha perigosa detectada. Dessa vez o controlador falha com suas saídas energizadas, mas a falha é detectada por diagnóstico e pode ser reparada. Da mesma forma no estado 3 há uma falha perigosa, entretanto a falha não é detectada por diagnósticos on-line.
A matriz de transição P para o sistema 1oo1 é:

$$P = \begin{bmatrix} 1-(\lambda^S+\lambda^D) & \lambda^{SD}+\lambda^{SU} & \lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 1-\mu_O & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.1}$$

4.2.2 Cálculo do MTTF

Para derivar uma fórmula que se ache o MTTF, usa-se as técnicas descritas no Capítulo 3. Em um primeiro passo, as linhas e colunas dos estados de falha na matriz de transição são truncadas. Esta operação resulta na matriz Q:

$$Q = [1-(\lambda^S+\lambda^D)] \tag{4.2}$$

Esta é subtraída da matriz identidade:

$$I - Q = 1 - [1-(\lambda^S+\lambda^D)] \tag{4.3}$$

$$I - Q = \lambda^S + \lambda^D \tag{4.4}$$

A matriz N é obtida a partir de $[I-Q]^{-1}$. Nesse caso,

$$N = \frac{1}{\lambda^S+\lambda^D} \tag{4.5}$$

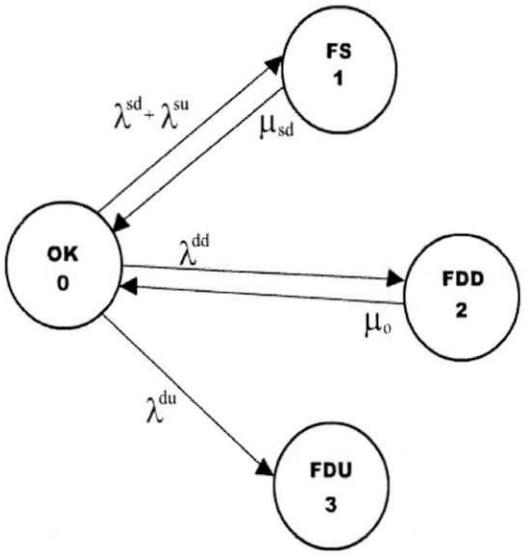

Figura 4.2: Modelo de Markov 1oo1

Como o MTTF é a soma dos elementos da linha de N para um dado estado inicial, temos simplesmente que:

$$MTTF = \frac{1}{\lambda^S + \lambda^D} \tag{4.6}$$

Para um determinado PLC de segurança cujas taxas de falha e de reparo estão na tabela 4.1, o seu MTTF em uma arquitetura 1oo1 seria:

$$MTTF = 61784 \texttt{ horas} \tag{4.7}$$

Tabela 4.1: Taxas de falha e de reparo de um PLC para cálculo do seu PFD e PFS

λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	μ_{SD}	μ_o
$9,996 \cdot 10^{-6}$	$9,800 \cdot 10^{-8}$	$5,956 \cdot 10^{-6}$	$1,120 \cdot 10^{-7}$	$0,0147$	$0,125$

4.2.3 Cálculo do PFD e PFS

A probabilidade do sistema permanecer em um determinado estado pode ser calculada através dos métodos propostos no capítulo 3, Modelos de Markov. Na tabela 4.1 temos as características de interesse de um PLC de segurança.

