Software para Avaliação de Confiabilidade de Sistemas Instrumentados de Segurança

Henrique Cunha Barroso

Dissertação de Mestrado submetida à Coordenação do Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande - Campus de Campina Grande como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Instrumentação Eletrônica e Controle

Péricles Rezende Barros, PhD.
Orientador

Campina Grande, Paraíba, Brasil

B277s Barroso, Henrique Cunha
Software para avaliacao de confiabilidade de sistemas instrumentados de seguranca / Henrique Cunha Barroso.- Campina Grande, 2009.
90 f. : il.

Dissertacao (Mestrado em Engenharia Eletrica) - Universidade Federal de Campina Grande, Centro de Engenharia Eletrica e Informatica.

1. Sistemas Instrumentados de Seguranca 2. Avaliacao de Confiabilidade 3. Software 4. Dissertacao I. Barros, Pericles Rezende, Dr. II. Universidade Federal de Campina Grande - Campina Grande (PB) III. Título

CDU 621.316.36(043)

Software para Avaliação de Confiabilidade de Sistemas Instrumentados de Segurança

Henrique Cunha Barroso

Dissertação de Mestrado apresentada em Março de 2009

Péricles Rezende Barros, PhD.
Orientador

José Sérgio da Rocha Neto, Dsc., UFCG
Componente da Banca

Benemar Alencar de Souza, Dsc., UFCG
Componente da Banca

Campina Grande, Paraíba, Brasil, Março de 2009

Dedicatória

Aos meus pais pela dedicação e pelo apoio incondicional em todos os momentos de minha formação.

Agradecimentos

Agradeço aos meus pais Arnaldo e Vandete e aos meus irmãos Alexandre e Rodrigo por sempre acreditarem e investirem em mim e por compreenderem a minha ausência durante a realização deste trabalho. Agradeço em especial a Lívia Bandeira pelo carinho, dedicação e pelo apoio nos momentos mais difíceis.

Agradeço ao meu orientador Péricles Rezende Barros pelos ensinamentos, amizade e apoio durante o desenvolvimento deste trabalho. Por toda confiança depositada e constante incentivo ao meu desenvolvimento acadêmico e profissional meu sincero agradecimento.

Agradeço aos engenheiros Marcelo Lima e Mário Campos do CENPES / Petrobras, pelas valiosas contribuições para o desenvolvimento deste trabalho.

Agradeço aos amigos George Acioli, Aretho Barbosa, João Batista, Marcus Berger, Airam Sausen, Alfranque Amaral e tantos outros com os quais tive o prazer de conviver todo este tempo.

Agradeço aos professores José Sérgio e Benemar Alencar pela participação na banca examinadora deste trabalho e aos grandes mestres que contribuíram com minha formação acadêmica.

Agradeço aos funcionários do Departamento de Engenharia Elétrica, em especial a Adail, Rosilda, Ângela e Suenia, por toda paciência e apoio ao longo de todo esse tempo.

Finalmente, agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ) pelo apoio financeiro que viabilizou a realização deste trabalho.

Resumo

Especificar e projetar adequadamente um Sistema Instrumentado de Segurança para uma unidade industrial é uma tarefa complexa e extensa. A análise dos efeitos ocasionados por eventuais falhas no processo, bem como a utilização de técnicas quantitativas para avaliação de segurança e confiabilidade permite a obtenção de um maior refinamento das medidas de proteção a serem adotadas para reduzir os riscos. O software apresentado foi desenvolvido para a avaliação de confiabilidade de Sistemas Instrumentados de Segurança. Ele é baseado no método de análise de Markov e utiliza um conjunto de modelos desenvolvidos para a representação de diversas configurações redundantes e lógicas de segurança distintas. O uso do software resulta na redução do tempo despendido na avaliação de projetos de SIS.

Abstract

To properly specify and design a Safety Instrumented System for a plant is a complex and extensive task. The analysis of the effects caused by possible process failures, as well as the use of quantitative techniques for assessing reliability and security allows one to obtain a higher refinement of protective measures to be adopted to reduce risks. The software tool presented was developed to evaluate the reliability and availability of Safety Instrumented Systems. The software is based on the Markov analysis method. It also uses a set of models developed for the representation of various redundant configurations and different security logics. The use of the software results in the reduction of the time spent in the evaluation process of SIS projects.

Sumário

Lista de Símbolos e Abreviaturas

β	Fator beta	[%]
Λ	Matriz de transição de estados do modelo de Markov	
λ	Taxa de falha	[1/h]
λ^{DD}	Taxa de falha perigosa detectada	[1/h]
λ^{DU}	Taxa de falha perigosa não detectada	[1/h]
λ^{D}	Taxa de falha perigosa	[1/h]
λ^{SD}	Taxa de falha segura detectada	[1/h]
λ^{SU}	Taxa de falha segura não detectada	[1/h]
λ^{S}	Taxa de falha espúria	[1/h]
Λ_Q	Matriz de transição truncada	
μ_O	Taxa de reparo *on line*	[1/h]
μ_{SD}	Taxa de reparo a partir do estado de falha segura	[1/h]
$A(t)$	Função disponibilidade no instante t	
C	Fator de cobertura de diagnóstico	[%]
I	Matriz identidade	
$MooN$	*M-out-of-N*	
$R(t)$	Função confiabilidade no instante t	
TC	Tempo de Campanha	[anos]
TR	Tempo de Reparo	[h]
FIT	Failure In Time (Falha por bilhão de horas)	
IEC	*International Eletrotechnical Commission*	
ISA	*Instrument Society of America*	

LT	*Level transmitter* (Transmissor de nível)
MTBF	*Mean Time Between Failures* (Tempo médio entre falhas)
MTTF	*Mean Time To First Failure* (Tempo médio para falhar)
MTTFs	*Mean Time To Failure Spurious* (Tempo médio para ocorrência de falha espúria)
MTTR	*Mean Time To Repair* (Tempo médio para reparo)
N.A.	Normalmente Aberto
N.F.	Normalmente Fechado
PES	*Programmable Electronic System* (Sistema eletrônico programável)
PFD	*Probability of Failure on Demand* (Probabilidade de falha na demanda)
PFDavg	*Average Probability of Failure on Demand* (Probabilidade média de falha na demanda)
PLC	Programmable Logic Controller (Controlador lógico programável)
PT	*Pressure transmitter* (Transmissor de pressão)
RRF	*Risk Reduction Factor* (Fator de redução de risco)
SFF	*Safe Failure Fraction* (Fração de falha segura)
SIF	*Safety Instrumented Function* (Função Instrumentada de Segurança)
SIL	*Safety Integrity Level* (Nível de integridade de segurança)
SIS	*Safety Instrumented System* (Sistema Instrumentado de Segurança)

Lista de Tabelas

Lista de Figuras

Capítulo 1

Introdução

1.1 Contexto

O crescimento da indústria observado no século XX, norteado principalmente pela busca do aumento da produtividade e qualidade dos produtos, apresentou como conseqüências novos desafios operacionais resultantes dos limites de segurança e riscos assumidos. O impacto de alguns fatores tais como o aumento da competitividade no mercado global e o crescente índice de regulamentações dos processos produtivos pode ser observado no nível cada vez maior de automação e sofisticação das plantas e na redução da dependência do elemento humano nas operações das mesmas. Mudanças estão ocorrendo no modo de operação das plantas industriais, não somente como forma de minimizar custos e reduzir a variabilidade no processo de fabricação. Segurança e confiabilidade tornaram-se parâmetros essenciais no projeto de sistemas de controle automático. Preocupações acerca de fatores como segurança de pessoal, proteção das instalações e do meio ambiente tem influenciado de forma cada vez mais significativa a especificação dos novos processos industriais. Os benefícios econômicos de um sistema seguro e confiável incluem menores perdas de produção, maior qualidade dos produtos, redução dos gastos com manutenção e custos associados.

Especificar e projetar adequadamente uma planta com os componentes corretos para otimizar a segurança é uma tarefa complexa e extensa. Todas as metodologias e ferramentas empregadas para estas funções tem por objetivo o aprimoramento do projeto geral da planta, com o conseqüente aumento da eficiência e redução dos custos associados à manutenção e operação dos sistemas de segurança de processo.

A regulamentação da segurança na indústria de processo iniciou-se aproximadamente no final dos anos 80. Nos EUA e na Europa, associações de fabricantes e

organismos internacionais como a ISA (*Instrument Society of America*) e a IEC (*International Eletrotechnical Commission*) vem elaborando e aprimorando normas para guiar o projeto, construção e manutenção de Sistemas Instrumentados de Segurança.

Através da análise de confiabilidade de sistemas instrumentados de segurança busca-se avaliar o risco de não atendimento a uma demanda do processo, desde a etapa do projeto até a etapa de comissionamento e operação, analisando-se os equipamentos instalados e os procedimentos operacionais adotados. Essa avaliação do risco é realizada por meio da análise de índices probabilísticos do sistema que, combinados com um julgamento próprio e sob critérios de decisão pré-estabelecidos, possibilita buscar soluções adequadas para contornar possíveis falhas que possam vir a comprometer a operação do sistema, de forma a minimizar o risco associado ao processo. Estes índices são calculados por meio de técnicas de análise de confiabilidade baseadas em princípios e conceitos matemáticos da teoria de probabilidade.

1.2 Revisão Bibliográfica

Vários métodos podem ser utilizados para se analisar a confiabilidade de Sistemas Instrumentados de Segurança. Alguns métodos bastante simples empregam técnicas de análise combinatória para análise de confiabilidade. No entanto, apesar da facilidade de utilização, estes métodos são bastante limitados em função de direcionarem a análise de confiabilidade para um único modo de falha do sistema. Em seus trabalhos, Goble (GOBLE, 1998), Summers (SUMMERS, 2000) e mais recentemente Guo e Yang (GUO; YANG, 2007) discutem alguns desses métodos.

Outras técnicas apresentam equações simplificadas através de aproximações baseadas em modelos genéricos simples como apresentado por Lima e Saito em (LIMA; SAITO, 2003). Neste, são apresentados alguns resultados de cálculos de alguns índices probabilísticos de confiabilidade baseados em equações simplificadas propostas no anexo B da norma IEC 61508 e na parte 2 da ISA TR84.00.02-2002. Apesar da facilidade de implementação, o uso de equações simplificadas geralmente acarreta resultados muito conservadores.

O método de Markov é um método no qual a confiabilidade do sistema é analisada através da representação de seus diferentes estados de operação e falha e das probabilidades de transição entre esses estados. Um dos primeiros trabalhos a abordar este método, apresentado por Bukowski e Goble (BUKOWSKI; GOBLE, 1995), discute

a utilização do método de Markov para analisar a confiabilidade de sistemas eletrônicos programáveis. Neste trabalho é apresentado um procedimento sistemático para a construção de modelos de Markov para sistemas reparáveis tolerantes a falhas. Em (GOBLE; BUKOWSKI, 2001a), Goble e Bukowski apresentam métodos baseados no método de Markov para o cálculo de determinados índices probabilísticos empregados na análise de confiabilidade de sistemas com múltiplos estados de falha. São discutidos aspectos operacionais e de segurança e propostas modificações nos modelos de Markov para o cálculo de índices derivados, em função de um estado de interesse em particular.

Comparada a outras técnicas existentes, o método de Markov possibilita uma modelagem completa, levando em consideração a maior parte dos aspectos que afetam a confiabilidade de SIS. Além disso, este método possibilita a análise da dinâmica das transições entre os diversos estados do sistema. Em (GOBLE; BUKOWSKI, 2001b) e em (BUKOWSKI; LELE, 1997) são discutidos os fatores que ocasionam as falhas devido a causas comuns e analisados seus efeitos em diversas arquiteturas de sistemas redundantes. Em outro trabalho (BUKOWSKI, 2001), Bukowski utiliza modelos de Markov para analisar os efeitos de inspeções periódicas no desempenho de sistemas de segurança críticos.

Outros trabalhos semelhantes que podem ser enumerados são (M.; GOBLE; BROMBACHER, 1996) e (GOBLE; BUKOWSKI; BROMBACHER, 1998).

Apesar de todo o potencial demonstrado pelo método de markov, o tamanho e a complexidade dos modelos desenvolvidos cresce em função do número de fatores incluídos e das diversas suposições assumidas, o que exige grande capacidade computacional, além de tornar a probabilidade de erros durante a construção dos modelos. Essas limitações levaram alguns estudiosos da área a questionar o uso do método de Markov para a avaliação de confiabilidade de sistemas.

Apesar disso, alguns estudiosos da área questionam o uso do método de Markov para a avaliação de confiabilidade de sistemas. Em seus trabalhos, Simpson e Kelly (SIMPSON; KELLY, 2003) e Gulland (GULLAND, 2003) propõem a proibição da utilização do método de Markov, alegando para tal que as suposições assumidas durante a modelagem dos sistemas acarretam resultados incoerentes.

Em (BUKOWSKI, 2005), Bukowski rebate essas afirmações e demonstra através de um estudo comparativo entre essas duas técnicas que o método de Markov fornece soluções exatas não apenas para modelos simples como também para modelos de maior complexidade representativos de cenários mais realistas.

Em (KNEGTERING; BROMBACHER, 1999), Knegtering e Brombacher propõem uma forma de reduzir os esforços computacionais requeridos para solucionar modelos de Markov de sistemas complexos. Neste, é descrita uma técnica que combina os métodos de Markov com diagramas de blocos de confiabilidade.

Recentemente, em (GUO; YANG, 2008) foi proposta uma nova técnica para criação automática de modelos de Markov para avaliação de confiabilidade de Sistemas Instrumentados de Segurança.

Nos últimos anos vem se discutindo o mérito das diversas técnicas existentes para a modelagem e análise de confiabilidade e disponibilidade de Sistemas Instrumentados de Segurança. A utilização de técnicas de análise diferentes, que fazem uso de metodologias de análise diferentes, pode acarretar na obtenção de resultados significativamente diferentes. Uma comparação entre algumas dessas técnicas é apresentada por Rouvroye e Brombacher em (ROUVROYE; BROMBACHER, 1999). Trabalho similar foi apresentado por Rouvroye e van den Bliek (ROUVROYE; BLIEK, 2002).

1.3 Organização do Texto

Este trabalho está organizado da seguinte forma:

No Capítulo 1 estão dispostos o contexto no qual este trabalho se insere, o objetivo geral almejado e a revisão bibliográfica realizada.

No Capítulo 2 são apresentados conceitos básicos de engenharia de confiabilidade relacionados ao estudo de confiabilidade e disponibilidade. São discutidos aspectos e conceitos referentes aos Sistemas Instrumentados de Segurança, e apresentadas algumas das arquiteturas mais comuns utilizadas pela indústria de processos.

No Capítulo 3 é abordado o método de análise de Markov a partir de critérios estabelecidos para a sua utilização no desenvolvimento do algoritmo de cálculo de confiabilidade para o software proposto.

No Capítulo 4 são apresentadas as principais características e funcionalidades do software desenvolvido, e discutidos alguns estudos de casos onde são calculados os principais índices probabilísticos com base nos quais é feita a avaliação de confiabilidade dos sistemas propostos.

No Capítulo 5 são apresentadas as conclusões do trabalho e sugestões de trabalhos futuros.

Capítulo 2

Confiabilidade e Segurança de Sistemas Instrumentados de Segurança

2.1 Introdução

Muitos enfoques diferentes podem ser adotados para se assegurar os níveis de confiabilidade e segurança desejáveis para um Sistema Instrumentado de Segurança, cada qual com suas próprias implicações de custo e restrições de implementação.

A avaliação de confiabilidade e segurança de Sistemas Instrumentados de Segurança é realizada por meio da análise de determinados índices probabilísticos, tanto em projetos de unidades novas, garantindo o correto dimensionamento dos equipamentos para se obter um nível de proteção adequado, quanto em instalações já existentes, visando identificar medidas que proporcionem melhoria de eficiência operacional.

2.2 Conceitos Importantes

Alguns conceitos básicos de engenharia de confiabilidade são necessários para a compreensão da análise proposta neste trabalho.

Confiabilidade

Confiabilidade $R(t)$ é a probabilidade de um sistema desempenhar de forma

satisfatória uma função, sob condições específicas, durante um período de tempo pré-determinado (GOBLE, 1998).

Matematicamente o parâmetro confiabilidade pode ser definido por

$$R(t) = P(t < T) \tag{2.1}$$

ou seja, a probabilidade de uma operação ser bem sucedida em um intervalo de tempo de zero a T, onde t corresponde ao instante de tempo de ocorrência da falha.

O conceito de confiabilidade é bastante abrangente, e por muitas vezes vago, uma vez que deve incluir todos os aspectos associados à capacidade do sistema operar satisfatoriamente. A análise da confiabilidade de componentes e subsistemas em função da probabilidade de ocorrência de falhas é uma etapa importante na análise de confiabilidade de um SIS.

Disponibilidade

A disponibilidade de um sistema, representada por $A(t)$, é a probabilidade de que, em um dado instante de tempo t, este sistema esteja funcionando satisfatoriamente em um determinado ambiente. Em outras palavras, disponibilidade é a probabilidade de um sistema estar disponível quando necessário. De forma simplificada, diz-se que a disponibilidade de um sistema é a relação entre o tempo de vida útil deste sistema e seu tempo total de vida. Isto pode ser representado pela fórmula abaixo:

$$A(t) = \frac{Vida \;\; útil}{Tempo \;\; total \;\; de \;\; vida} \tag{2.2}$$

A indisponibilidade, $\bar{A}(t)$ é dada por:

$$\bar{A}(t) = 1 - A(t) \tag{2.3}$$

Risco

O conceito de risco é definido como sendo o produto da freqüência com que um determinado evento ocorre pelas conseqüências resultantes da ocorrência desse evento (GOBLE, 1998).

Índices de risco estão associados a situações nas quais o sistema é incapaz de garantir o desempenho adequado devido a fatores incertos. Ainda que exista uma

grande dificuldade de se classificar o risco tido por aceitável, é possível identificar na literatura especializada diferentes tentativas de se estabelecer padrões para classificação do risco por parte de entidades governamentais e associações industriais.

Taxa de Falha

A taxa de falha instantânea, ou simplesmente taxa de falha, é um parâmetro bastante comum no campo da engenharia de confiabilidade. A taxa de falha indica o número de falhas por unidade de tempo de uma determinada quantidade de componentes expostos à falha.

$$\lambda(t) = \frac{Falhas \ \ por \ \ unidade \ \ de \ \ tempo}{Quantidade \ \ exposta} \tag{2.4}$$

É prática comum a representação da taxa de falha através da utilização de uma unidade denominada FIT - *Falhas por bilhão (10^9) de horas*.

Tempo Médio de Reparo - MTTR

O Tempo Médio de Reparo (MTTR - *Mean Time To Repair*) corresponde ao valor esperado da variável aleatória tempo de reparo, podendo ser definido alternativamente como sendo o tempo médio necessário para que um componente ou sistema seja reparado dada a ocorrência de uma falha. Essa definição inclui o tempo gasto com a detecção da ocorrência da falha, além do tempo necessário para a correção da falha identificada (GOBLE, 1998).

Tempo Médio entre Falhas - MTBF

O Tempo Médio entre Falhas (MTBF - *Mean Time Between Failures*) corresponde ao tempo médio entra a ocorrência de duas falhas.

2.3 Sistemas Instrumentados de Segurança

Na indústria são utilizadas diversas camadas de proteção para salvaguardar o processo. O número de camadas de proteção necessário depende da complexidade do processo e severidade potencial das conseqüências do cenário. Uma camada de proteção é uma parte distinta de uma planta projetada com a finalidade de se evitar a ocorrência ou reduzir as conseqüências de um evento específico. Camadas de proteção podem ser desde equipamentos e procedimentos operacionais a ações planejadas em resposta a condições adversas do processo (AICHE, 1993). Na Figura 2.1 são apresentadas alguns exemplos de camadas de proteção presentes em diversos processos industriais. As camadas são apresentadas por ordem de ativação esperada dada a ocorrência de uma condição de perigo.

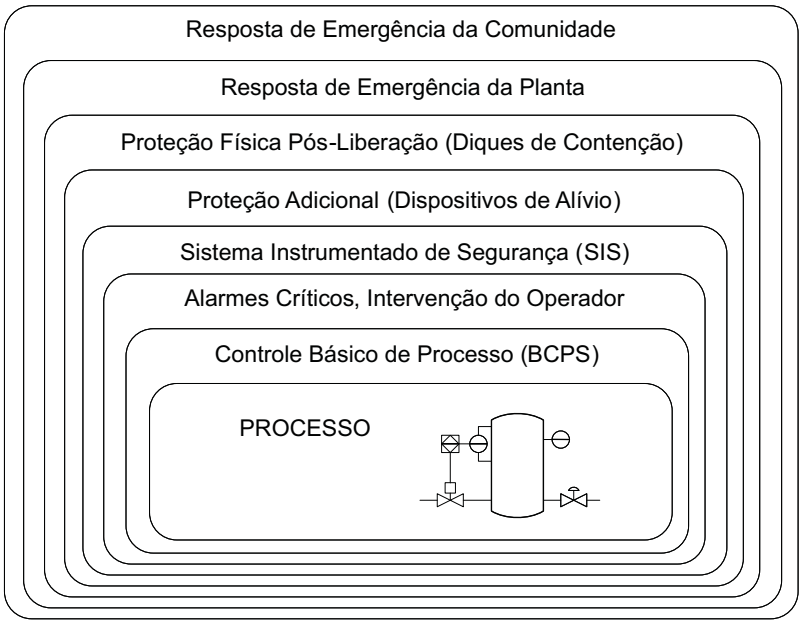


Figura 2.1: Exemplos de Camadas de Proteção.

A depender do cenário analisado, o sucesso na atuação de qualquer uma das camadas de proteção deve ser obrigatoriamente suficiente para prevenir as conseqüências avaliadas.

Observa-se que além dos diversos equipamentos e ações possíveis, são utilizados dois tipos de sistemas de controle automático: Sistema de Controle Regulatório ou Sistema Básico de Controle de Processo (BPCS - *Basic Process Control System*) e Sistemas Instrumentados de Segurança (SIS - *Safety Instrumented System*). A diferença entre os dois está na função que suas lógicas exercem. O primeiro está dedicado a manter as variáveis de processo controladas com o objetivo de otimizar o

desempenho do processo; o segundo volta-se para a segurança do processo, de forma a garantir que estas mesmas variáveis estejam dentro de limites considerados seguros para a operação da unidade.

Sistemas de segurança de processo são freqüentemente dispositivos de instrumentação e controle instalados para desempenhar função de proteção em adição ao sistema de controle regulatório. Esses sistemas de segurança monitoram o status de variáveis essenciais do processo, identificam situações de operação anormal da planta, alertam o operador e, em alguns casos, interrompem o processo evitando a ocorrência de eventos potencialmente perigosos. Estes permanecem inativos até que uma condição anormal e potencialmente perigosa ocorra.

Embora um sistema de segurança seja semelhante a um sistema regulatório de muitas formas, as diferenças residem em requisitos únicos de projeto, manutenção e integridade física. Para funcionar satisfatoriamente, um sistema de segurança requer um nível de desempenho e diagnóstico superior ao normalmente solicitado para um equipamento genérico de controle de processo.

Nos últimos anos, o conceito de Sistema Instrumentado de Segurança tem sido bastante discutido e divulgado entre profissionais dos mais distintos setores da indústria de processos, bem como no meio acadêmico. Um SIS é um sistema de controle cujo propósito é monitorar um processo industrial, detectar condições potencialmente perigosas e executar ações pré-programadas para prevenir a ocorrência de um evento perigoso ou ainda mitigar as conseqüências da ocorrência de tal evento. Em outras palavras, um SIS é projetado com a finalidade de levar automaticamente um processo para um estado seguro quando condições específicas de operação forem violadas, ou ainda executar ações que reduzam as conseqüências de um possível acidente industrial.

2.3.1 Composição de um SIS

Um SIS pode ser definido como sendo um conjunto de Funções Instrumentadas de Segurança (SIF - *Safety Instrumented Function*), implantadas em uma unidade de processo. Por sua vez, uma SIF é uma ação ou conjunto de ações adotadas por um SIS para levar o processo ou equipamento a um estado seguro, com respeito a um perigo específico (GOBLE; CHEDDIE, 2005). Na Figura 2.2 é apresentado um diagrama que exemplifica a relação entre SIF e SIS.

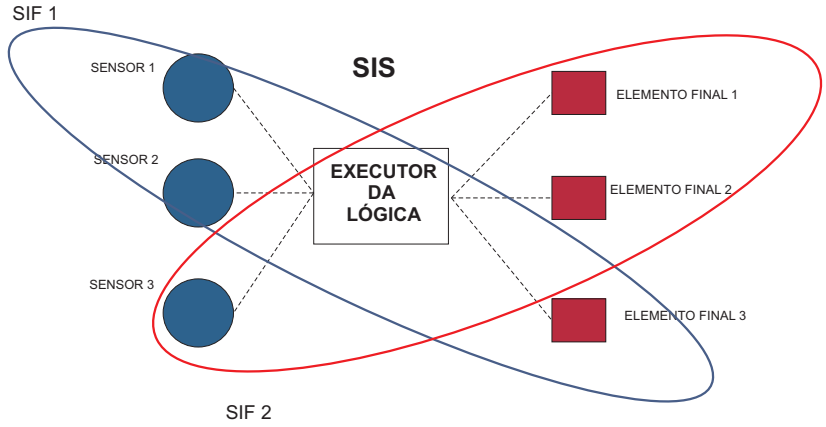


Figura 2.2: SIS e SIF.

Em alguns casos a função de segurança é projetada para reduzir o risco diminuindo a probabilidade de ocorrência de um perigo em potencial. Em outros casos a função de segurança irá reduzir o risco diminuindo a gravidade da conseqüência do evento.

Uma SIF é tipicamente composta por sensor(es), executor da lógica de segurança e elemento(s) atuador(es). Na Figura 2.3 é apresentado um exemplo típico de planta industrial contendo um SIS e um sistema básico de controle.

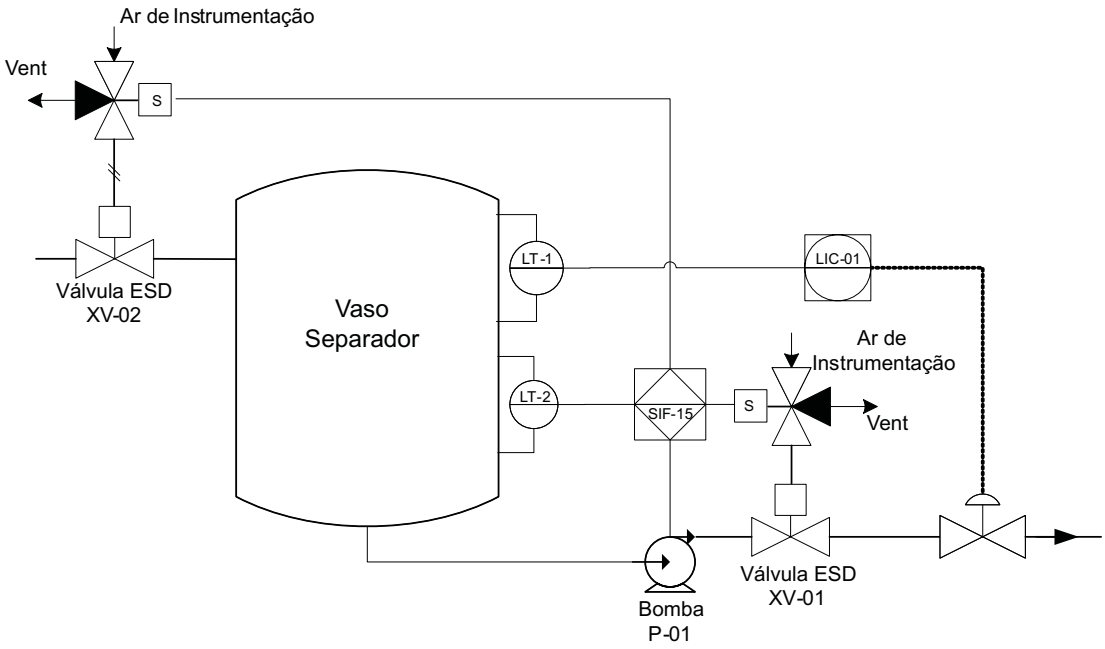


Figura 2.3: Exemplo de planta industrial contendo SIS e BPCS.

No exemplo acima é possível identificar a presença de dois tipos distintos de sistemas: BPCS e SIS. O sistema básico de controle é composto por um transmissor de nível, um controlador industrial e uma válvula de controle. Por sua vez, o SIS é constituído por um transmissor de nível, um CLP de segurança e dois elementos atuadores, cada sendo composto por uma válvula solenóide de 3 vias e uma válvula de segurança.

O SIS é implementado para garantir a segurança de um vaso separador contra um valor muito baixo do nível de líquido. É assumido que o líquido do separador é bombeado de forma contínua para outro vaso adjacente para posterior processamento. O nível de líquido no separador é controlado por uma malha de controle do BPCS. Além disso, o gás contido no separador é normalmente comprimido e distribuído.

Dentre os perigos potenciais associados a um nível muito baixo de líquido no vaso separador pode ser destacado o fluxo de gás sob alta pressão através do sistema de bombeamento. Algumas das possíveis conseqüências para esse cenário são:

1. Danos ao sistema de bombeamento;
2. Liberação de gases tóxicos e/ou inflamáveis para a atmosfera;
3. Perda de vidas.

A SIF analisada opera da seguinte forma: ao se detectar um nível abaixo de um valor limite pré-estabelecido, as válvulas XV-01 e XV-02 são fechadas. Assume-se que uma função de segurança específica assegura a proteção do sistema de bombeamento. Essa função auxiliar não é analisada neste exemplo.

2.3.2 Níveis de Integridade de Segurança

O conceito de Nível de Integridade de Segurança (SIL - *Safety Instrumented Level*), introduzido pelas normas ISA 84.01 (ISA, 1996) e IEC 61508 (IEC, 2000), estabelece uma ordem de grandeza para a redução do risco, ou seja, o nível de robustez necessário a ser implementado de forma a reduzir o risco do processo a níveis aceitáveis.

Os níveis SIL são categorias pré-definidas de redução de risco baseadas na Probabilidade de Falha na Demanda (PFD - *Probability of Failure on Demand*). Na Tabela 2.1 é apresentada a correlação entre o SIL, a PFD e a disponibilidade da SIF, conforme definido pela norma IEC 61508. Numa escala crescente de 1 a 4, quanto maior for o SIL, mais crítico será o processo.

Tabela 2.1: Níveis de Integridade de Segurança segundo a norma IEC 61508

SIL	PFD	Disponibilidade da SIF
4	$< 10^{-4}$	$> 99,99\%$
3	10^{-4} a 10^{-3}	$99,90$ a $99,99\%$
2	10^{-3} a 10^{-2}	99 a $99,90\%$
1	10^{-2} a 10^{-1}	90 a 99%

2.3.3 Arquiteturas *MooN*

Muitos enfoques diferentes podem ser adotados para se assegurar os níveis de confiabilidade e disponibilidade desejáveis para um Sistema Instrumentado de Segurança, cada qual com suas próprias implicações de custo e restrições de implementação.

Segundo a norma IEC 61508 (IEC, 2000), o projeto de um SIS deve atender a certos níveis mínimos de confiabilidade e segurança. Como forma de minimizar o impacto de falhas de componentes do SIS e, conseqüentemente, melhorar sua confiabilidade e disponibilidade, é comum a implementação de um certo nível de redundância de hardware ou software que assegure ao sistema de segurança a capacidade de tolerar eventuais falhas. No entanto, a implantação de redundância de hardware implica o uso de equipamentos e componentes adicionais aos que o sistema de segurança normalmente necessitaria para desempenhar sua função.

A escolha da arquitetura mais apropriada para cada sistema exige uma análise minuciosa dos critérios de segurança estabelecidos, além de informações a respeito

dos procedimentos de operação e manutenção adotados para o processo. Isso possibilita a determinação de uma solução que atenda da melhor forma possível às metas e requisitos operacionais e de segurança do processo.

Freqüentemente na literatura especializada é empregada a notação MooN (*M-out-of-N*) para denotar os diferentes esquemas de arquiteturas existentes. Tais esquemas são denominados esquemas de votação, ou simplesmente votação. Na Figura 2.4 é apresentado um diagrama que representa a lógica associada aos esquemas de votação mais comuns.

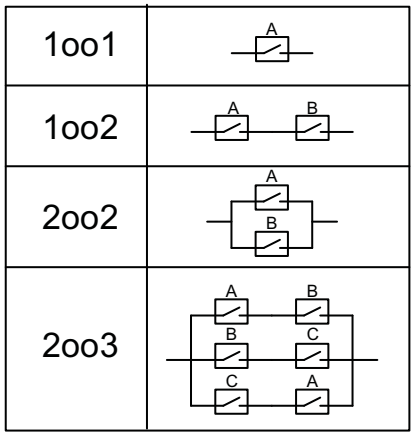


Figura 2.4: Esquemas de Votação MooN.

Nessa figura os elementos A, B e C representam unidades de controle responsáveis por energizar um processo.

A votação 1oo1 representa a arquitetura mais simples. A utilização de uma única unidade A não proporciona proteção contra eventuais falhas do sistema.

Na votação 1oo2 duas unidades A e B são dispostas numa configuração série. Essa configuração possibilita que o processo seja desenergizado na ocorrência de uma eventual falha em qualquer das duas unidades de controle. Essa votação é constantemente empregada quando se requer um alto nível de confiabilidade do sistema.

Na votação 2oo2 duas unidades A e B são dispostas numa configuração paralela. Neste caso, para que o processo seja desenergizado é necessário que as duas unidades falhem. A votação 2oo2 proporciona um alto índice de disponibilidade ao sistema.

A votação 2oo3 representa uma arquitetura mais sofisticada, sendo portanto utilizada quando se busca níveis elevados de confiabilidade e disponibilidade. De acordo com a lógica empregada por essa votação, é necessário que duas unidades falhem, de um total de três.

O conceito de arquitetura redundante pode ser extendido para os elementos da SIF, conforme apresentado a seguir.

Arquiteturas de Sensores

Na Figura 2.5 são apresentados exemplos de arquiteturas para sensores.

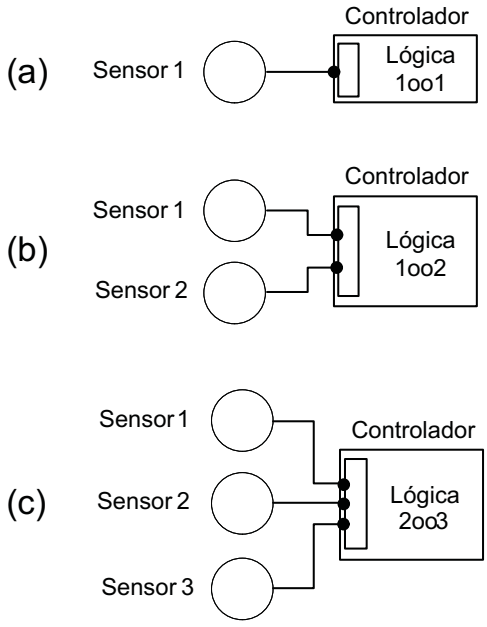


Figura 2.5: Exemplos de arquiteturas para sensores.

Na Figura 2.5a é apresentada uma arquitetura simples onde o equipamento executor da lógica de segurança realiza a medição de apenas um equipamento sensor. Esse tipo de votação é denominada 1oo1.

Na Figura 2.5b são utilizados dois sensores para a medição da mesma variável do processo. Uma votação 1oo2 entre sensores é obtida através da implementação de uma lógica de segurança que inicie o desligamento do processo caso uma condição perigosa seja detectada por qualquer um dos dois sensores.

A configuração apresentada na Figura 2.5c é utilizada quando deseja-se comparar a medição realizada por três sensores. A votação 2oo3 proporciona maior proteção contra desligamentos desnecessários decorrentes de falsas indicações de falha por parte dos sensores.

Arquiteturas de Elementos Finais

Na Figura 2.6 são apresentados exemplos de arquiteturas para elementos finais.

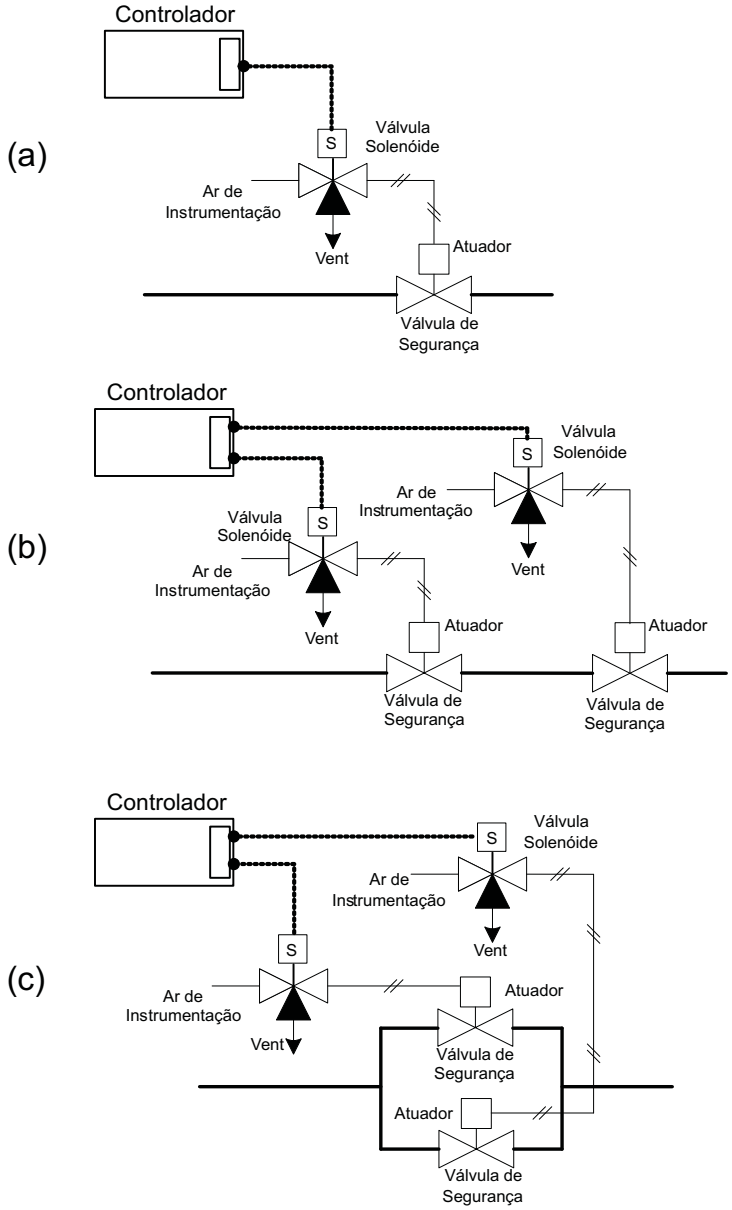


Figura 2.6: Exemplos de arquiteturas para elementos finais.

Na Figura 2.6a é apresentada uma arquitetura bastante simples, normalmente utilizada para válvulas de fechamento seguro. Essa arquitetura, denominada 1oo1, consiste de uma válvula solenóide de 3 vias, um elemento atuador e uma válvula de segurança do tipo *fail close*. Quando uma condição perigosa é detectada, o controlador desenergiza a válvula solenóide, interrompendo o fornecimento de ar para o atuador. Isso faz com que a válvula de segurança seja fechada.

Na Figura 2.6b é apresentada uma arquitetura 1oo2, composta por dois conjuntos de elementos finais disposto em série na linha do processo. Quando uma condição perigosa é detectada pelo controlador, os dois conjuntos são acionados. Qualquer dos dois conjuntos pode interromper o processo.

Uma arquitetura 2oo2 é apresentada na Figura 2.6c. A depender do tipo de processo, esse tipo de arquitetura proporciona maior disponibilidade caso ocorra uma falha em um dos conjuntos de válvulas.

A seguir são apresentadas algumas configurações típicas de Funções Instrumentadas de Segurança utilizadas para os níveis SIL 1, 2 e 3.

Arquitetura típica SIL 1

Na Figura 2.7 é apresentada uma arquitetura típica que satisfaz os requisitos de segurança SIL 1. Ela consiste de um único sensor, um controlador lógico programável de segurança e um conjunto elemento final, formado por uma válvula solenóide de 3 vias e por uma válvula de segurança pneumática.

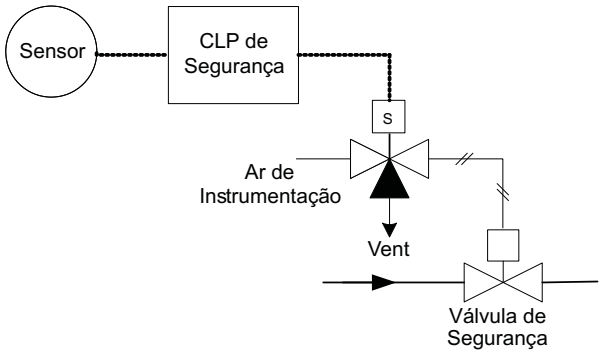


Figura 2.7: Função Instrumentada de Segurança SIL 1

Um exemplo de processo para o qual esse tipo de arquitetura SIL 1 é adequada é apresentado na Figura 2.8. Quando a pressão no vaso assume um valor muito elevado, superior a um valor limite de segurança operacional pré-estabelecido, o fluxo de entrada deve ser interrompido através do fechamento da válvula de segurança. Para a configuração exibida, o sistema normalmente falha de forma segura, isto é, durante a operação normal a válvula solenóide é mantida continuamente energizada, fornecendo suprimento constante de ar para que a válvula de segurança permaneça aberta. Qualquer falha que possivelmente venha a interromper o fornecimento de ar e/ou energia para o sistema resultará no fechamento da válvula de segurança e, conseqüentemente, na interrupção do fluxo para o vaso.

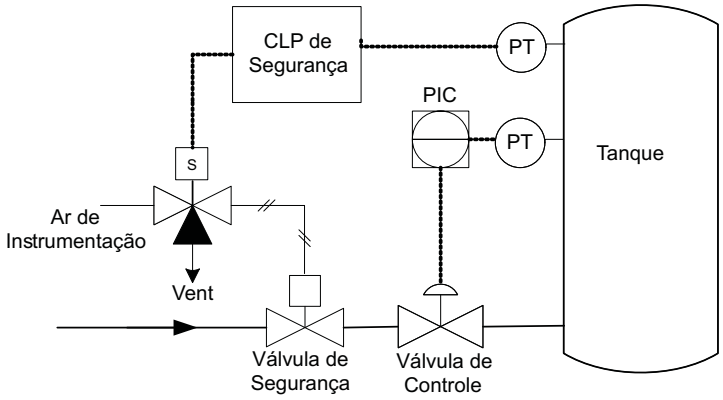


Figura 2.8: Exemplo de Processo

Arquitetura típica SIL 2

Na Figura 2.9 é apresentada uma arquitetura que satisfaz os requisitos de segurança SIL 2. Ela consiste de dois elementos sensores, um CLP de segurança e dois elementos atuadores. Os sensores são transmissores de pressão convencionais e estão dispostos numa configuração 1oo2, ou seja, qualquer um dos transmissores poderá interromper o processo dada uma situação de perigo operacional ou falha do equipamento de medição. Os elementos atuadores são compostos por válvulas do tipo *shutdown* operadas pneumaticamente através de válvulas solenóides individuais e estão dispostos numa configuração em série (votação 1oo2).

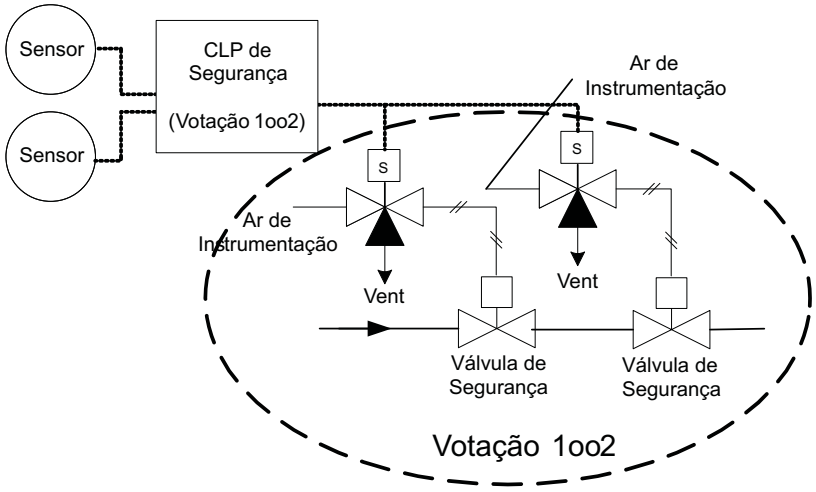


Figura 2.9: Função Instrumentada de Segurança típica SIL 2

Arquitetura típica SIL 3

Na Figura 2.10 é apresentada uma arquitetura que satisfaz os requisitos de segurança SIL 3. Ela consiste de três elementos sensores, um CLP de segurança e dois elementos atuadores. Os sensores são transmissores de pressão convencionais e estão dispostos numa configuração 2oo3, ou seja, quaisquer dois do conjunto de transmissores poderão interromper o processo dada uma situação de perigo operacional ou falha do equipamento de medição. Os elementos atuadores são compostos por válvulas do tipo *shutdown* operadas pneumaticamente através de válvulas solenóides individuais e estão dispostos numa configuração em série (votação 1oo2).

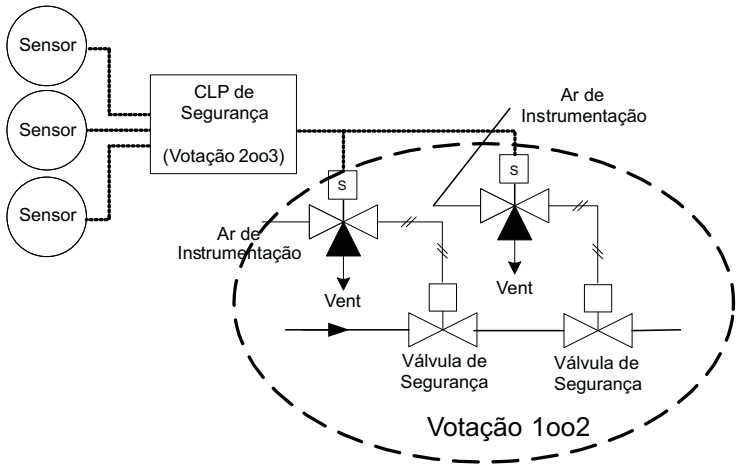


Figura 2.10: Função Instrumentada de Segurança típica SIL 3

2.4 Definição dos Índices de Confiabilidade e Segurança

A análise de confiabilidade e segurança de Sistemas Instrumentados de Segurança é composta por alguns índices probabilísticos. A seguir é apresentada a formulação matemática associada ao cálculo destes índices.

2.4.1 Probabilidade Média de Falha na Demanda - PFDavg

Para sistemas de proteção em geral, o atributo de confiabilidade de maior interesse é a Probabilidade de Falha na Demanda (PFD), ou seja, a probabilidade de que o sistema encontre-se impossibilitado de atuar no sentido de impedir ou mitigar

uma condição potencialmente perigosa (demanda) dada a ocorrência de uma falha. No caso de malhas de segurança, isto corresponde à não atuação no momento da demanda de um dos seus componentes.

O termo (PFD_{avg}) ou $PFD_{average}$ é utilizado para descrever a probabilidade média de falha em demanda, ou mais precisamente, a média aritmética da PFD sobre um intervalo de tempo definido. Em se tratando de sistemas de segurança, assume-se que esse intervalo de tempo corresponde ao período de inspeção e testes do sistema.

$$PFD_{avg} = \frac{1}{TI} \int_0^{TI} (PFD)dt \tag{2.5}$$

Dado que a PFD varia em função do intervalo de operação do processo, não assumindo valores constantes durante esse período, o valor médio da PFD mostra-se um parâmetro de análise muito útil, sendo adotado pelas diversas normas internacionais como um parâmetro de referência para se avaliar a confiabilidade de SIS.

Um outro parâmetro adicional é comumente utilizado para se avaliar a integridade de um SIS. O Fator de Redução de Risco (RRF - *Risk Reduction Factor*) é definido por:

$$RRF = \frac{Risco \;\; inerente}{Risco \;\; aceitável} \tag{2.6}$$

O RRF é obtido a partir da PFD_{avg}:

$$RRF = \frac{1}{PFD_{avg}} \tag{2.7}$$

Na Tabela 2.2 é apresentada a correlação entre a PFD_{avg} e o RRF.

Tabela 2.2: Níveis de Integridade de Segurança - SIL

SIL	PFD_{avg}	Disponibilidade da SIF	RRF
4	$< 10^{-4}$	$> 99,99\%$	> 10.000
3	10^{-4} a 10^{-3}	$99,90$ a $99,99\%$	10.000 a 1.000
2	10^{-3} a 10^{-2}	99 a $99,90\%$	1.000 a 100
1	10^{-2} a 10^{-1}	90 a 99%	100 a 10

2.4.2 Tempo Médio para Falhar - MTTF

O Tempo Médio para Falhar (MTTF - *Mean Time To Failure*) é definido como o tempo médio para a ocorrência de uma falha. Apesar de ser um dos parâmetros de maior relevância no estudo de confiabilidade e disponibilidade de sistemas, muitas vezes o MTTF é mal interpretado como sendo o tempo mínimo de vida útil garantida do sistema. Na Figura 2.11 é apresentada uma representação gráfica do MTTR, do MTBF e do MTTF.

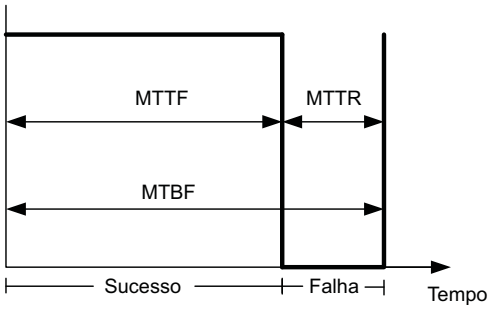


Figura 2.11: MTTR e MTBF.

2.4.3 Tempo Médio para Falhar de Forma Segura - MTTFs

Índice derivado do MTTF, o tempo médio para ocorrência de uma falha segura (MTTFs - *Mean Time To Failure Spurious*) corresponde ao tempo médio de operação a partir do estado de partida (estado de total operacionalidade) até a interrupção do processo sob a condição de interesse, ou seja, a ocorrência de uma falha classificada como segura (falha espúria). Neste intervalo de tempo supõe-se que existe a possibilidade de que falhas ocorridas em estados que não o de interesse possam ser corrigidas.

O MTTFs é um índice bastante representativo para a análise das conseqüências de desligamentos desnecessários do processo decorrentes de falhas espúrias.

2.5 Conclusão

Os requisitos de confiabilidade de sistemas instrumentados de segurança podem freqüentemente ser expressos em termos um tanto simplistas e sem uma compreensão completa das implicações decorrentes. Essa situação pode levar ao estabelecimento de especificações de projeto inadequadas, acarretando no dimensionamento incorreto do sistema proposto.

A determinação da melhor configuração para os sistemas, no que concerne ao nível de redundância necessário para a instalação de equipamentos críticos e a escolha da melhor política de operação e manutenção para a unidade devem ser pautadas em um processo de análise de confiabilidade do sistema, baseado na determinação de índices probabilísticos tais como a PFD_{avg}, o $MTTF$ e o $MTTF_S$. Essa análise pode ser realizada tanto em projetos de unidades novas, garantindo o correto dimensionamento dos equipamentos para se obter um nível de proteção adequado, quanto em instalações já existentes, visando identificar medidas que proporcionem melhoria de eficiência operacional, bem como a identificação da necessidade de modificação do sistema para correção de possíveis falhas.

Capítulo 3

Método de Análise de Markov

3.1 Introdução

O método de análise de Markov é apropriado sempre que o comportamento estocástico dos componentes de um sistema depende do estado dos demais componentes ou do estado do sistema. Por essa razão o método de análise de Markov é largamente utilizado para a avaliação probabilística de confiabilidade e segurança de Sistemas Instrumentados de Segurança.

Nas seções seguintes serão abordados os princípios básicos, procedimento de modelagem adotado e cálculo dos diversos índices probabilísticos a partir dos modelos desenvolvidos.

3.2 Cadeias de Markov

Processos estocásticos são de grande interesse para a análise da operação de um sistema em um determinado período de tempo. Um processo estocástico pode ser definido como uma coleção de variáveis aleatórias $X(t) : t \in T$, onde $X(t)$ representa uma característica mensurável de interesse no tempo t. Em outros termos, a variável aleatória $X(t)$ representa o estado do sistema em função do parâmetro (geralmente tempo) t. Embora T seja freqüentemente definido como sendo o conjunto dos reais não-negativos ($T \subseteq R_+ = [0, \infty)$), outros conjuntos são perfeitamente aplicáveis. Dentre os diversos tipos de processos estocásticos existentes, um processo em especial, denominado processo Markoviano, é abordado neste trabalho.

Um processo Markoviano, ou simplesmente processo de Markov, é um processo estocástico cujo passado não exerce influência sobre o futuro se o presente é especi-

ficado. Isto significa dizer que se $t_{n-1} < t_n$, então:

$$P\{X(t_n) = x_n \mid x(t), t = t_{n-1}\} = P\{X(t_n) = X_n \mid X(t_{n-1})\}. \tag{3.1}$$

A expressão (3.1) pode ser traduzida por: a probabilidade condicional de qualquer evento futuro dado qualquer evento passado e o estado presente $X(t_k) = x_k$ é independente do evento passado e depende somente do estado presente.

Em outros termos, um processo estocástico é dito ser um processo Markoviano se o estado futuro depende apenas do estado presente e não dos estados passados. Uma vez que o passado é desprezado, este tipo de processo estocástico é classificado como sendo um processo sem memória.

As probabilidades condicionais são denominadas probabilidades de transição e representam, portanto, a probabilidade do estado $X(k+1)$ ser x_{k+1} no instante $k+1$ dado que o estado $X(k)$ é x_k no instante k. A análise das probabilidades de transição entre os estados determina o comportamento estatístico da cadeia de Markov.