Os valores de taxa de falha e de reparo são substituídos na matriz de transição P.

$$P = \begin{bmatrix} 0,9999838 & 0,0000101 & 0,0000060 & 0,000001 \\ 0,0416667 & 0,9583333 & 0 & 0 \\ 0,0125 & 0 & 0,875 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.8}$$

Assumimos que a unidade está operando perfeitamente quando iniciada, logo a matriz S no momento de *startup* é definida como:

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \tag{4.9}$$

Após um ano (8760 horas), teríamos a seguinte matriz S:

$$S = \begin{bmatrix} 0,9987 & 2,419 \cdot 10^{-5} & 4,758 \cdot 10^{-5} & 9,803 \cdot 10^{-4} \end{bmatrix} \tag{4.10}$$

Como explicado no capítulo anterior, cada coluna do vetor-lina S representa a probabilidade de se estar em um determinado estado do modelo. Por exemplo, o valor de S(0) após 8760 horas é de 0,99873, isto é, o sistema possui probabilidade de 99,873% de se encontrar no estado 0, o qual, como foi definido no modelo da figura 4.2, indica que o sistema está operando sem falhas.

A PFS após um ano será dada pelo valor de S(1), já que no modelo o estado 1 representa falha do sistema de forma segura. A PFD será a soma de S(2) e S(3), no modelo o estado dois representa falha do sistema em demanda detectada e o estado três falha em demanda não detectada. Portanto a PFS e PFD do sistema após um ano, será:

$$PFS = S(1) = 0,00024195 \tag{4.11}$$

$$PFD = S(2) + S(3) = 0,0010279 \tag{4.12}$$

4.3 1oo2: Sistema de Canal Duplo

Dois controladores podem ser ligados para minimizar o efeito de falhas perigosas. No caso de dois controladores ligados em série no seus circuitos de saída, seria preciso que os dois falhassem de forma perigosa para que o sistema falhasse também de forma perigosa. Normalmente a configuração 1oo2 utiliza dois processadores independentes com suas respectivas portas de entrada e saída, figura 4.3. Esse sistema oferece baixa probabilidade de falha em demanda (PFD), mas aumenta a probabilidade de falhas de modo seguro (PFS).

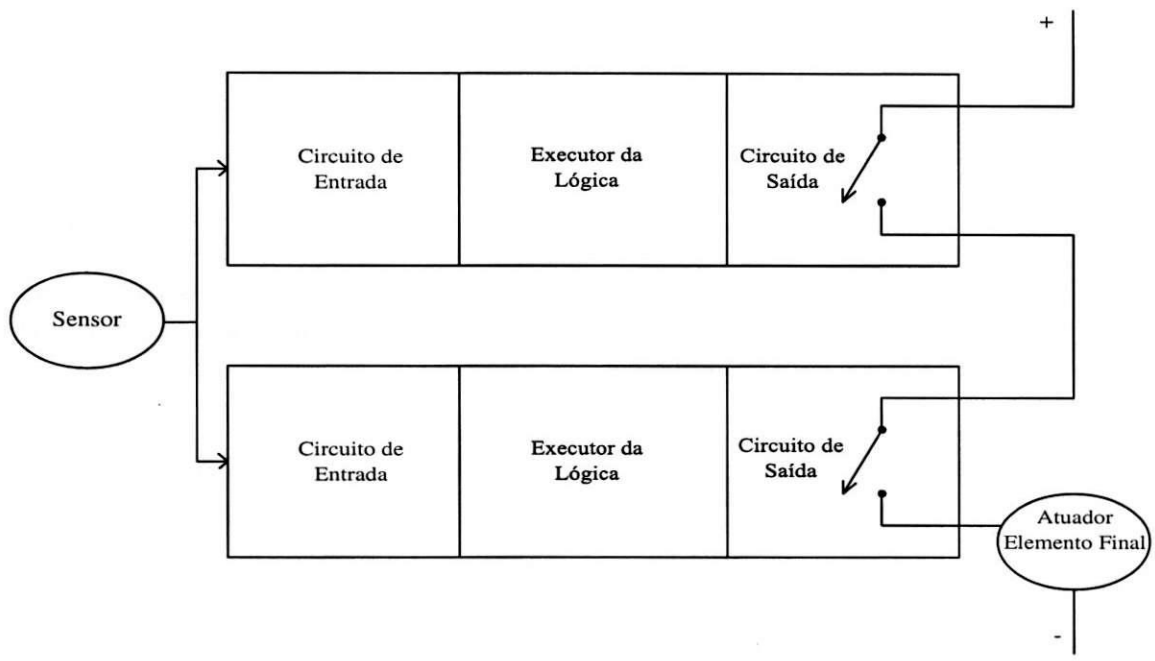

Figura 4.3: Arquitetura 1oo2

4.3.1 Falha por Causa Comum

Uma falha por causa comum é definida como a falha de mais de um componente devido à mesma causa. Um modelo chamado de Beta divide as taxas de falha dos componentes em dois, a porção normal, λ^N e a porção de causa comum, λ^C.

$$\lambda^C = \beta \cdot \lambda \tag{4.13}$$

$$\lambda^N = (1 - \beta) \cdot \lambda \tag{4.14}$$

O fator β é baseado nas chances de múltiplas unidades falharem devido ao mesmo motivo, isto leva em conta o local instalado, o isolamento elétrico, a resistência dos componentes ao ambiente e as diferenças entre os componentes redundantes [Wmg98].

Falha devido a causa comum pode resultar em falha segura ou perigosa do sistema. O sobrescrito SC é usado para designar falha segura por causa comum e o sobrescrito SN é usado para designar falha segura de modo normal. As falhas perigosas são também divididas em dois grupos: falha perigosa por causa comum (DC - *dangerous common*) e falha perigosa normal (DN - *dangerous normal*). As taxas de falha são divididas em

dois grupos multuamente exclusivos:

$$\lambda^S = \lambda^{SC} + \lambda^{SN} \tag{4.15}$$

$$\lambda^D = \lambda^{DC} + \lambda^{DN} \tag{4.16}$$

Dando sequência ao exemplo com um CLP de segurança usado para os cálculos na arquitetura 1oo1, preenchemos as tabelas 4.2 e 4.3 para um fator beta igual a 0,03 para dois CLPs ligados com redundância.

Tabela 4.2: Taxas de falha por causa comum de dois CLPs idênticos

λ^{SDC}	λ^{SUC}	λ^{DDC}	λ^{DUC}
$2,998 \cdot 10^{-7}$	$2,940 \cdot 10^{-9}$	$1,787 \cdot 10^{-7}$	$3,360 \cdot 10^{-9}$

Tabela 4.3: Taxas de falha por modo normal de dois CLPs idênticos

λ^{SDN}	λ^{SUN}	λ^{DDN}	λ^{DUN}
$9,696 \cdot 10^{-6}$	$9,506 \cdot 10^{-8}$	$5,777 \cdot 10^{-6}$	$1,086 \cdot 10^{-7}$

4.3.2 Modelo de Markov para 1oo2

O modelo de Markov para a arquitetura 1oo2, figura 4.4 possui três estados de operação com sucesso. No estado 0 os dois controladores operam normalmente. Nos estados 1 e 2 um dos dois controladores falhou com suas saídas energizadas, ainda assim o sistema opera com sucesso, visto que o outro controlador ainda desernegiza o atuador quando necessário. Pelo fato das falhas no estado 1 serem detectadas, um reparo com o sistema em funcionamento pode ser feito levando-o para o estado 0. Os estados 3, 4 e 5 são estados de falha de todo o sistema. No estado 3, o sistema falha com suas saídas desenergisadas. No estado 4, o sistema falha de forma detectável com suas saídas energizadas. Uma falha não detectada com as saídas do circuito energizadas acontece no estado 5. Observe ainda que apenas falhas de modo comum, ou seja, quando os dois módulos falham da mesma forma por uma mesma causa, é que é possível uma transição do sistema do estado 0, sem falhas, para os estados 4 ou 5 em que todo o sistema falha.