A descrição apresentada acima também pode ser aplicada para processos discretos no tempo. Nesse caso tem-se

$$P\{X(k+1) = x_{k+1} \mid X(k) = x_k, \cdots, X(0) = x_0\} = P\{X(k+1) = x_{k+1} \mid X(k) = x_k\}, \tag{3.2}$$

onde k é um valor inteiro não negativo.

3.3 Modelos de Markov

Modelos de Markov constituem uma ferramenta de modelagem bastante poderosa e flexível muito utilizada na representação do comportamento de sistemas reparáveis tolerantes a falhas e, portanto, assumem papel de destaque no processo de análise probabilística de confiabilidade de Sistemas Instrumentados de Segurança. Para o desenvolvimento de modelos de Markov utiliza-se apenas dois tipos de símbolos, apresentados na Figura 3.1. Os círculos representam estados que correspondem ao resultado das combinações entre sucesso e falha da operação dos componentes do sistema. Os arcos representam as probabilidades de transição entre os estados, levando-se em consideração todas as possíveis falhas e/ou reparos dos componentes do sistema.

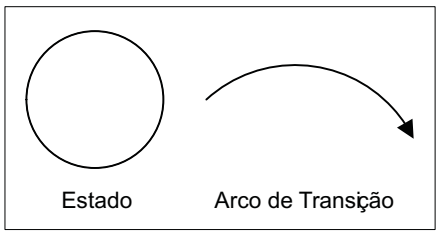


Figura 3.1: Simbologia do Modelo de Markov

Um modelo de Markov possibilita a representação de toda a operação de um sistema tolerante a falhas em um único diagrama, incluindo o esquema de redundância entre os diferentes níveis de componentes do sistema. Na Figura 3.2 é apresentado um exemplo de modelo de Markov para um sistema redundante genérico.

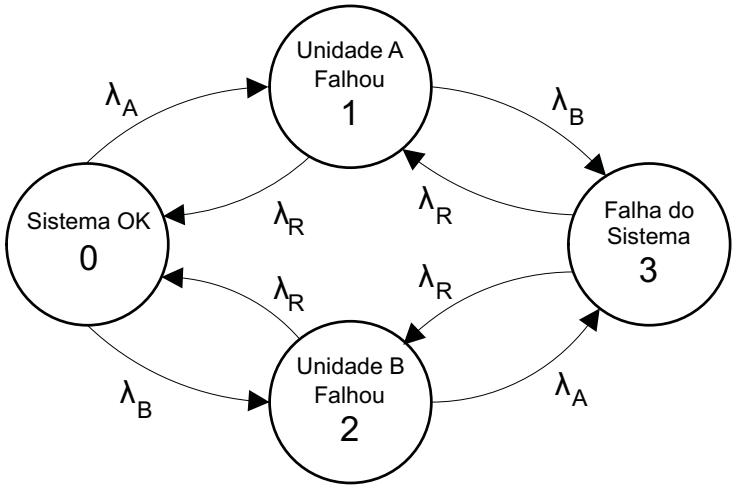


Figura 3.2: Modelo de Markov de um sistema redundante genérico

Um modelo de Markov pode ser classificado em termos de sua ergodicidade. Em um modelo do tipo ergótico ou regular cada estado pode ser alcançado a partir de qualquer outro estado, seja de forma direta ou indireta. Por sua vez, um modelo é denominado não ergótico ou absorvente quando um ou mais estados, assim que alcançados, interrompem o fluxo do processo. Nas Figuras 3.3 e 3.4 são apresentados exemplos de modelos regular e absorvente, respectivamente.

3.3.1 Considerações sobre a modelagem

O nível de detalhamento de um modelo de Markov para análise de confiabilidade depende dos objetivos da modelagem proposta. Durante o processo de modelagem deve-se dar ênfase a fatores relevantes e eliminar fatores de menor importância, de tal

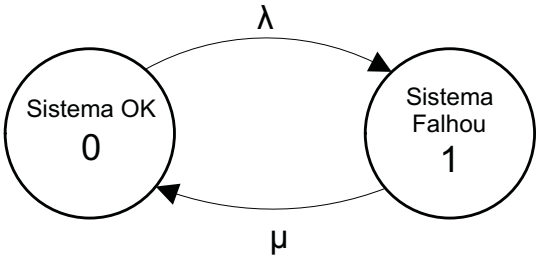


Figura 3.3: Modelo de Markov ergótico (regular)

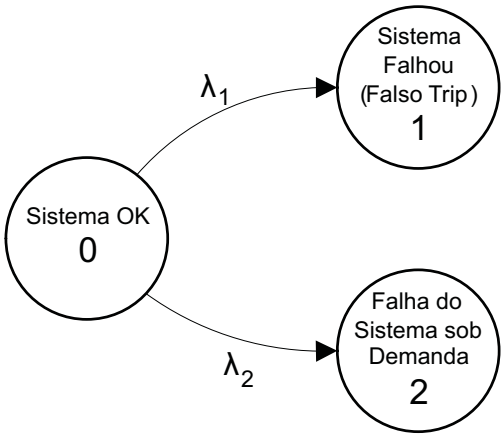


Figura 3.4: Modelo de Markov não ergótico (absorvente)

forma que o modelo obtido seja consistente e apresente dimensões que não dificultem por demais sua solução.

Simplificações e aproximações são recursos muito utilizados para se reduzir a complexidade do modelo, facilitando sua compreensão e análise. Entretanto, deve-se ter cautela ao se fazer uso desses recursos pois os resultados obtidos podem ser excessivamente otimísticos e possivelmente incorretos.

O primeiro passo do procedimento de modelagem corresponde à identificação e classificação das possíveis falhas em função de alguns fatores e dos efeitos que estes causam no SIS. A seguir são discutidos os fatores considerados na modelagem apresentada neste trabalho.

Modos de falha

Equipamentos de instrumentação podem falhar de formas diferentes. Esses tipos de falhas podem ser classificadas primariamente de acordo com as seguintes categorias:

- Falha Segura

  Uma falha segura de um instrumento pode ser definida como sendo uma falha que causa um falso Trip ou Trip espúrio de uma Função Instrumentada de Segurança.

  Uma definição mais formal, a nível de sistema, seria que uma falha segura leva o sistema a um estado seguro ou eleva a probabilidade de o sistema ser levado a um estado seguro.

- Falha Perigosa

  Uma falha perigosa impede que a Função Instrumentada de Segurança exerça sua função de proteção.

Alguns autores incluem nessa classificação uma outra categoria de falhas, denominada Falhas em Efeito. Segundo esses autores, falhas deste tipo não causam falsos Trips ou sequer exercem algum tipo de efeito sobre as funções instrumentadas de segurança (GOBLE; CHEDDIE, 2005).

Neste trabalho falhas sem efeito não são consideradas na modelagem proposta. A classificação aqui adotada é apresentada na Figura 3.5. Segundo essa classificação a taxa de falha total do sistema pode ser decomposta da seguinte forma:

$$\lambda_{Total} = \lambda^S + \lambda^D, \tag{3.3}$$

onde λ^S representa uma taxa de falha segura e λ^D representa uma taxa de falha perigosa.

Taxas de Reparo

Em sistemas reais assume-se que se um componente falha ele é reparado ou substituído por um novo componente. Se este novo componente falha, é substituído por outro e assim por diante. O componente reparado é tido como no mesmo estado que um componente novo. Entretanto, uma falha pode ocasionar desde uma simples

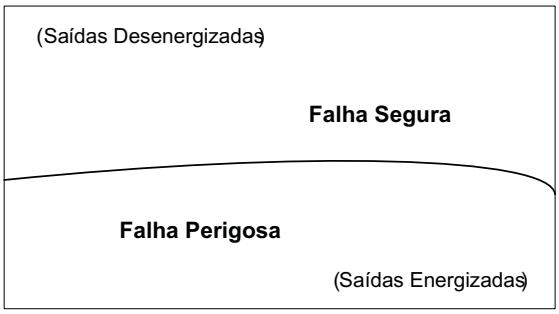


Figura 3.5: Classificação dos tipos de falha.

degradação da proteção do sistema até a interrupção da operação do mesmo. Faz-se necessário, portanto, uma distinção entre o tempo necessário para que seja realizado um simples reparo de uma falha que não interrompe a operação do sistema, e o tempo despendido com todos os procedimentos necessários para que o sistema seja posto novamente em operação após a detecção e correção de uma falha.

Como forma de realizar essa distinção foram utilizados neste trabalho dois tipos distintos de taxa de reparo. A primeira representa uma taxa de reparo *on line*, ou seja, uma taxa de reparo para falhas detectadas, mas que não interrompem o funcionamento do sistema (μ_O). A segunda representa a taxa referente ao tempo necessário para que o sistema seja reparado e reiniciado após a ocorrência de uma falha segura (μ_{SD}).

$$\mu_O = \frac{1}{MTTR} \tag{3.4}$$

e

$$\mu_{SD} = \frac{1}{t_{Start-up}}, \tag{3.5}$$

onde $t_{Start-up}$ representa o tempo necessário para que a falha seja reparada e o sistema seja reiniciado após a ocorrência de um desligamento ocasionado por um Trip espúrio.

O tempo de reparo afeta significativamente o desempenho de um sistema tolerante a falhas. Muitos dos métodos simplificados utilizados para a análise probabilística de confiabilidade de sistemas disponíveis na literatura especializada fornecem soluções aproximadas que são aceitáveis apenas para valores baixos de taxa de falha e intervalos de reparo curtos.

Falha de modo comum - O Modelo Beta

De um modo geral, os modelos de avaliação de confiabilidade consideram que as falhas dos componentes são estatisticamente independentes umas das outras. No entanto, para componentes redundantes, existe sempre a possibilidade de que algum grau de dependência entre as falhas dos componentes seja introduzido, devido a problemas comuns de projeto, fabricação, montagem, operação, localização, manutenção, entre outros. São as chamadas falhas de modo comum.

Dependendo do grau de dependência entre as falhas dos componentes redundantes, isto pode acarretar uma significativa redução do ganho de confiabilidade auferido pela colocação da redundância, resultando em um sistema bem menos confiável do que o esperado.

Uma falha de modo comum é definida como sendo a falha de mais de um componente, módulo, unidade ou sistema devido a uma mesma causa ou fator (GOBLE, 1998).

Falhas de projeto são as principais fontes de falhas de modo comum. Procedimentos operacionais e de manutenção incorretos também podem ocasionar esse tipo de falha. A crescente complexidade dos sistemas instrumentados de segurança tem elevado a probabilidade de ocorrência de falhas de modo comum.

Neste trabalho foi adotado o Modelo Beta, modelo bastante difundido para representar o efeito de falhas de modo comum na análise de sistemas redundantes. O Modelo Beta utiliza um fator multiplicador, denominado fator beta, para representar o percentual da taxa de falha total do componente que pode ser considerado como falha de modo comum. O Fator Beta pode assumir valores compreendidos numa faixa entre 0 e 100 %. Dessa forma é possível classificar a taxa de falha de cada componente do sistema em dois tipos distintos: normal (λ^N) e devido a causa comum (λ^C).

$$\lambda^C = \beta \times \lambda \tag{3.6}$$

e

$$\lambda^N = (1 - \beta) \times \lambda \tag{3.7}$$

De onde temos que

$$\lambda^S = \lambda^{SC} + \lambda^{SN} \tag{3.8}$$

e

$$\lambda^D = \lambda^{DC} + \lambda^{DN} \tag{3.9}$$

Na Figura 3.6 é apresentada uma representação gráfica da classificação das falhas segundo o Modelo Beta.

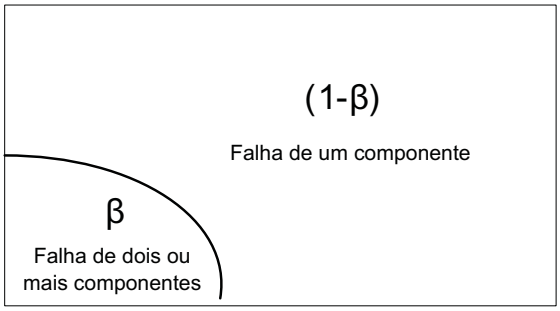


Figura 3.6: Classificação de falhas segundo o Modelo Beta.

Ao longo dos anos e com o avanço dos estudos sobre a confiabilidade e segurança dos processos industriais, profissionais da área têm proposto uma série de valores considerados adequados para o fator beta, tanto para falhas de hardware quando para falhas de software. Na literatura especializada encontram-se publicadas diversas estimativas de faixas de valores para o fator beta, obtidas em função dos mais diferentes tipos de análise de projeto e implementação de processos e sistemas. Uma avaliação qualitativa da implementação física e lógica do sistema pode e deve, sempre que possível, ser realizada para se estimar o valor adequado para o fator beta.

A seguir são apresentados de forma simplificada alguns dos critérios adotados como referências para essa avaliação, segundo o questionário proposto pela IEC em (IEC, 2000).

- Separação física e redundância;

  Unidades redundantes fisicamente separadas são menos suscetíveis a falhas devido a causa comum. A maioria dos efeitos de fatores ambientais fontes desse tipo de falha variam de forma não linear em função da distância de separação física.

- Diversidade;

  Diversidade é um conceito segundo o qual unidades com projeto diferentes são utilizadas em conjunto numa configuração redundante. A idéia básica é na ver-

dade bastante simples: componentes com diferentes processos de manufatura não serão afetados pelo mesmo tipo de falha ao mesmo tempo.

- Procedimentos operacionais e de manutenção.

Os efeitos de falhas de modo comum podem ser facilmente modelados por meio do método de análise de Markov. Na Figura 3.7 é apresentado um modelo de Markov que exemplifica a aplicação do modelo Beta para representar a ocorrência de falhas de modo comum em um sistema redundante. No estado 0 o sistema opera normalmente. No estado 1 ocorreu a falha de um dos equipamentos. O estado 2 representa o cenário de falha do sistema. As probabilidades de reparo foram omitidas no modelo para facilitar a visualização. A ocorrência de uma falha devido a causa comum é representada pelo arco que leva o sistema do estado 0 diretamente para o estado 2, indicando a falha simultânea dos dois componentes e, conseqüentemente, a falha geral do sistema.

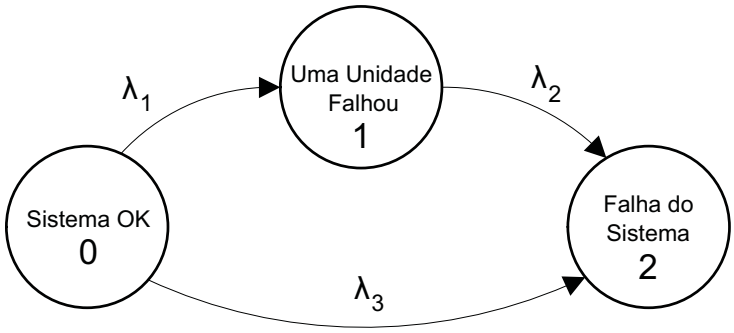


Figura 3.7: Modelo de Markov de um sistema redundante com ocorrência de falha por causa comum.

Auto Diagnóstico de falhas

A segurança e a confiabilidade de processos podem ser substancialmente melhoradas quando o sistema é capaz de detectar de maneira automática possíveis falhas de componentes. A detecção *on line* de falhas traz benefícios para o sistema. A identificação de falhas no momento em que estas ocorrem torna possível a redução do tempo de reparo do sistema, uma vez que não será mais necessário esperar por uma parada de manutenção programada para que as falhas sejam descobertas.

A maior parte dos equipamentos eletrônicos que compõem os Sistemas Instrumentados de Segurança modernos realiza periodicamente testes internos a fim de

identificar possíveis falhas, ou seja, a cada sinal enviado é realizado um auto diagnóstico e verificado se o sistema está ou não falho.

Para ilustrar o conceito de diagnóstico automático de falhas será considerado um sistema simples composto por duas chaves genéricas idênticas dispostas numa configuração em série (votação 1oo2). As chaves possuem pequenos módulos microprocessados responsáveis pela detecção de curto-circuito nos contatos (falha perigosa). A detecção desse tipo de falha ocorre da seguinte forma: em intervalos de tempo regulares os módulos de diagnóstico abrem os contatos durante microsegundos e verificam a corrente que flui através destes. Se o valor da corrente não diminui é sinal de que ocorreu um curto-circuito nos contatos e a falha é identificada.

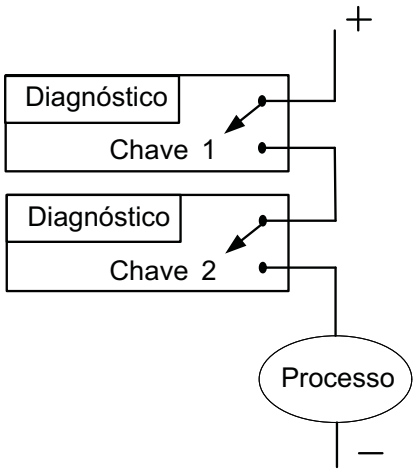


Figura 3.8: Sistema genérico 1oo2 com diagnóstico de falhas.

De modo geral, a capacidade de diagnóstico automático de um sistema possibilita a detecção da maioria das falhas, embora não a totalidade das falhas possíveis. Para modelar a eficiência desse auto diagnóstico emprega-se um coeficiente denominado Fator de Cobertura de Diagnóstico (C), o qual representa a fração da taxa de falhas detectáveis pelo auto diagnóstico. O Fator de Cobertura de Diagnóstico pode assumir valores compreendidos numa faixa entre 0 e 100 %.

$$\lambda^{SD} = C \times \lambda^{S} \tag{3.10}$$

$$\lambda^{SU} = (1 - C) \times \lambda^{S} \tag{3.11}$$

e

$$\lambda^{DD} = C \times \lambda^{D} \tag{3.12}$$

$$\lambda^{DU} = (1 - C) \times \lambda^{D} \tag{3.13}$$

Combinando os efeitos de falhas devido a causa comum com a capacidade de diagnóstico do sistema obtém-se novas categorias para as taxas de falha:

$$\lambda^{SDN} = (1 - \beta) \times \lambda^{SD} \tag{3.14}$$

$$\lambda^{SDC} = \beta \times \lambda^{SD} \tag{3.15}$$

$$\lambda^{SUN} = (1 - \beta) \times \lambda^{SU} \tag{3.16}$$

$$\lambda^{SUC} = \beta \times \lambda^{SU} \tag{3.17}$$

$$\lambda^{DDN} = (1 - \beta) \times \lambda^{DD} \tag{3.18}$$

$$\lambda^{DDC} = \beta \times \lambda^{DD} \tag{3.19}$$

$$\lambda^{DUN} = (1 - \beta) \times \lambda^{DU} \tag{3.20}$$

$$\lambda^{DUC} = \beta \times \lambda^{DU} \tag{3.21}$$

3.3.2 Procedimento para construção do modelo

Para a construção do modelo de Markov foi utilizado um procedimento sistemático baseado no método proposto por Bukowski e Goble em (BUKOWSKI; GOBLE, 1995). O procedimento é apresentado a seguir:

1. Identificar e classificar as possíveis falhas do sistema e de seus componentes;
2. Determinar as taxas de falha e de reparo dos componentes do sistema;
3. Iniciar a construção do modelo de Markov a partir do estado no qual todos os componentes estão operando normalmente;

4. Para cada tipo de falha identificado, adicionar um estado no modelo e identificar por meio de arcos de transição as taxas de falha e de reparo correspondentes.

Na Figura 3.9 é apresentado o modelo de um sistema simples, consistindo de duas chaves genéricas idênticas dispostas numa configuração em série (votação 1oo2, normalmente energizadas). Cada chave apresenta dois tipos distintos de falha: circuito aberto e curto-circuito. A falha do tipo circuito aberto é classificada como segura, pois desenergiza o processo. A falha do tipo curto-circuito é classificada como perigosa, pois impede que o processo seja interrompido caso uma condição potencialmente perigosa ocorra.

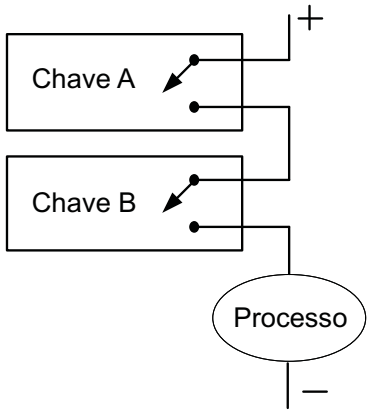


Figura 3.9: Sistema genérico com arquitetura 1oo2.

Para que o sistema como um todo falhe de forma perigosa é necessário que ocorra um curto-circuito em ambas as chaves, ou seja, que as duas chaves falhem de forma perigosa. Além disso, deve ser considerada ainda a possibilidade de as duas chaves virem a falhar ao mesmo tempo devido a uma mesma causa (modo comum). Esse cenário encontra-se representado através do diagrama de árvore de falta apresentado na Figura 3.10.

Para que o sistema falhe de forma segura basta que uma das chaves falhe de forma segura, ou seja, basta que uma das chaves falhe aberta. Novamente deve ser considerada a possibilidade de as duas chaves virem a falhar ao mesmo tempo devido a uma mesma causa. Esse cenário encontra-se representado através do diagrama de árvore de falta apresentado na Figura 3.11.

O modelo de Markov correspondente a esse sistema é apresentado na Figura 3.12. O estado 0 representa a situação na qual o sistema opera de forma bem sucedida. No estado 1 ocorreu uma falha perigosa em uma das chaves, mas o sistema continua

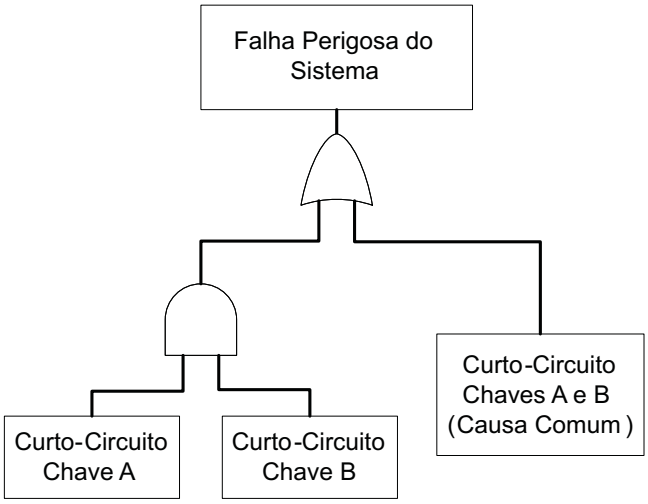


Figura 3.10: Diagrama de árvore de falta para sistema 1oo2.

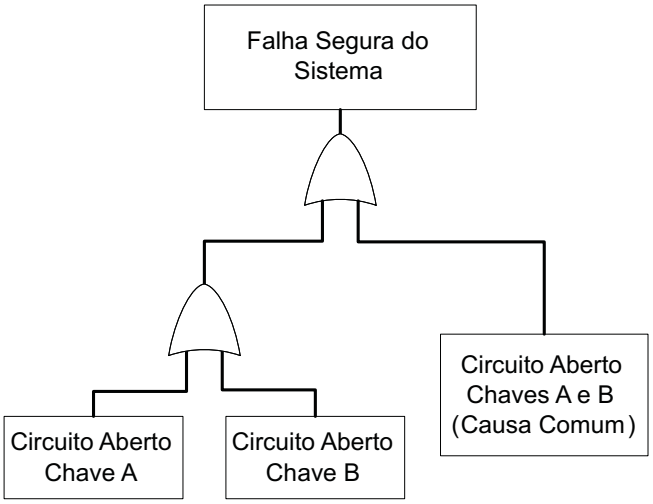


Figura 3.11: Diagrama de árvore de falta para sistema 1oo2.

operando. No estado 2 o sistema falhou de forma segura. É assumido que ao se atingir esse estado, todas as falhas serão reparadas e retorna-se ao estado 0. O estado 3 indica que o sistema falhou de forma perigosa.

O modelo apresentado na Figura 3.12 é bastante simples e desconsidera a capacidade de auto-diagnóstico de falhas do sistema. Um novo modelo, mais completo, apresentado na Figura 3.13 apresenta dois estados adicionais, em comparação ao modelo anterior. Neste novo modelo, o estado 0 continua representando a operação bem sucedida do sistema. Os estados 1 e 2 resultam da quebra do estado que representa a ocorrência de falha perigosa em uma das chaves em dois: o estado 1 indica a ocorrência de uma falha perigosa detectada; o estado 2 indica a ocorrência de uma falha perigosa não detectada. No estado 3 o sistema falha de forma segura.

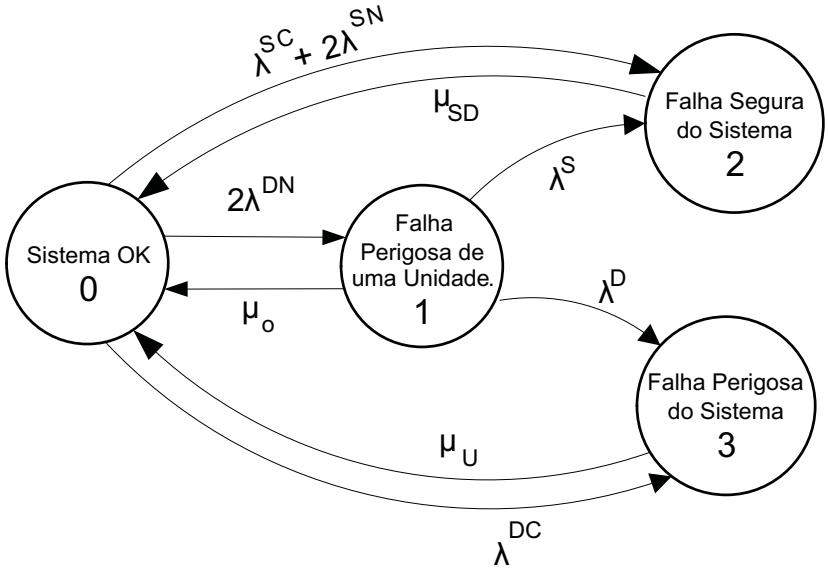


Figura 3.12: Modelo de Markov para sistema 1oo2.

Os estados 4 e 5 representam a falha perigosa do sistema, detectada e não detectada respectivamente. Nas Figuras 3.14 e 3.15 são apresentados novos diagramas para falhas perigosa e segura do sistema, respectivamente.

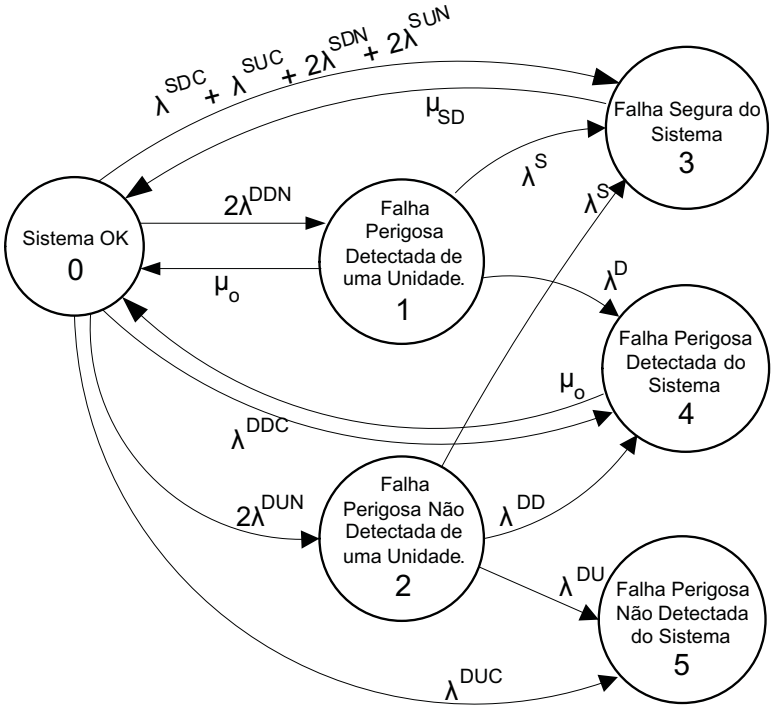


Figura 3.13: Modelo de Markov para sistema 1oo2 genérico com unidades idênticas e diagnóstico de falhas.