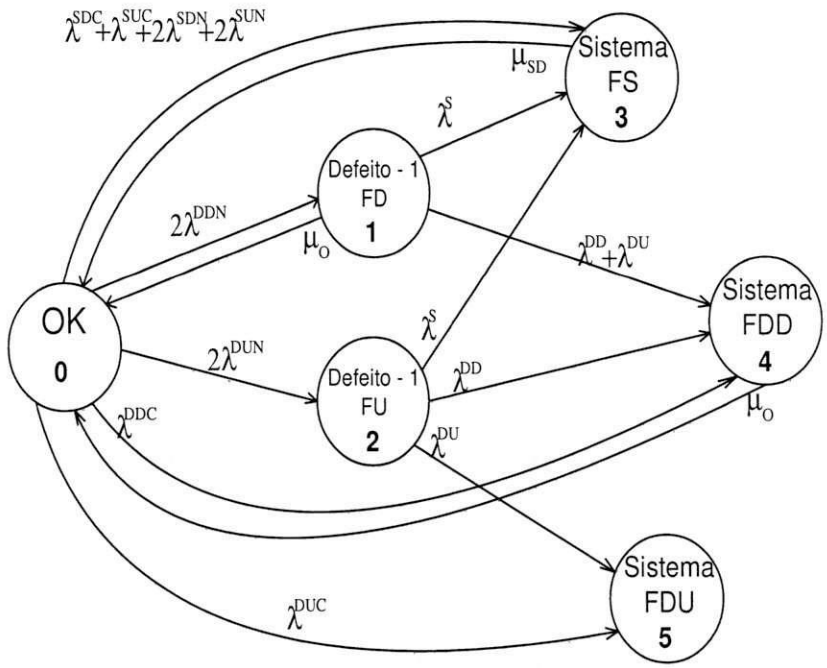

Figura 4.4: Modelo de Markov 1oo2

A matriz de transição, P, para o sistema 1oo2 é:

$$\begin{bmatrix} A_0 & 2\lambda^{DDN} & 2\lambda^{DUN} & \lambda^{SC}+2\lambda^{SN} & \lambda^{DDC} & +\lambda^{DUC} \\ \mu_O & A_1 & 0 & \lambda^S & \lambda^D & 0 \\ 0 & 0 & A_2 & \lambda^S & \lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 0 & 0 & A_3 & 0 & 0 \\ \mu_O & 0 & 0 & 0 & A_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_5 \end{bmatrix} \tag{4.17}$$

Onde

- $A_0 = 1 - (\lambda^{DC} + 2\lambda^{DN} + \lambda^{SC} + 2\lambda^{SN})$
- $A_1 = 1 - (\lambda^S + \lambda^D + \mu_O)$
- $A_2 = 1 - (\lambda^S + \lambda^D)$
- $A_3 = 1 - \mu_{SD}$
- $A_4 = 1 - \mu_O$
- $A_5 = 1$

4.3.3 Cálculo do MTTF

Para o cálculo do MTTF de uma arquitetura 1oo2 usaremos os dados de dois controladores de segurança idênticos com as características da tabela 4.1. Primeiramente substituimos os valores das taxas de falha e de reparo na matriz truncada Q, a qual possui apenas os índices 0, 1 e 2 da matriz de transição P.

$$Q = \begin{bmatrix} 0,9999682 & 0,0000116 & 0,0000002 \\ 0,125 & 0,8749838 & 0 \\ 0 & 0 & 0,9999838 \end{bmatrix} \tag{4.18}$$

Esta é subtraída da matriz identidade:

$$I - Q = \begin{bmatrix} 0,0000318 & -0,0000116 & -0,0000002 \\ -0,125 & 0,1250162 & 0 \\ 0 & 0 & 0,0000162 \end{bmatrix} \tag{4.19}$$

A matriz $[I - Q]$ é invertida para se obter a matriz N.

$$N = \begin{bmatrix} 49295,10 & 4,56 & 662,72 \\ 49288,72 & 12,55 & 662,63 \\ 0 & 0 & 61873,53 \end{bmatrix} \tag{4.20}$$

O MTTF é a soma dos elementos da linha de N para um dado estado inicial, assumindo que o sistema parta do estado 0,

$$MTTF = 49295,1 + 4,6 + 662,7 \tag{4.21}$$

$$MTTF = 49962 \texttt{ horas} \tag{4.22}$$

4.3.4 Cálculo do PFD e PFS

Da mesma forma como foi calculado para a arquitetura 1oo1, faremos os mesmos cálculos para se achar a PFD e a PFS de um sistema em votação 1oo2. Os valores de taxa de falha e de taxa de reparo são substituídos na matriz de transição P.

$$P = \begin{bmatrix} 0,9999682 & 0,0000116 & 0,0000002 & 0,0000199 & 0,0000002 & 0 \\ 0,125 & 0,8749838 & 0 & 0,0000101 & 0,0000061 & 0 \\ 0 & 0 & 0,9999838 & 0,0000101 & 0,0000060 & 0,0000001 \\ 0,0416667 & 0 & 0 & 0,9583333 & 0 & 0 \\ 0,125 & 0 & 0 & 0 & 0,875 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.23}$$

Assumimos que a unidade está operando perfeitamente quando iniciada, logo a matriz S no momento de *startup* é definida como:

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.24}$$

Após um ano (8760 horas), teríamos a seguinte matriz S:

$$S = \begin{bmatrix} 0,9976 & 9,219 \cdot 10^{-5} & 1,772 \cdot 10^{-3} & 4,765 \cdot 10^{-4} & 1,514 \cdot 10^{-6} & 3,028 \cdot 10^{-5} \end{bmatrix} \tag{4.25}$$

O valor de S(0) após 8760 horas é de 0,99763, isto é, o sistema possui probabilidade de 99,76% de se encontrar no estado 0, o qual, como foi definido no modelo da figura 4.4, indica que o sistema está operando sem falhas.

A PFS após um ano será dada pelo valor de S(3), já que no modelo o estado 3 representa falha do sistema de forma segura. A PFD será a soma de S(4) e S(5), no modelo o estado quatro representa falha do sistema em demanda detectada e o estado cinco falha em demanda não detectada. Portanto a PFS e PFD do sistema após um ano, será:

$$PFS = S(3) = 0,00047659 \tag{4.26}$$

$$PFD = S(4) + S(5) = 0,000031795 \tag{4.27}$$

4.4 2oo2: Sistema de Canal Duplo

Outro controlador com configuração igual foi desenvolvido para situações onde é indesejado haver falhas com saídas desenergizadas. As saídas dos dois controladores são ligadas em paralelo, figura 4.5. Se um controlador falha com a saída deseenergizada, o outro ainda é capaz de energizar a carga.

Uma desvantagem dessa configuração é a susceptibilidade a falhas em que a saída seja energizada, bastando apenas um controlador falhar com suas saídas energizadas para que todo sistema falhe.

4.4.1 Falha por Causa Comum

Devido ao fato de que a arquitetura 2oo2 mantém uma configuração com apenas dois CLPs idênticos em redudância, os resultados para as taxas de falha por causa comum e normal são os mesmos apresentados nas tabelas 4.2 e 4.3 para uma arquitetura 1oo2.