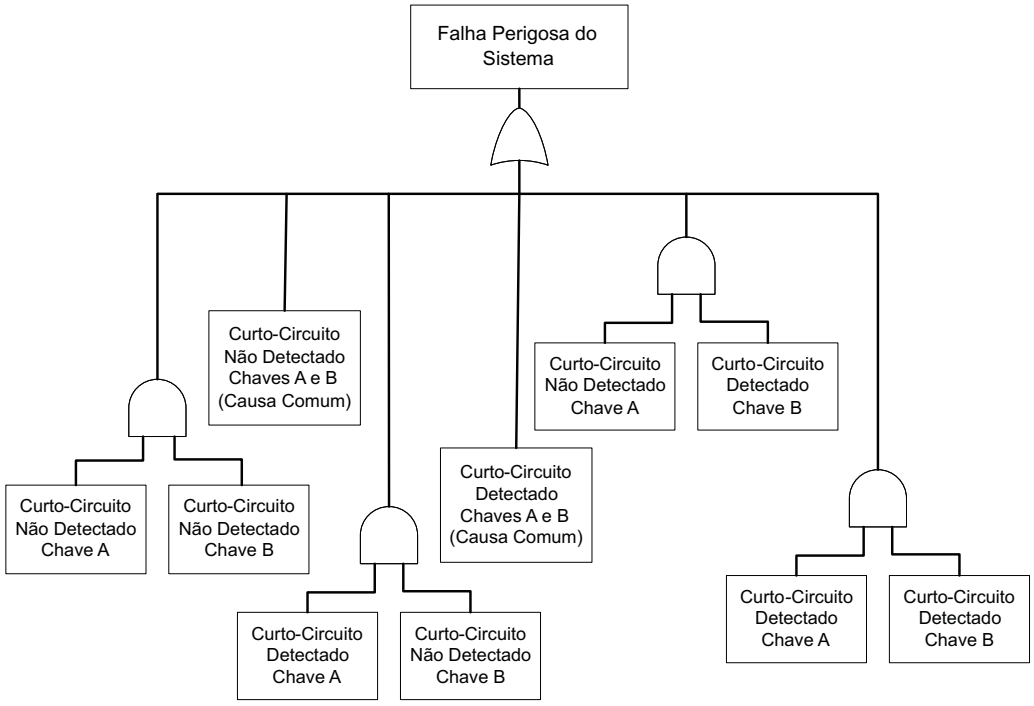


Figura 3.14: Diagrama de falha perigosa para sistema 1oo2 genérico com unidades idênticas e diagnóstico de falhas.

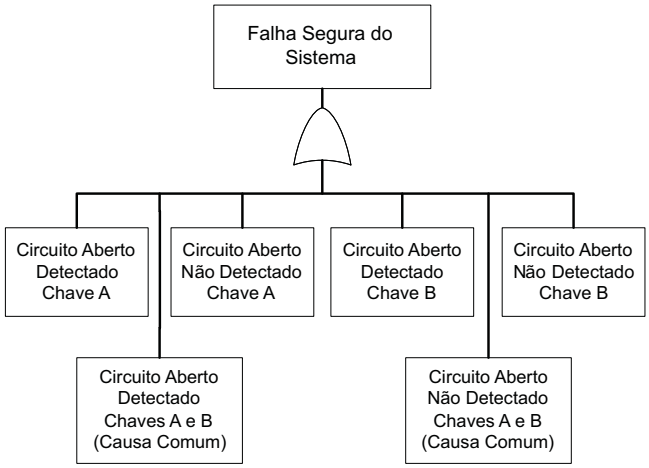


Figura 3.15: Diagrama de falha segura para sistema 1oo2 genérico com unidades idênticas e diagnóstico de falhas.

Com o objetivo de minimizar a probabilidade de falha devido a uma mesma causa, é comum a utilização de configurações redundantes compostas por equipamentos distintos. O modelo apresentado na Figura 3.13 pode ser modificado para representar o comportamento de um sistema 1oo2 genérico formado por unidades distintas. O novo modelo é apresentado a seguir na Figura 3.16.

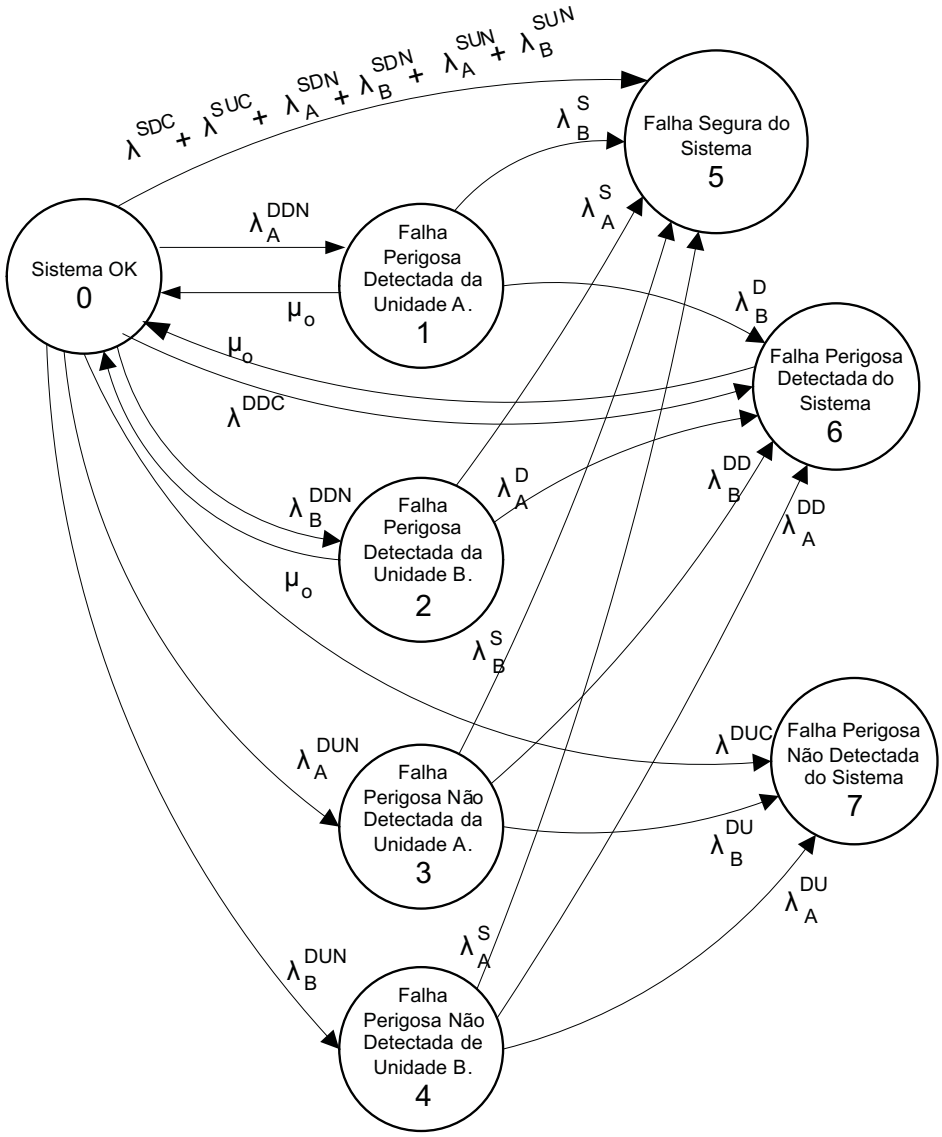


Figura 3.16: Modelo de Markov para sistema 1oo2 genérico com unidades distintas e diagnóstico de falhas.

3.4 Análise do Modelo

Para a análise dos modelos desenvolvidos e o cálculo dos índices de confiabilidade foi utilizado um procedimento baseado nos trabalhos apresentados por Goble e Cheddie (GOBLE; CHEDDIE, 2005) e Goble e Bukowski (GOBLE; BUKOWSKI, 2001a).

O primeiro passo para a análise do modelo de Markov desenvolvido é a sua representação em uma forma matricial.

3.4.1 Matriz de Transição

Qualquer modelo discreto de Markov pode ser representado por uma matriz $n \times n$, onde n é igual ao número de estados do modelo. Essa matriz, denominada Matriz de Probabilidade de Transição Estocástica, ou simplesmente Matriz de Transição, contém toda informação necessária a respeito do modelo de Markov.

Dado o modelo de Markov para um sistema redundante genérico com unidades idênticas apresentado na Figura 3.13, a matriz de transição que o representa é dada a seguir:

$$\Lambda = \begin{bmatrix} 1-\sum & 2\lambda^{DDN} & 2\lambda^{DUN} & \lambda^{S}+\lambda^{SN} & \lambda^{DDC} & \lambda^{DUC} \\ \mu_0 & 1-\sum & 0 & \lambda^{S} & \lambda^{D} & 0 \\ 0 & 0 & 1-\sum & \lambda^{S} & \lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 0 & 0 & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{3.22}$$

onde o termo $\sum$ representa a soma de todos os demais elementos da linha em questão.

Cada elemento da matriz de transição representa a probabilidade de transição do sistema entre os estados do modelo. Por exemplo, na matriz Λ em (3.22) o elemento $2\lambda^{DDN}$ referente à linha 0 e coluna 1 representa a probabilidade de transição entre os estados 0 e 1. De forma semelhante, o elemento $1-\sum$ referente à linha 0 e coluna 0 representa a probabilidade de o sistema permanecer no estado 0. Interpretação semelhante pode ser feita para os demais elementos da matriz Λ.

O estado de partida do modelo afeta o cálculo das probabilidades limite. Dessa forma, as probabilidades no instante de partida do modelo são especificadas através do vetor linha S. Esse vetor linha indica a probabilidade de que o modelo encontre-se em qualquer um dos estados existentes no instante inicial.

Para se analisar as probabilidades de estado do modelo de Markov em função do tempo, deve-se assumir um estado inicial para o sistema. Foi assumido que o sistema encontra-se inicialmente no estado 0 no instante de tempo $t = 0$. Isto é equivalente a dizer que o sistema opera normalmente imediatamente após sua fase de instalação e comissionamento.

3.4.2 Cálculo dos Índices de Confiabilidade e Disponibilidade

PFDavg e RRF

O valor da PFD é calculado a partir do somatório dos resultados obtidos através da multiplicação do vetor linha S pela matriz de transição P um número de vezes correspondente ao intervalo de tempo de interesse. O valor da PFD_{avg} é obtido simplesmente calculando-se o valor médio da PFD. Para o modelo apresentado na Figura 3.13 tem-se

$$S = S\Lambda \tag{3.23}$$

ou

$$S = S \begin{bmatrix} 1-\sum & 2\lambda^{DDN} & 2\lambda^{DUN} & \lambda^{S}+\lambda^{SN} & \lambda^{DDC} & \lambda^{DUC} \\ \mu_0 & 1-\sum & 0 & \lambda^{S} & \lambda^{D} & 0 \\ 0 & 0 & 1-\sum & \lambda^{S} & \lambda^{DD} & \lambda^{DU} \\ \mu_{SD} & 0 & 0 & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.24}$$

MTTF

Para o cálculo do MTTF deve-se criar uma matriz truncada que contenha apenas os estados transientes de sucesso do sistema. Isto é feito removendo-se as linhas e colunas referentes aos estados absorventes e/ou estados de falha do sistema. A matriz truncada Q para o modelo da Figura 3.13 é apresentada a seguir:

$$Q = \begin{bmatrix} 1-\sum & 2\lambda^{DDN} & 2\lambda^{DUN} \\ \mu_0 & 1-\sum & 0 \\ 0 & 0 & 1-\sum \end{bmatrix} \tag{3.25}$$

Observa-se que a matriz truncada Q apresentada em (3.25) foi obtida através da eliminação das linha e colunas correspondentes aos estados 3, 4 e 5 do modelo apresentado na Figura 3.13.

O passo seguinte é subtrair a matriz truncada Q da matriz identidade I.

$$I - Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 - \sum & 2\lambda^{DDN} & 2\lambda^{DUN} \\ \mu_0 & 1 - \sum & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3.26}$$

Em seguida deve-se inverter a matriz obtida após a subtração. O resultado dessa operação será uma nova matriz, denominada N. A matriz N fornece o número esperado de incrementos de tempo em que o sistema permanece em cada estado de sucesso do modelo, em função do estado de partida.

$$N = [I - Q]^{-1} \tag{3.27}$$

O MTTF é obtido através da adição dos elementos da linha referente ao estado de partida do sistema. Dessa forma, assumindo que o sistema comece a operar a partir do estado 0, o MTTF será resultado da soma dos elementos da linha 0 da matriz N.

MTTFs

Para o cálculo do MTTFs, o modelo de Markov apresentado na Figura 3.13 deve ser modificado. Deve-se remover o arco de transição que representa a probabilidade de reparo do estado que representa a falha segura do sistema. Dessa forma, o estado 5 passa a ser um estado absorvente. Um novo modelo é apresentado na Figura 3.17.

A partir do modelo modificado, o MTTFs será calculado através do procedimento apresentado anteriormente para o cálculo do MTTF.

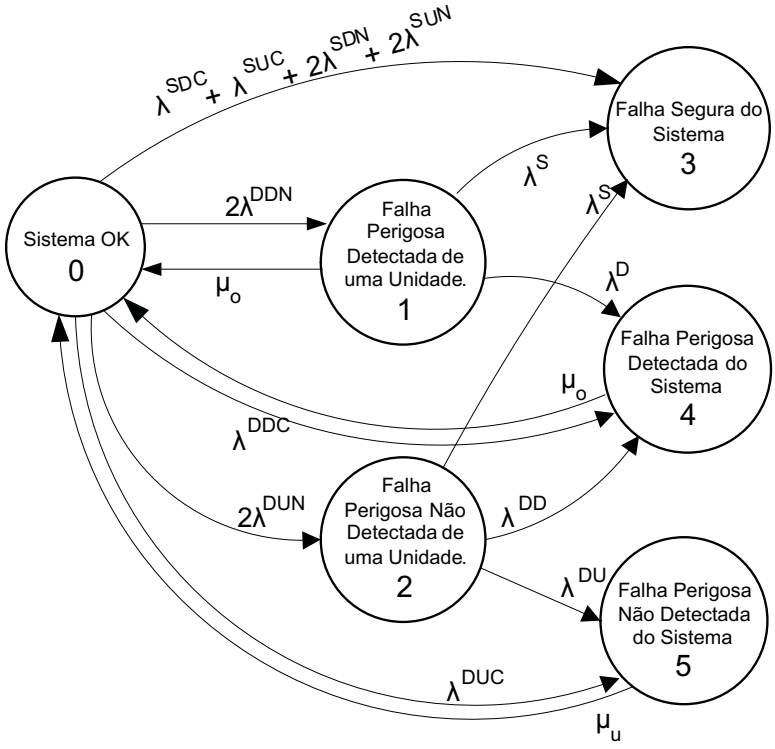


Figura 3.17: Modelo de Markov modificado para cálculo do MTTFs.

3.5 Conclusão

Diversos aspectos influenciam o comportamento dos sistemas e afetam diretamente o nível de complexidade dos modelos utilizados.

O uso de um procedimento sistemático para a construção dos modelos e a análise destes através da utilização de métodos numéricos simplifica o processo de análise, possibilitando a obtenção de resultados bastante precisos.

Capítulo 4

Software para Avaliação de Confiabilidade de SIS

4.1 Introdução

O software foi desenvolvido para apoiar a execução de avaliações de confiabilidade e disponibilidade de Sistemas Instrumentados de Segurança aplicados em áreas críticas de processos da indústria química e petroquímica.

Nas seções seguintes são discutidas as principais características e funcionalidades do software desenvolvido e apresentados alguns estudos de casos onde o software foi utilizado para o cálculo de índices de confiabilidade e segurança referentes a Sistemas Instrumentados de Segurança associados a processos bastante representativos na indústria química e petroquímica. Os resultados obtidos são comparados aos resultados obtidos através do uso do software exSILentia do fabricante Exida.

4.2 Software para Avaliação de Confiabilidade de SIS

4.2.1 Visão Geral

O software apresentado neste trabalho é o resultado de um projeto de P&D firmado entre a Universidade Federal de Campina Grande (UFCG) e o Centro de Pesquisas e Desenvolvimento Leopoldo Américo Miguez de Melo (CENPES/Petrobras). Através desse projeto buscava-se inicialmente o estudo e desenvolvimento de metodologias e técnicas para análise de confiabilidade e segurança de Sistemas Instrumentados

de Segurança implementados em unidades da Petrobras.

No entanto, no decorrer do projeto verificou-se que, a partir dos estudos realizados e dos modelos de confiabilidade desenvolvidos, seria interessante desenvolver uma ferramenta de software para auxiliar os novos projetos de SIS em atendimento a uma demanda interna da Petrobras. O software deveria possibilitar a realização da avaliação de confiabilidade através do cálculo de determinados índices de confiabilidade para verificação de atendimento ao SIL requerido de diferentes configurações de Funções Instrumentadas de Segurança que compõem um SIS. Dessa forma, engenheiros e especialistas da área poderiam facilmente determinar a melhor arquitetura do SIS através da análise de diferentes configurações possíveis.

Diferentemente de outras ferramentas de software desenvolvidas apenas para o cálculo do atributo de confiabilidade Probabilidade de Falha na Demanda (PFD) com base nas equações simplificadas propostas na Parte 6 da norma IEC 61508 (IEC, 2000), o software desenvolvido utiliza uma série de algoritmos baseados no método de análise de Markov (apresentado no capítulo 3) para o cálculo de índices de confiabilidade e segurança, tais como PFDavg e MTTFs. Além das vantagens da utilização desse método, o software ainda disponibiliza uma vasta base de dados de taxas de falha de equipamentos utilizados em implementações de SIS. Essa combinação permite uma análise completa e precisa de diversos cenários possíveis, dos mais simples aos mais complexos.

O software dispõem ainda de uma série de funcionalidades que facilitam o processo de análise, tais como a representação gráfica através de diagramas de blocos da configuração analisada em cada Função Instrumentada de Segurança e o cálculo do valor máximo de SIL de cada SIF, além de uma ferramenta para estimação do fator Beta de causa comum e a geração automática de relatórios com os dados utilizados e resultados da análise.

4.2.2 Arquitetura do Software

O software foi desenvolvido em linguagem de programação C# fazendo uso da plataforma .NET Microsoft Visual Studio 2008, e conta ainda com uma base de dados integrada, desenvolvida na plataforma SQL Server Compact Edition 3.5.

Concebido para utilização na plataforma Windows, o software é compatível com os sistemas operacionais XP e Vista. Na Figura 4.1 é apresentado um diagrama que representa a arquitetura do software desenvolvido.

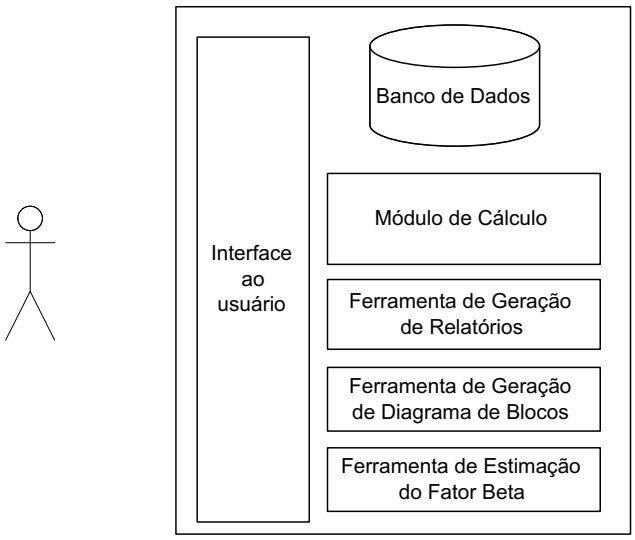


Figura 4.1: Arquitetura do software.

4.2.3 Descrição do Software

A interface do software foi elaborada de forma a tornar intuitiva a sua utilização por pessoas que já possuam algum conhecimento básico no que diz respeito ao processo de análise de risco e avaliação de confiabilidade e disponibilidade de SIS.

Na Figura 4.2 é apresentada a tela principal do software desenvolvido.

Figura 4.2: Tela principal do software.

Nessa tela estão localizados o menu principal de acesso às diversas funcionalidades do software.

A seguir são apresentadas as principais funcionalidades do software e as respectivas telas.

Criação de um novo projeto

Para criar um Novo Projeto deve-se selecionar a opção de menu Projeto>Novo, conforme apresentado na Figura 4.3.

Figura 4.3: Criando um novo projeto - Parte 1.

Será exibida a Tela Novo Projeto apresentada na Figura 4.4. Nesta tela devem ser inseridas as informações referentes ao novo projeto.

Figura 4.4: Criando um novo projeto - Parte 2.

Adicionando uma SIF ao projeto

Como visto anteriormente neste trabalho, um Sistema Instrumentado de Segurança é composto por diversas SIFs, identificadas durante uma fase preliminar do processo de análise de risco do processo. Dessa forma, a avaliação de confiabilidade e disponibilidade de um SIS é realizada por meio da avaliação das SIFs que o compõem. Portanto, para dar início a uma avaliação de SIS é necessário adicionar ao projeto criado as SIFs previamente identificadas.

O campo SIFs existente no canto superior esquerdo da Tela Principal agrupa todos os comandos necessários para essa tarefa. Para adicionar uma nova SIF ao projeto criado, deve-se clicar no botão Adicionar. Imediatamente será exibida uma caixa na qual deve-se inserir o nome da nova SIF, conforme apresentado na Figura 4.5.

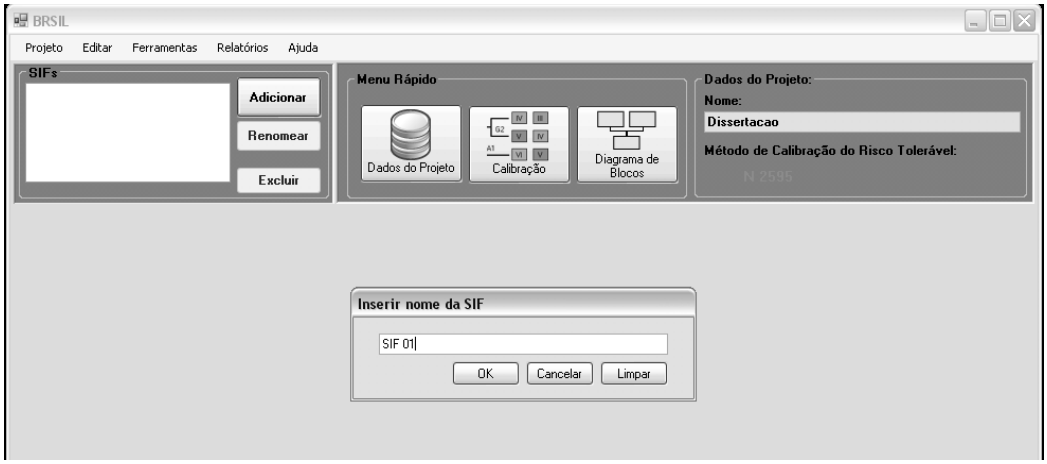


Figura 4.5: Adicionando uma SIF ao projeto.

Após isso, um conjunto de abas associadas à SIF adicionada será exibido na parte inferior da tela, conforme apresentado na Figura 4.6. Cada aba corresponde a uma etapa do processo de avaliação da SIF, sendo que a primeira disponibiliza um conjunto de campos para identificação da SIF e descrição do cenário associado.

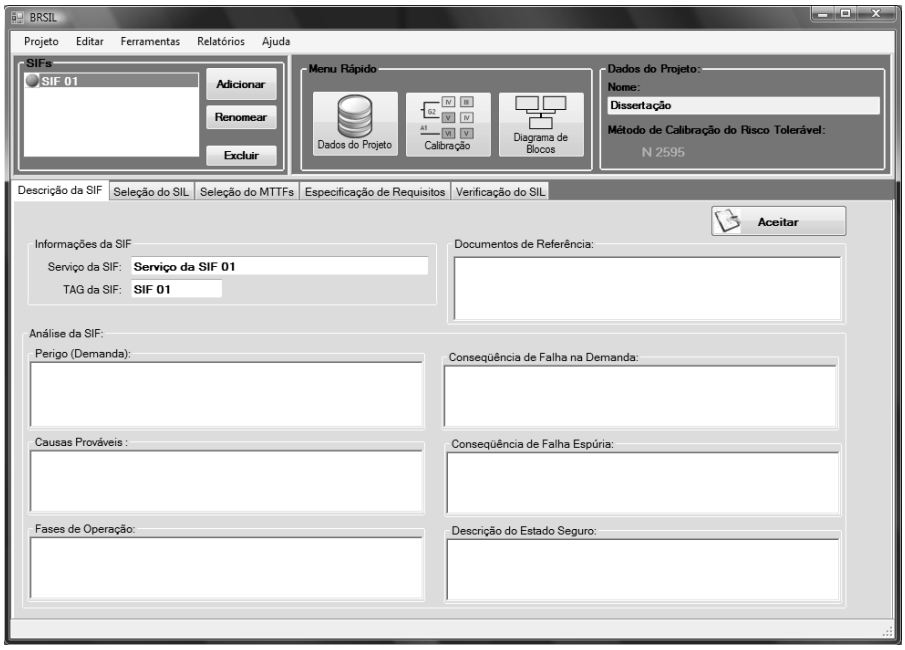


Figura 4.6: Tela de Descrição da SIF.

Especificando a SIF

O passo seguinte é a especificação dos elementos e parâmetros da SIF. Essa tarefa é realizada através da aba verificação do SIL, apresentada na Figura 4.7.

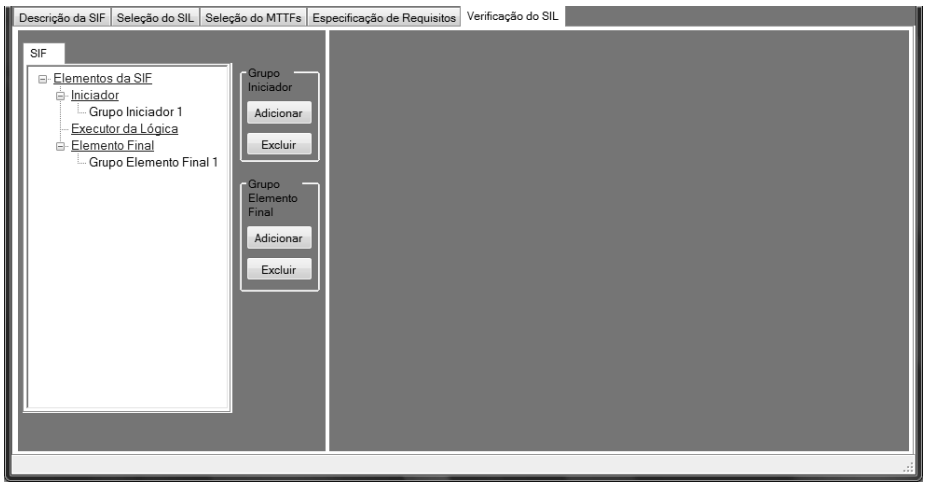


Figura 4.7: Tela de Especificação da SIF.