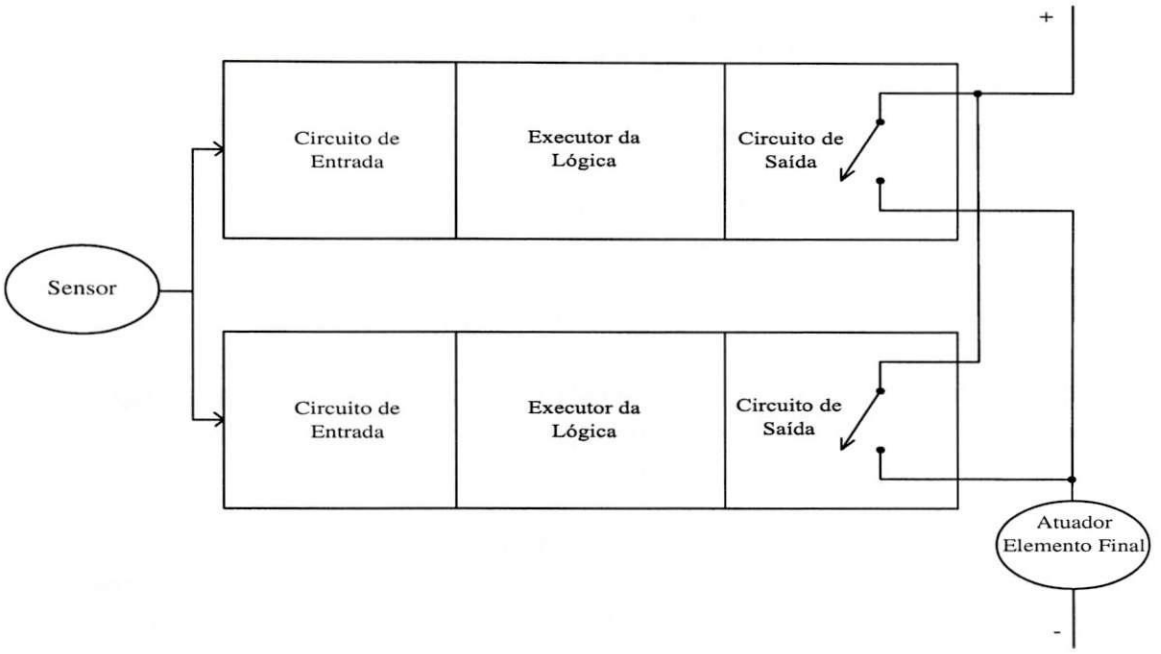

Figura 4.5: Arquitetura 2oo2

4.4.2 Modelo de Markov para 2oo2

Os estados de funcionamento de um sistema com arquitetura 2oo2 está representado em modelo de Markov na figura 4.5. O sistema opera com sucesso em três estados: 0, 1 e 2. O sistema falhou com suas saídas desenergizadas no estado 3. O sistema falhou com suas saídas energizadas nos estados 4 e 5. A matriz de transição, P, para o sistema 2oo2 é:

$$\begin{bmatrix} A_0 & 2\lambda^{SDN} & 2\lambda^{SUN} & \lambda^{SC} & \lambda^{DDC}+2\lambda^{DDN} & \lambda^{DUC}+2\lambda^{DUN} \\ \mu_O & A_1 & 0 & \lambda^{S} & \lambda^{D} & 0 \\ 0 & 0 & A_2 & \lambda^{S} & \lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 0 & 0 & A_3 & 0 & 0 \\ \mu_O & 0 & 0 & 0 & A_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & A_5 \end{bmatrix} \tag{4.28}$$