Uma SIF é composta por três elementos básicos: sensor (iniciador), executor da lógica e elemento final. Para facilitar a visualização foi adotada uma estrutura em árvore onde cada nó principal referencia um dos três elementos básicos que compõem a SIF, na seqüencia estabelecida acima. Na Figura 4.8 é apresentada a árvore de

navegação da SIF.

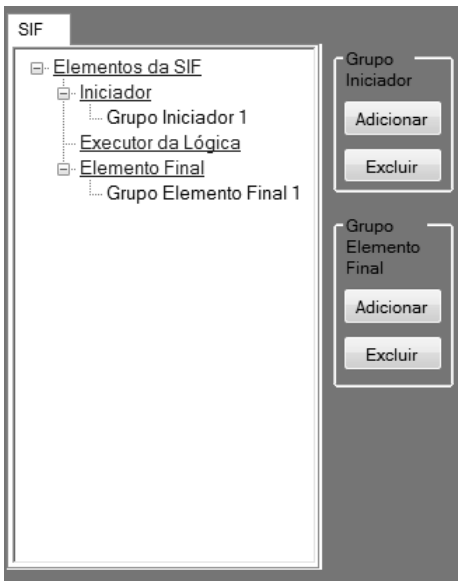


Figura 4.8: Árvore de Navegação da SIF.

Ainda segundo essa estrutura, cada elemento básico da SIF (nó) é composto por grupos (sub-nós) e cada um dos grupos é composto por elementos. Até 4 grupos podem ser adicionados ao nó iniciador da SIF, sendo que cada grupo pode ser composto por um número máximo de 3 elementos. Na Figura 4.9 é apresentado um diagrama de blocos que representa a estrutura adotada.

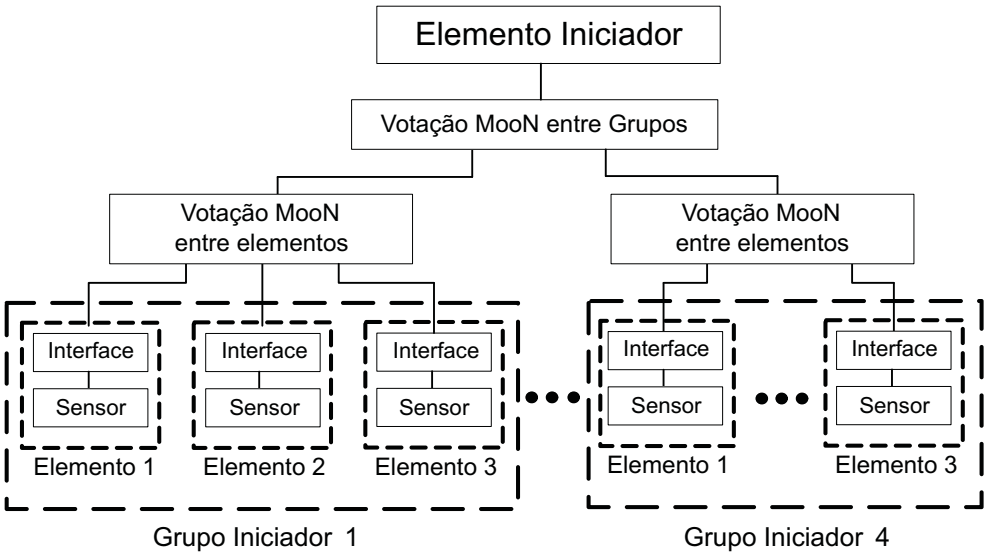


Figura 4.9: Diagrama do Elemento Iniciador da SIF.

Na Figura 4.10 é apresentada a tela para edição das propriedades do grupo iniciador criado.

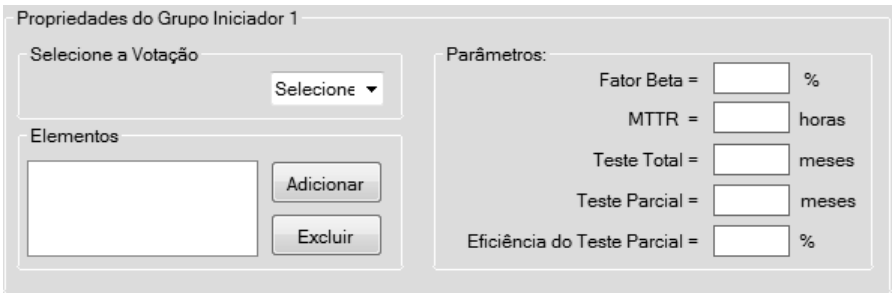


Figura 4.10: Tela de especificação do Grupo Iniciador.

Nessa tela deverão ser inseridos todos os parâmetros necessários para o cálculo dos índices de confiabilidade e disponibilidade associados a esse grupo. Além disso, é por meio dessa tela que são adicionados os elementos pertencentes ao grupo, e definido o esquema de votação que será empregado. O esquema de votação adotado corresponde ao número de elementos adicionados. As opções de votação possíveis são 1oo1, 1oo2, 2oo2, 1oo3, 2oo3 e 3oo3. Na Figura 4.11 é apresentada a tela para especificação dos elementos que compõem o grupo.

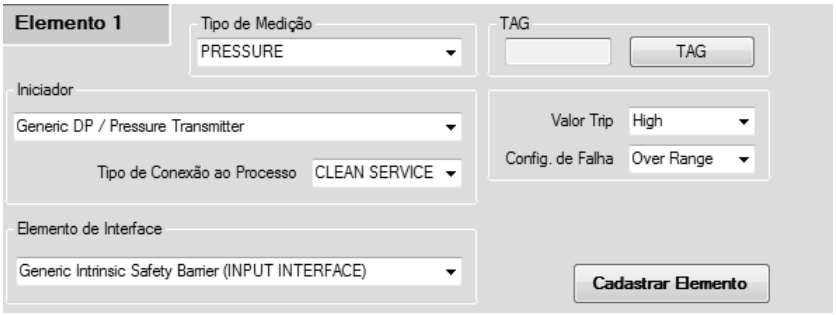


Figura 4.11: Tela de especificação do elemento do Grupo Iniciador.

Estrutura semelhante é adotada para o nó referente ao elemento final da SIF. Na Figura 4.12 é apresentado um diagrama de blocos que representa a estrutura adotada para o elemento final.

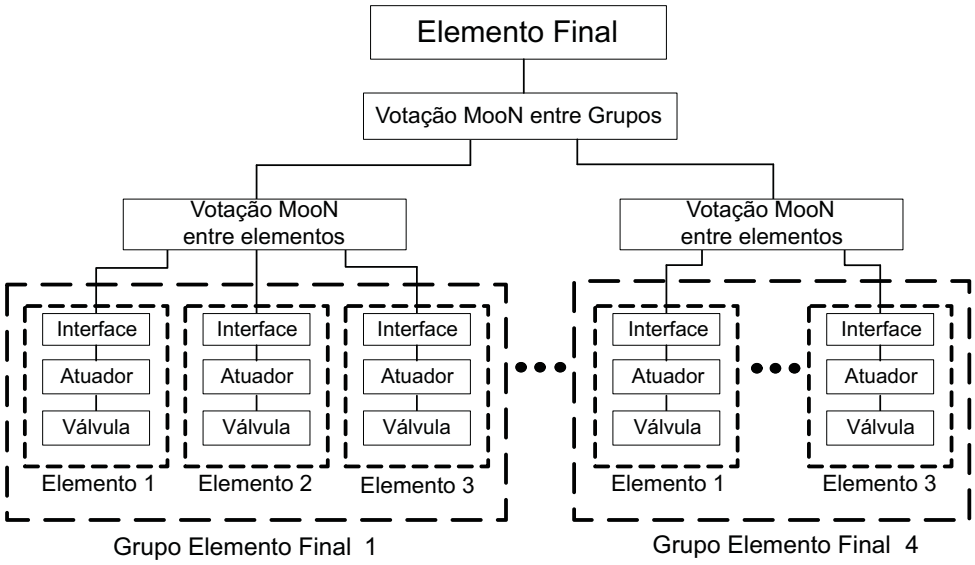


Figura 4.12: Diagrama do Elemento Final da SIF.

Nas Figuras 4.13 e 4.14 são apresentadas as telas para para edição das propriedades do grupo elemento final e para especificação dos elementos que o compõem, respectivamente.

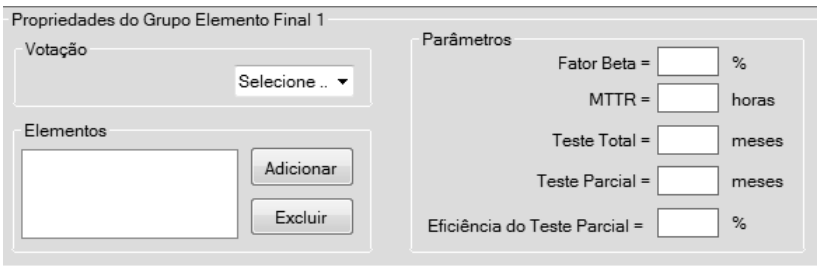


Figura 4.13: Tela de especificação do Grupo Elemento Final.

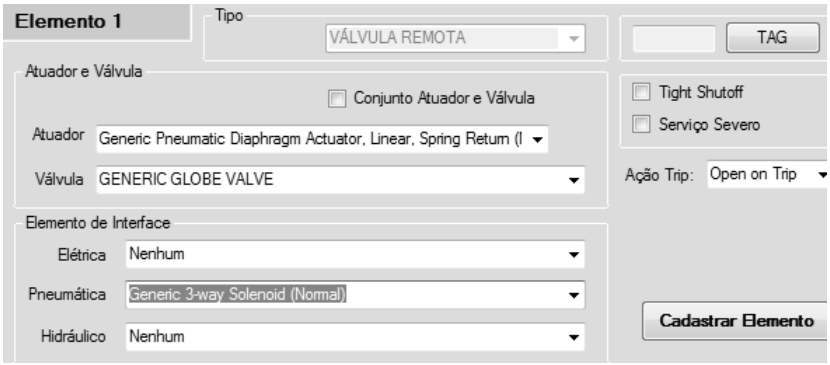


Figura 4.14: Tela de especificação do elemento do Grupo Elemento Final.

Assume-se que o elemento executor da lógica é único em cada SIF, logo não é permitida a adição de grupos ao nó referente a esse elemento básico. Na Figura 4.15 é apresentada a tela para especificação e edição das propriedades do executor da lógica.

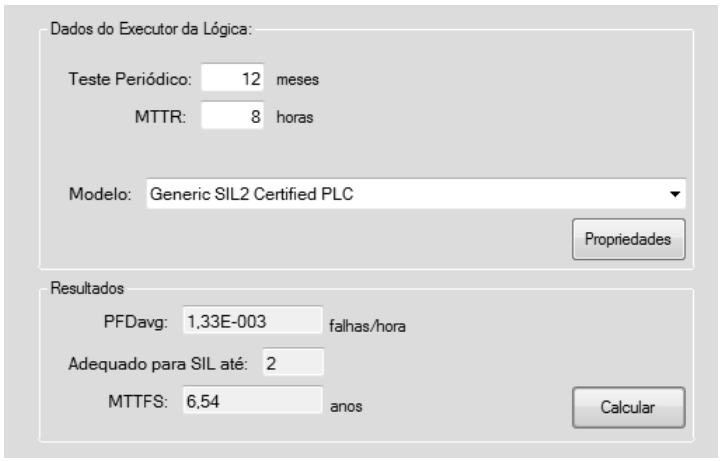


Figura 4.15: Tela de especificação do Executor da Lógica.

Visualizando os resultados da SIF

Para visualizar os resultados obtidos para cada grupo definido, deve-se selecionar o grupo desejado na árvore de navegação da SIF. Nas Figuras 4.16 e 4.17 são apresentadas a telas de exibição dos resultados dos cálculos realizados para os grupos Iniciador e Elemento Final, respectivamente.

Os resultados obtidos para os cálculos referentes ao elemento executor da lógica são apresentados na mesma tela de especificação e edição das propriedades apresentada na Figura 4.15.

Após a especificação de todas as partes componentes da SIF, o usuário poderá visualizar os resultados finais dos cálculos realizados e conferir se os índices obtidos encontram-se de acordo com os nível de integridade desejado. Para tal, o usuário deverá selecionar a opção Elementos da SIF localizada no topo da árvore de navegação da SIF. Na Figura 4.18 é apresentada a tela de exibição de resultados da SIF.

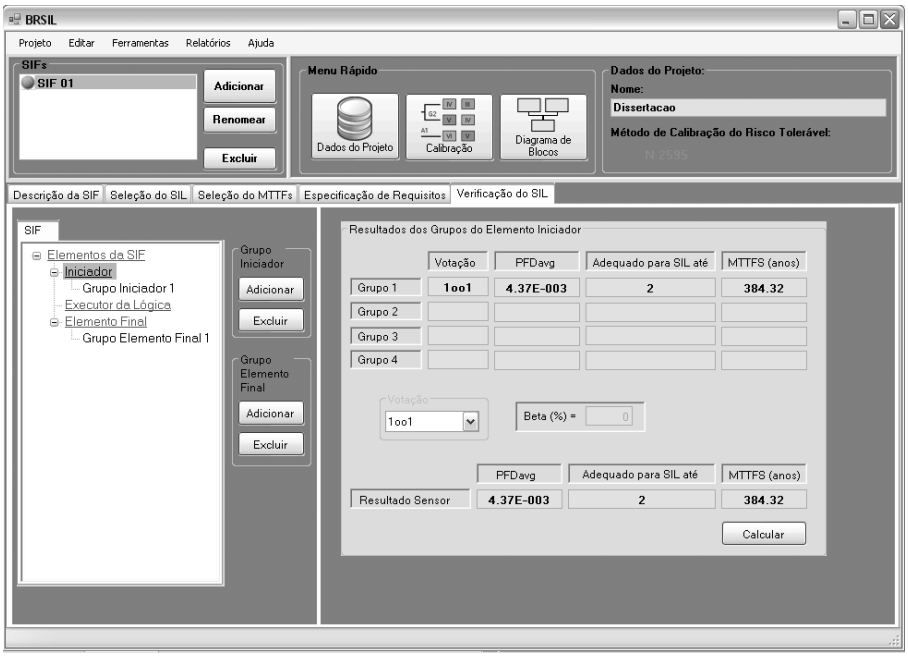


Figura 4.16: Tela de Resultados do Grupo Sensor.

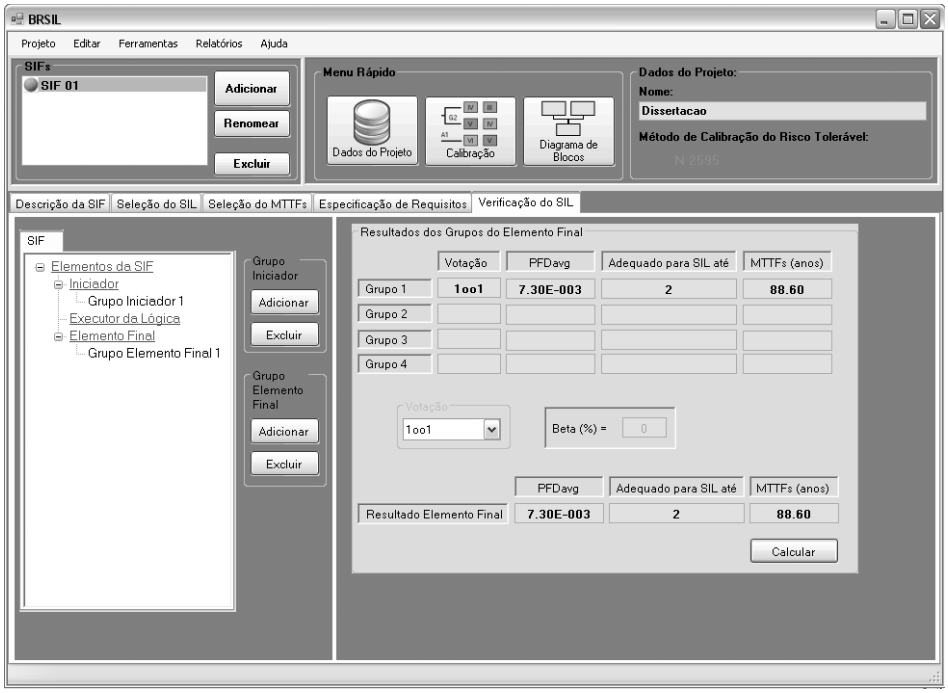


Figura 4.17: Tela de Resultados do Grupo Elemento Final.

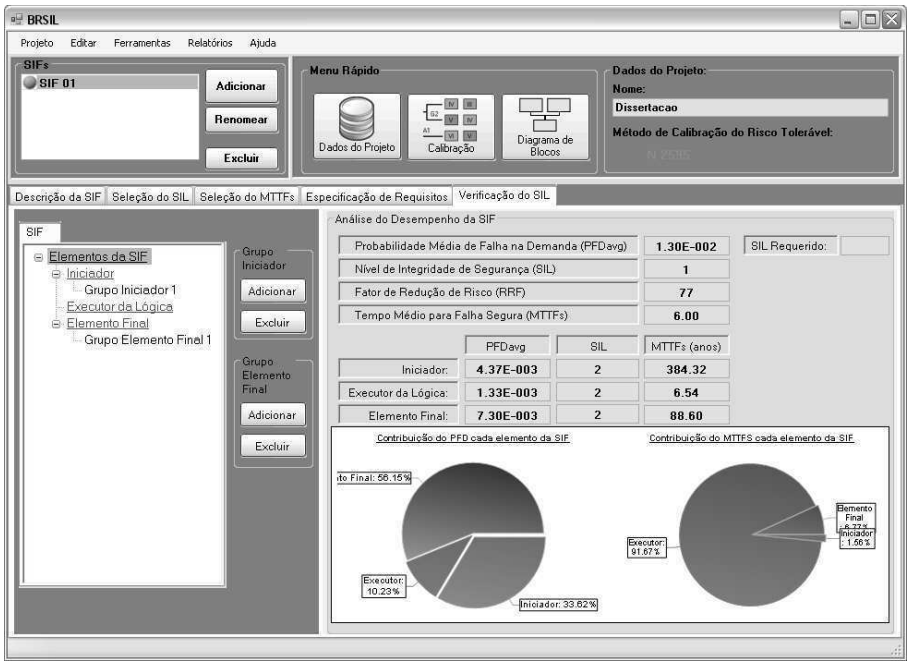


Figura 4.18: Tela de Resultados da SIF.

Visualizando a configuração implementada

A qualquer momento durante a etapa de especificação dos componentes da SIF é possível visualizar a configuração implementada por meio de um diagrama de blocos. Na Figura 4.19 é apresentado um exemplo de diagrama de blocos gerado.

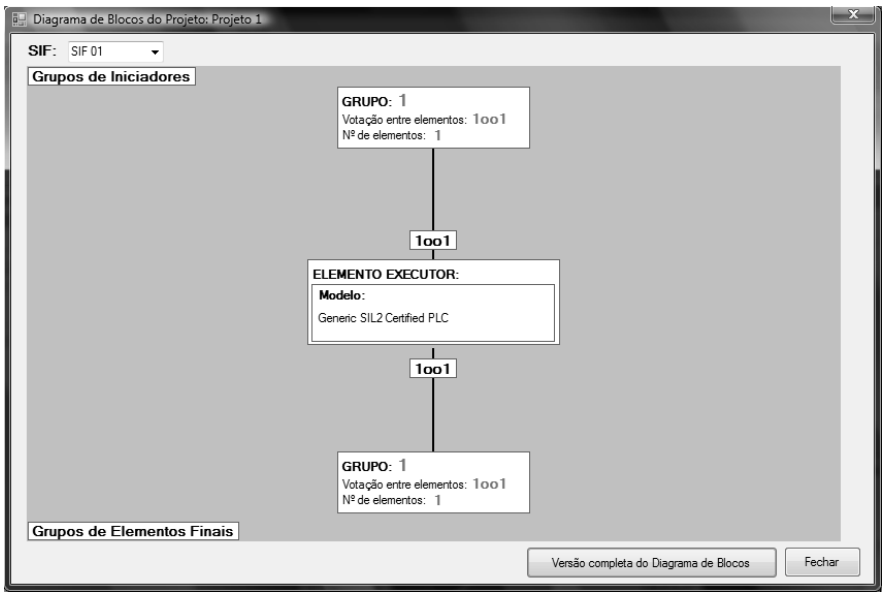


Figura 4.19: Exemplo de diagrama de blocos gerado.

Ferramenta de Estimação do Fator Beta de Causa Comum

Outra funcionalidade incorporada no software é a ferramenta para estimar o Fator Beta de causa comum. Essa ferramenta permite estimar um valor adequado para fator Beta a ser utilizado na avaliação através do preenchimento de um formulário simples. Para ter acesso a esta ferramenta deve-se clicar no menu Ferramentas>Estimador Beta. Na Figura 4.20 é apresentada a ferramenta.

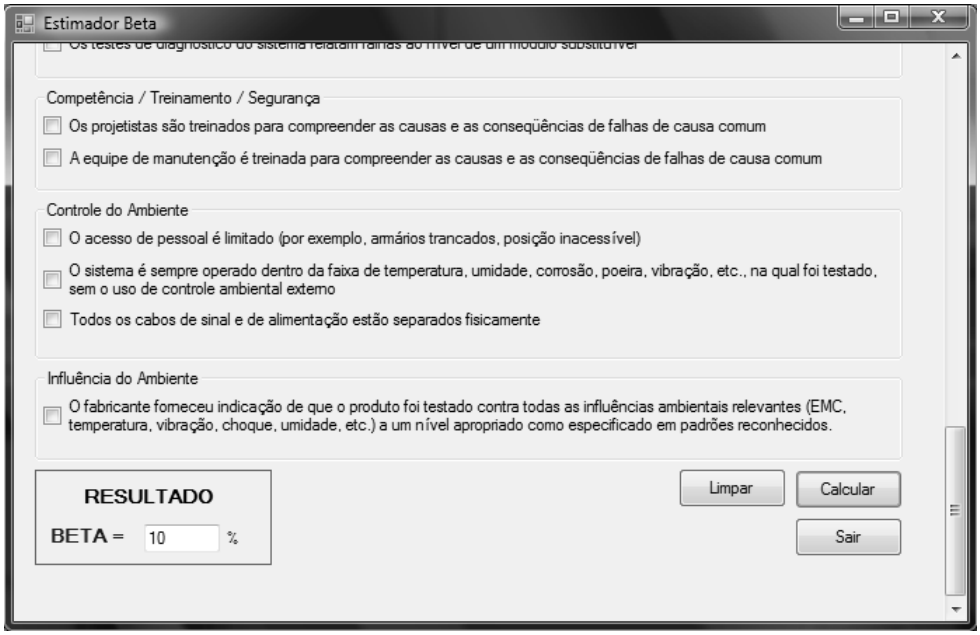


Figura 4.20: Ferramenta para estimação do Fator Beta de Causa Comum.

4.3 Estudos de Caso

Nesta seção são apresentados alguns estudos de casos onde são avaliados Sistemas Instrumentados de Segurança associados a processos bastante comuns na indústria química e petroquímica. Em cada caso são discutidos aspectos referentes à operação do processo e implementação do SIS e calculados os índices de confiabilidade e disponibilidade através do uso do software desenvolvido. O nível SIL resultante para cada SIF analisada é atribuído de acordo com classificação estabelecida pela norma IEC 61508 (IEC, 2000), em função da PFDavg calculada. Os valores adotados para os equipamentos foram retirados da base de dados de falha de equipamentos da Exida (EXIDA, 2003). Além disso, todas as taxas de falha referentes aos equipamentos selecionados e taxas de reparo utilizadas são assumidas constantes.

4.3.1 Estudo de Caso 1: Reator Químico

No exemplo a seguir é apresentada a análise de confiabilidade e disponibilidade do Sistema Instrumentado de Segurança projetado para garantir a proteção de um reator químico contra valores excessivos de pressão causados por um bloqueio no circuito de saída do reator. Valores de pressão acima de limites classificados como seguros podem ocasionar a ruptura das paredes do reator e a liberação de seu conteúdo para a atmosfera, resultando em danos a equipamentos e perdas de vidas, dentre outras conseqüências. O sistema descrito é apresentado na Figura 4.21.

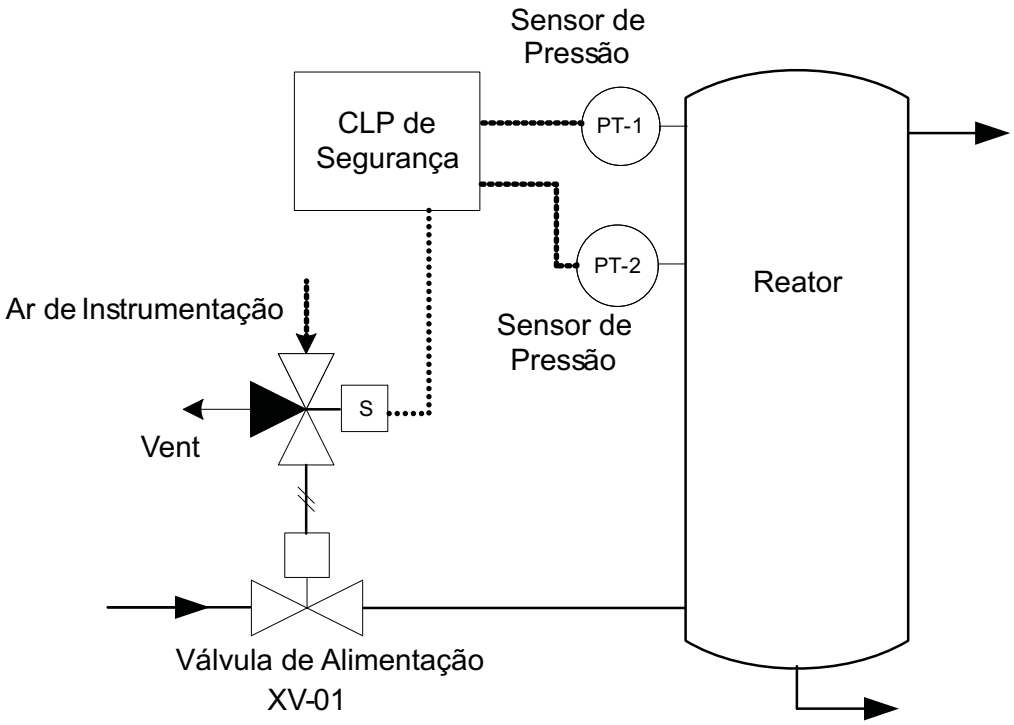


Figura 4.21: Estrutura do SIS associado ao Reator Químico.