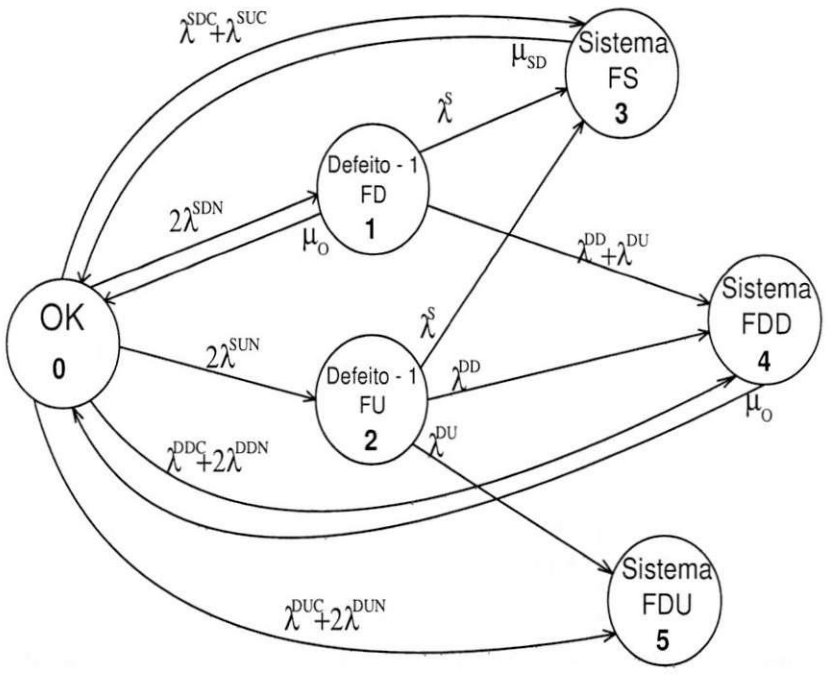

Figura 4.6: Modelo de Markov 1oo2

Onde

- $A_0 = 1 - (\lambda^{SC} + 2\lambda^{SN} + \lambda^{DC} + 2\lambda^{DN})$
- $A_1 = 1 - (\lambda^S + \lambda^D + \mu_O)$
- $A_2 = 1 - (\lambda^S + \lambda^D)$
- $A_3 = 1 - \mu_{SD}$
- $A_4 = 1 - \mu_O$
- $A_5 = 1$

4.4.3 Cálculo do MTTF

Para o cálculo do MTTF de uma arquitetura 2oo2 usaremos os dados de dois controladores de segurança idênticos com as características da tabela 4.1. Primeiramente substituimos os valores das taxas de falha e de reparo na matriz truncada Q, a qual

possui apenas os índices 0, 1 e 2 da matriz de transição P que correspondem aos estados em que o sistema funciona.

$$Q = \begin{bmatrix} 0,9999682 & 0,0000194 & 0,0000019 \\ 0,125 & 0,8749838 & 0 \\ 0 & 0 & 0,9999838 \end{bmatrix} \tag{4.29}$$

Esta é subtraída da matriz identidade:

$$I - Q = \begin{bmatrix} 0,0000318 & -0,0000194 & -0,0000019 \\ -0,125 & 0,1250162 & 0 \\ 0 & 0 & 0,0000162 \end{bmatrix} \tag{4.30}$$

A matriz $[I - Q]$ é invertida para se obter a matriz N.

$$N = \begin{bmatrix} 80325,11 & 12,46 & 944,90 \\ 80314,73 & 20,46 & 944,77 \\ 0 & 0 & 61873,53 \end{bmatrix} \tag{4.31}$$

O MTTF é a soma dos elementos da linha de N para um dado estado inicial, assumindo que o sistema parta do estado 0,

$$MTTF = 80325,11 + 12,46 + 944,90 \tag{4.32}$$

$$MTTF = 81282 \texttt{ horas} \tag{4.33}$$

4.4.4 Cálculo do PFD e PFS

Da mesma forma como foi obtido os resultados para a arquitetura 1oo1, faremos os mesmos cálculos para se achar a PFD e a PFS de um sistema em votação 2oo2. Os valores de taxa de falha e de taxa de reparo são substituídos na matriz de transição P.

$$P = \begin{bmatrix} 0,9999682 & 0,0000194 & 0,0000002 & 0,0000003 & 0,0000117 & 0,000000221 \\ 0,125 & 0,8749838 & 0 & 0,0000101 & 0,0000061 & 0 \\ 0 & 0 & 0,9999838 & 0,0000101 & 0,0000060 & 0,0000001 \\ 0,0416667 & 0 & 0 & 0,9583333 & 0 & 0 \\ 0,125 & 0 & 0 & 0 & 0,875 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.34}$$

Assumimos que a unidade está operando perfeitamente quando iniciada, logo a matriz S no momento de *startup* é definida como:

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.35}$$

Após um ano (8760 horas), teríamos a seguinte matriz S:

$$S = \begin{bmatrix} 0,996 & 1,545 \cdot 10^{-4} & 1,550 \cdot 10^{-3} & 7,653 \cdot 10^{-6} & 9,360 \cdot 10^{-5} & 1,930 \cdot 10^{-3} \end{bmatrix} \tag{4.36}$$

O valor de S(0) após 8760 horas é de 0,99626, isto é, o sistema possui probabilidade de $99,63\%$ de se encontrar no estado 0, o qual, como foi definido no modelo da figura 4.6, indica que o sistema está operando sem falhas.