O SIS deste exemplo é composto por uma única Função Instrumentada de Segurança constituída pelos seguintes equipamentos genéricos: dois transmissores de pressão idênticos PT-1 e PT-2, um CLP de segurança, uma válvula solenóide de 3 vias e uma válvula esfera de segurança XV-01. Na Figura 4.22 é apresentado um diagrama de blocos que representa a arquitetura adotada para a função de segurança. Quando um dos transmissores sinaliza que a pressão no interior do reator está acima de um valor limite pré-estabelecido a válvula XV-01 é fechada, interrompendo a alimentação do reator.

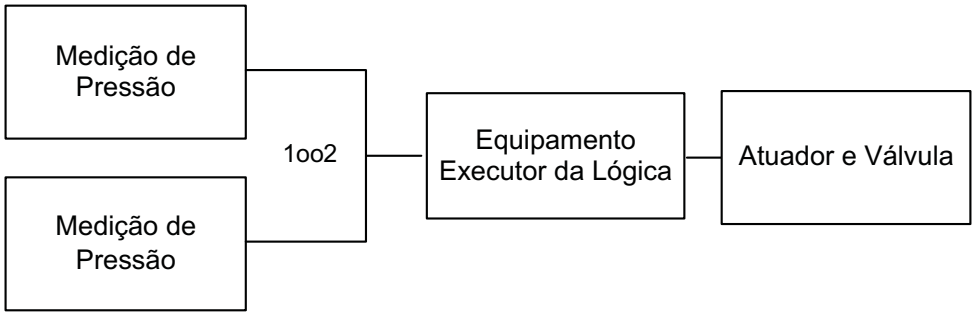


Figura 4.22: Representação da SIF do Reator Químico.

Os valores assumidos para os parâmetros utilizados nos cálculos e as taxas de falha dos equipamentos selecionados são apresentados nas Tabelas 4.1 e 4.2, respectivamente.

Tabela 4.1: Parâmetros utilizados na análise (Caso 1).

Descrição	Parâmetro	Valor
Tempo médio de reparo	MTTR	24h
Tempo de campanha	TC	10 anos
Tempo de Startup	$T_{Startup}$	30h
Intervalo de teste periódico	TI	12 meses
Fator Beta	β	5%
Fator de cobertura de diagnóstico	C	99%

Tabela 4.2: Taxas de falha dos equipamentos utilizados (Caso 1).

Equipamentos	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Transmissor de Pressão	-	3,00E-07	-	1,00E-06
CLP de Segurança	1,12E-05	1,35E-07	4,34E-06	2,69E-07
Válvula Solenóide 3 Vias	-	1,01E-06	-	5,85E-07
Válvula Esfera	-	5,00E-07	-	1,27E-06

Na Figura 4.23 é apresentada a tela de exibição dos resultados obtidos a partir da utilização do software desenvolvido para a análise realizado no estudo de caso 1.

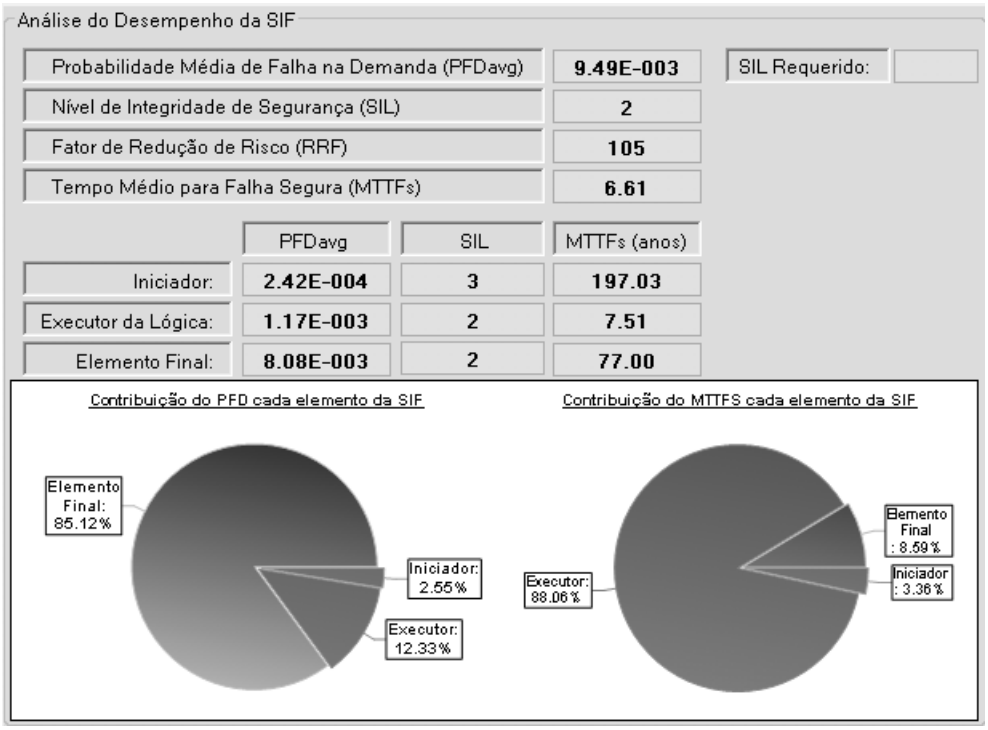


Figura 4.23: Tela de resultados para o Estudo de Caso 1.

A partir do valor obtido para a PFDavg total é possível classificar a SIF como sendo adequada para um nível SIL 2.

Observa-se que, dentre os três componentes básicos da SIF, o Elemento Final é o componente de maior contribuição para a probabilidade de falha na demanda do sistema.

Na Tabela 4.3 é apresentada uma comparação entre os resultados obtidos a partir do uso do software desenvolvido e os resultados obtidos através do uso do software de análise de confiabilidade exSILentia do fabricante Exida.

Tabela 4.3: Comparação entre os resultados obtidos (Caso 1).

	exSILentia		BR-SIL	
Elementos	PFDavg	MTTFs (anos)	PFDavg	MTTFs (anos)
Elemento Sensor	2,41E-04	195,97	2,42E-04	197,03
Executor da Lógica	1,17E-03	7,31	1,17E-03	7,51
Elemento Final	8,06E-03	76,22	8,08E-03	77,00

4.3.2 Estudo de Caso 2: Planta de Gás Natural

A seguir é realizada a análise de um Sistema Instrumentado de Segurança implantado em uma planta de produção de gás natural. Plantas de produção de óleo e gás, tanto *onshore* quanto *offshore*, operam com valores elevados de pressão, vazão e temperatura e os perigos e respectivas conseqüências devido a falhas operacionais e/ou de equipamentos podem ser catastróficos.

Neste exemplo considera-se um campo de produção formado por cinco poços localizados a uma distância de aproximadamente 2 a 10 Km da estação coletora. Na Figura 4.24 é apresentado um diagrama simplificado que representa a interconexão entre os poços e a planta de produção de gás natural.

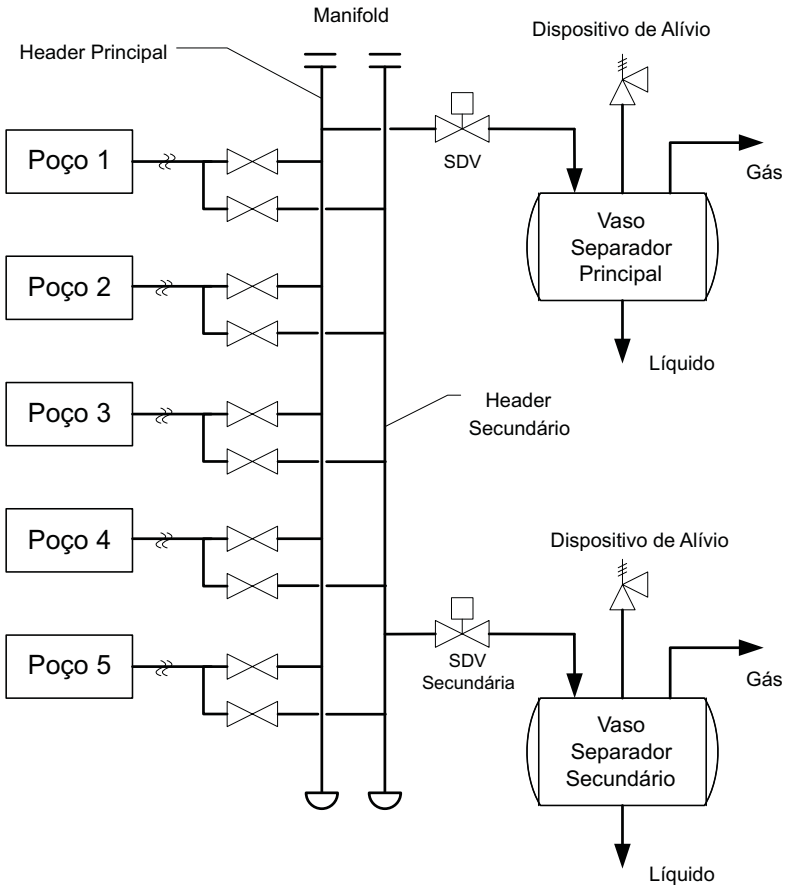


Figura 4.24: Diagrama simplificado do processo.

Os cinco poços do campo estão interligados a uma estação coletora através de linhas de 3", as quais chegam à estação por um *manifold* de recebimento com dois *headers*, um de produção e outro secundário. O *header* secundário permite o monitoramento da produção de cada poço de forma isolada. Após a passagem pelo *manifold*, o fluxo da produção é direcionado para um vaso separador principal, onde

ocorre a separação do condensado e outros líquidos contaminantes (inclusive água) do gás. Os processos de tratamento para o gás e o líquido resultantes da etapa de separação não são discutidos neste exemplo.

As válvulas de alívio presentes nos vasos separadores principal e secundário são conectadas a um terceiro *header* de segurança conectado a uma tocha (*flare*) para queima do gás. Por simplificação, o *header* de segurança e suas respectivas conexões não são exibidos na Figura 4.24.

Na Figura 4.25 são apresentados os principais equipamentos associados a cada poço e suas respectivas interligações com o BPCS e o SIS.

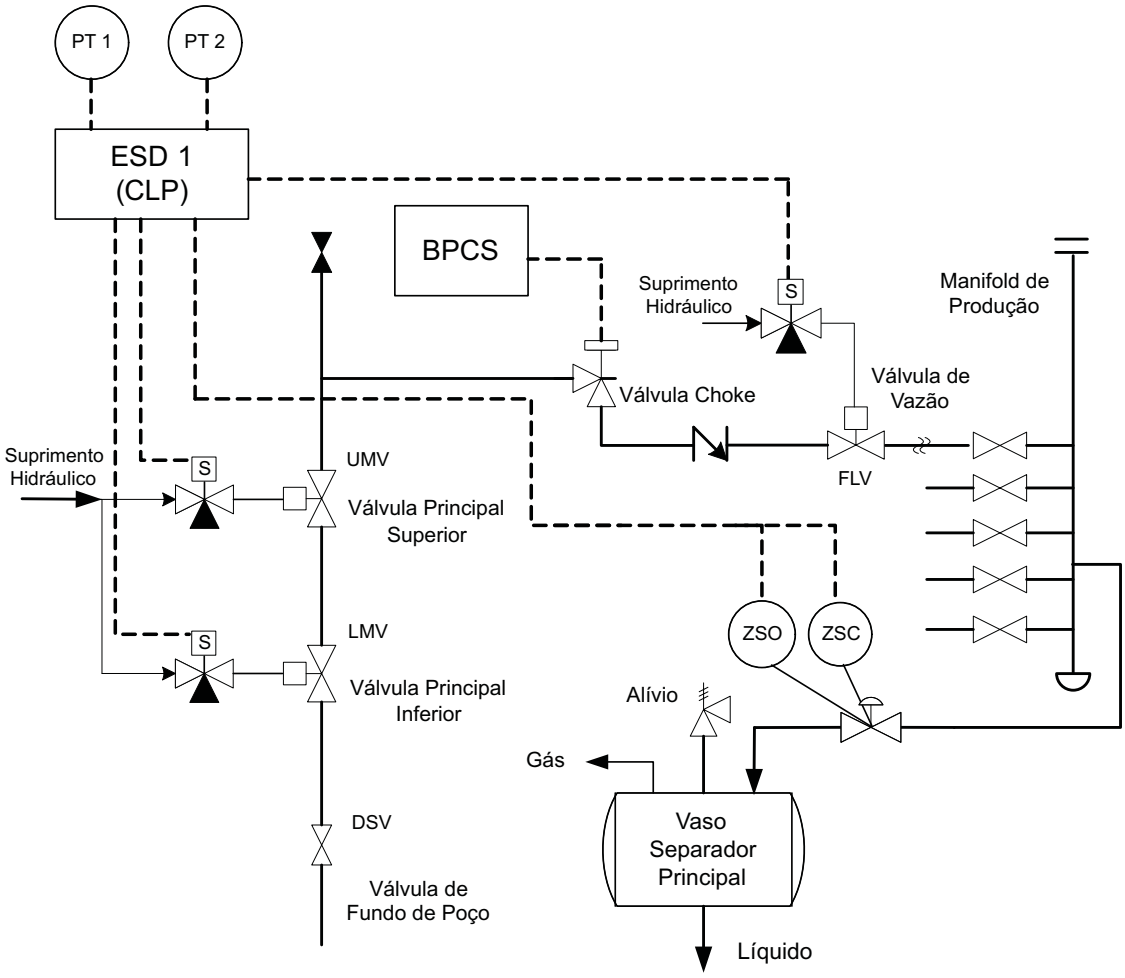


Figura 4.25: Diagrama do processo para cada poço de produção.

Em cada poço existe uma válvula *Choke* associada ao BPCS para o controle da vazão dos fluidos produzidos. Outras quatro válvulas são utilizadas para a segurança do processo. Essas válvulas são listadas a seguir.

- Válvula de segurança de fundo de poço (DSV - *Down-hole safety valve*)

Trata-se de uma válvula de segurança do tipo N.A. que atua de forma automática, independente de sinal externo. Quando a pressão atinge um valor pre-determinado, essa válvula sela o poço.

- Válvula de Trip principal inferior (LMV - *Lower master trip valve*)

  Localizada na linha de saída do poço, é uma válvula do tipo *fail close* operada hidraulicamente via uma válvula solenóide.

- Válvula de Trip principal superior (UMV - *Upper master trip valve*)

  Localizada imediatamente acima da válvula LMV, a UMV também é uma válvula do tipo *fail close* operada hidraulicamente via uma válvula solenóide.

- Válvula de vazão (FLV - *Flow-line valve*)

  Localizada após a válvula *Choke*, a válvula FLV é uma válvula do tipo *fail close* operada hidraulicamente via uma válvula solenóide.

Observa-se que, excetuando-se a válvula de segurança de fundo de poço (DSV), as demais válvulas são operadas hidraulicamente através de válvulas solenóides individuais e são do tipo N.F. ou "falha fechada"(*Fail close*). Assim, a perda de pressão hidráulica de alimentação irá ocasionar o fechamento das mesmas e, conseqüentemente, a interrupção da produção.

O sistema de proteção implementado utiliza um CLP de segurança como equipamento executor da lógica de segurança. Dois transmissores de pressão são utilizados numa configuração de votação 1oo2 para detecção de valores baixos e elevados de pressão. Chaves de posição sinalizam para o CLP de segurança se a válvula de *shutdown* localizada na entrada do separador principal está fechada. Também para as chaves de posição foi adotado um esquema de votação 1oo2. O subconjunto elemento final do SIS é composto pelas válvulas LMV, UMV e FLV e respectivas válvulas solenóides dispostas numa configuração em série (votação 1oo3).

O foco da análise apresentada neste exemplo será a Função Instrumentada de Segurança implementada para salvaguardar o processo contra um valor elevado de pressão na linha entre o poço e o *manifold* de produção. Dentre as diversas causas que podem levar a esse cenário de risco pode-se destacar:

- Causa 1 - O fechamento da válvula de *shutdown* localizada na entrada do vaso separador principal ocasionando valores de pressão excessivos nas linha de produção e *manifolds*. A conseqüência mais provável associada a este cenário é a ruptura de uma flange do *manifold* de produção.

- Causa 2 - Fechamento de uma válvula de admissão localizada na entrada do *manifold* de produção ocasionando sobrepressão na linha. A conseqüência mais provável associada a este cenário é a ruptura da linha de produção em qualquer ponto entre o poço e o *manifold* de produção.

Na figura 4.26 é apresentado um diagrama de blocos para a Função Instrumentada de Segurança para o cenário de sobrepressão na linha entre o poço e a entrada do vaso separador (causa 1).

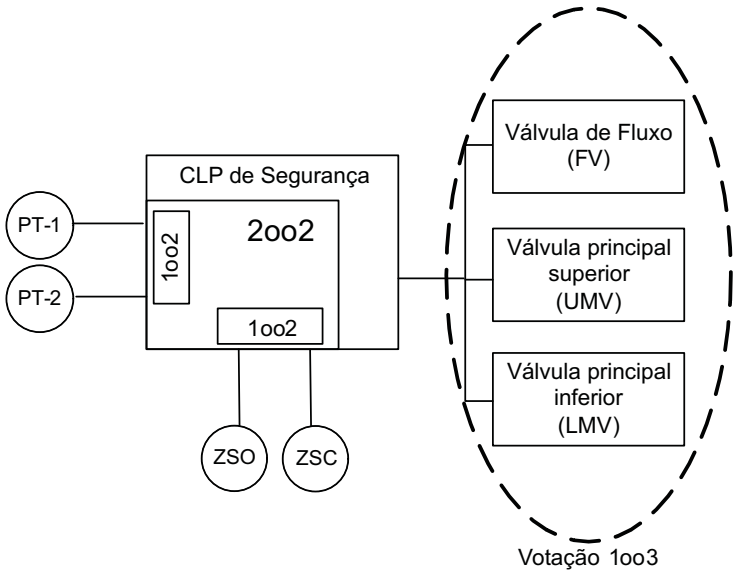


Figura 4.26: Diagrama de Blocos da SIF - Estudo de Caso 2.

Os valores assumidos para os parâmetros utilizados nos cálculos e as taxas de falha dos equipamentos selecionados são apresentados nas Tabelas 4.4 e 4.5, respectivamente.

Tabela 4.4: Parâmetros utilizados na análise (Caso 2).

Descrição	Parâmetro	Valor
Tempo médio de reparo	MTTR	24h
Tempo de campanha	TC	10 anos
Tempo de Startup	$T_{Startup}$	30h
Intervalo de teste periódico	TI	12 meses
Fator Beta	β	5%
Fator de cobertura de diagnóstico	C	99%

Tabela 4.5: Taxas de falha dos equipamentos utilizados (Caso 2).

Equipamentos	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Transmissor de Nível	-	1,00E-07	-	2,90E-06
Chave de Posição	-	1,50E-07	-	1,00E-07
CLP de Segurança	1,12E-05	1,35E-07	4,34E-06	2,69E-07
Válvula Solenóide 3 Vias	-	1,01E-06	-	5,85E-07
Válvula Esfera	-	5,00E-07	-	1,27E-06

Na Figura 4.27 é apresentada a tela de resultados para a análise realizada para o estudo de caso 2.

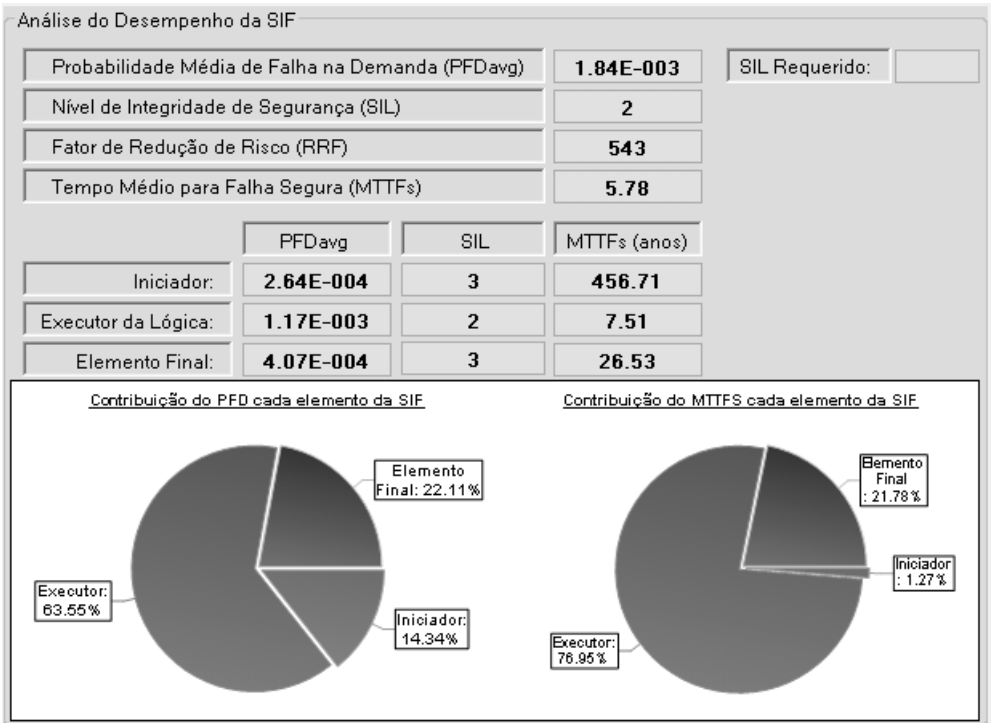


Figura 4.27: Tela de resultados para o Estudo de Caso 2.

A partir do valor obtido para a PFDavg total é possível classificar a SIF como sendo adequada para um nível SIL 2.

Observa-se que, dentre os três componentes básicos da SIF, o Executor da Lógica é o componente de maior contribuição para a probabilidade de falha na demanda do sistema.

Na Tabela 4.6 é apresentada uma comparação entre os resultados obtidos a partir do uso do software desenvolvido e os resultados obtidos através do uso do software de análise de confiabilidade exSILentia do fabricante Exida.

Tabela 4.6: Comparação entre os resultados obtidos (Caso 2).

	exSILentia		BR-SIL	
Elementos	PFDavg	MTTFs (anos)	PFDavg	MTTFs (anos)
Elemento Sensor	2,63E-04	455,93	2,64E-04	456,71
Executor da Lógica	1,17E-03	7,31	1,17E-03	7,51
Elemento Final	4,06E-04	26,38	4,07E-04	26,53

4.3.3 Estudo de Caso 3: Vaso Separador

A análise apresentada nesta seção está focalizada no trecho da planta de gás natural apresentada na Figura 4.24 onde se encontra o vaso separador, equipamento responsável pela separação da mistura líquido-gás.

Na Figura 4.28 são apresentados os principais equipamentos associados ao vaso separador e suas respectivas interligações com o BPCS e o SIS.

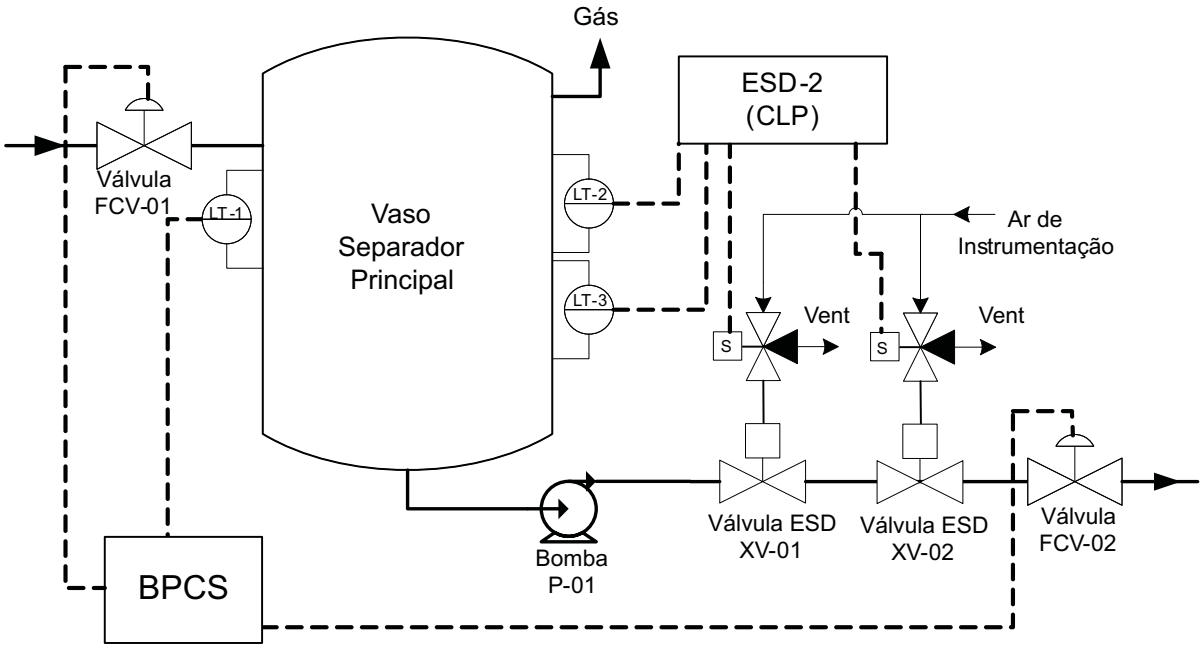


Figura 4.28: BPCS e SIS associados ao vaso separador.

O nível de líquido no separador é controlado por uma malha de controle do BPCS. É assumido que o líquido proveniente do separador é bombeado de forma contínua para outro vaso adjacente para posterior processamento. Além disso, o gás contido no separador é normalmente comprimido e distribuído.

Dentre os perigos potenciais associados a um nível muito baixo de líquido no vaso separador pode ser destacado o fluxo de gás sob alta pressão através do sistema de

bombeamento. Algumas das possíveis conseqüências para esse cenário são:

1. Danos ao sistema de bombeamento;
2. Liberação de gases tóxicos e/ou inflamáveis para a atmosfera;
3. Perda de vidas.

A Função Instrumentada de Segurança analisada opera da seguinte forma: ao se detectar um nível abaixo de um valor limite pré-estabelecido, as válvulas XV-01 e XV-02 são fechadas. Assume-se que uma função de segurança auxiliar assegura a proteção do sistema de bombeamento. Essa função auxiliar não é analisada.

Os valores assumidos para os parâmetros utilizados nos cálculos e as taxas de falha dos equipamentos selecionados são apresentados nas Tabelas 4.7 e 4.8, respectivamente.

Tabela 4.7: Parâmetros utilizados na análise (Caso 3).

Descrição	Parâmetro	Valor
Tempo médio de reparo	MTTR	24h
Tempo de campanha	TC	10 anos
Tempo de Startup	$T_{Startup}$	30h
Intervalo de teste periódico	TI	12 meses
Fator Beta	β	5%
Fator de cobertura de diagnóstico	C	98%

Tabela 4.8: Taxas de falha dos equipamentos utilizados (Caso 3).

Equipamentos	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Transmissor de Nível	-	1,00E-07	-	2,90E-06
CLP de Segurança	1,12E-05	1,35E-07	4,34E-06	2,69E-07
Válvula Solenóide 3 Vias	-	1,01E-06	-	5,85E-07
Válvula Esfera	-	5,00E-07	-	1,27E-06

Na Figura 4.29 é apresentada a tela de resultados para a análise realizada para o estudo de caso 1.

Na Tabela 4.9 é apresentada uma comparação entre os resultados obtidos a partir do uso do software desenvolvido e os resultados obtidos através do uso do software de análise de confiabilidade exSILentia do fabricante Exida.

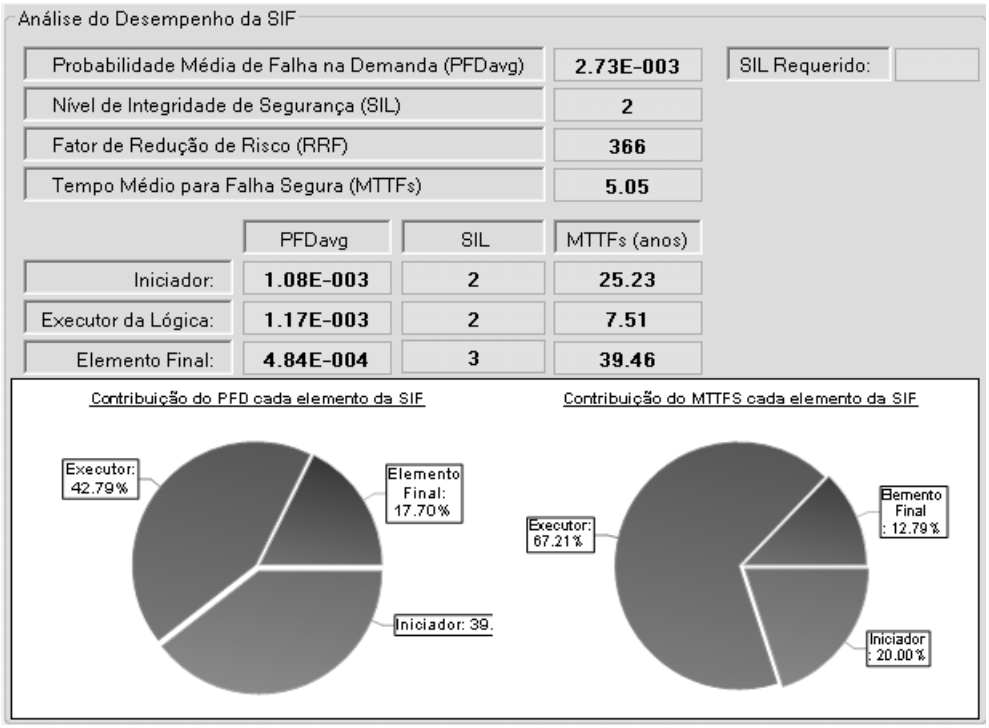


Figura 4.29: Tela de resultados para o Estudo de Caso 3.

Tabela 4.9: Comparação entre os resultados obtidos (Caso 3).

	exSILentia		BR-SIL	
Elementos	PFDavg	MTTFs (anos)	PFDavg	MTTFs (anos)
Elemento Sensor	1,08E-03	24,77	1,08E-03	25,23
Executor da Lógica	1,17E-03	7,31	1,17E-03	7,51
Elemento Final	4,83E-04	39,08	4,84E-04	39,46

4.4 Conclusão

Através das diferentes características apresentadas é possível observar que a utilização do software desenvolvido durante a etapa de projeto permite uma simulação bastante flexível e eficiente de diversas configurações de equipamentos e lógicas de votação utilizadas em implementações de SIS. Isso possibilita uma redução no tempo de análise necessário para determinar se o SIL obtido a partir da implementação proposta atinge o nível de redução de risco requerido pelo processo.

Observa-se que os resultados obtidos a partir do uso do software desenvolvido assemelham-se bastante àqueles obtidos através do uso do software utilizado como referência para comparação.

Capítulo 5

Considerações Finais e Conclusões

5.1 Conclusões

A determinação da melhor configuração para um Sistema Instrumentado de Segurança, no que concerne ao nível de redundância necessário para a instalação de equipamentos críticos e a escolha da melhor política de operação e manutenção para a unidade devem ser pautadas em um processo de avaliação de confiabilidade e disponibilidade, baseado na determinação de determinados índices probabilísticos tais como a PFD_{avg} e o $MTTF_S$.

Neste trabalho foi apresentado um software para avaliação de confiabilidade e disponibilidade de Sistemas Instrumentados de Segurança. Desenvolvido para ser utilizado como ferramenta durante a etapa de projeto de SIS de unidades da Petrobras, o software permite avaliar de forma bastante flexível e eficiente diversas configurações de equipamentos e lógicas de votação possíveis, proporcionando considerável redução do tempo despendido nesse processo.

O software conta com um algoritmo de cálculo baseado no método de análise de Markov. Isso, aliado ao conjunto de modelos desenvolvidos, possibilita a obtenção de resultados bastante precisos.

Verificou-se que uma base de dados atualizada é essencial para uma análise probabilística precisa e coerente do SIS. A utilização de uma base de dados genérica retirada de publicações fornecidas por fabricantes de equipamentos pode levar a resultados incoerentes e muito otimísticos. Isso se deve ao fato de os dados de falha serem obtidos a partir de ensaios em laboratório, sob condições de operação diferentes daquelas observadas em campo. Dessa forma, a utilização de uma base de dados específica, obtida a partir de um acompanhamento das falhas identificadas

nas unidades ao longo dos anos, tende a reduzir a incerteza da análise.

Por fim, os resultados obtidos e a adoção e utilização por parte da Petrobras comprovam a qualidade do software desenvolvido.

5.2 Propostas de Trabalhos Futuros

Possíveis avanços na linha de pesquisa incluem o estudo da combinação do método de análise de Markov apresentado neste trabalho com outros métodos existentes, como forma de possibilitar a representação de cenários mais complexos, e o estudo de técnicas para reduzir o incremento do esforço computacional resultante desse aumento de complexidade.

Outra alternativa seria incorporar ao software desenvolvido um mecanismo de geração automática dos modelos de Markov utilizados na representação dos cenários analisados.

Referências Bibliográficas

AICHE, C. for C. P. S. *Guidelines for Safe Automation of Chemical Processes*. NY: New York: American Institute of Chemical Engineers, 1993.

BUKOWSKI, J. V. Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Transactions of Reliability*, v. 50, n. 3, 2001.

BUKOWSKI, J. V. A comparison of techniques for computing pfd average. *IEEE RAMS*, v. 50, n. 3, 2005.

BUKOWSKI, J. V.; GOBLE, W. M. Using markov models for safety analysis of programmable electronic systems. *ISA Transactions*, v. 34, 1995.

BUKOWSKI, J. V.; LELE, A. The case for architecture-specific comon cause failure rates and how they affect system performance. *Proceedings of the Annual Reliability and Manitainability Sysposium. IEEE*, 1997.

EXIDA. *Safety Equipment Reliability Handbook*. [S.l.]: EXIDA, 2003.

GOBLE, W. M. *Control Systems Safety Evaluation and Reliability*. NC: Research Triangle Park: ISA, 1998.

GOBLE, W. M.; BUKOWSKI, J. V. Defining mean time-to-failure in a particular failure-state for multi-failure-state systems. *IEEE Transactions on Reliability*, v. 50, n. 2, 2001.

GOBLE, W. M.; BUKOWSKI, J. V. Verifying common cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model. *ISA Transactions*, v. 40, 2001.

GOBLE, W. M.; BUKOWSKI, J. V.; BROMBACHER, A. C. How diagnostic coverage improves safety in programmable electronic systems. *ISA Transactions*, v. 36, n. 4, p. 345–350, 1998.

GOBLE, W. M.; CHEDDIE, H. L. *Safety Instrumented System Verification: Pratical Probabilistic Calculation*. NC: Research Triangle Park: ISA, 2005.

GULLAND, W. G. *Repairable Redundant Systems and the Markov Fallacy*. [S.l.], 2003.

GUO, H.; YANG, X. A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety*, v. 92, 2007.

GUO, H.; YANG, X. Automatic creation of markov models for reliability assessment of safety instrumented systems. *Reliability Engineering and System Safety*, v. 93, 2008.

IEC. *Functional Safety of Electrical / Electronic/ Programmable Electronic Safety-related Systems*. Geneva: Switzerland, 2000.

ISA. *Application of Safety Instrumented Systems for the Process Industries*. NC: Research Triangle Park, 1996.

KNEGTERING, B.; BROMBACHER, A. C. Application of micro markov models for quantitative safety assessment to determine safety integrity levels as defined by the iec 61508 standard for functional safety. *Reliability Engineering and System Safety*, v. 66, 1999.

LIMA, M. L. de; SAITO, K. Quantitative analysis fot the design of safety instrumented system architecture. *ISA Expo*, 2003.

M., H.; GOBLE, W. M.; BROMBACHER, A. C. Creating markov models for applications in the process industry. *Proceedings of the 15th international conference on computer safety, reliability and security, SAFECOMP´96*, 1996.

ROUVROYE, J. L.; BLIEK, E. G. van den. Comparing safety analysis techniques. *Reliability Engineering and System Safety*, v. 75, 2002.

ROUVROYE, J. L.; BROMBACHER, A. C. New quantitative standards: different techniques, differentes results? *Reliability Engineering and System Safety*, v. 66, n. 2, p. 121–125, 1999.

SIMPSON, K. G. L.; KELLY, M. *Reliability Assessments of Repairable Systems - Is Markov Modelling Correct?* [S.l.], 2003.

SUMMERS, A. Viewpoint on isa tr84.0.02 - simplified methods and fault tree analysis. *ISA Transactions*, v. 39, n. 2, p. 125–131, 2000.

Apêndice A

Guia de Usuário BR-SIL

Este documento constitui um guia rápido para utilização do software BR-SIL.

A.1 Estrutura do BR-SIL

A estrutura do software foi desenvolvida visando a integração em uma única ferramenta das três fases da análise de segurança de SIFs (Seleção do SIL, Especificação dos Requisitos de Segurança e Verificação do SIL).

A Tela Principal do software é mostrada a seguir:

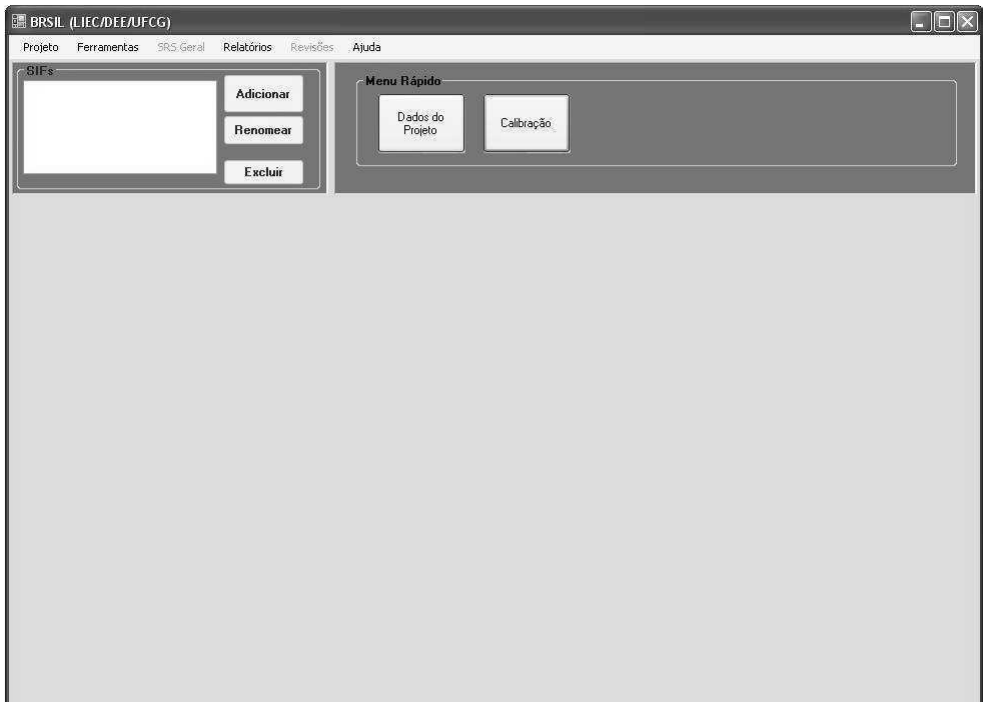


Figura A.1: Tela Principal do BR-SIL

A.2 Projetos

A.2.1 Criando um Novo Projeto

Para criar um Novo Projeto o usuário deve selecionar a opção de menu **Projeto>Novo**.

Figura A.2: Criando um Novo Projeto

Será exibida a Tela Novo Projeto apresentada na figura A.3. Por meio desta tela o usuário deverá inserir as informações referentes ao novo projeto.

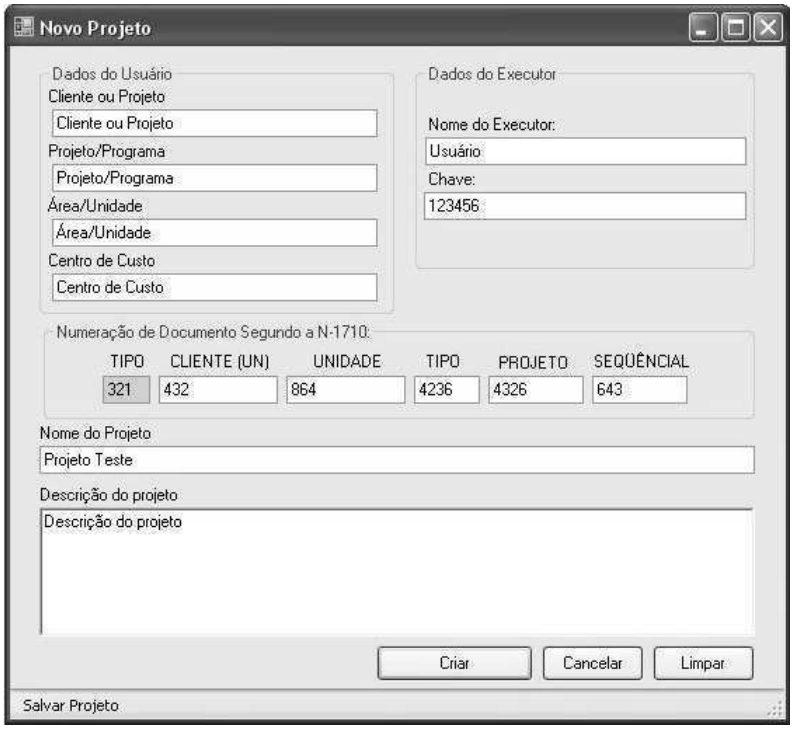


Figura A.3: Tela de Edição de Informações do Novo Projeto

Caso deseje o usuário pode cancelar a operação e retornar para a Tela Principal do programa clicando em Cancelar.

A.2.2 Abrindo um Projeto

Caso o usuário deseje acessar um projeto previamente salvo, deve-se selecionar a opção de menu **Projeto>Abrir Projeto**.

Figura A.4: Abrir um Projeto Salvo

Será então exibida a tela Listagem de Projetos, na qual o usuário deverá selecionar o projeto desejado dentre os projetos listados e clicar em Abrir. A tela Listagem de Projetos é apresentada a seguir:

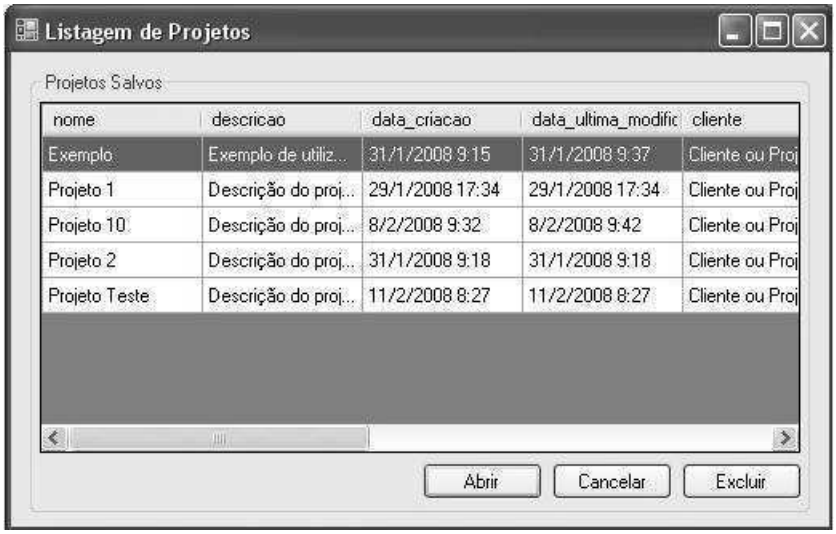


Figura A.5: Listagem dos Projetos Salvos

Caso deseje o usuário pode cancelar a operação e retornar para a Tela Principal do programa clicando em Cancelar.

A.2.3 Excluindo um Projeto

A exclusão de um projeto salvo também é realizada por meio da Tela Listagem de Projetos, apresentada na figura A.5. Para tal basta que o usuário selecione o projeto que deseja descartar e clique em Excluir. Logo em seguida será solicitado ao usuário que confirme a operação.

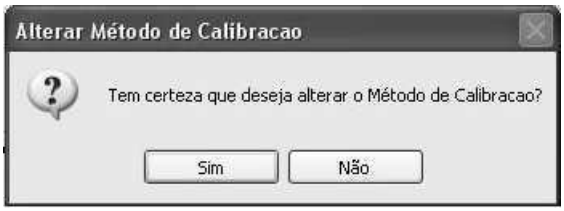


Figura A.6: Confirmação de Exclusão do Projeto Selecionado

É importante ressaltar que após a confirmação da operação de exclusão de um projeto, todas as informações referentes ao projeto excluído são permanentemente apagadas do bando de dados do BR-SIL não podendo, portanto, serem recuperadas.

A.3 Funções Instrumentadas de Segurança

A.3.1 Adicionando uma SIF ao Projeto

Cada projeto pode conter um número ilimitado de SIFs, que são listadas em um campo existente na Tela Principal conforme apresentado na figura a seguir:

Figura A.7: Lista das SIFs adicionadas

Após realizada a etapa de calibração do Risco Tolerável o usuário estará apto a adicionar SIFs ao projeto. Isto é feito clicando-se no botão Adicionar localizado no campo SIFs na Tela Principal (Figura A.8).

Figura A.8: Criando uma SIF

Na caixa que será exibida o usuário deverá inserir o nome da nova SIF e clicar em OK. Imediatamente após isso o nome da SIF criada será adicionado à lista de SIFs que compoem o atual projeto e será exibida na parte inferior da Tela Principal a Tela de edição das informações referentes à SIF criada (Figura A.10).

Figura A.9: SIF Adicionada

Para renomear uma SIF o usuário deverá seleciona-la na lista de SIFs e clicar no botão Renomear. Na caixa que será exibida o usuário deverá inserir o novo nome da SIF e clicar em OK.

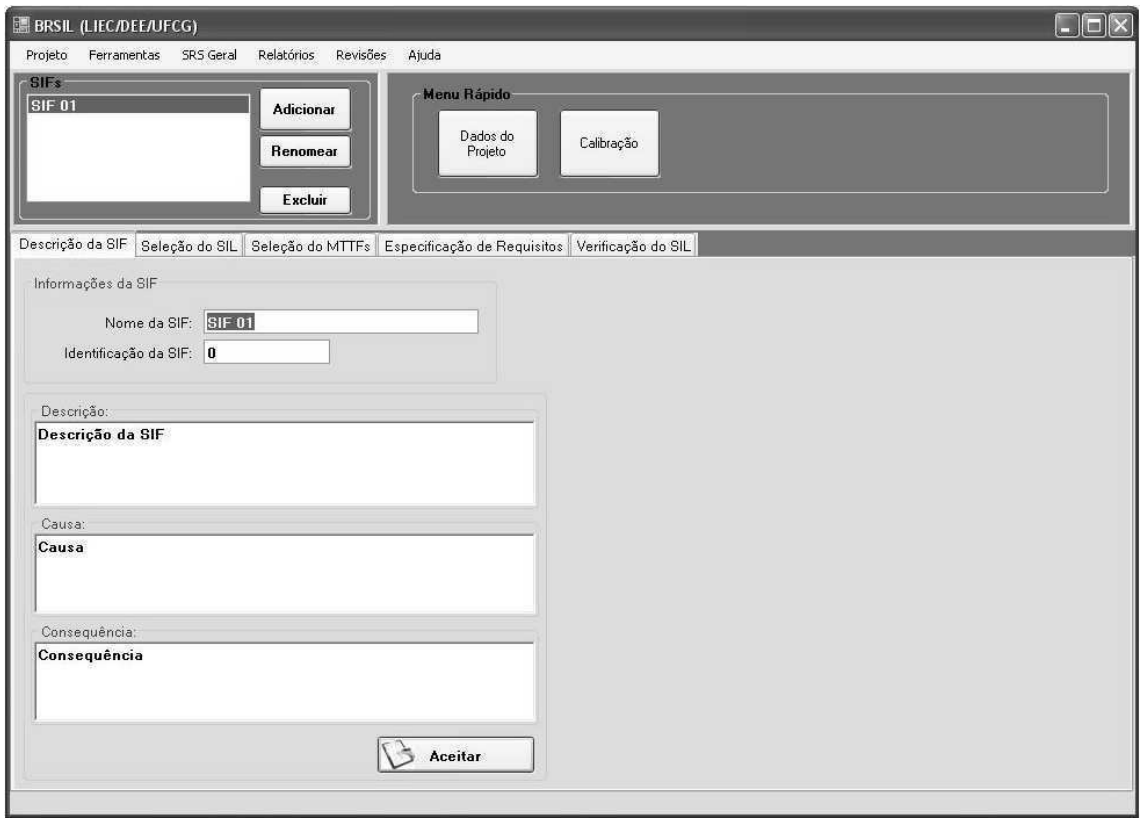


Figura A.10: Descrição da SIF

A.3.2 Descrição da Nova SIF

Na aba Descrição da SIF pertencente à tela de edição das informações da SIF o usuário poderá atribuir uma identificação e descrever a SIF em questão, bem como fornecer informações referentes à Causa e Consequência.

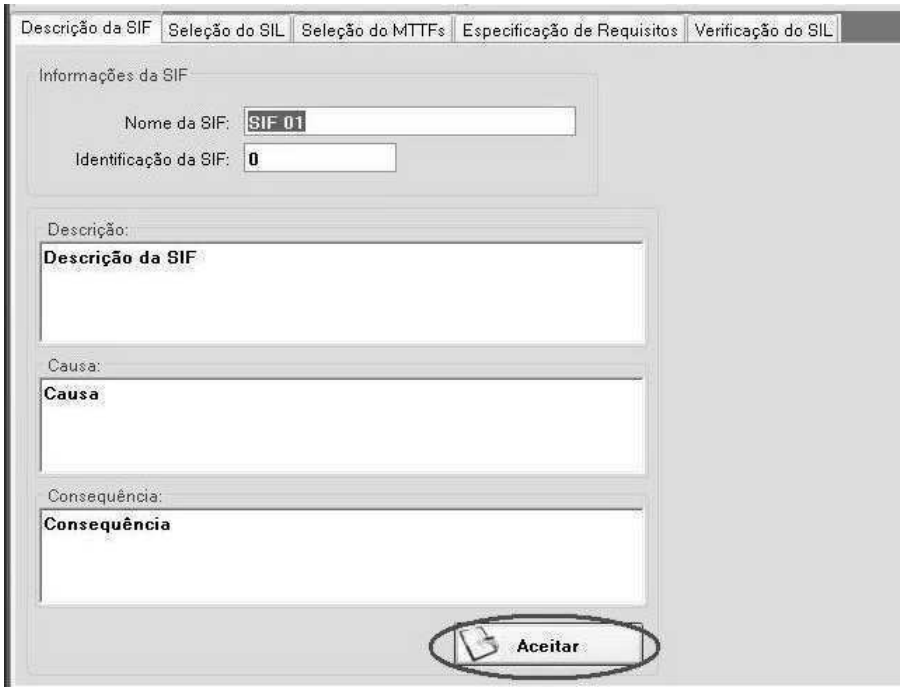


Figura A.11: Descrição da SIF

A.4 Verificação do SIL

Esta seção irá mostrar como percorrer todas as etapas do processo de verificação do SIL obtido com uma determinada configuração adotada para a SIF.

A.4.1 Estrutura da Aba Verificação do SIL

As três partes que compõem uma SIF são Sensor, Executor da Lógica e Elemento Final. O BR-SIL utiliza uma estrutura em árvore onde cada tópico corresponde a uma das três partes da SIF. Com isto buscou-se facilitar a visualização das partes que compõem a SIF, e guiar o usuário através das etapas do processo de verificação do SIL (Figura A.12).

Ainda segundo essa estrutura, cada parte da SIF é formada por Grupos, e cada Grupo é composto por Elementos. O BR-SIL permite que o usuário cadastre até 3 grupos para cada elemento da SIF (Sensor e Elemento Final). Cada Grupo pode ser composto por um número máximo de 3 Elementos. O esquema de votação adotado corresponde ao número de Grupos e de Elementos. As opções de votação disponíveis são 1oo1, 1oo2, 2oo2, 1oo3, 2oo3 e 3oo3 entre Elementos e 1oo1, 1oo2, 2oo2, 1oo3 e 3oo3 entre Grupos.

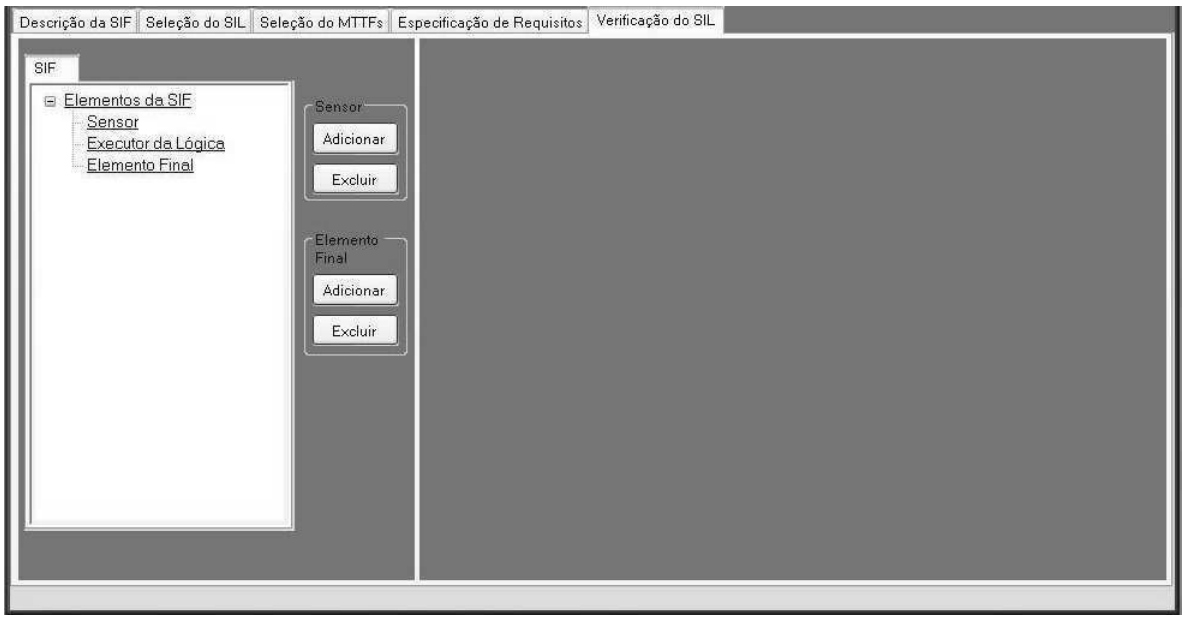


Figura A.12: Estrutura da Aba Verificação do SIL

A.4.2 Passo 1: Criando um Grupo Sensor

Na aba Verificação do SIL clique no botão Adicionar no campo Grupo Sensor. O usuário irá verificar que um novo tópico será inserido logo abaixo do tópico Sensor (Figura A.13).