A PFS após um ano será dada pelo valor de S(3), já que no modelo o estado 3 representa falha do sistema de forma segura. A PFD será a soma de S(4) e S(5), no modelo o estado quatro representa falha do sistema em demanda detectada e o estado cinco falha em demanda não detectada. Portanto a PFS e PFD do sistema após um ano, será:

$$PFS = S(3) = 0,00000765 \tag{4.37}$$

$$PFD = S(4) + S(5) = 0,00202 \tag{4.38}$$

Capítulo 5

Considerações Finais

Como foi exposto no trabalho, o projeto de um Sistema Instrumentado de Segurança parte da escolha do nível de integridade de segurança (SIL) das funções que esse SIS abriga. Para que os componentes de uma SIF não sejam superestimados é necessário que o valor do SIL resultante seja preciso. Como também foi visto, o valor do nível de integridade é diretamente relacionado ao valor da probabilidade de falha em demanda do sistema e, portanto, dependente do nível de complexidade do modelo escolhido para representar o sistema nos cálculos de probabilidades.

Além do modelo de Markov desenvolvido neste trabalho, outros métodos como a análise de árvore de falta e diagramas de blocos são também usados para se obter os índices de confiabilidade de um sistema instrumentado de segurança. A técnica mais complexa é o modelamento por diagramas de Markov, entretanto, esse método é o mais flexível por fornecer ao projetista maior liberdade em acrescer imperfeições ao modelo, consequentemente, é a técnica que possui resultados mais precisos.

Esse trabalho seviu como base para a construção de modelos mais detalhados e para outros tipos de arquiteturas no projeto de Confiabilidade de Sistemas Instrumentados de Segurança - CONFSISSEG. Nesse projeto foi criado o software BR-SIL que usa os diagramas de Markov para cálculo de confiabilidade e disponibilidade de funções instrumentadas de segurança. Os resultados apresentados no Capítulo 4, assim como outros diversos testes realizados ao longo do projeto, foram comparados aos resultados obtidos a partir do programa *exSILentia - Integrated Safety Lifecycle Tool* versão 1.3.4 da empresa de softwares *Exida*, em todos os casos não houve diferença maior que $0,08\%$ entre os valores.

Referências Bibliográficas

[Wmg98] Goble, William M. "Control Systems Safety Evaluation and Reliability". ISA - The Instrumentation, Systems, and Automation Society, 1998.

[Buk01a] Bukowski, Julia V. e Goble, W M. "Defining Mean Time-to-Failure in a Particular Failure-State for Multi-Failure-State Systems". IEEE Transactions on Reliability, Vol. 50, N° 2, Junho de 2001.

[Buk01b] Bukowski, Julia V. "Modeling and Analyzing the Effects of Periodic Ispection on the Performance of Safety-Critical Systems". IEEE Transactions on Reliability, Vol. 50, N° 3, Setembro de 2001.

[Mrz02] Marszal, Edward M. "Safety Integrity Level Selection - Systematic Methods Including Layer of Protection Analysis". ISA - The Instrumentation, Systems, and Automation Society, 2002.

[Wmg05] Goble, W. M. & Cheddie, H. "Safety Instrumented Systems Verification: Pratical Probabilistic Calculations". ISA - The Instrumentation, Systems, and Automation Society, 2005.

[Pap01] Papoulis, Athanasios & Pillai, S. Unnikrishna. Probability, Random Variables and Stochastic Processes. McGraw-Hill Science/Engineering/Math, 2001.