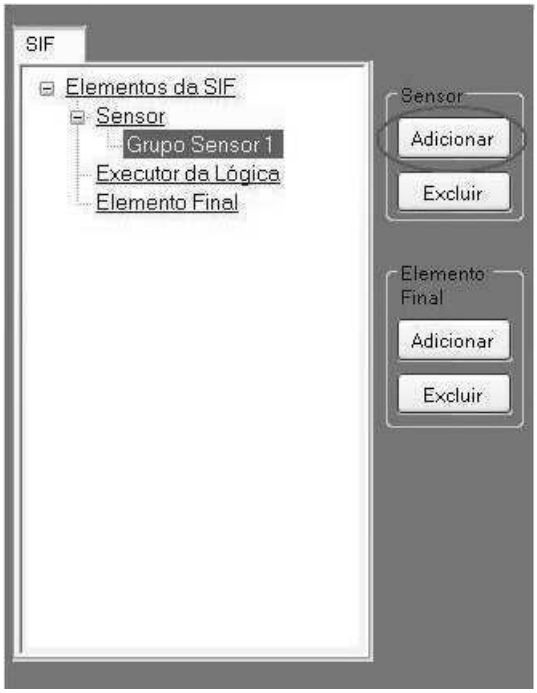


Figura A.13: Criando um Grupo Sensor

Na árvore de navegação da SIF selecione o Grupo Sensor criado para exibir o painel de configuração correspondente (Figura A.14). Esse painel apresenta os seguintes campos:

•**Descrição do Grupo** - Breve descrição para identificação do Grupo Criado;

•**Votação** - Votação que será utilizada entre os Elementos do Grupo;

•**Parâmetros** - Parâmetros de Confiabilidade;

•**Elementos** - Lista os Elementos que pertencem ao Grupo.

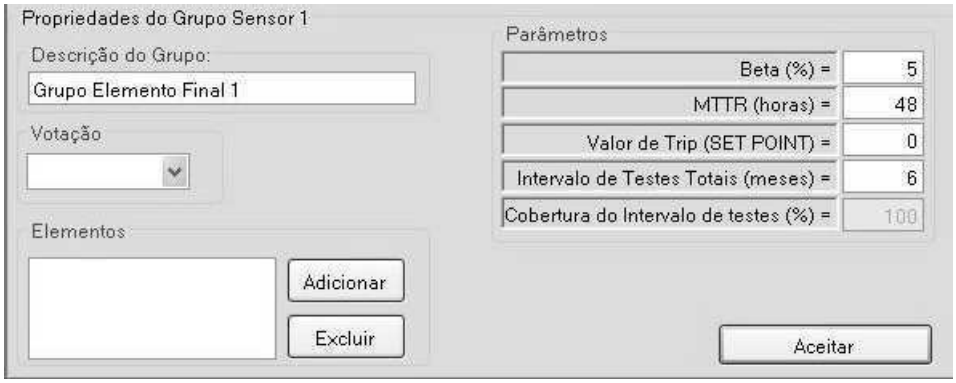


Figura A.14: Editando as informações do Grupo Sensor

Para o Grupo Sensor o usuário poderá especificar os seguintes parâmetros:

•**Fator Beta -** β **(%)**

O Fator Beta é o percentual de falhas devido à causa comum. O Fator Beta deve ser um número entre 0 e 100%. Consulte a seção A.5 para ajuda na determinação do Fator Beta Apropriado.

O campo referente ao Fator Beta só é habilitado quando existe mais de um Elemento no Grupo Sensor).

•**Tempo Médio para Reparo - MTTR (Horas)**

O MTTR indica o tempo esperado para se reparar os equipamentos do Grupo no caso de uma falha ser detectada. O MTTR deve ser um número inteiro entre 4 e 336 horas.

•**Intervalo de Testes - TI (Meses)**

Os Testes são inspeções periódicas realizadas para se detectar falhas em um sistema de segurança, de forma que, se necessário, o sistema possa ser restaurado para uma condição totalmente operacional, tal qual um equipamento novo.

O Intervalo de Testes é o intervalo de tempo entre dois Testes. Ele deve ser um número inteiro entre 1 e 360 meses.

•**Fator de Cobertura do Diagnóstico - CPT (%)**

O Fator de Cobertura do Diagnóstico indica a eficiência desses Testes. Um valor de 100% significa que 100% das falhas perigosas seriam detectadas no Teste. O Fator de Cobertura deve ser um valor inteiro entre 0 e 100%.

Em seguida o usuário deverá definir os Elementos que farão parte do Grupo Sensor.

A.4.3 Passo 2: Criando um Elemento Sensor

Para criar um Elemento clique no botão Adicionar localizado no campo Elementos do painel de configuração do Grupo Sensor (Figura A.15). Os Elementos criados são listados na tela. Basta selecionar um dos Elementos criados para que o painel de configuração correspondente será exibido (logo abaixo do painel de configuração do Grupo Sensor).

O painel de configuração do Elemento Sensor apresenta os seguintes campos:

•**Tipo de Medição** - Tipo de medição que será realizada. As opções disponíveis são: Pressão, Vazão, Nível e Temperatura.

•**Sensor** - Equipamento Sensor que será utilizado. Os ítens serão exibidos nesse campo em função do tipo de medição selecionado.

•**Tipo de Conexão ao Processo** - Tipo de conexão utilizada para conectar o equipamento sensor ao processo. As opções disponíveis são exibidas em função do tipo de medição selecionado.

•**Interface** - Equipamento de Interface que será utilizado.

•**Configurações** - Informações que definem o funcionamento do equipamento sensor e como este interage com o executor da lógica.

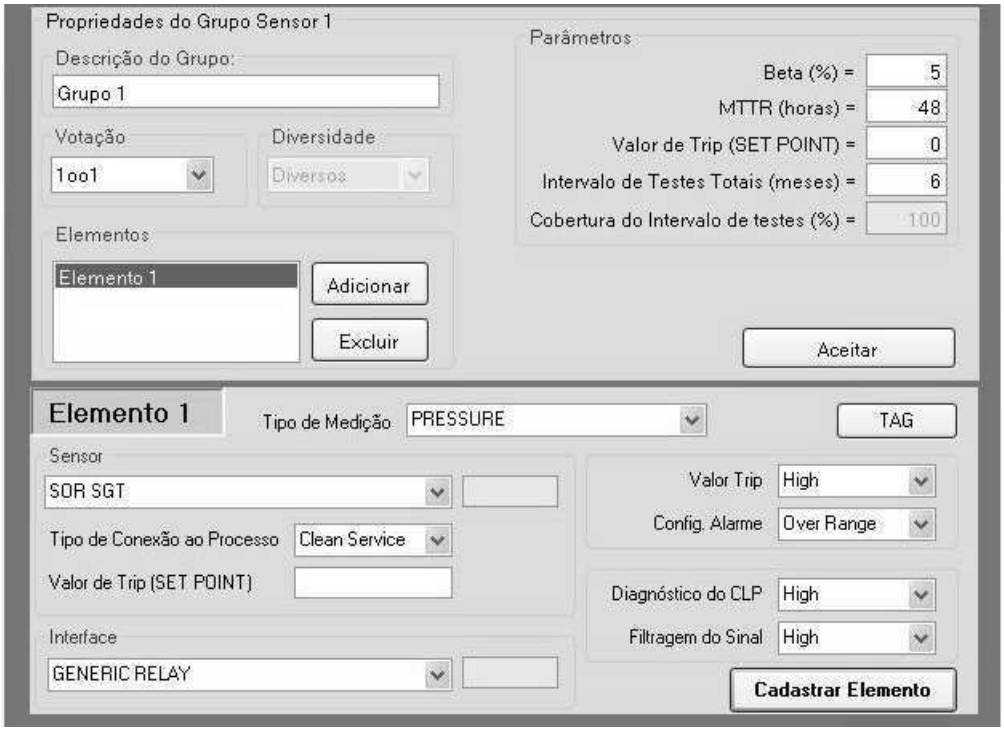


Figura A.15: Editando as informações do Elemento Sensor

Para visualizar o resultado obtidos para o Grupo que foi definido, o usuário deverá selecionar o tópico Sensor na árvore da SIF (Figura A.16). Será exibida uma tela com os resultados, conforme apresentado na Figura A.16.

Figura A.16: Visualização dos Resultados do Grupo Sensor

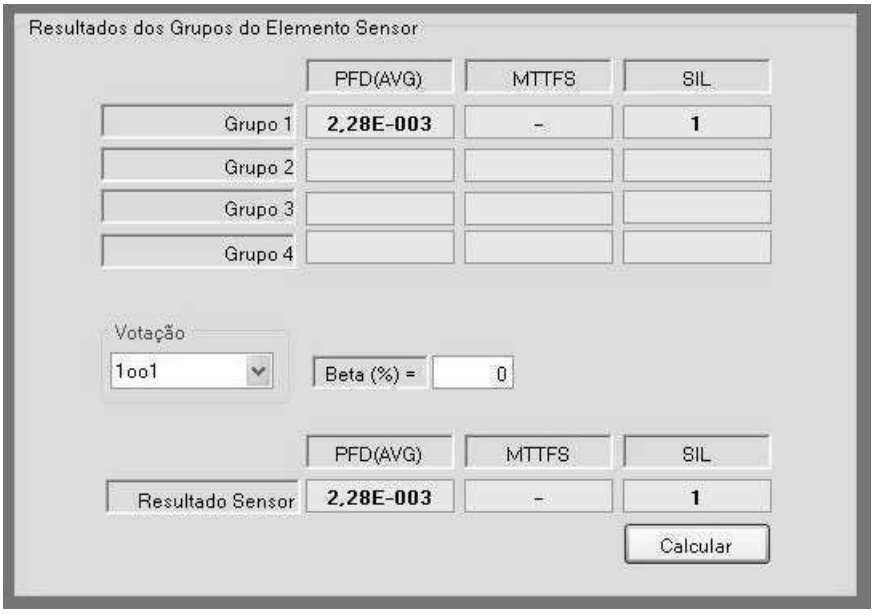


Figura A.17: Resultados do Grupo Sensor

A.4.4 Passo 3: Inserindo Informações do Executor da Lógica

Para inserir as informações referentes ao Executor da Lógica o usuário deverá selecionar o tópico Executor da Lógica na árvore de navegação da SIF (Figura A.18). Será exibido o painel de configuração apresentado na Figura A.19.

Figura A.18: Executor da Lógica

No campo Dados do Elemento Executor o usuário poderá especificar os parâmetros de confiabilidade de forma semelhante ao apresentado para o Grupo Sensor (ver Passo 1) e selecionar um equipamento cadastrado na base de dados do BR-SIL. O equipamento selecionado pelo usuário apresentará uma configuração de hardware padrão, com CPU, Fonte de Alimentação e um número definido de módulos diversos.

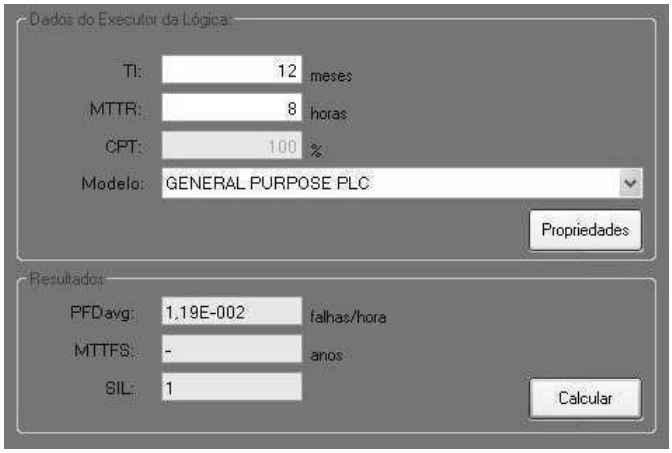


Figura A.19: Configurando o Executor da Lógica

A.4.5 Passo 4: Criando um Grupo Elemento Final

Na aba Verificação do SIL clique no botão Adicionar no campo Grupo Elemento Final. O usuário irá verificar que um novo tópico será inserido logo abaixo do tópico Elemento Final (Figura A.20).

Figura A.20: Criando um Grupo Elemento Final

Na árvore de navegação da SIF selecione o Grupo Elemento Final criado para exibir o painel de configuração correspondente (Figura A.21). Esse painel apresenta os seguintes campos:

•**Descrição do Grupo** - Breve descrição para identificação do Grupo Criado;

•**Votação** - Votação que será utilizada entre os Elementos do Grupo;

•**Parâmetros** - Parâmetros de Confiabilidade;

•**Elementos** - Lista os Elementos que pertencem ao Grupo.

Para o Grupo Elemento Final o usuário poderá especificar os seguintes parâmetros:

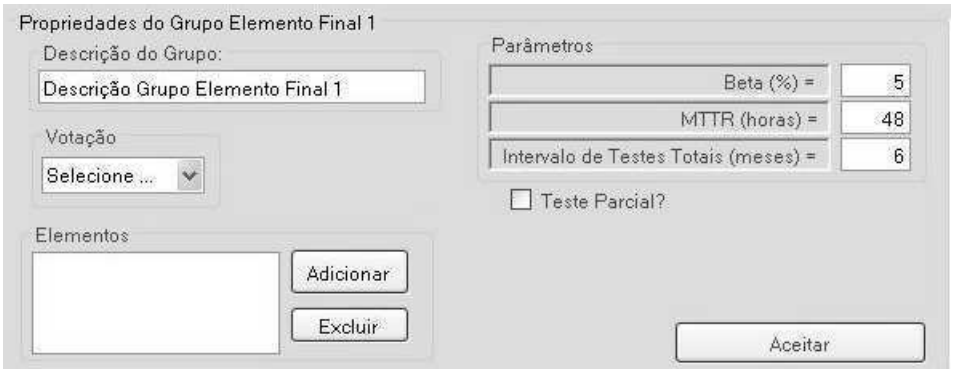


Figura A.21: Editando as informações do Elemento Final

•**Fator Beta - β (%)**

O Fator Beta é o percentual de falhas devido à causa comum. O valor do Fator Beta deve ser um número inteiro entre 0 e 100%. Consulte a seção A.5 para ajuda na determinação do Fator Beta Apropriado.

•**Tempo Médio para Reparo - MTTR (Horas)**

O MTTR indica o tempo esperado para se reparar os equipamentos do Grupo no caso de uma falha ser detectada. O MTTR deve ser um número inteiro entre 4 e 336 horas.

•**Intervalo de Testes - TI (Meses)**

Os Testes são inspeções periódicas realizadas para se detectar falhas em um sistema de segurança, de forma que, se necessário, o sistema possa ser restaurado para uma condição totalmente operacional, tal qual um equipamento novo.

O Intervalo de Testes é o intervalo de tempo entre dois Testes Totais. Ele deve ser um número inteiro entre 1 e 360 meses.

O campo referente ao Fator Beta de Causa Comum só é habilitado quando existe mais de um Elemento no Grupo Elemento Final). O valor do Fator Beta deverá corresponder a um número inteiro compreendido entre 0 e 100%.

Em seguida o usuário deverá definir os Elementos para compor o Grupo Elemento Final.

A.4.6 Passo 5: Criando um Elemento Final

Para criar um Elemento clique no botão Adicionar localizado no campo Elementos do painel de configuração do Grupo Elemento Final (Figura A.21). Os Elementos

criados são listados na tela. Basta selecionar um dos Elementos criados para que o painel de configuração correspondente será exibido (logo abaixo do painel de configuração do Grupo Elemento Final).

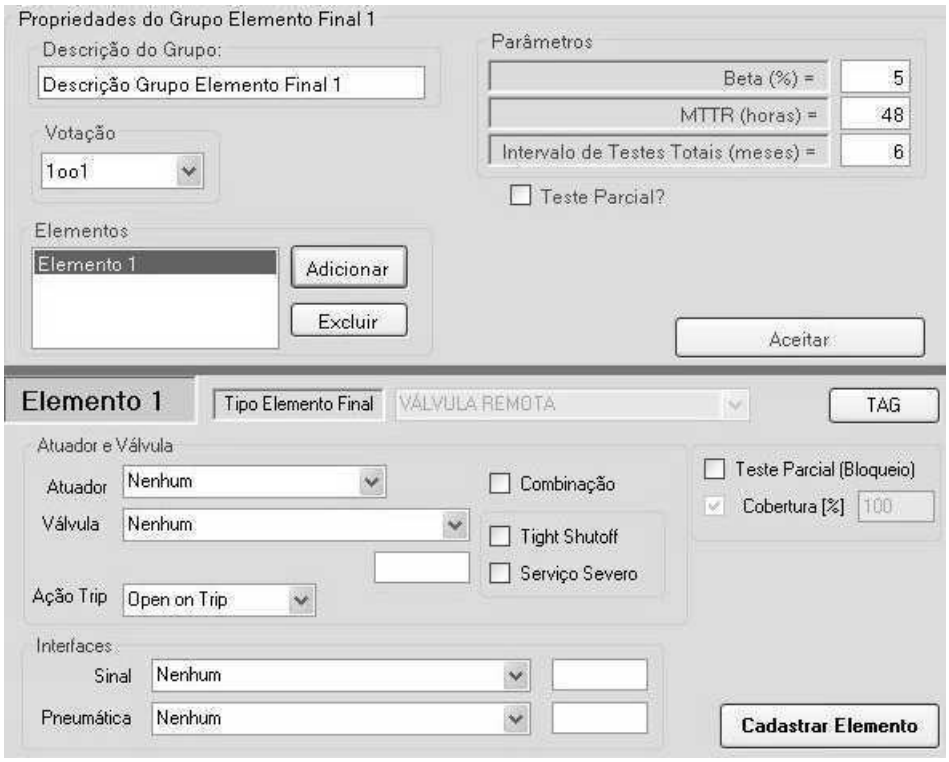


Figura A.22: Editando as informações do Elemento Final

O painel de configuração do Elemento Final apresenta os seguintes campos:

- **Tipo de Elemento Final**
- **Atuador**
- **Válvula**
- **Interfaces**
- **Configurações**

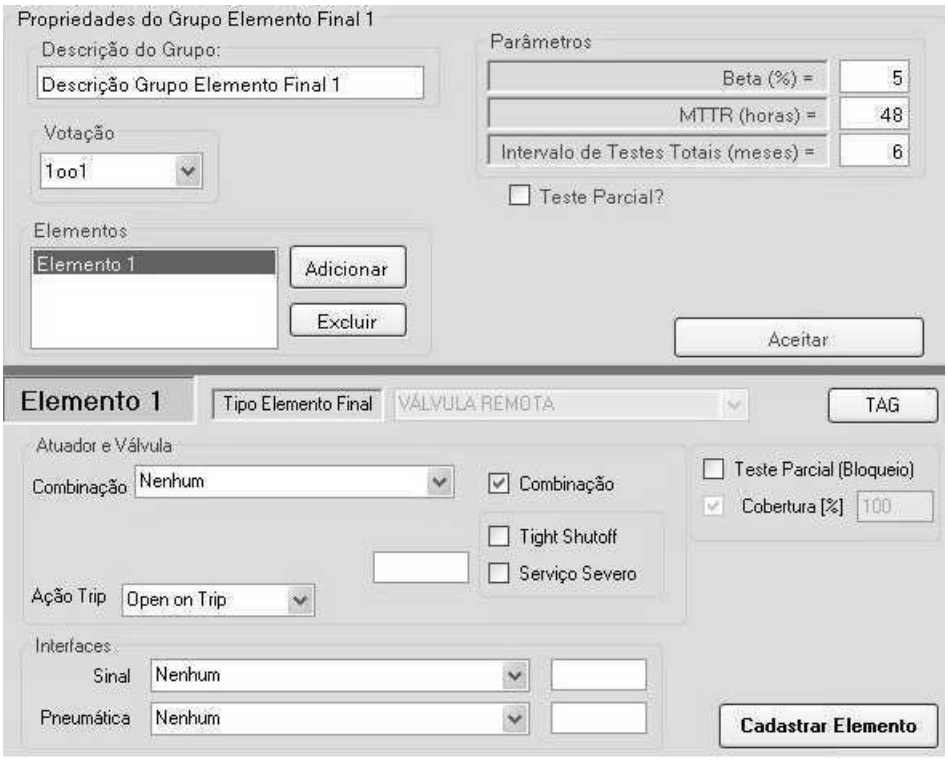
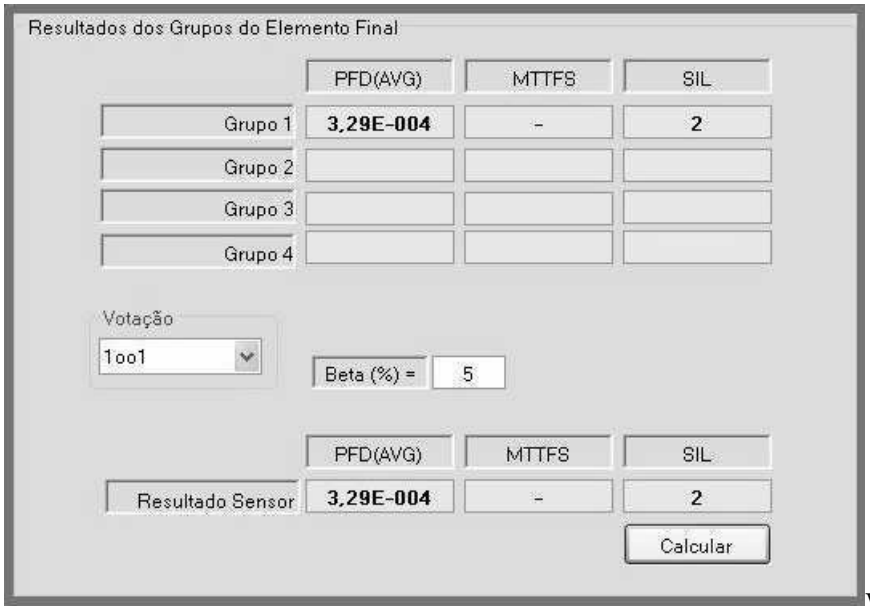


Figura A.23: Editando as informações do Elemento Final - Combinação

Para visualizar o resultado obtidos para o Grupo que foi definido, o usuário deverá selecionar o tópico Elemento Final na árvore da SIF (Figura A.24). Será exibida uma tela com os resultados, conforme apresentado na Figura A.25.

Figura A.24: Visualização dos Resultados do Elemento Final



w

Figura A.25: Resultados Elemento Final

A.4.7 Passo 5: Visualizando os Resultados

Após a especificação de todas as partes componentes da SIF, o usuário poderá visualizar os resultados finais dos cálculos realizados e conferir se os valores obtidos encontram-se de acordo com os nível de integridade desejado. Para tal, o usuário deverá selecionar a opção Elementos da SIF localizada no topo da árvore SIF, conforme apresentado na Figura A.26.

Figura A.26: Visualização dos Resultados da SIF

Será exibida uma tela correspondente à Figura A.27.

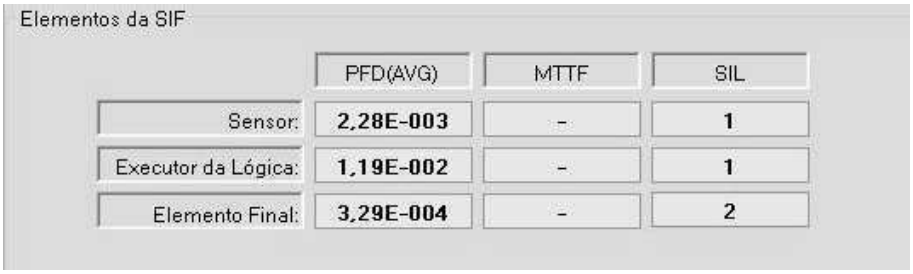


Figura A.27: Resumo dos Resultados da SIF

A.5 Ferramenta para estimar o Fator Beta

Outra funcionalidade incorporada no BR-SIL é o estimador BETA, que funciona como uma calculadora que determina o fator de cobertura BETA utilizado na verificação do SIL através do preenchimento de um formulário simples. Para ter acesso a esta ferramenta basta clicar no menu Ferramentas>Estimador BETA. Na Figura A.28 é apresentada a tela referente a esta ferramenta.

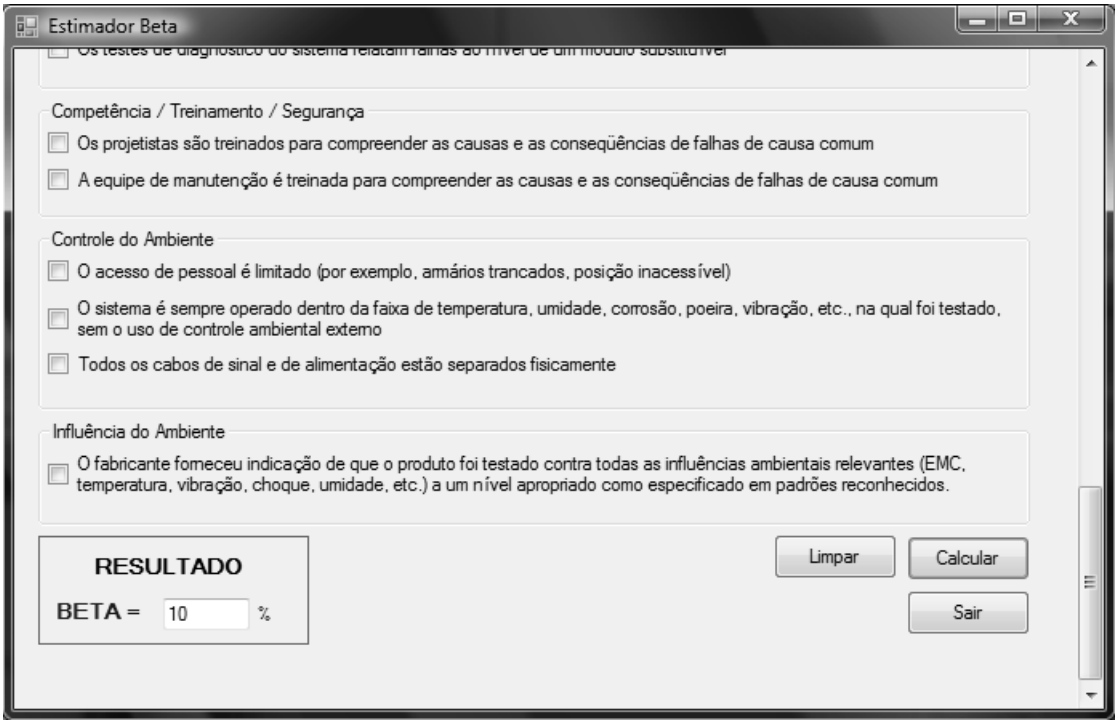


Figura A.28: Ferramenta para estimar o Fator Beta